CHAPTER 1

# Cisco Nexus 2000 Series Fabric Extenders

This chapter provide information on Cisco Nexus 2000 Series Fabric Extenders (FEXs). This chapter contains the following sections:

- Loop Prevention Enhancement on FEXs, page 1-1
- Traffic Storm Control, page 1-2

## Loop Prevention Enhancement on FEXs

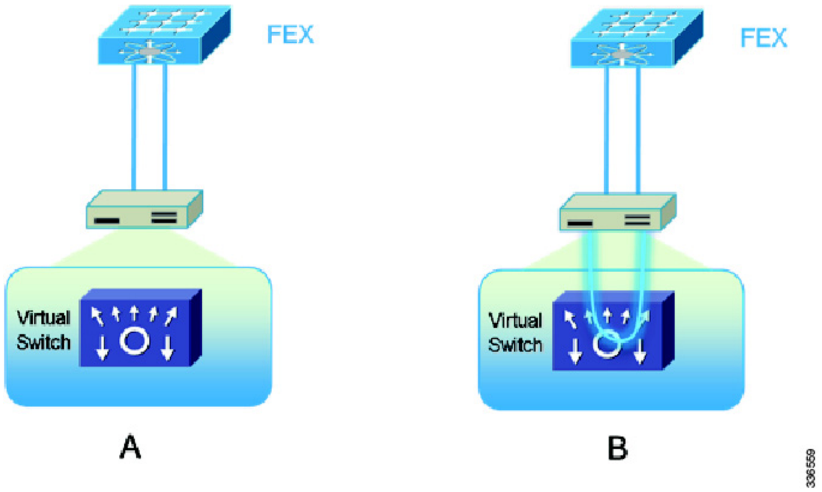
The FEX has two types of interfaces:

- Host Interfaces (HIFs) - Ports that you use to connect to the end host or server device.
- Network Interfaces (NIFs) - Ports that you use to connect to the parent switches. For more information on NIFs , see the "Network Interface Traffic Storm Control" section on page 1-3.

HIF interfaces are always configured as an edge port with Bridge Protocol Data Unit (BPDU) Guard enabled. The BPDU Guard detects loops within a network by sending BPDU messages to the port and putting the port into an error-disabled state. When an HIF experiences a linkup, the BPDU Guard sends out ten BPDUs to prevent any loops within the Layer 2 domain. A BPDU filter is then enabled on the interface and no additional BPDUs are sent out.

You can connect an HIF to a Hypervisor that contains a virtual network. Initially, the virtual network does not bridge the two ports on a server so it does not create a loop. However, a loop might occur if you make any adjustments to the configuration. In this case, the loop prevention mechanism of sending BPDUs at the linkup stage does not work because the links between the FEX and the server stay up. Figure 1-1shows how a loop might occur within a virtual network.

*Figure 1-1 FEX Connection to a Virtual Server*



To help with the detection of a loop in this environment, enter the **spanning-tree bpdufilter disable** command to enable the HIF ports to send out BPDUs. To enable the **spanning-tree bpdufilter disable** command, you must enter interface configuration mode. This example shows how to enable the feature on the port Ethernet 101/1/10:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface Ethernet 101/1/10
switch (config-if)# spanning-tree bpdufilter disable
switch (config-if)#
```

# Traffic Storm Control

A traffic storm occurs when packets flood the LAN and create excessive traffic and degrade network performance. You can use the traffic storm control feature to prevent LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces. Traffic storm control enables you to configure the traffic level to monitor the levels of the incoming broadcast, multicast, and unicast traffic over a 10-microsecond interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on that port, traffic storm control drops the traffic until the interval ends.

**Note** By default, Cisco NX-OS takes no corrective action when the traffic exceeds the configured level.

In the Nexus FEX architecture, the traffic storm control feature is implemented using the hardware resource on the Cisco Nexus 5500 and Cisco Nexus 6000 Series switches. For more information on implementiing the traffic storm control feature, see the *Cisco Nexus 2000 Fabric Extenders Hardware Installation Guide*.

**Note** This feature is not supported in the FEX architecture with the Cisco Nexus 5000 switch.

For more information about Fabric Extenders see the *Cisco Nexus 2000 Fabric Extenders Software Configuration Guide.*

# Network Interface Traffic Storm Control

Network interfaces (NIFs) are the uplinks interfaces on the FEX. The parent switch initiates an NIF traffic storm by monitoring the ingress traffic on the fabric ports. You can use these two methods to connect the FEX to the parent switch:

- Static pinning fabric interface connection.
- EtherChannel fabric interface connection.

With static pinning fabric interface connection, the NIF traffic storm control is configured under the physical fabric interface. The downlink host interfaces on the FEX are pinned to the fabric interfaces in the order that they were initially configured.

This example shows to configure a static pinning fabric interface connection to a switch:

```
switch(config)# interface type slot/port
switch(config-if)# storm-control { broadcast | multicast | unicast } level whole[.decimal]
```

With an EtherChannel fabric interface connection, the NIF traffic storm control feature is configured under the EtherChannel interface, which means that packets are evenly distributed over the links within the EtherChannel. If all the links within the EtherChannel are inside the same port application-specific integrated circuit (ASIC), the port ASIC is programmed with the configured level. If the links spread between different port ASICs, each ASIC is programmed proportionally to the links within the same ASIC. For example, an EtherChannel with three 10 Gigabit Ethernet links is configured with a storm-control level of 80 percent. Two 10 Gigabit Ethernet links are managed by port ASIC A. The third 10 Gigabit Ethernet link is managed by port ASIC B. Port ASIC A is programmed to monitor traffic with a threshold of 16 Gbps on both ports. Port ASIC B is programmed to monitor traffic with a threshold of 8 Gbps for that single port. If the FEX is dual home to two virtual port channnel (vPC) peered switches, you must ensure that both vPC peered switches have the same storm-control configuration under the EtherChannel interfaces.

This example shows how to configure an EtherChannel Fabric Interface connection to a switch:

```
switch(config)# interface port-channel number
switch(config-if)# storm-control { broadcast | multicast | unicast } level whole[.decimal]
```