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 2
- Cisco DNA Traffic Telemetry Appliance Connections, on page 3
- Configure Cisco DNA Traffic Telemetry Appliance Network Settings, on page 5

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
```

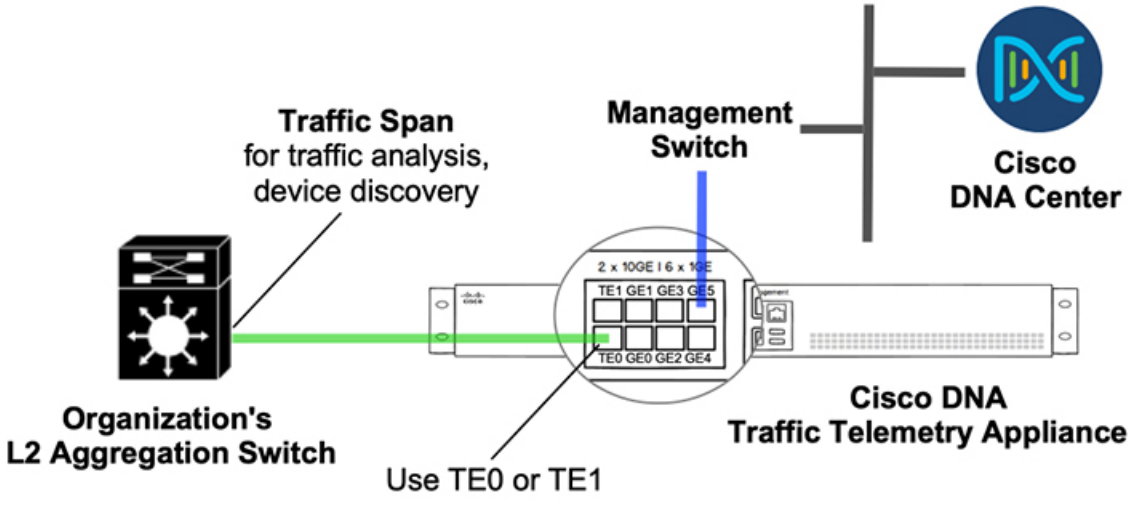
Cisco DNA Traffic Telemetry Appliance Connections

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

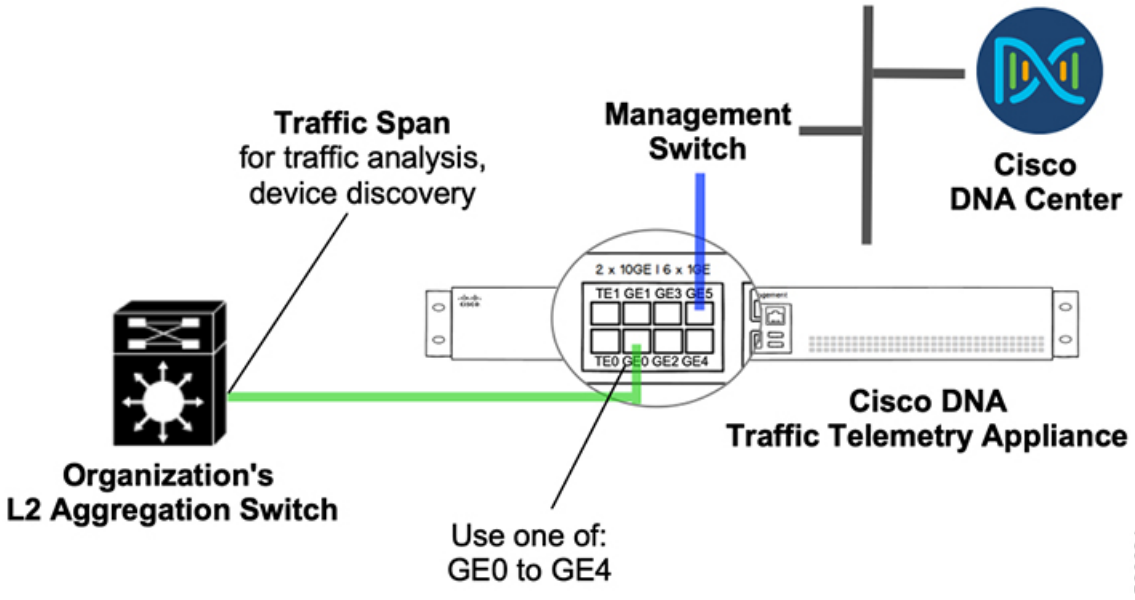
Cisco DNA Traffic Telemetry Appliance Port	Interface	Connection
TE0 or TE1	Te0/0/0 or Te0/0/1	Organization's aggregation switch, 10GE port: Span connection (for traffic analysis and device discovery)
GE5	Gi0/0/5	Management network

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
```