Performing Tasks Using the NX-OS Style CLI

- Mixed-Mode Encapsulation, on page 1
- Port Channel and Virtual Port Channel Configuration, on page 3
- Enhanced LACP Policy Support, on page 5
- SPAN Features, on page 6
- BPDU Features, on page 7
- IGMP Querier and Snooping, on page 8
- Intra-EPG Isolation Enforcement for Cisco ACI Virtual Edge, on page 9
- Distributed Firewall, on page 10

Mixed-Mode Encapsulation

Check or Change the VMM Domain Encapsulation Mode Using the NX-OS CLI

You can use the NX-OS CLI to check or change the encapsulation mode of a VMM domain.

Note If EPGs are associated to the VMM domain, you cannot change its switching mode. If you want the domain to use a different switching mode, delete and re-create it. However, you can change the switching mode of the VMM domain if no EPGs are associated to it.

Step 1 Check the VMM domain encapsulation mode.

Example:

```
apic1(config-vmware-ave)# show run
# Command: show running-config vmware-domain mininet1 configure-ave
# Time: Tue Nov 21 07:07:58 2017
  vmware-domain mininet1
    configure-ave
      switching mode vlan
      multicast-address 230.1.2.3
      exit
    exit
apic1(config-vmware-ave)#
```

Step 2 Change the VMM domain encapsulation mode.

Example:

```
apic1# configure
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# switching mode ?
 vlan      VLAN/SW Mode
 vxlan     VXLAN/SW Mode
 vxlan-ns  VXLAN/HW Mode
```

Override the VMM Domain Encapsulation Mode for an EPG Using the NX-OS Style CLI

After you create an EPG and associate it with a VMM domain, you can change the encapsulation mode of the EPG so it differs from or is the same of the VMM domain encapsulation mode.

Before you begin

You must already have created an EPG and have associated it with a VMM domain.

Specify the encapsulation mode for an EPG:

Example:

```
apic1(config)# tenant <tenant name>
apic1(config-tenant)# application <application name>
apic1(config-tenant-app)# epg <epg name>conf
apic1(config-tenant-app-epg)# vmware-domain member <vmm domain name>
apic1(config-tenant-app-epg-domain)# encap-mode auto | vlan | vxlan
apic1(config-tenant-app-epg-domain)# switching-mode AVE
```

You can choose one of the following encapsulation modes:

- **Auto**—This causes the EPG to use the same encapsulation mode as the VMM domain. This is the default configuration.
- **VLAN**—This overrides the domain's VXLAN configuration, and the EPG will use VLAN encapsulation. However, a fault will be triggered for the EPG if a VLAN pool is not configured on the domain.
- **VXLAN**—This overrides the domain's VLAN configuration, and the EPG will use VXLAN encapsulation. However, a fault will be triggered for the EPG if a multicast pool is not configured on the domain.

Port Channel and Virtual Port Channel Configuration

Configure Port Channel Mode Using the NX-OS Style CLI

Configure port channel mode.

Example:

```
apic1# conf t
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# channel-mode ?
 active       Set channeling mode to ACTIVE
 mac-pinning  Set channeling mode to MAC-PINNING
 on           Set channeling mode to ON (static)
 passive      Set channeling mode to PASSIVE
apic1(config-vmware-ave)# channel-mode <mode>
```

Configure a Port Channel Using the NX-OS Style CLI

Create a port channel.

Example:

```
apic1# config
apic1(config)# template port-channel cli-pc1
apic1(config-if)# channel-mode active
apic1(config-if)# vlan-domain member cli-vdom1

apic1(config-if)# show running-config
# Command: show running-config interface port-channel cli-pc1
# Time: Thu Oct  1 10:38:30 2015
  interface port-channel cli-pc1
    vlan-domain member cli-vdom1
    channel-mode active
    exit
```

Configure a VPC Using the NX-OS Style CLI

Configuring a Virtual Port Channel (VPC) using the NX-OS style CLI consists of two tasks. Your first configure a VPC domain and then configure the VPC on the switch interfaces.

Configure a VPC Domain Using the NX-OS Style CLI

Configure a VPC domain.

Example:

```
apic1# config
apic1(config)# vpc domain explicit 10 leaf 101 102

apic1(config-vpc)# show running-config
# Command: show running-config vpc domain explicit 10 leaf 101 102
# Time: Thu Oct  1 10:39:26 2015
  vpc domain explicit 10 leaf 101 102
    exit
```

Configure a VPC on Switch Interfaces Using NX-OS Style CLI

Configure a VPC on switch interfaces

Example:

```
apic1# config
apic1(config)# leaf 101 - 102
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# channel-group cli-pc1 vpc

apic1(config-leaf-if)# show running-config
# Command: show running-config leaf 101 - 102 interface ethernet 1/3
# Time: Thu Oct  1 10:41:15 2015
  leaf 101
    interface ethernet 1/3
      channel-group cli-pc1 vpc
      exit
    exit
  leaf 102
    interface ethernet 1/3
      channel-group cli-pc1 vpc
      exit
    exit
```

Configure Endpoint Retention Using the NX-OS Style CLI

Before you begin

You must have created a vCenter domain.

Step 1 In the CLI, enter configuration mode:

Example:

```
apic1# configure
apic1(config)#
```

Step 2 Configure a retention time for detached endpoints:

You can choose a delay of between 0 and 600 seconds. The default is 0.

Example:

```
apic1(config)# vmware-domain <domainName>

apic1(config-vmware)# ep-retention-time <value>
```

Enhanced LACP Policy Support

Create LAGs for DVS Uplink Port Groups Using the NX-OS Style CLI

Improve distributed virtual switch (DVS) uplink port group load balancing by putting the port groups into link aggregation groups (LAGs) and associating them with specific load-balancing algorithms. You can perform this task using the NX-OS style CLI.

Before you begin

You must have created a VMware vCenter virtual machine manager (VMM) domain for VMware VDS or Cisco Application Centric Infrastructure (ACI) Virtual Edge.

Create or delete an enhanced LACP policy.

Example:

```
apic1(config-vmware)# enhancedlacp  LAG name
apic1(config-vmware-enhancedlacp)# lbmode loadbalancing mode
apic1(config-vmware-enhancedlacp)# mode mode
apic1(config-vmware-enhancedlacp)# numlinks max number of uplinks
apic1(config-vmware)# no enhancedlacp LAG name to delete
```

What to do next

If you are using VMware VDS, associate endpoint groups (EPGs) to the domain with the enhanced LACP policy. If you are using Cisco Application Centric Infrastructure (ACI) Virtual Edge, associate internally created inside and outside port groups with the enhanced LACP policy, then associate EPGs to the domain with the policy.

Associate Internal Port Groups to VMware vCenter Domains with Enhanced LACP Policies Using the NX-OS Style CLI

Associate Cisco Application Centric Infrastructure (ACI) Virtual Edge internally created inside and outside port groups with a VMware vCenter domain with an enhanced LACP policy. You can perform this task using the NX-OS style CLI.

Before you begin

You must have created link aggregation groups (LAGs) for the distributed virtual switch (DVS) uplink port groups and associated a load-balancing algorithm to the LAGs.

Associate (or deassociate) internal endpoint groups (EPGs) to the VMM domain with the enhanced LACP policy.

Example:

```
apic1(config-vmware)# lag-policy name of the policy to associate
apic1(config-vmware)#  no lag-policy name of the policy to deassociate
```

What to do next

Associate EPGs with the VMware vCenter domain containing the enhanced LACP policy.

Associate Application EPGs to VMware vCenter Domains with Enhanced LACP Policies Using the NX-OS Style CLI

Associate application endpoint groups (EPGs) with the VMware vCenter domain with LAGs and a load-balancing algorithm. You can perform this task using NX-OS style CLI. You can also deassociate application EPGs from the domain.

Before you begin

You must have created link aggregation groups (LAGs) for distributed virtual switch (DVS) uplink port groups and associated a load-balancing algorithm to the LAGs.

Step 1 Associate an application EPG with the domain or deassociate it from the domain.

Example:

```
apic1(config-tenant-app-epg-domain)#  lag-policy name of the LAG policy to associate
apic1(config-tenant-app-epg-domain)# no  lag-policy name of the LAG policy to deassociate
```

Step 2 Repeat Step 1 for other application EPGs in the tenant as desired.

SPAN Features

Configure SPAN Using the NX-OS CLI

Step 1 Configure SPAN.

Example:

```
apic1(config)# monitor virtual session cli-vspan1
apic1(config-monitor-virtual)# source tenant cli-esx1 application cli-esx1 epg cli-vspan1 mac
<00:50:56:BA:BE:0F>
apic1(config-monitor-virtual-source)# direction both
apic1(config-monitor-virtual-source)# exit
apic1(config-monitor-virtual)# destination tenant cli-esx1 application cli-vspan1 epg cli-esx1b mac
 <00:50:56:BA:F0:E0>

apic1(config)# vmware-domain cli-esx
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# monitor virtual session cli-vspan1
```

Step 2 Verify the configuration.

Example:

```
apic1(config-monitor-virtual)# show running-config
# Command: show running-config monitor virtual session cli-vspan1
# Time: Thu Oct  8 11:20:09 2015
  monitor virtual session cli-vspan1
    source tenant cli-esx1 application cli-esx1 epg cli-esx1 mac 00:50:56:BA:BE:0F
      exit
    destination tenant cli-esx1 application cli-esx1 epg cli-esx1b mac 00:50:56:BA:F0:E0
    exi
```

BPDU Features

Configure BPDU Features Using the NX-OS Style CLI

Step 1 Enter the vmware-domain mode.

Example:

```
apic1# configure
apic1(config)# vmware-domain domain name
AVE-Vlan  AVE2-VXLAN  Test  Test2
```

Step 2 Create a spanning-tree interface policy.

Example:

```
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# spanning-tree
              bpdu-filter  bpdu-guard
apic1(config-vmware-ave)# spanning-tree
              bpdu-filter  Configure BPDU filter override on AVE uplink ports
              bpdu-guard   Configure BPDU guard override on AVE uplink ports
```

Step 3 Disable or enable BPDU filter.

Example:

```
apic1(config-vmware-ave)# spanning-tree bpdu-filter
                default  disable  enable
apic1(config-vmware-ave)# spanning-tree bpdu-filter
                default  Remove BPDU filter/guard override policy
                disable  Disable BPDU filter
```

```
                    enable   Enable BPDU filter
```

Step 4 Disable or enable BPDU guard.

```
apic1(config-vmware-ave)# spanning-tree bpdu-guard
               default  disable  enable
```

IGMP Querier and Snooping

Configure IGMP Querier Using the NX-OS Style CLI

Configure IGMP querier.

Example:

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ip address <192.168.1.1/24> snooping-querier
 <CR>
multi-site  Set the address as multi-site address
scope       Scope of the address among ['public', 'private']
secondary   Set the address as secondary address
```

Configure IGMP Snooping to Take Effect Immediately Using the NX-OS Style CLI

Configure IGMP snooping to take effect immediately.

Example:

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ip igmp snooping querier
```

Configure IGMP Snooping to Take Effect Later Using the NX-OS Style CLI

Configure IGMP snooping to take effect later.

Example:

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# template ip igmp snooping policy <foo_igmp>
apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping querier
```

Intra-EPG Isolation Enforcement for Cisco ACI Virtual Edge

Configure Intra-EPG Isolation for Cisco ACI Virtual Edge Using the NX-OS Style CLI

Before you begin

Make sure that VXLAN-related configuration is present on the Cisco ACI Virtual Edge VMM domain, particularly a Cisco ACI Virtual Edge fabric-wide multicast address and pool of multicast addresses (one per EPG).

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

Example:

```
# Command: show running-config tenant Tenant2 application AP-1 epg EPG-61
  tenant Tenant2
    application AP-1
      epg EPG-61
        bridge-domain member BD-61
        vmware-domain member D-AVE-SITE-2-3
          switching-mode AVE
          encap-mode vxlan
          exit
        isolation enforce            # This enables EPG into isolation mode.
        exit
      exit
    exit
```

What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab and View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab in this guide.

Distributed Firewall

Configure a Stateful Policy for Distributed Firewall Using the NX-OS Style CLI

Configure a stateful policy in the Cisco APIC.

Example:

```
apic1(config)# tenant Tenant1
apic1(config-tenant)# access-list TCP-511 apic1
apic1 (config-tenant-acl)# match icmp
apic1 (config-tenant-acl)# match raw TCP-511 dFromPort 443 dToPort 443 etherT ip prot 6 stateful yes

apic1 (config-tenant-acl)# match raw tcp etherT ip prot 6 sFromPort 443 sToPort 443 stateful yes
apic1 (config-tenant-acl)# match raw tcp-22out dFromPort 22 dToPort 22 etherT ip prot 6 stateful yes
 apic1(config-tenant-acl)# match raw tcp-all etherT ip prot 6 stateful yes
apic1(config-tenant-acl)# match raw tcp22-from etherT ip prot 6 sFromPort 22 sToPort 22 stateful yes
 apic1(config-tenant-acl)# exit apic1(config-tenant)# contract TCP511
apic1(config-tenant-contract)# subject TCP-ICMP
apic1(config-tenant-contract-subj)# access-group TCP-511 both
apic1(config-tenant-contract-subj)# access-group arp both
apic1(config-tenant-contract-subj)#
```

What to do next

Create a Distributed Firewall policy.

Enable Distributed Firewall or Change Its Mode Using the NX-OS Style CLI

You can use the NX-OS style CLI to enable Distribute Firewall or change its mode.

Enable Distributed Firewall or change its mode.

Example:

```
apic1# configure
apic1(config)# vmware-domain Direct-AVE2-VXLAN
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# firewall mode < any of below 3>
disabled  Disabled mode
enabled   Enabled mode
learning  Learning mode
```

Configure Parameters for Distributed Firewall Flow Information Using the NX-OS Style CLI

Step 1 Configure the parameters for the syslog server or servers.

Example:

```
apic1# configure
apic1(config)# logging server-group group name
apic1(config-logging)# server IP address severity severity level facility facility name  port 1-65535 mgmtepg MgmtEpg
```

You can repeat the last command for additional syslog servers; you can configure up to three syslog servers.

Step 2 Configure the parameters for the syslog source.

Example:

```
apic1# configure
apic1(config)#  vmware-domain Direct-AVE
apic1(config-vmware)#  configure-ave
apic1(config-vmware-ave)# firewall mode enabled
apic1(config-vmware-ave)# firewall-logging server-group group name action-type permit, deny severity severity polling-interval 60-86400
```

Note You must enter the **firewall mode enabled** command before you enter the **firewall-logging** command.

Note For the **firewall-logging** command, you can enter either **permit** or **deny**. You can also enter both, separated by a comma.