

10Gbps Optical Encryption Line Card for the Cisco NCS 2000 Series and Cisco ONS 15454 MSTP

Product Overview

Providing data confidentiality and data integrity over a fiber-optic communication channel, the Cisco® 10Gbps Optical Encryption Line Card brings encryption to the Cisco Network Convergence System (NCS) 2000 Series and the Cisco ONS 15454 Multiservice Transport Platform (MSTP). You get highly dependable security through the combined use of next-generation cryptography and Cisco's trustworthy systems initiative, helping to ensure a highly robust architecture and adherence to product security development best practices.

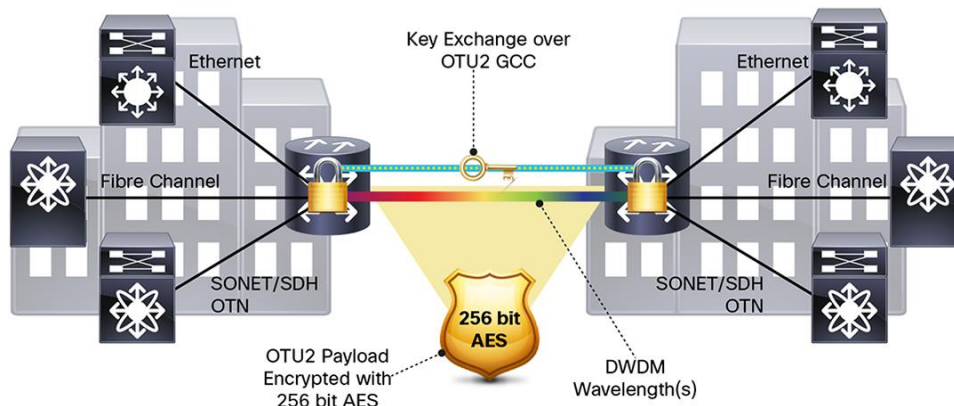
The encryption line card (Figure 1) is a single-slot card that fits into the Cisco NCS 2006 and 2002 and Cisco ONS 15454 MSTP M6 and M2 chassis. The card (part number: 15454-M-WSE-K9=) has 10 enhanced Small Form-Factor Pluggable Plus (SFP+) ports that support five independent encryption streams, providing superb density for 10-gigabit encryption services.

Figure 1. Cisco ONS 15454 10Gbps Optical Encryption Line Card



By encrypting the Optical Transport Network (OTN) payload, the 10G optical encryption line card is able to securely transport a variety of protocols including Ethernet, fibre channel, OTN, and OC-192/STM-64 across a DWDM, dark fiber, or leased line infrastructure (Figure 2).

Figure 2. Secure Point-to-Point Communication over DWDM Architecture



Features

- **Integrated transponder:** The encryption card supports both grey and dense wavelength-division multiplexing (DWDM) SFP+ optics on all ports with the option to use standard or enhanced Forward Error Correction (FEC) for longer reach.
- **Secure key exchange:** General communication channel 2 (GCC2), secured using Transport Layer Security (TLS) to mitigate a man-in-the-middle attack, is used to exchange the symmetric key for encryption between two communicating cards.
- **Single GUI for management:** The Cisco Transport Controller provides complete separation between security and transport operations by supporting role-based access control for different users.

Table 1 summarizes the features and benefits of the Cisco ONS 15454 10G optical encryption line card.

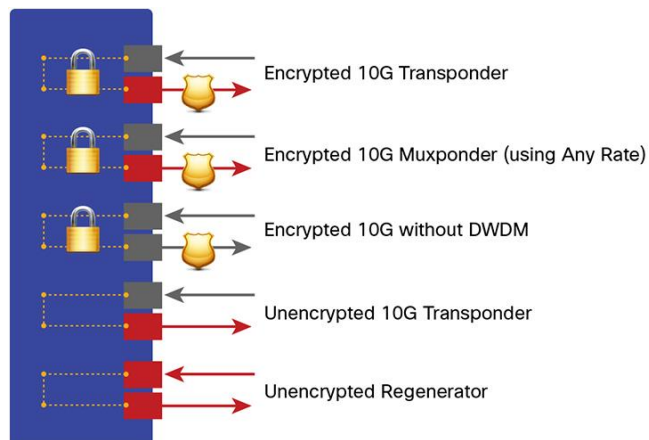
Table 1. Features and Benefits

Feature	Benefit
Secure boot	Helps ensure that only authentic software is running on the system at boot-up
Image signing	Helps ensure that only authentic software is running on the system at load time
Immutable identity	Helps ensure that hardware received is not counterfeit
Secure unique device identification	Provides cryptographic assertion of device identity, in turn used to authenticate the peer card
True random bit generation	Provides nondeterministic numbers used in key generation
Advanced cryptographic algorithms	Improves efficiency without sacrificing security
Cold zeroization	Erases critical security parameters on card reset or removal or chassis power down
Federal Information Processing Standard (FIPS) certification	Helps guarantee protection of critical security information

General Modes of Operation

- **Encryption only:** The card provides confidentiality for the information sent.
- **Transponder:** With encryption disabled, the card is a normal transponder, providing grey to DWDM conversion with FEC or E-FEC available for additional reach (Figure 3).
- **Regenerator:** The card performs standard optical-to-electrical-to-optical (O-E-O) regeneration of a DWDM signal.

Figure 3. Encryption Card Operational Modes



FIPS and Non-FIPS Mode of Operation

The encryption card is Federal Information Processing Standard (FIPS) 140-2 level 2 validated. To satisfy the FIPS requirement, the cryptographic module (in this case the encryption card and controller) must support a FIPS mode of operation in which only FIPS-approved algorithms are run.

When the FIPS mode is turned on, both the controller cards (active and standby transport node controllers or transport shelf controllers), as well as all encryption cards present in the chassis, will reboot. This is a traffic-affecting operation, and a warning is displayed on the craft terminal - the Cisco Transport Controller or Cisco Prime™ Optical - when FIPS mode is turned on. During reboot, the encryption cards and controllers run the FIPS Power On Self Tests (POST). Upon successful completion, the card enters FIPS mode. When setting FIPS mode off, only the controller cards require reboot.

Licensing

A licensed version of the line card providing a single encrypted stream offers a cost-effective solution for low channel counts. A flexible software upgrade license is applied to unlock an additional encryption stream (Table 2).

Table 2. 10Gbps Optical Encryption Line Card Software Licenses

Part Number	Description
15454-M-WSE-L-K9=	Wire Speed Encryption Unit, software license upgradable
L-NCS2K-WSE-1=	NCS 2K/MSTP License WSE - 1x Encryption Stream e-Delivery

Encryption Bundles

Services with speeds lower than 10 Gbps can be encrypted by first multiplexing them into an OTU2 signal using the Cisco ONS 15454 Any Rate Muxponder Card or Any Rate Xponder Card. Two card bundles are available (Table 3). An unlicensed bundle is ideal for an encrypted network with a large number of services with speeds lower than 10 Gbps, and a licensed bundle is available for networks that initially have a smaller number of services with speeds lower than 10 Gbps.

Table 3. Cisco ONS 15454 Any Rate Muxponder and Any Rate Xponder Bundles

Bundle Part Number	Constituents
15454-ARE-K9-SK	1 x 15454-M-WSE-K9, 1 x AR-XP-LIC, 1 x ONS-SC+-10G-SR and 1x ONS-XC-10G-SR-MM
15454-ARE-L-K9-SK	1 x 15454-M-WSE-L-K9, 1 x AR-MXP-LIC, 1 x ONS-SC+-10G-SR and 1x ONS-XC-10G-SR-MM

The proper feature license needs to be purchased on the Cisco ONS 15454 Any Rate Xponder or Muxponder cards, depending on the services that need to be aggregated. The same flexible software license needs to be purchased with the second bundle for additional encrypted services.

Protocol Transparency

When used in the Cisco ONS 15454 MSTP or Cisco NCS 2000 Series platforms, the encryption line card can transparently deliver the 10-Gbps services listed in Table 4 for cost-effective, secure, point-to-point transport.

Table 4. Client Protocol Mapping

Client		Mapping
Format	Rate (Gbps)	
10 Gigabit Ethernet LAN-PHY	10.3125	CBR-BMP clause 17.2.4 (ex G sup43 7.1) + GMP ODU2e to OPU3e4
10 Gigabit Ethernet LAN-PHY	10.3125	GFP-F
OTU2	10.709	ODU transparent + GMP ODU2 to OPU3e4
OTU2e	11.096	ODU transparent + GMP ODU2 to OPU3e4
OC-192/10GE WAN-PHY	9.953	AMP
8G Fibre Channel	8.5 (10G Fiber Channel payload)	GMP
10G Fibre Channel	10.0591	GFP-T
OTU1e	11.0491	BMP

FEC Capability

The encryption card supports an FEC mechanism on any of the SFP+ interfaces. This can be independently activated or disabled on all ports. Two software-configurable coding options are available:

- **Generic FEC (GFEC):** Standard G.975 Reed-Solomon algorithm.
- **Enhanced FEC (EFEC):** Standard G.975.1 (Sub-clause I.7) with 7 percent overhead. This FEC scheme uses two orthogonally concatenated BCH super-FEC codes, and the constructed code is decoded iteratively to rebuild the original frame.

Management

The Cisco NCS 2000 Series and ONS 15454 MSTP provide comprehensive management capabilities to support Operations, Administration, Maintenance, and Provisioning (OAM&P) capabilities through the integrated Cisco Transport Controller craft interface with support from the Cisco Prime Optical element management system. Role-based access control is enforced to help ensure that only authorized users are able to perform the desired operations, thus providing a complete separation between the transport and security domains.

Two new user profiles for performing security operations are available, in addition to the existing transport user profiles. They are a security super user and a security user. The former is available by default, while the latter is created by the security super user and assigned to specific encryption cards in the node.

Table 5. Security Capabilities of Cisco Transport Controller User Profiles

Panes		Security Super User	Security User	Transport User
Performance - Encryption PM	Refresh	✓	✓	✓
	Baseline	✓	✓	x
	Clear	✓	✓	x
Provisioning - Security Threshold		✓	✓	x
Encryption - GCC2 Settings		✓	✓	x
Encryption - Security		✓	✓	x
Encryption - Key Management		✓	✓	x

Panes		Security Super User	Security User	Transport User
Encryption - Advanced Settings		✓	✗	✗
Encryption - OTN Overhead for Packet Traffic		✓	✗	✗
Provisioning - Security - FIPS		✓	✗	✗

The user-card association is erased on chassis power-down or controller-card reboot. The security super user and security user passwords are hashed and stored using a FIPS-approved algorithm.

Protection Mechanisms

The 10G optical encryption line card supports Y-cable protection, in which a passive “Y” module splits the client signal across two line cards within the same chassis configured as a protection group. This protects the client signal from line card failures in addition to fibre failures, switching traffic from the working card/path to the protect card/path within 50 milliseconds. Y-cable protection is supported for 10 Gigabit Ethernet and OC-192/STM-64 client payloads.

By utilizing the Optical Protection Switching Module the encryption card also supports Optical Channel-Trail (OCH-Trail) protection, providing protection for the DWDM signal alone.

Product Specifications

Table 6 lists regulatory compliance information, and Table 7 shows the system requirements for the Cisco ONS 15454 encryption line card. Table 8 provides performance monitoring parameters. Table 9 provides card specifications, and Table 10 lists ordering information for the card.

Regulatory Compliance

Important: Not all compliance documentation may be completed at the time of product release. Please check with your Cisco sales representative for countries other than Canada, the United States, and the European Union.

Table 6. Regulatory Compliance

ANSI System	ETSI System
Countries Supported	
<ul style="list-style-type: none"> • Canada • United States • Korea • Japan • European Union 	<ul style="list-style-type: none"> • European Union • Africa • CSI • Australia • New Zealand • China • Korea • India • Saudi Arabia • South America
EMC (Class A)	
<ul style="list-style-type: none"> • ICES-003, 2004 • GR-1089-CORE Issue 4, NEBS EMC and Safety, June 2006 • FCC 47CFR15, 2007 	<ul style="list-style-type: none"> • ETSI EN 300 386 V1.4.1 (2008-04) Telecommunication network equipment EMC requirements (Note: EMC-1) • CISPR22:2008 and EN55022:2006/A1:2007 Information Technology Equipment (Emissions) (EMC-2) • CISPR24: 1997/A1:2001/A2:2002 and EN55024:1998/A1:2001/A2:2003: Information Technology Equipment - Immunity characteristics - Limits and Methods of Measurement (test levels)

ANSI System	ETSI System
Safety	
<ul style="list-style-type: none"> • CSA C22.2 #60950-1 - Edition 7, March 2007 • UL 60950-1 - Edition 2, March 2007 • GR-1089-CORE Issue 4, NEBS EMC and Safety, June 2006 	<ul style="list-style-type: none"> • UL 60950-1 - Edition 2, March 2007 • IEC 60950-1 Information technology equipment Safety Part 1: General requirements - Edition 2, 2005 and National Differences as per CB Bulletin 112A • IEC/EN 60950-1 (2006/10) with Amendment 11:2004 to EN 60950-1:2001, 1st Edition and National Differences as per CB Bulletin 112A. • EN 60950-1, Edition 2 (2006) Information technology equipment - Safety - Part 1: General requirements • CE Safety Directive: 2006/95/EC
Laser	
<ul style="list-style-type: none"> • UL 60950-1 - Edition 2, March 2007 • IEC 60825-1: 2001 Ed.1.2 (incl. am1+am2) Safety of laser products Part 1: Equipment classification, requirements and users guide • IEC60825-2 Ed.3 (2004) Safety of laser products Part 2: Safety of optical fiber communication systems + A1:2006 	<ul style="list-style-type: none"> • IEC 60825-1: 2001 Ed.1.2 (incl. am1+am2) Safety of laser products Part 1: Equipment classification, requirements and users guide • IEC60825-2 Ed.3 (2004) Safety of laser products Part 2: Safety of optical fibre communication systems + A1:2006 • 21CFR1040 (2008/04) (Accession Letter and CDRH Report) Automatic Laser Shutdown and restart (ALS) according to ITU-T G.664 (03/06). Guidance for Industry and FDA Staff (Laser Notice No. 50), June 2007 • Laser Products - Conformance with IEC 60825-1 and IEC 60601-2-22; Guidance for Industry and FDA Staff (Laser Notice No. 50), June 2007
Environmental	
<ul style="list-style-type: none"> • GR-63-CORE Issue 3, NEBS Physical Protection, March-2006 	<ul style="list-style-type: none"> • ETS 300-019-2-1 V2.1.2 (Storage, Class 1.1) • ETS 300-019-2-2 V2.1.2 (1999-09): Transportation, Class 2.3 • ETS 300-019-2-3 V2.2.2 (2003-04):Operational, Class 3.1E
Optical	
<ul style="list-style-type: none"> • GR-253-CORE - Issue 04 • ITU-T G.691 	<ul style="list-style-type: none"> • ITU-T G.709 • ITU-T G.975
Quality	
<ul style="list-style-type: none"> • TR-NWT-000332, Issue 4, Method 1 calculation for 20-year mean time between failure (MTBF) 	
Miscellaneous	
<ul style="list-style-type: none"> • GR-1089-CORE Issue 4, NEBS EMC and Safety (June 2006) (Note: NEBS-1) • GR-63-CORE Issue 3, NEBS Physical Protection (March 2006) (Note: NEBS-2) • ATT-TP-76200: 2008 • ANSI T1.315-2001 • GR-499: 2004 Transport Systems Generic Requirements (TSGR): Common Requirements • Common Criteria Certification - The ONS 15454 M2 and ONS 15454 M6 nodes are Common Criteria (CC) compliant. The CC certification from National Institute of Standards and Technology (NIST) using the Network Device Protection Profile (NDPP) helps ensure the node is accessed, managed, monitored and provisioned in a highly secure manner. The CC applies only to ONS 15454 M2 and ONS 15454 M6 stand-alone nodes with TNC/TSC/TNC-E/TSC-E cards as the node controller. 	

System Requirements and Other Specifications

Table 7. System Requirements

Component	
Processor	<ul style="list-style-type: none"> • TNC/TSC/TNC-E/TSC-E
Shelf assembly	<ul style="list-style-type: none"> • Cisco NCS2006-SA shelf assembly • Cisco NCS 2002-SA shelf assembly • Cisco ONS 15454-M6-SA shelf assembly with FTA2 • Cisco ONS 15454-M2-SA shelf assembly with FTA2
System software	<ul style="list-style-type: none"> • Cisco NCS 2000 Release 10.0 • Cisco ONS 15454 MSTP Release 9.8 ANSI/ETSI

Table 8. Performance Monitoring Parameters

Area	Parameter Name		Description
OTN	OTUk SM	ODUk PM	
	BBE-SM	BBE-PM	Number of background block errors
	BBER-SM	BBER-PM	Background block error ratio
	ES-SM	ES-PM	Number of errored seconds
	ESR-SM	ESR-PM	Errored seconds ratio
	SES-SM	SES-PM	Number of severely errored seconds
	SESR-SM	SESR-PM	Severely errored seconds ratio
	UAS-SM	UAS-PM	Number of unavailable seconds
	FC-SM	FC-PM	Number of failure counts
OC-192/STM-64	RS-BBE	MS-BBE	Number of Background Block Errors
	RS-BBER	MS-BBER	Background Block Errors Ratio
	RS-ES	MS-ES	Number of Errored Second
	RS-ESR	MS-ESR	Errored Seconds Ratio
	RS-SES	MS-SES	Number of Severely Errored Seconds
	RS-SESR	MS-SESR	Severely Errored Seconds Ratio
	RS-UAS	MS-UAS	Number of Unavailable Seconds
	RS-EB	MS-EB	Number of Errored Blocks
	RS-OFS	MS-OFS	Regenerator Section Out of Frame Sequence
FEC	Bit errors		Number of corrected bit errors
	Uncorrectable words		Number of uncorrectable words
Trunk optical performance monitoring	OPT		Transmit optical power
	LBC		Transmitter laser bias current
	OPR		Receiver optical power

Table 9. Card Specifications

Management	
Card LEDs	
Failure (FAIL)	Red
Active or standby (ACT/STBY)	Green/yellow
Signal fail (SF)	Yellow
Client port LEDs (per port)	
Active input signal	Green
Power (including worst-case pluggable configuration)	
Typical	110W (25C and -48VDC)
Maximum	160W (55C and -38VDC)
Physical	
Dimensions	Occupies 1 slot
Weight	1.24 kg (2.73 lbs)
Reliability and availability	
Mean time between failures (MTBF)	111,544 hrs

Management	
Latency (end to end) with encryption off	
G.709 - FEC disabled	6 microseconds
G.709 - Standard FEC	10 microseconds
G.709 - EFEC	144.8 microseconds
Latency (end to end) with encryption on	
G.709 - FEC disabled	6.8 microseconds
G.709 - Standard FEC	10.5 microseconds
G.709 - EFEC	145.4 microseconds
Storage temperature	-40 to 158°F (-40 to 70°C)
Operating temperature	
• Normal	32 to 104°F (0 to 40°C)
• Short-term*	23 to 131°F (-5 to 55°C)
Relative humidity	
• Normal	5% to 85%, noncondensing
• Short-term*	5% to 90% but not to exceed 0.024 kg water/kg of dry air

* Short-term refers to a period of not more than 96 consecutive hours and a total of not more than 15 days in 1 year (a total of 360 hours in any given year, but no more than 15 occurrences during that 1-year period). The values shown are valid for M6 or M2 chassis.

Warranty Information

Warranty information is available on Cisco.com at the [Product Warranties](#) page.

Ordering Information

This section provides information on the components or parts needed to install and use the product. It also provides a direct link to the Cisco Ordering Tool and lists part numbers in Table 10.

To place an order, visit the [Cisco Ordering Home Page](#). To download software, visit the [Cisco Software Center](#).

Table 10. Ordering Information

Part Number	Description
15454-M-WSE-K9=	Full Feature Wire Speed Encryption Unit
15454-M-WSE-L-K9=	Wire Speed Encryption Unit - SW license upgradable
L-NCS2K-WSE-1=	NCS 2K/MSTP License WSE - 1x Encryption Stream e-Delivery
15454-ARE-K9-SK	Kit - Contains WSE, SFP+ SR, XFP SR & AR-XP - LIC
15454-ARE-L-K9-SK	Kit - Contains WSE-L, SFP+ SR, XFP SR & AR-MXP-LIC

For More Information

<http://www.cisco.com/go/optical>




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)