Overview

This chapter provides an overview of the interface types supported by the Cisco NX-OS software.

Information About Interfaces

Cisco NX-OS supports multiple configuration parameters for each of the interface types supported. Most of these parameters are covered in this guide but some are described in other documents.

The table below shows where to get further information on the parameters you can configure for an interface.

Table 1: Interface Parameters

Feature Name	Parameters	Further Information
Basic parameters	description, duplex, error disable, flow control, MTU, beacon	"Configuring Basic Interface Parameters"
Layer 2	Layer 2 access and trunk port settings	"Configuring Layer 2 Interfaces"
	Layer 2 MAC, VLANs, private VLANs, Rapid PVST+, Multiple Spanning Tree, Spanning Tree Extensions	
	Port security	Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x
Layer 3	medium, IPv4 and IPv6 addresses	"Configuring Layer 3 Interfaces"
	bandwidth, delay, IP routing, VRFs	Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x

Feature Name	Parameters	Further Information
Port Channels	channel group, LACP	"Configuring Port Channels"
vPCs	Virtual port channels	"Configuring vPCs"
Tunnels	GRE Tunneling	"Configuring IP Tunnels"
Security	Dot1X, NAC, EOU, port security	Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x
FCoE	From Cisco NX-OS Release 5.2(1), you can run Fibre Channel over Ethernet (FCoE) on the Cisco Nexus 7000 Series Switches	

Ethernet Interfaces

Ethernet interfaces include access ports, trunk ports, private VLAN hosts and promiscuous ports, and routed ports.

Access Ports

An access port carries traffic for one VLAN. This type of port is a Layer 2 interface only. For more information about access-port interfaces, see "Configuring Layer 2 Interfaces."

Trunk Ports

A trunk port carries traffic for two or more VLANs. This type of port is a Layer 2 interface only. For more information about trunk-port interfaces, see "Configuring Layer 2 Interfaces."

Private VLAN Hosts and Promiscuous Ports

Private VLANs (PVLANs) provide traffic separation and security at the Layer 2 level. A PVLAN 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 called isolated and community VLANs.

In an isolated VLAN, PVLAN hosts communicate only with hosts in the primary VLAN. In a community VLAN, PVLAN hosts communicate only among themselves and with hosts in the primary VLAN but not with hosts in isolated VLANs or in other community VLANs. Community VLANs use promiscuous ports to communicate outside the PVLAN. Regardless of the combination of isolated and community secondary VLANs, all interfaces within the primary VLAN comprise one Layer 2 domain and require only one IP subnet.

You can configure a Layer 3 VLAN network interface, or switched virtual interface (SVI), on the PVLAN promiscuous port, which provides routing functionality to the primary PVLAN.

For more information on configuring PVLAN host and PVLAN promiscuous ports and all other PVLAN configurations, see the

Routed Ports

A routed port is a physical port that can route IP traffic to another device. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as the Spanning Tree Protocol (STP). For more information on routed ports, see the "Routed Interfaces" section.

Management Interface

You can use the management Ethernet interface to connect the device to a network for remote management using a Telnet client, the Simple Network Management Protocol (SNMP), or other management agents. The management port (mgmt0) is autosensing and operates in full-duplex mode at a speed of 10/100/1000 Mb/s.

For more information on the management interface, see the . You will also find information on configuring the IP address and default IP routing for the management interface in this document.

Port Channel Interfaces

A port channel is a logical interface that is an aggregation of multiple physical interfaces. You can bundle up to eight individual links to physical ports into a port channel to improve bandwidth and redundancy. You can also use port channeling to load balance traffic across these channeled physical interfaces. For more information about port-channel interfaces, see "Configuring Port Channels."

vPCs

Virtual port channels (vPCs) allow links that are physically connected to two different Cisco Nexus 7000 series devices to appear as a single port channel by a third device. The third device can be a switch, server, or any other networking device. You can configure a total of 748 vPCs on each device. vPCs provide Layer 2 multipathing. For more information about vPCs, see "Configuring vPCs."

Subinterfaces

You can create virtual subinterfaces on a parent interface configured as a Layer 3 interface. A parent interface can be a physical port or a port channel. Subinterfaces divide the parent interface into two or more virtual interfaces on which you can assign unique Layer 3 parameters such as IP addresses and dynamic routing protocols. For more information about subinterfaces, see the "Subinterfaces" section.

VLAN Network Interfaces

A VLAN network interface is a virtual routed interface that connects a VLAN on the device to the Layer 3 router engine on the same device. You can route across VLAN network interfaces to provide Layer 3 inter-VLAN routing. For more information about VLAN network interfaces, see the "VLAN Interfaces" section.

Loopback Interfaces

A virtual loopback interface is a virtual interface with a single endpoint that is always up. Any packet that is transmitted over a virtual loopback interface is immediately received by that interface. Loopback interfaces emulate a physical interface. For more information about subinterfaces, see the "Loopback Interfaces" section.

Tunnel Interfaces

Tunneling allows you to encapsulate arbitrary packets inside a transport protocol. This feature is implemented as a virtual interface to provide a simple interface for configuration. The tunnel interface provides the services necessary to implement any standard point-to-point encapsulation scheme. You can configure a separate tunnel for each link. For more information, see “Configuring IP Tunnels.”

Virtualization Interfaces

You can create multiple virtual device contexts (VDCs). Each VDC is an independent logical device to which you can allocate interfaces. Once an interface is allocated to a VDC, you can only configure that interface if you are in the correct VDC. For more information on VDCs, see the .

High Availability for Interfaces

Interfaces support stateful and stateless restarts. A stateful restart occurs on a supervisor switchover. After the switchover, Cisco NX-OS applies the runtime configuration after the switchover.

Licensing Requirements for Interfaces

vPC requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.

IP tunnels require an Enterprise Services license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply licenses, see the Cisco NX-OS Licensing Guide.

All other interfaces do not require a license.