Cisco NX-OS Software for Cisco Nexus 7000 Series Switches

Product Overview

Cisco® NX-OS Software is a modular multitasking and multithreaded operating system built with high availability, detailed fault management, and nondisruptive serviceability at its foundation. Cisco NX-OS helps ensure continuous operation and sets the standard for mission-critical environments. The modular design of Cisco NX-OS makes zero-impact operations a reality and enables exceptional operational flexibility.

Cisco NX-OS provides a robust and comprehensive feature set that fulfills the routing, switching, and storage networking requirements of present and future data centers. With an XML interface and a command-line interface (CLI) like that of Cisco IOS® Software, Cisco NX-OS provides state-of-the-art implementations of relevant networking standards as well as a variety of true data center-class Cisco innovations.

Cisco NX-OS powers the Cisco Nexus® Family of platforms: specifically, Cisco Nexus 7000, 5000, 4000, 3000, and 1000V Series Switches; Cisco Nexus 2000 Series Fabric Extenders; and Cisco MDS 9000 Series Multilayer Switches. Cisco NX-OS Software Release 6.1 is the latest release for the Cisco Nexus 7000 Series.

Features and Benefits

Flexibility and Scalability

- Software compatibility: Cisco NX-OS interoperates with Cisco products running any variant of the Cisco IOS Software operating system. It also interoperates with any networking OS that conforms to the networking standards listed as supported in this data sheet.

- Common software throughout the data center: Cisco NX-OS simplifies the data center operating environment and provides a unified OS designed to run all areas of the data center network, including storage, virtualization, and Layer 3 network protocols.

- Modular software design: Cisco NX-OS is designed to support distributed multithreaded processing on symmetric multiprocessors (SMPs), multicore CPUs, and distributed line-card processors. Computationally intensive tasks, such as hardware table programming, can be offloaded to dedicated processors distributed across the line cards. Cisco NX-OS modular processes are instantiated on demand, each in a separate protected memory space. Thus, processes are started and system resources allocated only when a feature is enabled. The modular processes are governed by a real-time preemptive scheduler that helps ensure the timely processing of critical functions.

  Virtual device contexts (VDCs): Cisco NX-OS offers the capability to segment OS and hardware resources into virtual contexts that emulate virtual devices. Each VDC has its own software processes, dedicated hardware resources (physical interfaces, VLANs, routing table size, Virtual Route Forwarding [VRF], etc.), and independent management environment. VDCs are instrumental in the consolidation of separate networks onto a common infrastructure, maintaining the administrative boundary separation and fault-isolation characteristics of physically separate networks while providing many of the operating cost benefits of a single infrastructure. Each VDC can be restarted without affecting the control, data, or management plane of other VDCs in the system.

Starting with Cisco NX-OS Software Release 6.1, administrator VDC and CPU shares[1] are supported. Administrator VDC enables network administrators to configure systemwide settings such as Control Plane Policing (CoPP); VDC creation, suspension, and deletion; and interface allocation. CPU shares provide the capability to configure CPU access and prioritization for each VDC.

- Support for Cisco Nexus fabric extenders: The Cisco Nexus 7000 Series Switch can act as the parent switch for the Cisco Nexus fabric extenders. Because it is a logical extension of its parent switch, the Cisco Nexus fabric extender inherits the functions and benefits offered by the Cisco Nexus 7000 Series Switch. The combination of the Cisco Nexus 2000 Series Fabric Extenders and Cisco Nexus 7000 Series Switches provides the benefits of top-of-rack (ToR) and end-of-row (EoR) network architectures, enabling data centers to scale the number of Gigabit Ethernet access ports, reducing cable runs and management points in the network. Please refer to the list of supported hardware components later in this document to see the Cisco Nexus fabric extenders supported.

Availability

- Continuous system operation: Cisco NX-OS provides continuous system operation, permitting maintenance, upgrades, and software certification without service interruption. The combination of process modularity, transparent In-Service Software Upgrade (ISSU) capability, and stateful graceful restart mitigates the effects of software upgrades and other operations.

- Hitless ISSU: Hitless ISSU provides the capability to perform transparent software upgrades on platforms with redundant supervisors, reducing downtime and allowing customers to integrate the newest features and functions with little or no negative effect on network operation.

- Smooth development of enhancements and problem fixes: The modularity of Cisco NX-OS allows new features, enhancements, and problem fixes to be transparently integrated into the software. These updated images can then be installed without disruption using Cisco ISSU.

- Process survivability: Critical processes are run in protected memory space and independently of each other and the kernel, providing detailed service isolation and fault containment and enabling modular patching and upgrading and rapid restartability. Individual processes can be restarted independently without loss of state information and without affecting data forwarding, so that after an upgrade or failure, processes restart in milliseconds without negatively affecting adjacent devices or services. Processes with a large number of states as IP routing protocols are restarted using standards-based nonstop forwarding (NSF) graceful restart mechanisms; other processes use a local persistent storage service (PSS) to maintain their state.

- Stateful supervisor failover: Redundant supervisors are kept synchronized at all times to enable rapid stateful supervisor failover. Sophisticated checks are in place to help ensure that the state is consistent and reliable throughout the entire distributed architecture after failover occurs.

- Reliable interprocess communication: Cisco NX-OS facilitates reliable communication between processes to help ensure that all messages are delivered and properly acted on during failure and adverse conditions. This communication helps ensure process synchronization and state consistency across processes that may be instantiated on processors distributed over multiple supervisors and I/O modules.

- Redundant switched Ethernet out-of-band channels (EOBCs): Cisco NX-OS can make full use of redundant EOBCs for communication between control and I/O module processors.

- Network-based availability: Network convergence is optimized by providing tools and functions to make both failover and fallback transparent and fast. For example, Cisco NX-OS provides Spanning Tree Protocol enhancements such as Bridge Protocol Data Unit (BPDU) guard, loop guard, root guard, BPDU filters, and bridge assurance to help ensure the health of the Spanning Tree Protocol control plane; Unidirectional Link Detection (UDLD) Protocol; NSF graceful restart of routing protocols; millisecond timers for First-Hop Resiliency Protocol (FHRP); Shortest-Path First (SPF) optimizations such as link-state advertisement (LSA) pacing and incremental SPF; IEEE 802.3ad link aggregation with adjustable timers; and Bidirectional Forwarding Detection (BFD).

Serviceability

- Troubleshooting and diagnostics: Cisco NX-OS is built with unique serviceability functions to enable network operators to take early action based on network trends and events, enhancing network planning and improving network operations center (NOC) and vendor response times. Cisco Smart Call Home, Cisco Generic Online Diagnostics (GOLD), and Cisco Embedded Event Manager (EEM) are some of the features that enhance the serviceability of Cisco NX-OS.

- Switched Port Analyzer (SPAN): The SPAN feature allows an administrator 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. Encapsulated Remote SPAN (ERSPAN) allows remote monitoring of multiple switches across the network by encapsulating SPAN traffic into a generic routing encapsulation (GRE) tunnel.

- Ethanalyzer: Cisco NX-OS includes a built-in packet analyzer to monitor and troubleshoot control- and data-plane traffic. The packet analyzer is based on the popular Wireshark open source network protocol analyzer.

- IP service-level agreements (SLAs): Cisco NX-OS IP SLAs enable customers to help ensure the service levels of new business-critical IP applications, as well as IP services that use data, voice, and video, in an IP network. Cisco has augmented traditional service-level monitoring and enhanced the IP infrastructure so that it is IP application aware, by measuring services both end to end and at the IP layer. With Cisco NX-OS IP SLAs, users can verify service guarantees, increase network reliability by validating network performance, proactively identify network problems, and increase their return on investment (ROI) by easing the deployment of new IP services. Cisco NX-OS IP SLAs use active monitoring to generate traffic in a continuous, reliable, and predictable manner, thus enabling the measurement of network performance and health.

- Cisco Smart Call Home: The Cisco Smart Call Home feature continuously monitors hardware and software components to provide email-based notification of critical system events. A versatile range of message formats is available for optimal compatibility with pager services, standard email, and XML-based automated parsing applications. The feature offers alert grouping capabilities and customizable destination profiles. It can be used, for example, to directly page a network support engineer, send an email message to a 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, enabling networking devices to inform IT when a problem occurs and helping ensure that the problem is acted on quickly, reducing time to resolution and increasing system uptime.

- Cisco GOLD: Cisco GOLD is a suite of diagnostic facilities to verify that hardware and internal data paths are operating as designed. Boot-time diagnostics, continuous monitoring, standby fabric loopback tests, and on-demand and scheduled tests are part of the Cisco GOLD feature set. This industry-leading diagnostics subsystem allows rapid fault isolation and continuous system monitoring critical in today's continuously operating environments.
- Cisco EEM: Cisco EEM is a powerful device and system management technology integrated into Cisco NX-OS. Cisco EEM helps customers harness the network intelligence intrinsic to the Cisco software and enables them to customize behavior based on network events as they happen.
- Cisco NetFlow: The Cisco NX-OS implementation of NetFlow supports NetFlow Versions 5 and 9 exports as well as the Flexible NetFlow configuration model. Cisco Nexus 7000 M-Series modules support Full NetFlow and Sampled NetFlow. Cisco Nexus 7000 F2-Series modules will support Sampled NetFlow in NX-OS release 6.1.2. F2 NetFlow sampling rate is greater than 1:8192 so that users have the flexibility to tune the sampling range (flows per second, amount of NetFlow data generated, etc.) based on their NetFlow requirements. In addition to Layer 3 NetFlow, Layer 2 NetFlow is supported across all line cards.

Manageability

- Programmatic XML interface: Based on the NETCONF industry standard, the Cisco NX-OS XML interface provides a consistent API for devices, enabling rapid development and creation of tools to enhance the network.
- Simple Network Management Protocol (SNMP): Cisco NX-OS complies with SNMPv1, v2c, and v3. A comprehensive collection of MIBs is supported.
- Configuration verification and rollback: With Cisco NX-OS, the system operator can verify the consistency of a configuration and the availability of necessary hardware resources prior to committing the configuration. A device can thus be preconfigured and the verified configuration applied at a later time. Configurations also include checkpoints to allow operators to roll back to a known good configuration as needed.
- Port profiles: Port profiles enable customers to define a policy once and then apply it many times across virtual and physical ports, significantly increasing both efficiency and flexibility in today's virtual data centers.
- Role-based access control (RBAC): With RBAC, Cisco NX-OS enables administrators to limit access to switch operations by assigning roles to users. Administrators can customize access and restrict it to the users who require it. Cisco NX-OS also provides a mechanism to distribute configuration of RBAC roles across devices running Cisco NX-OS for simplified deployment.
- Cisco Data Center Network Manager (DCNM): Cisco DCNM is a management solution dedicated to data center network operations. Cisco DCNM increases the overall data center infrastructure uptime and reliability, thereby enabling business continuity. The solution is designed for the Cisco NX-OS product family.
- Connectivity management processor (CMP) support: Cisco NX-OS supports the use of a CMP for lights-out, remote management of the platform. The CMP aids operations by providing an out-of-band access channel to the Cisco NX-OS console. IPv6 support for the CMP interface is also available, including ping6 and traceroute6.

Traffic Routing, Forwarding, and Management

- Ethernet switching: Cisco NX-OS is built to support high-density, high-performance Ethernet systems, and it provides a complete data center-class Ethernet switch feature set. The feature set includes IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1w and 802.1s); IEEE 802.1Q VLANs and trunks; QinQ; 16,000-subscriber VLANs; IEEE 802.3ad link aggregation; Link Layer Discovery Protocol (LLDP; IEEE 802.1AB); private VLANs; cross-chassis private VLANs; UDLD in aggressive and standard modes; VLAN Trunking Protocol (VTP) Versions 1 and 2 in client, server, pruning, and transparent modes; and traffic suppression (unicast, multicast, and broadcast). Spanning Tree Protocol enables transparent upgrades using Cisco ISSU in Spanning Tree Protocol environments, BPDU guard, loop guard, root guard, BPDU filters, bridge assurance, and jumbo frame support.

- Cisco Overlay Transport Virtualization (OTV): OTV is a "MAC address in IP" technique for supporting Layer 2 VPNs over any transport, whether it is Layer 2 based or Layer 3 based. By using the principles of MAC address routing, OTV provides an overlay that enables Layer 2 connectivity between separate Layer 2 domains while preserving the fault-isolation benefits of an IP-based interconnection. The core principles on which OTV operates are the use of a control protocol to advertise MAC address reachability information (instead of using data-plane learning) and packet switching of IP encapsulated Layer 2 traffic (instead of using circuit switching). Some of the main benefits achieved with OTV include:

  ○ Zero effect on existing network design: OTV is a transport-agnostic Layer 2 interconnect technology. The configuration is transparent to the sites under consideration.

  ○ Failure isolation: OTV preserves the failure boundary and site independence. OTV does not rely on traffic flooding to propagate reachability information for MAC addresses; instead, a control protocol is used to distribute such information, sites remain independent of each other, and failures do not propagate beyond the OTV edge device.

  ○ Optimized operations: OTV enables single-touch site additions and removals. This feature provides an important operational benefit because the configuration is succinct and uses a single protocol with no add-ons.

  ○ Optimal bandwidth use, resiliency, and scalability: OTV allows multipathing (cross-sectional bandwidth and end-to-end Layer 2 multipathing), transparent multihoming with built-in loop prevention, and multipoint connectivity in an easy-to-manage point-to-cloud model. It does not require the creation of closed tunnels, and the only state maintained is that of a MAC address routing table. The state is distributed and can be programmed in the hardware conditionally to allow the overlay to handle larger numbers of MAC addresses.

  ○ Transparent migration path: Because OTV is agnostic to the core and transparent to the sites, it can be incrementally deployed over any existing topology without altering its network design.

- Ethernet enhancement: The virtual PortChannel (vPC) feature allows one end of a PortChannel to be split across a pair of Cisco Nexus 7000 Series Switches. vPC provides Layer 2 multipathing through the elimination of Spanning Tree Protocol blocked ports in dual-homed connections. vPC enables fully used bisectional bandwidth and simplified Layer 2 logical topologies without the need to change the existing management and deployment models.

- Cisco FabricPath: Cisco FabricPath is a set of multipath Ethernet technologies that combine the reliability and scalability benefits of Layer 3 routing with the flexibility of Layer 2 networks, enabling IT to build massively scalable data centers. Cisco FabricPath offers a topology-based Layer 2 routing mechanism that provides an equal-cost multipath (ECMP) forwarding model. Cisco FabricPath implements an enhancement that solves the MAC address table scalability problem characteristic of switched Layer 2 networks. Furthermore, Cisco FabricPath supports enhanced vPC (vPC+), a technology similar to vPC that allows redundant interconnection of the existing Ethernet infrastructure to Cisco FabricPath without using Spanning Tree Protocol. Benefits introduced by the Cisco FabricPath technology include:
  - Operation simplicity: Cisco FabricPath embeds an autodiscovery mechanism that does not require any additional platform configuration. By offering Layer 2 connectivity, the "VLAN anywhere" characteristic simplifies provisioning and offers workload flexibility across the network.
  - High resiliency and performance: Because Cisco FabricPath is a Layer 2 routed protocol, it offers stability, scalability, and optimized resiliency along with network failure containment.
  - Massively scalable fabric: By building a forwarding model on 16-way ECMP routing, Cisco FabricPath helps prevent bandwidth bottlenecks and allows organizations to add capacity dynamically, without network disruption.
- IP routing: Cisco NX-OS supports a wide range of IPv4 and v6 services and routing protocols. It provides state-of-the-art implementations of the following routing protocols:
  - Open Shortest Path First (OSPF) Protocol Versions 2 (IPv4) and 3 (IPv6)
  - Intermediate System-to-Intermediate System (IS-IS) Protocol for IPv4 and IPv6
  - Border Gateway Protocol (BGP) for IPv4 and IPv6
  - Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 and IPv6
  - Routing Information Protocol Version 2 (RIPv2)

  The implementations of these protocols are fully compliant with the latest standards, providing modern enhancements and parameters such as 4-byte autonomous system numbers (ASNs), while shedding unused older functions in favor of a lean implementation that accelerates feature deployment and enhances system stability. NSF graceful restart (NSF-GR) is supported by all unicast protocols. All protocols support all interface types, including Ethernet interfaces, switched virtual interfaces (SVIs) and subinterfaces, PortChannels, tunnel interfaces, and loopback interfaces. The great variety of routing protocols and functions is complemented by a broad collection of IP services, including the following:
  - VRF-lite and MPLS VPNs as described in RFCs 2547 and 4364
  - Dynamic Host Configuration Protocol (DHCP) Helper
  - Unicast Reverse Path Forwarding (uRPF) for IPv4 and IPv6
  - Hot-Standby Routing Protocol (HSRP) for IPv4 and IPv6
  - Virtual Router Redundancy Protocol (VRRP) for IPv4
  - Gateway Load Balancing Protocol (GLBP) for IPv4
  - Enhanced object tracking
  - Policy-based routing (PBR) for IPv4 and IPv6

- Generic routing encapsulation (GRE) tunneling
- Unicast graceful restart for all protocols in IPv4
- Unicast graceful restart for OSPFv3 in IPv6
- IP Multicast: Cisco NX-OS provides an industry-leading IP Multicast feature set. The Cisco NX-OS implementation lays the foundation for the future development of a comprehensive portfolio of multicast-enabled network functions. In a way similar to its support for the unicast routing protocols, Cisco NX-OS includes state-of-the-art implementations of the following multicast protocols and functions:
  - Protocol-Independent Multicast Version 2 (PIMv2)
  - Source-Specific Multicast (SSM) for IPv4 and IPv6
  - PIM Sparse Mode (Any-Source Multicast [ASM] for IPv4 and IPv6)
  - Bidirectional PIM (Bidir PIM) for IPv4 and IPv6
  - Anycast Rendezvous Point (Anycast-RP)
  - Multicast NSF for IPv4 and v6
  - 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)
  - IGMP cache on non-disaster recovery for fast convergence
  - Policies for multicast configuration (**ip pim rp-addr** and **ip igmp join-group** or **static-group**)
  - IGMP group-specific queries to router ports only
  - Debug filters for IGMP snooping
- Quality of service (QoS): Cisco NX-OS supports numerous QoS mechanisms, including classification, marking, queuing, policing, and scheduling. Modular QoS CLI (MQC) is supported for all QoS features. MQC can be used to provide uniform configurations across various Cisco platforms.
- Multiprotocol Label Switching (MPLS): Cisco NX-OS supports a comprehensive set of MPLS features including label switching, Layer 3 VPNs, MPLS Traffic Engineering with Fast Reroute (FRR), Multicast VPNs for IPv4, and IPv6 provider edge (6PE) and IPv6 VPN provider edge (6VPE). These features, which interoperate with Cisco IOS Software, provide the foundation for network consolidation and centralization of services and policy control for a securely segmented network fabric, enabling reduced capital expenditures (CapEx) and operating expenses (OpEx) for IT managers.
- Fibre Channel over Ethernet (FCoE): FCoE is a standards-based encapsulation of Fibre Channel frames into Ethernet packets. This technology introduces storage I/O consolidation on top of Ethernet switching fabric in the data centers of the future. FCoE can now be deployed in director-class, highly available, modular platforms for the access layer and core of converged networks. In addition to FCoE hosts and targets support, VE-port support allows FCoE Inter-Switch Links (ISLs) to be formed, creating scalable, multihop FCoE topologies. The FCoE traffic in a Cisco Nexus 7000 Series Switch can be segmented using a dedicated storage VDC, providing an exceptional level of segmentation and isolation of the shared physical infrastructure.

- Location/ID Separation Protocol (LISP): LISP is an evolutionary routing architecture designed for Internet scale and global reach across organizations. The scalability of the routing system and the exhaustion of the IPv4 address space have motivated several proposals based on a common concept: the separation of the locator and identifier in the numbering of Internet devices, often called the Loc/ID split. LISP defines this protocol. The basic idea behind the Loc/ID split is that the current Internet routing and addressing architecture combines two functions: routing locators (RLOCs), which describe how a device is attached to the network, and endpoint identifiers (EIDs), which define "who" the device is, in a single numbering space: the IP address. The advantages include improved scalability of the routing system through greater aggregation of RLOCs. Cisco LISP virtual machine mobility (VM-mobility) is designed to enable global IP endpoint mobility across private networks as well as the Internet to provide a flexible connectivity continuum and enable global cloud computing across organizational boundaries.

- Traffic redirection: Cisco NX-OS supports Web Cache Control Protocol (WCCP) Version 2 in a Layer 2 forwarding mode. WCCP allows the use of cache engines to localize web traffic patterns in the network, enabling content requests to be fulfilled locally. Traffic localization reduces transmission costs and download time. WCCP enables the Cisco Nexus 7000 Series to transparently redirect content requests. The main benefit of transparent redirection is that users need not configure their browsers to use a web proxy. Instead, they can use the target URL to request content and have their requests automatically redirected to a cache engine. WCCP enables a series of cache engines, called a cache engine cluster, to provide content to a router or multiple routers. Clustering cache engines greatly improves the scalability, redundancy, and availability of the caching solution. Clustering of up to 32 cache engines per service group is supported.

- IEEE 1588-2008 (v2) Precision Time Protocol (PTP): IEEE 1588, or PTP, is a time synchronization protocol for nodes distributed across a network. It provides greater accuracy than other time synchronization protocols, such as NTP, because of its hardware time-stamp feature. The Cisco Nexus 7000 F-Series I/O module supports IEEE 1588 PTP in hardware. Pong, a new network monitoring tool that takes advantage of this IEEE 1588 time synchronization infrastructure, is used to diagnose the health of the network. Pong allows measuring of port-to-port delays and is similar to the well-known network monitoring utility ping, but provides a greater depth of network diagnostics.

Network Security
- Cisco TrustSec® security: As part of the Cisco TrustSec security suite, Cisco NX-OS provides outstanding data confidentiality and integrity, supporting standard IEEE 802.1AE link-layer cryptography with 128-bit Advanced Encryption Standard (AES) cryptography. Link-layer cryptography helps ensure end-to-end data privacy while allowing the insertion of security service devices along the encrypted path. The security group access control list (SGACL), a new network access control model, is based on security group tags instead of IP addresses, enabling implementation of policies that are more concise and easier to manage because of their topology independence.

- Additional network security features: In addition to Cisco TrustSec security, Cisco NX-OS delivers the following security features:
  ◦ Data path intrusion detection system (IDS) for protocol-conformance checks
  ◦ CoPP
  ◦ Message Digest Algorithm 5 (MD5) routing protocol authentication
  ◦ Cisco integrated security features, including Dynamic ARP Inspection (DAI), DHCP snooping, and IP source guard

- ◦ Authentication, authorization, and accounting (AAA) and TACACS+
- ◦ Secure Shell (SSH) Protocol Version 2
- ◦ SNMPv3 support
- ◦ Port security
- ◦ IEEE 802.1x authentication and RADIUS support
- ◦ Layer 2 Cisco Network Admission Control (NAC) LAN port IP
- ◦ Policies based on MAC addresses and IPv4 and IPv6 addresses supported by named ACLs (port-based ACLs [PACLs], VLAN-based ACLs [VACLs], and router-based ACLs [RACLs])

New Software Features in Cisco NX-OS Software Release 6.1

Table 1 lists the new software features in Cisco NX-OS Software Release 6.1.

Table 1.   New Software Features in Cisco NX-OS Software Release 6.1

Feature	Description
Pong	Added support for Cisco FabricPath traceroute pong
FCoE	FCoE support on F2 modules (part number N7K-F248XP-25) module with Cisco Nexus 7000 Series Supervisor 2 and Supervisor 2E
VDC scalability	8 VDCs on Cisco Nexus 7000 Series Supervisor 2E
administrator VDC	1 admin VDC on Cisco Nexus 7000 Series Supervisor 2 and Supervisor 2E
VDC control groups	Capability to configure CPU shares per VDC with Cisco Nexus 7000 Series Supervisor 2 and Supervisor 2E
ISISv6	ISISv6 single-topology support
ERSPAN	ERSPAN support on F1 and F2 modules
OSPF	Support for OSPF flexible distance manipulation
BGP add path	Support for BGP add path
PVALN	PVLAN support on F2 modules
RBACL	RBACL support on F2 modules
VACL	VACL capture support on M2 modules
Fabric extender scalability	Support for 45 fabric extender modules; requires Cisco Nexus 7000 Series Supervisor 2E
IP SLA	IP SLA support
QoS	DSCP-to-queue mapping on F2 modules

Product Specifications

Supported Standards

Tables 2 and 3 provide standards-compliance information for Cisco NX-OS Software on Cisco Nexus 7000 Series Switches.

Table 2.   IEEE Compliance

Standard	Description
IEEE 802.1D	MAC Bridges
IEEE 802.1s	Multiple Spanning Tree Protocol
IEEE 802.1w	Rapid Spanning Tree Protocol
IEEE 802.1ab	LLDP
IEEE 802.1AE	MAC Security (Link-Layer Cryptography)
IEEE 802.1Q	VLAN Tagging

Standard	Description
IEEE 802.1p	Class-of-Service (CoS) Tagging for Ethernet frames
IEEE 802.1x	Port-Based Network Access Control
IEEE 802.3ad	Link Aggregation with LACP
IEEE 802.3ab	1000BASE-T (10/100/1000 Ethernet over Copper)
IEEE 802.3z	Gigabit Ethernet
IEEE 802.3ae	10 Gigabit Ethernet
IEEE P802.1Qbb	Priority Flow Control
IEEE P802.1Qaz	Enhanced Transmission Selection
IEEE P802.1Qaz	Data Center Bridging (DCB) Exchange Protocol
IEEE 1588-2008	Precision Time Protocol
Fibre Channel Standards	
T11 FC-BB-5	Fibre Channel over Ethernet (FCoE)

Table 3.   RFC Compliance

Standard	Description
BGP	
RFC 1997	BGP Communities Attribute
RFC 2385	Protection of BGP Sessions with the TCP MD5 Signature Option
RFC 2439	BGP Route Flap Damping
RFC 2519	A Framework for Inter-Domain Route Aggregation
RFC 2545	Use of BGPv4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC 2858	Multiprotocol Extensions for BGPv4
RFC 3065	Autonomous System Confederations for BGP
RFC 3392	Capabilities Advertisement with BGPv4
RFC 4271	BGPv4
RFC 4273	BGPv4 MIB: Definitions of Managed Objects for BGPv4
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
RFC 5668	4-Octet AS Specific BGP Extended Community
ietf-draft	Bestpath Transition Avoidance (draft-ietf-idr-avoid-transition-05.txt)
ietf-draft	Peer TableObjects (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 (OSPFv3)
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

Standard	Description
RIP	
RFC 1724	RIPv2 MIB Extension
RFC 2082	RIPv2 MD5 Authentication
RFC 2453	RIP Version 2
IS-IS	
RFC 1142 (OSI 10589)	OSI 10589 Intermediate System-to-Intermediate System (IS-IS) Intra-Domain Routing Exchange Protocol
RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
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 Black-Hole 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 (draft-ietf-isis-igp-p2p-over-lan-06.txt)
IP Services	
RFC 768	User Datagram Protocol (UDP)
RFC 783	Trivial File Transfer Protocol (TFTP)
RFC 791	IP
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 959	FTP
RFC 1027	Proxy ARP
RFC 1305	Network Time Protocol (NTP) Version 3
RFC 1519	Classless Interdomain Routing (CIDR)
RFC 1542	BOOTP Relay
RFC 1591	Domain Name System (DNS) Client
RFC 1812	IPv4 Routers
RFC 2131	DHCP Helper
RFC 2338	VRRP
RFC 2474	Differentiated Services Field (DS Field)
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 Mechanism Using PIM and MSDP
RFC 3569	An Overview of SSM
RFC 3618	Multicast Source Discovery Protocol (MSDP)
RFC 3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 4601	Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)

Standard	Description
RFC 4607	Source-Specific Multicast for IP
RFC 4610	Anycast-RP using PIM
RFC 5132	IP Multicast MIB
ietf-draft	Traceroute Facility for IP Multicast (draft-ietf-idmr-traceroute-ipm-07.txt)
ietf-draft	Bidirectional Protocol Independent Multicast (BIDIR-PIM, draft-ietf-pim-bidir-09.txt)
Ietf-draft	Bidirectional Forwarding Detection
OTV	
Ietf-draft	Overlay Transport Virtualization (draft-hasmit-otv-00)
MPLS	
RFC 3031	MPLS Architecture
RFC 3032	MPLS Label-Stack Encoding
RFC 3036	LDP Specification
RFC 3478	Graceful Restart Mechanism for Label Distribution Protocol
RFC 3812	Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
RFC 3813	Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)
RFC 4382	MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base
RFC 3815	Definitions of Managed Objects for Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP)
IETF DRAFT	draft-ietf-mpls-fastreroute-mib: Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base for Fast Reroute
RFC 5036	LDP Specification (obsoletes RFC 3036): Partial Support
RFC 5443	LDP IGP Synchronization
IETF Draft	LDP Capabilities (draft-ietf-mpls-ldp-capabilties-04.txt draft)
IETF Draft	LDP Typed Wildcard FEC (draft-ietf-mpls-ldp-typed-wildcard-03.txt)
RFC 2685	Virtual Private Networks Identifier
RFC 2858	Multiprotocol Extensions for BGP-4
RFC 3107	Carrying Label Information in BGP-4
RFC 3630	Traffic Engineering (TE) Extensions to OSPF Version 2
RFC 4364	BGP or MPLS IP VPNs (No InterAS support)
RFC 4365	Applicability Statement for BGP or MPLS IP VPNs
RFC 4382	MPLS or BGP Layer 3 VPN MIB
RFC 4576	Using LSA Options Bit to Prevent Looping in BGP or MPLS IP VPNs (DN Bit)
RFC 4577	OSPF as the PE or CE Protocol in BGP or MPLS IP VPNs
RFC 4659	BGP-MPLS IP VPN Extension for IPv6 VPN (No InterAS support)
RFC 4760	Multi-protocol Extensions for BGP-4
RFC 4781	Graceful Restart Mechanism for BGP with MPLS
RFC 5305	IS-IS Extensions for Traffic Engineering
RFC 5307	IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
IETF DRAFT	BGP Custom Decision Process
RFC 2205	RSVPv1 Functional Specification
RFC 2209	RSVPv1 Message Processing Rules
RFC 2702	TE over MPLS
RFC 2747	RSVP Cryptographic Authentication
RFC 2961	RSVP Refresh Overhead Reduction Extensions
RFC 3209	RSVP-TE

Standard	Description
RFC 3270	MPLS Support of Differentiated Services
RFC 3784	ISIS-TE
RFC 4090	Fast Re-Route for RSVP-TE Extensions
RFC 4569	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 4798	Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)
LISP	
IETF DRAFT	LISP Canonical Address Format (LCAF)
IETF DRAFT	Locator/ID Separation Protocol (LISP)
IETF DRAFT	Interworking LISP with IPv4 and IPv6
IETF DRAFT	LISP Map-Versioning
IETF DRAFT	LISP Map Server
IETF DRAFT	LISP for Multicast Environments
TRILL	
IETF DRAFT	Compatible with Transparent Interconnection of Lots of Links (TRILL) - (Cisco FabricPath is based on TRILL)

Supported Hardware Components

- Cisco Nexus 7000 9-Slot Switch
- Cisco Nexus 7000 Series 9-Slot Fabric 2 Module
- Cisco Nexus 7000 Series 9-Slot System Fan Tray
- Cisco Nexus 7000 10-Slot Switch
- Cisco Nexus 7000 Series 10-Slot Fabric Module
- Cisco Nexus 7000 Series 10-Slot Fabric 2 Module
- Cisco Nexus 7000 Series 10-Slot System Fan Tray
- Cisco Nexus 7000 Series 10-Slot Fabric Fan Tray
- Cisco Nexus 7000 18-Slot Switch
- Cisco Nexus 7000 Series 18-Slot Fabric Module
- Cisco Nexus 7000 Series 18-Slot Fabric 2 Module
- Cisco Nexus 7000 Series 18-Slot Fan Tray
- Cisco Nexus 7000 6.0-kW AC Power Supply Module
- Cisco Nexus 7000 7.5-kW AC Power Supply Module
- Cisco Nexus 7000 6.0-kW DC Power Supply Module
- Cisco Nexus 7000 Series Supervisor 1 Module
- Cisco Nexus 7000 Series Supervisor 2 Module
- Cisco Nexus 7000 Series Supervisor 2E Module
- Cisco Nexus 7000 Series 48-Port 10/100/1000 Ethernet Module (M1-Series)
- Cisco Nexus 7000 Series 48-Port 10/100/1000 Ethernet Module (M1-XL-Series)
- Cisco Nexus 7000 Series 48-Port Gigabit Ethernet Module (M1-XL-Series)
- Cisco Nexus 7000 Series 48-Port Gigabit Ethernet SFP Module (M1-Series)
- Cisco Nexus 7000 Series 48-Port Gigabit Ethernet SFP Module (M1-XL-Series)

- Cisco Nexus 7000 Series 8-Port 10 Gigabit Ethernet Module (M1-XL-Series)
- Cisco Nexus 7000 Series 32-Port 10 Gigabit Ethernet Module (M1-Series)
- Cisco Nexus 7000 Series 32-Port 10 Gigabit Ethernet Module (M1-XL-Series)
- Cisco Nexus 7000 Series 24-Port 10 Gigabit Ethernet Module (M2-XL-Series)
- Cisco Nexus 7000 Series 6-Port 40 Gigabit Ethernet Module (M2-XL Series)
- Cisco Nexus 7000 Series 2-Port 100 Gigabit Ethernet Module (M2-XL Series)
- Cisco Nexus 7000 Series 32-Port 1/10 Gigabit Ethernet Module (F1-Series)
- Cisco Nexus 7000 Series 48-Port 1/10 Gigabit Ethernet Small Form-Factor (SFP) and Enhanced SFP (SFP+) Module (F2-Series)
- Cisco Nexus 2248TP GE Fabric Extender
- Cisco Nexus 2232PP 10GE Fabric Extender
- Cisco Nexus 2224TP GE Fabric Extender
- Cisco Nexus 2248TP-E GE Fabric Extender
- Cisco Nexus 2232TM 10GE Fabric Extender

Licensing

Cisco NX-OS for the Cisco Nexus 7000 Series offers a suite of licenses, each of which enables a unique set of features as shown in Table 6. All the license features except FCoE are chassis based, meaning each license enables the features within that license for all I/O modules and single or redundant supervisors that reside in the chassis. The only exception to this is FCoE, which requires a license for each I/O module.

The Base license offers a comprehensive feature set at no additional cost, and incremental capabilities can be added with additional licenses. The LAN Enterprise license (N7K-LAN1K9) enables a complete list of Layer 3 protocols, and the VDC licenses (N7K-ADV1K9 and N7K-VDC1K9) enable VDCs for Cisco Nexus 7000 Series Supervisor 1, Supervisor 2, and Supervisor 2E Modules. Note that all Cisco Nexus 7000 Series licenses enable independent features; thus, there is no hierarchy in which one license includes the features of another license. For example, Layer 3 protocols and VDCs require both the LAN Enterprise license and the VDC license.

The Transport Services license (N7K-TRS1K9) enables an IP-based data center interconnect (DCI) solution by including the OTV and LISP technologies. The Enhanced Layer 2 license (N7K-EL21K9) enables Cisco FabricPath, the latest Cisco technology to massively scale Layer 2 data centers. The Scalable Services license, applied on a per-chassis basis, enables Cisco Nexus 7000 XL-Series capabilities on all XL-capable line cards in the chassis. MPLS services such as Layer 3 VPN, MPLS traffic engineering (MPLS-TE), multicast virtual private network (MVPN), and 6PE and 6VPE are enabled with the MPLS license (N7K-MPLS1K9).

Storage features are enabled with the FCoE licenses and the SAN license. FCoE is licensed on a per-module basis and enables FCoE functions on the Cisco Nexus 7000 F1-Series and F2-Series I/O modules. FCoE is the only license that is not chassis based. The next sections provide more information about each license.

LAN Enterprise Package

The following functions are available only with the Enterprise license of Cisco NX-OS Software Release 6.1:

- IP routing
  - OSPFv2 and v3 (IPv4 and IPv6)
  - IS-IS (IPv4)
  - BGP (IPv4 and IPv6)
  - EIGRP (IPv4 and IPv6)
- IP Multicast
  - PIM: Sparse, Bidir, ASM, and SSM modes (IPv4 and IPv6)
  - MSDP (IPv4)
- PBR (IPv4 and IPv6)
- GRE tunnels

VDC Licenses

The VDC licenses enable the use of the following functions in Cisco NX-OS:

- 4 VDCs + 1 Administrator VDC[2]: Four VDC licenses for Cisco Nexus 7000 Series Supervisor 1 and 2 Modules
- +4 VDCs: Increments VDC licenses by four; allows Cisco Nexus 7000 Series Supervisor 2 Enhanced to scale up to eight VDCs

Transport Services Package

The Transport Services package enables the use of the following functions in Cisco NX-OS:

- OTV[3]
- LISP

Enhanced Layer 2 Package

The Enhanced Layer 2 Package enables the use of the following functions in Cisco NX-OS:

- Cisco FabricPath
- Pong

Scalable Feature License

The Scalable Feature license provides the flexibility to enable systemwide Cisco Nexus 7000 XL-Series capabilities without requiring a hardware module change or upgrade. A single license per system enables all XL-capable I/O modules to operate in XL mode. After the single system license is added to a system, all modules that are XL capable are enabled with no additional licensing.

MPLS Feature License[4]

The MPLS feature license enables the use of the following functions in Cisco NX-OS:

- MPLS VPN
- LDP
- MPLS QoS
- TE and FRR
- mVPN
- MPLS OAM
- 6PE and 6VPE

FCoE Feature License

The FCoE feature license enables director-class multihop FCoE implementation in a highly available modular switching platform for the access layer and core of a converged network fabric. FCoE is supported on the Cisco Nexus 7000 F1-Series and F2-Series line cards. This license also enables the use of a storage VDC for the FCoE traffic within the Cisco Nexus 7000 Series. VDC licenses are not required to enable the storage VDC. FCoE support requires Cisco Nexus 7000 Series Supervisor 2 or Supervisor 2E.

Storage Enterprise Feature License[5]

The Storage Enterprise feature license enables Inter-VSAN Routing (IVR), advanced security features such as VSAN-based access controls, and fabric bindings for open systems.

Ordering Information

To place an order, visit the Cisco Ordering homepage. To download software, visit the Cisco Software Center. Tables 4 and 5 list the Cisco Nexus 7000 Series licenses and software images available and their part numbers.

Table 4.   Cisco Nexus 7000 Series Licenses

Description	Part Number
Nexus 7000 LAN Enterprise License (L3 protocols)	N7K-LAN1K9
Nexus 7000 VDC Licenses[a] (VDC)	N7K-ADV1K9, N7K-VDC1K9
Nexus 7000 Enhanced Layer 2 License (FabricPath)	N7K-EL21K9
Nexus 7000 Transport Services License (OTV/LISP)	N7K-TRS1K9
Nexus 7000 MPLS License	N7K-MPLS1K9
Nexus 7009 Scalable Feature License	N7K-C7009-XL
Nexus 7010 Scalable Feature License	N7K-C7010-XL
Nexus 7018 Scalable Feature License	N7K-C7018-XL
Nexus 7000 SAN Enterprise License	N7K-SAN1K9
Cisco FCoE License for Nexus 7000 32-port 10G SFP+ (F1)	N7K-FCOEF132XP
Cisco FCoE License for Nexus 7000 48 port 10G SFP/SFP+ (F2)	N7K-FCOEF248XP
DCNM for Nexus 7000	DCNM-N7K-K9
DCNM for SAN Advanced Edition for Nexus 7000	DCNM-SAN-N7K-K9

Table 5.   Cisco Nexus 7000 Series Images

Description	Part Number
Cisco NX-OS Release 4.2 Software for the Cisco Nexus 7000 Supervisor 1	N7KS1K9-42
Cisco NX-OS Release 5.0 Software for the Cisco Nexus 7000 Supervisor 1	N7KS1K9-50
Cisco NX-OS 5.0 No Payload Encryption Software (no CTS)	N7KS1NPEK9-50
Cisco NX-OS Release 5.1 Software for the Cisco Nexus 7000 Supervisor 1	N7KS1K9-51
Cisco NX-OS 5.1 No Payload Encryption Software (no CTS)	N7KS1NPEK9-51
Cisco NX-OS Release 5.2 Software for the Cisco Nexus 7000 Supervisor 1	N7KS1K9-52
Cisco NX-OS 5.2 No Payload Encryption Software (no CTS)	N7KS1NPEK9-52
Cisco NX-OS Release 6.0 Software for the Cisco Nexus 7000 Supervisor 1	N7KS1K9-60
Cisco NX-OS 6.0 No Payload Encryption Software (no CTS)	N7KS1NPEK9-60
Cisco NX-OS Release 6.1 Software for the Cisco Nexus 7000 Supervisor 1	N7KS1K9-61
Cisco NX-OS Release 6.1 Software for the Cisco Nexus 7000 Supervisor 1 Payload Encryption Software (no CTS)	N7KS1NPEK9-61
Cisco NX-OS Release 6.1 Software for the Cisco Nexus 7000 Supervisor 2	N7KS2K9-61
Cisco NX-OS Release 6.1 Software for the Cisco Nexus 7000 Supervisor 2 Payload Encryption Software (no CTS)	N7KS2NPEK9-61

Table 6 provides a summary of Cisco NX-OS features and licenses.

Table 6.   Cisco NX-OS Features and Licenses

Scalable Services (XL)				
Enterprise LAN	**VDC Licenses**	**Enhanced Layer 2**	**MPLS**	**FCoE**[b]
• IP routing • OSPFv2 • OSPFv3 • IS-IS • ISIS for IPv6 • BGP for IPv4 • BGP for IPv6 • EIGRP for IPv4 • EIGRP for IPv6 • BFD • IP Multicast • PIM: Sparse, Bidir, ASM, and SSM for IPv4 and IPv6 • Multicast Source Discovery Protocol (MSDP) for IPv4 • PBR for IPv4 and IPv6 • GRE Tunnels	• 4 VDCs: 4 VDC licenses for Cisco Nexus 7000 Series Supervisor 1 and 2 • +4 VDCs: Increments VDC licenses by 4; allows Cisco Nexus 7000 Series Supervisor 2E to scale up to 8 VDCs	• Cisco FabricPath • Pong	• MPLS VPN • LDP • MPLS QoS • TE and FRR • mVPN • MPLS OAM • 6PE and 6VPE	• Multihop FCoE • FCoE forwarder (FCF) • FCoE initialization Protocol (FIP)
	Transport Services			**Storage Enterprise**
	• OTV • LISP			• IVR • VSAN-based access control
Base	vPC, port profile, WCCP, port security, Cisco GOLD, Cisco EEM, TACACS, LACP, ACL, QoS, Spanning Tree Protocol, Spanning Tree Protocol guards, UDLD, Cisco Discovery Protocol, CoPP, uRPF, IP source guard, DHCP snooping, CMP, ISSU, single sign-on (SSO), DAI, Cisco Smart Call Home, SNMP, IEEE 802.1x, SPAN, NetFlow v5 and v9, IEEE 1588, static routes, VRF route leaking, Cisco TrueSec[c], and DCB			

More information about Cisco NX-OS licensing can be found in the Cisco NX-OS Licensing Guide:
http://www.cisco.com/en/US/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html.

Cisco Services

Cisco offers a wide range of services to help accelerate your success in deploying and optimizing Cisco Nexus 7000 Series Switches in your data center. Cisco's innovative services are delivered through a unique combination of people, processes, tools, and partners and are focused on helping you increase operation efficiency and improve your data center network. Cisco Advanced Services uses an architecture-led approach to help you align your data center infrastructure with your business goals and achieve long-term value. Cisco SMARTnet® Service helps you resolve mission-critical problems with direct access at any time to Cisco network experts and award-winning resources. With this service, you can take advantage of the Cisco Smart Call Home service capability, which offers proactive diagnostics and real-time alerts on your Cisco Nexus 7000 Series Switches. Spanning the entire network lifecycle, Cisco Services helps protect your investment, optimize network operations, support migration, and strengthen your IT expertise. For more information about Cisco Data Center Services, visit http://www.cisco.com/go/dcservices.

For More Information

For more information about Cisco NX-OS, visit the product homepage at http://www.cisco.com/go/nxos or contact your local account representative.

[1] Administrator VDC and CPU shares require a Cisco Nexus 7000 Series Supervisor 2 or Supervisor 2E Module in Cisco NX-OS 6.1.
[2] Administrator VDC is supported only on Cisco Nexus 7000 Series Supervisor 2.
[3] For OTV deployment, the LAN Enterprise and VDC license packages are required.
[4] For MPLS deployment, the LAN Enterprise package is required.
[5] For IVR using the SAN license, the FCoE package is required.

[a] The VDC license was called the Advanced license before Cisco NX-OS Software Release 6.1.
[b] This license is a per module-based license.
[c] Cisco TrustSec was added to the Base license in Cisco NX-OS Software Release 6.1. Prior to this release, it was in Advanced license package.

Printed in USA   C78-437306-14   05/13