Improving Convergence Between On-Premises ACI Sites and Cloud Sites

Revised: October 13, 2022,

New and Changed Information

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

Release Version	Feature	Description
25.0(4)	Solution for faster convergence/ fast failover using Bidirectional Forwarding Detection Protocol in Cisco Cloud ACI hybrid cloud deployments.	This release provides solution for faster convergence/ fast failover using Bidirectional Forwarding Detection protocol in Cisco Cloud ACI hybrid cloud deployments

About Bidirectional Forwarding Detection Protocol

OSPF is primarily used as an underlay protocol for inter-site connectivity to a Cisco ACI on-premises datacenter in Cisco Cloud APIC deployments. The failover time (the time to switch to an alternate path when the initial path fails because the physical interface is down) with the OSPF timers is around 40 seconds. For more information about the bidirectional forwarding detection protocol, see IOS BFD Documentation

✎

Note   Although this document uses AWS Direct Connect as an example, the fast failover time applies to deployments with Direct Connect (AWS) and Express Route (Azure).

Beginning with release 25.0(4), the solution for faster traffic convergence/fast failover is the Bidirectional Forwarding Detection (BFD) protocol in Cisco Cloud ACI hybrid cloud deployments. The BFD protocol includes the exchange of BFD control packets between two systems to activate and maintain BFD neighbor sessions between routers.

Once the BFD has been enabled on the relevant interfaces and at the router level for the appropriate routing protocols the following steps occur:

1. A BFD Session is created

2. BFD timers are negotiated

3. The BFD Peers begin to send BFD Control packets to each other at the negotiated interval

Failure to receive these control packets in the negotiated duration will bring down BFD sessions, in turn, bringing down the corresponding protocol (in this case, the OSPF session used for inter-site connectivity). This will aide in faster convergence by having the overlay switched immediately to an alternate path.

Currently, the BFD timer is set for 1000 millisecs, based on the average round trip time from a local region to a datacenter.

Reference Topology For AWS Cloud APIC to Onprem ACI connectivity over AWS Direct Connect (DX)

Cisco Nexus Dashboard Orchestrator
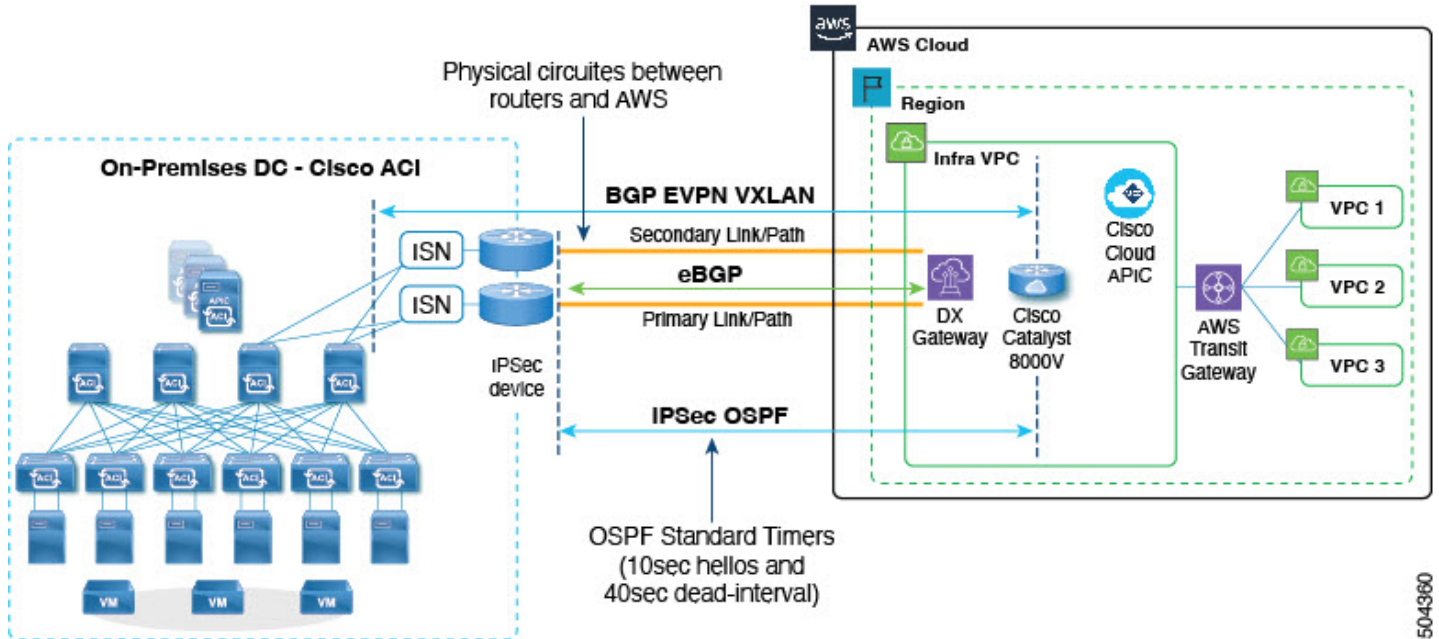
This example configuration has the following characteristics:-

1. Two Direct Connect routers for connectivity to cloud sites from a Cisco ACI on-premises datacenter.

2. **An Underlay** of 2 x 2 IPSec tunnels with OSPF to the 2 Cisco Catalyst 8000V in the cloud Infra

3. **An Overlay** of BGP EVPN with VXLAN encapsulation.

When one of the physical direct connect links fails, the expectation is a fast convergence of traffic by switching to the alternate direct connect link. Enabling the BFD protocol for OSPF on the IPSec tunnels will help in quick detection of the trigger and in turn help to bring down the corresponding OSPF session.

Supported Deployment Cases

The following inter-site connectivity deployment cases are supported with release 25.0(4):

1. For IPsec tunnel to onPrem with OSPF underlay Over Private Peering

2. For IPsec tunnel to onPrem with OSPF underlay Over Public Internet

Note For the Release 25.0(4) we only support BFD for inter-site connectivity for AWS and Azure from On-Premises Cisco ACI

Verifying and Changing BFD Configuration

How to Enable or Disable the BFD Protocol

The BFD protocol can be enabled or disabled between sites only from the Nexus Dashboard Orchestrator. The option to enable/disable the BFD protocol will be available under **Advanced Settings** as shown below.
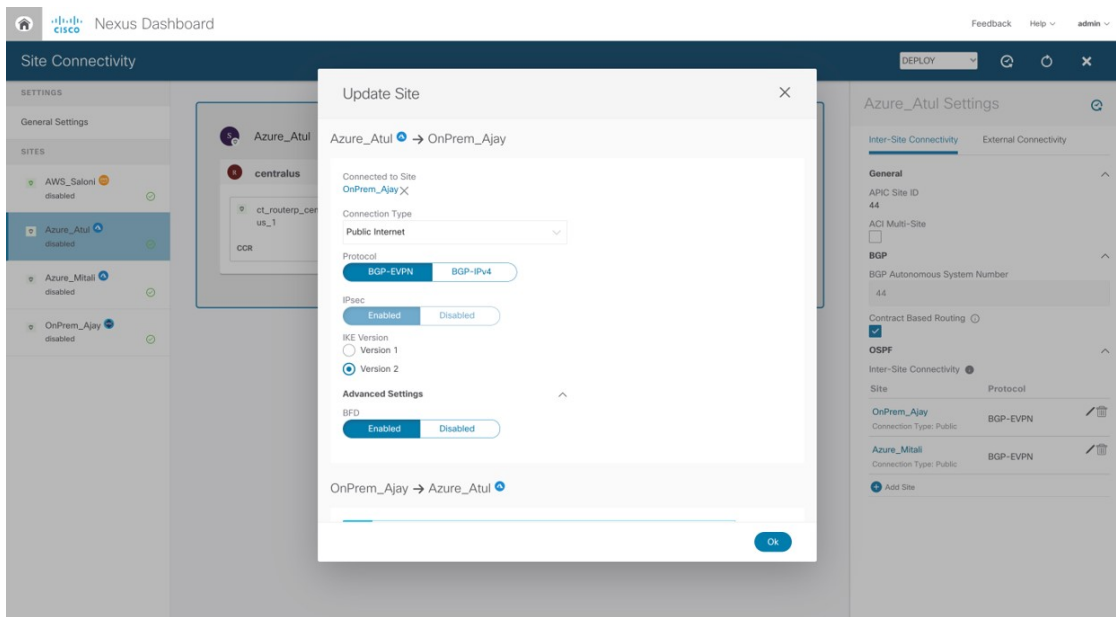
Note   BFD does not get enabled automatically for all deployments and tunnels. It needs to be enabled specifically for the intersite peerings that need BFD.

Verifying BFD Configuration

Based on the NDO configuration, Cloud APIC displays the operational status of the BFD protocol for each tunnel. The following information will be available under the **BFD Operational Settings** section -

1. **BFD Session Status** - The session status will either up or down depending on whether the BFD session is active or not.

2. **Echo Interval** - This displays the negotiated echo value.

3. **Tx Interval and Rx Interval** - These are the constant slow timers with the echo.

4. **Detection Multiplier** - This displays the negotiated multiplier value.

To view the Operational data in the Cloud APIC GUI, you can also follow the given path.

1. Click **Cloud Resources**.

2. Click **Routers**.

3. Select the Router for which you would like to view the Operational Data.

4. Expand the Router information view in a new tab.

5. Click on **Cloud Resources** in the Router information window.

6. Select **Tunnel** from the list of resources available on the left side.

Changing BFD Configuration

For the release 25.0(4), a default policy is auto-configured in Cisco Cloud APIC with default timer values which are only configurable by POST.

To modify the timer values to suit the latency in the deployment, the following REST API POST can be used -

```
<fvTenant name="infra">
<cloudBfdPol name="default" minTxIntervalMs="250" minRxIntervalMs="250" multiplier="4"/>
</fvTenant>
```

> **Note** The value for `minTxIntervalMs` and `minRxIntervalMs` can be set between 50- 9999 ms. The value for `multiplier` can be set between 3-50.

> **Note** Having timers that are too aggressive can cause session flaps.