

Cisco C-NIM-WAN-2X and C-NIM-WAN-4S Module Configuration Guide

Cisco C-NIM-WAN-2X and C-NIM-WAN-4S module 2

Prerequisites 2

Limitation 3

Configure C-NIM-WAN-2X and C-NIM-WAN-4S Network Interface Modules 3

Related Documents 8

Revised: October 27, 2025

Cisco C-NIM-WAN-2X and C-NIM-WAN-4S module

The Cisco C-NIM-WAN-2X and C-NIM-WAN-4S are the next generation Form-factor WAN NIM modules that provide enhanced security, reliability, and performance. The Cisco C-NIM-WAN-2X module provides Small Form-Factor Pluggable Plus (SFP+), 10G and 1 Gigabit connectivity. The Cisco C-NIM-WAN-4S module provides 1 Gigabit SFP connectivity. Cisco C-NIM-WAN-2X and C-NIM-WAN-4S support Layer 3 configurable Ethernet network. The Cisco C-NIM-WAN-2X and C-NIM-WAN-4S modules are supported only in a NIM slot. These modules are supported in the SM-NIM Carrier Adapter in the non-NEBS setup.

Supported platforms

The table provides information about the platforms that support the Cisco C-NIM-WAN-2X and C-NIM-WAN-4S modules.

Platforms	C-NIM-WAN-2X	C-NIM-WAN-4S
C8375-E-G2	Yes	Yes

This chapter includes these topics:

Prerequisites

Cisco IOS XE 17.18.1a or a later release is required to install the Cisco C-NIM-WAN-2X and C-NIM-WAN-4S Network Interface Modules.

To determine the version of Cisco IOS software that is running on your router, log in to the router and enter the **show version** command:

```
Cisco IOS XE Software, Version BLD_V1718_THROTTLE_LATEST_20250513_033132_V17_18_0_38
Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
17.18.20250513:042531 [BLD_V1718_THROTTLE_LATEST_20250513_033132:/nobackup/mcpre/s2c-build-ws 101]
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Mon 12-May-25 21:26 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: v17.15(1.19d).s2.cp.RSA2K
Crestone-1 uptime is 4 minutes
Uptime for this control processor is 5 minutes
System returned to ROM by Reload Command
System image file is "bootflash:c8kg2be-universalk9.17.18.01.0.700_V17_18_0_38.SSA.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
```

```
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

-----------------------------------------------------------------
Technology     Type         Technology-package Technology-package
                            Current           Next Reboot
-----------------------------------------------------------------
Smart License  Subscription advantage          advantage

The current crypto throughput level is 10000 kbps (Aggregate)


Smart Licensing Status: Smart Licensing Using Policy

cisco C8375-E-G2 (1RU) processor with 3703488K/6147K bytes of memory.
Processor board ID FDO2721M02R
Router operating mode: Autonomous
1 Virtual Ethernet interface
4 Gigabit Ethernet interfaces
4 2.5 Gigabit Ethernet interfaces
8 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Configuration register is 0x3922
```

Limitation

This section describes limitations for the Cisco C-NIM-WAN-2X and C-NIM-WAN-4S modules.

- Set the same negotiation setting as peer site (both auto or non-auto) for 1000Base-X based SFP on C-NIM-4X module. If you do not have the same negotiation setting, the link will be down.
- Supports 10G SFP+ WAN MACsec scaling limits to a maximum of 16 peers on port basis. The 1G WAN port supports maximum of 8 peers on port basis.

Configure C-NIM-WAN-2X and C-NIM-WAN-4S Network Interface Modules

This section describes how to configure the Cisco C-NIM-WAN-2X and C-NIM-WAN-4S features and some important concepts about the Cisco C-NIM-WAN-2X and C-NIM-WAN-4S modules:

Features

This section includes features supported on C-NIM-WAN-2X and C-NIM-WAN-4S :

PLIM

A physical layer interface module (PLIM) provides the packet interfaces for the routing system. Optics modules on the PLIM contain ports to which fiber-optic cables are connected. User data is received and transmitted through the PLIM ports.

Configure PLIM

To configure PLIM, perform these steps:

Procedure

Step 1 **enable**

Example:

```
Router>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Router#configure terminal
```

Enters global configuration mode.

Step 3 **interface** *interface-id*

Example:

```
Device(config-if)# interface gigabitethernet 0/1/0
```

Specifies the PLIM interface on which you want to enable multicast routing, and enters interface configuration mode.

Step 4 **plim qos input map ipv4v6 qos-value-based**

Example:

```
Device(config-if)# plim qos input map ipv4v6 qos-value-based
```

Attaches the ingress classification class-map template with the specified interface.

Step 5 **plim qos input map ipv4v6 qos-value 0 - 63 queue strict-priority**

Example:

```
Device(config-if)# plim qos input map ipv4v6 qos-value 0 - 63 queue strict-priority
```

Sets a priority queue on Gigabit Ethernet interface.

Step 6 **exit**

Example:

```
Device(config-if)# exit
```

Exits configuration mode and returns the device to global configuration mode.

WAN MACSec

The WAN MACsec and MKA feature introduces MACsec support on WAN, uplink support, Pre-shared key support for the Macsec Key Agreement protocol (MKA) and Certificate-based MACsec Encryption.

Configure MACsec on the interface

To configure the MACsec on the interface, perform these steps.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **mka policy** *policy-name*

Example:

```
Device(config)# mka policy MKAPolicy
```

Configures an MKA policy.

Step 4 **key-server priority** *key-server-priority*

Example:

```
Device(config-mka-policy)# key-server priority 200
```

(Optional) Configures MKA key server priority.

Step 5 **macsec-cipher-suite** {**gcm-aes-128** | **gcm-aes-256**}

Example:

```
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-256
```

(Optional) Configures cipher suite(s) for secure association key (SAK) derivation. Each of the cipher suite options can be repeated only once, but they can be used in any order.

Step 6 **confidentiality-offset** { **0** | 30 | **50**}

Example:

```
Device(config-mka-policy)# confidentiality-offset 30
```

(Optional) Configures confidentiality offset for MACsec operation.

Step 7 **key chain** *key-chain-name* [**macsec**]

Example:

```
Device(config)# Key chain keychain1 macsec
```

Configures a key chain and enters keychain configuration mode

Step 8 **key** *hex-string*

Example:

```
Device(config-keychain)# key 9ABCD
```

Configures a key and enters keychain key configuration mode.

Note
From Cisco IOS XE Everest Release 16.6.1 onwards, the Connectivity Association Key name (CKN) uses exactly the same string, which is configured as the hex-string for the key. For more information about this behavior change, see the section titled "MKA-PSK: CKN Behavior Change" after this task.

Step 9 **cryptographic-algorithm** {**aes-128-cmac** | **aes-256-cmac**}

Example:

```
Device(config-keychain-key)# cryptographic-algorithm gcm-aes-128
```

Set cryptographic authentication algorithm.

Step 10 **key-string** {[**0** | **6**] *pwd-string* | **7** | *pwd-string*}

Example:

```
Device(config-keychain-key)# key-string 0 pwd
```

Sets the password for a key string.

Step 11 **interface** *type number*

Example:

```
Device(config-if)# interface GigabitEthernet 0/0/0
```

Enters the configuration mode for the specified interface on the router.

Step 12 **ip address** *address mask*

Example:

```
Device(config-if)# ip address 101.1.1.1 255.255.255.0
```

Sets the IP address and subnet mask for the specified interface.

Step 13 **mka policy** *policy-name*

Example:

```
Device(config-if)# mka policy MKAPolicy
```

Configures an MKA policy.

Step 14 **mka pre-shared-key key-chain** *key-chain-name*

Example:

```
Device(config-if)# mka pre-shared-key key-chain key-chain-name
```

Configures an MKA pre-shared-key key-chain keychain1

Note
The MKA Pre-shared key can be configured on either physical interface or subinterfaces and not on both physical and subinterfaces.

Step 15 **macsec**

Example:

```
Device(config-if)# macsec
```

Enables the MACsec under the interface.

Step 16 **end**

Example:

```
Device(config-mka-policy)# end
```

Returns to privileged EXEC mode.

Configuring MACsec and MKA on interfaces

To configure MACsec and MKA on an interface, perform these steps:

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** *type number*

Example:

```
Device(config)# interface GigabitEthernet 0/0/0
```

Enters interface configuration mode.

Step 4 **mka policy** *policy-name*

Example:

```
Device(config-if)# mka policy MKAPolicy
```

Configures an MKA policy

Step 5 **mka pre-shared-key key-chain** *key-chain-name*

Example:

```
Device(config-if)# mka pre-shared-key key-chain key-chain-name
```

Configures an MKA pre-shared-key key-chain keychain1

Note
The MKA Pre-shared key can be configured on either physical interface or subinterfaces and not on both physical and subinterfaces.

Step 6 **macsec**

Example:

```
Device(config-if)# macsec
```

Configures MACsec for the EAPOL frame ethernet type.

Step 7 **macsec replay-protection window-size** *window-size number*

Example:

```
Device(config-if)# macsec replay-protection window-size 10
```

Sets the MACsec window size for replay protection.

Step 8 **end**

Example:

```
Device(config-if)# end
```

Returns to privileged EXEC mode.

Related Documents

Related Topic	Document Title
Installing the Cisco Catalyst C-NIM-WAN-2X and C-NIM-WAN-4S Module	Hardware Installation Guide for Cisco C-NIM-WAN-2X and C-NIM-WAN-4S Modules

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.