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:

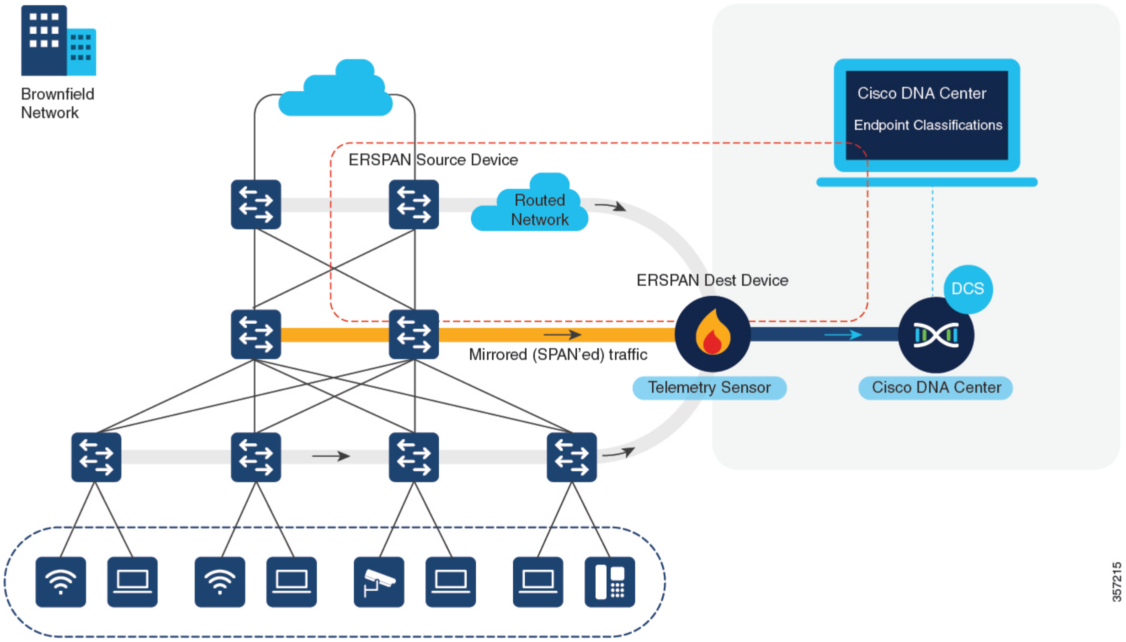
```
switch(config)#do show run | inc monitor
 monitoring
monitor session 1 source vlan 10 , 20 , 30
monitor session 1 destination interface Gi1/0/19
```

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 1: 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>**

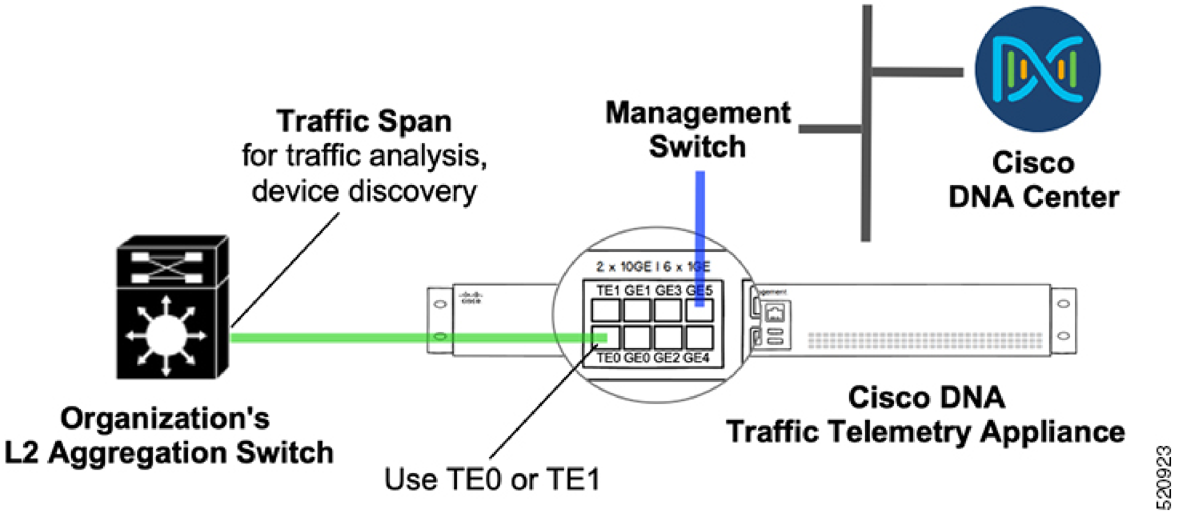
Cisco DNA Traffic Telemetry Appliance Connections

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

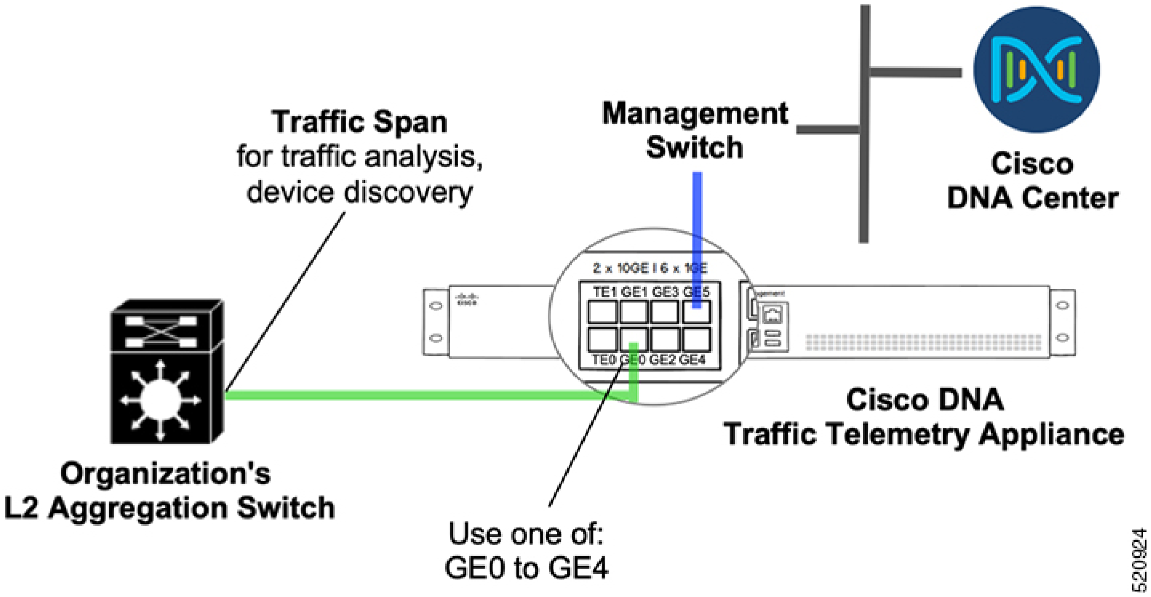
Cisco DNA Traffic Telemetry Appliance Port	Interface	Connection
TE0 or TE1	Te0/0/0 or Te0/0/1	Organization's aggregation switch, 10GE port: Span connection (for traffic analysis and device discovery)
GE5	Gi0/0/5	Management network

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
```