



CHAPTER 3

Fabric Extender Features

The Cisco Nexus 2000 Series Fabric Extender allows a single switch—and a single consistent set of switch features—to be supported across a large number of hosts and servers. By supporting a large server-domain under a single management entity, policies can be enforced more efficiently.

Some of the features of the parent switch cannot be extended onto the Fabric Extender.

This chapter describes the supported features of the Fabric Extender and includes the following sections:

- [Host Interfaces, page 3-1](#)
- [VLANs and Private VLANs, page 3-1](#)
- [Quality of Service, page 3-2](#)
- [Access Control Lists, page 3-2](#)
- [Switched Port Analyzer, page 3-2](#)
- [Fabric Interface Features, page 3-3](#)

Host Interfaces

Host interfaces are for host or server connectivity only; host interfaces cannot connect to another network. These interfaces are always enabled as edge ports; as they come up, these ports immediately transition to the forwarding state. Host interfaces are always enabled with BPDU Guard. If a BPDU is received, the port is immediately placed in an error-disabled state which keeps the link down.

You can enable host interfaces to accept Cisco Discovery Protocol (CDP) packets. This protocol only works when it is enabled for both ends of a link.

Ingress and egress packet counters are provided on each host interface.

IGMP snooping is supported on all host interfaces.

EtherChannel port bundling is not supported on host interfaces. The Fabric Extender supports a single EtherChannel on its fabric interfaces, allowing you to bundle its uplinks to the parent switch.

VLANs and Private VLANs

The Fabric Extender supports Layer 2 VLAN trunks and IEEE 802.1Q VLAN encapsulation. Host interfaces can be members of private VLANs with the following restrictions:

- You can configure a host interface as an isolated or community access port only.

Send feedback to nx5000-docfeedback@cisco.com

- You cannot configure a host interface as a promiscuous port.
- You cannot configure a host interface as a PVLAN trunk port.

Quality of Service

The Fabric Extender provides two user queues for its quality of service (QoS) support, one for all no-drop classes and one for all drop classes. The classes configured on its parent switch are mapped to one of these two queues; traffic for no-drop classes is mapped one queue and traffic for all drop classes is mapped to the other. Egress policies are also restricted to these two classes.

The parent switch provides two predefined class maps for matching broadcast or multicast traffic; class-all-flood and class-ip-multicast. These classes are ignored on the Fabric Extender.

Host interfaces support pause frames, implemented using IEEE 802.3x link-level flow control (LLC). By default, flow control send is on and flow control receive is off on all host interfaces. Autonegotiation is enabled on the host interfaces. Per class flow control is set according to the QoS classes.

Host interfaces support jumbo frames (up to 9216 bytes); however a per-host interface maximum transmission unit (MTU) is not supported. Instead, MTU is set according to the QoS classes. You modify MTU by setting policy and class maps on the parent switch. Because the Fabric Extender has only two user queues, the MTU for the drop-queue is set to the maximum MTU of all drop classes MTU on the no-drop queue is set to the maximum MTU of all no-drop classes.

For more information about quality of service, see the *Cisco Nexus 5000 Series CLI Software Configuration Guide*.

Access Control Lists

The Fabric Extender supports the full range of ingress access control lists (ACLs) that are available on its parent switch.



Note

These ACLs are supported only if the Fabric Extender-to-parent switch fabric connection is in static pinning mode (for more information, see the [“Static Pinning Fabric Interface Connection”](#) section on page 1-5).

Switched Port Analyzer

You can configure the host interfaces on the Fabric Extender as Switched Port Analyzer (SPAN) source ports. Fabric Extender ports cannot be configured as a SPAN destination. Only one SPAN session is supported for all the host interfaces on the same Fabric Extender. Ingress source (Rx), egress source (Tx), or both monitoring is supported.



Note

All IP multicast traffic on the set of VLANs that a Fabric Extender host interface belongs to is captured in the SPAN session. It is not possible to separate the traffic by IP multicast group membership.

Send feedback to nx5000-docfeedback@cisco.com

If ingress and egress monitoring is configured for host interfaces on the same Fabric Extender, you may see a packet twice: once as the packet ingresses on an interface with Rx configured, and again as the packet egresses on an interface with Tx configured.

Fabric Interface Features

The Fabric Extender fabric interfaces support static EtherChannel and priority flow control (PFC). PFC allows you to apply pause functionality to specific classes of traffic on an interface (instead of all the traffic on the interface). During the initial discovery and association process, SFP+ validation and digital optical monitoring (DOM) are performed as follows:

- The Fabric Extender performs a local check on the uplink SFP+ transceiver. If it fails the security check, the LED flashes but the link is still allowed to come up.
- The Fabric Extender local check is bypassed if it is running its backup image.
- The parent switch performs SFP validation again during fabric interface bring up. It keeps the fabric interface down if SFP validation fails.

Once an interface on the parent switch is configured in fex-fabric mode, all other features that were configured on that port and are not relevant to this mode are deactivated. If the interface is reconfigured to remove fex-fabric mode, the previous configurations are reactivated.



Note

Per class flow control mode is enabled by default on the fabric interfaces. When a fabric interface is configured on the parent switch, PFC mode is enabled by default and cannot be changed.

Send feedback to nx5000-docfeedback@cisco.com