Configuring OpenFlow

This chapter contains the following sections:

Information About OpenFlow

OpenFlow is a specification from the Open Networking Foundation (ONF) that defines a flow-based forwarding infrastructure (L2-L4 Ethernet switch model) and a standardized application programmatic interface (protocol definition) to learn capabilities, add and remove flow control entries and request statistics. OpenFlow allows a controller to direct the forwarding functions of a switch through a secure channel.

Cisco ONE Platform Kit provides the ability to host Cisco internal or external third party applications on or adjacent to Cisco's networking infrastructure, and enables programmatic access to networking services in a controlled and consistent manner. When hosting applications on Cisco routers or switches, the applications will run within a virtual-machine or container.

OpenFlow Limitations

The Cisco Nexus 5500 and Cisco Nexus 6000 switches do not support the OpenFlow action to rewrite the layer-2 destination MAC address. Therefore, the XNC controller use cases such as Topology Independent

Forwarding and Latency Optimized Forwarding may not be work correctly on the Cisco Nexus 5500 and Cisco Nexus 6000 switches.

Supported Interface Types

The following is a list of supported interface types:

- Regular Layer 2 physical ports (switchport)
- Layer 2 port channels

Unsupported Interface Types

The following is a list of unsupported interface types:

- Layer 3 ports (no switchport)
- Fabric extender ports
- Virtual Port-Channel (VPC) ports
- Layer 3 Port-Channel

Supported Interface Modes

The following is a list of supported interface modes:

- Access port
- Trunk port

Supported Match Fields

The following are lists of supported match fields:

- Layer 2 header
  - Ethertype
  - VLAN ID
  - VLAN priority (PCP)
  - Source MAC address
  - Destination MAC address
- Layer 3 header
  - Source IP address

    - Destination IP address
    - Layer 4 protocol
    - Differentiated services Code Point (DSCP)
- Layer 4 header
    - Source port
    - Destination port
- Ingress Interface

Supported Actions

The following is a list of supported actions:

- Redirect the packet to one output port
- Redirect the packet to multiple output ports
- Set the VLAN tag (vlan rewrite) on egress
- Strip the VLAN tag on egress
- Divert the datapath packet to the OpenFlow controller
- Drop the packet

Scale Flow Numbers

- The Cisco Nexus device supports a maximum of 65535 flows in total. The device supports a combination of up to 3500 ACL-table flows and 62K MAC-table flows.
- The Cisco Nexus device supports up to 64 flows when the action is punt-to-controller.

Pipeline Support

OpenFlow policies can be applied to the ACL-table and the MAC-table. OpenFlow relates tables by means of the ‘pipeline’ concept. The Cisco Nexus device supports two pipelines, 201 and 202. You can toggle the pipeline between 201and 202 by entering the **pipeline** *id* command in the openflow-agent logical switch configuration.

- Pipeline 201
    - All the flows are added to the ACL-table. For example, ACL TCAM.
    - ACL-table flows with the action as redirect or drop gets installed in the IFACL region of the ACL-TCAM.

- ACL-table flows with the action punt-to-controller are installed in the SUP region of the ACL-TCAM.

- Pipeline 202
  - Flows can be added to both the ACL-table(ACL TCAM) and the MAC-table(STM table).
  - Flows with only L2-dest-mac and VLAN as the match criteria are installed in the MAC-table. The remaining flows are installed in ACL-table
  - Supported actions for the MAC-table are redirect-to-port and drop.
  - The MAC-table supports a higher scale number than the ACL-table.

Prerequisites for OpenFlow

The OpenFlow agent requires the Cisco Nexus device to be configured with OpenFlow specific commands in order to support topology discovery and the installation of flows. The Cisco Nexus device works in a hybrid mode so that the default commands from the startup-config file are executed upon boot up. This might create an undesirable effect and therefore must be changed.

Note If you change or negate these required commands, it can lead to unpredictable system behavior.

VLAN Creation

The following command is used to create the necessary VLANs in an OpenFlow-controller switch. This command creates the OpenFlow specific VLANs in the VLAN database.

```
vlan x[-y]
```

Even with the hybrid-Ships-In-Night mode of operation, we recommend that you segregate the VLANs among the OpenFlow-controlled ports and the regular ports. You should take caution in ensuring that the VLANs are not shared among the OpenFlow and non-OpenFlow ports in order to prevent traffic leaks.

Interface Level Configurations

To make the interfaces connected to other switches receive spanned traffic, the interface is connected to the analyzer and configured to support OpenFlow. The **interface ethernet** command changes the parser to the interface submode. Before entering the **mode openflow** command which enables OpenFlow support on the interface, the following commands are required:

- **switchport mode trunk**
- **switchport trunk allowed vlan x-y**

In order for the strip-vlan functionality to work on the Cisco Nexus device, the trunk port must be configured with the native VLAN.

Cisco One controllers can perform topology discovery of OpenFlow enabled ports. To allow topology discovery on trunk ports, the native VLANs must be configured on trunk ports

switchport trunk native vlan z

When an interface is added to the OpenFlow logical switch, the following commands are applied to the interface implicitly:

- **mode openflow**
- **spanning-tree bpdufilter enable**
- **no lldp transmit**

Template Based TCAM Carving for OpenFlow

The Cisco Nexus device supports template-based TCAM carving. To configure OpenFlow on the device, you must make a number of changes to the TCAM carving regions using the template based TCAM carving commands.

To support higher scale numbers for OpenFlow policies, the IFACL-region of the TCAM must be recarved accordingly. To apply TCAM carving for a maximum flow scale, enter the following commands:

```
switch(config)# hardware profile tcam resource template openflow
switch(config-tcam-templ)# vacl 64
switch(config-tcam-templ)# ifacl 3520
switch(config-tcam-templ)# qos 128
switch(config-tcam-templ)# rbacl 64
switch(config-tcam-templ)# span 64
switch(config)# hardware profile tcam resource service-template openflow
```

Enter the following command to verify the TCAM carving: **show hardware profile tcam resource template** *tmplt-name*

Note Configuring TCAM carving requires that the Cisco Nexus device be reloaded.

Setting Up an OpenFlow Virtual Service

The virtual service manager allows you to enable the OpenFlow agent application to run as a virtual service on a container. To setup a virtual service for OpenFlow you must perform the following tasks:

- Download the application OVA package to your system.
- Install the OVA package for a named virtual service. For example:

```
switch#virtual-service install name openflow-agent package file-url
```

- Configure and activate the virtual service. For example:

```
switch(config)#virtual-service openflow-agent
switch(config-virt-serv)#activate
```

To upgrade a software package installed on a virtual service you use the **virtual-service upgrade name** *application-name* **package** *file-url* command.

Note An active virtual service can not be updated.

To remove a software package installed on a virtual service you use the **virtual-service uninstall name** *application-name* command.

Note An active virtual service can not be removed.

Enabling OpenFlow

OpenFlow capability is enabled by entering the **hardware profile openflow** command to allocate the hardware resources required for the OpenFlow agent. Following a switch reload, the **hardware profile** command is used to configure ACL Feature Manager (AFM) and Forwarding Manager (FWM) modules for OpenFlow functionality.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **hardware profile openflow**	Allocates the hardware resources required for the OpenFlow agent.
Step 3	switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts b copying the running configuration to the startup configuration.
Step 4	switch#**reload**	Reloads the operating system on the switch.

Configuring the OpenFlow Switch

You must enable OpenFlow on the switch, for the configuration to take effect.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	**openflow** **Example:** `switch(config)# openflow`	Enters OpenFlow configuration mode.
Step 3	**switch** *switch-number* **Example:** `switch(config-ofa)# switch 1`	Specifies the OpenFlow logical switch and enters OpenFlow switch configuration mode.
Step 4	**pipeline {201|202}**	Specifies the pipeline mode.

	Command or Action	Purpose
	Example: `switch(config-ofa-switch)# pipeline 201`	OpenFlow policies can be applied to the ACL-table and the MAC-table. Cisco Nexus devices support two pipelines, 201 and 202. This command allows you to switch between the supported pipeline modes.
Step 5	**controller ipv4** *ipv4-address* **port** *port-number***vrf** *vrf-name* **security** {**none** | **tls**} **Example:** `switch(config-ofa-switch)# controller ipv4 192.0.2.10 port 6653 vrf mnagement security none`	Establishes the connection with the controller over the specified VRF. You can disable or enable the TLS.
Step 6	**of-port interface** *interface-type slot / port* **Example:** `switch(config-ofa-switch)# interface ethernet 2/5`	Adds the interface to the OpenFlow logical switch.
Step 7	**default-miss cascade** {**drop** | **controller** | **normal**} **Example:** `switch(config-ofa-switch)# default-miss cascade normal`	Enables hybrid-normal mode on the switch. To change the OpenFlow agent from hybrid-normal to punt-to-controller mode use the **default-miss cascade controller** command. To change th OpenFlow agent from hybrid-normal to default-drop mode, use the **default-miss cascade drop** command.
Step 8	**max-backoff** *back-off-time* **Example:** `switch(config-ofa-switch)# max-backoff 7`	Sets the OpenFlow controller maximum backoff timer. The default value is 8 seconds.
Step 9	**probe-internal** *interval-time* **Example:** `switch(config-ofa-switch)# probe-interval 6`	Sets the OpenFlow controller probe interval timer. The default value is 5 seconds.
Step 10	**exit** **Example:** `switch(config-ofa-switch)# exit`	Exits OpenFlow switch configuration mode.
Step 11	**exit** **Example:** `switch(config-ofa)# exit`	Exits OpenFlow configuration mode.

Verifying OpenFlow

Use one of the following commands to verify the configuration:

Command	Purpose
show running-config | section openflow	Displays the OpenFlow running configuration information.
show running-config interface ethernet *slot*/*port*	Displays the running configuration for a specific ethernet interface.
show openflow *openflow-agent* **switch** *number* **controllers**	Displays information about the OpenFlow agent connectivity to controller
show openflow *openflow-agent* **switch** *number* **flows**	Displays information about the OpenFlow agent flows.
show openflow *openflow-agent* **switch** *number* **ports**	Displays information about the OpenFlow agent port status.