CHAPTER 1

Product Overview

The Cisco Nexus 5000 Series is a family of top-of-rack switches for the data center. The Nexus 5020 switch is a 10-Gigabit Ethernet and Fibre Channel over Ethernet (FCoE) switch with 1.04 Tbps switching throughput. The Nexus 5020 provides low-latency wire-speed switching for up to 52 10-Gigabit Ethernet ports.

The Nexus 5020 switch supports FCoE to provide data center I/O consolidation (IOC). Optional Fibre Channel-capable expansion modules provide four or eight native Fibre Channel SAN interfaces.

This chapter describes the Cisco Nexus 5000 Series switches and includes the following sections:

- New Technologies in the Cisco Nexus 5000 Series, page 1-1
- Cisco Nexus 5000 Series Switch Hardware, page 1-3
- Cisco Nexus 5000 Series Switch Software, page 1-4
- Typical Deployment Topologies, page 1-8
- Supported Standards, page 1-11

New Technologies in the Cisco Nexus 5000 Series

Cisco Nexus 5000 Series switches introduce several new technologies, which are described in the following sections:

- Fibre Channel over Ethernet, page 1-1
- I/O Consolidation, page 1-2
- Virtual Interfaces, page 1-3

Fibre Channel over Ethernet

Fibre Channel over Ethernet (FCoE) provides a method of encapsulating Fibre Channel traffic over a physical Ethernet link. FCoE frames use a unique Ethertype so that FCoE traffic and standard Ethernet traffic can be carried on the same link.

Fibre Channel traffic requires a lossless transport layer. Native Fibre Channel implements lossless service using a buffer-to-buffer credit system. For FCoE traffic, the Ethernet link must provide lossless service.

Ethernet links on Cisco Nexus 5000 Series switches provide two mechanisms to ensure lossless transport for FCoE traffic: link-level flow control and priority flow control.

IEEE 802.3x link-level flow control allows a congested receiver to signal the far end to pause the data transmission for a short period of time. The pause functionality is applied to all the traffic on the link.

The priority flow control (PFC) feature applies pause functionality to specific classes of traffic on the Ethernet link. For example, PFC can provide lossless service for the FCoE traffic, and best-effort service for the standard Ethernet traffic. PFC can provide different levels of service to specific classes of Ethernet traffic (using IEEE 802.1p traffic classes).

I/O Consolidation

I/O consolidation (IOC) allows a single network technology to carry IP, SAN and IPC traffic.

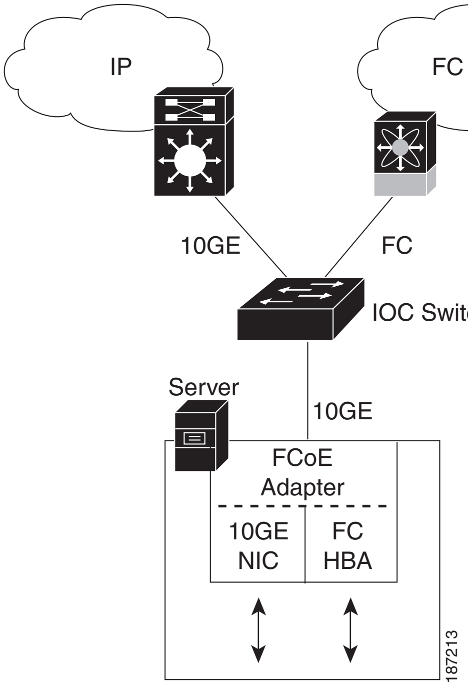
FCoE enables an evolutionary approach to IOC. The upper Fibre Channel layers are unchanged, so the Fibre Channel operational model is maintained. FCoE network management and configuration is similar to a native Fibre Channel network.

Cisco Nexus 5000 Series switches use FCoE to carry Fibre Channel and Ethernet traffic on the same physical Ethernet connection between the switch and the server. At the server, the connection terminates to a converged network adapter (CNA) . The adapter presents two interfaces to the server's operating system (OS): one Ethernet NIC interface and one Fibre Channel HBA interface. The server OS is not aware of the FCoE encapsulation (See Figure 1-1)

At the switch, the incoming Ethernet port separates the Ethernet and Fibre Channel traffic (using Ethertype to differentiate the frames). Ethernet frames and Fibre Channel frames are switched to their respective network-side interfaces.

Cisco Nexus 5000 Series switches provide quality of service (QoS) capabilities to ensure lossless service across the switch for Fibre Channel traffic. Best-effort service can be applied to all of the Ethernet traffic or specific classes of Ethernet traffic can be configured with different QoS levels.

Figure 1-1 I/O Consolidation



Virtual Interfaces

When FCoE is enabled, a physical Ethernet cable carries traffic for a logical Ethernet connection and a logical Fibre Channel connection.

The Cisco Nexus 5000 Series switch uses virtual interfaces to represent the logical connections that are carried on the same physical Ethernet. The Cisco Nexus 5000 Series switch supports virtual Ethernet and virtual Fibre Channel interfaces.

For configuration purposes, virtual Ethernet and virtual Fibre Channel interfaces are implemented as Layer 2 subinterfaces of the physical Ethernet interface.

Link-level features (such as link debounce timer and CDP) are configured on the physical Ethernet interface. Logical Layer 2 Ethernet features (such as VLAN membership and ACLs) are configured on the virtual Ethernet interfaces. Logical Fibre Channel features (such as VSAN membership) are configured on the virtual Fibre Channel interfaces.

Cisco Nexus 5000 Series Switch Hardware

The Cisco Nexus 5000 Series includes the Nexus 5020 switch. The Nexus 5020 switch hardware is described in the following topics:

- Chassis, page 1-3
- Expansion Modules, page 1-3
- Ethernet Interfaces, page 1-4
- Fibre Channel Interfaces, page 1-4
- Management Interfaces, page 1-4

Chassis

The Nexus 5020 switch is a 2 RU chassis designed for rack mounting. The chassis supports redundant fans and power supplies.

The Nexus 5020 switching fabric is low latency, nonblocking and supports Ethernet frame sizes from 64 to 9216 bytes.

Expansion Modules

The Nexus 5020 switch has two slots for optional expansion modules. The following expansion modules are available:

- N5K-M1404 provides four 10-Gigabit Ethernet ports, and four 1/2/4 Gb Fibre Channel ports.
- N5K-M1600 provides six 10-Gigabit Ethernet ports.

The expansion modules are field-replaceable units (FRUs) that support online insertion and removal (OIR).

Ethernet Interfaces

The Nexus 5020 switch has 40 fixed 10-Gigabit Ethernet ports equipped with SFP+ interface adapters. Up to 12 additional 10-Gigabit Ethernet ports are available on the expansion modules.

All of the 10-Gigabit Ethernet ports support FCoE. Each port can be used as a downlink (connected to a server) or as an uplink (to the data center LAN).

Fibre Channel Interfaces

Fibre Channel ports are optional on the Nexus 5020 switch. Up to eight Fibre Channel ports are available when using expansion modules.

Each Fibre Channel port can be used as a downlink (connected to a server) or as an uplink (to the data center SAN fabric).

Management Interfaces

The Nexus 5020 switch has two dedicated management interfaces (one serial console port and one 10/100/1000 Ethernet interface).

Cisco Nexus 5000 Series Switch Software

The Cisco Nexus 5000 Series switch is a Layer 2 device, which runs the Cisco Nexus operating system (NX-OS). The Cisco Nexus 5000 Series switch software is described in the following topics:

- Ethernet Switching, page 1-4
- FCoE and Fibre Channel Switching, page 1-5
- Licensing, page 1-5
- QoS, page 1-5
- Serviceability, page 1-5
- Switch Management, page 1-6
- Network Security Features, page 1-7
- Virtual Device Contexts, page 1-8

Ethernet Switching

Cisco Nexus 5000 Series switches are designed to support high-density, high-performance Ethernet systems and provide the following Ethernet switching features:

- IEEE 802.1D-2004 Rapid and Multiple Spanning Tree Protocols (802.1w and 802.1s)
- IEEE 802.1Q VLANs and trunks
- IEEE 802.3ad link aggregation
- Private VLANs
- Traffic suppression (unicast, multicast, and broadcast)

FCoE and Fibre Channel Switching

Cisco Nexus 5000 Series switches support data center I/O consolidation (IOC) by providing FCoE interfaces (to the servers) and native Fibre Channel interfaces (to the SAN).

FCoE and Fibre Channel switching includes the following features:

- Cisco fabric services
- N-port virtualization
- VSANs and VSAN trunking
- Zoning
- Distributed device alias service
- SAN port channels

Licensing

Cisco Cisco Nexus 5000 Series switches are shipped with the licenses installed. The switch provides commands to manage the licenses and install additional licenses.

QoS

The Cisco Nexus 5000 Series switch provides quality of service (QoS) capabilities such as traffic prioritization and bandwidth allocation on egress interfaces.

The default QoS configuration on the switch provides lossless service for Fibre Channel and FCoE traffic. QoS can be configured to provide additional classes of service for Ethernet traffic.

Serviceability

The Cisco Nexus 5000 Series switch serviceability functions provide data for network planning and help to improve problem resolution time.

This section includes the following topics:

- Switched Port Analyzer, page 1-5
- Ethanalyzer, page 1-6
- Call Home, page 1-6
- Online Diagnostics, page 1-6
- Switch Management, page 1-6

Switched Port Analyzer

The switched port analyzer (SPAN) feature allows an administrator to analyze all traffic between ports by nonintrusively directing the SPAN session traffic to a SPAN destination port that has an external analyzer attached to it.

Ethanalyzer

Ethanalyzer is a Cisco NX-OS protocol analyzer tool based on the Wireshark (formerly Ethereal) open source code. Ethanalyzer is a command-line version of Wireshark for capturing and decoding packets. You can use Ethanalyzer to troubleshoot your network and analyze the control-plane traffic. For more information about Ethanalyzer, see *Cisco NX-OS Troubleshooting Guide, Release 4.0*.

Call Home

The Call Home feature continuously monitors hardware and software components to provide e-mail-based notification of critical system events. A versatile range of message formats is available for optimal compatibility with pager services, standard e-mail, and XML-based automated parsing applications. The feature offers alert grouping capabilities and customizable destination profiles. This feature can be used, for example, to directly page a network support engineer, send an e-mail message to a network operations center (NOC), and employ Cisco AutoNotify services to directly generate a case with the Cisco Technical Assistance Center (TAC). This feature is a step toward autonomous system operation, which enables networking devices to inform IT when a problem occurs and helps to ensure that the problem is resolved quickly.

Online Diagnostics

Cisco generic online diagnostics (GOLD) is a suite of diagnostic facilities to verify that hardware and internal data paths are operating as designed. Boot-time diagnostics, continuous monitoring, and on-demand and scheduled tests are part of the Cisco GOLD feature set. GOLD allows rapid fault isolation and continuous system monitoring.

Switch Management

This section includes the following topics:

- Simple Network Management Protocol, page 1-6
- Configuration Verification and Rollback, page 1-6
- Role-Based Access Control, page 1-7
- Configuration Methods, page 1-7

Simple Network Management Protocol

Cisco NX-OS is compliant with Simple Network Management Protocol (SNMP) version 1, version 2, and version 3. A full set of Management Information Bases (MIBs) is supported.

Configuration Verification and Rollback

With the Cisco Nexus 5000 Series switch, you can verify the consistency of a configuration and the availability of necessary hardware resources before committing the configuration. A device can be preconfigured, and the verified configuration can be applied at a later time. Configurations also include checkpoints to allow the switch operator to revert to a known good configuration as needed.

Role-Based Access Control

With role-based access control (RBAC), you can limit access to switch operations by assigning roles to users. Administrators can customize access and restrict it to the users who require it.

Configuration Methods

You can configure Cisco Nexus 5000 Series switches using direct network configuration methods or web services hosted on a Fabric Manager server.

This section includes the following topics:

- Configuring with CLI, XML Management Interface, or SNMP, page 1-7
- Configuring with Cisco MDS Fabric Manager, page 1-7

Configuring with CLI, XML Management Interface, or SNMP

You can configure Cisco Nexus 5000 Series switches using the command line interface (CLI), the XML management interface over SSH, or SNMP as follows:

- CLI —You can configure switches using the CLI from an SSH session, a Telnet session. or the console port. SSH provides a secure connection to the device.
- XML Management Interface over SSH—You can configure switches using the XML management interface, which is a programming interface based on the NETCONF protocol that complements the CLI functionality. For more information, see the *Cisco NX-OS XML Management Interface User Guide, Release 4.0*.
- SNMP—SNMP allows you to configure switches using Management Information Bases (MIBs).

Configuring with Cisco MDS Fabric Manager

You can configure Cisco Nexus 5000 Series switches using the Fabric Manager client, which runs on a local PC and uses the Fabric Manager server.

Network Security Features

Cisco NX-OS Release 4.0 includes the following security features:

- Authentication, authorization, and accounting (AAA) and TACACS+
- IEEE 802.1x authentication and RADIUS
- Secure Shell (SSH) Protocol Version 2
- Simple Network Management Protocol Version 3 (SNMPv3)
- Port security
- DHCP snooping
- MAC ACLs and IP ACLs, including port-based ACLs (PACLs) and VLAN-based ACLs (VACLs).

Virtual Device Contexts

Cisco NX-OS can segment operating system and hardware resources into virtual device contexts (VDC) that emulate virtual devices. The Cisco Nexus 5000 Series switch does not support multiple VDCs. All switch resources are managed in the default VDC.

Typical Deployment Topologies

In this release, the Nexus 5020 switch is typically deployed in the following topologies:

- Ethernet TOR Switch Topology, page 1-8
- IOC Topology, page 1-10

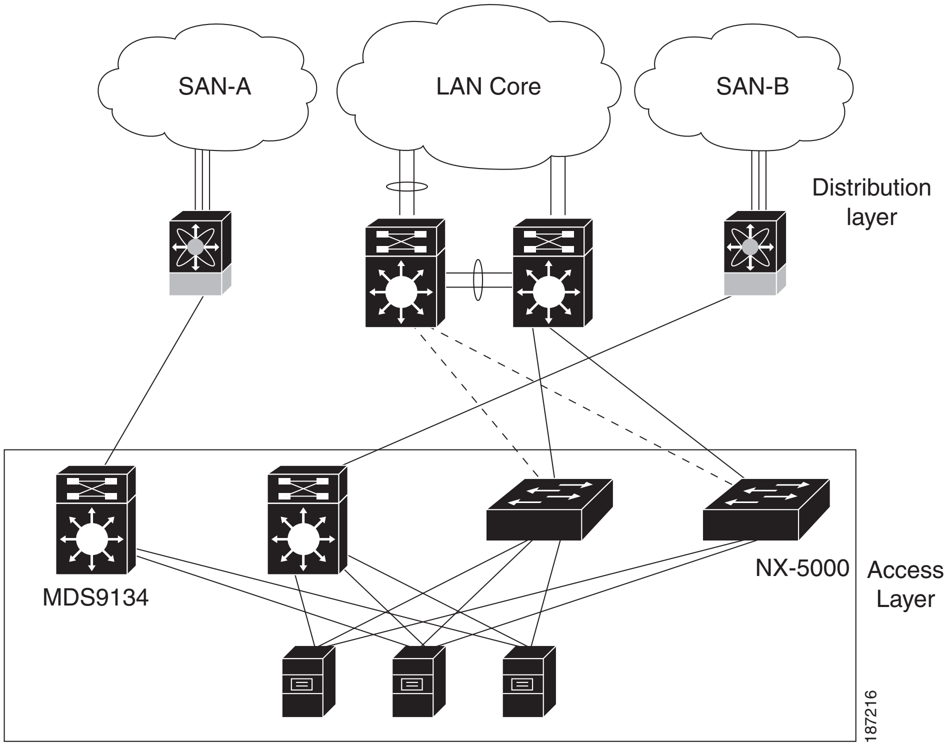
Ethernet TOR Switch Topology

The Nexus 5020 switch can be deployed as a 10-Gigabit Ethernet top-of-rack (TOR) switch, with uplinks to the data center LAN distribution layer switches. An example configuration in shown in Figure 1-2.

In this example, the blade server rack incorporates blade switches that support 10-Gigabit Ethernet uplinks to the Nexus 5020 switch. The blade switches do not support FCoE, so there is no FCoE traffic and no Fibre Channel ports on the Nexus 5020 switch.

In the example configuration, the Nexus 5020 switch has Ethernet uplinks to two Catalyst switches. If STP is enabled in the data center LAN, the links to one of the switches will be STP active and the links to the other switch will be STP blocked.

Figure 1-2 Ethernet TOR Switch Topology



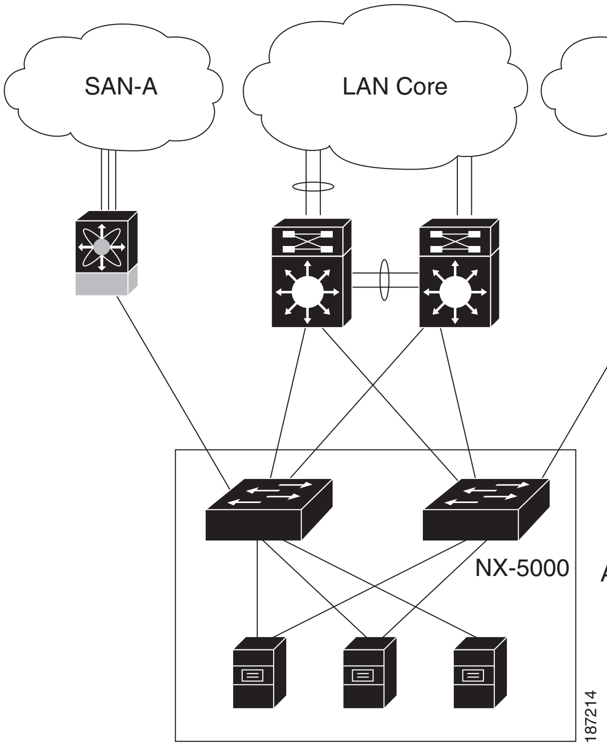
All of the server-side ports on the Nexus 5020 switch are running standard Ethernet. FCoE is not required, so the server ports are connected using 10-Gigabit Ethernet NICs.

The servers are connected to the data center SAN through MDS 9134 SAN switches. The server Fibre Channel ports require standard Fibre Channel HBAs.

IOC Topology

Figure 1-3 shows a typical I/O consolidation (IOC) scenario for the Nexus 5020 switch.

Figure 1-3 I/O Consolidation Topology



The Nexus 5020 switch connects to the server ports using FCoE. Ports on the server require converged network adapters. For redundancy, each server connects to both Nexus 5020 switches. Dual-port CNA adapters can be used for this purpose. The CNA is configured in active-passive mode, and the server needs to support server-based failover.

On the Nexus 5020 switch, the Ethernet network-facing ports are connected to two Catalyst 6500 switches. Depending on required uplink traffic volume, there may be multiple ports connected to each Catalyst 6500 switch, configured as port channels. If STP is enabled in the data center LAN, the links to one of the switches will be STP active and the links to the other switch will be STP blocked.

The Nexus 5020 SAN network-facing ports are connected to Cisco MDS 9000 Family switches. Depending on required traffic volume, there may be multiple Fibre Channel ports connected to each MDS 9000 Family switch, configured as SAN port channels.

Supported Standards

Table 1-1 lists the standards supported by the Cisco Nexus 5000 Series switches.

Table 1-1 IEEE Compliance

Standard	Description
802.1D	MAC Bridges
802.1s	Multiple Spanning Tree Protocol
802.1w	Rapid Spanning Tree Protocol
802.1AE	MAC Security (link layer cryptography)
802.3ad	Link aggregation with LACP
802.3ae	10 Gigabit Ethernet
802.1Q	VLAN Tagging
802.1p	Class of Service Tagging for Ethernet frames
802.1x	Port-based network access control