



CHAPTER 1

Overview

This chapter provides an overview of the interface types supported in Cisco Nexus 1000V.

This chapter includes the following sections:

- [Simplifying Interface Configuration with Port Profiles, page 1-1](#)
- [Information About Interfaces, page 1-2](#)
- [High Availability for Interfaces, page 1-3](#)

Simplifying Interface Configuration with Port Profiles

In Cisco Nexus 1000V, port profiles are used to configure interfaces. A port profile can be assigned to multiple interfaces giving them all the same configuration. Changes to the port profile can be propagated automatically to the configuration of any interface assigned to it.

In VMware VirtualCenter (VC) a port profile is represented as a port group. The vEthernet or Ethernet interfaces are assigned in VC to a port profile for:

- Defining port configuration by policy.
- Applying a single policy across a large number of ports.
- Supporting both vEthernet and Ethernet ports.

Port profiles that are configured as uplinks, can be assigned by the server administrator to physical ports (a vmnic or a pnice). Port profiles that are not configured as uplinks can be assigned to a VM virtual port.



Note

While manual interface configuration overrides that of the port profile, it is not the recommended process. Manual interface configuration is only used, for example, to quickly test a change or allow a port to be disabled without having to change the inherited port profile.

For more information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)*.

For more information about assigning port profiles, see your VMware documentation.

To verify that the profiles are assigned as expected, use the following show commands:

show port-profile usage

show running-config interface *interface-id*

Note: The output of the command **show running-config interface** *interface-id* shows a config line such as, `inherit port-profile MyProfile`, indicating the inherited port profile.

Send document comments to nexus1k-docfeedback@cisco.com.

**Note**

Inherited port profiles cannot be changed or removed from an interface using the Cisco Nexus 1000V CLI. This can only be done through the VC.

**Note**

Inherited port profiles are automatically configured by the Cisco Nexus 1000V when the ports are attached on the hosts. This is done by matching up the VMware port group assigned by the system administrator with the port profile that created it.

Information About Interfaces

This section includes the following topics:

- [Ethernet Interfaces, page 1-2](#)
- [Virtual Ethernet Interfaces, page 1-3](#)
- [Management Interface, page 1-3](#)
- [Port Channel Interfaces, page 1-3](#)

Ethernet Interfaces

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

This section includes the following topics:

- [Access Ports, page 1-2](#)
- [Trunk Ports, page 1-2](#)
- [Private VLAN Ports, page 1-2](#)

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 [Chapter 3, “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 [Chapter 3, “Configuring Layer 2 Interfaces.”](#)

Private VLAN Ports

Private VLANs (PVLANS) are used to segregate Layer 2 ISP traffic and convey it to a single router interface. PVLANS achieve device isolation by applying Layer 2 forwarding constraints that allow end devices to share the same IP subnet while being Layer 2 isolated. In turn, the use of larger subnets reduces address management overhead. Three separate port designations are used, each having its own unique set of rules regulating the ability of each connected endpoint to communicate with other connected endpoints within the same private VLAN domain.

Send document comments to nexus1k-docfeedback@cisco.com.

For more information about PVLAN, see the document, *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(1)*.

Virtual Ethernet Interfaces

Virtual Ethernet (vEthernet or vEth) interfaces are logical interfaces. Each vEth interface corresponds to a switch interface connected to a virtual port. These include the following interface types:

- VM (interfaces connected to VM NICs)
- service console
- vmkernel

The vEth interfaces are created on the Cisco Nexus 1000V to represent virtual ports in use on the distributed virtual switch.

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. For more information on the management interface, see the *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(1)*.

Port Channel Interfaces

A port channel is a logical interface that aggregates 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 [Chapter 5, “Configuring Port Channels.”](#)

Configuration Limits

[Table 1-1](#) lists the Cisco Nexus 1000V Release 4.0(4)SV1(1) configuration limits for port channels.

Table 1-1 Cisco NX-OS Release 4.1 Configuration Limits

Feature	Maximum Limit
Active VLANs	512
Port channels	256

High Availability for Interfaces

Interfaces support stateful and stateless restarts. A stateful restart occurs on a supervisor switchover. After the switchover, Cisco Nexus 1000V applies the runtime configuration after the switchover.

Send document comments to nexus1k-docfeedback@cisco.com.