Cisco APIC Layer 2 Networking Configuration Guide

First Published: 2017-04-11
Last Modified: 2019-01-31

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

PREFACE

Preface xi
  Audience xi
  Document Conventions xi
  Related Documentation xiii
  Documentation Feedback xiv
  Obtaining Documentation and Submitting a Service Request xiv

CHAPTER 1

New and Changed 1
  New and Changed Information 1

CHAPTER 2

Cisco ACI Forwarding 9
  ACI Fabric Optimizes Modern Data Center Traffic Flows 9
  VXLAN in ACI 10
  Layer 3 VNIDs Facilitate Transporting Inter-subnet Tenant Traffic 12

CHAPTER 3

Prerequisites for Configuring Layer 2 Networks 15
  Layer 2 Prerequisites 15

CHAPTER 4

Networking Domains 17
  Networking Domains 17
  Related Documents 18
  Bridge Domains 18
    About Bridge Domains 18
  VMM Domains 18
    Virtual Machine Manager Domain Main Components 18
    Virtual Machine Manager Domains 19
Contents

Configuring Physical Domains 20
Configuring a Physical Domain 20
Configuring a Physical Domain Using the REST API 20

CHAPTER 5  Bridging 23
Bridged Interface to an External Router 23
Bridge Domains and Subnets 24
Bridge Domain Options 26
Creating a Tenant, VRF, and Bridge Domain Using the GUI 27
Creating a Tenant, VRF, and Bridge Domain Using the NX-OS Style CLI 28
Creating a Tenant, VRF, and Bridge Domain Using the REST API 30
Configuring an Enforced Bridge Domain 30
Configuring an Enforced Bridge Domain Using the NX-OS Style CLI 31
Configuring an Enforced Bridge Domain Using the REST API 32
Configuring Flood in Encapsulation for All Protocols and Proxy ARP Across Encapsulations 33

CHAPTER 6  EPGs 39
About Endpoint Groups 39
Endpoint Groups 39
Access Policies Automate Assigning VLANs to EPGs 42
Per Port VLAN 43
VLAN Guidelines for EPGs Deployed on VPCs 45
Deploying an EPG on a Specific Port 45
Deploying an EPG on a Specific Node or Port Using the GUI 45
Deploying an EPG on a Specific Port with APIC Using the NX-OS Style CLI 46
Deploying an EPG on a Specific Port with APIC Using the REST API 47
Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port 48
Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port 48
Creating Domains, and VLANS to Deploy an EPG on a Specific Port Using the GUI 49
Creating AEP, Domains, and VLANs to Deploy an EPG on a Specific Port Using the NX-OS Style CLI 50
Creating AEP, Domains, and VLANs to Deploy an EPG on a Specific Port Using the REST API 51
Deploying EPGs to Multiple Interfaces Through Attached Entity Profiles 52
Deploying an Application EPG through an AEP or Interface Policy Group to Multiple Ports  52
Deploying an EPG through an AEP to Multiple Interfaces Using the APIC GUI  52
Deploying an EPG through an Interface Policy Group to Multiple Interfaces Using the NX-OS Style CLI  53
Deploying an EPG through an AEP to Multiple Interfaces Using the REST API  54
Intra-EPG Isolation  56
Intra-EPG Endpoint Isolation  56
Intra-EPG Isolation for Bare Metal Servers  56
  Intra-EPG Isolation for Bare Metal Servers Using the GUI  57
  Configuring Intra-EPG Isolation for Bare Metal Servers Using the NX-OS Style CLI  58
  Configuring Intra-EPG Isolation for Bare Metal Servers Using the REST API  60
Intra-EPG Isolation for VMware vDS  60
  Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch  60
  Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the GUI  62
  Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the NX-OS Style CLI  63
  Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the REST API  64
Intra-EPG Isolation for AVS  65
  Intra-EPG Isolation Enforcement for Cisco AVS  65
  Configuring Intra-EPG Isolation for Cisco AVS Using the GUI  66
  Configuring Intra-EPG Isolation for Cisco AVS Using the NX-OS Style CLI  67
  Configuring Intra-EPG Isolation for Cisco AVS Using the REST API  67
  Choosing Statistics to View for Isolated Endpoints on Cisco AVS  68
  Viewing Statistics for Isolated Endpoints on Cisco AVS  68

CHAPTER 7   Access Interfaces  71

Physical Ports  71
  Configuring Leaf Switch Physical Ports Using Policy Association  71
  Configuring Leaf Switch Physical Ports Using Port Association  72
  Configuring Physical Ports in Leaf Nodes and FEX Devices Using the NX-OS CLI  73
Port Cloning  76
  Cloning Port Configurations  76
Cloning a Configured Leaf Switch Port Using the APIC GUI  

Port Channels  
ACI Leaf Switch Port Channel Configuration Using the GUI  
Configuring Port Channels in Leaf Nodes and FEX Devices Using the NX-OS CLI  
Configuring Two Port Channels Applied to Multiple Switches Using the REST API  

Virtual Port Channels  
ACI Virtual Port Channel Workflow  
ACI Leaf Switch Virtual Port Channel Configuration Using the GUI  
Configuring Virtual Port Channels in Leaf Nodes and FEX Devices Using the NX-OS CLI  
Configuring Virtual Port Channels Using the REST API  
Configuring a Single Virtual Port Channel Across Two Switches Using the REST API  
Configuring a Virtual Port Channel on Selected Port Blocks of Two Switches Using the REST API  
Configuring a Single Virtual Port Channel Across Two Switches Using the REST API  

Reflective Relay  
Reflective Relay (802.1Qbg)  
Enabling Reflective Relay Using the Advanced GUI  
Enabling Reflective Relay Using the NX-OS CLI  
Enabling Reflective Relay Using the REST API  

FEX Interfaces  
Configuring Port, PC, and VPC Connections to FEX Devices  
ACI FEX Guidelines  
FEX Virtual Port Channels  
Configuring a Basic FEX Connection Using the GUI  
Configuring FEX Port Channel Connections Using the GUI  
Configuring FEX VPC Connections Using the GUI  
Configuring an FEX VPC Policy Using the REST API  
Configuring FEX Connections Using Profiles with the NX-OS Style CLI  
Configuring Port Profiles to Change Ports from Uplink to Downlink or Downlink to Uplink  
Configuring Port Profiles  
Port Profile Configuration Summary  
Configuring a Port Profile Using the GUI  
Configuring a Port Profile Using the NX-OS Style CLI  
Configuring a Port Profile Using the REST API
CHAPTER 8

FCoE Connections  121

Supporting Fibre Channel over Ethernet Traffic on the ACI Fabric  121
Configuring FCoE Using the Advanced GUI  124

FCoE GUI Configuration  124
FCoE Policy, Profile, and Domain Configurations  124
Deploying FCoE vFC Ports Using the APIC GUI  127
Deploying EPG Access to vFC Ports Using the APIC GUI  133
Deploying the EPG to Support the FCoE Initiation Protocol  136
Undeploying FCoE Connectivity Using the APIC GUI  138

Configuring FCoE Using the NX_OS Style CLI  140

FCoE NX-OS Style CLI Configuration  140
Configuring FCoE Connectivity Without Policies or Profiles Using the NX-OS Style CLI  140
Configuring FCoE Connectivity With Policies and Profiles Using the NX-OS Style CLI  143
Configuring FCoE Over FEX Using NX-OS Style CLI  147
Verifying FCoE Configuration Using the NX-OS Style CLI  149
Undeploying FCoE Elements Using the NX-OS Style CLI  150

Configuring FCoE Using the REST API  151
Configuring FCoE Connectivity Using the REST API  151
Configuring FCoE Over FEX Using REST API  154
Undeploying FCoE Connectivity through the REST API or SDK  158

CHAPTER 9

Fibre Channel NPV  165

Fibre Channel Connectivity Overview  165
FC NPV Guidelines and Limitations  166
Configuring FC NPV Using the GUI  167

FC Connectivity Basic Configuration Using the APIC GUI  172
Configuring FC Connectivity Without Policies or Profiles Using the NX-OS CLI  173
Configuring FC Connectivity With Policies or Profiles Using the NX-OS CLI  174
Configuring FC Connectivity Using the REST API  176

CHAPTER 10

802.1Q Tunnels  181

About ACI 802.1Q Tunnels  181
Traffic Storm Control  225
  About Traffic Storm Control  225
  Storm Control Guidelines  225
  Configuring a Traffic Storm Control Policy Using the GUI  226
  Configuring a Traffic Storm Control Policy Using the NX-OS Style CLI  228
  Configuring a Traffic Storm Control Policy Using the REST API  229

MACsec  231
  About MACsec  231
  Guidelines and Limitations for MACsec  232
  Configuring MACsec for Fabric Links Using the GUI  234
  Configuring MACsec for Access Links Using the GUI  234
  Configuring MACsec Parameters Using the APIC GUI  235
  Configuring MACsec Keychain Policy Using the GUI  235
  Configuring MACsec Using the NX-OS Style CLI  236
  Configuring MACsec Using the REST API  238
Preface

This preface includes the following sections:

- Audience, on page xi
- Document Conventions, on page xi
- Related Documentation, on page xiii
- Documentation Feedback, on page xiv
- Obtaining Documentation and Submitting a Service Request, on page xiv

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Virtual machine installation and administration
- Server administration
- Switch and network administration

Document Conventions

Command descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Bold text indicates the commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic text indicates arguments for which the user supplies the values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
</tbody>
</table>
## Convention

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nested set of square brackets or braces indicate optional or required</td>
</tr>
<tr>
<td>choices within optional or required elements. Braces and a vertical bar</td>
</tr>
<tr>
<td>within square brackets indicate a required choice within an optional</td>
</tr>
<tr>
<td>element.</td>
</tr>
<tr>
<td>variable</td>
</tr>
<tr>
<td>Indicates a variable for which you supply values, in context where italics</td>
</tr>
<tr>
<td>cannot be used.</td>
</tr>
<tr>
<td>string</td>
</tr>
<tr>
<td>A nonquoted set of characters. Do not use quotation marks around the</td>
</tr>
<tr>
<td>string or the string will include the quotation marks.</td>
</tr>
</tbody>
</table>

Examples use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screen font</td>
<td>Terminal sessions and information the switch displays are in screen font.</td>
</tr>
<tr>
<td>boldface screen font</td>
<td>Information you must enter is in boldface screen font.</td>
</tr>
<tr>
<td>italic screen font</td>
<td>Arguments for which you supply values are in italic screen font.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
<tr>
<td>[]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line</td>
</tr>
<tr>
<td></td>
<td>of code indicates a comment line.</td>
</tr>
</tbody>
</table>

This document uses the following conventions:

### Note

Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

### Caution

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

### Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS
Related Documentation

Application Policy Infrastructure Controller (APIC) Documentation

The following companion guides provide documentation for APIC:

- Cisco APIC Getting Started Guide
- Cisco APIC Basic Configuration Guide
- Cisco ACI Fundamentals
- Cisco APIC Layer 2 Networking Configuration Guide
- Cisco APIC Layer 3 Networking Configuration Guide
- Cisco APIC NX-OS Style Command-Line Interface Configuration Guide
- Cisco APIC REST API Configuration Guide
- Cisco APIC Layer 4 to Layer 7 Services Deployment Guide
- Cisco ACI Virtualization Guide
- Cisco Application Centric Infrastructure Best Practices Guide

All these documents are available at the following URL: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Cisco Application Centric Infrastructure (ACI) Documentation


Cisco Application Centric Infrastructure (ACI) Simulator Documentation


Cisco Nexus 9000 Series Switches Documentation


Cisco Application Virtual Switch Documentation

Cisco Application Centric Infrastructure (ACI) Integration with OpenStack Documentation


Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to apic-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to What’s New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.
New and Changed Information

The following table provides an overview of the significant changes to the chapters in his guide up to the current release. The table does not provide an exhaustive list of all changes made to the topics or of the new features up to this release.

Table 1: New Features and Changed Information for Cisco APIC 3.2(1x)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced Breakout Support on Profiled QSFP Ports on N9K-C93180YC-FX Switches</td>
<td>Support is added for 100 Gigabit (Gb) (4X25Gb) and 40Gb (4X10Gb) dynamic breakouts on profiled QSFP ports on the N9K-C93180YC-FX switch (in ACI mode).</td>
<td>Dynamic Breakout Ports</td>
</tr>
<tr>
<td>Enhanced Port Profile Support on N9K-C93180YC-FX Switches</td>
<td>Support is added on the N9K-C93180YC-FX switch for port profiles to change ports from uplink to downlink or downlink to uplink.</td>
<td>Configuring Port Profiles to Change Ports from Uplink to Downlink or Downlink to Uplink</td>
</tr>
<tr>
<td>Fibre Channel NPV</td>
<td>Support for FC traffic over the Fabric</td>
<td>Fibre Channel Connectivity</td>
</tr>
<tr>
<td>Cloning Port Configurations</td>
<td>Support for cloning port configurations is added. After you configure a leaf switch port, you can copy the configuration and apply it to other ports.</td>
<td>Access Interfaces</td>
</tr>
</tbody>
</table>
Where Documented
Description
Where Documented

Flood in encapsulation enhancements
Information is added about protocols supporting the Flood in Encapsulation option for bridge domains or EPGs.
Bridging

Table 2: New Features and Changed Information for Cisco APIC 3.1(2m)

<table>
<thead>
<tr>
<th>Feature or Change</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced Breakout Support on Profiled QSFP Ports on N9K-C9336C-FX2 Switches</td>
<td>Support is added for 100Gb (4X25Gb) and 40Gb(4X10Gb) dynamic breakouts on profiled QSFP ports on the N9K-C9336C-FX2 switch (in ACI mode).</td>
<td>Dynamic Breakout Ports</td>
</tr>
</tbody>
</table>

Table 3: New Features and Changed Information for Cisco APIC 3.1(1)

<table>
<thead>
<tr>
<th>Feature or Change</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabling IP Learning per Bridge Domain</td>
<td>IP learning per bridge domain is disabled when two hosts are connected as active and standby hosts to the Cisco ACI switches. The MAC learning still occurs in the hardware but the IP learning only occurs from the ARP/GARP/ND processes. This enhancement allows for flexible deployments, for example, firewalls or local gateways.</td>
<td>Bridge Domain Options</td>
</tr>
<tr>
<td>MACsec</td>
<td>MACsec provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys.</td>
<td>MACsec</td>
</tr>
<tr>
<td>Feature or Change</td>
<td>Description</td>
<td>Where Documented</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Flood in Encapsulation</td>
<td>Beginning with Cisco ACI Release 3.1(1) on the Cisco ACI switches with the next generation ASICs and onwards, all protocols are flooded in encapsulation. Multiple EPGs are now supported under one bridge domain with an external switch. When two EPGs share the same BD and the Flood in Encapsulation option is turned on, the EPG flooding traffic does not reach the other EPG. It overcomes the challenges of using the Cisco ACI switches with the Virtual Connect (VC) tunnel network.</td>
<td>Flood in Encapsulation</td>
</tr>
</tbody>
</table>
| Basic GUI topics removed | Basic GUI procedures are no longer supported | The following topics have been removed:  
• Creating a Tenant, VRF, and Bridge Domain Using the Basic GUI  
• Configuring an Enforced Bridge Domain Using the Basic GUI  
• Deploying FCoE vFC Ports Using the Basic GUI  
• Creating a VSAN Domain Using the APIC Basic GUI  
• Configuring 802.1Q Tunnel Interfaces Using the Basic GUI  
• Configuring Dynamic Breakout Ports with the Basic GUI |
| Breakout Support for 100Gb (4X25Gb) Ports on N9K-C93180LC-EX Switches | Support is added for 100Gb (4X25Gb) dynamic breakouts on the N9K-C93180LC-EX switch (in ACI mode). | Dynamic Breakout Ports |
### Table 4: New Features and Changed Information for Cisco APIC 3.0(x)

<table>
<thead>
<tr>
<th>Feature or Change</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q-in-Q Encapsulation Mapping for EPGs</td>
<td>With this release, you can map double-tagged VLAN traffic ingressing on a regular interface, PC, or VPC to an EPG.</td>
<td>Q-in-Q Encapsulation Mapping for EPGs</td>
</tr>
<tr>
<td>Enforced Bridge Domain</td>
<td>Enforced bridge domain is supported, in which an endpoint in a subject endpoint group (EPG) can only ping subnet gateways within the associated bridge domain. With this configuration enabled, you can create a global exception list of IP addresses which can ping any subnet gateway.</td>
<td>Enforced Bridge Domain in Bridging</td>
</tr>
<tr>
<td>Configuring Leaf Switch Using Port Association</td>
<td>Using these GUI steps, you can now choose the port and then apply a policy to it.</td>
<td>Configuring Leaf Switch Physical Ports Using Port Association</td>
</tr>
</tbody>
</table>

### Table 5: New Features and Changed Information for Cisco APIC 2.3(1e) Release

<table>
<thead>
<tr>
<th>Feature or Change</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q Tunnel enhancements</td>
<td>Now you can configure ports on core-switches for use in Dot1q Tunnels for multiple customers. You can also define access VLANs to distinguish between customers consuming the corePorts. You can also disable MAC learning on Dot1q Tunnels.</td>
<td>802.1Q Tunnels</td>
</tr>
<tr>
<td>Symmetric hashing</td>
<td>Symmetric hashing is now supported on port channels.</td>
<td>Port Channels</td>
</tr>
<tr>
<td>Reflective relay (802.1Qbg)</td>
<td>Reflective relay transfers switching for virtual machines out of the host server to an external network switch. It provides connectivity between VMs on the same physical server and the rest of the network. It allows policies that you configure on the Cisco APIC to apply to traffic between the VMs on the same server.</td>
<td>Access Interfaces</td>
</tr>
<tr>
<td>Feature or Change</td>
<td>Description</td>
<td>Where Documented</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Traffic Storm control</td>
<td>Allows you to configure Storm Control on each traffic type separately.</td>
<td>Traffic Storm Control</td>
</tr>
<tr>
<td>Unicast/Multicast differentiation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 6: New Features and Changed Information in Cisco APIC Release 2.2(2e)**

<table>
<thead>
<tr>
<th>Feature or Change</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Reorganization</td>
<td>The topics in this guide were collected from Cisco APIC Basic Configuration Guide and the following APIC articles:</td>
<td>Cisco APIC Layer 2 Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>• Cisco ACI and 802.1Q Tunnels</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco APIC EPG Deployment to Specific Ports Using Domains, Attach Entity Profiles, and VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco APIC and Traffic Storm Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco APIC and Dynamic Breakout Ports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco APIC and Proxy ARP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Deploying an EPG on a Specific Port Using Cisco APIC</td>
<td></td>
</tr>
</tbody>
</table>

**Table 7: New Features and Changed Behavior in Cisco APIC 2.2 (1n) Release**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCoE over FEX</td>
<td>You can now configure FCoE over FEX ports.</td>
<td>FCoE Connections</td>
</tr>
<tr>
<td>CDP supported in policies on interfaces to FEX devices</td>
<td>In this release, support is added for CDP on interfaces to FEX devices.</td>
<td>Access Interfaces</td>
</tr>
<tr>
<td>802.1Q Tunnels</td>
<td>You can now configure 802.1Q tunnels on edge ports to enable point-to-multi-point tunneling of Ethernet frames in the fabric, with Quality of Service (QoS) priority settings.</td>
<td>802.1Q Tunnels</td>
</tr>
</tbody>
</table>
**Dynamic Breakout Ports**

To enable a 40 Gigabit Ethernet (GE) leaf switch port to be connected to 4-10GE capable (downlink) devices (connected with Cisco 40-Gigabit to 4X10-Gigabit breakout cables), you configure the 40GE port to breakout (split) to 4-10GE ports.

---

**Table 8: New Features and Changed Information for Cisco APIC 2.1(x) Release**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Breakout Ports</td>
<td>To enable a 40 Gigabit Ethernet (GE) leaf switch port to be connected to 4-10GE capable (downlink) devices (connected with Cisco 40-Gigabit to 4X10-Gigabit breakout cables), you configure the 40GE port to breakout (split) to 4-10GE ports.</td>
<td><em>Dynamic Breakout Ports.</em></td>
</tr>
</tbody>
</table>

---

**Table 9: New Features and Changed Information for Cisco APIC 2.0(2x) Release**

<table>
<thead>
<tr>
<th>Feature or Change</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision to topic Configuring a Traffic Storm Control Policy Using the CLI</td>
<td>The topic was replaced with a new topic that uses the NX-OS Style CLI.</td>
<td>See Configuring a Traffic Storm Control Policy Using the NX-OS Style CLI in Traffic Storm Control.</td>
</tr>
</tbody>
</table>

---

**Table 10: New Features and Changed Behavior in Cisco APIC for Cisco APIC Release 2.0(1m)**

<table>
<thead>
<tr>
<th>Feature or Change</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy ARP</td>
<td>Proxy ARP in Cisco ACI enables endpoints within a network or subnet to communicate with other endpoints without knowing the real MAC address of the endpoints. Proxy ARP is aware of the location of the traffic destination, and offers its own MAC address as the final destination instead.</td>
<td><em>Proxy ARP</em></td>
</tr>
</tbody>
</table>

---

**Table 11: New Features and Changed Information for Cisco APIC 2.1(x) Release**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fibre Channel over Ethernet (FCoE) support</td>
<td>An overview and configuration topics for implementing FCoE connectivity over the ACI fabric.</td>
<td><em>FCoE Connections</em></td>
</tr>
</tbody>
</table>
### Table 11: New Features and Changed Behavior in Cisco APIC for Cisco APIC Release 1.3(1g)

<table>
<thead>
<tr>
<th>Feature or Change</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Removed object model CLI procedure and replaced with NX-OS-Style CLI procedures.</td>
<td>Creating AEP, Domains, and VLANs to Deploy an EPG on a Specific Port Using the NX-OS CLI Deploying and EPG on a Specific Port with APIC Using the NX-OS Style CLI</td>
</tr>
</tbody>
</table>
Cisco ACI Forwarding

This chapter contains the following sections:

- ACI Fabric Optimizes Modern Data Center Traffic Flows, on page 9
- VXLAN in ACI, on page 10
- Layer 3 VNIDs Facilitate Transporting Inter-subnet Tenant Traffic, on page 12

ACI Fabric Optimizes Modern Data Center Traffic Flows

The Cisco ACI architecture addresses the limitations of traditional data center design, and provides support for the increased east-west traffic demands of modern data centers.

Today, application design drives east-west traffic from server to server through the data center access layer. Applications driving this shift include big data distributed processing designs like Hadoop, live virtual machine or workload migration as with VMware vMotion, server clustering, and multi-tier applications.

North-south traffic drives traditional data center design with core, aggregation, and access layers, or collapsed core and access layers. Client data comes in from the WAN or Internet, a server processes it, and then it exits the data center, which permits data center hardware oversubscription due to WAN or Internet bandwidth constraints. However, Spanning Tree Protocol is required to block loops. This limits available bandwidth due to blocked links, and potentially forces traffic to take a suboptimal path.

In traditional data center designs, IEEE 802.1Q VLANs provide logical segmentation of Layer 2 boundaries or broadcast domains. However, VLAN use of network links is inefficient, requirements for device placements in the data center network can be rigid, and the VLAN maximum of 4094 VLANs can be a limitation. As IT departments and cloud providers build large multi-tenant data centers, VLAN limitations become problematic.

A spine-leaf architecture addresses these limitations. The ACI fabric appears as a single switch to the outside world, capable of bridging and routing. Moving Layer 3 routing to the access layer would limit the Layer 2 reachability that modern applications require. Applications like virtual machine workload mobility and some clustering software require Layer 2 adjacency between source and destination servers. By routing at the access layer, only servers connected to the same access switch with the same VLANs trunked down would be Layer 2-adjacent. In ACI, VXLAN solves this dilemma by decoupling Layer 2 domains from the underlying Layer 3 network infrastructure.
As traffic enters the fabric, ACI encapsulates and applies policy to it, forwards it as needed across the fabric through a spine switch (maximum two-hops), and de-encapsulates it upon exiting the fabric. Within the fabric, ACI uses Intermediate System-to-Intermediate System Protocol (IS-IS) and Council of Oracle Protocol (COOP) for all forwarding of endpoint to endpoint communications. This enables all ACI links to be active, equal cost multipath (ECMP) forwarding in the fabric, and fast-reconverging. For propagating routing information between software defined networks within the fabric and routers external to the fabric, ACI uses the Multiprotocol Border Gateway Protocol (MP-BGP).

**VXLAN in ACI**

VXLAN is an industry-standard protocol that extends Layer 2 segments over Layer 3 infrastructure to build Layer 2 overlay logical networks. The ACI infrastructure Layer 2 domains reside in the overlay, with isolated broadcast and failure bridge domains. This approach allows the data center network to grow without the risk of creating too large a failure domain.

All traffic in the ACI fabric is normalized as VXLAN packets. At ingress, ACI encapsulates external VLAN, VXLAN, and NVGRE packets in a VXLAN packet. The following figure shows ACI encapsulation normalization.

![Figure 1: ACI Fabric](image)
Forwarding in the ACI fabric is not limited to or constrained by the encapsulation type or encapsulation overlay network. An ACI bridge domain forwarding policy can be defined to provide standard VLAN behavior where required.

Because every packet in the fabric carries ACI policy attributes, ACI can consistently enforce policy in a fully distributed manner. ACI decouples application policy EPG identity from forwarding. The following illustration shows how the ACI VXLAN header identifies application policy within the fabric.

The ACI VXLAN packet contains both Layer 2 MAC address and Layer 3 IP address source and destination fields, which enables efficient and scalable forwarding within the fabric. The ACI VXLAN packet header source group field identifies the application policy endpoint group (EPG) to which the packet belongs. The VXLAN Instance ID (VNID) enables forwarding of the packet through tenant virtual routing and forwarding (VRF) domains within the fabric. The 24-bit VNID field in the VXLAN header provides an expanded address space for up to 16 million unique Layer 2 segments in the same network. This expanded address space gives IT departments and cloud providers greater flexibility as they build large multitenant data centers.

VXLAN enables ACI to deploy Layer 2 virtual networks at scale across the fabric underlay Layer 3 infrastructure. Application endpoint hosts can be flexibly placed in the data center network without concern for the Layer 3 boundary of the underlay infrastructure, while maintaining Layer 2 adjacency in a VXLAN overlay network.
Layer 3 VNIDs Facilitate Transporting Inter-subnet Tenant Traffic

The ACI fabric provides tenant default gateway functionality that routes between the ACI fabric VXLAN networks. For each tenant, the fabric provides a virtual default gateway that spans all of the leaf switches assigned to the tenant. It does this at the ingress interface of the first leaf switch connected to the endpoint. Each ingress interface supports the default gateway interface. All of the ingress interfaces across the fabric share the same router IP address and MAC address for a given tenant subnet.

The ACI fabric decouples the tenant endpoint address, its identifier, from the location of the endpoint that is defined by its locator or VXLAN tunnel endpoint (VTEP) address. Forwarding within the fabric is between VTEPs. The following figure shows decoupled identity and location in ACI.

**Figure 4: ACI Decouples Identity and Location**

VXLAN uses VTEP devices to map tenant end devices to VXLAN segments and to perform VXLAN encapsulation and de-encapsulation. Each VTEP function has two interfaces:

- A switch interface on the local LAN segment to support local endpoint communication through bridging
- An IP interface to the transport IP network

The IP interface has a unique IP address that identifies the VTEP device on the transport IP network known as the infrastructure VLAN. The VTEP device uses this IP address to encapsulate Ethernet frames and transmit the encapsulated packets to the transport network through the IP interface. A VTEP device also discovers the remote VTEPs for its VXLAN segments and learns remote MAC Address-to-VTEP mappings through its IP interface.

The VTEP in ACI maps the internal tenant MAC or IP address to a location using a distributed mapping database. After the VTEP completes a lookup, the VTEP sends the original data packet encapsulated in VXLAN with the destination address of the VTEP on the destination leaf switch. The destination leaf switch de-encapsulates the packet and sends it to the receiving host. With this model, ACI uses a full mesh, single hop, loop-free topology without the need to use the spanning-tree protocol to prevent loops.

The VXLAN segments are independent of the underlying network topology; conversely, the underlying IP network between VTEPs is independent of the VXLAN overlay. It routes the encapsulated packets based on the outer IP address header, which has the initiating VTEP as the source IP address and the terminating VTEP as the destination IP address.

The following figure shows how routing within the tenant is done.
For each tenant VRF in the fabric, ACI assigns a single L3 VNID. ACI transports traffic across the fabric according to the L3 VNID. At the egress leaf switch, ACI routes the packet from the L3 VNID to the VNID of the egress subnet.

Traffic arriving at the fabric ingress that is sent to the ACI fabric default gateway is routed into the Layer 3 VNID. This provides very efficient forwarding in the fabric for traffic routed within the tenant. For example, with this model, traffic between 2 VMs belonging to the same tenant, on the same physical host, but on different subnets, only needs to travel to the ingress switch interface before being routed (using the minimal path cost) to the correct destination.

To distribute external routes within the fabric, ACI route reflectors use multiprotocol BGP (MP-BGP). The fabric administrator provides the autonomous system (AS) number and specifies the spine switches that become route reflectors.
Layer 3 VNIDs Facilitate Transporting Inter-subnet Tenant Traffic
Prerequisites for Configuring Layer 2 Networks

• Layer 2 Prerequisites, on page 15

Layer 2 Prerequisites

Before you begin to perform the tasks in this guide, complete the following:

• Install the ACI fabric and ensure that the APIC controllers are online, and the APIC cluster is formed and healthy—For more information, see Cisco APIC Getting Started Guide, Release 2.x.

• Create fabric administrator accounts for the administrators that will configure Layer 2 networks—For instructions, see the User Access, Authentication, and Accounting and Management chapters in Cisco APIC Basic Configuration Guide.

• Install and register the target leaf switches in the ACI fabric—For more information, see Cisco APIC Getting Started Guide, Release 2.x.

For information about installing and registering virtual switches, see Cisco ACI Virtualization Guide.

• Configure the tenants, VRFs, and EPGs (with application profiles and contracts) that will consume the Layer 2 networks—For instructions, see the Basic User Tenant Configuration chapter in Cisco APIC Basic Configuration Guide.

Caution

If you install 1 Gigabit Ethernet (GE) or 10GE links between the leaf and spine switches in the fabric, there is risk of packets being dropped instead of forwarded, because of inadequate bandwidth. To avoid the risk, use 40GE or 100GE links between the leaf and spine switches.
Layer 2 Prerequisites
Networking Domains

This chapter contains the following sections:

- Networking Domains, on page 17
- Bridge Domains, on page 18
- VMM Domains, on page 18
- Configuring Physical Domains, on page 20

Networking Domains

A fabric administrator creates domain policies that configure ports, protocols, VLAN pools, and encapsulation. These policies can be used exclusively by a single tenant, or shared. Once a fabric administrator configures domains in the ACI fabric, tenant administrators can associate tenant endpoint groups (EPGs) to domains.

The following networking domain profiles can be configured:

- VMM domain profiles (vmmDomP) are required for virtual machine hypervisor integration.
- Physical domain profiles (physDomP) are typically used for bare metal server attachment and management access.
- Bridged outside network domain profiles (l2extDomP) are typically used to connect a bridged external network trunk switch to a leaf switch in the ACI fabric.
- Routed outside network domain profiles (l3extDomP) are used to connect a router to a leaf switch in the ACI fabric.
- Fibre Channel domain profiles (fcDomP) are used to connect Fibre Channel VLANs and VSANs.

A domain is configured to be associated with a VLAN pool. EPGs are then configured to use the VLANs associated with a domain.

Note

EPG port and VLAN configurations must match those specified in the domain infrastructure configuration with which the EPG associates. If not, the APIC will raise a fault. When such a fault occurs, verify that the domain infrastructure configuration matches the EPG port and VLAN configurations.
Related Documents

For more information about Layer 3 Networking, see Cisco APIC Layer 3 Networking Configuration Guide.

For information about configuring VMM Domains, see Cisco ACI Virtual Machine Networking in Cisco ACI Virtualization Guide.

Bridge Domains

About Bridge Domains

A bridge domain (BD) represents a Layer 2 forwarding construct within the fabric. One or more endpoint groups (EPGs) can be associated with one bridge domain or subnet. A bridge domain can have one or more subnets that are associated with it. One or more bridge domains together form a tenant network. When you insert a service function between two EPGs, those EPGs must be in separate BDs. To use a service function between two EPGs, those EPGs must be isolated; this follows legacy service insertion based on Layer 2 and Layer 3 lookups.

VMM Domains

Virtual Machine Manager Domain Main Components

ACI fabric virtual machine manager (VMM) domains enable an administrator to configure connectivity policies for virtual machine controllers. The essential components of an ACI VMM domain policy include the following:

- **Virtual Machine Manager Domain Profile**—Groups VM controllers with similar networking policy requirements. For example, VM controllers can share VLAN pools and application endpoint groups (EPGs). The APIC communicates with the controller to publish network configurations such as port groups that are then applied to the virtual workloads. The VMM domain profile includes the following essential components:
  - **Credential**—Associates a valid VM controller user credential with an APIC VMM domain.
  - **Controller**—Specifies how to connect to a VM controller that is part of a policy enforcement domain. For example, the controller specifies the connection to a VMware vCenter that is part a VMM domain.

**Note**

A single VMM domain can contain multiple instances of VM controllers, but they must be from the same vendor (for example, from VMware or from Microsoft).

- **EPG Association**—Endpoint groups regulate connectivity and visibility among the endpoints within the scope of the VMM domain policy. VMM domain EPGs behave as follows:
  - The APIC pushes these EPGs as port groups into the VM controller.
• An EPG can span multiple VMM domains, and a VMM domain can contain multiple EPGs.

• **Attachable Entity Profile Association**—Associates a VMM domain with the physical network infrastructure. An attachable entity profile (AEP) is a network interface template that enables deploying VM controller policies on a large set of leaf switch ports. An AEP specifies which switches and ports are available, and how they are configured.

• **VLAN Pool Association**—A VLAN pool specifies the VLAN IDs or ranges used for VLAN encapsulation that the VMM domain consumes.

## Virtual Machine Manager Domains

An APIC VMM domain profile is a policy that defines a VMM domain. The VMM domain policy is created in APIC and pushed into the leaf switches.

*Figure 6: ACI VMM Domain VM Controller Integration*

VMM domains provide the following:

• A common layer in the ACI fabric that enables scalable fault-tolerant support for multiple VM controller platforms.

• VMM support for multiple tenants within the ACI fabric.

VMM domains contain VM controllers such as VMware vCenter or Microsoft SCVMM Manager and the credential(s) required for the ACI API to interact with the VM controller. A VMM domain enables VM mobility within the domain but not across domains. A single VMM domain can contain multiple instances of VM controllers but they must be the same kind. For example, a VMM domain can contain many VMware vCenters managing multiple controllers each running multiple VMs but it may not also contain SCVMM Managers. A VMM domain inventories controller elements (such as pNICs, vNICs, VM names, and so forth) and pushes policies into the controller(s), creating port groups, and other necessary elements. The ACI VMM domain listens for controller events such as VM mobility and responds accordingly.
Configuring Physical Domains

Configuring a Physical Domain

Physical domains control the scope of where a given VLAN namespace is used. The VLAN namespace that is associated with the physical domain is for non-virtualized servers, although it can also be used for static mapping of port-groups from virtualized servers. You can configure a physical domain for physical device types.

Before you begin

- Configure a tenant.

Procedure

| Step 1 | On the menu bar, click Fabric. |
| Step 2 | On the submenu bar, click External Access Policies. |
| Step 3 | In the Navigation pane, expand Physical and External Domains and click Physical Domains. |
| Step 4 | From the Actions drop-down list, choose Create Physical Domain. The Create Physical Domain dialog box appears. |
| Step 5 | Complete the following fields: |

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the physical domain profile.</td>
</tr>
<tr>
<td>Associate Attachable Entity Profiles</td>
<td>Choose the attachable entity profiles to be associated to this domain.</td>
</tr>
<tr>
<td>VLAN Pool</td>
<td>The VLAN pool used by the physical domain. The VLAN pool specifies the range or pool for VLANs that is allocated by the APIC for the service graph templates that are using this physical domain. Click Dynamic or Static allocation.</td>
</tr>
</tbody>
</table>

| Step 6 | (Optional) Add a AAA security domain and click the Select check box. |
| Step 7 | Click Submit. |

Configuring a Physical Domain Using the REST API

A physical domain acts as the link between the VLAN pool and the Access Entity Profile (AEP). The domain also ties the fabric configuration to the tenant configuration, as the tenant administrator is the one who associates domains to EPGs, while the domains are created under the fabric tab. When configuring in this order, only the profile name and the VLAN pool are configured.
Procedure

Configure a physical domain by sending a post with XML such as the following example:

Example:

```xml
<physDomP dn="uni/phys-bsprint-PHY" lcOwn="local" modTs="2015-02-23T16:13:21.906-08:00"
    monPolDn="uni/fabric/monfab-default" name="bsprint-PHY" ownerKey="" ownerTag="" status=""
    uid="8131">
    <infraRsVlanNs childAction="" forceResolve="no" lcOwn="local"
        modTs="2015-02-23T16:13:22.065-08:00"
        monPolDn="uni/fabric/monfab-default" rType="mo" rn="rsvlanNs" state="formed"
        stateQual="none"
        status="" tCl="fvnsVlanInstP" tDn="uni/infra/vlanns-[bsprint-vlan-pool]-static"
        tType="mo" uid="8131"/>
    <infraRsVlanNsDef forceResolve="no" lcOwn="local" modTs="2015-02-23T16:13:22.065-08:00"
        rType="" status=""
        tCl="fvnsVlanInstP" tDn="uni/infra/vlanns-[bsprint-vlan-pool]-static"
        tType="mo"/>
    <infraRtDomP lcOwn="local" modTs="2015-02-23T16:13:22.065-08:00"
        rn="rtdomP-[uni/infra/attentp-bsprint-AEP]"
        status="" tCl="infraAttEntityP" tDn="uni/infra/attentp-bsprint-AEP"/>
</physDomP>
```
Bridging

This chapter contains the following sections:

- Bridged Interface to an External Router, on page 23
- Bridge Domains and Subnets, on page 24
- Creating a Tenant, VRF, and Bridge Domain Using the GUI, on page 27
- Creating a Tenant, VRF, and Bridge Domain Using the NX-OS Style CLI, on page 28
- Creating a Tenant, VRF, and Bridge Domain Using the REST API, on page 30
- Configuring an Enforced Bridge Domain, on page 30
- Configuring Flood in Encapsulation for All Protocols and Proxy ARP Across Encapsulations, on page 33

Bridged Interface to an External Router

As shown in the figure below, when the leaf switch interface is configured as a bridged interface, the default gateway for the tenant VNID is the external router.

*Figure 7: Bridged External Router*

The ACI fabric is unaware of the presence of the external router and the APIC statically assigns the leaf switch interface to its EPG.
Bridge Domains and Subnets

A bridge domain (fvBD) represents a Layer 2 forwarding construct within the fabric. The following figure shows the location of bridge domains (BDs) in the management information tree (MIT) and their relation to other objects in the tenant.

*Figure 8: Bridge Domains*

A BD must be linked to a VRF (also known as a context or private network). With the exception of a Layer 2 VLAN, it must have at least one subnet (fvSubnet) associated with it. The BD defines the unique Layer 2 MAC address space and a Layer 2 flood domain if such flooding is enabled. While a VRF defines a unique IP address space, that address space can consist of multiple subnets. Those subnets are defined in one or more BDs that reference the corresponding VRF.

The options for a subnet under a BD or under an EPG are as follows:

- **Public**—the subnet can be exported to a routed connection.
- **Private**—the subnet applies only within its tenant.
- **Shared**—the subnet can be shared with and exported to multiple VRFs in the same tenant or across tenants as part of a shared service. An example of a shared service is a routed connection to an EPG present in another VRF in a different tenant. This enables traffic to pass in both directions across VRFs. An EPG that provides a shared service must have its subnet configured under that EPG (not under a BD), and its scope must be set to advertised externally, and shared between VRFs.

**Note**

Shared subnets must be unique across the VRF involved in the communication. When a subnet under an EPG provides a Layer 3 external network shared service, such a subnet must be globally unique within the entire ACI fabric.

BD packet behavior can be controlled in the following ways:
### Packet Type | Mode
--- | ---
ARP | You can enable or disable **ARP Flooding**; without flooding, ARP packets are sent with unicast.  
**Note** If the limitIpLearnToSubnets in fvBD is set, endpoint learning is limited to the BD only if the IP address is in a configured subnet of the BD or an EPG subnet that is a shared service provider.

Unknown Unicast | **L2 Unknown Unicast**, which can be **Flood** or **Hardware Proxy**.  
**Note** When the BD has **L2 Unknown Unicast** set to **Flood**, if an endpoint is deleted the system deletes it from both the local leaf switches as well as the remote leaf switches where the BD is deployed, by selecting **Clear Remote MAC Entries**. Without this feature, the remote leaf continues to have this endpoint learned until the timer expires.  
Modifying the **L2 Unknown Unicast** setting causes traffic to bounce (go down and up) on interfaces to devices attached to EPGs associated with this bridge domain.

Unknown IP Multicast | **L3 Unknown Multicast Flooding**  
**Flood**—Packets are flooded on ingress and border leaf switch nodes only. With N9K-93180YC-EX, packets are flooded on all the nodes where a bridge domain is deployed.  
**Optimized**—Only 50 bridge domains per leaf are supported. This limitation is not applicable for N9K-93180YC-EX.

L2 Multicast, Broadcast, Unicast | **Multi-Destination Flooding**, which can be one of the following:  
- **Flood in BD**—flood in bridge domain  
- **Flood in Encapsulation**—flood in encapsulation  
- **Drop**—drop the packets
Beginning with Cisco APIC Release 3.1(1), on the Cisco Nexus 9000 series switches (with names ending with EX and FX and onwards), the following protocols can be flooded in encapsulation or flooded in a bridge domain: OSPF/OSPFv3, BGP, EIGRP, CDP, LACP, LLDP, ISIS, IGMP, PIM, ST-BPDU, ARP/GARP, RARP, ND.

Note
Bridge domains can span multiple switches. A bridge domain can contain multiple subnets, but a subnet is contained within a single bridge domain. If the bridge domain (fvBD) limitIPLearnToSubnets property is set to yes, endpoint learning will occur in the bridge domain only if the IP address is within any of the configured subnets for the bridge domain or within an EPG subnet when the EPG is a shared service provider. Subnets can span multiple EPGs; one or more EPGs can be associated with one bridge domain or subnet. In hardware proxy mode, ARP traffic is forwarded to an endpoint in a different bridge domain when that endpoint has been learned as part of the Layer 3 lookup operation.

Bridge Domain Options
A bridge domain can be set to operate in flood mode for unknown unicast frames or in an optimized mode that eliminates flooding for these frames. When operating in flood mode, Layer 2 unknown unicast traffic is flooded over the multicast tree of the bridge domain (GiPo). For the bridge domain to operate in optimized mode you should set it to hardware-proxy. In this case, Layer 2 unknown unicast frames are sent to the spine-proxy anycast VTEP address.

Caution
Changing from unknown unicast flooding mode to hw-proxy mode is disruptive to the traffic in the bridge domain.

If IP routing is enabled in the bridge domain, the mapping database learns the IP address of the endpoints in addition to the MAC address.

The Layer 3 Configurations tab of the bridge domain panel allows the administrator to configure the following parameters:

- **Unicast Routing**: If this setting is enabled and a subnet address is configured, the fabric provides the default gateway function and routes the traffic. Enabling unicast routing also instructs the mapping database to learn the endpoint IP-to-VTEP mapping for this bridge domain. The IP learning is not dependent upon having a subnet configured under the bridge domain.

- **Subnet Address**: This option configures the SVI IP addresses (default gateway) for the bridge domain.

- **Limit IP Learning to Subnet**: This option is similar to a unicast reverse-forwarding-path check. If this option is selected, the fabric will not learn IP addresses from a subnet other than the one configured on the bridge domain.
Enabling Limit IP Learning to Subnet is disruptive to the traffic in the bridge domain.

**Disabling IP Learning per Bridge Domain**

IP learning per bridge domain is disabled when two hosts are connected as active and standby hosts to the Cisco ACI switches. The MAC learning still occurs in the hardware but the IP learning only occurs from the ARP/GARP/ND processes. This functionality allows for flexible deployments, for example, firewalls or local gateways.

See the following guidelines and limitations for disabling IP learning per bridge domain:

- Layer 3 multicast is not supported because the source IP address is not learned to populate the S,G information in the remote top-of-rack (ToR) switches.
- As the DL bit is set in the VXLAN header, the MAC address is also not learned from the data path in the remote TORs. It results in flooding of the unknown unicast traffic from the remote TOR to all TORs in the fabric where this BD is deployed. It is recommended to configure the BD in proxy mode to overcome this situation if endpoint dataplane learning is disabled.
- ARP should be in flood mode and GARP based detection should be enabled.
- When IP learning is disabled, Layer 3 endpoints are not flushed in the corresponding VRF. It may lead to the endpoints pointing to the same TOR forever. To resolve this issue, flush all the remote IP endpoints in this VRF on all TORs.
- On Cisco ACI switches with Application Leaf Engine (ALE), the inner MAC address is not learned from the VXLAN packets.
- When dataplane learning is disabled on a BD, the existing local endpoints learned via dataplane in that BD are not flushed. If the data traffic is flowing, the existing local endpoints do not age out.

When IP learning is disabled, you have to enable the Global Subnet Prefix check option in System > System Settings > Fabric Wide Setting > Enforce Subnet Check in the Online Help.

**Creating a Tenant, VRF, and Bridge Domain Using the GUI**

If you have a public subnet when you configure the routed outside, you must associate the bridge domain with the outside configuration.

**Procedure**

**Step 1**
On the menu bar, choose Tenants > Add Tenant.

**Step 2**
In the Create Tenant dialog box, perform the following tasks:

a) In the Name field, enter a name.

b) Click the Security Domains + icon to open the Create Security Domain dialog box.

c) In the Name field, enter a name for the security domain. Click Submit.

d) In the Create Tenant dialog box, check the check box for the security domain that you created, and click Submit.
Creating a Tenant, VRF, and Bridge Domain Using the NX-OS Style CLI

This section provides information on how to create tenants, VRFs, and bridge domains.

Before creating the tenant configuration, you must create a VLAN domain using the `vlan-domain` command and assign the ports to it.
Procedure

Step 1  Create a VLAN domain (which contains a set of VLANs that are allowable in a set of ports) and allocate VLAN inputs, as follows:

Example:

In the following example ("exampleCorp"), note that VLANs 50 - 500 are allocated.

apic1# configure
apic1(config)# vlan-domain dom_exampleCorp
apic1(config-vlan)# vlan 50-500
apic1(config-vlan)# exit

Step 2  Once the VLANs have been allocated, specify the leaf (switch) and interface for which these VLANs can be used. Then, enter "vlan-domain member" and then the name of the domain you just created.

Example:

In the following example, these VLANs (50 - 500) have been enabled on leaf 101 on interface ethernet 1/2-4 (three ports including 1/2, 1/3, and 1/4). This means that if you are using this interface, you can use VLANS 50-500 on this port for any application that the VLAN can be used for.

apic1(config-vlan)# leaf 101
apic1(config-vlan)# interface ethernet 1/2-4
apic1(config-leaf-if)# vlan-domain member dom_exampleCorp
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit

Step 3  Create a tenant in global configuration mode, as shown in the following example:

Example:

apic1(config)# tenant exampleCorp

Step 4  Create a private network (also called VRF) in tenant configuration mode as shown in the following example:

Example:

apic1(config)# tenant exampleCorp
apic1(config-tenant)# vrf context exampleCorp_v1
apic1(config-tenant-vrf)# exit

Step 5  Create a bridge domain (BD) under the tenant, as shown in the following example:

Example:

apic1(config-tenant)# bridge-domain exampleCorp_b1
apic1(config-tenant-bd)# vrf member exampleCorp_v1
apic1(config-tenant-bd)# exit

Note  In this case, the VRF is "exampleCorp_v1".

Step 6  Allocate IP addresses for the BD (ip and ipv6), as shown in the following example.

Example:

apic1(config-tenant)# interface bridge-domain exampleCorp_b1
apic1(config-tenant-interface)# ip address 172.1.1.1/24
Creating a Tenant, VRF, and Bridge Domain Using the REST API

Procedure

**Step 1**
Create a tenant.

**Example:**
```
POST https://apic-ip-address/api/mo/uni.xml
<fvTenant name="ExampleCorp"/>
```

When the POST succeeds, you see the object that you created in the output.

**Step 2**
Create a VRF and bridge domain.

**Note**
The Gateway Address can be an IPv4 or an IPv6 address. For more about details IPv6 gateway address, see the related KB article, KB: Creating a Tenant, VRF, and Bridge Domain with IPv6 Neighbor Discovery.

**Example:**
```
URL for POST: https://apic-ip-address/api/mo/uni/tn-ExampleCorp.xml

<fvTenant name="ExampleCorp">
  <fvCtx name="pvn1"/>
  <fvBD name="bd1">
    <fvRsCtx tnFvCtxName="pvn1"/>
    <fvSubnet ip="10.10.100.1/24"/>
  </fvBD>
</fvTenant>
```

**Note**
If you have a public subnet when you configure the routed outside, you must associate the bridge domain with the outside configuration.

Configuring an Enforced Bridge Domain

An enforced bridge domain (BD) configuration entails creating an endpoint in a subject endpoint group (EPG) which can only ping subnet gateways within the associated bridge domain.
With this configuration, you can then create a global exception list of IP addresses which can ping any subnet gateway.

**Figure 9: Enforced Bridge Domain**

- The exception IP addresses can ping all of the BD gateways across all of your VRFs.
- A loopback interface configured for an L3 out does not enforce reachability to the IP address that is configured for the subject loopback interface.
- When an eBGP peer IP address exists in a different subnet than the subnet of the L3out interface, the peer subnet must be added to the allowed exception subnets.
  Otherwise, eBGP traffic is blocked because the source IP address exists in a different subnet than the L3out interface subnet.

### Configuring an Enforced Bridge Domain Using the NX-OS Style CLI

This section provides information on how to configure your enforced bridge domain using the NX-OS style command line interface (CLI).

**Procedure**

1. **Step 1** Create and enable the tenant:

   **Example:**
   In the following example ("cokeVrf") is created and enabled.
   ```
   apic1(config-tenant)# vrf context cokeVrf
   apic1(config-tenant-vrf)# bd-enforce enable
   ```
Step 2
Add the subnet to the exception list.

Example:
apic1(config)# bd-enf-exp-ip add 1.2.3.4/24
apic1(config)# exit

You can confirm if the enforced bridge domain is operational using the following type of command:
apic1# show running-config all | grep bd-enf
bd-enforce enable
bd-enf-exp-ip add 1.2.3.4/24

Example
The following command removes the subnet from the exception list:
apic1(config)# no bd-enf-exp-ip 1.2.3.4/24
apic1(config)# tenant coke
apic1(config-tenant)# vrf context cokeVrf

What to do next
To disable the enforced bridge domain run the following command:
apic1(config-tenant-vrf)# no bd-enforce enable

Configuring an Enforced Bridge Domain Using the REST API

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a tenant.</td>
<td>When the POST succeeds, you see the object that you created in the output.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>POST</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://apic-ip-address/api/mo/uni.xml">https://apic-ip-address/api/mo/uni.xml</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;fvTenant name=&quot;ExampleCorp&quot;/&gt;</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Create a VRF and bridge domain.</td>
<td>Note The Gateway Address can be an IPv4 or an IPv6 address. For more about details IPv6 gateway address, see the related KB article, KB: Creating a Tenant, VRF, and Bridge Domain with IPv6 Neighbor Discovery.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL for POST:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://apic-ip-address/api/mo/uni/tn-ExampleCorp.xml">https://apic-ip-address/api/mo/uni/tn-ExampleCorp.xml</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;fvTenant name=&quot;ExampleCorp&quot;&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;fvCtx name=&quot;pvn1&quot;/&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;fvBD name=&quot;bd1&quot;&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;fVRsCtx tnFvCtxName=&quot;pvn1&quot;/&gt;</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Flood in Encapsulation for All Protocols and Proxy ARP Across Encapsulations

ACI uses the Bridge Domain (BD) as the Layer 2 broadcast boundary and each BD can include multiple Endpoint Groups (EPGs). You can bind an encapsulation VLAN to the desired EPG to carry user traffic. In some design scenarios, flooding can cross different user VLANs (EPGs) when the EPGs are in the same BD.

Flood in Encapsulation is mainly used when the external device is using the Virtual Connect Tunnel mode where one MAC address is maintained per vNet (the endpoint device does not include VLAN ID in MAC address table).

Using multiple VLANs in tunnel mode can introduce a few challenges. In a typical deployment using ACI with a single tunnel, as illustrated in the following figure, there are multiple EPGs under one BD. In this case, certain traffic is flooded within the BD (and thus in all the EPGs), with the risk of MAC learning ambiguities that can cause forwarding errors.

### Command or Action

```
<fvTenant>
  <fvBD>
    <fvSubnet ip="10.10.100.1/24"/>
  </fvBD>
</fvTenant>
```

For adding an exception IP, use the following post:

```
https://apic-ip-address/api/node/mo/uni/infra.xml
```

```
<bdEnforceExceptionCont>
  <bdEnforceExceptIp ip="11.0.1.0/24"/>
</bdEnforceExceptionCont>
```

**Note** If you have a public subnet when you configure the routed outside, you must associate the bridge domain with the outside configuration.
In this topology, the fabric has a single tunnel network defined that uses one uplink to connect with the ACI leaf node. Two user VLANs, VLAN 10 and VLAN 11 are carried over this link. The BD domain is set in flooding mode as the servers’ gateways are outside the ACI cloud. ARP negotiations occur in the following process:

- The server sends one ARP broadcast request over the VLAN 10 network.
- The ARP packet travels through the tunnel network to the external server, which records the source MAC address, learned from its downlink.
- The server then forwards the packet out its uplink to the ACI leaf switch.
- The ACI fabric sees the ARP broadcast packet entering on access port VLAN 10 and maps it to EPG1.
- Because the BD is set to flood ARP packets, the packet is flooded within the BD and thus to the ports under both EPGs as they are in the same BD.
- The same ARP broadcast packet comes back over the same uplink.
- The external server sees the original source MAC address from this uplink.

Result: the external device has the same MAC address learned from both the downlink port and uplink port within its single MAC forwarding table, causing traffic disruptions.

**Recommended Solution**

The **Flood in Encapsulation** option is used to limit flooding traffic inside the BD to a single encapsulation. When two EPGs share the same BD and **Flood in Encapsulation** is enabled, the EPG flooding traffic does not reach the other EPG.
Beginning with Cisco APIC Release 3.1(1), on the Cisco Nexus 9000 series switches (with names ending with EX and FX and onwards), all protocols are flooded in encapsulation. Also when enabling **Flood in Encapsulation** for any inter-VLAN traffic, Proxy ARP ensures that the MAC flap issue does not occur, and it limits all flooding (ARP, GARP, and BUM) to the encapsulation. This applies for all EPGs under the bridge domain where it is enabled.

**Note**

Before Cisco APIC release 3.1(1), these features are not supported (Proxy ARP and all protocols being included when flooding within encapsulation). In an earlier Cisco APIC release or earlier generation switches (without EX or FX on their names), if you enable **Flood in Encapsulation** it does not function, no informational fault is generated, but APIC decreases the health score by 1.

The recommended solution is to support multiple EPGs under one BD by adding an external switch. This design with multiple EPGs under one bridge domain with an external switch is illustrated in the following figure.

*Figure 11: Design with Multiple EPGs Under one Bridge Domain with an External Switch*
Within the same BD, some EPGs can be service nodes and other EPGs can have flood in encapsulation configured. A Load Balancer resides on a different EPG. The load balancer receives packets from the EPGs and sends them to the other EPGs (There is no Proxy ARP and flood within encapsulation does not take place).

If you want to add flood in encapsulation only for selective EPGs, using the NX-OS style CLI, enter the `flood-on-encapsulation enable` command under EPGs.

If you want to add flood in encapsulation for all EPGs, you can use the `multi-destination encap-flood` CLI command under the bridgedomain.

Using the CLI, flood in encapsulation configured for an EPG takes precedence over flood in encapsulation that is configured for a bridge domain.

When both BDs and EPGs are configured, the behavior is described as follows:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood in encapsulation at the EPG and flood in</td>
<td>Flood in encapsulation takes place for the traffic on all VLANs within</td>
</tr>
<tr>
<td>encapsulation at the bridge domain</td>
<td>the bridge domain.</td>
</tr>
<tr>
<td>No flood in encapsulation at the EPG and flood in</td>
<td>Flood in encapsulation takes place for the traffic on all VLANs within</td>
</tr>
<tr>
<td>encapsulation at the bridge domain</td>
<td>the bridge domain.</td>
</tr>
<tr>
<td>Flood in encapsulation at the EPG and no flood in</td>
<td>Flood in encapsulation takes place for the traffic on that VLAN within</td>
</tr>
<tr>
<td>encapsulation at the bridge domain</td>
<td>the EPG of the bridge domain.</td>
</tr>
<tr>
<td>No flood in encapsulation at the EPG and no flood in</td>
<td>Flooding takes place within the entire bridge domain.</td>
</tr>
<tr>
<td>encapsulation at the bridge domain</td>
<td></td>
</tr>
</tbody>
</table>

**Multi-Destination Protocol Traffic**

The EPG/BD level broadcast segmentation is supported for the following network control protocols:

- OSPF
- EIGRP
- CDP
- LACP
- LLDP
- IS-IS
- BGP
- IGMP
- PIM
- STP-BPDU (flooded within EPG)
- ARP/GARP (controlled by ARP Proxy)
- ND
Limitations

Here are the limitations for using flood in encapsulation for all protocols:

- Flood in encapsulation does not work in ARP unicast mode.
- Neighbor Solicitation (NS/ND) is not supported for this release.
- You must enable per-port CoPP with flood in encapsulation.
- Flood in encapsulation is supported only in BD in flood mode and ARP in flood mode. BD spine proxy mode is not supported.
- IPv4 L3 multicast is not supported.
- IPv6 is not supported.
- VM migration to a different VLAN has momentary issues (60 seconds).
- A load balancer acting as a gateway is supported, for example, in one to one communication between VMs and the load balancer in non-proxy mode. No Layer 3 communication is supported. The traffic between VMs and the load balancer is on Layer 2. However, if intra-EPG communication passes through the load balancer, then the load balancer changes the SIP and SMAC; otherwise it can lead to a MAC flap. Therefore, Dynamic Source Routing (DSR) mode is not supported in the load balancer.
- Setting up communication between VMs through a firewall, as a gateway, is not recommended because if the VM IP address changes to the gateway IP address instead of the firewall IP address, then the firewall can be bypassed.
- Prior releases are not supported (even interoperating between prior and current releases).
- The Proxy ARP and Flood in Encapsulation features are not supported for VXLAN encapsulation.
- A mixed-mode topology with Application Leaf Engine (ALE) and Application Spine Engine (ASE) is not recommended and is not supported with flood in encapsulation. Enabling them together can prevent QoS priorities from being enforced.
- Flood in encapsulation is not supported with Remote Leaf switches and Cisco ACI Multi-Site.
- Flood in encapsulation is not supported for Common Pervasive Gateway (CPGW).
This chapter contains the following sections:

- About Endpoint Groups, on page 39
- Deploying an EPG on a Specific Port, on page 45
- Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port, on page 48
- Deploying EPGs to Multiple Interfaces Through Attached Entity Profiles, on page 52
- Intra-EPG Isolation, on page 56

**About Endpoint Groups**

**Endpoint Groups**

The endpoint group (EPG) is the most important object in the policy model. The following figure shows where application EPGs are located in the management information tree (MIT) and their relation to other objects in the tenant.
An EPG is a managed object that is a named logical entity that contains a collection of endpoints. Endpoints are devices that are connected to the network directly or indirectly. They have an address (identity), a location, attributes (such as version or patch level), and can be physical or virtual. Knowing the address of an endpoint also enables access to all its other identity details. EPGs are fully decoupled from the physical and logical topology. Endpoint examples include servers, virtual machines, network-attached storage, or clients on the Internet. Endpoint membership in an EPG can be dynamic or static.

The ACI fabric can contain the following types of EPGs:

- Application endpoint group (fvAEpg)
- Layer 2 external outside network instance endpoint group (l2extInstP)
- Layer 3 external outside network instance endpoint group (l3extInstP)
- Management endpoint groups for out-of-band (mgmtOoB) or in-band (mgmtInB) access.

EPGs contain endpoints that have common policy requirements such as security, virtual machine mobility (VMM), QoS, or Layer 4 to Layer 7 services. Rather than configure and manage endpoints individually, they are placed in an EPG and are managed as a group.

Policies apply to EPGs, never to individual endpoints. An EPG can be statically configured by an administrator in the APIC, or dynamically configured by an automated system such as vCenter or OpenStack.
When an EPG uses a static binding path, the encapsulation VLAN associated with this EPG must be part of a static VLAN pool. For IPv4/IPv6 dual-stack configurations, the IP address property is contained in the `fvStIp` child property of the `fvStCEp` MO. Multiple `fvStIp` objects supporting IPv4 and IPv6 addresses can be added under one `fvStCEp` object. When upgrading ACI from IPv4-only firmware to versions of firmware that support IPv6, the existing IP property is copied to an `fvStIp` MO.

Regardless of how an EPG is configured, EPG policies are applied to the endpoints they contain.

WAN router connectivity to the fabric is an example of a configuration that uses a static EPG. To configure WAN router connectivity to the fabric, an administrator configures an `l3extInstP` EPG that includes any endpoints within an associated WAN subnet. The fabric learns of the EPG endpoints through a discovery process as the endpoints progress through their connectivity life cycle. Upon learning of the endpoint, the fabric applies the `l3extInstP` EPG policies accordingly. For example, when a WAN connected client initiates a TCP session with a server within an application (fvAEPg) EPG, the `l3extInstP` EPG applies its policies to that client endpoint before the communication with the `fvAEPg` EPG web server begins. When the client server TCP session ends and communication between the client and server terminate, that endpoint no longer exists in the fabric.

If a leaf switch is configured for static binding (leaf switches) under an EPG, the following restrictions apply:

- The static binding cannot be overridden with a static path.
- Interfaces in that switch cannot be used for routed external network (L3out) configurations.
- Interfaces in that switch cannot be assigned IP addresses.

Virtual machine management connectivity to VMware vCenter is an example of a configuration that uses a dynamic EPG. Once the virtual machine management domain is configured in the fabric, vCenter triggers the dynamic configuration of EPGs that enable virtual machine endpoints to start up, move, and shut down as needed.

### IP-Based EPGs

Although encapsulation-based EPGs are commonly used, IP-based EPGs are suitable in networks where there is a need for large numbers of EPGs that cannot be supported by Longest Prefix Match (LPM) classification. IP-based EPGs do not require allocating a network/mask range for each EPG, unlike LPM classification. Also, a unique bridge domain is not required for each IP-based EPG. The configuration steps for an IP-based EPG are like those for configuring a virtual IP-based EPG that is used in the Cisco AVS vCenter configuration.

Observe the following guidelines and limitations of IP-based EPGs:

- IP-based EPGs are supported starting with the APIC 1.1(2x) and ACI switch 11.1(2x) releases on the following Cisco Nexus N9K switches:
  - Switches with "E" on the end of the switch name, for example, N9K-C9372PX-E.
  - Switches with "EX" on the end of the switch name, for example, N9K-93108TC-EX.

  The APIC raises a fault when you attempt to deploy IP-based EPGs on older switches that do not support them.
• IP-based EPGs can be configured for specific IP addresses or subnets, but not IP address ranges.

• IP-based EPGs are not supported in the following scenarios:
  • In combination with static EP configurations.
  • External, infrastructure tenant (infra) configurations will not be blocked, but they do not take effect, because there is no Layer 3 learning in this case.
  • In Layer 2-only bridge domains, IP-based EPG does not take effect, because there is no routed traffic in this case. If proxy ARP is enabled on Layer 3 bridge domains, the traffic is routed even if endpoints are in the same subnet. So IP-based EPG works in this case.
  • Configurations with a prefix that is used both for shared services and an IP-based EPG.

Access Policies Automate Assigning VLANs to EPGs

While tenant network policies are configured separately from fabric access policies, tenant policies are not activated unless their underlying access policies are in place. Fabric access external-facing interfaces connect to external devices such as virtual machine controllers and hypervisors, hosts, routers, or Fabric Extenders (FEXs). Access policies enable an administrator to configure port channels and virtual port channels, protocols such as LLDP, CDP, or LACP, and features such as monitoring or diagnostics.

Figure 13: Association of Endpoint Groups with Access Policies

In the policy model, EPGs are tightly coupled with VLANs. For traffic to flow, an EPG must be deployed on a leaf port with a VLAN in a physical, VMM, L2out, L3out, or Fiber Channel domain. For more information, see Networking Domains, on page 17.

In the policy model, the domain profile associated to the EPG contains the VLAN instance profile. The domain profile contains both the VLAN instance profile (VLAN pool) and the attachable Access Entity Profile (AEP), which are associated directly with application EPGs. The AEP deploys the associated application...
EPGs to all the ports to which it is attached, and automates the task of assigning VLANs. While a large data center could easily have thousands of active virtual machines provisioned on hundreds of VLANs, the ACI fabric can automatically assign VLAN IDs from VLAN pools. This saves a tremendous amount of time, compared with trunking down VLANs in a traditional data center.

**VLAN Guidelines**

Use the following guidelines to configure the VLANs where EPG traffic will flow.

- Multiple domains can share a VLAN pool, but a single domain can only use one VLAN pool.
- To deploy multiple EPGs with same VLAN encapsulation on a single leaf switch, see Per Port VLAN, on page 43.

**Per Port VLAN**

In ACI versions prior to the v1.1 release, a given VLAN encapsulation maps to only a single EPG on a leaf switch. If there is a second EPG which has the same VLAN encapsulation on the same leaf switch, the ACI raises a fault.

Starting with the v1.1 release, you can deploy multiple EPGs with the same VLAN encapsulation on a given leaf switch (or FEX), in the Per Port VLAN configuration, similar to the following diagram:

![Per Port VLAN Diagram](image)

To enable deploying multiple EPGs using the same encapsulation number, on a single leaf switch, use the following guidelines:

- EPGs must be associated with different bridge domains.
- EPGs must be deployed on different ports.
- Both the port and EPG must be associated with the same domain that is associated with a VLAN pool that contains the VLAN number.
- Ports must be configured with `portLocal VLAN` scope.
For example, with Per Port VLAN for the EPGs deployed on ports 3 and 9 in the diagram above, both using VLAN-5, port 3 and EPG1 are associated with Dom1 (pool 1) and port 9 and EPG2 are associated with Dom2 (pool 2).

Traffic coming from port 3 is associated with EPG1, and traffic coming from port 9 is associated with EPG2. This does not apply to ports configured for Layer 3 external outside connectivity.

**Note**

Avoid adding more than one domain to the AEP that is used to deploy the EPG on the ports, to avoid the risk of traffic forwarding issues.

Only ports that have the `vlanScope` set to `portLocal` allow allocation of separate (Port, VLAN) translation entries in both ingress and egress directions. For a given port with the `vlanScope` set to `portGlobal` (the default), each VLAN used by an EPG must be unique on a given leaf switch.

**Note**

Per Port VLAN is not supported on interfaces configured with Multiple Spanning Tree (MST), which requires VLAN IDs to be unique on a single leaf switch, and the VLAN scope to be global.

**Reusing VLAN Numbers Previously Used for EPGs on the Same Leaf Switch**

If you have previously configured VLANs for EPGs that are deployed on a leaf switch port, and you want to reuse the same VLAN numbers for different EPGs on different ports on the same leaf switch, use a process, such as the following example, to set them up without disruption:

In this example, EPGs were previously deployed on a port associated with a domain including a VLAN pool with a range of 9-100. You want to configure EPGs using VLAN encapsulations from 9-20.

1. Configure a new VLAN pool on a different port (with a range of, for example, 9-20).
2. Configure a new physical domain that includes leaf ports that are connected to firewalls.
3. Associate the physical domain to the VLAN pool you configured in step 1.
4. Configure the VLAN Scope as `portLocal` for the leaf port.
5. Associate the new EPGs (used by the firewall in this example) to the physical domain you created in step 2.
6. Deploy the EPGs on the leaf ports.
VLAN Guidelines for EPGs Deployed on VPCs

When an EPG is deployed on a VPC, it must be associated with the same domain (with the same VLAN pool) that is assigned to the leaf switch ports on the two legs of the VPC.

In this diagram, EPG A is deployed on a VPC that is deployed on ports on Leaf switch 1 and Leaf switch 2. The two leaf switch ports and the EPG are all associated with the same domain, containing the same VLAN pool.

Deploying an EPG on a Specific Port

Deploying an EPG on a Specific Node or Port Using the GUI

Before you begin

You can create an EPG on a specific node or a specific port on a node.

Procedure

Step 1 Log in to the Cisco APIC.
Step 2 Choose Tenants > tenant.
Step 3 In the left navigation pane, expand tenant, Application Profiles, and the application profile.
Step 4 Right-click Application EPGs and choose Create Application EPG.
Step 5 In the Create Application EPG STEP 1 > Identity dialog box, complete the following steps:
   a) In the Name field, enter a name for the EPG.
   b) From the Bridge Domain drop-down list, choose a bridge domain.
   c) Check the Statically Link with Leaves/Paths check box.
      This check box allows you to specify on which port you want to deploy the EPG.
   d) Click Next.
   e)
f) From the Path drop-down list, choose the static path to the destination EPG.

**Step 6**
In the Create Application EPG STEP 2 > Leaves/Paths dialog box, from the Physical Domain drop-down list, choose a physical domain.

**Step 7**
Complete one of the following sets of steps:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want to deploy the EPG on...</td>
<td>Then</td>
</tr>
<tr>
<td>A node</td>
<td>1. Expand the Leaves area.</td>
</tr>
<tr>
<td></td>
<td>2. From the Node drop-down list, choose a node.</td>
</tr>
<tr>
<td></td>
<td>3. In the Encap field, enter the appropriate VLAN.</td>
</tr>
<tr>
<td></td>
<td>4. (Optional) From the Deployment Immediacy drop-down list, accept the default On Demand or choose Immediate.</td>
</tr>
<tr>
<td></td>
<td>5. (Optional) From the Mode drop-down list, accept the default Trunk or choose another mode.</td>
</tr>
<tr>
<td>A port on the node</td>
<td>1. Expand the Paths area.</td>
</tr>
<tr>
<td></td>
<td>2. From the Path drop-down list, choose the appropriate node and port.</td>
</tr>
<tr>
<td></td>
<td>3. (Optional) In the Deployment Immediacy field drop-down list, accept the default On Demand or choose Immediate.</td>
</tr>
<tr>
<td></td>
<td>4. (Optional) From the Mode drop-down list, accept the default Trunk or choose another mode.</td>
</tr>
<tr>
<td></td>
<td>5. In the Port Encap field, enter the secondary VLAN to be deployed.</td>
</tr>
<tr>
<td></td>
<td>6. (Optional) In the Primary Encap field, enter the primary VLAN to be deployed.</td>
</tr>
</tbody>
</table>

**Step 8**
Click Update and click Finish.

**Step 9**
In the left navigation pane, expand the EPG that you created.

**Step 10**
Complete one of the following actions:

- If you created the EPG on a node, click Static Leafs, and in the work pane view details of the static binding paths.
- If you created the EPG on a port of the node, click Static Ports, and in the work pane view details of the static binding paths.

### Deploying an EPG on a Specific Port with APIC Using the NX-OS Style CLI

**Procedure**

**Step 1**
Configure a VLAN domain:
Example:

```bash
apic1(config)# vlan-domain dom1
apic1(config-vlan)# vlan 10-100
```

**Step 2** Create a tenant:

**Example:**

```bash
apic1# configure
apic1(config)# tenant t1
```

**Step 3** Create a private network/VRF:

**Example:**

```bash
apic1(config-tenant)# vrf context ctx1
apic1(config-tenant-vrf)# exit
```

**Step 4** Create a bridge domain:

**Example:**

```bash
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# vrf member ctx1
apic1(config-tenant-bd)# exit
```

**Step 5** Create an application profile and an application EPG:

**Example:**

```bash
apic1(config-tenant)# application AP1
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# bridge-domain member bd1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
```

**Step 6** Associate the EPG with a specific port:

**Example:**

```bash
apic1(config)# leaf 1017
apic1(config-leaf)# interface ethernet 1/13
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# switchport trunk allowed vlan 20 tenant t1 application AP1 epg EPG1
```

**Note** The vlan-domain and vlan-domain member commands mentioned in the above example are a pre-requisite for deploying an EPG on a port.

---

**Deploying an EPG on a Specific Port with APIC Using the REST API**

**Before you begin**

The tenant where you deploy the EPG is created.
Procedure

Deploy an EPG on a specific port.

Example:

```xml
<fvTenant name="<tenant_name>" dn="uni/tn-test1">
  <fvCtx name="<network_name>" pcEnfPref="enforced" knwMcastAct="permit"/>
  <fvBD name="<bridge_domain_name>" unkMcastAct="flood">
    <fvRsCtx tnFvCtxName="<network_name/>
  </fvBD>
  <fvAp name="<application_profile>">
    <fvAEPg name="<epg_name>">
      <fvRsPathAtt tDn="topology/pod-1/paths-1017/pathep-[eth1/13]" mode="regular"
        instrImedcy="immediate" encap="vlan-20"/>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port

This topic provides a typical example of how to create physical domains, Attach Entity Profiles (AEP), and VLANs that are mandatory to deploy an EPG on a specific port.

Note

All endpoint groups (EPGs) require a domain. Interface policy groups must also be associated with Attach Entity Profile (AEP), and the AEP must be associated with a domain, if the AEP and EPG have to be in same domain. Based on the association of EPGs to domains and of interface policy groups to domains, the ports and VLANs that the EPG uses are validated. The following domain types associate with EPGs:

- Application EPGs
- Layer 3 external outside network instance EPGs
- Layer 2 external outside network instance EPGs
- Management EPGs for out-of-band and in-band access

The APIC checks if an EPG is associated with one or more of these types of domains. If the EPG is not associated, the system accepts the configuration but raises a fault. The deployed configuration may not function properly if the domain association is not valid. For example, if the VLAN encapsulation is not valid for use with the EPG, the deployed configuration may not function properly.
Creating Domains, and VLANS to Deploy an EPG on a Specific Port Using the GUI

Before you begin

- The tenant where you deploy the EPG is already created.
- An EPG is statically deployed on a specific port.

Procedure

Step 1

Step 2
In the Navigation pane, click Quick Start.

Step 3
In the Work pane, click Configure an Interface, PC, and VPC.

Step 4
In the Configure an Interface, PC, and VPC dialog box, click the + icon to select switches and perform the following actions:

a) From the Switches drop-down list, check the check box for the desired switch.

b) In the Switch Profile Name field, a switch name is automatically populated.

   Note Optionally, you can enter a modified name.

c) Click the + icon to configure the switch interfaces.

d) In the Interface Type field, click the Individual radio button.

e) In the Interfaces field, enter the range of desired interfaces.

f) In the Interface Selector Name field, an interface name is automatically populated.

   Note Optionally, you can enter a modified name.

g) In the Interface Policy Group field, choose the Create One radio button.

h) From the Link Level Policy drop-down list, choose the appropriate link level policy.

   Note Create additional policies as desired, otherwise the default policy settings are available.

i) From the Attached Device Type field, choose the appropriate device type.

j) In the Domain field, click the Create One radio button.

k) In the Domain Name field, enter a domain name.

l) In the VLAN field, click the Create One radio button.

m) In the VLAN Range field, enter the desired VLAN range. Click Save, and click Save again.

n) Click Submit.

Step 5
On the menu bar, click Tenants. In the Navigation pane, expand the appropriate Tenant_name > Application Profiles > Application EPGs > EPG_name and perform the following actions:

a) Right-click Domains (VMs and Bare-Metals), and click Add Physical Domain Association.

b) In the Add Physical Domain Association dialog box, from the Physical Domain Profile drop-down list, choose the appropriate domain.

c) Click Submit.

The AEP is associated with a specific port on a node and with a domain. The physical domain is associated with the VLAN pool and the Tenant is associated with this physical domain.
The switch profile and the interface profile are created. The policy group is created in the port block under the interface profile. The AEP is automatically created, and it is associated with the port block and with the domain. The domain is associated with the VLAN pool and the Tenant is associated with the domain.

Creating AEP, Domains, and VLANs to Deploy an EPG on a Specific Port Using the NX-OS Style CLI

Before you begin

- The tenant where you deploy the EPG is already created.
- An EPG is statically deployed on a specific port.

Procedure

Step 1
Create a VLAN domain and assign VLAN ranges:

Example:

apic1(config)# vlan-domain domP
apic1(config-vlan)# vlan 10
apic1(config-vlan)# vlan 25
apic1(config-vlan)# vlan 50-60
apic1(config-vlan)# exit

Step 2
Create an interface policy group and assign a VLAN domain to the policy group:

Example:

apic1(config)# template policy-group PortGroup
apic1(config-pol-grp-if)# vlan-domain member domP

Step 3
Create a leaf interface profile, assign an interface policy group to the profile, and assign the interface IDs on which the profile will be applied:

Example:

apic1(config)# leaf-interface-profile InterfaceProfile1
apic1(config-leaf-if-profile)# leaf-interface-group range
apic1(config-leaf-if-group)# policy-group PortGroup
apic1(config-leaf-if-group)# interface ethernet 1/11-13
apic1(config-leaf-if-profile)# exit

Step 4
Create a leaf profile, assign the leaf interface profile to the leaf profile, and assign the leaf IDs on which the profile will be applied:

Example:

apic1(config)# leaf-profile SwitchProfile-1019
apic1(config-leaf-profile)# leaf-interface-profile InterfaceProfile1
apic1(config-leaf-profile)# leaf-group range
Creating AEP, Domains, and VLANs to Deploy an EPG on a Specific Port Using the REST API

Before you begin

- The tenant where you deploy the EPG is already created.
- An EPG is statically deployed on a specific port.

Procedure

**Step 1** Create the interface profile, switch profile and the Attach Entity Profile (AEP).

**Example:**

```xml
<infraInfra>
  <infraNodeP name="<switch_profile_name>" dn="uni/infra/nprof-<switch_profile_name>">
    <infraLeafS name="SwitchSelector" descr="" type="range">
      <infraNodeBlk name="nodeBlk1" descr="" to="1019" from="1019"/>
    </infraLeafS>
    <infraRsAccPortP tDn="uni/infra/accportprof-<interface_profile_name>"/>
  </infraNodeP>

  <infraAccPortP name="<interface_profile_name>" dn="uni/infra/accportprof-<interface_profile_name>">
    <infraHPortS name="portSelector" type="range">
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-<port_group_name>" fexId="101"/>
      <infraPortBlk name="block2" toPort="13" toCard="1" fromPort="11" fromCard="1"/>
    </infraHPortS>
  </infraAccPortP>

  <infraAccPortGrp name="<port_group_name>" dn="uni/infra/funcprof/accportgrp-<port_group_name>">
    <infraRsAttEntP tDn="uni/infra/attentp-<attach_entity_profile_name>"/>
    <infraRsHIfPol tnFabricHIfPolName="1GHifPol"/>
  </infraAccPortGrp>

  <infraAttEntityP name="<attach_entity_profile_name>" dn="uni/infra/attentp-<attach_entity_profile_name>">
    <infraRsDomP tDn="uni/phys-<physical_domain_name>"/>
  </infraAttEntityP>
</infraInfra>
```

**Step 2** Create a domain.

**Example:**
Deploying EPGs to Multiple Interfaces Through Attached Entity Profiles

Deploying an Application EPG through an AEP or Interface Policy Group to Multiple Ports

Through the APIC Advanced GUI and REST API, you can associate attached entity profiles directly with application EPGs. By doing so, you deploy the associated application EPGs to all those ports associated with the attached entity profile in a single configuration.

Through the APIC REST API or the NX-OS style CLI, you can deploy an application EPG to multiple ports through an Interface Policy Group.

Deploying an EPG through an AEP to Multiple Interfaces Using the APIC GUI

You can quickly associate an application with an attached entity profile to quickly deploy that EPG over all the ports associated with that attached entity profile.

Before you begin

• The target application EPG is created.
• The VLAN pools has been created containing the range of VLANs you wish to use for EPG Deployment on the AEP.
• The physical domain has been created and linked to the VLAN Pool and AEP.
• The target attached entity profile is created and is associated with the ports on which you want to deploy the application EPG.

**Procedure**

**Step 1**
Navigate to the target attached entity profile.

a) Open the page for the attached entity profile to use. In the GUI, click **Fabric > External Access Policies > Policies > Global > Attachable Access Entity Profiles**.

b) Click the target attached entity profile to open its Attachable Access Entity Profile window.

**Step 2**
Click the **Show Usage** button to view the leaf switches and interfaces associated with this attached entity profile.

The application EPGs associated with this attached entity profile are deployed to all the ports on all the switches associated with this attached entity profile.

**Step 3**
Use the **Application EPGs** table to associate the target application EPG with this attached entity profile. Click **+** to add an application EPG entry. Each entry contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application EPGs</td>
<td>Use the drop down to choose the associated Tenant, Application Profile, and target application EPG.</td>
</tr>
<tr>
<td>Encap</td>
<td>Enter the name of the VLAN over which the target application EPG will communicate.</td>
</tr>
<tr>
<td>Primary Encap</td>
<td>If the application EPG requires a primary VLAN, enter the name of the primary VLAN.</td>
</tr>
<tr>
<td>Mode</td>
<td>Use the drop down to specify the mode in which data is transmitted:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Trunk</strong> -- Choose if traffic from the host is tagged with a VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Access</strong> -- Choose if traffic from the host is tagged with an 802.1p tag.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Access Untagged</strong> -- Choose if the traffic from the host is untagged.</td>
</tr>
</tbody>
</table>

**Step 4**
Click **Submit**.

The application EPGs associated with this attached entity profile are deployed to all the ports on all the switches associated with this attached entity profile.

---

**Deploying an EPG through an Interface Policy Group to Multiple Interfaces Using the NX-OS Style CLI**

In the NX-OS CLI, an attached entity profile is not explicitly defined to associate with an EPG for rapid deployment; instead the interface policy group is defined, assigned a domain, applied to all the ports associated with a VLAN and configured to include the application EPG to be deployed over that VLAN.
Before you begin

- The target application EPG is created.
- The VLAN pools have been created containing the range of VLANs you wish to use for EPG Deployment on the AEP.
- The physical domain has been created and linked to the VLAN Pool and AEP.
- The target attached entity profile is created and is associated with the ports on which you want to deploy the application EPG.

Procedure

**Step 1**

Associate the target EPG with the interface policy group.

The sample command sequence specifies an interface policy group **pg3** associated with VLAN domain, **domain1**, and with VLAN **1261**. The application EPG, **epg47** is deployed to all interfaces associated with this policy group.

**Example:**

```
apic1(config)# template policy-group pg3
apic1(config-pol-grp-if)# vlan-domain member domain1
apic1(config-pol-grp-if)# switchport trunk allowed vlan 1261 tenant tn10 application pod1-AP
epg epg47
```

**Step 2**

Check the target ports to ensure deployment of the policies of the interface policy group associated with application EPG.

The output of the sample **show** command sequence indicates that policy group **pg3** is deployed on Ethernet port **1/20** on leaf switch **1017**.

**Example:**

```
apic1# show run leaf 1017 int eth 1/20
# Command: show running-config leaf 1017 int eth 1/20
leaf 1017
    interface ethernet 1/20
    policy-group pg3
    exit
exit
ifav28-ifc1#
```

Deploying an EPG through an AEP to Multiple Interfaces Using the REST API

The interface selectors in the AEP enable you to configure multiple paths for an AEPg. The following can be selected:

1. A node or a group of nodes
2. An interface or a group of interfaces
The interfaces consume an interface policy group (and so an infra:AttEntityP).

3. The infra:AttEntityP is associated to the AEPg, thus specifying the VLANs to use.
   An infra:AttEntityP can be associated with multiple AEPgs with different VLANs.

When you associate the infra:AttEntityP with the AEPg, as in 3, this deploys the AEPg on the nodes selected in 1, on the interfaces in 2, with the VLAN provided by 3.

In this example, the AEPg uni/tn-Coke/ap-AP/epg-EPG1 is deployed on interfaces 1/10, 1/11, and 1/12 of nodes 101 and 102, with vlan-102.

**Before you begin**

- Create the target application EPG (AEPg).
- Create the VLAN pool containing the range of VLANs you wish to use for EPG deployment with the Attached Entity Profile (AEP).
- Create the physical domain and link it to the VLAN pool and AEP.

**Procedure**

To deploy an AEPg on selected nodes and interfaces, send a post with XML such as the following:

**Example:**

```xml
<infraInfra dn="uni/infra">
  <infraNodeP name="NodeProfile">
    <infraLeafS name="NodeSelector" type="range">
      <infraNodeBlk name="NodeBlock" from_="101" to="102"/>
    </infraLeafS>
  </infraNodeP>
  <infraAccPortP name="InterfaceProfile">
    <infraHPortS name="InterfaceSelector" type="range">
      <infraPortBlk name="InterfaceBlock" fromCard="1" toCard="1" fromPort="10" toPort="12"/>
    </infraHPortS>
  </infraAccPortP>
  <infraFuncP>
    <infraAccPortGrp name="PortGrp">
      <infraRsAttEntP tDn="uni/infra/attentp-AttEntityProfile"/>
    </infraAccPortGrp>
  </infraFuncP>
  <infraAttEntityP name="AttEntityProfile">
    <infraGeneric name="default">
      <infraRsFuncToEpg tDn="uni/tn-Coke/ap-AP/epg-EPG1" encap="vlan-102"/>
    </infraGeneric>
  </infraAttEntityP>
</infraInfra>
```
Intra-EPG Isolation

Intra-EPG Endpoint Isolation

Intra-EPG endpoint isolation policies provide full isolation for virtual or physical endpoints; no communication is allowed between endpoints in an EPG that is operating with isolation enforced. Isolation enforced EPGs reduce the number of EPG encapsulations required when many clients access a common service but are not allowed to communicate with each other.

An EPG is isolation enforced for all ACI network domains or none. While the ACI fabric implements isolation directly to connected endpoints, switches connected to the fabric are made aware of isolation rules according to a primary VLAN (PVLAN) tag.

Note

If an EPG is configured with intra-EPG endpoint isolation enforced, these restrictions apply:

- All Layer 2 endpoint communication across an isolation enforced EPG is dropped within a bridge domain.
- All Layer 3 endpoint communication across an isolation enforced EPG is dropped within the same subnet.
- Preserving QoS CoS priority settings is not supported when traffic is flowing from an EPG with isolation enforced to an EPG without isolation enforced.

Intra-EPG Isolation for Bare Metal Servers

Intra-EPG Isolation for Bare Metal Servers

Intra-EPG endpoint isolation policies can be applied to directly connected endpoints such as bare metal servers. Examples use cases include the following:

- Backup clients have the same communication requirements for accessing the backup service, but they don't need to communicate with each other.
- Servers behind a load balancer have the same communication requirements, but isolating them from each other protects against a server that is compromised or infected.
Bare metal EPG isolation is enforced at the leaf switch. Bare metal servers use VLAN encapsulation. All unicast, multicast and broadcast traffic is dropped (denied) within isolation enforced EPGs. ACI bridge-domains can have a mix of isolated and regular EPGs. Each Isolated EPG can have multiple VLANs where intra-vlan traffic is denied.

**Fig 15: Intra-EPG Isolation for Bare Metal Servers**

**Configuring Intra-EPG Isolation for Bare Metal Servers Using the GUI**

The port the EPG uses must be associated with a bare metal server interface in the physical domain that is used to connect the bare metal servers directly to leaf switches.

**Procedure**

**Step 1** In a tenant, right click on an Application Profile, and open the Create Application EPG dialog box to perform the following actions:

a) In the Name field, add the EPG name (intra_EPG-deny).

b) For Intra EPG Isolation, click Enforced.

c) In the Bridge Domain field, choose the bridge domain from the drop-down list (bd1).

d) Check the Statically Link with Leaves/Paths check box.

e) Click Next.

**Step 2** In the Leaves/Paths dialog box, perform the following actions:

a) In the Path section, choose a path from the drop-down list (Node-107/eth1/16) in Trunk Mode.

   Specify the Port Encap (vlan-102) for the secondary VLAN.

   **Note** If the bare metal server is directly connected to a leaf switch, only the Port Encap secondary VLAN is specified.

   Specify the Primary Encap (vlan-103) for the primary VLAN.
b) Click **Update**.

c) Click **Finish**.

---

### Configuring Intra-EPG Isolation for Bare Metal Servers Using the NX-OS Style CLI

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In the CLI, create an intra-EPG isolation EPG:</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;The VMM case is below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ifav19-ifcl(config)# tenant Test_Isolation</td>
<td>In the CLI, create an intra-EPG isolation EPG:</td>
<td></td>
</tr>
<tr>
<td>ifav19-ifcl(config-tenant)# application PVLAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ifav19-ifcl(config-tenant-app)# epg EPG1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ifav19-ifcl(config-tenant-app-epg)# show running-config</td>
<td></td>
<td></td>
</tr>
<tr>
<td># Command: show running-config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tenant Test_Isolation application PVLAN epg EPG1 tenant Test_Isolation application PVLAN epg EPG1 bridge-domain member BD1 contract consumer bare-metal contract consumer default contract provider Isolate_EPG isolation enforce</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exit ifav19-ifcl(config)# leaf ifav19-leaf3 ifav19-ifcl(config-leaf)# interface ethernet 1/16 ifav19-ifcl(config-leaf-if)# show running-config ifav19-ifcl(config-leaf-if)# switchport trunk native vlan 101 tenant Test_Isolation application PVLAN epg StaticEPG primary-vlan 100 exit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Verify the configuration:&lt;br&gt;<strong>Example:</strong>&lt;br&gt;show epg StaticEPG detail Application EPG Data:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant</td>
<td>Test_Isolation</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>PVLAN</td>
<td></td>
</tr>
<tr>
<td>AEPg</td>
<td>StaticEPG</td>
<td></td>
</tr>
<tr>
<td>BD</td>
<td>BD1</td>
<td></td>
</tr>
<tr>
<td>uSeg EPG</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>Intra EPG Isolation</td>
<td>enforced</td>
<td></td>
</tr>
<tr>
<td>Vlan Domains</td>
<td>phys</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Consumed Contracts: bare-metal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provided Contracts: default, Isolate_EPG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denied Contracts:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qos Class: unspecified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag List:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMM Domains:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>Type</td>
<td></td>
</tr>
<tr>
<td>Primary</td>
<td>Encap</td>
<td></td>
</tr>
<tr>
<td>Encap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>DVS1</td>
<td>VMware</td>
<td>On</td>
</tr>
<tr>
<td>Demand</td>
<td>immediate</td>
<td>formed</td>
</tr>
<tr>
<td>auto</td>
<td>auto</td>
<td></td>
</tr>
</tbody>
</table>

<p>| Static Leaves: |         |
| Node | Encap | Deployment |
| Immediacy Mode |  |</p>
<table>
<thead>
<tr>
<th>Modification Time</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>

<p>| Static Paths: |         |
| Node | Interface | Encap |</p>
<table>
<thead>
<tr>
<th>Modification Time</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>

<p>| Static Endpoints: |         |</p>
<table>
<thead>
<tr>
<th>Node</th>
<th>Interface</th>
<th>Encap</th>
<th>End Point MAC</th>
<th>End Point IP Address</th>
<th>Modification Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>------------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------------</td>
<td>------------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
Configuring Intra-EPG Isolation for Bare Metal Servers Using the REST API

Before you begin

The port the EPG uses must be associated with a bare metal server interface in the physical domain.

Procedure

Step 1
Send this HTTP POST message to deploy the application using the XML API.

Example:

```
POST https://apic-ip-address/api/mo/uni/tn-ExampleCorp.xml
```

Step 2
Include this XML structure in the body of the POST message.

Example:

```
<fvTenant name="Tenant_BareMetal">
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <fvRsBd tnFvBDName="bd"/>
      <fvRsDomAtt tDn="uni/phys-Dom1"/>
      <!-- PATH ASSOCIATION -->
      <fvRsPathAtt tDn="topology/pod-1/paths-1017/pathep-[eth1/2]" encap="vlan-51"
        primaryEncap="vlan-100" instrImedcy='immediate'/>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

Intra-EPG Isolation for VMWare vDS

Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch

Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or uSeg EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another. However, conditions exist in which total isolation of the endpoint devices from one another within an EPG is desirable. For example, you may want to enforce intra-EPG isolation if the endpoint VMs in the same EPG belong to multiple tenants, or to prevent the possible spread of a virus.

A Cisco ACI virtual machine manager (VMM) domain creates an isolated PVLAN port group at the VMware VDS or Microsoft Hyper-V Virtual Switch for each EPG that has intra-EPG isolation enabled. A fabric administrator specifies primary encapsulation or the fabric dynamically specifies primary encapsulation at the time of EPG-to-VMM domain association. When the fabric administrator selects the VLAN-pri and VLAN-sec values statically, the VMM domain validates that the VLAN-pri and VLAN-sec are part of a static block in the domain pool.

Note

When intra-EPG isolation is not enforced, the VLAN-pri value is ignored even if it is specified in the configuration.
VLAN-pri/VLAN-sec pairs for the VMware VDS or Microsoft Hyper-V Virtual Switch are selected per VMM domain during the EPG-to-domain association. The port group created for the intra-EPG isolation EPGs uses the VLAN-sec tagged with type set to PVLAN. The VMware VDS or the Microsoft Hyper-V Virtual Switch and fabric swap the VLAN-pri/VLAN-sec encapsulation:

- Communication from the Cisco ACI fabric to the VMware VDS or Microsoft Hyper-V Virtual Switch uses VLAN-pri.
- Communication from the VMware VDS or Microsoft Hyper-V Virtual Switch to the Cisco ACI fabric uses VLAN-sec.

**Figure 16: Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch**

Note these details regarding this illustration:

1. EPG-DB sends VLAN traffic to the Cisco ACI leaf switch. The Cisco ACI egress leaf switch encapsulates traffic with a primary VLAN (PVLAN) tag and forwards it to the Web-EPG endpoint.

2. The VMware VDS or Microsoft Hyper-V Virtual Switch sends traffic to the Cisco ACI leaf switch using VLAN-sec. The Cisco ACI leaf switch drops all intra-EPG traffic because isolation is enforced for all intra VLAN-sec traffic within the Web-EPG.

3. The VMware VDS or Microsoft Hyper-V Virtual Switch VLAN-sec uplink to the Cisco ACI Leaf is in isolated trunk mode. The Cisco ACI leaf switch uses VLAN-pri for downlink traffic to the VMware VDS or Microsoft Hyper-V Virtual Switch.
4. The PVLAN map is configured in the VMware VDS or Microsoft Hyper-V Virtual Switch and Cisco ACI leaf switches. VM traffic from WEB-EPG is encapsulated in VLAN-sec. The VMware VDS or Microsoft Hyper-V Virtual Switch denies local intra-WEB EPG VM traffic according to the PVLAN tag. All intra-ESXi host or Microsoft Hyper-V host VM traffic is sent to the Cisco ACI leaf using VLAN-Sec.

Related Topics
For information on configuring intra-EPG isolation in a Cisco AVS environment, see Intra-EPG Isolation Enforcement for Cisco AVS, on page 65.

Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the GUI

Procedure

Step 1 Log into Cisco APIC.
Step 2 Choose Tenants > tenant.
Step 3 In the left navigation pane expand the Application Profiles folder and appropriate application profile.
Step 4 Right-click the Application EPGs folder and then choose Create Application EPG.
Step 5 In the Create Application EPG dialog box, complete the following steps:
   a) In the Name field, add the EPG name.
   b) In the Intra EPG Isolation area, click Enforced.
   c) In the Bridge Domain field, choose the bridge domain from the drop-down list.
   d) Associate the EPG with a baremetal/physical domain interface or with a VM Domain.
      • For the VM Domain case, check the Associate to VM Domain Profiles check box.
      • For the bare metal case, check the Statically Link with Leaves/Paths check box.
   e) Click Next.
   f) In the Associated VM Domain Profiles area, click the + icon.
   g) From the Domain Profile drop-down list, choose the desired VMM domain.
      For the static case, in the Port Encap (or Secondary VLAN for Micro-Seg) field, specify the secondary VLAN, and in the Primary VLAN for Micro-Seg field, specify the primary VLAN. If the Encap fields are left blank, values will be allocated dynamically.
      Note For the static case, a static VLAN must be available in the VLAN pool.

Step 6 Click Update and click Finish.
Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the NX-OS Style CLI

Procedure

Step 1  In the CLI, create an intra-EPG isolation EPG:

Example:
The following example is for VMware VDS:

```
apic1(config)# tenant Test_Isolation
apic1(config-tenant)# application PVLAN
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# show running-config
# Command: show running-config tenant Tenant_VMM application Web epg intraEPGDeny
tenant Tenant_VMM
application Web
epg intraEPGDeny
  bridge-domain member VMM_BD
  vmware-domain member PVLAN encap vlan-2001 primary-encap vlan-2002 push on-demand
  vmware-domain member mininet
  exit
  isolation enforce
  exit
  exit
  exit
apic1(config-tenant-app-epg)#
```

Example:
The following example is for Microsoft Hyper-V Virtual Switch:

```
apic1(config)# tenant Test_Isolation
apic1(config-tenant)# application PVLAN
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# show running-config
# Command: show running-config tenant Tenant_VMM application Web epg intraEPGDeny
tenant Tenant_VMM
application Web
epg intraEPGDeny
  bridge-domain member VMM_BD
  microsoft-domain member domain1 encap vlan-2003 primary-encap vlan-2004
  microsoft-domain member domain2
  exit
  isolation enforce
  exit
  exit
  exit
apic1(config-tenant-app-epg)#
```

Step 2  Verify the configuration:

Example:

```
show epg StaticEPG detail
Application EPG Data:
  Tenant : Test_Isolation
  Application : PVLAN
  AEPg : StaticEPG
  BD : VMM_BD
  uSeg EPG : no
```
Intra EPG Isolation: **enforced**

Vlan Domains: **VMM**

Consumed Contracts: VMware_vDS-Ext

Provided Contracts: default, Isolate_EPG

Denied Contracts: 

Qos Class: unspecified

Tag List:

**VMM Domains:**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Type</th>
<th>Deployment Immediacy</th>
<th>Resolution Immediacy</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encap</td>
<td>Primary</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

Ensap Primary

<table>
<thead>
<tr>
<th>Encap</th>
<th>Type</th>
<th>Deployment Immediacy</th>
<th>Resolution Immediacy</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVS1</td>
<td>VMware</td>
<td>On Demand</td>
<td>immediate</td>
<td>formed</td>
</tr>
<tr>
<td>auto</td>
<td>auto</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

**Static Leaves:**

<table>
<thead>
<tr>
<th>Node</th>
<th>Encap</th>
<th>Deployment Immediacy</th>
<th>Mode</th>
<th>Modification Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Static Paths:</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Interface</td>
<td>Encap</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>1018</td>
<td>eth101/1/1</td>
<td>vlan-100</td>
</tr>
<tr>
<td>1019</td>
<td>eth1/16</td>
<td>vlan-101</td>
</tr>
</tbody>
</table>

**Static Endpoints:**

<table>
<thead>
<tr>
<th>Node</th>
<th>Interface</th>
<th>Encap</th>
<th>End Point MAC</th>
<th>End Point IP Address</th>
<th>Modification Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Dynamic Endpoints:**

Encap: (P): Primary VLAN, (S): Secondary VLAN

<table>
<thead>
<tr>
<th>Node</th>
<th>Interface</th>
<th>Encap</th>
<th>End Point MAC</th>
<th>End Point IP Address</th>
<th>Modification Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1017</td>
<td>eth1/3</td>
<td>vlan-943(P)</td>
<td>00:50:56:B3:64:C4</td>
<td>2016-02-17T18:35:32.224-08:00</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the REST API**

**Procedure**

**Step 1** Send this HTTP POST message to deploy the application using the XML API.

**Example:**

---
POST https://apic-ip-address/api/mo/uni/tn-ExampleCorp.xml

Step 2
For a VMware VDS or Microsoft Hyper-V Virtual Switch deployment, include one of the following XML structures in the body of the POST message.

Example:
The following example is for VMware VDS:

```xml
?fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <fvRsBd tnFvBDName="bd" />
      <!-- STATIC ENCAP ASSOCIATION TO VMM DOMAIN-->
      <fvRsDomAtt encap="vlan-2001" instrImedcy="lazy" primaryEncap="vlan-2002" resImedcy="immediate" tDn="uni/vmmp-VMware/dom-DVS1">
    </fvAEPg>
  </fvAp>
</fvTenant>
```

Example:
The following example is for Microsoft Hyper-V Virtual Switch:

```xml
?fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <fvRsBd tnFvBDName="bd" />
      <!-- STATIC ENCAP ASSOCIATION TO VMM DOMAIN-->
      <fvRsDomAtt tDn="uni/vmmp-Microsoft/dom-domain1">
        <fvRsDomAtt encap="vlan-2004" instrImedcy="lazy" primaryEncap="vlan-2003" resImedcy="immediate" tDn="uni/vmmp-Microsoft/dom-domain2">
      </fvAEPg>
  </fvAp>
</fvTenant>
```

Intra-EPG Isolation for AVS

Intra-EPG Isolation Enforcement for Cisco AVS

By default, endpoints with an EPG can communicate with each other without any contracts in place. However, you can isolate endpoints within an EPG from each other. In some instances, you might want to enforce endpoint isolation within an EPG to prevent a VM with a virus or other problem from affecting other VMs in the EPG.

You can configure isolation on all or none of the endpoints within an application EPG; you cannot configure isolation on some endpoints but not on others.

Isolating endpoints within an EPG does not affect any contracts that enable the endpoints to communicate with endpoints in another EPG.

Isolating endpoints within an EPG will trigger a fault when the EPG is associated with Cisco AVS domains in VLAN mode.
Using intra-EPG isolation on a Cisco AVS microsegment (uSeg) EPG is not currently supported. Communication is possible between two endpoints that reside in separate uSeg EPGs if either has intra-EPG isolation enforced, regardless of any contract that exists between the two EPGs.

### Configuring Intra-EPG Isolation for Cisco AVS Using the GUI

Follow this procedure to create an EPG in which the endpoints of the EPG are isolated from each other.

The port that the EPG uses must belong to one of the VM Managers (VMMs).

#### Before you begin

Make sure that Cisco AVS is in VXLAN mode.

#### Procedure

1. Log in to Cisco APIC.
2. Choose Tenants, expand the folder for the tenant, and then expand the Application Profiles folder.
3. Right-click an application profile, and choose Create Application EPG.
4. In the Create Application EPG dialog box, complete the following actions:
   a) In the Name field, enter the EPG name.
   b) In the Intra EPG Isolation area, click Enforced.
   c) From the Bridge Domain drop-down list, choose the bridge domain.
   d) Check the Associate to VM Domain Profiles check box.
   e) Click Next.
   f) In the Associate VM Domain Profiles area, click the plus icon, and from the Domain Profile drop-down list, choose the desired VMM domain.
   g) Click Update and click FINISH.

#### What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choosing Statistics to View for Isolated Endpoints on Cisco AVS and Viewing Statistics for Isolated Endpoints on Cisco AVS in this guide.
Configuring Intra-EPG Isolation for Cisco AVS Using the NX-OS Style CLI

Before you begin
Make sure that Cisco AVS is in VXLAN mode.

Procedure

In the CLI, create an intra-EPG isolation EPG:

Example:

```bash
# Command: show running-config
tenant TENANT1
application APP1
    epg EPG1
        bridge-domain member VMM_BD
        vmware-domain member VMMDOM1
        isolation enforce <---- This enables EPG into isolation mode.
        exit
exit
```

What to do next
You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choosing Statistics to View for Isolated Endpoints on Cisco AVS and Viewing Statistics for Isolated Endpoints on Cisco AVS in this guide.

Configuring Intra-EPG Isolation for Cisco AVS Using the REST API

Before you begin
Make sure that Cisco AVS is in VXLAN mode.

Procedure

Step 1
Send this HTTP POST message to deploy the application using the XML API.

Example:

```plaintext
POST
https://192.0.20.123/api/mo/uni/tn-ExampleCorp.xml
```

Step 2
For a VMM deployment, include the XML structure in the following example in the body of the POST message.

Example:

```
Example:
Example:
    <fvTenant name="Tenant_VMM">
        <fvAp name="Web">
            <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
                <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
            </fvAEPg>
        </fvAp>
    </fvTenant>
```
Choosing Statistics to View for Isolated Endpoints on Cisco AVS

If you configured intra-EPG isolation on a Cisco AVS, you need to choose statistics—such as denied connections, received packets, or transmitted multicast packets—for the endpoints before you can view them.

Procedure

Step 1 Log into Cisco APIC.
Step 2 Choose Tenants > tenant.
Step 3 In the tenant navigation pane, choose Application Profiles > profile > Application EPGs, and then choose the EPG containing the endpoint the statistics for which you want to view.
Step 4 In the EPG Properties work pane, click the Operational tab to display the endpoints in the EPG.
Step 5 Double-click the endpoint.
Step 6 In the Properties dialog box for the endpoint, click the Stats tab and then click the check icon.
Step 7 In the Select Stats dialog box, in the Available pane, choose the statistics that you want to view for the endpoint and then use the right-pointing arrow to move them into the Selected pane.
Step 8 Click SUBMIT.

Viewing Statistics for Isolated Endpoints on Cisco AVS

If you configured intra-EPG isolation on a Cisco AVS, once you have chosen statistics for the endpoints, you can view them.

Before you begin

You must have chosen statistics to view for isolated endpoints. See "Choosing Statistics to View for Isolated Endpoints for Cisco AVS" in this guide for instructions.

Procedure

Step 1 Log into Cisco APIC.
Step 2 Choose Tenants > tenant.
**Step 3**  In the tenant navigation pane, choose Application Profiles > profile > Application EPGs, and then choose the EPG containing the endpoint the statistics for which you want to view.

**Step 4**  In the EPG Properties work pane, click the Stats tab to display the statistics for the EPG.

The central pane displays the statistics that you chose earlier. You can change the view by clicking the table view or chart view icon on the upper right side of the work pane.
Viewing Statistics for Isolated Endpoints on Cisco AVS
Access Interfaces

This chapter contains the following sections:

- Physical Ports, on page 71
- Port Cloning, on page 76
- Port Channels, on page 77
- Virtual Port Channels, on page 87
- Reflective Relay, on page 99
- FEX Interfaces, on page 102
- Configuring Port Profiles to Change Ports from Uplink to Downlink or Downlink to Uplink, on page 114

Physical Ports

Configuring Leaf Switch Physical Ports Using Policy Association

The procedure below uses a Quick Start wizard.

Note

This procedure provides the steps for attaching a server to an ACI leaf switch interface. The steps would be the same for attaching other kinds of devices to an ACI leaf switch interface.

Figure 17: Switch Interface Configuration for Bare Metal Server
Before you begin

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
- The target leaf switches are registered in the ACI fabric and available.

Procedure

**Step 1** On the APIC menu bar, navigate to Fabric > External Access Policies > Quick Start, and click Configure an interface, PC, and VPC.

**Step 2** In the Select Switches To Configure Interfaces work area, click the large + to select switches to configure. In the Switches section, click the + to add switch ID(s) from the drop-down list of available switch IDs and click Update.

**Step 3** Click the large + to configure switch interfaces.

The interface policy group is a named policy that specifies the group of interface policies you will apply to the selected interfaces of the switch. Examples of interface policies include Link Level Policy (for example, 1gbit port speed), Storm Control Interface Policy, and so forth.

**Note** The Attached Device Type domain is required for enabling an EPG to use the interfaces specified in the switch profile.

- a) Specify individual as the interface type to use.
- b) Specify the interface ID to use.
- c) Specify the interface policies to use.
- d) Specify the attached device type to use. Choose Bare Metal for connecting bare metal servers. Bare metal uses the phys domain type.
- e) Click Save to update the policy details, then click Submit to submit the switch profile to the APIC.

The APIC creates the switch profile, along with the interface, selector, and attached device type policies.

**Verification:** Use the CLI show int command on the switch where the server is attached to verify that the switch interface is configured accordingly.

What to do next

This completes the basic leaf interface configuration steps.

**Note** While this configuration enables hardware connectivity, no data traffic can flow without a valid application profile, EPG, and contract that is associated with this hardware configuration.

Configuring Leaf Switch Physical Ports Using Port Association

This procedure provides the steps for attaching a server to an ACI leaf switch interface. The steps would be the same for attaching other kinds of devices to an ACI leaf switch interface.
Before you begin

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.

- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.

- The target leaf switches are registered in the ACI fabric and available.

Procedure

Step 1

On the APIC menu bar, navigate to Fabric > Inventory > Inventory, choose a pod and navigate to the Configure tab.

A graphical representation of the switch appears. Choose the port to configure. Once selected, port configure type will appear at the top in the form of a highlighted port configuration type. Choose configuration type and those configuration parameters will appear.

Step 2

Once you have assigned the appropriate fields to the configuration, click Submit.

In this configuration, all changes to the leaf switch are done by selecting the port and applying the policy to it. All leaf switch configuration is done right here on this page.

You have selected the port then applied a policy to it.

What to do next

This completes the basic leaf interface configuration steps.

Configuring Physical Ports in Leaf Nodes and FEX Devices Using the NX-OS CLI

The commands in the following examples create many managed objects (MOs) in the ACI policy model that are fully compatible with the REST API/SDK and GUI. However, the CLI user can focus on the intended network configuration instead of ACI model internals.

The following figure shows examples of Ethernet ports directly on leaf nodes or FEX modules attached to leaf nodes and how each is represented in the CLI. For FEX ports, the fex-id is included in the naming of the port itself as in ethernet 101/1/1. While describing an interface range, the ethernet keyword need not be repeated as in NX-OS. Example: interface ethernet 101/1/1-2, 102/1/1-2.
- Leaf node ID numbers are global.
- The `fex-id` numbers are local to each leaf.
- Note the space after the keyword `ethernet`.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>apic1# configure</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>leaf node-id</code></td>
<td>Specifies the leaf or leafs to be configured. The <code>node-id</code> can be a single node ID or a range of IDs, in the form <code>node-id1-node-id2</code>, to which the configuration will be applied.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>apic1(config)# leaf 102</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>interface type</code></td>
<td>Specifies the interface that you are configuring. You can specify the interface type and identity. For an Ethernet port, use “ethernet slot / port.”</td>
</tr>
<tr>
<td></td>
<td>Example: <code>apic1(config-leaf)# interface ethernet 1/2</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) <code>fex associate node-id</code></td>
<td>If the interface or interfaces to be configured are FEX interfaces, you must use this command to attach the FEX module to a leaf node before configuration.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>apic1(config-leaf-if)# fex associate 101</code></td>
<td>Note: This step is required before creating a port-channel using FEX ports.</td>
</tr>
</tbody>
</table>
Step 5

speed speed

Example:
apic1(config-leaf-if)# speed 10G

The speed setting is shown as an example. At this point you can configure any of the interface settings shown in the table below.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>shut</td>
<td>Shut down physical interface</td>
</tr>
<tr>
<td>speed speedValue</td>
<td>Set the speed for physical interface</td>
</tr>
<tr>
<td>link debounce time</td>
<td>Set link debounce</td>
</tr>
<tr>
<td>negotiate auto</td>
<td>Configure negotiate</td>
</tr>
<tr>
<td>cdp enable</td>
<td>Disable/enable Cisco Discovery Protocol (CDP)</td>
</tr>
<tr>
<td>mcp enable</td>
<td>Disable/enable Mis-cabling Protocol (MCP)</td>
</tr>
<tr>
<td>lldp transmit</td>
<td>Set the transmit for physical interface</td>
</tr>
<tr>
<td>lldp receive</td>
<td>Set the LLDP receive for physical interface</td>
</tr>
<tr>
<td>spanning-tree {bpdu-guard</td>
<td>bpdu-filter} {enable</td>
</tr>
<tr>
<td>storm-control level percentage [ burst-rate percentage ]</td>
<td>Storm-control configuration (percentage)</td>
</tr>
<tr>
<td>storm-control pps packets-per-second burst-rate packets-per-second</td>
<td>Storm-control configuration (packets-per-second)</td>
</tr>
</tbody>
</table>

Examples

Configure one port in a leaf node. The following example shows how to configure the interface eth1/2 in leaf 101 for the following properties: speed, cdp, and admin state.

apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/2
apic1(config-leaf-if)# speed 10G
apic1(config-leaf-if)# cdp enable
apic1(config-leaf-if)# no shut

Configure multiple ports in multiple leaf nodes. The following example shows the configuration of speed for interfaces eth1/1-10 for each of the leaf nodes 101-103.

apic1(config)# leaf 101-103
apic1(config-leaf)# interface eth 1/1-10
Attach a FEX to a leaf node. The following example shows how to attach a FEX module to a leaf node. Unlike in NX-OS, the leaf port Eth1/5 is implicitly configured as fabric port and a FEX fabric port-channel is created internally with the FEX uplink port(s). In ACI, the FEX fabric port-channels use default configuration and no user configuration is allowed.

**Note**
This step is required before creating a port-channel using FEX ports, as described in the next example.

```
apic1(config)# leaf 102
apic1(config-leaf)# interface eth 1/5
apic1(config-leaf-if)# fex associate 101
```

Configure FEX ports attached to leaf nodes. This example shows configuration of speed for interfaces eth1/1-10 in FEX module 101 attached to each of the leaf nodes 102-103. The FEX ID 101 is included in the port identifier. FEX IDs start with 101 and are local to a leaf.

```
apic1(config)# leaf 102-103
apic1(config-leaf)# interface eth 101/1/1-10
apic1(config-leaf-if)# speed 1G
```

## Port Cloning

### Cloning Port Configurations

In the Cisco APIC Release 3.2 and later, the Port Cloning feature is supported. After you configure a leaf switch port, you can copy the configuration and apply it to other ports. This is only supported in the APIC GUI (not in the NX-OS style CLI).

Port cloning is used for small numbers of leaf switch ports (interfaces) that are individually configured, not for interfaces configured using Fabric Access Policies, that you deploy on multiple nodes in the fabric.

Port cloning is only supported for Layer 2 configurations.

The following policies are not supported on a cloned port:

- Attachable Access Entity
- Storm Control
- DWDM
- MACsec
Cloning a Configured Leaf Switch Port Using the APIC GUI

This task describes how to clone a leaf switch port that you previously configured. For more information about configuring ports, see Cisco APIC Layer 2 Networking Configuration Guide.

Before you begin
Configure a leaf switch port (with supported Layer 2 policies) in the GUI under Fabric > Inventory, and one of the following:

- Topology > Interface > Configuration Mode
- Pod > Interface > Configuration Mode
- Pod> Leaf > Interface > Configuration Mode

Procedure

Step 1 On the Menu bar, choose Fabric > Inventory.
Step 2 Navigate to the location where you configured the first port.
Step 3 For example, expand Pod and choose Leaf.
Step 4 Click Interface and choose Configuration from the drop-down list under Mode.
Step 5 Click the + icon on the interface menu bar to choose the leaf switch where the port to clone is located.
Step 6 Right-click the port you previously configured and choose Copy.
Step 7 Right-click the port on which you want to copy the configuration and choose Paste.

Port Channels

ACI Leaf Switch Port Channel Configuration Using the GUI

The procedure below uses a Quick Start wizard.
This procedure provides the steps for attaching a server to an ACI leaf switch interface. The steps would be the same for attaching other kinds of devices to an ACI leaf switch interface.

**Figure 18: Switch Port Channel Configuration**

**Before you begin**
- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
- The target leaf switches are registered in the ACI fabric and available.

**Procedure**

**Step 1** On the APIC menu bar, navigate to **Fabric > External Access Policies > Quick Start**, and click **Configure an interface, PC, and VPC**.

**Step 2** In the **Select Switches To Configure Interfaces** work area, click the large + to select switches to configure. In the **Switches** section, click the + to add switch ID(s) from the drop-down list of available switch IDs and click **Update**.

**Step 3** Click the large + to configure switch interfaces.

The interface policy group is a named policy that specifies the group of interface policies you will apply to the selected interfaces of the switch. Examples of interface policies include Link Level Policy (for example, 1gbit port speed), Storm Control Interface Policy, and so forth.

**Note** The **Attached Device Type** is required for enabling an EPG to use the interfaces specified in the switch profile.

- a) Specify **pc** as the interface type to use.
- b) Specify the interface IDs to use.
- c) Specify the interface policies to use. For example, click the **Port Channel Policy** drop-down arrow to choose an existing port channel policy or to create a new port channel policy.
Choosing to create a port channel policy displays the Create Port Channel Policy dialog box where you can specify the policy details and enable features such as symmetric hashing. Also note that choosing the Symmetric hashing option displays the Load Balance Hashing field, which enables you to configure hash tuple. However, only one customized hashing option can be applied on the same leaf switch.

- Symmetric hashing is not supported on the following switches:
  - Cisco Nexus 93128TX
  - Cisco Nexus 9372PX
  - Cisco Nexus 9372PX-E
  - Cisco Nexus 9372TX
  - Cisco Nexus 9372TX-E
  - Cisco Nexus 9396PX
  - Cisco Nexus 9396TX

Note

- Choosing to create a port channel policy displays the Create Port Channel Policy dialog box where you can specify the policy details and enable features such as symmetric hashing. Also note that choosing the Symmetric hashing option displays the Load Balance Hashing field, which enables you to configure hash tuple. However, only one customized hashing option can be applied on the same leaf switch.

- Symmetric hashing is not supported on the following switches:
  - Cisco Nexus 93128TX
  - Cisco Nexus 9372PX
  - Cisco Nexus 9372PX-E
  - Cisco Nexus 9372TX
  - Cisco Nexus 9372TX-E
  - Cisco Nexus 9396PX
  - Cisco Nexus 9396TX

Note

- Specify the attached device type to use. Choose Bare Metal for connecting bare metal servers. Bare metal uses the phys domain type.
- Click Save to update the policy details, then click Submit to submit the switch profile to the APIC.
  - The APIC creates the switch profile, along with the interface, selector, and attached device type policies.

Verification: Use the CLI show int command on the switch where the server is attached to verify that the switch interface is configured accordingly.

What to do next

This completes the port channel configuration steps.

Note

- While this configuration enables hardware connectivity, no data traffic can flow without a valid application profile, EPG, and contract that is associated with this hardware configuration.

Configuring Port Channels in Leaf Nodes and FEX Devices Using the NX-OS CLI

Port-channels are logical interfaces in NX-OS used to aggregate bandwidth for multiple physical ports and also for providing redundancy in case of link failures. In NX-OS, port-channel interfaces are identified by user-specified numbers in the range 1 to 4096 unique within a node. Port-channel interfaces are either configured explicitly (using the interface port-channel command) or created implicitly (using the channel-group command). The configuration of the port-channel interface is applied to all the member ports of the port-channel. There are certain compatibility parameters (speed, for example) that cannot be configured on the member ports.
In the ACI model, port-channels are configured as logical entities identified by a name to represent a collection of policies that can be assigned to set of ports in one or more leaf nodes. Such assignment creates one port-channel interface in each of the leaf nodes identified by an auto-generated number in the range 1 to 4096 within the leaf node, which may be same or different among the nodes for the same port-channel name. The membership of these port-channels may be same or different as well. When a port-channel is created on the FEX ports, the same port-channel name can be used to create one port-channel interface in each of the FEX devices attached to the leaf node. Thus, it is possible to create up to N+1 unique port-channel interfaces (identified by the auto-generated port-channel numbers) for each leaf node attached to N FEX modules. This is illustrated with the examples below. Port-channels on the FEX ports are identified by specifying the fex-id along with the port-channel name (interface port-channel foo fex 101, for example).

- N+1 instances per leaf of port-channel foo are possible when each leaf is connected to N FEX nodes.
- Leaf ports and FEX ports cannot be part of the same port-channel instance.
- Each FEX node can have only one instance of port-channel foo.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>apic1# configure</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>template port-channel channel-name</td>
<td>Creates a new port-channel or configures an existing port-channel (global configuration).</td>
</tr>
<tr>
<td>Example:</td>
<td>apic1(config)# template port-channel foo</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Deploys the EPG with the VLAN on all ports with which the port-channel is associated.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
apic1(config-po-ch-if)# switchport access vlan 4 tenant ExampleCorp application Web epg webEpg
```

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Channel-mode active</th>
</tr>
</thead>
</table>

**Example:**

```bash
apic1(config-po-ch-if)# channel-mode active
```

**Note**

To enable symmetric hashing, enter the `lACP symmetric-hash` command:

```bash
apic1(config-po-ch-if)# lACP symmetric-hash
```

**Note**

The `channel-mode` command is equivalent to the `mode` option in the channel-group command in NX-OS. In ACI, however, this is supported for the port-channel (not on a member port).

Symmetric hashing is not supported on the following switches:

- Cisco Nexus 93128TX
- Cisco Nexus 9372PX
- Cisco Nexus 9372PX-E
- Cisco Nexus 9372TX
- Cisco Nexus 9372TX-E
- Cisco Nexus 9396PX
- Cisco Nexus 9396TX

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Exit</th>
</tr>
</thead>
</table>

**Example:**

```bash
apic1(config-po-ch-if)# exit
```

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Leaf node-id</th>
</tr>
</thead>
</table>

**Example:**

```bash
apic1(config)# leaf 101
```

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Interface type</th>
</tr>
</thead>
</table>

**Example:**

```bash
apic1(config-leaf)# interface ethernet 1/1-2
```

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Channel-group channel-name</th>
</tr>
</thead>
</table>

**Example:**

```bash
apic1(config-leaf-if)# channel-group foo
```

Assigns the interface or range of interfaces to the port-channel. Use the keyword `no` to remove the interface from the port-channel. To change the port-channel assignment on an interface,
you can enter the `channel-group` command without first removing the interface from the previous port-channel.

This setting and other per-port LACP properties can be applied to member ports of a port-channel at this point.

In the ACI model, these commands are allowed only after the ports are member of a port channel. If a port is removed from a port channel, configuration of these per-port properties are removed as well.

The following table shows various commands for global configurations of port channel properties in the ACI model. These commands can also be used for configuring overrides for port channels in a specific leaf in the (config-leaf-if) CLI mode. The configuration made on the port-channel is applied to all member ports.

<table>
<thead>
<tr>
<th>CLI Syntax</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] speed &lt;speedValue&gt;</td>
<td>Set the speed for port-channel</td>
</tr>
<tr>
<td>[no] link debounce time &lt;time&gt;</td>
<td>Set Link Debounce for port-channel</td>
</tr>
<tr>
<td>[no] negotiate auto</td>
<td>Configure Negotiate for port-channel</td>
</tr>
<tr>
<td>[no] cdp enable</td>
<td>Disable/Enable CDP for port-channel</td>
</tr>
<tr>
<td>[no] mcp enable</td>
<td>Disable/Enable MCP for port-channel</td>
</tr>
<tr>
<td>[no] lldp transmit</td>
<td>Set the transmit for port-channel</td>
</tr>
<tr>
<td>[no] lldp receive</td>
<td>Set the lldp receive for port-channel</td>
</tr>
<tr>
<td>spanning-tree &lt;bpduguard</td>
<td>Configure spanning tree BPDU</td>
</tr>
<tr>
<td></td>
<td>bpdufilter&gt; &lt;enable</td>
</tr>
<tr>
<td>[no] storm-control level &lt;percentage&gt; [ burst-rate &lt;percentage&gt; ]</td>
<td>Storm-control configuration (percentage)</td>
</tr>
<tr>
<td>[no] storm-control pps &lt;packet-per-second&gt; burst-rate &lt;packets-per-second&gt;</td>
<td>Storm-control configuration (packets-per-second)</td>
</tr>
<tr>
<td>[no] channel-mode { active</td>
<td>passive</td>
</tr>
<tr>
<td>[no] lacp min-links &lt;value&gt;</td>
<td>Set minimum number of links</td>
</tr>
<tr>
<td>[no] lacp max-links &lt;value&gt;</td>
<td>Set maximum number of links</td>
</tr>
<tr>
<td>[no] lacp fast-select-hot-standby</td>
<td>LACP fast select for hot standby ports</td>
</tr>
</tbody>
</table>
Feature CLI Syntax | Feature
--- | ---
[no] lacp graceful-convergence | LACP graceful convergence
[no] lacp load-defer | LACP load defer member ports
[no] lacp suspend-individual | LACP individual Port suspension
[no] lacp port-priority | LACP port priority
[no] lacp rate | LACP rate

Examples

Configure a port channel (global configuration). A logical entity foo is created that represents a collection of policies with two configurations: speed and channel mode. More properties can be configured as required.

The channel mode command is equivalent to the mode option in the channel group command in NX-OS. In ACI, however, this supported for the port-channel (not on member port).

```plaintext
apic1(config)# template port-channel foo
apic1(config-po-ch-if)# switchport access vlan 4 tenant ExampleCorp application Web epg webEpg
apic1(config-po-ch-if)# speed 10G
apic1(config-po-ch-if)# channel-mode active
```

Configure ports to a port-channel in a FEX. In this example, port channel foo is assigned to ports Ethernet 1/1-2 in FEX 101 attached to leaf node 102 to create an instance of port channel foo. The leaf node will auto-generate a number, say 1002 to identify the port channel in the switch. This port channel number would be unique to the leaf node 102 regardless of how many instance of port channel foo are created.

The configuration to attach the FEX module to the leaf node must be done before creating port channels using FEX ports.

```plaintext
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 101/1/1-2
apic1(config-leaf-if)# channel-group foo
```

In Leaf 102, this port channel interface can be referred to as interface port-channel foo FEX 101.

```plaintext
apic1(config)# leaf 102
apic1(config-leaf)# interface port-channel foo fex 101
apic1(config-leaf)# shut
```

Configure ports to a port channel in multiple leaf nodes. In this example, port channel foo is assigned to ports Ethernet 1/1-2 in each of the leaf nodes 101-103. The leaf nodes will auto generate a number
unique in each node (which may be same or different among nodes) to represent the port-channel interfaces.

```bash
apic1(config)# leaf 101-103
apic1(config-leaf)# interface ethernet 1/1-2
apic1(config-leaf-if)# channel-group foo
```

Add members to port channels. This example would add two members eth1/3-4 to the port-channel in each leaf node, so that port-channel foo in each node would have members eth 1/1-4.

```bash
apic1(config)# leaf 101-103
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group foo
```

Remove members from port channels. This example would remove two members eth1/2, eth1/4 from the port channel foo in each leaf node, so that port channel foo in each node would have members eth 1/1, eth1/3.

```bash
apic1(config)# leaf 101-103
apic1(config-leaf)# interface eth 1/2,1/4
apic1(config-leaf-if)# no channel-group foo
```

Configure port-channel with different members in multiple leaf nodes. This example shows how to use the same port-channel foo policies to create a port-channel interface in multiple leaf nodes with different member ports in each leaf. The port-channel numbers in the leaf nodes may be same or different for the same port-channel foo. In the CLI, however, the configuration will be referred as interface port-channel foo. If the port-channel is configured for the FEX ports, it would be referred to as interface port-channel foo fex <fex-id>.

```bash
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/1-2
apic1(config-leaf-if)# channel-group foo
apic1(config-leaf-if)# exit
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group foo
apic1(config-leaf-if)# exit
apic1(config)# leaf 103
apic1(config-leaf)# interface ethernet 1/5-8
apic1(config-leaf-if)# channel-group foo
apic1(config-leaf-if)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/1-2
apic1(config-leaf-if)# channel-group foo
```

Configure per port properties for LACP. This example shows how to configure member ports of a port-channel for per-port properties for LACP.

**Note**

In ACI model, these commands are allowed only after the ports are member of a port channel. If a port is removed from a port channel, configuration of these per-port properties would be removed as well.

```bash
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/1-2
```
Configure admin state for port channels. In this example, a port-channel foo is configured in each of the leaf nodes 101-103 using the channel-group command. The admin state of port-channel(s) can be configured in each leaf using the port-channel interface. In ACI model, the admin state of the port-channel cannot be configured in the global scope.

// create port-channel foo in each leaf
apic1(config)# leaf 101-103
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group foo

// configure admin state in specific leaf
apic1(config)# leaf 101
apic1(config-leaf)# interface port-channel foo
apic1(config-leaf-if)# shut

Override config is very helpful to assign specific vlan-domain, for example, to the port-channel interfaces in each leaf while sharing other properties.

// configure a port channel global config
apic1(config)# interface port-channel foo
apic1(config-if)# speed 1G
apic1(config-if)# channel-mode active

// create port-channel foo in each leaf
apic1(config)# leaf 101-103
apic1(config-leaf)# interface ethernet 1/1-2
apic1(config-leaf-if)# channel-group foo

// override port-channel foo in leaf 102
apic1(config)# leaf 102
apic1(config-leaf)# interface port-channel foo
apic1(config-leaf-if)# speed 10G
apic1(config-leaf-if)# channel-mode on
apic1(config-leaf-if)# vlan-domain dom-foo

This example shows how to change port channel assignment for ports using the channel-group command. There is no need to remove port channel membership before assigning to other port channel.

apic1(config)# leaf 101-103
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group foo
apic1(config-leaf-if)# channel-group bar

Configuring Two Port Channels Applied to Multiple Switches Using the REST API

This example creates two port channels (PCs) on leaf switch 17, another port channel on leaf switch 18, and a third one on leaf switch 20. On each leaf switch, the same interfaces will be part of the PC (interface 1/10 to 1/15 for port channel 1 and 1/20 to 1/25 for port channel 2). The policy uses two switch blocks because
each a switch block can contain only one group of consecutive switch IDs. All these PCs will have the same configuration.

**Note**

Even though the PC configurations are the same, this example uses two different interface policy groups. Each Interface Policy Group represents a PC on a switch. All interfaces associated with a given interface policy group are part of the same PCs.

**Before you begin**

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
- The target leaf switch and protocol(s) are configured and available.

**Procedure**

To create the two PCs, send a post with XML such as the following:

**Example:**

```
<infraInfra dn="uni/infra">
  <infraNodeP name="test">
    <infraLeafS name="leafs" type="range">
      <infraNodeBlk name="nblk" from="17" to="18"/>
      <infraNodeBlk name="nblk" from="20" to="20"/>
    </infraLeafS>
    <infraRsAccPortP tDn="uni/infra/accportprof-test1"/>
    <infraRsAccPortP tDn="uni/infra/accportprof-test2"/>
  </infraNodeP>

  <infraAccPortP name="test1">
    <infraHPortS name="pselc" type="range">
      <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="10" toPort="15"/>
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-bndlgrp1"/>
    </infraHPortS>
  </infraAccPortP>

  <infraAccPortP name="test2">
    <infraHPortS name="pselc" type="range">
      <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="20" toPort="25"/>
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-bndlgrp2"/>
    </infraHPortS>
  </infraAccPortP>

  <infraFuncP>
```

Cisco APIC Layer 2 Networking Configuration Guide
Virtual Port Channels

ACI Virtual Port Channel Workflow

This workflow provides an overview of the steps required to configure a virtual port channel (VPC).

Figure 19: Virtual port channel configuration

1. Prerequisites

- Ensure that you have read/write access privileges to the infra security domain.
- Ensure that the target leaf switches with the necessary interfaces are available.
When creating a VPC domain between two Leaf nodes, please considering the hardware model limitations:

- Generation 1 switches are compatible only with other Generation 1 Switches. These switch models can be identified by the lack of “EX”, or “FX” at the end of the switch name. For example N9K-9312TX.

- Generation 2 and later switches can be mixed together in a VPC domain. These switch models can be identified with “EX”, “FX” or “FX2” at the end of the switch name. For example N9K-93108TC-EX, or N9K-9348GC-FXP.

Example:

Compatible VPC Switch Pairs:

- N9K-9312TX & N9K-9312TX
- N9K-93108TC-EX & N9K-9348GC-FXP
- Nexus 93180TC-FX & Nexus 93180YC-FX
- Nexus 93180YC-FX & Nexus 93180YC-FX

Incompatible VPC Switch Pairs:

- N9K-9312TX & N9K-93108TC-EX
- N9K-9312TX & Nexus 93180YC-FX

 Configure the Virtual Port Channel

1. On the APIC menu bar, navigate to Fabric > External Access Policies > Quick Start, and click Configure an interface, PC, and VPC to open the quick start wizard.

2. Provide the specifications for the policy name, switch IDs and the interfaces the virtual port channel will use. Add the Interface Policy parameters, such as group port speed, storm control, CDP, LLDP. Add the Attached Device Type as an External Bridged Device and specify the VLAN and domain that will be used.

3. Use the CLI `show int` command on the ACI leaf switches where the external switch is attached to verify that the switches and virtual port channel are configured accordingly.

**Note:** While this configuration enables hardware connectivity, no data traffic can flow without a valid application profile, EPG, and contract that is associated with this hardware configuration.

Configure the Application Profile

1. On the APIC menu bar, navigate to Tenant > tenant-name > Quick Start, and click Create an application profile under the tenant quick start wizard.

2. Configure the endpoint groups (EPGs), contracts, bridge domain, subnet, and context.
3. Associate the application profile EPGs with the virtual port channel switch profile created above.

ACI Leaf Switch Virtual Port Channel Configuration Using the GUI

The procedure below uses a Quick Start wizard.

Note
This procedure provides the steps for attaching a trunked switch to a ACI leaf switch virtual port channel. The steps would be the same for attaching other kinds of devices to an ACI leaf switch interface.

Figure 20: Switch Virtual Port Channel Configuration

Note
LACP sets a port to the suspended state if it does not receive an LACP PDU from the peer. This can cause some servers to fail to boot up as they require LACP to logically bring-up the port. You can tune behavior to individual use by disabling **LACP suspend individual**. To do so, create a port channel policy in your vPC policy group, and after setting the mode to LACP active, remove **Suspend Individual Port**. Now the ports in the vPC will stay active and continue to send LACP packets.

Note
Adaptive Load Balancing (ALB) (based on ARP Negotiation) across virtual port channels is not supported in the ACI.

**Before you begin**

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
- The target leaf switches are registered in the ACI fabric and available.
When creating a VPC domain between two leaf switches, both switches must be in the same switch generation, one of the following:

- Generation 1 - Cisco Nexus N9K switches without “EX” on the end of the switch name; for example, N9K-9312TX
- Generation 2 – Cisco Nexus N9K switches with “EX” on the end of the switch model name; for example, N9K-93108TC-EX

Switches such as these two are not compatible VPC peers. Instead, use switches of the same generation.

---

**Procedure**

**Step 1**  On the APIC menu bar, navigate to **Fabric > External Access Policies > Quick Start**, and click **Configure an interface, PC, and VPC**.

**Step 2**  In the **Configure an interface, PC, and VPC** work area, click the large + to select switches. The **Select Switches To Configure Interfaces** work area opens.

**Step 3**  Select switch IDs from the drop-down list, name the profile, then click **Save**. The saved policy displays in the **Configured Switch Interfaces** list.

**Step 4**  Configure the **Interface Policy Group** and **Attached Device Type** that the virtual port channel will use for the selected switches.

The interface policy group is a named policy that specifies the group of interface policies you will apply to the selected interfaces of the switch. Examples of interface policies include Link Level Policy (for example, 1gbit port speed), Storm Control Interface Policy, and so forth.

**Note**  The **Attached Device Type** domain is required for enabling an EPG to use the interfaces specified in the switch profile.

a) Specify **vpc** the interface type (individual, PC, or VPC) to use.
b) Specify the interface IDs to use.
c) Specify the interface policies to use.
d) Specify the attached device type to use. Choose **External Bridged Devices** for connecting a switch.
e) Specify the **Domain**, and **VLAN Range**.
f) Click **Save** to update the policy details, then click **Submit** to submit the switch profile to the APIC. The APIC creates the switch profile, along with the interface, selector, and attached device type policies.

**Verification:** Use the CLI **show int** command on the leaf switches where the external switch is attached to verify that the **vpc** is configured accordingly.

---

**What to do next**

This completes the switch virtual port channel configuration steps.
While this configuration enables hardware connectivity, no data traffic can flow without a valid application profile, EPG, and contract that is associated with this hardware configuration.

Configuring Virtual Port Channels in Leaf Nodes and FEX Devices Using the NX-OS CLI

A Virtual Port Channel (VPC) is an enhancement to port-channels that allows connection of a host or switch to two upstream leaf nodes to improve bandwidth utilization and availability. In NX-OS, VPC configuration is done in each of the two upstream switches and configuration is synchronized using peer link between the switches.

Note

When creating a VPC domain between two leaf switches, both switches must be in the same switch generation, one of the following:

- Generation 1 - Cisco Nexus N9K switches without “EX” on the end of the switch name; for example, N9K-9312TX
- Generation 2 – Cisco Nexus N9K switches with “EX” on the end of the switch model name; for example, N9K-93108TC-EX

Switches such as these two are not compatible VPC peers. Instead, use switches of the same generation.

The ACI model does not require a peer link and VPC configuration can be done globally for both the upstream leaf nodes. A global configuration mode called **vpc context** is introduced in ACI and VPC interfaces are represented using a type **interface vpc** that allows global configuration applicable to both leaf nodes.

Two different topologies are supported for VPC in the ACI model: VPC using leaf ports and VPC over FEX ports. It is possible to create many VPC interfaces between a pair of leaf nodes and similarly, many VPC interfaces can be created between a pair of FEX modules attached to the leaf node pairs in a straight-through topology.

VPC considerations include:

- The VPC name used is unique between leaf node pairs. For example, only one VPC 'corp' can be created per leaf pair (with or without FEX).
- Leaf ports and FEX ports cannot be part of the same VPC.
- Each FEX module can be part of only one instance of VPC corp.
- VPC context allows configuration
- The VPC context mode allows configuration of all VPCs for a given leaf pair. For VPC over FEX, the **fex-id** pairs must be specified either for the VPC context or along with the VPC interface, as shown in the following two alternative examples.

```
(config)# vpc context leaf 101 102
(config-vpc)# interface vpc Reg fex 101 101
```
In the ACI model, VPC configuration is done in the following steps (as shown in the examples below).

A VLAN domain is required with a VLAN range. It must be associated with the port-channel template.

1. VLAN domain configuration (global config) with VLAN range
2. VPC domain configuration (global config)
3. Port-channel template configuration (global config)
4. Associate the port-channel template with the VLAN domain
5. Port-channel configuration for VPC (global config)
6. Configure ports to VPC in leaf nodes
7. Configure L2, L3 for VPC in the vpc context

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>apic1# configure</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan-domain[dynamic] [type domain-type]</td>
<td>Configures a VLAN domain for the virtual port-channel (here with a port-channel template).</td>
</tr>
<tr>
<td>Example:</td>
<td>apic1(config)# vlan-domain dom1 dynamic</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>vlanrange</td>
<td>Configures a VLAN range for the VLAN domain and exits the configuration mode. The range can be a single VLAN or a range of VLANs.</td>
</tr>
<tr>
<td>Example:</td>
<td>apic1(config-vlan)# vlan 1000-1999 apic1(config-vlan)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>vpc domain explicit domain-id leaf node-id1 node-id2</td>
<td>Configures a VPC domain between a pair of leaf nodes. You can specify the VPC domain ID in the explicit mode along with the leaf node pairs.</td>
</tr>
<tr>
<td>Example:</td>
<td>apic1(config)# vpc domain explicit 1 leaf 101 102</td>
<td>Alternative commands to configure a VPC domain are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• vpc domain [consecutive</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| **The consecutive and reciprocal options allow auto configuration of a VPC domain across all leaf nodes in the ACI fabric.**  

- **vpc domain consecutive domain-start leaf start-node end-node**  
  This command configures a VPC domain consecutively for a selected set of leaf node pairs. |

| **Step 5** | **peer-dead-interval interval**  
**Example:**  
apic1(config-vpc)# peer-dead-interval 10 | Configures the time delay the Leaf switch waits to restore the VPC before receiving a response from the peer. If it does not receive a response from the peer within this time, the Leaf switch considers the peer dead and brings up the VPC with the role as a master. If it does receive a response from the peer it restores the VPC at that point. The range is from 5 seconds to 600 seconds. The default is 200 seconds. |

| **Step 6** | **exit**  
**Example:**  
apic1(config-vpc)# exit | Returns to global configuration mode. |

| **Step 7** | **template port-channel channel-name**  
**Example:**  
apic1(config)# template port-channel corp | Creates a new port-channel or configures an existing port-channel (global configuration).  
All VPCs are configured as port-channels in each leaf pair. The same port-channel name must be used in a leaf pair for the same VPC. This port-channel can be used to create a VPC among one or more pairs of leaf nodes. Each leaf node will have only one instance of this VPC. |

| **Step 8** | **vlan-domain member vlan-domain-name**  
**Example:**  
vlan-domain member dom1 | Associates the port channel template with the previously configured VLAN domain. |

| **Step 9** | **switchport access vlan vlan-id tenant tenant-name application application-name epg epg-name**  
**Example:**  
apic1(config-po-ch-if)# switchport access vlan 4 tenant ExampleCorp application Web epg webEpg | Deploys the EPG with the VLAN on all ports with which the port-channel is associated. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>channel-mode active</td>
<td>Note A port-channel must be in active channel-mode for a VPC.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config-po-ch-if)# channel-mode active</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config-po-ch-if)# exit</td>
<td>Returns to configure mode.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td></td>
</tr>
<tr>
<td>leaf node-id1 node-id2</td>
<td>Specifies the pair of leaf switches to be configured.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config)# leaf 101-102</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td></td>
</tr>
<tr>
<td>interface type leaf/interface-range</td>
<td>Specifies the interface or range of interfaces that you are configuring to the port-channel.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf)# interface ethernet 1/3-4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td></td>
</tr>
<tr>
<td>[no] channel-group channel-name vpc</td>
<td>Assigns the interface or range of interfaces to the port-channel. Use the keyword <strong>no</strong> to remove the interface from the port-channel. To change the port-channel assignment on an interface, you can enter the <strong>channel-group</strong> command without first removing the interface from the previous port-channel.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# channel-group corp vpc</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td></td>
</tr>
<tr>
<td>vpc context leaf node-id1 node-id2</td>
<td>The vpc context mode allows configuration of VPC to be applied to both leaf node pairs.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config)# vpc context leaf 101 102</td>
<td></td>
</tr>
<tr>
<td><strong>Step 18</strong></td>
<td></td>
</tr>
<tr>
<td>interface vpc channel-name</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config-vpc)# interface vpc blue fex 102 102</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 19**      | (Optional) **[no]** shutdown | Administrative state configuration in the vpc context allows changing the admin state of a VPC with one command for both leaf nodes. |
| **Example:**     | apic1(config-vpc-if)# no shut | |

### Example

This example shows how to configure a basic VPC.

```bash
apic1# configure
apic1(config)# vlan-domain dom1 dynamic
apic1(config-vlan)# vlan 1000-1999
apic1(config-vlan)# exit
apic1(config)# vpc domain explicit 1 leaf 101 102
apic1(config-vpc)# peer-dead-interval 10
apic1(config-vpc)# exit
apic1(config)# template port-channel corp
apic1(config-po-ch-if)# vlan-domain member dom1
apic1(config-po-ch-if)# channel-mode active
apic1(config-po-ch-if)# exit
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group corp vpc
apic1(config-leaf-if)# exit
apic1(config)# vpc context leaf 101 102
```

This example shows how to configure VPCs with FEX ports.

```bash
apic1(config-leaf)# interface ethernet 101/1/1-2
apic1(config-leaf-if)# channel-group Reg vpc
apic1(config)# vpc context leaf 101 102
apic1(config-vpc)# interface vpc corp
apic1(config-vpc-if)# exit
apic1(config-vpc)# interface vpc red fex 101 101
apic1(config-vpc-if)# switchport
apic1(config-vpc-if)# exit
apic1(config-vpc)# interface vpc blue fex 102 102
apic1(config-vpc-if)# shut
```

### Configuring Virtual Port Channels Using the REST API

#### Configuring a Single Virtual Port Channel Across Two Switches Using the REST API

The two steps for creating a virtual port channel across two switches are as follows:
• Create a fabricExplicitGEp: this policy specifies the leaf switch that pairs to form the virtual port channel.
• Use the infra selector to specify the interface configuration.

The APIC performs several validations of the fabricExplicitGEp and faults are raised when any of these validations fail. A leaf can be paired with only one other leaf. The APIC rejects any configuration that breaks this rule. When creating a fabricExplicitGEp, an administrator must provide the IDs of both of the leaf switches to be paired. The APIC rejects any configuration which breaks this rule. Both switches must be up when fabricExplicitGEp is created. If one switch is not up, the APIC accepts the configuration but raises a fault. Both switches must be leaf switches. If one or both switch IDs corresponds to a spine, the APIC accepts the configuration but raises a fault.

Before you begin
• The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
• An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
• The target leaf switch and protocol(s) are configured and available.

Procedure

To create the fabricExplicitGEp policy and use the intra selector to specify the interface, send a post with XML such as the following example:

Example:

```xml
<fabricProtPol pairT="explicit">  
<fabricExplicitGEp name="tG" id="2">  
<fabricNodePEp id="18"/>  
<fabricNodePEp id="25"/>
</fabricExplicitGEp>
</fabricProtPol>
```

Configuring a Virtual Port Channel on Selected Port Blocks of Two Switches Using the REST API

This policy creates a single virtual port channel (VPC) on leaf switches 18 and 25, using interfaces 1/10 to 1/15 on leaf 18, and interfaces 1/20 to 1/25 on leaf 25.

Before you begin
• The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
• An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
• The target leaf switch and protocol(s) are configured and available.
When creating a VPC domain between two leaf switches, both switches must be in the same switch generation, one of the following:

- **Generation 1** - Cisco Nexus N9K switches without “EX” on the end of the switch name; for example, N9K-9312TX
- **Generation 2** – Cisco Nexus N9K switches with “EX” on the end of the switch model name; for example, N9K-93108TC-EX

Switches such as these two are not compatible VPC peers. Instead, use switches of the same generation.

**Procedure**

To create the VPC send a post with XML such as the following example:

**Example:**

```xml
<infraInfra dn="uni/infra">
  <infraNodeP name="test1">
    <infraLeafS name="leafs" type="range">
      <infraNodeBlk name="nblk"
        from_="18" to_="18"/>
    </infraLeafS>
    <infraRsAccPortP tDn="uni/infra/accportprof-test1"/>
  </infraNodeP>

  <infraNodeP name="test2">
    <infraLeafS name="leafs" type="range">
      <infraNodeBlk name="nblk"
        from_="25" to_="25"/>
    </infraLeafS>
    <infraRsAccPortP tDn="uni/infra/accportprof-test2"/>
  </infraNodeP>

  <infraAccPortP name="test1">
    <infraHPortS name="psselc" type="range">
      <infraPortBlk name="blk1"
        fromCard="1" toCard="1"
        fromPort="10" toPort="15"/>
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-bndlgrp"/>
    </infraHPortS>
  </infraAccPortP>

  <infraAccPortP name="test2">
    <infraHPortS name="psselc" type="range">
      <infraPortBlk name="blk1"
        fromCard="1" toCard="1"
        fromPort="20" toPort="25"/>
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-bndlgrp"/>
    </infraHPortS>
  </infraAccPortP>
</infraInfra>
```
Configuring a Single Virtual Port Channel Across Two Switches Using the REST API

The two steps for creating a virtual port channel across two switches are as follows:

- Create a fabricExplicitGEp: this policy specifies the leaf switch that pairs to form the virtual port channel.
- Use the infra selector to specify the interface configuration.

The APIC performs several validations of the fabricExplicitGEp and faults are raised when any of these validations fail. A leaf can be paired with only one other leaf. The APIC rejects any configuration that breaks this rule. When creating a fabricExplicitGEp, an administrator must provide the IDs of both of the leaf switches to be paired. The APIC rejects any configuration which breaks this rule. Both switches must be up when fabricExplicitGEp is created. If one switch is not up, the APIC accepts the configuration but raises a fault. Both switches must be leaf switches. If one or both switch IDs corresponds to a spine, the APIC accepts the configuration but raises a fault.

Before you begin

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
- The target leaf switch and protocol(s) are configured and available.

Procedure

To create the fabricExplicitGEp policy and use the intra selector to specify the interface, send a post with XML such as the following example:

Example:

```xml
<fabricProtPol pairT="explicit">
    <fabricExplicitGEp name="tG" id="2">
        <fabricNodePEp id="18"/>
        <fabricNodePEp id="25"/>
    </fabricExplicitGEp>
</fabricProtPol>
```
Reflective Relay

Reflective Relay (802.1Qbg)

Reflective relay is a switching option beginning with Cisco APIC Release 2.3(1). Reflective relay—the tagless approach of IEEE standard 802.1Qbg— forwards all traffic to an external switch, which then applies policy and sends the traffic back to the destination or target VM on the server as needed. There is no local switching. For broadcast or multicast traffic, reflective relay provides packet replication to each VM locally on the server.

One benefit of reflective relay is that it leverages the external switch for switching features and management capabilities, freeing server resources to support the VMs. Reflective relay also allows policies that you configure on the Cisco APIC to apply to traffic between the VMs on the same server.

In the Cisco ACI, you can enable reflective relay, which allows traffic to turn back out of the same port it came in on. You can enable reflective relay on individual ports, port channels, or virtual port channels as a Layer 2 interface policy using the APIC GUI, NX-OS CLI, or REST API. It is disabled by default.

The term Virtual Ethernet Port Aggregator (VEPA) is also used to describe 802.1Qbg functionality.

Reflective Relay Support

Reflective relay supports the following:

- IEEE standard 802.1Qbg tagless approach, known as reflective relay.

  Cisco APIC Release 2.3(1) release does not support the IEE standard 802.1Qbg S-tagged approach with multichannel technology.

- Physical domains.

  Virtual domains are not supported.

- Physical ports, port channels (PCs), and virtual port channels (VPCs).

  Cisco Fabric Extender (FEX) and blade servers are not supported. If reflective relay is enabled on an unsupported interface, a fault is raised, and the last valid configuration is retained. Disabling reflective relay on the port clears the fault.

- Cisco Nexus 9000 series switches with EX or FX at the end of their model name.

Enabling Reflective Relay Using the Advanced GUI

Reflective relay is disabled by default; however, you can enable it on a port, port channel, or virtual port channel as a Layer 2 interface policy on the switch. You first configure a policy and then associate the policy with a policy group.

Note

This procedure can be performed in the GUI in Advanced mode only.
Before you begin

This procedure assumes that you have set up the Cisco Application Centric Infrastructure (ACI) fabric and installed the physical switches.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Cisco APIC, choosing Advanced mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose Fabric &gt; External Access Policies &gt; &gt; Interface Policies and then open the Policies folder.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click the L2 Interface folder and choose Create L2 Interface Policy.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Create L2 Interface Policy dialog box, enter a name in the Name field.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Reflective Relay (802.1Qbg) area, click enabled.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Choose other options in the dialog box as needed.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click SUBMIT.</td>
</tr>
<tr>
<td>Step 8</td>
<td>In the Policies navigation pane, open the Policy Groups folder and click the Leaf Policy Groups folder.</td>
</tr>
<tr>
<td>Step 9</td>
<td>In the Leaf Policy Groups central pane, expand the ACTIONS drop-down list, and choose Create Leaf Access Port Policy Group, Create PC Interface Policy Group, Create VPC Interface Policy Group, or Create PC/VPC Override Policy Group.</td>
</tr>
<tr>
<td>Step 10</td>
<td>In the policy group dialog box, enter a name in the Name field.</td>
</tr>
<tr>
<td>Step 11</td>
<td>From the L2 Interface Policy drop-down list, choose the policy that you just created to enable Reflective Relay.</td>
</tr>
<tr>
<td>Step 12</td>
<td>Click SUBMIT.</td>
</tr>
</tbody>
</table>

Enabling Reflective Relay Using the NX-OS CLI

Reflective relay is disabled by default; however, you can enable it on a port, port channel, or virtual port channel as a Layer 2 interface policy on the switch. In the NX-OS CLI, you can use a template to enable reflective relay on multiple ports or you can enable it on individual ports.

Before you begin

This procedure assumes that you have set up the Cisco Application Centric Infrastructure (ACI) fabric and installed the physical switches.

Procedure

Enable reflective relay on one or multiple ports:

Example:

This example enables reflective relay on a single port:

```bash
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/2
apic1(config-leaf-if)# switchport vepa enabled
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```
Enabling Reflective Relay Using the REST API

Reflective relay is disabled by default; however, you can enable it on a port, port channel, or virtual port channel as a Layer 2 interface policy on the switch.

Before you begin

This procedure assumes that you have set up the Cisco Application Centric Infrastructure (ACI) fabric and installed the physical switches.
Procedure

Step 1 Configure a Layer 2 Interface policy with reflective relay enabled.

Example:

```xml
<l2IfPol name="VepaL2IfPol" vepa="enabled"/>
```

Step 2 Apply the Layer 2 interface policy to a leaf access port policy group.

Example:

```xml
<infraAccPortGrp name="VepaPortG">
  <infraRsL2IfPol tnL2IfPolName="VepaL2IfPol"/>
</infraAccPortGrp>
```

Step 3 Configure an interface profile with an interface selector.

Example:

```xml
<infraAccPortP name="vepa">
  <infraHPortS name="pselc" type="range">
    <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="20" toPort="22">
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-VepaPortG"/>
    </infraPortBlk>
  </infraHPortS>
</infraAccPortP>
```

Step 4 Configure a node profile with node selector.

Example:

```xml
<infraNodeP name="VepaNodeProfile">
  <infraLeafS name="VepaLeafSelector" type="range">
    <infraNodeBlk name="VepaNodeBlk" from="101" to="102"/>
  </infraLeafS>
  <infraRsAccPortP tDn="uni/infra/accportprof-vepa"/>
</infraNodeP>
```

---

**FEX Interfaces**

**Configuring Port, PC, and VPC Connections to FEX Devices**

FEX connections and the profiles used to configure them can be created using the GUI, NX-OS Style CLI, or the REST API.

Interface profiles for configuring FEX connections are supported since Cisco APIC, Release 3.0(1k).

For information on how to configure them using the NX-OS style CLI, see the topics about configuring ports, PCs and VPCs using the NX-OS style CLI.

**ACI FEX Guidelines**

Observe the following guidelines when deploying a FEX:
Assuming that no leaf switch front panel ports are configured to deploy and EPG and VLANs, a maximum of 10,000 port EPGs are supported for being deployed using a FEX.

For each FEX port or vPC that includes FEX ports as members, a maximum of 20 EPGs per VLAN are supported.

FEX Virtual Port Channels

The ACI fabric supports Cisco Fabric Extender (FEX) server-side virtual port channels (VPC), also known as an FEX straight-through VPC.

Note

When creating a VPC domain between two leaf switches, both switches must be in the same switch generation, one of the following:

- Generation 1 - Cisco Nexus N9K switches without “EX” or "FX" on the end of the switch name; for example, N9K-9312TX
- Generation 2 – Cisco Nexus N9K switches with “EX" or "FX" on the end of the switch model name; for example, N9K-93108TC-EX

Switches such as these two are not compatible VPC peers. Instead, use switches of the same generation.

Figure 21: Supported FEX VPC Topologies

Supported FEX VPC port channel topologies include the following:

- Both VTEP and non-VTEP hypervisors behind a FEX.
• Virtual switches (such as AVS or VDS) connected to two FEXs that are connected to the ACI fabric (VPCs directly connected on physical FEX ports is not supported - a VPC is supported only on port channels).

Note
When using GARP as the protocol to notify of IP to MAC binding changes to different interfaces on the same FEX you must set the bridge domain mode to ARP Flooding and enable EP Move Detection Mode: GARP-based Detection, on the L3 Configuration page of the bridge domain wizard. This workaround is only required with Generation 1 switches. With Generation 2 switches or later, this is not an issue.

Configuring a Basic FEX Connection Using the GUI

The procedure below uses a Quick Start wizard that automatically creates some necessary policies for FEX deployment. The main steps are as follows:

1. Configure a switch profile that includes an auto-generated FEX profile.
2. Customize the auto-generated FEX Profile to enable attaching a server to a single FEX port.

Figure 22: Basic FEX Configuration

Note
This procedure provides the steps for attaching a server to the FEX. The steps would be the same for attaching any device to an ACI attached FEX.

Note
Configuring FEX connections with FEX IDs 165 to 199 is not supported in the APIC GUI. To use one of these FEX IDs, configure the profile using the NX-OS style CLI. For more information, see Configuring FEX Connections Using Interface Profiles with the NX-OS Style CLI.
Before you begin

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
- The target leaf switches, interfaces, and protocol(s) are configured and available.
- The FEX is powered on and connected to the target leaf interfaces

Note

A maximum of eight members is supported in fabric port-channels connected to FEXs.

Procedure

Step 1

On the APIC, create a switch profile using the Fabric > External Access Policies > Quick Start Configure Interface, PC, And VPC wizard.

a) On the APIC menu bar, navigate to Fabric > Access Policies > Quick Start.

b) In the Quick Start page, click the Configure an interface, PC, and VPC option to open the Configure Interface, PC And VPC wizard.

c) In the Configure an interface, PC, and VPC work area, click the + to add a new switch profile.

d) In the Select Switches To Configure Interfaces work area, click the Advanced radio button.

e) Select the switch from the drop-down list of available switch IDs.

Troubleshooting Tips

In this procedure, one switch is included in the profile. Selecting multiple switches allows the same profile to be used on multiple switches.

f) Provide a name in the Switch Profile Name field.

g) Click the + above the Fexes list to add a FEX ID and the switch ports to which it will connect to the switch profile.

You must configure FEX IDs 165 - 199, using the NX-OS style CLI. See Configuring FEX Connections Using Interface Profiles with the NX-OS Style CLI.

h) Click Save to save the changes. Click Submit to submit the switch profile to the APIC.

The APIC auto-generates the necessary FEX profile (<switch policy name>_FexP<FEX ID>) and selector (<switch policy name>_ifselector).

Verification: Use the CLI show fex command on the switch where the FEX is attached to verify that the FEX is online.

Step 2

Customize the auto-generated FEX Profile to enable attaching a server to a single FEX port.

a) In the Navigation pane, locate the switch policy you just created in the policies list. You will also find the auto-generated FEX the <switch policy name>_FexP<FEX ID> profile.

b) In the work pane of the <switch policy name>_FexP<FEX ID> profile, click the + to add a new entry to the Interface Selectors For FEX list.

The Create Access Port Selector dialog opens.

c) Provide a name for the selector.
d) Specify the FEX interface IDs to use.
e) Select an existing *Interface Policy Group* from the list or *Create Access Port Policy Group*.

The access port policy group is a named policy that specifies the group of interface policies you will apply to the selected interfaces of the FEX. Examples of interface policies include Link Level Policy (for example, 1gbit port speed), Attach Entity Profile, Storm Control Interface Policy, and so forth.

**Note** Within the interface policy group, the *Attached Entity Profile* is required for enabling an EPG to use the interfaces specified in the FEX port selector.

f) Click **Submit** to submit the FEX profile to the APIC. The APIC updates the FEX profile.

**Verification:** Use the CLI `show int` command on the switch where the FEX is attached to verify that the FEX interface is configured accordingly.

This completes the basic FEX configuration steps.

---

**What to do next**

While this configuration enables hardware connectivity, no data traffic can flow without a valid application profile, EPG, and contract that is associated with this hardware configuration.

---

### Configuring FEX Port Channel Connections Using the GUI

The main steps are as follows:

1. Configure an FEX profile to use FEX ports to form a port channel.
2. Configure the port channel to enable attaching a server.

*Figure 23: FEX port channel*
This procedure provides the steps for attaching a server to the FEX port channel. The steps would be the same for attaching any device to an ACI attached FEX.

Before you begin

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
- The target leaf switch, interfaces, and protocol(s) are configured and available.
- The FEX is configured, powered on, and connected to the target leaf interfaces

Procedure

**Step 1**

On the APIC, add a port channel to a FEX profile.

a) On the APIC menu bar, navigate to **Fabric > External Access Policies > Interfaces > Leaf Interfaces > Profiles**.

b) In the **Navigation Pane**, select the FEX profile.

   APIC auto-generated FEX profile names are formed as follows: `<switch policy name>_FexP<FEX ID>`.

c) In the **FEX Profile** work area, click the `+` to add a new entry to the **Interface Selectors For FEX** list.

   The **Create Access Port Selector** dialog opens.

**Step 2**

Customize the **Create Access Port Selector** to enable attaching a server to the FEX port channel.

a) Provide a name for the selector.

b) Specify the FEX interface IDs to use.

c) Select an existing **Interface Policy Group** from the list or **Create PC Interface Policy Group**.

   The port channel interface policy group specifies the group of policies you will apply to the selected interfaces of the FEX. Examples of interface policies include Link Level Policy (for example, 1gbit port speed), Attach Entity Profile, Storm Control Interface Policy, and so forth.

   **Note** Within the interface policy group, the **Attached Entity Profile** is required for enabling an EPG to use the interfaces specified in the FEX port selector.

d) In the **Port Channel Policy** option, select static or dynamic LACP according to the requirements of your configuration.

e) Click **Submit** to submit the updated FEX profile to the APIC.

   The APIC updates the FEX profile.

**Verification**: Use the CLI **show port-channel summary** command on the switch where the FEX is attached to verify that the port channel is configured accordingly.
What to do next

This completes the FEX port channel configuration steps.

---

Note

While this configuration enables hardware connectivity, no data traffic can flow without a valid application profile, EPG, and contract that is associated with this hardware configuration.

---

Configuring FEX VPC Connections Using the GUI

The main steps are as follows:

1. Configure two existing FEX profiles to form a virtual port channel.

2. Configure the virtual port channel to enable attaching a server to the FEX port channel.

---

Before you begin

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.

- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.

- The target leaf switch, interfaces, and protocol(s) are configured and available.

- The FEXes are configured, powered on, and connected to the target leaf interfaces
When creating a VPC domain between two leaf switches, both switches must be in the same switch generation, one of the following:

- Generation 1 - Cisco Nexus N9K switches without “EX” on the end of the switch name; for example, N9K-9312TX
- Generation 2 – Cisco Nexus N9K switches with “EX” on the end of the switch model name; for example, N9K-93108TC-EX

Switches such as these two are not compatible VPC peers. Instead, use switches of the same generation.

### Procedure

#### Step 1
On the APIC, add a virtual port channel to two FEX profiles.

a) On the APIC menu bar, navigate to Fabric > External Access Policies > Interfaces > Leaf Interfaces > Profiles.

b) In the Navigation Pane, select the first FEX profile. APIC auto-generated FEX profile names are formed as follows: &lt;switch policy name&gt;_FexP&lt;FEX ID&gt;.

c) In the FEX Profile work area, click the + to add a new entry to the Interface Selectors For FEX list. The Create Access Port Selector dialog opens.

#### Step 2
Customize the Create Access Port Selector to enable attaching a server to the FEX virtual port channel.

a) Provide a name for the selector.

b) Specify the FEX interface ID to use. Typically, you will use the same interface ID on each FEX to form the virtual port channel.

c) Select an existing Interface Policy Group from the list or Create VPC Interface Policy Group.

The virtual port channel interface policy group specifies the group of policies you will apply to the selected interfaces of the FEX. Examples of interface policies include Link Level Policy (for example, 1gbit port speed), Attach Entity Profile, Storm Control Interface Policy, and so forth. The Attached Entity Profile is required for enabling an EPG to use the interfaces specified in the FEX port selector.

d) In the Port Channel Policy option, select static or dynamic LACP according to the requirements of your configuration.

e) Click Submit to submit the updated FEX profile to the APIC. The APIC updates the FEX profile.

**Verification:** Use the CLI show port-channel summary command on the switch where the FEX is attached to verify that the port channel is configured accordingly.

#### Step 3
Configure the second FEX to use the same Interface Policy Group just specified for the first FEX.

a) In the FEX Profile work area of the second FEX profile, click the + to add a new entry to the Interface Selectors For FEX list. The Create Access Port Selector dialog opens.

b) Provide a name for the selector.
c) Specify the FEX interface ID to use.
   Typically, you will use the same interface ID on each FEX to form the virtual port channel.

d) From the drop-down list, select the same virtual port channel Interface Policy Group just used in the first FEX profile.
   The virtual port channel interface policy group specifies the group of policies you will apply to the selected interfaces of the FEX. Examples of interface policies include Link Level Policy (for example, 1gbit port speed), Attach Entity Profile, Storm Control Interface Policy, and so forth.

   Note Within the interface policy group, the Attached Entity Profile is required for enabling an EPG to use the interfaces specified in the FEX port selector.

e) Click Submit to submit the updated FEX profile to the APIC.
   The APIC updates the FEX profile.

   Verification: Use the CLI show vpc extended command on the switch where one of the FEXes is attached to verify that the virtual port channel is configured accordingly.

What to do next
This completes the FEX virtual port channel configuration steps.

Note While this configuration enables hardware connectivity, no data traffic can flow without a valid application profile, EPG, and contract that is associated with this hardware configuration.

Configuring an FEX VPC Policy Using the REST API

This task creates a FEX virtual port channel (VPC) policy.

Before you begin
• The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
• An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
• The target leaf switch, interfaces, and protocol(s) are configured and available.
• The FEXes are configured, powered on, and connected to the target leaf interfaces
When creating a VPC domain between two leaf switches, both switches must be in the same switch generation, one of the following:

- **Generation 1** - Cisco Nexus N9K switches without “EX” on the end of the switch name; for example, N9K-9312TX
- **Generation 2** - Cisco Nexus N9K switches with “EX” on the end of the switch model name; for example, N9K-93108TC-EX

Switches such as these two are not compatible VPC peers. Instead, use switches of the same generation.

**Procedure**

To create the policy linking the FEX through a VPC to two switches, send a post with XML such as the following example:

**Example:**

```xml
<polUni>
  <infraInfra dn="uni/infra">
    <infraNodeP name="fexNodeP105">
      <infraLeafS name="leafs" type="range">
        <infraNodeBlk name="test" from_="105" to="105"/>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/accportprof-fex116nif105"/>
    </infraNodeP>
    <infraNodeP name="fexNodeP101">
      <infraLeafS name="leafs" type="range">
        <infraNodeBlk name="test" from_="101" to="101"/>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/accportprof-fex113nif101"/>
    </infraNodeP>
    <infraAccPortP name="fex116nif105">
      <infraHPortS name="pselc" type="range">
        <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="45" toPort="48" />
      </infraHPortS>
      <infraRsAccBaseGrp tDn="uni/infra/fexprof-fexHIF116/fexbundle-fex116" fexId="116"/>
    </infraAccPortP>
    <infraAccPortP name="fex113nif101">
      <infraHPortS name="pselc" type="range">
        <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="45" toPort="48" />
      </infraHPortS>
      <infraRsAccBaseGrp tDn="uni/infra/fexprof-fexHIF113/fexbundle-fex113" fexId="113"/>
    </infraAccPortP>
  </infraInfra>
</polUni>
```
Configuring an FEX VPC Policy Using the REST API

```xml
fromCard="1" toCard="1" fromPort="15" toPort="16" />
</infraPortBlk>
<infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-fexPCbundle" />
</infraPortS>
<infraPortS name="pselc-fexVPC" type="range">
  <infraPortBlk name="blk"
    fromCard="1" toCard="1" fromPort="17" toPort="18" >
    <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-fexPCbundle" />
  </infraPortBlk>
</infraHPortS>

<infraFexP name="fexHIF116">
  <infraFexBndlGrp name="fex116" />
  <infraHPortS name="pselc-fexVPC" type="range">
    <infraPortBlk name="blk"
      fromCard="1" toCard="1" fromPort="17" toPort="18" >
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-fexPCbundle" />
    </infraPortBlk>
  </infraHPortS>
  <infraHPortS name="pselc-fexaccess" type="range">
    <infraPortBlk name="blk"
      fromCard="1" toCard="1" fromPort="47" toPort="47" >
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-fexaccport" />
    </infraPortBlk>
  </infraHPortS>
</infraFexP>

<infraFexP name="fexHIF116">
  <infraFexBndlGrp name="fex116" />
  <infraHPortS name="pselc-fexVPC" type="range">
    <infraPortBlk name=" blk"
      fromCard="1" toCard="1" fromPort="17" toPort="18" >
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-fexPCbundle" />
    </infraPortBlk>
  </infraHPortS>
  <infraHPortS name="pselc-fexaccess" type="range">
    <infraPortBlk name=" blk"
      fromCard="1" toCard="1" fromPort="47" toPort="47" >
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-fexaccport" />
    </infraPortBlk>
  </infraHPortS>
</infraFexP>

<infraFuncP>
  <infraAccBndlGrp name="fexPCbundle" lagT="link">
    <infraRsLacpPol tnLacpLagPolName='staticLag'/>
    <infraRsHIfPol tnFabricHIfPolName="1GHIfPol" />
    <infraRsAttEntP tDn="uni/infra/attenp-fexvpcAttEP"/>
  </infraAccBndlGrp>
</infraFuncP>

<infraAccBndlGrp name="fexvpcbundle" lagT="node">
  <infraRsLacpPol tnLacpLagPolName='staticLag'/>
  <infraRsHIfPol tnFabricHIfPolName="1GHIfPol" />
  <infraRsAttEntP tDn="uni/infra/attenp-fexvpcAttEP"/>
</infraAccBndlGrp>
</infraFuncP>

<fabricHIfPol name="1GHIfPol" speed="1G" />
<infraAttEntityP name="fexvpcAttEP">
  <infraProvAcc name="provfunc"/>
  <infraRsDomP tDn="uni/phys-fexvpcDOM"/>
</infraAttEntityP>
```
Configuring FEX Connections Using Profiles with the NX-OS Style CLI

Use this procedure to configure FEX connections to leaf nodes using the NX-OS style CLI.

Note
Configuring FEX connections with FEX IDs 165 to 199 is not supported in the APIC GUI. To use one of these FEX IDs, configure the profile using the following commands.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>apic1# configure</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>leaf-interface-profile name</td>
<td>Specifies the leaf interface profile to be configured.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>apic1(config)# leaf-interface-profile fexIntProf1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>leaf-interface-group name</td>
<td>Specifies the interface group to be configured.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>apic1(config-leaf-if-profile)# leaf-interface-group leafIntGrp1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>fex associate fex-id [template template-type fex-template-name]</td>
<td>Attaches a FEX module to a leaf node. Use the optional template keyword to specify a template to be used. If it does not exist, the system creates a template with the name and type you specified.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>apic1(config-leaf-if-group)# fex associate 101</td>
<td></td>
</tr>
</tbody>
</table>

Example

This merged example configure a leaf interface profile for FEX connections with ID 101.

```
apic1# configure
apic1(config)# leaf-interface-profile fexIntProf1
apic1(config-leaf-if-profile)# leaf-interface-group leafIntGrp1
apic1(config-leaf-if-group)# fex associate 101
```
Configuring Port Profiles to Change Ports from Uplink to Downlink or Downlink to Uplink

Configuring Port Profiles

Prior to Cisco APIC, Release 3.1(1), conversion from uplink port to downlink port or downlink port to uplink port (in a port profile) was not supported on Cisco ACI leaf switches. Starting with Cisco APIC Release 3.1(1), uplink and downlink conversion is supported on Cisco Nexus 9000 series switches with names that end in EX or FX, and later (for example, N9K-C9348GC-FXP). A FEX connected to converted downlinks is also supported.

This functionality is supported on the following Cisco switches:

- N9K-C9348GC-FXP
- N9K-C93180LC-EX and N9K-C93180YC-FX
- N9K-93180YC-EX, N9K-C93180YC-EX, and N9K-C93180YC-EXU
- N9K-C93108TC-EX and N9K-C93108TC-FX
- N9K-C9336C-FX2 (only downlink to uplink conversion supported)

Restrictions

Fast Link Failover policies and port profiles are not supported on the same port. If port profile is enabled, Fast Link Failover cannot be enabled or vice versa.

The last 2 uplink ports of supported TOR switches cannot be converted to downlink ports (they are reserved for uplink connections.)

Up to Cisco APIC Release 3.2, port profiles and breakout ports are not supported on the same ports.

With Cisco APIC Release 3.2 and later, dynamic breakouts (both 100Gb and 40Gb) are supported on profiled QSFP ports on the N9K-C93180YC-FX switch. Breakout and port profile are supported together for conversion of uplink to downlink on ports 49-52. Breakout (both 10g-4x or 25g-4x options) is supported on downlink profiled ports.

Guidelines

In converting uplinks to downlinks and downlinks to uplinks, consider the following guidelines.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decommissioning nodes with port profiles</td>
<td>If a decommissioned node has the Port Profile feature deployed on it, the port conversions are not removed even after decommissioning the node. It is necessary to manually delete the configurations after decommission, for the ports to return to the default state. To do this, log onto the switch, run the <code>setup-clean-config.sh</code> script, and wait for it to run. Then, enter the <code>reload</code> command.</td>
</tr>
</tbody>
</table>
### FIPS

When you enable or disable Federal Information Processing Standards (FIPS) on a Cisco ACI fabric, you must reload each of the switches in the fabric for the change to take effect. The configured scale profile setting is lost when you issue the first reload after changing the FIPS configuration. The switch remains operational, but it uses the default scale profile. This issue does not happen on subsequent reloads if the FIPS configuration has not changed.

FIPS is supported on Cisco NX-OS release 13.1(1) or later.

If you must downgrade the firmware from a release that supports FIPS to a release that does not support FIPS, you must first disable FIPS on the Cisco ACI fabric and reload all the switches in the fabric for the FIPS configuration change.

### Maximum uplink port limit

When the maximum uplink port limit is reached and ports 25 and 27 are converted from uplink to downlink and back to uplink on Cisco 93180LC-EX switches:

On Cisco 93180LC-EX Switches, ports 25 and 27 are the native uplink ports. Using the port profile, if you convert port 25 and 27 to downlink ports, ports 29, 30, 31, and 32 are still available as four native uplink ports. Because of the threshold on the number of ports (which is maximum of 12 ports) that can be converted, you can convert 8 more downlink ports to uplink ports. For example, ports 1, 3, 5, 7, 9, 13, 15, 17 are converted to uplink ports and ports 29, 30, 31 and 32 are the 4 native uplink ports (the maximum uplink port limit on Cisco 93180LC-EX switches).

When the switch is in this state and if the port profile configuration is deleted on ports 25 and 27, ports 25 and 27 are converted back to uplink ports, but there are already 12 uplink ports on the switch (as mentioned earlier). To accommodate ports 25 and 27 as uplink ports, 2 random ports from the port range 1, 3, 5, 7, 9, 13, 15, 17 are denied the uplink conversion and this situation cannot be controlled by the user.

Therefore, it is mandatory to clear all the faults before reloading the leaf node to avoid any unexpected behavior regarding the port type. It should be noted that if a node is reloaded without clearing the port profile faults, especially when there is a fault related to limit-exceed, the port might not be in an expected operational state.

### Breakout Limitations

<table>
<thead>
<tr>
<th>Switch</th>
<th>Releases</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>N9K-C9332PQ</td>
<td>Cisco APIC 2.2 (1n) and higher</td>
<td>• 40Gb dynamic breakouts into 4X10Gb ports are supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ports 13 and 14 do not support breakouts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Port profiles and breakouts are not supported on the same port.</td>
</tr>
</tbody>
</table>
### Limitations

- 40G and 100Gb dynamic breakouts are supported on ports 1 through 24 on odd numbered ports.
- When the top ports (odd ports) are broken out, then the bottom ports (even ports) are error disabled.
- Port profiles and breakouts are not supported on the same port.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Releases</th>
<th>Limitations</th>
</tr>
</thead>
</table>
| N9K-C93180LC-EX         | Cisco APIC 3.1(1i) and higher | • 40G and 100Gb dynamic breakouts are supported on ports 1 through 24 on odd numbered ports.  
|                         |                           | • When the top ports (odd ports) are broken out, then the bottom ports (even ports) are error disabled.  
|                         |                           | • Port profiles and breakouts are not supported on the same port.           |
| N9K-C9336C-FX2          | Cisco APIC 3.1(2m) and higher | • 40G and 100Gb dynamic breakouts are supported on ports 1 through 30.  
|                         |                           | • Port profiles and breakouts are not supported on the same port.           |
| N9K-C93180YC-FX         | Cisco APIC Release 3.2(1x) and higher | • 40G and 100Gb dynamic breakouts are supported on ports 49 through 52, when they are on profiled QSFP ports. To use them for dynamic breakout, perform the following steps:  
|                         |                           | • Convert ports 49-52 to front panel ports (downlinks).  
|                         |                           | • Perform a port-profile reload, using one of the following methods:  
|                         |                           | • In the APIC GUI, navigate to Fabric > Inventory > Pod > Leaf, right-click Chassis and choose Reload.  
|                         |                           | • In the NX-OS style CLI, enter the setup-clean-config.sh -k script, wait for it to run, and then enter the reload command.  
|                         |                           | • Apply breakouts on the profiled ports 49-52.  
|                         |                           | • Ports 53 and 54 do not support either port profiles or breakouts. |

### Port Profile Configuration Summary

The following table summarizes supported uplinks and downlinks for the switches that support port profile conversions from Uplink to Downlink and Downlink to Uplink.
<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Default Links</th>
<th>Max Uplinks (Fabric Ports)</th>
<th>Max Downlinks (Server Ports)</th>
<th>Release Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>N9K-C9348GC-FXP</td>
<td>48 x 100M/1G BASE-T downlinks 4 x 10/25-Gbps SFP28 uplinks 2 x 40/100-Gbps QSFP28 uplinks</td>
<td>48 x 100M/1G BASE-T downlinks 4 x 10/25-Gbps SFP28 uplinks 2 x 40/100-Gbps QSFP28 uplinks</td>
<td>Same as default</td>
<td>3.1(1i)</td>
</tr>
<tr>
<td>N9K-C93180LC-EX</td>
<td>24 x 40-Gbps QSFP 28 downlinks 6 x 40/100-Gbps QSFP 28 uplinks Or 12 x 100-Gbps QSFP 28 downlinks 6 x 40/100-Gbps QSFP 28 uplinks</td>
<td>12 x 40-Gbps QSFP 28 downlinks 12 x 40/100-Gbps QSFP 28 uplinks Or 6 x 100-Gbps QSFP 28 downlinks 12 x 40/100-Gbps QSFP 28 uplinks</td>
<td>4 x 40-Gbps QSFP 28 downlinks 2 x 40/100-Gbps QSFP 28 downlinks Or 4 x 40/100-Gbps uplinks</td>
<td>3.1(1i)</td>
</tr>
<tr>
<td>N9K-C93180YC-EX</td>
<td>48 x 10/25-Gbps fiber downlinks 6 x 40/100-Gbps QSFP28 uplinks</td>
<td>48 x 10/25-Gbps fiber downlinks 6 x 40/100-Gbps QSFP28 uplinks</td>
<td>48 x 10/25-Gbps fiber downlinks 4 x 40/100-Gbps QSFP28 downlinks 2 x 40/100-Gbps QSFP28 uplinks</td>
<td>3.1(1i)</td>
</tr>
<tr>
<td>N9K-C9336C-FX2</td>
<td>30 x 40/100-Gbps QSFP28 downlinks 6 x 40/100-Gbps QSFP28 uplinks</td>
<td>18 x 40/100-Gbps QSFP28 downlinks 18 x 40/100-Gbps QSFP28 uplinks</td>
<td>Same as default</td>
<td>3.1(2m)</td>
</tr>
</tbody>
</table>
Configuring a Port Profile Using the GUI

This procedure explains how to configure a port profile, which determines the port type: uplink or downlink.

Before you begin

• The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
• An APIC fabric administrator account is available that will enable creating or modifying the necessary fabric infrastructure configurations.
• The target leaf switches are registered in the ACI fabric and available.

Procedure

Step 1 From the Fabric menu, select Inventory.
Step 2 In the left navigation pane of the Inventory screen, select Topology.
Step 3 Under Topology tab, select the Interface tab in the right navigation pane.
Step 4 Select the mode as Configuration.
Step 5 Add a leaf switch by clicking on the + icon (Add Switches) in the table menu.
Step 6 In the Add Switches table, select the Switch ID and click Add Selected.

When you select the port, the available option is highlighted.

Step 7 Select the ports and choose the new port type as Uplink or Downlink.

The last two ports are reserved for uplink. These cannot be converted to downlink ports.

Step 8 After clicking uplink or downlink, click Submit (reload the switch on your own later) or Submit and Reload Switch.

Note Reload the switch for the change in the uplink or downlink configuration to take effect.

Configuring a Port Profile Using the NX-OS Style CLI

To configure a port profile using the NX-OS style CLI, perform the following steps:

Before you begin

• The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
• An APIC fabric administrator account is available that will enable creating or modifying the necessary fabric infrastructure configurations.
• The target leaf switches are registered in the ACI fabric and available.
Procedure

**Step 1**
**configure**

Enters global configuration mode.

**Example:**
```
apic1# configure
```

**Step 2**
**leaf node-id**

Specifies the leaf or leaf switches to be configured.

**Example:**
```
apic1(config)# leaf 102
```

**Step 3**
**interface type**

Specifies the interface that you are configuring. You can specify the interface type and identity. For an Ethernet port, use ethernet slot/port.

**Example:**
```
apic1(config-leaf)# interface ethernet 1/2
```

**Step 4**
**port-direction {uplink | downlink}**

Determines the port direction or changes it. This example configures the port to be a downlink.

**Note**
On the N9K-C9336C-FX switch, changing a port from uplink to downlink is not supported.

**Example:**
```
apic1(config-leaf-if)# port-direction downlink
```

**Step 5**

Log on to the leaf switch where the port is located and enter the `setup-clean-config.sh -k` command, then the `reload` command.

---

**Configuring a Port Profile Using the REST API**

**Before you begin**

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
- An APIC fabric administrator account is available that will enable creating or modifying the necessary fabric infrastructure configurations.
- The target leaf switches are registered in the ACI fabric and available.

**Procedure**

**Step 1**

To create a port profile that converts a downlink to an uplink, send a post with XML such as the following:
Verifying Port Profile Configuration and Conversion Using the NX-OS Style CLI

You can verify the configuration and the conversion of the ports using the `show interface brief` CLI command.

**Note**
Port profile can be deployed only on the top ports of a Cisco N9K-C93180LC-EX switch, for example, 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, and 23. When the top port is converted using the port profile, the bottom ports are hardware disabled. For example, if Eth 1/1 is converted using the port profile, Eth 1/2 is hardware disabled.

**Procedure**

**Step 1**
This example displays the output for converting an uplink port to downlink port. Before converting an uplink port to downlink port, the output is displayed in the example. The keyword `routed` denotes the port as uplink port.

**Example:**

```
switch# show interface brief
<snip>
Eth1/49 -- eth routed down sfp-missing 100G(D) --
Eth1/50 -- eth routed down sfp-missing 100G(D) --
<snip>
```

**Step 2**
After configuring the port profile and reloading the switch, the output is displayed in the example. The keyword `trunk` denotes the port as downlink port.

**Example:**

```
switch# show interface brief
<snip>
Eth1/49 0 eth trunk down sfp-missing 100G(D) --
Eth1/50 0 eth trunk down sfp-missing 100G(D) --
<snip>
```
FCoE Connections

This chapter contains the following sections:
- Supporting Fibre Channel over Ethernet Traffic on the ACI Fabric, on page 121
- Configuring FCoE Using the Advanced GUI, on page 124
- Configuring FCoE Using the NX_OS Style CLI, on page 140
- Configuring FCoE Using the REST API, on page 151

Supporting Fibre Channel over Ethernet Traffic on the ACI Fabric

ACI enables you to configure and manage support for Fibre Channel over Ethernet (FCoE) traffic on the ACI fabric.

FCoE is a protocol that encapsulates Fibre Channel (FC) packets within Ethernet packets, thus enabling storage traffic to move seamlessly from a Fibre Channel SAN to an Ethernet network.

A typical implementation of FCoE protocol support on the ACI fabric enables hosts located on the Ethernet-based ACI fabric to communicate with SAN storage devices located on an FC network. The hosts are connecting through virtual F ports deployed on an ACI leaf switch. The SAN storage devices and FC network are connected through an FCF bridge to the ACI fabric through a virtual NP port, deployed on the same ACI leaf switch as is the virtual F port. Virtual NP ports and virtual F ports are also referred to generically as virtual Fibre Channel (vFC) ports.
As of release version 2.0(1), FCoE support is limited to N9K-C93180YC-EX and N9K-C93108TC-EX hardware. With release version 2.2(1), the N9K-C93180LC-EX 40 Gigabit Ethernet (GE) ports can be used as F or NP ports. However, if they are enabled for FCoE, they cannot be enabled for 40GE port breakout. FCoE is not supported on breakout ports.

From release version 2.2(2), N9K-C93180YC-FX and N9K-C93108TC-FX hardware supports FCoE. With release 2.3(1), FCoE support on Fex ports for the hardware N9K-C93180YC-FX and N9K-C93108TC-FX is available.

As of release version 2.2(x), FCoE is also supported on the following FEX Nexus devices:

- N2K-C2348UPQ-10GE
- N2K-C2348TQ-10GE
- N2K-C2232PP-10GE
- N2K-B22DELL-P
- N2K-B22HP-P
- N2K-B22IBM-P
- N2K-B22DELL-P-FI

Note

The vlan used for FCoE should have vlanScope set to Global. vlanScope set to portLocal is not supported for FCoE. The value is set via the L2 Interface Policy l2IfPol.

Topology Supporting FCoE Traffic Through ACI

The topology of a typical configuration supporting FCoE traffic over the ACI fabric consists of the following components:
One or more ACI leaf switches configured through FC SAN policies to function as an NPV backbone.

Selected interfaces on the NPV-configured leaf switches configured to function as F ports. F ports accommodate FCoE traffic to and from hosts running SAN management or SAN-consuming applications.

Selected interfaces on the NPV-configured leaf switches to function as NP ports. NP ports accommodate FCoE traffic to and from an FCF bridge.

The FCF bridge receives FC traffic from fibre channel links typically connecting SAN storage devices and encapsulates the FC packets into FCoE frames for transmission over the ACI fabric to the SAN management or SAN Data-consuming hosts. It receives FCoE traffic and repackages it back to FC for transmission over the fibre channel network.
In the above ACI topology, FCoE traffic support requires direct connections between the hosts and F ports and direct connections between the FCF device and NP port.

APIC servers enable an operator to configure and monitor the FCoE traffic through the APIC GUI, the APIC NX-OS style CLI, or through application calls to the APIC REST API.

**Topology Supporting FCoE Initialization**
In order for FCoE traffic flow to take place as described, you'll also need to set up separate VLAN connectivity over which SAN Hosts broadcast FCoE Initialization protocol (FIP) packets to discover the interfaces enabled as F ports.

**vFC Interface Configuration Rules**
Whether you set up the vFC network and EPG deployment through the APIC GUI, NX-OS style CLI, or the REST API, the following general rules apply across platforms:

- F port mode is the default mode for vFC ports. NP port mode must be specifically configured in the Interface policies.
- The load balancing default mode is for leaf-switch or interface level vFC configuration is src-dst-ox-id.
- One VSAN assignment per bridge domain is supported.
- The allocation mode for VSAN pools and VLAN pools must always be static.
- vFC ports require association with a VSAN domain (also called Fibre Channel domain) that contains VSANS mapped to VLANS.

## Configuring FCoE Using the Advanced GUI

### FCoE GUI Configuration

#### FCoE Policy, Profile, and Domain Configurations
You can use the APIC GUI under the Fabric Access Policies tab to configure policies, policy groups, and profiles to enable customized and scaled-out deployment and assignment of FCoE supporting F and NP ports on your ACI leaf switches. Then, under the APIC the Tenant tab, you can configure EPG access to those ports.

#### Policies and Policy Groups
APIC policies and policy groups you create or configure for FCoE support include the following:

**Access Switch Policy Group**
The combination of switch-level policies that support FCoE traffic through ACI leaf switches.
You can associate this policy group with a leaf profile to enable FCoE support on designated ACI leaf switches.
This policy group consists of the following policies:

- **Fiber Channel SAN Policy**
  Specifies the EDTOV, RATOV, and MAC Address prefix (also called the FC map) values used by the NPV leaf.

- **Fiber Channel Node Policy**
  Specifies the load balance options and FIP keep alive intervals that apply to FCoE traffic associated with this switch policy group.

**Interface Policy Groups**

The combination of interface-level policies that support FCoE traffic through interfaces on ACI leaf switches.

You can associate this policy group with an FCoE supportive interface profile to enable FCoE support on designated interfaces.

You configure two interface policy groups: One policy group for F ports, and one policy group for NP ports.

The following policies in the interface policy group apply to FCoE enablement and traffic:

- **Priority Flow Control Policy**
  Specifies the state of priority flow control (PFC) on the interfaces to which this policy group is applied.
  This policy specifies under what circumstances QoS-level priority flow control will be applied to FCoE traffic.

- **Fiber Channel Interface Policy**
  Specifies whether the interfaces to which this policy group is applied are to be configured as F ports or NP ports.

- **Slow Drain Policy**
  Specifies the policy for handling FCoE packets that are causing traffic congestion on the ACI Fabric.

**Global Policies**

The APIC global policies whose settings can affect the performance characteristics of FCoE traffic on the ACI fabric.

The Global **QoS Class Policies** for **Level1**, **Level2**, or **Level3** connections, contain the following settings that affect FCoE traffic on the ACI fabric:

- **PFC Admin State must be set to Auto**
  Specifies whether to enable priority flow control to this level of FCoE traffic (default value is false).

- **No Drop COS**
  Specifies whether to enable a no-drop policy for this level of FCoE traffic designated with a certain Class of Service (CoS) level.

  **Note:** QoS level enabled for PFC and FCoE no-drop must match with the Priority Group ID enabled for PFC on CNA.
Note: Only one QoS level can be enabled for no-drop and PFC, and the same QoS level must be associated with FCoE EPGs.

- QoS Class—Priority flow control requires that CoS levels be globally enabled for the fabric and assigned to the profiles of applications that generate FCoE traffic.
  
  CoS Preservation must also be enabled—Navigate to Fabric > Access Policies > Global Policies > QoS Class and enable Preserve COS Dot1p Preserve.

Note: Some legacy CNAs may require the Level2 Global QoS Policy to be used as the No Drop PFC, FCoE (Fibre Channel over Ethernet) QoS Policy. If your Converged Network Adapters (CNAs) are not logging into the fabric, and you have noticed that no FCoE Initiation Protocol (FIP) frames are being sent by the CNAs, try enabling Level2 as the FCoE QoS policy. The Level2 policy must be attached to the FCoE EPGs in use and only 1 QoS level can be enabled for PFC no-drop.

Profiles

APIC profiles that you can create or configure for FCoE support include the following:

Leaf Profile

- Specifies the ACI Fabric leaf switches on which to configure support of FCoE traffic.
- The combination of policies contained in the access switch policy group can be applied to the leaf switches included in this profile.

Interface Profiles

- Specifies a set of interfaces on which to deploy F Ports or NP Ports.
- You configure at least two leaf interface profiles: One interface profile for F ports, and one interface profile for NP ports.
- The combination of policies contained in the interface policy group for F ports can be applied to the set of interfaces included in the interface profile for F ports.
- The combination of policies contained in the interface policy group for NP ports can be applied to the set of interfaces included in the interface profile for NP ports.

Attached Entity Profile

- Binds the interface policy group settings with the Fibre Channel domain mapping.

Domains

Domains that you create or configure for FCoE support include the following:

Physical Domain

- A virtual domain created to support LANs for FCoE VLAN Discovery. The Physical domain will specify the VLAN pool to support FCoE VLAN discovery.

Fiber Channel Domain

- A virtual domain created to support virtual SANs for FCoE connections.
A Fibre Channel domain specifies a VSAN pool, VLAN pool and the VSAN Attribute over which the FCoE traffic is carried.

- **VSAN pool** - a set of virtual SANs which you associate with existing VLANs. Individual VSANs can be assigned to associated FCoE-enabled interfaces in the same way that VLANs can be assigned to those interfaces for Ethernet connectivity.

- **VLAN pool** - the set of VLANs available to be associated with individual VSANs.

- **VSAN Attribute** - The mapping of a VSAN to a VLAN.

**Tenant Entities**

Under the Tenant tab, you configure bridge domain and EPG entities to access the FCoE ports and exchange the FCoE traffic.

The entities include the following:

- **Bridge Domain (configured for FCoE support)**
  
  A bridge domain created and configured under a tenant to carry FCoE traffic for applications that use FCoE connections.

- **Application EPG**
  
  The EPG under the same tenant to be associated with the FCoE bridge domain.

- **Fiber Channel Path**
  
  Specifies the interfaces enabled as FCoE F ports or NP ports to be associated with the selected EPG. After you associate the Fibre Channel path with an EPG the FCoE interface is deployed in the specified VSAN.

**Deploying FCoE vFC Ports Using the APIC GUI**

The APIC GUI enables you to create customized node policy groups, leaf profiles, interface policy groups, interface profiles, and virtual SAN domains that system administrators can re-use to ensure that all interfaces they designate as F ports or NP ports to handle FCoE traffic have consistent FCoE-related policies applied.

**Before you begin**

- The ACI fabric is installed.

- If you deploy over a port channel (PC) topology, the port channel is set up as described in ACI Leaf Switch Port Channel Configuration Using the GUI, on page 77.

- If you deploy over a virtual port channel (VPC) topology, the VPC is set up as described in ACI Leaf Switch Virtual Port Channel Configuration Using the GUI, on page 89.

- Deployment of NP Port over a VPC-PO is NOT supported.

**Procedure**

**Step 1**

Create an FCoE supportive switch policy group to specify and combine all the leaf switch policies that support FCoE configuration.
This policy group will be applied to the leaf switches that you want to serve as NPV hosts.

a) In the APIC GUI, starting on the APIC menu bar, click **Fabric > External Access Policies > Switches > Leaf Switches > Policy Groups**.

b) Right-click **Policy Groups** and click **Create Access Switch Policy Group**.

c) In the **Create Access Switch Policy Group** dialog, specify the settings described below and then click **Submit**.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifies the switch policy group. Enter a name that indicates the FCoE supportive function of this switch policy group. For example, <strong>fcoe_switch_policy_grp</strong>.</td>
</tr>
<tr>
<td>Fiber Channel SAN Policy</td>
<td>Specifies the following SAN Policy values:</td>
</tr>
<tr>
<td></td>
<td>• FC Protocol EDTOV (default: 2000)</td>
</tr>
<tr>
<td></td>
<td>• FC Protocol RATOV (default: 10000)</td>
</tr>
<tr>
<td></td>
<td>• MAC address prefix (also called FC map) used by the leaf switch. This value should match the value of the peer device connected on the same port. Typically the default value OE:FC:00 is used.</td>
</tr>
<tr>
<td></td>
<td>Click the drop-down option box.</td>
</tr>
<tr>
<td></td>
<td>• To use the default EDTOV, RATOV, and MAC address prefix values, click <strong>default</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To use the value specified in an existing policy, click that policy.</td>
</tr>
<tr>
<td></td>
<td>• To create a new policy to specify a new customized MAC address prefix, click <strong>Create Fiber Channel SAN Policy</strong> and follow the prompts.</td>
</tr>
</tbody>
</table>

**Step 2**  
Create a leaf profile for leaf switches to support FCoE traffic.

This profile specifies a switch or set of leaf switches to assign the switch policy group that was configured in the previous step. This association enables that set of switches to support FCoE traffic with pre-defined policy settings.

a) Starting at the APIC menu bar, click **Fabric > External Access Policies > Switches > Leaf Switches > Profiles**

b) Right-click **Leaf Profiles**, then click **Create Leaf Profile**.

c) In the **Create Leaf Profile** dialog create and name the leaf profile (for example: NPV-1)

d) Also in the **Create Leaf Profile** dialog, locate the **Leaf Selectors** table, click + to create a new table row and specify the leaf switches to serve as NPV devices.

e) In the new table row choose a leaf name, blocks, and assign the switch policy group that you created in the previous step.

f) Click **Next** and then click **Finish**.

**Step 3**  
Create at least two FCoE-supportive interface policy groups: one to combine all policies that support FCoE F port interfaces, and one to combine all policies that support FCoE NP port interfaces.

These interface policy groups are to be applied to the interface profiles that are applied to interfaces that are to serve as F ports and NP ports.
a) On the APIC menu bar, click **Fabric > External Access Policies > Interfaces > Leaf Interfaces > Policy Groups.**

b) Right-click **Policy Groups**, then, depending on how port access is configured, click one of the following options: **Create Leaf Access Port Policy Group**, **Create PC Interface Port Policy Group**, or **Create VPC Interface Port Policy Group**.

**Note**
- If you deploy over a PC interface, view **ACI Leaf Switch Port Channel Configuration Using the GUI**, on page 77 for additional information.
- If you deploy over a VPC interface, view **ACI Leaf Switch Virtual Port Channel Configuration Using the GUI**, on page 89 for additional information.

c) In the policy group dialog, specify for inclusion the Fibre Channel Interface policy, the slow drain policy, and the priority flow control policy you configure.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of this policy group. Enter a name that indicates the FCoE supportive function of this Leaf Access Port Policy Group and the port type, (F or NP) that it is intended to support, for example: fcoe_f_port_policy or fcoe_np_port_policy.</td>
</tr>
</tbody>
</table>
| Priority Flow Control Policy | Specifies the state of the Priority Flow Control (PFC) on the interfaces to which this policy group is applied. Options include the following:  
  - **Auto** (the default value) Enables priority flow control (PFC) on local port on the no-drop CoS as configured, on the condition that values advertised by the DCBX and negotiated with the peer succeed. Failure causes priority flow control to be disabled on the no-drop CoS.  
  - **Off** disables FCoE priority flow control on the local port under all circumstances.  
  - **On** enables FCoE PFC on the local port under all circumstances.  
  Click the drop-down option box:  
    - To use the default values, click **default**.  
    - To use the value specified in an existing policy, click that policy.  
    - To create a new policy specifying different values, click **Create Priority Flow Control Policy** and follow the prompts.  
  **Note** PFC requires that Class of Service (CoS) levels be globally enabled for the fabric and assigned to the profiles of applications that generate FCoE traffic. Also CoS Preservation must be enabled. To enable it, navigate to **Fabric > External Access Policies > Policies > Global > QoS Class and enable Preserve COS Dot1p Preserve.** |
| Slow Drain Policy       | Specifies how to handle FCoE packets that are causing traffic congestion on the ACI fabric. Options include the following:  
  - Congestion Clear Action (default: disabled) |
**Policy** | **Description**
---|---
| | Action to be taken during FCoE traffic congestion. Options include:
| | • Err - disable - Disable the port.
| | • Log - Record congestion in the Event Log.
| | • Disabled- Take no action.
| | • Congestion Detect Multiplier (default: 10)
The number of pause frames received on a port that triggers a congestion clear action to address FCoE traffic congestion.
| | • Flush Admin State
| | • Enabled - Flush the buffer.
| | • Disabled - Don't flush the buffer.
| | • Flush Timeout (default: 500 milliseconds)
Threshold in milliseconds to trigger buffer flush drop during congestion.
| | • To use the default values, click **default**.
| | • To use the value specified in an existing policy, click that policy.
| | • To create a new policy specifying different values, click **Create Slow Drain Policy** and follow the prompts.

### Step 4
Create at least two interface profiles: one profile to support F port connections, one profile to support NP port connections, and optional additional profiles to be associated with additional port policy variations.

a) Starting at the APIC bar menu click **Fabric > External Access Policies > Interfaces > Leaf Interfaces > Profiles**.
b) Right-click **Profiles** and choose **Create Leaf Interface Profile**.
c) In the **Create Leaf Interface Profile** dialog, enter a descriptive name for the profile, for example, **FCoE F port Interface profile-1**.
d) Locate the Interface **Selectors** table and click + to display the **Create Access Port Selector** dialog. This dialog enables you to display a range of interfaces and apply settings to the fields described in the following table.

<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive name for this range.</td>
</tr>
<tr>
<td>Interface IDs</td>
<td>Specifies the set of interfaces to which this range applies.</td>
</tr>
<tr>
<td></td>
<td>• To include all interfaces in the switch, choose <strong>All</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To include an individual interface in this range, specify single Interface ID, for example: <strong>1/20</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To include a range of interfaces in this range, enter the lower and upper values separated by a dash, for example: <strong>1/10 – 1/15</strong>.</td>
</tr>
</tbody>
</table>
### Description

Specify separate, non-overlapping ranges of interfaces when configuring interface profiles for F ports and an NP port.

### Interface Policy Group

The name of either the F port interface policy group or the NP port policy group that you configured in the previous step.

- To designate the interfaces included in this profile as F ports, choose the interface policy group that you configured for F ports.
- To designate the interfaces included in the profile as NP ports, choose the interface policy group that you configured for NP ports.

### Step 5

Click **Submit**. Repeat the previous step so that you at least have interface profiles for both F ports and an NP port.

### Step 6

Configure whether to apply global QoS policies to FCoE traffic.

You can specify different QoS policies to different levels (1, 2, or 3) of FCoE traffic.

a) Starting at the APIC bar menu click **Fabric > External Access Policies > Policies > Global > QoS Class Policies** and enable the **Preserve CoS** flag in the **QoS Class Policies** pane.

b) In the **QoS Class Policy - Level 1**, **QoS Class Policy - Level 2**, or **QoS Class Policy - Level 3** dialog, edit the following fields to specify the PFC and no-drop CoS. Then click **Submit**.

**Note**: Only 1 Level can be configured for PFC and no-drop CoS.

### Policy

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFC Admin State</td>
<td>Whether to enable priority flow control to this level of FCoE traffic (default value is false).</td>
</tr>
<tr>
<td></td>
<td>Enabling priority flow control sets the <strong>Congestion Algorithm</strong> for this level of FCoE traffic to <strong>no-drop</strong>.</td>
</tr>
<tr>
<td>CoS</td>
<td>The CoS level to impose no drop FCoE packet handling even in case of FCoE traffic congestion</td>
</tr>
</tbody>
</table>

### Step 7

Define a Fibre Channel domain. Create a set of virtual SANs (VSANs) and map them to set of existing VLANs.

a) Starting at the APIC bar menu click **Fabric > External Access Policies > Physical and External Domains > Fiber Channel Domains**.

b) Right-click **Fiber Channel Domains** and click **Create Fiber Channel Domain**.

c) In the **Fiber Channel Domain** dialog, specify the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name or label you want to assign the VSAN domain you are creating. (For example: vsan-dom2)</td>
</tr>
<tr>
<td>VSAN Pool</td>
<td>The pool of VSANs assigned to this domain.</td>
</tr>
<tr>
<td></td>
<td>• To select an existing VSAN pool, click the drop-down and choose a listed pool. If you want to revise it, click the Edit icon.</td>
</tr>
<tr>
<td>Option</td>
<td>Description/Action</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Create a VSAN Pool | To create a VSAN pool, click **Create a VSAN Pool**. If you open the dialog to create a VSAN pool, follow the prompts configure the following:  
  • A Static resource allocation method to support FCoE.  
  • A range of VSANs that will be available to assign to FCoE F port interfaces and NP port interfaces.  
  **Note** Minimum range value is 1. Maximum range value is 4078. Configure multiple ranges of VSANs if necessary. |
| VLAN Pool    | The pool of VLANs available to be mapped to by the members of the VSAN pool. A VLAN pool specifies numerical ranges of VLANs you want available to support FCoE connections for this domain. The VLANs in the ranges you specify are available for VSANs to map to them.  
  • To select an existing VLAN pool, click the drop-down and choose a listed pool. If you want to revise it, click the Edit icon.  
  • To create a VLAN pool, click **Create a VLAN Pool**. If you open the dialog to create a VLAN pool, follow the prompts configure the following:  
  • A Static resource allocation method to support FCoE.  
  • A range of VLANs that will be available for VSANs to map to.  
  **Note** Minimum range value is 1. Maximum range value is 4094. Configure multiple ranges of VLANs if necessary. |
| VSAN Attr    | The VSAN Attributes map for this domain  
  The VSAN Attributes map VSANs in the VSAN pool to VLANs in the VLAN pool.  
  • To select an existing VSAN Attributes map, click the drop-down and choose a listed map. If you want to revise it, click the Edit icon.  
  • To create a VSAN Attributes map, click **Create VSAN Attributes**. If you open the dialog to configure the VSAN attributes, follow the prompts configure the following:  
  • The appropriate load balancing option (src-dst-ox-id or src-dst-id).  
  • Mapping of individual VSANs to individual VLANs, for example: vsan-8 to vlan-10  
  **Note** Only VSANs and VLANs in the ranges you specified for this domain can be mapped to each other. |

**Step 8** Create an attached entity profile to bind the Fibre Channel domain with your policy group.
a) On the APIC menu bar, click **Fabric > External Access Policies > Interfaces > Leaf Interfaces > Policy Groups > interface_policy_group_name**.

In this step `interface_policy_group_name` is the interface policy group that you defined in Step 2.

b) In the interface policy group dialog, Click the Attached Entity Profile drop-down and choose an existing Attached Entity Profile or click **Create Attached Entity Profile** to create a new one.

c) In the Attached Entity Profile dialog specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for this Attached Entity Profile</td>
</tr>
<tr>
<td>Domains To Be Associated To Interfaces</td>
<td>Lists the domain to be associated with the interface policy group. In this case, choose the Fibre Channel domain you configured in Step 8.</td>
</tr>
</tbody>
</table>

**Step 9**

Associate the leaf profile and the F port and NP port interface profiles.

a) Starting at the APIC menu bar, click **Fabric > External Access Policies > Switches > Leaf Switches > Profiles** then click the name of the leaf profile you configured in Step 2.

b) In the **Create Leaf Profile** dialog, locate the **Associated Interface Selector Profiles** table, click + to create a new table row and choose the F port interface profile you created in Step 5.

c) Again on the **Associated Interface Selector Profiles** table, click + to create a new table row and choose the NP port interface profile you created in Step 5.

d) Click **Submit**.

**What to do next**

After successful deployment of virtual F ports and NP ports to interfaces on the ACI fabric, the next step is for system administrators to enable EPG access and connection over those interfaces.

For more information, see **Deploying EPG Access to vFC Ports Using the APIC GUI**, on page 133.

**Deploying EPG Access to vFC Ports Using the APIC GUI**

After you have configured ACI fabric entities to support FCoE traffic and F port and NP port functioning of designated interfaces, your next step is to configure EPG access to those ports.

**Before you begin**

- The ACI fabric is installed.
- A Fibre Channel Forwarding (FCF) switch with a Fibre Channel FC connection to a FC network (for example SAN storage, is physically attached by Ethernet to an ACI leaf switch port).
- A host application that needs to access the FC network is physically attached by Ethernet to a port on the same ACI leaf switch.
- Leaf policy groups, leaf profiles, interface policy groups, interface profiles, and Fibre Channel domains have all been configured to support FCoE traffic.
### Procedure

**Step 1** Under an appropriate tenant configure an existing bridge domain to support FCoE or create a bridge domain to support FCoE.

<table>
<thead>
<tr>
<th>Option:</th>
<th>Actions</th>
</tr>
</thead>
</table>
| To configure an existing bridge domain for FCoE | 1. Click Tenant > tenant_name > Networking > Bridge Domains > bridge_domain_name.  
2. In the Type field of the bridge domain’s Properties panel, click fc.  
3. Click Submit. |
| To create a new bridge domain for FCoE | 1. Click Tenant > tenant_name > Networking > Bridge Domains > Actions > Create a Bridge Domain.  
2. In the Name field of the Specify Bridge Domain for the VRF dialog, enter a bridge domain name.  
3. In the Type field of Specify Bridge Domain for the VRF dialog, click fc.  
4. In VRF field select a VRF from the drop-down or click Create VRF to create and configure a new VRF.  
5. Finish the bridge domain configuration.  
6. Click Submit. |

**Step 2** Under the same tenant, configure an existing EPG or create a new EPG to associate with the FCoE-configured bridge domain.

<table>
<thead>
<tr>
<th>Option:</th>
<th>Actions</th>
</tr>
</thead>
</table>
| To associate an existing EPG | 1. Click Tenant > tenant_name > Application Profiles > ap1 > Application EPGs > epg_name.  
2. In the QoS class field choose the quality of service (Level1, Level2, or Level3) to assign to traffic generated by this EPG.  
If you configured one of the QoS levels for priority-flow control no-drop congestion handling and you want FCoE traffic handled with no-dropped packet priority, assign that QoS level to this EPG.  
3. In the Bridge Domain field of the EPG’s Properties panel, click the drop-down list and choose the name of a bridge domain configured for Type: fcoe.  
4. Click Submit.  
**Note** If you change the Bridge Domain field, you must wait 30-35 seconds between changes. Changing the Bridge Domain field too rapidly causes vFC interfaces on the NPV Switch to fail and a switch reload must be executed. |
**Actions**

To create and associate a new EPG

1. Click `Tenant > tenant_name > Application Profiles > ap1 > Application EPGs`.
2. Right-click `Application EPGs` and click `Create Application EPG`.
3. In the **QoS class** field choose the quality of service (Level1, Level2, or Level3) to assign to traffic generated by this EPG.
   
   If you configured one of the QoS levels for priority-flow control no-drop congestion handling and you want FCoE traffic handled with no-dropped packet priority, assign that QoS level to this EPG.
4. In the **Bridge Domain** field of the **Specify the EPG Identity** dialog, click the drop-down list and choose the name of a bridge domain configured for Type: fcoe.
   
   **Note** If you change the Bridge Domain field, you must wait 30-35 seconds between changes. Changing the Bridge Domain field too rapidly causes vFC interfaces on the NPV Switch to fail and a switch reload must be executed.
5. Finish the bridge domain configuration.
6. Click **Finish**.

---

### Step 3

Add a Fibre Channel Domain association with the EPG.

a) Click `Tenant > tenant_name > Application Profiles > ap1 > Application EPGs > epg_name > Domains & Bare Metal`.

b) Right-click `Domains & Bare Metal` and click `Add Fiber Channel Domain Association`.

c) In the **Add Fiber Channel Domain Association** dialog, locate the Fiber Channel Domain Profile Field.

d) Click the drop-down list and choose the name of the Fibre Channel domain that you previously configured.

e) Click **Submit**.

### Step 4

Under the associated EPG define a Fibre Channel path.

The Fibre Channel path specifies the interfaces enabled as FCoE F ports or NP ports to be associated with the selected EPG.

a) Click `Tenant > tenant_name > Application Profiles > ap1 > Application EPGs > epg_name > Fiber Channel (Paths)`.

b) Right-click **Fiber Channel (Paths)** and click **Deploy Fiber Channel**.

c) In the **Deploy Fiber Channel** dialog configure the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Path Type</strong></td>
<td>The type of interface (Port, Direct Port Channel, or Virtual Port Channel) being accessed for sending and receiving FCoE traffic.</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>The Node-interface path through which FCoE traffic associated with the selected EPG will flow. Click the drop-down list and choose from the listed interfaces.</td>
</tr>
</tbody>
</table>

**Note** Choose only the interfaces previously configured as F ports or NP ports. Choosing interfaces that you did not configure causes only default values to apply to those interfaces.
To deploy FCoE over FEX, select the FEX ports previously configured.

**Note**

The VSAN which will use the interface selected in the **Path** field.

**Note**

The specified VSAN must be in the range of VSANs that was designated for the VSAN pool.

In most cases, all interfaces that this EPG is configured to access must be assigned the same VSAN, unless you specify a Fibre Channel path over a Virtual Port Channel (VPC) connection. In that case, you can specify two VSANs, one for each leg of the connection.

**VSAN Mode**

The mode (**Native** or **Regular**) in which the selected VSAN accesses the selected interface.

Every interface configured for FCoE support, requires one VSAN and only one VSAN configured for Native mode. Any additional VSANs assigned to the same interface must access it in Regular mode.

**Pinning label**

(Optional) This option applies only if you are mapping access to an F port and it is necessary to bind this F port with a specific uplink NP port. It associates a pinning label (pinning label 1 or pinning label 2) with a specific NP port. You can then assign that pinning label to the target F port. This association causes the associated NP port to serve in all cases as the uplink port to the target F Port.

Choose a pinning label and associate it with an interface configured as an NP port.

This option implements what is also referred to as "traffic-mapping."

**Note**

The F port and the associated Pinning Label NP port must be on the same Leaf switch.

---

**Step 5**

Click **Submit**.

**Step 6**

Repeat steps 4 and 5 for every FCoE enabled interface to which you are mapping EPG access.

**Step 7**

Verify successful deployment, as follows:

a) Click **Fabric > Inventory > Pod_name > leaf_name > Interfaces > VFC interfaces**.

The interfaces on which you deployed ports are listed under VFC Interfaces.

---

**What to do next**

After you have set up EPG access to the vFC interfaces, the final step is to set up the network supporting the FCoE initialization protocol (FIP), which enables discovery of those interfaces.

For more information, see Deploying the EPG to Support the FCoE Initiation Protocol, on page 136.

---

**Deploying the EPG to Support the FCoE Initiation Protocol**

After you have configured FCoE EPG access to your server ports, you must also configure EPG access to support the FCoE Initiation Protocol (FIP).
Before you begin

• The ACI fabric is installed.

• A host application that needs to access the FC network is physically attached by Ethernet to a port on the same ACI leaf switch.

• Leaf policy groups, leaf profiles, interface policy groups, interface profiles, and Fibre Channel domains have all been configured to support FCoE traffic as described in the topic Deploying EPG Access to vFC Ports Using the APIC GUI, on page 133.

• EPG access the vFC ports is enabled as described in the topic Deploying EPG Access to vFC Ports Using the APIC GUI, on page 133.

Procedure

Step 1 Under the same tenant configure an existing bridge domain to support FIP or create a regular bridge domain to support FIP.

<table>
<thead>
<tr>
<th>Option: To configure an existing bridge domain for FCoE</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Click Tenant &gt; tenant_name &gt; Networking &gt; Bridge Domains &gt; bridge_domain_name.</td>
</tr>
<tr>
<td></td>
<td>2. In the Type field of the bridge domain's Properties panel, click Regular.</td>
</tr>
<tr>
<td></td>
<td>3. Click Submit.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option: To create a new bridge domain for FCoE</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Click Tenant &gt; tenant_name &gt; Networking &gt; Bridge Domains &gt; Actions &gt; Create a Bridge Domain.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name field of the Specify Bridge Domain for the VRF dialog, enter a bridge domain name.</td>
</tr>
<tr>
<td></td>
<td>3. In the Type field of Specify Bridge Domain for the VRF dialog, click Regular.</td>
</tr>
<tr>
<td></td>
<td>4. In VRF field select a VRF from the drop-down or click Create VRF to create and configure a new VRF.</td>
</tr>
<tr>
<td></td>
<td>5. Finish the bridge domain configuration.</td>
</tr>
<tr>
<td></td>
<td>6. Click Submit.</td>
</tr>
</tbody>
</table>

Step 2 Under the same tenant, configure an existing EPG or create a new EPG to associate with the regular-type bridge domain.

<table>
<thead>
<tr>
<th>Option: To associate an existing EPG</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Click Tenant &gt; tenant_name &gt; Application Profiles &gt; ap1 &gt; Application EPGs &gt; epg_name.</td>
</tr>
<tr>
<td></td>
<td>2. In the Bridge Domain field of the EPG's Properties panel, click the drop-down list and choose the name of the regular bridge domain that you just configured to support FIP.</td>
</tr>
</tbody>
</table>
**Step 3** Add a Physical Domain association with the EPG.

a) Click Tenant > tenant_name > Application Profiles > ap1 > Application EPGs > epg_name > Domains & Bare Metal.
b) Right-click Domains & Bare Metal and click Add Physical Domain Association.
c) In the Add Physical Domain Association dialog, locate Physical Domain Profile Field.
d) Click the drop-down list and choose the name of the physical domain that contains the LAN that intended for use in FIP support.
e) Click Submit.

**Step 4** Under the associated EPG define a path.

The path specifies the interfaces enabled as FCoE F ports or NP ports to be associated with the selected EPG.

a) Click Tenant > tenant_name > Application Profiles > ap1 > Application EPGs > epg_name > Static Bindings (Paths).
b) Right-click Static Binding (Paths) and click Deploy Static EPG on PC, VPC, or Interface.
c) In the Path Type field, specify the port type (Port, Direct Port Channel, or Virtual Port Channel) on which you want to deploy an F mode vFC.
d) In the Path field, specify all the paths on which are deployed the F ports.
e) Choose the VLAN Encap that you want to use as your FCoE VLAN discovery and 802.1p(access) as port mode.
f) Click Submit.

The FCoE components will begin the discovery process to initiate the operation of the FCoE network.

**Undeploying FCoE Connectivity Using the APIC GUI**

To undo FCoE enablement of leaf switch interfaces on the ACI fabric, delete the Fibre Channel path and Fibre Channel domain and its elements that you defined in Deploying FCoE vFC Ports Using the APIC GUI, on page 127.
If during clean up you delete the Ethernet configuration object (infraHPortS) for a vFC port (for example, in the Interface Selector table on the Leaf Interface Profiles page of the GUI), the default vFC properties remain associated with that interface. For example it the interface configuration for vFC NP port 1/20 is deleted, that port remains a vFC port but with default F port setting rather than non-default NP port setting applied.

**Before you begin**

You must know the name of the Fibre Channel path and Fibre Channel domain including its associated VSAN pool, VLAN pool, and VSAN Attributes map that you specified during FCoE deployment.

**Procedure**

**Step 1**
Delete the associated Fibre Channel path to undeploy vFC from the port/vsan whose path was specified on this deployment.

This action removes vFC deployment from the port/vsan whose path was specified on this deployment.

a) Click Tenants > tenant_name > Application Profiles > app_profile_name > Application EPGs > app_epg_name > Fiber Channel (Paths). Then right-click the name of the target Fibre Channel path and choose Delete.

b) Click Yes to confirm the deletion.

**Step 2**
Delete the VLAN to VSAN map that you configured when you defined the Fibre Channel domain.

This action removes vFC deployment from all the elements defined in the map.

a) Click Fabric > External Access Policies > Pools > VSAN Attributes. Then right-click the name of the target map and choose Delete.

b) Click Yes to confirm the deletion.

**Step 3**
Delete the VLAN and VSAN pools that you defined when you defined the Fibre Channel domain.

This action eliminates all vFC deployment from the ACI fabric.

a) Click Fabric > External Access Policies > Pools > VSAN and then, right-click the name of the target VSAN pool name and choose Delete.

b) Click Yes to confirm the deletion.

c) Click Fabric > External Access Policies > Pools > VLAN then, right-click the target VLAN pool name and choose Delete.

d) Click Yes to confirm the deletion.

**Step 4**
Delete the Fibre Channel Domain that contained the VSAN pool, VLAN pool, and Map elements you just deleted.

a) Click Tenants > tenant_name > Application Profiles > Fiber Channel Domains. Then right-click the name of the target Fibre Channel Domain and choose Delete.

b) Click Yes to confirm the deletion.

**Step 5**
You can delete the tenant/EPG/App and the selectors if you don’t need them.
### Configuring FCoE Using the NX_OS Style CLI

#### FCoE NX-OS Style CLI Configuration

**Configuring FCoE Connectivity Without Policies or Profiles Using the NX-OS Style CLI**

The following sample NX-OS style CLI sequences configure FCoE connectivity for EPG e1 under tenant t1 without configuring or applying switch-level and interface-level policies and profiles.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Under the target tenant configure a bridge domain to support FCoE traffic.</td>
</tr>
<tr>
<td></td>
<td>The sample command sequence creates bridge domain b1 under tenant t1 configured to support FCoE connectivity.</td>
</tr>
</tbody>
</table>

**Example:**

```
apic1(config)# tenant t1
napic1(config-tenant)# vrf context v1
napic1(config-tenant-vrf)# exit
napic1(config-tenant)# bridge-domain b1
napic1(config-tenant-bd)# fc
napic1(config-tenant-bd)# vrf member v1
napic1(config-tenant-bd)# exit
napic1(config-tenant)# exit
```

| **Step 2**        | Under the same tenant, associate the target EPG with the FCoE-configured bridge domain. |
|                   | The sample command sequence creates EPG e1 and associates that EPG with the FCoE-configured bridge domain b1. |

**Example:**

```
apic1(config)# tenant t1
napic1(config-tenant)# application a1
napic1(config-tenant-app)# epg e1
napic1(config-tenant-app-epg)# bridge-domain member b1
napic1(config-tenant-app-epg)# exit
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 3    | `apic1(config-tenant-app)# exit`  
`apic1(config-tenant)# exit` | In Example A, the sample command sequence creates VSAN domain, *dom1* with VSAN pools and VLAN pools, maps VSAN 1 to VLAN 1 and maps VSAN 2 to VLAN 2. |
|      | **Example:**  
A  
`apic1(config)# vsan-domain dom1`  
`apic1(config-vsan)# vsan 1-10`  
`apic1(config-vsan)# vlan 1-10`  
`apic1(config-vsan)# fcoe vsan 1 vlan 1 loadbalancing src-dst-ox-id`  
`apic1(config-vsan)# fcoe vsan 2 vlan 2` |  
|      | B  
`apic1(config)# template vsan-attribute pol1`  
`apic1(config-vsan-attr)# fcoe vsan 2 vlan 12 loadbalancing src-dst-ox-id`  
`apic1(config-vsan-attr)# fcoe vsan 3 vlan 13 loadbalancing src-dst-ox-id`  
`apic1(config-vsan)# exit`  
`apic1(config)# vsan-domain dom1`  
`apic1(config-vsan)# vsan 1-10`  
`apic1(config-vsan)# vlan 1-10`  
`apic1(config-vsan)# inherit vsan-attribute pol1`  
`apic1(config-vsan)# exit` | In Example B, an alternate sample command sequence creates a reusable VSAN attribute template *pol1* and then creates VSAN domain *dom1*, which inherits the attributes and mappings from that template. |
| 4    | Create the physical domain to support the FCoE Initialization (FIP) process.  
**Example:**  
`apic1(config)# vlan-domain fipVlanDom`  
`apic1(config-vlan)# vlan 120`  
`apic1(config-vlan)# exit` | In the example, the command sequence creates a regular VLAN domain, *fipVlanDom*, which includes VLAN 120 to support the FIP process. |
| 5    | Under the target tenant configure a regular bridge domain.  
**Example:**  
`apic1(config)# tenant t1`  
`apic1(config-tenant)# vrf context v2`  
`apic1(config-tenant-vrf)# exit`  
`apic1(config-tenant)# bridge-domain fip-bd`  
`apic1(config-tenant-bd)# vrf member v2`  
`apic1(config-tenant-bd)# exit`  
`apic1(config-tenant)# exit` | In the example, the command sequence creates bridge domain *fip-bd*. |
| 6    | Under the same tenant, associate this EPG with the configured regular bridge domain.  
**Example:** | In the example, the command sequence associates EPG *epg-fip* with bridge domain *fip-bd*. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>apic1(config)# tenant t1</td>
<td>In example A the command sequence enables interface 1/2 on leaf switch 101 to function as an F port and associates that interface with VSAN domain dom1.</td>
</tr>
<tr>
<td>apic1(config-tenant)# application a1</td>
<td>Each of the targeted interfaces must be assigned one (and only one) VSAN in native mode. Each interface may be assigned one or more additional VSANs in regular mode.</td>
</tr>
<tr>
<td>apic1(config-tenant-app)# epg epg-fip</td>
<td>The sample command sequence associates the target interface 1/2 with:</td>
</tr>
<tr>
<td>apic1(config-tenant-app-epg)# bridge-domain member fip-bd</td>
<td>• VLAN 120 for FIP discovery and associates it with EPG epg-fip and application a1 under tenant t1.</td>
</tr>
<tr>
<td>apic1(config-tenant-app-epg)# exit</td>
<td>• VSAN 2 as a native VSAN and associates it with EPG e1 and application a1 under tenant t1.</td>
</tr>
<tr>
<td>apic1(config-tenant-app)# exit</td>
<td>• VSAN 3 as a regular VSAN.</td>
</tr>
<tr>
<td>apic1(config-tenant)# exit</td>
<td>In example B, the command sequence configures a VFC over a VPC with the same VSAN on both the legs. From the CLI you cannot specify different VSANs on each leg. The alternate configuration can be carried out in the APIC advanced GUI.</td>
</tr>
</tbody>
</table>

### Step 7
Configure a VFC interface with F mode.

**Example:**

A

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/2
apic1(config-leaf-if)# vlan-domain member fipVlanDom
apic1(config-leaf-if)# switchport trunk
  native vlan 120 tenant t1 application
  a1 epg epg-fip
apic1(config-leaf-if)# exit

apic1(config-leaf)# interface vfc 1/2
apic1(config-leaf-if)# switchport mode f
apic1(config-leaf-if)# vsan-domain member dom1
apic1(config-leaf-if)# switchport vsan
  2 tenant t1 application a1 epg e1
apic1(config-leaf-if)# switchport trunk
  allowed vsan 3 tenant t1 application
  a1 epg e2
apic1(config-leaf-if)# exit
```

**Example:**

B

```
apic1(config)# vpc context leaf 101 102
apic1(config-vpc)# interface vpc vpc1
apic1(config-vpc-if)# vlan-domain member vfdom100
apic1(config-vpc-if)# vsan-domain member dom1
apic1(config-vpc-if)# #For FIP discovery
apic1(config-vpc-if)# switchport trunk
  native vlan 120 tenant t1 application
  a1 epg epg-fip
apic1(config-vpc-if)# switchport vsan 2
  tenant t1 application a1 epg e1
apic1(config-vpc-if)# exit
apic1(config-vpc)# exit
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# channel-group vpc1 vpc
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> C</td>
<td></td>
</tr>
<tr>
<td>apic1(config)# leaf 101</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf)# interface vfc-po pcl</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# vsan-domain member dom1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# switchport vsan 2 tenant t1 application a1 epg e1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# exit</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# interface ethernet 1/2</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# channel-group pcl</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# exit</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Configure a VFC interface with NP mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config)# leaf 101</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf)# interface vfc 1/4</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# switchport mode np</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# vsan-domain member dom1</td>
<td></td>
</tr>
<tr>
<td>The sample command sequence enables interface 1/4 on leaf switch 101 to function as an NP port and associates that interface with VSAN domain dom1.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Assign the targeted FCoE-enabled interfaces a VSAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# switchport trunk allowed vsan 1 tenant t1 application a1 epg e1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# switchport vsan 2 tenant t4 application a4 epg e4</td>
<td></td>
</tr>
<tr>
<td>Each of the targeted interfaces must be assigned one (and only one) VSAN in native mode. Each interface may be assigned one or more additional VSANs in regular mode.</td>
<td></td>
</tr>
<tr>
<td>The sample command sequence assigns the target interface to VSAN 1 and associates it with EPG e1 and application a1 under tenant t1. &quot;trunk allowed&quot; assigns vsan 1 regular mode status. The command sequence also assigns the interface a required native mode VSAN 2. As this example shows, it is permissible for different VSANs to provide different EPGs running under different tenants access to the same interfaces.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring FCoE Connectivity With Policies and Profiles Using the NX-OS Style CLI

The following sample NX-OS style CLI sequences create and use policies to configure FCoE connectivity for EPG e1 under tenant t1.

---

**Configuring FCoE Connectivity With Policies and Profiles Using the NX-OS Style CLI**

The following sample NX-OS style CLI sequences create and use policies to configure FCoE connectivity for EPG e1 under tenant t1.
### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under the target tenant configure a bridge domain to support FCoE traffic.</td>
<td>The sample command sequence creates bridge domain <code>b1</code> under tenant <code>t1</code> configured to support FCoE connectivity.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1# configure</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config)# tenant t1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant)# vrf context v1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant-vrf)# exit</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant)# bridge-domain b1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant-bd)# fc</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant-bd)# vrf member v1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant-bd)# exit</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant)# exit</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config)#</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under the same tenant, associate your target EPG with the FCoE configured bridge domain.</td>
<td>The sample command sequence creates EPG <code>e1</code> associates that EPG with FCoE-configured bridge domain <code>b1</code>.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config)# tenant t1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant)# application a1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant-app)# epg e1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant-app-epg)# bridge-domain member b1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant-app-epg)# exit</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant-app)# exit</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-tenant)# exit</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config)#</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a VSAN domain, VSAN pools, VLAN pools and VSAN to VLAN mapping.</td>
<td>In Example A, the sample command sequence creates VSAN domain, <code>dom1</code> with VSAN pools and VLAN pools, maps VSAN 1 VLAN 1 and maps VSAN 2 to VLAN 2</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>A</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config)# vsan-domain dom1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-vsan)# vsan 1-10</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-vsan)# vlan 1-10</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-vsan)# fcoe vsan 1 vlan 1 loadbalancing src-dst-ox-id</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-vsan)# fcoe vsan 2 vlan 2</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>B</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config)# template vsan-attribute pol1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-vsan-attr)# fcoe vsan 2 vlan 12 loadbalancing src-dst-ox-id</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>apic1(config-vsan-attr)# fcoe vsan 3 vlan 13 loadbalancing src-dst-ox-id</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In Example B, an alternate sample command sequence creates a reusable vsan attribute template <code>pol1</code> and then creates VSAN domain <code>dom1</code>, which inherits the attributes and mappings from that template.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>apic1(config-vsan-attr)# exit</td>
<td></td>
</tr>
<tr>
<td>apic1(config)# vsan-domain dom1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-vsan)# inherit vsan-attribute pol1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-vsan)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Create the physical domain to support the FCoE Initialization (FIP) process.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config)# vlan-domain fipVlanDom</td>
<td>The sample command sequence creates Fibre Channel SAN policy <code>ffp1</code> to specify a combination of error-detect timeout values (EDTOV), resource allocation timeout values (RATOV), and the default FC map values for FCoE-enabled interfaces on a target leaf switch.</td>
</tr>
<tr>
<td>apic1(config)# vlan-pool fipVlanPool</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configure a Fibre Channel SAN policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1#</td>
<td></td>
</tr>
<tr>
<td>apic1# configure</td>
<td></td>
</tr>
<tr>
<td>apic1(config)# template fc-fabric-policy ffp1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-fc-fabric-policy)# fctimer e-d-tov 1111</td>
<td></td>
</tr>
<tr>
<td>apic1(config-fc-fabric-policy)# fctimer r-a-tov 2222</td>
<td></td>
</tr>
<tr>
<td>apic1(config-fc-fabric-policy)# fcoe fcmap 0E:FC:01</td>
<td></td>
</tr>
<tr>
<td>apic1(config-fc-fabric-policy)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Create a Fibre Channel node policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config)# template fc-leaf-policy flp1</td>
<td>The sample command sequence creates Fibre Channel node policy <code>flp1</code> to specify a combination of disruptive load-balancing enablement and FIP keep-alive values. These values also apply to all the FCoE-enabled interfaces on a target leaf switch.</td>
</tr>
<tr>
<td>apic1(config-fc-leaf-policy)# fcoe fka-adv-period 44</td>
<td></td>
</tr>
<tr>
<td>apic1(config-fc-leaf-policy)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Create Node Policy Group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config)# template leaf-policy-group lpg1</td>
<td>The sample command sequence creates a Node Policy group, <code>lpg1</code>, which combines the values of the Fibre Channel SAN policy <code>ffp1</code> and Fibre Channel node policy, <code>flp1</code>. The combined values of this node policy group can be applied to Node profiles configured later.</td>
</tr>
<tr>
<td>apic1(config-leaf-policy-group)# inherit fc-fabric-policy ffp1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-policy-group)# inherit fc-leaf-policy flp1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-policy-group)# exit</td>
<td></td>
</tr>
<tr>
<td>apic1(config)# exit</td>
<td></td>
</tr>
<tr>
<td>apic1#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Create a Node Profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>apic1(config)# leaf-profile lp1</td>
<td>The sample command sequence creates node profile <code>lp1</code> associates it with node policy group <code>lpg1</code>, node group <code>lg1</code>, and leaf switch 101.</td>
</tr>
<tr>
<td>apic1(config-leaf-profile)# leaf-group lg1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-group)# leaf 101</td>
<td></td>
</tr>
</tbody>
</table>

---

**FCoE Connections**

**Configuring FCoE Connectivity With Policies and Profiles Using the NX-OS Style CLI**

---

**Cisco APIC Layer 2 Networking Configuration Guide**

145
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>apic1(config-leaf-group)# leaf-policy-group lpg1</td>
<td>The sample command sequence creates interface policy group <strong>lpg1</strong> and assigns a combination of values that determine priority flow control enablement, F port enablement, and slow-drain policy values for any interface that this policy group is applied to.</td>
</tr>
<tr>
<td><strong>Step 9</strong> Create an interface policy group for F port interfaces.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>apic1(config)# template policy-group lpg1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# priority-flow-control mode auto</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# switchport mode f</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain pause timeout 111</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain congestion-timeout count 55</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain congestion-timeout action log</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# switchport mode np</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain pause timeout 111</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain congestion-timeout count 55</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain congestion-timeout action log</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> Create an interface policy group for NP port interfaces.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>apic1(config)# template policy-group lpg2</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# priority-flow-control mode auto</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# switchport mode np</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain pause timeout 111</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain congestion-timeout count 55</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain congestion-timeout action log</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# switchport mode np</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain pause timeout 111</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain congestion-timeout count 55</td>
<td></td>
</tr>
<tr>
<td>apic1(config-pol-grp-if)# slow-drain congestion-timeout action log</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> Create an interface profile for F port interfaces.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>apic1(config)# leaf-interface-profile lip1</td>
<td>The sample command sequence creates an interface profile <strong>lip1</strong> for F port interfaces, associates the profile with F port specific interface policy group <strong>lpg1</strong>, and specifies the interfaces to which this profile and its associated policies applies.</td>
</tr>
<tr>
<td>apic1(config-leaf-if-profile)# description 'test description lip1'</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if-profile)# leaf-interface-group lgi1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if-group)# description 'test description lgi1'</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if-group)# policy-group lpg1</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if-group)# interface ethernet 1/2-6, 1/9-13</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> Create an interface profile for NP port interfaces.</td>
<td>The sample command sequence creates an interface profile <strong>lip2</strong> for NP port interfaces, associates the profile with NP port specific interface policy group <strong>lpg2</strong>, and specifies the</td>
</tr>
</tbody>
</table>
### Configuring FCoE Over FEX Using NX-OS Style CLI

FCoE ports are configured as port VSANs.

**Procedure**

#### Step 1
Configure Tenant and VSAN domain:

**Example:**

```plaintext
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# bridge-domain b1
apic1(config-tenant-bd)# fc
apic1(config-tenant-bd)# vrf member v1
apic1(config-tenant-bd)# exit
apic1(config-tenant)# application a1
apic1(config-tenant-app)# epg e1
apic1(config-tenant-app-epg)# bridge-domain member b1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant)# exit

apic1(config)# vsan-domain dom1
apic1(config-vsan)# vlan 1-100
apic1(config-vsan)# vsan 1-100
apic1(config-vsan)# fcoe vsan 2 vlan 2 loadbalancing src-dst-ox-id
apic1(config-vsan)# fcoe vsan 3 vlan 3 loadbalancing src-dst-ox-id
apic1(config-vsan)# fcoe vsan 5 vlan 5
apic1(config-vsan)# exit
```

#### Step 2
Associate FEX to an interface:
**Example:**

```
apc1(config)# leaf 101
apc1(config-leaf)# interface ethernet 1/12
apc1(config-leaf-if)# fex associate 111
apc1(config-leaf-if)# exit
```

**Step 3** Configure FCoE over FEX per port, port-channel, and VPC:

**Example:**

```
apc1(config-leaf)# interface vfc 111/1/2
apc1(config-leaf-if)# vsan-domain member dom1
apc1(config-leaf-if)# switchport vsan 2 tenant t1 application al epg e1
apc1(config-leaf-if)# exit

apc1(config-leaf)# interface vfc-po pc1 fex 111
apc1(config-leaf-if)# vsan-domain member dom1
apc1(config-leaf-if)# switchport vsan 2 tenant t1 application a1 epg e1
apc1(config-leaf-if)# exit

apc1(config-leaf)# interface ethernet 111/1/3
apc1(config-leaf-if)# channel-group pc1
apc1(config-leaf-if)# exit

apc1(config)# vpc domain explicit 12 leaf 101 102
apc1(config-vpc)# exit
apc1(config)# vpc context leaf 101 102
apc1(config-vpc)# interface vpc vpc1 fex 111 111
apc1(config-vpc-if)# vsan-domain member dom1
apc1(config-vpc-if)# switchport vsan 2 tenant t1 application a1 epg e1
apc1(config-vpc-if)# exit

apc1(config-vpc)# exit
```

**Step 4** Verify the configuration with the following command:

**Example:**

```
apc1(config-vpc)# show vsan-domain detail
vsan-domain : dom1

vsan : 1-100
vlan : 1-100

Leaf Interface Vsan Vlan Vsan-Mode Port-Mode Usage
---------- ------------ ---- ---- --------- --------- ---------
101 vfc111/1/2 2 2 Native Tenant: t1 Deployed
          App: a1
          Epg: e1

101 PC:pc1 5 5 Native Tenant: t1 Deployed
          App: a1
          Epg: e1
```
Verifying FCoE Configuration Using the NX-OS Style CLI

The following `show` command verifies the FCoE configuration on your leaf switch ports.

**Procedure**

Use the `show vsan-domain` command to verify FCoE is enabled on the target switch.

The command example confirms FCoE enabled on the listed leaf switches and its FCF connection details.

**Example:**

```
ifav-isim8-ifc1# show vsan-domain detail
vsan-domain : iPostfcocoeDomP1
vsan : 1-20 51-52 100-110 200 1999 3100-3101 3133
vlan : 1-20 51-52 100-110 200 1999 3100-3101 3133

<table>
<thead>
<tr>
<th>Leaf</th>
<th>Interface</th>
<th>Vsan</th>
<th>Vlan</th>
<th>Vsan Mode</th>
<th>Port Mode</th>
<th>Usage</th>
<th>Tenant:</th>
<th>Operational</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>vfc1/11</td>
<td>1</td>
<td>1</td>
<td>Regular</td>
<td>F</td>
<td></td>
<td>ipost101</td>
<td>Deployed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>App: ipost1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Epg: ipost1</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>vfc1/12</td>
<td>1</td>
<td>1</td>
<td>Regular</td>
<td>NP</td>
<td></td>
<td>ipost101</td>
<td>Deployed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>App: ipost1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Epg: ipost1</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>PC:infraAccBndl 4</td>
<td>4</td>
<td>Regular</td>
<td>NP</td>
<td>Tenant: ipost101</td>
<td>Deployed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Grp_pc01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>App: ipost4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Epg: ipost4</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>vfc1/30</td>
<td>2000</td>
<td></td>
<td>Native</td>
<td></td>
<td></td>
<td>t1</td>
<td>Not deployed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>App: a1</td>
<td>(invalid-path)</td>
</tr>
</tbody>
</table>
```
Undeploying FCoE Elements Using the NX-OS Style CLI

Any move to undeploy FCoE connectivity from the ACI fabric requires that you remove the FCoE components on several levels.

Procedure

**Step 1**

List the attributes of the leaf port interface, set its mode setting to default, and then remove its EPG deployment and domain association.

The example sets the port mode setting of interface vfc 1/2 to default and then removes the deployment of EPG e1 and the association with VSAN Domain dom1 from that interface.

**Example:**

```
apic1(config)# leaf 101
apic1(config-leaf)# interface vfc 1/2
apic1(config-leaf-if)# show run
# Command: show running-config leaf 101 interface vfc 1 / 2
# Time: Tue Jul 26 09:41:11 2016
leaf 101
  interface vfc 1/2
  vsan-domain member dom1
  switchport vsan 2 tenant t1 application a1 epg e1
exit
exit
apic1(config-leaf-if)# no switchport mode
apic1(config-leaf-if)# no switchport vsan 2 tenant t1 application a1 epg e1
apic1(config-leaf-if)# no vsan-domain member dom1
apic1(config-leaf-if)# exit
```

**Step 2**

List and remove the VSAN mapping and the VLAN and VSAN pools.

The example removes the VSAN VLAN mapping for vsan 2, VLAN pool 1-10, and VSAN pool 1-10 from VSAN domain dom1.

**Example:**

```
apic1(config)# vsan-domain dom1
apic1(config-vsan)# show run
# Command: show running-config vsan-domain dom1
# Time: Tue Jul 26 09:43:47 2016
vsan-domain dom1
  vsan 1-10
  vlan 1-10
  fcoe vsan 2 vlan 2
exit
apic1(config-vsan)# no fcoe vsan 2
apic1(config-vsan)# no vlan 1-10
apic1(config-vsan)# no vsan 1-10
apic1(config-vsan)# exit
```
NOTE: To remove a template-based VSAN to VLAN mapping use an alternate sequence:

```
apic1(config)# template vsan-attribute <template_name>
apic1(config-vsan-attr)# no fcoe vsan 2
```

**Step 3**  
Delete the VSAN Domain.  
The example deletes VSAN domain `dom1`.  
**Example:**

```
apic1(config)# no vsan-domain dom1
```

**Step 4**  
You can delete the associated tenant, EPG, and selectors if you do not need them.

---

**Configuring FCoE Using the REST API**

**Configuring FCoE Connectivity Using the REST API**  
You can configure FCoE-enabled interfaces and EPGs accessing those interfaces using the FCoE protocol with the REST API.

**Procedure**

**Step 1**  
To create a VSAN pool, send a post with XML such as the following example.  
The example creates VSAN pool `vsanPool1` and specifies the range of VSANs to be included.  
**Example:**

```
https://apic-ip-address/api/mo/uni/infra/vsanns-[vsanPool1]-static.xml
```

```
<fvnsVsanInstP name="vsanPool1" allocMode="static">
  <fvnsVsanEncapBlk name="encap" from="vsan-5" to="vsan-100"/>
</fvnsVsanInstP>
```

**Step 2**  
To create a VLAN pool, send a post with XML such as the following example.  
The example creates VLAN pool `vlanPool1` and specifies the range of VLANs to be included.  
**Example:**

```
https://apic-ip-address/api/mo/uni/infra/vlanns-[vlanPool1]-static.xml
```

```
<fvnsVlanInstP name="vlanPool1" allocMode="static">
  <fvnsEncapBlk name="encap" from="vlan-5" to="vlan-100"/>
</fvnsVlanInstP>
```

**Step 3**  
To create a VSAN-Attribute policy, send a post with XML such as the following example.  
The example creates VSAN attribute policy `vsanattr1`, maps `vsan-10` to `vlan-43`, and maps `vsan-11` to `vlan-44`.  
```
<fvnsVsanAttP name="vsanattr1" allocMode="static">
  <fvnsEncapBlk name="encap" from="vsan-10" to="vlan-43"/>
  <fvnsEncapBlk name="encap" from="vsan-11" to="vlan-44"/>
</fvnsVsanAttP>
```
Step 4
To create a Fibre Channel domain, send a post with XML such as the following example.

The example creates VSAN domain vsanDom1.

Example:

https://apic-ip-address/api/mo/uni/fc-vsanDom1.xml

```xml
<!-- Vsan-domain -->
<fcDomP name="vsanDom1">
  <fcRsVsanAttr tDn="uni/infra/vsanattrp-[vsanattr1]"/>
  <infraRsVlanNs tDn="uni/infra/vlanns-[vlanPool1]-static"/>
  <fcRsVsanNs tDn="uni/infra/vsanns-[vsanPool1]-static"/>
</fcDomP>
```

Step 5
To create the tenant, application profile, EPG and associate the FCoE bridge domain with the EPG, send a post with XML such as the following example.

The example creates a bridge domain bd1 under a target tenant configured to support FCoE and an application EPG epg1. It associates the EPG with VSAN domain vsanDom1 and a Fibre Channel path (to interface 1/39 on leaf switch 101). It deletes a Fibre channel path to interface 1/40 by assigning the <fvRsFcPathAtt> object with “deleted” status. Each interface is associated with a VSAN.

Note Two other possible alternative vFC deployments are also displayed. One sample deploys vFC on a port channel. The other sample deploys vFC on a virtual port channel.

Example:

https://apic-ip-address/api/mo/uni/tn-tenant1.xml

```xml
<!-- bridge domain -->
<fvBD name="bd1" type="fc">
  <fvRsCtx tnFvCtxName="vrf1"/>
</fvBD>

<!-- Sample deployment of vFC on a port channel -->
<fvRsFcPathAtt vsanMode="native" vsan="vsan-10" tDN="topology/pod-1/paths 101/pathep-pc01"/>
```
Step 6

To create a port policy group and an AEP, send a post with XML such as the following example.

The example executes the following requests:

- Creates a policy group `portgrp1` that includes an FC interface policy `fcIfPol1`, a priority flow control policy `pfcIfPol1` and a slow-drain policy `sdIfPol1`.
- Creates an attached entity profile (AEP) `AttEntP1` that associates the ports in VSAN domain `vsanDom1` with the settings to be specified for `fcIfPol1`, `pfcIfPol1`, and `sdIfPol1`.

Example:

```
https://apic-ip-address/api/mo/uni.xml
<polUni>
  <infraInfra>
  <infraFuncP>
    <infraAccPortGrp name="portgrp1">
      <infraRsFcIfPol tnFcIfPolName="fcIfPol1"/>
      <infraRsAttEntP tDn="uni/infra/attentp-AttEntP1"/>
      <infraRsQosPfcIfPol tnQosPfcIfPolName="pfcIfPol1"/>
      <infraRsQosSdIfPol tnQosSdIfPolName="sdIfPol1"/>
    </infraAccPortGrp>
  </infraFuncP>
  </infraInfra>
</polUni>
```

Step 7

To create a node selector and a port selector, send a post with XML such as the following example.

The example executes the following requests:

- Creates node selector `leafsel1` that specifies leaf node 101.
- Creates port selector `portsel1` that specifies port 1/39.

Example:

```
https://apic-ip-address/api/mo/uni.xml
<polUni>
  ...
```
Step 8  To create a vPC, send a post with XML such as the following example.

**Example:**

```
https://apic-ip-address/api/mo/uni.xml
<polUni>
	<fabricInst>
		<vpcInstPol name="vpc01" />
		<fabricProtPol pairT="explicit" >
			<fabricExplicitGEp name="vpc01" id="100" >
				<fabricNodePEp id="101"/>
				<fabricNodePEp id="102"/>
				<fabricRsVpcInstPol tnVpcInstPolName="vpc01" />
			</fabricExplicitGEp>
		</fabricProtPol>
	</fabricInst>
</polUni>
```

---

**Configuring FCoE Over FEX Using REST API**

**Before you begin**
- Follow the steps 1 through 4 as described in Configuring FCoE Connectivity Using the REST API, on page 151

**Procedure**

**Step 1** Configure FCoE over FEX (Selectors): Port:

**Example:**
Step 2  Tenant configuration:

Example:

```xml
defTenant name="tenant1">
  <defCtx name="vrf1"/>

  <!-- bridge domain -->
  <defBD name="bd1" type="fc">
    <defRsCtx tnDefCtxName="vrf1"/>
  </defBD>

  <defAp name="app1">
    <defAEPg name="epg1">
      <defRsBd tnDefBDName="bd1"/>
      <defRsDomAtt tDn="uni/fc-vsanDom1"/>
      <defRsFCPathAtt tDn="topology/pod-1/paths-101/extpaths-110/pathep-[eth1/17]" vsan="vsan-11" vsanMode="native"/>
    </defAEPg>
  </defAp>
</defTenant>
```

Step 3  Configure FCoE over FEX (Selectors): Port-Channel:

Example:

```xml
<infraInfra dn="uni/infra">
  <infraNodeP name="nprof1">
    <infraLeafS name="leafsel1" type="range">
      <infraNodeBlk name="nblk1" from_="101" to_="101"/>
    </infraLeafS>
    <infraRsAccPortP tDn="uni/infra/accportprof-pprof1"/>
  </infraNodeP>

  <infraAccPortP name="pprof1">
    <infraHPortS name="portsel1" type="range">
      <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="17" toPort="17"></infraPortBlk>
    </infraHPortS>
  </infraAccPortP>

  <infraFuncP>
    <infraAccPortGrp name="portgrp1">
      <infraRsAttEntP tDn="uni/infra/attentp-attentp1"/>
    </infraAccPortGrp>
  </infraFuncP>

  <infraFexP name="fexprof1">
    <infraFexBndlGrp name="fexbundle1"/>
    <infraHPortS name="portsel2" type="range">
      <infraPortBlk name="blk2" fromCard="1" toCard="1" fromPort="20" toPort="20"></infraPortBlk>
    </infraHPortS>
  </infraFexP>

  <infraAttEntityP name="attentp1">
    <infraRsDomP tDn="uni/fc-vsanDom1"/>
  </infraAttEntityP>
</infraInfra>
```
<infraLeafS name="leafsell" type="range">
  <infraNodeBlk name="nblk1" from="101" to="101"/>
</infraLeafS>
<infraRsAccPortP tDn="uni/infra/accportprof-pprof1" />

<infraNodeP>
  <infraAccPortP name="pprof1">
    <infraHPortS name="portsel1" type="range">
      <infraPortBlk name="blk1"
        fromCard="1" toCard="1" fromPort="18" toPort="18"></infraPortBlk>
      <infraRsAccBaseGrp tDn="uni/infra/fexprof-fexprof1/fexbundle-fexbundle1" fexId="111"
        />
    </infraHPortS>
  </infraAccPortP>
</infraNodeP>

<infraNodeP>
  <infraFexP name="fexprof1">
    <infraFexBndlGrp name="fexbundle1"/>
    <infraHPortS name="portsel1" type="range">
      <infraPortBlk name="blk1"
        fromCard="1" toCard="1" fromPort="20" toPort="20"></infraPortBlk>
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-pc1" />
    </infraHPortS>
  </infraFexP>
</infraNodeP>

<infraNodeP>
  <infraFuncP>
    <infraAccBndlGrp name="pc1">
      <infraRsAttEntP tDn="uni/infra/attentp-attentp1" />
    </infraAccBndlGrp>
  </infraFuncP>
</infraNodeP>

Step 4  Tenant configuration:

Example:

<fvTenant name="tenant1">
  <fvCtx name="vrf1"/>

  <!-- bridge domain -->
  <fvBD name="bd1" type="fc">
    <fvRsCtx tnFvCtxName="vrf1" />
  </fvBD>

  <fvAp name="app1">
    <fvAEPg name="epgl1"/>
    <fvRsBd tnFvBDName="bd1" />
    <fvRsDomAtt tDn="uni/fc-vsanDom1" />
    <fvRsFcPathAtt tDn="topology/pod-1/paths-101/extpaths-111/pathep-[pc1]" vsan="vsan-11" vsanMode="native" />
  </fvAEPg>
</fvAp>
</fvTenant>

Step 5  Configure FCoE over FEX (Selectors): VPC:

Example:

<polUni>
  <fabricInst>
    <vpcInstPol name="vpc1"/>
  </fabricProtPol pairT="explicit" >
Step 6  
Tenant configuration:

Example:

```xml
<fvTenant name="tenant1">
  <fvCtx name="vrf1"/>
  <!-- bridge domain -->
  <fvBD name="bd1" type="fc">
    <fvRsCtx tnFvCtxName="vrf1"/>
  </fvBD>
  <fvAp name="app1">
    <fvAEPg name="egp1">
      <fvRsBd tnFvBDName="bd1" />
      <fvRsDomAtt tDn="uni/fc-vsanDom1" />
      <fvRsFcPathAtt vsanMode="native" vsan="vsan-11" tDn="topology/pod-1/protpaths-101-102/extprotpaths-111-111/pathep-[vpc1]"/>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

Step 7  
Selector configuration:

Example:

```xml
<infraInfra>
  <infraNodeP name="nprof1">
    <infraLeafS name="leafsell1" type="range">
      <infraNodeBlk name="nblk1" from="101" to="101"/>
    </infraLeafS>
    <infraRsAccPortP tDn="uni/infra/accportprof-pprof1"/>
  </infraNodeP>

  <infraNodeP name="nprof2">
    <infraLeafS name="leafsell2" type="range">
      <infraNodeBlk name="nblk2" from="102" to="102"/>
    </infraLeafS>
    <infraRsAccPortP tDn="uni/infra/accportprof-pprof2"/>
  </infraNodeP>

  <infraAccPortP name="pprof1">
    <infraHPortS name="portsell1" type="range">
      <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="18" toPort="18"/>
    </infraHPortS>
    <infraRsAccBaseGrp tDn="uni/infra/fexprof-fexprof1/fexbundle-fexbundle1" fexId="111"/>
  </infraAccPortP>
  <infraAccPortP name="pprof2">
    <infraHPortS name="portsell2" type="range">
      <infraPortBlk name="blk2" fromCard="1" toCard="1" fromPort="18" toPort="18"/>
    </infraHPortS>
    <infraRsAccBaseGrp tDn="uni/infra/fexprof-fexprof2/fexbundle-fexbundle2" fexId="111"/>
  </infraAccPortP>
</infraInfra>
```
Undeploying FCoE Connectivity through the REST API or SDK

To undeploy FCoE connectivity through the APIC REST API or SDK, delete the following objects associated with the deployment:

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;fvRsFcPathAtt&gt;</code> (Fibre Channel Path)</td>
<td>The Fibre Channel path specifies the vFC path to the actual interface. Deleting each object of this type removes the deployment from that object's associated interfaces.</td>
</tr>
<tr>
<td><code>&lt;fcVsanAttrpP&gt;</code> (VSAN/VLAN map)</td>
<td>The VSAN/VLAN map maps the VSANs to their associated VLANs deleting this object removes the association between the VSANs that support FCoE connectivity and their underlying VSANs.</td>
</tr>
<tr>
<td><code>&lt;fvnsVsanInstP&gt;</code> (VSAN pool)</td>
<td>The VSAN pool specifies the set of VSANs available to support FCoE connectivity. Deleting this pool removes those VSANs.</td>
</tr>
<tr>
<td>Object</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>&lt;vnsVlanIsntP&gt;</code> (VLAN pool)</td>
<td>The VLAN pool specifies the set of VLANs available for VSAN mapping. Deleting the associated VLAN pool cleans up after an FCoE undeployment, removing the underlying VLAN entities over which the VSAN entities ran.</td>
</tr>
<tr>
<td><code>&lt;fcDomP&gt;</code> (VSAN or Fibre Channel domain)</td>
<td>The Fibre Channel domain includes all the VSANs and their mappings. Deleting this object undeploys vFC from all interfaces associated with this domain.</td>
</tr>
<tr>
<td><code>&lt;fvAEPg&gt;</code> (application EPG)</td>
<td>The application EPG associated with the FCoE connectivity. If the purpose of the application EPGs was only to support FCoE-related activity, you might consider deleting this object.</td>
</tr>
<tr>
<td><code>&lt;fvAp&gt;</code> (application profile)</td>
<td>The application profile associated with the FCoE connectivity. If the purpose of the application profile was only to support FCoE-related activity, you might consider deleting this object.</td>
</tr>
<tr>
<td><code>&lt;fvTenant&gt;</code> (tenant)</td>
<td>The tenant associated with the FCoE connectivity. If the purpose of the tenant was only to support FCoE-related activity, you might consider deleting this object.</td>
</tr>
</tbody>
</table>

**Note**
If during clean up you delete the Ethernet configuration object (infraHPortS) for a vFC port, the default vFC properties remain associated with that interface. For example if the interface configuration for vFC NP port 1/20 is deleted, that port remains a vFC port but with default F port setting rather than non-default NP port setting applied.

The following steps undeploy FCoE-enabled interfaces and EPGs accessing those interfaces using the FCoE protocol.

**Procedure**

**Step 1**
To delete the associated Fibre Channel path objects, send a post with XML such as the following example.
The example deletes all instances of the Fibre Channel path object `<fvRsFcPathAtt>`.

**Note** Deleting the Fibre Channel paths undeploys the vFC from the ports/VSANs that used them.

**Example:**

```xml
https://apic-ip-address/api/mo/uni/tn-tenant1.xml

<vTenant name="tenant1">
  <fvCtx name="vrf1"/>
  !-- bridge domain -->
  <fvBD name="bd1" type="fc">
    <fvRsCtx tnFvCtxName="vrf1" />
  </fvBD>
</vTenant>
```

---

If the VLAN pool specifies the set of VLANs available for VSAN mapping. Deleting the associated VLAN pool cleans up after an FCoE undeployment, removing the underlying VLAN entities over which the VSAN entities ran.
Step 2 To delete the associated VSAN/VLAN map, send a post such as the following example. The example deletes the VSAN/VLAN map vsanattr1 and its associated <fcVsanAttrpP> object.

Example:
https://apic-ip-address/api/mo/uni/infra/vsanattrp-[vsanattr1].xml

<fcVsanAttrP name="vsanattr1" status="deleted">
  <fcVsanAttrPEntry vlanEncap="vlan-43" vsanEncap="vsan-10" status="deleted"/>
  <fcVsanAttrPEntry vlanEncap="vlan-44" vsanEncap="vsan-11" lbType="src-dst-ox-id" status="deleted"/>
</fcVsanAttrP>

Step 3 To delete the associated VSAN pool, send a post such as the following example. The example deletes the VSAN pool vsanPool1 and its associated <fvnsVsanInstP> object.

Example:
https://apic-ip-address/api/mo/uni/infra/vsanns-[vsanPool1]-static.xml

<!-- Vsan-pool -->
<fvnsVsanInstP name="vsanPool1" allocMode="static" status="deleted">
  <fvnsVsanEncapBlk name="encap" from="vsan-5" to="vsan-100"/>
</fvnsVsanInstP>

Step 4 To delete the associated VLAN pool, send a post with XML such as the following example. The example deletes the VLAN pool vlanPool1 and its associated <fvnsVlanInstP> object.

Example:
https://apic-ip-address/api/mo/uni/infra/vlanns-[vlanPool1]-static.xml

<!-- Vlan-pool -->
<fvnsVlanInstP name="vlanPool1" allocMode="static" status="deleted">
  <fvnsEncapBlk name="encap" from="vlan-5" to="vlan-100"/>
</fvnsVlanInstP>

Step 5 To delete the associated Fibre Channel domain, send a post with XML such as the following example.
The example deletes the VSAN domain `vsanDom1` and its associated `<fcDomP>` object.

**Example:**

```xml
https://apic-ip-address/api/mo/uni/fc-vsanDom1.xml
<fcDomP name="vsanDom1" status="deleted">
  <fcRsVsanAttr tDn="uni/infra/vsanattrp-[vsanattr1]"/>
  <infraRsVlanNs tDn="uni/infra/vlanns-[vlanPool1]-static"/>
  <fcRsVsanNs tDn="uni/infra/vsanns-[vsanPool1]-static"/>
</fcDomP>
```

**Step 6**

**Optional:** If appropriate, you can delete the associated application EPG, the associated application profile, or the associated tenant.

**Example:**

In the following sample, the associated application EPG `epg1` and its associated `<fvAEPg>` object is deleted.

```xml
https://apic-ip-address/api/mo/uni/tn-tenant1.xml
<fvTenant name="tenant1"/>
  <fvCtx name="vrf1"/>
  <!-- bridge domain -->
  <fvBD name="bd1" type="fc">
    <fvRsCtx tnFvCtxName="vrf1"/>
  </fvBD>
  <fvAp name="app1">
    <fvAEPg name="epg1" status="deleted">
      <fvRsBd tnFvBDName="bd1"/>
      <fvRsDomAtt tDn="uni/fc-vsanDom1"/>
      <fvRsFcPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/39]" vsan="vsan-11" vsanMode="native" status="deleted"/>
      <fvRsFcPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/40]" vsan="vsan-10" vsanMode="regular" status="deleted"/>
    </fvAEPg>
    <!-- Sample undeployment of vFC on a port channel -->
    <fvRsFcPathAtt vsanMode="native" vsan="vsan-10" tDn="topology/pod-1/paths-101/pathep-pc01" status="deleted"/>
  </fvAp>
  // Sample undeployment of vFC on a virtual port channel -->
  <fvRsFcPathAtt vsanMode="native" vsan="vsan-10" tDn="topology/pod-1/paths-101/pathep-vpc01" status="deleted"/>
  <fvRsFcPathAtt vsanMode="native" vsan="vsan-10" tDn="topology/pod-1/paths-102/pathep-vpc01" status="deleted"/>
</fvTenant>
```

**Example:**

In the following example, the associated application profile `app1` and its associated `<fvAp>` object is deleted.

```xml
https://apic-ip-address/api/mo/uni/tn-tenant1.xml
<fvTenant name="tenant1">
  <fvCtx name="vrf1"/>
  <!-- bridge domain -->
</fvTenant>
Undeploying FCoE Connectivity through the REST API or SDK

Example:

In the following example, the entire tenant tenant1 and its associated <fvTenant> object is deleted.

https://apic-ip-address/api/mo/uni/tn-tenant1.xml

```xml
<fvTenant name="tenant1" status="deleted">
  <fvCtx name="vrf1"/>
</fvTenant>

<!-- bridge domain -->
<fvBD name="bd1" type="fc" status="deleted">
  <fvRsCtx tnFvCtxName="vrf1"/>
</fvBD>

<fvAp name="app1">
  <fvAEPg name="epg1" status="deleted">
    <fvRsBd tnFvBDName="bd1"/>
    <fvRsDomAtt tDn="uni/fc-vsanDom1"/>
    <fvRsFcPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/39]" vsan="vsan-11" vsanMode="native" status="deleted"/>
    <fvRsFcPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/40]" vsan="vsan-10" vsanMode="regular" status="deleted"/>
  </fvAEPg>
</fvAp>
```

<!-- Sample undeployment of vFC on a port channel -->
```xml
<fvRsFcPathAtt vsanMode="native" vsan="vsan-10" tDN="topology/pod-1/paths 101/pathep-pc01" status="deleted"/>
```

<!-- Sample undeployment of vFC on a virtual port channel -->
```xml
<fvRsFcPathAtt vsanMode="native" vsan="vsan-10" tDN="topology/pod-1/paths-101/pathep-vpc01" status="deleted"/>
<fvRsFcPathAtt vsanMode="native" vsan="vsan-10" tDN="topology/pod-1/paths-102/pathep-vpc01" status="deleted"/>
```

</fvAp>
</fvTenant>
Fibre Channel NPV

This chapter contains the following sections:

- Fibre Channel Connectivity Overview, on page 165
- FC NPV Guidelines and Limitations, on page 166
- Configuring FC NPV Using the GUI, on page 167
- FC Connectivity Basic Configuration Using the APIC GUI, on page 172
- Configuring FC Connectivity Without Policies or Profiles Using the NX-OS CLI, on page 173
- Configuring FC Connectivity With Policies or Profiles Using the NX-OS CLI, on page 174
- Configuring FC Connectivity Using the REST API, on page 176

Fibre Channel Connectivity Overview

A switch is in NPV mode after enabling NPV. NPV mode applies to an entire switch. All end devices connected to a switch that are in NPV mode must log in as an N port to use this feature (loop-attached devices are not supported). All links from the edge switches (in NPV mode) to the NPV core switches are established as NP ports (not E ports), which are used for typical inter-switch links.

FC NPV Benefits

FC NPV provides the following:

- Increased number of hosts that connect to the fabric without adding domain IDs in the fabric
- Connection of FC and FCoE hosts and targets to SAN fabrics using FC interfaces
- Automatic traffic mapping
- Static traffic mapping
- Disruptive automatic load balancing

FC NPV Mode

Feature-set fcoe-npv in ACI will be enabled automatically by default when first FCoE/FC configuration is pushed.
FC Topology

The topology of a typical configuration supporting FC traffic over the ACI fabric consists of the following components:

- A Leaf can be connected to a FC switch by using FCoE NP port or native FC NP port.
- An ACI Leaf can be directly connected with a server/Storage using FCoE links.
- FC/FCoE traffic is not sent to fabric/spine. A Leaf switch does not do local switching for FCoE traffic. The switching is done by a core switch which is connected with a leaf switch via FC/FCoE NPV link.
- Multiple FDISC followed by Flogi is supported with FCoE host and FC/FCoE NP links.

FC NPV Guidelines and Limitations

When configuring FC NPV, note the following guidelines and limitations:
• Ports 1 through 48 are available for FC configuration. Ports 49 through 54 cannot be converted to FC ports.
• FC port mode as F port is not supported.
• SAN port-channel is not supported.
• FCoE Host via FEX over FC NPV link is not supported.
• FC Speed auto and 32G are not supported.
• FC Uplink (NP) connectivity to Brocade Port Blade FC16-32 is not supported when ACI leaf 93180YC-FX port is configured in 8G Speed.
• FC trunk mode ON and Auto is not supported.
• FC fill pattern ARBFF is not supported.
• FC is not supported on 40G and breakout ports.
• FEX bring-up is not supported in FC ports.
• FC NPV support is limited to N9K-C93180YC-FX as of release 3.2(1).
• Port conversion from Ethernet to FC and vice versa requires reload of the switch. Currently only one contiguous range of ports can be converted to FC ports, and this range must be multiple of 4 ending with a port number that is multiple of 4. e.g. 1-4, 1-8, or 21-24.

Configuring FC NPV Using the GUI

Before you begin

• The ACI fabric is installed.

• If you deploy over a port channel (PC) topology, the port channel is set up as described in ACI Leaf Switch Port Channel Configuration Using the GUI, on page 77.

• If you deploy over a virtual port channel (VPC) topology, the VPC is set up as described in ACI Leaf Switch Virtual Port Channel Configuration Using the GUI, on page 89.

• Deployment of NP Port over a VPC-PO is NOT supported.

Procedure

Step 1
Create an FC NPV supportive switch policy group to specify and combine all the leaf switch policies that support FC NPV configuration.
This policy group will be applied to the leaf switches that you want to serve as NPV hosts.

a) In the APIC Advanced GUI, starting on the APIC menu bar, click Fabric > External Access Policies > Switches > Leaf Switches > Policy Groups.

b) Right-click Policy Groups and click Create Access Switch Policy Group.
c) In the **Create Access Switch Policy Group** dialog, specify the settings described below and then click **Submit**.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifies the switch policy group. Enter a name that indicates the FCoE supportive function of this switch policy group. For example, <em>fcoe_switch_policy_grp</em>.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Fiber Channel SAN Policy | Specifies the following SAN Policy values:  
  • FC Protocol EDTOV (default: 2000)  
  • FC Protocol RATOV (default: 10000)  
  • MAC address prefix (also called FC map) used by the leaf switch. This value should match the value of the peer device connected on the same port. Typically the default value OE:FC:00 is used. |
|                   | Click the drop-down option box.  
  • To use the default EDTOV, RATOV, and MAC address prefix values, click **default**.  
  • To use the value specified in an existing policy, click that policy.  
  • To create a new policy to specify a new customized MAC address prefix, click **Create Fiber Channel SAN Policy** and follow the prompts. |

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
</table>
| Fiber Channel Node Policy | Specifies the following values:  
  • Disruptive Load Balance (default: disabled)  
    Specifies whether to execute disruptive load balancing on FCoE traffic should new uplinks come online.  
  • FIP Keep Alive Intervals (default: 8)  
    Specifies the keep alive intervals that apply to FCoE connections. |
|                   | Click the drop-down option box.  
  • To use the default values, click **default**.  
  • To use the value specified in an existing policy, click that policy.  
  • To create a new policy specifying different values, click **Create Fiber Channel Node Policy** and follow the prompts. |

**Step 2**  
Create a leaf profile for leaf switches to support FC NPV traffic.

This profile specifies a switch or set of leaf switches to assign the switch policy group that was configured in the previous step. This association enables that set of switches to support FC NPV traffic with pre-defined policy settings.

a) Starting at the APIC menu bar, click **Fabric > External Access Policies > Switches > Leaf Switches > Profiles**
b) Right-click **Profiles**, then click **Create Leaf Profile**.
c) In the Create Leaf Profile dialog create and name the leaf profile (for example: NPV-1).

d) Also in the Create Leaf Profile dialog, locate the Leaf Selectors table, click + to create a new table row and specify the leaf switches to serve as NPV devices.

e) In the new table row choose a leaf name, blocks, and assign the switch policy group that you created in the previous step.

f) Click Next and then click Finish.

**Step 3**

Create a FC-supportive interface policy group:

a) On the APIC menu bar, click Fabric > External Access Policies > Interfaces > Leaf Interfaces > Policy Groups > FC Interface.

b) Right-click FC Interface to open the Create FC Interface Policy Group dialog box.

c) In the Create FC Interface Policy Group dialog box perform the following actions:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifies the FC Interface Policy Group. Enter a name that indicates the FC supportive function of this interface policy group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fibre Channel Interface Policy</th>
<th>Specifies the Fiber Channel Interface Policy values:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Name—The name of Fiber Channel Interface Policy.</td>
<td></td>
</tr>
<tr>
<td>• Port Mode—NP (Port Mode F is not supported in 3.2(1) release).</td>
<td></td>
</tr>
<tr>
<td>• Trunk Mode—Trunk-off (trunk-on and auto are not supported in 3.2(1) release).</td>
<td></td>
</tr>
<tr>
<td>• Speed—4Gbps/8Gbps/16Gbps (auto and 32Gbps is not supported in 3.2(1) release).</td>
<td></td>
</tr>
<tr>
<td>• Fill Pattern—IDLE (ARBFF is not supported in 3.2(1) release).</td>
<td></td>
</tr>
<tr>
<td>• Receive Buffer Credit—64 (Default)</td>
<td></td>
</tr>
</tbody>
</table>

Click the drop-down option box:

• To use the value specified in an existing policy, click that policy.

• To create a new policy specifying different values, click Fiber Channel Interface Policy and follow the prompts.

**Step 4**

Create an interface profile to support NP port connections, and optional additional profiles to be associated with additional port policy variations.

a) Starting at the APIC bar menu click Fabric > External Access Policies > Interfaces > Leaf Interfaces > Profiles.

b) Right-click Profiles and choose Create Leaf Interface Profile.

c) In the Create Leaf Interface Profile dialog, enter a descriptive name for the profile, for example, FC_NP_port_Interface-Profile-1.

d) Locate the Interface Selectors table and click + to display the Create Access Port Selector dialog. This dialog enables you to display a range of interfaces and apply settings to the fields described in the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive name for this range.</td>
</tr>
<tr>
<td>Interface IDs</td>
<td>Specifies the set of interfaces to which this range applies.</td>
</tr>
</tbody>
</table>
To include a range of interfaces in this range, enter the lower and upper values separated by a dash, for example: 1/5–16.

**Step 5**

Configure whether to apply global QoS policies to FC NPV traffic.

You can specify different QoS policies to different levels (1, 2, or 3) of FC and FCoE traffic.


b) In the QoS Class Policy - Level 1, QoS Class Policy - Level 2, or QoS Class Policy - Level 3 dialog, edit the following fields to specify the PFC and no-drop CoS. Then click Submit.

**Note** Only 1 Level can be configured for PFC and no-drop CoS.

### Policy Description

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFC Admin State</td>
<td>Whether to enable priority flow control to this level of FC traffic (default value is false). Enabling priority flow control sets the Congestion Algorithm for this level of FC traffic to no-drop.</td>
</tr>
<tr>
<td>CoS</td>
<td>The CoS level to impose no drop FC packet handling even in case of FC traffic congestion</td>
</tr>
</tbody>
</table>

**Step 6**

Define a Fibre Channel domain. Create a set of virtual SANs (VSANs) and map them to set of existing VLANs.

a) Starting at the APIC bar menu click Fabric > External Access Policies > Physical and External Domains > Fiber Channel Domains.

b) Right-click Fiber Channel Domains and click Create Fiber Channel Domain.

c) In the Fiber Channel Domain dialog, specify the following settings:

### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name or label you want to assign the VSAN domain you are creating. (For example: vsan-dom2)</td>
</tr>
<tr>
<td>VSAN Pool</td>
<td>The pool of VSANs assigned to this domain.</td>
</tr>
<tr>
<td></td>
<td>• To select an existing VSAN pool, click the drop-down and choose a listed pool. If you want to revise it, click the Edit icon.</td>
</tr>
<tr>
<td></td>
<td>• To create a VSAN pool, click Create a VSAN Pool.</td>
</tr>
<tr>
<td></td>
<td>If you open the dialog to create a VSAN pool, follow the prompts configure the following:</td>
</tr>
<tr>
<td></td>
<td>• A Static resource allocation method to support FCoE.</td>
</tr>
<tr>
<td></td>
<td>• a range of VSANs that will be available to assign to FCoE F port interfaces and NP port interfaces.</td>
</tr>
</tbody>
</table>
### Option | Description/Action
--- | ---
**Note** | Minimum range value is 1. Maximum range value is 4078. Configure multiple ranges of VSANs if necessary.

**VLAN Pool** | The pool of VLANS available to be mapped to by the members of the VSAN pool. A VLAN pool specifies numerical ranges of VLANS you want available to support FCoE connections for this domain. The VLANS in the ranges you specify are available for VSANs to map to them.

- To select an existing VLAN pool, click the drop-down and choose a listed pool. If you want to revise it, click the Edit icon.
- To create a VLAN pool, click **Create a VLAN Pool**.

If you open the dialog to create a VLAN pool, follow the prompts configure the following:

- A **Static** resource allocation method to support FCoE.
- a range of VLANS that will be available for VSANs to map to.

**Note** | Minimum range value is 1. Maximum range value is 4094. Configure multiple ranges of VLANS if necessary.

**VSAN Attr** | The VSAN Attributes map for this domain

The VSAN Attributes map VSANs in the VSAN pool to VLANS. in the VLAN pool

- To select an existing VSAN Attributes map, click the drop-down and choose a listed map. If you want to revise it, click the Edit icon.
- To create a VSAN Attributes map, click **Create VSAN Attributes**.

If you open the dialog to configure the VSAN attributes, follow the prompts configure the following:

- The appropriate load balancing option (src-dst-ox-id or src-dst-id).
- Mapping of individual VSANs to individual VLANS, for example: vsan-8 to vlan-10

**Note** | Only VSANs and VLANS in the ranges you specified for this domain can be mapped to each other.

---

### Step 7
Create an attached entity profile to bind the Fibre Channel domain with your policy group.

a) On the APIC menu bar, click **Fabric > External Access Policies > Interfaces > Leaf Interfaces > Policy Groups > interface_policy_group_name**.

In this step **interface_policy_group_name** is the interface policy group that you defined in Step 3.

b) In the interface policy group dialog, Click the Attached Entity Profile drop-down and choose an existing Attached Entity Profile or click **Create Attached Entity Profile** to create a new one.

c) In the Attached Entity Profile dialog specify the following settings:
Step 8  Associate the leaf profile and the NP port interface profiles.

a) Starting at the APIC menu bar, click Fabric > External Access Policies > Switches > Leaf Switches > Profiles > leaf_switch_profile_name.

In this step leaf_switch_profile_name is the profile that you defined in Step 2.

b) Again on the Associated Interface Selector Profiles table, click + to create a new table row and choose the NP port interface profile you created in Step 5.

c) Click Submit.

Note  The FC selected port/s configuration does not take effect until after the switch has been reloaded.

---

**FC Connectivity Basic Configuration Using the APIC GUI**

For simplified interface configuration of Fibre Channel connectivity use the following steps:

**Before you begin**

- The ACI fabric is installed.
- Deployment of NP Port over a VPC-PO is NOT supported.

**Procedure**

**Step 1**  In the APIC Advanced GUI, starting on the APIC menu bar, click Fabric > Inventory > Topology, within the Topology Work Pane select Interface.

**Step 2**  In the Mode drop-down, select Ethernet/FC.

**Step 3**  In the Interface menu bar, click on the + icon to open the Add Switches dialog box and select switch/es to be configured and click Add Selected.

**Step 4**  Select the port/s to be configured for FC and click Submit and then click Reload and Submit.

**Note**  The FC selected port/s configuration does not take affect until after the selection has been reloaded and submitted.
Configuring FC Connectivity Without Policies or Profiles Using the NX-OS CLI

The sample command sequence below creates bridge domain b1 under tenant t1 configured to support FCoE connectivity.

Before you begin

• Under the target tenant configure a bridge domain to support FCoE traffic.

Procedure

Step 1
To create a bridge domain for FCoE connectivity:

Example:

```bash
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# bridge-domain b1
apic1(config-tenant-bd)# fc
apic1(config-tenant-bd)# vrf member v1
apic1(config-tenant-bd)# exit
apic1(config-tenant)# exit
```

Step 2
Under the same tenant, associate the target EPG with the FCoE-configured bridge domain. The sample command sequence below creates EPG e1 and associates that EPG with the FCoE-configured bridge domain b1:

Example:

```bash
apic1(config)# tenant t1
apic1(config-tenant)# application a1
apic1(config-tenant-app)# epg e1
apic1(config-tenant-app-epg)# bridge-domain member b1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
```

Step 3
The following example creates vsan domain dom1 with vsans 1-10:

Example:

```bash
apic1(config)# vsan-domain dom1
apic1(config-vsan)# vsan 1-10
```

Step 4
Convert range of ports from Ethernet to FC mode. The following example converts port 1/1-4 on switch 101 to FC:

Example:

```bash
apic1# config
apic1(config)# leaf 101
apic1(config-leaf)# slot 1
apic1(config-leaf-slot)# port 1-4 type fc
apic1(config-leaf-slot)# exit
apic1(config-leaf)# exit
```
Port conversion from Ethernet to FC and vice versa requires reload of switch.

**Step 5** Configure FC interface in NP mode. The following example sets various interface properties on interface fc 1/10 and associates that interface with VSAN domain dom1. Each of the targeted interfaces must be assigned one (and only one) VSAN in native mode. The sample command sequence associates the target interface 1/10 with VSAN 10 as a native VSAN and associates it with EPG e1 and application a1 under tenant t1.

**Example:**
```
apic1(config-leaf)# interface fc 1/10
napic1(config-leaf-fc-if)# switchport mode [f | np]
apic1(config-leaf-fc-if)# switchport rxbbcredit <16-64>
apic1(config-leaf-fc-if)# switchport speed [16G | 32G | 4G | 8G | auto | unknown]
apic1(config-leaf-fc-if)# vsan-domain member dom1
napic1(config-leaf-fc-if)# switchport vsan 10 tenant t1 application a1 epg e1
```

**Step 6** Create traffic map to pin server ports to uplink ports. The following example creates Traffic map for vFC 1/47 server interface pinned to FC 1/7 uplink interface:

**Example:**
```
apic1# config
napic1(config)# leaf 101
napic1(config-leaf)# npv traffic-map server-interface vfc 1/47 label label1 tenant tenant1 application app1 epg epg1
napic1(config-leaf)# npv traffic-map external-interface fc 1/7 tenant tenant1 label label1
```

---

**Configuring FC Connectivity With Policies or Profiles Using the NX-OS CLI**

The sample command sequence below creates bridge domain b1 under tenant t1 configured to support FCoE connectivity.

**Before you begin**

- Under the target tenant configure a bridge domain to support FCoE traffic.

**Procedure**

**Step 1** To create a bridge domain for FCoE connectivity:

**Example:**
```
apic1(config)# tenant t1
napic1(config-tenant)# vrf context v1
napic1(config-tenant-vrf)# exit
napic1(config-tenant)# bridge-domain b1
napic1(config-tenant-bd)# fc
napic1(config-tenant-bd)# vrf member v1
napic1(config-tenant-bd)# exit
napic1(config-tenant)# exit
```
Step 2  Under the same tenant, associate the target EPG with the FCoE-configured bridge domain. The sample command sequence below creates EPG e1 and associates that EPG with the FCoE-configured bridge domain b1:

Example:

```
apic1(config)# tenant t1
apic1(config-tenant)# application a1
apic1(config-tenant-app)# epg e1
apic1(config-tenant-app-epg)# bridge-domain member b1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
```

Step 3  Create a VSAN domain. The following example creates vsan domain dom1 with vsans 1-10:

Example:

```
apic1(config)# vsan-domain dom1
apic1(config-vsan)# vsan 1-10
```

Step 4  Create an interface policy group for NP port interfaces. The sample command sequence creates FC interface policy group ipg2 and assigns a combination of values that determine values for any interface that this policy group is applied to:

Example:

```
apic1(config)# template fc-policy-group ipg1
apic1(config-fc-pol-grp-if)# switchport ?
   fill-pattern Configure fill pattern for fc interface
   mode Configure port mode for fc interface
   rxbbcredit Configure rxBBCredit for fc interface
   speed Configure speed for fc interface
   trunk-mode Configure trunk-mode for fc interface
apic1(config-fc-pol-grp-if)# switchport fill-pattern [ARBFF | IDLE]
apic1(config-fc-pol-grp-if)# switchport mode [f | np]
apic1(config-fc-pol-grp-if)# switchport rxbbcredit <16-64>
apic1(config-fc-pol-grp-if)# switchport speed [16G | 32G | 4G | 8G | auto | unknown]
apic1(config-fc-pol-grp-if)# vsan-domain member dom1
```

Step 5  Create an interface profile for FC port interfaces. The sample command sequence creates an interface profile lip1 for FC port interfaces, associates the profile with FC interface policy group ipg1, and specifies the interfaces to which this profile and its associated policies applies:

Example:

```
apic1# configure
apic1(config)# leaf-interface-profile lip1
apic1(config-leaf-if-profile)# description 'test description lip1'
apic1(config-leaf-if-profile)# leaf-interface-group lig1
apic1(config-leaf-if-group)# description 'test description lig1'
apic1(config-leaf-if-group)# fc-policy-group ipg1
apic1(config-leaf-if-group)# interface fc 1/1-4
```

Step 6  Create a leaf profile, assign the leaf interface profile to the leaf profile, and assign the leaf IDs on which the profile will be applied:

Example:

```
apic1(config)# leaf-profile lp103
apic1(config-leaf-profile)# leaf-interface-profile lip1
apic1(config-leaf-profile)# leaf-group range
apic1(config-leaf-group)# leaf 103
apic1(config-leaf-group)#
```

Fibre Channel NPV

Configuring FC Connectivity With Policies or Profiles Using the NX-OS CLI
After associating leaf interface profile to leaf, reload of leaf is required to bring up these ports as FC ports.

---

**Configuring FC Connectivity Using the REST API**

You can configure FC-enabled interfaces and EPGs accessing those interfaces using the FC protocol with the REST API.

**Procedure**

**Step 1**
To create a VSAN pool, send a post with XML such as the following example. The example creates VSAN pool vsanPool1 and specifies the range of VSANs to be included:

**Example:**
https://apic-ip-address/api/mo/uni/infra/vsanns-[vsanPool1]-static.xml

```xml
<!-- Vsan-pool -->
<fvnsVsanInstP allocMode="static" name="vsanPool1">
  <fvnsVsanEncapBlk from="vsan-10" name="encap" to="vsan-11"/>
</fvnsVsanInstP>
```

**Step 2**
To create a VLAN pool, send a post with XML such as the following example. The example creates VLAN pool vlanPool1 and specifies the range of VLANs to be included:

**Example:**
https://apic-ip-address/api/mo/uni/infra/vlanns-[vlanPool1]-static.xml

```xml
<!-- Vlan-pool -->
<fvnsVlanInstP allocMode="static" name="vlanPool1">
  <fvnsEncapBlk from="vlan-10" name="encap" to="vlan-11"/>
</fvnsVlanInstP>
```

**Step 3**
To create a VSAN-Attribute policy, send a post with XML such as the following example. The example creates VSAN attribute policy vsanattr1, maps vsan-10 to vlan-10, and maps vsan-11 to vlan-11.

**Example:**
https://apic-ip-address/api/mo/uni/infra/vsanattrp-[vsanattr1].xml

```xml
<fcVsanAttrP name="vsanattr1">
  <fcVsanAttrPEntry lbType="src-dst-ox-id" vsanEncap="vsan-10" vlanEncap="vlan-10"/>
  <fcVsanAttrPEntry lbType="src-dst-ox-id" vsanEncap="vsan-11" vlanEncap="vlan-11"/>
</fcVsanAttrP>
```

**Step 4**
To create a Fibre Channel domain, send a post with XML such as the following example. The example creates VSAN domain vsanDom1:

**Example:**
https://apic-ip-address/api/mo/uni/fc-vsanDom1.xml

```xml
<!-- Vsan-domain -->
<fcVsanDomP name="vsanDom1">
  <fcRsVsanNs tDn="uni/infra/vsanns-[vsanPool1]-static"/>
</fcVsanDomP>
```
<fcRsVsanAttr tDn="uni/infra/vsanattrp-[vsanattr1]"/>
<infraRsVlanNs tDn="uni/infra/vlanns-[vlanPool1]-static"/>
</fcDomP>

Step 5
To create a FC interface policy group and an AEP, send a post with XML. The example executes the following requests:

- Creates a FC interface policy group portgrp1 that includes an FC interface policy fcIfPol1.
- Creates an attached entity profile (AEP) AttEntP1 that associates the ports in VSAN domain vsanDom1 with the settings to be specified for fcIfPol1.

Example:
https://apic-ip-address/api/mo/uni.xml
<polUni>
 <infraInfra>
  <infraFuncP>
   <infraFcAccPortGrp name="portgrp1">
    <infraRsFcL2IfPol tnFcIfPolName="fcIfPol1"/>
    <infraRsFcAttEntP tDn="uni/infra/attentp-AttEntP1"/>
   </infraFcAccPortGrp>
  </infraFuncP>
 </infraInfra>
</polUni>

Step 6
To convert port range 5-8 to FC ports, send a post with XML such as the following example. The example executes the following requests:

- Creates node selector leafsel1 that specifies leaf node 101.
- Creates port selector portsel1 that specifies ports in range 5-8.
- Configures FC interface policy group to convert these ports to FC ports.

Example:
https://apic-ip-address/api/mo/uni.xml
<polUni>
 <infraInfra>
  <infraNodeP name="nprof1">
   <infraLeafS name="leafsel1" type="range">
    <infraNodeBlk name="nblk1" from_="101" to="101"/>
   </infraLeafS>
   <infraRsAccPortP tDn="uni/infra/accportprof-nprof1"/>
  </infraNodeP>
  <infraAccPortP name="pprof1">
   <infraHPortS name="portsel1" type="range">
    <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="5" toPort="8"/>
   </infraHPortS>
  </infraAccPortP>
 </infraInfra>
</polUni>
After applying FC interface policy group, switch reload is required to bring up the ports as FC ports. Currently only one contiguous range of ports can be converted to FC ports, and this range must be multiple of 4 ending with a port number that is multiple of 4.

E.g. 1-4, 1-8, or 21-24.

**Step 7**

To create the tenant, application profile, EPG and associate the FC bridge domain with the EPG, send a post with XML such as the following example. The example creates a bridge domain bd1 under a target tenant configured to support FC and an application EPG epg1. It associates the EPG with VSAN domain vsanDom1 and a Fibre Channel path to interface 1/7 on leaf switch 101. Each interface is associated with a VSAN.

**Example:**

https://apic-ip-address/api/mo/uni/tn-tenant1.xml

```xml
<fvTenant name="tenant1">
  <fvCtx name="vfc_t1_v1"/>
  <!-- bridge domain -->
  <fvBD name="bd1" unicastRoute="no" type="fc">
    <fvRsCtx tnFvCtxName="vfc_t1_v1"/>
  </fvBD>
  <fvAp name="app1">
    <fvAEPg name="epg1">
      <fvRsBd tnFvBDName="bd1"/>
      <fvRsDomAtt tDn="uni/func-vsanDom1"/>
      <fvRsDomAtt tDn="uni/phys-vsanDom1"/>
      <fvRsFcPathAtt tDn="topology/pod-1/paths-102/pathep-[fc1/7]" vsan="vsan-10" vsanMode="native">
        <fcPinningLbl name="label1"/>
      </fvRsFcPathAtt>
      <fvRsFcPathAtt tDn="topology/pod-1/paths-102/pathep-[fc1/8]" vsan="vsan-10" vsanMode="native">
        <fcPinningLbl name="label1"/>
      </fvRsFcPathAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

**Step 8**

To create traffic map to pin server ports to uplink ports, send a post with XML such as the following example.

Traffic map vFC 1/47 pinned to FC 1/7:

**Example:**

https://apic-ip-address/api/mo/uni/tn-tenant1.xml

```xml
<fvTenant name="tenant1">
  <fvAp name="app1">
    <fvAEPg name="epg1">
      <fvRsFcPathAtt tDn="topology/pod-1/paths-102/pathep-[eth1/47]" vsan="vsan-10" vsanMode="native">
        <fcPinningLbl name="label1"/>
      </fvRsFcPathAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

https://apic-ip-address/api/mo/uni/tn-vfc_t1.xml

```xml
<fvTenant name="tenant1">
  <fcPinningP name="label1">
    <fcRsPinToPath tDn="topology/pod-1/paths-102/pathep-[fc1/7]"/>
  </fcPinningP>
</fvTenant>
```
If traffic map pinning is configured first time, then the FCoE port needs to be shut before configuring the first traffic map.

Note
802.1Q Tunnels

This chapter contains the following sections:

• About ACI 802.1Q Tunnels, on page 181
• Configuring 802.1Q Tunnels Using the GUI, on page 183
• Configuring 802.1Q Tunnels Using the NX-OS Style CLI, on page 185
• Configuring 802.1Q Tunnels Using the REST API, on page 188

About ACI 802.1Q Tunnels

With Cisco ACI and Cisco APIC Release 2.2(1x) and higher, you can configure 802.1Q tunnels on edge (tunnel) ports to enable point-to-multi-point tunneling of Ethernet frames in the fabric, with Quality of Service (QoS) priority settings. A Dot1q Tunnel transports untagged, 802.1Q tagged, and 802.1ad double-tagged frames as-is across the fabric. Each tunnel carries the traffic from a single customer and is associated with a single bridge domain. ACI front panel ports can be part of a Dot1q Tunnel. Layer 2 switching is done based on Destination MAC (DMAC) and regular MAC learning is done in the tunnel. Edge-port Dot1q Tunnels
are supported on second-generation (and later) Cisco Nexus 9000 series switches with "EX" on the end of the switch model name.

With Cisco ACI and Cisco APIC Release 2.3(x) and higher, you can also configure multiple 802.1Q tunnels on the same core port to carry double-tagged traffic from multiple customers, each distinguished with an access encapsulation configured for each 802.1Q tunnel. You can also disable MAC Address Learning on 802.1Q tunnels. Both edge ports and core ports can belong to an 802.1Q tunnel with access encapsulation and disabled MAC Address Learning. Both edge ports and core ports in Dot1q Tunnels are supported on third-generation Cisco Nexus 9000 series switches with "FX" on the end of the switch model name.

Terms used in this document may be different in the Cisco Nexus 9000 Series documents.

<table>
<thead>
<tr>
<th>ACI Documents</th>
<th>Cisco Nexus 9000 Series Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Port</td>
<td>Tunnel Port</td>
</tr>
<tr>
<td>Core Port</td>
<td>Trunk Port</td>
</tr>
</tbody>
</table>

The following guidelines and restrictions apply:

- Layer 2 tunneling of VTP, CDP, LACP, LLDP, and STP protocols is supported with the following restrictions:
  - Link Aggregation Control Protocol (LACP) tunneling functions as expected only with point-to-point tunnels using individual leaf interfaces. It is not supported on port-channels (PCs) or virtual port-channels (vPCs).
  - CDP and LLDP tunneling with PCs or vPCs is not deterministic; it depends on the link it chooses as the traffic destination.
  - To use VTP for Layer 2 protocol tunneling, CDP must be enabled on the tunnel.
  - STP is not supported in an 802.1Q tunnel bridge domain when Layer 2 protocol tunneling is enabled and the bridge domain is deployed on Dot1q Tunnel core ports.
  - ACI leaf switches react to STP TCN packets by flushing the end points in the tunnel bridge domain and flooding them in the bridge domain.
  - CDP and LLDP tunneling with more than two interfaces flood packets on all interfaces.
  - With Cisco APIC Release 2.3(x) or higher, the destination MAC address of Layer 2 protocol packets tunneled from edge to core ports is rewritten as 01-00-0c-cd-cd-d0 and the destination MAC address of Layer 2 protocol packets tunneled from core to edge ports is rewritten with the standard default MAC address for the protocol.

- If a PC or VPC is the only interface in a Dot1q Tunnel and it is deleted and reconfigured, remove the association of the PC/VPC to the Dot1q Tunnel and reconfigure it.

- With Cisco APIC Release 2.2(x) the Ethertypes for double-tagged frames must be 0x9100 followed by 0x8100. However, with Cisco APIC Release 2.3(x) and higher, this limitation no longer applies for edge ports, on third-generation Cisco Nexus switches with "FX" on the end of the switch model name.

- For core ports, the Ethertypes for double-tagged frames must be 0x8100 followed by 0x8100.
• You can include multiple edge ports and core ports (even across leaf switches) in a Dot1q Tunnel.

• An edge port may only be part of one tunnel, but a core port can belong to multiple Dot1q tunnels.

• With Cisco APIC Release 2.3(x) and higher, regular EPGs can be deployed on core ports that are used in 802.1Q tunnels.

• L3Outs are not supported on interfaces enabled for Dot1q Tunnels.

• FEX interfaces are not supported as members of a Dot1q Tunnel.

• Interfaces configured as breakout ports do not support 802.1Q tunnels.

• Interface-level statistics are supported for interfaces in Dot1q Tunnels, but statistics at the tunnel level are not supported.

Configuring 802.1Q Tunnels Using the GUI

Configuring 802.1Q Tunnel Interfaces Using the APIC GUI

Configure the interfaces that will use the tunnel, with the following steps:

Before you begin

Create the tenant that will be using the tunnel.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>On the menu bar, click Fabric &gt; External Access Policies.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Navigation bar, click Policies &gt; Interface &gt; L2 Interface.</td>
</tr>
</tbody>
</table>
| Step 3 | Right-click L2 Interface, select Create L2 Interface Policy, and perform the following actions:  
  a) In the Name field, type a name for the Layer 2 Interface policy.  
  b) Optional. Add a description of the policy. We recommended that you describe the purpose for the L2 Interface Policy.  
  c) To create an interface policy that enables an interface to be used as an edge port in a Dot1q Tunnel, in the QinQ field, click edgePort.  
  d) To create an interface policy that enables an interface to be used as a core port in Dot1q Tunnels, in the QinQ field, click corePort. |
| Step 4 | Apply the L2 Interface policy to a Policy Group with the following steps:  
  a) Click on Fabric > External Access Policies > Interfaces > Leaf Interfaces and expand Policy Groups.  
  b) Right-click Leaf Access Port, PC Interface, or VPC Interface and choose one of the following, depending on the type of interface you are configuring for the tunnel.  
    • Create Leaf Access Port Policy Group  
    • Create PC Policy Group  
    • Create VPC Policy Group |
c) In the resulting dialog box, perform the following actions:

- In the **Name** field, type a name for the policy group.
  Optional. Add a description of the policy group. We recommend that you describe the purpose of the policy group.

- In the **L2 Interface Policy** field, click on the down-arrow and choose the L2 Interface Policy that you previously created.

- If you are tunneling the CDP Layer 2 Tunneled Protocol, click on the **CDP Policy** down-arrow, and in the policy dialog box add a name for the policy, disable the Admin State and click **Submit**.

- If you are tunneling the LLDP Layer 2 Tunneled Protocol, click on the **LLDP Policy** down-arrow, and in the policy dialog box add a name for the policy, disable the Transmit State and click **Submit**.

- Click **Submit**.

**Step 5**  
Create a Leaf Interface Profile with the following steps:

a) Click on **Fabric > External Access Policies > Interfaces > Leaf Interfaces > Profiles**.

b) Right-click on **Profiles**, select **Create Leaf Interface Profile**, and perform the following steps:

- In the **Name** field, type a name for the **Leaf Interface Profile**.
  Optional. Add a description.

- In the **Interface Selectors** field, click the +, and enter the following information:

  - In the **Name** field, type a name for the interface selector.
    Optional. Add a description.

  - In the **Interface IDs** field, enter the **Dot1q Tunnel** interface or multiple interfaces to be included in the tunnel.

  - In the **Interface Policy Group** field, click on the down arrow and select the interface policy group that you previously created.

**Step 6**  
To create a static binding of the tunnel configuration to a port, click on **Tenant > Networking > Dot1Q Tunnels**. Expand **Dot1Q Tunnels** and click on the **Dot1Q Tunnels policy_name** perviously created and perform the following actions:

a) Expand the **Static Bindings** table to open **Create Static Binding** dialog box.

b) In the **Port** field, select the type of port.

c) In the **Node** field, select a node from the drop-down.

d) In the **Path** field, select the interface path from the drop-down and click **Submit**.
Configuring 802.1Q Tunnels Using the NX-OS Style CLI

You can use ports, port-channels, or virtual port channels for interfaces included in a Dot1q Tunnel. Detailed steps are included for configuring ports. See the examples below for the commands to configure edge and core port-channels and virtual port channels.

Create a Dot1q Tunnel and configure the interfaces for use in the tunnel using the NX-OS Style CLI, with the following steps:

Dot1q Tunnels must include 2 or more interfaces. Repeat the steps (or configure two interfaces together), to mark each interface for use in a Dot1q Tunnel. In this example, two interfaces are configured as edge-switch ports, used by a single customer.

Use the following steps to configure a Dot1q Tunnel using the NX-OS style CLI:

1. Configure at least two interfaces for use in the tunnel.
2. Create a Dot1q Tunnel.
3. Associate all the interfaces with the tunnel.

Before you begin
Configure the tenant that will use the Dot1q Tunnel.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>apic1# configure</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure two interfaces for use in an 802.1Q tunnel, with the following steps:</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>leaf ID</td>
<td>Identifies the leaf where the interfaces of the Dot1q Tunnel will be located.</td>
</tr>
<tr>
<td>Example:</td>
<td>apic1(config)# leaf 101</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>interface ethernet slot/port</td>
<td>Identifies the interface or interfaces to be marked as ports in a tunnel.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf)# interface ethernet 1/13-14</td>
<td>Mark the interfaces for use in an 802.1Q tunnel, and then leaves the configuration mode. The example shows configuring some interfaces for edge port use. Repeat steps 3 to 5 to configure more interfaces for the tunnel.</td>
<td></td>
</tr>
<tr>
<td>Step 5 switchport mode dot1q-tunnel {edgePort</td>
<td>corePort}</td>
<td>Example:</td>
</tr>
<tr>
<td>apic1(config-leaf-if)# switchport mode dot1q-tunnel edgePort</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apic1(config)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6 Create an 802.1Q tunnel with the following steps:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 7 leaf ID</td>
<td>Returns to the leaf where the interfaces are located.</td>
<td></td>
</tr>
<tr>
<td>apic1(config)# leaf 101</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 8 interface ethernet {slot</td>
<td>port}</td>
<td>Returns to the interfaces included in the tunnel.</td>
</tr>
<tr>
<td>apic1(config-leaf)# interface ethernet 1/13-14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 9 switchport tenant {tenant-name</td>
<td>dot1q-tunnel} tunnel-name</td>
<td>Associates the interfaces to the tunnel and exits the configuration mode.</td>
</tr>
<tr>
<td>apic1(config-leaf-if)# switchport tenant tenant64 dot1q-tunnel vrf64_edgetunnel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apic1(config)# leaf 102</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf)# interface ethernet 1/10, 1/21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# switchport mode dot1q-tunnel corePort</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example: Configuring an 802.1Q Tunnel Using Ports with the NX-OS Style CLI**

The example marks two ports as edge port interfaces to be used in a Dot1q Tunnel, marks two more ports to be used as core port interfaces, creates the tunnel, and associates the ports with the tunnel.

apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/13-14
apic1(config-leaf-if)# switchport mode dot1q-tunnel edgePort
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 1/10, 1/21
apic1(config-leaf-if)# switchport mode dot1q-tunnel corePort
Example: Configuring an 802.1Q Tunnel Using Port-Channels with the NX-OS Style CLI

The example marks two port-channels as edge-port 802.1Q interfaces, marks two more port-channels as core-port 802.1Q interfaces, creates a Dot1q Tunnel, and associates the port-channels with the tunnel.
Example: Configuring an 802.1Q Tunnel Using Virtual Port-Channels with the NX-OS Style CLI

The example marks two virtual port-channels (VPCs) as edge-port 802.1Q interfaces for the Dot1q Tunnel, marks two more VPCs as core-port interfaces for the tunnel, creates the tunnel, and associates the virtual port-channels with the tunnel.

apic1# configure
apic1(config)# vpc domain explicit 1 leaf 101 102
apic1(config)# vpc context leaf 101 102
apic1(config-vpc)# interface vpc vpc1
apic1(config-vpc-if)# switchport mode dot1q-tunnel edgePort
apic1(config-vpc-if)# exit
apic1(config)# vpc domain explicit 1 leaf 103 104
apic1(config)# vpc context leaf 103 104
apic1(config-vpc)# interface vpc vpc2
apic1(config-vpc-if)# switchport mode dot1q-tunnel corePort
apic1(config-vpc-if)# exit
apic1(config)# tenant tenant64
apic1(config-tenant)# dot1q-tunnel vrf64_tunnel
apic1(config-tenant-tunnel)# l2protocol-tunnel cdp
apic1(config-tenant-tunnel)# l2protocol-tunnel lldp
apic1(config-tenant-tunnel)# access-encap 200
apic1(config-tenant-tunnel)# mac-learning disable
apic1(config-tenant-tunnel)# exit
apic1(config-tenant)# exit
apic1(config-leaf)# interface ethernet 1/6
apic1(config-leaf-if)# channel-group vpc1 vpc
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 104
apic1(config-leaf)# interface ethernet 1/6
apic1(config-leaf-if)# channel-group vpc1 vpc
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config-vpc)# interface vpc vpc1
apic1(config-vpc-if)# switchport tenant tenant64 dot1q-tunnel vrf64_tunnel
apic1(config-vpc-if)# exit

Configuring 802.1Q Tunnels Using the REST API

Configuring 802.1Q Tunnels With Ports Using the REST API

Create a Dot1q Tunnel, using ports, and configure the interfaces for it with steps such as the following examples.

Before you begin
Configure the tenant that will use the Dot1q Tunnel.
Procedure

Step 1 Create a **Dot1q Tunnel** using the REST API with XML such as the following example.
The example configures the tunnel with the LLDP Layer 2 tunneling protocol, adds the access encapsulation VLAN, and disables MAC learning in the tunnel.

**Example:**
```
<fvTnlEPg name="VRF64_dot1q_tunnel" qiqL2ProtTunMask="lldp" accEncap="vlan-10" fwdCtrl="mac-learn-disable" >
  <fvRsTnlpathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/13]"/>
</fvTnlEPg>
```

Step 2 Configure a Layer 2 Interface policy with static binding with XML such as the following example.
The example configures a Layer 2 interface policy for edge-switch ports. To configure a policy for core-switch ports, use `corePort` instead of `edgePort` in the `l2IfPol` MO.

**Example:**
```
<l2IfPol name="VRF64_L2_int_pol" qinq="edgePort" />
```

Step 3 Apply the Layer 2 Interface policy to a Leaf Access Port Policy Group with XML such as the following example.

**Example:**
```
<infraAccPortGrp name="VRF64_L2_Port_Pol_Group" >
  <infraRsL2IfPol tDn="uni/infra/funcprof/accportgrp-VRF64_L2_Port_Pol_Group" />
</infraAccPortGrp>
```

Step 4 Configure a Leaf Profile with an Interface Selector with XML such as the following example:

**Example:**
```
<infraAccPortP name="VRF64_dot1q_leaf_profile" >
  <infraHPortS name="vrf64_access_port_selector" type="range">
    <infraPortBlk name="block2" toPort="15" toCard="1" fromPort="13" fromCard="1"/>
    <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-VRF64_L2_Port_Pol_Group"/>
  </infraHPortS>
</infraAccPortP>
```

Example

The following example shows the port configuration for edge ports in two posts.

**XML with Post 1:**
```
<polUni>
  <infraInfra>
    <l2IfPol name="testL2IfPol" qinq="edgePort"/>
    <infraNodeP name="Node_101_phys">
      <infraLeafS name="phys101" type="range">
        <infraNodeBlk name="test" from="101" to="101"/>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/funcprof/accportprof-phys21"/>
    </infraNodeP>
    <infraAccPortP name="phys21">
      <infraHPortS name="physHPortS" type="range">
        <infraPortBlk name="phys21" fromCard="1" toCard="1" fromPort="21" toPort="21"/>
      </infraHPortS>
    </infraAccPortP>
  </infraNodeP>
</polUni>
```
Configuring 802.1Q Tunnels With PCs Using the REST API

Create a Dot1q Tunnel, using PCs, and configure the interfaces for it with steps such as the following examples.

**Before you begin**
Configure the tenant that will use the Dot1q Tunnel.

**Procedure**

**Step 1**
Create a Dot1q Tunnel using the REST API with XML such as the following example.

The example configures the tunnel with the LLDP Layer 2 tunneling protocol, adds the access encapsulation VLAN, and disables MAC learning in the tunnel.

**Example:**
```xml
<nfTnEpg name="WEB" qiqL2ProtTunMask=lldp accEncap="vlan-10" fwdCtrl="mac-learn-disable">
  <nfRsTnlpathAtt tDn="topology/pod-1/paths-101/pathEpg-[eth1/21]"/>
</nfTnEpg>
```

**Step 2**
Configure a Layer 2 Interface policy with static binding with XML such as the following example.

The example configures a Layer 2 interface policy for edge-switch ports. To configure a Layer 2 interface policy for core-switch ports, use `corePort` instead of `edgePort` in the `l2IfPol` MO.

**Example:**
```xml
<l2IfPol name="testL2IfPol" qinq="edgePort"/>
```

**Step 3**
Apply the Layer 2 Interface policy to a PC Interface Policy Group with XML such as the following:
Example:

```
<infraAccBndlGrp name="po2" lagT="link">
  <infraRsL2IfPol tnL2IfPolName="testL2IfPol"/>
</infraAccBndlGrp>
```

Step 4 Configure a Leaf Profile with an Interface Selector with XML such as the following:

Example:

```
<infraAccPortP name="PC">
  <infraHPortS name="allow" type="range">
    <infraPortBlk name="block2" fromCard="1" toCard="1" fromPort="10" toPort="11" />
    <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-po2"/>
  </infraHPortS>
</infraAccPortP>
```

Example

The following example shows the PC configuration in two posts.

This example configures the PC ports as edge ports. To configure them as core ports, use `corePort` instead of `edgePort` in the `l2IfPol` MO, in Post 1.

XML with Post 1:

```
<infraInfra dn="uni/infra">
  <infraNodeP name="bLeaf3">
    <infraLeafS name="leafs3" type="range">
      <infraNodeBlk name="nblk3" from="101" to="101">
      </infraNodeBlk>
    </infraLeafS>
    <infraRsAccPortP tDn="uni/infra/accportprof-shipping3"/>
  </infraNodeP>
  <infraAccPortP name="shipping3">
    <infraHPortS name="pselc3" type="range">
      <infraPortBlk name="blk3" fromCard="1" toCard="1" fromPort="24" toPort="25"/>
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-accountingLag3"/>
    </infraHPortS>
  </infraAccPortP>
  <infraFuncP>
    <infraAccBndlGrp name="accountingLag3" lagT='link'>
      <infraRsAttEntP tDn="uni/infra/attentp-default"/>
      <infraRsLacpPol tnLacpLagPolName='accountingLacp3'/>
      <infraRsL2IfPol tnL2IfPolName="testL2IfPol3"/>
    </infraAccBndlGrp>
  </infraFuncP>
</infraInfra>
```

XML with Post 2:

```
<polUni>
  <fvTenant dn="uni/tn-Coke" name="Coke">
    <!-- bridge domain -->
    <fvTenantPg name="WEB6" qiqL2ProtTunMask="lldp" accEncap="vlan-10" fwdCtrl="mac-learn-disable"/>
  </fvTenant>
</polUni>
```
Configuring 802.1 Q Tunnels With VPCs Using the REST API

Create a Dot1q Tunnel, using VPCs, and configure the interfaces for it with steps such as the following examples.

**Before you begin**

Configure the tenant that will use the Dot1q Tunnel.

**Procedure**

**Step 1**
Create an 802.1Q tunnel using the REST API with XML such as the following example.

The example configures the tunnel with a Layer 2 tunneling protocol, adds the access encapsulation VLAN, and disables MAC learning in the tunnel.

**Example:**

```xml
<vzFilter name="WEB" qigL2ProtTunMask=lldp accEncap="vlan-10" fwdCtrl="mac-learn-disable">
  <vzRsTnlPathAtt tDn="topology/pod-1/protpaths-101-102/pathep-[po4]" />
</vzFilter>
```

**Step 2**
Configure a Layer 2 interface policy with static binding with XML such as the following example.

The example configures a Layer 2 interface policy for edge-switch ports. To configure a Layer 2 interface policy for core-switch ports, use the `qinq="corePort"` port type.

**Example:**

```xml
<l2IfPol name="testL2IfPol" qinq="edgePort"/>
```

**Step 3**
Apply the Layer 2 Interface policy to a VPC Interface Policy Group with XML such as the following:

**Example:**

```xml
<infraAccBndlGrp name="po4" lagT="node">
  <infraRsL2IfPol tnL2IfPolName="testL2IfPol"/>
</infraAccBndlGrp>
```

**Step 4**
Configure a Leaf Profile with an Interface Selector with XML such as the following:

**Example:**

```xml
<infraAccPortP name="VPC">
  <infraHPortS name="allow" type="range">
    <infraPortBlk name="block2" fromCard="1" toCard="1" fromPort="10" toPort="11" />
    <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-po4"/>
  </infraHPortS>
</infraAccPortP>
```
Example

The following example shows the VPC configuration in three posts.

This example configures the VPC ports as edge ports. To configure them as core ports, use `corePort` instead of `edgePort` in the `l2IfPol` MO, in Post 2.

**XML with Post 1:**

```xml
<polUni>
    <fabricInst>
        <fabricProtPol pairT="explicit">
            <fabricExplicitGEp name="101-102-vpc1" id="30">
                <fabricNodePEp id="101"/>
                <fabricNodePEp id="102"/>
            </fabricExplicitGEp>
        </fabricProtPol>
    </fabricInst>
</polUni>
```

**XML with Post 2:**

```xml
<infraInfra dn="uni/infra">
    <infraNodeP name="bLeaf1">
        <infraLeafS name="leafs" type="range">
            <infraNodeBlk name="nblk" from="101" to="101">
                </infraNodeBlk>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-shipping1"/>
    </infraNodeP>

    <infraNodeP name="bLeaf2">
        <infraLeafS name="leafs" type="range">
            <infraNodeBlk name="nblk" from="102" to="102">
                </infraNodeBlk>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-shipping2"/>
    </infraNodeP>

    <infraAccPortP name="shipping1">
        <infraHPortS name="pselect" type="range">
            <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="4" toPort="4"/>
            <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-accountingLag1"/>
        </infraHPortS>
    </infraAccPortP>

    <infraAccPortP name="shipping2">
        <infraHPortS name="pselect" type="range">
            <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="2" toPort="2"/>
            <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-accountingLag2"/>
        </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
        <infraAccBndlGrp name="accountingLag1" lagT='node'>
            <infraRsAttEntP tDn="uni/infra/attentp-default"/>
            <infraRsLacpPol tnLacpLagPolName='accountingLacp1'/>
            <infraRsL2IfPol tnL2IfPolName='testL2IfPol'/>
        </infraAccBndlGrp>

        <infraAccBndlGrp name="accountingLag2" lagT='node'>
            <infraRsAttEntP tDn="uni/infra/attentp-default"/>
            <infraRsLacpPol tnLacpLagPolName='accountingLacp1'/>
            <infraRsL2IfPol tnL2IfPolName='testL2IfPol'/>
        </infraAccBndlGrp>
    </infraFuncP>
</infraInfra>
```
Configuring 802.1Q Tunnels With VPCs Using the REST API

XML with Post 3:

```xml
<polUni>
  <fvTenant dn="uni/tn-Coke" name="Coke">
    <!-- bridge domain -->
    <fvTfgEp name="WEB6" qiqL2ProtTunMask="lldp" accEncap="vlan-10" fwdCtrl="mac-learn-disable">
      <fvRsTnlpathAtt tDn="topology/pod-1/protpaths-101-102/pathep-[accountingLag2]"/>
    </fvTfgEp>
  </fvTenant>
</polUni>
```
Q-in-Q Encapsulation Mapping for EPGs

Using Cisco APIC, you can map double-tagged VLAN traffic ingressing on a regular interface, PC, or VPC to an EPG. When this feature is enabled, when double-tagged traffic enters the network for an EPG, both tags are processed individually in the fabric and restored to double-tags when egressing the ACI switch. Ingressing single-tagged and untagged traffic is dropped.

This feature is only supported on Nexus 9300-FX platform switches.

Both the outer and inner tag must be of EtherType 0x8100.

MAC learning and routing are based on the EPG port, sclass, and VRF, not on the access encapsulations.

QoS priority settings are supported, derived from the outer tag on ingress, and rewritten to both tags on egress.

EPGs can simultaneously be associated with other interfaces on a leaf switch, that are configured for single-tagged VLANs.

Service graphs are supported for provider and consumer EPGs that are mapped to Q-in-Q encapsulated interfaces. You can insert service graphs, as long as the ingress and egress traffic on the service nodes is in single-tagged encapsulated frames.

The following features and options are not supported with this feature:

- Per-Port VLAN feature
- FEX connections
- Mixed Mode is not supported. For example, an interface in Q-in-Q encapsulation mode can have a static path binding to an EPG with double-tagged encapsulation only, not with regular VLAN encapsulation.
- STP and the “Flood in Encapsulation” option
- Untagged and 802.1p mode
- Multi-pod and Multi-Site
• Legacy bridge domain
• L2Out and L3Out connections
• VMM integration
• Changing a port mode from routed to Q-in-Q encapsulation mode is not supported
• Per-vlan MCP is not supported between ports in Q-in-Q encapsulation mode and ports in regular trunk mode.
• When VPC ports are enabled for Q-in-Q encapsulation mode, VLAN consistency checks are not performed.

Configuring Q-in-Q Encapsulation Mapping for EPGs Using the GUI

Enabling Q-in-Q Encapsulation on Specific Leaf Switch Interfaces Using the GUI

Leaf switch ports, PCs, or VPCs are enabled for Q-in-Q encapsulation mode in the Interface tab of one of the following locations in the APIC GUI.

- Fabric > Inventory > Topology
- Fabric > Inventory > Pod
- Fabric > Inventory > Pod > leaf-name

Configure VPCs on the Topology or Pod ConfigureInterface tab.

Before you begin

The tenant, application profile, and the application EPG that will be mapped with an interface configured for Q-in-Q mode should be created.

Procedure

Step 1  On the menu bar, choose Fabric > Inventory and click Topology, Pod, or expand Pod and choose a leaf.
Step 2  On the Topology or Pod panel ConfigureInterface tab.
Step 3  Click the Operation/Configuration toggle-button to display the configuration panel.
Step 4  Click + to add diagrams of leaf switches, choose one or more switches, and click Add Selected.
On the leaf-name panel ConfigureInterface tab, a diagram of the switch appears automatically, after you click the Operation/Configuration toggle-button.
Step 5  Click the interfaces to be enabled for Q-in-Q encapsulation mode.
Step 6  To configure a port, perform the following steps:
a) Click L2 on the upper left.
Enabling Q-in-Q Encapsulation for Leaf Interfaces With Fabric Interface Policies Using the GUI

Enable leaf interfaces, PCs, and VPCs for Q-in-Q encapsulation, using a leaf interface profile.

Before you begin

The tenant, application profile, and the application EPG that will be mapped with an interface configured for Q-in-Q mode should be created.

Procedure

2. On the Navigation bar, click Policies > Interface > L2 Interface.
3. Right-click L2 Interface, select Create L2 Interface Policy, and perform the following actions:
   a) In the Name field, enter a name for the Layer 2 Interface policy.
   b) Optional. Add a description of the policy. We recommend that you describe the purpose for the L2 Interface Policy.
   c) To create an interface policy that enables Q-in-Q encapsulation, in the QinQ field, click doubleQtagPort.
   d) Click Submit.
4. Apply the L2 Interface policy to a Policy Group with the following steps:
   a) Click on Fabric > External Access Policies > Interfaces > Leaf Interfaces, and expand Policy Groups.
   b) Right-click Leaf Access Port, PC Interface, or VPC Interface and choose one of the following, depending on the type of interface you are configuring for the tunnel.
      - Create Leaf Access Port Policy Group
      - Create PC Policy Group
      - Create VPC Policy Group
c) In the resulting dialog box, enter the policy group name, choose the L2 Interface policy that you previously created, and click Submit.

**Step 5** Create a Leaf Interface Profile with the following steps:

a) Click on Fabric > External Access Policies > Interface > Leaf Interfaces > Profiles.
b) Right-click on Leaf Profiles, choose Create Leaf Interface Policy, and perform the following steps:
   • In the Name field, type a name for the Leaf Interface Profile.
     Optional. Add a description.
   • On the Interface Selectors field, click the +, and enter the following information:
     • In the Name field, type a name for the interface selector.
       Optional. Add a description.
     • Enter the selector name, and optionally, a description.
     • In the Interface IDs field, enter the interface or multiple interfaces to be included in the profile.
     • In the Interface Policy Group field, choose the interface policy group that you previously created.

---

**Mapping an EPG to a Q-in-Q Encapsulation-Enabled Interface Using the GUI**

You can associate EPGs with Q-in-Q encapsulation-enabled interfaces in one of the following models:

• Deploy a static EPG on specific Q-in-Q encapsulation-enabled interfaces
• Synchronously link an EPG with a Q-in-Q encapsulation-enabled leaf switch
• Associate an EPG with a Q-in-Q encapsulation-enabled endpoint (with a static MAC address)

All three tasks are performed in the same area of the APIC GUI.

**Before you begin**

• Create the tenant, application profile, and application EPG that will be mapped with an interface configured for Q-in-Q mode.
• The target interfaces should be configured for Q-in-Q encapsulation.

**Procedure**

**Step 1** In the menu bar, click Tenants > tenant-name.

**Step 2** In the Navigation pane, expand Application Profiles > application-profile-name > Application EPGs > application-EPG-name.

**Step 3** To deploy a static EPG on an interface, PC, or VPC that has been enabled for Q-in-Q mode, perform the following steps:
a) Under the application EPG, right-click Static Ports and choose Deploy Static EPG on PC, VPC, or Interface.
b) Choose the path type, the node, and the path to the Q-in-Q enabled interface.
c) On the Port Encap (or Secondary VLAN for Micro-Seg) field, choose QinQ and enter the outer and inner VLAN tags for traffic mapped to the EPG.
d) Click Submit.

Step 4
To statically link an EPG with a node enabled with Q-in-Q mode, perform the following steps:
a) Under the application EPG, right-click Static Leafs and choose Statically Link With Node.
b) In the Node field, choose the Q-in-Q-enabled switches from the list.
c) On the Encap field, choose QinQ and enter the outer and inner VLAN tags for the EPG.
d) Click Submit.

Step 5
To associate an EPG with a static endpoint, perform the following steps:
a) Under the application EPG, right-click Static EndPoints and choose Create Static EndPoint.
b) Enter the MAC address of the interface.
c) Choose the path type, node, and path to the Q-in-Q encapsulation-enabled interface.
d) Optional. Add IP addresses for the endpoint.
e) On the Encap field, choose QinQ and enter the outer and inner VLAN tags.
f) Click Submit.

Mapping EPGs to Q-in-Q Encapsulated Leaf Interfaces Using the NX-OS Style CLI

Enable an interface for Q-in-Q encapsulation and associate the interface with an EPG.

Before you begin
Create the tenant, application profile, and application EPG that will be mapped with an interface configured for Q-in-Q mode.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>apic1# configure</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>leaf number</td>
<td>Specifies the leaf to be configured.</td>
</tr>
<tr>
<td>Example:</td>
<td>apic1(config)# leaf 101</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface ethernet slot/port</td>
<td>Specifies the interface to be configured.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><code>apic1 (config-leaf)# interface ethernet 1/25</code></td>
<td>Enables an interface for Q-in-Q encapsulation.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>switchport mode dot1q-tunnel doubleQtagPort</code> <strong>Example:</strong> <code>apic1(config-leaf-if)# switchport mode dot1q-tunnel doubleQtagPort</code></td>
<td>Enables an interface for Q-in-Q encapsulation.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>switchport trunk qinq outer-vlan vlan-number inner-vlan vlan-number tenant tenant-name application application-name epg epg-name</code> <strong>Example:</strong> <code>apic1(config-leaf-if)# switchport trunk qinq outer-vlan 202 inner-vlan 203 tenant tenant64 application AP64 epg EPG64</code></td>
<td>Associates the interface with an EPG.</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

The following example enables Q-in-Q encapsulation (with outer-VLAN ID 202 and inner-VLAN ID 203) on the leaf interface 101/1/25, and associates the interface with EPG64.

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/25
apic1(config-leaf-if)# switchport mode dot1q-tunnel doubleQtagPort
apic1(config-leaf-if)# switchport trunk qinq outer-vlan 202 inner-vlan 203 tenant tenant64 application AP64 epg EPG64
```

---

## Mapping EPGs to Q-in-Q Encapsulation Enabled Interfaces Using the REST API

### Before you begin

Create the tenant, application profile, and application EPG that will be mapped with an interface configured for Q-in-Q mode.

### Procedure

Enable an interface for Q-in-Q encapsulation and associate the interface with an EPG, with XML such as the following example:

**Example:**

```xml
<polUni>
  <fvTenant dn="uni/tn-tenant64" name="tenant64">
    <fvCtx name="VRF64"/>
    <fvBD name="BD64_1">
      <fvRsCtx tnFvCtxName="VRF64"/>
      <fvRsSct context="tenant64">
        <fvRsSct name="application AP64">
          <fvRsSct name="epg EPG64">
```

---

200 Cisco APIC Layer 2 Networking Configuration Guide
Q-in-Q Encapsulation Mapping for EPGs

Mapping EPGs to Q-in-Q Encapsulation Enabled Interfaces Using the REST API

```xml
<fvSubnet ip="20.0.1.2/24"/>
</fvBD>
<fvAp name="AP64">
  <fvAEPg name="WEB7">
    <fvRsBd tnFvBDName="BD64_1"/>
    <fvRsQinqPathAtt tnDn="topology/pod-1/paths-101/pathep-[eth1/25]" encap="qinq-202-203"/>
  </fvAEPg>
</fvAp>
</fvTenant>
</polUni>
```
CHAPTER 12

Dynamic Breakout Ports

This chapter contains the following sections:

• Configuration of Dynamic Breakout Ports, on page 203
• Configuring Dynamic Breakout Ports Using the APIC GUI, on page 204
• Configuring Dynamic Breakout Ports Using the NX-OS Style CLI, on page 207
• Configuring Dynamic Breakout Ports Using the REST API, on page 210

Configuration of Dynamic Breakout Ports

Breakout cables are suitable for very short links and offer a cost effective way to connect within racks and across adjacent racks.

Breakout enables a 40 Gigabit (Gb) port to be split into four independent and logical 10Gb ports or a 100Gb port to be split into four independent and logical 25Gb ports.

Before you configure breakout ports, connect a 40Gb port to four 10Gb ports or a 100Gb port to four 25Gb ports with one of the following cables:

• Cisco QSFP-4SFP10G
• Cisco QSFP-4SFP25G

The 40Gb to 10Gb dynamic breakout feature is supported on the access facing ports of the following switches:

• N9K-C9332PQ
• N9K-C93180LC-EX
• N9K-C9336C-FX

The 100Gb to 25Gb breakout feature is supported on the access facing ports of the following switches:

• N9K-C93180LC-EX
• N9K-C9336C-FX2
• N9K-C93180YC-FX

Observe the following guidelines and restrictions:
• In general, breakouts and port profiles (ports changed from uplink to downlink) are not supported on the same port.

However, from Cisco APIC, Release 3.2, dynamic breakouts (both 100Gb and 40Gb) are supported on profilled QSFP ports on the N9K-C93180YC-FX switch.

• Fast Link Failover policies are not supported on the same port with the dynamic breakout feature.

• Breakout subports can be used in the same way other port types in the policy model are used.

• When a port is enabled for dynamic breakout, other policies (expect monitoring policies) on the parent port are no longer valid.

• When a port is enabled for dynamic breakout, other EPG deployments on the parent port are no longer valid.

• A breakout sub-port can not be further broken out using a breakout policy group.

Configuring Dynamic Breakout Ports Using the APIC GUI

Configure a Breakout Leaf Port with a Leaf Interface Profile, associate the profile with a switch, and configure the sub ports with the following steps.

**Procedure**

**Before you begin**

• The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.

• An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.

• The target leaf switches are registered in the ACI fabric and available.

• The 40GE or 100GE leaf switch ports are connected with Cisco breakout cables to the downlink ports.

**Procedure**

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

**Step 2** In the Navigation pane, expand Interfaces and Leaf Interfaces and Profiles.

**Step 3** Right-click Profiles and choose Create Leaf Interface Profile.

**Step 4** Type the name and optional description, click the + symbol on Interface Selectors.

**Step 5** Perform the following:

a) Type a name (and optional description) for the Access Port Selector.
b) In the **Interface IDs** field, type the slot and port for the breakout port.

c) In the **Interface Policy Group** field, click the down arrow and choose Create Leaf Breakout Port Group.

d) Type the name (and optional description) for the **Leaf Breakout Port Group**.

e) In the **Breakout Map** field, choose `10g-4x` or `25g-4x`.

   For switches supporting breakout, see Configuration of Dynamic Breakout Ports, on page 203.

f) Click **Submit**.

**Step 6**

To assign a Breakout Port to an EPG, perform the following steps:

On the menu bar, choose **Tenant > Application Profiles > Application EPG**. Right-click on **Application EPG** to open Create Application EPG dialog box, and perform the following steps:

a) Select the **Statically Link with Leaves/Paths** check box to gain access to the **Leaves/Paths** tab in the dialog box.

b) Complete one of the following sets of steps:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want to deploy</td>
<td><strong>Then</strong></td>
</tr>
<tr>
<td>the EPG on...</td>
<td></td>
</tr>
<tr>
<td>A node</td>
<td>1. Expand the <strong>Leaves</strong> area.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Node</strong> drop-down list, choose a node.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Encap</strong> field, enter the appropriate VLAN.</td>
</tr>
<tr>
<td></td>
<td>4. (Optional) From the <strong>Deployment Immediacy</strong> drop-down list, accept the</td>
</tr>
<tr>
<td></td>
<td>default <strong>On Demand</strong> or choose <strong>Immediate</strong>.</td>
</tr>
<tr>
<td></td>
<td>5. (Optional) From the Mode drop-down list, accept the default <strong>Trunk</strong> or</td>
</tr>
<tr>
<td></td>
<td>choose another mode.</td>
</tr>
<tr>
<td>A port on the node</td>
<td>1. Expand the <strong>Paths</strong> area.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Path</strong> drop-down list, choose the appropriate node and port.</td>
</tr>
<tr>
<td></td>
<td>3. (Optional) In the <strong>Deployment Immediacy</strong> field drop-down list, accept</td>
</tr>
<tr>
<td></td>
<td>the default <strong>On Demand</strong> or choose <strong>Immediate</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. (Optional) From the Mode drop-down list, accept the default <strong>Trunk</strong> or</td>
</tr>
<tr>
<td></td>
<td>choose another mode.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Port Encap</strong> field, enter the secondary VLAN to be deployed.</td>
</tr>
<tr>
<td></td>
<td>6. (Optional) In the <strong>Primary Encap</strong> field, enter the primary VLAN to be</td>
</tr>
<tr>
<td></td>
<td>deployed.</td>
</tr>
</tbody>
</table>

**Step 7**

To associate the Leaf Interface Profile to a the leaf switch, perform the following steps:

a) Expand **Switches** and **Leaf Switches**, and **Profiles**.

b) Right-click **Profiles** and select Create Leaf Profiles.

c) Type the name and optional description of the Leaf Profile.

d) Click the + symbol on the **Leaf Selectors** area.

e) Type the leaf selector name and an optional description.
f) Click the down arrow on the **Blocks** field and choose the switch to be associated with the breakout leaf interface profile.

g) Click the down arrow on the **Policy Group** field and choose **Create Access Switch Policy Group**.

h) Type a name and optional description for the Access Switch Policy Group.

i) Optional. Enable other policies.

j) Click **Submit**.

k) Click **Update**.

l) Click **Next**.

m) In the **Associations Interface Selector Profiles** area, choose the Interface Selector Profile you previously created for the breakout port.

n) Click **Finish**.

**Step 8**

To verify the breakout port has been split into four sub ports, perform the following steps:

a) On the Menu bar, click **Fabric > Inventory**.

b) On the Navigation bar, click the Pod and Leaf where the breakout port is located.

c) Expand **Interfaces** and **Physical Interfaces**. You should see four ports at the position where the breakout port was configured. For example, if you configured 1/10 as a breakout port, you should see the following:

   • eth1/10/1
   • eth1/10/2
   • eth1/10/3
   • eth1/10/4

**Step 9**

To configure the sub ports, perform the following steps:

a) On the Menu bar, click **Fabric > External Access Policies**.

b) On the Navigation bar, expand **Interfaces**, **Leaf Interfaces**, **Profiles**, and the breakout leaf interface profile you previously created.

c) Click the Breakout Port Access Port Selector profile you previously created.

d) On the **Sub Port Blocks** area, click the + symbol.

e) In the **Interface IDs** field, enter the IDs for the four sub ports in a format such as 1/10/1-4.

f) Click **Submit**.

**Step 10**

To apply the Policy Group to an individual interface which links the AAEP to the port, perform the following steps:

a) Navigate to **Interfaces > Leaf Interfaces > Profiles** and right-click to open **Create Access Port Selector**.

b) In the **Name** field, select a name for the breakout Access Port Selector policy.

c) In the **Interface Policy Group** field, select **Create Leaf Access Port Policy Group**.

d) In the **Name** field, select a name for the breakout Leaf Access Port Group Policy.

e) In the **Attached Entity Profile** field, select the AAEP profile to attach to the policy group.

f) Click **Submit**.
# Configuring Dynamic Breakout Ports Using the NX-OS Style CLI

Use the following steps to configure a breakout port, verify the configuration, and configure an EPG on a sub port, using the NX-OS style CLI.

## Before you begin

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
- The target leaf switches are registered in the ACI fabric and available.
- The 40GE or 100GE leaf switch ports are connected with Cisco breakout cables to the downlink ports.

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>leaf ID</td>
<td>Selects the leaf switch where the breakout port will be located and enters leaf configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config)# leaf 101</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface ethernet slot/port</td>
<td>Identifies the interface to be enabled as a 40 Gigabit Ethernet (GE) breakout port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config-leaf)# interface ethernet 1/16</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>breakout 10g-4x</td>
<td>Enables the selected interface for breakout.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config-leaf-if)# breakout 10g-4x</td>
<td><strong>Note</strong> For switch support for the Dynamic Breakout Port feature, see Configuration of Dynamic Breakout Ports, on page 203.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show run</td>
<td>Verifies the configuration by showing the running configuration of the interface and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config-leaf-if)# show run</td>
<td></td>
</tr>
<tr>
<td># Command: show running-config leaf 101</td>
<td></td>
<td></td>
</tr>
<tr>
<td>leaf 101</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface ethernet 1/16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>breakout 10g-4x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf-if)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apic1(config-leaf)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>tenant tenant-name</td>
<td>Selects or creates the tenant that will consume the breakout ports and enters tenant configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config)# tenant tenant64</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>vrf context vrf-name</td>
<td>Creates or identifies the Virtual Routing and Forwarding (VRF) instance associated with the tenant and exits the configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config-tenant)# vrf context vrf64</td>
<td>apic1(config-tenant-vrf)# exit</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>bridge-domain bridge-domain-name</td>
<td>Creates or identifies the bridge-domain associated with the tenant and enters BD configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config-tenant)# bridge-domain bd64</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>vrf member vrf-name</td>
<td>Associates the VRF with the bridge-domain and exits the configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config-tenant-bd)# vrf member vrf64</td>
<td>apic1(config-tenant-bd)# exit</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>application application-profile-name</td>
<td>Creates or identifies the application profile associated with the tenant and the EPG.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config-tenant)# application app64</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>epg epg-name</td>
<td>Creates or identifies the EPG and enters into EPG configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config-tenant)# epg epg64</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>bridge-domain member bridge-domain-name</td>
<td>Associates the EPG with the bridge domain and returns to global configuration mode. Configure the sub ports as desired, for example, use the speed command in leaf interface mode to configure a sub port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config-tenant-app-epg)# bridge-domain member bd64</td>
<td>apic1(config-tenant-app-epg)# exit</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>leaf leaf-name</td>
<td>Associates the EPG with a break-out port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>apic1(config)# leaf 1017</td>
<td>apic1(config-leaf)# interface ethernet 1/13</td>
</tr>
</tbody>
</table>
### Purpose

The `vlan-domain` and `vlan-domain member` commands mentioned in the above example are a prerequisite for deploying an EPG on a port.

### Command or Action

<table>
<thead>
<tr>
<th>Note</th>
<th>The <code>vlan-domain</code> and <code>vlan-domain member</code> commands mentioned in the above example are a prerequisite for deploying an EPG on a port.</th>
</tr>
</thead>
</table>

### Step 14

**speed** *interface-speed*

**Example:**

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/16/1
apic1(config-leaf-if)# speed 10G
apic1(config-leaf-if)# exit
```

**Enters leaf interface mode, sets the speed of an interface, and exits the configuration mode.**

### Step 15

**show run**

**Example:**

```
apic1(config-leaf)# show run
```

**After you have configured the sub ports, entering this command in leaf configuration mode displays the sub port details.**

The port on leaf 101 at interface 1/16 is confirmed enabled for breakout with sub ports 1/16/1, 1/16/2, 1/16/3, and 1/16/4.

### Example

This example configures the port for breakout:

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/16
apic1(config-leaf-if)# breakout 10g-4x
```

This example configures the EPG for the sub ports.

```
apic1(config)# tenant tenant64
apic1(config-tenant)# vrf context vrf64
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# bridge-domain bd64
apic1(config-tenant-bd)# vrf member vrf64
apic1(config-tenant-bd)# exit
apic1(config-tenant)# application app64
apic1(config-tenant-app)# epg epg64
apic1(config-tenant-app-epg)# bridge-domain member bd64
apic1(config-tenant-app-epg)# end
```

This example sets the speed for the breakout sub ports to 10G.

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/16/1
apic1(config-leaf-if)# speed 10G
apic1(config-leaf-if)# exit

apic1(config-leaf)# interface ethernet 1/16/2
apic1(config-leaf-if)# speed 10G
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/16/3
apic1(config-leaf-if)# speed 10G
```

---

Dynamic Breakout Ports

Configuring Dynamic Breakout Ports Using the NX-OS Style CLI

---

Cisco APIC Layer 2 Networking Configuration Guide

209
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/16/4
apic1(config-leaf-if)# speed 10G
apic1(config-leaf-if)# exit

This example shows the four sub ports connected to leaf 101, interface 1/16.

apic1#(config-leaf)# show run
  # Command: show running-config leaf 101
  # Time: Fri Dec 2 00:51:08 2016
  leaf 101
    interface ethernet 1/16/1
      speed 10G
      negotiate auto
      link debounce time 100
      exit
    interface ethernet 1/16/2
      speed 10G
      negotiate auto
      link debounce time 100
      exit
    interface ethernet 1/16/3
      speed 10G
      negotiate auto
      link debounce time 100
      exit
    interface ethernet 1/16/4
      speed 10G
      negotiate auto
      link debounce time 100
      exit
    interface ethernet 1/16
      breakout 10g-4x
      exit
    interface vfc 1/16

Configuring Dynamic Breakout Ports Using the REST API

Configure a Breakout Leaf Port with an Leaf Interface Profile, associate the profile with a switch, and configure the sub ports with the following steps.

For switch support for the breakout feature, see Configuration of Dynamic Breakout Ports, on page 203.

Procedure

Before you begin

- The ACI fabric is installed, APIC controllers are online, and the APIC cluster is formed and healthy.
- An APIC fabric administrator account is available that will enable creating the necessary fabric infrastructure configurations.
- The target leaf switches are registered in the ACI fabric and available.
- The 40GE or 100GE leaf switch ports are connected with Cisco breakout cables to the downlink ports.
## Procedure

### Step 1
Configure a breakout policy group for the breakout port with JSON, such as the following example:

**Example:**

In this example, we create an interface profile 'brkout44' with the only port 44 underneath its port selector. The port selector is pointed to a breakout policy group 'new-brkoutPol'.

```json
{
    "infraAccPortP": {
        "attributes": {
            "dn": "uni/infra/accportprof-brkout44",
            "name": "brkout44",
            "rn": "accportprof-brkout44",
            "status": "created,modified"
        },
        "children": [{
            "infraHPortS": {
                "attributes": {
                    "dn": "uni/infra/accportprof-brkout44/hports-new-brekoutPol-typ-range",
                    "name": "new-brkoutPol",
                    "rn": "hports-new-brkoutPol-typ-range",
                    "status": "created,modified"
                },
                "children": [{
                    "infraPortBlk": {
                        "attributes": {
                            "dn": "uni/infra/accportprof-brkout44/hports-new-brkoutPol-typ-range/portblk-block2",
                            "fromPort": "44",
                            "toPort": "44",
                            "name": "block2",
                            "rn": "portblk-block2",
                            "status": "created,modified"
                        }
                    }
                },
                "infraRsAccBaseGrp": {
                    "attributes": {
                        "tDn": "uni/infra/funcprof/brkoutportgrp-new-brkoutPol",
                        "status": "created,modified"
                    },
                    "children": []
                }
            }
        }]
    }
}
```

### Step 2
Create a new switch profile and associate it with the port profile, previously created, with JSON such as the following example:

**Example:**

In this example, we create a new switch profile 'leaf1017' with switch 1017 as the only node. We associate this new switch profile with the port profile 'brkout44' created above. After this, the port 44 on switch 1017 will have 4 sub ports.
Example:

```json
{
  "infraNodeP": {
    "attributes": {
      "dn": "uni/infra/nprof-leaf1017",
      "name": "leaf1017",
      "rn": "nprof-leaf1017",
      "status": "created,modified"
    },
    "children": [
      {
        "infraLeafS": {
          "attributes": {
            "dn": "uni/infra/nprof-leaf1017/leaves-1017-typ-range",
            "type": "range",
            "name": "1017",
            "rn": "leaves-1017-typ-range",
            "status": "created"
          },
          "children": [
            {
              "infraNodeBlk": {
                "attributes": {
                  "dn": "uni/infra/nprof-leaf1017/leaves-1017-typ-range/nodeblk-102bf7dc60e63f7e",
                  "from": "1017",
                  "to": "1017",
                  "name": "102bf7dc60e63f7e",
                  "rn": "nodeblk-102bf7dc60e63f7e",
                  "status": "created"
                },
                "children": []
              }
            }
          ]
        }
      },
      {
        "infraRsAccPortP": {
          "attributes": {
            "tDn": "uni/infra/accportprof-brkout44",
            "status": "created,modified"
          },
          "children": []
        }
      }
    ]
  }
}
```

Step 3 Configure the subports.

Example:

This example configures subports 1/44/1, 1/44/2, 1/44/3, 1/44/4 on switch 1017, for instance, in the example below, we configure interface 1/44/3. It also creates the `infraSubPortBlk` object instead of the `infraPortBlk` object.

```json
{
  "infraAccPortP": {
    "attributes": {
      "dn": "uni/infra/accportprof-brkout44",
      "name": "brkouttest1",
      "rn": "accportprof-brkout44",
      "status": "created,modified"
    },
    "children": []
  }
}
```
Step 4 Deploy an EPG on a specific port.

Example:

```xml
<fvTenant name="<tenant_name>" dn="uni/tn-test1">
  <fvCtx name="<network_name>" pcEnfPref="enforced" knwMcastAct="permit"/>
  <fvBD name="<bridge_domain_name>" unkMcastAct="flood">
    <fvRsCtx tnFvCtxName="<network_name/>">
  </fvBD>
  <fvAp name="<application_profile>">
    <fvAEPg name="<epg_name>">
      <fvRsPathAtt tDn="topology/pod-1/paths-1017/pathep-[eth1/13]" mode="regular" instrImedcy="immediate" encap="vlan-20"/>
    </fvAEPg>
  </fvAp>
</fvTenant>
```
Proxy ARP

This chapter contains the following sections:

- About Proxy ARP, on page 215
- Guidelines and Limitations, on page 221
- Proxy ARP Supported Combinations, on page 221
- Configuring Proxy ARP Using the Advanced GUI, on page 222
- Configuring Proxy ARP Using the Cisco NX-OS Style CLI, on page 222
- Configuring Proxy ARP Using the REST API, on page 224

About Proxy ARP

Proxy ARP in Cisco ACI enables endpoints within a network or subnet to communicate with other endpoints without knowing the real MAC address of the endpoints. Proxy ARP is aware of the location of the traffic destination, and offers its own MAC address as the final destination instead.

To enable Proxy ARP, intra-EPG endpoint isolation must be enabled on the EPG see the following figure for details. For more information about intra-EPG isolation and Cisco ACI, see the Cisco ACI Virtualization Guide.
Proxy ARP within the Cisco ACI fabric is different from the traditional proxy ARP. As an example of the communication process, when proxy ARP is enabled on an EPG, if an endpoint A sends an ARP request for endpoint B and if endpoint B is learned within the fabric, then endpoint A will receive a proxy ARP response from the bridge domain (BD) MAC. If endpoint A sends an ARP request for endpoint B, and if endpoint B is not learned within the ACI fabric already, then the fabric will send a proxy ARP request within the BD. Endpoint B will respond to this proxy ARP request back to the fabric. At this point, the fabric does not send a proxy ARP response to endpoint A, but endpoint B is learned within the fabric. If endpoint A sends another ARP request to endpoint B, then the fabric will send a proxy ARP response from the BD MAC.

The following example describes the proxy ARP resolution steps for communication between clients VM1 and VM2:

1. VM1 to VM2 communication is desired.
Figure 28: VM1 to VM2 Communication is Desired.

Table 14: ARP Table State

<table>
<thead>
<tr>
<th>Device</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>IP = * MAC = *</td>
</tr>
<tr>
<td>ACI fabric</td>
<td>IP = * MAC = *</td>
</tr>
<tr>
<td>VM2</td>
<td>IP = * MAC = *</td>
</tr>
</tbody>
</table>

2. VM1 sends an ARP request with a broadcast MAC address to VM2.

Figure 29: VM1 sends an ARP Request with a Broadcast MAC address to VM2
Table 15: ARP Table State

<table>
<thead>
<tr>
<th>Device</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>IP = VM2 IP; MAC = ?</td>
</tr>
<tr>
<td>ACI fabric</td>
<td>IP = VM1 IP; MAC = VM1 MAC</td>
</tr>
<tr>
<td>VM2</td>
<td>IP = * MAC = *</td>
</tr>
</tbody>
</table>

3. The ACI fabric floods the proxy ARP request within the bridge domain (BD).

Figure 30: ACI Fabric Floods the Proxy ARP Request within the BD

Table 16: ARP Table State

<table>
<thead>
<tr>
<th>Device</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>IP = VM2 IP; MAC = ?</td>
</tr>
<tr>
<td>ACI fabric</td>
<td>IP = VM1 IP; MAC = VM1 MAC</td>
</tr>
<tr>
<td>VM2</td>
<td>IP = VM1 IP; MAC = BD MAC</td>
</tr>
</tbody>
</table>

4. VM2 sends an ARP response to the ACI fabric.
Figure 31: VM2 Sends an ARP Response to the ACI Fabric

Table 17: ARP Table State

<table>
<thead>
<tr>
<th>Device</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>IP = VM2 IP; MAC = ?</td>
</tr>
<tr>
<td>ACI fabric</td>
<td>IP = VM1 IP; MAC = VM1 MAC</td>
</tr>
<tr>
<td>VM2</td>
<td>IP = VM1 IP; MAC = BD MAC</td>
</tr>
</tbody>
</table>

5. VM2 is learned.

Figure 32: VM2 is Learned
**Table 18: ARP Table State**

<table>
<thead>
<tr>
<th>Device</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>IP = VM2 IP; MAC = ?</td>
</tr>
<tr>
<td>ACI fabric</td>
<td>IP = VM1 IP; MAC = VM1 MAC</td>
</tr>
<tr>
<td></td>
<td>IP = VM2 IP; MAC = VM2 MAC</td>
</tr>
<tr>
<td>VM2</td>
<td>IP = VM1 IP; MAC = BD MAC</td>
</tr>
</tbody>
</table>

6. VM1 sends an ARP request with a broadcast MAC address to VM2.

*Figure 33: VM1 Sends an ARP Request with a Broadcast MAC Address to VM2*

**Table 19: ARP Table State**

<table>
<thead>
<tr>
<th>Device</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>IP = VM2 IP MAC = ?</td>
</tr>
<tr>
<td>ACI fabric</td>
<td>IP = VM1 IP MAC = VM1 MAC</td>
</tr>
<tr>
<td></td>
<td>IP = VM2 IP MAC = VM2 MAC</td>
</tr>
<tr>
<td>VM2</td>
<td>IP = VM1 IP MAC = BD MAC</td>
</tr>
</tbody>
</table>

Figure 34: ACI Fabric Sends a Proxy ARP Response to VM1

Table 20: ARP Table State

<table>
<thead>
<tr>
<th>Device</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>IP = VM2 IP; MAC = BD MAC</td>
</tr>
<tr>
<td>ACI fabric</td>
<td>IP = VM1 IP; MAC = VM1 MAC</td>
</tr>
<tr>
<td></td>
<td>IP = VM2 IP; MAC = VM2 MAC</td>
</tr>
<tr>
<td>VM2</td>
<td>IP = VM1 IP; MAC = BD MAC</td>
</tr>
</tbody>
</table>

Guidelines and Limitations

Consider these guidelines and limitations when using Proxy ARP:

- Proxy ARP is supported only on isolated EPGs. If an EPG is not isolated, a fault will be raised. For communication to happen within isolated EPGs with proxy ARP enabled, you must configure uSeg EPGs. For example, within the isolated EPG, there could be multiple VMs with different IP addresses, and you can configure a uSeg EPG with IP attributes matching the IP address range of these VMs.

- ARP requests from isolated endpoints to regular endpoints and from regular endpoints to isolated endpoints do not use proxy ARP. In such cases, endpoints communicate using the real MAC addresses of destination VMs.

Proxy ARP Supported Combinations

The following proxy ARP table provides the supported combinations:
### Configuring Proxy ARP Using the Advanced GUI

#### Before you begin
- The appropriate tenant, VRF, bridge domain, application profile and EPG must be created.
- Intra-EPG isolation must be enabled on the EPG where proxy ARP has to be enabled.

#### Procedure

**Step 1**  
On the menubar, click Tenant > Tenant_name.

**Step 2**  
In the Navigation pane, expand the Tenant_name > Application Profiles > Application_Profile_name > Application EPGs, right click Create Application EPG dialog box to perform the following actions in the Create Application EPG dialog box:
- In the Name field, add an EPG name.

**Step 3**  
In the Intra EPG Isolation field, choose Enforced.  
When Intra EPG isolation is enforced, the Forwarding Control field becomes available.

**Step 4**  
In the Forwarding Control field, check the check box for proxy-arp.  
This enables proxy-arp.

**Step 5**  
In the Bridge Domain field, choose the appropriate bridge domain to associate from the drop-down list.

**Step 6**  
Choose the remaining fields in the dialog box as appropriate, and click Finish.

### Configuring Proxy ARP Using the Cisco NX-OS Style CLI

#### Before you begin
- The appropriate tenant, VRF, bridge domain, application profile and EPG must be created.
- Intra-EPG isolation must be enabled on the EPG where proxy ARP has to be enabled.
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Example: apic1# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> tenant tenant-name</td>
<td>Enters the tenant configuration mode.</td>
</tr>
<tr>
<td>Example: apic1(config)# tenant Tenant1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> application application-profile-name</td>
<td>Creates an application profile and enters the application mode.</td>
</tr>
<tr>
<td>Example: apic1(config-tenant)# application Tenant1-App</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> epg application-profile-EPG-name</td>
<td>Creates an EPG and enter the EPG mode.</td>
</tr>
<tr>
<td>Example: apic1(config-tenant-app)# epg Tenant1-epg1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> proxy-arp enable</td>
<td>Enables proxy ARP.</td>
</tr>
<tr>
<td>Example: apic1(config-tenant-app-epg)# proxy-arp enable</td>
<td><strong>Note</strong> You can disable proxy-arp with the no proxy-arp command.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Returns to application profile mode.</td>
</tr>
<tr>
<td>Example: apic1(config-tenant-app-epg)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Returns to tenant configuration mode.</td>
</tr>
<tr>
<td>Example: apic1(config-tenant-app)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example: apic1(config-tenant)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure proxy ARP.

```
apic1# conf t
apic1(config)# tenant Tenant1
apic1(config-tenant)# application Tenant1-App
```
Configuring Proxy ARP Using the REST API

Before you begin

- Intra-EPG isolation must be enabled on the EPG where proxy ARP has to be enabled.

Procedure

Configure proxy ARP.

Example:

```xml
<polUni>
  <fvTenant name="Tenant1" status="">
    <fvCtx name="EngNet"/>
    <!-- bridge domain -->
    <fvBD name="BD1">
      <fvRsCtx tnFvCtxName="EngNet"/>
      <fvSubnet ip="1.1.1.1/24"/>
    </fvBD>
    <fvAp name="Tenant1_app">
      <fvAEPg name="Tenant1_epg" pcEnfPref="enforced" fwdCtrl="proxy-arp">
        <fvRsBd tnFvBDName="BD1"/>
        <fvRsDomAtt tDn="uni/vmmp-VMware/dom-dom9"/>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```
Traffic Storm Control

This chapter contains the following sections:

- About Traffic Storm Control, on page 225
- Storm Control Guidelines, on page 225
- Configuring a Traffic Storm Control Policy Using the GUI, on page 226
- Configuring a Traffic Storm Control Policy Using the NX-OS Style CLI, on page 228
- Configuring a Traffic Storm Control Policy Using the REST API, on page 229

About Traffic Storm Control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. You can use traffic storm control policies to prevent disruptions on Layer 2 ports by broadcast, unknown multicast, or unknown unicast traffic storms on physical interfaces.

By default, storm control is not enabled in the ACI fabric. ACI bridge domain (BD) Layer 2 unknown unicast flooding is enabled by default within the BD but can be disabled by an administrator. In that case, a storm control policy only applies to broadcast and unknown multicast traffic. If Layer 2 unknown unicast flooding is enabled in a BD, then a storm control policy applies to Layer 2 unknown unicast flooding in addition to broadcast and unknown multicast traffic.

Traffic storm control (also called traffic suppression) allows you to monitor the levels of incoming broadcast, multicast, and unknown unicast traffic over a one second interval. During this interval, the traffic level, which is expressed either as percentage of the total available bandwidth of the port or as the maximum packets per second allowed on the given port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends. An administrator can configure a monitoring policy to raise a fault when a storm control threshold is exceeded.

Storm Control Guidelines

Configure traffic storm control levels according to the following guidelines and limitations:

- Typically, a fabric administrator configures storm control in fabric access policies on the following interfaces:
  - A regular trunk interface.
• A direct port channel on a single leaf switch.

• A virtual port channel (a port channel on two leaf switches).

• For port channels and virtual port channels, the storm control values (packets per second or percentage) apply to all individual members of the port channel. Do not configure storm control on interfaces that are members of a port channel.

**Note**

On switch hardware starting with the APIC 1.3(x) and switch 11.3(x) release, for port channel configurations, the traffic suppression on the aggregated port may be up to two times the configured value. The new hardware ports are internally subdivided into these two groups: slice-0 and slice-1. To check the slicing map, use the `vsh lc command show platform internal hal 12 port gpd` and look for `slice 0` or `slice 1` under the `Sl` column. If port-channel members fall on both slice-0 and slice-1, allowed storm control traffic may become twice the configured value because the formula is calculated based on each slice.

• When configuring by percentage of available bandwidth, a value of 100 means no traffic storm control and a value of 0.01 suppresses all traffic.

• Due to hardware limitations and the method by which packets of different sizes are counted, the level percentage is an approximation. Depending on the sizes of the frames that make up the incoming traffic, the actual enforced level might differ from the configured level by several percentage points. Packets-per-second (PPS) values are converted to percentage based on 256 bytes.

• Maximum burst is the maximum accumulation of rate that is allowed when no traffic passes. When traffic starts, all the traffic up to the accumulated rate is allowed in the first interval. In subsequent intervals, traffic is allowed only up to the configured rate. The maximum supported is 65535 KB. If the configured rate exceeds this value, it is capped at this value for both PPS and percentage.

• The maximum burst that can be accumulated is 512 MB.

• On an egress leaf switch in optimized multicast flooding (OMF) mode, traffic storm control will not be applied.

• On an egress leaf switch in non-OMF mode, traffic storm control will be applied.

• On a leaf switch for FEX, traffic storm control is not available on host-facing interfaces.

• Traffic storm control unicast/multicast differentiation is not supported on Cisco Nexus C93128TX, C9396PX, C9396TX, C93120TX, C9332PQ, C9372PX, C9372TX, C9372PX-E, or C9372TX-E switches.

## Configuring a Traffic Storm Control Policy Using the GUI

**Procedure**

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

**Step 2** In the submenu bar, click **External Access Policies**.
Step 3: In the Navigation pane, expand Policies.

Step 4: Expand Interface.

Step 5: Right-click Storm Control and choose Create Storm Control Interface Policy.

Step 6: In the Create Storm Control Interface Policy dialog box, enter a name for the policy in the Name field.

Step 7: In the Configure Storm Control field, click the radio button for either All Types or Unicast, Broadcast, Multicast.

Note: Selecting the Unicast, Broadcast, Multicast radio button allows you to configure Storm Control on each traffic type separately.

Step 8: In the Specify Policy In field, click the radio button for either Percentage or Packets Per Second.

Step 9: If you chose Percentage, perform the following steps:
   a) In the Rate field, enter a traffic rate percentage.
      Enter a number between 0 and 100 that specifies a percentage of the total available bandwidth of the port. When the ingress traffic is either equal to or greater than this level during a one second interval, traffic storm control drops traffic for the remainder of the interval. A value of 100 means no traffic storm control. A value of 0 suppresses all traffic.
   b) In the Max Burst Rate field, enter a burst traffic rate percentage.
      Enter a number between 0 and 100 that specifies a percentage of the total available bandwidth of the port. When the ingress traffic is equal to or greater than, traffic storm control begins to drop traffic.

Note: The Max Burst Rate should be greater than or equal to the value of Rate.

Step 10: If you chose Packets Per Second, perform the following steps:
   a) In the Rate field, enter a traffic rate in packets per second.
      During this interval, the traffic level, expressed as packets flowing per second through the port, is compared with the traffic storm control level that you configured. When the ingress traffic is equal to or greater than the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.
   b) In the Max Burst Rate field, enter a burst traffic rate in packets per second.
      During this interval, the traffic level, expressed as packets flowing per second through the port, is compared with the burst traffic storm control level that you configured. When the ingress traffic is equal to or greater than the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

Step 11: Click Submit.

Step 12: Apply the storm control interface policy to an interface port.
   a) In the menu bar, click Fabric.
   b) In the submenu bar, click External Access Policies.
   c) In the Navigation pane, expand Interfaces.
   d) Expand Leaf Interfaces.
   e) Expand Policy Groups.
   f) Select Leaf Policy Groups.

Note: If your APIC version is earlier than 2.x, you select Policy Groups.
Select the leaf access port policy group, the PC interface policy group, the VPC interface policy group, or the PC/VPC override policy group to which you want to apply the storm control policy.

In the Work pane, click the drop down for Storm Control Interface Policy and select the created Traffic Storm Control Policy.

Click Submit.

### Configuring a Traffic Storm Control Policy Using the NX-OS Style CLI

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | Enter the following commands to create a PPS policy:  
**Example:**  
(config)# template policy-group pg1  
(config-pol-grp-if)# storm-control pps 10000 burst-rate 10000 |
| **Step 2** | Enter the following commands to create a percent policy:  
**Example:**  
(config)# template policy-group pg2  
(config-pol-grp-if)# storm-control level 50 burst-rate 60 |
| **Step 3** | Configure storm control on physical ports, port channels, or virtual port channels:  
**Example:**  
[no] storm-control  
[unicast|multicast|broadcast] level <percentage> [burst-rate <percentage>]  
[no] storm-control  
[unicast|multicast|broadcast] pps <packet-per-second> [burst-rate <packet-per-second>]  
sd-tb2-ifc1# configure terminal  
sd-tb2-ifc1(config)# leaf 102  
sd-tb2-ifc1(config)# interface ethernet 1/19  
sd-tb2-ifc1(config-leaf)# storm-control unicast level 35 burst-rate 45  
sd-tb2-ifc1(config-leaf)# storm-control broadcast level 36 burst-rate 36 |
Configuring a Traffic Storm Control Policy Using the REST API

To configure a traffic storm control policy, create a `stormctrl:IfPol` object with the desired properties.

To create a policy named MyStormPolicy, send this HTTP POST message:

```plaintext
POST https://192.0.20.123/api/mo/uni/infra/stormctrlifp-MyStormPolicy.json
```

In the body of the POST message, include the following JSON payload structure to specify the policy by percentage of available bandwidth:

```json
{"stormctrlIfPol":
{"attributes":
{"dn":"uni/infra/stormctrlifp-MyStormPolicy",
"name":"MyStormPolicy",
"rate":"75",
"burstRate":"85",
"rn":"stormctrlifp-MyStormPolicy",
"status":"created"
},
"children":[]
}
}
```

In the body of the POST message, include the following JSON payload structure to specify the policy by packets per second:

```json
{"stormctrlIfPol":
{"attributes":
{"dn":"uni/infra/stormctrlifp-MyStormPolicy",
"name":"MyStormPolicy",
"ratePps":"12000",
"burstPps":"15000",
"rn":"stormctrlifp-MyStormPolicy",
"status":"created"
},
"children":[]
}
}
```
Apply the traffic storm control interface policy to an interface port.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<infraInfra status='created,modified'>
  <infraHPathS name='__ui_l101_eth1--3' status='created, modified'>
    <infraRsPathToAccBaseGrp tDn='uni/infra/functprof/accportgrp-__ui_l101_eth1--3' status='created,modified'>
      <infraRsHPathAtt tDn='topology/pod-1/paths-101/pathep-[eth1/3]' status='created,modified'>
    </infraRsHPathAtt>
  </infraHPathS>
</infraInfra>
```

**Cisco APIC Layer 2 Networking Configuration Guide**

230
CHAPTER 15

MACsec

This chapter contains the following sections:

- About MACsec, on page 231
- Guidelines and Limitations for MACsec, on page 232
- Configuring MACsec for Fabric Links Using the GUI, on page 234
- Configuring MACsec for Access Links Using the GUI, on page 234
- Configuring MACsec Parameters Using the APIC GUI, on page 235
- Configuring MACsec Keychain Policy Using the GUI, on page 235
- Configuring MACsec Using the NX-OS Style CLI, on page 236
- Configuring MACsec Using the REST API, on page 238

About MACsec

MACsec is an IEEE 802.1AE standards based Layer 2 hop-by-hop encryption that provides data confidentiality and integrity for media access independent protocols.

MACsec, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys.

The 802.1AE encryption with MKA is supported on all types of links, that is, host facing links (links between network access devices and endpoint devices such as a PC or IP phone), or links connected to other switches or routers.

MACsec encrypts the entire data except for the Source and Destination MAC addresses of an Ethernet packet. The user also has the option to skip encryption up to 50 bytes after the source and destination MAC address.

To provide MACsec services over the WAN or Metro Ethernet, service providers offer Layer 2 transparent services such as E-Line or E-LAN using various transport layer protocols such as Ethernet over Multiprotocol Label Switching (EoMPLS) and L2TPv3.

The packet body in an EAP-over-LAN (EAPOL) Protocol Data Unit (PDU) is referred to as a MACsec Key Agreement PDU (MKPDU). When no MKPDU is received from a participants after 3 hearbeats (each heartbeat is of 2 seconds), peers are deleted from the live peer list. For example, if a client disconnects, the participant on the switch continues to operate MKA until 3 heartbeats have elapsed after the last MKPDU is received from the client.
APIC Fabric MACsec

The APIC will be responsible for the MACsec keychain distribution to all the nodes in a Pod or to particular ports on a node. Below are the supported MACsec keychain and MACsec policy distribution supported by the APIC.

- A single user provided keychain and policy per Pod
- User provided keychain and user provided policy per fabric interface
- Auto generated keychain and user provided policy per Pod

A node can have multiple policies deployed for more than one fabric link. When this happens, the per fabric interface keychain and policy are given preference on the affected interface. The auto generated keychain and associated MACsec policy are then given the least preference.

APIC MACsec supports two security modes. The MACsec **must secure** only allows encrypted traffic on the link while the **should secure** allows both clear and encrypted traffic on the link. Before deploying MACsec in **must secure** mode, the keychain must be deployed on the affected links or the links will go down. For example, a port can turn on MACsec in **must secure** mode before its peer has received its keychain resulting in the link going down. To address this issue the recommendation is to deploy MACsec in **should secure** mode and once all the links are up then change the security mode to **must secure**.

*Note* Any MACsec interface configuration change will result in packet drops.

MACsec policy definition consists of configuration specific to keychain definition and configuration related to feature functionality. The keychain definition and feature functionality definitions are placed in separate policies. Enabling MACsec per Pod or per interface involves deploying a combination of a keychain policy and MACsec functionality policy.

*Note* Using internal generated keychains do not require the user to specify a keychain.

APIC Access MACsec

MACsec is used to secure links between leaf switch L3out interfaces and external devices. APIC provides GUI and CLI to allow users to program the MACsec keys and MacSec configuration for the L3Out interfaces on the fabric on a per physical/pc/vpc interface basis. It is the responsibility of the user to make sure that the external peer devices are programmed with the correct MacSec information.

**Guidelines and Limitations for MACsec**

Configure MACsec according to the following guidelines and limitations:

- Fex ports are not supported for MACsec.
- Must-secure mode is not supported at Pod level.
- A MACsec policy with name ‘default’ is not supported.
- Auto key generation is only supported at the Pod level for fabric ports.
• MACSEC is not supported on Remote Leafs.

• Do not clean reboot a node if the fabric ports of that node is running MACsec in must-secure mode.

• Adding a new node to a Pod or stateless reboot of a node in a Pod which is running MACsec, must-secure mode requires changing the mode to should-secure in order for the node to join the Pod.

• Upgrade/Downgrade should only be initiated if the fabric links are in should-secure mode. Once upgrade/downgrade has completed, then the mode can be changed to must-secure. Upgrading/Downgrading in must-secure mode will result in nodes losing connectivity to the fabric. Recovering from connectivity loss requires that the fabric links of the nodes visible to the APIC be configured to should-secure mode. If the fabric was downgraded to a version which does not support MACsec, then nodes which are out of fabric will need to be clean rebooted.

• For PC/VPC interface, MACsec can be deployed via policy groups per PC/VPC interface. Port selectors are used to deploy the policies to a particular set of ports. Therefore, it is the user’s responsibility to create the right port selector corresponding to the L3Out interfaces.

• It is recommended that MACsec policies be configured to should-secure mode before a configuration is exported.

• All the links on a spine are considered fabric links. However, if a spine link is used for IPN connectivity, then this link will be treated as an access link. This means that MACsec access policy needs to be used to deploy MACsec on these links.

• MACSEC Sessions may take up to a minute to form or tear down when a new key is added to an empty keychain or an active key is deleted from keychain.

Deploying must-secure mode
Incorrect deployment procedure of a policy that is configured for must-secure mode can result in a loss of connectivity. The procedure below should be followed in order to prevent such issues:

• It is necessary to ensure that each link pair has their keychains before enabling MACsec must-secure mode. To ensure this, the recommendation is to deploy the policy in should-secure mode, and once MACsec sessions are active on the expected links, change the mode to must-secure.

• Attempting to replace the keychain on a MACsec policy that is configured to must-secure can cause links to go down. The recommended procedure outlined below should be followed in this case:
  • Change MACsec policy that is using the new keychain to should-secure mode.
  • Verify that the affected interfaces are using should-secure mode.
  • Update MACsec policy to use new keychain.
  • Verify that relevant interfaces with active MACsec sessions are using the new keychain.
  • Change MACsec policy to must-secure mode.

• The following procedure should be followed to disable/remove a MACsec policy deployed in must-secure mode:
  • Change the MACsec policy to should-secure.
  • Verify that the affected interfaces are using should-secure mode.
  • Disable/remove the MACsec policy.
Keychain Definition

- There should be one key in the keychain with a start time of now. If must-secure is deployed with a keychain that doesn’t have a key that is immediately active then traffic will be blocked on that link until the key becomes current and a MACsec session is started. If should-secure mode is being used then traffic will be unencrypted until the key becomes current and a MACsec session has started.

- There should be one key in the keychain with an end time of infinite. When a keychain expires, then traffic is blocked on affected interfaces which are configured for must-secure mode. Interfaces configured for should-secure mode transmit unencrypted traffic.

- There should be overlaps in the end time and start time of keys that are used sequentially to ensure the MACsec session stays up when there is a transition between keys.

Configuring MACsec for Fabric Links Using the GUI

Procedure

Step 1
On the menu bar, click Fabric > Fabric Policies > Policies > MACsec > Interfaces. In the Navigation pane, right click on Interfaces to open Create MACsec Fabric Interface Policy and perform the following actions:

a) In the Name field, enter a name for the MACsec Fabric Interface policy.

b) In the MACsec Parameters field, either select a previously configured MACsec Parameters policy or create a new one.

c) In the MACsec Keychain Policy field, either select a previously configured MACsec Parameters policy or create a new one and click Submit.

To create a MACsec Keychain Policy, see Configuring MACsec Keychain Policy Using the GUI, on page 235.

Step 2
To apply the MACsec Fabric Interface Policy to a Fabric Leaf or Spine Port Policy Group, in the Navigation pane, click Interfaces > Leaf/Spine Interfaces > Policy Groups > Spine/Leaf Port Policy Group_name. In the Work pane, select the MACsec Fabric Interface Policy just created.

Step 3
To apply the MACsec Fabric Interface Policy to a Pod Policy Group, in the Navigation pane, click Pods > Policy Groups > Pod Policy Group_name. In the Work pane, select the MACsec Fabric Interface Policy just created.

Configuring MACsec for Access Links Using the GUI

Procedure

Step 1
On the menu bar, click Fabric > External Access Policies. In the Navigation pane, click on Policies > Interface > MACsec > Interfaces and right click on Interfaces to open Create MACsec Fabric Interface Policy and perform the following actions:

a) In the Name field, enter a name for the MACsec Access Interface policy.
b) In the MACsec Parameters field, either select a previously configured MACsec Parameters policy or create a new one.

c) In the MACsec Keychain Policy field, either select a previously configured MACsec Parameters policy or create a new one and click Submit.

To create a MACsec Keychain Policy, see Configuring MACsec Keychain Policy Using the GUI, on page 235.

Step 2

To apply the MACsec Access Interface Policy to a Fabric Leaf or Spine Port Policy Group, in the Navigation pane, click Interfaces > Leaf/Spine Interfaces > Policy Groups > Spine/Leaf Policy Group_name. In the Work pane, select the MACsec Fabric Interface Policy just created.

---

### Configuring MACsec Parameters Using the APIC GUI

**Procedure**

**Step 1**

On the menu bar, click Fabric > Access Policies. In the Navigation pane, click on Interface Policies > Policies and right click on MACsec Policies to open Create MACsec Access Parameters Policy and perform the following actions:

a) In the Name field, enter a name for the MACsec Access Parameters policy.
b) In the Security Policy field, select a mode for encrypted traffic and click Submit.

**Note** Before deploying MACsec in Must Secure Mode, the keychain must be deployed on the affected interface or the interface will go down.

**Step 2**

To apply the MACsec Access Parameters Policy to a Leaf or Spine Port Policy Group, in the Navigation pane, click Interface Policies > Policy Groups > Spine/Leaf Policy Group_name. In the Work pane, select the MACsec Access Interface Policy just created.

---

### Configuring MACsec Keychain Policy Using the GUI

**Procedure**

**Step 1**

On the menu bar, click Fabric > Fabric Policies > Policies > MACsec > KeyChains. In the Navigation pane, right click on KeyChains to open Create MACsec Keychain Policy and perform the following actions:

a) In the Name field, enter a name for the MACsec Fabric Interface policy.
b) Expand the MACsec Key Policy table to create the Key policy.

**Step 2**

In the MACsec Key Policy dialog box perform the following actions:

a) In the Name field, enter a name for the MACsec Key policy.
b) In the Key Name field, enter a key name (up to 64 hexadecimal characters).
Note: A maximum of 64 keys are supported per keychain.

c) In the **Pre-shared Key** field, enter the pre-shared key information.

**Note**
- For 128-bit cipher suites only 32 character PSKs are permitted.
- For 256-bit cipher suites only 64 Character PSKs are permitted.

d) In the **Start Time** field, select a date for the key to become valid.

e) In the **End Time** field, select a date for the key to expire. Click **Ok** and **Submit**.

**Note:** When defining multiple keys in a keychain, the keys must be defined with overlapping times in order to assure a smooth transition from the old key to the new key. The endTime of the old key should overlap with the startTime of the new key.

For configuring the Keychain policy through Access Policies, on the menu bar click **Fabric > External Access Policies**. In the **Navigation** pane, click on **Policies > Interface > MACsec > MACsec KeyChain Policies** and right click on to open **Create MACsec Keychain Policy** and perform the steps above.

### Configuring MACsec Using the NX-OS Style CLI

**Procedure**

**Step 1**
Configure MACsec Security Policy for access interfaces

**Example:**

```
apic1# configure
apic1(config)#  template macsec access security-policy accmacsecpol1
apic1(config-macsec-param)#  cipher-suite gcm-aes-128
apic1(config-macsec-param)#  conf-offset offset-30
apic1(config-macsec-param)#  description 'description for mac sec parameters'
apic1(config-macsec-param)#  key-server-priority 1
apic1(config-macsec-param)#  sak-expiry-time 110
apic1(config-macsec-param)#  security-mode must-secure
apic1(config-macsec-param)#  window-size 1
apic1(config-macsec-param)#  exit
apic1(config)#
```

**Step 2**
Configure MACsec key chain for access interface:

PSK can be configured in 2 ways:

**Note**
- Inline with the **psk-string** command as illustrated in key 12ab below. The PSK is not secure because it is logged and exposed.
- Entered separately in a new command **Enter PSK string** after the **psk-string** command as illustrated in key ab12. The PSK is secured because it is only echoed locally and is not logged.

**Example:**
apic1# configure
apic1(config)# template macsec access keychain acckeychainpoll
apic1(config-macsec-keychain)# description 'macsec key chain kc1'
apic1(config-macsec-keychain)# key 12ab
apic1(config-macsec-keychain-key)# life-time start 2017-09-19T12:03:15 end 2017-12-19T12:03:15
apic1(config-macsec-keychain-key)# psk-string 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)# exit
apic1(config-macsec-keychain)# key ab12
apic1(config-macsec-keychain-key)# life-time start now end infinite
apic1(config-macsec-keychain-key)# psk-string
Enter PSK string: 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)# exit
apic1(config-macsec-keychain)# exit
apic1(config)#

Step 3 Configure MACsec interface policy for access interface:

Example:
apic1# configure
apic1(config)# template macsec access interface-policy accmacsecifpol1
apic1(config-macsec-if-policy)# inherit macsec security-policy accmacsecpoll keychain acckeychainpoll
apic1(config-macsec-if-policy)# exit
apic1(config)#

Step 4 Associate MACsec interface policy to access interfaces on leaf (or spine):

Example:
apic1# configure
apic1(config)# template macsec access interface-policy accmacsecifpol1
apic1(config-macsec-if-policy)# inherit macsec security-policy accmacsecpoll keychain acckeychainpoll
apic1(config-macsec-if-policy)# exit
apic1(config)

Step 5 Configure MACsec Security Policy for fabric interfaces:

Example:
apic1(config)# configure
apic1(config)# template macsec fabric security-policy fabmacsecpoll
apic1(config-macsec-param)# cipher-suite gcm-aes-xpn-128
apic1(config-macsec-param)# description 'description for mac sec parameters'
apic1(config-macsec-param)# window-size 1
apic1(config-macsec-param)# sak-expiry-time 100
apic1(config-macsec-param)# security-mode must-secure
apic1(config-macsec-param)# exit
apic1(config)#

Step 6 Configure MACsec key chain for fabric interface:

PSK can be configured in 2 ways:

Note  
- Inline with the `psk-string` command as illustrated in key 12ab below. The PSK is not secure because it is logged and exposed.
- Entered separately in a new command `Enter PSK string` after the `psk-string` command as illustrated in key ab12. The PSK is secured because it is only echoed locally and is not logged.

Example:
apic1(config)# configure
apic1(config)# template macsec fabric security-policy fabmacsecpoll
apic1(config-macsec-param)# cipher-suite gcm-aes-xpn-128
apic1(config-macsec-param)# description 'description for mac sec parameters'
apic1(config-macsec-param)# window-size 1
apic1(config-macsec-param)# sak-expiry-time 100
apic1(config-macsec-param)# security-mode must-secure
apic1(config-macsec-param)# exit
apic1(config)# template macsec fabric keychain fabkeychainpoll
apic1(config-macsec-keychain)# description 'macsec key chain kc1'
apic1(config-macsec-keychain)# key 12ab
apic1(config-macsec-keychain-key)# psk-string 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)# life-time start 2016-09-19T12:03:15 end 2017-09-19T12:03:15
apic1(config-macsec-keychain-key)# exit
apic1(config-macsec-keychain)# key cd78
apic1(config-macsec-keychain-key)# psk-string 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)# life-time start now end infinite
apic1(config-macsec-keychain-key)# exit
apic1(config-macsec-keychain)# exit
apic1(config)#

Step 7 Associate MACsec interface policy to fabric interfaces on leaf (or spine):

Example:
apic1(config)# configure
apic1(config)# leaf 101
apic1(config-leaf)# fabric-interface ethernet 1/52-53
apic1(config-leaf-if)# inherit macsec interface-policy fabmacsecifpol2
apic1(config-leaf-if)# exit
apic1(config-leaf)#

Configuring MACsec Using the REST API

Apply a MACsec policy to all Pods in the fabric:

Example:

```xml
<fabricInst>
  <macsecFabPolCont>
    <macsecFabParamPol name="fabricParam1" secPolicy="should-secure" replayWindow="120">
      <macsecKeyChainPol name="fabricKC1">
        <macsecKeyPol name="Key1" preSharedKey="0102030405060708090A0B0C0D0E0F10" keyName="A1A2A3A0" startTime="now" endTime="infinite"/>
      </macsecKeyChainPol>
    </macsecFabParamPol>
    <macsecRsToParamPol tDn="uni/fabric/macsecpcontfab/fabparamp-fabricParam1"/>
    <macsecRsToKeyChainPol tDn="uni/fabric/macsecpcontfab/keychainp-fabricKC1"/>
  </macsecFabPolCont>
  <fabricFuncP>
    <fabricPodPGrp name = "PodPG1">
      <fabricRsMacsecPol tnMacsecFabIfPolName="fabricPodPoll1"/>
    </fabricPodPGrp>
  </fabricFuncP>
</fabricInst>
```
Applying a MACsec access policy on eth1/4 of leaf-101:

Example:

```xml
<infraInfra>
  <macsecPolCont>
    <macsecParamPol name="accessParam1" secPolicy="should-secure" replayWindow="120">
      <macsecKeyChainPol name="accessKC1">
        <macsecKeyPol name="Key1" preSharedKey="0102030405060708090A0B0C0D0E0F10" keyName="A1A2A3A0" startTime="now" endTime="infinite"/>
      </macsecKeyChainPol>
    </macsecKeyChainPol>
    <macsecIfPol name="accessPol1">
      <macsecRsToParamPol tDn="uni/infra/macsecpcont/paramp-accessParam1"/>
      <macsecRsToKeyChainPol tDn="uni/infra/macsecpcont/keychainp-accessKC1"/>
    </macsecIfPol>
  </macsecPolCont>
  <infraFuncP>
    <infraAccPortGrp name = "LeTestPGrp">
      <infraRsMacsecIfPol tnMacsecIfPolName="accessPol1"/>
    </infraAccPortGrp>
  </infraFuncP>
</infraInfra>
```

Applying a MACsec fabric policy on eth1/49 of leaf-101 and eth 5/1 of spine-102:

```xml
<infraInfra>
  <macsecFabPolCont>
    <macsecFabParamPol name="fabricParam1" secPolicy="should-secure" replayWindow="120">
      <macsecKeyChainPol name="fabricKC1">
        <macsecKeyPol name="Key1" preSharedKey="0102030405060708090A0B0C0D0E0F10" keyName="A1A2A3A0" startTime="now" endTime="infinite"/>
      </macsecKeyChainPol>
    </macsecKeyChainPol>
    <macsecFabIfPol name="fabricPoll" useAutoKeys="0">
      <macsecRsToParamPol tDn="uni/fabric/macsecpcontfab/fabparamp-fabricParam1"/>
      <macsecRsToKeyChainPol tDn="uni/fabric/macsecpcontfab/keychainp-fabricKC1"/>
    </macsecFabIfPol>
  </macsecFabPolCont>
</infraInfra>
```
<fabricLePortPGrp name = "LeTestPGrp">
   <fabricRsMacsecFabIfPol tnMacsecFabIfPolName="fabricPol1"/>
</fabricLePortPGrp>

<fabricSpPortPGrp name = "SpTestPGrp">
   <fabricRsMacsecFabIfPol tnMacsecFabIfPolName="fabricPol1"/>
</fabricSpPortPGrp>

</fabricFuncP>

<fabricLFPathS name="leaf">
   <fabricRsLFPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/49]" />
   <fabricRsPathToLePortPGrp tDn="uni/fabric/funcprof/leportgrp-LeTestPGrp" />
</fabricLFPathS>

<fabricSpPortP name="spine_profile">
   <fabricSFPortS name="spineIf" type="range">
      <fabricPortBlk name="spBlk" fromCard="5" fromPort="1" toCard="5" toPort="1" />
   </fabricSFPortS>
</fabricSpPortP>

<fabricSpineP name="SpNode" >
   <fabricRsSpPortP tDn="uni/fabric/spportp-spine_profile" />
   <fabricSpineS name="spsw" type="range">
      <fabricNodeBlk name="node102" to="102" from="102" />
   </fabricSpineS>
</fabricSpineP>
</fabricInst>