
# Configuring Switching on DCNM-LAN Client

This chapter briefly introduces the following features:



For detailed configuration guide, please refer to Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x.

# Configuring VLANs

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure virtual LANs (VLANs) on NX-OS devices.

*A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment.*

*Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in that VLAN. Each VLAN is considered as a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a bridge or a router.*

*All ports are assigned to the default VLAN (VLAN1) when the device first comes up. A VLAN interface, or switched virtual interface (SVI), is a Layer 3 interface that is created to provide communication between VLANs.*

*The devices support 4094 VLANs in accordance with the IEEE 802.1Q standard. These VLANs are organized into several ranges, and you use each range slightly differently. Some of these VLANs are reserved for internal use by the device and are not available for configuration.*

**Note** *Inter-Switch Link (ISL) trunking is not supported on the Cisco NX-OS.*

# Configuring Private VLANs

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure private VLANs. Private VLANs provide additional protection at the Layer 2 level.

Private VLANs provide traffic separation and security at the Layer 2 level.

A private VLAN is one or more pairs of a primary VLAN and a secondary VLAN, all with the same primary VLAN. The two types of secondary VLANs are isolated and community VLANs. Hosts on isolated VLANs communicate only with hosts in the primary VLAN. Hosts in a community VLAN can communicate only among themselves and with hosts in the primary VLAN but not with hosts in isolated VLANs or in other community VLANs.

Regardless of the combination of isolated and community secondary VLANs, all interfaces within the primary VLAN comprise one Layer 2 domain, and therefore, require only one IP subnet.

# Configuring STP Extensions

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure Spanning Tree Protocol (STP) extensions on Cisco Nexus 7000 Series NX-OS devices.

*The software supports the following Cisco proprietary features:*

- *Spanning tree port types—The default spanning tree port type is normal. You can configure interfaces connected to Layer 2 hosts as edge ports and interfaces connected to Layer 2 switches or bridges as network ports.*
- *Bridge Assurance—Once you configure a port as a network port, Bridge Assurance sends BPDUs on all ports and moves a port into the blocking state if it no longer receives BPDUs. This enhancement is available only when you are running Rapid PVST+ or MST.*
- *BPDU Guard—BPDU Guard shuts down the port if that port receives a BPDU.*
- *BPDU Filter—BPDU Filter suppresses sending and receiving BPDUs on the port.*
- *Loop Guard—Loop guard helps prevent bridging loops that could occur because of a unidirectional link failure on a point-to-point link.*
- *Root Guard—The root guard feature prevents a port from becoming root port or blocked port. If a port configured for root guard receives a superior BPDU, the port immediately goes to the root-inconsistent (blocked) state.*

# Configuring Rapid PVST+

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure the Rapid per VLAN Spanning Tree (Rapid PVST+) protocol on NX-OS devices.

# Configuring MST

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure Multiple Spanning Tree (MST) on NX-OS devices.

For more information about the Data Center Network Manager features, see the *Cisco DCNM Fundamentals Configuration Guide.*

# Configuring Link-State Tracking

**Note** The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure link-state tracking on the Cisco Nexus 4000 Series device.

The link-state tracking feature binds the link state of multiple interfaces and provides redundancy in the network. In link-state tracking, you configure the server network adapters in a primary or secondary relationship known as teaming. The interfaces are grouped into link-state groups and if the link is lost on a primary interface, connectivity transparently moves to the secondary interface.

**Note** Link-state tracking is applicable only for the Cisco Nexus 4000 Series platform, beginning with the DCNM 4.2(3) release.

# Configuring FabricPath Switching

**Note** You must have an F Series module installed in your Cisco Nexus 7000 Series chassis in order to run FabricPath and conversational learning.

FabricPath switching allows multipath networking at the Layer 2 level. The FabricPath network still delivers packets on a best-effort basis (which is similar to the Classical Ethernet [CE] network), but the FabricPath network can use multiple paths for Layer 2 traffic.

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure FabricPath switching on the Cisco Nexus 7000 Series NX-OS devices.

# FabricPath Forwarding

Beginning with Cisco Release 5.1(2) for the Nexus 700 Series devices, you can create additional, nondefault FabricPath topologies. Each additional topology also has two forwarding trees. Additionally, you can display information about the interfaces and reachability status of the FabricPath network.

**Note** See the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* for more information on displaying the FabricPath topologies.

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes the forwarding behavior of FabricPath on the Cisco Nexus 7000 Series NX-OS devices.

# Configuring Advanced FabricPath Features

You can do advanced configurations using FabricPath for the FabricPath Intermediate System-to-Intermediate System (IS-IS) protocol.

For more information about the Data Center Network Manager features, see the Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x.

# Using the Layer 2 Security Audit Wizard

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to use the Layer 2 Security Audit Wizard.

The Security Audit Wizard allows you to examine the existing Layer 2 security features such as port security, dynamic ARP inspection (DAI), DHCP snooping, IP Source Guard, and traffic storm control configured on different devices. It also allows you to report and apply configurations that are missing on the device.

For more information about the Data Center Network Manager features, see the *Cisco DCNM Fundamentals Configuration Guide.*

# Configuring Dynamic ARP Inspection

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure dynamic Address Resolution Protocol (ARP) inspection (DAI) on an NX-OS device.

Dynamic ARP inspection (DAI) ensures that only valid ARP requests and responses are relayed. When DAI is enabled and properly configured, a device performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets

DAI can determine the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the device. It can also contain static entries that you create. If the ARP packet is received on a trusted interface, the device forwards the packet without any checks. On untrusted interfaces, the device forwards the packet only if it is valid.

**Note** The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this section. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

**Note** System-message logging levels for DAI must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* .

For more information about the Data Center Network Manager features, see the *Cisco DCNM Fundamentals Configuration Guide.*

# Configuring Port Security

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure port security on NX-OS devices.

You can use port security to configure Layer 2 Ethernet interfaces and Layer 2 port-channel interfaces that allow inbound traffic from only a restricted set of MAC addresses. The MAC addresses in the restricted set are called secure MAC addresses. In addition, the device does not allow traffic from these MAC addresses on another interface within the same VLAN. The number of MAC addresses that the device can secure is configurable per interface.

**Note** The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this section. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.This chapter includes the following sections:

**Note** System-message logging levels for port security must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* .

For more information about the Data Center Network Manager features, see the *Cisco DCNM Fundamentals Configuration Guide.*

# Configuring DHCP Snooping

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping on an NX-OS device.

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. DHCP snooping performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- (Not in 4.0) Rate-limits DHCP traffic from trusted and untrusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

Dynamic ARP inspection (DAI) and IP Source Guard also use information stored in the DHCP snooping binding database.

**Note** The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this section. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

**Note** System-message logging levels for DHCP snooping must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* .

# Configuring IP Source Guard

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure IP Source Guard on NX-OS devices.

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings:

- Entries in the DHCP snooping binding table.
- Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent attacks that rely on spoofing the IP address of a valid host. To circumvent IP Source Guard, an attacker would have to spoof both the IP address and the MAC address of a valid host.

**Note** The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this section. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

**Note** System-message logging levels for IP Source Guard must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* .

# Configuring Traffic Storm Control

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure traffic storm control on the NX-OS device.

Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming traffic over a 1-second 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 the port, traffic storm control drops the traffic until the interval ends.

# Configuring IGMP Snooping

**Note** The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

**Note** Cisco recommends that you do not disable IGPM snooping on the device. If you disable IGMP snooping, you may see reduced multicast performance because of excessive false flooding within the device.

The Internet Group Management Protocol (IGMP) snooping software examines Layer 2 IP multicast traffic within a VLAN to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid flooding the entire VLAN. The IGMP snooping feature tracks which ports are attached to multicast-capable routers to help the routers forward IGMP membership reports. The IGMP snooping software responds to topology change notifications. By default, IGMP snooping is enabled on the device.

# Configuring FCoE Initialization Protocol Snooping

The Fiber Channel over Ethernet (FCoE) Initialization Protocol (FIP) is a Layer 2 protocol for end point discovery and fabric association. FIP has its own EtherType and uses its own frame formats.

FIP has two phases: discovery and login. Once the discovery of end nodes and login is complete, FCoE traffic can start flowing between the endpoints.

By snooping on FIP packets during the discovery and login phases, intermediary bridges can implement dynamic data integrity mechanisms using access control lists (ACLs) that permit only valid FCoE traffic between the ENode and the FCoE forwarder (FCF).

A bridge implementing the above functionality is what we refer to as the FIP Snooping Bridge. The process implementing this feature is called FIP Snooping Manager (FIPSM). FIPSM is capable of supporting both Fabric Provided MAC Addresses (FPMAs) and Server Provided MAC Addresses (SPMAs).

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure the Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) snooping feature using the Cisco Data Center Network Manager (DCNM)