Overview

This chapter contains the following sections:

Fibre Channel over Ethernet

Fibre Channel over Ethernet (FCoE) allows Fibre Channel traffic to be encapsulated 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.

Classic Ethernet is a best-effort protocol; in the event of congestion, Ethernet will discard packets, relying on higher level protocols to provide retransmission and other reliability mechanisms. Fibre Channel traffic requires a lossless transport layer; as a data storage protocol, it is unacceptable to lose a single data packet. Native Fibre Channel implements a lossless service at the transport layer using a buffer-to-buffer credit system.

For FCoE traffic, the Ethernet link must provide a lossless service. Ethernet links on Cisco Nexus devices 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).

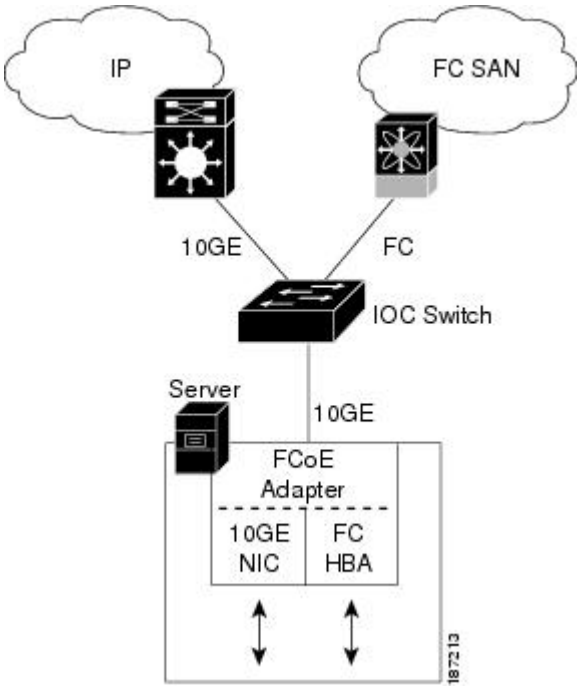
Data Center I/O Consolidation

I/O consolidation allows a single network technology to carry IP, SAN, and IPC traffic. FCoE is the single network technology that allows I/O consolidation. 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 devices 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 host bus adapter (HBA) interface.

The server OS is not aware of the FCoE encapsulation (see the following figure). 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.

Figure 1: I/O Consolidation



Cisco Nexus devices provide quality of service (QoS) capabilities to ensure lossless or best-effort service across the switch. For Fibre Channel traffic (FCoE) you should apply the lossless QoS classes. By default, best-effort service is applied to all of the Ethernet traffic. You can configure different QoS levels for specific classes of Ethernet traffic.

Virtual Interfaces

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

The Cisco Nexus device uses virtual interfaces to represent the logical Fibre Channel connections. For configuration purposes, virtual Fibre Channel interfaces are implemented as Layer 2 subinterfaces of the physical Ethernet interface.

Ethernet features (such as the link debounce timer and VLAN membership) are configured on the physical Ethernet interface. Logical Fibre Channel features (such as VSAN membership) are configured on the virtual Fibre Channel interfaces.

Ethernet Switching

Cisco Nexus devices are Layer 2 devices, which run Cisco NX-OS.

Cisco Nexus devices 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
- EtherChannels and virtual port channels (vPCs)
- Traffic suppression (unicast, multicast, and broadcast)

FCoE and Fibre Channel Switching

Cisco Nexus devices support data center I/O consolidation 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

QoS

Cisco Nexus devices provide 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 must be configured to use native FC or FCoE or FC and FCoE.

The following commands will enable the default QoS configuration which must be configured for native FC or FCoE or FC and FCoE:

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-default-out-policy
switch(config-sys-qos)# service-policy type qos input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type network-qos fcoe-default-nq-policy
```

Note Before enabling FCoE on the Cisco Nexus 5500 Series device, you must attach the pre-defined FCoE policy maps to the type qos, type network-qos, and type queuing policy maps.

Virtual Port Channels

A virtual port channel (vPC) allows links that are physically connected to two different Cisco Nexus devices or Cisco Nexus 2000 Series Fabric Extenders to appear as a single port channel. A vPC can provide multipathing, which allows you to create redundancy by enabling multiple parallel paths between nodes and load balancing traffic where alternative paths exist.

Serviceability

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

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 analyse the control-plane traffic.

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

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.

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

Configuring with CLI, XML Management Interface, or SNMP

You can configure Cisco Nexus devices 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 Interfaces User Guide*.
- SNMP—SNMP allows you to configure switches using Management Information Bases (MIBs).

Configuring with Cisco Data Center Network Manager

You can configure Cisco Nexus Series switches using the Data Center Network Manager (DCNM) client, which runs on a local PC and uses the DCNM server.

For more information, see the *Cisco DCNM Configuration Guides*.

Configuring with Cisco MDS Fabric Manager

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

For more information, see the Cisco Nexus Fabric Manager Software guide for your device.

Network Security Features

Cisco NX-OS includes the following security features:

- Authentication, authorization, and accounting (AAA) and TACACS+
- RADIUS
- Secure Shell (SSH) Protocol Version 2
- Simple Network Management Protocol Version 3 (SNMPv3)
- 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 device does not support multiple VDCs. All switch resources are managed in the default VDC.

For more information, see the *Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts*.

Licensing

The Cisco Nexus device is shipped with its licenses installed. The switch provides commands to manage the licenses and install additional licenses.

Typical Deployment Topologies

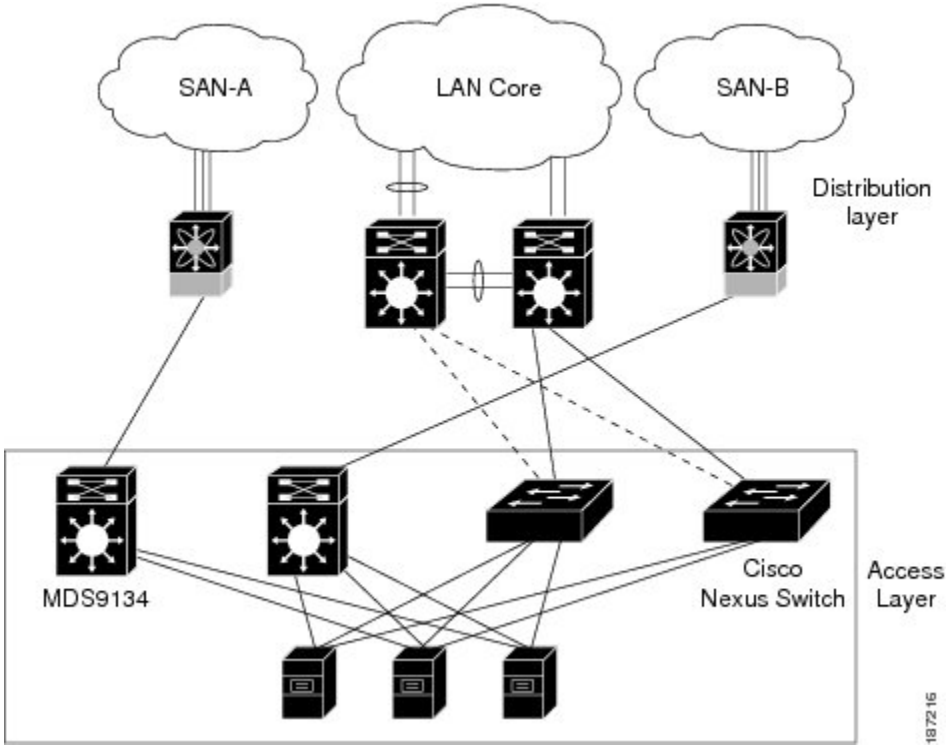
Ethernet TOR Switch Topology

The Cisco Nexus device 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 the following figure.

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

In the example configuration, the Cisco Nexus device 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 2: Ethernet TOR Switch Topology



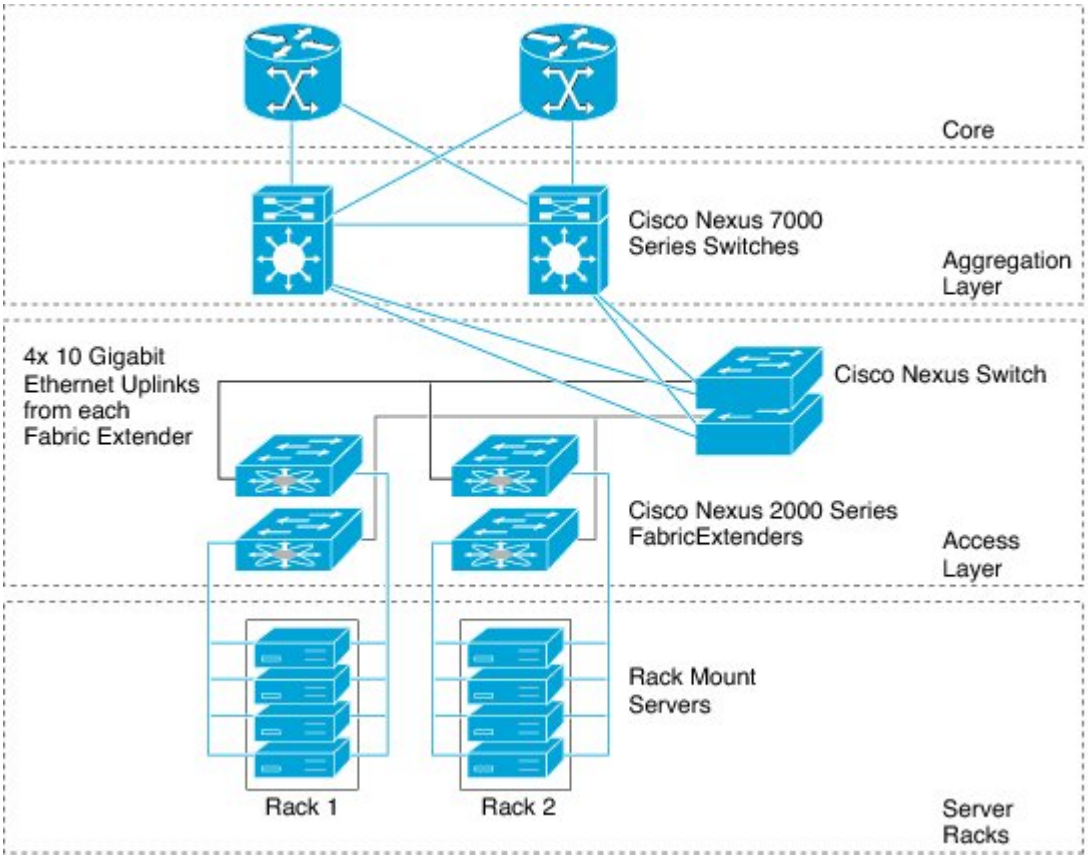
All of the server-side ports on the Cisco Nexus device are running standard Ethernet. FCoE is not required, so the server ports are connected using 10-Gigabit Ethernet NICs.

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

Fabric Extender Deployment Topology

The following figure shows a simplfied configuration using the Cisco Nexus 2000 Series Fabric Extender in combination with the Cisco Nexus device h to provide a simplified and cost-effective 1-Gigabit TOR solution.

Figure 3: Fabric Extender Deployment Topology



In the example configuration, the Fabric Extender top-of-rack units provide 1-Gigabit host interfaces connected to the servers. The Fabric Extender units are attached to their parent Cisco Nexus devices with 10-Gigabit fabric interfaces.

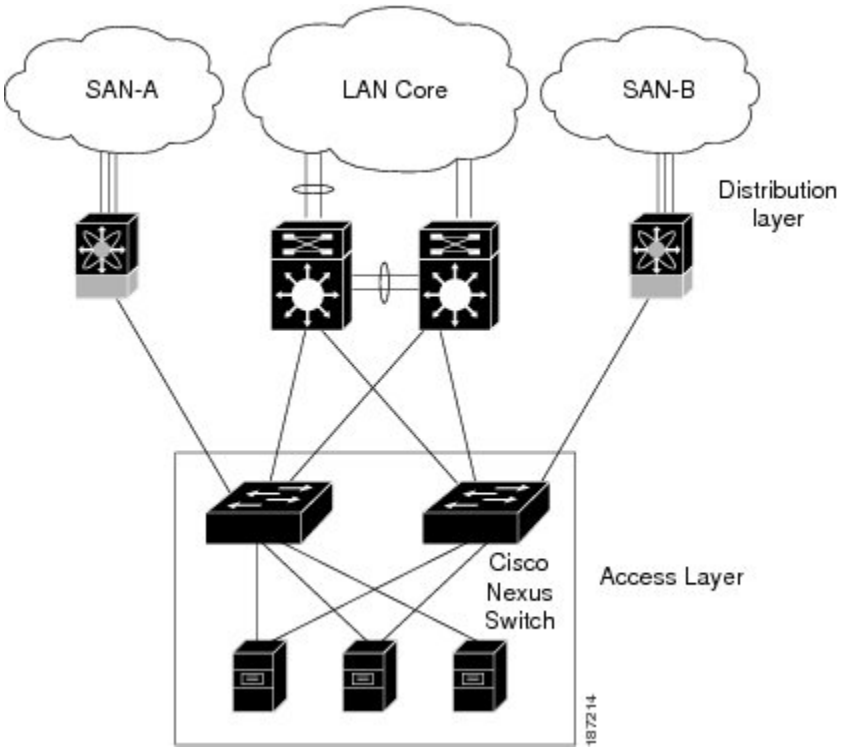
Each Fabric Extender acts as a Remote I/O Module on the parent Cisco Nexus device. All device configurations are managed on the Cisco Nexus device and configuration information is downloaded using inband communication to the Fabric Extender.

See the *Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide* for an overview of the Fabric Extender and configuration details.

Data Center I/O Consolidation Topology

The following figure shows a typical I/O consolidation scenario for the Cisco Nexus device.

Figure 4: I/O Consolidation Topology



The Cisco Nexus device connects to the server ports using FCoE. Ports on the server require converged network adapters. For redundancy, each server connects to both 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 Cisco Nexus device, the Ethernet network-facing ports are connected to two Catalyst 6500 Series switches. Depending on required uplink traffic volume, there may be multiple ports connected to each Catalyst 6500 Series 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 SAN network-facing ports on the Cisco Nexus device are connected to Cisco MDS 9000 Family switches. Depending on the required traffic volume, there may be multiple Fibre Channel ports connected to each MDS 9000 Family switch, configured as SAN port channels.

Supported Standards

The following table lists the standards supported by the Cisco Nexus devices.

Table 1: IEEE Compliance

Standard	Description
802.1D	MAC Bridges
802.1s	Multiple Spanning Tree Protocol
802.1w	Rapid Spanning Tree Protocol
802.3ad	Link aggregation with LACP
802.3ae	10-Gigabit Ethernet
802.1Q	VLAN Tagging
802.1p	Class of Service Tagging for Ethernet frames