Cisco DNA Traffic Telemetry Appliance Hardware Installation Guide

First Published: 2020-09-03

Last Modified: 2020-09-08

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **Cisco DNA Traffic Telemetry Appliance Overview** 1

Information About the Cisco DNA Traffic Telemetry Appliance 1

Hardware Features of the Cisco DNA Traffic Telemetry Appliance 2

Cisco DNA Traffic Telemetry Appliance Front View 2

Cisco DNA Traffic Telemetry Appliance LEDs 3

Cisco DNA Traffic Telemetry Appliance Management Connections 4

Cisco DNA Traffic Telemetry Appliance Rear View 4

Cisco DNA Traffic Telemetry Appliance GE Ports 5

Field-Replaceable Units for the Cisco DNA Traffic Telemetry Appliance 5

Cisco Product Identification Standard 6

Unique Device Identifier 6

Serial Number and PID/VID Label Location 7

CHAPTER 2 **Supported Hardware Components** 9

Supported Hardware Components 9

Supported Small Form-Factor Pluggable (SFP and SFP+) Transceivers 10

Supported NIMs 11

NIM-SSD 11

Cisco DNA Traffic Telemetry Appliance Power Supplies 11

Power Supplies for the Cisco DNA Traffic Telemetry Appliance 11

Cisco DNA Traffic Telemetry Appliance Power Supply Fans 12

Cisco DNA Traffic Telemetry Appliance AC Power Supply 12

Cisco DNA Traffic Telemetry Appliance DC Power Supply 13

AC/DC Power System Input Range and Voltage for the Cisco DNA Traffic Telemetry Appliance 14

Power Cords Supported by the Cisco DNA Traffic Telemetry Appliance 14

CHAPTER 3 **Removing and Replacing FRUs** 17

Removing and Replacing the Cisco DNA Traffic Telemetry Appliance Power Supplies 17

Removing AC Power Supplies from the Cisco DNA Traffic Telemetry Appliance 18

Installing AC Power Supplies in the Cisco DNA Traffic Telemetry Appliance 19

Removing DC Input Power from the Cisco DNA Traffic Telemetry Appliance 21

Installing DC Input Power on the Cisco DNA Traffic Telemetry Appliance 21

Wiring the DC Input Power Source 22

Removing and Replacing the Cisco DNA Traffic Telemetry Appliance USB Flash Memory Stick or Secure Token 23

Removing and Replacing the Cisco DNA Traffic Telemetry Appliance DIMM 24

Removing and Replacing the Cisco DNA Traffic Telemetry Appliance DIMM Memory Module 25

Removing a Cisco DNA Traffic Telemetry Appliance DIMM 26

Replacing a Cisco DNA Traffic Telemetry Appliance DIMM 27

Removing and Replacing a NIM on the Cisco DNA Traffic Telemetry Appliance 29

Removing a NIM 30

Replacing a NIM 30

Removing and Replacing an SSD from the NIM-SSD Module 30

Removing an SSD from the NIM-SSD Module 31

Installing an SSD into the NIM-SSD Module 32

Repacking the Appliance 33

CHAPTER 4 **Appliance Specifications** 35

Cisco DNA Traffic Telemetry Appliance Specifications 35

Cisco DNA Traffic Telemetry Appliance Memory and Storage Options 36

CHAPTER 5 **Signals and Pinouts** 37

Management Ethernet Port Signals and Pinouts 37

Console Port Signals and Pinouts 37

Auxiliary Port Signals and Pinouts 38

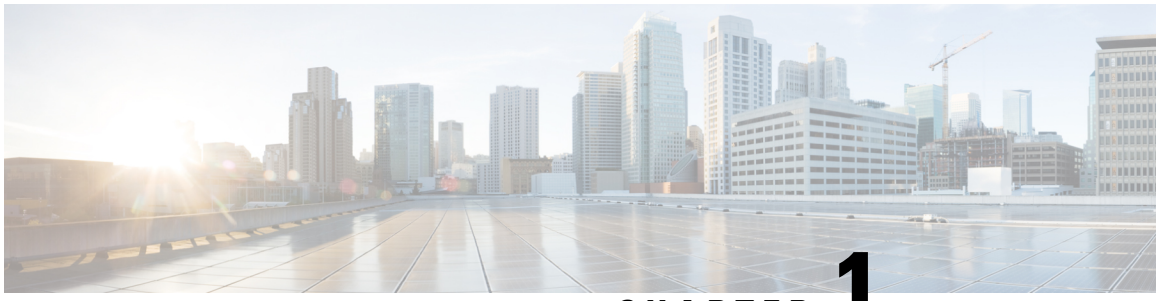
CHAPTER 6 **Upgrading the ROMMON and CPLD** 39

Upgrading the ROMMON 39

Compatibility Requirements 39
Checking the Current ROMMON Version 39
Upgrading the ROMMON for the Cisco DNA Traffic Telemetry Appliance 40
Example: Upgrading a ROMMON 41
Hardware That Requires a CPLD Upgrade 43
Upgrading the CPLD 43
Checking Hardware and Software Compatibility 44
Using Cisco Feature Navigator 44

CHAPTER 7 License Verification 45
Viewing the Cisco IOS License Level 45
Viewing License Information 46

CHAPTER 8 Operating with Cisco DNA Center 47
Configure the Network 47
Configure the Encapsulated Remote Switching Port Analyzer 48
Configure an ERSPAN Source Session 49
Configure an ERSPAN Destination Session 49
Verify Commands and Debug Commands 49
Cisco DNA Traffic Telemetry Appliance Connections 50
Configure Cisco DNA Traffic Telemetry Appliance Network Settings 51



CHAPTER 1

Cisco DNA Traffic Telemetry Appliance Overview

This chapter contains information about the Cisco DNA Traffic Telemetry Appliance, and contains the following sections:

- Information About the Cisco DNA Traffic Telemetry Appliance, on page 1
- Hardware Features of the Cisco DNA Traffic Telemetry Appliance, on page 2
- Field-Replaceable Units for the Cisco DNA Traffic Telemetry Appliance, on page 5
- Cisco Product Identification Standard, on page 6
- Serial Number and PID/VID Label Location, on page 7

Information About the Cisco DNA Traffic Telemetry Appliance

The Cisco DNA Traffic Telemetry Appliance is a telemetry sensor platform that is used to generate telemetry from mirrored IP network traffic and share it with Cisco DNA Center for application and endpoint visibility. Network traffic is received from switches and routers via Switched Port Analyzer (SPAN) mirroring and fed into the Cisco DNA Traffic Telemetry Appliance mirroring interfaces. The Cisco DNA Traffic Telemetry Appliance analyzes the received traffic to produce a telemetry stream for Cisco DNA Center that is sent via the appliance network interface.

The Cisco DNA Traffic Telemetry Appliance offers a compact form factor that consumes less rack space and power.

Table 1: Platform Booting Methods

Boot Method	Booting Command from ROMMON	Supported in IOS XE 17.3.1
Bin boot	rommon> boot bootflash:ttam-universalk9.*.SSA.bin	Yes
Install boot	rommon> boot bootflash:packages.conf	No

Note Install boot is not supported in Cisco IOS XE Amsterdam 17.3.1. The impact of this limitation is the boot time: .bin boot takes more time than the Install boot, because the slower ROMMON retrieves the entire ttam-universalk9.*.SSA.bin from the bootflash to the memory.

Hardware Features of the Cisco DNA Traffic Telemetry Appliance

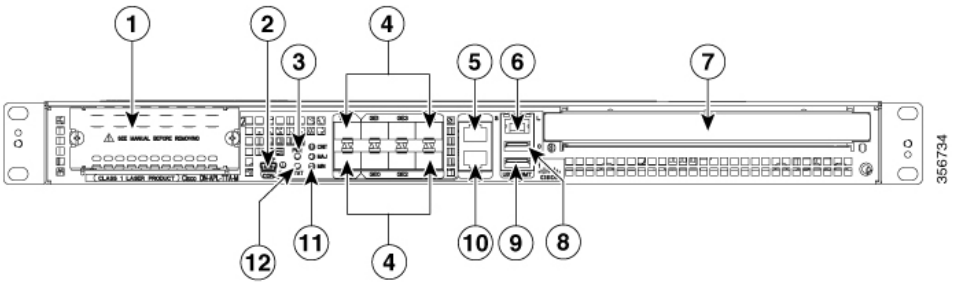
The Cisco DNA Traffic Telemetry Appliance supports these features:

- Up to 16-GB memory configuration of DDR3 error-correcting code-protected field-replaceable memory, with single-bit error correction and multi-bit error detection
- RJ-45 console ports and auxiliary ports, and a mini USB console port
- One copper Ethernet 10/100/1000 Mbps network management port
- An embedded USB (eUSB) flash module that supports 8 GB of nonvolatile flash storage
- Two USB 2.0 ports for USB flash sticks or USB secure tokens (secure key distribution)
- Stratum 3E network clocking per GR-1244-CORE, using 1588, 10 GE, GE, or Network Interface Module (NIM) interfaces as timing sources
- Six built-in 1-GE SFP-only interfaces (do not support SFP+), and two built-in 10-GE SFP+ interfaces (support only 10-GE rate) that support SyncE
- Software redundancy using Dual IOS, similar to all other nonhardware telemetry appliances
- LED indicators for Ethernet and console status, as well as visual system state indications
- Command-line interface (CLI), alarm, network management, logging, statistics aggregation, and onboard failure logging (OBFL)
- Environmental chassis management
- 10 MB ternary content-addressable memory (TCAM)
- Up to 20 Gbps sustained forwarding data traffic through the chassis
- One Network Interface Module (NIM) bay

Cisco DNA Traffic Telemetry Appliance Front View

The following figure shows the front of the Cisco DNA Traffic Telemetry Appliance.

Figure 1: Cisco DNA Traffic Telemetry Appliance Front View

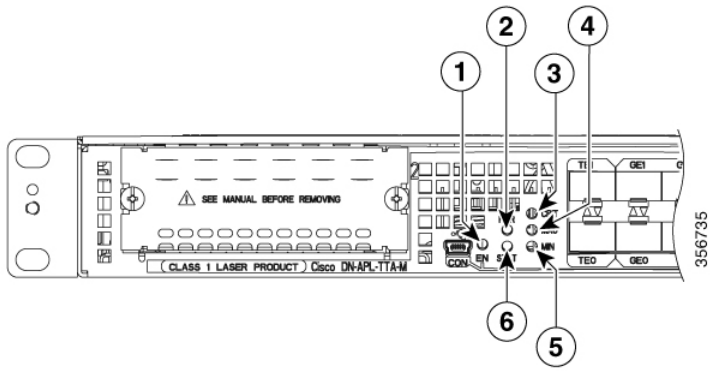


1	NIM slots	7	—
2	CON—One mini eUSB port	8	USB port 0
3	PWR—Power LED	9	USB port 1
4	Six built-in 1 GE SFP-only interfaces (do not support SFP+), and two built-in 10 GE SFP+ interfaces (support only 10-GE rate)	10	CON—One RJ-45/RS-232 compatible console port
5	AUX—One RJ-45/RS-232 compatible auxiliary port	11	CRIT LED—Critical alarm indicator MAJ LED—Major alarm indicator MIN LED—Minor alarm indicator
6	MGMT—One RJ-45 10/100/1000 management Ethernet port. The management port has two LEDs, L and S. L green indicates Link operations. S blinks the negotiated Ethernet speed (1 blink equals 10 Mbps, 2 blinks equals 100 Mbps, 3 blinks equals 1 000 Mbps).	12	STAT—Status LED

Cisco DNA Traffic Telemetry Appliance LEDs

The following figure shows the front panel of the Cisco DNA Traffic Telemetry Appliance:

Figure 2: Common LEDs for the Cisco DNA Traffic Telemetry Appliance



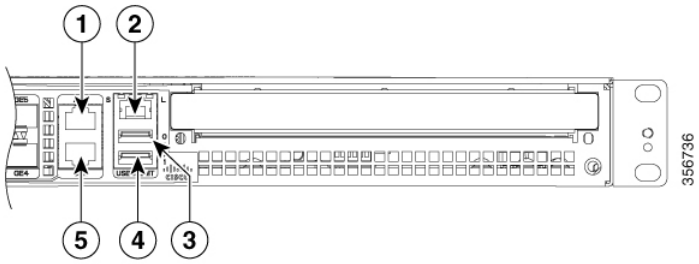
No.	LED Label	LED	Color	Behavior in the Power-Up State
1	PWR	Power	Green	All the power supplies are within operational limits.
2	MAJ	MAJOR	Red	Major alarm indicator.
3	CRIT	CRITICAL	Red	Critical alarm indicator. Will be off when the appliance is initially powered up and all the configured components are available.
4	MIN	MINOR	Amber	Minor alarm indicator

No.	LED Label	LED	Color	Behavior in the Power-Up State
5	STAT	STATUS	Green	Cisco IOS has successfully booted.
			Yellow	The system is at ROMMON.
			Red	System failure. Will be off when the appliance is powered up.
6	EN	USB Console Enable	Green	Indicates that the mini eUSB connector is used as the console.
			Off	Indicates that the RJ-45 connector is being used as the console.

Cisco DNA Traffic Telemetry Appliance Management Connections

The following figure shows the Cisco DNA Traffic Telemetry Appliance's management storage connections.

Figure 3: Management Connections for the Cisco DNA Traffic Telemetry Appliance



1	AUX—One RJ-45/RS-232 compatible auxiliary port.	4	USB port 1
2	MGMT —one RJ-45 10/100/1000 management Ethernet port. The Management Port has two LEDs, L and S. L green indicates Link operations. S blinks the negotiated Ethernet speed (1 blink 10 Mbps, 2 blinks 100 Mbps, 3 blinks, 1 000 Mbps).	5	CON—One RJ-45/RS-232 compatible console port
3	USB port 0		—

Cisco DNA Traffic Telemetry Appliance Rear View

The following figure shows the rear of the Cisco DNA Traffic Telemetry Appliance.

Figure 4: Cisco DNA Traffic Telemetry Appliance Rear View

Four internal fans draw cooling air into the chassis and across internal components to maintain an acceptable operating temperature. The fans are located in the center of the chassis. The fans are numbered from 0 to 3, right to left.

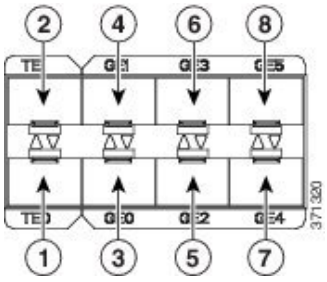
Two power supplies, either two AC power supplies or two DC power supplies, are accessed from the rear of the appliance and are hot-swappable.

Note The Cisco DNA Traffic Telemetry Appliance can support two AC or two DC power supplies. Do not install mixed AC and DC power supply units in the same chassis.

Cisco DNA Traffic Telemetry Appliance GE Ports

The 8-GE SFP+ ports are indicated in the front bezel with orange highlights, and the GE SFP ports are indicated with yellow highlights. The following figure shows the port numbering.

Figure 5: GE Port Numbering



1	8 GE SFP+ Port 0/0/0	5	GE SFP Port 0/0/2
2	8 GE SFP+ Port 0/0/1	6	GE SFP Port 0/0/3
3	GE SFP Port 0/0/0	7	GE SFP Port 0/0/4
4	GE SFP Port 0/0/1	8	GE SFP Port 0/0/5

Field-Replaceable Units for the Cisco DNA Traffic Telemetry Appliance

The Cisco DNA Traffic Telemetry Appliance has a number of FRUs. These include:

- Dual In-line Memory Modules (DIMMs)
- NIMs
- SSD and SSD NIM assembly
- USB flash or secure token memory stick
- AC and DC power supplies

For more information, see the Removing and Replacing FRUs, on page 17 section.

Cisco Product Identification Standard

This section describes the Cisco products and services product identification standard. This feature provides you with the ability to effectively integrate and manage Cisco products in your network and business operations.

Unique Device Identifier

The Unique Device Identifier (UDI) is the Cisco product identification standard for hardware products. A product identification standard removes barriers to enterprise automation and can help you reduce operating expenses.

The UDI provides a consistent electronic, physical, and associated business-to-business information product identification standard.

The UDI is a combination of the data elements shown in the following table.

Table 2: UDI Elements

UDI Data Element	Electronic Visibility	Physical Visibility	Description
PID	Yes	Yes	Product ID, also known as product name, model name, product number
VID	Yes	Yes	Version ID
SN	Yes	Yes	Serial number, the unique instance of the PID
Entity Name	Yes	—	Type, such as chassis, slot, or power supply
Product Description	Yes	—	Additional product information

The combination of serial number and product ID (PID) is unique and consistent across all Cisco products. The PID that is coded on hardware is called a base product identifier.

Additional orderable PIDs can be associated to a base PID. For instance, an orderable PID may describe a packaging configuration for a product or a bundled group of products sold, tested, and shipped together. Specific unique device identifier (UDI) benefits include the following:

- Identifies:
  - Individual Cisco products in your networks
  - PIDs and serial numbers for service and replaceable products
  - Version IDs (VIDs) for product version visibility
- Facilitates discovery of products subject to recall or upgrade
- Enhances inventory automation of Cisco products

The Cisco product identification standard provides the following features:

- Version visibility: Cisco continuously improves products through feature additions. Product changes are indicated by incrementing the VID, which provides version visibility to help you understand and manage product changes. VID management ensures consistency of changes from product to product.
- Operating expense reduction: Cisco UDIs provide accurate and detailed network inventory information; identifying each Cisco product in a network element through a standard interface. Cisco operating systems can view and use this data, allowing you to automate your electronic inventory.
- Consistency across product layers: The UDIs are embedded in the hardware products and cannot be overwritten. Operating and management systems discover UDIs through standard interfaces and display UDIs in standard outputs. Standard interfaces include the IETF standard ENTITY-MIB.

The **show diag subslot eeprom** command displays the PID, VID, PCB serial number, hardware revision, and other such information.

The following is sample output from the **show diag subslot eeprom** command:

```
Device# show diag subslot 0/0 eeprom
MIDPLANE EEPROM data:
        Product Identifier (PID) : DN-APL-TTA-M
        Version Identifier (VID) : V00
        PCB Serial Number        : JAE17450EUV
        Top Assy. Part Number    : 68-4703-06
        Hardware Revision        : 0.1
        Asset ID                 :
        CLEI Code                : CMMP410DRA
```

Note Common Language Equipment Identification (CLEI) code is a ten-digit character code that identifies a specific product. A CLEI code is applied to each part within a Cisco DNA Traffic Telemetry Appliance as they are programmed in manufacturing for shipment to customers.

The **show license udi** command displays UDI information.

The following is sample output from the **show license udi** command:

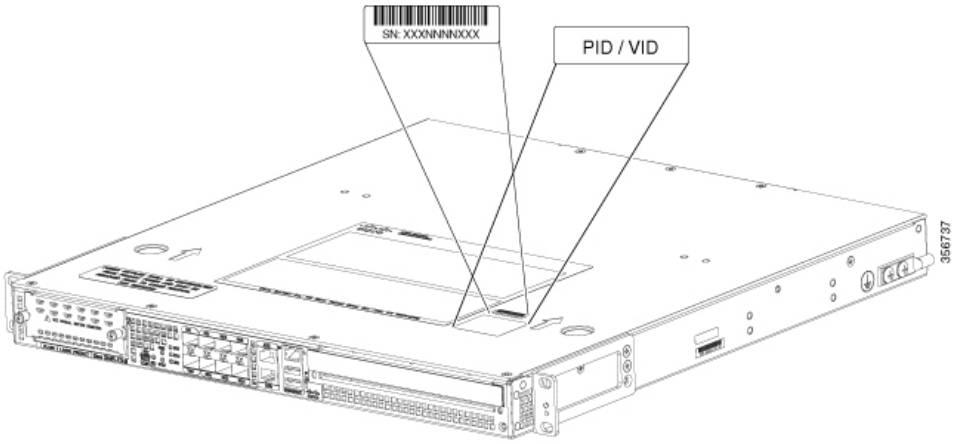
```
Device# show license udi
SlotID   PID                    SN                     UDI
-------------------------------------------------------------------------------
*6       DN-APL-TTA-M            JAE17190302     DN-APL-TTA-M:JAE17190302
```

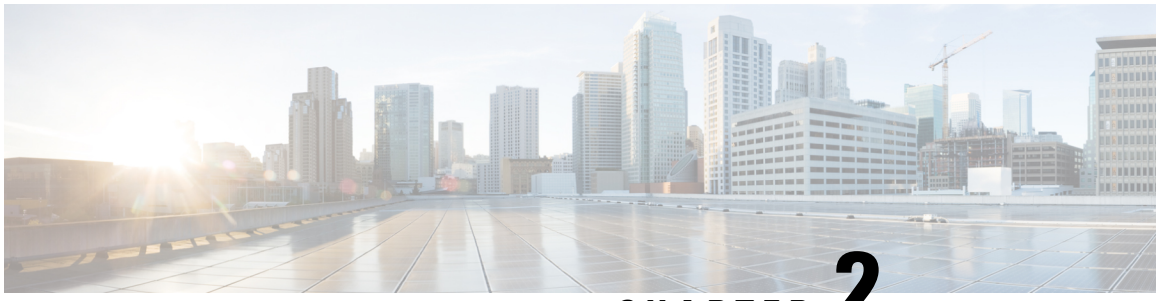
Note For complete information on the product identification standard, see http://www.cisco.com/go/udi/.

Serial Number and PID/VID Label Location

The following figure shows a Cisco DNA Traffic Telemetry Appliance chassis along with the location of the serial number and the PID/VID label.

Figure 6: Cisco DNA Traffic Telemetry Appliance Serial Number and PID/VID Label Location





CHAPTER 2

Supported Hardware Components

This chapter contains information about the supported hardware components on the Cisco DNA Traffic Telemetry Appliance, and contains the following sections:

- Supported Hardware Components, on page 9
- Supported Small Form-Factor Pluggable (SFP and SFP+) Transceivers, on page 10
- Supported NIMs, on page 11
- Cisco DNA Traffic Telemetry Appliance Power Supplies, on page 11

Supported Hardware Components

The following table lists the hardware components supported on the Cisco DNA Traffic Telemetry Appliance.

Table 3: Supported Hardware Components

Component	Description
Chassis	1 RU form factor
Ethernet Ports	Six built-in Gigabit Ethernet and two built-in 10-Gigabit Ethernet ports
ESP	A nonmodular, fixed ESP with a default throughput of 2.5 Gbps, which is upgradable with a software-activated performance license of 5 Gbps, 10 Gbps, or 20 Gbps.
Route Processor	Single integrated route processor
SIP	Integrated SIP
NIM Slots	1
USB Slots	2

Supported Small Form-Factor Pluggable (SFP and SFP+) Transceivers

The following tables list the supported SFP optics and SFP copper interfaces on the Cisco DNA Traffic Telemetry Appliance.

Table 4: Supported 1 GE SFP Optics and SFP Copper Interfaces

PID	Description
SFP-GE-S	1000BASE-SX SFP (DOM)
GLC-SX-MMD	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM
SFP-GE-L	1000BASE-LX/LH SFP (DOM)
GLC-LH-SMD	1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM
SFP-GE-Z	1000BASE-ZX Gigabit Ethernet SFP (DOM)
SFP-GE-T	1000BASE-T SFP (NEBS 3 ESD)
GLC-BX-U	1000BASE-BX SFP, 1310NM
GLC-BX-D	1000BASE-BX SFP, 1490NM
GLC-TE	1000BASE-T SFP transceiver module for category 5 copper wire
GLC-EX-SMD	GE SFP, LC Connector, EX transceiver
GLC-ZX-SMD	1000BASE-ZX SFP transceiver module, SMF, 1550nm, DOM
DWDM-SFP	1000BASE DWDM
CWDM-SFP	1000BASE CWDM
GLC-BX40-D-I	1000BASE BX40-D
GLC-BX40-DA-I	1000BASE BX40-DA
GLC-BX40-U-I	1000BASE BX40-U
GLC-BX80-D-I	1000BASE BX80-D
GLC-BX80-U-I	1000BASE BX80-U
GLC-GE-100FX	100BASE-FX

Note The Cisco DNA Traffic Telemetry Appliance does not support GLC-SX-MM and GLC-LH-SM. You can use GLC-SX-MMD instead of GLC-SX-MM and GLC-LH-SMD instead of GLC-LH-SM.

Table 5: Supported 10 GE SFP Optics and SFP Copper Interface

PID	Description
SFP-10G-SR	10GBASE-SR SFP+ Module for MMF
SFP-10G-SR-X	10GBASE-SR SFP Module for Extended Temp range
SFP-10G-LR	10GBASE-LR SFP+ Module for SMF
SFP-10G-LR-X	10GBASE-LR SFP Module for Extended Temp range
SFP-10G-ER	10GBASE-ER SFP+ Module for SMF

Supported NIMs

The Cisco DNA Traffic Telemetry Appliance supports the following NIM form factors:

NIM-SSD

The following table lists the supported NIM with Solid State Disk (SSD) on the Cisco DNA Traffic Telemetry Appliance:

Table 6: Supported NIM SSDs

Part Number	Description
NIM-SSD	NIM Carrier Card for SSD drives
SSD-SATA-400G	400 GB, SATA Solid State Disk

Cisco DNA Traffic Telemetry Appliance Power Supplies

The Cisco DNA Traffic Telemetry Appliance supports AC and DC power supply options. The modular chassis configurations support the installation of two power supplies for redundancy. When an external power supply fails or is removed, the other power supply provides power requirements for the chassis. This allows you to hot-swap the power supply without impacting the functionality of the appliance.

Power Supplies for the Cisco DNA Traffic Telemetry Appliance

Each Cisco DNA Traffic Telemetry Appliance power supply provides 250 W of output power. The power supplies are used in a 1 + 1 redundant configuration. There is no input switch on the faceplate of the power supplies. A power supply is switched from Standby to On by way of a system chassis STANDBY/ON switch. When facing the rear of the chassis, power supply slot 0 (PS0) is to the left (next to the power supply standby switch) and power supply slot 1(PS1) is to the right.

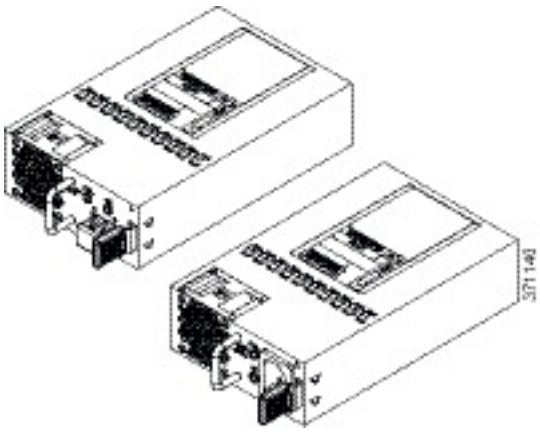
The Cisco DNA Traffic Telemetry Appliance supports the following power supplies:

- ASR1001-X-PWR-AC power supply: Provides 250 W output power with DC voltage output of +12 V. The AC power supply operates between +85 and +264 VAC. The AC power supply current shares on the 12 V output and is used in a dual hot pluggable configuration.
- ASR1001-X-PWR-DC power supply: Provides 242 W output power with DC voltage output of +12 V. The power supply operates between ?40 and ?72 VDC. The DC power supply current shares on the 12 V output and is used in a dual hot-pluggable configuration.

Note The Cisco DNA Traffic Telemetry Appliance can support two AC or two DC power supplies. Do not install mixed AC and DC power supply units in the same chassis.

The following figure shows both the DC and AC power supplies for the Cisco DNA Traffic Telemetry Appliance.

Figure 7: Cisco DNA Traffic Telemetry Appliance DC Power Supply and AC Power Supply



Cisco DNA Traffic Telemetry Appliance Power Supply Fans

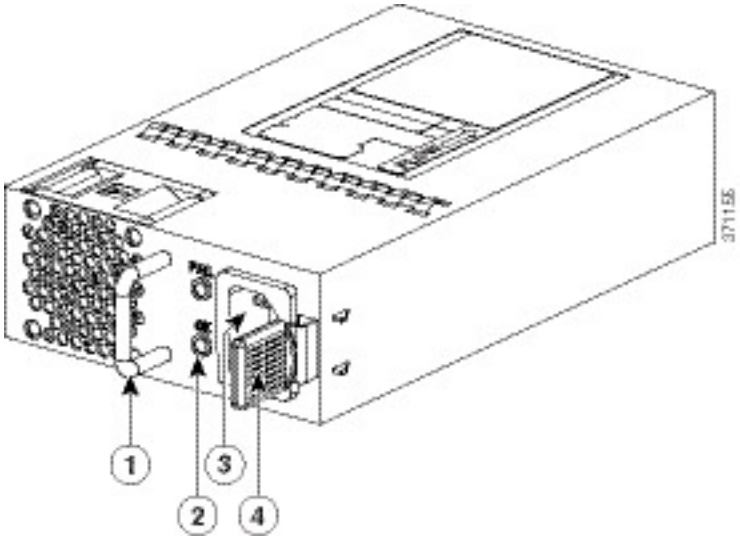
The fans in the power supply module of the Cisco DNA Traffic Telemetry Appliance are used for cooling the power supply module itself while system-level cooling is provided by four fans within the chassis. The power supplies do not depend on the system-level fans for cooling. Fan failure is determined by fan-rotation sensors.

Note The fans in the power supply modules will run as soon as the power supply is plugged in, even if the Standby switch is in the Standby position.

Cisco DNA Traffic Telemetry Appliance AC Power Supply

The Cisco DNA Traffic Telemetry Appliance has two AC power supplies in the rear of the chassis. The input receptacle is an IEC60320 C14 type of filtered AC inlet. The current rating on the connector is 10 A. The following figure shows the Cisco DNA Traffic Telemetry Appliance power supply.

Figure 8: Cisco DNA Traffic Telemetry Appliance AC Power Supply



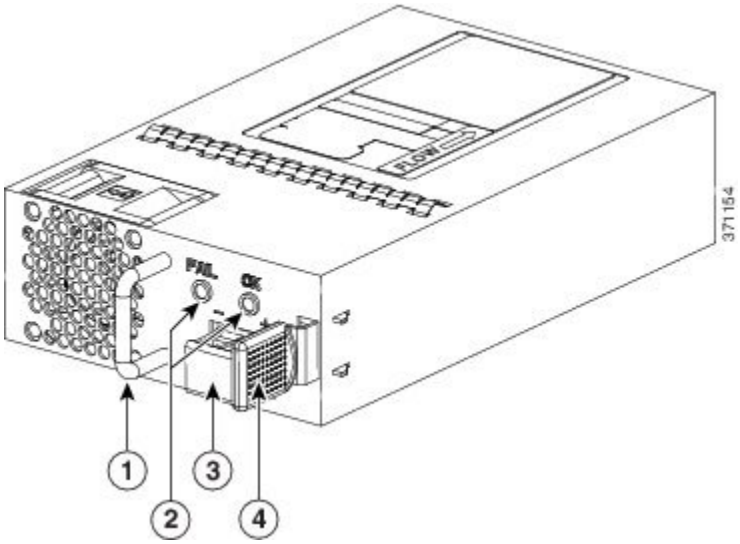
1	Handle	3	AC power connector
2	FAIL and OK LEDs	4	Retaining latch

Cisco DNA Traffic Telemetry Appliance DC Power Supply

The Cisco DNA Traffic Telemetry Appliance DC input connector is a two-wire connector with connection polarity from left to right (when facing the unit) of negative (?) positive (+).

The power supply has a handle to be used for insertion and extraction. The module must be supported with one hand because of its length. The following figure shows the Cisco DNA Traffic Telemetry Appliance DC power supply.

Figure 9: Cisco DNA Traffic Telemetry Appliance DC Power Supply



1	Handle	3	DC power connector
2	FAIL and OK LEDs	4	Retaining latch

AC/DC Power System Input Range and Voltage for the Cisco DNA Traffic Telemetry Appliance

The power supply DC Input Range is –40 to –72 VDC, and the AC Input Range is +85 to +264 VAC. The following table describes the Cisco DNA Traffic Telemetry Appliance power supply LEDs.

Table 7: AC and DC Power Supply LEDs

LED Color and State	Description
OK - (Solid green)	Input power is on and within the normal operating range. On the AC unit, the LED is solid green when the system in powered on. When the system is powered off, the LED will blink until the AC power is removed.
OK - (Blinking Green at the rate of one blink per second)	Input power that is within the normal operating range is being supplied, but the Standby switch is in the Standby position (and not in the On position).
Fail - (Red)	Power output has failed.
Off	Power supply is shut down.

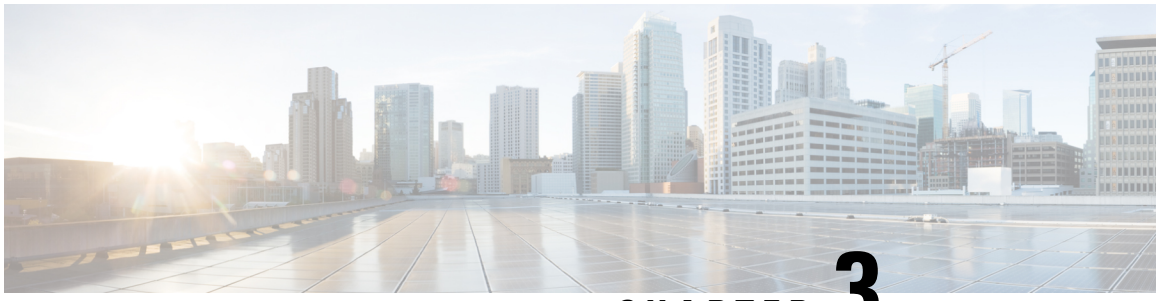
Power Cords Supported by the Cisco DNA Traffic Telemetry Appliance

The following table lists the power cords that are supported by the Cisco DNA Traffic Telemetry Appliance.

Table 8: Power Cords Supported by the Cisco DNA Traffic Telemetry Appliance

Power Cord Item Number	Description
CAB-AC	Power Cord, 110 V
CAB-ACA Plug	Power Cord, Australia, 10 A
CAB-ACC	Power Cord, China
CAB-ACE AC	Power Cord, Europe, C13, CEE 7, 1.5 M
CAB-ACI AC	Power Cord, Italy, C13, CEI 23-16, 2.5 m
CAB-ACR AC	Power Cord, Argentina, C13, EL 219 (IRAM 2073), 2.5m
CAB-ACS AC	Power Cord, Switzerland, C13, IEC 60884-1, 2.5 m
CAB-ACU AC	Power Cord, UK, C13, BS 1363, 2.5 m

Power Cord Item Number	Description
CAB-IND AC	Power Cord, India
CAB-JPN AC	Power Cord, Japan, C13, JIS C 8303, 2.5 m
CAB-L620P-C13-US	Power Cord, 250 VAC, 15A, NEMA L6-20 to C13, U.S.
CAB-L620P-C13-JPN	Power Cord, 250 VAC, 15A, NEMA L6-20 to C13, Japan
CAB-C13-CBN Cabinet Jumper	Power Cord, 250 VAC 10 A, C14-C13 Connectors
CAB-C13-C14-JMPR Cabinet Jumper	Power Cord, 250 VAC 13 A, C14-C15 Connector
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2-Meter Length
CAB-C13-C14-AC	Power Cord Jumper, C13-C14 Connectors, 3-Meter Length



CHAPTER 3

Removing and Replacing FRUs

This chapter describes procedures for removing and replacing field-replaceable units (FRUs) from the Cisco DNA Traffic Telemetry Appliance.

- Removing and Replacing the Cisco DNA Traffic Telemetry Appliance Power Supplies, on page 17
- Removing and Replacing the Cisco DNA Traffic Telemetry Appliance USB Flash Memory Stick or Secure Token, on page 23
- Removing and Replacing the Cisco DNA Traffic Telemetry Appliance DIMM, on page 24
- Removing and Replacing a NIM on the Cisco DNA Traffic Telemetry Appliance, on page 29
- Removing and Replacing an SSD from the NIM-SSD Module, on page 30
- Repacking the Appliance, on page 33

Removing and Replacing the Cisco DNA Traffic Telemetry Appliance Power Supplies

The following sections describes the procedures for removing and replacing the Cisco DNA Traffic Telemetry Appliance power supplies.

Note The Cisco DNA Traffic Telemetry Appliance has redundant power supplies that can be hot-swapped.

Danger The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed. Statement 1077

Danger When you install the unit, the ground connection must always be made first and disconnected last. Statement 1046

Danger Before performing any of the following procedures, ensure that power is removed from the DC circuit. Statement 1003

Danger Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030

Removing AC Power Supplies from the Cisco DNA Traffic Telemetry Appliance

This section describes how to remove an AC power supply from the Cisco DNA Traffic Telemetry Appliance. The appliance has two power supply slots, power supply slot 0 (PS0) next to the Standby switch and power supply slot 1 (PS1) to the right, as shown in the following figures.

Note The appliance has redundant power supplies that can be hot-swapped.

Follow these steps to remove an AC power supply from the appliance:

Step 1 At the rear of the appliance, ensure that the power switch is in the Standby position.

Note It is not required to place the power switch in the Standby position if you want to hot-swap a single power supply.

Step 2 Unplug the power cable from the power supply as shown in the following figure.

Step 3 Press the retaining latch towards the pull handle, grasp the handle with one hand, and pull the power supply out of the slot while supporting the weight of the power supply with the other hand, as shown in the following figure.

Figure 10: Removing the AC Power Supply Cable in Slot PS1

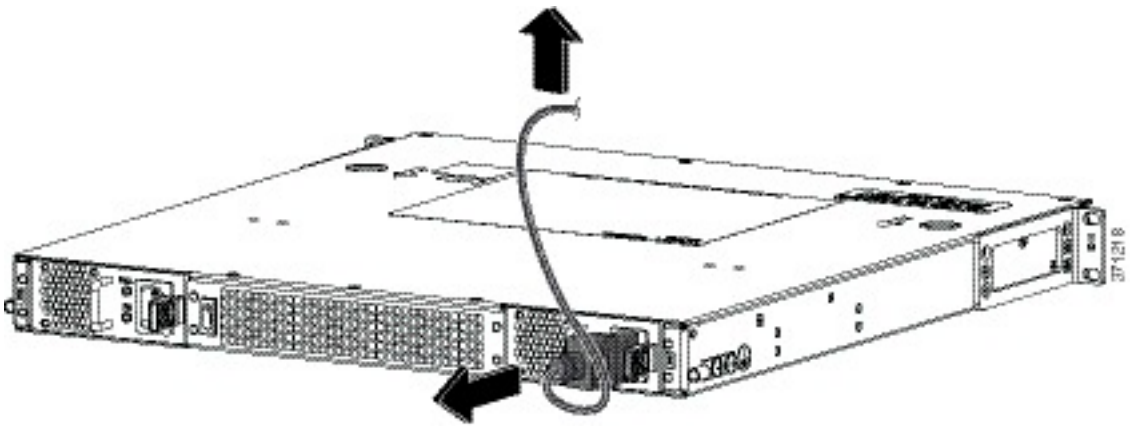
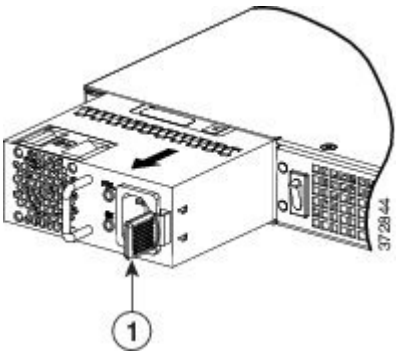


Figure 11: Removing the AC Power Supply



1	Retaining latch

Step 4 Repeat these steps if you want to remove the other AC power supply.

What to do next

This completes the procedure for removing the AC power supplies from the Cisco DNA Traffic Telemetry Appliance.

Installing AC Power Supplies in the Cisco DNA Traffic Telemetry Appliance

Note Do not install the power supplies with the chassis cover off.

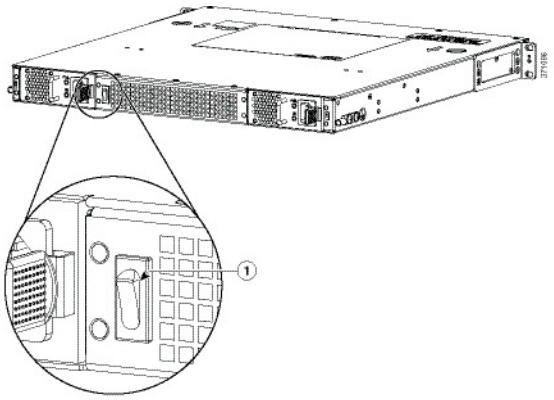
Follow these steps to install AC power supplies in the Cisco DNA Traffic Telemetry Appliance.

Step 1 At the rear of the chassis, ensure that the power switch on the chassis is in the Standby position.

The following figure shows the AC power supply Standby switch.

Note It is not required to place the power switch in the Standby position if you want to hot-swap a single power supply.

Figure 12: AC Power Supply Standby Switch



1	Standby switch, which does not disconnect power from the power source.

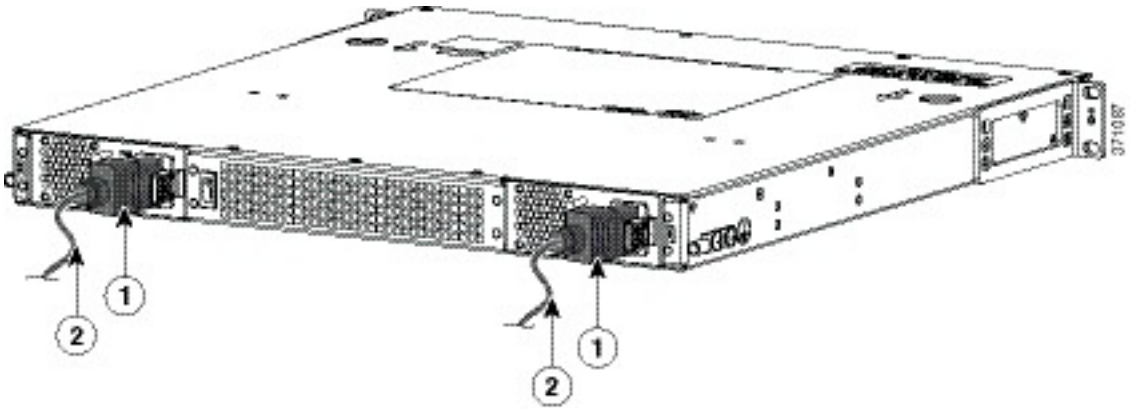
Step 2 Insert the power supply module into the appropriate slot(s), making sure that the retention latch is firmly placed. You can verify that the power supply module is firmly latched by gently pulling the power supply handle.

Step 3 Insert the power supply cables firmly into the power supplies.

Note Ensure that both power supplies are inserted firmly and the power cords are in place.

Step 4 Ensure that the AC power cords are positioned, as shown in the following figure.

Figure 13: Correct Position of the AC Power Supply Cables



1	AC power supply	2	Position of power supply cable

Step 5 If you have changed the Standby switch to the standby position in step 1, turn the Standby switch to the On position.

The power supply LEDs are illuminated (green).

What to do next

This completes the procedure for connecting AC input power.

Removing DC Input Power from the Cisco DNA Traffic Telemetry Appliance

Note The appliance has redundant power supplies that can be hot-swapped.

Follow these steps to remove a DC power supply from the Cisco DNA Traffic Telemetry Appliance.

Step 1 Turn off the circuit breaker from the power source.

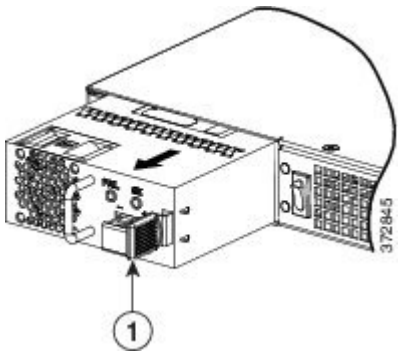
Step 2 At the rear of the appliance, ensure that the power switch is in the Standby position.

Note It is not required to place the power switch in the Standby position if you want to hot-swap a single power supply.

Step 3 Unscrew the two terminal block wire connectors (negative and positive) on the unit. See the following figure.

Step 4 Press the retaining latch towards the pull handle, grasp the handle with one hand, and pull the power supply out of the slot while supporting the weight of the power supply with the other hand. See the following figure.

Figure 14: Removing DC Power Supply



1	Retaining latch

Installing DC Input Power on the Cisco DNA Traffic Telemetry Appliance

Danger Before performing any of the following procedures, ensure that power is removed from the DC circuit. Statement 1003

Danger Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030

This section describes how to install the DC power supply input power leads to the Cisco DNA Traffic Telemetry Appliance DC input power supply. Before you begin, read these important notices:

- The color coding of the DC input power supply leads depends on the color coding of the DC power source at your site. Ensure that the lead color coding you choose for the DC input power supply matches the lead color coding used at the DC power source and verify that the power source is connected to the negative (–) terminal and to the positive (+) terminal on the power supply.
- Ensure that the chassis ground is connected on the chassis before you begin installing the DC power supply. See Attaching a Chassis Ground Connection.

Wiring the DC Input Power Source

The Cisco DNA Traffic Telemetry Appliance DC power supply has a terminal block that is installed into the power supply terminal block header.

Use the following steps to wire the DC input power source:

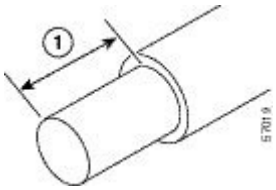
Step 1 Turn off the circuit breaker from the power source.

Step 2 At the rear of the appliance, ensure that the power switch is in the Standby position.

Note It is not required to place the power switch in the Standby position if you want to hot-swap a single power supply.

Step 3 Use a wire-stripping tool to strip each of the two wires coming from the DC input power source and strip the wires to approximately 0.39 inch (10 mm) + 0.02 inch (0.5 mm). Do not strip more than the recommended length of wire because doing so could leave the wire exposed from the terminal block. The following figure shows a stripped DC input power source wire.

Figure 15: Stripped DC Input Power Source Wire



1	0.39 inch (10 mm) is the recommended wire-strip length for the terminal block.

Danger An exposed wire lead from a DC input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC input power source wire extends from the terminal block. Statement 122

Step 4 Identify the positive and negative feed positions for the terminal block connection. The wiring sequence is:

a. Positive (+) lead wire (right)

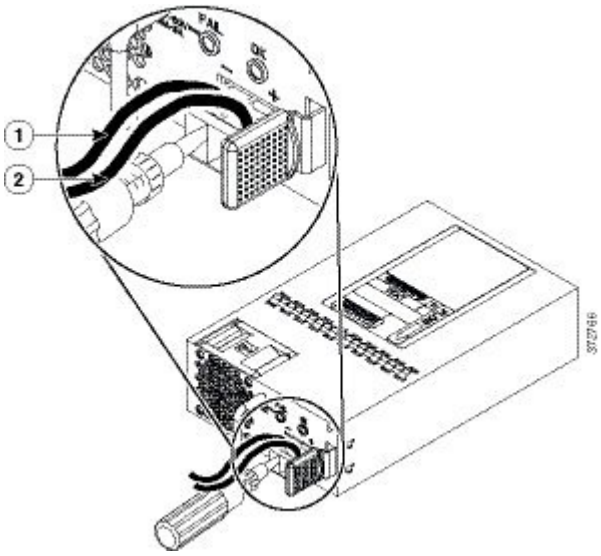
b. Negative (?) lead wire (left)

Step 5 Insert the exposed wire into the terminal block. Ensure that you cannot see any wire lead outside the plastic cover. Only wires with insulation should extend from the terminal block.

Caution Do not overtorque the terminal block captive screws. Ensure that the connection is snug, but the wire is not crushed. Verify by tugging lightly on each wire to ensure that they do not move.

Step 6 Use a screwdriver to tighten the terminal block captive screws, as shown in the following figure.

Figure 16: DC Power Supply with Lead Wires



1	Negative (?) lead wire	2	Positive (+) lead wire

Step 7 Repeat these steps for the remaining DC input power source wire as applicable.

Step 8 Use a tie wrap to secure the wires to the rack, so that the wires are not pulled from the terminal block by casual contact.

Step 9 Turn on the circuit breaker at the power source.

Step 10 If you have changed the Standby switch to the standby position in step 1, turn the Standby switch to the On position.

The power supply LEDs illuminate green.

What to do next

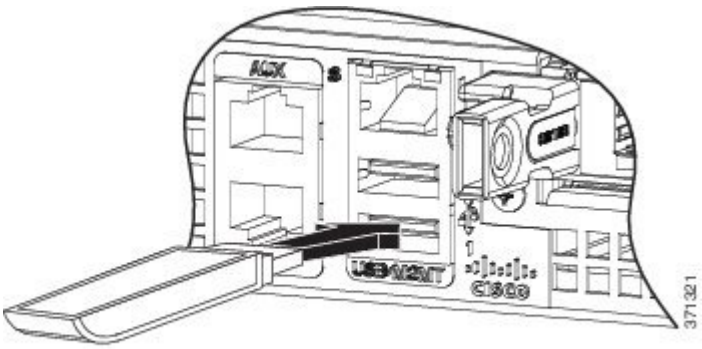
This completes the procedure for connecting the DC power supply in the Cisco DNA Traffic Telemetry Appliance.

Removing and Replacing the Cisco DNA Traffic Telemetry Appliance USB Flash Memory Stick or Secure Token

The Cisco DNA Traffic Telemetry Appliance contains ports for a flash memory stick or a secure token, to store configurations or Cisco IOS XE consolidated packages.

The following figure shows USB port 0 or 1 connector on the Cisco DNA Traffic Telemetry Appliance for the flash memory stick or secure token.

Figure 17: FlashToken Memory Stick Port



Caution Do not remove a USB flash memory stick or secure token when issuing a file access command or a read/write operation to the flash memory stick or secure token when it is processing. The appliance might reload or the USB flash memory stick or secure token may get damaged. Prior to the removal of the USB device, check to see if the USB activity LED on the front panel is flashing.

To remove and then replace a USB flash token memory stick, follow these steps:

Step 1 Pull the flash memory stick or secure token from the USB port.

Step 2 To replace a Cisco USB flash memory stick or secure token, insert the module into USB port 0 or 1, as shown in the preceding figure. The flash memory stick or secure token can be inserted only in one way, and can be inserted or removed regardless of whether the appliance is powered up or not.

This completes the USB flash memory installation procedure.

Removing and Replacing the Cisco DNA Traffic Telemetry Appliance DIMM

This section describes how to replace the DIMMs on the Cisco DNA Traffic Telemetry Appliance.

Note The appliance supports an 8-GB and 16-GB configuration.

You might have to upgrade a DIMM if you upgraded to a new Cisco IOS feature set or release that requires more memory.

Removing and Replacing the Cisco DNA Traffic Telemetry Appliance DIMM Memory Module

Perform the following steps before you begin the process of removing and replacing a DIMM memory module:

- Use an ESD-preventive wrist strap.
- Back up the data that you want to save.
- Remove the power supplies before you remove the chassis top cover.

Caution The top cover cannot be removed until the power supplies are removed from the chassis. The chassis has a safety mechanism built in to prevent the removal of the top cover until the power supplies are removed.

- The DIMM component is keyed and slotted for easier connection.
- The appliance has two DIMM slots.

The following table shows the slots that are supported for inserting the memory DIMMs in the appliance.

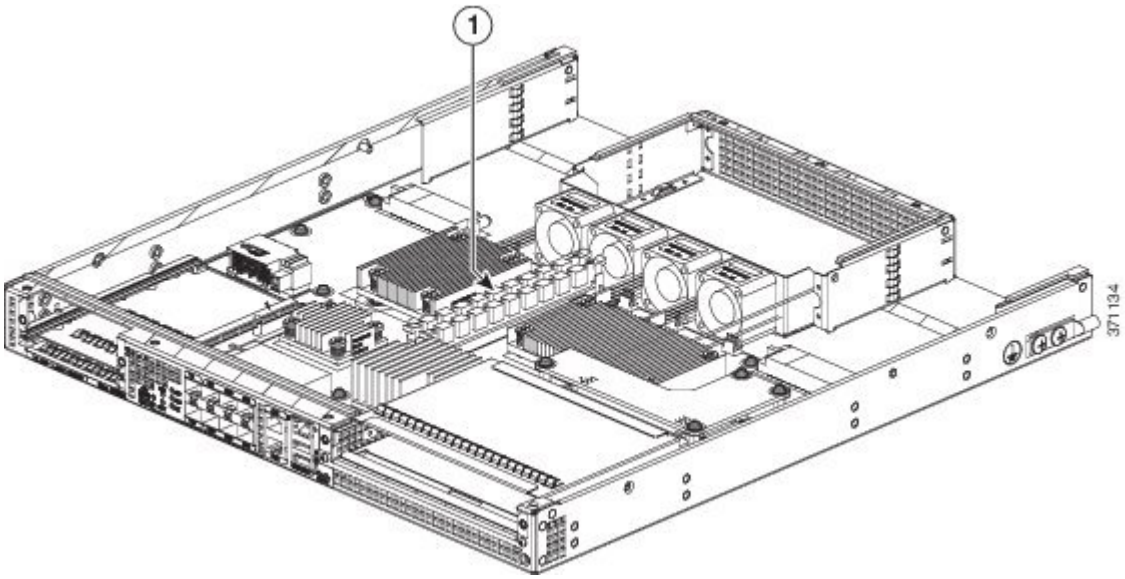
Table 9: Supported Slots for Inserting the DIMMs

Memory PID Option	Slot 0 (U101D)	Slot 1 (U103D)
U1D0	4 GB	4 GB
U1D1	8 GB	8 GB

This section describes how to remove the chassis cover and then remove and replace the DIMMs.

The following figure shows the location of the DIMM slots in the appliance.

Figure 18: Internal Component Location



1	Cisco DNA Traffic Telemetry Appliance DIMM location (two slots)

Removing a Cisco DNA Traffic Telemetry Appliance DIMM

Follow these steps to remove a Cisco DNA Traffic Telemetry Appliance DIMM:

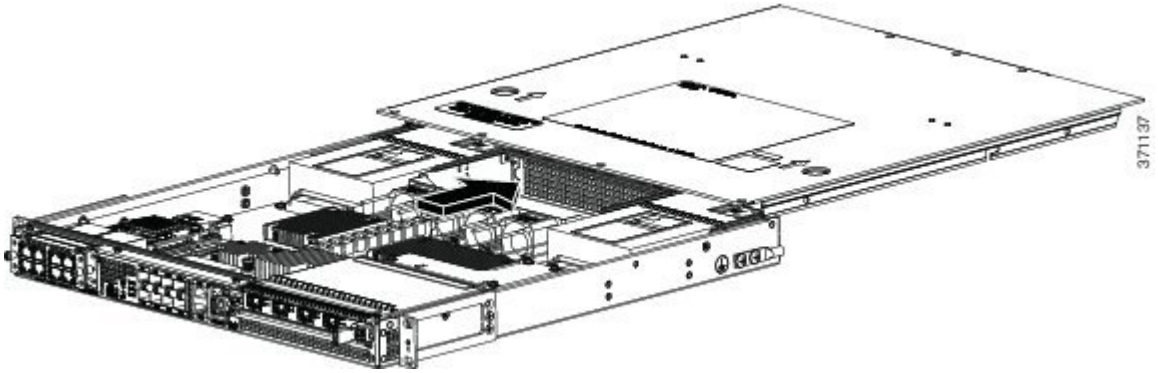
Step 1 With an ESD wrist strap on, remove the power supplies from the chassis.

Note The chassis cover cannot be removed until the power supplies are removed from the chassis.

Step 2 After the power supplies are removed, remove the chassis top cover:

a) Remove all the top surface screws on the chassis cover.
b) Remove the two side screws from the left and the right side of the chassis.
c) Using both hands, gently slide the cover slightly backward and off of the chassis.

Figure 19: Removing the Cover



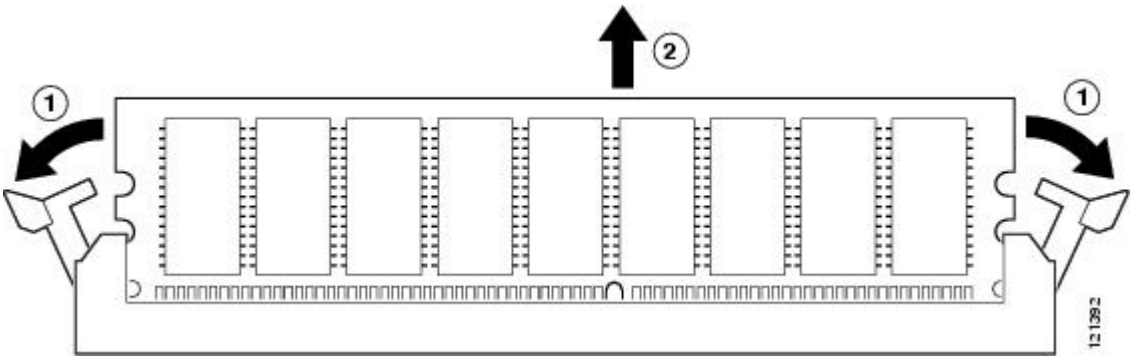
Note The cover will not come off the chassis if the power supplies are present in the chassis.

Step 3 Position the chassis so that you have the most comfortable access to the chassis to remove the DIMM.

Step 4 Locate the DIMMs on the appliance. See the following figure.

Step 5 Pull down the DIMM module spring latches to release the corresponding DIMM from the socket. See the following figure.

Figure 20: DIMM Module Spring Latches to Remove the DIMMs from the Appliance



Step 6 When both ends of the DIMM are released from the socket, grasp each end of the DIMM with your thumb and forefinger and pull the DIMM completely out of the socket. Handle only the edges of the DIMM; avoid touching the memory module, pins, and the metal traces (the metal fingers along the connector edge of the DIMM) along the socket edge.

Step 7 Place the DIMM in an antistatic bag to protect it from ESD damage.

Step 8 Repeat Step 5 through Step 7 for the remaining DIMMs, if required, for your upgrade.

What to do next

This completes the steps for removing the DIMMs from the chassis.

Replacing a Cisco DNA Traffic Telemetry Appliance DIMM

This section lists the steps to replace a DIMM in the Cisco DNA Traffic Telemetry Appliance.

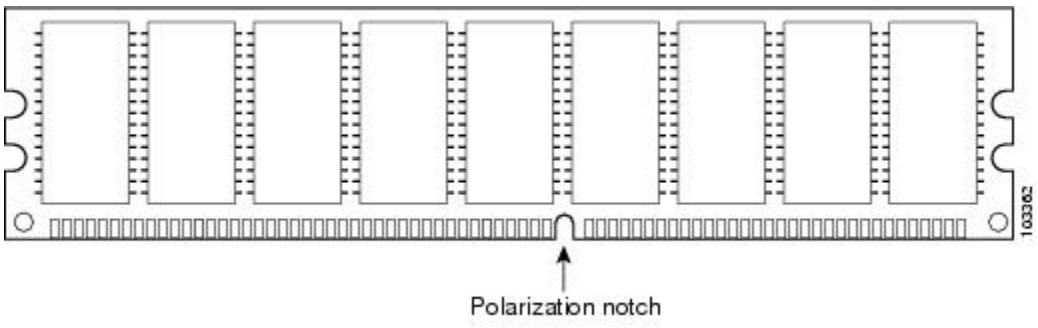
Step 1 Place the DIMM on an antistatic mat or pad while wearing an antistatic device, such as a wrist strap.

Caution DIMMs are sensitive components that can be shorted by mishandling; they are susceptible to ESD damage. Handle the DIMM by the edges only, and avoid touching the pins.

Step 2 Remove the new DIMM from the antistatic bag.

Step 3 Locate the polarization notch and align the DIMM with the socket before inserting it. See the following figure.

Figure 21: DIMM Polarization Notch

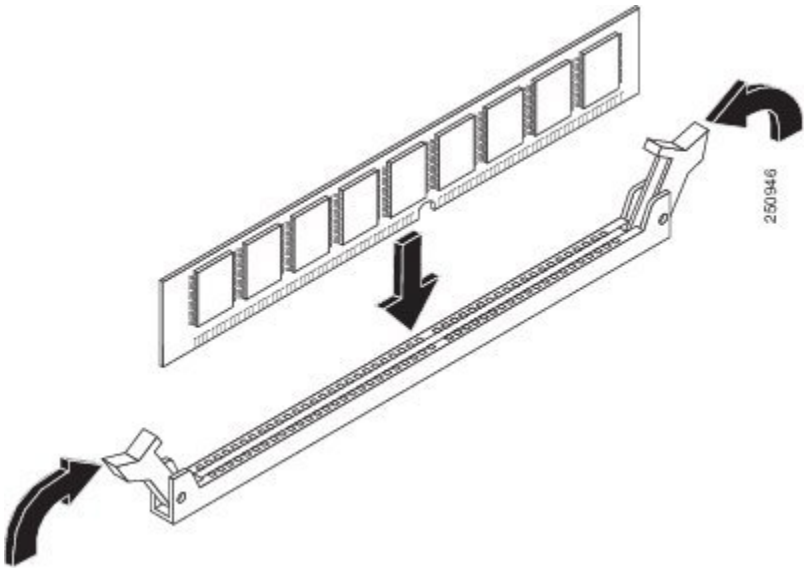


Step 4 Gently insert the new DIMM, taking care not to damage the pins on the edge of the DIMM. Using two hands, hold both sides of DIMM?s top edges with your index fingers and thumbs and gently slide the DIMM straight in to the socket. Press the top of the DIMM towards the socket, being careful to apply force only on the DIMM that is parallel with the plane of the DIMM.

Caution When inserting DIMMs, use firm but not excessive pressure. If you damage a socket, you will have to return the appliance for repair.

Step 5 Use light insertion force and insert smoothly, but ensure that the DIMM is inserted straight. If necessary, rock the DIMM gently back and forth to seat it properly. The following figure shows how to install the DIMM in the socket for the appliance.

Figure 22: Installing a DIMM in the Socket of the Appliance



Step 6 After the DIMM is installed, check whether the release levers are flush against the sides of the DIMM socket. If they are not, the DIMM might not be seated properly. If the DIMM appears misaligned, carefully remove it according to the removal procedure and then reseat it in the socket. Push the DIMM firmly back into the socket until the release levers are flush against the sides of the DIMM socket.

Step 7 Repeat Step 4 through Step 6 for the remaining DIMM.

Step 8 Replace the top cover:

a) Slide the cover onto the chassis ensuring that the interlock hook feature fits on the chassis cover and base.
b) Install the top surface screws and the side screws and tighten them slightly.

Step 9 Install the power supplies in the chassis.

What to do next

This completes the procedure for replacing the DIMM.

After you have correctly installed the DIMMs, the system should reboot properly.

If the system fails to reboot properly or if the console terminal displays a checksum or memory error after you have installed the new DIMMs, ensure that both the DIMMs are installed correctly. If necessary, shut down the system and remove the chassis cover. Check the DIMMs by looking straight down on them to inspect them at eye level. The DIMMs should be aligned at the same angle and the same height when properly installed. If a DIMM appears to stick out or rest in the socket at a different angle from the other, remove the DIMM and reinsert it. Replace the top chassis cover, and reboot the system for another installation check.

Note After several attempts, if the system fails to restart properly, contact a Cisco service representative for assistance. Before you call, make note of any error messages, unusual LED states, or other indications that might help solve the problem.

Removing and Replacing a NIM on the Cisco DNA Traffic Telemetry Appliance

The OIR feature allows you to install and replace a NIM while the appliance is operating. You do not have to shut down the system's power, although you should not run traffic through the NIM while it is being removed. OIR is a method that is seamless to end users on the network.

Note As you disengage the NIM from the appliance, OIR shuts down all the active interfaces in the NIM.

We recommend that you have the following tools and parts readily available for installing a NIM:

- Number 2 Phillips or a 3/16-inch flat-blade screwdriver
- NIM
- Cables
- Your own ESD-prevention equipment or the disposable grounding wrist strap included with all upgrade kits, FRUs, and spares
- Antistatic mat or surface, or static shielding bag

If you need additional equipment, contact a Cisco service representative for ordering information.

Removing a NIM

To remove a NIM, follow these steps.

Step 1 Attach an ESD wrist strap between you and an unpainted chassis surface.

Step 2 Stop the NIM so that there is no traffic running through the NIM when it is removed, using the following steps:

Caution Removing a NIM while traffic is flowing through the ports may cause system disruption.

a) At the # prompt, enter **hw-module subslot 0/2 stop** and press **Enter**.
b) At the # prompt, enter **end** and press **Enter**.

Step 3 Disconnect all the cables from the NIM.

Step 4 Unscrew the captive installation screws on either side of the NIM.

Step 5 Grasp the handles using both hands and pull out the NIM.

You have completed the NIM removal procedure.

Replacing a NIM

To replace a NIM, follow these steps:

Step 1 To insert a NIM, locate the guide rails that hold the NIM in place. They are at the top left and top right of the NIM slot and are recessed about an inch.

Step 2 Carefully slide the NIM all the way in using both hands until the NIM is firmly seated in the NIM interface connector. When fully seated, the NIM might be slightly behind the faceplate.

Step 3 After the NIM is properly seated, fasten the NIM in place with the captive installation screws on either side of the NIM.

Note Ensure that you screw down the captive installation screws to provide appropriate connectivity.

The NIM should power up after installation.

Step 4 Use the **show platform** command to verify whether the status of subslot 0/2 is OK.

You have completed the NIM replacement procedure.

Removing and Replacing an SSD from the NIM-SSD Module

This section explains how to remove a solid state drive (SSD) from the NIM-SSD module.

Caution The NIM-SSD module of the Cisco DNA Traffic Telemetry Appliance recognizes both hard drives as one partition. For example, two 200-GB hard drives are treated as one 400-GB hard drive. Because there is no data backup capability in the NIM-SSD module, replacing any SSD will cause complete data loss. Ensure that you clean up and back up all important data before replacing any SSD.

Restrictions

- The Cisco DNA Traffic Telemetry Appliance does not support dynamic removal and shutdown of SSD drives while the NIM-SSD module is still powered on. Such ungraceful actions may cause disk corruption and you will see kernel messages indicating that the module did not shutdown gracefully. Power down the NIM-SSD module and wait for the power LED to turn off before removing and replacing the SSD.
- Cisco SSD Carrier Card NIM without SSD drives is not supported.

Removing an SSD from the NIM-SSD Module

To remove an SSD from the NIM-SSD module, follow these steps:

Step 1 Access the NIM-SSD slot.

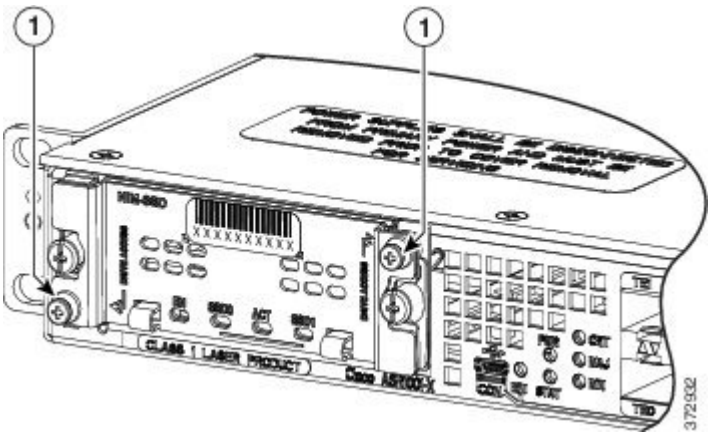
Step 2 Stop the SSD module using the following steps:

a) At the # prompt, enter **hw-module subslot 0/2 stop** and press **Enter**.

b) At the # prompt, enter **end** and press **Enter**.

Step 3 Unscrew the captive installation screws on either side of the NIM-SSD to remove the front faceplate of the NIM, as shown in the following figure.

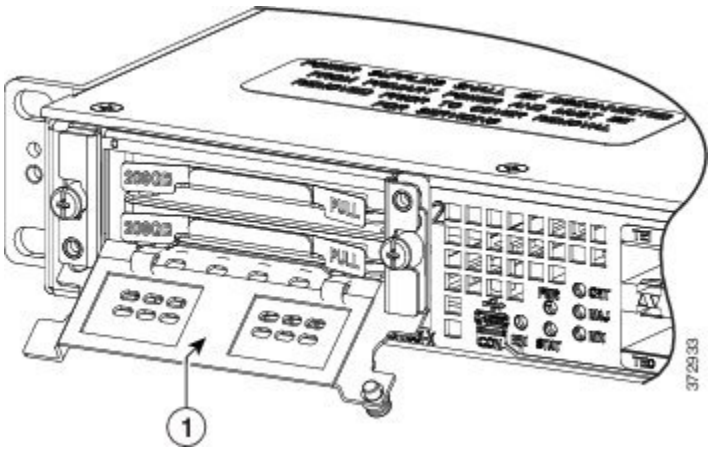
Figure 23: Captive Installation Screws Location



1. Captive screws on the SSD slot cover attaching the SSD drive to the NIM carrier card

Step 4 Pull the NIM-SSD card slot cover down, exposing the SSD slot, as shown in the following figure.

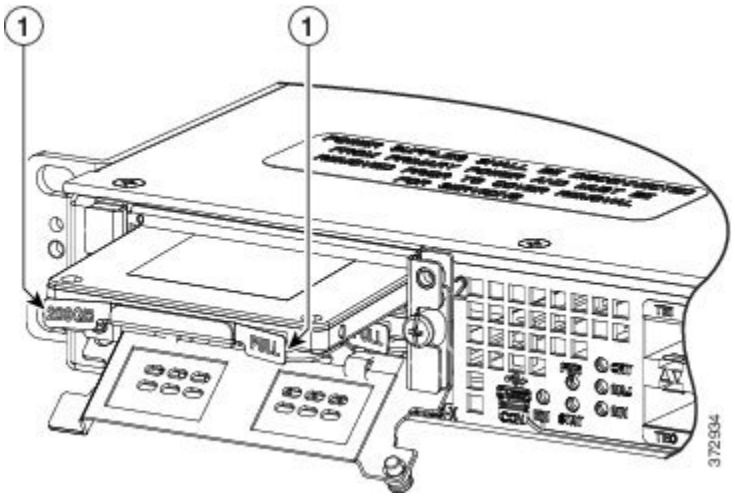
Figure 24: Slot Cover



1. Carrier card slot cover

Step 5 Pull the NIM-SSD out of the connector on the motherboard using both hands, as shown in the following figure. While pulling, keep the NIM-SSD parallel with the motherboard to prevent damage to the slot and the standoff.

Figure 25: Pulling Out the SSD



1. Tabs to pull out the SSD drive

Step 6 Place the NIM-SSD in an antistatic bag to protect it from ESD damage.

This completes the removal of the NIM-SSD.

Installing an SSD into the NIM-SSD Module

To install an SSD into the NIM-SSD module, follow these steps:

Step 1 On the NIM-SSD, loosen the captive screws that retain the SSD card slot cover.

Step 2 Pull the NIM-SSD card slot cover down, exposing the SSD slot.

Step 3 Insert an SSD into the appropriate slot.

Step 4 The SSD(s) connector end should be inserted first, with the connector side facing down and the serial number facing up.

Step 5 Pull the NIM-SSD card slot cover up and into place over the SSD.

Step 6 Verify that the NIM-SSD is installed correctly.

Step 7 Start the NIM-SSD module using the following steps:

a) At the # prompt, enter **hw-module subslot 0/2 start** and press **Enter**.
b) At the # prompt, enter **end** and press **Enter**.

Step 8 Use the **show platform** command and the **show inventory** command to verify whether the status of subslot 0/2 is OK.

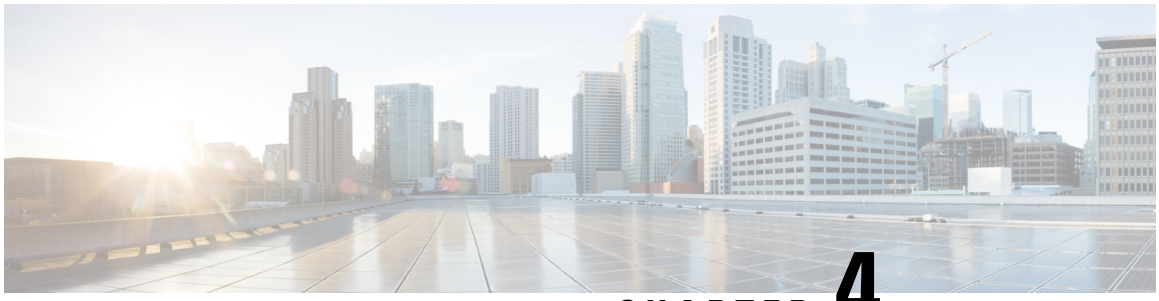
Step 9 Use the **dir hardisk:** command to verify whether the total file size of the hard disk partitions is correct.

You have completed the NIM-SSD replacement procedure.

Repacking the Appliance

If your system is damaged, you must repack it for return shipment.

Before you return the appliance or move it to a different location, repack the system using the original packaging material.



CHAPTER 4

Appliance Specifications

This chapter provides the appliance specifications.

- Cisco DNA Traffic Telemetry Appliance Specifications, on page 35
- Cisco DNA Traffic Telemetry Appliance Memory and Storage Options, on page 36

Cisco DNA Traffic Telemetry Appliance Specifications

The following table lists the Cisco DNA Traffic Telemetry Appliance physical specifications.

Note The Cisco DNA Traffic Telemetry Appliance has the route processor, embedded services processor, and **SIP** integrated in the chassis.

Table 10: Cisco DNA Traffic Telemetry Appliance Specifications

Description	Specification
Dimensions (H x W x D)	Height: 1.71 in. (43.43 mm) Width: 17.3 in. (439.42 mm) Depth: 22.50 in. (571.5 mm) including card handles, cable-management brackets, and power supply handles)
Weight	25 lb fully loaded
Nominal operating temperature	0° to 40° C
Short-term operating temperature	0° to 50° C
Nominal operating humidity	10 to 90% relative humidity
Short-term operating humidity	5 to 90%
Storage temperature	–20° to +70° C

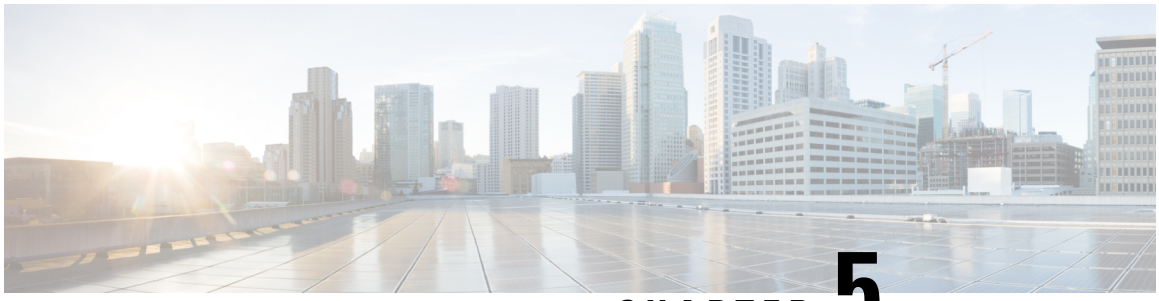
Description	Specification
Power consumption	• Maximum (DC): 242 W • Maximum (AC): 250 W • Maximum (Out): 250 W

Cisco DNA Traffic Telemetry Appliance Memory and Storage Options

The following table lists the hardware memory and storage options supported on the Cisco DNA Traffic Telemetry Appliance.

Table 11: Memory and Storage Options for Cisco DNA Traffic Telemetry Appliance

Memory Type	Default	Maximum System Support
ESP	4 GB DRAM	4 GB DRAM
Route Processor	The Cisco DNA Traffic Telemetry Appliance comes with 8 GB DRAM (default)	16 GB DRAM maximum
External USB flash memory	The Cisco DNA Traffic Telemetry Appliance supports two USB flash memory secure tokens	—
Solid State Drive (SSD)	Two 400-GB SATA SSDs	—



CHAPTER 5

Signals and Pinouts

This chapter provides the Cisco DNA Traffic Telemetry Appliance signals and pinout specifications.

- Management Ethernet Port Signals and Pinouts, on page 37
- Console Port Signals and Pinouts, on page 37
- Auxiliary Port Signals and Pinouts, on page 38

Management Ethernet Port Signals and Pinouts

The following table lists the Management Ethernet 10/100 RJ-45 port pinouts.

Table 12: RJ-45 Management Ethernet Port Pinouts

Pin	Signal	Direction	Description
1	TX/RX AData +	I/O	T/R data +
2	TX/RX AData -	I/Ot	T/R data -
3	TX/RX BData +	I/O	T/R Data +
4	TX/RX CData +	I/O	T/R Data + (Unused for 10/100)
5	TX/RX CData -	I/O	T/R Data - (Unused for 10/100)
6	TX/RX BData -	I/O	T/R Data -
7	TX/RX DData +	I/O	T/R Data + (Unused for 10/100)
8	TX/RX DData -	I/O	T/R Data - (Unused for 10/100)

Console Port Signals and Pinouts

The following table lists the pinouts of the dual RJ-45 ports for the front panel console port.

Table 13: Console Port Pinout for the Cisco DNA Traffic Telemetry Appliance

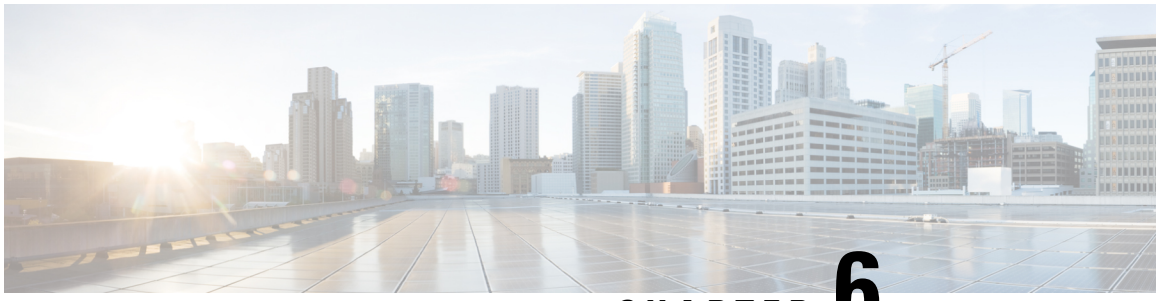
Pin	Signal	Direction	Description
1	RTS	Output	Request to Send (tied to pin 8, CTS)
2	DTR	Output	Data Terminal Ready (always On)
3	TXD	Output	Transmit Data
4	GND	—	Ring Indicator
5	GND	—	—
6	RXD	Input	Receive Data
7	DSR	Input	Unused
8	CTS	Input	Clear to Send (tied to pin 1, RTS)

Auxiliary Port Signals and Pinouts

The following table lists the pinouts of the dual RJ-45 ports for the auxiliary port.

Table 14: Auxiliary Port Pinouts for the Cisco DNA Traffic Telemetry Appliance

Pin	Signal	Direction	Description
1	RTS	Output	Request to Send
2	DTR	Output	Data Terminal Ready (always On)
3	TXD	Output	Transmit Data
4	RI	Input	Ring Indicator
5	GND	—	—
6	RXD	Input	Receive Data
7	DSR/DCD	Input	Data Set Ready/Data Carrier Detect
8	CTS	Input	Clear to Send



CHAPTER 6

Upgrading the ROMMON and CPLD

This chapter describes the procedures to upgrade the ROMMON on the Cisco DNA Traffic Telemetry Appliance.

- Upgrading the ROMMON, on page 39
- Hardware That Requires a CPLD Upgrade, on page 43
- Upgrading the CPLD, on page 43
- Checking Hardware and Software Compatibility, on page 44
- Using Cisco Feature Navigator, on page 44

Upgrading the ROMMON

The ROMMON must be upgraded on the Cisco DNA Traffic Telemetry Appliance if the system message on the appliance indicates that the ROMMON requires an upgrade, or when a Cisco technical support representative suggests a ROMMON upgrade.

Compatibility Requirements

Note For information about the compatibility between the ROMMON releases and the Cisco DNA Traffic Telemetry Appliance, see the "ROMMON Release Requirements " section in the Cisco DNA Traffic Telemetry Appliance Release Notes.

To upgrade the ROMMON image, you must have access to the privileged EXEC mode prompt or the diagnostic mode prompt on the appliance.

Checking the Current ROMMON Version

If you are unsure whether a ROMMON upgrade is required, follow the instructions provided in this section.

Run the **show rom-monitor** command or the **show platform** command to display the version of ROMMON running on your appliance. If the output shows that the release to which you plan to upgrade is already installed, you need not upgrade the ROMMON.

For a single form-factor platform, such as the Cisco DNA Traffic Telemetry Appliance, all of the following commands display the same output:

- **show rom-monitor 0**
- **show rom-monitor F0**
- **show rom-monitor FP**
- **show rom-monitor R0**
- **show rom-monitor RP**

In the following example, the output of the **show rom-monitor** command indicates that an upgrade to Release 15.4(2r)S is not required:

```
Device# show rom-monitor 0
System Bootstrap, Version 15.4(2r)S, RELEASE SOFTWARE (fc1)
Copyright (c) 1994-2014  by cisco Systems, Inc.
```

Upgrading the ROMMON for the Cisco DNA Traffic Telemetry Appliance

Use this procedure to upgrade the ROMMON for the Cisco DNA Traffic Telemetry Appliance:

Step 1 (Optional) Run the **show platform** command or the **show rom-monitor** *slot* command to see the current release number of ROMMON on the hardware.

Step 2 If the ROMMON image has not been copied onto the appliance, copy the PKG file that is made available as part of this ROMMON release onto the bootflash: or usb[0-1]: file system using the **copy** *source-location destination-location* command.

Step 3 Run the **dir** *file-system* command to verify that the ROMMON file is copied into the specified directory.

Step 4 Run the **upgrade rom-monitor filename** *location* **all** command to begin the ROMMON image upgrade, where *location* is the path to the ROMMON file.

Caution Do not remove hardware, turn off power, or interrupt the appliance in any way during the ROMMON upgrade. Although the appliance should be able to recover from most interruptions during the ROMMON upgrade, certain scenarios may cause unpredictable problems.

Step 5 Messages pertaining to the upgrade are displayed on the console. After the display of these messages stops and the device prompt is available, run the **reload** command to reload the appliance.

Note If you change the configuration register setting through Cisco IOS after initiating a ROMMON upgrade, but before reloading the appliance, the configuration register setting will not be applied. Reload the appliance and allow the ROMMON upgrade to be applied prior to changing the configuration register in Cisco IOS.

Step 6 If autoboot has not been enabled by using the **config-register 0x2102** command, run the **boot** *filesystem:/file-location* command at the ROMMON prompt to boot the Cisco IOS XE image, where *filesystem:/file-location* is the path to the consolidated package file. The ROMMON upgrade is not permanent for any piece of hardware until the Cisco IOS XE image is booted.

Note If you enter the **reset** command twice when booting from the ROMMON prompt, the ROMMON upgrade will automatically fall back to the previous ROMMON image. The following message appears after you enter the reset command the second time, and the earlier version of the ROMMON image is installed: Rommon upgrade requestedMaximum upgrade attempts exceeded, continuing with old Rommon...

Step 7 Run the **enable** command at the user prompt to enter the privileged EXEC mode after the boot is complete.

Step 8 Run the **show platform** command or the **show rom-monitor** *slot* command to verify whether the ROMMON has been upgraded.

Example: Upgrading a ROMMON

The following sequence of commands is an example of the procedure to upgrade the ROMMON on a Cisco DNA Traffic Telemetry Appliance:

```
Device# copy tftp boot
Address or name of remote host []? 2.0.0.2
Source filename []? images/nightster/dn-apl-tta-m-rommon.154-2r.S.pkg
Destination filename [dn-apl-tta-m-rommon.154-2r.S.pkg]?
Accessing tftp://2.0.0.2/images/nightster/dn-apl-tta-m-rommon.154-2r.S.pkg...
Loading images/nightster/dn-apl-tta-m-rommon.154-2r.S.pkg from 2.0.0.2 (via GigabitEthernet0):
 !
[OK - 3832112 bytes]
3832112 bytes copied in 1.206 secs (3177539 bytes/sec)
Device# upgrade rom-monitor filename bootflash:dn-apl-tta-m-rommon.154-2r.S.pkg all
Chassis model Cisco DNA Traffic Telemetry Appliance has a single rom-monitor.
Upgrade rom-monitor
Target copying rom-monitor image file
File size : //tmp/rommon_upgrade/latest.bin
File size is : 3211264
FIPS File size is : 3211264
ROMMON Image Type : X86
File /tmp/rommon_upgrade/latest.bin is a FIPS ROMMON image
FIPS-140-3 Load Test on /tmp/rommon_upgrade/latest.bin has PASSED.
Authenticity of the image has been verified.
4259840+0 records in
4259840+0 records out
131072+0 records in
131072+0 records out
655360+0 records in
655360+0 records out
Checking upgrade image...
3211264+0 records in
6272+0 records out
Upgrade image MD5 signature is b806b4bffb47e9be24d26ecd976212e8
Burning upgrade partition...
3211264+0 records in
3211264+0 records out
Checking upgrade partition...
3211264+0 records in
3211264+0 records out
Copying ROMMON environment
4259840+0 records in
4259840+0 records out
131072+0 records in
131072+0 records out
131072+0 records in
131072+0 records out
655360+0 records in
655360+0 records out
Upgrade flash partition MD5 signature is b806b4bffb47e9be24d26ecd976212e8
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the RP.
Device# reload
Proceed with reload? [confirm]
*Mar 24 17:39:33.712 EDT: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
```

```
 Command.Mar 24 17:39:48.058 R0/0: %PMAN-5-EXITACTION: P rocess manager is exiting: process
 exit with reload chassis code
Initializing Hardware ...
System integrity status: 00000610
System Bootstrap, Version 12.2(20140222:162915) [rommon_release_1_49 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2014  by cisco Systems, Inc.
Compiled Sat 02/22/2014  9:10:52.81
Current image running: Boot ROM1
Last reset cause: LocalSoft
DN-APL-TTA-M platform with 8388608 Kbytes of main memory
Rommon upgrade requested
Flash upgrade reset 1 in progress
.......
Initializing Hardware ...
System integrity status: 00000610
System Bootstrap, Version 15.4(2r)S, RELEASE SOFTWARE (fc1)
Copyright (c) 1994-2014  by cisco Systems, Inc.
Current image running: *Upgrade in progress* Boot ROM0
Last reset cause: BootRomUpgrade
***          Incorrect BIOS parameters           ***
*** Correcting the BIOS parameters and rebooting ***
Initializing Hardware ...
System integrity status: 00000610
System Bootstrap, Version 12.2(20140222:162915) [rommon_release_1_49 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2014  by cisco Systems, Inc.
Compiled Sat 02/22/2014  9:10:52.81
Current image running: Boot ROM1
Last reset cause: LocalSoft
DN-APL-TTA-M platform with 8388608 Kbytes of main memory
Rommon upgrade requested
Flash upgrade reset 2 in progress
.......
Initializing Hardware ...
System integrity status: 00000610
System Bootstrap, Version 15.4(2r)S, RELEASE SOFTWARE (fc1)
Copyright (c) 1994-2014  by cisco Systems, Inc.
Current image running: *Upgrade in progress* Boot ROM0
Last reset cause: BootRomUpgrade
DN-APL-TTA-M platform with 8388608 Kbytes of main memory
```

Note From here, you can manually reload from the ROMMON prompt, or let the appliance auto boot directly to Cisco IOS.

The **show platform** command displays the upgraded version of the ROMMON:

```
Device# show platform
Chassis type: DN-APL-TTA-M
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         DN-APL-TTA-M           ok                    17:51:08
0/0      BUILT-IN-2T+6X1GE   ok                    17:50:18
0/1      SPA-1X10GE-L-V2     ok                    17:50:18
R0        DN-APL-TTA-M          ok                     17:51:08
R0/0                          ok, active            17:51:08
R0/1                          ok, standby           17:49:51
F0        DN-APL-TTA-M           ok, active            17:51:08
```

```
P0         ASR1001X-PWR-AC     ok                    17:50:44
P1         ASR1001X-PWR-AC     ok                    17:50:42
P2         ASR1001-X-FANTRAY   ok                    17:50:45
Slot       CPLD Version        Firmware Version
---------  ------------------  ------------------------------------
0          14022717            15.4(2r)S << New ROMmon is confirmed
R0         14022717            15.4(2r)S
F0         14022717            15.4(2r)S
```

Hardware That Requires a CPLD Upgrade

The Cisco DNA Traffic Telemetry Appliance has the capability to allow users to perform Complex Programmable Logic Device (CPLD) upgrades in the field.

For details about Cisco DNA Traffic Telemetry Appliance hardware configuration combinations that require a CPLD field-programmable upgrade for components, see "Upgrading Field Programmable Hardware Devices for Cisco DNA Traffic Telemetry Appliance."

Upgrading the CPLD

To upgrade the CPLD, follow these steps:

Step 1 Copy the **.pkg** file to your bootflash directory.

Step 2 Enter the **upgrade hw-programmable cpld filename bootflash:**<*cpld.pkg*>**RP active** command:

Device# upgrade hw-programmable cpld filename bootflash:nightster_cpld_14041015.pkg RP active

Upgrade CPLD on Route-Processor 0 from current version 13081317 to 14041015 [Press Enter to confirm]

This command could take up to 10 minutes, please wait and do not power-cycle the chassis or the card. Otherwise, hardware may be unrecoverable. The system will be automatically power-cycled upon completion. [Press Enter to confirm]

Note If you decide not to upgrade the CPLD after step 2, press **Ctrl-C** to quit.

Step 3 Press **Enter**.

The appliance upgrades the CPLD, and information is displayed onscreen. The appliance then power cycles and returns to your configuration register-based setting (Cisco IOS boot or ROMMON prompt).

Step 4 To confirm that the upgrade is complete, enter the **show platform** command:

Device# show platform

Chassis type: DN-APL-TTA-M

Slot Type State Insert time (ago)

--------- ------------------- --------------------- -----------------

0 DN-APL-TTA-M ok 2d22h

0/0 BUILT-IN-2T+6X1GE ok 2d20h

R0 DN-APL-TTA-M ok, active 2d22h

F0 DN-APL-TTA-M ok, active 2d22h

P0 ASR1001X-PWR-AC ok 2d22h

P1 ASR1001X-PWR-AC ps, fail 2d22h

P2 ASR1001-X-FANTRAY f1, fail 2d22h

Slot CPLD Version Firmware Version

--------- ------------------- --

0 **14041015** 15.4(2r)S

R0 **14041015** 15.4(2r)S

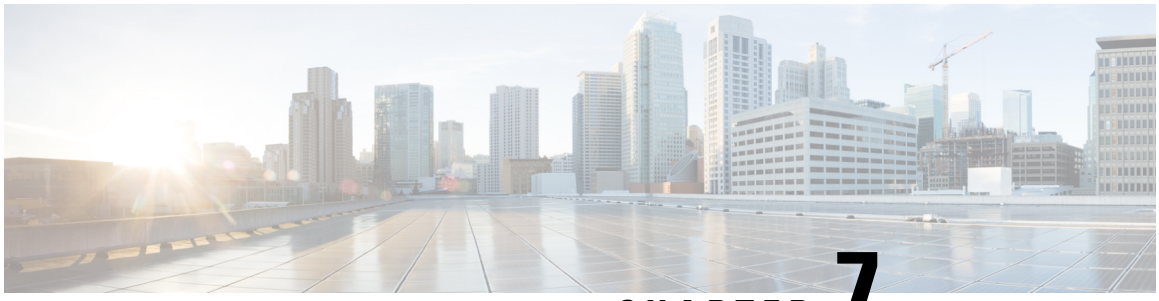
F0 **14041015** 15.4(2r)S

Checking Hardware and Software Compatibility

Cisco software is packaged in feature sets consisting of software images that support specific platforms. The feature sets that are available for a specific platform depend on which Cisco software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, use Cisco Feature Navigator or the corresponding software release notes.

Using Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.



CHAPTER 7

License Verification

This chapter provides information about verifying the Cisco IOS license level and viewing the appliance license.

- Viewing the Cisco IOS License Level, on page 45
- Viewing License Information, on page 46

Viewing the Cisco IOS License Level

Use the **show version** command to determine the Cisco IOS license level in the appliance. For example:

Device# **show version**

.

.

.

License Level: adventerprise

License Type: RightToUse

Next reload license Level: adventerprise

.

Table 15: show version Command Output Description

Field Name	Description
License Level: adventerprise	Indicates the current Cisco IOS license code level.
License Type: RightToUse	Indicates whether you are utilizing a permanent (purchased) license, an evaluation 60-day license, or a Right-to-Use license that would indicate that the purchase of a license is required.
Next reload license Level: adventerprise	Indicates the startup configuration definition that will be used for the next reload instance.

Use the **show running-config** command or the **show startup-config** command to view the license-level information. The following example displays sample output from the **show running-config** command:

Device# **show running-config**

.

.

.

license boot level adventerprise

.

.

Table 16: show running-config Command Output Description

Field Name	Description
license boot level adventerprise	Indicates the current requested Cisco lOS license level to boot.

Viewing License Information

Use the **show license udi** command to determine the Universal Device Identifier (UDI) information of your chassis. This may be required at the time of purchasing a new license. The following example displays sample output from the **show license udi** command:

Device# **show license udi**

UDI: PID:DN-APL-TTA-M,SN:JAE1719030L

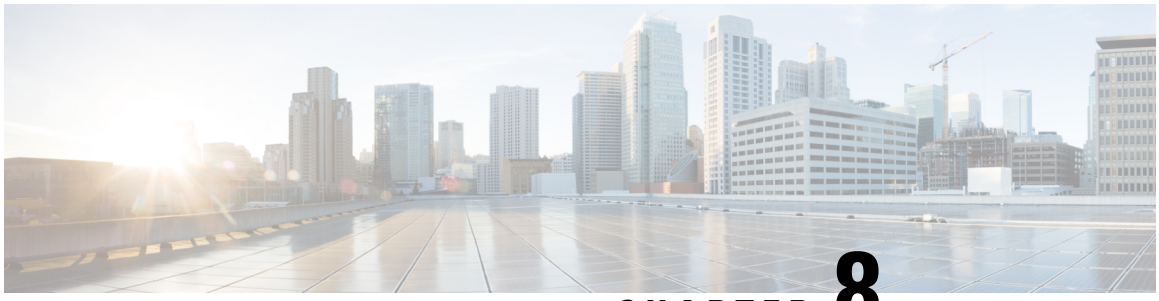
Device# **show license summary**

```
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED

License Authorization:
  Status: AUTHORIZED - RESERVED

License Usage:
  License                Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  Cisco_DNA_TTA_Advantage (DNA_TTA_A)                      1 AUTHORIZED
```



CHAPTER 8

Operating with Cisco DNA Center

This chapter describes how the Cisco DNA Traffic Telemetry Appliance operates with Cisco DNA Center and how to connect the network to the appliance.

- Configure the Network, on page 47
- Configure the Encapsulated Remote Switching Port Analyzer , on page 48
- Cisco DNA Traffic Telemetry Appliance Connections, on page 50
- Configure Cisco DNA Traffic Telemetry Appliance Network Settings, on page 51

Configure the Network

Configure a Span of L2 Traffic

On the organization's network, configure a Layer 2 (L2) aggregation switch, or similar, to span a stream of the L2 traffic to the Cisco DNA Traffic Telemetry Appliance. This must be a distribution layer switch (based on a three-layer networking model of access layer, distribution layer, core layer) in order to include traffic and devices from all segments of the access layer.

The Cisco DNA Traffic Telemetry Appliance uses the span for traffic analysis and device discovery. When configuring the span, include all desired VLANs. For example, you might choose to include all VLANs for the organization's operational traffic, while excluding traffic from a VLAN used for a testing lab. Alternatively, you might include all VLANs.

Example Configuration of Organization's Aggregation Switch

This example, executed on a Cisco switch, configures a span of traffic for VLANs 10, 20, and 30, on gigabitEthernet port 19.

```
switch(config)#monitor session 1 source vlan 10 , 20 , 30 both
switch(config)#monitor session 1 destination interface gigabitEthernet 1/0/19
```

To verify:

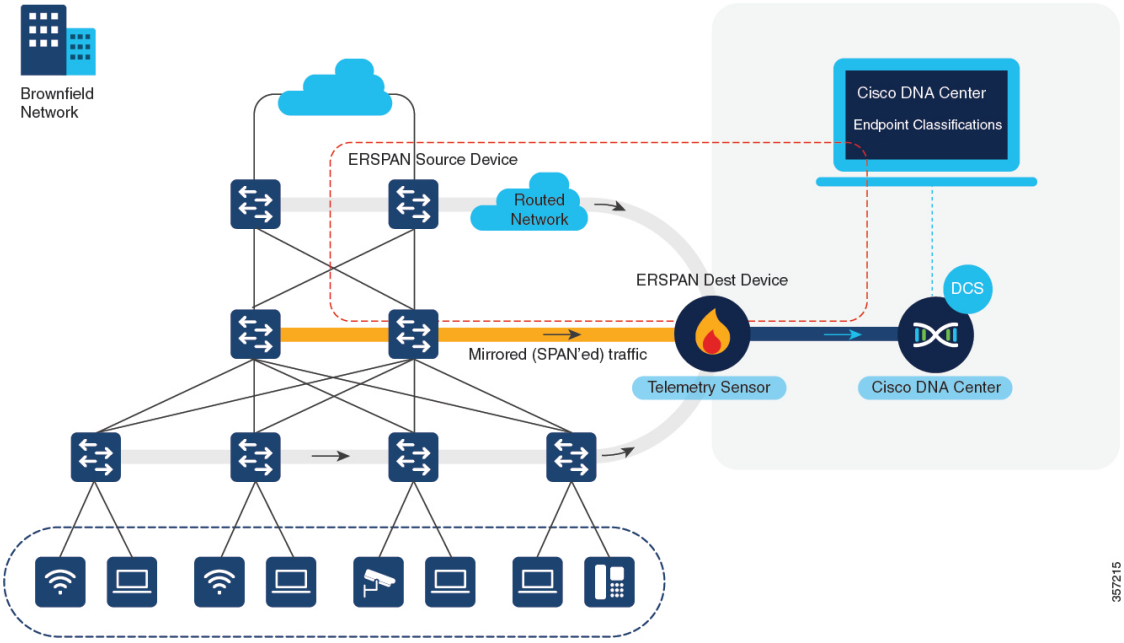
```
switch(config)#do show run | inc monitor
 monitoring
monitor session 1 source vlan 10 , 20 , 30
monitor session 1 destination interface Gi1/0/19
```

Configure the Encapsulated Remote Switching Port Analyzer

The Cisco DNA Traffic Telemetry Appliance supports the Encapsulated Remote Switching Port Analyzer (ERSPAN) feature on both source and destination ports. The ERSPAN transports mirrored traffic over an IP network. The traffic is encapsulated at the source router and transferred across the network. The packet is decapsulated at the destination router and then sent to the destination interface. The ERSPAN consists of an ERSPAN source session, routable ERSPAN Generic Routing Encapsulation (GRE) traffic, and an ERSPAN destination session. You can configure the network devices to mirror traffic on specific ports or VLANs and send the traffic to the telemetry sensor for deep packet inspection (DPI). The telemetry sensor receives and processes the data from a port that is configured as ERSPAN. The port's source sessions and destination sessions are on different switches.

The Cisco DNA Traffic Telemetry Appliance supports seven monitoring interfaces and one telemetry interface. The monitoring interfaces receive traffic from a switch or router through ERSPAN mirroring. The Cisco DNA Traffic Telemetry Appliancesends the traffic to Network-Based Application Recognition (NBAR) to analyze and produce the NetFlow telemetry stream for DNA Center.

Figure 26: Topology for ERSPAN Decapsulation on Cisco DNA Traffic Telemetry Appliance



You can configure the monitoring interface with an IPv4 address. This interface acts as an ERSPAN decapsulation interface and terminates the ERSPAN traffic and removes the ERSPAN header. After removing the IPv4 address, the traffic is sent to the next available monitoring interface or tunnel. This interface acts as an ERSPAN destination interface and analyzes the original traffic through NBAR.

Use the following commands to configure the ERSPAN destination interface:

- **ip nbar protocol-discovery**
- **ip flow monitor**
- **performance monitor**

Configure an ERSPAN Source Session

This example shows how to configure an ERSPAN source session:

```
interface GigabitEthernet1/0/1
 ip address 100.0.0.1 255.255.255.0
 media-type rj45
 negotiation auto
 cdp enable

monitor session 2 type erspan-source
 source interface Gi1/0/0
  destination
  erspan-id 100
  mtu 2000
  ip address 100.0.0.2
  ipv6 dscp 0
  ipv6 ttl 0
  origin ip address 100.0.0.1
```

Configure an ERSPAN Destination Session

This example shows how to configure an ERSPAN destination session:

```
interface GigabitEthernet0/0/2
 ip address 100.0.0.2 255.255.255.0
 negotiation auto
 cdp enable

interface Loopback0
 ip address 9.9.9.6 255.255.255.255
 ipv6 address 9::6/128

interface Loopback1
 ip address 33.33.33.33 255.255.255.0

interface Tunnel1003
 no ip address
 ip nbar protocol-discovery ipv4
 cdp enable
 tunnel source Loopback0
 tunnel destination 33.33.33.33

monitor session 1 type erspan-destination
 destination interface Tu1003
 source
  erspan-id 100
  ip address 100.0.0.2
```

Verify Commands and Debug Commands

Use the following commands to troubleshoot and verify your configuration:

- **show cdp neighbors**
- **show udp neighbors**
- **debug platform hardware qfp active feature erspan datapath all**
- **debug platform hardware qfp active feature erspan client all**

- **set platform software trace forwarding-manager f0 erspan debug**
- **set platform software trace forwarding-manager r0 erspan debug**
- **show platform hardware qfp active feature erspan session <1-1024>**

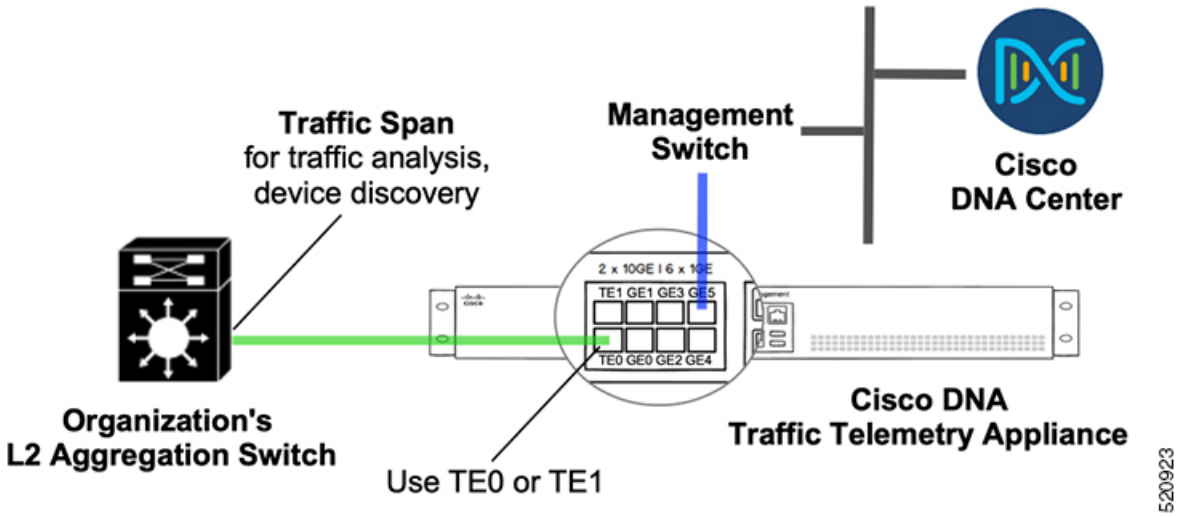
Cisco DNA Traffic Telemetry Appliance Connections

This section describes the connections to make when using a Cisco DNA Traffic Telemetry Appliance.

Option 1: Organization's Aggregation Switch Has 10GE Port Available

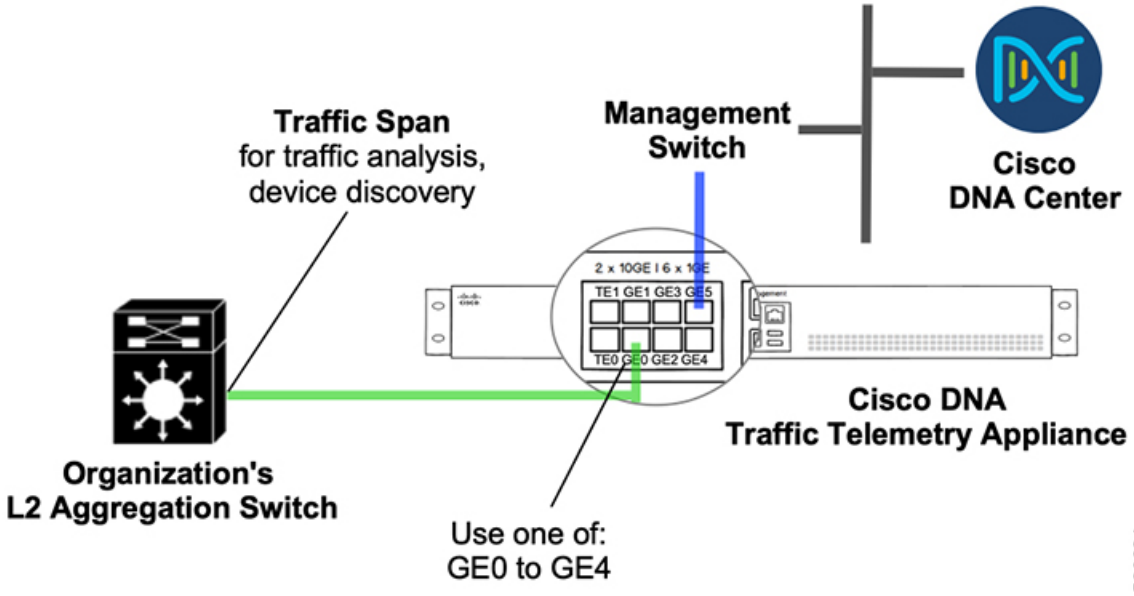
Cisco DNA Traffic Telemetry Appliance Port	Interface	Connection
TE0 or TE1	Te0/0/0 or Te0/0/1	Organization's aggregation switch, 10GE port: Span connection (for traffic analysis and device discovery)
GE5	Gi0/0/5	Management network

Note 10 Gigabit Ethernet (10GE) ports are commonly labeled **TE**.



Option 2: Organization's Aggregation Switch Has 1GE Ports Only

Cisco DNA Traffic Telemetry Appliance Port	Interface	Connection
Any one of: GE0 to GE4	Gi0/0/0 to Gi0/0/4	Organization's aggregation switch, GE port: Span connection (for traffic analysis and device discovery)
GE5	Gi0/0/5	Management network



Configure Cisco DNA Traffic Telemetry Appliance Network Settings

Network settings include:

- Cisco DNA Traffic Telemetry Appliance interface
- Default route

1. Connect the network port to reach Cisco DNA Center and configure the IP address on the appliance. Example:

```
#show run int gigabitEthernet 0/0/5
interface GigabitEthernet0/0/5
description ***** Management Interface  ********
ip address 10.33.100.13 255.255.255.0
negotiation auto
cdp enable
end
```

2. (Optional) Configure the loopback IP address. Example:

```
interface Loopback0
ip address 10.33.33.26 255.255.255.255
```

3. Configure the credentials and enable the password, SSH, and NETCONF. Example:

```
hostname <hostname>
 username dna privilege 15 algorithm-type scrypt secret <password>
enable secret <password>
        service password-encryption
ip domain name dnasolutions.com
ip ssh version 2
         line vty 0 15
            login local
            transport input ssh
            transport preferred none
  ip ssh source-interface loopback0
aaa new-model
aaa authentication login default local
aaa authorization exec default local
netconf-yang
```

4. Configure the default route. Example:

```
ip route 0.0.0.0 0.0.0.0 10.33.100.1
```

5. In a wireless environment, for wireless traffic monitoring, configure NBAR support for CAPWAP:

```
conf t
ip nbar classification tunneled-traffic capwap
```