Cisco DNA Traffic Telemetry Appliance Command Reference

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

Read Me First

Read Me First

This guide summarizes the frequently used CLI commands that the Cisco DNA Traffic Telemetry Appliance uses to:

- Show the span connection status.
- Monitor the status of links and interfaces.
- Perform Control And Provisioning of Wireless Access Points (CAPWAP) stripping when the wireless CAPWAP tunnel traffic streams through the appliance.
- Perform basic troubleshooting.
- Monitor application performance.

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.

Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on cisco.com is not required.

Notes

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Related References

- Cisco IOS Command References, All Releases
- QoS: NBAR Configuration Guide, Cisco IOS XE Gibraltar 16.10.x

Related Documentation

We recommend that you read the following documents relating to the Cisco DNA Traffic Telemetry Appliance:

For This Type of Information...	See This Document...
Release information, including new features, limitations, and open bugs.	Release Notes
Installation and configuration of the Cisco DNA Traffic Telemetry Appliance, including postinstallation tasks.	Hardware Installation Guide
Use of the Cisco DNA Center GUI and its applications.	Cisco DNA Center User Guide, "Cisco AI Endpoint Analytics" chapter

For This Type of Information...	See This Document...
Use of the Cisco DNA Assurance GUI.	Cisco DNA Assurance User Guide, "Monitor Application Health" chapter
Cisco IOS software configuration information and support.	Command Reference
International agency compliance, safety, and statutory information for the Cisco DNA Traffic Telemetry Appliance.	Regulatory Compliance and Safety Information

Read Me First

Commands to Monitor Link and Interface Status

Commands to Monitor Link and Interface Status

Commands to Monitor Link and Interface Status

1. Verify that the links are up:

   show ip int brief

```
Interface              IP-Address      OK?   Method    Status    Protocol
Te0/0/0                unassigned      YES   NVRAM     up        up
Te0/0/1                unassigned      YES   NVRAM     up        up
GigabitEthernet0/0/0   unassigned      YES   NVRAM     up        up
GigabitEthernet0/0/1   unassigned      YES   NVRAM     up        up
GigabitEthernet0/0/2   unassigned      YES   NVRAM     up        up
GigabitEthernet0/0/3   unassigned      YES   NVRAM     up        up
GigabitEthernet0/0/4   unassigned      YES   NVRAM     up        up
GigabitEthernet0/0/5   10.56.197.144   YES   NVRAM     up        up
```

2. Verify that traffic is arriving to the interfaces:

   show interfaces summary

```
TTA#show interfaces  summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                IHQ         IQD         OHQ         OQD       RXBS       RXPS       TXBS       TXPS       TRTL
------------------------------------------------------------------------------------------------------------------------
  Te0/0/0                    0           0           0           0          0          0          0          0          0
  Te0/0/1                    0           0           0           0          0          0          0          0          0
* GigabitEthernet0/0/0       0           0           0           0          0          0          0          0          0
* GigabitEthernet0/0/1       0           0           0           0    2832000        520          0          0          0
* GigabitEthernet0/0/2       0           0           0           0     500000        104          0          0          0
* GigabitEthernet0/0/3       0           0           0           0  139768000      32455          0          0          0
* GigabitEthernet0/0/4       0           0           0           0          0          0          0          0          0
```

3. Verify the interface counters:

   show interfaces *<interface-name>*

```
TTA#show interfaces gigabitEthernet 0/0/2
GigabitEthernet0/0/2 is up, line protocol is up
  Hardware is BUILT-IN-2T+6X1GE, address is 0000.0000.0004 (bia 0000.0000.0004)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 116/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 10Mbps, link type is auto, media type is T
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:12, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 4565000 bits/sec, 949 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     420245 packets input, 254656108 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
     129 carrier transitions
```

4. Verify that traffic is classified by NBAR (CBAR):

   sh ip nbar protocol-discovery stats packet-count

```
Last clearing of "show ip nbar protocol-discovery" counters 04:29:32


                                Input                     Output
                                -----                     ------
Protocol                        Packet Count              Packet Count
--------------------------------- ------------------------ ------------------------
dicom                           95158                     0
dhcp                            15334                     0
hl7                             9186                      0
apple-ios-updates               8885                      0
mdns                            6231                      0
snmp                            3192                      0
Total                           137986                    0
```

Commands to Monitor Link and Interface Status

Troubleshooting Commands

Troubleshooting Commands

1. Check the Cisco DNA Traffic Telemetry Appliance hardware status:

```
show platform
Chassis type: DN-APL-TTA-M

Slot      Type                      State          Insert time (ago)
--------- ------------------        ----------     --------------
0         DN-APL-TTA-M              ok             1w2d
0/0       BUILT-IN-2T+6X1GE         ok             1w2d
0/2       NIM-SSD                   ok             1w2d
R0        DN-APL-TTA-M              ok, active     1w2d
F0        DN-APL-TTA-M              ok, active     1w2d
P0        ASR1001-X-PWR-AC          ps, fail       1w2d
P1        ASR1001-X-PWR-AC          ok             1w2d
P2        DN-APL-TTA-M-FANTRAY      ok             1w2d

Slot      CPLD Version       Firmware Version
--------- -------------      ----------------
0         14041015           17.1(1r)
R0        14041015           17.1(1r)
F0        14041015           17.1(1r)
```

2. Check the management and traffic interface status:

```
show ip interface brief
Interface              IP-Address      OK?  Method Status    Protocol
Te0/0/0                unassigned      YES  NVRAM  up        up
Te0/0/1                unassigned      YES  NVRAM  up        up
GigabitEthernet0/0/0   unassigned      YES  NVRAM  up        up
GigabitEthernet0/0/1   unassigned      YES  NVRAM  up        up
GigabitEthernet0/0/2   unassigned      YES  NVRAM  up        up
GigabitEthernet0/0/3   unassigned      YES  NVRAM  up        up
GigabitEthernet0/0/4   unassigned      YES  NVRAM  up        up
GigabitEthernet0/0/5   10.56.197.144   YES  NVRAM  up        up
GigabitEthernet0       10.56.197.144   YES  manual administratively down down
```

3. Verify the connectivity to Cisco DNA Center:

   ping *<Cisco-DNA-Center-IP-address>* **source gigabitEthernet 0/0/5**

   Example:

```
ping 10.56.197.145 source gigabitEthernet 0/0/5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.56.197.145, timeout is 2 seconds:
Packet sent with a source address of 10.56.197.144
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 m
```

4. Display the interface statistics:

   show interface *<interface-name>*

   Example:

```
show interface gigabitEthernet 0/0/5
GigabitEthernet0/0/5 is up, line protocol is up
  Hardware is BUILT-IN-2T+6X1GE, address is 0000.0000.0007 (bia 0000.0000.0007)
  Internet address is 10.56.197.144/22
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
```

```
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
Full Duplex, 1000Mbps, link type is auto, media type is unknown media type
output flow-control is on, input flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 3d23h
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 15000 bits/sec, 13 packets/sec
5 minute output rate 488000 bits/sec, 46 packets/sec
   9534722 packets input, 2308678895 bytes, 0 no buffer
   Received 2034580 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 1411677 multicast, 0 pause input
   20205964 packets output, 21781423520 bytes, 0 underruns
   Output 2650 broadcasts (0 IP multicasts)
   0 output errors, 0 collisions, 0 interface resets
   57374 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 pause output
   0 output buffer failures, 0 output buffers swapped out
```

5. Show the appliance configuration:

   show running-config
   show startup-config

6. View the system log:

   show log

7. Collect the tech support file:

   show tech-support

8. Show CPU and memory usage:

   show processes cpu
   show processes memory

9. Show system information:

   show version

   The **show version** command displays the configuration of the system hardware, the software version, and the names and sources of configuration files and the boot images. This command also displays information about how the system was last started and how long the appliance has been running since that start.

   The command output is similar to the following:

```
show  version
Cisco IOS XE Software, Version BLD_V173_1_THROTTLE_LATEST_20200723_003000_V17_3_0_226
Cisco IOS Software, TTA Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version

17.3.20200723:005607
[S2C-build-v173_1_throttle-298-/nobackup/mcpre/BLD-BLD_V173_1_THROTTLE_LATEST_20200723_003000
 285]
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 23-Jul-20 07:55 by <ID>
```

Troubleshooting Commands

```
Cisco IOS-XE software, Copyright (c) 2005-2020 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: 17.1(1r)

nightsterReg7 uptime is 2 hours, 30 minutes
Uptime for this control processor is 2 hours, 34 minutes
System returned to ROM by Reload Command at 06:21:53 IST Sat Jul 25 2020
System restarted at 06:27:11 IST Sat Jul 25 2020
System image file is
"bootflash:ttam-universalk9.BLD_V173_1_THROTTLE_LATEST_20200723_003000_V17_3_0_226.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.

License Type: Smart License is permanent
License Level: adventerprise
Next reload license Level: adventerprise
The current throughput level is 20000000 kbps

Smart Licensing Status: UNREGISTERED/EVAL EXPIRED

cisco DN-APL-TTA-M (1NG) processor (revision 1NG) with 6829417K/6147K bytes of memory.
Processor board ID JAE194707F2
Router operating mode: Autonomous
6 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
6684671K bytes of eUSB flash at bootflash:.
937689088K bytes of SATA hard disk at harddisk:.

Configuration register is 0x2102
```

10. Verify SD-AVC service information:

```
sh avc sd-service info summary
Status: CONNECTED

Device ID: JAE194707F2
Device segment name: AppRecognition
Device address: 10.10.10.2
Device OS version: 17.03.01prd15
```

```
Device type: DN-APL-TTA-M

Active controller:
   Type  : Primary
   IP    : 10.10.10.1
   Status: Connected
```

11. Verify SD-AVC service information - DCS enabled:

```
show avc sd-service info detailed | inc DCS
DCS configuration summary:
DCS mode  : ENABLED
```

Troubleshooting Commands

Application Performance Monitoring Commands

Commands for application performance monitoring (APM) refer to Assurance-related metrics collected per network application, for flows forwarded through specific interfaces, to support Assurance monitoring by Cisco DNA Center.

APM Overview

Cisco DNA Assurance

Assurance collects and analyzes network data to help provide better and more consistent network performance. Cisco DNA Center uses Flexible NetFlow (FNF) to collect specific network metrics for Assurance, providing quantitative and qualitative information about devices in the network. The FNF records designed for Assurance-related metrics are specially optimized for improved performance.

FNF provides a pair of record types (for IPv4 and IPv6) to collect data for Assurance. Monitoring Assurance metrics using these dedicated record types is optimized to provide better performance, as compared with typical FNF monitors configured to collect the same metrics. (Modifying the records cancels the dedicated performance enhancements for Assurance, and may prevent attaching a monitor to an interface.)

Manual Configuration

In typical use, Cisco DNA Center configures the monitors to collect data for Assurance, without requiring user input. However, it is also possible to use these record types manually.

Metrics Collected for Assurance

Most of the metrics collected for Assurance are metrics that have been available through FNF and other monitor types, but when they are collected specifically for Assurance records, some metrics may behave slightly differently.

Table 1: Metrics

Metric	Information
match ipv4/ipv6 version	IPv4/IPv6 version from IPv4/IPv6 header. [1]
match ipv4/ipv6 protocol	Layer 4 protocol from the IPv4/IPv6 header.
match application name	Application ID.
match connection client ipv4/ipv6 address	Field name: clientIPv4/IPv6Address IPv4/IPv6 client address in the IP packet header. The client is the device that triggered the session creation, and remains the same for the life of the session. [2]
match connection server ipv4/ipv6 address	Field name: serverIPv4/IPv6Address IPv4/IPv6 server address in the IP packer header. The server is the device that replies to the client, and remains the same for the life of the session. [2]
match connection server transport port	Field name: serverTransportPort Server transport port identifier. This may be the source or destination transport port. The server is the device that replies to the client, and remains the same for the life of the session. [2]
match flow observation point	Field name: observationPointId Identifier of an observation point unique for each observation domain. [2]
collect connection initiator	Field name: biflowDirection By convention, this field is set to Initiator. [2]
collect flow direction	Direction (ingress/egress) of the initiator side of the flow (as is set by convention in the connection initiator field).

Metric	Information
collect routing vrf input	Field name: ingressVRFID (Applies only to routers, not wireless controllers) VRF ID from incoming packets on a router. If a packet arrives on an interface that does not belong to a VRF, a VRF ID of 0 is recorded.
collect wireless client mac address	(Applies only to wireless controllers) Field name: staMacAddress The IEEE 802 MAC address of a wireless station (STA).
collect timestamp absolute first	Field name: flowStartMilliseconds The absolute timestamp of the first packet of the flow.
collect timestamp absolute last	Field name: flowEndMilliseconds The absolute timestamp of the last packet of the flow.
collect connection new-connections	Field name: connectionCountNew This information element counts the number of TCP or UDP connections which were opened during the observation period. The observation period may be specified by the flow start and end timestamps. [2]
collect connection server counter packets long	Field name: serverPackets Number of layer 4 packets in a flow from the server. The server is the device that replies to the client, and remains the same for the life of the session. [2]
collect connection server counter bytes network long	Field name: serverOctets Overall IP packet bytes in a flow from the server. The server is the device that replies to the client, and remains the same for the life of the session. [2]
collect connection client counter packets long	Field name: clientPackets Number of layer 4 packets in a flow from the client. The client is the device that triggered the session creation, and remains the same for the life of the session. [2]
collect connection client counter bytes network long	Overall IP packet bytes from client to server. [2]

Metric	Information
collect connection delay network client-to-server sum	Field name: sumNwkTime Network delay is the round-trip time between the client and the server, as measured by the observation point, calculated once per session. The value of this information element is the sum of all network delays observed for the sessions of this flow. [2] [3]
collect connection delay network to-server sum	Field name: sumServerNwkTime Server network delay is the round-trip time between the observation point and the server, calculated once per session. The value of this information element is the sum of all server network delays observed for the sessions of this flow. [2] [3]
collect connection client counter packets retransmitted	Field name: retransClientPackets Number of packets retransmitted by the client. [2] [3]
collect connection server counter packets retransmitted	Field name: retransServerPackets Number of packets retransmitted by the server. [3]
collect connection delay application sum	Field name: sumServerRespTime The sum of all application delays observed for all responses of the flow. [2] [3]
collect connection server counter responses	Field name: numRespsCountDelta Total number of responses sent by the server. [2] [3]

Notes

- [1] See the Cisco IOS Flexible NetFlow Command Reference.
- [2] See the Cisco AVC Field Definition Guide.
- [3] This metric can be used in Cisco Performance Monitor record types. It can be used with FNF only as part of the specially optimized Assurance-related records. Attempting to use this metric in a different FNF record type causes the record to be rejected when attaching it to an interface.

Configure Assurance Monitors Outside of Cisco DNA Center

In typical use, Cisco DNA Center configures the monitors without requiring additional user input, but it is possible to configure monitors for Assurance-related metrics manually.

Method	Applicable to...	See section...
ezPM profile	Platforms that support ezPM Not wireless controllers	Configure Assurance Monitors Using ezPM, on page 21
Predefined FNF records for Assurance	Routers Wireless controllers	Configure Assurance Monitors Using Predefined FNF Records, on page 22

Configure Assurance Monitors Using ezPM

Applicable to: routers, not wireless controllers

The application-assurance ezPM profile makes use of the application performance monitoring (APM) FNF records designed for Assurance-related metrics. Configuring APM with ezPM simplifies the configuration as compared to working with the FNF records directly.

1. Configure the ezPM context.

   performance monitor context *context-name* **profile application-assurance**
   traffic-monitor assurance-monitor ipv4
   traffic-monitor assurance-monitor ipv6

2. Attach the context to an interface. The following command attaches the performance monitor to an interface, monitoring both input and output.

   interface *interface*
   performance monitor context *context-name*

Result

This attaches monitors to the interface to collect Assurance-related metrics.

Example

In the following example, a monitor called *apm* is attached to the Gigabit Ethernet 1 interface.

```
performance monitor context apm profile application-assurance
traffic-monitor assurance-monitor ipv4
traffic-monitor assurance-monitor ipv6

interface GigabitEthernet1
performance monitor context apm
```

Configure Assurance Monitors Using Predefined FNF Records

Applicable to: routers, wireless controllers

ezPM is the preferred method for configuring monitors for Assurance-related metrics, but it is also possible to use the FNF records predefined for these metrics. For platforms that do not support ezPM, predefined FNF records are the preferred method.

The FNF records designed for Assurance-related metrics are optimized for improved performance.

Routing Platforms

1. Define two flow monitors for assurance-related metrics, one for IPv4 and one for IPv6.

   ```
   flow monitor monitor-name-for-ipv4
   cache entries 100000 {Optional. Recommended value depends on platform.}
   record netflow ipv4 assurance
   flow monitor monitor-name-for-ipv6
   cache entries 100000 {Optional. Recommended value depends on platform.}
   record netflow ipv6 assurance
   ```

2. Attach the context to an interface. The following command attaches the performance monitor to an interface, monitoring both input and output.

   ```
   interface interface
   ip flow monitor monitor-name-for-ipv4 input
   ip flow monitor monitor-name-for-ipv4 output
   ipv6 flow monitor monitor-name-for-ipv6 input
   ipv6 flow monitor monitor-name-for-ipv6 output
   ```

Result

The preceding commands attach two IPv4 and two IPv6 monitors to the interface for collecting the metrics that are needed for Assurance.

Example

This example defines monitors called assurance-ipv4 and assurance-ipv6, and attaches the monitors to the GigabitEthernet1 interface.

```
flow monitor assurance-ipv4
cache entries 100000
record netflow ipv4 assurance

flow monitor assurance-ipv6
cache entries 100000
record netflow ipv6 assurance

interface GigabitEthernet1
ip flow monitor assurance-ipv4 input
ip flow monitor assurance-ipv4 output
ipv6 flow monitor assurance-ipv6 input
ipv6 flow monitor assurance-ipv6 output
```

Wireless Platforms

1. Enter the configuration mode for the relevant wireless profile.

```
interface policy-name
```

2. Define two monitors for the wireless controller, one for IPv4 and one for IPv6.

```
flow monitor monitor-name-wlc-for-ipv4
cache entries 100000 {Optional. Recommended value depends on platform.}
record wireless avc ipv4 assurance
flow monitor monitor-name-wlc-for-ipv6
cache entries 100000 {Optional. Recommended value depends on platform.}
record wireless avc ipv6 assurance
```

3. Attach the two flow monitors to the wireless profile, including input and output traffic.

```
wireless profile policy policy-name
ip flow monitor monitor-name-for-wireless-ipv4 input
ip flow monitor monitor-name-for-wireless-ipv4 output
ipv6 flow monitor monitor-name-for-wireless-ipv6 input
ipv6 flow monitor monitor-name-for-wireless-ipv6 output
```

Example

This example defines monitors called *assurance-wlc-ipv4* and *assurance-wlc-ipv6*, and attaches the monitors to a wireless profile.

```
flow monitor assurance-wlc-ipv4
cache entries 100000
record wireless avc ipv4 assurance

flow monitor assurance-wlc-ipv6
cache entries 100000
record wireless avc ipv6 assurance

wireless profile policy AVC_POL
central association
central switching
ip flow monitor assurance-wlc-ipv4 input
ip flow monitor assurance-wlc-ipv4 output
ipv6 flow monitor assurance-wlc-ipv6 input
ipv6 flow monitor assurance-wlc-ipv6 output
no shutdown
```

About Attaching the Assurance Monitors to Interfaces

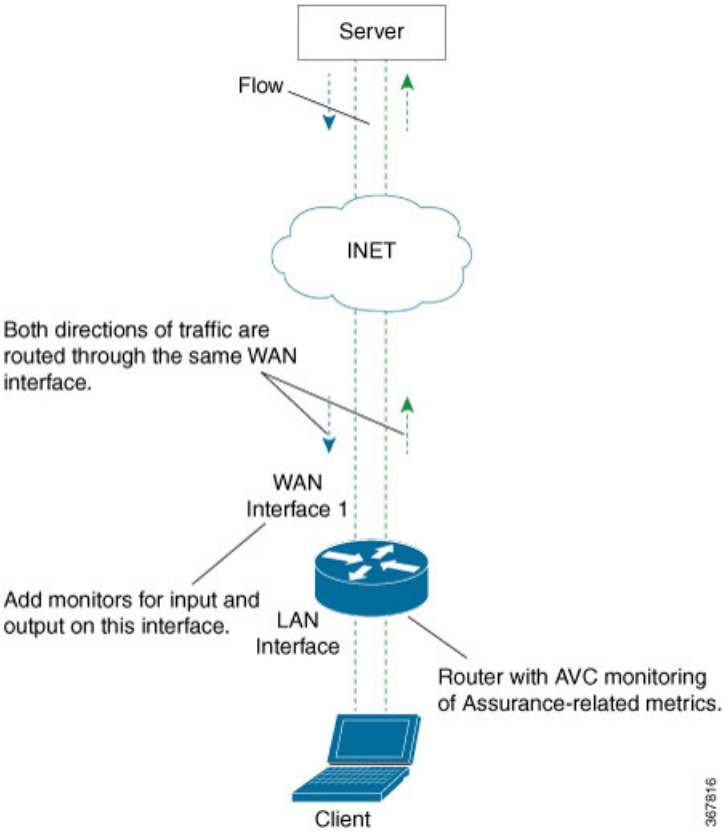
Monitor a Flow on Only One Interface

Monitors for Assurance-related metrics should only see a single flow one time. In the typical symmetric routing scenario, they should monitor the flow on only one interface.

Do not attach monitors for Assurance-related metrics to two separate interfaces that handle both directions of the same flow. Doing so will cause incorrect traffic metrics to be reported. For example, if traffic enters a device on interface A and leaves on interface B, do not attach monitors for Assurance-related metrics to both interfaces A and B.

The following figure shows the typical symmetric routing, with monitors for input and output on the same interface.

Figure 1: Symmetric Routing

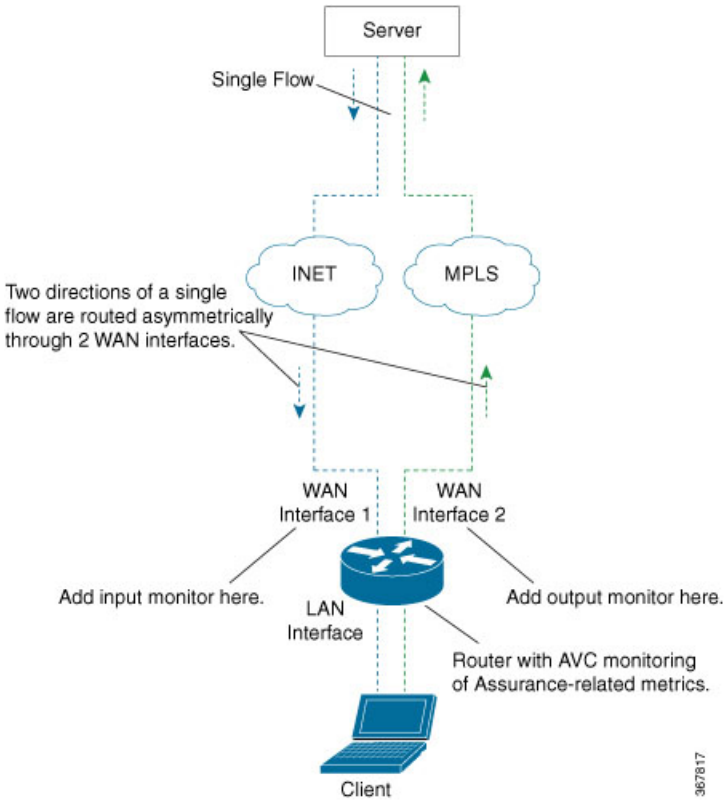


Asymmetric Routing

In some cases, such as for asymmetric routing, it might be necessary to attach a monitor for input on one interface, and a monitor for output on another interface.

In some scenarios, a single flow may be routed asymmetrically, with upstream and downstream traffic for the flow occurring on two different interfaces. In this case, place monitors for input and output on two separate interfaces to monitor the complete flow.

Figure 2: Asymmetric Routing



View Details of Assurance Records and Contexts

After you attach a context to an interface, two **show** commands can be used to display information about Assurance records or about contexts.

Displaying Structure of the Assurance Record

The following command displays the structure of the predefined Assurance records (IPv4 and IPv6).

show flow record netflow {ipv4 | ipv6} assurance

Displaying Configuration of a Context

The following command displays the full configuration of a specified context.

show performance monitor context *context-name* **configuration**

The following output shows the Assurance-related monitoring through an ezPM context, called ApmContext, attached to a router interface.

```
Device#show performance monitor context ApmContext configuration
!================================================================================
!                Equivalent Configuration of Context ApmContext                !
!================================================================================
!Exporters
!==========
!
flow exporter ApmContext-1
description performance monitor context ApmContext exporter
destination 64.103.113.128 vrf FNF
source GigabitEthernet2/2/0
transport udp 2055
export-protocol ipfix
template data timeout 300
option interface-table timeout 300
option vrf-table timeout 300
option sampler-table timeout 300
option application-table timeout 300
option application-attributes timeout 300
!
!Access Lists
!=============
!Class-maps
!===========
!Samplers
!=========
!Records and Monitors
!=====================
!
flow record ApmContext-app_assurance_ipv4
description ezPM record
match ipv4 version
match ipv4 protocol
match application name
match connection client ipv4 address
match connection server ipv4 address
match connection server transport port
match flow observation point
collect routing vrf input
collect flow direction
```

```
collect timestamp absolute first
collect timestamp absolute last
collect connection initiator
collect connection new-connections
collect connection server counter responses
collect connection delay network to-server sum
collect connection client counter packets retransmitted
collect connection delay network client-to-server sum
collect connection delay application sum
collect connection server counter packets long
collect connection client counter packets long
collect connection server counter packets retransmitted
collect connection server counter bytes network long
collect connection client counter bytes network long
!
!
flow monitor ApmContext-app_assurance_ipv4
description ezPM monitor
exporter ApmContext-1
cache timeout active 60
cache entries 100000
record ApmContext-app_assurance_ipv4
!
!
flow record ApmContext-app_assurance_ipv6
description ezPM record
match ipv6 version
match ipv6 protocol
match application name
match connection client ipv6 address
match connection server transport port
match connection server ipv6 address
match flow observation point
collect routing vrf input
collect flow direction
collect timestamp absolute first
collect timestamp absolute last
collect connection initiator
collect connection new-connections
collect connection server counter responses
collect connection delay network to-server sum
collect connection client counter packets retransmitted
collect connection delay network client-to-server sum
collect connection delay application sum
collect connection server counter packets long
collect connection client counter packets long
collect connection server counter packets retransmitted
collect connection server counter bytes network long
collect connection client counter bytes network long
!
!
flow monitor ApmContext-app_assurance_ipv6
description ezPM monitor
exporter ApmContext-1
cache timeout active 60
cache entries 100000
record ApmContext-app_assurance_ipv6
!
!Interface Attachments
!======================
interface TenGigabitEthernet2/0/0
ip flow monitor ApmContext-app_assurance_ipv4 input
ip flow monitor ApmContext-app_assurance_ipv4 output
```

```
ipv6 flow monitor ApmContext-app_assurance_ipv6 input
ipv6 flow monitor ApmContext-app_assurance_ipv6 output
```

Sample APM Configuration for Wireless Platforms

```
!
! local exporter … records are punted to wncd for 'show avc'.
! ssid option table will enable  the display of SSID name even though the SSID is not in
record
!
flow exporter avc_show
destination local wlc
source Vlan1
template data timeout 30
option ssid-table timeout 30
!
flow monitor avc_assurance
exporter avc_show
cache timeout inactive 60
cache timeout active 60
record wireless avc ipv4 assurance
!
flow monitor avc_assurance_rtp
exporter avc_show
cache timeout inactive 60
cache timeout active 60
record wireless avc ipv4 assurance-rtp

wireless profile policy AVC_POL
ipv4 flow monitor avc_assurance input
ipv4 flow monitor avc_assurance output
ipv4 flow monitor avc_assurance_rtp input
ipv4 flow monitor avc_assurance_rtp output
no shutdown
!
wireless tag policy AVC_TAG
wlan EWLC_SSID policy AVC_POL
!
wlan EWLC_SSID 2 EWLC_SSID
no security wpa
no security wpa akm dot1x
no security wpa mpsk
security wpa mpsk
no security wpa wpa2 ciphers aes
no shutdown

ap F4CF.E220.8400
policy-tag AVC_TAG
```

Sample APM Configuration for Wired Platforms

```
performance monitor context apm profile application-assurance
exporter destination 10.156.29.140  source GigabitEthernet0/0/4  transport udp vrf FNF port
 2000
 traffic-monitor assurance-monitor
 traffic-monitor assurance-rtp-monitor

!
interface GigabitEthernet0/0/1
ip address 2.1.1.1 255.255.255.0
negotiation auto
performance monitor context apm

!
interface GigabitEthernet0/0/4
vrf forwarding FNF
ip address 10.56.29.32 255.255.255.0
negotiation auto
```

Show Debug Statistics

```
#show platform hardware qfp active feature nbar function asd_show_stats

FNF Assurance Stats:
client_tcp_pkts 5
server_tcp_pkts 3
client_udp_pkts 0
server_udp_pkts 0

handle_tcp_udp_pkts 8
handle_and_collapse_non_tcp_udp_pkts 0
handle_other_pkts 0
handle_gen_error_pkts 0

max_concurrent_fos 1
alloc_fo 1
free_fo 1
alloc_fo_failed 0
attach_fo_failed 0
free_fo_failed 0
pkt_failed_get_cft_info 0
pkt_failed_get_cft_ind 0
is_nbar_final_cls_api_error 0

report_new_connections 1
report_new_sessions 1
report_num_responses 1
collapse_flow_final_cls 0
collapse_flow_periodic 0
collapse_flow_eof 1
collapse_void_no_pkts 0

client_retrans_pkts 0
server_retrans_pkts 0

ipv4_connections 1
ipv6_connections 0
tcp_connections 1
udp_connections 0
```

Clear Debug Statistics

```
#show platform hardware qfp active feature nbar function asd_stats_reset

FNF Assurance Stats have been reset
```

Assurance-Related Metrics and Elephant Flows

In networking, especially long flows are called *elephant flows* and can pose a challenge to networking resources.

In a case where a single high-burst flow consumes too many QFP resources, the monitor collecting Assurance metrics might stop collecting qualitative metrics for the flow, to preserve resources for other traffic. No other traffic is affected.

Quantitative metrics are collected fully:

- Flow packets start time
- Flow packets end time
- Packets
- Bytes

Qualitative metrics are not collected fully:

- Total network delay sum (in the TCP handshake)
- Network to-server delay sum (in the TCP handshake)
- Client packets retransmitted
- Server packets retransmitted
- Application delay sum
- Number of server application responses

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

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
```

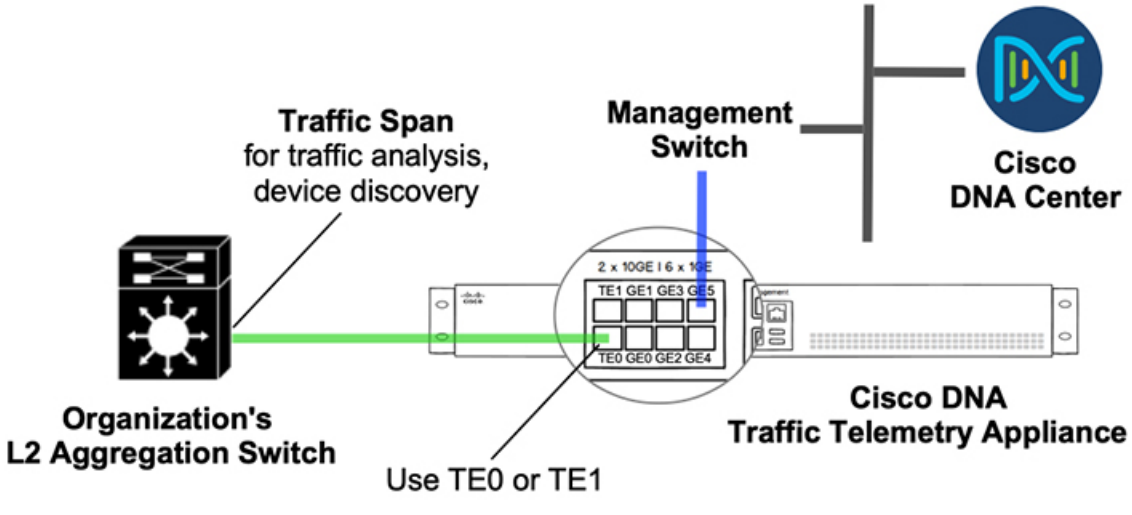
Cisco DNA Traffic Telemetry Appliance Connections

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

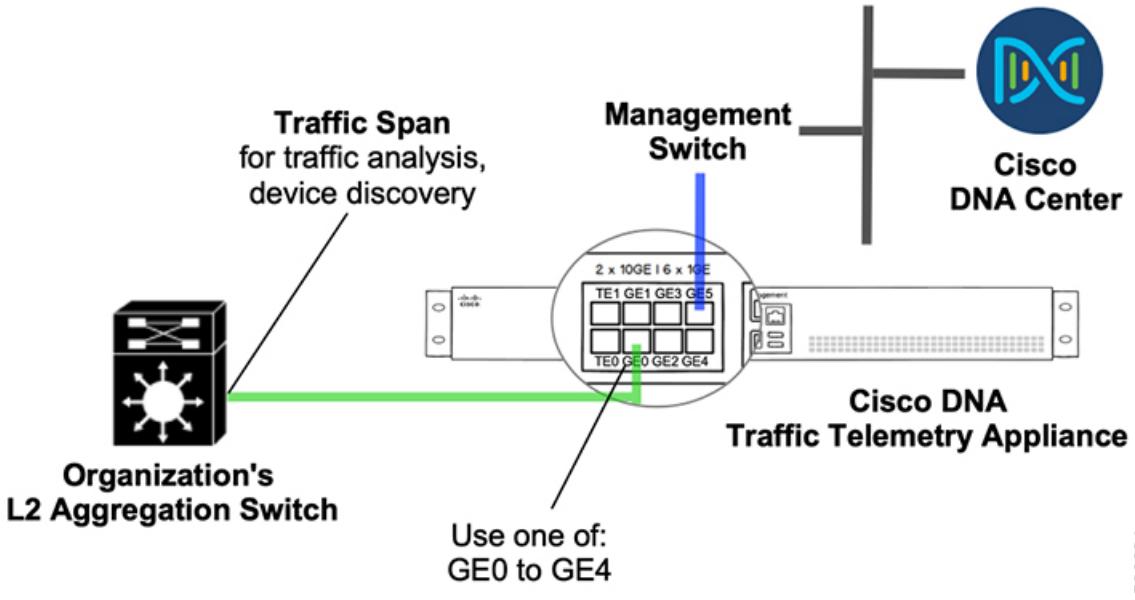
Cisco DNA Traffic Telemetry Appliance Port	Interface	Connection
TE0 or TE1	Te0/0/0 or Te0/0/1	Organization's aggregation switch, 10GE port: Span connection (for traffic analysis and device discovery)
GE5	Gi0/0/5	Management network

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


Traffic Span
for traffic analysis,
device discovery
Management
Switch
Cisco
DNA Center
2 x 10GE | 6 x 1GE
TE1 GE1 GE3 GE5
TE0 GE0 GE2 GE4
Cisco DNA
Traffic Telemetry Appliance
Organization's
L2 Aggregation Switch
Use one of:
GE0 to GE4
520924

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
```