Cisco NX-OS Software Release 4.0

PB439504

Cisco® NX-OS Release 4.0, the first release of the Cisco NX-OS Software, provides a rich and comprehensive feature set to address the high demands of mission-critical data centers. Table 1 lists the hardware supported by Cisco NX-OS, and Table 2 lists the features of the software.

Table 1. Hardware Supported

Description	Part Number
Cisco Nexus 7000 Series 10 Slot Chassis	N7K-C7010
Cisco Nexus 7000 Series Supervisor Module	N7K-SUP1
Cisco Nexus 7000 Series 6kW AC Power Supply	N7K-AC-6.0KW
Cisco Nexus 7000 Series 32 Port 10Gb Ethernet Module	N7K-M132XP-12
Cisco Nexus 7000 Series 48 Port 10/100/1000 Ethernet Module	N7K-M148GT-11
Cisco Nexus 7000 10 Slot Fabric Module	N7K-C7010-FAB-1

Table 2. Software Features

Software Feature	Description
Virtual device contexts (VDCs)	VDCs emulate a virtual device. Each VDC has its own software processes, dedicated hardware resources (interfaces), and independent management environment.
Cisco In Service Software Upgrade (ISSU)	Cisco ISSU provides the capability to perform transparent software upgrades on platforms with redundant supervisors.
Process survivability	Individual processes can be restarted independently without loss of state information and without affecting data forwarding. Highly stateful processes such as IP routing protocols are restarted using standards-based non-stop forwarding (NSF) graceful restart mechanisms, and other processes use a local persistent storage service (PSS) to maintain their state.
Support for distributed and parallel processing	Cisco NX-OS is designed to support distributed multithreaded processing on symmetric multiprocessors (SMPs), multicore CPUs, and distributed line card processors.
Stateful supervisor failover	Redundant supervisors are kept synchronized at all times to enable rapid stateful supervisor failover.
Modular software fix capability	Fixes addressing caveats in the software are developed modularly and can be quickly incorporated into the software image.
Network-based availability	• Spanning Tree Protocol enhancements, to guarantee 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 protocols • Shortest-path first (SPF) optimizations (link-state advertisement [LSA] pacing and incremental SPF) • IEEE 802.3ad link aggregation with adjustable timers
Switched Port Analyzer (SPAN)	SPAN nonintrusively directs copies of the traffic on selected ports to a destination port that may have an external analyzer attached to it.
Embedded packet analyzer	The built-in packet analyzer helps monitor and troubleshoot control plane traffic.
Cisco Generic Online Diagnostics (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, and on-demand and scheduled tests are part of the Cisco GOLD feature set.
Cisco Embedded Event Manager (EEM)	Based on a set of configurable network events, Cisco EEM can initiate user-defined actions; for example, it can generate syslog notifications or even send commands from the command-line interface (CLI) to modify traffic routing.

Cisco Netflow	Cisco NX-OS implementation of Netflow supports version 5 and version 9 exports as well as the Flexible Netflow configuration model and hardware-based Sampled Netflow for enhanced scalability.
Smart Call Home	Smart Call Home continuously monitors hardware and software components to provide e-mail-based notification of critical system events.
Simple Network Management Protocol (SNMP)	Cisco NX-OS complies with SNMP Versions 1, 2, and 3. A rich collection of MIBs is supported.
Programmatic Extensible Markup Language (XML) interface	The XML interface provides a consistent API for the device.
Configuration verification and rollback	The consistency of a configuration can be verified, along with the availability of necessary hardware resources, prior to committing the configuration. Configurations are also checkpointed to allow operators to roll back to a known good configuration as needed.
Role-based access control (RBAC)	Different levels of management privileges can be customized for different users.
Connectivity management processor (CMP) support	Cisco NX-OS supports the use of a CMP for remote “lights-out” management of the platform. The CMP aids operations by providing an out-of-band access channel to the Cisco NX-OS console.
Ethernet switching	• Rapid Per VLAN Spanning Tree Plus (PVST+) (IEEE 802.1D-2004 and 802.1w) • Multi-Instance Spanning Tree Protocol (MISTP) (IEEE 802.1Q and 802.1s) • IEEE 802.1Q VLANs and trunks • 16,384 VLANs • IEEE 802.3ad link aggregation • Private VLANs and cross-chassis private-VLANs • Unidirectional Link Detection (UDLD) Protocol in Aggressive and Standard modes • Traffic suppression (unicast, multicast, and broadcast), SST • Spanning Tree Protocol enhancements: bridge protocol data unit (BPDU) guard, loop guard, root guard, BPDU filters, and bridge assurance • Jumbo frame support
Seamless Spanning Tree (SST) Protocol	This extension to the Spanning Tree Protocol allows user traffic to remain uninterrupted during ISSU+ operations when connecting to SST-aware switches.
Bridge assurance for Spanning Tree Protocol	This protocol enhances the Spanning Tree Protocol to prevent bridging loops caused by continuous data forwarding in the absence of an operational Spanning Tree Protocol control plane. Control plane failures can be caused by a software glitch or undetected unidirectional links.
IP routing	The following protocols are supported with the graceful restart function: • Open Shortest Path First (OSPF) Protocol Versions 2, and 3 (IPv6) • Intermediate System-to-Intermediate System (IS-IS) Protocol • Border Gateway Protocol (BGP) • Enhanced Interior Gateway Protocol (EIGRP) • Routing Information Protocol (RIP) Version 2
IP services	The following IP services are supported in Cisco NX-OS Release 4.0: • Virtual Routing and Forwarding (VRF) • Dynamic Host Configuration Protocol (DHCP) relay • Unicast Reverse Path Forwarding (uRPF) • Hot-Standby Routing Protocol (HSRP) • Virtual Router Redundancy Protocol (VRRP) • Gateway Load Balancing Protocol (GLBP) • Enhanced object tracking (EOT) • Policy-based routing (PBR) • Generic routing encapsulation (GRE) tunneling

IP Multicast	• Protocol Independent Multicast Version 2 (PIMv2) • Source Specific Multicast (SSM) • PIM Sparse mode (Any Source Multicast [ASM]) (IPv4 and IPv6) • Bidirectional Protocol Independent Multicast (Bidir PIM) • Anycast Rendezvous Points (RP) • Multicast NSF for IPv4 and IPv6 • Rendezvous point discovery using Bootstrap Router (BSR), Auto-RP, and Static mode • Internet Group Management Protocol (IGMP) Version 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)
Quality of service (QoS)	The following QoS functions are supported in the Cisco Modular QoS CLI (MQC) framework: • Ingress and egress queuing and scheduling • Traffic classification based on QoS class (class of service [CoS], IP precedence, or differentiated services code point [DSCP]) and protocol fields • Traffic marking or remarking • QoS class (CoS, IP precedence, or DSCP) mutation • Ingress and egress aggregate and color-aware policing
Cisco TrustSec	The Cisco TrustSec security suite provides these features: • Data confidentiality and integrity with IEEE 802.1AE 128-bit Advanced Encryption Standard (AES) link-layer cryptography • Network device and host authentication using IEEE 802.1x • Scalable network access control with security group access control lists (SGACLs)
Network security	Beyond Cisco TrustSec, Cisco NX-OS Release 4.0 delivers the following security features: • Intrusion detection system (IDS) for protocol conformance checks. • Control plane policing (CoPP) • MD5 routing protocol authentication • Cisco Integrated Security Features (CISF) including: ◦ Dynamic Address Resolution Protocol (ARP) inspection (DAI) ◦ DHCP snooping ◦ 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 Access Control (NAC) and LAN-port-IP • Named ACLs: Port ACLs (PACLs), VLAN ACLs (VACLs), and router ACLs (RACLs) support policies based on MAC and IPv4 addresses

Supported Standards

Table 3. 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
802.3ab	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

Table 4. RFC Compliance

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
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
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 routng 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 (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
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 Rendevous 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
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

Ordering Information

Cisco NX-OS is available in three license levels. A rich feature set is provided with the Base license, which is bundled with the hardware at no extra cost. The Enterprise license enables incremental functions that are applicable to many enterprise deployments. The Advanced Services license enables next-generation functions such as VDCs and Cisco TrustSec. Table 3 summarizes the three packages.

Table 5. License Packages

Package	Contents
Base package	Provides a rich feature set appropriate for most data center requirements

Enterprise package	Provides incremental functions available only with the Enterprise license:
	• IP routing
	  ◦ OSPF v2, and v3 (IPv4 and IPv6)
	  ◦ IS-IS (IPv4)
	  ◦ BGP (IPv4)
	  ◦ EIGRP (IPv4)
	• IP Multicast
	  ◦ PIM: Sparse, Bidir, and SSM modes
	  ◦ MSDP
	• PBR
	• GRE tunnels

Advanced package	The Advanced Services license enables use of the following functions in Cisco NX-OS Release 4.0: • VDCs • Cisco TrustSec

To place an order, visit the Cisco Ordering homepage. To download software, visit the Cisco Software Center. Table 4 provides ordering information.

Table 6. Ordering Information

Product Name	Part Number
Cisco NX-OS Enterprise LAN License	N7K-LAN1K9
Cisco NX-OS Advanced LAN License	N7K-ADV1K9
Cisco NX-OS 4.0 Software for the Cisco Nexus 7000 Supervisor 1	N7KS1K9-401A1.1

Cisco Service and Support

Cisco offers a wide range of services to help accelerate your success deploying and optimizing Cisco Nexus 7000 Series Switches in your data center. Our innovative services are delivered through a unique combination of people, processes, tools, and partners, and are focused on helping you increase operational efficiency and improve your data center network. Cisco Advanced Services use an architecture-led approach to help you align your data center infrastructure to your business goals and provide long-term value. Cisco SMARTnet® Service helps you resolve mission critical problems with direct access anytime to Cisco network experts and award-winning resources. With this service, you can take advantage of the Smart Call Home service capability that offers proactive diagnostics, and real-time alerts on your Cisco Nexus 7000 switches. Spanning the entire network lifecycle, Cisco Services help maximize investment protection, optimize network operations, provide migration support, 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 the Cisco NX-OS, visit the product homepage at: http://www.cisco.com/go/nxos or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

C25-439504-00 01/08