ciena

Optical Metro 5130

Security Policy for Optical Metro 5130

Release 4.0

What's inside...

Security kit

Applying tamper-evident seals

Configuring the Optical Metro 5130

Roles, Services, Authentication, Finite State Model and Cryptographic Key Management

This document applies to:

Firmware version – 4.00.008.927

Hardware versions:

- Chassis NTB200BAE5 Rev: 03
- S-DNM NTB211AAE5 Rev: 02
- Filler NTB207BAE5 Rev: 02

NTB26403 - Standard Issue 2.4

August 2011

Printed in Canada

Security Policy document revision history

Revision history

The following table provides the revision history for this document.

Version (Issue #)	Date	Comments
1.0	February, 2010	Initial draft for review.
1.2	April, 2010	Revised from internal review.
1.6	June, 2010	Revised with comments from EWA.
1.7	August, 2010	Revised with further comments from EWA.
1.8	September, 2010	Revised with further comments from EWA.
2.0	September, 2010	Revised with further comments from EWA, submitted to NIST.
2.1	January, 2011	Revised with further comments from EWA.
2.2	February, 2011	Revised with further comments from EWA.
2.3	February, 2011	Revised Table 4.2.
2.4	August, 2011	Revised Figure 1-8, Page 1-7 and Page 3-4.

Contents

Security Policy document revision history iii
About this document vi

Security kit 1

Cryptographic module overview 2
- Chassis 4
- Logical interfaces 6
- LEDs 10

Security kit contents 14
Physical Security 14
Tamper-evident seals 14

Applying tamper-evident seals 1

Applying tamper-evident seals 1

Configuring the Optical Metro 5130 1

Required configuration settings 2
- FIPS mode of operation 2
- Authentication modes 3
- Intrusion attempt handling 3
- SNMP 4
- IPSec transport mode 4
- Encryption 5

Roles, Services, Authentication, Finite State Model and Cryptographic Key Management 1

User accounts, roles and services 1
- Maintenance role 2
- Crypto Officer role 2
- User role 2
- Backups and restores 2
- Passwords 2

Configuring the OM 5130 to non-FIPS mode 3
- Displaying FIPS mode and state 4

Initialization of encryption keys 4
- Zeroization 5

Finite State Model 5

Self-tests 6
Mitigation of other attacks 8
Services and Cryptographic Key Management 8
OM 5130 FIPS Approved Algorithms 13
Non-FIPS Approved Algorithms 13

About this document

This guide describes how to provision the Optical Metro 5130 (OM 5130) for secure operation and it is the non-proprietary Cryptographic Module Security Policy for the OM 5130. This security policy describes how the OM 5130 meets the security requirements of FIPS 140-2, and how to operate the OM 5130 in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the OM 5130, firmware version 4.00.008.927.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at:
http://csrc.nist.gov/groups/STM/cmvp/index.html

Topics covered include:

- "Cryptographic module overview"
- "Security kit contents"
- "Tamper-evident seals"
- "Applying tamper-evident seals"
- "Roles, Services, Authentication, Finite State Model and Cryptographic Key Management"

This document is part of the complete FIPS 140-2 submission package. In addition to this document, the complete submission package contains the following:

- Vendor Evidence Document
- Finite State Machine
- Source code listing
- Other supporting documentation

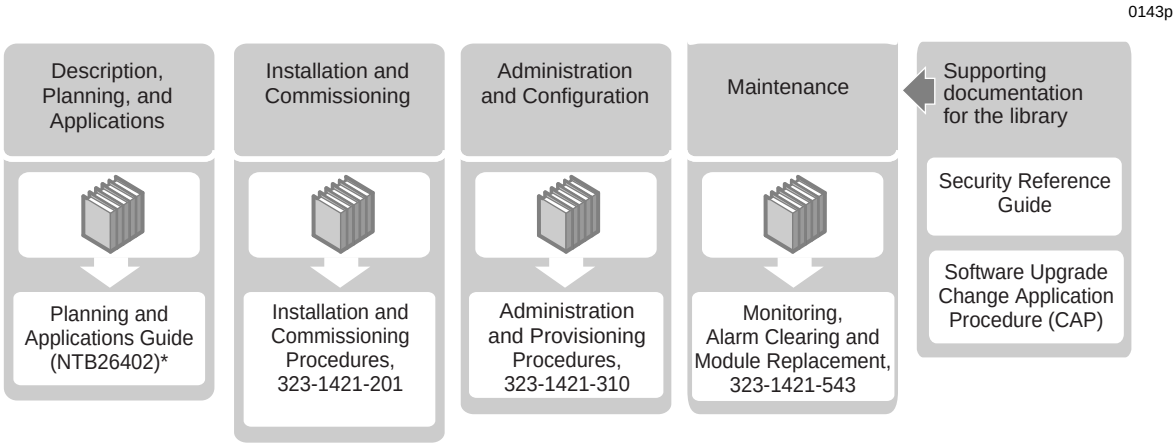
Audience

The following members of your company are the intended audience of this document:

- security administrators
- network administrators

OM 5130 Release 4.0 library

The following roadmap shows the structure of the Optical Metro 5130 product documentation.



* Includes list of abbreviations and master index

You can access the library by visiting www.ciena.com, under the learning & support heading.

Technical Publications

The *OM 5130 product documentation* consist of descriptive information and procedures.

Descriptive information

These documents provide detailed descriptive information about OM 5130, including system software and hardware descriptions, technical specifications, and ordering information.

Procedures

These documents contain all procedures required to install, provision, and maintain the OM 5130.

References in this document

This document refers to:

- *Administration and Provisioning Procedures,* 323-1421-310.
- *Planning and Applications Guide,* NTB26402
- *Network Security Dashboard User Guide*, 323-1421-199
- *Monitoring, Alarm Clearing and Module Replacement,* 323-1421-543

Security kit

The Optical Metro 5130 security kit enables you to configure the Optical Metro 5130 (OM 5130) to ensure secure operation and protection of cryptographic parameters. The requirements found in this document are based on the Federal Information Processing Standard (FIPS) 140-2 Level 2 security requirements.

The tamper evident seals shall be installed for the module to operate in a FIPS approved mode of operation.

Table 1-1 specifies the targeted security level for each FIPS 140-2 section.

Table 1-1
FIPS 140-2 Section Security Levels

Section	Security level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	NA
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	NA

Cryptographic module overview

The OM 5130 cost effectively simplifies data file mobility between data centers. The OM 5130 increases WAN efficiency, natively consolidates data and storage networks onto a common WAN link and delivers definable time-of-day bandwidth management that allocates bandwidth to the required application at the required time of day.

The cryptographic module is a multiple-chip standalone cryptographic module.

The OM 5130 is commonly used to extend data centers to secondary and regional data centers for data protection and regulatory compliancy purposes. WAN connectivity between these locations is supported over Ethernet or Coarse Wavelength Division Multiplexing (CWDM).

The cryptographic module for the OM 5130 (Figure 1-1) system includes:

- One OM 5130 chassis with associated common equipment (NTB200BAE5)
- One or more S-DNM modules (NTB211AAE5)
  - — one S-DNM and two filler cards (see Figure 1-2, Figure 1-3, and Figure 1-4) or
  - — two S-DNMs and one filler card, (see Figure 1-5, Figure 1-6, and Figure 1-7) or
  - — three S-DNMs (see Figure 1-1)
- One or more filler cards (NTB207BAE5)
- One Optical Metro 5130 security kit (NTB209LAE6)

Figure 1-1
Optical Metro 5130 (S-DNMs in slots 1, 2 and 3)

Note: The cryptographic module boundary is the entire OM 5130. The cryptographic module is a multiple-chip standalone cryptographic module.

Figure 1-2
Optical Metro 5130 (S-DNM in slot 1 and filler cards in slots 2 and 3)

Figure 1-3
Optical Metro 5130 (S-DNM in slot 2 and filler cards in slots 1 and 3)

Figure 1-4
Optical Metro 5130 (S-DNM in slot 3 and filler cards in slots 1 and 2)

Figure 1-5
Optical Metro 5130 (S-DNMs in slots 1 and 2 and filler card in slot 3)

Figure 1-6
Optical Metro 5130 (S-DNMs in slots 1 and 3 and filler card in slot 2)

Figure 1-7
Optical Metro 5130 (S-DNMs in slots 2 and 3 and filler card in slot 1)

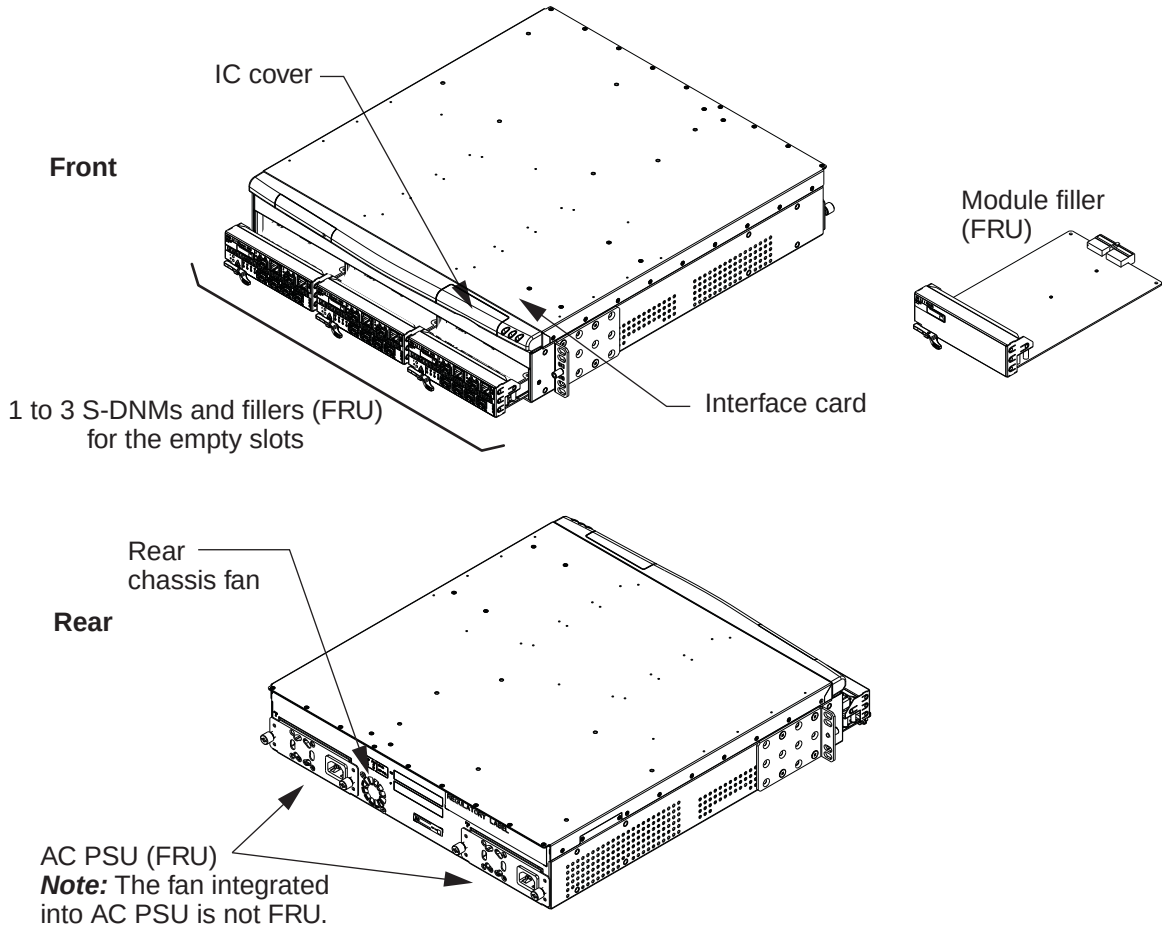
Chassis

The 2U chassis is a three-slot rack-mountable unit with rear and front access. The chassis is designed to fit in a server environment and is shipped with mounting brackets for installation in a 19 in., 23 in., or ETSI server rack. See *Installation and Commissioning Procedures*, 323-1421-201, for installation procedures. See Ordering information in the *Planning Guide*, NTB26402 for information about ordering 19 in., 23 in., or ETSI installation kits.

The 2U chassis provides two redundant power supplies.

Figure 1-8 on page 1-5 shows front and rear views of the 2U chassis. The Secure DNM (S-DNM) can be equipped in service slots 1, 2, or 3.

Figure 1-8
2U chassis equipped with various modules



Legend

AC PSU = alternating current Power Supply Unit
FRU = field-replaceable unit
IC = Interface Card
S-DNM = Secure Dynamic Network Module

Note 1: The midplane, midplane fans, and Interface card, are integrated into the chassis and are not removable.
Note 2: Grounding is achieved through the third (green/ground) wire in the AC power cables.

Logical interfaces

The hardware supports the logical interfaces described in Table 1-2.

Table 1-2
Logical interfaces

Optical Metro 5130 physical interface	FIPS 140-2 logical interface(s)	Description	Status Output Interface (LEDs)
S-DNM Client Ports	Data Input Interface Data Output Interface	See "Secure Dynamic Network Module interfaces" on page 1-7.	See "Secure Dynamic Network Module" on page 1-10.
S-DNM WAN Ports	Data Input Interface Data Output Interface Control Input Interface	See "Secure Dynamic Network Module interfaces" on page 1-7.	See "Secure Dynamic Network Module" on page 1-10.
Chassis Ethernet Port Chassis Serial Port Chassis USB Port	Control Input Interface Data Input Interface	See "Interface Card" on page 1-8.	See "Interface Card" on page 1-12.
Chassis Ethernet Port Chassis Serial Port Chassis USB Port	Status Output Interface Data Output Interface	See "Interface Card" on page 1-8.	See "Interface Card" on page 1-12.
Plugs on AC Power Supply Unit (PSU) A & B	Power Interface	See "Power Supply Unit" on page 1-9.	See "Power Supply Unit" on page 1-13.
NMI button	Control Input Interface	See "Interface Card" on page 1-8.	None
Reset button	Control Input Interface	See "Interface Card" on page 1-8.	None

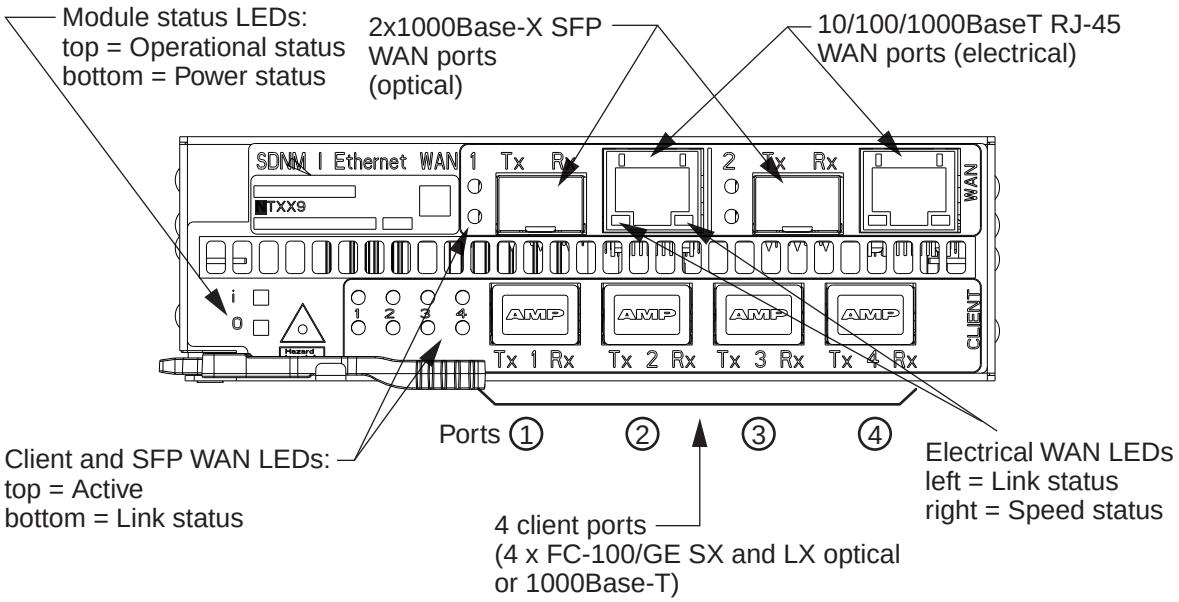
Secure Dynamic Network Module interfaces

The Secure Dynamic Network Module is a single-slot service module that accepts plain text data from up to four independent LAN/SAN client ports. The Secure Dynamic Network Module aggregates the data (encrypted or bypassed) from the client ports into two WAN physical interfaces for transport across the wide area network.

Additional S-DNMs do not affect security as they do not provide any addition control interfaces, and all keys are input and output in the same manner regardless of the number of S-DNMs. There were two S-DNMs used in the test configuration.

Figure 1-9 shows the ports on the Secure Dynamic Network Module. Table 1-3 describes the ports on the Secure Dynamic Network Module.

Figure 1-9
Example of module faceplate



Note: Client ports 1, 2, 3, 4 are Small Form-factor Pluggable (SFP) client ports. WAN ports 1 and 2 support 10/100/1000Base-T (RJ-45) and 2x1000Base-X SFP.

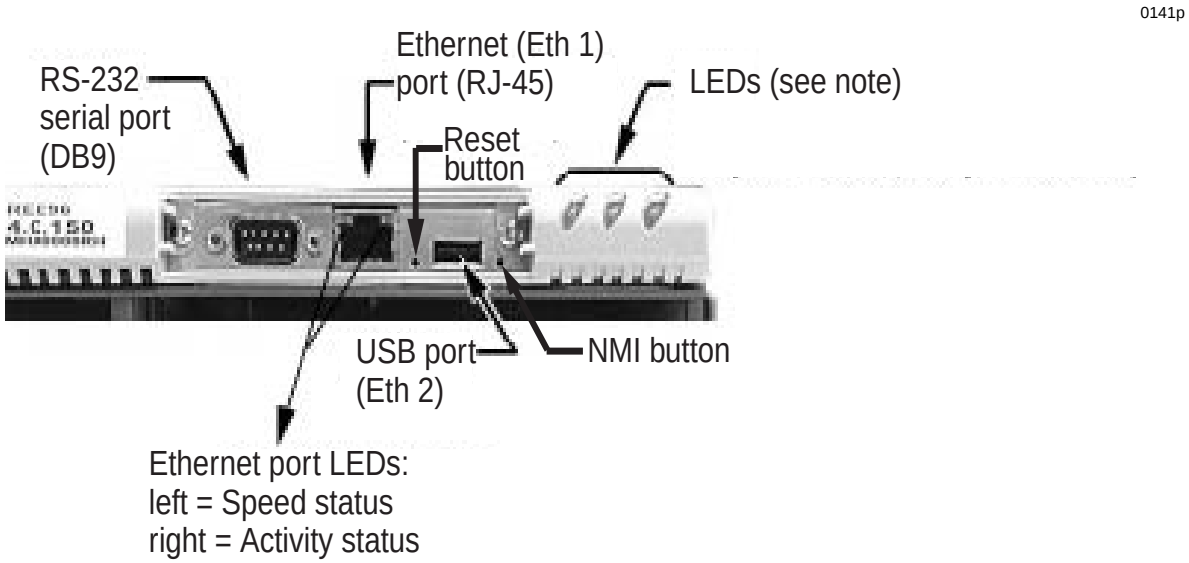
Table 1-3
Secure Dynamic Network Module

WAN-1 and WAN-2 ports	10/100/1000 BaseT RJ-45 WAN ports	Client-1, Client-2, Client-3, and Client-4 ports
• used to interconnect to the wide area network (WAN) through switches, hubs or other WAN access/transport devices • You can only use either the GE or the 10/100/1000BaseT at one time on a WAN port. • All RJ-45 Ethernet ports are autosensing and support autonegotiation, full and half duplex operation (autonegotiation to full duplex).		• used to connect to FC, GE, or 1000Base-T subtending Storage Area Network (SAN) equipment

Interface Card

Figure 1-10 shows the ports on the Interface Card. Table 1-4 describes the ports on the Interface Card.

Figure 1-10
Interface Card without cover



Note: The LEDs provide (from left to right): Shelf status, PSU B, and PSU A.

Table 1-4
Interface Card ports

RS-232 serial port (DB9)	Ethernet port (10/100 Mbps RJ-45)	USB port (10Mbps)
• dial-in support through a modem attached to this port • supports OM 5130 Site Manager and CLI using PPP • supports connections using a terminal server setup with PPP	• hosts 3 management interfaces for the node: Site Manager, CLI, or SNMP Manager • two LEDs dedicated to Ethernet traffic monitoring: one LED for activity and one LED for speed • All RJ-45 Ethernet ports are autosensing and support autonegotiation, full and half duplex operation (autonegotiation to full duplex).	• provides secadmin and observer access to the Eth 2 IP interface by a USB to Ethernet adapter (an ASIX 8817x chips-based) using the OM 5130 CLI and SNMP Manager.

Power Supply Unit

The pluggable alternating current Power Supply Unit (AC PSU) is located in the rear of the chassis. Figure 1-11 shows the AC PSU.

Figure 1-11
Power Supply Unit

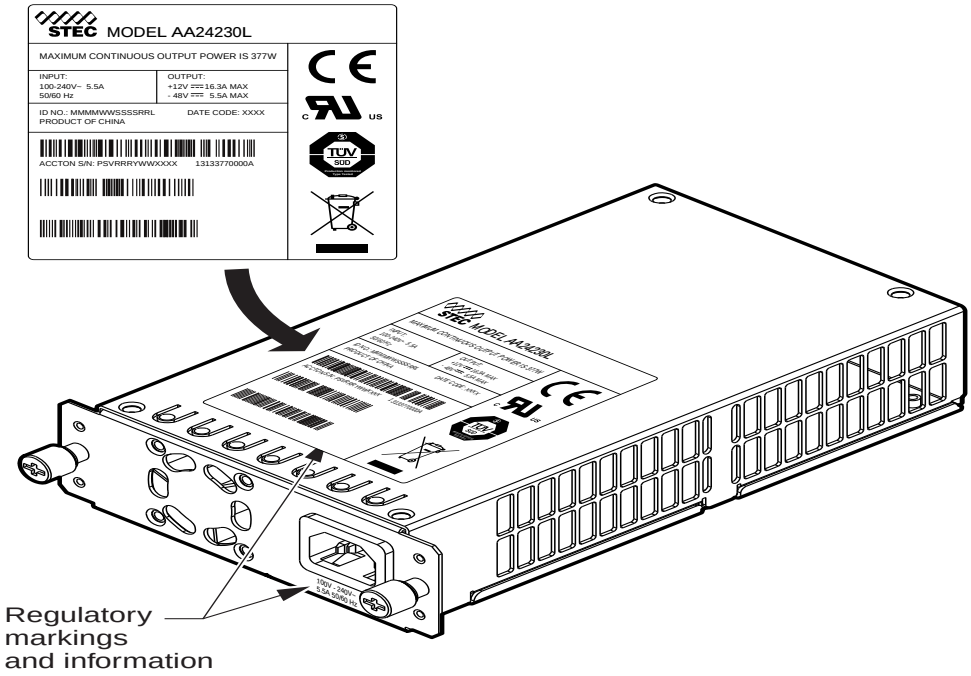
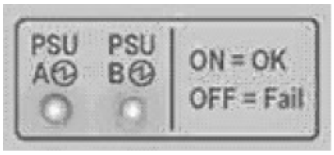


Figure 1-12
LEDs related to PSU faults on back of the chassis



LEDs

This section describes the LEDs for the:

- "Secure Dynamic Network Module" on page 1-10
- "Interface Card" on page 1-12
- "Power Supply Unit" on page 1-13

Secure Dynamic Network Module

The following tables describe the LEDs of the S-DNM:

- Table 1-5 describes the module LEDs
- Table 1-6 describes the client port LEDs
- Table 1-7 describes the SFP WAN port LEDs
- Table 1-8 describes the RJ-45 WAN port LEDs

See Figure 1-9 on page 1-7 for the location of the above LEDs on the module.

Table 1-5
S-DNM status LEDs

Power	Operation		Description
Green	Red	Green	
OFF	X	X	No DC power or power out of range
ON	X	X	DC power is available to the internal circuitry
ON	OFF	OFF	Module is in reset mode or is out-of-service
ON	OFF	ON	Self-test passed successfully and module is operational
ON	ON	OFF	Boot or self-test failed and critical alarm raised on the S-DNM

Table 1-6
Client port LEDs

Active		Link	Description
Red	**Green**	**Yellow**	
OFF	OFF	OFF	Facility out-of-service (OOS); safe to remove fiber
OFF	OFF	ON	Facility OOS or no channel assignment and fault condition detected; safe to remove fiber
OFF	ON	OFF	Facility in-service (IS) with channel assignment running error-free traffic; do not remove fiber
OFF	ON	ON	Facility IS with channel assignment and fault condition detected; safe to remove fiber
ON	OFF	OFF	Pluggable module transceiver failure; safe to remove fiber and pluggable module
ON	OFF	ON	Not applicable
ON	ON	OFF	
ON	ON	ON	

Table 1-7
SFP WAN port LEDs

Active		Link	Description
Red	**Green**	**Yellow**	
OFF	OFF	OFF	Facility OOS; safe to remove fiber
OFF	OFF	ON	Facility OOS or no channel assignment and fault condition detected; safe to remove fiber
OFF	ON	OFF	Facility IS with channel assignment running error-free traffic; do not remove fiber
OFF	ON	ON	Facility IS with channel assignment and fault condition detected; safe to remove fiber
ON	OFF	OFF	SFP transceiver failure; safe to remove fiber and SFP
ON	OFF	ON	Not applicable
ON	ON	OFF	
ON	ON	ON	

Table 1-8
RJ-45 WAN port LEDs

Link	Speed		Description
Green	**Green**	**Yellow**	
OFF	OFF	OFF	No link
ON	OFF	OFF	10 Mbit/s link
ON	ON	OFF	100 Mbit/s link
ON	OFF	ON	1000 Mbit/s link
Flash	X	X	Data being transmitted/received

Interface Card

The Interface Card has three main LEDs, and two LEDs on the Ethernet port.

On the 2U chassis, the three main LEDs provide:

- Shelf status (see Table 1-9)
- AC power status for power supply A - The power status LED is green when power is available. If power is not available or is out of range, the LED is off.
- AC power status for power supply B - The power status LED is green when power is available. If power is not available or is out of range, the LED is off.

Table 1-9
Interface Card shelf status LEDs

Shelf Status		Description
Green	**Red**	
ON	OFF	Shelf is Operational
Blinking	OFF	Running boot / self-tests
OFF	OFF	Shelf is in reset mode
OFF	ON	Self-test failed, or Critical or Major Alarm raised on OM 5130

The two LEDs on the Ethernet port provide link speed and link activity. See Table 1-10.

Table 1-10
Interface Card Ethernet Port LEDs

Link Speed		Link Activity	Description
Green	**Amber**	**Green**	
ON	OFF	Blinks	Link is 100 Mbit/s and up.
OFF	ON	Blinks	Link is 10 Mbit/s and up.
OFF	OFF	OFF	Link is not available.

Power Supply Unit

The Interface Card on the front of the chassis includes LEDs that indicate power status. See Table 1-11 on page 1-13.

Table 1-11
AC Power Status LEDs

LEDs on the front of the chassis		LEDs on the back of the chassis		Description
PS-A	**PS-B**	**PS-A**	**PS-B**	
ON	ON	ON	ON	Power is available to both power supplies.
ON	OFF	ON	OFF	Power Supply Unit-B Missing
OFF	ON	OFF	ON	Power Supply Unit-A Missing
ON	OFF	ON	OFF	AC power feed for PSU-B missing
OFF	ON	OFF	ON	AC power feed for PSU-A missing
ON	OFF	ON	OFF	Voltage out of range PSU-B
OFF	ON	OFF	ON	Voltage out of range for PSU-A
ON	OFF	ON	OFF	Power Supply PSU-B Failed
OFF	ON	OFF	ON	Power Supply PSU-A Failed
OFF	OFF	OFF	OFF	Power Supply Unit-A and Power Supply Unit-B missing
OFF	OFF	OFF	OFF	AC power feed for PSU-A and PSU-B missing
OFF	OFF	OFF	OFF	Voltage out of range for PSU-A and PSU-B
OFF	OFF	OFF	OFF	Power Supply PSU-A and PSU-B Failed

Security kit contents

Table 1-12 lists the items contained in the Optical Metro 5130 security kit (NTB209LAE6).

Table 1-12
Optical Metro 5130 security kit contents

Description	Quantity
Optical Metro 5130 tamper-evident seals	10 (9 required with 1 spare)
Security Policy	1

Physical Security

A thick steel case protects the OM 5130. The OM 5130 meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designed for business use (Class A). The steel case may be removed to allow access to the CRC motherboard by unscrewing the screws on the top cover of the unit. The S-DNMs may be removed by pulling the S-DNM's front latch to allow access to the S-DNM motherboard.

Once the tamper-evident seals are applied, the cover and S-DNMs can not be removed without signs of tampering.

Tamper-evident seals

The tamper-evident seals are bright yellow vinyl seals with self-adhesive backings that provide evidence of tampering when unauthorized access to the OM 5130 is attempted. Any attempt to access the OM 5130 will result in one or more of the tamper-evident seals being damaged.

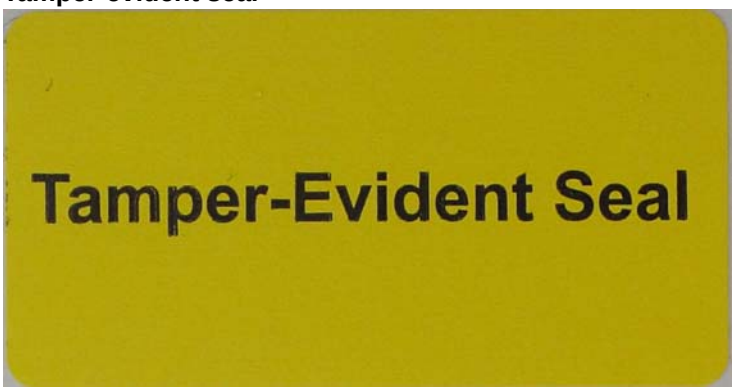
Figure 1-13 on page 1-15 shows an example of a tamper-evident seal.

If an attempt is made to peel off the destructible vinyl seal, a residue is left behind that is very difficult to remove. Other signs of tampering include warped or bent metal covers, and scratches in the paint of the module.

CAUTION
To ensure security of the system, any extra seals should be secured and controlled by the Crypto Officer. It is recommended that the seals be inspected monthly for any signs of damage or tampering.

Replacement seals (NTB209LBE6) can be separately ordered.

Figure 1-13
Tamper-evident seal



Applying tamper-evident seals

This chapter describes how to apply tamper-evident seals.

Applying tamper-evident seals

Before you begin, note the following:

- You must apply the tamper-evident seals yourself. Ciena does not apply the seals.
- The tamper-evident seals are very fragile and require careful handling.
- You must press the seal firmly to the chassis to ensure proper adhesion. Sufficient pressure and time is required for proper adhesion. You can achieve higher initial bonds through increased application pressure.
- You must allow 24 hours under ambient conditions for the adhesive on the tamper-evident seal to completely cure.
- If you need to replace an S-DNM or power supply unit, the Crypto Officer must first zeroize the keys and passwords on the OM 5130. See "Zeroization" on page 4-5. Once the zeroization has been completed, remove the seals on the S-DNM or PSU and replace the S-DNM or PSU using the module replacement procedure in *Monitoring, Alarm Clearing and Module Replacement*, 323-1421-543.

ATTENTION

The system is not fully secure until the adhesive has completely cured. Curing can take up to 24 hours.

Applying the seals

Follow these steps to apply the tamper-evident seals to the system:

1 Ensure that the temperature of the chassis is above 10°C. The recommended temperature is approximately 20°C.

2 Turn off and unplug the system.

3 Remove any grease, dirt, or oil from the area where the seal is to be applied. Alcohol wipes are recommended for this purpose.

4 Clean each S-DNM / filler card faceplate where the faceplate is notched (top left-hand corner of the module). See Figure 2-1 on page 2-2 and Figure 2-2 on page 2-2.

5 Insert the S-DNM / Filler cards into the chassis. Ensure the modules are fully seated and latched.

6 Apply the seals exactly as shown in Figure 2-3 on page 2-3, Figure 2-4 on page 2-4 and Figure 2-5 on page 2-5 with the seals overlapping the seams. The overlap is approximately 50% on each part the seal is secured against. Seals are required in a total of nine locations on the chassis.

Once the seals are applied, you are now ready to set the OM 5130 in the FIPS operating mode, see "FIPS mode of operation" on page 3-2.

Figure 2-1
Filler card faceplate

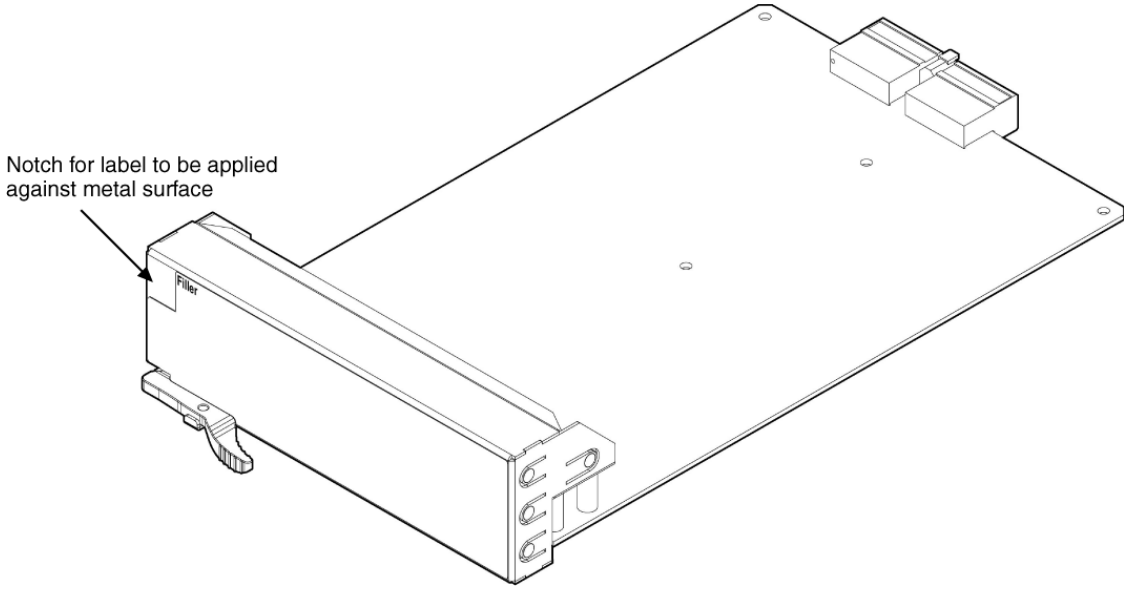


Figure 2-2
S-DNM faceplate

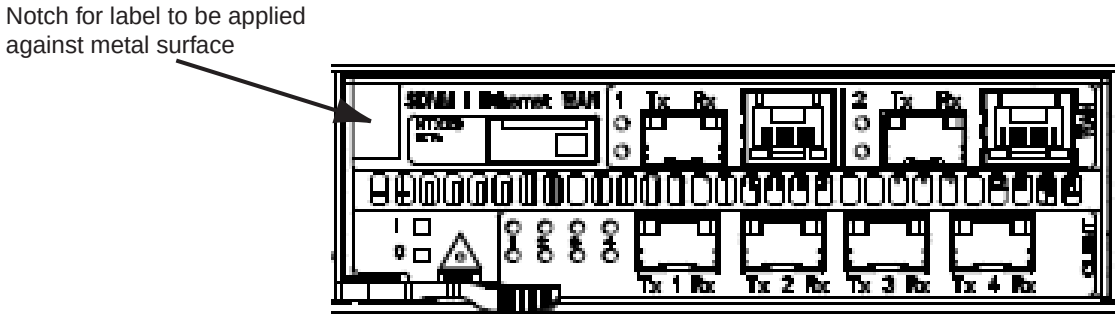


Figure 2-3
Tamper-evident seals applied to the front and right sides of the chassis (5 locations)

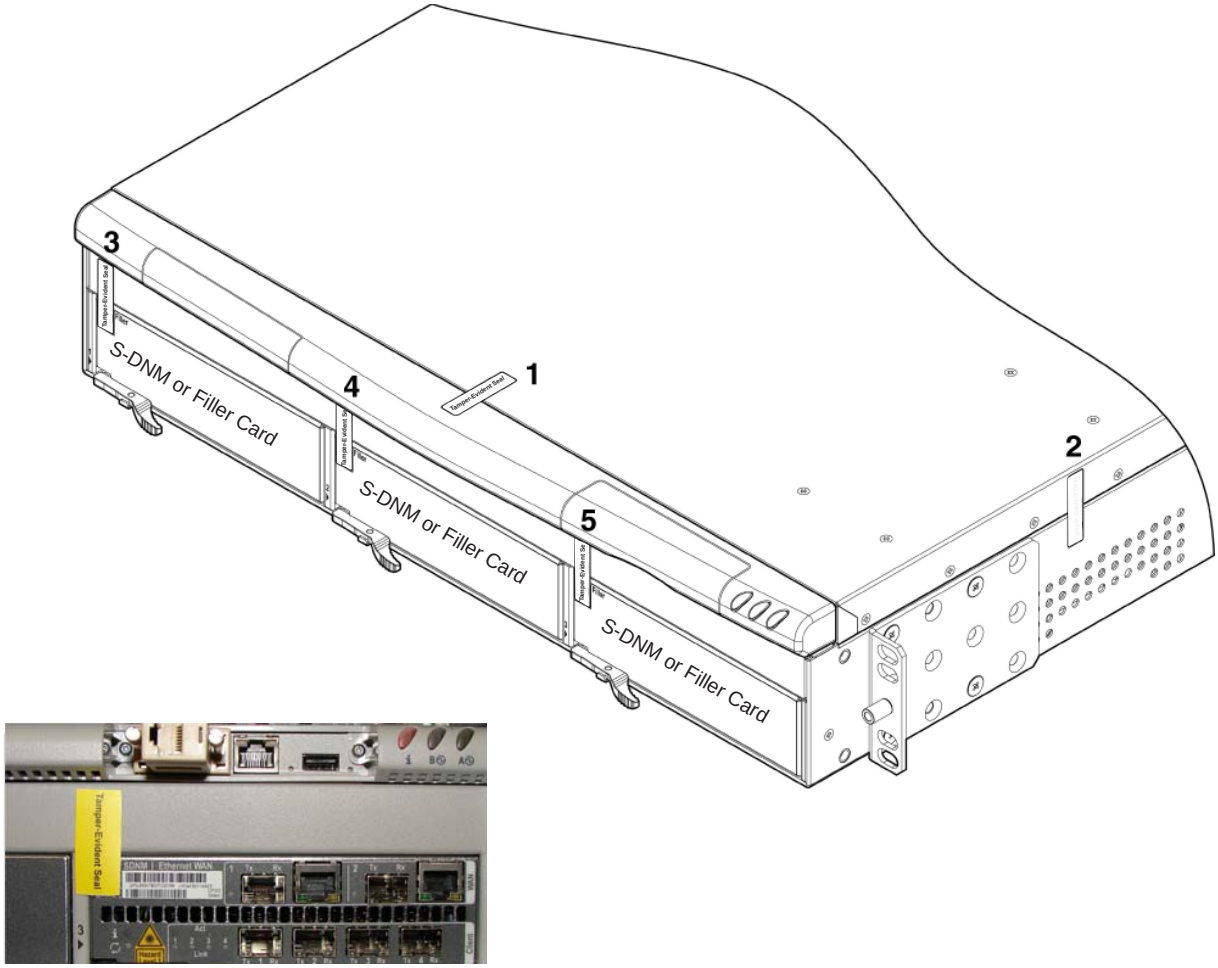


Figure 2-4
Tamper-evident seals applied to the left side of the chassis (2 locations)

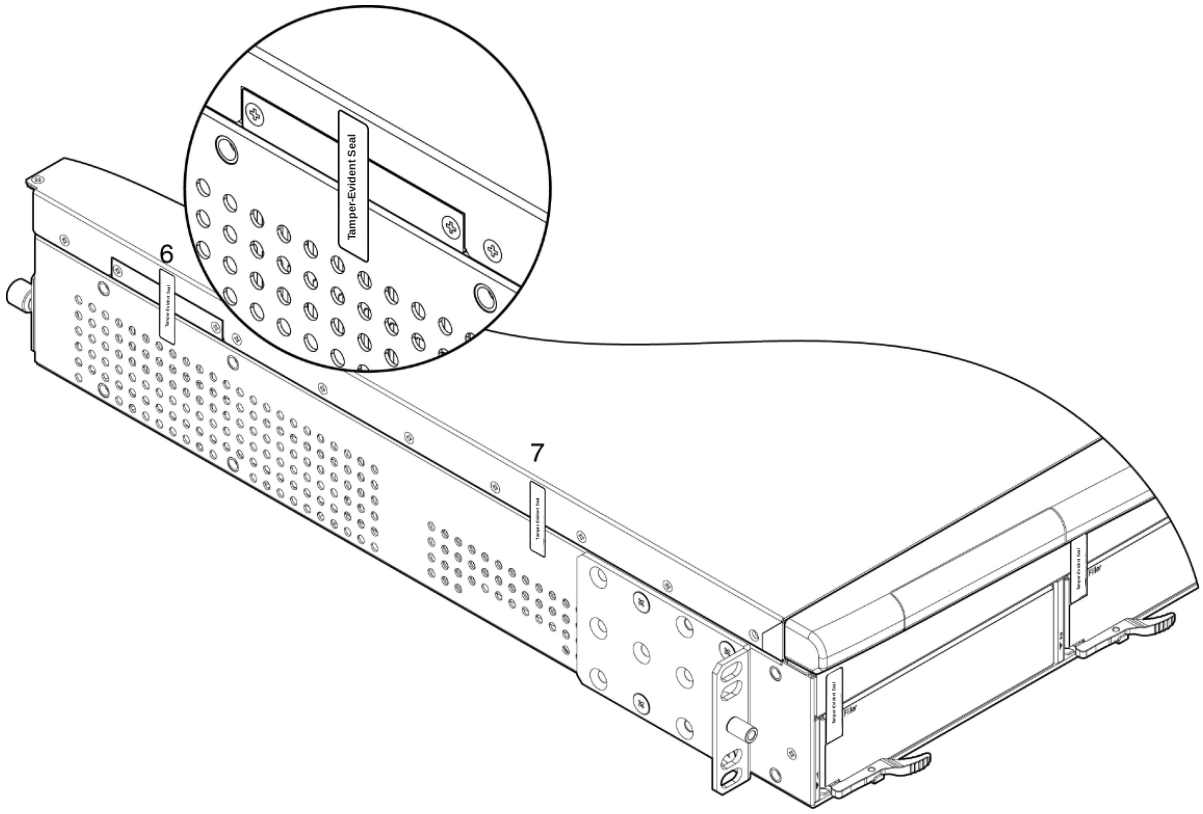
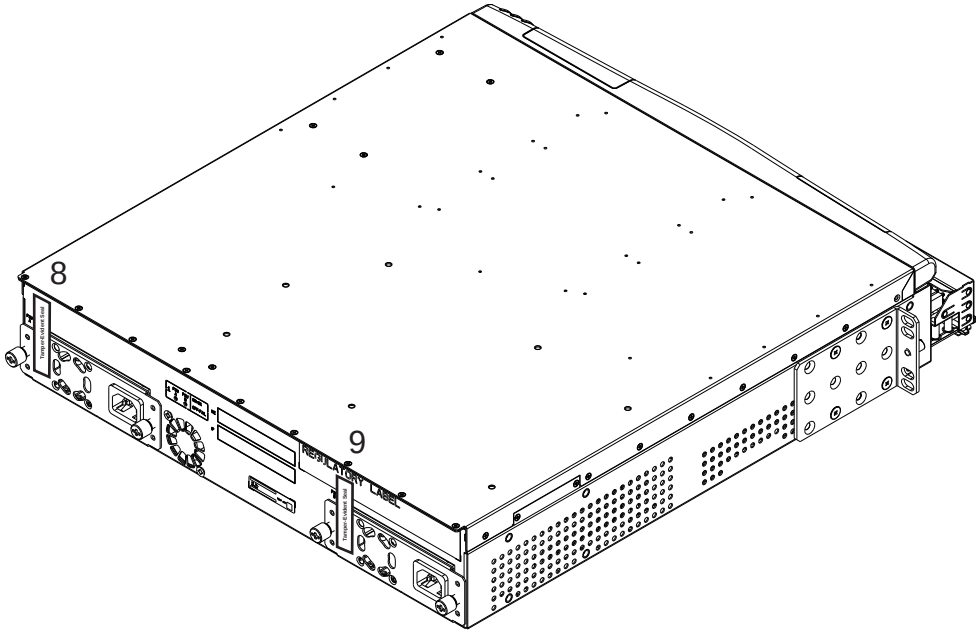


Figure 2-5
Tamper-evident seals applied to the back side of the chassis over the alternating current Power Supply Units (AC PSUs) (2 locations)



Configuring the Optical Metro 5130

This chapter describes how to configure the Optical Metro 5130 (OM 5130) for FIPS mode of operation. See Table 3-1 for an overview of required tasks.

Table 3-1
Configuring the Optical Metro 5130 for FIPS mode of operation

Task	Details
Set the OM 5130 in the FIPS mode	page 3-2
Enable complex password validation	page 3-2
Set the authentication mode to local account	page 3-3
Enable intrusion attempt handling	page 3-3
Enable IPSec	page 3-4
Enable encryption	page 3-5

Required configuration settings

This section provides the recommended configuration settings for a secure mode of operation. This section describes the following:

- FIPS mode of operation
- Authentication modes
- Intrusion attempt handling
- IPSec transport mode
- Encryption

FIPS mode of operation

The OM 5130 can be operated in FIPS mode or non-FIPS mode. You must place the module in FIPS mode with the secadmin user privilege.

To access the system with a secadmin user privilege, you must log into the CLI through a SSH V2 connection. Site Manager can be used to display FIPS settings. All modules (S-DNMs / filler cards) must be installed in the OM 5130 shelf before the OM 5130 is configured to operate in FIPS mode.

ATTENTION

The OM 5130 can only operate in the FIPS mode of operation if the factory installed firmware is 4.00.008.927 and an upgrade has not been performed in the non-FIPS mode.

ATTENTION

Daisy chaining In Band Comms is not permitted when operating in a FIPS approved manner.

Configuring the OM 5130 for FIPS operation

The following command will place the OM 5130 in the FIPS mode:

```
configure security fips mode enabled
```

ATTENTION

During a non-FIPS mode to FIPS mode transition, the OM 5130 is restarted and OM 5130 configuration is deleted, passwords are reset to default values, and cryptographic keys are zeroized. The OM 5130 IP configuration is an exception and it is preserved during the transition.

Enabling alternating bypass

To put the OM 5130 into an alternating bypass state, complete the following steps:

1 Put the particular client port out of service using the following command. You must be logged in as an admin user over a CLI or Site Manager session.

```
configure port state disabled
```

2 Enable FIPS bypass capability for the particular client port using the following command. You must be logged in as a secadmin user over an IPSec session.

```
configure security fips bypass-service
```

3 Disable the data encryption on the particular client port using the following command. You must be logged in as a secadmin user over a CLI IPSec session. This step must be executed within 2 minutes after executing step 2. If step 3 is not completed within 2 minutes, repeat step 2.

```
configure encryption state disabled
```

Note: When a OM 5130 transitions to the FIPS alternating bypass state, the internal bypass test is executed. If the bypass self-test fails, the OM 5130 enters the Non-Recoverable Error state. For more information see "FIPS error state" on page 4-4.

Authentication modes

Local account authentication mode must be provisioned for access to the OM 5130 when in FIPS mode.

Note 1: Central authentication mode using RADIUS is not allowed in FIPS mode. The command to set central authentication is rejected with an error message when the OM 5130 is in FIPS mode.

Note 2: For a node using a central authentication mode, any attempt to set it to the FIPS mode is blocked until the authentication mode is changed to local.

Intrusion attempt handling

OM 5130 supports intrusion attempt handling. This feature allows you to specify

- the number of invalid login attempts (range is 2 to 20) a user is allowed before the user is locked out and an Intrusion Attempt alarm raised. This feature is set using the following command;

```
configure security thresholds max-attempts <2
to 20>
```

- the duration of the lockout (maximum of 60 seconds). This feature is set using the following command;.

```
configure security thresholds lockout-time
<0-60>
```

Users are locked out based on their originating address. Security logs record the originating address and connection type of invalid login attempts.

Note: Results of previous authentications are stored in volatile memory and cleared when the OM 5130 is powered off.

ATTENTION

You must set the number of invalid login attempts to 5 and the duration of the lockout to 60 seconds. See *Administration and Provisioning Procedures* (323-1421-310) for the procedure to set intrusion attempt handling.

The probability of a random intrusion attempt working within a minute when the invalid login attempt is set to 5 and the time-out is set to 60 seconds would be 5 in 8,771,466,662,398 or 1 in 1,754,293,332,480. For more information on Passwords see page 4-2.

SNMP

- Site Manager uses SNMP.
- No critical security parameters other than the SNMP passwords are communicated through Site Manager.

  See *Planning and Applications Guide*, NTB26402 for more information on Site Manager.

IPSec transport mode

OM 5130 supports IPSec to secure OAM (Operations, Administration, and Maintenance) traffic. IPSec allows all OAM traffic over a secure tunnel and through the system firewall. Specifically, IPSec allows you to perform upgrade and traffic advisor operations over a secure tunnel with the firewall enabled.

ATTENTION

You must enable IPSec in FIPS mode to be compliant with FIPS 140-2. IPSec must be provisioned to use SHA-1 authentication, Triple-DES encryption and Diffie-Hellman group 14 key agreement to be FIPS 140-2 compliant. See *Administration and Provisioning Procedures* (323-1421-310) to provision IPSec.

Note: Remote management of an OM 5130 that is more than one OM 5130 away on the WAN interface is not allowed in a FIPS compliant mode of operation.

Encryption

Encryption must be provisioned through the command line interface (CLI) with a secure shell (SSH V2) connection over an IPSec session. You must provision encryption with the secadmin user class.

Below is an overview of the steps to set up encryption:

1 Disable the administrative state of the near-end and far-end ports.

2 Enable the secadmin user account and change the password of the account.

3 Log into CLI with the secadmin user through SSH V2 with IPSec enabled.

4 Generate the encryption key at the near-end port, then load the key to the peer port.

5 Enable encryption on each port. You can then enable the administrative state of each port.

Note: Enabling or disabling a port can be performed with an admin or operator account. After encryption is enabled, keys can be changed in-service by a secadmin user account. There is no need to disable encryption or to disable the port.

See *Administration and Provisioning Procedures* (323-1421-310) for the complete encryption procedure.

Roles, Services, Authentication, Finite State Model and Cryptographic Key Management

This chapter describes the following critical security parameters and finite state model and it also includes the following sections:

- "User accounts, roles and services" on page 4-1
- "Configuring the OM 5130 to non-FIPS mode" on page 4-3
- "Initialization of encryption keys" on page 4-4
- "Finite State Model" on page 4-5
- "Self-tests" on page 4-6
- "Mitigation of other attacks" on page 4-8
- "Services and Cryptographic Key Management" on page 4-8
- "OM 5130 FIPS Approved Algorithms" on page 4-13
- "Non-FIPS Approved Algorithms" on page 4-13

User accounts, roles and services

The OM 5130 supports multiple simultaneous users and internally maintains the separation of roles and services performed by each operator. Identity-based user accounts can be created with one of the following privileges: admin, secadmin, operator, or observer. Only users with secadmin privileges have access to configuration commands for FIPS, data encryption and secadmin account management. Secadmin users can login to the OM 5130 via SSH V2 and IPSec to the IP, via the Ethernet port, or through a PPP session with a direct connection to the shelf's serial port with SSH V2. For a detailed description of all user privileges for each access type, see *Planning and Applications Guide*, NTB26402.

The following sections describe the Maintenance role, Crypto Officer role, and User role.

Maintenance role

The only authorized physical maintenance actives are the replacement of S-DNMs and PSUs. The Crypto Officer must first zeroize the keys and passwords on the OM 5130 before these maintenance activities can be performed. After the S-DNM or PSU has been replaced, the Crypto Officer must re-apply new tamper evident seals, and re-configure the OM 5130 into FIPS mode.

To zeroize the keys and passwords use the following command described in the Zeroization section:

```
configure node commission state decommissioned
```

Crypto Officer role

A secadmin user assumes the Crypto Officer role. Crypto Officer services include the ability to:

— configure encryption on the client ports

— configure FIPS mode

— configure additional secadmin users

User role

The user role is a user with admin, operator or observer user privileges. The user role does not have Crypto Officer role privileges.

- **admin** - has access to all configure and show commands except the configuration commands for data encryption, FIPS provisioning and secadmin account management.
- **operator** - has access to all configure and show commands except configuration commands for FIPS provisioning, data encryption, security (including IPSec), commissioning, and backup, restore, and upgrade.
- **observer** - has access to show commands only. This privilege does not allow access to configuration commands.

Backups and restores

Backups are used to save configuration details. Backups and restores are not to be performed in FIPS mode for the OM 5130 to remain in a FIPS-compliant mode of operation.

Passwords

Passwords are used to authenticate the identity of the user. A password must be an alphanumeric string between 8 and 10 characters. When complex password validation is enabled, the following additional rules are enforced:

- Password must not be a repeat or the reverse of the associated user name.
- Password must not contain the same three characters used consecutively.
- Password must contain at least three of the following:

— one lower case alpha character

— one upper case alpha character

— one numeric character

— one special character

Supported special characters are: exclamation mark (!), single quote ('), pound sign (#), dollar sign ($), percentage sign (%), brackets (()), asterisk (*), plus (+), minus (-), period (.), slash(/), less than(<), equal to (=), greater than (>), at (@), square brackets ([]), circumflex accent (^), under score (_), curly brackets({}), pipe (|), tilde (~).

The following special characters are not allowed: comma (,), double quote ("), semi-colon (;), colon (:), ampersand (&), question mark (?), back-slash (\), space and all control characters.

There are 26 lower case plus 26 upper case plus 10 digits plus 24 special characters for a total of 86 characters. When complex password validation is enabled, if the minimum password length of 8 characters is used, the minimum combinations that are possible are:
10 x 24 x 26 x 26 x 86 x 86 x 85 x 86 - 2 = 8,771,466,662,398.
The odds of guessing a password are less than 1 in 8,771,466,662,398 and hence a brute force mechanism would take a significantly long time to succeed.

Passwords are hashed with SHA-256 and stored in the OM 5130's internal database. The hashed passwords can be zeroized. See Zeroization on page 4-5.

ATTENTION

FIPS mode of operation requires that you enable complex password validation. See *Administration and Provisioning Procedures* (323-1421-310) for user account procedures.

Configuring the OM 5130 to non-FIPS mode

The following command will place the OM 5130 in the non-FIPS operating mode:

```
configure security fips mode disabled
```

ATTENTION

During a FIPS mode to non-FIPS mode transition, the OM 5130 is restarted and the OM 5130 configuration (including the passwords) is deleted. Once the OM 5130 configuration is deleted, the OM 5130 is in a decommissioned state. All keys and CSPs are zeroized during a FIPS mode to non-FIPS mode transition, see Zeroization on page 4-5.

Displaying FIPS mode and state

The following command will display FIPS mode and state:

```
show security fips
```

If the OM 5130 is in FIPS approved mode, the command output will be:

```
Mode: FIPS Approved
```

FIPS error state

Recoverable Error State

An OM 5130 transitions to the Recoverable Error State when one of the following conditions are met:

- Failure of any of the following tests:
  - firmware load test
  - conditional S-DNM self-test
- The S-DNM or filler card was removed or inserted on the OM 5130 (requires a power cycle to recover)

Non-Recoverable Error State

An OM 5130 transitions to the Non-Recoverable Error state when one of the following conditions are met:

- Failure of any of the following tests:
  - OM 5130 power-on and boot time self-tests
  - Continuous Random Number Generator Test
  - alternating bypass test

While an OM 5130 is in an Non-Recoverable Error state:

- All the OM 5130 transport slots are powered down. As a result all data output via the data output interfaces on the OM 5130 is inhibited
- The OM 5130 is accessible over CLI only. All TCP/UDP ports except 21 (telnet) and 22 (SSH) are blocked.
- A log is generated to notify the user about the reason which caused the node to transition to the error state.

  Note: Do not attempt to do an upgrade if the OM 5130 is in the FIPS Error state. The OM 5130 cannot be considered as operating in a FIPS Approved mode of operation if an upgrade is performed while the OM 5130 is in the Error state.

Initialization of encryption keys

OM 5130 uses Advanced Encryption Standard (AES)-256 keys to encrypt client traffic over the WAN. Encryption keys are zeroized by any of the following actions, resulting in a loss of traffic:

- Disabling encryption for a client port. This action zeroizes the encryption key for the port.

- Decommissioning the system. This action zeroizes all encryption keys on the system.
- Restoring provisioning data. This action zeroizes all encryption keys on the system.
- Deprovisioning (deleting) the S-DNM. This action zeroizes all encryption keys on the S-DNM.
- Restarting the system or the S-DNM when there are expired encryption keys. This action zeroizes all expired keys on the system or S-DNM.

Note: Disabling the administrative state of a port does not initialize the encryption key of the port.

Zeroization

In FIPS mode, keys can be zeroized and passwords reset to default values through the command line interface (CLI) with a secure shell (SSH) connection and IPSec. Use a secadmin user privilege to zeroize the encryption keys.

Note: If you need to replace an S-DNM or power supply unit (PSU), the Crypto Officer must first zeroize the keys on the OM 5130. Once the keys have been zeroized, remove the seals on the S-DNM or PSU and replace the S-DNM or PSU using the replacement procedures in *Monitoring, Alarm Clearing and Module Replacement*, 323-1421-543. The Crypto Officer should re-apply new tamper-evident seals as needed according to section, Applying tamper-evident seals on page 2-1, and configure the OM 5130 into FIPS mode and then restart the OM 5130.

The following command will zeroize (overwritten with zeroes) AES secret keys and IPSec pre-shared keys:

```
configure encryption key zeroize enable
configure node restart
```

The following command will remove all configurations, zeroize all secret and private keys, re-initialize the seed key for the FIPS-approved RNG, restore userids and passwords to default values, release the OM 5130 from FIPS approved mode and restore the OM 5130 system to the default values before decommissioning or shipping for repair:

```
configure node commission state decommissioned
```

Finite State Model

In the FIPS mode the OM 5130 system can be in one of the following states:

- Crypto Officer Service state
- User Service state
- Bypass state

- Non-Recoverable Error state
- Recoverable Error state
- Power On state
- Power-up self tests state
- Crypto state
- Authentication state
- Authentication Lockout state
- Zeroize state
- Conditional tests state
- Physical Maintenance state
- Power Off state

Self-tests

The OM 5130 includes an array of self-tests that are run during startup (power-up tests) and periodically during operations (conditional tests). Power-up self-tests do not involve any inputs from or actions by the user. At any time, the operator is capable of commanding the OM 5130 to perform the power-up self-tests by performing a restart using the following command: `configure node restart.`

The cryptographic module is available to perform services only after successfully completing the power-up self-tests.

A passed self-test for the OM 5130 FIPS mode is shown by the successful booting up of the node or by viewing event messages listed in the logs. The failure of a self-test for the OM 5130 FIPS mode are also shown as event messages in the logs. See *Monitoring, Alarm Clearing, and Module Replacement*, 323-1421-543 for a complete listing of OM 5130 log events. Also, the S-DNM Green Operation status LED when ON indicates that the power-up self-tests passed and the OM 5130 is operational. See Table 1-5, “S-DNM status LEDs,” on page 10.

The power-up self-tests include firmware integrity tests, known answer tests (KATs) for the hardware implementation of AES, and KATs for the FIPS-approved algorithms implemented in firmware.

For the known answer test for the AES algorithm implementation in the FPGA, fixed and hard coded values are applied to the data input, key input and counter input of the Encryption/Decryption engines. The output is then compared against a hard coded 128 bit expected value and an alarm raised if the test fails.

If the power up test fails, then a test fail event will occur and the OM 5130 will be in a FIPS error state.

The following lists the Cryptographic known answer tests:

- Cryptographic Algorithm Tests:
  - AES encryption and decryption known answer tests for hardware implementation
  - HMAC-SHA-1 message authentication known answer test for firmware implementation
  - FIPS 186-2 DRNG known answer test for firmware implementation
  - SHA-1 hashing known answer test for firmware implementation
  - SHA-256 hashing known answer test for firmware implementation
  - SHA-512 hashing known answer test for firmware implementation
  - Triple-DES encryption and decryption known answer tests for firmware implementation
- Firmware Integrity Test
  - HMAC-SHA-1
- Conditional tests include:
  - FIPS 186-2 DRNG Continuous Random Number Generator Test
  - a firmware/FPGA load integrity test for FIPS-approved upgrades

    The firmware/FPGA load integrity test uses the HMAC-SHA-1 authentication algorithm.
  - the alternating bypass state test

    The bypass test checks that if a fully encrypted service is moved to a bypass service (by removing encryption from one client) that the remaining clients are still encrypted. It also checks that if a bypass service is moved to a fully cryptographic service that all clients are encrypted.

    The bypass state test runs if the encryption state is changed from enabled to disabled for any client port.

In addition to the self-tests required by the FIPS 140-2 specification the OM 5130 FIPS node firmware performs the All S-DNM self-test. During the All S-DNM self-test, the firmware verifies that for each slot the module type installed is an S-DNM or filler card and not a DNM card. This test is executed at node boot time.

Note: If any of the self-tests fail, the OM 5130 transitions into a FIPS error state. See FIPS error state on page 4-4 for more information.

Mitigation of other attacks

This section is not applicable. No claims are made that the OM 5130 mitigates against any other attacks than those covered by targeted FIPS 140-2 Security Levels for this validation.

Services and Cryptographic Key Management

Table 4-1 and Table 4-2 contain a listing of Optical Metro 5130 critical security parameters. For detailed service descriptions see *Planning Guide,* NTB26402.

Table 4-1
OM 5130 Services

Services	Description	Input	Output	Keys/CSPs and type of Access	Privilege level (Role)
Configure OM 5130	Defines network interfaces and settings, configures the client and WAN ports.	command & parameters	command response	Password — read — write IPSec pre-shared keys — read — write	admin (user)
Create admin users	Creates and deletes admin users.	command & parameters	command response	Password — read — write IPSec pre-shared keys — read — write	admin (user)
Create secadmin users	Creates and deletes secadmin users.	command & parameters	command response	Password — read — write IPSec pre-shared keys — read — write	secadmin (Crypto Officer)
Monitor status	Displays the OM 5130 configuration, alarms, logs and statistics.	command & parameters	command response	none	admin (user) secadmin (Crypto Officer)

Table 4-1
OM 5130 Services

Services	Description	Input	Output	Keys/CSPs and type of Access	Privilege level (Role)
Configure Encryption	Configures encryption, create pass phrase, generate keys.	command & parameters	command response	AES secret keys — read — write RNG seed key — read — write RNG seed — read — write	secadmin (Crypto Officer)
Packet FEC	Adds FEC to WAN packets.	packets without FEC on client ports	packets with FEC on WAN ports	none	admin (user)
Compression	Compresses outgoing WAN packets, uncompresses incoming WAN packets.	uncompressed packets on client ports	compressed packets on WAN ports	none	admin (user)
In-band management	Adds management packets on outgoing WAN ports.	none	management packets on WAN ports	HMAC-SHA-1 secret keys, Triple DES secret keys, AES secret keys; Diffie-Hellman public and private keys — read — write	admin (user)
WAN protection	Enables traffic redundancy on WAN ports.	command & parameters	command response	none	admin (user)
DNM equipment protection	Enables DNM redundancy.	command & parameters	command response	none	admin (user)
Execution of power-up self-tests	OM 5130 power up self-tests	none	none	none	none

Table 4-1
OM 5130 Services

Services	Description	Input	Output	Keys/CSPs and type of Access	Privilege level (Role)
Upgrade	Upgrades the OM 5130 to a newer firmware release.	upgrade command, ftp server IP address and password, firmware release file name	firmware is upgraded and old firmware is deleted	Password — read HMAC-SHA-1 secret key — read	admin (user)
Backup	Performs a backup of the OM 5130 configuration. Backup is not a FIPS-approved service.	backup command, ftp server IP address and password, back-up file name	OM 5130 configuration (excluding encryption keys) is stored on the ftp server	none	admin (user)
Restore	Performs a restore of the OM 5130 configuration from a previously saved backup. Restore is not a FIPS-approved service.	backup command, ftp server IP address and password, back-up file name	OM 5130 configuration is replaced by the backup file on ftp server. Encryption keys are zeroized.	none	admin (user)
IPSec	Manages the OM 5130 with IPSec.	command, username & password	status information	HMAC-SHA-1 secret keys, IPSec preshared keys, Triple DES secret keys, AES secret keys; and Diffie-Hellman public and private keys — read — write	admin (user) secadmin (Crypto Officer)
Ethernet login	Manages the OM 5130 with remote access to the Ethernet port.	command, username & password	status information	Password — read — write IPSec pre-shared keys — read — write	admin (user) secadmin (Crypto Officer)

Table 4-1
OM 5130 Services

Services	Description	Input	Output	Keys/CSPs and type of Access	Privilege level (Role)
USB login	Manages the OM 5130 with direct connection to the USB port.	command, username & password	status information	Password — read — write IPSec pre-shared keys — read — write	secadmin (Crypto Officer)
Serial port login	Manages the OM 5130 with direct connection to the Serial port via PPP.	command, username & password	status information	Password — read — write	admin (user) secadmin (Crypto Officer)
Zeroization	Zeorizes AES secret keys and IPSec pre-shared keys.	zeroization command	Zeroizes AES secret keys and IPSec pre-shared keys.	AES secret keys — write IPSec pre-shared keys — read — write	secadmin (Crypto Officer)
Decommission	Restores the OM 5130 to default factory settings.	decommission command	zeroizes all keys, restores userids and passwords to default, removes all other users, and removes all configurations	Password — read — write IPSec pre-shared keys — read — write AES secret keys — write HMAC-SHA-1 secret keys — write Diffie Hellman private keys — write Triple DES secret keys — write RNG seed key — write	admin (user) secadmin (Crypto Officer)
Note: The keys and CSPs can be zeroized using Zeroization on page 4-5.					

Table 4-2
Critical security parameters (CSP)

Critical Security Parameter	Length	Key Strength	Establishment Mechanism	State within OM 5130	Zeroized
AES secret keys	256 bits	256 bits	ED/EE - Transported to the OM 5130 encrypted with Triple DES. NA - Generated internally using FIPS 186-2 PRNG.	plain text	Overwritten with zeroes
Triple DES secret keys	168 bits	112 bits	ED/EE - Agreed upon using Diffie-Hellman and IKE.	ephemeral	Overwritten with zeroes
HMAC-SHA-1 Firmware Load Test key	128 bits	128 bits	NA - Hardcoded	plain text	NA
HMAC-SHA-1 secret keys	128 bits	128 bits	ED/EE - Agreed upon using Diffie-Hellman and IKE.	ephemeral	Overwritten with zeroes
HMAC-SHA1 secret key for integrity verification of firmware	128 bits	128 bits	NA - Hardcoded	plain text	NA
Diffie-Hellman private keys	2048 bits	112 bits	NA - Generated internally using FIPS 186-2 PRNG	plain text	Overwritten with zeroes
RNG seed key	64 bytes	-	NA - Generated internally using gathered entropy	ephemeral	Overwritten with new value
RNG seed	64 bytes	-	NA - Generated internally using gathered entropy	ephemeral	Overwritten with new value
IPSec pre-shared keys	16-150 characters	-	ED/EE - Transported to the OM 5130 encrypted with Triple DES.	plain text	Overwritten with zeroes

Table 4-2
Critical security parameters (CSP)

Critical Security Parameter	Length	Key Strength	Establishment Mechanism	State within OM 5130	Zeroized
Passwords	8-10 characters	-	ED/EE - Transported to the OM 5130 encrypted with Triple DES	hashed with SHA-256	Overwritten with hashed default values
Initial Basic Seed	128 bits	-	Time stamps collectedprior to passing them through SHA-1	ephemeral	Overwritten with new value
Note: The keys and CSPs can be zeroized using Zeroization on page 4-5.					

OM 5130 FIPS Approved Algorithms

This section lists the OM 5130 FIPS approved algorithms:

- 256-bit AES encryption and decryption in the CTR mode of operation - Algorithm Validation number 1462
- 3-key Triple-DES encryption and decryption in the CBC mode of operation as part of the IPSec protocol – Algorithm Validation number 986
- SHA-1, SHA-256, SHA-512 hashing - Algorithm Validation number 1324
- HMAC-SHA-1 message authentication in IPSec and for firmware integrity verification - Algorithm Validation number 859
- Regular FIPS 186-2 RNG with x-Change Notice or k-Change Notice - Algorithm Validation number 799

Non-FIPS Approved Algorithms

This section lists the OM 5130 non-FIPS approved algorithms:

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- DSA (key generation and signature generation and verification; non-compliant)
- OM 5130 Key-based scrambler for Backup and Restore
- MD5 hashing
- Blowfish
- DES
- AES for IPSec

Ciena

Optical Metro 5130 Security Policy

NTB26403
Standard Release 4.0 Issue 2.4
August 2011
Printed in Canada