Nortel Networks

OPTera Metro 3500 Multiservice Platform
Network Surveillance

What's inside...

Telemetry byte-oriented serial (TBOS)
Provisioning path trace and modifying section trace
Provisioning the network processor
Span of control
Map topology
Provisioning TID address resolution protocol (TARP)
Test access

N⊘RTEL
NETWORKS™

Contents

Map topology   5-1

Procedures for map topology   5-1

Provisioning TID address resolution protocol (TARP)   6-1

Procedures for TARP   6-1

Test access   **7-1**

Terms and conditions   **8-1**

About this document

This document describes provisioning network surveillance features in unidirectional path-switched rings (UPSRs), bidirectional line-switched rings (BLSR), or linear configurations.

Supported software

This document supports the software releases for Nortel Networks OPTera Metro 3500 Multiservice Platform Release 12.0.

Supported hardware

This document supports the OPTera Metro 3500 shelf and Universal OPTera Metro 3500 shelf.

Hardware naming conventions

The following naming conventions are used throughout this document to identify the OPTera Metro 3500 hardware:

* The extended shelf processor (SPx) is referred to as the shelf processor.

* The extended network processor (NPx) is referred to as the network processor.

Audience

The following members of your company are the intended audience of this Nortel Networks technical publication (NTP):

* planners

* provisioners

* network administrators

* transmission standards engineers

Standards

The Telecommunications Industry Association (TIA) and the Electronics Industries Alliance (EIA) accepted RS-232 as a standard in 1997 and renumbered this standard as TIA/EIA-232. In this document, RS-232 is used to reflect current labels on the hardware and in the software for the OPTera Metro 3500 Multiservice Platform.

OPTera Metro 3500 NTP Library

EX1478p

Guides and Shelf Setup	TL1 Reference	Operations, Administration and Provisioning	Maintenance	Supporting documentation for the OPTera Metro 3500 Library
About the OPTera Metro 3500 NTP Library (323-1059-090)	TL1 Reference (323-1059-190)	System Reconfiguration (323-1059-224)	Performance Monitoring (323-1059-510)	Change Application Procedures (CAPs)
Planning and Ordering Guide (NTRN10AM)		Security and Administration (323-1059-302)	Network Surveillance (323-1059-520)	Data Communications Network Planning Guide (NTR710AM)
OPTera Connect DX/HDX, OM3000 and OC-48/TN-16X Interworking Application Guide (NTRN15AA)		Provisioning Synchronization (323-1059-310)	Alarm and Trouble Clearing (323-1059-543)	OPTera Metro 3000 series DWDM Application Guide (NTRN12AA)
OPTera Metro 3500 Network InteroperabilityGuide (NTRN16AA)		Protection Switching (323-1059-311)		OPTera Packet Edge System Planning Guide (NTRN10YK)
Installation (323-1059-201)		Bandwidth Management (323-1059-320)		OPTera Packet Edge System Network Applications and Management (NTRN11YK)
Commissioning (323-1059-210)		Provisioning Equipment and Facilities (323-1059-350)		OPTera Packet Edge System User Guide (NTN465YG)
System Testing (323-1059-222)				Site Manager Planning and Installation Guide, Rel 6.0 (NTNM35FA)

Technical support and information

For technical support and information from Nortel Networks, refer to the following table.

Technical Assistance Service	
For service-affecting problems: For 24-hour emergency recovery or software upgrade support, that is, for: • restoration of service for equipment that has been carrying traffic and is out of service • issues that prevent traffic protection switching • issues that prevent completion of software upgrades	**North America:** 1-800-4NORTEL (1-800-466-7835) **International:** 001-919-992-8300
For non-service-affecting problems: For 24-hour support on issues requiring immediate support or for 14-hour support (8 a.m. to 10 p.m. EST) on non-urgent issues.	**North America:** 1-800-4NORTEL (1-800-466-7835) ***Note:*** You require an express routing code (ERC). To determine the ERC, see our corporate Web site at www.nortelnetworks.com. Click on the Express Routing Codes link. **International:** Varies according to country. For a list of telephone numbers, see our corporate Web site at www.nortelnetworks.com. Click on the Contact Us link.
Global software upgrade support: For non-service affecting software upgrade issues	**North America:** 1-800-4NORTEL (1-800-466-7835) **International:** Varies according to country. For a list of telephone numbers, see our corporate Web site at www.nortelnetworks.com. Click on the Contact Us link.

Telemetry byte-oriented serial (TBOS)

Procedures for TBOS

Procedure 1-1
Adding a TBOS mapping assignment

Use this procedure to add a network element to the TBOS span of control of a TBOS head-end. You must have a network element defined as TBOS head-end.

Note: For descriptive information about TBOS, refer to the *Planning and Ordering Guide,* NTRN10AM. For TBOS mapping tables, refer to Mapping of TBOS displays on page 1-5 and Mapping of TBOS display points to alarms on page 1-6.

Requirements

Refer to Map Topology to ensure the existence of a connection between the new network element to add and the TBOS head-end network element. To see Map Topology, see Retrieving a new map on page 5-3.

To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the TBOS head-end network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Ensure the TBOS head-end network element is selected.
3	Select TBOS from the Faults drop-down menu.
	Note: The existing TBOS mapping assignments for the TBOS head-end are displayed.
4	Click Add to open the Add TBOS Mapping dialog box.
5	Select a number from the Display drop-down list.
	Note: You can select any number. Numbers which have been assigned to other network elements will not be available from the list.
6	Select the network element you want to add from the Network Element drop-down list.
7	Click Apply.
8	Repeat step 4 through step 7 if you have more network elements to add.
9	Click OK.

<div align="center">**—end—**</div>

Procedure 1-2
Editing a TBOS mapping assignment

Use this procedure to edit the network elements under the span of control of a TBOS head-end. You must have a network element defined as TBOS head-end.

Note: For descriptive information about TBOS, refer to the *Planning and Ordering Guide,* NTRN10AM. For TBOS mapping tables, refer to Mapping of TBOS displays on page 1-5 and Mapping of TBOS display points to alarms on page 1-6.

Requirements

Refer to Map Topology to ensure the existence of a connection between the network elements and the TBOS head-end network element. To see Map Topology, see Retrieving a new map on page 5-3.

To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the TBOS head-end network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Ensure the TBOS head-end network element is selected.
3	Select TBOS from the Faults drop-down menu.
	Note: The existing TBOS mapping assignments for the TBOS head-end are displayed.
4	Select the mapping assignment that you want to edit.
5	Click Edit to open the Edit TBOS Mapping dialog box.
6	Select the new network element for the Display number from the Network Element drop-down list.
7	Click OK.

—end—

Procedure 1-3
Deleting a TBOS mapping assignment

Use this procedure to delete a network element from the span of control of a TBOS head-end.

Note: For descriptive information about TBOS, refer to the *Planning and Ordering Guide,* NTRN10AM. For TBOS mapping tables, refer to Mapping of TBOS displays on page 1-5 and Mapping of TBOS display points to alarms on page 1-6.

Requirements

To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the TBOS head-end network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Ensure the TBOS head-end network element is selected.
3	Select TBOS from the Faults drop-down menu.
	Note: The existing TBOS mapping assignments for the TBOS head-end are displayed.
4	Select the mapping assignment that you want to delete.
5	Click Delete.

<div align="center">—end—</div>

Mapping of TBOS displays

Page	Display position	Bits
1	1 2	1 to 32 33 to 64
2	3 4	1 to 32 33 to 64
3	5 6	1 to 32 33 to 64
4	7 8	1 to 32 33 to 64
5	9 10	1 to 32 33 to 64
6	11 12	1 to 32 33 to 64
7	13 14	1 to 32 33 to 64
8	15 16	1 to 32 33 to 64

Mapping of TBOS display points to alarms

Bits	TBOS display point	Alarm
1	Critical	All critical alarms
2	Major	All major alarms
3	Minor	All minor alarms
4	Environmental Alarm #1	Environmental Alarm #1
5	Environmental Alarm #2	Environmental Alarm #2
6	Environmental Alarm #3	Environmental Alarm #3
7	Environmental Alarm #4	Environmental Alarm #4
	Note: TBOS cannot monitor environmental alarms 5 - 16.	
8	Remote	All remote alarms
9	OCn Facility Fail	OCn Rx line AIS
		OCn Rx loss of frame
		OCn Rx loss of signal
		OCn Rx RFI
		OCn Rx section trace mismatch
		OCn Rx signal failure
		OCn signal degrade
10	T3 Facility Fail	DS3 Rx AIS
		DS3 Tx AIS
		DS3 Rx loss of frame
		DS3 Tx loss of frame
		DS3 Rx loss of signal
		DS3 Tx loss of signal
		DS3 Rx bipolar violations
		DS3 Rx yellow
		DS3 loopback active
		DS3 test signal active

Bits	TBOS display point	Alarm
11	T1 Facility Fail	DS1 Rx AIS
		DS1 Tx AIS
		DS1 Rx frequency out of range
		DS1 Tx frequency out of range
		DS1 Rx loss of frame
		DS1 Tx loss of frame
		DS1 Rx loss of signal
		DS1 Tx loss of signal
		DS1 Rx out of frequency
		DS1 Rx bipolar violations
		DS1 Rx yellow
		DS1 loopback active
		DS1 test signal active
12	EC-1 Facility Fail	EC1 loopback active
		EC1 Rx AIS
		EC1 Rx loss of frame
		EC1 Rx loss of signal
		EC1 Rx RFI
13	Comm Fail	TBOS connection failure
		SDCC link failure

Bits	TBOS display point	Alarm
14	STS Path	Forced STSn path switch complete
		STS Rx loss of pointer
		STS Rx AIS
		STS Rx unequipped
		STS Rx path trace mismatch
		STS Rx signal label mismatch
		STS Rx RFI
		STS Rx excessive BIP error rate
		STS signal degrade
		STS3C Rx loss of pointer
		STS3C Rx AIS
		STS3C Rx unequipped
		STS3C Rx path trace mismatch
		STS3C Rx signal label mismatch
		STS3C Rx RFI
		STS3C Rx excessive BIP error rate
		STS3C signal degrade
		STS12C Rx AIS
		STS12C Rx excessive BIP error rate
		STS12C Rx loss of pointer
		STS12C unsupported concatenated service
		STS24C Rx AIS
		STS24C Rx excessive BIP error rate
		STS24C Rx loss of pointer
		STS48C Rx AIS
		STS48C Rx excessive BIP error rate
		STS48C Rx loss of pointer

Bits	TBOS display point	Alarm
15	VT Path	Forced VT1.5 path switch complete
		All Provisioned VTs Rx AIS
		All Provisioned VTs Rx unequipped
		All Provisioned VTs Rx signal label mismatch
		All Provisioned VTs Rx RFI
		All Provisioned VTs Rx excessive BIP error
		All Provisioned VTs Rx loss of pointer
		All Provisioned VTs Rx signal degrade
		VT Rx AIS
		VT Rx unequipped
		VT Rx signal label mismatch
		VT Rx RFI
		VT Rx excessive BIP error
		VT Rx loss of pointer
		VT Rx signal degrade
16	NP facility fail	Remote Alarm(s)
		Remote Fail
		ILAN SP Port Failure
		ILAN1 Port Failure
		ILAN2 Port Failure

Bits	TBOS display point	Alarm
17 18 19 20	OC-n equipment fail DS3, DS3x3, DS3/VT equipment fail DS1, E1-DS1 equipment fail EC-1, EC-1x3 equipment fail	BITSin-A Rx Loss of Signal BITSin-A Rx Loss of Frame BITSin-A Rx AIS BITSin-A BPV exceeds 10-3 BITSin-B Rx Loss of Signal BITSin-B Rx Loss of Frame BITSin-B Rx AIS BITSin-B BPV exceeds 10-3 Circuit pack below baseline Circuit pack mismatch Circuit pack missing Circuit pack failed Circuit pack unknown Database Corruption Detected Database Save and Restore Failed Database Restore in Progress Disk Full Duplicate SID detected Latch Open Loss of BITSout-A Pri. Timing Ref. Loss of BITSout-A Sec. Timing Ref. Loss of BITSout-B Pri. Timing Ref. Loss of BITSout-B Sec. Timing Ref. Loss of shelf primary timing reference Loss of shelf secondary timing reference Loss of traffic Low voltage Power failure-A Power failure-B SP version mismatch Transport data recovery failed Upgrade failed

Bits	TBOS display point	Alarm
22	Sync Alarm	Loss of BITSout-A Pri. timing ref.
		Loss of BITSout-A Sec. timing ref.
		Loss of BITSout-B Pri. timing ref.
		Loss of BITSout-B Sec. timing ref.
		BITSin-A Rx Loss of signal
		BITSin-A Rx Loss of frame
		BITSin-A Rx AIS
		BITSin-A Rx BPV exceeds 10-3
		BITSin-B Rx Loss of signal
		BITSin-B Rx Loss of frame
		BITSin-B Rx AIS
		BITSin-B Rx BPV exceeds 10-3
		Circuit pack failed - Sync
		Shelf Pri Ref Rx Degraded SSM
		Shelf Sec Ref Rx Degraded SSM
		BITSout-A Pri Ref Rx Degraded SSM
		BITSout-A Sec Ref Rx Degraded SSM
		BITSout-B Pri Ref Rx Degraded SSM
		BITSout-B Sec Ref Rx Degraded SSM
		PLL not locked to timing
24	NP Equipment Fail	Circuit pack missing
		Circuit pack failed
		Circuit pack mismatch
		Circuit pack unknown
25	Ethernet Facility Fail	Bridge port not in forwarding state
		Link pulse missing
26	Ethernet Equipment Fail	Circuit pack missing
		Circuit pack mismatch
		Circuit pack failed
		Intercard fail
		Intercard suspected
29	Critical (remote)	All critical alarms appearing on network elements connected by fiber to the TBOS head-end network element and under the TBOS span of control of the head-end network element.

Bits	TBOS display point	Alarm
30	Major (remote)	All major alarms appearing on network elements connected by fiber to the TBOS head-end network element and under the TBOS span of control of the head-end network element.
31	Minor (remote)	All minor alarms appearing on network elements connected by fiber to the TBOS head-end network element and under the TBOS span of control of the head-end network element.
32 (Reserved)		
Note: TBOS cannot monitor environmental alarms 5 - 16.		

Provisioning path trace and modifying section trace

Procedures for section and path trace

Procedure 2-1
Retrieving section trace messages

Use this procedure to retrieve the section trace values on OC-n facilities.

Step	Action
1	Ensure you are logged in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Ensure the network element is selected in the navigation tree.
3	Select Equipment & Facility Provisioning from the Configuration drop-down menu.
4	Select an optical interface circuit pack from the Equipment area.
5	Select the port number from the Facility area.
6	Click Section Trace in the Facility area to open the Section Trace dialog box.
	Note 1: The section trace fail mode, format, and section trace values are displayed. For a description of the fail modes, see Section trace fail mode options on page 2-3.
	Note 2: You can have multiple Section Trace dialog boxes opened at the same time.
7	Click OK to close the Section Trace dialog box.

<div align="center">**—end—**</div>

Section trace fail mode options

Fail mode options	Description
Alarms off	All alarms are off. There is no traffic protection.
Alarms on	All alarms are on. There is no traffic protection.
Alarms on, with traffic protection	All alarms are on with full traffic protection.

Procedure 2-2
Editing section trace messages

Use this procedure to edit the section trace fail mode, format, and section trace values on OC-n facilities.

The value to transmit, and the value to expect in the receive direction can be in either string or numeric format:

- STRING - 15 bytes long printable alphanumeric ASCII string

  Note: The following characters are not supported:
  comma (,), semicolon (;), colon (:), equal sign (=), question mark (?), percent sign (%), and double quote (")

- NUMERIC - any value from 0 through 255 in decimal integer form

Requirement

To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Ensure the network element is selected in the navigation tree.
3	Select Equipment & Facility Provisioning from the Configuration drop-down menu.
4	Select an optical interface circuit pack from the Equipment area.
5	Select the port number from the Facility area.
6	Click Section Trace in the Facility area to open the Section Trace dialog box.
	Note: You can have multiple Section Trace dialog boxes opened at the same time.

Procedure 2-2 (continued)
Editing section trace messages

Step	Action
7	Select a section trace fail mode from the Fail mode drop-down list. For a description of the fail mode, see Section trace fail mode options on page 2-3. ***Note:*** If you select the fail mode Alarms on, with traffic protection, you cannot edit the other parameters in the Section Trace dialog box.
8	Select a format from the Format drop-down list. ***Note:*** Changing the format returns the expected Rx and transmitted values to default.
9	Enter the expected Rx value.
10	Enter the transmitted value.
11	If the Section Trace dialog box includes an OC48 interworking check box and the facility is interworking with a SONET network element other than OPTera Metro 3000, select the check box.
12	You can click on the Retrieve button, to retrieve the actual incoming section trace values or click OK to close the Section Trace dialog box.

—**end**—

Procedure 2-3
Retrieving path trace messages

Use this procedure to retrieve path trace values for DS3 or OC-n facilities.

Note: If there are no cross-connects, you cannot retrieve path trace values.

Step	Action
1	Ensure you are logged in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Ensure the network element is selected in the navigation tree.
3	Select Equipment & Facility Provisioning from the Configuration drop-down menu.
4	Select an optical interface or DS3 circuit pack from the Equipment area.
5	Select the port number from the Facility area.
6	Click Path Trace in the Facility area to open the Path Trace dialog box.
	Note: If there are no cross-connects, the Path Trace button is disabled.
7	For OC-n facilities, select an STS number from the drop-down list.
	Note 1: For both DS3 and OC-n facilities, the expected incoming path trace message is displayed in the Expected Rx field, and the outgoing path trace message is displayed in the Transmitted field.
	Note 2: If the facility is OOS, the actual Rx value cannot be retrieved.
8	Click OK to close the Path Trace dialog box.

—*end*—

Procedure 2-4
Enabling or disabling path trace messages

Use this procedure to enable or disable path trace monitoring for DS3 or OC-n facilities.

> *Note:* If there are no cross-connects, you cannot enable or disable path trace monitoring.

Requirement
To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Ensure the network element is selected in the navigation tree.
3	Select Equipment & Facility Provisioning from the Configuration drop-down menu.
4	Select an optical interface or DS3 circuit pack from the Equipment area.
5	Select the port number from the Facility area.
6	Click Path Trace in the Facility area to open the Path Trace dialog box.
	Note: If there are no cross-connects, the Path Trace button is disabled.
7	For OC-n facilities, select an STS number from the drop-down list.
8	For both DS3 and OC-n facilities, select the Path trace enabled check box to enable path trace monitoring, or deselect the check box to disable path trace monitoring as you want.
9	Click OK to close the Path Trace dialog box.

—**end**—

Procedure 2-5
Editing path trace messages

Use this procedure to edit path trace values for DS3 or OC-n facilities.

Note: If there are no cross-connects, you cannot retrieve path trace values.

You can enter a string of up to 62 characters to provision a path trace message. The following characters are not supported when provisioning a path trace message: comma (,), semicolon (;), colon (:), equal sign (=), percent sign (%), question mark (?), and double quotes (").

Requirement

To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the network element. For instructions, see .
2	Ensure the network element is selected in the navigation tree.
3	Select Equipment & Facility Provisioning from the Configuration drop-down menu.
4	Select an optical interface or DS3 circuit pack from the Equipment area.
5	Select the port number from the Facility area.
6	Click Path Trace in the Facility area to open the Path Trace dialog box. *Note:* If there are no cross-connects, the Path Trace button is disabled.
7	For OC-n facilities, select an STS number from the drop-down list.
8	For both DS3 and OC-n facilities, select or deselect the Path trace enabled check box, to enable or disable path trace monitoring as you want.
9	Enter the expected Rx value.
10	Enter the transmitted value.
11	Click OK to close the Path Trace dialog box.

—**end**—

Provisioning the network processor

Procedures for network processor facilities

Procedure 3-1
Adding a network processor facility

Use this procedure to provision a facility on the network processor.

DANGER
Do not create an ILAN loop. ILAN loops can degrade the performance of the network processor and cause the network processor circuit pack to fail.

Requirements

To perform this procedure you must

- use an account with a level 3 user privilege code (UPC) or higher

- ensure that the appropriate cable and connection are present before provisioning a facility

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select NP Facility from the Configuration drop-down menu.
4	Click Add to open the Add NP Facility dialog box.
	Note: The Add button is disabled when all NP facilities have been provisioned.
5	Select an unprovisioned facility type from the Facility type drop-down list.
6	Click OK.

—end—

Procedure 3-2
Editing a COLAN facility

Use this procedure to edit a central office local area network (COLAN) facility.

Requirements

To perform this procedure you must

- ensure that the network processor (NPx) is accessible.

    Note: When a restart has occurred, you cannot access the NPx until the NPx database is released.

- use an account with a level 3 user privilege code (UPC) or higher.
- obtain the IP address and associated parameters (network mask, default gateway, broadcast address) to be assigned to COLAN from the network administrator.

    Note 1: The assigned IP address and all associated parameters must be in the standard dot notation, n.n.n.n. ($0 \leq n \leq 255$), for example, 47.45.5.38.

    Note 2: Unique IP addresses for every individual network processor are suggested because it reduces the risk of duplicate IP addresses in a network.

    Note 3: The network processor IP address is copied and stored on the co-located SP only when the NPx and the co-located SP are running the same release software. If the NPx software release is different from that of the colocated SP software, the NPx does not copy its provisioning data (including IP address) to the colocated SP. If the NPx IP address is different from the stored NPx IP address on the SP, then upon restart or NPx replacement, the desired IP address must be manually provisioned into the NPx.

    Note 4: Regardless of whether the NPx has copied its provisioning data and IP address to the colocated SP, upon restart or NPx replacement, the NPx retrieves whatever NPx provisioning data is available (including the stored NPx IP address) from the colocated SP.

    Note 5: When you provision the IP address using this procedure, a gratuitous ARP (address resolution protocol) message is broadcasted. This ARP message purges router ARP tables of the original network processor hardware address with the new network processor hardware address. This technique allows IP communications to the network processor to recover within minutes following the replacement of the network processor circuit pack.

—continued—

Procedure 3-2 (continued)
Editing a COLAN facility

Note 6: Some routers may not support gratuitous ARP. In this case, IP communication to the replacement network processor is unavailable until the original network processor hardware address entry in the router ARP table expires.

Note 7: The editing of the gateway address parameter to a non-zero value fails if the IP address parameter is not compatible with the gateway address parameter. The addresses are compatible as long as the network part of the addresses match. The network part of an address is obtained by performing a bit-wise and operation on that address with the network mask. For example, if the network mask is set to 255.0.0.0 then 47.u.v.w and 47.x.y.z are compatible. As a second example, if the network mask is set to 255.128.0.0 then 47.u.v.w and 47.x.y.z are compatible as long as the most significant bit of u and x match (that is u and x are both $\geq$ 128 or u and x are both $<$ 128). As a third example, if the network mask is set to 255.255.0.0 then 47.u.v.w and 47.x.y.z are compatible as long as u = x. All variables are in the range of 0 through 255.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select NP Facility from the Configuration drop-down menu.
4	Select COLAN from the NP Facility table.
5	Click Edit to open the Edit COLAN dialog box.
6	Enter the parameter values as required. See COLAN parameters on page 3-5.
7	Click OK.

—**end**—

COLAN parameters

Parameter	Valid value	Description
GATEWAY	0.0.0.0 (default) n.n.n.n	COLAN default gateway Router for packets with unknown destination. The value 0.0.0.0 will delete the currently provisioned gateway.
NETMASK	0.0.0.0 (default) Class A: 255.n.n.n Class B: 255.255.n.n Class C: 255.255.255.n Class D: 255.255.255.n Class E: 255.255.255.n	COLAN network mask The value 0.0.0.0 means that the network mask is assigned automatically by the network processor, based on the network class of the IP address.
BROADCAST	0.0.0.0 (default) n.n.n.n	COLAN broadcast address The value 0.0.0.0 means the broadcast address is assigned automatically by the network processor based on the IP address.

Procedure 3-3
Editing X.25 parameters

Use this procedure to view and edit the upper layer, lower layer, or physical port parameters on an X.25 facility.

To edit the virtual circuit parameters, see Editing the PVC parameter values on page 3-12, and Editing the SVC parameter values on page 3-14.

Requirement

To perform this procedure you must use an account with a level 3 user privilege code (UPC) or higher.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select NP Facility from the Configuration drop-down menu.
4	Select X25 from the NP Facility table.
5	Click Edit to open the Edit X25 dialog box.
6	Select the Upper Layer, Lower Layer, or Physical Port tab as required. For more information on the parameters, see Upper layer parameters on page 3-7, Lower layer parameters on page 3-9, and Physical port parameters on page 3-10.
7	Edit the parameters as required. *Note 1:* For Upper Layer parameters, the CCITT version, Maximum circuits, and Maximum DTE interfaces parameters are not editable. *Note 2:* For Lower Layer parameters, the Number of LAPB, and Type parameters are not editable.
8	Click OK.

—*end*—

Upper layer parameters

Parameter	Range	Default	Description
CCITT Version			The CCITT version number is not editable.
Maximum circuits			The maximum number of supported circuits is not editable.
Maximum DTE interfaces			The maximum number of supported DTE interfaces is not editable.
Negotiate flow control (NFC)	On or Off		Can only select from the drop-down list.
Tx packet size	16-4096		NFC transmission packet size
Rx packet size	16-4096		NFC receive packet size
Tx window size	Based on Modulus value		The NFC transmission window size is based on the modulus value. If the Modulus value is 8, the range is from 1 to 7. If the Modulus value is 128, the range is from 1 to 127.
Rx window size	Based on Modulus value		The NFC receive window size is based on the modulus value. If the Modulus value is 8, the range is from 1 to 7. If the Modulus value is 128, the range is from 1 to 127.
Negotiate throughput class	On or Off		Can only select from the drop-down list.
Speed of transmitter	7-11		Can only select from the drop-down list.
Speed of receiver	7-11		Can only select from the drop-down list.
Network user id	Maximum 20 characters		Network user ID (SVC only)
MODULUS	8 or 128	8	modulus value
Maximum Tx size	16-4096	128	Maximum transmitting packet size
Maximum Rx size	16-4096	128	Maximum receiving packet size
Window size	Based on Modulus value	2	The packet window size is based on the modulus value. If the Modulus value is 8, the range is from 1 to 7. If the Modulus value is 128, the range is from 1 to 127.
T20	5-500 seconds	180 seconds	DTE restart time-out (5-second increments)
T21	5-500 seconds	200 seconds	DTE call request time-out (5-second increments)

T22	5-500 seconds	180 seconds	DTE reset time-out (5-second increments)
T23	5-500 seconds	180 seconds	Declare time-out (5-second increments)
N20	1-255	1	Number of T20 retries
N22	1-255	1	Number of T22 retries
N23	1-255	1	Number of T23 retries
D-Bit	Yes or No	Yes	Delivery Confirmation Option

Lower layer parameters

Parameter	Range	Default	Description
Number of LAPB			The number of LAPB links is not editable.
TYPE			Data terminal equipment. This parameter is not editable.
Modulus	8 or 128	8	modulus value
K	Based on the Modulus value		Window size for transmitter is based on the modulus value. If the Modulus value is 8, the range is from 1 to 7. If the Modulus value is 128, the range is from 1 to 127.
T1	500-10000 milliseconds	500 ms	Acknowledgment timer (500-ms increments)
T3	10000-300000 milliseconds	30000 ms	Link inactivity timer (500-ms increments)
N1	1080-16440 bits	1080 bits	Maximum length of an I frame (increments of 8 bits)
N2	1-30	30	Maximum number of retransmissions

Physical port parameters

Parameter	Range	Default	Description
CTS pin enabled	selected for enabled, or deselected for disabled	selected	To enable or disable CTS pin configuration
DCD pin enabled	selected for enabled, or deselected for disabled	deselected	To enable or disable DCD pin configuration
DSR pin enabled	selected for enabled, or deselected for disabled	deselected	To enable or disable DSR pin configuration
DSR on	selected for enabled, or deselected for disabled	selected	To enable or disable DSR pin initial value when DSR pin is enabled
DTR pin enabled	selected for enabled, or deselected for disabled	selected	To enable or disable DTR pin configuration
DTR on	selected for enabled, or deselected for disabled	selected	To enable or disable DTR pin initial value when DTR pin is enabled
RTS pin enabled	selected for enabled, or deselected for disabled	selected	To enable or disable RTS pin configuration
RTS	On, Off, or Auto	On	To enable or disable RTS pin initial value when RTS pin is enabled. When Auto is selected, the RTS value is under hardware control.
Receive	Rx External, or Tx External	Rx External	Source of receive clock
Transmit	Rx External, or Tx External	Tx External	Source of transmit clock

Procedure 3-4
Changing a SVC to a PVC

Use this procedure to

- change a switched virtual circuit (SVC) to a permanent virtual circuit (PVC)

- provision the PVC

For parameter values, see Virtual circuit parameters on page 3-15.

Requirement

To perform this procedure you must use an account with a level 3 user privilege code (UPC) or higher.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select NP Facility from the Configuration drop-down menu.
4	Select X25 from the NP Facility table.
5	Click Edit to open the Edit X25 dialog box.
6	Select the Virtual Circuit tab.
7	Select the virtual circuit number from the Circuit number drop-down list.
8	Select PVC from the Type drop-down list.
9	Enter a value in the Logical channel number field.
	Note: The Logical channel number must be provisioned for a PVC. The value can be of 0 to 255.
10	Select a value from the Logical channel group number drop-down list.
	Note: The Logical channel group number must be provisioned for a PVC.
11	Edit other parameters as required.
12	Click OK.
	Note: If you want to edit the PVC parameter values, see Editing the PVC parameter values on page 3-12.

—**end**—

Procedure 3-5
Editing the PVC parameter values

Use this procedure to edit the permanent virtual circuit (PVC) parameter values.

For parameter values, see Virtual circuit parameters on page 3-15.

Requirement

To perform this procedure you must use an account with a level 3 user privilege code (UPC) or higher.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select NP Facility from the Configuration drop-down menu.
4	Select X25 from the NP Facility table.
5	Click Edit to open the Edit X25 dialog box.
6	Select the Virtual Circuit tab.
7	Select the PVC number from the Circuit number drop-down list.
8	Edit the parameters as required.
9	Click OK.

<div align="center">—end—</div>

Procedure 3-6
Changing a PVC to a SVC

Use this procedure to change a a permanent virtual circuit (PVC) to a switched virtual circuit (SVC).

To change a PVC to a SVC, the PVC is deleted and the circuit is restored as an SVC with default parameter values based on the upper layer X.25 parameters.

Requirement

To perform this procedure you must use an account with a level 3 user privilege code (UPC) or higher.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select NP Facility from the Configuration drop-down menu.
4	Select X25 from the NP Facility table.
5	Click Edit to open the Edit X25 dialog box.
6	Select the Virtual Circuit tab.
7	Select the virtual circuit number from the Circuit number drop-down list.
8	Select SVC from the Type drop-down list.
9	Click Apply.
10	Click Yes in the confirmation dialog box.
	Note: If you want to edit the SVC parameter values, see Editing the SVC parameter values on page 3-14.

—*end*—

Procedure 3-7
Editing the SVC parameter values

Use this procedure to edit the switched virtual circuit (SVC) parameter values.

The SVC parameters are automatically assigned default values based on the upper layer X.25 parameters. When you edit the upper layer parameters, the changes apply to all SVCs.

For parameter values, see Virtual circuit parameters on page 3-15, or Upper layer parameters on page 3-7.

Requirement

To perform this procedure you must use an account with a level 3 user privilege code (UPC) or higher.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select NP Facility from the Configuration drop-down menu.
4	Select X25 from the NP Facility table.
5	Click Edit to open the Edit X25 dialog box.
6	Select the Upper Layer tab.
7	Edit the following parameter values as required: Window size, T21, T22, T23, N22, N23, and D-Bit.
8	Click Apply.

Note: To view the changes, select the Virtual Circuit tab, the SVC parameters are assigned default values based on the upper layer X.25 parameters.

—**end**—

Virtual circuit parameters

Parameter	Range	Default	Description
D-Bit	Yes/No	Yes	Delivery confirmation option
Maximum receiving packet size	16-4096	128	
Maximum transmitting packet size	16-4096	128	
N22	1-255	1	Number of T22 retries
N23	1-255	1	Number of T23 retries
T21	5-500 seconds	200 seconds	DTE call request time-out (5-second increment)
T22	5-500 seconds	180 seconds	DTE reset time-out (5-second increment)
T23	5-500 seconds	180 seconds	Declare time-out (5-second increment)
Window size	Based on the Modulus value	2	The packet window size is based on the modulus value. If the Modulus value is 8, the range is from 1 to 7. If the Modulus value is 128, the range is from 1 to 127.

Procedure 3-8
Retrieving the manual area addresses of the network processor

Use this procedure to retrieve the manual area addresses of the open systems interconnection (OSI) stack on the network processor.

A manual address identifies the network to which the network element or network processor belongs.

Requirement

To perform this procedure, you must

- ensure that the network processor is accessible
- use an account with a level 4 user privilege code (UPC) or higher

    Note: When a restart has occurred, you cannot access the network processor until the network processor database is released.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select Node Information from the Configuration drop-down menu.
4	Click Upper Layer SDCC to open the Upper Layer SDCC dialog box.
	Note: All the manual area addresses previously provisioned are displayed.
5	Click Cancel.

—end—

Procedure 3-9
Adding or editing a manual area address

Use this procedure to add or edit a manual area address. Three manual area addresses can be provisioned. A manual address identifies the network to which the network element or network processor belongs. When the network processor is provisioned, manual area address number 1 has a default setting of 490000 (Nortel network address).

The manual area address is a string of 6 through 26 hexadecimal characters:

- numbers zero through nine
- letters A through F

You must have at least one manual area address provisioned. For example, if you want to edit the address in manual area address number 1 and it is the only address provisioned, you must first provision an address in manual area address number 2 or 3. Ensure that all other nodes in the network share the same manual area address before deleting the address in manual area address number 1.

⚠ **CAUTION**
Risk of traffic loss
This procedure can affect traffic carried by the network element. Do not edit a manual area address if it is the only manual area address shared with the network element(s) with which it is communicating.

Note: OSI routing requires that entities required to communicate with each other (for example, a shelf processor and a network processor) share a common area address. A network processor and its co-located shelf processor must always have a common area address for proper operation. This is particularly important after a network processor restart (including network processor replacement and insertion) to allow the network processor to recover its database from the co-located shelf processor. This is also required for site commissioning of a new network processor which has no other means of communications other than shelf processor-network processor through ILAN over the backplane (see *Commissioning,* 323-1059-210 for information on site commissioning a network processor).

—**continued**—

Procedure 3-9 (continued)
Adding or editing a manual area address

Requirements

To perform this procedure, you must

- ensure that the network processor is accessible

- use an account with a level 4 user privilege code (UPC) or higher

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select Node Information from the Configuration drop-down menu.
4	Click Upper Layer SDCC to open the Upper Layer SDCC dialog box.
5	Do one of the following as required: • Select a blank row to add a manual area address. • Select an existing manual area address to edit it. *Note:* You cannot edit a manual area address if it is the only one in the Upper Layer SDCC dialog box.
6	Click Edit to open the Edit Manual Area Address dialog box.
7	Enter either the whole area address or the area address components. See Manual Area Address components on page 3-19. *Note:* If you enter the area address components, and after you have completed the Domain field, you see that four zeros pop up in the Area address field (in between the organization ID and the domain), do not delete the four zeros.
8	Click OK. *Note:* The list of area addresses is updated in the Upper Layer SDCC dialog box.
9	Click Cancel to close the dialog box.

—end—

Manual Area Address components

Address component	Range
Address format ID	Maximum 2 hexadecimal characters
Initial domain ID	Maximum 4 hexadecimal characters
DSP format ID	Maximum 2 hexadecimal characters
Organization ID	Maximum 6 hexadecimal characters
Domain	Maximum 4 hexadecimal characters
Area	Maximum 4 hexadecimal characters
Note: Contact your system administrator if you do not know the area address components for your network.	

Procedure 3-10
Deleting a manual area address

Requirements

To perform this procedure, you must

- use an account with a level 4 user privilege code (UPC) or higher

- ensure that the network processor is accessible

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select Node Information from the Configuration drop-down menu.
4	Click Upper Layer SDCC to open the Upper Layer SDCC dialog box.
5	Select a manual area address from the list.
6	Click Delete.
	Note: If the address selected is the only one on the list, the Delete button is disabled.
7	Click Cancel to close the dialog box.

—end—

Procedure 3-11
Deleting a network processor facility

Requirement

To perform this procedure you must use an account with a level 3 user privilege code (UPC) or higher.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select NP Facility from the Configuration drop-down menu.
4	Select a facility from the NP Facility table.
5	Click Delete.
	Note: The Delete button is disabled if ILANSP or ILANNP is selected. They are autoprovisoned and cannot be deleted.
6	Click Yes in the confirmation dialog box.

—*end*—

Span of control

Procedures for span of control

Procedure 4-1
Retrieving network elements in the span of control of a network processor

Requirement

To perform this procedure, you must ensure that the network processor is accessible. If a restart has occurred, you cannot access the network processor until the network processor database is released.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor (NP) in the navigation tree.
3	Select the NP Span of Control from the Configuration drop-down menu.
4	Select the Show both accounts check box to display the NP Span of control table of both level 5 accounts.

—end—

Procedure 4-2
Adding a network element to the span of control of a network processor

Use this procedure to add a network element to a network processor (NP) span of control.

When only one level 5 user account is active on a network processor, the network processor can have a maximum of sixteen network elements in its span of control. The network processor allows up to two level 5 users to retrieve alarms and events from the network elements within its span of control. If two level 5 user accounts are active, the number of network elements in the network processor span of control is reduced by half. In addition, each level 5 account user on the network processor must access the same network elements in the network processor span of control.

Requirements

To perform this procedure you must

- use an account with a level 4 user privilege code (UPC) or higher
- ensure that the network processor is accessible. If a restart has occurred, you cannot access the network processor until the network processor database is released.

Step	Action
1	Log in to the NP. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the NP in the navigation tree.
3	Select Span of Control from the Configuration drop-down menu.
4	Click Add to open the Add to Span of Control dialog box.
5	Select the network element to add from the network element table. You can select multiple network elements by pressing the Ctrl key while you select.
6	Enter the user identifier and password of the network element.
	Note: If centralized security administration (CSA) is enabled on both the NP and the network element, only the user identifier is required. The span of control application will only log in successfully if the NP and network element have the same shared secret. See 323-1059-302, "Centralized security administration" for information on setting the CSA state and shared secret. If CSA is disabled on either the NP or network element, both the user identifier and password are required.
7	Click OK.

—continued—

Procedure 4-2 (continued)
Adding a network element to the span of control of a network processor

Step	Action
8	In the Span of Control window, check the Release column to determine if there are any network elements running pre-Release 11.0/11.1 software.

9	**If**	**Then**
	there **are no** network elements in your SOC running pre-Release 11.0/11.1 software	you have completed this procedure
	there **are** network elements in your SOC running pre-Release 11.0/11.1 software	go to step 10

Ensuring the SOC list is ordered correctly

10

> ⚠️ **CAUTION**
> **Temporary loss of surveillance**
> Performing the following steps of this procedure will disable surveillance for up to 2 minutes on network elements that are removed and then added to the NPx SOC.

In the File menu, click CommLog, then select the NPx for this SOC.

11   In the Configuration menu, select Span of Control.

12   Click Refresh.

13   In the CommLog, note the list order of the network elements in your SOC.

14	**If**	**Then**
	there are pre-Release 11.0/11.1 network elements listed above Release 11.0/11.1/12.0 network elements in the CommLog SOC list	go to step 15
	there are no pre-Release 11.0/11.1 network elements listed above Release 11.0/11.1/12.0 network elements in the CommLog SOC list	you have completed this procedure.

15   Record all of the pre-Release 11.0/11.1 network elements listed (in the CommLog SOC list) above Release 11.0/11.1/12.0 network elements.

—**continued**—

Procedure 4-2 (continued)
Adding a network element to the span of control of a network processor

Step	Action
16	For each network element recorded in step 15, retrieve the protection scheme of the optical interfaces linking to the other network elements of the SOC.
	a. In the navigation tree, select the network element.
	b. In the Protection menu, select Status.
	c. In the Protection Status window, under Protection summary, select the line rate of the optical interface linking to the network.
	d. Under OCn equipment protection details, determine the protection scheme of the optical interface linking to the network.
	e. If the protection scheme is not 1+1, then remove this network element from your recorded list of network elements (recorded in step 15).
17	In the navigation tree, select the NPx.
18	In the Configuration menu, select Span of Control.
19	In the Span of Control window, select the network elements in your list recorded in step 15.
	a. Select one network element in the list.
	b. For each subsequent network element, hold down the CTRL key while selecting the network element.
20	Click Delete.
21	Click Yes in the confirmation dialog box.
22	In the Span of Control window, click Add.
23	In the Add to Span of Control dialog box, select the network elements recorded in step 15.
	Note: If some of the network elements require different user IDs and/or passwords from one another, then only group together those network elements that share the same user ID and password.
	a. Select one network element in the list.
	b. For each subsequent network element, hold down the CTRL key while selecting the network element.
24	In the User ID box, enter the required user ID.
25	In the Password box, enter the required password.
26	Click Apply.
27	If all of the network elements recorded in step 15 have not yet been re-added to the SOC, then perform step 23 to step 27 for the next grouping of network elements with common user ID and password.
28	Click OK.

—**end**—

Procedure 4-3
Removing a network element from the span of control of a network processor

Requirements

To perform this procedure you must

- use an account with a level 4 user privilege code (UPC) or higher

- ensure that the network processor is accessible. If a restart has occurred, you cannot access the network processor until the network processor database is released.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor (NP) in the navigation tree.
3	Select the NP Span of Control from the Configuration drop-down menu.
4	Select the Show both accounts check box to display the NP Span of Control table of both level 5 accounts.
5	Select the network element to delete from the NP Span of Control table.
	Note: You can select multiple network elements by pressing Ctrl while you select.
6	Click Delete.
7	Click Yes in the confirmation dialog box.

—**end**—

Map topology

Procedures for map topology

Background menu procedures

Options menu procedures

Miscellaneous procedures

Procedure 5-1
Retrieving a new map

Use this procedure to display a new map of a network.

The map view provides a graphical display of all network elements in a network processor (NP) span of control, as well as the adjacent neighbors of those network elements.

Note 1: Opening Map Topology will automatically provide a new map if a map has not been saved before in Site Manager default directory. However, if a map of a network processor has been saved in the default directory, opening Map Topology for the network processor will load the saved map from the default directory. In that case, you use this procedure if you want to display a new map instead of the saved map.

Note 2: For the map view to display connections between a network element within the NP span of control and an adjacent neighbor outside the span of control, the network element and its adjacent neighbor must be connected through a section data communication channel (SDCC). The SDCC connection can occur through any OC-n, EC-1, or EC-1x3 circuit pack. EC-1x12 circuit packs do not support SDCC.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	In the Configuration menu, select Span of Control.
4	In the Span of Control window, check the Release column to determine if there are any network elements running pre-Release 11.0/11.1 software.

Step	If	Then go to
5	there **are no** network elements in your SOC running pre-Release 11.0/11.1 software	step 26
	there **are** network elements in your SOC running pre-Release 11.0/11.1 software	step 6

—continued—

Procedure 5-1 (continued)
Retrieving a new map

Step	Action

6

> ⚠ **CAUTION**
> **Temporary loss of surveillance**
> Performing the following steps of this procedure will disable surveillance for up to 2 minutes on network elements that are removed and then added to the NPx SOC.

In the File menu, click CommLog, then select the NPx for this SOC.

7   In the Configuration menu, select Span of Control.

8   Click Refresh.

9   In the CommLog, note the list order of the network elements in your SOC.

10

If	Then go to
there are pre-Release 11.0/11.1 network elements listed above Release 11.0/11.1/12.0 network elements in the CommLog SOC list	step 11
there are no pre-Release 11.0/11.1 network elements listed above Release 11.0/11.1/12.0 network elements in the CommLog SOC list	step 26

11   Record all of the pre-Release 11.0/11.1 network elements listed (in the CommLog SOC list) above Release 11.0/11.1/12.0 network elements.

12   For each network element recorded in step 11, retrieve the protection scheme of the optical interfaces linking to the other network elements of the SOC.

    a.   In the navigation tree, select the network element.

    b.   In the Protection menu, select Status.

    c.   In the Protection Status window, under Protection summary, select the line rate of the optical interface linking to the network.

    d.   Under OCn equipment protection details, determine the protection scheme of the optical interface linking to the network.

    e.   If the protection scheme is not 1+1, then remove this network element from your recorded list of network elements (recorded in step 11).

—**continued**—

Procedure 5-1 (continued)
Retrieving a new map

Step	Action
13	If there are no network elements remaining in your recorded list (begun in step 11), then go to step 26.
14	In the navigation tree, select the NPx.
15	In the Configuration menu, select Span of Control.
16	In the Span of Control window, select the network elements in your list recorded in step 11.
	a. Select one network element in the list.
	b. For each subsequent network element, hold down the CTRL key while selecting the network element.
17	Click Delete.
18	Click Yes in the confirmation dialog box.
19	In the Span of Control window, click Add.
20	In the Add to Span of Control dialog box, select the network elements recorded in step 11.
	Note: If some of the network elements require different user IDs and/or passwords from one another, then only group together those network elements that share the same user ID and password.
	a. Select one network element in the list.
	b. For each subsequent network element, hold down the CTRL key while selecting the network element.
21	In the User ID box, enter the required user ID.
22	In the Password box, enter the required password.
23	Click Apply.
24	If all of the network elements recorded in step 11 have not yet been re-added to the SOC, then perform step 20 to step 24 for the next grouping of network elements with common user ID and password.
25	Click OK.
26	Select Map Topology from the Configuration drop-down menu.
27	Select New map from NP from the File drop-down menu of Map Topology.
	Note 1: There is a pause while the map is drawn.
	Note 2: If you perform a reconfiguration procedure and the Map Topology window is open, a deleted link or network element will display as deleted. To completely remove a deleted link or network element from the map, select New map from NP from the File drop-down menu.

—**end**—

Procedure 5-2
Saving a map

Use this procedure to save a map of a network.

You can save a map in the Site Manager default directory, or a specific directory.

> *Note:* If a map of a network processor has been saved in the default directory with a default name, opening Map Topology of the network processor will automatically load the saved map from the default directory. To set the default directory, see Setting the default directory to save a map on page 5-7.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3.
2	Select Save map to file from the File drop-down menu.
3	Browse for and select the location where you want to save the map in the Save Map File dialog box. *Note 1:* Your selected location is displayed in the Look in field. *Note 2:* If you want to save a map to be loaded as the default map for a network processor, select the default directory.
4	Enter a file name in the File name field. *Note 1:* To save a map to be loaded as the default map for a network processor, name the file TID.map where TID is the target identifier or name of the network processor. *Note 2:* You can find the TID of the network processor within the brackets [] in the title bar of the Map Topology window.
5	Click Save.

—end—

Procedure 5-3
Setting the default directory to save a map

Use this procedure to set the default directory in Site Manager.

If a default map of a network processor has been saved in the default directory, opening Map Topology of the network processor will automatically load the saved map from the default directory.

Step	Action
1	Start Site Manager.
2	Click Cancel in the Login dialog box.
3	Select Preferences from the Edit drop-down menu.
4	Select the Default Directory tab.
5	Click Choose.
6	Browse for and select a location that you want in the Select default directory dialog box.
	Note: Your selected location is displayed in the File name field.
7	Click Select.
8	Click OK in the Edit Preferences dialog box.

—**end**—

Procedure 5-4
Retrieving an existing map

Use this procedure to retrieve a network map from a specific directory.

Note: Opening Map Topology will automatically load the map saved in the Site Manager default directory, if a map has been saved in the default directory.

Step	Action
1	Log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select a network processor in the navigation tree.
3	In the Configuration menu, select Span of Control.
4	In the Span of Control window, check the Release column to determine if there are any network elements running pre-Release 11.0/11.1 software.

5	**If**	**Then** go to
	there **are no** network elements in your SOC running pre-Release 11.0/11.1 software	step 26
	there **are** network elements in your SOC running pre-Release 11.0/11.1 software	step 6

6

CAUTION
Temporary loss of surveillance
Performing the following steps of this procedure will disable surveillance for up to 2 minutes on network elements that are removed and then added to the NPx SOC.

In the File menu, click CommLog, then select the NPx for this SOC.

7	In the Configuration menu, select Span of Control.
8	Click Refresh.
9	In the CommLog, note the list order of the network elements in your SOC.

—continued—

Procedure 5-4 (continued)
Retrieving an existing map

Step	Action

10	**If**	**Then** go to
	there are pre-Release 11.0/11.1 network elements listed above Release 11.0/11.1/12.0 network elements in the CommLog SOC list	step 11
	there are no pre-Release 11.0/11.1 network elements listed above Release 11.0/11.1/12.0 network elements in the CommLog SOC list	step 26

11   Record all of the pre-Release 11.0/11.1 network elements listed (in the CommLog SOC list) above Release 11.0/11.1/12.0 network elements.

12   For each network element recorded in step 11, retrieve the protection scheme of the optical interfaces linking to the other network elements of the SOC.

    a.   In the navigation tree, select the network element.

    b.   In the Protection menu, select Status.

    c.   In the Protection Status window, under Protection summary, select the line rate of the optical interface linking to the network.

    d.   Under OCn equipment protection details, determine the protection scheme of the optical interface linking to the network.

    e.   If the protection scheme is not 1+1, then remove this network element from your recorded list of network elements (recorded in step 11).

13   If there are no network elements remaining in your recorded list (begun in step 11), then go to step 26.

14   In the navigation tree, select the NPx.

15   In the Configuration menu, select Span of Control.

16   In the Span of Control window, select the network elements in your list recorded in step 11.

    a.   Select one network element in the list.

    b.   For each subsequent network element, hold down the CTRL key while selecting the network element.

17   Click Delete.

18   Click Yes in the confirmation dialog box.

19   In the Span of Control window, click Add.

<div align="center">—continued—</div>

Procedure 5-4 (continued)
Retrieving an existing map

Step	Action
20	In the Add to Span of Control dialog box, select the network elements recorded in step 11.
	Note: If some of the network elements require different user IDs and/or passwords from one another, then only group together those network elements that share the same user ID and password.
	a. Select one network element in the list.
	b. For each subsequent network element, hold down the CTRL key while selecting the network element.
21	In the User ID box, enter the required user ID.
22	In the Password box, enter the required password.
23	Click Apply.
24	If all of the network elements recorded in step 11 have not yet been re-added to the SOC, then perform step 20 to step 24 for the next grouping of network elements with common user ID and password.
25	Click OK.
26	Select Map Topology from the Configuration drop-down menu.
27	Select Load map from file from the File drop-down menu of the Map Topology dialog box.
28	Browse for and select the required map file in the Load Map File dialog box.
29	Click Load.
	Note: If you perform a reconfiguration procedure and the Map Topology window is open, a deleted link or network element will display as deleted. To completely remove a deleted link or network element from the map, select New map from NP from the File drop-down menu.

—**end**—

Procedure 5-5
Selecting or deselecting all nodes on a map

Use this procedure to select or deselect all nodes on a network map.

Note 1: A selected node has a white outline.

Note 2: When Layout is selected from the Edit drop-down menu, you cannot select or deselect all nodes.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Hold down the Shift key and click to select multiple network elements or select one of the following from the Edit drop-down menu.

   •   Select all
        if you want to select all nodes

   •   Deselect all
        if you want to deselect all nodes

<div align="center">—end—</div>

Procedure 5-6
Removing a disabled network element or link on a map

Use this procedure to remove a disabled network element or link on a map.

A disabled item is represented by a broken line. When a network element or link is removed from the network processor span of control after a map is retrieved, the network element is displayed as disabled on the map. The links leading from the network element are also disabled.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Right-click on the network element square symbol or link, and select Remove from map from the pop-up menu.

—**end**—

Procedure 5-7
Removing all disabled items on a map

Use this procedure to delete all disabled network elements and links on a map.

A disabled item is represented by a broken line. When a network element or link is removed from the network processor span of control after a map is retrieved, the network element is displayed as disabled on the map. The links leading from the network element are also disabled.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see , or .
2	Select Delete all removed items from the Edit drop-down menu.
	Note: When Layout is selected from the Edit drop-down menu, you cannot select Delete all removed items.

<div align="center">—end—</div>

Procedure 5-8
Moving network elements on a map

Use this procedure to reposition network elements on a map.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Layout from the Edit drop-down menu.
	Note: Once Layout is selected, the Layout mode toolbar appears at the bottom of the map. It has three icons: Select, Zoom in (+), and Zoom out (-).
3	Select, hold, and drag the network element square symbol to a new position as required.
	Note 1: You can group multiple squares by holding down the Shift key while you select the squares. Then reposition the multiple squares as a group.
	Note 2: To ungroup multiple squares, click anywhere other than the squares.
4	Deselect Layout from the Edit menu to disable the Layout mode.
	Note: The Layout mode toolbar at the bottom of the map disappears.

—end—

Procedure 5-9
Zooming in and out on a map

Use this procedure to zoom in to focus on more details, or to zoom out to see more at once when a map is displayed.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Layout from the Edit drop-down menu.
	Note: Once Layout is selected, the Layout mode toolbar appears at the bottom of the map. It has three icons: Select, Zoom in (+), and Zoom out (-).
3	Click on the Zoom in (+), or Zoom out (-) icon as required.
	Note: All items on the map are resized except for text.
4	Deselect Layout from the Edit menu to disable the Layout mode.
	Note: The Layout mode toolbar at the bottom of the map disappears.

<div align="center">—end—</div>

Procedure 5-10
Adding a label to a map

Use this procedure to add a label anywhere within the map.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Labels from the Edit drop-down menu.
	Note: When Layout is selected from the Edit drop-down menu, you cannot edit the text of Labels.
3	Click a location on the map where you want to add a label.
	Note: A scrolling text entry field where you can enter a single line of text appears.
4	Enter the required text.
5	Deselect Labels from the Edit drop-down menu to disable the Labels mode.

—**end**—

Procedure 5-11
Editing a label on a map

Use this procedure to edit any label on a map.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Labels from the Edit drop-down menu.
	Note: When Layout is selected from the Edit drop-down menu, you cannot edit the text of Labels.
3	Click on the text of the label that you want to edit.
	Note: The text is now within a text entry field.
4	Edit the text as required.
	Note 1: For all labels except the node name labels, you can enter only a single line of text.
	Note 2: For the node name labels, you can press Shift-Enter at the end of a text of line to enter a new line of text, that is, you can have a node name label with multiple lines of text. After editing a node name label, the node's target identifier can still be retrieved. See Setting display options on page 5-33.
5	Deselect Labels from the Edit drop-down menu to disable the Labels mode.

—**end**—

Procedure 5-12
Deleting a label on a map

Use this procedure to delete a label on a map.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Labels from the Edit drop-down menu.
	Note: When Layout is selected from the Edit drop-down menu, you cannot edit the text of Labels.
3	Click on the text of the label that you want to delete.
	Note: The text is now within a text entry field.
4	Delete the text of the label.
5	Deselect Labels from the Edit drop-down menu to disable the Labels mode.

—end—

Procedure 5-13
Repositioning a label on a map

Use this procedure to reposition any labels on a map, other than the node name label on a network element.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Layout from the Edit drop-down menu.
	Note: Once Layout is selected, the Layout mode toolbar appears at the bottom of the map. It has three icons: Select, Zoom in (+), and Zoom out (-).
3	Select, hold, and drag the label to a new position as required.
4	Deselect Layout from the Edit menu to disable the Layout mode.

<div align="center">

—end—

</div>

Procedure 5-14
Changing the color setting of the map background, grid, or labels

Use this procedure to change the color setting of the map background, the grid, or labels on a map.

To see the effect of changing the color setting of the grid or labels, you must first display the grid or have a label on your map.

> *Note:* You cannot change the color setting of a node name label on a network element.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Color from the Edit drop-down menu to open the Color settings dialog box.
3	Select the item you want to change (map background, grid, or labels) from the drop-down list at the bottom of the Color settings dialog box.
4	Select the color you want from the pallet under Colors.
	Note 1: Alternatively, you can click within the color wheel to select the required color, and use the color slider to meet your full requirement. To operate the color slider, select the pointer, hold and slide up and down.
	Note 2: You can also enter color values to mix your color.
5	Click Apply.
6	Click Cancel to close the dialog box.

—end—

Procedure 5-15
Modifying the grid on a map

Use this procedure to show the grid, to snap to grid, and to change the grid spacing.

You can enable the snap to grid command without showing the grid.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select one of the following from the Edit drop-down menu

  - Show grid
    if you want to show the grid

  - Snap to grid
    if you want to align the upper left hand corner of an item on the map to the nearest grid points

  - Grid settings
    if you want to adjust the grid spacing.

    Note: When Layout is selected from the Edit drop-down menu, you cannot edit the Grid settings.

                    —end—

Procedure 5-16
Clearing a single alarm balloon

Use this procedure to remove an alarm balloon graphic on a map.

Note: Only the balloon graphic is removed. This procedure does not clear the alarm.

Alarm balloons display the number and severity of the highest severity alarm raised on a network element since you last refreshed or retrieved the map. Alarm balloons only apply to logged-in network elements under the NP span of control.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Right-click on the alarm balloon, and select Clear balloon from the pop-up menu.
	Note: Alternatively, you can also click on the network element square symbol to select it (so that a white outline appears), and select Clear selected balloons from the Faults drop-down menu.

—end—

Procedure 5-17
Clearing all alarm balloons

Use this procedure to remove all alarm balloon graphics on a map.

> *Note:* Only the balloon graphics are removed. This procedure does not clear the alarms.

Alarm balloons display the number and severity of the highest severity alarm raised on a network element since you last refreshed or retrieved the map. Alarm balloons only apply to logged-in network elements under the NP span of control.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Clear all balloons from the Faults drop-down menu.

<div align="center">

—**end**—

</div>

Procedure 5-18
Logging in to network elements from Map Topology

Use this procedure to log in to network elements with the same user profile specified for the gateway network processor (NP).

Requirement

You must be logged out of the network elements and the network elements must be under the NP span of control.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Ensure that Layout and Labels are not selected on the Edit drop-down menu.
	Note 1: If Layout is selected, the Security menu is disabled, but you can right-click on a network element, and select Autologin from the pop-up menu. In this case, you cannot log in to multiple network elements at one time.
	Note 2: If Labels is selected, you can log in to all network elements by selecting Select all from the Edit drop-down menu, and select Autologin from the Security drop-down menu. In this case, you must log in to all network elements at the same time.
3	Click on the required network element to select it.
	Note: You can select multiple network elements to log in by holding down the Shift key while you select the square symbols. Or you can select all network elements by selecting Select all from the Edit drop-down menu.
4	Select Autologin from the Security drop-down menu.
	Note: Alternatively, if only one network element is selected, you can right-click on it and select Autologin from the pop-up menu.

—end—

Procedure 5-19
Logging in to network elements as a different user

Use this procedure to log in to network elements with a different user profile from the gateway network processor (NP).

Requirement

You must be logged out of the network elements and the network elements must be under the NP span of control.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Ensure that Layout and Labels are not selected on the Edit drop-down menu.
	Note 1: If Layout is selected, the Security menu is disabled, but you can right-click on a network element, select Login as from the pop-up menu, and go to step 5. In this case, you cannot log in to multiple network elements at one time.
	Note 2: If Labels is selected, you can log in to all network elements by selecting Select all from the Edit drop-down menu, and select Login as from the Security drop-down menu. In this case, you must log in to all network elements at the same time.
3	Click on the required network element to select it.
	Note: You can select multiple network elements to log in by holding down the Shift key while you select the square symbols. Or you can select all network elements by selecting Select all from the Edit drop-down menu.
4	Select Login as from the Security drop-down menu.
	Note: Alternatively, if only one network element is selected, you can right-click on it and select Login as from the pop-up menu.
5	Enter the user ID and password in the Login as dialog box.
6	Click Login in the dialog box.

—end—

Procedure 5-20
Logging out of network elements from Map Topology

Requirement

You must be logged in to the network elements and the network elements must be under the network processor span of control.

Step	Action
1	Ensure that Layout and Labels are not selected on the Edit drop-down menu.
	Note 1: If Layout is selected, the Security menu is disabled, but you can right-click on a network element, and select Logout from the pop-up menu. In this case, you cannot log out of multiple network elements at one time.
	Note 2: If Labels is selected, you can log out of all network elements by selecting Select all from the Edit drop-down menu, and select Logout from the Security drop-down menu. In this case, you must log out of all network elements at the same time.
2	Click on the required network element to select it.
	Note: You can select multiple network elements to log out by holding down the Shift key while you select the square symbols. Or you can select all network elements by selecting Select all from the Edit drop-down menu.
3	Select Logout from the Security drop-down menu.
	Note: Alternatively, if only one network element is selected, you can right-click on it and select Logout from the pop-up menu.

—**end**—

Procedure 5-21
Adding a background image to a map

Use this procedure to add a background image to a map.

Requirement

Your background image must be of image type *.gif.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Load image from the Background drop-down menu.
3	Browse for and select the location where you want to retrieve the background image in the Select Background Image dialog box.
4	Enter a file name in the File name field.
5	Click Load.

—**end**—

Procedure 5-22
Showing or hiding a background image on a map

Use this procedure to toggle the display of the background image on or off. You must have had the background image loaded before you can toggle the display on or off.

When the background image is hidden, the map appears less cluttered.

Step	Action
1	Retrieve a map with a background image loaded. For instructions, see Adding a background image to a map on page 5-27.
2	Select or deselect Visible from the Background drop-down menu to toggle the display of the background image on or off.

—end—

Procedure 5-23
Resizing a background image on a map automatically

Use this procedure to enable Site Manager to resize the background image to fit in the display window automatically.

Step	Action
1	Retrieve a map with a background image loaded. For instructions, see Adding a background image to a map on page 5-27.
2	Select Stretch to fit from the Background drop-down menu.

—**end**—

Procedure 5-24
Resizing a background image on a map manually

Use this procedure to resize a background image manually.

Step	Action
1	Retrieve a map with a background image loaded. For instructions, see Adding a background image to a map on page 5-27.
2	Select Repositioning from the Background drop-down menu.
3	Click on the background image once.
4	Click, hold, and drag a sizing handle (the square that appears at each corner and along the sides of the rectangle that surrounds a selected image) towards or away from an image to shrink or enlarge the image.

—**end**—

Procedure 5-25
Moving a background image on a map

Use this procedure to reposition a background image on a map.

Step	Action
1	Retrieve a map with a background image loaded. For instructions, see Adding a background image to a map on page 5-27.
2	Select Repositioning from the Background drop-down menu.
3	Click and hold around the centre of the background image, and drag the image to the required position.

<div align="center">

—end—

</div>

Procedure 5-26
Removing a background image on a map

Use this procedure to remove the background image completely.

When you want to display the image again, you need to reload the image. This is different from temporarily hiding the display of the image.

To hide the background image display temporarily, see Showing or hiding a background image on a map on page 5-28.

Step	Action
1	Retrieve a map with a background image loaded. For instructions, see Adding a background image to a map on page 5-27.
2	Select Clear image from the Background drop-down menu.

<div align="center">—**end**—</div>

Procedure 5-27
Setting display options

Use this procedure to set display options.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select one of the following from the Options menu:

- Notify on change. This option displays a message that prompts the refresh of the map when a provisioning change occurs on a network element under the network processor (NP) span of control.

- Show slot number. This option displays the slot numbers of connecting equipment on the map topology links. A network element must be under the NP span of control to display slot numbers.

- Show alarm tooltips. This option displays alarm information for a network element in the map topology when you move the cursor over the network element. The network element must be under the NP span of control. For a logged-in network element, the information includes the target identifier and number of alarms. For a logged-out network element, only the target identifier is shown.

- Show link tooltips. This option displays link information when you move the cursor over a link in the map topology. The information includes the target identifier of the near-end and far-end network elements; the slot number, port number, and type of the connecting equipment; and the protection mode. If the far-end network element is not in the NP span of control, the far-end slot and port number display "0".

—end—

Procedure 5-28
Viewing the slot connections for all network elements

Use this procedure to display network connections in a table.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Show slot table from the Options drop-down menu.

—end—

Procedure 5-29
Highlighting the links between network elements on a map

Use this procedure to highlight links between network elements on a map.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Select Show slot table from the Options drop-down menu.
3	Select the Show selections on map check box.
4	Select the rows in the Slot table that represent the links that you want to highlight on the map.
5	Click Close.

<div align="center">—**end**—</div>

Procedure 5-30
Displaying the active alarms of a network element

Use this procedure to display the Active Alarms window of a network element in the map. You must be logged in to the network element and the network element must be under the network processor span of control.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Ensure that you have logged in to the required network element. For instructions on how to log in to a network element, see Logging in to network elements from Map Topology on page 5-24.
3	Right-click on the network element, and select Show alarms from the pop-up menu.
	Note: Alternatively, if there is an alarm balloon on the network element, you can double-click on the alarm balloon to display the Active Alarms window of the network element.
	—end—

Procedure 5-31
Displaying the shelf graphics of a network element

Use this procedure to display the shelf graphics of a network element in the map. You must be logged in to the network element and the network element must be under the network processor span of control.

Step	Action
1	Retrieve a map in the Map Topology window. For instructions, see Retrieving a new map on page 5-3, or Retrieving an existing map on page 5-8.
2	Ensure that you have logged in to the required network element. For instructions on how to log in to a network element, see Logging in to network elements from Map Topology on page 5-24.
3	Right-click on the network element, and select Show shelf level graphics from the pop-up menu.

<div align="center">—end—</div>

Procedure 5-32
Printing within Map Topology

Use this procedure to print a map displayed in Map Topology, or a slot table displayed in the Slot table dialog box.

Step	Action
1	Select the Map Topology window or Slot table dialog box as required.
2	Press Alt+Print Screen to copy the window or dialog box into the buffer of your computer system.
3	Paste the buffer into a text editor or a graphic editor according to the documentation for the application.
4	Print the window or dialog box according to the documentation for the application.

—**end**—

Provisioning TID address resolution protocol (TARP)

Procedures for TARP

Procedure 6-1
Editing TARP configuration parameters

Use this procedure to edit TARP configuration parameter.

Requirement

To perform this procedure, you must be logged into the network element with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Ensure the network element is selected in the navigation tree.
3	Select TARP Provisioning from the Configuration drop-down menu.
4	Select the Configuration tab and click Edit to open the Edit TARP configuration dialog box.
5	Edit the TARP configuration parameter values as required.
	Note 1: For possible parameter values, see TARP configuration parameters on page 6-3.
	Note 2: If you want to reset all configuration parameter values to their default values, click Default.
6	Click OK.

—*end*—

TARP configuration parameters

Parameters	Possible values	Description
TARP mode	PROPAGATION; ORIGINATION; BOTH; NONE	The default TARP messaging mode is BOTH.
Protocol address type	Any 2-hexadecimal digits	The default is FE for connectionless network protocol (CLNP) type of address.
Network selector	Any 2-hexadecimal digits	The default is AF for CLNP type of address.
Throttle&Period	0 to 32767 for throttle; 1 to 32767 seconds for period	Throttle and period is the maximum number of protocol data units (PDUs) processed within the interval period. The default is 300&2, which is 300 PDUs within 2 seconds.
Type 1 waiting period	0 to 3600 seconds	The default TARP type 1 message response waiting period is 15 seconds.
Type 3 waiting period	0 to 3600 seconds	The default Address resolution request response waiting period is 40 seconds.
PDU lifetime	0 to 65535 hops	The default TARP time-to-live is 100 hops.
PDU sequence number	0 to 65535	The PDU sequence number is used for loop detection. The default is 0.
Loop detection buffer life	1 to 10 minutes	The default is 5 minutes.
Loop detection buffer flush	0 to 1440 minutes	Loop detection buffer flush is the period how often the loop detection buffer is deleted. The default is 5 minutes.
Data cache flush	0 to 1440 minutes	Data cache flush is the period how often the data cache table is deleted. The default is 1440 minutes.

Procedure 6-2
Adding an entry in the TARP tables

Use this procedure to add an entry in the following TARP tables:

- Data cache
- Disabled adjacency
- Manual adjacency
- Loop detection
- Disabled circuit/port

Note: You cannot add an entry in the Computed adjacency table.

Requirement

To perform this procedure, you must be logged into the network element with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Ensure the network element is selected in the navigation tree.
3	Select TARP Provisioning from the Configuration drop-down menu.
4	Select the Tables tab.
5	Select the radio button of the table to be modified from the Table area.
6	Click Add and enter the relevant information in the Add dialog box.
	Note 1: For possible parameter values, see TARP table parameters on page 6-5.
	Note 2: For the Disabled adjacency table or the Manual adjacency table, you only need to provide information for either the system ID or NSAP. Select the radio button, and then enter the value or select from the drop-down list.
	Note 3: Whenever you want to enter the NSAP value, you can, as an alternative, click the Build NSAP button to build the NSAP value. See Building or editing an NSAP value on page 6-10.
7	Click OK.

—end—

TARP table parameters

Table	Parameters	Possible values
Computed Adjacency	NSAP/ TID	A 40-digit hexadecimal number/ a string of up to 20 characters
	PortID	Possible values: LAN0, DCC-3, DCC-4, DCC-5, DCC-6, DCC-7, DCC-8, DCC-9, DCC-10, DCC-11, DCC-12
Data Cache	TID	A string of up to 20 characters
	NSAP	A 40-digit hexadecimal number
Disabled Adjacency	NSAP/ System ID	A 40-digit hexadecimal number/ a 12-digit hexadecimal number
Disabled Circuit/Port	Port ID	Possible values: LAN0, DCC-3, DCC-4, DCC-5, DCC-6, DCC-7, DCC-8, DCC-9, DCC-10, DCC-11, DCC-12
Loop Detection	System ID	A 12-digit hexadecimal number
	Sequence number	Values range from 0 to 65535.
Manual Adjacency	NSAP/ System ID	A 40-digit hexadecimal number/ a 12-digit hexadecimal number
Note: You cannot add to, modify, or delete the Computed adjacency table parameter values.		

Procedure 6-3
Editing an entry in the TARP tables

Use this procedure to edit an entry in the following TARP tables:

- Data cache

- Disabled adjacency

- Manual adjacency

- Loop detection

- Disabled circuit/port

Note: You cannot edit an entry in the Computed adjacency table.

Requirement

To perform this procedure, you must be logged into the network element with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Ensure the network element is selected in the navigation tree.
3	Select TARP Provisioning from the Configuration drop-down menu.
4	Select the Tables tab.
5	Select the radio button of the table to be modified from the Table area.
6	Select the required entry in the TARP table.
7	Click Edit and revise the information in the Edit dialog box as required.
	Note 1: For possible parameter values, see TARP table parameters on page 6-5.
	Note 2: For the Disabled adjacency table or the Manual adjacency table, you only need to provide information for either the system ID or NSAP. Select the radio button, and then enter the value or select from the drop-down list.
	Note 3: Whenever you want to enter the NSAP value, you can, as an alternative, click the Build NSAP button to build the NSAP value. See Building or editing an NSAP value on page 6-10.
8	Click OK.

—end—

Procedure 6-4
Deleting an entry in the TARP tables

Use this procedure to delete an entry in the following TARP tables:

- Data cache
- Disabled adjacency
- Manual adjacency
- Loop detection
- Disabled circuit/port

Note: You cannot delete an entry in the Computed adjacency table.

Requirement

To perform this procedure, you must be logged into the network element with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Ensure the network element is selected in the navigation tree.
3	Select TARP Provisioning from the Configuration drop-down menu.
4	Select the Tables tab.
5	Select the radio button of the table to be modified from the Table area.
6	Select the required entry in the TARP table.
7	Click Delete.
8	Click Yes in the confirmation dialog box.

—end—

Procedure 6-5
Performing a TARP echo function

Use this procedure to perform a TARP echo function.

A TARP echo function is a protocol function that tests communication between network elements by sending TARP protocol data units (PDUs) and receiving a response.

Requirement

To perform this procedure, you must be logged into the network element with a level 3 or higher user privilege code (UPC).

Step	Action
1	Ensure you are logged in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Ensure the network element is selected in the navigation tree.
3	Select TARP Provisioning from the Configuration drop-down menu.
4	Select the Echo Function tab.
5	Do one of the following to provide the address: • Select the TID radio button, and select a TID from the drop-down list, or enter a new TID. • Select the NSAP radio button, and select a NSAP from the drop-down list, or enter a new NSAP. Alternatively you can click 'Build NSAP' to build a new NSAP value. See Building or editing an NSAP value on page 6-10.
6	Modify the Iteration, Rate, and Timeout values as required. See TARP echo function (TEF) parameters on page 6-9.
7	Click Operate.

—**end**—

TARP echo function (TEF) parameters

Parameter	Value	Description
Address Type	TID NSAP	Target identifier, a string of up to 20 characters Network service access point, a 40-digit hexadecimal number
Iteration	1 to 65535	Iterations of TARP type 5 messages to be transmitted. The default is 1.
Rate	1000 to 180000 milliseconds	Rate of sent requests. Wait for response before sending each request. The default is 1000.
Timeout	1000 to 180000 milliseconds	Maximum time to wait for a response to each echo request. The default is 1500.

Procedure 6-6
Building or editing an NSAP value

Use this procedure to build or edit a network service access point (NSAP) value through the Build NSAP dialog box in Site Manager.

The NSAP value is a long number of 40 hexadecimal digits. The Build NSAP dialog box breaks the NSAP value into smaller components, and allows you to enter the shorter component numbers.

Step	Action
1	Ensure you are logged in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Ensure the network element is selected in the navigation tree.
3	Select TARP Provisioning from the Configuration drop-down menu.
4	Select the Echo Function tab.
5	Select the NSAP radio button.
6	Click the Build NSAP button.
7	Enter a value for all six area address components. For format requirement, see NSAP component format on page 6-11.
	Note: After you have completed the Domain field, four zeros appear in the Area address field (between the organization ID and the domain). Do not delete the four zeros.
8	Select a System ID from the drop-down list, or enter a new value.
9	Enter a Network selector.
10	Click OK.
	Note: The NSAP is displayed in the window or dialog box where you clicked Build NSAP.

—end—

NSAP component format

Parameter	Format
Address format ID	2-digit hexadecimal number
Initial domain ID	4-digit hexadecimal number
DSP format ID	2-digit hexadecimal number
Organization ID	6-digit hexadecimal number
Reserved	4-digit hexadecimal number
Domain	4-digit hexadecimal number
Area	4-digit hexadecimal number
System ID	12-digit hexadecimal number
Network selector	2-digit hexadecimal number

Test access

Procedures for test access

Procedure 7-1
Setting up for a test access session

Use this procedure to ensure that you have all the required components for a test access session. For an overview of a possible test access setup, see Test access components on page 7-3. Supported test access modes are shown in the following illustrations:

- Test access monitor - Single FAD, MONE mode on page 7-11
- Test access monitor - Single FAD, MONF mode on page 7-11
- Test access monitor - Dual FAD, MONEF mode on page 7-11
- Test access split - Single FAD SPLTE mode on page 7-14
- Test access split - Single FAD, SPLTF mode on page 7-14
- Test access split -Single FAD SPLTA mode on page 7-14
- Test access split -Dual FAD, SPLTEF mode on page 7-15

Requirements
- If you are using a testing operations system (TOS) ensure that it can communicate with the test head.
- Ensure that the test head can communicate with the network element.
- Ensure that you have test access interface cables (DS1, DS3, DS3VT, or EC-1) and connectors as required.
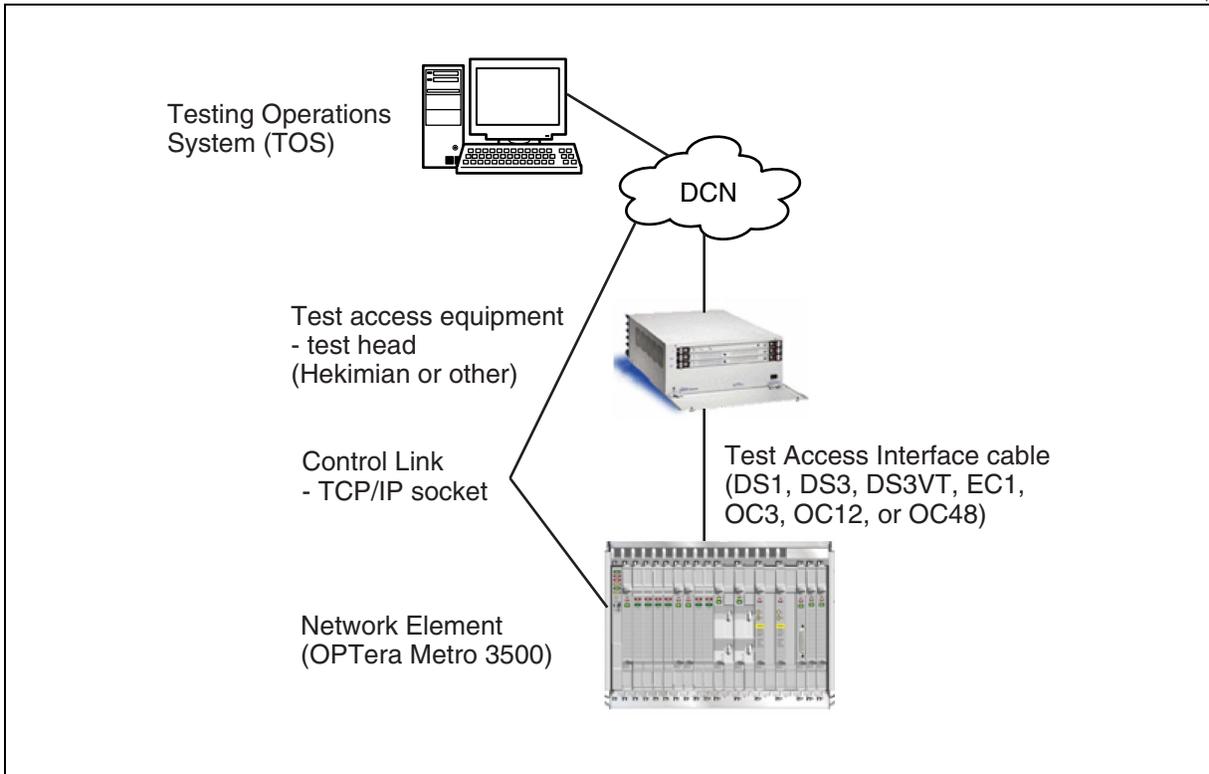
Step	Action
1	Determine the facility of the connection to be tested.
2	Connect the interface cable to the port on the test head (for example, Hekimian test set).
3	Connect the other end of the interface cable to the facility on the cross-connect panel of the OPTera Metro 3500.
4	Provision the test access ports, see Provisioning a test access port on page 7-5.

—end—

Test access components

ex1396p

Testing Operations System (TOS)

DCN

Test access equipment
- test head
(Hekimian or other)

Control Link
- TCP/IP socket

Test Access Interface cable
(DS1, DS3, DS3VT, EC1,
OC3, OC12, or OC48)

Network Element
(OPTera Metro 3500)

Procedure 7-2
Setting the test access time out period

Use this procedure to set the test access time out period on a network element. If the network element does not receive any test access TL1 commands within the time out period, a test access loss of association is triggered. During a test access loss of association, the test access session is released, and original connections are restored.

Note 1: If the time out period is set to 0, loss of association is not monitored and therefore never triggered.

Note 2: The time out period has a provisionable range of 0 to 900 seconds with a default value of 300 seconds. When this period is not set as a 30 second increment, the time is rounded up to the next 30 second interval. For example, if the time out period is set to 31 seconds, the actual time out occurs at 60 seconds.

Note 3: A REPT-STAT command is sent to the network element to check that the data link is operational. If no test access commands are sent to the network element for a period less than the time out period, a REPT-STAT command is sent. On receipt of this command, the network element sends an acknowledgment within 2 seconds. The format of the REPT-STAT command is:

```
REPT-STAT:[TID]::CTAG;
```

| **<TID>** | Target identifier |
| **<CTAG>** | Correlation tag |

The response OK is sent by the network element as acknowledgement to the REPT-STAT command.

Requirements

Ensure that you have a user privilege level of 3.

Step	Action
1	Log in to a network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation area.
3	Click Edit in the System area of the Node Information window (General tab).
4	Enter the Test Access Time Out value in the Edit System dialog.
5	Click OK to save the changes and close the dialog.

—end—

Procedure 7-3
Provisioning a test access port

Use this procedure to provision one or more test access ports (TAP). A facility (and all of its channels) is reserved as a TAP when the primary state is OOS and secondary state is Test access.

Note 1: Test access ports can be pre-provisioned.

Note 2: Only test access connections can use the test access port.

Note 3: When a facility is provisioned as a TAP, the Loss of Signal LED only becomes active if an existing signal on this facility is removed.

Note 4: For an EC-1 facility, you can only provision a test access port at the STS-1 level. If you provision a test access port on an EC-1 facility, all of the VT1.5 frames within the STS-1 signal are also provisioned for test access.

Requirements

- Ensure that you have a user privilege level of 3.

- Ensure that the circuit pack that you want to provision as the TAP is not in a protection slot or in slot 11 or 12. A TAP must be a working port and it cannot be assigned to a high speed slot.

- Ensure that there are no cross-connects provisioned on the port you want to provision as the TAP.

Step	Action
1	Log in to a network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation area.
3	Select Equipment & Facility Provisioning from the Configuration drop-down menu to open the Equipment & Facility Provisioning window.
4	In the Equipment area of the Equipment & Facility Provisioning window, select the circuit pack where you want to provision the TAP.
5	In the Facility area, select the facility that you want to provision as a TAP.
6	Click Edit in the Facility area to open the Edit facility dialog box.
7	Select OOS from the Primary state drop-down list.

—continued—

Procedure 7-3 (continued)
Provisioning a test access port

Step	Action
8	Click OK.
	A warning appears.
9	Click Yes.
10	In the Facility area, select the same facility if it is not selected.
11	Click Edit in the Facility area to open the Edit facility dialog box.
12	Select Test access from the Secondary state drop down list.
13	Click OK.
	The facility primary state is OOS and the secondary state is Test access.

—**end**—

Procedure 7-4
Deprovisioning a test access port

Use this procedure to de-provision the facility state so that it is no longer a TAP.

Note: When a facility is provisioned as a TAP, the Loss of Signal LED only becomes active if an existing signal on this facility is removed.

Requirements

Ensure that you have a user privilege level of 3.

Step	Action
1	Ensure there is not a test access session on the port you want to de-provision the facility state, see Retrieving test access information on page 7-17.
2	In the Equipment area of the Equipment & Facility Provisioning window, select the circuit pack with the TAP.
3	In the Facility area, select the facility with the TAP.
4	Click Edit in the Facility area to open the Edit facility dialog box.
5	Select Test access deactivate from the Secondary state drop-down list.
6	Click OK.
7	To put the facility back in-service, continue with step 8 otherwise this procedure is complete.
8	In the Facility area, select the same facility if it is not selected.
9	Click Edit in the Facility area to open the Edit facility dialog box.
10	Select IS from the Primary state drop-down list.
11	Click OK.
	The facility primary state is IS and the secondary state no longer shows Test access.

—end—

Procedure 7-5
Creating a test access session

Use this procedure to create a test access session on an existing T1 or T3 facility or on a VT1.5, STS1, STS-3c, STS-12c, STS-24c, or STS-48c path type. A test access session is created in the monitor mode. Monitor test access sessions are non-intrusive and therefore do not trigger a protection switch or affect traffic.

Monitor test access sessions can be either single FAD (MONE or MONF) or dual FAD (MONEF), see:

- Test access monitor - Single FAD, MONE mode on page 7-11
- Test access monitor - Single FAD, MONF mode on page 7-11
- Test access monitor - Dual FAD, MONEF mode on page 7-11

Table 7-1 summarizes the supported cross-connects in test access monitor state. The left column lists the cross-connect type, which can be either the FromAid (equipment side) or the ToAid (facility side). The top row specifies the mode.

Table 7-1
Supported test access cross-connect types (monitor mode)

Cross-connect type	MONE (FromAid)	MONF (ToAid)	MONEF (FromAid & ToAid)
1WAY (Unidirectional)	Yes	No	No
2WAY (Bidirectional)	Yes	Yes	Yes
1WAYPR (Unidirectional Path Ring)	Yes	No	No
2WAYPR (Bidirectional Path Ring)	Yes	No	No
2WAYBR (Bidirectional Bridge Ring)	Yes	No	No
FFP (Facility Protection Group)	Yes	No	No

—continued—

Procedure 7-5 (continued)
Creating a test access session

Note 1: Multiple test access connections can be established on the designated test access port as long as the designated test access port has sufficient bandwidth to support the connection.

Note 2: During a test access session, original connections can not be deleted or edited in any way.

Note 3: The maximum number of TAPs a shelf can have is equal to the number of working ports the shelf configuration can support in its tributary slots.

Note 4: The maximum number of test access sessions supported is 28.

Requirements

- Ensure that the test access ports are provisioned. See Provisioning a test access port on page 7-5.

- To establish DFAD Test Access Session on a test access port which supports multiple channels, there must be an adjacent channel available on the TAP (the specific TapAid being a odd channel, the adjacent channel being an increment of the TapAid).

- To establish a Dual FAD test access session on a TAP that has bandwidth to support only one channel, ensure that a successive working port is reserved as TAP.

  Note: The successive port is the next incremental port number. If the circuit pack does not support a successive port, then the successive port will be the first port on the circuit pack located in the successive (next highest numbered) working slot.

- To establish Dual FAD test access session on a TAP that supports multiple channels, an odd channel is designated for the test session, and the successive even channel must be available for the test access.

- Ensure that the network element or connection is not in an upgrade, loopback, or rollover state.

- Ensure that you have a user privilege level of 3.

—continued—

Procedure 7-5 (continued)
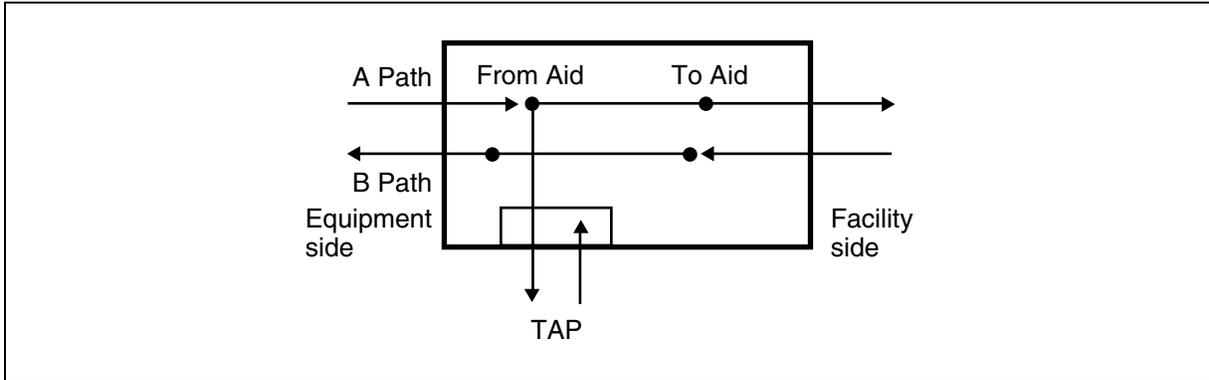**Creating a test access session**

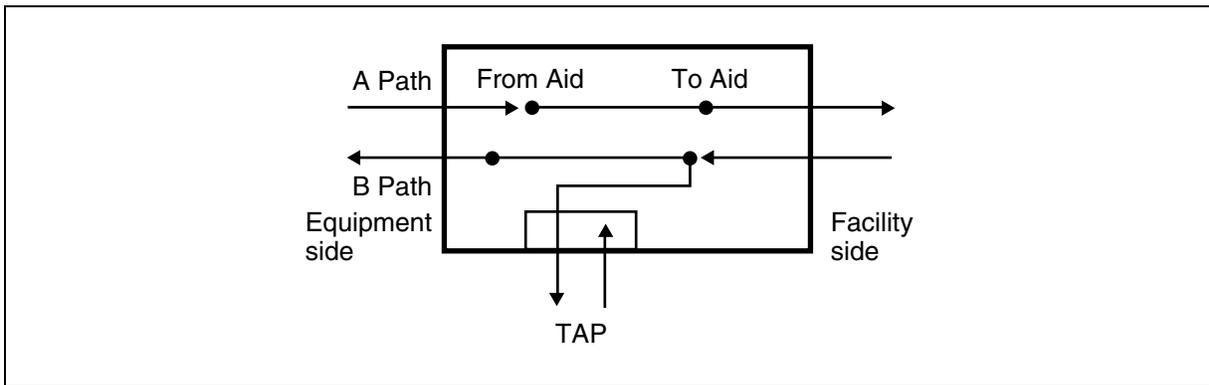| Step	Action
1	Log in to the network element. See .
2	Select the network element in the navigation area.
3	Select Nodal Cross-Connects in the Configuration menu. ***Note:*** If this is the initial launch of the Nodal Cross-Connects window, click Yes in the Retrieve Nodal Cross-Connects dialog box.
4	Click Refresh.
5	Select the required cross-connect in the cross-connect list.
6	Select the Test Access Sessions tab in the Details area.
7	Click Add to open the Add Test Access Session dialog box.
8	Select the endpoint cross-connect in the Endpoint list.
9	Select the equipment in the Equipment list.
10	Select the test access port in the Test Access Port list.
11	For an STS-level endpoint, select the STS number in the STS list. For a VT1.5-level endpoint, select the VTG group in the VTG list and the VT number in the VT list.
12	Select the test access mode in the Mode list.
13	Select the Automatic timeout check box if you want the test access session dropped when the link is dropped. By default, the test access session is maintained when the link is dropped. ***Note:*** The timeout feature only applies when using a Hekimian test set for the test access session. If you are not using a Hekimian test set, the test access session is always maintained when the link is dropped, even if the timeout feature is selected.
14	Click OK.

—**end**—

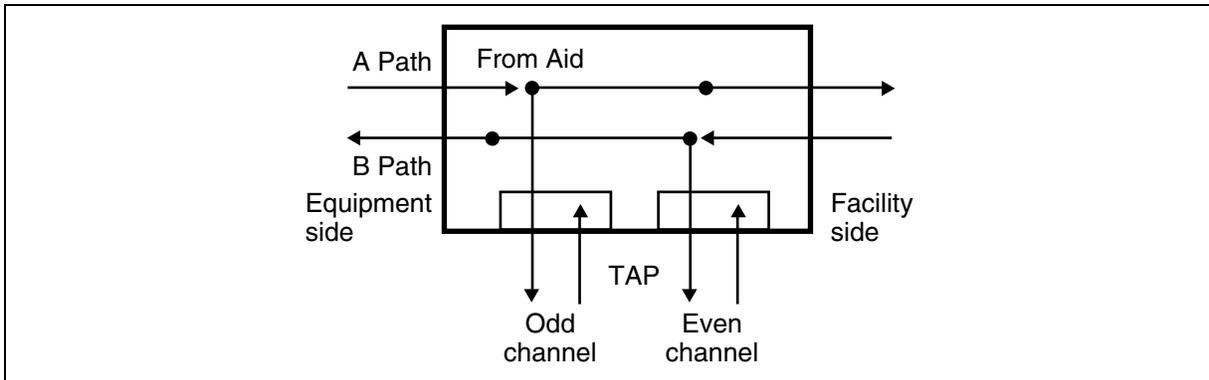## Test access monitor - Single FAD, MONE mode

EX1400

A Path   From Aid   To Aid

B Path
Equipment   Facility
side   side

TAP

Test access monitor - Single FAD, MONF mode

EX1399

A Path   From Aid   To Aid

B Path
Equipment   Facility
side   side

TAP

Test access monitor - Dual FAD, MONEF mode

EX1401

A Path   From Aid

B Path
Equipment   Facility
side   side

TAP

Odd   Even
channel   channel

Procedure 7-6
Changing the mode of a test access session

Use this procedure to change the mode of a test access session to monitor or split.

Monitor test access sessions can be either single FAD (MONE or MONF) or dual FAD (MONEF), see;

Note: Monitoring test access sessions are non-intrusive and therefore do not trigger a protection switch or affect traffic.

Split test access sessions can be either single FAD (SPLTE, SPLTF or SPLTA) or dual FAD (SPLTEF), see;

Note: A split test access session is an intrusive, service affecting operation.

For a listing of supported mode transitions, see Table 7-2. For a listing of supported cross-connect types, see Table 7-1 and Table 7-3.

Table 7-2
Supported mode transitions

From/To	MONE	MONF	MONEF	SPLTE	SPLTF	SPLTEF	SPLTA
MONE		Yes	Yes	Yes	Yes	Yes	Yes
MONF	Yes		Yes	Yes	Yes	Yes	Yes
MONEF	Yes	Yes		Yes	Yes	Yes	Yes
SPLTE	Yes	Yes	Yes		No	No	No
SPLTF	Yes	Yes	Yes	No		No	No
SPLTEF	Yes	Yes	Yes	No	No		No
SPLTA	Yes	Yes	Yes	No	No	No	

—continued—

Procedure 7-6 (continued)
Changing the mode of a test access session

Table 7-3
Supported test access cross-connect types (split mode)

Cross-connect type/Mode	SPLTE	SPLTF	SPLTEF	SPLTA
1WAY (Unidirectional)	No	No	No	Yes
2WAY(Bidirectional)	Yes	Yes	Yes	Yes
1WAYPR (Unidirectional Path Ring)	No	No	No	No
2WAYPR (Bidirectional Path Ring)	Yes	No	No	No
2WAYBR (Bidirectional Bridge Ring)	Yes	No	No	No
FFP (Facility Protection Group)	Yes	No	No	No

Note 1: All connections must be monitor mode before entering a split mode.

Note 2: Protection switching is not available on connections provisioned as test access split.

Requirements

- Ensure Creating a test access session on page 7-8 was completed successfully.

- Ensure that you have a user privilege level of 3.

| Step	Action
1	Log in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation area.
3	Select Nodal Cross-Connects in the Configuration menu.
	Note: If this is the initial launch of the Nodal Cross-Connects window, click Yes in the Retrieve Nodal Cross-Connects dialog box.
4	Click Refresh.
5	Select the Test Access Sessions tab in the Details area.
6	Select the required test access session from the list.
7	Click Edit to open the Edit Test Access Session dialog box.
8	Select the new test access mode in the Mode list.
9	Click OK.
	If the new mode is service-affecting, a confirmation dialog box appears. Click Yes to continue.

—end—

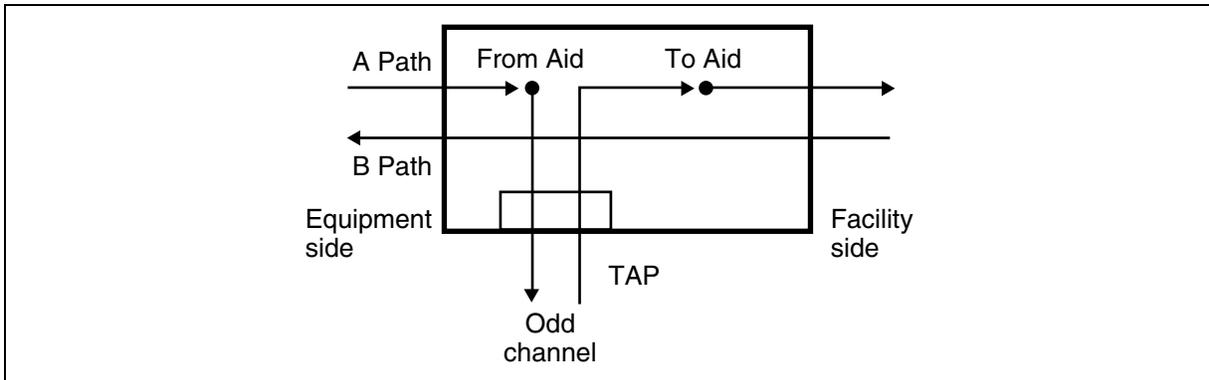## Test access split - Single FAD SPLTE mode

ex1402
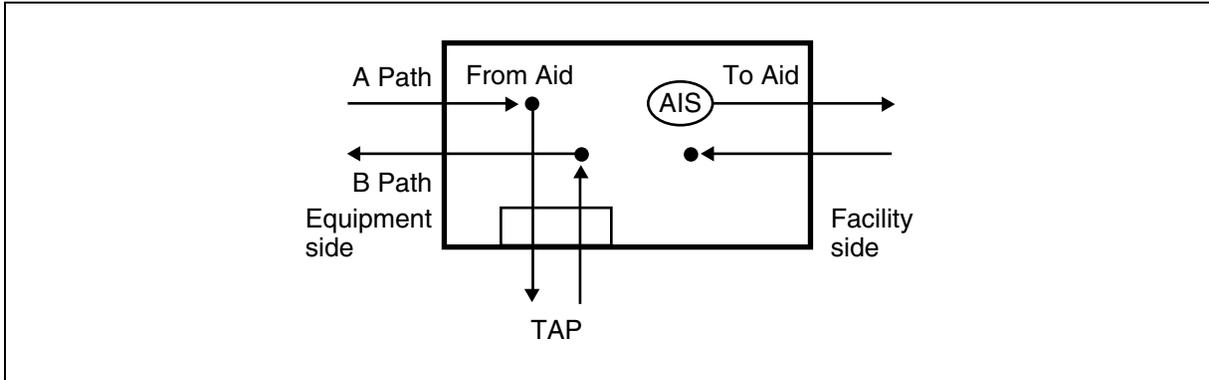
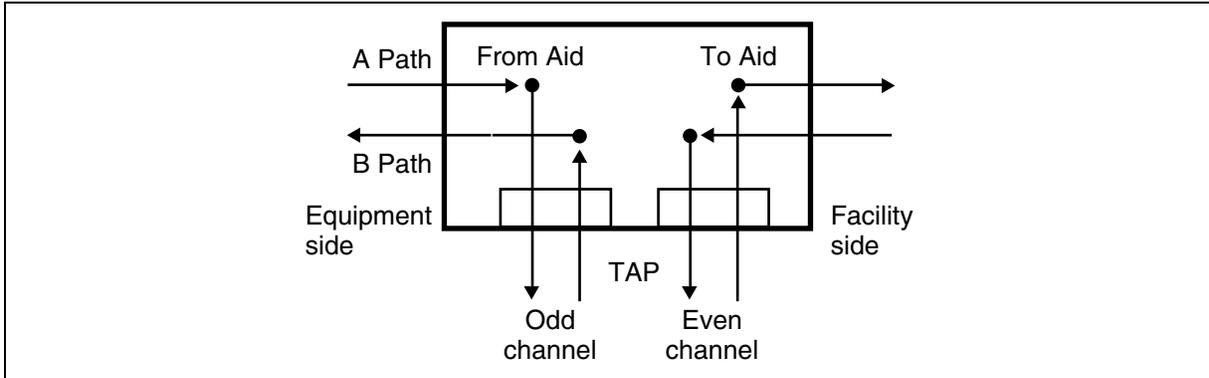## Test access split - Single FAD, SPLTF mode

ex1403
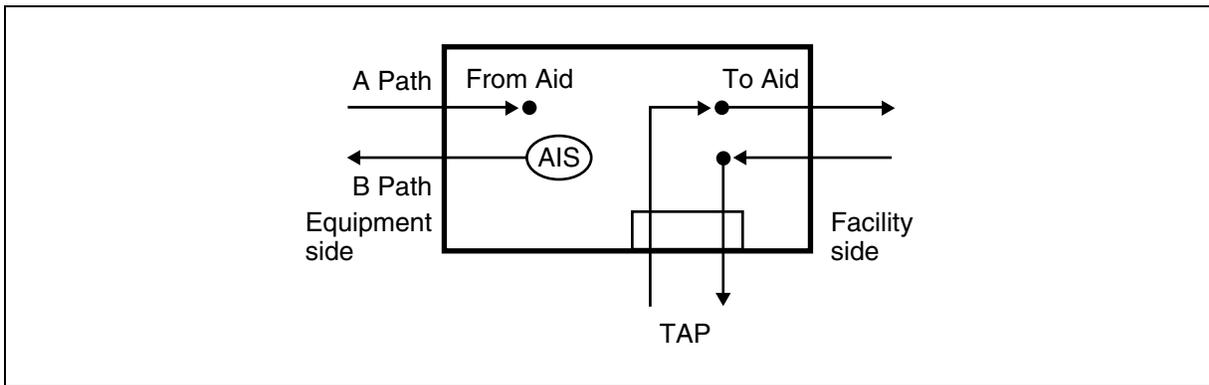
Test access split -Single FAD SPLTA mode

ex1405

Test access split -Dual FAD, SPLTEF mode

ex1406

Procedure 7-7
Releasing test access sessions manually

Use this procedure to release one or more test access sessions on a network element. Original connections are automatically restored when a test access session is released. Test access sessions can be released from both the monitor mode or the split mode.

Depending on the test access time out period or the automatic timeout value, a test access session can automatically be terminated if the network element does not receive any test access commands within the test access time out period. For information on the test access time out period, see Setting the test access time out period on page 7-4. For information on setting the automatic timeout value, see Creating a test access session on page 7-8.

Note: If you are using the REACTexpress application, follow SPIRENT documentation to release a test access session.

Requirements

Ensure that you have a user privilege level of 3.

Step	Action
1	Log in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation area.
3	Select Nodal Cross-Connects in the Configuration menu.
	Note: If this is the initial launch of the Nodal Cross-Connects window, click Yes in the Retrieve Nodal Cross-Connects dialog box.
4	Click Refresh.
5	Select the Test Access Sessions tab in the Details area.
6	Select the required test access session(s) from the list.
7	Click Delete to release the selected test access sessions.
8	Click Yes in the confirmation dialog box.
	The selected test access sessions are released.

—end—

Procedure 7-8
Retrieving test access information

Use this procedure to retrieve TAP information for a network element.

Note 1: If you are using the REACTexpress application, follow SPIRENT documentation to retrieve a test access session.

Note 2: For an EC-1 facility, a test access port is provisioned at the STS-1 level, but all of the VT1.5 frames within the STS-1 signal are also provisioned for test access.

| Step	Action
1	Log in to the network element. See .
2	Select the network element in the navigation area.
3	Select Nodal Cross-Connects in the Configuration menu.
	Note: If this is the initial launch of the Nodal Cross-Connects window, click Yes in the Retrieve Nodal Cross-Connects dialog box.
4	Click Refresh.
5	Select the Test Access Sessions tab in the Details area.

—end—

Procedure 7-9
Performing path level loopback testing

Use this procedure to setup for path level loopback testing. See Loopback testing using SPLTE mode.

Step	Action
1	Determine the test access port which will be used to perform loopback testing.
2	Using an interface cable, connect a physical loopback on the test access port on the cross-connect panel of the OPTera Metro 3500.
3	Provision the test access port facility as test access, see Provisioning a test access port on page 7-5.
4	Create a test access session in the MONE mode between a test access port channel (TAPAID) and the cross connect (FromAID) which will be placed in loopback. Refer to Creating a test access session on page 7-8.
5	Change the mode of the test access session to SPLTE. See Changing the mode of a test access session on page 7-12. The cross-connect is now in loopback state.
6	Review test results.
7	Once testing is complete, release the test access session. See Releasing test access sessions manually on page 7-16.

—*end*—

Loopback testing using SPLTE mode

Ex1432p
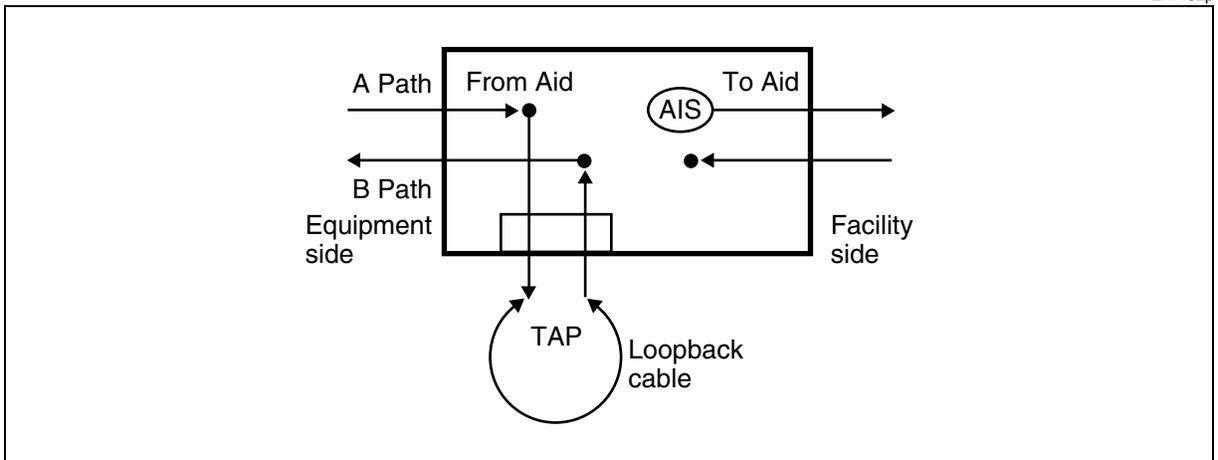
Terms and conditions

Completion of a purchase agreement is required prior to purchasing OPTera Metro 3500 products and/or services. Contact one of the following:

- your Nortel Networks sales person
- telephone: Suzanne Calton (972) 685-2888
- email CONTMGNT@nortelnetworks.com

Statement of Conditions

Portions of the code in this software may be Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the University of California, Berkeley and its contributors.

4 Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of the code in this software may be Copyright © 1988 Juniper Networks, Inc. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1   Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2   Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of the code in this software may be Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software. $FreeBSD: src/lib/libmd/md5c.c,v 1.11 1999/12/29 05:04:20 peter Exp $This code is the same as the code published by RSA Inc. It has been edited for clarity and style only.

Nortel Networks

OPTera Metro 3500
Multiservice Platform
Network Surveillance

NORTEL
NETWORKS™