

Cisco NCS 2000 100-Gbps Multirate Muxponder

The Cisco NCS 2000 100-Gbps Multirate Muxponder efficiently aggregates and secures multiple protocols for transport over dense wavelength division multiplexing (DWDM) wavelengths.

Product Overview

As bandwidth demands increase rapidly, you're growing your network with 100- and 200-Gbps DWDM wavelengths. You can efficiently fill that massive capacity with flexible aggregation, and use powerful transport-layer encryption to secure your data against intrusion, with the Cisco NCS 2000 100-Gbps Multi-Rate Muxponder.

Features and Benefits

The Cisco NCS 2000 100-Gbps Multirate Muxponder (Figure 1) is a plug-in module for the Cisco Network Convergence System 2000 series. It multiplexes a variety of protocols into a 100-Gbps optical transport network (OTN) payload, and it can interface with 100-Gbps or 200-Gbps DWDM line cards for transport across a DWDM infrastructure.

The line card features two Enhanced Small Form-Factor Pluggable (SFP+) ports, two Quad Small Form-Factor Pluggable Plus (QSFP+) ports, and one port supporting the Cisco CPAK pluggable transceiver. The card can aggregate multiple 10-Gbps and 40-Gbps clients, or a single 100-Gbps client, into an ODU-4 container, for transmission across the chassis backplane to a paired DWDM trunk card.

The Cisco NCS 2000 100-Gbps Multirate Muxponder can optionally encrypt the ODU-4 payload using state-of-the-art public key cryptography, as well as apply card-to-card and payload authentication, helping to ensure data confidentiality and integrity. The card leverages Cisco's trustworthy systems technologies initiative, promoting a highly robust architecture and adherence to product security development best practices.

Figure 1. Cisco NCS 2000 100-Gbps Multirate Muxponder



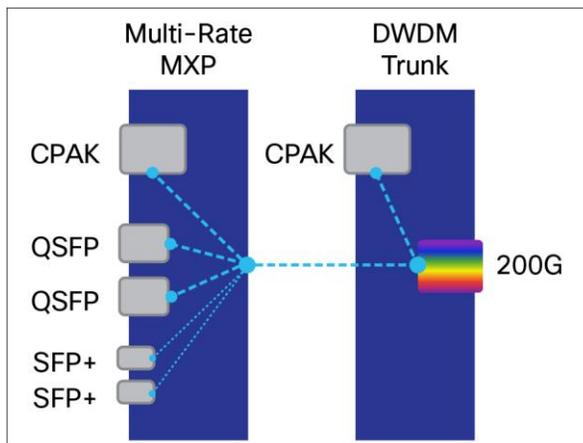
Feature	Benefit
10-Gbps, 40-Gbps, and 100-Gbps protocol aggregation in one line card	Reduce wasted capacity, require fewer trunk wavelengths, and decrease capital expenditures by efficiently filling 100-Gbps and 200-Gbps DWDM wavelengths.
Flexible modes of operation	Simplify operations by relying on one card type to aggregate 10-, 40-, and 100-Gbps protocols into 100- or 200-Gbps DWDM wavelengths. Integrated OTN encryption and authentication means that no additional protocol-specific devices or licenses are required to secure your data.
Advanced transport layer encryption	Deploy a highly secure and reliable transport solution. The card implements Cisco's proactive, cross-discipline approach to policies, processes, and technologies, including secure boot, image signing, immutable identity, secure unique device identification, true random bit generation, cold zeroization, and advanced cryptographic algorithms.
Y-cable Protection	Protect the client signal from line card failures and fiber failures by switching traffic from the working card or path to the protect card or path within 50 milliseconds. A passive "Y" module splits the client signal across two line cards within the same chassis configured as a protection group.
Link Layer Discovery Protocol (LLDP)	Discover and verify the MAC address of Ethernet switches connected to 10 Gigabit Ethernet client ports.

Flexible Operational Modes

The Cisco NCS 2000 100-Gbps Multirate Muxponder can operate in multiple modes to support a variety of applications.

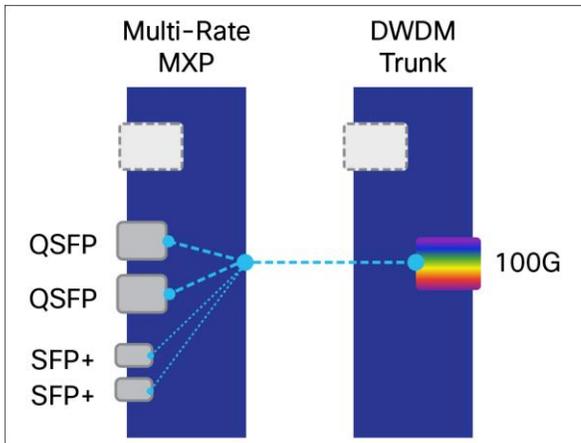
200-Gbps Muxponder Client - One or two line cards can be paired with the Cisco NCS 2000 200-Gbps Multirate DWDM Line Card to efficiently multiplex 10- and 40-Gbps signals or one 100-Gbps signal into a 200-Gbps coherent DWDM interface (Figure 2). Encryption and authentication can optionally be applied to each card's aggregated payload.

Figure 2. 200-Gbps Muxponder Client



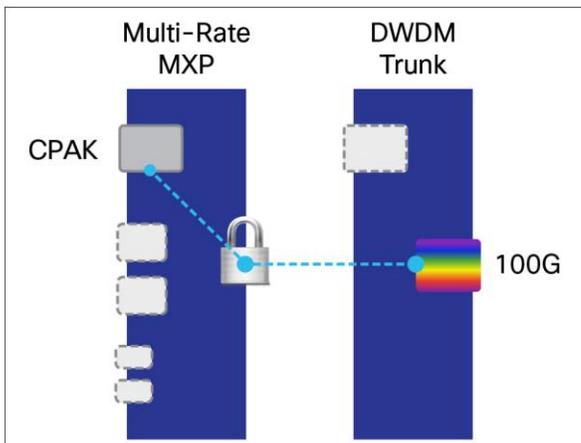
100-Gbps Muxponder Client - The line card can be paired with the Cisco NCS 2000 100-Gbps DWDM Line Card with Soft Decision FEC or the Cisco NCS 2000 200-Gbps Multirate DWDM Line Card to efficiently multiplex 10- and 40-Gbps signals into a 100-Gbps coherent DWDM interface (Figure 3). Encryption and authentication can optionally be applied to the aggregated payload.

Figure 3. 100-Gbps Muxponder Client



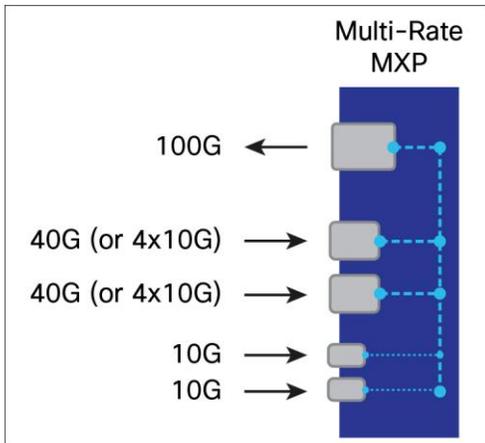
100-Gbps Transponder Client - The line card can be paired with the Cisco NCS 2000 100-Gbps DWDM Line Card with Soft Decision FEC or the Cisco NCS 2000 200-Gbps Multirate DWDM Line Card to transport 100-Gbps signals over a coherent DWDM interface (Figure 4). This mode is primarily intended for encryption and authentication of the 100-Gbps payload, as an unencrypted 100-Gbps client can use the DWDM line card's integrated CPAK interface.

Figure 4. 100-Gbps Transponder Client



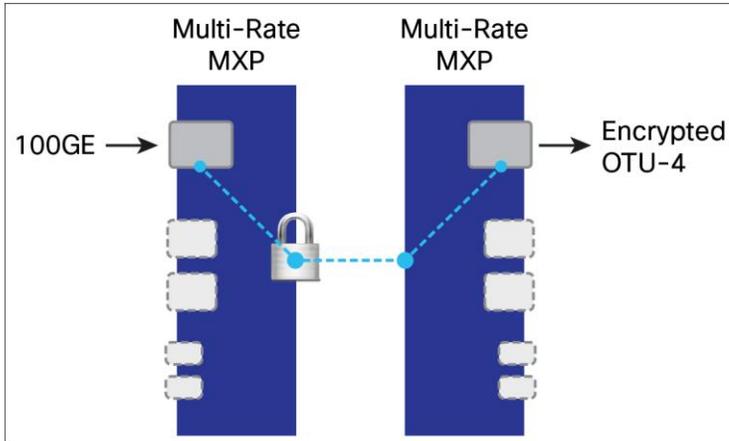
Standalone Muxponder - The line card can operate in a standalone mode in which 10- and 40-Gbps client signals are aggregated into an OTU-4 utilizing the CPAK client interface. This mode could be used to transport the output of the Cisco NCS 2000 100-Gbps Multirate Muxponder over dark fiber or a third-party DWDM system.

Figure 5. Standalone Muxponder



Back-to-Back 100-Gbps Encryptor - By pairing two line cards “back to back” across the chassis backplane, a 100 Gigabit Ethernet client can be encapsulated into an ODU-4, encrypted, transmitted across the chassis backplane, and retransmitted as an OTU-4 using a Cisco CPAK on the paired line card (Figure 6). This allows you to transport the signal over dark fiber or interface with third-party DWDM systems.

Figure 6. Back-to-Back 100-Gbps Encryptor



Flexible Client Support

The Cisco NCS 2000 100-Gbps Multirate Muxponder supports a wide range of client interfaces through its Cisco CPAK, QSFP+, and SFP+ interfaces. The Cisco CPAK supports 100-Gbps signals including 100 Gigabit Ethernet and OTU-4, in standards-compliant short-reach and long-reach variants. QSFP+ ports can interface with 40-Gbps clients, such as 40 Gigabit Ethernet, OTU-3, and OC-768/STM-256, as well as four 10-Gigabit clients using the appropriate pluggable transceiver and breakout cable. In combination with the two SFP+ ports, this allows the line card to aggregate any combination of 10- and 40-Gbps clients up to the total 100-Gbps payload. Please refer to Table 2 for a complete list of supported client protocols.

Encryption

The Cisco NCS 2000 100-Gbps Multirate Muxponder provides protocol-agnostic, wire-speed encryption over a 100-Gbps ODU-4 payload. Encryption functionality is engineered in collaboration with Cisco's Trustworthy Systems Technologies group, promoting a highly robust architecture and adherence to product security development best practices, including:

- **Immutable identity:** Cryptographically assertable, hardware-based identity through X.509 certificates deters counterfeiting and provides standardized network identification.
- **Boot-time integrity:** Boot verification is rooted in hardware to help ensure that only authentic Cisco software boots and that its integrity is intact.
- **Load-time integrity:** This is achieved through the digital image signing process, which involves signing a software package and verifying the signature on the image during the equipment boot process.
- **Secure control plane:** The key exchange between the encryption cards uses the G.709 GCC2 channel, which is secured using Transport Layer Security (TLS).
- **Secure data plane:** The confidentiality of the data is protected through TLS-based encryption, its integrity through authentication, and its availability through multiple optical protection mechanisms.

The Cisco NCS 2000 100-Gbps Multirate Muxponder will undergo the following government certifications to meet mission-critical requirements.

- Federal Information Processing Standard (FIPS) 140-2 Level 2 validation
- Common Criteria Network Device Protection Profile (NDPP) compliance
- Unified Capabilities Approved Products List (UC-APL)

Feature Availability

Availability of features is dependent upon the software release. Please refer to the [Cisco NCS 2002 and NCS 2006 Line Card Configuration Guide](#) for specific feature availability.

Product Specifications

Product specifications for the Cisco NCS 2000 100-Gbps Multi-Rate Muxponder are provided in Table 1.

Table 1. Regulatory Compliance

ANSI System	ETSI System
Countries and Regions 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)

ANSI System	ETSI System
	<ul style="list-style-type: none"> • 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)
Safety	
<ul style="list-style-type: none"> • CSA C22.2 #60950-1 - Edition 7, March 2007 • UL 60950-1 - Edition 2, December 2011 • GR-1089-CORE Issue 6, NEBS EMC and Safety, May 2011 	<ul style="list-style-type: none"> • IEC 60950-1 Information technology equipment Safety Part 1: General requirements - Edition 2, 2005 + Amendment 1 2009 • EN 60950-1: Edition 2 (2006) Information technology equipment - Safety - Part 1: General requirements + A11:2009 + A1:2010 + A12:2011. • CE Safety Directive: 2006/95/EC
Laser	
<ul style="list-style-type: none"> • 21CFR1040 (2008/04) (Accession Letter and CDRH Report) Guidance for Industry and FDA Staff (Laser Notice No. 50), June 2007 	<ul style="list-style-type: none"> • IEC 60825-1: 2007 Ed. 2.0 Safety of laser products Part 1: Equipment classification, requirements and users guide • IEC60825-2 Ed.3.2 (2010) Safety of laser products Part 2: Safety of optical fibre communication systems.
Environmental	
<ul style="list-style-type: none"> • GR-63-CORE Issue 4, Network Equipment Building Standards (NEBS) Physical Protection, April 2012 	<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 6 May 2011, NEBS EMC and Safety • GR-63-CORE Issue 4 April 2012, NEBS Physical Protection • ATT-TP-76200: 2008 • ANSI T1.315-2001 • GR-499: 2004 Transport Systems Generic Requirements (TSGR): Common Requirements 	

Table 2. Client Payload Mapping

Client		Mapping
Format	Rate (Gbps)	
10GE LAN-PHY	10.3125	BMP mapped into OPU2e (with frame stuffing bits, per G.709 17.2.4 & G.Sup43 7.1)
	10.3125	GFP-F clause 17.4.1 (ex G sup43 7.3) + GMP ODU2 to OPU3e4
OC-192/STM-64	9.953	CBR-BMP clause 17.2.2 (Sync) + GMP ODU2 to OPU3e4
10G FC	10.518	513b Transc + AMP GFP-F clause 17.8.2 + GMP ODU2e to OPU3e4
8G FC	8.500	CBR-BMP clause 17.9 (OduFlex) + GMP ODU2 to OPU3e4
OTU2	10.709	ODU transparent + GMP ODU2 to OPU3e4
OTU2e	11.096	ODU transparent + GMP ODU2 to OPU3e4
OC-768/STM-256	39.813	BMP mapped into OPU3 (fixed stuff, CBR40G per G.709 17.2.3) PTI=3
40 Gigabit Ethernet	41.250	Transcoded and GMP mapped into OPU3 (per G.709 17.7.4.1, Annex B, Appendix VII & VIII)
OTU-3	43.018	Transparent G.709 standard
100 Gigabit Ethernet	103.125	GMP mapped into OPU4 (fixed stuff, per G.709 17.7.5)
OTU-4	111.809	Transparent G.709 standard

Performance Monitoring

Ethernet interfaces support the following remote network monitoring (RMON) counters listed in Table 3.

Table 3. RMON Counters Supported by Ethernet Interfaces

Counter	Description
rxTotalPkts	Good frames that are successfully received from the client line interface by the device
etherStatsPkts	Total number of frames received on an interface (The received is referred to a probe on the interface so count both Rx and Tx directions.)
etherStatsOctets	The total number of octets of data, including those in good and bad frames, received from the client line side by the device (This count excludes Preamble byte(s) SFD and Extension byte(s) but includes the Destination and Source addresses, Length/Type field, Q-tag prefix, MAC client data/pad and FCS.)
etherStatsOversizePkts	Good jumbo-frames that are successfully received from the client line interface by the device (Jumbo frames are frames of length 1519 to the configured Max frame size.)
dot3StatsFCSErrors	Receive frames that are an integral number of octets in length and do not pass the FCS check
dot3StatsAlignmentErrors	Receive frames that are not an integral number of octets in length and do not pass the FCS check
dot3StatsSymbolErrors	Received frames that have an associated RX_ER assertion during a data reception error event (MII) or data reception error event or carrier extension error (GMII) from the PCS
dot3StatsFramesTooLong	Receive frames that exceed the maximum permitted frame size, as programmed, and had no other errors
etherStatsJabbers	Receive frames that exceed the maximum permitted frame size, as programmed, and had a bad Frame Check Sequence (FCS)
etherStatsUndersizePkts	Receive frames containing less than the minimum permitted frame size, as programmed, and had no other errors
etherStatsFragments	Receive frames containing less than the minimum permitted frame size, as programmed, and had a bad Frame Check Sequence (FCS)
etherStatsPkts64Octets	Good and bad frames received that were 64 octets in length (excluding framing bits but including FCS)
etherStatsPkts65to127Octets	Good and bad frames received that were between 65 and 127 octets in length (excluding framing bits but including FCS)
etherStatsPkts128to255Octets	Good and bad frames received that were between 128 and 255 octets in length (excluding framing bits but including FCS)
etherStatsPkts256to511Octets	Good and bad frames received that were between 256 and 511 octets in length (excluding framing bits but including FCS)
etherStatsPkts512to1023Octets	Good and bad frames received that were between 512 and 1023 octets in length (excluding framing bits but including FCS)
etherStatsPkts1024to1518Octets	Good and bad frames received that were between 1024 and 1518 octets in length (excluding framing bits but including FCS)
ifInUcastPkts	Good frames that are successfully received and are directed to a unicast group address
ifInMulticastPkts	Good frames that are successfully received and are directed to a multicast group address
etherStatsMulticastPkts	Good multicast frames successfully received or transmitted on an interface
ifInBroadcastPkts	Good frames that are successfully received and are directed to a broadcast group address
etherStatsBroadcastPkts	Good broadcast frames successfully received or transmitted on an interface.
ifInErrors	The sum for this interface of dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs, dot3StatsInternalMacReceiveErrors and dot3StatsSymbolErrors.
IfOutUcastPkts	Good frames that were successfully transmitted to a unicast group destination address
IfOutMulticastPkts	Good frames that were successfully transmitted to a multicast group destination address
IfOutBroadcastPkts	Good frames that were successfully transmitted to a Broadcast group destination address
etherStatsPkts1519toMaxSizeOctets	Good and bad frames received that were between 1519 octets in length and the maximum frame size as programmed within the RMAC Max Frame Length Configuration Register (excluding framing bits but including FCS)

Counter	Description
mediaInStatsTXFramesBadCRC	Transmitted frames that are an integral number of octets in length and do not pass the FCS check
mediaInStatsTXShortPkts	Transmitted frames containing less than the minimum permitted frame size as programmed with the transmit MAC Min Frame Length Configuration Register
dot3StatsLCVErrors/mediaInStatsRxLcvErrors	Received line code violations at the PCS layer
dot3StatsLayer1Errors	Number of Layer 1 errors as defined within the following conditions: <ul style="list-style-type: none"> • During Packet Reception - Layer 1 errors are counted only one time per packet. The error is indicated as a direct result of a line side protocol violation in which RX_DV is asserted. This is an uncommon event that could be the reason why a device loses synchronization. • During Interpacket Reception - The Layer 1 error is indicated as a direct result of a line side protocol violation in which RX_DV is deasserted. This is an uncommon event. The Layer 1 error is also asserted on detection of a False Carrier indication and an errored byte (interpacket) signal encoding. When the error is asserted during interpacket reception, it is statistically asserted only in the vector.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters
txTotalPkts	Total packets good/bad that are egressing

8- and 10-gigabit Fibre Channel interfaces support the RMON counters listed in Table 4.

Table 4. RMON Counters Supported by 8- and 10-Gigabit Fibre Channel Interfaces

Counter	Description
rxTotalPkts	Receive frame counter: number of received packets
mediaInStatsRxFramesTruncated	Receive undersize frame counter: number of received frames that are too small
mediaInStatsRxFramesTooLong	Receive oversize frame counter: number of received FC packets with length > 2148 (2148 is the maximum length for standard FC packets.)
mediaInStatsRxFrameBadCRC	Receive frame CRC error counter: received frame with bad CRC
ifInOctets	Receive (frame) octets counter: total number of octets received on the interface including framing octet
ifInErrors	Receive total errored frame counter: Receive oversizeCRC me + Receive Undersize Frame + Receive CRC Errored Frame

GFP virtual ports support the RMON counters listed in Table 5.

Table 5. RMON Counters Supported by GFP Virtual Ports

Counters	Description
gfpStatsRxFrame	Number of received GFP frames
gfpStatsTxFrame	Number of transmitted GFP frames
gfpStatsRxCRCErrors	Number of packets received with a payload FCS error
gfpStatsRxOctets	Number of GFP bytes received
gfpStatsTxOctets	Number of GFP bytes transmitted
gfpStatsRxSBitErrors	Sum of all the single bit errors (In the GFP CORE HDR at the GFP-T receiver, these are correctable.)
gfpStatsRxMBitErrors	Sum of all the multiple bit errors (In the GFP CORE HDR at the GFP-T receiver, these are uncorrectable.)
gfpStatsRxTypeInvalid	Number of receive packets dropped due to Client Data Frame UPI errors
gfpStatsCFSRaised	Number of GFP client signal fail frames detected at the GFP-T receiver
gfpStatsLFDRaised	Count of core HEC CRC multiple bit errors Note: This count is only of eHec multiple bit errors when in frame. This can be looked at as a count of when the state machine goes out of frame.
gfpRxCmfFrame	Number of received client management frames

Product specifications for the Cisco NCS 2000 100-Gbps Multirate Muxponder are provided in Table 6.

Table 6. Card Specifications

Management	
Card LEDs	
<ul style="list-style-type: none"> Failure (FAIL) Active/standby (ACT/STBY) Signal fail (SF) 	Red Green/yellow Yellow
Client port LEDs (per port)	
<ul style="list-style-type: none"> Active input signal 	Green
Power (Including Worst-Case Pluggable Optics)	
Typical	130W (25C and -48VDC)
Maximum	150W (55C and -38VDC)
Physical	
Dimensions	Occupies 1 slot
Weight	1.38 kg (3.04 lbs)
Reliability and Availability	
Mean time between failures (MTBF)	550, 440 hrs
Latency (End to End)	
SFP+ or QSFP+ port	46 microseconds
Cisco CPAK client port	29 microseconds
Storage temperature	-40°C to 70°C (-40°F to 158°F)
Operating temperature	
<ul style="list-style-type: none"> Normal Short-term¹ 	0°C to 40°C (32°F to 104°F) -5°C to 55°C (23°F to 131°F)
Relative humidity	
<ul style="list-style-type: none"> Normal Short-term¹ 	5% to 85%, noncondensing 5% to 90% but not to exceed 0.024 kg water/kg of dry air
¹ 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 the NCS 2006 and NCS 2002 chassis.	

System Requirements

System requirements for the Cisco NCS 2000 100-Gbps Multirate Muxponder are provided in Table 7.

Table 7. Cisco NCS 2000 100-Gbps Multi-Rate Muxponder System Requirements

Component	Cisco NCS 2006 or ONS 15454 M6	Cisco NCS 2002 or ONS 15454 M2
Processor	15454-M-TNCE, 15454-M-TSCE, 15454-M-TSC, 15454-M-TNC	15454-M-TNCE, 15454-M-TSCE, 15454-M-TSC, 15454-M-TNC
Shelf Assembly	NCS2006-SA, 15454-M6-SA	NCS2002-SA, 15454-M2-SA
Shelf Door	NCS2006-DDR, 15454-M6-DDR	NCS2002-DDR, 15454-M2-DDR
Fan Tray	15454-M6-FTA2, NCS2006-FTA	15454-M2-FTA2, NCS2002-FTA
Power Supply	NCS2006-DC40 NCS2006-DC NCS2006-DC20 NCS2006-AC 15454-M6-AC2 15454-M6-AC	NCS2002-DC NCS2002-DC-E 15454-M2-DC 15454-M2-DC-E NCS2002-AC 15454-M2-AC

Component	Cisco NCS 2006 or ONS 15454 M6	Cisco NCS 2002 or ONS 15454 M2
System Software	Release 10.3 or later	Release 10.3 or later
Slot Compatibility	2 through 7	2 through 3

Ordering Information

Ordering information for the Cisco NCS 2000 100-Gbps Multirate Muxponder is provided in Table 8 and Table 9.

Table 8. Cisco NCS 2000 100-Gbps Multirate Muxponder Ordering Information

Part Number	Product Description
NCS2K-MR-MXP-LIC	10/40/100G MR Muxponder - Licensable for Encryption

Table 9. Supported Pluggables for the Cisco NCS 2000 100-Gbps Multirate Muxponder

Part Number	Product Description
10G	
ONS-SC+-10G-LR=	SFP+ LR - Commercial Temp
ONS-SC+-10G-SR=	SFP+ SR - Commercial Temp
ONS-SC+-10G-C=	10G full C-Band tunable SFP+, 50GHz, LC
ONS-SC+-10G-EPXX.X	10G EP, SFP+ 15XX.XX, 100 GHz, LC (50 GHz, fixed frequency, 80 channels)
40G	
QSFP-40G-SR4	40GBASE-SR4, 4 lanes, 850 nm MMF
ONS-QSFP-40G-SR4=	40GBASE-SR4 QSFP Transceiver Module with MPO Connector
100G	
CPAK-100G-LR4	100GBASE-LR4 Cisco CPAK Module for SMF
CPAK-100G-SR10	100GBASE-SR10 Cisco CPAK Module for MMF

Warranty Information

The following warranty terms apply to the Cisco Network Convergence System 2000, as well as services you may use during the warranty period. Your formal warranty statement appears in the Cisco Information Packet that accompanies your Cisco product.

- Hardware warranty duration: Five years
- Software warranty duration: One year
- Hardware replacement, repair, or refund procedure: Cisco or our service center will use commercially reasonable efforts to ship a replacement part for delivery within 15 working days after receipt of the defective product at Cisco's site. Actual delivery times of replacement products may vary depending on customer location

Product warranty terms and other information applicable to Cisco products are available at:

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

Cisco and Partner Services

Cisco Services for Migrating Converged IP+Optical Solutions

Services from Cisco and our partners help you get the most value from your investments in Cisco's converged IP+Optical solution, quickly and cost effectively. We can help you design, implement, and validate your solution to speed migration and cutover. Coordinate every step through to interworking. Strengthen your team. And make the most of tomorrow's opportunities. Learn more at <http://www.cisco.com/go/spservices>.

For More Information

Cisco optical solutions have already helped enterprises and service providers around the world reduce costs, simplify service provisioning, and support a wide range of new applications. To find out how Cisco Systems Optical Solutions can help your organization, contact your local account representative, or visit <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)