Cisco Optical Networking Solution (ONS) 15454 Multiservice Transport Platforms (MSTPs) & NCS 2000 Series Security Policy

Hardware Versions: 15454-M6-SA=, 15454-M2-SA=, NCS2002-SA=, NCS2006-SA=, NCS2015-SA-DC=, 15454-M-WSE-K9, NCS2K-MR-MXP-LIC=, with FIPS Kit: CISCO-FIPS-KIT=

Firmware Version: 10.5

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Version 1.0

June 20, 2016

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Table of Contents

1 INTRODUCTION 1

1.1 PURPOSE 1
1.2 MODULE VALIDATION LEVEL 1
1.3 REFERENCES 1
1.4 TERMINOLOGY 1
1.5 DOCUMENT ORGANIZATION 2

2 CISCO OPTICAL NETWORKING SOLUTION (ONS) MODULE DESCRIPTION 3

2.1 ONS MULTISERVICE TRANSPORT PLATFORMS (15454-M6-SA=, 15454-M2-SA=, NCS2002-SA=, NCS2006-SA=, NCS2015-SA-DC=) 3
2.2 CONTROLLER CARDS (15454-M-TNC-K9, 15454-M-TSC-K9, 15454-M-TNCE-K9, 15454-M-TSCE-K9, NCS2K-TNCS-K9=, AND NCS2K-TNCS-O-K9=) 3
2.3 ENCRYPTION CARDS (15454-M-WSE-K9 AND NCS2K-MR-MXP-LIC=) 3
2.4 LINE CARD (15454-M-10X10G-LC, AND NCS2K-200G-CK-LIC=) 6
2.5 VALIDATED CONFIGURATION 6

3 CRYPTOGRAPHIC BOUNDARY 8

4 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES 8

5 ROLES, SERVICES AND AUTHENTICATION 9

5.1.1 User Services 10
5.1.2 Crypto Officer Services 10
5.2 UNAUTHENTICATED SERVICES 11
5.3 CRYPTOGRAPHIC KEY/CSP MANAGEMENT 11
5.4 CRYPTOGRAPHIC ALGORITHMS 13
5.4.1 Approved Cryptographic Algorithms 13
5.4.2 Non-FIPS Approved Algorithms Allowed in FIPS Mode 15
5.4.3 Non-FIPS Approved Algorithms 15
5.5 SELF-TESTS 15
5.5.1 Power On Self-Tests (POSTs) 15
5.5.2 Conditional Tests 16
5.6 PHYSICAL SECURITY 16

6 SECURE OPERATION 37

6.1 INITIAL SETUP 37
6.2 SYSTEM INITIALIZATION AND CONFIGURATION 37
6.3 HTTPS MANAGEMENT REQUIREMENTS AND CRYPTOGRAPHIC ALGORITHMS 37
6.4 SSHV2 MANAGEMENT REQUIREMENTS AND CRYPTOGRAPHIC ALGORITHMS 37

7 RELATED DOCUMENTATION 37

8 OBTAINING DOCUMENTATION 38

8.1 CISCO.COM 38
8.2 PRODUCT DOCUMENTATION DVD 38

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

8.3 ORDERING DOCUMENTATION 38
9 DOCUMENTATION FEEDBACK 39
10 CISCO PRODUCT SECURITY OVERVIEW 39
10.1 REPORTING SECURITY PROBLEMS IN CISCO PRODUCTS 39
11 OBTAINING TECHNICAL ASSISTANCE 40
11.1 CISCO TECHNICAL SUPPORT & DOCUMENTATION WEBSITE 40
11.2 SUBMITTING A SERVICE REQUEST 40
11.3 DEFINITIONS OF SERVICE REQUEST SEVERITY 41
12 OBTAINING ADDITIONAL PUBLICATIONS AND INFORMATION 41

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1 Introduction

1.1 Purpose

This is the non-proprietary Cryptographic Module Security Policy for the Cisco Optical Networking Solution (ONS) 15454 Multiservice Transport Platforms (MSTPs) & NCS 2000 Series Security Policy (Firmware Version: 10.5). This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 2 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

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/index.html.

1.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**2**

Table 1: **Module Validation Level**

1.3 References

This document deals only with the capabilities and operations of the Cisco Optical Networking Solution (ONS) in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the FIPS modules may be referred to as the module, ONS, or by any of the individual component names listed below.

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1.5 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

Vendor Evidence document
Finite State Machine
Other supporting documentation as additional references

This document provides an overview of the module and explains the secure configuration and operation. This introduction section is followed by Section 2, which details the general features and functionality of the module. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2 Cisco Optical Networking Solution (ONS) Module Description

2.1 ONS Multiservice Transport Platforms (15454-M6-SA=, 15454-M2-SA=, NCS2002-SA=, NCS2006-SA=, NCS2015-SA-DC=)

The Cisco ONS 15454 Multiservice Transport Platforms (MSTPs) and NCS 2000 Series provide capital and operational efficiency by addressing the increasing demand for multiple services, greater transport capacity, networking flexibility, multiple distance options, and management simplicity in a single platform. With innovative technology, Cisco ONS systems introduce intelligence to Dense Wavelength Division Multiplexing (DWDM) transmission, thus allowing the optimization of next-generation networks across multiple layers and removing costly Optical-Electrical-Optical (OEO) devices for network segmentation or regeneration.

The Cisco ONS systems provide features such as multilayer graphical network, node, and card visibility; comprehensive network-based service provisioning; and graphical software wizards to simplify and speed user operations for such tasks as initial network turn-up, service provisioning, and network, node, and bandwidth upgrades. The Cisco ONS systems use the embedded software architecture and control plane to introduce a level of operational simplicity exceptional in DWDM networks.

The Cisco ONS systems deliver a comprehensive set of features, allowing customers worldwide to support the requirements of next-generation transport networks.

2.2 Controller Cards (15454-M-TNC-K9, 15454-M-TSC-K9, 15454-M-TNCE-K9, 15454-M-TSCE-K9, NCS2K-TNCS-K9=, and NCS2K-TNCS-O-K9=)

The Cisco Transport Node Controller (TNC) and Transport Shelf Controller (TSC) and the enhanced versions (TNCE and TSCE, respectively) are next-generation system processors for the Cisco ONS systems. The Cisco controller cards perform system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection and resolution, SONET and SDH data-communications-channel (DCC) termination, system DC input-voltage monitoring, and system fault detection, and they support multishelf connections. The TNC and TNCE cards also have two optical service channels that support a supervisory data channel (SDC), distribution of synchronous clocking, and a 100-Mbps user data channel (UDC). The enhanced versions, TNCE and TSCE, support the IEEE1588v2 Precision Timing Protocol (PTP) and time of day (ToD) with pulse per second (PPS), in addition to support for Synchronous Ethernet (SyncE)/Source Specific Multicast (SSM) and traditional Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) Building Integrated Timing Supply (BITS) timing, which the TNC and TSC also support.

2.3 Encryption Cards (15454-M-WSE-K9 and NCS2K-MR-MXP-LIC=)

The Cisco ONS Optical Encryption Cards brings secure transport capability to the ONS systems product family by providing data confidentiality and data integrity over a fiber optic communication channel through the combination of Cryptography and Trusted Product Architecture. Each SFP+ (enhanced small form-factor pluggable) port can accept gray or DWDM pluggable optics, with trunk ports supporting G.709 Digital Wrapper for carrier class OAM, plus Forward Error Correction (FEC) for longer reach. The single slot cards are

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

compatible with the ONS 15454 MSTP M6 and M2 chassis, allowing up to 30 encrypted 10G streams in a 6RU footprint.

The following pictures are representative each of the modules hardware model:

Figure 1: Cisco 15454-M2-SA

Figure 2: Cisco 15454-M6-SA

Figure 3: Cisco NCS2002-SA

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 4: Cisco NCS2006-SA

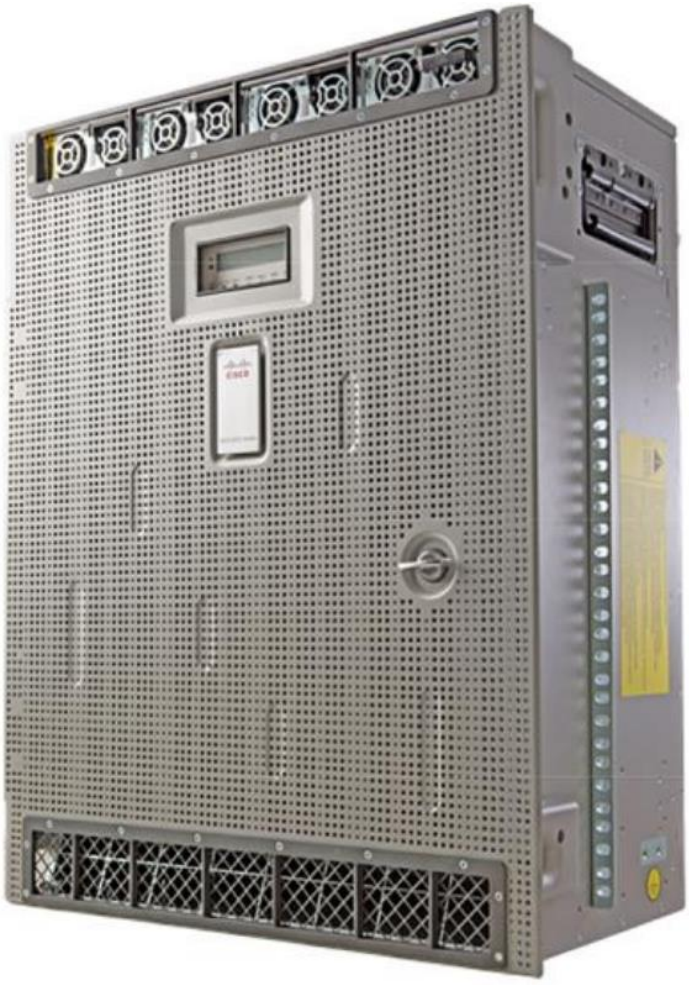


Figure 5: Cisco NCS2015-SA

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.4 Line Cards (15454-M-10X10G-LC, and NCS2K-200G-CK-LIC=)

Cisco® ONS systems support both the Cisco ONS 15454 10-Port 10 Gbps Line Card and the NCS2K 200 Gbps Line card, which simplifies the integration and transport of interfaces and services into enterprise or service provider optical networks.

2.5 Validated configuration

The validated platforms consist of the following components:

- Chassis:
  - 15454-M2-SA=
  - 15454-M6-SA=
  - NCS2002-SA=
  - NCS2006-SA=
  - NCS2015-SA=
- Controller Cards:
  - 15454-M-TNC-K9
  - 15454-M-TSC-K9
  - 15454-M-TNCE-K9
  - 15454-M-TSCE-K9
  - NCS2K-TNCS-O-K9
  - NCS2K-TNCS-K9 (only supported on the NCS2015 chassis)
- Encryption Cards:
  - 15454-M-WSE-K9
  - NCS2K-MR-MXP-LIC=
- Line Cards:
  - 15454-M-10X10G-LC
  - NCS2K-200G-CK-LIC=
- FIPS Kit:
  - CISCO-FIPS-KIT=
- Pluggable Optics used with Encryption Cards:
  - ONS-SC+-10G-SR=
  - CPAK-100G-SR10=
  - QSFP-4x10G-LR-S=
  - ONS-QSFP-40G-SR4=

The switches included as part of the FIPS validation may be configured in the following configurations:

Chassis	Controller Card(s)	Encryption Card(s)	Line Card(s)
15454-M2-SA	**Single** 15454-M-TNC-K9	**Up to two (2)** 15454-M-WSE-K9	
	Single 15454-M-TSC-K9	**Up to two (2)** NCS2K-MR-MXP-LIC=	
	Single 15454-M-TNCE-K9	**Up to two (2)** 15454-M-WSE-K9	

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Chassis	Controller Card(s)	Encryption Card(s)	Line Card(s)
	Single 15454-M-TSCE-K9	**Up to two (2)** NCS2K-MR-MXP-LIC=	
	Single 15454-M-TNC-K9		**Single** 15454-M-10X10G-LC
	Single 15454-M-TSC-K9		**Single** NCS2K-200G-CK-LIC=
	Single 15454-M-TNCE-K9		**Single** 15454-M-10X10G-LC
	Single 15454-M-TSCE-K9		**Single** NCS2K-200G-CK-LIC=
15454-M6-SA	**Single** 15454-M-TNC-K9	**Up to six (6)** 15454-M-WSE-K9	
	Single 15454-M-TSC-K9	**Up to six (6)** 15454-M-WSE-K9	
	Single 15454-M-TNCE-K9	**Up to six (6)** 15454-M-WSE-K9	
	Single 15454-M-TSCE-K9	**Up to six (6)** 15454-M-WSE-K9	
	Dual 15454-M-TNC-K9	**Up to six (6)** 15454-M-WSE-K9	
	Dual 15454-M-TSC-K9	**Up to six (6)** 15454-M-WSE-K9	
	Dual 15454-M-TNCE-K9	**Up to six (6)** 15454-M-WSE-K9	
	Dual 15454-M-TSCE-K9	**Up to six (6)** 15454-M-WSE-K9	
	Single 15454-M-TNC-K9		**Single** 10X10G-LC
	Single 15454-M-TSC-K9		**Single** 10X10G-LC
	Single 15454-M-TNCE-K9		**Single** 10X10G-LC
	Single 15454-M-TSCE-K9		**Single** 10X10G-LC
NCS2002-SA=	**Single** NCS2K-TNCS-O-K9	**Up to two (2)** 15454-M-WSE-K9	
	Single NCS2K-TNCS-O-K9	**Up to two (2)** NCS2K-MR-MXP-LIC=	
	Single NCS2K-TNCS-O-K9		**Single** 15454-M-10X10G-LC
	Single NCS2K-TNCS-O-K9		**Single** NCS2K-200G-CK-LIC=
NCS2006-SA=	**Single** NCS2K-TNCS-O-K9	**Up to six (6)** 15454-M-WSE-K9	
	Single NCS2K-TNCS-O-K9	**Up to six (6)** NCS2K-MR-MXP-LIC=	
	Dual NCS2K-TNCS-O-K9	**Up to six (6)** 15454-M-WSE-K9	
	Dual NCS2K-TNCS-O-K9	**Up to six (6)** NCS2K-MR-MXP-LIC=	
	Single NCS2K-TNCS-O-K9		**Single** 15454-M-10X10G-LC

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Chassis	Controller Card(s)	Encryption Card(s)	Line Card(s)
	Single NCS2K-TNCS-O-K9		**Single** NCS2K-200G-CK-LIC=
NCS2015-SA=	**Single** NCS2K-TNCS-O-K9	**Up to fifteen (15)** 15454-M-WSE-K9	
	Single NCS2K-TNCS-O-K9	**Up to fifteen (15)** NCS2K-MR-MXP-LIC=	
	Dual NCS2K-TNCS-O-K9	**Up to fifteen (15)** 15454-M-WSE-K9	
	Dual NCS2K-TNCS-O-K9	**Up to fifteen (15)** NCS2K-MR-MXP-LIC=	
	Single NCS2K-TNCS-K9	**Up to fifteen (15)** 15454-M-WSE-K9	
	Single NCS2K-TNCS-K9	**Up to fifteen (15)** NCS2K-MR-MXP-LIC=	
	Dual NCS2K-TNCS-K9	**Up to fifteen (15)** 15454-M-WSE-K9	
	Dual NCS2K-TNCS-K9	**Up to fifteen (15)** NCS2K-MR-MXP-LIC=	
	Single NCS2K-TNCS-O-K9		**Single** 15454-M-10X10G-LC
	Single NCS2K-TNCS-O-K9		**Single** NCS2K-200G-CK-LIC=
	Single NCS2K-TNCS-K9		**Single** 15454-M-10X10G-LC
	Single NCS2K-TNCS-K9		**Single** NCS2K-200G-CK-LIC=

Table 2: Module Configurations

3 Cryptographic Boundary

The cryptographic boundary is defined as being the physical enclosure of the chassis.

All of the functionality described in this publication is provided by components within this cryptographic boundary. The module can incorporate up to one or two controller cards (depending on chassis used), and up to six (6) encryption cards (depending on the chassis used) or one line card in a single configuration, detailed in Table 2 above.

4 Cryptographic Module Ports and Interfaces

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The module provides no power to external devices and takes in its power through normal power input/cord. The following table lists all possible logical/physical interface configurations.

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Physical Interfaces	FIPS 140-2 Logical Interfaces
Encryption Card: • SFP+ ports (NCS2K-MR-MXP-LIC – 2, 15454-M-WSE-K9 – 10) Controller Card: • RJ-45 Ethernet Port • Up to two SFP (small form-factor pluggable) ports Line Card: • SFP+ ports (10) • 100-Gbps Channel Express (CXP)(1)	Data Input Interface
Encryption Card: • SFP+ ports (NCS2K-MR-MXP-LIC – 2, 15454-M-WSE-K9 – 10) Controller Card: • RJ-45 Ethernet Port • Up to two SFP ports Line Card: • SFP+ ports (10) • 100-Gbps Channel Express (CXP)(1)	Data Output Interface
Controller Card: • RJ-45 Ethernet Port • Up to two SFP ports • BITS port	Control Input Interface
Encryption Card: • SFP+ ports (NCS2K-MR-MXP-LIC – 2, 15454-M-WSE-K9 – 10) • LED Controller Card: • RJ-45 Ethernet Port • Up to two SFP ports LED	Status Output Interface

Table 3: Cisco ONS Interfaces

Notes:

1. The M2 platform includes a single USB port disabled by TEL.

2. The RS232 port (on each Controller Card) that was protected by the front cover of each chassis should not be used while in FIPS mode.

5 Roles, Services and Authentication

The cryptographic module supports role-based authentication. There are two roles in the Switch that may be assumed the Crypto Officer (CO) role and the User role. The administrator of the module assumes the Crypto Officer role and associated services in order to configure and maintain ONS, while the Users exercise only the basic User services. A complete description of all the management and configuration capabilities of the module can be found in the Cisco ONS 15454 DWDM Reference Manual, http://www.cisco.com/en/US/docs/optical/15000r9_2/dwdm/reference/guide/454d92_ref.html.

All CO/User passwords must be 8 characters up to 25 characters with a minimum of one letter and one number. If six (6) integers, one (1) special character and one (1) alphabet are used

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 251,595,800 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 10 x 9 x 8 x 7 x 6 x 5 x 32 x 52). In order to successfully guess the sequence in one minute would require the ability to make over 4,193,280 guesses per second, which far exceeds the operational capabilities of the module. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

5.1.1 User Services

Users enter the system via an HTTPS or SSHv2 connection.

The services available to the User role consist of the following:

Services and Access	Description	Keys and CSPs
Status Functions (r)	View state of node and connection and version of software currently running.	N/A
Network Functions (r,w)	Connect to other nodes and initiate diagnostic network services (i.e., ping, mtrace).	N/A
Terminal Functions (r)	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	N/A
Perform Self-Tests (r)	Perform the FIPS 140 start-up tests on demand	N/A

Table 4: User Role Services (r = read w = write)

5.1.2 Crypto Officer Services

During initial configuration of the module, the Crypto Officer password is defined. A Crypto Officer can assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration of the module.

The Crypto Officer services consist of the following:

Services and Access	Description	Keys and CSPs
Configure the module (r,w)	Define network interfaces and settings, enable interfaces and network services, set system date and time, and load authentication information.	User passwords
Define Rules and Filters (r,w,d)	Create packet Filters that are applied to User data streams for each node.	User password
View Status Functions (r)	View the module configuration, active sessions, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	User password
Manage the Module (r,w,d)	Log off users, shutdown or reload the module, erase the memory, view complete configurations, manager user rights, perform firmware update, and restore configurations.	User password
Optical TLS Encryption (using TLS1.2) (r,w,d)	Configure Optical TLS Encryption parameters, provide entry and output of CSPs.	TLS pre-master secret, TLS Traffic Keys
SSHv2 (r,w,d)	Configure SSHv2 connection.	Optical TLS server private key, Optical TLS pre-master secret, RFC 5705 Key Expansion Optical Master Secret, Optical TLS Encryption Key #1, Optical TLS Encryption Key #2, Optical TLS Encryption Key #3

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Services and Access	Description	Keys and CSPs
HTTPS (r,w,d)	Configure HTTPS connection	HTTPS TLS server private key, HTTPS TLS pre-master secret, HTTPS TLS Encryption Key, HTTPS TLS Integrity Key
Self-Tests (r)	Execute the FIPS 140 start-up tests on demand	N/A
User services. (r,w,d)	The Crypto Officer has access to all User services.	User password

Table 5: Crypto Officer Services (r = read w = write d = delete)

5.2 Unauthenticated Services

The services available to unauthenticated users are:

- Viewing the status output from the module's LEDs
- Powering the module on and off using the power switch

5.3 Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. All zeroization consists of overwriting the memory that stored the key.

The module is in the approved mode of operation only when FIPS 140-2 approved algorithms are used (except DH and RSA key transport which are allowed in the approved mode for key establishment despite being non-approved).

All Diffie-Hellman (DH)/ECDH keys agreed upon for individual tunnels are directly associated with that specific connection. RSA Public keys are entered into the modules using digital certificates which contain relevant data such as the name of the public key's owner, which associates the key with the correct entity. All other keys are associated with the user/role that entered them.

The module supports the following keys and critical security parameters (CSPs).

Key/CSP Name	Algorithm	Description	Storage Location	Zeroization Method
DRBG entropy input	SP 800-90A CTR_DRBG	This is the entropy for SP 800-90A.	SDRAM	power cycle the device
DRBG seed	SP 800-90A CTR_DRBG	This is the seed for SP 800-90A.	SDRAM	power cycle the device
DRBG V	SP 800-90A CTR_DRBG	Internal V value used as part of SP 800-90ACTR_DRBG	SDRAM	power cycle the device
DRBG key	SP 800-90A CTR_DRBG	Internal Key value used as part of SP 800-90A CTR_DRBG	SDRAM	power cycle the device
Diffie-Hellman private key	Diffie-Hellman (224 - 379 bits)	The private exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	SDRAM	Automatically after shared secret generated.
Diffie-Hellman public key	Diffie-Hellman (2048-4096 bits)	The public exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	SDRAM	Automatically after shared secret generated.
Diffie-Hellman shared secret	Diffie-Hellman (2048-4096 bits)	The shared secret used in Diffie-Hellman (DH) exchange. Zeroized after DH key agreement.	SDRAM	Automatically after key agreement.

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Key/CSP Name	Algorithm	Description	Storage Location	Zeroization Method
EC Diffie-Hellman private key	Elliptic Curve Diffie-Hellman (P-256, P-384 and P-521)	The private exponent used in Elliptic Curve Diffie-Hellman (ECDH) exchange.	SDRAM	Automatically after shared secret generated.
EC Diffie-Hellman public key	Elliptic Curve Diffie-Hellman (P-256, P-384 and P-521)	The public exponent used in Elliptic Curve Diffie-Hellman (ECDH) exchange.	SDRAM	Automatically after shared secret generated.
EC Diffie-Hellman shared secret	Elliptic Curve Diffie-Hellman (P-256, P-384 and P-521)	The shared secret in Elliptic Curve Diffie-Hellman (ECDH) exchange. Zeroized after ECDH key agreement.	SDRAM	Automatically after key agreement.
SSHv2 server private key	RSA (2048 bits)	2048 bit RSA private key used for SSHv2.	NVRAM	Deleted via the GUI interface
SSHv2 server public key	RSA (2048 bits)	2048 bit RSA p key used for SSHv2.	SDRAM	Automatically when SSH session terminated
SSHv2 session keys	Triple-DES (168 bits), AES (128/192/256 bits)	This is the SSH v2session key. It is zeroized when the SSH session is terminated.	SDRAM	Automatically when SSH session terminated
HTTPS TLS server private key	RSA (2048 bits)	2048 bit RSA private key used for SSLV3.1/TLS.	NVRAM	Deleted via the GUI interface
HTTPS TLS server public key	RSA (2048 bits)	2048 bit RSA public key used for SSLV3.1/TLS.	SDRAM	Automatically when TLS session is terminated
HTTPS TLS pre-master secret	Shared Secret	Shared Secret created using asymmetric cryptography from which new TLS session keys can be created	SDRAM	Automatically when TLS session is terminated
HTTPS TLS session keys	Triple-DES (168 bits), AES (128/192/256 bits)	Key used to encrypt TLS session data	SDRAM	Automatically when TLS session is terminated
Optical TLS server private key	RSA (2048 bits)	2048 bits RSA private key used for Optical TLS.	NVRAM	Deleted via the GUI interface
Optical TLS server public key	RSA (2048 bits)	2048 bit RSA public key used for Optical TLS.	SDRAM	Automatically when TLS session is terminated
Optical TLS pre-master secret	Shared Secret	Shared Secret created using asymmetric cryptography from which new TLS session keys can be created	SDRAM	Automatically when TLS session is terminated
Optical TLS key expansion master key	Shared Secret	Optical key extracted using RFC 5705 TLS Key Extractor. Used to derive client/server keys.	SDRAM	Automatically when TLS session is terminated
Optical TLS client key	AES (256 bits)	Optical traffic key derived via NIST SP 800-108 Key Derivation.	SDRAM	Automatically when TLS session is terminated
Optical TLS session key	AES (256 bits)	Optical traffic key derived via NIST SP 800-108 Key Derivation.	SDRAM	Automatically when TLS session is terminated
User password	Shared Secret	The password of the User role. 8-25 characters long, including at least one letter and at least one number character. This password is zeroized by overwriting it with a new password.	NVRAM	Overwrite with new password
CO password	Shared Secret	The password of the CO role. 8-25 characters long, including at least one letter and at least one number character. This password is zeroized by overwriting it with a new password.	NVRAM	Overwrite with new password

Table 6: CSP Table

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

5.4 Cryptographic Algorithms

The module is in the approved mode of operation only when FIPS 140-2 approved algorithms are used (except DH and RSA key transport which are allowed in the approved mode for key establishment despite being non-approved). The module implements a variety of approved and non-approved algorithms.

5.4.1 Approved Cryptographic Algorithms

The module supports the following FIPS 140-2 approved algorithm implementations:

	ONS Controller Card Implementation	ONS Encryption Card Implementation	15454 Series FPGA Implementation	NCS2K Series FPGA Implementation
AES	#3771 ECB (e/d; 128, 192, 256); CBC (e/d; 128, 192, 256); CTR (i/e; 128, 192, 256)	#3770 ECB (e/d; 128, 192, 256); CTR (i/e; 128, 192, 256)	#2352 ECB (e/d; 256) #2369 GCM (KS: AES_256(e/d) Tag Length(s): 128) AAD Lengths tested: (256, 1024); IV Lengths Tested: (8, 1024); 96BitIV_Supported; OtherIVLen_Supported GMAC_Supported XTS(KS: XTS_256((e/d) (f)) Note: While implemented XTS is not used by the module	#2769 ECB (e/d; 256) #2770 GCM (KS: AES_256(e/d) Tag Length(s): 128) AAD Lengths tested: (896, 1024); IV Lengths Tested: (8, 1024); 96BitIV_Supported GMAC_Supported AES XTS(KS: XTS_256((e/d) (f)) Note: While implemented XTS is not used by the module
Triple-DES	2098 TECB(KO 2 d only)	N/A	N/A	N/A
SHS	3141 SHA-1 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	3140 SHA-1 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	N/A	N/A
HMAC	2471 HMAC-SHA1 (Key Sizes: KS<BS KS=BS KS>BS) HMAC-SHA256 (Key Size: KS<BS KS=BS KS>BS) HMAC-SHA384 (Key Size: KS<BS KS=BS KS>BS) HMAC-SHA512 (Key Size: KS<BS KS=BS KS>BS)	2470 HMAC-SHA1 (Key Sizes: KS<BS KS=BS KS>BS) HMAC-SHA256 (Key Size: KS<BS KS=BS KS>BS) HMAC-SHA384 (Key Size: KS<BS KS=BS KS>BS) HMAC-SHA512 (Key Size: KS<BS KS=BS KS>BS)	N/A	N/A
RSA	1941 FIPS186-4: 186-4KEY(gen): FIPS186-4_Fixed_e (10001);	1940 FIPS186-4:	N/A	N/A

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

	PGM(ProvPrimeConditio n) (2048 SHA(256)) (3072 SHA(256)) ALG[ANSIX9.31] Sig(Gen): (2048 SHA(256)) Sig(Ver): (1024 SHA(1, 256)) (2048 SHA(1, 256)) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(256)) (3072 SHA(256)) SIG(Ver) (1024 SHA(1, 256)) (2048 SHA(1, 256)) (3072 SHA(1, 256))	186-4KEY(gen): FIPS186-4_Fixed_e (10001); PGM(ProvPrimeConditi on) (2048 SHA(256)) (3072 SHA(256)) ALG[ANSIX9.31] Sig(Gen): (2048 SHA(256, 384, 512)) (3072 SHA(256, 384, 512)) Sig(Ver): (1024 SHA(1, 256, 384, 512)) (2048 SHA(1, 256, 384, 512)) (3072 SHA(1, 256, 384, 512)) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(256)) SIG(Ver) (1024 SHA(1, 256)) (2048 SHA(1, 256))		
DRBG	1041 Hash_Based DRBG: [Prediction Resistance Tested: Enabled (SHA-1, SHA-256, SHA-384, SHA-512)] HMAC_Based DRBG: [Prediction Resistance Tested: Enabled (SHA-1, SHA-256, SHA-384, SHA-512)] CTR_DRBG: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128, AES-192, AES-256)	1040 CTR_DRBG: [Prediction Resistance Tested: Enabled; BlockCipher_No_df: (AES-128, AES-192, AES-256)]	N/A	N/A
CVL	316 TLS(TLS1.0/1.1) SSH (SHA 1, 256)	317 TLS(TLS1.0/1.1)	N/A	N/A
SP 800-108 KDF	N/A	79 CTR_Mode: (Llength(Min8 Max48) MACSupported([HMAC SHA1] [HMACSHA224] [HMACSHA256] [HMACSHA384] [HMACSHA512]) LocationCounter([After FixedData]) rlength([8]))	N/A	N/A

Table 7: FIPS Algorithm Certificates

Caveat: The TLS protocol (for which its KDF was implemented as per NIST SP 800-135 rev1 and validated by the CAVP with CVL certificate numbers #316 and #317. The TLS protocol has

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

not been reviewed or tested by the CAVP and CMVP.

Note: The module use of AES GCM complies with the Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations defined in SP 800-52.

5.4.2 Non-FIPS Approved Algorithms Allowed in FIPS Mode

The following key establishments despite being non-approved are available:

- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- Elliptic Curve Diffie-Hellman (key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- NDRNG

5.4.3 Non-FIPS Approved Algorithms

Cisco Optical Networking Solution (ONS) cryptographic module implements the following non-Approved algorithms are not permitted for use in the FIPS 140-2 mode of operations:

- MD5
- DES,
- HMAC-MD5
- RC4

5.5 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The module includes an array of self-tests that are run during startup and periodically during operations. In the error state, all secure data transmission is halted and the module outputs status information indicating the failure.

5.5.1 Power On Self-Tests (POSTs)

- Encryption Card Firmware Known Answer Tests (KATs)
    - AES (encrypt/decrypt) KATs
    - DRBG KAT
    - HMAC (HMAC-SHA-1/256/512) KATs
    - RSA KAT

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

- Controller Card Firmware KATs
  - AES (encrypt/decrypt) KATs
  - DRBG KAT
  - HMAC (HMAC-SHA-1/256/512) KATs
  - RSA KAT
  - Triple-DES (encrypt/decrypt) KATs

- Hardware (FPGA) KATs
  - AES-GCM KAT
  - AES-XTS KAT

- Firmware Integrity Test (32-bit CRC)

5.5.2 Conditional Tests

- Encryption Card Firmware conditional tests
  - Continuous random number generation test for approved DRBG
  - Continuous random number generation test for non-approved NDRNG
  - Pair-Wise Consistency Test for RSA

- Controller Card Firmware conditional tests
  - Continuous random number generation test for approved DRBG
  - Continuous random number generation test for non-approved NDRNG
  - Pair-Wise Consistency Test for RSA

- Firmware Load Test

5.6 Physical Security

The module is entirely encased by a metal, opaque case. The module natively meets the FIPS 140-2 opacity requirements. However, tamper evident labels are required to meeting the FIPS 140-2 tamper evidence requirements.

Once the module has been configured to meet FIPS 140-2 Level 2 requirements, the module cannot be accessed without signs of tampering. Any attempt to open ONS will damage the tamper evidence seals or the material of the module cover. Tamper evidence seals can be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices. The word “OPEN” will appear if the label was peeled back.

All Critical Security Parameters are stored and protected within each module's tamper evident enclosure. The Crypto Officer is responsible for properly placing all tamper evident labels. The FIPS kit includes 15 of the seals. Please be aware that the extra tamper evident labels/seals shall be securely stored by the Crypto Officer. These security labels are very fragile and cannot be removed without clear signs of damage to the labels. The Crypto-Officer should inspect the seals for evidence of tamper as determined by their deployment policies (every 30 days is recommended). If the seals show evidence of tamper, the Crypto-Officer should assume that the modules have been compromised and contact Cisco.

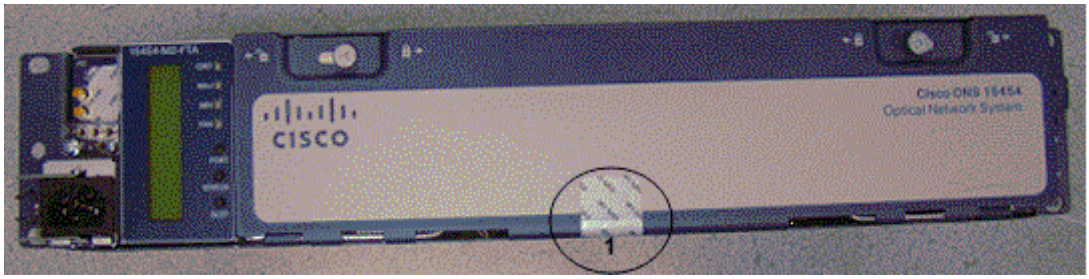
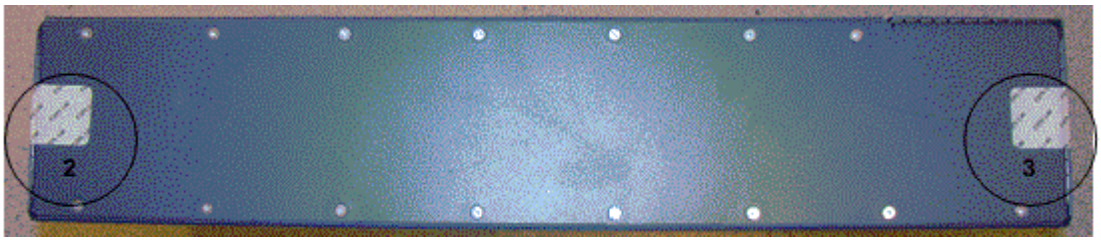
© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

The module shall require the following number of labels, part number CISCO-FIPS-KIT= to be affixed:

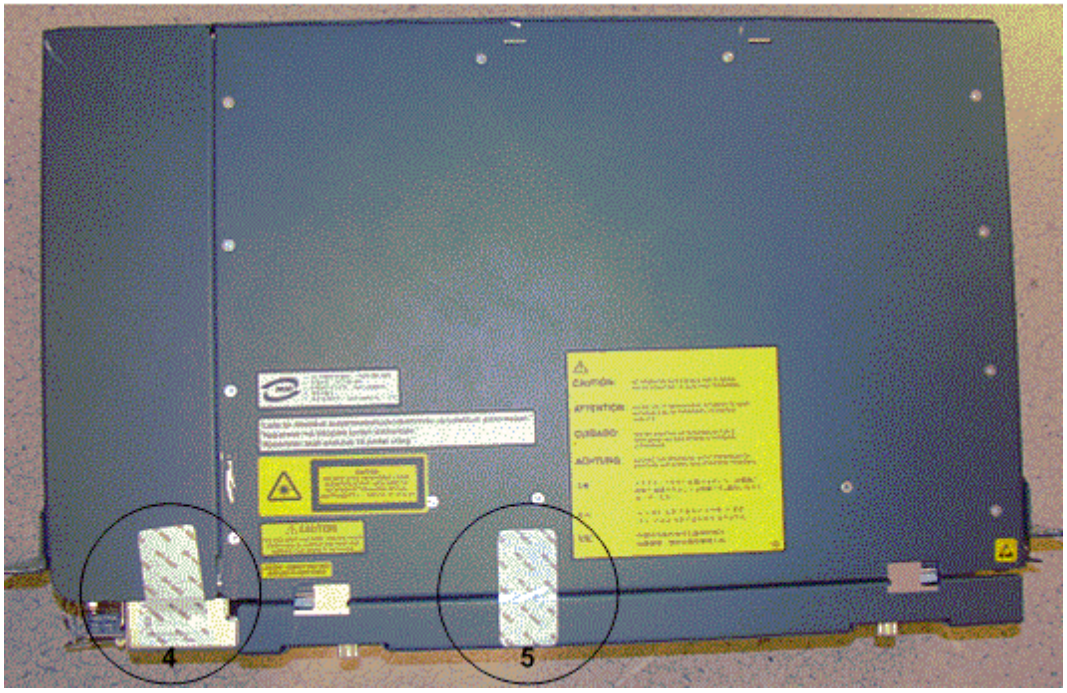
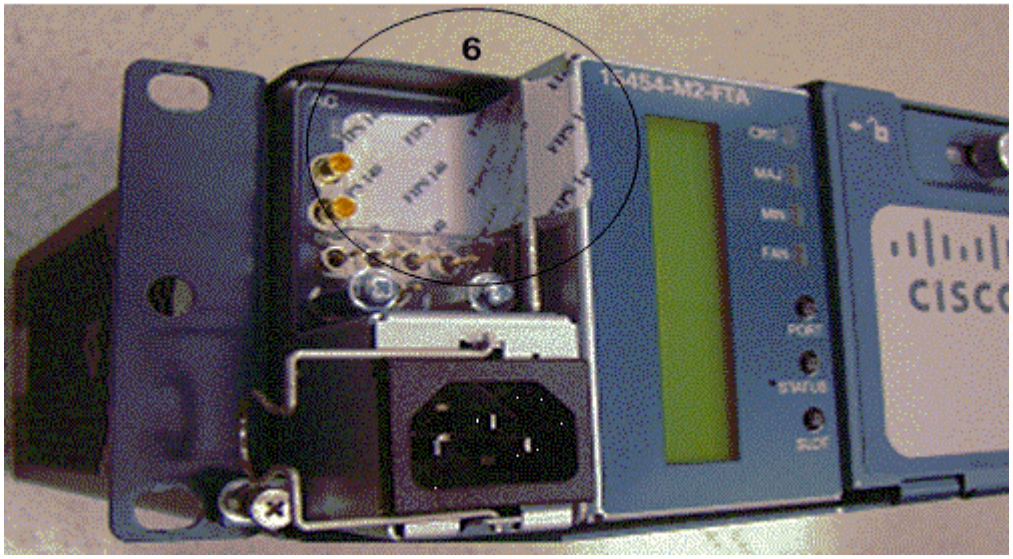
- Cisco 15454-M2-SA : 6 Tamper Evidence Labels
- Cisco 15454-M6-SA : 5 Tamper Evidence Labels
- Cisco NCS2002-SA= : 11 Tamper Evidence Labels
- Cisco NCS2006-SA= : 7 Tamper Evidence Labels
- Cisco NCS2015-SA-DC= : 7 Tamper Evidence Labels

The Tamper evident labels must be applied as shown in the pictures below, for the module to operate in FIPS mode. Prior to applying the seals the system surface must be cleaned with a mild detergent and dried. Then the seals can be applied.

View	M2 – TEL Placement and Numbering
Front	
Back	

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	M2 – TEL Placement and Numbering
Top	
USB Cover	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

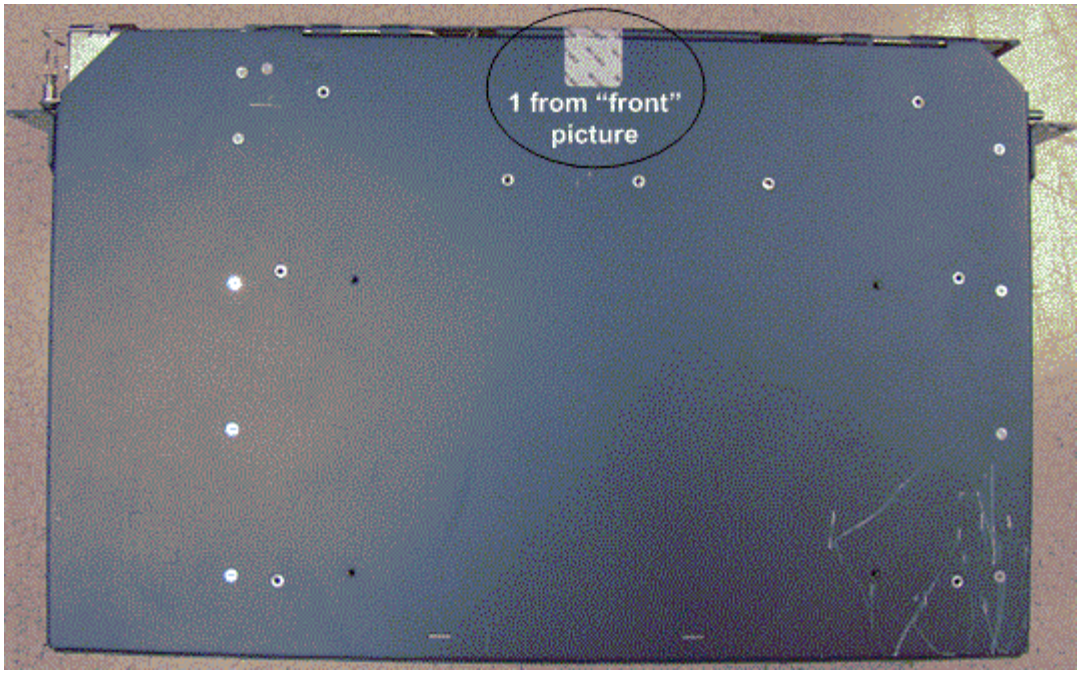
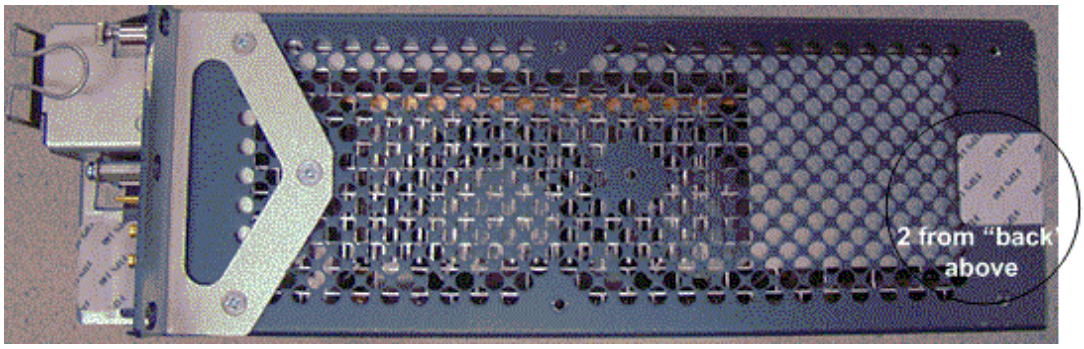
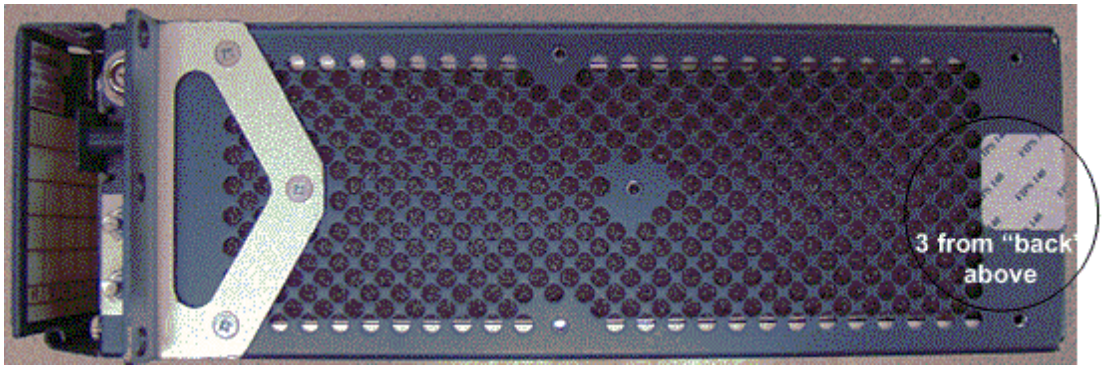
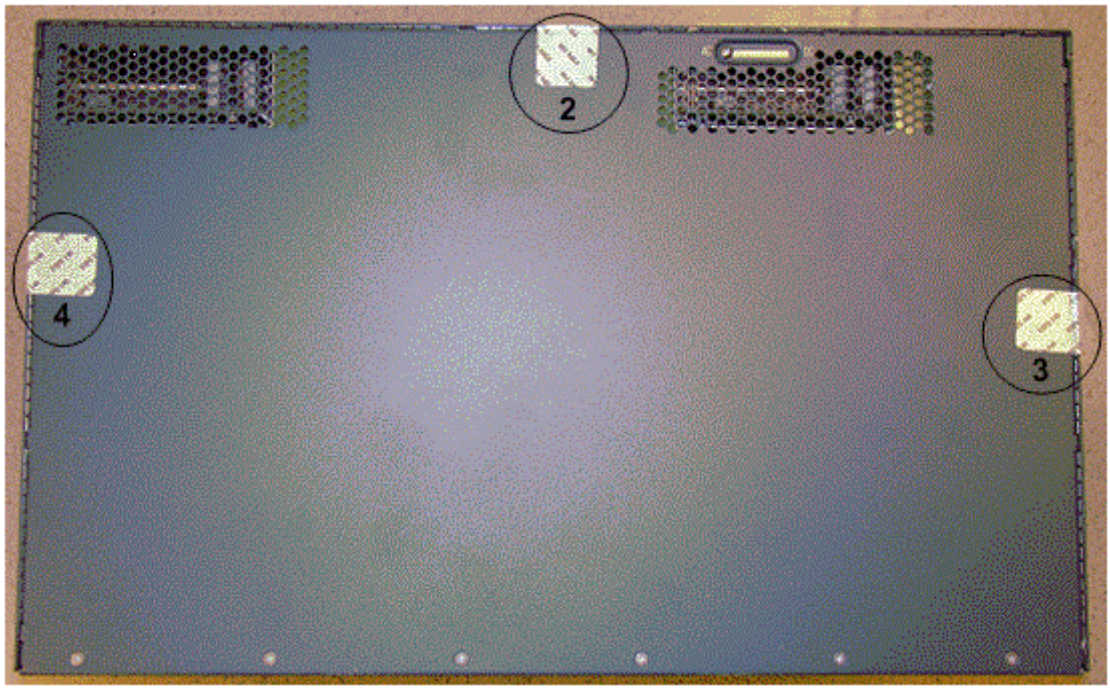
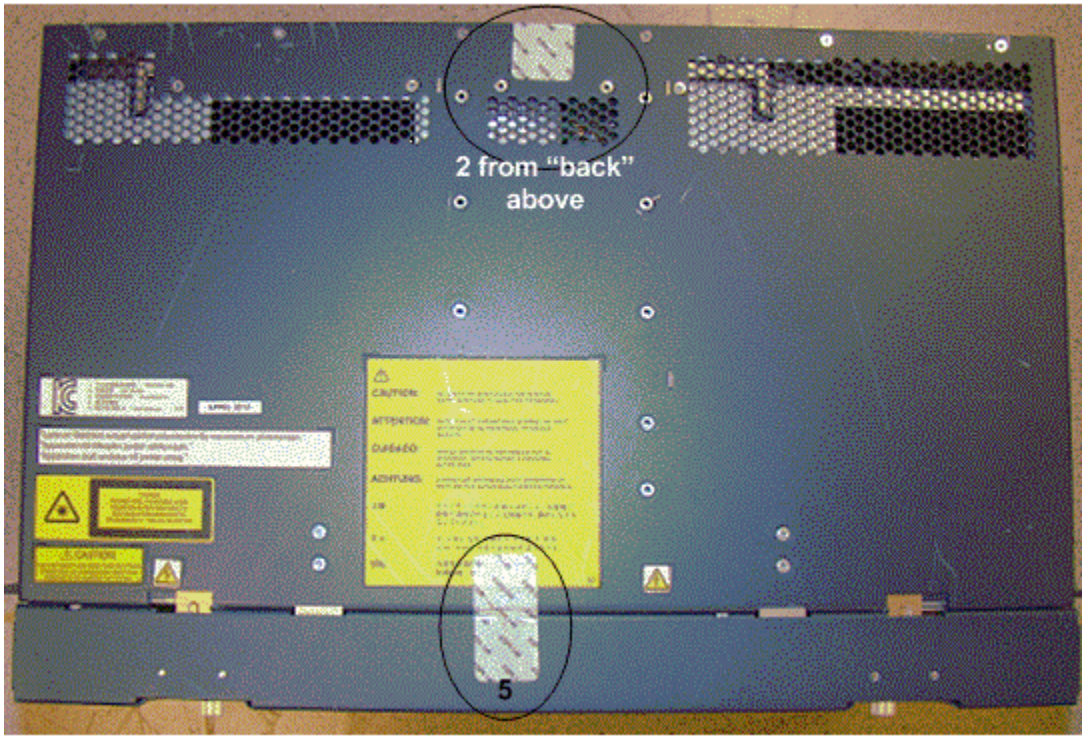
View	M2 – TEL Placement and Numbering
Bottom	
Left	
Right	

Table 8: **M2 TEL Placement**

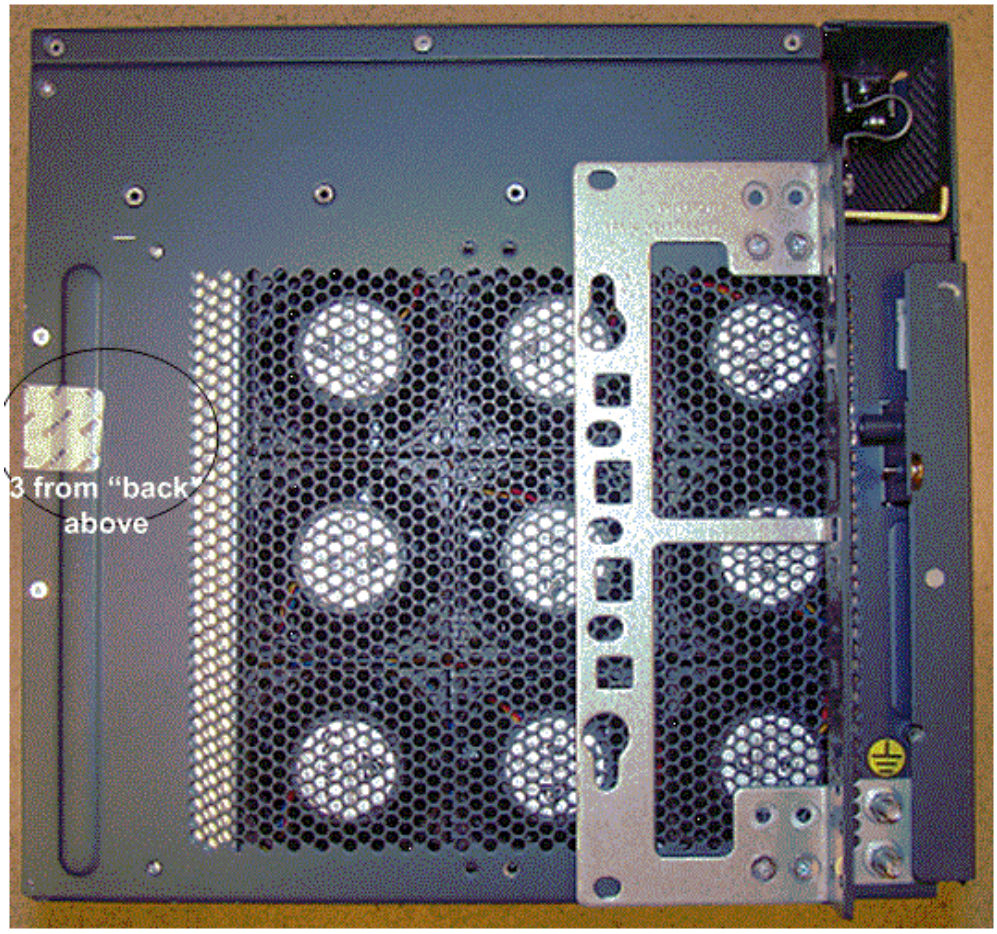
© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	M6 – TEL Placement and Numbering
Front	
Back	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	M6 – TEL Placement and Numbering
Top	
Bottom	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	M6 – TEL Placement and Numbering
Left	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

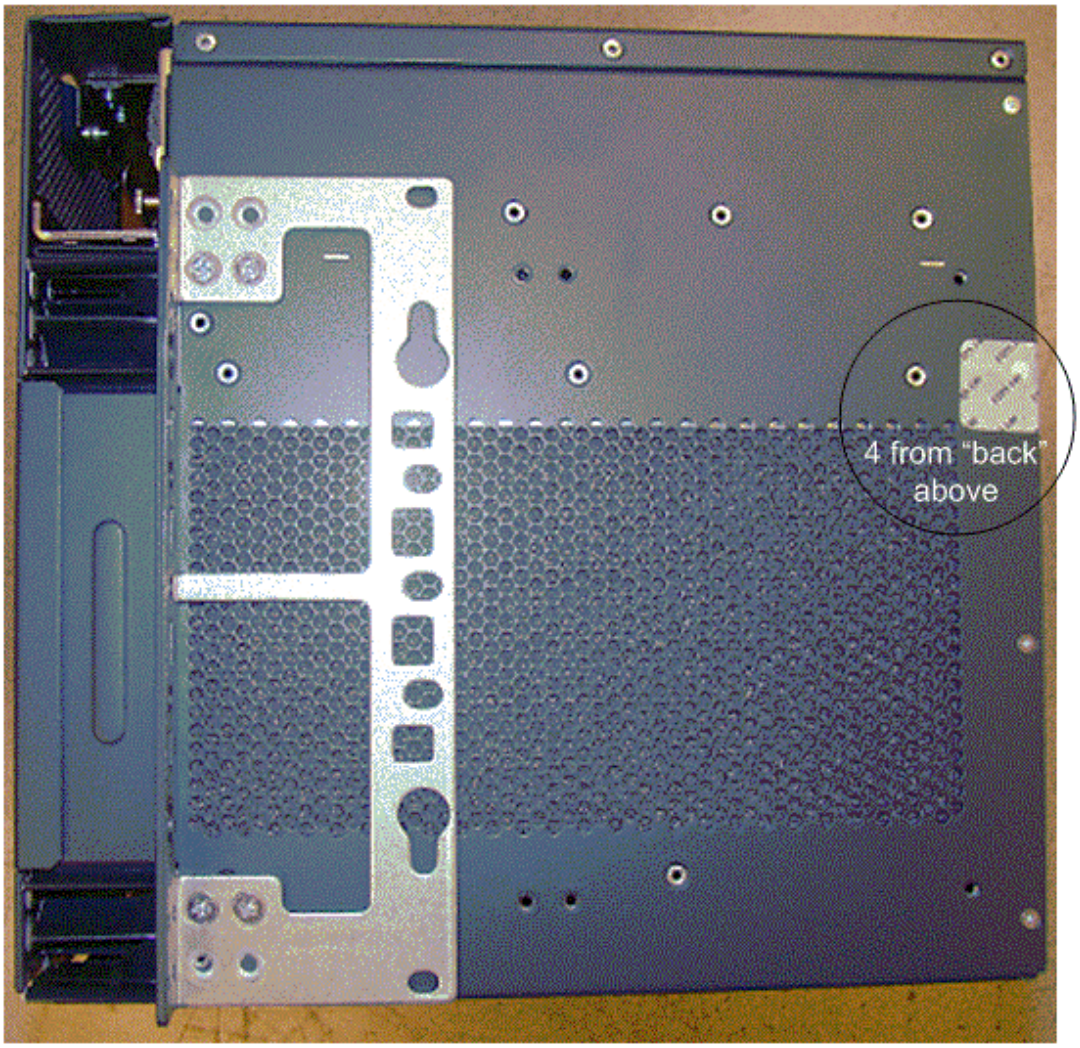
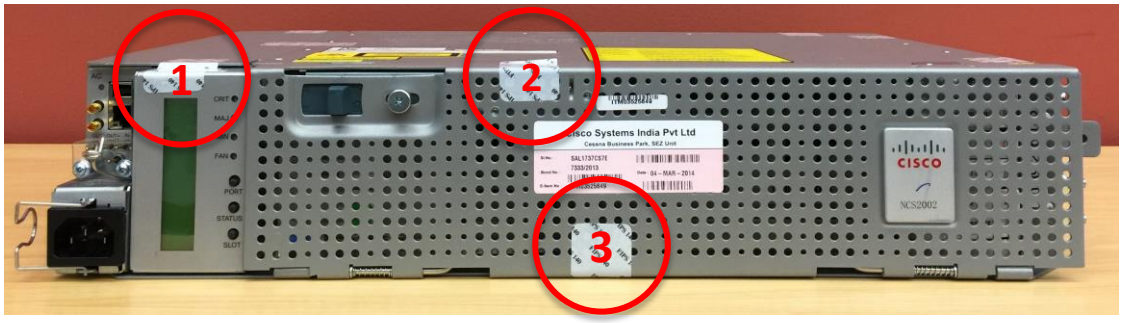
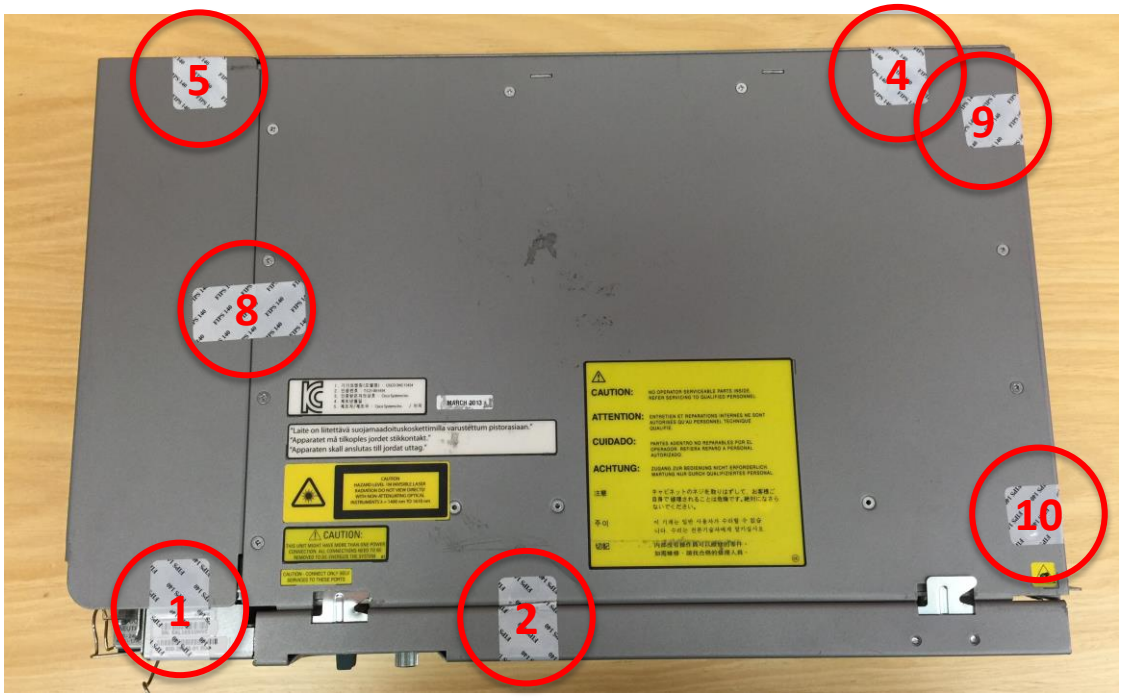
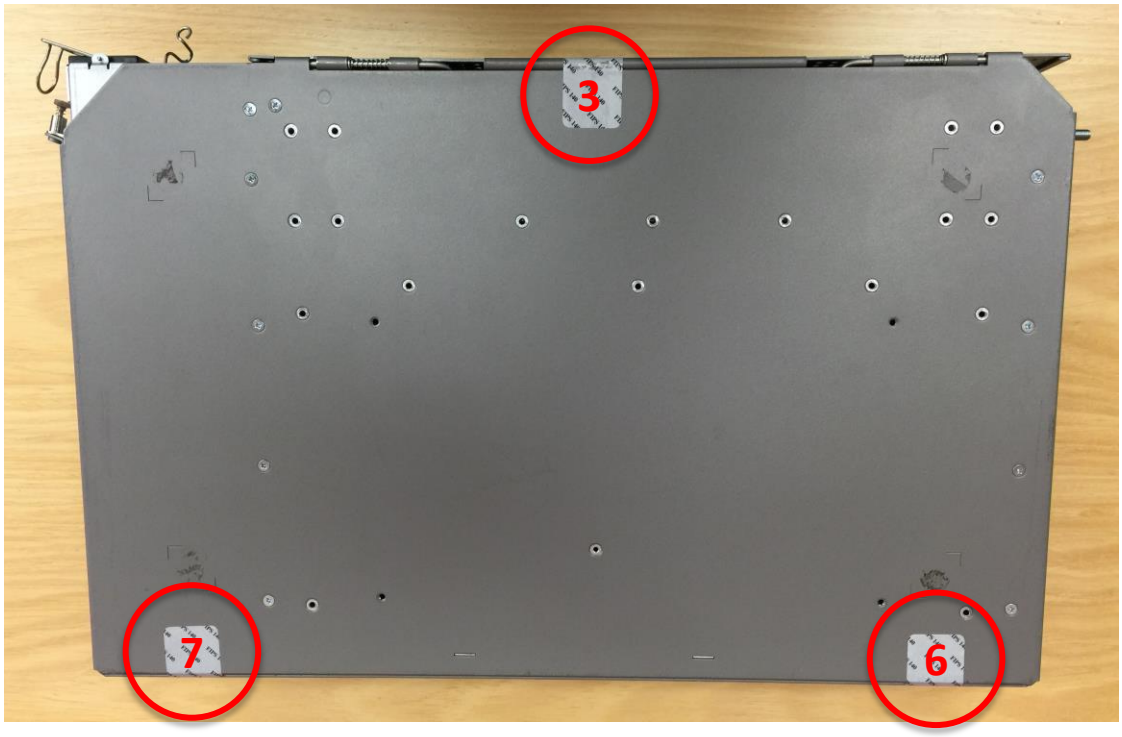
View	M6 – TEL Placement and Numbering
Right	

Table 9: **M6 TEL Placement**

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	NCS2002 – TEL Placement and Numbering
Front	
Back	
Top	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

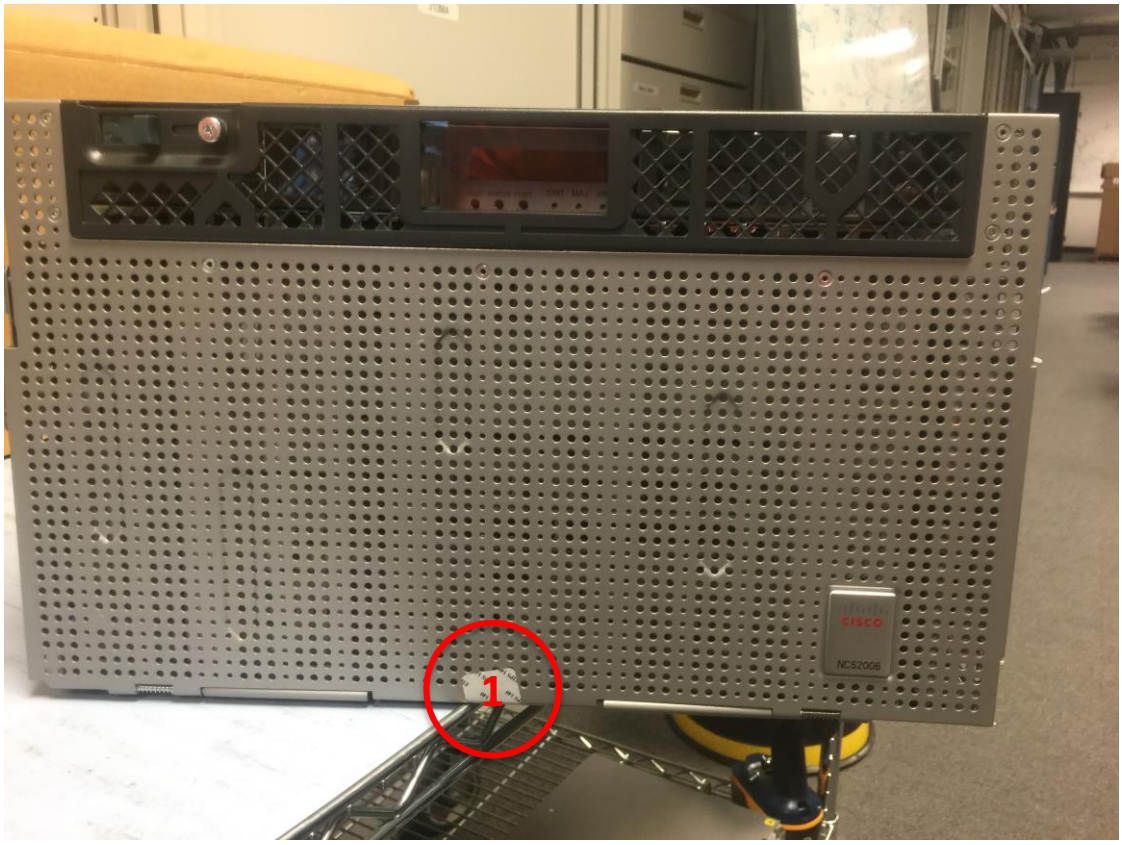
View	NCS2002 – TEL Placement and Numbering
Bottom	
Left	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

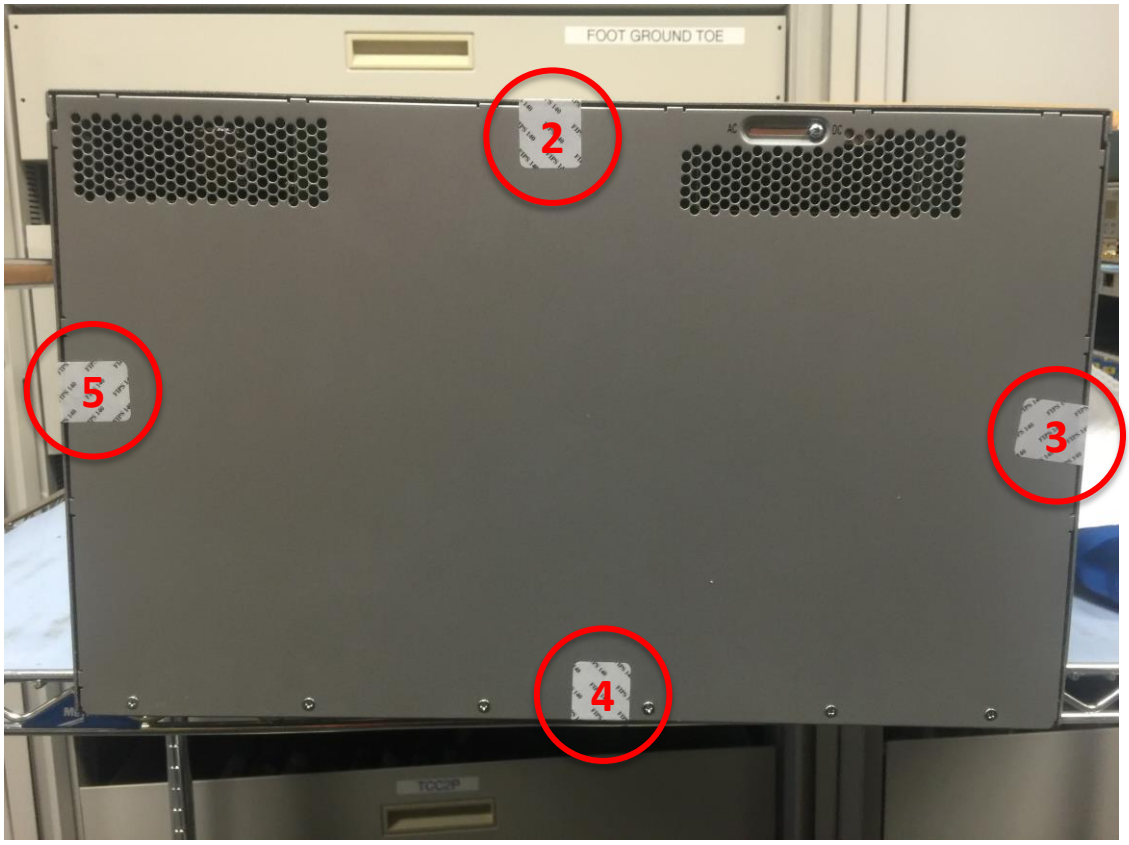
View	NCS2002 – TEL Placement and Numbering
Right	

Table 10: **NCS2002 TEL Placement**

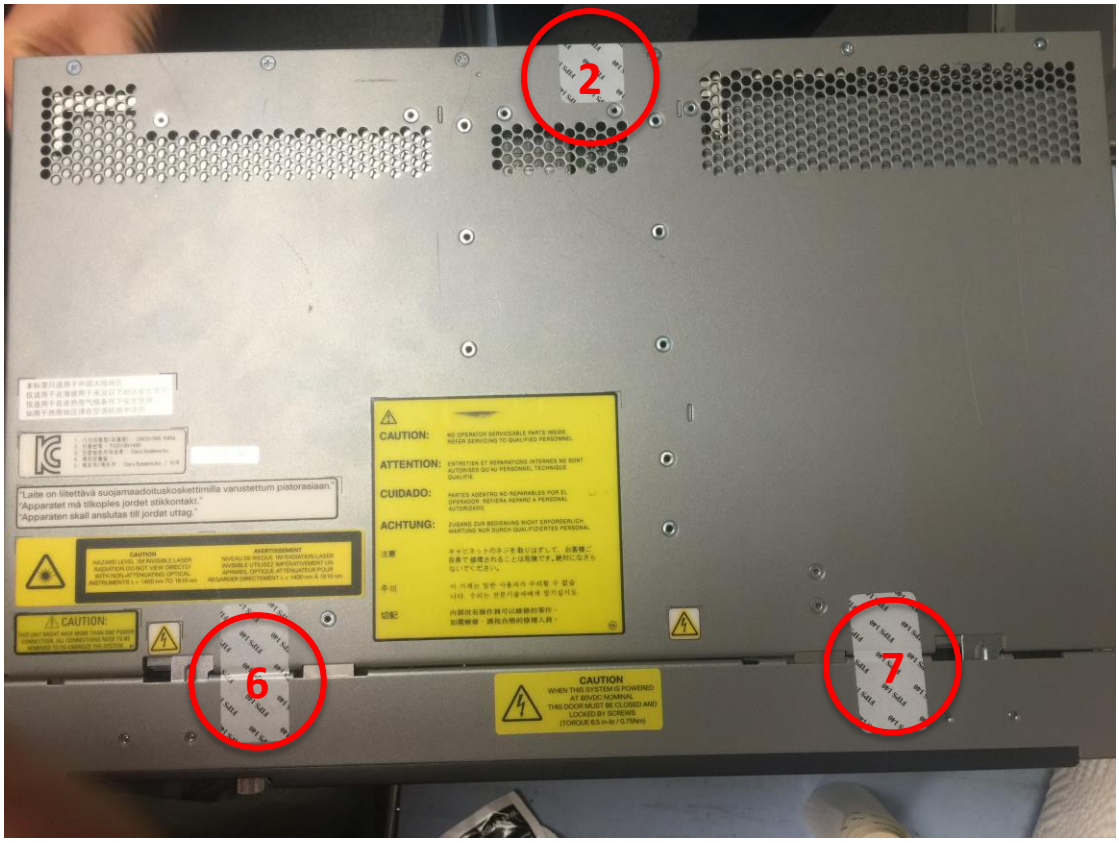
© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	NCS2006 – TEL Placement and Numbering
Front	

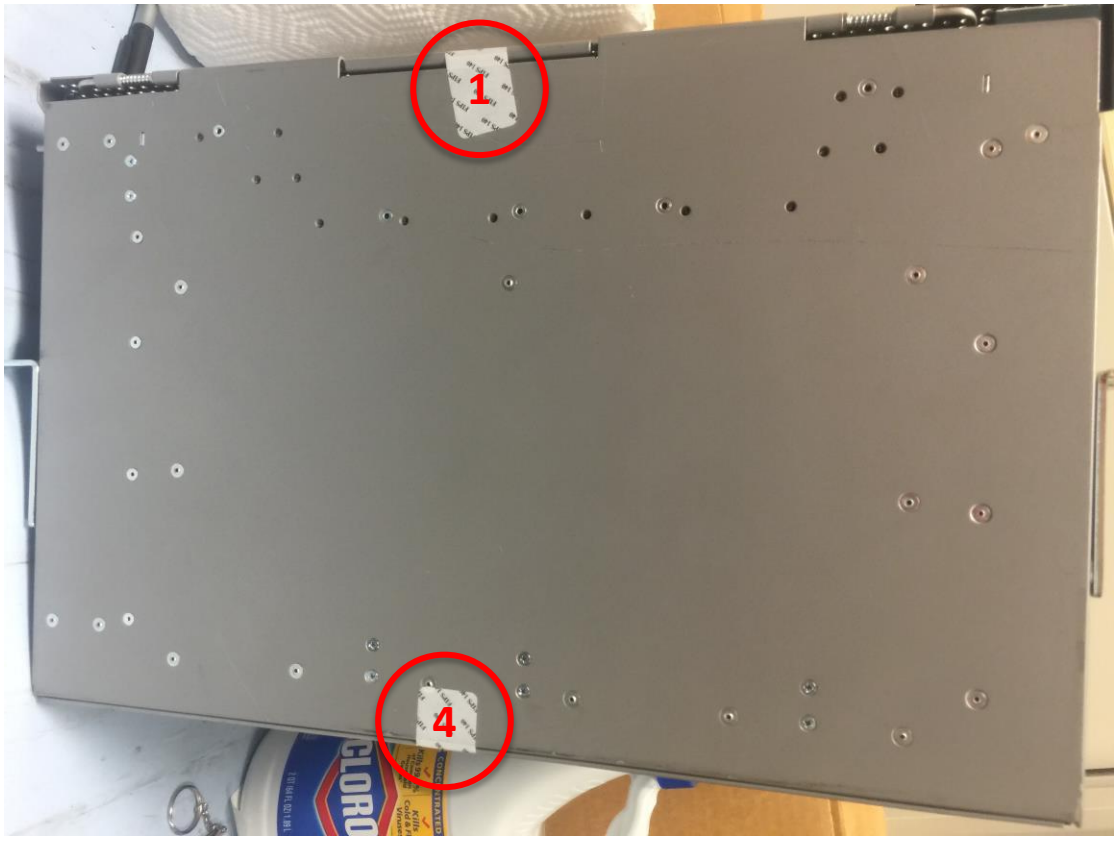
© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	NCS2006 – TEL Placement and Numbering
Back	

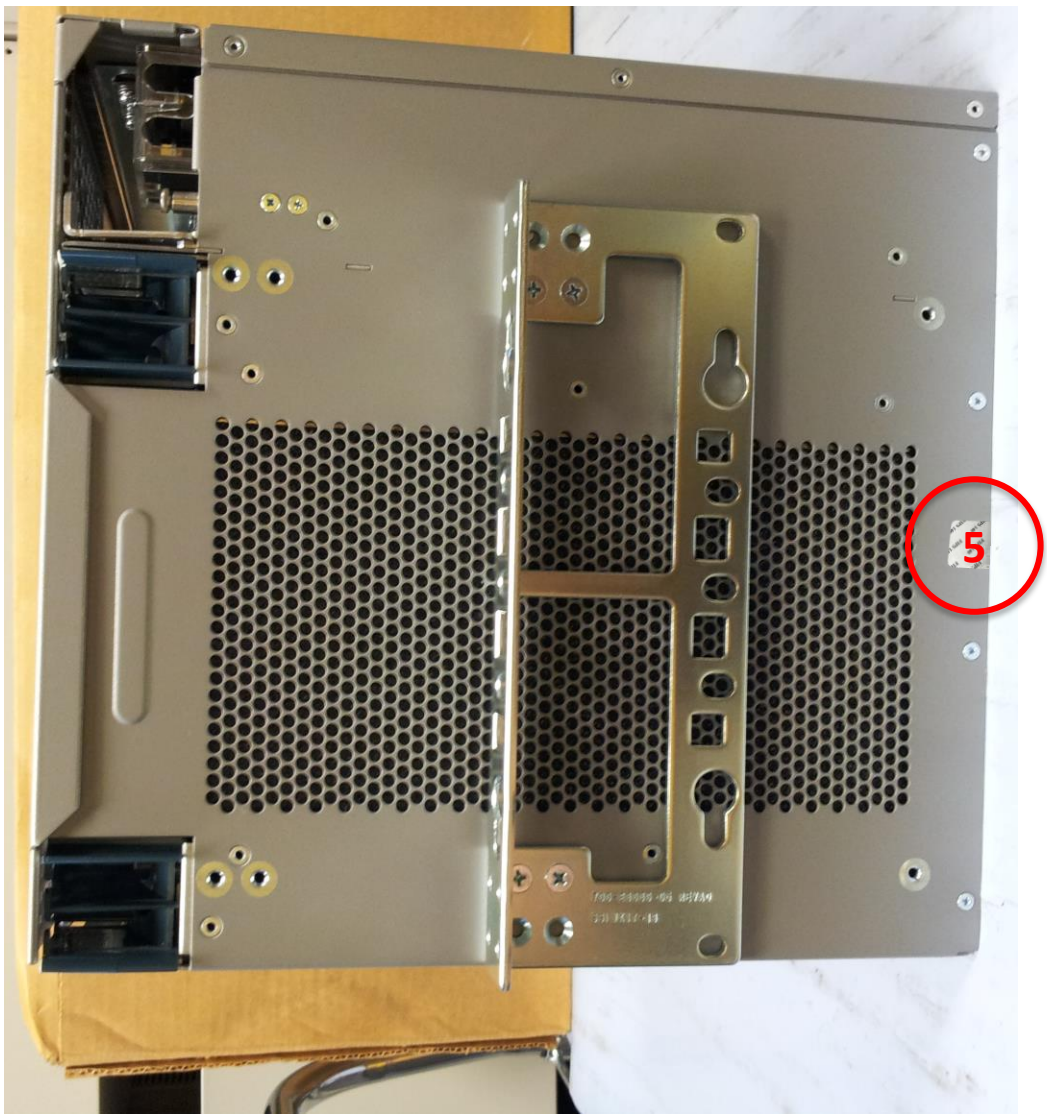
© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	NCS2006 – TEL Placement and Numbering
Top	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	NCS2006 – TEL Placement and Numbering
Bottom	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	NCS2006 – TEL Placement and Numbering
Left	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

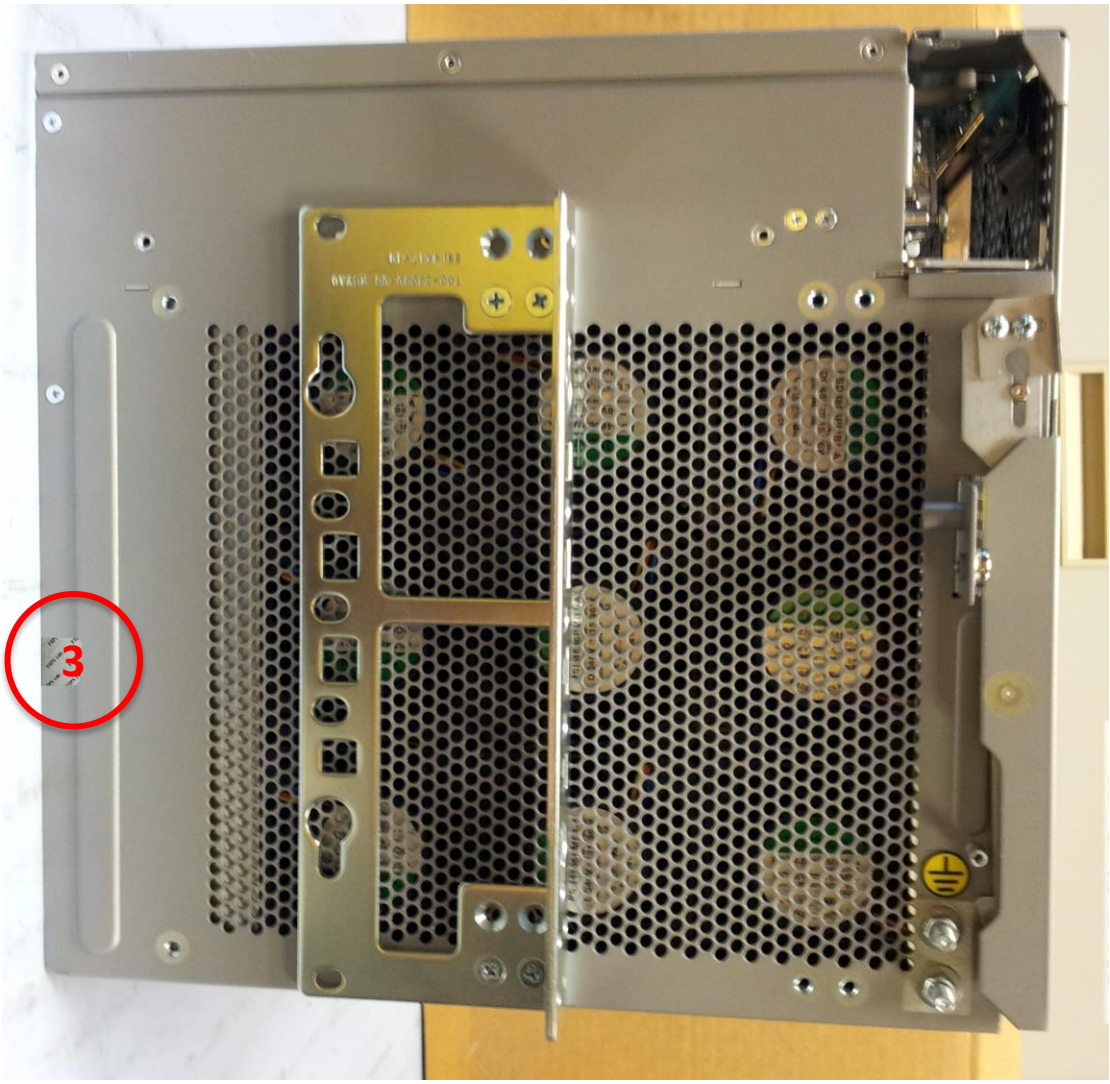
View	NCS2006 – TEL Placement and Numbering
Right	

Table 11: **NCS2006 TEL Placement**

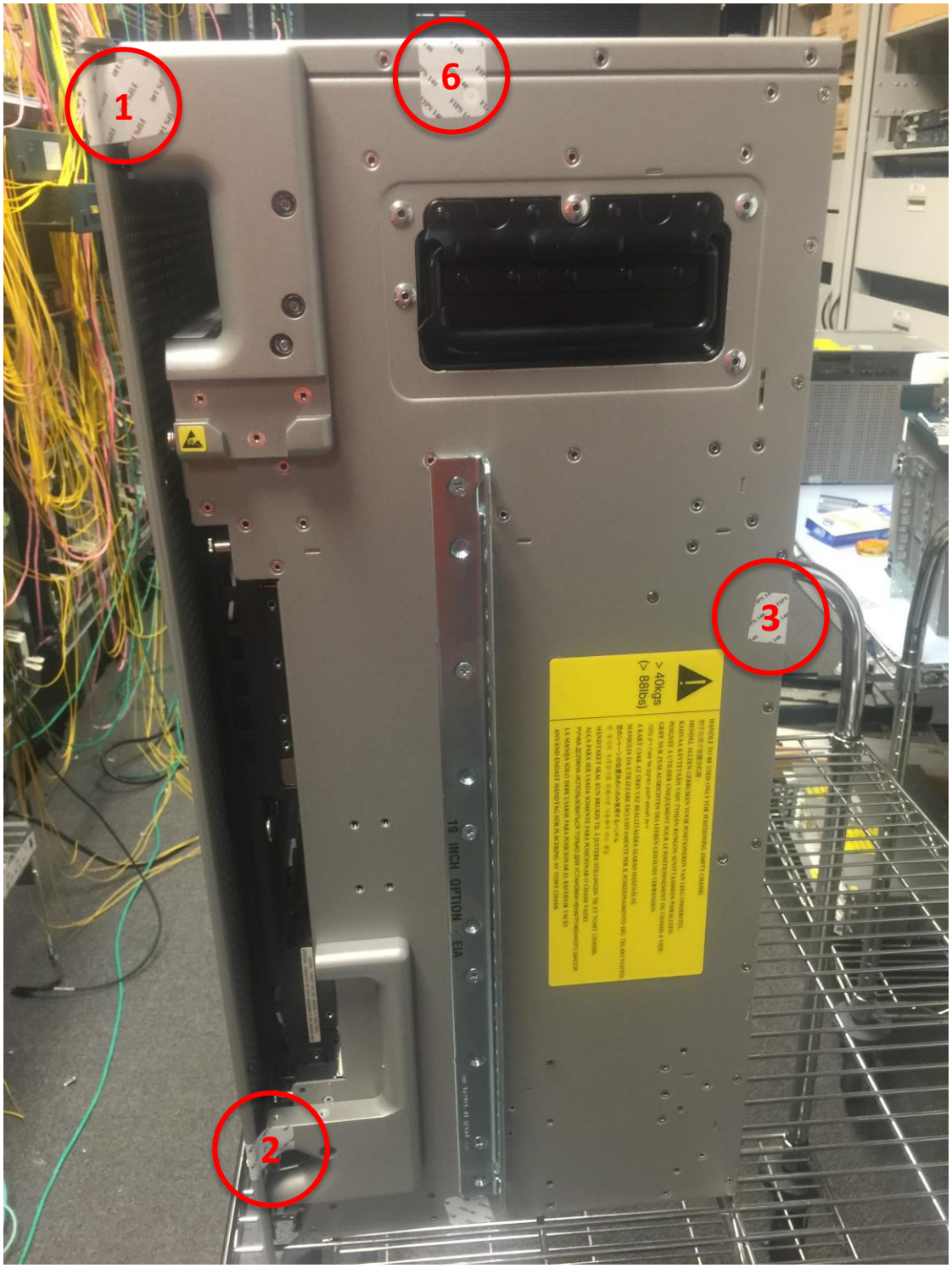
© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	NCS2015 – TEL Placement and Numbering
Front	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	NCS2015 – TEL Placement and Numbering
Back	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	NCS2015 – TEL Placement and Numbering
Left	

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

View	NCS2015 – TEL Placement and Numbering
Right	

Table 12: **NCS2015 TEL Placement**

© Copyright 2016 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

6 Secure Operation

The Cisco Optical Networking Solution (ONS) meets all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

6.1 Initial Setup

1. The Crypto Officer must apply tamper evidence labels as described in of this document. Please be aware that the RS232 port (on each Controller Card) that was protected by the front cover of each chassis should not be used while in FIPS mode.

2. On the GUI make the following changes:
    a. Provisioning/Access
        i. TL1 – Access: Secure
        ii. Shell – Access: Secure
        iii. EMS - Access: Secure
        iv. SNMP – Access: Secure
        v. Psuedo IOS – Access: Secure
    b. Provisioning/FIPS
        i. FIPS: Enabled

6.2 System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration.

6.3 HTTPS Management Requirements and Cryptographic Algorithms

1. When negotiating TLS cipher suites, only FIPS approved algorithms may be specified.
2. All versions of SSL except version 3.1 must not be used in FIPS mode of operation.
3. The following algorithms are not FIPS approved and should not be used in the FIPS-approved mode:
    a. MD5
    b. HMAC-MD5
    c. RC4
    d. DES

6.4 SSHv2 Management Requirements and Cryptographic Algorithms

1. SSH v2access to the module is only allowed if SSH v2 is configured to use a FIPS-approved algorithm.
2. Note: All users must still authenticate after remote access is granted.

Remote access is permitted via SSHv2 and HTTPS. While in FIPS 140-2 Mode of Operations the modules will enforce use of Approved algorithms for the management protocols .

7 Related Documentation

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

This document deals only with operations and capabilities of the security appliances in the technical terms of a FIPS 140-2 cryptographic device security policy. More information is available on the security appliances from the sources listed in this section and from the following source:

- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the security appliances.

8 Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

8.1 Cisco.com

You can access the most current Cisco documentation at this URL:
http://www.cisco.com/techsupport

You can access the Cisco website at this URL:
http://www.cisco.com

You can access international Cisco websites at this URL:
http://www.cisco.com/public/countries_languages.shtml

8.2 Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:
http://www.cisco.com/go/marketplace/

8.3 Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:
http://www.cisco.com/go/marketplace/
Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

9 Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.
You can send comments about Cisco documentation to bug-doc@cisco.com.
You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:
Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883
We appreciate your comments.

10 Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:
http://www.cisco.com/go/psirt
If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:
http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

10.1 Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Tip
We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
The link on this page has the current PGP key ID in use.

11 Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

11.1 Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:
http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:
http://tools.cisco.com/RPF/register/register.do

Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

11.2 Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:
http://www.cisco.com/techsupport/servicerequest

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)EMEA: +32 2 704 55 55USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:
http://www.cisco.com/techsupport/contacts

11.3 Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.
Severity 1 (S1) – Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
Severity 2 (S2) – Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
Severity 3 (S3) – Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.
Severity 4 (S4) – You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

12 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

http://www.cisco.com/packet

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

http://www.cisco.com/en/US/learning/index.html

© Copyright 2016 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.