High Availability in OpenFlow Mode

High Availability in OpenFlow mode supports Stateful Switchover (SSO) and Nonstop Forwarding (NSO). SSO works with NSF to minimize the amount of time a network is unavailable to its users following a switchover.

Restrictions for High Availability in OpenFlow Mode

- Stateful switchover (SSO) is not supported with Transport Layer Security (TLS).
- You cannot configure both TCP and Secure Socket Layer (SSL) connections on the OpenFlow controller.

Information About OpenFlow

The following sections provide more information about the feature.

High Availability in OpenFlow Mode

In Cisco IOS XE Bengaluru 17.5.1, Cisco Catalyst 9400 Series Switches support high availability in OpenFlow mode. A chassis-based platform, the Cisco Catalyst 9400 Series Switch supports dual supervisors. One of the supervisors act as the active, and the other as the standby.

Prior to the introduction of this feature, during a switchover, the OpenFlow controller deleted all installed flows on the device before resending all flows that led to the disruption of the forwarding traffic. Also during a switchover, the OpenFlow controller connection was reset, and re-established, and the controller deleted all installed flows.

With the high availability feature, the active supervisor establishes a connection with the OpenFlow controller, and all flows sent by the controller are programmed onto the device by the active supervisor. When the active supervisor fails due to software or hardware failure, or when a manual switchover from the active to standby supervisor is triggered, all flows are retained. The OpenFlow agent on the new active supervisor will continue

the TCP session with the OpenFlow controller, and the connection will not be terminated by the OpenFlow agent.

Stateful Switchover

Stateful switchover (SSO) maintains stateful protocol and application information to retain user session information during a switchover. The flows sent to the OpenFlow device by the controller are retained during a switchover from the active supervisor to the standby supervisor, so that the controller does not have to re-install the flows. It also provides a faster switchover relative to high system availability.

In devices that support dual supervisors, SSO takes advantage of the supervisor redundancy to increase the network availability. SSO establishes one of the supervisors as the active and the other as the standby, and then synchronizes critical state information between them. Following an initial synchronization between the two supervisors, SSO dynamically maintains state information between them.

SSO is used with the Cisco Nonstop Forwarding (NSF) feature.

With NSF, even during a switchover, packets are forwarded based on the flow entries programmed by the OpenFlow controller.

Symmetric High Availability

Symmetric high availability is when the both the active and standby supervisors are up and running before the active OpenFlow agent establishes an OpenFlow TCP connection with the OpenFlow controller.

In symmetric high availability mode, both the active and standby supervisors operate independently. Only the active supervisor exchanges OpenFlow protocol messages with the controller. All TCP packets received by the active supervisor from the OpenFlow controller are duplicated to the standby supervisor. The OpenFlow hardware table configuration, group table entries, and flow entries in both the active and standby supervisors are synchronized.

Asymmetric High Availability

In asymmetric high availability the standby supervisor boots up only after the active OpenFlow agent establishes an OpenFlow TCP connection with the controller. When the standby boot up, the flows installed by the controller on the active supervisor, and the TCP controller connection are not synchronized on the standby. The high availability process on the active supervisor does a bulk sync to synchronize the controller TCP connection, and sends flows, groups, OpenFlow Table Feature Message installed on the active to the standby supervisor. The statistics counters on the standby supervisor are synchronized next, so that the standby can receive the duplicated, controller sent packets.

When the standby supervisor fails to install the Table Feature Message sent by the active, the standby supervisor notifies the active of the failure. On receiving the failure information, the active supervisor will not initiate any further synchronization to the standby. The active supervisor will mark the installation failure as a bulk sync failure, logs an error message, and notifies the standby supervisor. The standby supervisor reloads upon receiving the message. In case of group mod and flow mod failures, the same process is followed.

Statistics are also synchronized from the active supervisor to the standby during the bulk sync. Statistics synchronization failure is ignored, because the statistics are synchronized dynamically every few seconds after the bulk sync.

Probe Interval

The active supervisor maintains the OpenFlow TCP connection with the controller through the management interface, GigabitEthernet 0/0, and this connection is synchronized with the standby supervisor. The active supervisor probes the controller-connection based on the configured probe interval.

After a switchover, the management interface on the new active takes a minimum of 13 seconds to become operational. Packets sent by the controller until then are not received, and this can lead to the disconnecting of the OpenFlow TCP connection. To avoid the OpenFlow agent timeout due to the probe-interval, a default value of 40 seconds is automatically configured on active supervisor.

How to Configure High Availability in OpenFlow Mode

Configuring High Availability in OpenFlow Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **openflow**
4. **switch 1 pipeline 1**
5. **controller ipv4** *ip-address* **port** *port-number* **vrf** *vrf-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**openflow** **Example:** `Device(config)# openflow`	Enables OpenFlow configuration and enters OpenFlow configuration mode.
Step 4	**switch 1 pipeline 1** **Example:** `Device(config-openflow)# switch 1 pipeline 1`	Configures a logical switch and pipeline, and enters OpenFlow switch configuration mode.
Step 5	**controller ipv4** *ip-address* **port** *port-number* **vrf** *vrf-name* **Example:**	Connects to an OpenFlow controller. **Note** High Availability is not supported with TLS.

	Command or Action	Purpose
	`Device(config-openflow-switch)# controller ipv4 10.2.2.2 port 6633 vrf Mgmt-vrf`	
Step 6	**end** **Example:** `Device(config-openflow-switch)# end`	Exits OpenFlow switch configuration mode and returns to privileged EXEC mode.

Configuration Examples for High Availability in OpenFlow Mode

Examples: Configuring High Availability in OpenFlow Mode

The following example shows how to configure high availability in OpenFlow mode:

```
Device> enable
Device# configure terminal
Device(config)# openflow
Device(config-openflow)# switch 1 pipeline 1
Device(config-openflow-switch)# controller ipv4 10.2.2.2 port 6633 vrf Mgmt-vrf
Device(config-openflow-switch)# end
```

Verifying the High Availability Configuration

The following is sample output from the **show openflow switch** *switch-number* **controller** command. The output fields, connected should be yes, state should be active, and the negotiated protocol version should the same on the standby supervisor.

```
Device# show openflow switch 1 controller

Logical Switch Id: 1
Total Controllers: 1

  Controller: 1
    172.16.18.85:6636
    Protocol: tcp
    VRF: Mgmt-vrf
    Connected: Yes
    Role: Equal
    Negotiated Protocol Version: OpenFlow 1.3
    Last Alive Ping: 2021-01-29 08:44:59 UTC
    state: ACTIVE
    sec_since_connect: 4893
```

The following is sample output from the **show tcp ha connection** command. The state should show ESTAB on both the active and standby supervisors.

```
Device# show tcp ha connection

 SSO enabled for 1 connections
TCB           Local Address         Foreign Address       (state)    Conn Id
```

```
7F53B1ADE1E0  172.21.18.87.23401    172.16.18.85.6636      ESTAB       1
```

Feature Information for High Availability in OpenFlow Mode

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for High Availability in OpenFlow Mode

Feature Name	Release	Feature Information
High Availability in OpenFlow Mode	Cisco IOS XE Bengaluru 17.5.1	High availability in OpenFlow mode supports SSO and NSO. In Cisco IOS XE Bengaluru 17.5.1, this feature was introduced on the following platform: • Catalyst 9400 Series Switches