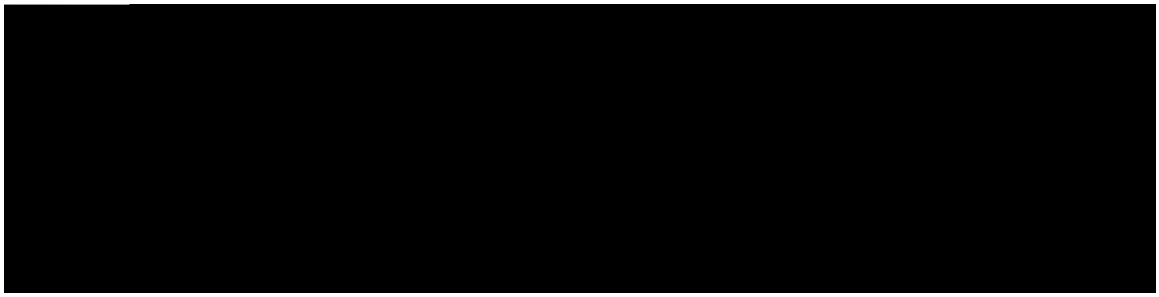
Cisco APIC Troubleshooting Guide

Last Modified: 2016-09-28

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

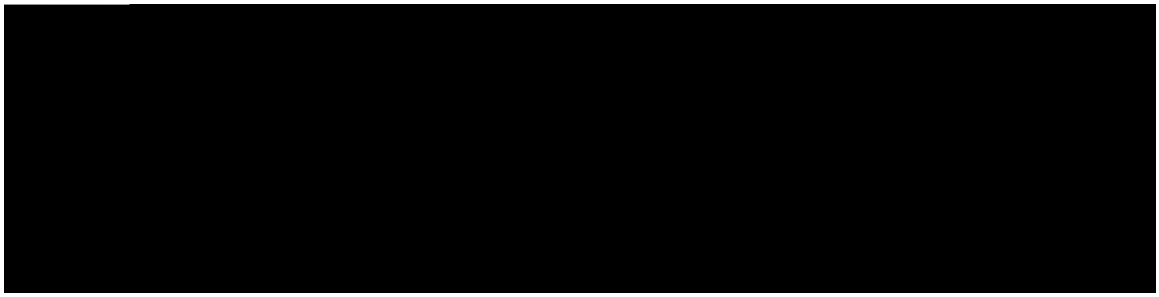


CONTENTS

CHAPTER 6

Using the Cisco

Port Tracking Using the



Preface

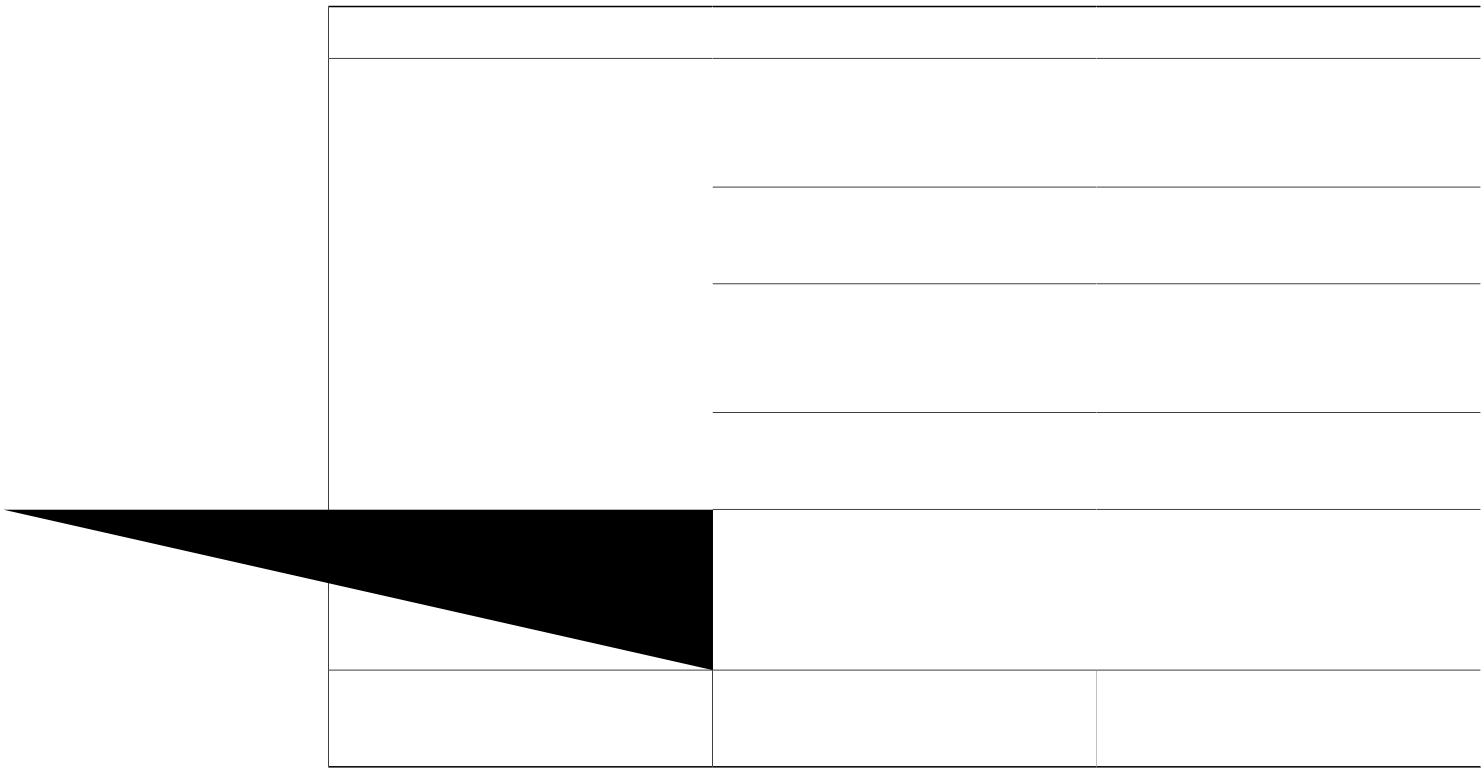
This preface includes the following sections:

Audience

This guide

CHAPTER 1

New and Changed



CHAPTER 2

CHAPTER 3

Troubleshooting the Cisco APIC Cluster

This chapter contains information about cluster

CHAPTER

Recovering Cisco APIC Passwords and Accessing Special Logins

This chapter explains how to recover your Cisco APIC

```
  at any time accepts your changes.]
< rhgb quiet selinux=0 audit=1  aci-admin-passwd-reset
```

Step 9 Press **Enter** to save the file.

Step 10 Press **b** to boot the APIC.

Note To cancel the password reset operation and return to the default boot parameters, press **Esc** and **Enter**.

Step 11 The APIC boots and prompts for a new

CHAPTER 3

Cisco APIC Troubleshooting Operations

This chapter explains how to perform the basic troubleshooting operations and contains the following sections:

3 Check that the cluster has

1. In the menu bar, click **System**.
2. In the submenu bar, click **Controllers**.
3. Under **Controllers,** click the APIC node that you

CHAPTER 6

Using the Cisco APIC Troubleshooting Tools

This

- Enabling and Viewing

c) From the **Name** drop-down list, choose

```
       "ownerTag":"",
       "status":"",
       "uid":"15374"
}}}]}
```

Step 3 The following example shows how to use the **show acllog**

Step 7 The following example shows how to use the **show acllog drop l2 pkt**

- Atomic counters require an active fabric Network Time Protocol (NTP) policy.
- Atomic counters work for IPv6 sources and destinations but configuring source and destination IP addresses across IPv4 and IPv6 addresses is not allowed.
- An atomic counter policy configured with fvCEp as the source and/or destination counts only the traffic that is from/to the MAC and IP addresses that are present in the fvCEp managed objects (MOs). If the fvCEp MO has M

EP_to_EPG

Enabling and Viewing Digital Optical Monitoring Statistics

Real-time digital optical monitoring (DOM) data is collected from SFPs, SFP+, and XFPs periodically and compared with warning and alarm threshold table values. The DOM data collected are transceiver transmit bias current, transceiver transmit power, transceiver receive power, and transceiver power supply voltage.

Enabling Digital Optical Monitoring Using the GUI

Before you can view digital optical monitoring (DOM) statistics about a physical interface,

f)

Filtering by Health Score

You can filter health scores using the following tools:

- Health Scroll Bar — You can use the health scroll bar to dictate which objects are visible; lowering the score allows you to see only objects with a degraded health score.
- Displaying Degraded Health Scores — To display only the degraded health scores, click the Gear icon and choose **Show only degraded health scores**.

Viewing Tenant Health

To vie application health,
25 104890Q 8L W K

Port Tracking Using the NX-OS CLI

This procedure explains how to use the

Configuring SNMP for Monitoring and Managing Devices

This section explains how to configure

Before You Begin

To allow SNMP communications, you must configure the following:

- Configure an

b) From the **SNMP Policy** drop-down list, choose the SNMP policy that you configured and click **Submit**.

Step 12 Under **Pod Policies**, expand **Profiles** and click **default**.

Step 13 In the **Work pane**, from the **Fabric Policy Group** drop-down list, choose

Configuring an SNMP T

About SPAN

You can use the Switched Port Analyzer (SPAN) utility to perform detailed troubleshooting

Configuring a SPAN Session

This procedure shows how to configure a SPAN policy to forward replicated source packets to a remote traffic analyzer.

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 **Troubleshooting Policies**, and expand **SPM**

Show

Command	Purpose
debug platform internal stats logging level *log_level*	Sets the debug logging level.
debug platform internal stats logging {**err**|**trace**|**flow**}	Sets the debug logging type.

Managing Statistics Thresholds Using the GUI

Step 1 On the menu bar, choose **Fabric > Fabric Policies**.

Step 2 In the **Navigation** pane, click

- APIC مم The APIC cleans up objects including interfaces, EPGs, temperature sensors, and health statistics after one hour.

Specifying Syslog Sources and Destinations

This section explains how to create syslog destination groups, a syslog source, and

Creating a Syslog Destination and Destination Group

Before You Begin

Create a syslog

About Traceroute

The traceroute tool is used

i) Click **Submit** to launch the traceroute.

Step 6 In the **Navigation** pane or the **Traceroute Policies** table, click the traceroute policy.
The traceroute policy is displayed

Step 7 Click **SEARCH**.
A box

Step 10 Click **START** at the

Step 3 If

From the **Scheduler** pull-down menu, select either an existing schedule or create a new one by selecting **Create**

Supply the credentials (**User Name** and **Password**) of the server in the **Authentication Required** window. The troubleshooting report is then downloaded locally to your system.

The **ALL REPORTS** window appears (shown as

Hovering

The **Faults** screen shows the topology that

White boxes indicate that there are no issues to

Note By default, counters with zero values are hidden but the user can choose to see all the values.

You can also view all of the statistics for all managed objects at once by clicking the All icon (

The same logic applies if you click the **All** icon. All three tabs (**DROP STATS**, **CONTRACT DROPS**, and **TRAFFIC STATS)** are also available and have the same type

Related Topics

Using the Contracts Troubleshooting Screen, on page 70

Using the Contracts Troubleshooting Screen

Click **Contracts** in the left navigation pane (shown as follows) to begin using the **Contracts** troubleshooting screen.

Each one of the blue table heading rows (shown above) indicates a filter. There are multiple rows under each filter that indicate multiple filter

- Any to Any
- Context Deny

These contracts are categorized from the Source

If you select the All icon ( ) for the **All Changes** screen, you can see all the events indicating any changes

Using the Traceroute Troubleshooting Screen

Click

This protocol is uni-directional, in that it does a traceroute from the Source leaf to the Destination endpoint only.

- **tcp**
  This protocol is also bi-directional, as described above for the **udp** protocol.

- **udp**
  This protocol is bi-directional, in that it does a traceroute from the

Related Topics

Using the Atomic Counter Troubleshooting Screen, on page 79

Using the Atomic Counter Troubleshooting Screen

Click

The results are shown in two different formats. You can view them in either a brief format, which includes a summary,

Using the SPAN Troubleshooting Screen

Click **SPAN** in the left navigation pane (shown as follows) to begin using the **SPAN** troubleshooting screen.

Using this screen, you can span (or mirror) bi-directional traffic and redirect it to the analyzer. In a SPAN session, you are making a copy and sending it to the analyzer.

This copy goes to a particular host (the analyzer IP address) and then you can use

When you press the **Play** button, the polices are created on the system. When you press the **Stop** button,

interactive API

To create

generatereport API

To

getreportstatus API

To get the status of a generated report using the API,

deletesession API

To delete a particular troubleshooting session using the API, use the **deletesession** API. The module name

Used

- getsessiondetail API

Syntax Description

O	A				D			)		
- s					S		n			
- d					D		n			
- s					S		IP a			
- d					D		IP a			
-					S		MA			
- d					D		MA			
- s					L3		s	IP a		
- dP					L3		d	IP a		
- s			t		S	t	o t t		s	
-					En	t	o t t		s	
					Ti	w	f t	t	s	s f
					s	t				

P

- analyser	???
- desttype	Destination type
- spansrcports	Span source ports

generatereport API

To generate a troubleshooting report using the API, use the **generatereport** API. The module name is

Note There are no optional arguments (**opt_args**) for the getreportslist API.

getsessionslist API

To get a list of troubleshooting sessions using the API, use the **getsessionslist** API. The module name is **tr**

Format of report to be generated

Scheduler name for

contracts API

T

The following table lists the optional arguments (**opt_args**) and descriptions for each.

Syntax Description

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

Inspecting the Tunnel Interface Status

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

Step 1	In the menu bar, click **Fabric**.
Step 2	In the sub mR . eratihe lick

Example:

```
spine1# ls /mit/sys/bgp/inst/dom-apple/af-ipv4-ucast/
ctrl-l2vpn-evpn  ctrl-vpnv4-ucast  hostleak  summary
```

Step 2 Verify that the config-MO has been successfully processed by BGP, by entering a command such as the following in the spine-switch CLI:

Example:

```
spine1# show bgp lly
```

Shared RD: 192.41.1.5:4123 (L3VNI 2097154)
Paths: (1 available, best #1)
Flags: (0x00010a 00000000) on xmit-list, is not in rib/evpn
Multipath: eBGP iBGP

  Advertised path-id 1
  Path type: local 0x4000008c 0x0 ref 0, path is valid, is best path
  AS-Path: NONE, path locally originated
  EVPN network: [5]:[0]:[0]:[16]:[10.6.0.0]:[0.0.0.0] (VRF apple)
    10.10.41.2 (metric 0) from 0.0.0.0 (192.41.1.5)
      Origin IGP, MED not set, localpref 100, weight 32768
      Received

CHAPTER 9

Performing a Rebuild of the Fabric

This chapter explains how to rebuild your fabric.

Rebuilding the Fabric

This procedure is extremely disru

- No Java issues

Step 1 If you would like to retain your current configuration, you can perform a configuration export using the following procedure: http://www.cisco.com/c/en/us/td/docs/switches/

CHAPTER 10

Verifying IP-Based EPG Configurations

There are two types of endpoint groups (EPGs) that you can create: application EPGs and IP-based EPGs. IP-based EPGs differ from regular application EPGs in that they are

This is a view from the APIC point of view. You can

Once the configuration is there, when the packets arrive, the switch uses these objects to classify them.

Step 8 Verify that the pcTags for all the endpoints and IP addresses that you configured match. Every EPG has a

Verifying IP-EPG Configurations Using Switch Commands

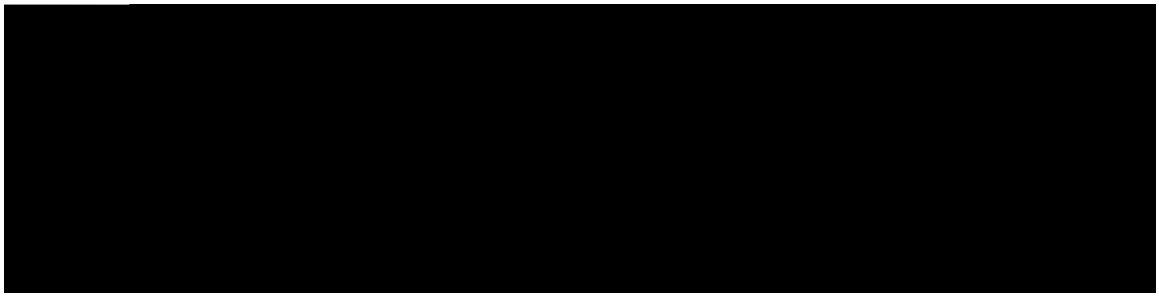
This procedure explains how to use switch commands to verify you IP-EPG ("IpCkt") configurations.

Step 1 Log in to the leaf.

Step 2 Navigate to the /mit/sys directory.

Step 3 In the /mit/sys directory, find ctx (vrf context directory)

Step 4 In the VRF cts directory, go to the specific BD directory where the IpCkt is configured.
You should see the IpCkt.
"IpCkt" and



CHAPTER

Example:

```
$LEAF_Address/api/node/mo/topology/pod-1/node-$LEAF_Id/sys/action.xml
<actionLSubj oDn="sys/phys-[eth1/49]">
<l1EthIfSetInServiceLTask adminSt='start'/>
</actionLSubj>
```

CHAPTER 12

Determining Why a PIM Interface Was Not Created

A PIM interface (pim:if) is created for L3Out interfaces (note that L3Out SVI interfaces are not supported), multicast tunnel interfaces (per VRF), SVI interfaces corresponding to PIM-enabled pervasive BDs, and l

A PIM Interface Was Not Created For a Multicast Tunnel Interface

If a PIM interface

CHAPTER 19

Confirming the Port Security Installation

This chapter explains how to confirm the port security installation in the APIC and leaf switch using Visore and how to confirm port security has been programmed in the hardware using the Cisco NX-OS-style CLI. For information about configuring port security, see the *Cisco Port Security* document.

This chapter contains the following sections:

Example:

CHAPTER 1

CHAPTER 19

Determining the Supported SSL Ciphers

Determining the Supported SSL Ciphers Using the CLI

Before You Begin

This section describes how to use the CLI to determine which SSL ciphers are supported.

Step 1 Get the supported ciphers in your openssl environment, shown as follows:

Example:

```
openssl ciphers 'ALL:eNULL'
```

Step 2 Separate the ciphers using sed or some other tool, shown

Example:

CHAPTER 10

Removing Unwanted _ui_ Objects

Changes made through the APIC Basic GU

Perform the POST tp

Syntax Description

Option	Function
	Displays the data layer state for a service on

APPENDIX B

DETAILED STEPS

Sendin an On-Demand Tech Suppo

Sendi Demand Techsupport File e GUI

Step 1 In the menu bar, cl

Step 2

</fileRemt m G m a o mt t

APPENDIX C

Finding the Switch Inventory

Knowing your switch model and serial numbers can help TAC support with troubleshooting your fabric. This section explains how to find the switch model and serial numbers using the Cisco APIC GUI, CLI, and REST API.

Finding Your Switch Inventory Using the NX-OS CLI

This section

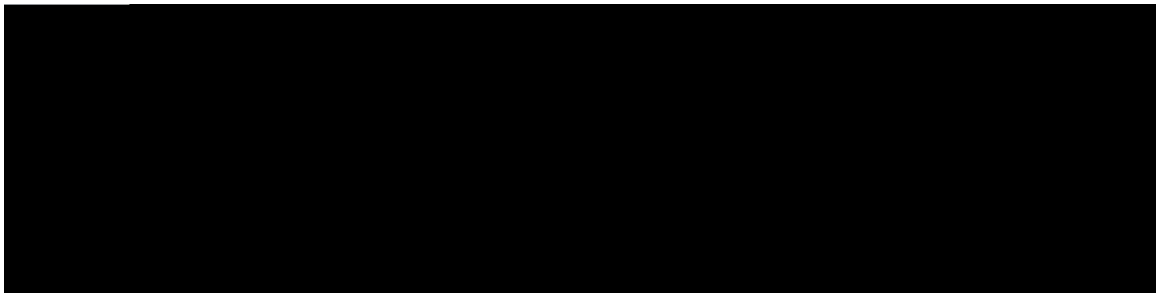
```
is not available

================================================================================
```

Finding Your Switch Inventory Using the REST API

This section explains how to find your switch model and serial numbers using the REST API

Find your switch inventory as

"id":"105",



INDEX