Troubleshooting Steps for Endpoint Connectivity Problems

This chapter lists the steps for troubleshooting endpoint connectivity issues using the Cisco APIC tools, contains procedures for inspecting the operational status of your endpoints and tunnel interfaces, and explains how to connect an SFP module.

This chapter contains the following sections:

Troubleshooting Endpoint Connectivity

Procedure

Step 1　　Inspect the operational status of each endpoint.

The operational status will reveal any fault or misconfiguration of the endpoints. See

Inspecting the Endpoint Status, on page 2 .

Step 2　　Inspect the status of the tunnel interface.

The operational status will reveal any fault or misconfiguration of the tunnel. See Inspecting the Tunnel Interface Status, on page 3.

Step 3　　Perform a traceroute between the endpoint groups (EPGs).

A traceroute will reveal any problems with intermediate nodes, such as spine nodes, between the endpoints. See Performing a Traceroute Between Endpoints.

Step 4　　Configure an atomic counter on an endpoint.

The atomic counter will confirm whether the source endpoint is transmitting packets or the destination endpoint is receiving packets, and whether the number of packets received equals the number of packets sent. See Configuring Atomic Counters.

Step 5　　Inspect the contracts under each EPG.

Inspect the contracts under each EPG to make sure they allow the traffic that should flow between the EPGs. As a test, you can temporarily open the contracts to allow unrestricted traffic.

Step 6 Configure a SPAN policy to forward source packets to a monitoring node.

A packet analyzer on the monitoring node will reveal any packet issues such as an incorrect address or protocol. See Configuring a SPAN Session.

Inspecting Endpoint and Tunnel Interface Status

This section explains how to inspect the operational status of endpoints and tunnel interfaces. Performing these procedures enables you to reveal any fault or misconfiguration of the endpoints and tunnel interfaces.

Inspecting the Endpoint Status

Procedure

Step 1 In the menu bar, click **Tenants**.

Step 2 In the submenu bar, click the tenant that contains the source endpoint.

Step 3 In the **Navigation** pane, expand the tenant, expand **Application Profiles**, and expand the application profile that contains the endpoint.

Step 4 Expand **Application EPGs** and click the EPG to be inspected.

Step 5 In the **Work** pane, from the list of endpoints in the **Endpoint** table, double-click the source endpoint to open the **Client End Point** dialog box.

Step 6 In the **Client End Point** dialog box, verify the endpoint properties and click the **Operational** tab.

Step 7 In the **Operational** tab, view the health, status, and fault information.

In the **Status** table, click any items with entries, such as changes, events, or faults.

Step 8 Close the **Client End Point** dialog box.

Step 9 In the **Endpoint** table, view the **Interface** entry for the endpoint and note the node and tunnel IDs.

Step 10 Repeat this procedure for the destination endpoint.

Note   Occasionally, bidirectional traffic is interrupted between IP addresses in two micro-segmented EPGs deployed behind two leaf switches in the fabric. This can occur when the IP addresses are transitioning because of a configuration change from micro-segment EPG to base EPG. Or conversely, this can occur on two different leaf switches at the same time while bidirectional traffic is running. In this case, the policy tag for each remote endpoint still points to its previous EPG.

Workaround: Manually clear the remote endpoints on the switches or wait for the remote endpoint to age out. To clear the endpoints, log on to the CLI on each switch and enter the **clear system internal epm endpoint** command with the appropriate option. For example, if your endpoints are based on the IP address, enter **clear system internal epm endpoint key vrf** *vrf_name* **{ip | ipv6}** *ip-address*. The endpoints are then relearned with the correct policy tag.

Inspecting the Tunnel Interface Status

This procedure shows how to inspect the operational status of the tunnel interface.

Procedure

Step 1   In the menu bar, click **Fabric**.

Step 2   In the submenu bar, click **Inventory**.

Step 3   In the **Navigation** pane, expand the pod and expand the node ID of the source endpoint interface.

Step 4   Under the node, expand **Interfaces**, expand **Tunnel Interfaces**, and click the tunnel ID of the source endpoint interface.

Step 5   In the **Work** pane, verify the tunnel interface properties and click the **Operational** tab.

Step 6   In the **Operational** tab, view the health, status, and fault information.

In the **Status** table, click any items with entries, such as changes, events, or faults.

Step 7   Repeat this procedure for the destination endpoint interface.

Connecting an SFP Module

When you connect an SFP module to a new card, you need to create a link speed policy for the module to communicate with the card. Follow these steps to create a link speed policy.

Procedure

Step 1   Create an interface policy to specify the link speed:

Example:

```
<fabricHIfPol name="SpeedPol" speed="1G"/>
```

Step 2   Reference the link speed policy within an interface policy group:

Example:

```
<infraAccPortGrp name="myGroup">
   <infraRsHIfPol tnFabricHIfPolName="SpeedPol"/>
</infraAccPortGrp>
```

```
<infraAccPortGrp name="myGroup">
```