Configuring FEX-Based ACL Classification

This chapter contains the following sections:

- Information About FEX-based ACL Classification, on page 1
- Guidelines and Limitations for FEX-Based ACL Classification, on page 2
- Configuring FEX-Based ACL Classification, on page 3
- Verifying the FEX-Based ACL Classification, on page 8
- Configuration Examples for FEX-based ACL Classification, on page 8

Information About FEX-based ACL Classification

The Fabric Extender (FEX) based Access Control List (ACL) Classification feature uses ternary content addressable memory (TCAM) resources on a FEX to perform ACL-based packet classification of incoming packets on the switch.

Overview of FEX-based ACL Classification

The FEX-based ACL Classification feature uses TCAM resources on a FEX to perform ACL-based packet classification of incoming packets on the switch. When QoS policies are processed on a FEX, the policies are enforced on the switch and on the associated FEX or FEXes.

By default this feature is disabled. When the feature is enabled, and if the existing system-level QoS policy is accepted by the FEX, the QoS policy is enforced by the FEX. If the existing system-level QoS policy is not accepted by the FEX, an error message is displayed and the fabric ports associated with the FEX are error-disabled, which prevents the FEX from being online.

If the feature is disabled, the existing system-level QoS policy is removed from the FEX and the enforcement of the existing QoS policy is changed from ACL-based to CoS-based. The TCAM entries are removed and packet classification on the FEX is done using the cos2q map in the FEX hardware.

When this feature is enabled, QoS policies are enforced as follows:

- System level QoS policies are enforced on a FEX in the ACL-based approach. That is, TCAM entries are created and programed on FEX ASICs. If the QoS policy is not accepted on a FEX, the command is rejected and an error message is generated. A system level QoS policy is always programmed and enforced completely on the switches and all associated FEXes.

- Interface level QoS policies are enforced on the FEX. That is, TCAM entries in the corresponding FEX ASIC are taken and programmed. If the QoS policy is not accepted on the target interface, the command is rejected and an error message is generated.

Guidelines and Limitations for FEX-Based ACL Classification

When you are configuring Fabric Extender (FEX)-based Access Control List (ACL) classification, you should be aware of the following guidelines and limitations:

- FEX-based ACL classification can be configured for the following interfaces:
  - Global
  - Host interface (HIF) ports
  - HIF port channels
  - VPC
  - 2-Layer VPC
- Only QoS policies are applied at system-level, HIF ports and HIF port channels will be offloaded to FEX platforms.
- In each switching subsystem (SS) on the FEX ASIC, interface-level policies are programmed in TCAM entries in a top-down fashion and system-level policies are programmed in a bottom-up fashion.
- All the match and set criteria supported in a QoS policy are supported even when a policer is present in the policy. FEX supports Layer 3 operations (fragments) and Layer 4 operations (source and destination port ranges). However, policies with TCP flags or Layer 2 operations are not allowed on FEX interfaces.
- QoS policies are not supported on HIF ports that have Virtual Ethernet Interfaces (VETHs) attached.
- If a QoS policy is applied to a HIF port, the classification is applied only to incoming traffic with no VNTAG.
- You could define match criteria for a QoS policy so that the criteria also matches the control protocol traffic. If you configure the policy on a HIF port, the control traffic could also get policed. Therefore, the match criteria should be very specific to the required flow of traffic.
- If a QoS policy is configured on a HIF port or a port channel, the policy is enforced by the FEX and not the switch. However, policy rewrites occur on the switch only.
- Because TCAM entries are not available at network interface (NIF) ports, network-to-host (N2H) traffic is not classified in an ACL-based manner. Instead, N2H traffic is classified in a CoS-based manner.
- ACL-based QoS policy offload is supported on the following platforms:
  - N2224TP Fabric Extender 24x1G 2x10G SFP+ Module
  - N2232P Fabric Extender 32x10G SFP+ 8x10G SFP+ Module
  - N2232TM Fabric Extender 32x10GBase-T 8x10G SFP+ Module
  - N2248T Fabric Extender 48x1G 4x10G SFP+ Module
  - N2248TP E Fabric Extender 48x1G 4x10G SFP+ Module

- N2248PQ Fabric Extender 48x10G SFP+ 16x10G SFP+ Module
- N2232TM-E Fabric Extender 32x10GBase-T 8x10G SFP+ Module
- NB22IBM Fabric Extender 14x10G SFP+ 8x10G SFP+ Module
- N2348UPQ Fabric Extender 6x40G QSFP 48x10G SFP+ FEX

- When a policy is offloaded, the number of access control entries (ACEs) in the policy, which are applied on the FEX, should not exceed 30.

Note In Cisco NX-OS Release 7.3(x), the FEX offload capability using interface QoS policies is upto 100 ACEs, and upto only 30 ACEs using system QoS policies.

- ACL-based QoS policy offload is not supported on the following platforms:
  - N2148T Fabric Extender 48x1G 4x10G SFP+ Module

Configuring FEX-Based ACL Classification

Configuring FEX ACL-based QoS Policy Enforcement

To configure the FEX ACL-based QoS policy enforcement, you must enable policy offloading on each Fabric Extender individually. When you enable the feature on a FEX and if the existing system-level QoS policy is accepted by the FEX, the QoS policy is enforced by the FEX. However, if the existing system-level QoS policy is not accepted by the FEX, the fabric ports associated with the FEX are error-disabled, which then prevents the FEX from being online.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	**FEX** *chassis_ID* **Example:** `switch(config)# fex 101`	Enters fabric extender configuration mode.
Step 3	**hardware** *card-type* **qos-policy-offload** **Example:** `switch(config-fex)# hardware N2232P qos-policy-offload`	Enables QoS policy offloading on a Cisco Nexus N2232P Fabric Extender. **Note** When a policy is offloaded, the number of access control entries (ACEs) in the policy, which are applied on the FEX, should not exceed 30.

	Command or Action	Purpose
Step 4	**exit** **Example:** `switch(config-fex)# exit`	Updates the configuration and exits fabric extender configuration mode.
Step 5	(Optional) switch(config-if)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring the FEX ACL-based Interface-Level QoS Policy

When FEX ACL-based QoS policy enforcement is enabled and the interface-level QoS policy is applied successfully, two TCAM entries are created at the top of the TCAM region on the FEX ASIC.

Before you begin

You must enable FEX ACL-based QoS policy enforcement on the switch and on any fabric extenders that you want to use.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	**class-map type qos match-all** *class-name* **Example:** `switch(config)# class-map type qos match-all cmap-qos01`	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**match access-group name** *acl-name* **Example:** `switch(config-cmap-qos)# match access-group name acl-01`	Specifies the named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class.
Step 4	**exit** **Example:** `switch(config-cmap-qos)# exit`	Updates the configuration and exits class map configuration mode.
Step 5	**policy-map type qos** *policy-name* **Example:** `switch(config)# policy-map type qos pmap-qos01`	Creates a named object that represents a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.

	Command or Action	Purpose
Step 6	**class** *class-name* **Example:** `switch(config-pmap-qos)# class cmap-qos01`	Associates a class map with the policy map, and enters configuration mode for the specified system class. **Note** The associated class map must be the same type as the policy map type.
Step 7	**set qos-group** *qos-group-value* **Example:** `switch(config-pmap-c-qos)# set qos-group 1`	Configures one or more **qos-group** values to match on for classification of traffic into this class map. There is no default value.
Step 8	**interface ethernet** *fex-id/slot/port* **Example:** `switch(config)# interface ethernet 127/1/1`	Enters interface configuration mode.
Step 9	**service-policy type qos input** *policy-map-name* **Example:** `switch(config-if)# service-policy type qos input pmap-qos01`	Attaches the policy map to the interface.
Step 10	**exit** **Example:** `switch(config-if)# exit`	Updates the configuration and exits interface configuration mode.

When the policy is successfully applied, two TCAM entries are created at the top of the TCAM region on the FEX ASIC. The following is an example of that TCAM entry:

```
K-keyType, L-label, B-bindcheck, DH-L2DA, CT-cdceTrnst
    L(IF-ifacl V-vacl Q-qos R-rbacl)

    [8]> K:IP (3/0) IN v4 L-[Q-ff/8 ]
    [8]  SA:ffffff00/c0a80200 DA:00000000/00000000
    [8]-> cos_rw:0 cos:4 de_rw:0 de:0 fwd_to_cpu:0 cos2q_ow:1

    [9]> K:IP/ETH (2/0) IN L-[Q-ff/8 ]
    [9]-> cos_rw:0 cos:2 de_rw:0 de:0 fwd_to_cpu:0 cos2q_ow:1
```

Configuring FEX ACL-based System-Level QoS Policy

When FEX ACL-based QoS policy enforcement is enabled and the system-level QoS policy is applied successfully, two TCAM entries are created at the bottom of the TCAM region on the FEX ASIC.

Before you begin

You must enable FEX ACL-based QoS policy enforcement on the switch and on any fabric extenders that you want to use.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	**class-map type qos match-all** *class-name* **Example:** `switch(config)# class-map type qos match-all cmap-qos01`	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**match access-group name** *acl-name* **Example:** `switch(config-cmap-qos)# match access-group name acl-01`	Specifies the named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class.
Step 4	**exit** **Example:** `switch(config-cmap-qos)# exit`	Updates the configuration and exits class map configuration mode.
Step 5	**policy-map type qos** *policy-name* **Example:** `switch(config)# policy-map type qos pmap-qos01`	Creates a named object that represents a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 6	**class** *class-name* **Example:** `switch(config-pmap-qos)# class cmap-qos01`	Associates a class map with the policy map, and enters configuration mode for the specified system class. **Note** The associated class map must be the same type as the policy map type.
Step 7	**set qos-group** *qos-group-value* **Example:** `switch(config-pmap-c-qos)# set qos-group 1`	Configures one or more **qos-group** values to match on for classification of traffic into this class map. There is no default value.
Step 8	**system** *system-name* **Example:** `switch(config)# system qos`	Enters QoS system configuration mode.
Step 9	**service-policy type qos input** *policy-map-name*	Attaches the classification policy to the system.

	Command or Action	Purpose
	Example: `switch(config-sys-qos)# service-policy type qos input pmap-qos01`	
Step 10	**exit** **Example:** `switch(config-sys-qos)# exit`	Updates the configuration and exits QoS system configuration mode.

When the policy is successfully applied, two TCAM entries are created at the bottom of the TCAM region on the FEX ASIC. The following is an example of that TCAM entry:

```
K-keyType, L-label, B-bindcheck, DH-L2DA, CT-cdceTrnst
    L(IF-ifacl V-vacl Q-qos R-rbacl)

    [253]> K:IP (3/0) IN v4 L-[]
    [253]  SA:ffffff00/c0a80200 DA:00000000/00000000
    [253]-> cos_rw:0 cos:4 de_rw:0 de:0 fwd_to_cpu:0 cos2q_ow:1

    [254]> K:ALL (0/0) IN L-[]
    [254]-> cos_rw:0 cos:2 de_rw:0 de:0 fwd_to_cpu:0 cos2q_ow:1
```

Disabling FEX ACL-based QoS Policy Enforcement

You can disable FEX ACL-based QoS policy enforcement for an individual FEX. If you disable the feature the existing system-level QoS policy is removed from the FEX and the enforcement of the existing QoS policy is changed from ACL-based to CoS-based. In addition, the TCAM entries are removed and packet classification on the FEX is done using the cos2q map in the FEX hardware.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	**FEX** *chassis_ID* **Example:** `switch(config)# fex 101`	Enters fabric extender configuration mode.
Step 3	**no hardware** *card-type* **qos-policy-offload** **Example:** `switch(config-fex)# no hardware N2232P qos-policy-offload`	Disables QoS policy offloading on a Cisco Nexus N2232P Fabric Extender.
Step 4	**exit** **Example:** `switch(config-fex)# exit`	Updates the configuration and exits fabric extender configuration mode.
Step 5	(Optional) switch(config-if)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Verifying the FEX-Based ACL Classification

To verify FEX-based ACL classification, perform one of these tasks:

Command	Purpose
show running-config	Displays the contents of the currently running configuration file, including information on FEX-based ACL classification settings.
show queueing interface	Displays the queuing information for FEX Ethernet interfaces, including information about the QoS configuration.

Configuration Examples for FEX-based ACL Classification

The following example shows how to create an IPv4 access control list (ACL):

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics
```

The following example shows how to enable the FEX-based ACL Classification feature on the switch and on a Cisco Nexus N2232P Fabric Extender associated with the switch:

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# hardware N2232P qos-policy-offload
switch(config-fex)# exit
```

The following example shows how to configure an ACL-based QoS policy at interface-level for use with the FEX ACL-based QoS policy enforcement feature:

```
switch# configure terminal
switch(config)# class-map type qos match-all cmap-qos01
switch(config-cmap-qos)# match access-group name acl-01
switch(config-cmap-qos)# exit
switch(config)# policy-map type qos pmap-qos01
switch(config-pmap-qos)# class cmap-qos01
switch(config-pmap-c-qos)# set qos-group 2
switch(config)# interface ethernet 101/1/1
switch(config-if)# service-policy type qos input pmap-qos01
switch(config-if)# exit
```

The following example shows how to configure an ACL-based QoS policy at system-level for use with the FEX ACL-based QoS policy enforcement feature:

```
switch# configure terminal
switch(config)# class-map type qos match-all cmap-qos01
switch(config-cmap-qos)# match access-group name acl-01
switch(config-cmap-qos)# exit
switch(config)# policy-map type qos pmap-qos01
switch(config-pmap-qos)# class cmap-qos01
switch(config-pmap-c-qos)# set qos-group 2
switch(config)# system qos
switch(config-sys-qos)# service-policy type qos input pmap-qos01
switch(config-sys-qos)# exit
```

The following example shows how to disable the FEX-based ACL Classification feature on the switch and on a Cisco Nexus N2232P Fabric Extender associated with the switch:

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# no hardware N2232P qos-policy-offload
switch(config-fex)# exit
```

The following example shows how to display the ACL-based QoS policy configuration:

```
switch(config-pmap-nq)# show queuing interface ethernet 108/1/48
if_slot 40, ifidx 0x1f6b0bc0
Ethernet108/1/48 queuing information:
  Input buffer allocation:
  Qos-group: 0  2  (shared)
  frh: 2
  drop-type: drop
  cos: 0 1 2 3 4 5 6
  xon       xoff      buffer-size
  ---------+---------+-----------
  34560     39680     48640

  Queueing:
  queue    qos-group    cos            priority  bandwidth mtu
  --------+------------+--------------+---------+---------+----
  2        0            0 1 2 3 4 5 6   WRR        10      1600
  4        2                            WRR         0      1600

  Queue limit: 66560 bytes

  Queue Statistics:
  queue  rx              tx
  ------+---------------+---------------
  2      0               5103082
  4      5103093         0

  Port Statistics:
  rx drop         rx mcast drop   rx error        tx drop         mux ovflow
  ---------------+---------------+---------------+---------------+--------------
  0               0               0               0               InActive

  Priority-flow-control enabled: no
  Flow-control status:
  cos     qos-group   rx pause  tx pause  masked rx pause
  -------+-----------+---------+---------+---------------
  0              0    xon       xon       xon
  1              0    xon       xon       xon
  2              0    xon       xon       xon
  3              0    xon       xon       xon
  4              0    xon       xon       xon
  5              0    xon       xon       xon
  6              0    xon       xon       xon
  7            n/a    xon       xon       xon
```