Configuration Zones

About Configuration Zones

Configuration zones divide the Cisco Application Centric Infrastructure (ACI) fabric into different zones that can be updated with configuration changes at different times. This limits the risk of deploying a faulty configuration on the entire fabric at once that might disrupt traffic or even bring the fabric down. An administrator can deploy a configuration to a defined non-critical zone, and then deploy it to defined critical zones when satisfied that it is suitable. Similar to the way that UCS Manager functions, a configuration zone is essentially an additional "user acknowledge" type of policy that forces users to verify configuration changes before applying the changes.

You can choose one of the following deployment modes for a configuration zone:

- Enabled—Pending updates are sent immediately
- Disabled—New updates are postponed
- Triggered—Pending updates are sent immediately, and the deployment mode is reset to the value it had before being triggered

Without configuration zones enabled, policy changes will take effect on all fabric nodes once the configuration is set and standard programming criteria are met. With configuration zones enabled, you can have these policy changes transition to a state of "postponed" until a user acknowledges the change to be applied in specific zones.

Zones can encompass an entire POD, or can encompass a subset of fabric nodes.
Prerequisites for Configuration Zones

You must meet the following prerequisites to use configuration zones:

- You must be using the Application Policy Infrastructure Controller (APIC) 1.2(2) release or later

Guidelines and Limitations for Configuration Zones

The following guidelines and limitations apply for configuration zones:

- Do not upgrade, downgrade, commission, or decommission nodes in a disabled configuration zone.
- Nodes can only be part of a single zone. Attempting to place a node in multiple zones will generate a server error.
- Do not separate virtual port channel (vPC) member nodes into different configuration zones. If the nodes are in different configuration zones, then the vPCs' modes become mismatched if the interface policies are modified and deployed to only one of the vPC member nodes.

Recommended Configuration procedure for Configuration Zones

As configuration zones can be manually defined, zone definition will typically encompass a logical "non-critical zone" and a "critical zone." The intent is that fabric-wide changes can be allowed to be made only on the non-critical zone first. This gives network operators a chance to verify the configuration and behaviors to ensure expectations are met. Once verification has been performed on the non-critical zone, the change can then be applied to the critical zone.

For procedures for defining configuration zones, see the Cisco APIC Troubleshooting Guide at the following URL:


Verifying the Configuration Zones Using the GUI

The following procedure verifies the configuration zones by using the Application Policy Infrastructure Controller (APIC) GUI.

Procedure

1. On the menu bar, choose System > Config Zones.
2. In the Work pane, in the Select Zone drop-down list, choose the zone that you want to verify.
   You can view and modify the zone's configuration.
Configuration Examples for Configuration Zones

For configuration zone examples using the different user interfaces, see the Cisco APIC Configuration Zones knowledge base article at the following URL:

Additional References for Configuration Zones

For more information about configuration zones, see the Cisco APIC Configuration Zones knowledge base article at the following URL:

Shared Services

About Shared Services

Shared services is the paradigm of taking endpoints within one tenant/VRF and allowing them to communicate with endpoints within another tenant/VRF. Shared services enables this communications across tenants while preserving the isolation and security policies of the individual tenants. A routed connection to an external network is an example of a shared service that multiple tenants use.

Prerequisites for Shared Services

You must meet the following prerequisites to use shared services:

- A Cisco Application Centric Infrastructure (ACI) fabric that has been fully initialized
- At least 2 user-created tenants to share services between, one will be the provider and one will be the consumer
- At least 1 EPG within each of these tenants
- A subnet defined under the provider EPG as “Shared between VRFs”

Guidelines and Limitations for Shared Services

The following guidelines and limitations apply when using shared services:

- As of Release 1.2, shared services can be performed with a shared subnet defined under the bridge domain (BD).
  - The preferred method remains having the shared subnet defined under the EPG to be shared to another tenant.
  - Prior to this, shared services required that the provider subnet be defined under the EPG that was to be shared.
• Contracts for shared service must have the scope set to **Global**. The default scope is **VRF** and will not work for shared services.

• For BD-to-BD shared services: Given User-Tenant A to User-Tenant B, each tenant has a contract that is associated as a provider under an EPG and is exported to the other tenant. The same EPG takes the subsequently imported contract and has it applied as a consumed contract interface.
  • All EPGs that communicate with BD to BD Shared Services have at least two contract relationships, one as a provider and one as a consumed contract interface.

• When using BD-to-BD shared services, due to the extra configuration and rules associated with having a provider set within both tenants, limit the fabric to roughly 16k EPGs.

• In the case of vzAny, you *must* define the provider EPG shared subnet under the EPG in order to properly derive the pcTag (classification) of the destination from the consumer (vzAny) side. If you are migrating from a BD-to-BD shared services configuration, where both the consumer and provider subnets are defined under bridge domains, to vzAny acting as a shared service consumer, you must take an extra configuration step where you add the provider subnet to the EPG with the shared flags at minimum.

  ![Note](image)

  If you add the EPG subnet as a duplicate of the defined BD subnet, ensure that both definitions of the subnet always have the same flags defined. Failure to do so can result in unexpected fabric forwarding behavior.

• Subnets leaked from multiple consumer networks into a VRF, or vice versa, must be disjointed and must not overlap. If two consumers are mistakenly configured with the same subnet, recovery from this condition is done by removing the subnet configuration for both then reconfiguring the subnets correctly.

• Subnets leaked across VRFs must have the **Shared between VRFs** and **ND RA Prefix** options enabled, to be defined on the BD or the EPG.

---

### Recommended Configuration Procedure of Shared Services Using the GUI

The following procedure to configure the contract(s) that will utilize shared services using the Application Policy Infrastructure Controller (APIC) GUI.

**Procedure**

| Step 1 | From the menu bar, choose **Tenants > tenant_name**. |
| Step 2 | In the **Navigation** pane, choose **Security Policies > Contracts > contract_name**. |
| Step 3 | In the **Work** pane, click the **Policy** tab and set the **Scope** field to **Global**. |

**Note** If performing BD-BD shared services, a contract set to scope **Global** should exist within both tenants to be exported to one another.
Configuration Examples for Shared Services Using the GUI

The following procedure provides an example of configuring shared services using the Application Policy Infrastructure Controller (APIC) GUI.

Procedure

Step 1  
To set the shared services contract as a provider for an EPG with a shared subnet: on the menu bar, choose Tenants > tenant_name.

Step 2  
In the Navigation pane, choose tenant_name > Application Profiles > profile_name > Application EPGs > epg_name > Contracts.

Step 3  
Right-click on Contracts, choose Add Provided Contract, and enter a name for the contract in the Name field.

Step 4  
To export the contract from one tenant to another: in the Navigation pane, choose Security Profiles > Contracts.

a)  
Right-click on Contracts and choose Export Contract. Enter the appropriate information for the Name, Contract and Tenant fields. Click Submit when finished.

Step 5  
To apply the contract to the consumer EPG within the imported tenant as a consumed contract interface: in the Navigation pane, choose tenant_name > Application Profiles > profile_name > Application EPGs > epg_name > Contracts.

Step 6  
Right-click on Contracts, choose Add Consumed Contract Interface, and enter a name for the contract in the Name field.

Note  
If performing BD-BD shared services, repeat the procedure between tenants before communication will be successful between both EPGs.

Additional References for Shared Services

For more information on EPG Static Binding Modes, see the Cisco Application Centric Infrastructure Fundamentals Guide at the following URL:


EPG Static Binding

About EPG Static Binding Modes

Static bindings enable you to statically link the EPG to either a path (node/interface) or to an entire leaf. This binding essentially forces the bound node to perform programming of the defined VLAN for classification of incoming traffic. Without a static binding, traffic going into the fabric will not be classified into an EPG and subsequently will not be forwarded.
Prerequisites for EPG Static Binding Modes

You must meet the following prerequisites to use EPG static binding modes:

- The Cisco Application Centric Infrastructure (ACI) fabric must be initialized.
- Access policies must be configured that correspond to the defined path.

Guidelines and Limitations for EPG Static Binding Modes

The following guidelines and limitations apply when using EPG static binding mode:

- If access policies associated with a domain have not been provisioned properly, the EPG will generate a fault when a static binding is applied.
- Faults indicating invalid path typically refer to some missing access policies given the defined path.
- Faults indicating VLAN issues typically refer to a missing VLAN association given the defined path.
- When a port is set to Untagged, that port can no longer be utilized as an untagged port in other EPGs.
  - For this to be accomplished, deploy the EPG instead as 802.1p.
- When utilizing 802.1p defined ports with other definitions on the same port as trunked, packets will egress this interface as VLAN-0, or as untagged in the case of EX switches.
  - Most devices process VLAN-0 as an untagged packet and have no issues.
  - For hosts that cannot VLAN-0 as an untagged packet, the setting must be Untagged.

Recommended Configuration procedure of EPG Static Binding Modes

The following 3 port modes can be applied when configuring EPG static binding modes:

- **Trunk (Tagged - classic IEEE 802.1q trunk)** — Traffic for the EPG is sourced by the leaf switch with the specified VLAN tag. The leaf switch also expects to receive traffic tagged with that VLAN to be able to associate it with the EPG. Traffic received untagged is discarded.

- **Access (Untagged)** — Traffic for the EPG is sourced by the leaf as untagged. Traffic received by the leaf switch as untagged or with the tag specified during the static binding configuration is associated with the EPG.

- **Access (802.1p)** — If only one EPG is bound to that interface, the behavior is identical as in the untagged case. If other EPGs are associated with the same interface, traffic for the EPG is sourced with an IEEE 802.1q tag using VLAN 0 (IEEE 802.1p tag), or is sourced as untagged in the case of EX switches.

Verifying the EPG Static Binding Modes Using the GUI

The following procedure verifies the EPG static binding mode configuration using the Cisco Application Policy Infrastructure Controller (APIC) GUI.
**Procedure**

**Step 1**  
On the menu bar, choose TENANTS > All Tenants.

**Step 2**  
In the Work pane, double-click the desired tenant's name.

- If you are using the Advanced GUI Mode of the Cisco APIC GUI, then from the Navigation pane, expand Application Profiles > profile_name > Application EPGs > application_epg_name > Static Ports.

- If you are using the Basic GUI Mode of the Cisco APIC GUI, then from the Navigation pane, expand tenant_name > Application Profiles > profile_name > Application EPGs > application_epg_name.

**Step 3**  
From the Navigation pane, click Static Ports.

Your static ports are listed in a summary table inside the Work pane. See the Mode column in the summary table to verify the EPG static binding modes.

---

**Configuration Examples for EPG Static Binding Modes Using the GUI**

The following procedure provides an example of configuring EPG static binding modes using the Application Policy Infrastructure Controller (APIC) GUI.

**Procedure**

**Step 1**  
Configure contract labels (consumer and provider). On the menu bar, choose TENANTS > All Tenants.

**Step 2**  
In the Work pane, double-click the desired tenant's name.

- If you are using the Advanced GUI Mode of the APIC GUI, then from the Navigation pane, expand Application Profiles > profile_name > Application EPGs > application_epg_name.

- If you are using the Basic GUI Mode of the APIC GUI, then from the Navigation pane, expand tenant_name > Application Profiles > profile_name > Application EPGs > application_epg_name.

**Step 3**  
In the Navigation pane, right-click on Static Ports to open the Deploy Static EPG On PC, VPC, Or Interface dialog box and perform the following tasks:

a) In the Path Type and Path fields, click the port type and the drop-down menu to navigate the node path.
b) In the Port Encap field, enter in the VLAN ID.
c) In the Deployment Immediacy field, choose the deployment type.
d) In the Mode field, choose the mode type.
e) Click Submit.
Additional References for EPG Static Binding Modes

For more information on EPG static binding modes, see the Cisco Application Centric Infrastructure Fundamentals Guide at the following URL:


In-Band and Out-of-Band Management

About In-Band and Out-of-Band Management

You can use in-band or out-of-band when designing the management plane and connectivity for the Cisco Application Centric Infrastructure (ACI) fabric. Out-of-band management utilizes its own set of specific ports that only exist on the out-of-band management plane. There is no configuration available to merge the out-of-band management plane into the data plane of the ACI fabric. Out-of-band management typically has its specifics ports connected to a device that only manages out-of-band network traffic. The following figure illustrates out-of-band management:

Figure 1: Out-of-Band Management

In-band management refers to utilizing the data plane for management traffic. In the case of ACI, this refers to having Application Policy Infrastructure Controller (APIC)-sourced management ports go through the leaf nodes to allow for management communication to devices hanging directly off of these leaf switch ports. The following figure illustrates in-band management:
You can utilize both in-band and out-of-band management simultaneously, but there are limitations that must be taken into account for this scenario.

**Prerequisites for In-Band and Out-of-Band Management**

You must meet the following prerequisites to use in-band or out-of-band management:

- Have an understanding of level of tenancy for the environment in question
- Have an understanding of services requiring management communication to the Application Policy Infrastructure Controller (APIC), such as managed Layer 4 to Layer 7 devices or VMM integration
- Have an understanding of potential tenants' management design and how they will present their management network to the Cisco Application Centric Infrastructure (ACI) fabric

**Guidelines and Limitations for In-Band and Out-of-Band Management**

The following guidelines and limitations apply for in-band and out-of-band management:

- Out-of-band management ports are mgmt0 ports on the switch nodes and the two LAN-On-Motherboard (LOM) ports on the Application Policy Infrastructure Controller (APIC). This configuration should not be changed on the APICs.
• In-band management ports are the front panel ports on the leaf nodes and the two PCIE VIC ports connected to the fabric on the APIC.

• Out-of-band and in-band management connectivity policies reside within tenant "mgmt."

• The out-of-band management address assignment that is set during the APIC startup script does not have an object created to represent that assignment. This must be done after fabric initialization to get an object representation within the MIT.

• The APIC management address sources traffic to the management address of various devices for integrations. For example, the APIC management must have communication to the management address of vCenter for VMM integration to be successful. This can be through in-band or out-of-band.

• When in-band management is set up, the APIC always prefers in-band for any traffic sourced from the APIC. Out-of-band is still accessible for devices that are sending requests to the out-of-band address specifically.

• There is no configuration available to leak the out-of-band management plane from the APIC into the data plane. This can only be accomplished by physically cabling out-of-band network devices directly into the data plane. Cisco does not recommend this setup. The preferred setup for this type of design would be to utilize in-band management.

• When utilizing in-band management with multi-tenancy, shared services will be used extensively to leak tenant management subnets into the fabric's in-band subnet.

**Recommended Configuration procedure of In-Band and Out-of-Band Management**

For the configuration procedures for in-band and out-of-band management, see the *Cisco APIC Basic Configuration Guide* at the following URL:


**Verifying the In-Band and Out-of-Band Management Configuration Using the GUI**

Depending on how the management address was set, there are a few locations from the GUI where you can verify the address assignment. The following procedure shows how to verify the address assignment from the different locations.

**Procedure**

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

**Step 2** In the **Navigation** pane, choose **Tenant mgmt > Node Management Addresses > Static Node Management Addresses**.

In the **Work** pane, you can see the in-band and out-of-band static management address assignment.

**Step 3** In the **Navigation** pane, choose **Tenant mgmt > Node Management Addresses > name_of_policy**.
In the Work pane, you can see the dynamic address assignments that can be created to provision mgmt addresses. If created, they specify the node ID, address assignment, and in-band or out-of-band assignment of the addresses.

### Verifying the In-Band and Out-of-Band Management Configuration Using the NX-OS-Style CLI

The following procedure verifies the in-band and out-of-band management configuration using the NX-OS-style CLI.

#### Procedure

**Step 1** View the out-of-band interfaces:

```
apic1# ifconfig oobmgmt
```

**Step 2** View the in-band interfaces:

```
apic1# ifconfig bond 0.vlan
```

`vlan` is the ID of the VLAN that is assigned as the in-band VLAN.

### Additional References for In-Band and Out-of-Band Management

For more information about shared services guidelines, see the *Cisco Application Centric Infrastructure Fundamentals Guide*.

For more information about NTP utilizing in-band or out-of-band management, see the *Cisco APIC Basic Configuration Guide*.

You can find these documents at the following URL:


### Out-of-Band Management Contracts

#### About Out-of-Band Management Contracts

For out-of-band management, hosts defined within the external management network instance profile can communicate with the nodes in the out-of-band management endpoint group only by using special out-of-band contracts. Regular contracts cannot be used with the out-of-band management endpoint group.
Prerequisites for Out-of-Band Management Contracts

You must meet the following prerequisites to use out-of-band management contracts:

• The Cisco Application Policy Infrastructure Controllers (APICs) must be setup.

• The fabric must be initialized.

Guidelines and Limitations for Out-of-Band Management Contracts

The following guidelines and limitations apply when using out-of-band management contracts:

• Starting with Cisco APIC Release 1.2(2), when a contract is provided on an out-of-band node management endpoint group, the default Cisco APIC out-of-band contract source address is the local subnet that is configured on the out-of-band node management address. Prior to Cisco APIC Release 1.2(2), any address was allowed to be the default Cisco APIC out-of-band contract source address.

• If a contract is consumed on the external management network instance profile, any flow that is not defined will default in only the out-of-band subnet having access to it.

Recommended Configuration Procedure of Out-of-Band Management Contracts

Using the GUI

The following procedure restricts out-of-band management through contract and subnet definitions within the node management EPG and external management network connectivity profile using the Cisco APIC GUI.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure out-of-band management. On the menu bar, choose Tenants &gt; mgmt.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Navigation pane, choose Tenant mgmt &gt; Node Management EPGs &gt; .</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, double-click Out-of-Band_name and expand the Provided Out-of-Band Contract table to configure.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure the consumer contract association and consumer subnet. In the Navigation pane, choose External Management Network Instance Profiles.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Work pane, double-click External Management Network Instance Profile_name and expand the Consumed Out-of-Band Contracts and Subnets tables to configure.</td>
</tr>
</tbody>
</table>

Verifying the Out-of-Band Management Contracts

From the Cisco APIC, out-of-band contracts can be verified from the iptables where a new target entry named fp-default now exists.
**Procedure**

In the chain for **fp-default**, there are entries based on the defined subnet. In the example below, only subnet 192.168.1.0/24 is allowing oob access.

**Example:**

```
pod3-apic1# iptables -L
Chain INPUT (policy DROP)
  target     prot opt source           destination
fp-default  all -- anywhere           anywhere
apic-default-drop all -- anywhere     anywhere
apic-default-allow all -- anywhere    anywhere
apic-default all -- anywhere          anywhere
...
```

Where a new target entry named **fp-default** exists, there are entries based on the defined subnet at the chain for **fp-default**. In the above example, only subnet 192.168.1.0/24 is being allowed out-of-band access.

---

**Configuration Examples for Out-of-Band Management Contracts**

The following procedure provides an example of configuring out-of-band management contracts using the Cisco APIC GUI.

To establish management connectivity to a Cisco ACI-mode fabric switch or an APIC controller, you must perform the following configuration in APIC.

- Create a node management EPG, either inband or out-of-band, that will include the nodes to be managed (leaf and spine switches and APIC controllers).
- Create an external management network instance profile that will include management hosts.
- Configure and associate a filter and contract to allow communication between the external management network instance profile and the node management EPG.
- Access the **Advanced GUI** mode.
Procedure

Step 1  On the menu bar, choose TENANTS > mgmt.
Step 2  In the Navigation pane, expand Security Policies.
Step 3  Right-click Out-of-Band Contracts then click Create Out-of-Band Contract.
Regular contracts cannot be used with an out-of-band node management endpoint group.
Step 4  In the Create Out-of-Band Contracts dialog box, perform the following tasks:
a)  In the Name field, enter a name for the contract.
b)  Expand Subjects. In the Create Contract Subject dialog box, in the Name field, enter a subject name.
c)  Expand Filters, and in the Name field from the drop-down list, choose the name of the filter (default).
   Click Update and click OK.
d)  In the Create Out-of-Band Contract dialog box, click Submit.
Step 5  Right-click Node Management EPGs and click Create Out-of-Band Management EPG.
An out-of-band management endpoint group consists of switches (leaves/spines) and Cisco APICs that are part of the associated out-of-band management zone.
Step 6  In the Create Out-of-Band Management EPG dialog box, perform the following tasks:
a)  In the Name field, enter a name for the EPG.
b)  Expand Provided Out-of-Band Contracts, and in the OOB Contract field, from the drop-down list, choose the name of the contract you created. Click Update, and click OK.
   The out-of-band contract is associated with the node management EPG.
c)  In the Create Out-of-Band Management EPG dialog box, click Submit.
Step 7  Right-click External Management Network Instance Profiles and click Create External Management Network Instance Profile.
Hosts that are part of regular endpoint groups cannot communicate with the nodes in the out-of-band management endpoint group. Any host that is part of a special group known as the instance profile can communicate with the nodes in an out-of-band management endpoint group using special out-of-band contracts.
Step 8  In the Create External Management Network Instance Profile dialog box, perform the following tasks:
a)  In the Name field, enter a name for the instance profile.
b)  Expand Consumed Out-of-Band Contracts, and in the Out-of-Band Contract field, from the drop-down list, choose the name of the contract you created. Click Update.
c)  Expand Subnets and type the external subnet IP address and subnet mask of the managing hosts. Click Update, and click OK.
   The out-of-band contract is associated with the subnet.
d)  In the Create External Management Network Instance Profile dialog box, click Submit.

Additional References for Out-of-Band Management Contracts

For more information on out-of-band management, see the Cisco Application Centric Infrastructure Fundamentals Guide at the following URL:
application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html