NORTEL NETWORKS

Nortel Networks Multiservice Switch 15000 in Succession Networks

Replacing an OC-3/STM-1 FP

PT-AAL1/UA-AAL1

NN10254-913

Nortel Networks Multiservice Switch 15000 in Succession Networks

Replacing an OC-3/STM-1 FP

PT-AAL1/UA-AAL1

Publication: NN10254-913
Document status: Standard
Document version: (I)SN07S1
Document date: September 2004

Printed in Canada

Publication history

September 2004

(I)SN07S1 Standard
Contains standard information for the (I)SN07 FCS release

Contents

List of figures

List of tables

About this document

The following topics are discussed in this section:

Who should read this document and why

This document is intended for people who are replacing an optical function processor (FP) card that is installed in a Nortel Networks Multiservice Switch 15000 shelf, which is part of a Packet Trunking - AAL1 (PT-AAL1) or a Universal Access (UA-AAL1) solution.

What you need to know

ATTENTION Before replacing the optical FP, read through this entire document to ensure that you understand the tasks involved and you prevent unintentional services outages.

Before replacing an optical FP, you must clearly understand the potential impacts to traffic caused by removing the card from the shelf by reviewing your Network Specification book. This book identifies the connections configured on the card and the card's sparing situation.

In addition, you need to understand the architecture of the Succession portfolio by reviewing NN10320-100 *ATM Solutions Basics*. You also need to understand how the Nortel Networks Multiservice Switch 15000 node was configured to accommodate the Succession architecture by reviewing the NN10114-511 *Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP*.

To perform the procedures discussed in this document, you must have an extensive knowledge of Multiservice Switch software.

How this document is organized

This document presents a detailed flow chart of the specific tasks required to replace an optical FP on Nortel Networks Multiservice Switch 15000 devices that are part of a PT-AAL1 or a UA-AAL1 solution. The specific procedures you must do to complete these tasks are presented in the supporting sections.

This document contains the following sections:

- "Optical FP replacement overview" (page 17)
- "Determining the status of an optical FP" (page 19)
- "Switching far-end traffic to the mate FP" (page 29)
- "Replacing an optical FP" (page 61)
- "Removing an FP from service" (page 37)
- "Returning the FP to service" (page 81)

Document terminology

This document uses the following terms for the card replacement procedures:

- Target FP refers to the function processor to be replaced.
- Mate FP refers to the FP that is to support all services while the target FP is being replaced.

What's new in this document

There were no new features added to this document.

Text conventions

This document uses the following text conventions:

- `nonproportional spaced plain type`

  Nonproportional spaced plain type represents system generated text or text that appears on your screen.

- **`nonproportional spaced bold type`**

  Nonproportional spaced bold type represents words that you should type or that you should select on the screen.

- *italics*

  Statements that appear in italics in a procedure explain the results of a particular step and appear immediately following the step.

  Words that appear in italics in text are for naming.

- [`optional_parameter`]

  Words in square brackets represent optional parameters. The command can be entered with or without the words in the square brackets.

- <`general_term`>

  Words in angle brackets represent variables which are to be replaced with specific values.

- UPPERCASE, lowercase

  Nortel Networks Multiservice Switch system commands are not case-sensitive and do not have to match commands and parameters exactly as shown in this document, with the exception of string options values (for example, file and directory names) and string attribute values.

- |

  This symbol separates items from which you may select one; for example, ON|OFF indicates that you may specify ON or OFF. If you do not make a choice, a default ON is assumed.

- ...

  Three dots in a command indicate that the parameter may be repeated more than once in succession.

The term absolute pathname refers to the full specification of a path starting from the root directory. Absolute pathnames always begin with the slash (/) symbol. A relative pathname takes the current directory as its starting point, and starts with any alphanumeric character (other than /).

CS2000 MAP terminal text conventions

Commands, parameters, and responses in this document conform to the following conventions:

- Input prompt (>)

  An input prompt (>) indicates that the information that follows is a command:

  ```
  >BSYC
  ```

- Commands and fixed parameters

  Commands and fixed parameters that are entered at an interface are shown in uppercase letters:

  ```
  >BSY CTRL
  ```

- Variables

  The letters or numbers that the variable represents must be entered. Each variable is explained in a list that follows the command string. Variables are shown in lowercase letters:

  ```
  >BSY  CTRL  ctrl_no
  ```

- Responses7

  Responses are shown in the following type style:

  ```
  FP 3 Busy CTRL 0: Command request has been submitted.

  FP 3 Busy CTRL 0: Command passed.
  ```

Related documents

You may need to refer to the following documents while replacing an optical FP:

- NN10600-130 *Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
- NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
- NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
- NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference*
- NN 10225-512 *Nortel Networks Multiservice Switch 15000 and Media Gateway 15000 in Succession Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP*
- NN10070-461 *Upgrading Nortel Networks Multiaservice Switch 15000 in Succession Networks PT-AAL1/UA-AAL1/UA-IP*
- NN10185-461 *Upgrading Preside MDM in Succession Networks*

How to get more help

For information on training, problem reporting, and technical support, see the "Nortel Networks support services" section in the *NN10600-030 Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.

You can also contact Nortel Networks Global Networks Technical Support (GNTS) for advice or assistance.

Chapter 1
Optical FP replacement overview

This section includes the overview for replacing an optical function processor (FP) card, including one in a pair that is configured for dual-FP LAPS operation. A dual-FP LAPS configuration means port-to-port sparing from card-to-card for paired adjacent optical FPs in the same Nortel Networks Multiservice Switch 15000 shelf. Replacing an FP includes

- replacing a failed FP
- upgrading an FP

This document supports replacing all versions of the following Multiservice Switch 15000 optical function processor (FP) cards:

- 4-port OC-3/STM-1 ATM (with PECs NTHR21 or NTHW15)
- 16-port OC-3/STM-1 ATM (with PECs NTHW21 or NTHW31)
- 4-port OC-12/STM-4 ATM (with PECs NTHW11 or NTHW86)

The FP replacement maintains all Succession PT-AAL1 or UA-AAL1 services operating on a dual-FP configuration.

The series of procedures that are required to replace an optical FP are summarized in “Task flow of optical FP replacement” (page 17).

Task flow of optical FP replacement

The high-level sequence of procedures to replace an optical FP that is part of a PT-AAL1 or UA-AAL1 solution are as follows.

Task flow navigation

1 “Determining the status of an optical FP” (page 19)

2 “Switching far-end traffic to the mate FP” (page 29)

3 “Removing an FP from service” (page 37)

4 “Replacing an optical FP” (page 61)

5 “Returning the FP to service” (page 81)

Chapter 2
Determining the status of an optical FP

Before replacing an optical FP, you must gather information on the card type, sparing configuration, and card status. Record this information so that it can be used for other procedures involved with replacing an optical FP.

Comparing the card type of an inserted card and its configured slot

Make sure the card physically inserted in a slot matches the type of card configured for that slot in the system software.

Prerequisites

- Perform the following procedure in operational mode. For more information, see "Operational mode" in NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.

Procedure steps

1. Display the card type of the card inserted in a particular slot:

   ```
   display Shelf Card/<m> insertedcardType
   ```

2. Display the type of card configured for the slot.

   ```
   display Shelf Card/<m> cardType
   ```

   If the configured card type does not match the inserted card type, the processor card does not start and its status LED turns solid amber.

3. Look up the minimum software load for the card type of the product engineering code (PEC) of the inserted card in NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference* to ensure that the vintage of the card is compatible with the vintage of the software. If they are not compatible, decide whether to upgrade the software for the node (a migration) or to replace the FP with a compatible card.

Variable definitions

Variable	Value
<m>	is the slot number of the processor card.

Displaying the software version and features on an FP

An incompatible software load can damage an FP beyond a field repair. Ensure that the software running on the node meets the minimum software requirement for a replacement FP.

Procedure steps

1 Identify and record the software level or PCR that is running on the target FP:

```
display Software AvList
```

2 Identify and record the logical processor type loaded on the target FP:

```
display -p LogicalProcessor/<m> logicalProcessorType
```

Variable values

Variable	Value
<m>	is 2 to 15 for the number of the slot in which the logical processor resides. Slot 0 and slot 1 are reserved for control processors.

Checking the LEDs on each optical FP

Visually inspect the LEDs on the FP and the mate FP to determine their status.

Procedure steps

1. Review the LED status on both the target and the mate FP, and refer to the “Procedure job aid” (page 22) to determine the status of the FP.
2. Verify that the LED on the mate FP is solid green. With dual-FPs in a LAPS configuration, both FPs are active.

   Note: If the LED is not showing a solid green signal, the FP is not in ready to support services switched-over from the mate FP. Review NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* to resolve the problem.

Procedure job aid

LED display	Function processor status
No color (unlit)	No power is reaching the FP.
Solid red	The FP is powered and is either performing self-tests or, after 30 seconds, is faulty. The FP may also be locked.
Slow pulsing red	The FP has passed self-tests but has not yet fully loaded its software.
Slow pulsing green	The FP’s software is fully loaded but not yet activated. It may be initializing or in standby mode.
Fast pulsing green	The FP is running as a standby.
Solid green	The FP is in active service.
Solid amber	The FP is not faulty, but cannot operate. (For example, the FP is not provisioned in software, or the slot was provisioned for one FP type but another type was inserted.)

Determining if alarms are generated for an FP

Before replacing a target FP, verify that the mate FP is ready to assume all services by checking that there have been no alarms raised on the FP.

To monitor which alarms are generated, see the procedure for viewing alarms in the active mode in 241-6001-011 *Preside MDM Fault Management User Guide*, version 14.1 or later.

Procedure steps

1 Verify the alarm status of an FP:

```
display Shelf Card/<m> alarmStatus
```

Note: The Active Alarm List (AALIST) feature must be enabled on the node. See NN10600-561 *Nortel Networks Multiservice Switch 7400/15000/20000 Data Management* for details.

The system indicates that the card has one of the following alarm statuses:

- underRepair
- critical
- major
- minor
- alarmOutstanding

2 If the card has failed, review the *failureCause* attribute value to determine why:

```
display Shelf Card/<m> failureCause
```

The system responds with one of the following values for the failureCause attribute:

- none
- wrongCardType
- notConfigured
- cannotLoadSoftware
- failedSelfTests
- notResponding

- backplaneConnectivityProblem
- unsupportedPecCode

3 Determine if the card is generating a hardware alarm:

```
display Shelf Card/<m> hardwareAlarm
```

The system responds with either the value *none* or *batteryFeedFailure* for the *hardwareAlarm* attribute.

4 Decide if the reason for the alarm is associated with your replacement activities and continue.

If the remedy action is not directly associated with your card replacement, do whichever one has the higher priority for maintaining traffic on that node in your network.

Variable values

Variable	Value
<m>	is 2 to 15 for the number of the slot in which the failed card resides. Slot 0 and slot 1 are reserved for control processors.

Removing from service an optical FP configured with LAPS

Remove from service an optical function processor (FP) that is configured for line automatic protection switching (LAPS) before removing the card.

Prerequisites

- If you are unfamiliar with removing FPs from service, see "Considerations for replacing function processors" in NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.
- Identify from your site records if any private network-to-network (PNNI) links pass through either of the FP pair. The procedure will indicate when to remove the PNNI links from service.
- An FP that supports only intra-card LAPS (single-FP LAPS) has port-to-port sparing on the same card. For this configuration, follow the procedure "Removing from service an unspared FP" in NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.
- Perform the following procedure in operational mode. For more information, see "Operational mode" in NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.

Procedure steps

1 Identify and record the software level or PCR that is running in the node containing the FP. You will need it to label the PCR onto the faceplate of the card.

```
display software avl
```

Note: The response indicates the configured (provisioned) software that is running on the node, not the software that might be loaded on the inactive CP. When removing a card for re-deployment or repair, it is important to know what version of software was running on it.

2 Verify that the card supports LAPS.

```
display -p laps/*
```

If the card was configured for LAPS, the response will indicate a status of the working and protection lines for the card pair you plan to work on.

3 For dual-FP LAPS, there can be ports providing service (active) on both cards so there is no card with a standby status. Identify which card was originally designated as the standby card by entering the command:

```
display Shelf Card/* sps
```

The value under *Card* in the response is the slot number. Under *osiStby*, the value *serv* means that the card is active while *hot* means that the card is the hot standby.

4 Identify which SONET lines are providing service (as opposed to being on hot standby).

```
display laps/* nearendrxactiveline
```

The lines with status *working* are providing service while the lines with *protec* are on hot standby. When *nearEndRequest* indicates

- *signalFailure* it usually means a cable has been cut
- *signalDegrade* it usually means a bit error
- *forcedSwitch* it means a manual switchover was invoked and the mate port is not available

5 Ensure that LAPS is not degraded.

```
display laps/* osiState
```

Under *osiAvail*, determine if any LAPS has a status of *degraded*. If so, you must determine the cause of the degradation and fix it on either card before proceeding with this procedure. Record all port numbers that are degraded, then refer to NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* to do the task to determine FP problems with the procedure on determining the cause of degraded LAPS. Return to this procedure when the degradations are fixed.

CAUTION

Risk of service interruption from a degraded LAPS

You must determine the cause of each degraded LAPS port because a switchover to one means it can remain out of service longer than 50 milliseconds.

6 When removing the card from service for an upgrade or a re-deployment (as opposed to a failure), ensure that traffic is running on the mate FP. If

traffic is not running on the mate before the removal, it is unlikely traffic will run on the replacement FP after the return to service.

a. Verify that the *atmif* is in service and active, and that there are no unexpected ATMIF alarms.

b. Verify that the UNI, PNNI, and IISP links are in service and active.

c. Verify that all connections are up and passing traffic, including VPTs, and that there are no signalling alarms.

7 Check all software alarms that are generated by the node that houses the FP being replaced. Address the remedial action of any alarm involving equipment or software for the FP being replaced.

8 Prepare the far-end ports for the near-end ports being removed from service. This step applies to any FP.

9 If your site records indicated that you have at least one PNNI link passing through the FP to be removed from service, you must first busy or lock the PNNI link at the far end to remove it from service. At the facility level of operation, as opposed to the service level, transfer the PNNI traffic off the target FP to its mate by following the procedure “Switching SONET line protection to the mate FP” in NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.

10 Transfer any traffic from the ports on the near-end target card to the mate card and block the target card and ports from being put into service.

```
lock -force Shelf Card/<m>
```

Note: Whether the card ports are configured as *unidirectional* or *bidirectional*, or as a *revertive* or *non-revertive* mode, the command *lock* handles all associated Multiservice Switch connections. For information about these attributes, refer to “Configuring line and equipment protection for Multiservice Switch 15000 and Multiservice Switch 20000 optical interfaces in NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.

11 Observe the traffic on the active card to ensure it is flowing. Use appropriate test equipment to monitor the cell counts.

12 If the switchover did not occur, abort this procedure and refer to NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* for diagnosing FPs. For FP fiber optic cards with LAPS, if the active (target) and standby (mate) LEDs on the faceplates do not swap within 50 milliseconds, the switchover may not occur.

Variable definitions

Variable	Value
<m>	is the slot number of the standby card configured in this procedure. For information about the command *lock*, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*. Whenever a card is locked, the alarm 7012 0100 is generated. Whenever a standby card is locked, the alarm 7054 0105 is generated. The alarms are described in NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.

Chapter 3
Switching far-end traffic to the mate FP

Switching far-end traffic to the mate function processor (FP) transfers traffic away from the target FP in a dual-FP LAPS configuration. When the far-end of a pair of FPs is not a Nortel Networks Multiservice Switch node, removing a near-end FP from service can adversely affect the service of far-end traffic. That is, when the near-end FPs switch over services, non-Multiservice Switch far-end connections do not automatically switch over and services are lost. This procedure minimizes the loss of far-end traffic of a target FP before removing the FP from service.

If the system has already removed an FP of a dual-FP LAPS configuration from service due to a failure, skip this procedure because traffic has already been dropped.

- "Prerequisites to switching far-end traffic to the mate FP" (page 29)
- "Task flow for switching the far-end traffic to the mate FP" (page 30)

Prerequisites to switching far-end traffic to the mate FP

- Refer to the Network Specification Book to determine which links have been configured and to determine the sparing arrangement for the target FP to be replaced.
- If you experience any problems while switching traffic, contact Nortel Networks Global Networks Technical Support (GNTS).

Task flow for switching the far-end traffic to the mate FP

The task flow for switching the far-end traffic to the mate FP shows you the sequence of procedures required to transfer active traffic away from the target FP. The sequence of procedures is:

1 "Blocking CS2000 traffic to the target FP" (page 30)

2 "Switching MG4000, IW-SPM, or DPT-SPM traffic to the mate FP" (page 32)

3 "Switching SONET line protection to the mate FP" (page 34)

Blocking CS2000 traffic to the target FP

Perform this procedure to block the traffic from CS2000 to the FP to be replaced if the FP has a provisioned AMDI link. If an AMDI link is not assigned to the target FP to be replaced, then proceed to "Switching MG4000, IW-SPM, or DPT-SPM traffic to the mate FP" (page 32).

Prerequisites

- If an AMDI link is present on the target FP, ensure that there is at least one other AMDI link in service (in the same group) which is connected to another card.
- Refer to the Network Specification Book to determine if an AMDI link is configured on the FP card to be replaced. If so, note this AMDI port's slot number, side of shelf (rear or front), device position (upper or lower) and link number (0 or 1).
- If the AMDI link on the target FP is the only one in service, stop and contact Nortel Networks Global Networks Technical Support (GNTS).

Procedure steps

1 From the CI level of the Communication Server 2000, list TABLE XAMDILNK:

```
TABLE XAMDILNK;LIST ALL
```

Record the LINKNO field for the AMDI link as indicated by the previously referenced AMDI port identification.

2 From the CI level of the Communication Server 2000 MAP, list TABLE ATMCONN:

```
TABLE ATMCONN;LIST ALL
```

Record all MG4000 with the same LINKNO as indicated in step 1.

3 From the CI level of the Communication Server 2000 MAP, post the MG4000s that are assigned to the target FP to be replaced as identified in the Network Specification Book, and verify each link's mate CORECONN is in the INSV state:

```
MAPCI;MTC;PM;POST <mg4k_number>;ATMCONN;CORECONN
```

If the mate CORECONN is not indicated as *INSV*, stop and contact Nortel Networks GNTS.

4 From the CI level of the Communication Server 2000 MAP, block the traffic from the CS2000 AMDI link to the target FP:

```
MAPCI;MTC;XAC;AMDI

BSY <Slot> <Side_of_Shelf> <Device_Position>
<link_number> force
```

Variable values

Variable	Value
<Device_ Position>	is upper or lower for the position of the AMDI port
<link_ number>	is 0 or 1 for the link number
<Side_of_ shelf>	is front or rear for the side of the shelf where the AMDI port is located
<Slot>	is the slot number in the CS2000 where IOP or HIOP is inserted

Switching MG4000, IW-SPM, or DPT-SPM traffic to the mate FP

If the node has not already transferred all links to the mate FP, perform this procedure to switch any active traffic running on the MG4000, IW-SPM, and DPT-SPM links from the *providingService* FP to the *hotStandby* FP.

Prerequisites

- The sparing arrangement must provide an FP card to be the mate for the FP to be replaced. These are pairs of cards in adjacent slots (that is, slots 2 and 3, slots 3 and 4) up to and including slots 14 and 15.
- Refer to the Network Specification Book to determine which ATMRM (0 or 1) has been configured for each MG4000, IW-SPM, and DPT-SPM connected to the FP to be replaced.
- Refer to the Network Specification Book to determine what links have been configured on the FP to be replaced.

Procedure steps

1 From the CI level of the Communication Server 2000 MAP, post the SPM device configured on the SONET ports of the FP to be replaced:

```
MAPCI;MTC;PM;POST SPM <PMNo>
```

If the state of both ATMRM (0 and 1) are *INSV*, go to step 2.

If the state of either ATMRM does not indicate its state as *INSV*, stop and contact Nortel Networks GNTS.

2 Identify which ATM RM and carrier is active and which is inactive. At the posted SPM device from step 1, determine which ATM RM is active and inactive by observing the “A” (active) or “I” (inactive) status under the activity column of the MAP display.

If the active ATM RM is working off the target FP, go to step 3.

If the active ATM RM is working off the mate FP, go to step 4.

3 From the CI level of the Communication Server 2000 MAP, protection switch the active unit to the inactive unit:

```
SELECT ATM <x>

PROT
```

```
MANUAL <x> <y>
```

4 For each additional MG4000, IW SPM, and DPT SPM connected to the target FP, repeat step 1 through to step 4.

Variable values

Variable	Value
<PMNo>	is the number of the SPM to be posted
<x>	is 0 or 1 for the number of the active ATMRM that is connected to the SONET ports of the FP to be replaced
<y>	is 0 or 1 (opposite <x>) for the number of the inactive ATMRM that is connected to the SONET ports of the FP to be replaced

Switching SONET line protection to the mate FP

Perform this procedure to transfer the active SONET line (working or protection) from the target FP to be replaced to the mate FP. You must complete this procedure before locking the SONET ports on the FP to be replaced to ensure that there is no impact on services.

Prerequisites

- The sparing arrangement must provide an FP card to be the mate for the FP to be replaced. These are pairs of cards in adjacent slots (that is, slots 2 and 3, slots 3 and 4) up to and including slots 14 and 15.
- Refer to the Network Specification Book to determine which SONET ports are configured on the FP to be replaced.

Procedure steps

1 Display all instances of LAPS currently operating on the node:

```
display -p laps/*
```

Record all of the LAPS instances operating on the FP to be replaced.

2 Determine if there are active SONET lines operating on the FP to be replaced:

```
display laps/<m> nearEndRxActiveLine
```

Record the LAPS instances displayed under *neRxLine*.

3 Switch the active SONET lines from the LP to be replaced to the hotStandby LP.

If the active SONET line is the protection line on the FP to be replaced:

```
switch -protectionToWorking Laps/<m>
```

If the active SONET line is the protection line on the FP to be replaced:

```
switch -workingToProtection Laps/<m>
```

4 Lock each SONET port on the FP to be replaced:

```
lock -force lp/<n> sonet/<p>
```

Note: Check for critical alarms in CS2000 to ensure that all previous steps were done properly.

5 At the far-end node, lock each SONET port connected to the FP to be replaced:

```
lock -force lp/<m> sonet/<o>
```

Note: Check for critical alarms in CS2000 to ensure that all previous steps were done properly.

Variable values

Variable	Value
<m>	is the number of the LAPS instance on the FP to be replaced
<n>	is the number of the logical processor associated with the FP to be replaced
<o>	is the number of the SONET ports configured on the LP to be replaced
<p>	is the number of the SONET ports configured on the LP located on the far-end node

Chapter 4
Removing an FP from service

You must remove an FP from service before you can remove the card from the shelf.

Locking an FP is the prescribed method of removing it from service because it prevents the node from establishing new connections on that card. You must ensure that an FP is locked before you physically remove it from the shelf. If you remove an FP before it is locked, all services and connections supported by that FP are lost and system alarms are generated. Removing the card from service without locking it means some services will not automatically return to service with the card.

If the FP is spared, traffic is diverted to the spare FP when the active FP is locked. Before locking an FP, you should visually inspect the spare FP to verify that the LED is showing a fast flashing green signal, indicating that it is in standby mode and ready to be put into service. If any other signal is displayed, the FP is not in standby mode and the switchover will fail. If other LED patterns are displayed, see NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* for an explanation of these LED patterns and suggested procedures for placing the FP in the appropriate state.

Procedures to remove an optical FP from service

The task of replacing an optical FP involves a coordinated combination of software commands and physical actions. The combination depends on the configuration of the cards.

This section includes the various procedures that are done as part of removing an FP from service, listed alphabetically.

Decommissioning an FP

Decommission an FP if you are re-deploying an FP from one slot to another and the replacement FP for the original slot is a different FP type.

Prerequisites

- Perform the following procedure in provisioning mode.

Procedure steps

1. Set the *cardtype* attribute to none:

   ```
   set Shelf Card/<m> cardType none
   ```

2. If the FP was configured as a spare card, delete the spare card for the LP:

   ```
   set Lp/<n> spareCard !
   ```

3. If the FP was configured as a main card, delete the LP and all associated services. See “Deleting an LP” (page 40).
4. Activate configuration changes. See “Activating configuration changes” (page 76).

Variable definitions

Variable	Value
<m>	is the slot number of the processor card you want to decommission. Nortel Networks Multiservice Switch 15000 node slot numbers start at zero.
<n>	is the number of the LP.

Deleting an LP

Delete an LP by deleting its *LogicalProcessor* (*Lp*) component. When you delete an *Lp* component, you also delete all its subcomponents.

Prerequisites

- You must also delete services that were associated with the deleted Lp component. To delete all associated services simultaneously, use the command *clear -rf prov*. Alternatively, you can delete every associated service individually using the command *delete*.
- If you delete an LP and are left with a processor card with no LP assigned to it, that processor card does not load when you activate your configuration changes.
- If you delete the last LP running a particular software feature, the CP resets when you activate your configuration changes. This situation occurs when the deleted LP uses an LPT that is not used by any other LP and contains a feature not contained by any other currently used LP:
- Perform the following procedure in provisioning mode.

Procedure steps

1 Delete the LP:

```
delete Lp/<n>
```

This command deletes the *Lp* component and all its subcomponents. The number of components deleted appears.

Note: If you have deleted the LP of an active card, the semantic check indicates that the card will reset when you activate the configuration changes. If you have deleted the last LP running a particular software feature, the semantic check also indicates that the CP will reset when you activate the configuration.

Variable definitions

Variable	Value
<n>	is number of the LP you want to delete.

Locking an FP

Lock a function processor (FP) during maintenance or troubleshooting activities to remove it from service. Locking an FP prevents the card from running the software configuration defined in its logical processor (LP). Locking an FP that is in a sparing configuration means the system cannot use it during a card replacement activity.

Prerequisites

- To ensure that the FP shuts down correctly, the associated LP must be unlocked when you lock the card.
- If you are unfamiliar with lock command concepts, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*.
- Before locking an FP in software, ensure that you are aware of the consequences to the far end of the connection. Use your site records (for example, a Network Specification Book) to identify what is connected to the FP at the far end, and then determine the impact of removing the FP from service.
- Before locking the target FP of a protected (spared) pair, determine the status of its mate card using the appropriate procedure in "Determining the status of an optical FP" (page 19).
  - If the status of the card is other than in-service, see "Status LEDs of a CP or FP" for the meaning of the possible LEDs and see NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* for suggested procedures for placing the FP in the appropriate state.
- In a dual-FP inter-card LAPS configuration, manually forcing a switchover causes the mate port to keep the traffic. If the mate port is out of service and the switchover is forced, any traffic on the active port is lost. To prevent loss of traffic from a card replacement that is not due to card failure, you may first have to replace the card that has the most failed ports. When the statuses of a dual-FP LAPS configuration are queried in software, that is the time to decide which card of the pair is to be replaced first.

- If you are locking an FP to prepare it for removal, the procedures in "Removing an FP from service" (page 37) indicate when to use the command in order to minimize the impacts that locking or force locking has on services.
- Perform the following procedure in operational mode.

Procedure steps

CAUTION
Risk of service loss
Forcing an active (in-service) FP into the locked state causes the FP to drop the traffic on the FP, depending on how equipment protection is configured for that FP. If the FP is unspared, all traffic is dropped. If the FP is a spared optical card, up to 50 milliseconds of traffic can be lost. If the FP is a spared electrical card, up to 100 milliseconds of traffic can be lost.

1 Lock the optical FP using the command:

```
lock -force Shelf Card/<m>
```

Variable definitions

Variable	Value
<m>	is the slot number of the function processor card.

Locking a function processor supporting information

All function processors (FPs) should be locked in software prior to removing it from a slot, especially an FP that is configured for equipment protection. Locking an FP

- removes it from service and prevents the node from establishing new connections on that card
- prevents it from running the software configuration defined in its logical processor (LP)

If the FP is currently running an LP, locking the FP puts the card into the shutting down state. The FP stays in the shutting down state until the LP stops running. An LP stops running when you lock it or when some condition causes it to restart (an operator command or an error). After the LP stops running, the FP moves to the locked state.

If you are running certain configured services on the FP, the LP will never stop running, in which case you need to use the *-force* option to lock the card. The *-force* option bypasses intermediate states and immediately moves the FP to the locked state. For spared optical FPs, the *-force* option can cause up to 50 ms of traffic to be dropped. For spared electrical FPs, the *-force* option can cause up to 100 ms or more of traffic to be dropped depending on the type of sparing panel. The amount of dropped traffic also depends on what the card is, what it is configured for, and how much traffic is in progress. The LP restarts only when you restart the function processor card.

The person who will replace the card and the software operator who locks the card must coordinate their efforts to ensure that the FP is locked in software before physically removing the card. If you remove a standby FP before it is locked, the active FP can try to switch over its traffic to it, but will not be able to. All traffic on the active FP can be lost.

Locking a function processor (FP) prevents it from running the software configuration defined in its logical processor (LP). If the processor card is currently running an LP, locking the FP puts the card into the shutting down state. The card stays in the shutting down state until the LP stops running. An LP stops running when you lock it or when some condition causes it to restart (an operator command or an error). After the LP stops running, the FP moves to the locked state.

If you lock an FP that has a defined spare card (is configured for equipment protection), the LP switches over to the standby card. On Nortel Networks Multiservice Switch 15000 FPs, its LED status light is solid red when the card is locked.

> ***Note:*** With line automatic protection switching (LAPS), the status LEDs on the faceplates of paired FPs do not indicate which one is active or standby. For example, both can have solid green LEDs. Before replacing a card that has been configured for LAPS, the standby card must be

identified by software commands. The software query must occur very close to the actual time of card removal to minimize allowing the system to automatically switch over the cards. For information about configuring line equipment protection and manually switching FPs configured for LAPS, see NN10600-550 *Nortel Networks Multiservice Switch 7400/ 15000/20000 Common Configuration Procedures*.

When an FP is configured for equipment protection, locking the standby FP means preventing the standby FP from receiving traffic or being used as a backup. Locking is usually done to the standby FP. When you wish to replace an active FP, for example, for an upgrade or re-deployment, you must consider forcing a manual switchover in software so that the standby FP takes over the active FP's traffic and the two FPs switch activity. Switching activity means the standby becomes the active FP, and the active FP becomes the standby.

The maximum switchover time is 50 milliseconds in the case of optical interfaces and 100 milliseconds for electrical interfaces. After a switchover completes, an in-service standby FP shows a fast-flashing green status LED on its faceplate and it can be locked.

Unlocking an FP causes it to restart, that is, triggers software activities to return the FP to service.

Preparing an active FP for being replaced

The reason for preparing an active FP for being replaced is typically because you are doing an upgrade, downgrade, or re-deployment. With spared cards, it is likely that you have already replaced the standby mate card. Your administration decides whether the active card is also to be replaced.

Prerequisites

- For Nortel Networks Multiservice Switch systems in general, FP maintenance activities with protected cards is always to the standby card. To perform maintenance activities on an active card, it must first become the standby card.
- In a dual-FP LAPS configuration, the mate card must be prepared for being replaced if it is part of an FP upgrade (rather than a failure). The sooner the mate card is prepared for being replaced (becomes the target card), the fewer active connections will be established on that card.
- With electrical FPs, preparing a spared active FP for being replaced means ensuring that the standby FP is ready to accommodate the traffic of the active FP with minimal impact on traffic. When the standby card has already undergone a replacement and has been confirmed to be in-service, this is an opportune time to replace the active mate. Before physically replacing an active mate, its traffic must be switched over to its standby mate so that the mate becomes the active and the active becomes the standby.
- If the FP is unspared, removing it from service drops traffic. The only preparation for an active unspared FP is to choose a period of lowest traffic before removing it from service. If your network was configured to back up the traffic of an unspared FP, removing the FP from service may cause the network to reroute far-end traffic away from the FP. For example, the configuration can have an intra-network card as opposed to an access card, have a node connected to two nodes to split services, or have PNNI links. Your site records should indicate whatever setup the network has.
- For more information on the commands that are used in the following procedure, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*.
- Perform the following procedure in operational mode.

Procedure steps

1. If the card was configured for LAPS, ensure that LAPS is not degraded. (For an electrical FP, skip this step.)

   ```
   display laps/* osiState
   ```

   Under *osiAvail*, determine if any LAPS has a status of *degraded*. If so, you must determine the cause of the degradation. For example, if the mate port is out of service, an active port can be degraded because it cannot be switched over to an out-of-service port. You must fix any degraded *laps* on both cards before performing with this procedure.

2. Check all software alarms that are generated by the node that houses the FP being replaced. All alarms are described in NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.

   For a spared FP, address the remedial action of any alarm indicating that the standby or mate FP is not available to take over the traffic of the active FP.

   For an unspared FP, consider the status of the far end and address the worst problem first.

3. If your site records indicate that the network was configured to back up the traffic of an unspared FP, removing the FP from service may cause the network to reroute far-end traffic away from the FP. For example, the configuration can have an intra-network card as opposed to an access card or have a node connected to two nodes to split services. PNNI links may have been set up to do this. If your site records indicate that one or more PNNI links pass through the FP, busy or lock each of those links at the far end.

4. Verify that the former standby card is now carrying traffic (is in service).

   ```
   display Shelf Card/* sps
   ```

   Record the slot number of the in-service LP.

5. Transfer the traffic from the active card to the standby card and block the system's access to the standby card.

   ```
   lock -force Shelf Card/<m>
   ```

   Whenever a card is locked, the alarm 7012 0100 is generated. Whenever a standby card is locked, the alarm 7054 0105 is generated.

Note: Whether the card ports are configured as *unidirectional* or *bidirectional*, or as a *revertive* or *non-revertive* mode, the command *lock* handles all associated Multiservice Switch system connections at the far end.

6 Observe the status LED on the faceplate of the standby FP. When the switchover completes, its LED cycles to solid green to indicate a successful switchover.

If the LED is other than solid green, the switchover did not occur. Contact your next level of support to determine your next step.

7 Verify that the former standby card is now carrying traffic (is in service).

```
display Shelf Card/* sps
```

Record the slot number of the in-service LP.

8 Observe the traffic on the active card to ensure it is flowing. Use appropriate test equipment to monitor the cell counts.

9 If the switchover did not occur, abort this procedure and refer to NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* for diagnosing FPs.

- For FP fiber optic cards, if the active and standby LEDs on the faceplates do not swap within 50 milliseconds, the switchover may not occur.
- For FP cards with electrical interfaces (such as DS3s, E3s, or E1s), if the active and standby LEDs on the faceplates do not swap within 100 milliseconds, the switchover will not occur. Ensure also that the LED on the sparing panel faceplate for the Spare card is lit to indicate active traffic.

10 If you are performing this procedure as part of an FP replacement, in the NN10600-130 *Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*, perform the procedures for replacing a spared (standby) FP.

If you are performing this procedure as part of testing an FP protected pair, or for any other reason, return to the task that sent you.

Variable definitions

Variable	Value
<m>	is the slot number of the active card. For information about the command *lock*, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*.

Removing from service a failed FP

Confirm a function processor (FP) has already been automatically removed from service by the system due to a failure, and lock it to prevent the software from trying to use it when a replacement FP is inserted. This applies to any FP.

Prerequisites

- When an FP has been removed from service by the system, an unspared FP is not providing service and a standby FP is not available for a backup. Minimize the impact of an out-of-service FP by performing the procedure as soon as possible. An out-of-service FP shows a solid red LED and alarm 7012 100 is generated.
- Check for other alarms to determine if other equipment is causing the FP to be out-of-service. Address the remedial action when the system allows it. All alarms are described in NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.
- When you were upgrading, downgrading, or redeploying an FP when the failed FP was discovered, you must fix the failed FP first.
- Identify from your site records whether any private network-to-network (PNNI) links pass through the failed FP. These links may not automatically return to service when the FP is replaced, and may need to be reconfigured or manually unlocked.
- For more information on the commands that are used in the following procedure, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*.
- Perform the following procedure in operational mode.

Procedure steps

1 Identify and record the software level or PCR that is running on the node containing the out-of-service FP. You will need it to label the PCR onto the faceplate of the card.

```
display switch avl
```

Note: The response indicates the configured (provisioned) software that is running through the node, not the software that might be loaded on the inactive CP. When removing a card for re-deployment or repair, it is important to know what version of software was running on it.

2 Confirm the card is out of service.

```
display Shelf Card/<m>
```

If the *operationalState* indicates *disabled*, the card is out-of-service.

3 Check all software alarms that are generated by the node that houses the FP that is out of service. Address the remedial action of any alarm involving equipment or software for the FP being replaced.

4 When the system automatically removes a card from service, it has run software tests that failed. Examine the test results to determine why the card was removed from service by the system. Query commands of FP test results are described in NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*.

5 Lock the out-of-service card to prevent the system from trying to use it when the replacement is inserted. Refer to “Removing an FP from service” (page 37).

Variable definitions

Variable	Value
<m>	is the slot number of the standby card determined in this procedure. For information about the command *lock*, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*. Whenever a card is locked, the alarm 7012 0100 is generated. Whenever a standby card is locked, the alarm 7054 0105 is generated. The alarms are described in NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.

Removing from service an optical FP configured with LAPS

Remove from service an optical function processor (FP) that is configured for line automatic protection switching (LAPS) in the node before removing the card. LAPS is port-to-port protection between paired adjacent FPs (dual-FP LAPS or inter-card LAPS) or on the same FP (single-FP LAPS or intra-card LAPS).

Prerequisites

- Dual-FP LAPS is also referred to as inter-card LAPS. Single-FP LAPS is also referred to as intra-card LAPS.
- When you are upgrading, downgrading, or redeploying a card that is configured for paired card protection through LAPS, always plan to switch the traffic from one FP (the target) to its mate. Then removing the target FP from service minimizes the affects on traffic.
- After a port or FP is removed from service by you or the system, an attempted switchover causes the traffic to be lost because the port or card is not available. To prevent the loss, the port must be manually locked in the software. If the active card or port fails while the mate is out of service, traffic on the active card or port is lost.
- Unless the FP has already been removed from service by the system, minimize the risk of not having a backup by doing the procedure during the period of lowest traffic for that FP. An out-of-service FP shows a solid red LED.
- Identify from your site records whether any private network-to-network (PNNI) links pass through either of the FP pair. The procedure will indicate when to remove the PNNI links from service.
- Identify from your site records if the optical card to be removed from service has been configured for line automatic protection switching (LAPS). Not all Nortel Networks Multiservice Switch 15000 and Multiservice Switch 20000 optical FPs support LAPS. NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference* identifies which FPs support LAPS, but does not indicate if an FP is configured to use the capability.

- An FP that supports only intra-card LAPS (single-FP LAPS) has port-to-port sparing on the same card. For this configuration, follow the procedure "Removing from service an unspared FP" (page 56).
- Each FP of a protected pair that supports inter-card LAPS (dual-FP LAPS) can have ports providing service (the equivalent of active) or on hot standby (the equivalent of inactive or standby). The LED status of both cards is solid green, indicating both are active even if all ports on one card are on hot standby. In this case, the following procedure temporarily removes one of the cards from service by switching traffic to its mate.
- Prior to removing the card from service, you will be asked to monitor all alarms for the node that houses the FP being replaced. Contact your next level of Nortel Networks technical support to assist you. Check for alarms generated against the FP pair. For any alarms indicating the need for remedial action other than replacing the FP, complete the action before removing the FP from service. All alarms are described in NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.
- During the removal from service, monitor alarms generated for equipment that is involved in the connection paths of the FP being replaced. Address the remedial action when the system allows it.
- For more information on the commands that are used in the following procedure, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*.
- Perform the following procedure in operational mode.

Procedure steps

1. Identify and record the software level or PCR that is running in the node containing the FP. You will need it to label the PCR onto the faceplate of the card.

   ```
   display switch avl
   ```

   Note: The response indicates the configured (provisioned) software that is running through the node, not the software that might be loaded on the inactive CP. When removing a card for re-deployment or repair, it is important to know what version of software was running on it.

2. Verify that the card supports LAPS.

```
display -p laps/*
```

If the card was configured for LAPS, the response will indicate a status of the working and protection lines for the card pair you plan to work on.

3 For dual-FP LAPS, there can be ports providing service (active) on both cards so there is no card with a standby status. Identify which card was originally designated as the standby card by entering the command:

```
display Shelf Card/* sps
```

The value under *Card* in the response is the slot number. Under *osiStby*, the value *serv* means that the card is active while *hot* means that the card is the hot standby.

4 Identify which SONET lines are providing service (as opposed to being on hot standby).

```
display laps/* nearendrxactiveline
```

The lines with status *workin* are providing service while the lines with *protec* are on hot standby. When *nearEndRequest* indicates

- signalFailure it usually means a cable has been cut
- signalDegrade it usually means a bit error
- forcedSwitch it means a manual switchover was invoked and the mate port is not available

5 Ensure that LAPS is not degraded.

```
display laps/* osiState
```

Under *osiAvail*, determine if any LAPS has a status of *degraded*. If so, you must determine the cause of the degradation and fix it on both cards before continuing this procedure. Record all port numbers that are degraded then see NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* for the task to find the procedure to determine the cause of degraded LAPS. Return to this procedure when the degradations are fixed.

CAUTION

Risk of service interruption from a degraded LAPS

You must determine the cause of each degraded LAPS port because a switchover to one means it can remain out of service longer than 50 milliseconds.

6 When removing the card from service for an upgrade or a re-deployment (as opposed to a failure), ensure that traffic is running on the mate FP. If traffic is not running on the mate before the removal, it is unlikely traffic will run on the replacement FP after the return to service.

a. Verify that the *atmif* is in service and active, and that there are no unexpected ATMIF alarms.

b. Verify that the UNI, PNNI, and IISP links are in service and active.

c. Verify that all connections are up and passing traffic, including VPTs, and that there are no signalling alarms.

7 Check all software alarms that are generated by the node that houses the FP being replaced. Address the remedial action of any alarm involving equipment or software for the FP being replaced.

8 Prepare the far-end ports for the near-end ports being removed from service. This step applies to any FP.

9 If your site records indicated that you have at least one PNNI link passing through the FP to be removed from service, you must first busy or lock the PNNI link at the far end to remove it from service. At the facility level of operation, as opposed to the service level, transfer the PNNI traffic off the target FP to its mate by following the procedure “Switching SONET line protection to the mate FP” (page 34).

10 Transfer any traffic from the ports on the near-end target card to the mate card and block the target card and ports from being put into service.

```
lock -force Shelf Card/<m>
```

Note: Whether the card ports are configured as *unidirectional* or *bidirectional*, or as a *revertive* or *non-revertive* mode, the command *lock* handles all associated Multiservice Switch system connections.

11 Observe the traffic on the active card to ensure it is flowing. Use appropriate test equipment to monitor the cell counts.

12 If the switchover did not occur, abort this procedure and see NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000*

Fault and Performance Management: Troubleshooting for diagnosing FPs. For FP fiber optic cards with LAPS, if the active (target) and standby (mate) LEDs on the faceplates do not swap within 50 milliseconds, the switchover may not occur.

13 If you are performing this procedure to test an FP, return immediately to NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*.

Variable definitions

Variable	Value
<m>	is the slot number of the standby card configured in this procedure. For information about the command *lock*, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*. Whenever a card is locked, the alarm 7012 0100 is generated. Whenever a standby card is locked, the alarm 7054 0105 is generated. The alarms are described in NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.

Removing from service an unspared FP

Remove an unspared (unprotected) function processor (FP) from service before removing the FP from the shelf. This procedure applies to any type of FP.

Prerequisites

- Check for alarms generated against the equipment the FP connects to. At the time you are about to remove the unspared FP from service, use the alarm data to determine which equipment should be fixed first in order to minimize the extent of removing the unspared card from service. The alarms are described in NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.
- When an unspared FP is removed from service by you or the system, the traffic on the card is dropped. Unless the FP has already been removed from service by the system, minimize the out-of-service impact by doing the procedure during the period of lowest traffic for that FP. An out-of-service FP shows a solid red LED.
- Before removing an unspared FP from service, decide how to minimize the impact on traffic at the far end of the FP. If the unspared FP is in service or partially in service (its LED is solid green), locking it before removal causes an impact on traffic from the far end connection. The extent of traffic loss for traffic in progress and for subsequent incoming traffic depends on how much traffic is occurring and is likely to occur for the duration of the replacement and how the far-end equipment and software is set up for redundancy at your network level of system engineering. If the far end node is a Nortel Networks Multiservice Switch device, the system takes care of the connections according to the way the cards are configured.
- Identify from your site records whether any private network-to-network (PNNI) links pass through the FP. The procedure will indicate when to remove the PNNI links from service.
- Identify from your site records if the optical card to be removed from service has been configured for line automatic protection switching (LAPS) between pairs of ports on the same card. Not all Nortel Networks Multiservice Switch 15000 and Multiservice Switch 20000 optical FPs support intra-LAPS. NN10600-551 *Nortel Networks Multiservice Switch*

7400/15000/20000 FP Configuration Reference identifies which FPs support LAPS, but does not indicate if an FP is configured to use the capability. When an unspared card with intra-LAPS is removed from service, the traffic on the port pair is dropped.

- Plan how to replace an unspared FP quickly and safely to minimize how long the FP's traffic links will be out of service.
- Although an unspared FP can have been removed from service by the system, you must always ensure that the card has been removed from service and lock it in software before physically removing it from the shelf. Otherwise, the replacement card may not fully return to service, or inserting the card can cause the shelf to reset.
- For more information on the commands that are used in the following procedure, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*.
- Perform the following procedure in operational mode.

Procedure steps

1 Identify and record the software level or PCR that is running in the node that has the standby FP.

```
display switch avl
```

Note: The response indicates the configured (provisioned) software that is running through the node, not the software that might be loaded on the inactive CP. When removing a card for re-deployment or repair, it is important to know what version of software was running on it. Label the PCR onto the faceplate.

2 Typically, when an unspared FP is removed from service, all traffic to that FP is dropped.

CAUTION

Risk of service interruption

When an unspared card is removed from service either manually or automatically by the system (for example, by the command *lock*), all traffic to the card is dropped. If you must remove an in-service card from service, ensure that you do it during a period of lowest traffic for that card, and you do not delay inserting the replacement card.

If your site records indicate that the network was configured to back up the traffic of an unspared FP, removing the FP from service may cause the network to reroute far-end traffic away from the FP. For example, the configuration can have an intra-network card as opposed to an access card or have a node connected to two nodes to split services. PNNI links may have been set up to do this. If your site records indicate that one or more PNNI links pass through the FP, busy or lock each of those links at the far end.

3 Check all software alarms that are generated by the node that houses the FP being replaced. Address the remedial action of any alarm indicating that the standby or mate FP is not available to take over the traffic of the active FP.

4 Prevent a shelf reset by entering the command:

```
lock -force Shelf Card/<m>
```

Whenever a card is locked, the alarm 7012 0100 is generated. Whenever a standby card is locked, the alarm 7054 0105 is generated. The alarms are described in NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.

Note: For a VSP3 card, do not lock the gigabit Ethernet ports.

5 If you are performing this procedure to replace an FP, return immediately to NN10600-130 *Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade* to replace the out-of-service FP.

If you are performing this procedure to test an FP, return immediately to NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*.

Variable definitions

Variable	Value
<m>	is the slot number of the card. For information about the command *lock*, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*.

Chapter 5
Replacing an optical FP

Replace an optical FP when:

- the FP or a port on the card fails
- the FP is to be re-deployed to a different card slot
- the FP is being upgraded by an FP of the same type but a later (or earlier) hardware vintage, using the same PCR software vintage, and typically with an increase in feature capabilities

When changing the software release level of the replacement card, the upgrade is a migration. Documentation for software migrations can be found in either

- NN 10070-461 *Upgrading Nortel Networks Multiservice Switch 15000 in Succession Networks PT-AAL1/UA-AAL1*
- NN 10185-461 *Upgrading Preside MDM in Succession Networks*

Before replacing an optical FP, address the following prerequisites.

- "Prerequisites for replacing an FP" (page 62)
- "When changing the configuration of an FP at replacement" (page 68)
- "Prerequisites for upgrading an FP" (page 68)

Prerequisites for replacing an FP

You need extensive knowledge of Nortel Networks Multiservice Switch software and the Succession portfolio architecture. You also need an understanding of your Succession Network topology and the connectivity between the Multiservice Switch nodes and the various Succession Network elements. You need to interpret your Network Specification Book, and identify what is connected to the targeted FP for replacement.

Before removing an FP from service, decide how to minimize the impact on traffic at the far end of the FP unless the FP has already been removed from service by the system (its LED is solid red). If the far end node is a Nortel Networks Multiservice Switch device, the system takes care of the connections according to the way the cards are configured and according to their operational status during the replacement.

All of the optical FPs on a Multiservice Switch 15000 shelf can be installed in 1+1 protected pairs and appropriately configured in software. To prevent the loss of calls, this replacement strategy only applies to FPs that have been provisioned with one-for-one equipment sparing.

Optical FP pairs that support line automatic protection switching (LAPS) between two FPs can have ports on either FP carrying active traffic. Before removing the target FP from service, switch any active traffic to its mate.

The table “Summary replacement activity for a card based on the card’s configuration setup” (page 63) indicates the maintenance activity to maintain or restore traffic for a replacement that is the same type of card and a compatible vintage.

Table 1
Summary replacement activity for a card based on the card's configuration setup

Setup	Card status	Action summary for replacement	Impact on traffic
spared card, standby	in service	Force lock the standby card in software, replace it, and unlock it.	none, provided the active card remains in service while the standby card is replaced
spared card, standby	failed or partially failed	Force lock the standby card in software, replace it, and unlock it.	none, provided the active card remains in service while the standby card is replaced
spared card, active	in-service	Switch the traffic of the active card to the standby card and lock the new standby card (formerly the active), then replace the new standby card and unlock it.	up to 50 ms is lost for optical FPs, and more for electrical FPs depending on the type of sparing panel
intra-card LAPS (spared ports, same card)	in-service	Port sparing cannot be supported for intra-card LAPS while the card is replaced unless the card is also spared and any PVCs were configured for an inter-card port mapping. Follow the action for the card according to its equipment protection configuration.	cell loss occurs through intra-port sparing when the card is removed and until the replacement card reloads
intra-card LAPS (spared ports, same card)	failed or partially failed	Intra-card port sparing cannot be supported while the card has failed. Force lock the card, replace it, and unlock it.	traffic through the ports was already lost and will resume when the replacement card reloads
inter-card LAPS (spared ports, different card)	in-service	One of the two active cards must be removed from service. Follow the action for the card according to its equipment protection configuration.	cell loss occurs with inter-port sparing when a card is removed from service

(Sheet 1 of 2)

Table 1 (continued)
Summary replacement activity for a card based on the card's configuration setup

Setup	Card status	Action summary for replacement	Impact on traffic
inter-card LAPS (spared ports, different card)	failed or partially failed	One of the two active cards has been removed from service by the system. Follow the action for the card according to its equipment protection configuration.	cell loss has already occurred when the system removed the card from service
unspared card	failed or partially failed	Force lock the card then replace it without delay.	cell loss of traffic that was in progress and blocked traffic until the replacement card is returned to service
unspared card	in-service	During the card's lowest period of traffic, prepare the far-end equipment for a loss of traffic to and from the card, force lock it, then replace the card without delay.	cell loss of traffic that was in progress and blocked traffic until the FP and far end are returned to service

(Sheet 2 of 2)

Before replacing the FP, you must address the following criteria.

- Ensure that the minimum level of software for operating the replacement is running on the node. To verify the minimum software requirements of an FP type, see the description of that FP in NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference*.
- Ensure that the hardware version of the replacement card is compatible. The hardware version is part of the product engineering code (PEC) that identifies a card. Most FPs with the same first six alphanumeric digits are compatible to operate. Spared FPs with different versions are limited to sparing only their common functionality. For information about what a PEC is, see "Product engineering codes (PECs)". If you are in doubt about the compatibility of your replacement card, or if the specific vintage is no longer available, contact your local Nortel Networks sales or support representative to determine the status of compatibility.

- For FPs with PQC12 technology, the node must have PCR 3.0 software level or a later release. The technology of each type of FP is described in NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference*.
- When a replacement card has been inserted into a slot, you should test each port while it is out of service, then test the card when it is returned to service but still has a standby status. Traffic cannot run through a port while it is being tested, and traffic might run on the card while it is being tested provided it was configured to enable it. Running a test on the card while traffic progresses may affect the far end of the FP. The duration of testing is user-defined. Decide before the replacement card is inserted whether you will run the card or port tests. For the description of the tests and the software attributes, see NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* for testing function processors and function processor ports.
- Review your Network Specification book to identify the connections configured on the card that is to be replaced, especially if the card is spared with equipment protection.
- Whenever possible, schedule the replacement of a spared FP or pair of FPs during their period of lowest traffic. This minimizes the risk of having no backup for the mate FP while the target FP is being replaced.
- To prevent outages during a card replacement, ensure that the two to four links between the CS2000 and the node are configured in pairs and that these pairs have been distributed between Nortel Networks Multiservice Switch 15000 shelves to create redundancy. Ensure that there are redundant AMDI PVC VCC numbers to separate FPs on distributed nodes. Ensure that each PVC is enabled.

Always monitor the generation of alarms before, during and after a card replacement. Equipment that is associated with the connection path of an FP can change status at any time. Monitoring alarms allows you to keep the priority actions for the node and the network in focus.

Before handling any tools or installing a hardware part on or near the device or its frame, ensure that you are familiar with "avoiding equipment damage by static electricity" and "Cleaning the ends of fiber cables" in NN10600-130 *Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*.

CAUTION

Risk of service degradation by condensation

When moving a card between rooms with very different levels of temperature and humidity (for example, from non-air conditioned to air conditioned), condensation can form on the card. Condensation on a card can affect its ability to fully operate. Before inserting a card into a shelf, ensure that the card has been unpacked in the same room as the Multiservice Switch equipment for at least one hour. The time allows the card to adjust to the ambient temperature and humidity of the room.

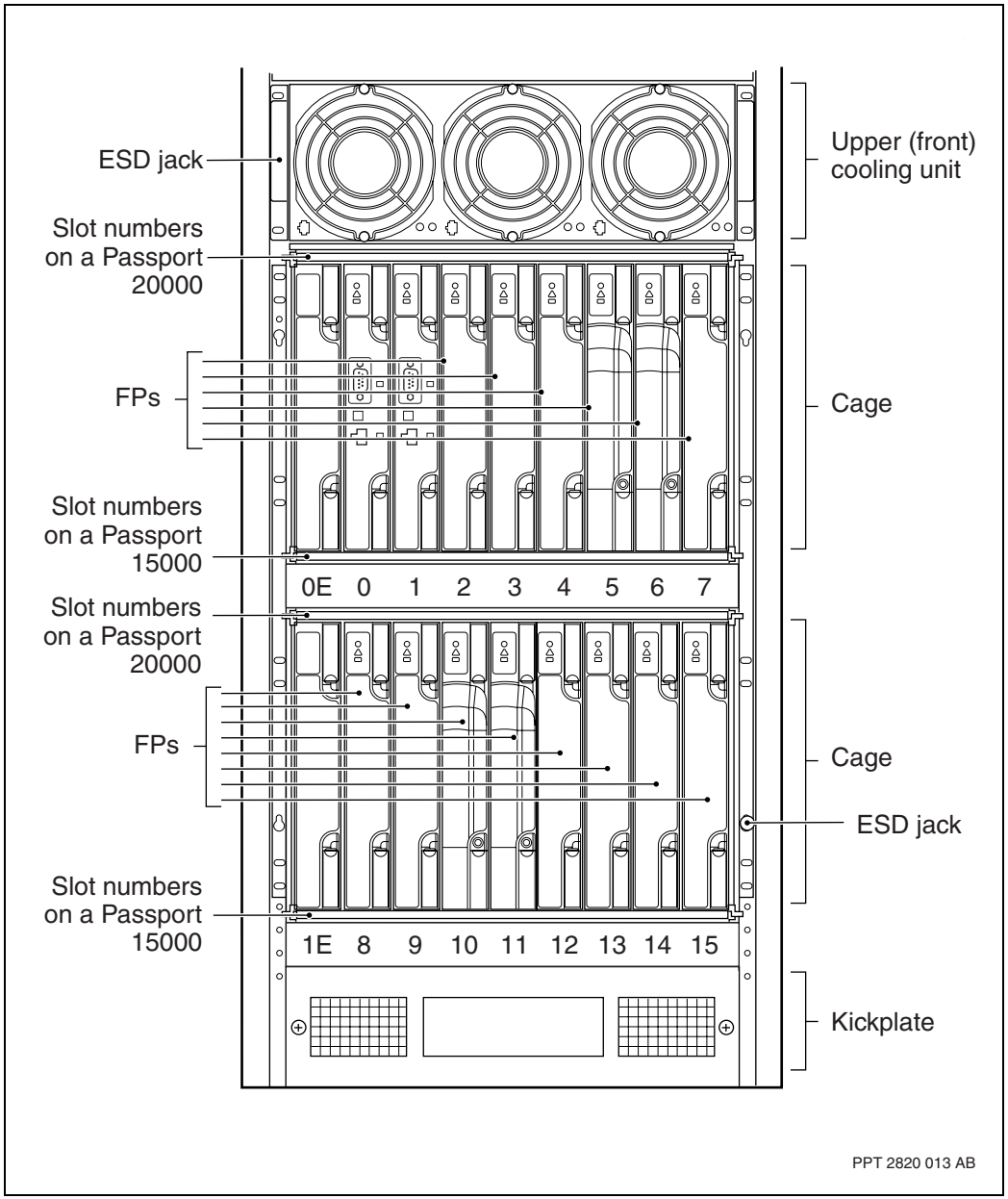
CAUTION

Risk of damage to equipment from software

Ensure that the replacement FP has a version of product engineering code (PEC) that is compatible with the version of Multiservice Switch software release that will be loaded onto it. An incompatible load can damage the FP beyond a field repair. For the PCR version of an FP, see the description of that FP type in NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference*.

If you have any problems during a card replacement, contact Nortel Networks Global Networks Technical Support (GNTS) for assistance.

Figure 1
Locations of FPs



When changing the configuration of an FP at replacement

Your configuration choices are identified by FP card type and PEC in NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference*.

After changing the services or functionality of an FP by reconfiguring the slot, you may have to reset the FP after it is inserted. Usually this reset occurs automatically as part of commit prov. Some kinds of reconfiguring require a reset for the changes to take effect on the FP.

The software commands to reset an FP are described in NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*, the section on re-initializing a processor card.

Prerequisites for upgrading an FP

Upgrading an FP means replacing an FP that is already installed and configured with one that offers more features.

Upgrade an FP while an unspared FP or active FP of a protected (spared) pair is operating without faults. If you no longer have a compatible replacement for a failed FP, you can use the opportunity to reconfigure the slot for a different card type, that is, re-deploy the card slot.

> ***Note:*** For FPs with PQC12 technology, the node must have PCR 3.0 software level or a later release. The technology of each type of FP is described in NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference*.

Replacing a spared or unspared optical FP

Before replacing an FP, ensure that sure that you have addressed all of the prerequisites for replacing an optical FP.

Replacing a spared or unspared optical FP is divided into

- "Removing an optical FP from a shelf" (page 69)
- "Inserting an optical FP into a shelf" (page 73)

Note: These procedures address whether the target FP is in service or out of service.

Removing an optical FP from a shelf

Remove an optical FP from a shelf as follows.

1 Identify from your site records if the optical target FP is

- an unspared card
- an optical card with ports configured in software for inter-card or intra-card LAPS

2 Gather information about the status of the target FP and its mate if it is configured for dual-FP LAPS operation. Perform the procedures identified in "Determining the status of an optical FP" (page 19) and return to this procedure.

3 Remove the FP from service according to the card configuration that applies in "Removing an FP from service" (page 37), including when the system has removed the card from service due to a failure, and return to this procedure.

Note: If the LED of the card is solid red, and alarm 7012 0100 has been generated for that card, the system has already removed the card from service.

4 At the front of the node, locate the target FP to be replaced.

5 Label the FP faceplate with the software level or from "Removing an FP from service" on page 37 that is running on the card.

6 Observe the LED status of the FP to be replaced. After being locked, the LED on the card is solid red.

If the LED result is not solid red, the switchover between dual-FPs did not occur properly. Contact Global Networks Technical Support (GNTS) to determine your next step.

7 Plug a grounding strap (part number A0378999) into an ESD receptacle at the front of the node and wear it on a wrist. The hole is threaded to provide friction for a press-fit.

8 Record the position of each cable connector relative to the label of the connector on the faceplate. Each cable should already have been labeled with port connection information that will enable you to quickly reconnect the cables to appropriate ports.

9 For fiber optic cards with cable hoods on the faceplate of the card, release the hood by turning the lower latching screw counter-clockwise a 1/4 turn with a slotted screw driver. Turn the screw by hand, not a power tool. Lift the hood upwards and hold it perpendicular to the faceplate.

CAUTION

Risk of service interruption

Unseating an FP while at least one traffic port cable is still connected to the faceplate means that any PNNI links and some services (for example, ATM) to that FP through that port will be dropped and will not recover when a replacement FP is returned to service. Always disconnect all cables after locking a card and before unseating it.

10 Unplug the cable connectors on the faceplate of the FP. While unplugging, pull straight away from the faceplate connector.

For SC, LC, or MT-RJ fiber cable connectors, fully pinch the tab on the connector against its side and pull straight out. Cover the ferrule with a dust cap.

CAUTION

Risk of damage to the fiber transceivers on the FPs

When engaging or disengaging a fiber optical cable connector to the connector on the FP faceplate (the transceiver), you can damage the nose shield on the connector or the optic transceiver by improper coupling. This especially applies to MT-RJ connectors.

Before attempting to engage each fiber cable connector, you must ensure that the connector's guide ridge is aligned with the transceiver's keyway.

Before pulling the cable connector away from the transceiver, you must ensure that the tab (latch) on the cable connector is fully pinched against its side.

11 Allow the cables to hang aside temporarily. Do not allow your actions to snag a connector since this can disengage the connector from the cable without it being visibly obvious.

12 On the faceplate of the FP, fully swing out the upper and lower latches until they stop.

13 Place fingers on the exposed tabs to gently but firmly slide the FP out of its slot. Hold only the edges of the FP. Be careful because an FP weighs up to 5.4 kg (12 lbs).

14 Put the FP aside onto its original packaging. Record the PCR software level onto the container of the card so that the card's software load can be identified without opening the container. Pack the card later to minimize the amount of time the card slot will be out of service.

15 Compare the PEC of the removed FP with the PEC of its replacement. The first 6 alphanumerical characters of the PECs must be the same (for example, NTHR23AA and NTHR23BA) for a replacement due to a failure or an upgrade.

16 If more functionality is available on the higher version of the FP (same type), then additional software configuration may be required, as described in NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference*. Change the software configuration of the FP as required before inserting the replacement.

17 If the replacement FP has a different card type, then the slot must be decommissioned and reconfigured for the re-deployment.

See NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference* to identify configuration choices, and NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures* to configure the card.

Minimize the impact or risk of removing the target FP by "Inserting an optical FP into a shelf" (page 73) immediately.

Inserting an optical FP into a shelf

Inserting an FP into a shelf assumes you have an empty slot and are continuing from the procedure "Removing an optical FP from a shelf" (page 69). (Initial FP installations involve different steps which are described in NN10600-130 *Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*.)

Insert an optical FP into an empty slot as follows.

1. If the replacement card required reconfiguration, perform "Activating configuration changes" (page 76) while the slot is empty.
2. Check the container of the FP to determine if a PCR software level is identified on it. Cards that are redeployed should indicate what software was running on them. New cards will not necessarily indicate the PCR software that is pre-loaded at the factory.
3. Open the packaging of the new FP.
4. Holding the replacement FP by its faceplate edges with the latches on the right side of the faceplate, align the end with the pins to the channels in the slot. Avoid touching anything on the FP.
5. Gently push the FP into the slot until the FP stops moving. There are keyways and guide pins to ensure that the FP aligns with the connections at the backplane (inside at the rear of the shelf). If you feel resistance, do not force the FP in. Remove it and check the backplane pins.

   If no pins are bent, re-seat the FP. If at least one pin is bent, do not insert the FP and contact GNTS.
6. Close the latches flush against the faceplate.
7. Release the cable hood latch on a fiber card, lift the hood upwards, and hold it perpendicular to the faceplate.

CAUTION

Risk of damage to the fiber transceivers on the FPs

When engaging or disengaging a fiber optical cable connector to the connector on the FP faceplate (the transceiver), you can damage the nose shield on the connector or the optic transceiver by improper coupling. This especially applies to MT-RJ connectors.

Before attempting to engage each fiber cable connector, you must ensure that the connector's guide ridge is aligned with the transceiver's keyway.

Before pulling the cable connector away from the transceiver, you must ensure that the tab (latch) on the cable connector is fully pinched against its side.

When connecting the fiber cables, progress from the bottom right side of the faceplate to the top, then from the bottom of the left side of the faceplate to the top (when a second column of connectors is present). Align each fiber connector perpendicular with the keyway of the transceiver and press the connector into it until the tab clicks. The click confirms engagement.

Connecting the cables bottom to top and right to left lessens the entanglement of cables under the fiber hood and along the cable management trough at the front of the shelf assembly as each cable is added.

Note: Insert each connector gently and smoothly into the transceiver until feeling very slight resistance up to the click. Ensure that the connector keyway guide is aligned and perpendicular with the keyway in the transceiver. If the connector is duplex (2 simplex connectors clipped together), you must handle both insertions simultaneously. If you feel greater than very slight resistance, do not force it. Ensure that the tab is fully pinched, remove the cable connector, and re-align the cable connector before repeating the insertion.

8 Plug the FP cables back into the faceplate, progressing from the bottom to the top. Match each cable label to the appropriate port number. All types of connectors used on a Multiservice Switch 15000 FPs engage only one way. Fiber connectors have a keyway guide and a press-down tab that clicks into position to indicate the connector is fully seated. Other types of connectors have other methods of alignment and engagement.

Note: For MT-RJ connectors, insert the end gently and smoothly perpendicular to the transceiver until feeling very slight resistance up to the click. If you feel greater than very slight resistance, do not force it. Ensure that the tab is fully pinched, remove the cable connector, and re-align the cable connector before repeating the insertion.

9 Observe the LED of the replaced FP. Eventually it should become solid green to indicate in service.

If the LED stays solid red after loading is attempted, the card is an incompatible vintage or was previously loaded with software that is incompatible with the current software running on the node. Use a compatible card.

The pattern of LEDs when an FP is seated are described in “Checking the LEDs on each optical FP” (page 22).

10 Return the FP to service according to the procedure in “Returning an FP to service” (page 82), and return to this procedure.

11 If the replacement FP has no label indicating its former PCR software level, add the same PCR that was identified in “Removing an FP from service” (page 37).

If the replacement FP already has a label that indicates the former PCR software version with the current PCR version, ensure that it is compatible with what is running on the node.

12 Carefully fasten the port cable clusters in place. Keep all cables of one FP together. Do not crimp any cables when fastening them together.

For optical FPs with hoods over the faceplate, do not fasten cables under the hood.

13 Pack the removed FP into its original box or an equivalent ESD-protected container.

14 As required by your administration, make the active card of a spared (redundant) pair of cards the standby card. All virtual circuits (such as PVCs, SVCs, and SPVCs) are automatically re-established during a switchover.

With dual-FP LAPS configurations, returning the replaced FP to service means it is initially a standby FP until system configuration or fault management makes at least one port on it become active, thereby making the standby FP active with its mate.

Activating configuration changes

Several procedures in this document ask that you complete the configuration changes. When you complete the configuration changes, you are activating the configuration changes, confirming that you want to activate them, and saving the changes. You are instructed to complete the configuration changes only at the end of procedures that you perform in provisioning mode.

CAUTION

Activating a provisioning view can affect service

Activating a provisioning view can result in a control processor reload or restart, causing all services on the node to fail. See NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference* for more information.

Activate configuration changes as follows.

1 Verify that the provisioning changes you have made are acceptable:

```
check Prov
```

Correct any errors and verify the provisioning changes again.

2 If you want to store the provisioning changes in a file, save the provisioning view:

```
save Prov
```

3 If you want these and other changes made in the edit view to take effect immediately, activate, confirm, and commit the provisioning changes:

```
activate Prov

confirm Prov

commit Prov
```

4 End the provisioning session:

```
end Prov
```

Unpacking a card

A card is shipped in a separate anti-ESD container in groups of one or more. The product engineering code (PEC) of the card is labeled on the outside of the container.

Prerequisites

Cards can be damaged by electrostatic discharge (ESD) or conduct it onto another part that is ESD-sensitive. Prevent ESD damage to parts by wearing an antistatic wrist strap (part number A0378999). Before opening the card container, move to the location of the equipment. The package must be near the shelf so that a person wearing the wrist strap can reach the package while plugged into an ESD jack.

CAUTION
Risk of damage to equipment by ESD
Unpack a circuit card only minutes before it is to be inserted in its slot in the shelf. The packaging protects the circuitry from electrostatic discharge (ESD).

CAUTION
Risk of damage to equipment by ESD
Whenever unpacking or handling unpacked circuit cards, always wear an antistatic wrist strap that is plugged into an appropriate electrostatic discharge (ESD) receptacle. Hold a card by its faceplate. Never touch other parts (for example, electrical connections, pins, soldered surfaces, or chips).

Unpack an FP as described in “Procedure steps” (page 77).

Procedure steps

Before unpacking a card, ensure that you are familiar with the “Prerequisites” (page 77).

1 Carefully move the containers to the Nortel Networks Multiservice Switch 15000 node location.

2 Wear a wrist strap (part number A0378999) and plug the connector into an ESD jack. The jacks are distinguished as threaded knobs or holes and are usually accompanied by a the symbol for a grounding point. For the first plug-in, you may have to puncture the grounding strip between the jack and the upright. The threads provide friction for the connector. Some locations of the jacks are shown in the figure "Location of ESD jacks, front lower (shown) or upper shelf" (page 79).

3 Open the card container. When cutting the tape or straps that seal the container, make very shallow cuts. Open the box ends before the sides so that you can raise the middle slightly to cut it.

4 Gently remove any loose padding surrounding the contents, if present. Avoid contacting the rows of pins with the packing material.

5 Placing your hands only on the edges of the card, carefully remove the card. If in a pouch, remove the card in it. Be ready for the card to be heavier than it looks. An FP weighs about 5.5 kg (12 lbs).

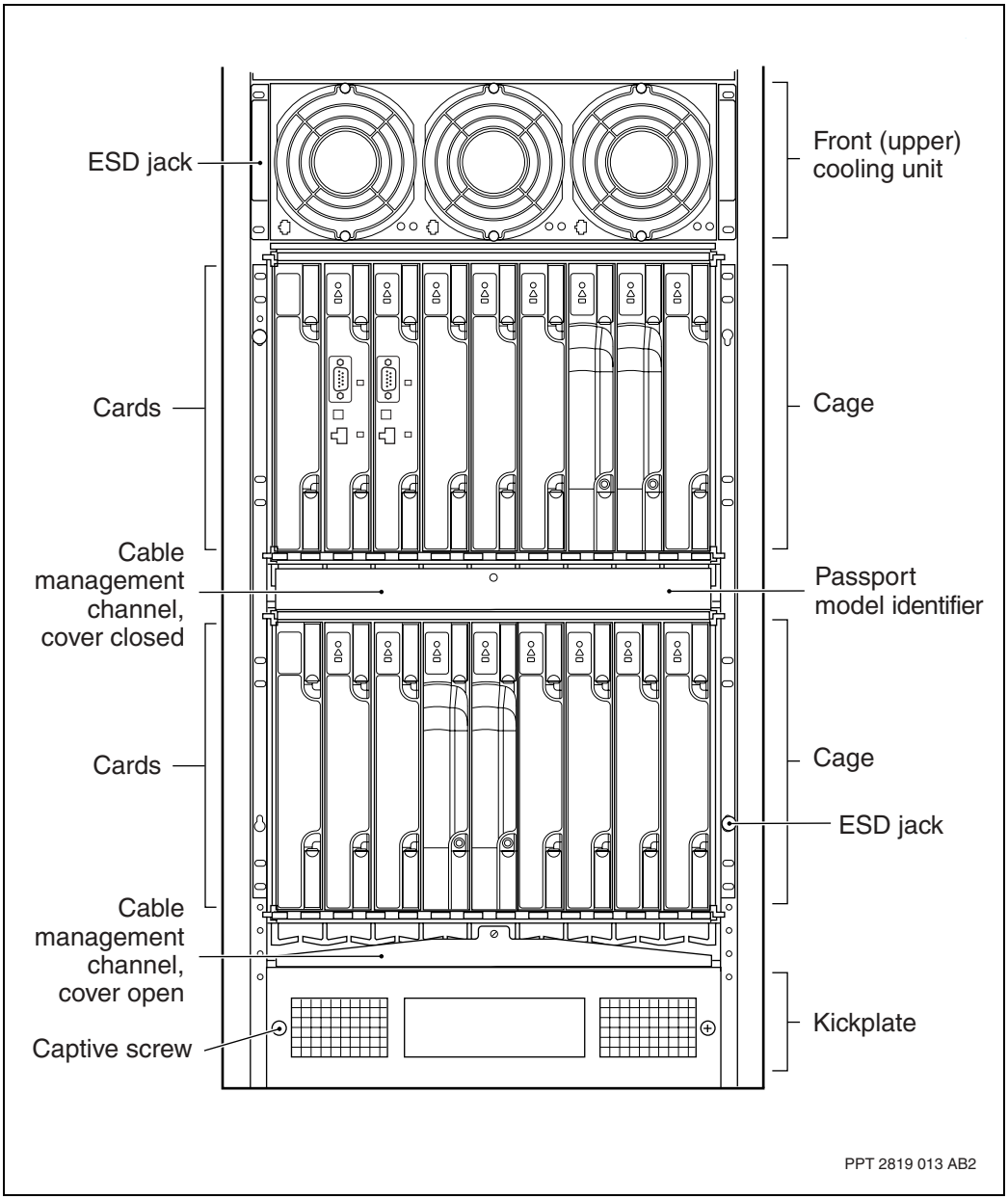
6 In an area near the equipment that is relatively free of ESD, remove the part from the pouch or container by holding only its edges or sides. For any part that has what looks like a circuit board or a connector, avoid touching the connector or anything on the board.

7 Store the anti-ESD pouch and the container in case the card must be returned or stored later.

8 If the unit seems undamaged, continue with the replacement procedure.

9 Store the original packing material and container in case the part must be stored, re-deployed, or returned later.

Figure 2
Location of ESD jacks, front lower (shown) or upper shelf



Chapter 6
Returning the FP to service

Returning the replaced FP to service involves

- waiting for the card to be loaded with software
- verifying the card type of the replacement card matches the configured card type for the slot
- testing the ports while the card is out of service (optional)
- unlocking the card
- testing the card while it is in-service and on standby
- re-establishing the far-end links to the replaced FP
- verifying the success of the return to service
- soaking the replaced card (optional)

These activities are identified in the procedure “Returning an FP to service” (page 82).

Returning an FP to service

After inserting the replacement FP into its slot, return the FP to service. Returning an FP to service involves ensuring that it is going to operate correctly before and after unlocking it in software. This procedure includes electrical and optical FPs.

Prerequisites

- Monitor for alarms generated against the equipment that the FP connects to. While the replaced FP is returning to service, alarms generated for linked equipment can help indicate the progressive operation of the replaced FP, and the status of connected equipment. All alarms are described in NN10600-500 *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*.
- For more information on the commands that are used in the following procedure, see NN10600-050 *Nortel Networks Multiservice Switch 7400/15000/20000 Command Reference*.
- Perform the following procedure in operational mode.

Procedure steps

1. Verify that the replacement FP is appropriate for the software configuration of the slot by performing the procedure “Comparing the card type of an inserted card and its configured slot” (page 20).
2. While the replacement FP is inserted and out of service, test each port according to the type of FP as described in NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*. This is optional.
3. As required, return to service any equipment that is involved in the port connection up to the far-end termination. If the equipment is not Nortel Networks Multiservice Switch it will also have to be unlocked. Since the FP is still locked, local and far-end alarms will still be generated.
4. After port testing passes, unlock the FP so that it can return to service.

   ```
   unlock Shelf Card/<m>
   ```

   Whenever a card is unlocked, the alarm 7012 0100 is generated. Whenever a standby card is unlocked, the alarm 7054 0105 is generated.

Wait until the cycling of the LEDs ends at fast flashing green. If the LED stays solid red after loading is attempted, the card is an incompatible vintage. Use a compatible card.

5 If the FP was re-configured, identify whether the type of FP or any of the changed services require an FP reset.

6 Test the card according to its type as described in NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*.

7 Perform the procedure “Re-establishing links to the CS2000 from the replaced FP” (page 85).

8 Perform the procedure “Verifying that MG4000, IW-SPM, and DPT-SPM links have returned to service” (page 86).

9 Ensure that the spared services on the FP are up and running. For a spared fiber optic card, check that LAPS is not degraded.

```
display Shelf Card/* sps
```

For an unspared card, check that the status of the logical processor (LP) is working.

```
display lp/<n>
```

From the response, perform the following.

- Verify that the *atmif* is in service and active, and that there are no unexpected ATMIF alarms.
- Verify that the UNI, PNNI, and IISP links are in service and active.
- Verify that all connections are up and passing traffic, including VPTs, and that there are no signalling alarms.

10 Ensure that LAPS on the FP is operating normally.

```
display laps/*
```

Specifically confirm that the line that was worked on is operating.

11 Ensure that the SONET and SDH ports on the FP are operating normally.

```
display lp/* son/*

display lp/* sdh/*
```

Specifically confirm that the port associated with the fixed line is operating.

12 Check for alarms indicating a problem with the newly replaced FP. If you detect unexpected alarms indicating:

- at least one disabled LAPS line
- an STS alarm on an optical card
- a port alarm on an electrical card

Contact Nortel Networks Global Networks Technical Support (GNTS) to determine your course of action.

13 While the FP is returning to service, verify that:

- the Tx and Rx connections continue to increase
- there are no cell mis-insertions
- PVC connections are OK
- SVC and SPVC connections are OK

Otherwise, contact GNTS.

14 Monitor for any alarms that have been generated for any equipment that is linked to the node that houses the replaced FP. Alarms for linked nodes provide more status information about the operation of the replaced.

15 Return to service any disabled non-Multiservice Switch far-end equipment and verify in-service throughput. This includes unlocking or returning to service any PNNI links that were removed from service.

16 Soak the card according to your site requirements.

17 If you are doing this procedure after replacing an FP, return immediately to “Replacing a spared or unspared optical FP” (page 69) to continue replacing the FP.

If you are doing this procedure after testing an FP, you have completed the task.

Variable definitions

Variable	Value
<m>	is the slot number of the processor card.
<n>	is the number of the LP. Note the LP number of the in-service card.

Re-establishing links to the CS2000 from the replaced FP

After replacing the target FP, you must re-establish the CS2000 links on the replacement card.

Prerequisites

- The replaced FP must be unlocked.
- The status LED on the replaced FP must be solid green.

Procedure steps

1 From the CI level of the Call Server MAP, return the AMDI links to service:

```
MAPCI;MTC;XAC;AMDI

RTS <Slot> <Side_of_Shelf> <Device_Position>
<link_number>
```

2 Wait for the AMDI link to return to service and clear.

Note: If the link fails to return to service, contact Nortel Networks Global Networks Technical Support (GNTS) for assistance.

Variable values

Variable	Value
<Device_ Position>	is upper or lower for the position of the AMDI port
<link_ number>	is 0 or 1 for the link number

Variable	Value
<Side_of_ shelf>	is front or rear for the side of the shelf where the AMDI port is located
<Slot>	is the slot number in the CS2000 where IOP or HIOP is inserted

Verifying that MG4000, IW-SPM, and DPT-SPM links have returned to service

This procedure verifies that the links to the MG4000s, IW-SPMs, and DPT-SPMs have returned to service after replacing the target FP.

Prerequisites

- The replaced FP must be unlocked.
- The status LED on the replaced FP must be solid green.
- Refer to the list of connections used in "Switching MG4000, IW-SPM, or DPT-SPM traffic to the mate FP" (page 32)

Procedure steps

1 From the CI level of the Communication Server 2000 MAP, return to service the ATMRM that is currently in the MANB state:

```
MAPCI;MTC;PM;POST <spm_number>

Select ATM <x>

RTS nowait
```

Note: If the state of the ATMRM does not change to *INSV*, stop and contact Nortel Networks Global Networks Technical Support (GNTS).

2 From the CI level of the Communication Server 2000 MAP, query the ATM Framework state:

```
MAPCI NODISP;MTC;PM;POST

<spm_number>;ATMCONN;QUERY ATMFW
```

Verify the FrWk status is *PVC & SVC capable*

Verify the Saal Status is *connected*

Verify the Carrier/Physical Layer status is *Up*

Verify the Crossover APS/Layer is:

Self: XoverMode TxAct OwnRxFiber

Mate: XoverMode TxInAct MyOwnRxFiber

Note: If the state of the ATM Framework does not indicate the above noted states, stop and contact Nortel Networks GNTS.

3 From the CI level of the Communication Server 2000 MAP, check each ATM carrier assigned to an IW SPM to determine if they have returned to service:

```
MAPCI;MTC;TRKS;CARRIER

POST SPM <iwspm> OC3S
```

Note: If any link fails to return to service, contact Nortel Networks GNTS for assistance.

4 Switch traffic from the selected SPM to the replaced optical FP:

```
MAPCI NODISP;MTC;PM;POST <spm_number>

SELECT ATM <y>

PROT

MANUAL <y> <x>
```

5 For each additional MG4000, IW SPM, and DPT SPM connected to the replaced FP, repeat step 1 through to step 5.

Variable values

Variable	Value
<spm_number>	is the number of MG4000, IW-SPM, or DPT-SPM configured on the SONET ports of the replaced target FP

Variable	Value
<x>	is 0 or 1 for the number of active ATMRM that is connected to the SONET ports of the replaced target FP
<y>	is 0 or 1 (depending on <x> for the number of the inactive ATMRM that is connected to the SONET ports of the replaced target FP

Nortel Networks Multiservice Switch 15000 in Succession Networks

Replacing an OC-3/STM-1 FP

PT-AAL1/UA-AAL1

(I)SN07

Publication: NN10254-913
Document status: Standard
Document version: (I)SN07S1
Document date: September 2004
Printed in Canada

NORTEL NETWORKS