



## Overview

---

This chapter provides an overview of the Cisco NX-OS software.

- [Software Compatibility](#), page 1
- [Serviceability](#), page 3
- [Manageability](#), page 4
- [Traffic Routing, Forwarding, and Management](#), page 5
- [Quality of Service](#), page 7
- [Network Security](#), page 7
- [Licensing](#), page 8
- [Supported Standards](#), page 8

## Software Compatibility

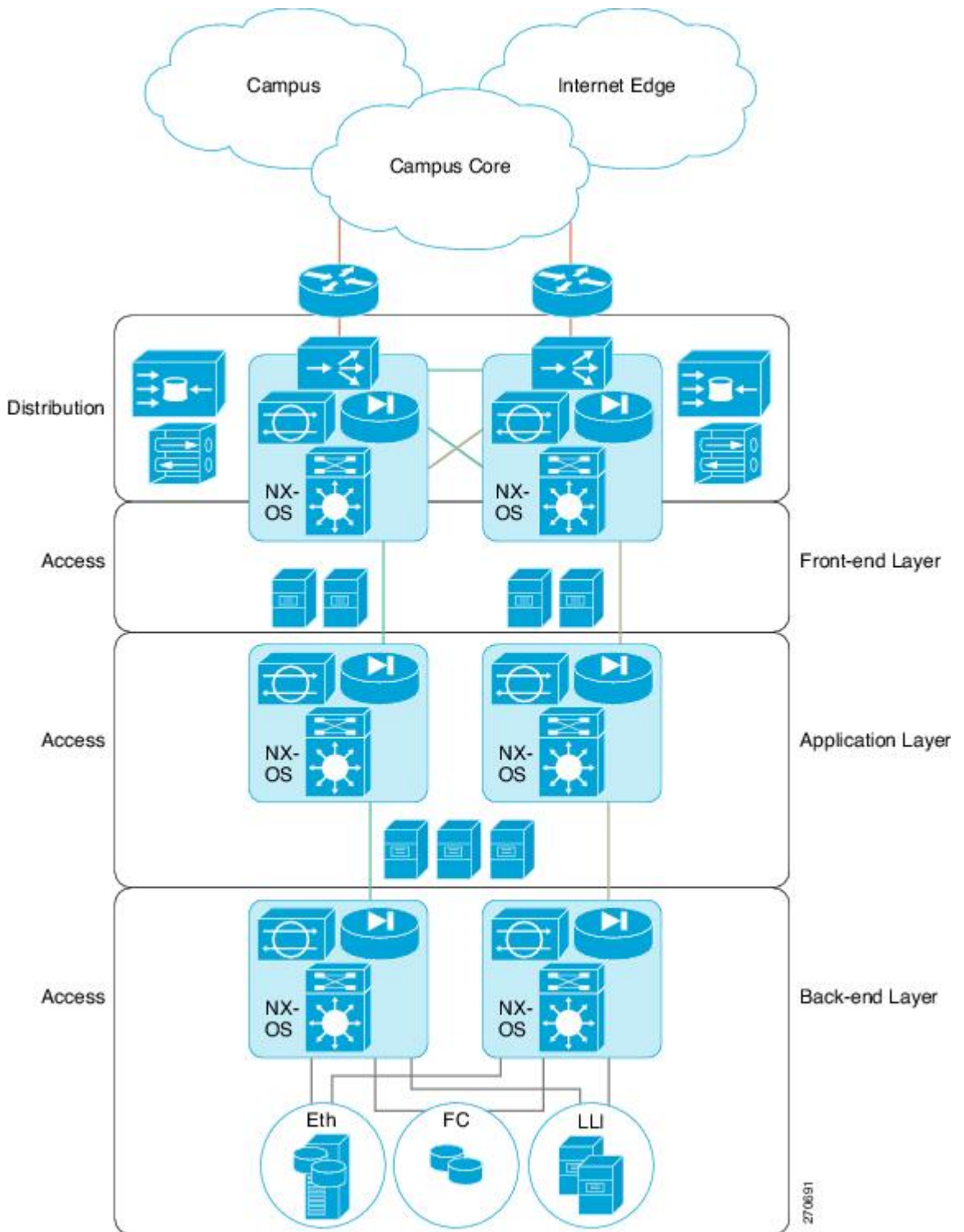
The Cisco NX-OS software interoperates with Cisco products that run any variant of the Cisco IOS software. The Cisco NX-OS software also interoperates with any networking operating system that conforms to the IEEE and RFC compliance standards.

## Common Software Throughout the Data Center

The Cisco NX-OS software provides a unified operating system that is designed to run all areas of the data center network including the LAN and Layer 4 through Layer 7 network services.

This figure shows an overview of the Cisco NX-OS software in the data center.

**Figure 1: Cisco NX-OS in a Data Center**



## Modular Software Design

The Cisco NX-OS software supports distributed multithreaded processing on symmetric multiprocessors (SMPs), multi-core CPUs, and distributed data module processors. The Cisco NX-OS software offloads computationally intensive tasks, such as hardware table programming, to dedicated processors distributed across the data modules. The modular processes are created on demand, each in a separate protected memory space. Processes are started and system resources are allocated only when you enable a feature. A real-time preemptive scheduler helps to ensure the timely processing of critical functions.

## Virtual Device Contexts

The Cisco NX-OS software can segment system and hardware resources into virtual contexts that emulate virtual devices. Each virtual device context (VDC) has its own software processes, dedicated hardware resources (interfaces), and an independent management environment. With VDCs, you can consolidate separate networks onto a common infrastructure, which maintain the administrative boundary separation and fault isolation characteristics of physically separate networks, and provide many of the operational cost benefits of a single infrastructure. For more information, see the [Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.2](#).

## Serviceability

The Cisco NX-OS software has serviceability functions that allow the device to respond to network trends and events. These features help you with network planning and improving response times.

## Switched Port Analyzer

The Switched Port Analyzer (SPAN) feature allows you to analyze all traffic between ports (called the SPAN source ports) by nonintrusively directing the SPAN session traffic to a SPAN destination port that has an external analyzer attached to it. For more information about SPAN, see the [Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.2](#).

## Ethalyzer

Ethalyzer is a Cisco NX-OS protocol analyzer tool based on the Wireshark (formerly Ethereal) open source code. Ethalyzer is a command-line version of Wireshark for capturing and decoding packets. You can use Ethalyzer to troubleshoot your network and analyze the control-plane traffic. For more information about Ethalyzer, see the [Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.2](#).

## 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. It offers alert grouping capabilities and customizable destination profiles. You can use this feature, 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). For more information about Call Home, see the [Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.2](#).

## Online Diagnostics

Cisco generic online diagnostics (GOLD) 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. For information about configuring GOLD, see the [Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.2](#).

## Embedded Event Manager

Cisco Embedded Event Manager (EEM) is a device and system management feature that helps you to customize behavior based on network events as they happen. For information about configuring EEM, see the [Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.2](#).

## NetFlow

The Cisco NX-OS NetFlow implementation supports version 5 and version 9 exports. It also supports the Flexible NetFlow configuration model and hardware-based Sampled NetFlow for enhanced scalability. For more information about NetFlow, see the [Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.2](#).

## Manageability

This section describes the manageability features in the Cisco NX-OS software.

### Simple Network Management Protocol

The Cisco NX-OS software is compliant with Simple Network Management Protocol (SNMP) version 1, version 2, and version 3. A large number of MIBs is supported. For more information about SNMP, see the [Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.2](#).

### Configuration Verification and Rollback

The Cisco NX-OS software allows you to verify the consistency of a configuration and the availability of necessary hardware resources prior to committing the configuration. You can preconfigure a device and apply the verified configuration at a later time. Configurations also include checkpoints that allow you to roll back to a known good configuration as needed. For more information about rollback, see the [Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.2](#).

## Role-Based Access Control

With role-based access control (RBAC), you can limit access to device operations by assigning roles to users. You can customize access and restrict it to the users who require it. For more information about RBAC, see the [Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.2](#).

## Connectivity Management Processor

The Cisco NX-OS software supports the use of a Connectivity Management Processor (CMP) for remote platform management. The CMP provides an out-of-band access channel to the Cisco NX-OS console. For more information about CMP, see the [Cisco Nexus 7000 Series Connectivity Management Processor Configuration Guide](#).

## Cisco NX-OS Device Configuration Methods

You can configure devices using the CLI from a Secure Shell (SSH) session or a Telnet session. SSH provides a secure connection to the device. The CLI configuration guides and command references are organized by feature. For more information, see the Cisco NX-OS configuration guides and the Cisco NX-OS command references. For more information on SSH and Talent, see the [Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.2](#).

You can also configure devices using the XML management interface, which is a programmatic method based on the NETCONF protocol that complements the CLI. For more information, see the [Cisco NX-OS XML Management Interface User Guide, Release 4.2](#).

## Traffic Routing, Forwarding, and Management

This section describes the traffic routing, forwarding, and management features supported by the Cisco NX-OS software.

### Ethernet Switching

The Cisco NX-OS software supports high-density, high-performance Ethernet systems and provides 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
- 16,000-subscriber VLANs
- IEEE 802.3ad link aggregation
- Private VLANs
- Cross-chassis private VLANs
- Unidirectional Link Detection (UDLD) in aggressive and standard modes

For more information, see the [Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.2](#) and the [Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.2](#).

## IP Routing

The Cisco NX-OS software supports IP version 4 (IPv4) and IP version 6 (IPv6) and the following routing protocols:

- Open Shortest Path First (OSPF) Protocol Versions 2 (IPv4) and 3 (IPv6)
- Intermediate System-to-Intermediate System (IS-IS) Protocol
- Border Gateway Protocol (BGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Routing Information Protocol Version 2 (RIPv2)

The Cisco NX-OS software implementations of these protocols are fully compliant with the latest standards and include 4-byte autonomous system numbers (ASNs) and incremental shortest path first (SPF). All unicast protocols support Non-Stop Forwarding Graceful Restart (NSF-GR). All protocols support all interface types, including Ethernet interfaces, VLAN interfaces, subinterfaces, port channels, tunnel interfaces, and loopback interfaces.

For more information, see the [Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.2](#).

## IP Services

The following IP services are available in the Cisco NX-OS software:

- Virtual Routing and Forwarding (VRF)
- Dynamic Host Configuration Protocol (DHCP) Helper
- Hot-Standby Routing Protocol (HSRP)
- Gateway Load Balancing Protocol (GLBP)
- Enhanced Object Tracking
- Policy-Based Routing (PBR)
- Unicast Graceful Restart for all protocols in IPv4 Unicast Graceful Restart for OSPFv3 in IPv6

For more information, see the [Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.2](#).

## IP Multicast

The Cisco NX-OS software includes the following multicast protocols and functions:

- Protocol Independent Multicast (PIM) Version 2 (PIMv2)
- Source Specific Multicast (SSM)
- PIM sparse mode (Any-Source Multicast [ASM] for IPv4 and IPv6)

**Note**

The Cisco NX-OS software does not support PIM dense mode.

- Bidirectional Protocol Independent Multicast (Bidir PIM)
- Anycast rendezvous point (Anycast-RP)
- Multicast NSF for IPv4 and IPv6
- RP-Discovery using bootstrap router (BSR) (Auto-RP and static)
- Internet Group Management Protocol (IGMP) Versions 1, 2, and 3 router role
- IGMPv2 host mode
- IGMP snooping
- Multicast Listener Discovery (MLD) Protocol Version 2 (for IPv6)
- Multicast Source Discovery Protocol (MSDP) (for IPv4 only)

For more information, see the [Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 4.2](#).

## Quality of Service

The Cisco NX-OS software supports quality of service (QoS) functions for classification, marking, queuing, policing, and scheduling. Modular QoS CLI (MQC) supports all QoS features. You can use MQC to provide uniform configurations across various Cisco platforms. For more information, see the [Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 4.2](#).

## Network Security

This section describes the network security features support by the Cisco NX-OS software.

### Cisco TrustSec

Cisco TrustSec security provides data confidentiality and integrity and supports standard IEEE 802.1AE link-layer cryptography with 128-bit Advanced Encryption Standard (AES) cryptography. Link-layer cryptography guarantees end-to-end data privacy while allowing the insertion of security service devices along the encrypted path. Cisco TrustSec uses security group access control lists (SGACLs), which are based on security group tags instead of IP addresses. SGACLs enable policies that are more concise and easier to manage due to their topology independence. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.2*.

### Additional Network Security Features

In addition to Cisco TrustSec, the Cisco NX-OS software includes the following security features:

- Data path intrusion detection system (IDS) for protocol conformance checks

- Control Plane Policing (CoPP)
- Message-digest algorithm 5 (MD5) routing protocol authentication
- Cisco-integrated security features, including Dynamic Address Resolution Protocol (ARP) inspection (DAI), DHCP snooping, and IP Source Guard
- Authentication, authorization, and accounting (AAA)
- RADIUS and TACACS+
- SSH Protocol Version 2
- SNMPv3
- Port security
- IEEE 802.1X authentication
- Layer 2 Cisco Network Admission Control (NAC) LAN port IP
- Policies based on MAC and IPv4 addresses supported by named ACLs (port-based ACLs [PACLs], VLAN-based ACLs [VACLs], and router-based ACLs [RACLs])
- Traffic storm control (unicast, multicast, and broadcast)
- Unicast Reverse Path Forwarding (Unicast RPF)

For more information, see the [Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.2](#).

## Licensing

The Cisco NX-OS software licensing feature allows you to access premium features on the device after you install the appropriate license for that feature. Any feature not included in a license package is bundled with the Cisco NX-OS software and is provided to you at no extra charge.

You must purchase and install a license for each device.



### Note

With the exception of the Cisco TrustSec feature, you can enable a feature without installing its license. The Cisco NX-OS software gives you a grace period that allows you to try a feature before purchasing its license. You must install the Advanced Services license package to enable the Cisco TrustSec feature.

For detailed information about Cisco NX-OS software licensing, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.2*.

For information about troubleshooting licensing issues, see the [Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 4.x](#).

## Supported Standards

This table lists the IEEE compliance standards.



**Table 1: IEEE Compliance Standards**

| 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                   |
| 802.3ab  | 1000BaseT (10/100/1000 Ethernet over copper) |
| 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            |

This table lists the RFC compliance standards.

**Table 2: RFC Compliance Standards**

| Standard | Description   |
|----------|---|
| BGP      |   |
| RFC 1997 | BGP Communities Attribute                                   |
| RFC 2385 | Protection of BGP Sessions via the TCP MD5 Signature Option |
| RFC 2439 | BGP Route flap damping                                      |
| RFC 2519 | A Framework for Inter-Domain Route Aggregation              |
| RFC 2858 | Multiprotocol Extensions for BGP-4                          |
| RFC 3065 | Autonomous System Confederations for BGP                    |
| RFC 3392 | Capabilities Advertisement with BGP-4                       |

| Standard   | Description  |
|------------|--|
| RFC 4271   | BGP version 4  |
| RFC 4273   | BGP4 MIB - Definitions of Managed Objects for BGP-4                    |
| RFC 4456   | BGP Route reflection   |
| RFC 4486   | Subcodes for BGP cease notification message                            |
| RFC 4724   | Graceful Restart Mechanism for BGP                                     |
| RFC 4893   | BGP Support for Four-octet AS Number Space                             |
| ietf-draft | Bestpath transition avoidance (draft-ietf-idr-avoid-transition-05.txt) |
| ietf-draft | Peer table objects (draft-ietf-idr-bgp4-mib-15.txt)                    |
| ietf-draft | Dynamic Capability (draft-ietf-idr-dynamic-cap-03.txt)                 |
| OSPF       |  |
| RFC 2370   | OSPF Opaque LSA Option   |
| RFC 2328   | OSPF Version 2   |
| RFC 2740   | OSPF for IPv6 (OSPF version 3)   |
| RFC 3101   | OSPF Not-So-Stubby-Area (NSSA) Option                                  |
| RFC 3137   | OSPF Stub Router Advertisement   |
| RFC 3509   | Alternative Implementations of OSPF Area Border Routers                |
| RFC 3623   | Graceful OSPF Restart  |
| RFC 4750   | OSPF Version 2 MIB   |
| RIP        |  |
| RFC 1724   | RIPv2 MIB extension  |

| Standard             | Description   |
|----------------------|---|
| RFC 2082             | RIPv2 MD5 Authentication  |
| RFC 2453             | RIP Version 2   |
| IS-IS                |   |
| RFC 1142 (OSI 10589) | OSI 10589 Intermediate system to intermediate system intra-domain routing exchange protocol                                   |
| RFC 1195             | Use of OSI IS-IS for routing in TCP/IP and dual environment.  |
| RFC 2763             | Dynamic Hostname Exchange Mechanism for IS-IS   |
| RFC 2966             | Domain-wide Prefix Distribution with Two-Level IS-IS  |
| RFC 2973             | IS-IS Mesh Groups   |
| RFC 3277             | IS-IS Transient Blackhole Avoidance   |
| RFC 3373             | Three-Way Handshake for IS-IS Point-to-Point Adjacencies  |
| RFC 3567             | IS-IS Cryptographic Authentication  |
| RFC 3847             | Restart Signaling for IS-IS   |
| ietf-draft           | Internet Draft Point-to-point operation over LAN in link-state routing protocols<br>(draft-ietf-isis-igp-p2p-over-lan-06.txt) |
| IP Services          |   |
| RFC 768              | UDP   |
| RFC 783              | TFTP  |
| RFC 791              | IP  |
| RFC 792              | ICMP  |
| RFC 793              | TCP   |
| RFC 826              | ARP   |

| Standard     | Description   |
|--------------|---|
| RFC 854      | Telnet  |
| RFC 959      | FTP   |
| RFC 1027     | Proxy ARP   |
| RFC 1305     | NTP v3  |
| RFC 1519     | CIDR  |
| RFC 1542     | BootP relay   |
| RFC 1591     | DNS client  |
| RFC 1812     | IPv4 routers  |
| RFC 2131     | DHCP Helper   |
| RFC 2338     | VRRP  |
| RFC 2784     | Generic Routing Encapsulation (GRE)   |
| IP-Multicast |   |
| RFC 2236     | Internet Group Management Protocol, Version 2   |
| RFC 2710     | Multicast Listener Discovery (MLD) for IPv6   |
| RFC 3376     | Internet Group Management Protocol, Version 3   |
| RFC 3446     | Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) |
| RFC 3569     | An Overview of Source-Specific Multicast (SSM)  |
| RFC 3618     | Multicast Source Discovery Protocol (MSDP)  |
| RFC 3810     | Multicast Listener Discovery Version 2 (MLDv2) for IPv6   |

| Standard   | Description  |
|------------|--|
| RFC 4601   | ASM - Sparse Mode (PIM-SM): Protocol Specification (Revised)                                   |
| RFC 4607   | Source-Specific Multicast for IP   |
| RFC 4610   | Anycast-RP Using Protocol Independent Multicast (PIM)  |
| ietf-draft | Mtrace server functionality, to process mtrace-requests, draft-ietf-idmr-traceroute-ipm-07.txt |
| ietf-draft | Bi-directional Protocol Independent Multicast (BIDIR-PIM), draft-ietf-pim-bidir-09.txt         |

