NTN465GF 323-1059-210

Nortel Networks

OPTera Metro 3500 Multiservice Platform

Commissioning

Standard Release 12.0 Issue 1 November 2003

What's inside...

NORTEL NETWORKS

Printed in Canada

Contents

About this document

This document describes how to

- commission a shelf processor (SP) and network processor (NP) in preparation for network element site testing
- add network accounts, password management and managing the network element name, date, and time

Supported software

This document supports the software release 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 Multiservice Platform 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):

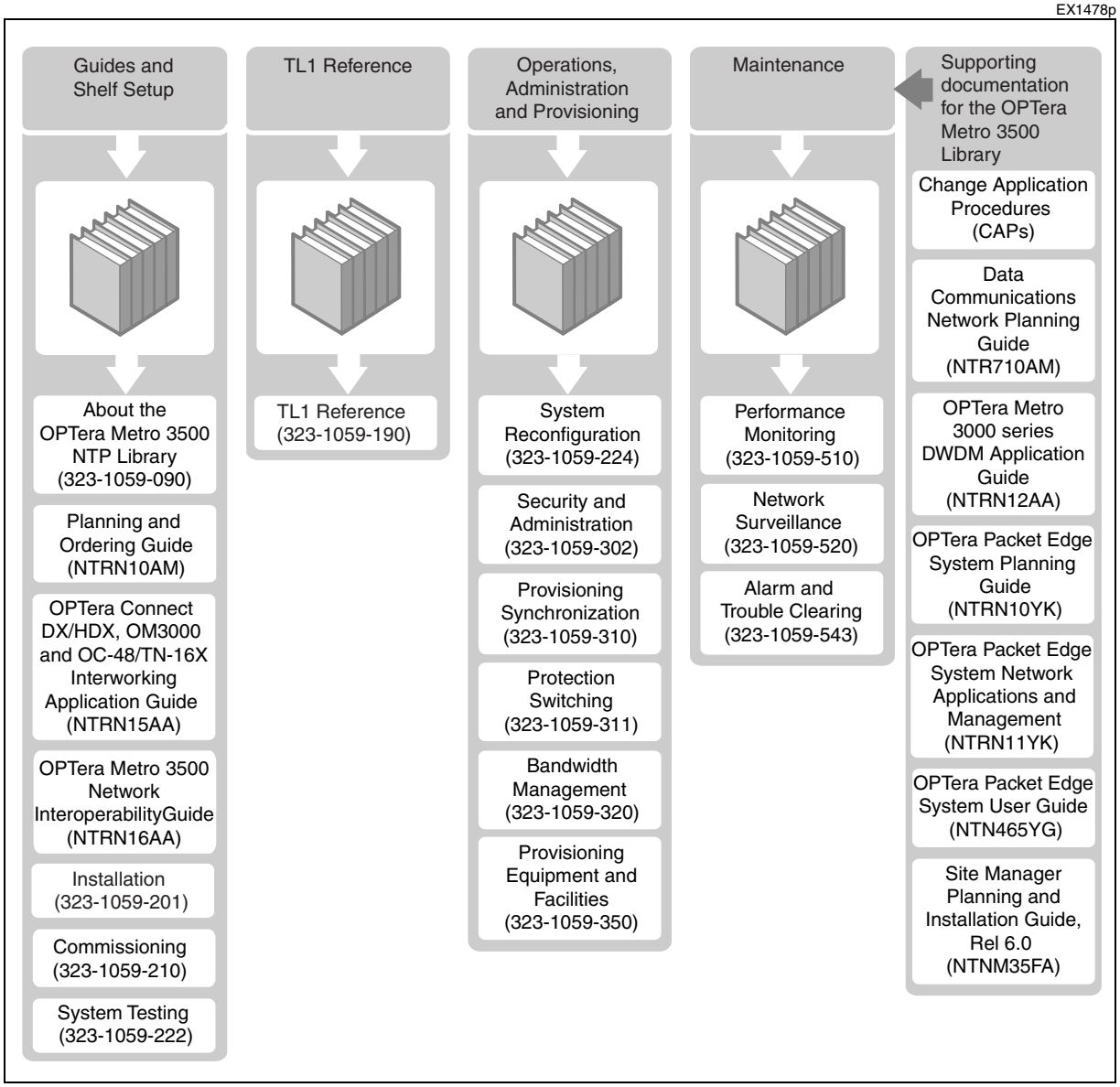
- planners
- provisioners
- network administrators
- transmission standards engineers

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



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

Safety instructions

This section contains safety guidelines that must be followed for personal safety and for the correct handling and operation of equipment.

Warnings and safety precautions

To avoid injury, follow all danger warnings provided with this product and the safety procedures established by your company.

To avoid damage to equipment or service interruptions, follow all caution warnings provided with this product and the safety procedures established by your company.

In this documentation, danger and caution notices are as follows.

DANGER
Risk of personal injury
A danger warning with this symbol indicates a risk of personal injury.

DANGER
Risk of electrical shock
A danger warning with this symbol indicates a risk of personal injury caused by an electrical hazard.

CAUTION
Risk of service interruption
A caution warning with this symbol indicates a risk of service interruption or equipment damage.

CAUTION
Risk of circuit pack damage
A caution warning with this symbol is always used to alert the user to use antistatic protection to avoid damaging circuit packs.

Circuit packs and small form factor pluggable (SFP) modules

All circuit packs and SFP modules are subject to damage by rough handling or from electrostatic discharge. Follow the following procedures to avoid damaging the circuit packs and SFP modules.

Avoiding the development of static electricity

Static electricity charges build up on the body when a person walks a short distance. This static electricity is enough to damage a circuit pack or SFP module. When you work on a shelf, on cables connected to a circuit pack, on a circuit pack, or on an SFP module, always wear a skin-contact ground strap or other appropriate personal grounding device. Ground straps can be the wrist type, or the conductive shoe or heel grounder. Your company can provide antistatic protection by mounting the bays on conductive floor coverings.

All circuit packs and SFP modules are shipped in antistatic containers that are marked with the following symbol.

ATTENTION
OBSERVER DES PRECAUTIONS POUR LA MANIPULATION. DISPOSITIFS SENSIBLES AUX CHARGES STATIQUES

ATTENTION
OBSERVE PRECAUTIONS FOR HANDLING ELECTROSTATIC SENSITIVE DEVICES

Handling, installing, or replacing circuit packs and SFP modules

CAUTION
Risk of service interruption
Using radio communication devices like cellular telephones can cause service interruptions. For example, a -1 W North American cellular telephone must not be used within 30 cm of a system with an open service access front cover.

When handling, installing, or replacing circuit packs and SFP modules, you must observe the following precautions:

- To guard against electrostatic discharge (ESD), wear a wrist strap or other static grounding device before removing a circuit pack or SFP module from its package or from a shelf.
- Place each circuit pack and SFP module in an antistatic bag or container when it is not mounted in a shelf.
- Handle each circuit pack by the faceplate.
- Do not touch the solder side of the circuit pack, the pin connector, or the components.
- Do not stack circuit packs on or against each other.
- Inspect all circuit packs and SFP modules for damage, before installation into the shelf. Inspect all connectors to ensure pins are not damaged.
- Do not force circuit packs or SFP modules into their packaging material.
- Cover the connectors of the transmit and receive optical interface circuit packs with clean dust caps at all times.

To prevent damage to circuit packs while in storage, you must avoid the following:

- accumulation of dirt or dust on the pin connectors
- damage to the board or its components

CAUTION
Risk of service interruption
Board warpage (to boards stored in areas where the humidity can exceed 95% and the temperature can exceed 70°C).

Transporting circuit packs

When transporting circuit packs and SFP modules, place each circuit pack in its original antistatic shielding bag, padding, and box.

Optical fibers

Optical fibers are either single or multiple strand. The following information and precautions apply to all optical fibers.

Laser radiation

All Nortel Networks optical products and associated optical test equipment use laser sources that emit light energy into fiber-optic cables. This energy is within the red (visible) and infrared (invisible) areas of the electromagnetic spectrum.

Laser products are subject to federal regulations, state or provincial regulations, and local practices. Regulation 21CFR 1040 of the U.S. Bureau of Radiological Health requires manufacturers to approve each laser product as Class I, II, III, or IV depending on the characteristics of the laser radiation emitted. In terms of health and safety, Class I products present the least hazard (none at all), while class IV products present the greatest hazard.

During testing and maintenance, some procedures require the handling of optical fibers and transmitters with the dust caps removed. Under these conditions, laser radiation within the limits of Class IIIb can be present.

DANGER

Risk of personal injury

The radiation level produced during testing is of enough amplitude to cause injury to personnel and caution must be exercised to avoid exposure. This precaution applies to any point in the system where the laser signal can be accessed (for example, at the optical connectors on the optical interface circuit packs).

Handling optical fibers

DANGER
Risk of personal injury
Avoid direct exposure to fiber-optic ends or fiber-optic connector ends where the laser signal can be accessed.

Handle fiber-optic cables with caution. Position fiber-optic cables in a safe location during installation.

CAUTION
Risk of equipment damage
Place all optical fiber cuttings in a appropriate container.

Protect fiber-optic connectors with dust caps when they are not connected.

Follow manufacturer instructions when using an optical test set. Incorrect calibration or control settings can result in hazardous levels of radiation.

Replacing optical fibers

When there is an accidental break in the fiber-optic cable, power off all laser sources to the cable or disconnect the remote cable end from the laser sources. The sources can be located in a central office, subscriber premises, or a remote location.

Radio-frequency emissions

The following regulatory notice applies to all Nortel Networks SONET transmission products.

This equipment has been tested and found to comply with the limits for a Class A digital device according to Part 15 of the FCC Rules. These limits are designed to provide acceptable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used according to the instruction manual, can cause harmful interference to radio communications. Operation of this equipment in a residential area can cause harmful interference, in which case users must correct the interference at their cost.

Equipment location

To prevent access by a unqualified personnel, all equipment must be placed in controlled access areas (dedicated equipment rooms, equipment closets, or the like) as described in articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA No. 70. If this equipment cannot be installed in a controlled area, the front cover must be locked.

Site commissioning

Procedures for site commissioning

Procedure 2-1
Commissioning a new shelf processor

The process of commissioning a shelf processor prepares a network element for site testing. Commissioning includes the following tasks:

- changing the password for a default User ID
- adding user accounts to the network element
- setting the centralized security administration (CSA) attributes for the network element
- setting the time of day synchronization status as active and setting the offset threshold value
- selecting the network processor timing source for time of day synchronization
- changing the network element date and time
- changing the network element time zone
- changing the network element name

Requirements

To perform this procedure you must

- directly connect your PC to the shelf processor at the network element site, for each network element in the system
- commission the shelf processor before you commission the NPx

CAUTION
Risk of loss of functionality
Ensure that every network element and network processor has a unique system identifier (SID). If you are changing the name of a network element or NPx, ensure that the new SID is unique.

Step	Action
1	If the shelf power is off, put the power switch on the face of power cards A and B to on.
2	Connect the PC to the RS232 connector on theshelf processor. Refer to *Installation*, 323-1059-201 for RS-232 DCE DB25 cable pinout and assembly.
3	Launch the Preside Site Manager application and log in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network element on page 2-1.

—continued—

Procedure 2-1 (continued)
Commissioning a new shelf processor

Step	Action
4	Change the password of the default User ID. See 323-1059-302, Procedures for user account management and administration on page 3-1.
5	Record the new default User ID passwords in the commissioning data table; see Network element commissioning data on page 2-4.
6	Repeat step 4 and step 5 to change the password for each default User ID. You have completed the Changing of the password of a default User ID.
7	Add a user account to the network element. See 323-1059-302, Procedures for user account management and administration on page 3-1.
8	Record the new User ID and password in the commissioning data table; see Network element commissioning data on page 2-4.
9	Repeat step 7 and step 8 for every new User ID. You have completed the Adding a user account procedure.
10	Set the CSA attributes for the network element. Specify the authentication mode, the alternate authentication mode, the primary and secondary security gateways, and the shared secret. See 323-1059-302, Procedures for user account management and administration on page 3-1.
11	If time of day synchronization will be implemented on this network element, go to step 12 otherwise, go to step 15.
12	Set the time of day synchronization status to On and set the Offset Threshold value. See 323-1059-302, Editing time of day synchronization parameters on the network processor or network element on page 8-2.
13	Set the time of day timing servers for the shelf processor. See 323-1059-302, Setting time of day servers on the network processors or network element on page 8-4.
14	Set the time of day timing offset and daylight savings time parameters. See 323-1059-302, Setting time offset and daylight savings offset on page 8-8. You have set up time of day synchronization on this shelf processor.
15	Set the network element date and time, time zone, and name, See 323-1059-302, Procedures for user account management and administration on page 3-1. ***Note:*** After you change the name of the network element, and click OK, the network element will restart.
16	Record the new network element name in the commissioning data table; see Network element commissioning data on page 2-4.
17	Log in to the network element. See 323-1059-302, Logging in to a network element automatically on page 2-30. **—end—**

Network element commissioning data

Network element number and location	TID	User ID	New password
		Admin	
		Surveil	

Procedure 2-2
Commissioning a new network processor

The process of commissioning a network processor includes the following tasks:

- changing the password for a default User ID
- adding user accounts to the NPx
- setting the centralized security administration (CSA) attributes for the network processor
- setting the time of day parameters on the NPx
- setting the timing sources for time of day synchronization on the NPx
- setting the NPx time zone
- changing the name of the NPx

Note: The NPx continuously retrieves the date and time from the shelf processor and updates the date and time if the difference is more than 2 minutes.

Requirements

To perform this procedure you must

- directly connect your PC to the shelf processor at the NPx site. Refer to *Installation*, 323-1059-201 for RS-232 DCE DB25 cable pinout and assembly
- commission the shelf processor before commissioning the NPx

CAUTION
Risk of loss of functionality
Ensure that every network element and network processor has a unique system identifier (SID). If you are changing the name of a network element or network processor, ensure that the SID name is unique.

Step	Action
1	Ensure the NPx is installed in the shelf.
2	Launch the Preside Site Manager application and log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network element on page 2-1.

—continued—

Procedure 2-2 (continued)
Commissioning a new network processor

Step	Action
3	Change the password of a default User ID. See 323-1059-302, Procedures for user account management and administration on page 3-1.
4	Record the new User ID passwords in the commissioning data table. See Network processor commissioning data on page 2-7.
5	Repeat step 3 and step 4 to change the password for each default User ID. You have completed the password changing procedure.
6	Add a user account to the network processor. See 323-1059-302, Procedures for user account management and administration on page 3-1.
7	Record the new User ID and password in the commissioning data table; see Network processor commissioning data on page 2-7.
8	Repeat step 6 and step 7 for each new user ID to be added.
9	Click OK to close the dialog box. You have completed the adding user account procedure.
10	Set the CSA attributes for the network processor. Specify the authentication mode, the alternate authentication mode, the primary and secondary RADIUS servers, and the shared secrets. See 323-1059-302, Procedures for user account management and administration on page 3-1.
11	If time of day synchronization will be implemented on this network element, go to step 12. Otherwise, go to step 15.
12	Set the time of day synchronization parameters including; status, minimum polling interval, maximum polling interval, and offset interval. See 323-1059-302, Editing time of day synchronization parameters on the network processor or network element on page 8-2.
13	Set the time of day timing servers for the network processor. See 323-1059-302, Setting time of day servers on the network processors or network element on page 8-4.
14	Set the time of day timing offset and daylight savings time parameters. See 323-1059-302, Setting time offset and daylight savings offset on page 8-8. You have set up time of day synchronization on this network processor.
15	Set the network processor time zone, and name. See 323-1059-302, Procedures for user account management and administration on page 3-1.
16	Record the new name of the NPx in the commissioning data table; see Network element commissioning data on page 2-4.
17	Log in to the NPx using the new name.
18	To provision the NPx refer to 323-1059-302, Upgrading the software load on a network processor on page 6-55.

—end—

Network processor commissioning data

Network processor number and location	TID	User ID	New password
		Admin	
		Surveil	

Procedure 2-3
Verifying shelf processor commissioning

Use this procedure to verify and validate that the shelf processor has been properly commissioned. The commisioning information should be compared to site documents to ensure accuracy.

Requirements

To perform this procedure you must

- directly connect your PC to the shelf processor at the network element site, for each network element in the system
- commission the shelf processor before you commission the NPx

CAUTION
Risk of loss of functionality
Ensure that every network element and network processor has a unique system identifier (SID). If you are changing the name of a network element or network processor, ensure that the new SID is unique.

Step	Action
1	If the shelf power is off, set the power switch on the face of power cards A and B to on.
2	Connect the PC to the RS-232 connector on theshelf processor. Refer to *Installation*, 323-1059-201 for RS-232 DCE DB25 cable pinout and assembly.
3	Launch the Preside Site Manager application and log in to the network element. For instructions, see 323-1059-302, Procedures for logging in to a network element on page 2-1.
4	Ensure the customer or designated representative has the applicable user ID and password settings.
5	Display and verify the user account details for a network processor or network element. For instructions, see 323-1059-302, Procedures for user account management and administration on page 3-1.
6	Display and verify the centralized security administration (CSA) attributes for the shelf processor. See 323-1059-302, Procedures for user account management and administration on page 3-1.

—continued—

Procedure 2-3 (continued)
Verifying shelf processor commissioning

Step	Action
7	Display and verify the time of day details for a shelf processor or network element. For instructions, see 323-1059-302, Displaying time of day server details and parameters on page 8-7.
8	Display and verify the network element date and time, time zone, name, node type, node function, software release, default AINS value, and SDTH value. For instructions, see 323-1059-302, Procedures for user account management and administration on page 3-1.
9	Set the network element date and time as required. For instructions, see 323-1059-302, Procedures for user account management and administration on page 3-1.

—end—

Procedure 2-4
Verifying network processor commissioning

Use this procedure to verify and validate that the network processor has been properly commissioned. The commissioning information should be compared to site documents to ensure accuracy.

Requirements

To perform this procedure you must

- directly connect your PC to theshelf processor at the NPx site. Refer to *Installation*, 323-1059-201 for RS-232 DCE DB25 cable pinout and assembly
- commission the shelf processor before commissioning the NPx

CAUTION
Risk of loss of functionality
Ensure that every network element and NPx has a unique system identifier (SID). If you are changing the name of a network element or NPx, ensure that the SID name is unique.

Step	Action
1	Ensure the NPx is installed in the shelf.
2	Launch the Preside Site Manager application and log in to the network processor. For instructions, see 323-1059-302, Procedures for logging in to a network element on page 2-1.
3	Ensure the customer or designated representative has the applicable user ID and password settings.
4	Display and verify the user account details for a network processor or network element. For instructions, see 323-1059-302, Procedures for user account management and administration on page 3-1.
5	Display and verify the centralized security administration (CSA) attributes for the network processor. See 323-1059-302, Procedures for user account management and administration on page 3-1
6	Display and verify the time of day details for a network processor or network element. For instructions, see 323-1059-302, Displaying time of day server details and parameters on page 8-7.
7	Display and verify the network element time zone, and name. For instructions, see 323-1059-302, Procedures for user account management and administration on page 3-1.

—continued—

Procedure 2-4 (continued)
Verifying network processor commissioning

Step	Action
8	Set the network element date and time as required. For instructions, see 323-1059-302, Procedures for user account management and administration on page 3-1.

—end—

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

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

Commissioning

323-1059-210
Standard Release 12.0 Issue 1
November 2003
Printed in Canada

NORTEL NETWORKS™