Cisco NX-OS Software Release 7.3(0)D1(1) for Cisco Nexus 7000 Series and Nexus 7700 Series Switches

PB736957

This product bulletin introduces Cisco® NX-OS Software Release 7.3(0)D1(1) for Cisco Nexus® 7000 Series and Cisco Nexus 7700 Series Switches(Figure 1). This document summarizes the new features that this new release supports.

Figure 1. Cisco Nexus 7000 Series and Nexus 7700 Series Switches

New Features

Cisco NX-OS 7.3(0)D1(1) for Cisco Nexus 7000 Series and 7700 Series switches provides a robust and comprehensive feature set to address the high demands of mission-critical data centers.

NX-OS 7.3(0)D1(1) supports all hardware and software supported in prior NX-OS releases except the hardware listed in the "Hardware Support" section of this document. In addition, NX-OS 7.3(0)D1(1) delivers new programmability and automation features for the Cisco Nexus 7000 Series and Nexus 7700 Series switches. In particular, Cisco Programmable Fabric now includes some significant enhancements such as spine-and-leaf Virtual Extensible LAN (VXLAN) Ethernet VPN (EVPN) with Multiprotocol Label Switching (MPLS) Layer 3 VPN (L3VPN) hand-off. It also includes Chef and Puppet agent support for automation, Cisco TrustSec® security enhancements, and new storage capabilities. The following list summarizes the main new software features in this release:

- Programmable Fabric enhancements:
  - VXLAN EVPN control-plane support with the Cisco Nexus 7000 Series Switch acting as a leaf switch (Distributed IP Anycast Gateway), border-leaf switch, and spine switch with support for Bidirectional Protocol-Independent Multicast (PIM-BIDIR) and PIM Anysource Multicast (PIM-ASM) in the underlay
  - VXLAN data center interconnect (DCI) hand-off, which includes classical Ethernet Layer 2 hand-off and hand-off to MPLS L3VPN and LISP enabled networks
  - Auto-configuration for VXLAN EVPN networks, including Virtual Machine Tracker auto-configuration
  - VXLAN operations, administration, and management (OAM) support
- Programmability enhancements:
  - Support for Chef and Puppet agents
  - Support for OpenFlow on F3-Series modules
- Dynamic Route Leaking Using Route Targets Between Default VRF and Created VRF
- Ethernet link OAM
- Flexible ternary content-addressable memory (TCAM) chaining for F3-Series
- Virtual port channel (vPC) hitless role change
- Cisco Intelligent Traffic Director (ITD) enhancements:
  - Access control list (ACL)–based load balancing
  - Optimized Node Insertion and Removal
- Graceful insertion and removal (GIR) enhancements:
  - Protocol isolate
- Cisco TrustSec enhancements –
  - Subnet to security group tag (SGT) Mapping
  - SGT Exchange Protocol Version 3 (SXPv3)
  - Security group ACL (SGACL) monitor mode
  - SGACL ACLLOG
- IEEE 802.1BA: Audio Video Bridging (AVB) Systems, which includes support for the following specifications:
  - IEEE 802.1AS-gPTP: Generalized Precision Time Protocol (gPTP)
  - IEEE 802.1Qat: Multiple Stream Reservation Protocol (MSRP)
  - IEEE 802.1Qav: Forwarding and Queuing for Time-Sensitive Streams (FQTSS)
- Fibre Channel over Ethernet (FCoE) enhancements:
  - FCoE over fabric extender (FEX) on F3
  - iSCSI TLV
- Layer 3 enhancements
  - Bidirectional Forwarding Detection (BFD) on link aggregation group (LAG) member link
  - MPLS traffic engineering (TE) enhancements
  - IPv6 enhancements

Hardware Support

The following hardware is not supported in NX-OS 7.3(0)D1(1):

- Cisco Nexus 7000 - 48 Port 10/100/1000, RJ-45 (N7K-M148GT-11)
- Cisco Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+) (N7K-M132XP-12)
- Cisco Nexus 7000 - 48 Port 1G, SFP (N7K-M148GS-11)
- Cisco Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module(N7K-C7010-FAB-1)
- Cisco Nexus 7000 - 18 Slot Chassis - 46Gbps/Slot Fabric Module(N7K-C7018-FAB-1)
- Cisco Nexus 7000 - 32 Port 1G/10G Ethernet Module, SFP/SFP+ (N7K-F132XP-15)
- Cisco Nexus 7000 Series Supervisor 1 Module

NX-OS 7.3(0)D1(1) supports all other hardware supported in prior NX-OS software releases.

Software Support

NX-OS 7.3(0)D1(1) supports all the software features previously supported on the Cisco Nexus 7000 Series and & Nexus 7700 Series Switches up through NX-OS 7.2(0)D1(1).

NX-OS 7.3(0)D1(1) is compatible with Cisco In-Service Software Upgrade (ISSU) with NX-OS Releases 7.2(0)D1(1) and 7.2(1)D1(1). In addition, NX-OS 7.3(0)D1(1) supports the new software features described in Table 1.

For more detailed information about supported features and ISSU, refer to the NX-OS 7.3(0)D1(1) release notes (see "For More Information" at the end of this document).

Table 1. New Features in Cisco NX-OS Release 7.3(0)D1(1)

Category	New Feature	Description
Programmable Fabric	VXLAN (L2/L3 gateway and Border Gateway Protocol [BGP] EVPN)	VXLAN with the Multiprotocol BGP (MP-BGP) EVPN control plane is supported with the Cisco Nexus 7000 Series Switch acting as a leaf switch (L2/L3 gateway with Distributed Anycast Gateway and vPC), border-leaf switch (L2/L3 Gateway, LISP, MPLS, VRF-lite, and Classic Ethernet Layer 2 with and without vPC), and spine switch with and without a route reflector. For VXLAN multi-destination traffic, PIM-ASM and Bidirectional-PIM are required.
	VXLAN DCI hand-off	The VXLAN DCI hand-off on the border-leaf and spine switches includes classical Ethernet Layer 2 hand-off and hand-off to networks that support MPLS L3VPN and LISP, enabling consolidation of border- leaf and provider-edge switches in a single device, reducing capital expenditures (CapEx).
	VXLAN EVPN auto-configuration	Virtual Machine Tracker auto-configuration automatically configures a tenant for provisioning. The Virtual Machine Tracker auto-configuration retrieves information about a tenant from the database (Lightweight Directory Access Protocol [LDAP]) and sends the necessary configuration commands for the provisioning process.
	VXLAN OAM	Ethernet OAM is a protocol for installing, monitoring, and troubleshooting Ethernet networks to enhance management in VXLAN-based overlay networks.
Programmability	Support for Chef and Puppet agents	Open agents such as Chef and Puppet provide automated network configuration and management capabilities. These agents cannot be directly installed on the Cisco Nexus switches. Instead, they run in a special environment: a decoupled execution space within a Linux Container (LXC) called the Open Agent Container (OAC).
	OpenFlow on F3-Series	Cisco Plug-in for OpenFlow provides better control over networks, making them more open, programmable, and application aware.
	Network Configuration Protocol (NETCONF) RFC 47471 compliance	NETCONF (RFC 4741) is an IETF network management protocol that provides mechanisms for installing, manipulating, and deleting network device configurations.

Category	New Feature	Description
Application Experience and IT Simplicity	GIR: protocol isolate	The default mode for GIR is now isolate. By using the **isolate** command to isolate the protocols, the switch can be isolated from the network but not shut down. This approach retains neighborship and prevents loss of data traffic.
	Link OAM (IEEE802.3ah)	Link OAM allows service providers to monitor and troubleshoot a single physical point-to-point Ethernet link. Service providers can monitor specific events, take actions on events, and troubleshoot. This feature thus enables proactive fault detection and link fault management and isolation.
	Intelligent Traffic Director enhancements: • ACL-based load balancing • Optimized Node Insertion/Removal	ACL-based load balancing is used to simultaneously filter and load-balance the traffic with a user-defined ACL.
		With optimized node insertion and removal, users can dynamically add or remove nodes with little disruption to the existing traffic, regardless of whether the Intelligent Traffic Director service is shut down or active.
	Flexible TCAM chaining for F3-Series	Chaining two banks within a TCAM enables two lookups, with two results per packet per direction, which helps the user manage larger ACLs spread across multiple TCAM banks and allows the configuration of up to two ACL features per destination.
	Hitless vPC role change enhancements for Spanning Tree Protocol and vPC	The vPC hitless role change provides a framework for switching the vPC roles between vPC peers without affecting traffic flows.
	Enhanced monitoring capabilities: • Cisco NetFlow on control-plane policing (CoPP) interface • 4000 VLANs per Cisco Switched Port Analyzer (SPAN) or Encapsulated Remote SPAN (ERSPAN) session	The NetFlow on CoPP interface feature uses traffic flows to provide statistics for network traffic accounting, network monitoring, and network planning on the CoPP interface.
		Support for 4000 VLANs per SPAN or ERSPAN session enables the monitoring session to monitor all ports and VLANs in the Ethernet virtual device context (VDC).
	Cisco IOS® Software parity features: • 63-character host name • Exec Banner • 32-character Network Time Protocol (NTP) authentication key	The character limit for a switch name and a host name is increased from 32 to 63 alphanumeric characters.
		The Exec banner is displayed after a user logs in to a switch. This banner can be used to post reminders to your network administrators.
		Beginning with NX-OS 7.3(0)D1(1), you can use up to 32 alphanumeric characters for the MD5 string.
Security	Cisco TrustSec features: • Subnet-to-SGT mapping • SXPv3 • SGACL Monitor Mode • SGACL Permit and deny ACLLOG indication	Subnet to security group tag (SGT) mapping binds an SGT to all the host addresses of a specified subnet. After this mapping is implemented, the Cisco TrustSec solution imposes the SGT on any incoming packet that has a source IP address that belongs to the specified subnet. This approach enables the user to enforce Cisco TrustSec policy on traffic flowing through data center hosts.
		SXPv3 supports the transport of the IPv4 Subnet to SGT bindings.
		The monitor mode provides a convenient way to roll back before enforcing the security policy if the security policy contains errors. It gives administrators increased visibility into the outcome of policy actions before policies are enforced and confirms that the subject policy meets the security need. It denies access to resources if individuals are not authorized. It also reduces the time needed to deploy a Cisco TrustSec system.
		The SGACL ACLLOG enables the user to observe the effects of the SGACL policies after the enforcement at the egress point. The user can check the following: • Whether the flow was permitted or denied • Whether the flow is monitored or enforced by the SGACL
	Login Block Per User	The Login Block Per User feature helps detect suspected Denial of Service (DoS) attacks and slow down dictionary attacks. You can configure login parameters to block logins per user (applicable only for local users).
Media Solutions	Audio Video Bridging – IEEE 802.1	AVB enables standards-based support of high-quality media over an Ethernet network.
Fabric Extender	Isolated private VLAN (PVLAN) support on fabric extender host interface (HIF)	Users can configure PVLAN isolated host and secondary trunk ports on fabric extender ports. The parent switch must be a Cisco Nexus 7000 Series Switch.

Category	New Feature	Description
Storage	FCoE over FEX on F3-Series	FCoE over FEX allows Fibre Channel traffic to be carried on a fabric extender port. This feature is now supported on F3-Series modules. The following FCoE features are supported for NX-OS 7.3(0)D(1)1: • FCoE over FEX with F3-Series (N2K-C2348UPQ-10GE, B22HP, N2K-C2232PP-10GE) • F3-Series FCoE support with physical port vPC and vPC+ • F3-Series FCoE support for fabric extenders with physical port vPC and vPC+
	iSCSI TLV	iSCSI TLV lowers the solution cost of deployment of iSCSI over loss-less Ethernet over FCoE. No hardware or gateways are needed to convert iSCSI to Fibre Channel traffic. Now iSCSI targets are present that can perform end-to-end iSCSI processing with initiators.
Layer 3 Leadership	RFC 7130 BFD LAG member link	Per-link BFD enables users to configure individual BFD sessions on every Link Aggregation Group (LAG) member interface.
	MPLS traffic engineering (TE) enhancements: • MPLS traffic engineering constrained shortest path first (TE CSPF) cost limit • CSPF enhancements • Logging of label switched path (LSP) and fast reroute (FRR) events	The CSPF cost- limit feature allows you to specify a maximum permitted total cost for a tunnel's path and invalidate it if the cost exceeds this value. The configured cost limit applies to the type of metric used to calculate the tunnel's path, which can be the Interior Gateway protocol (IGP) or traffic engineering link metric. By default, a cost limit is not imposed.
		The following CSPF enhancements are available: Hop limit, Dynamic available bit rate (ABR) determination, Interface address as destination, Strict and loose intra-area paths, Link-load balancing.
		Logging LSP and FRR events enables you to generate system logs for the events related to tunnels, LSPs, and FRR.
	IPv6 enhancements • BGP Prefix-Independent Convergence (PIC) Edge for IPv6 • BFD support for Hot Standby Router Protocol (HSRP) for IPv6 • Open Shortest Path First Version 3 (OSPFv3) IP Security (IPSec) authentication • Lightweight Dynamic Host Configuration Protocol Version 6 (DHCPv6) Relay (LDRA)	BGP PIC for Edge improves BGP convergence after a network failure. This convergence is applicable to edge failures in an IP network. With this release, BGP PIC Edge support is now extended to the IPv6 address family.
		BFD can now support all IPv4 and IPv6 HSRP groups.
		OSPFv3 IPSec authentication enhances NX-OS OSPFv3 to add authentication and encryption to its packets. It uses the IPSec authentication header with MD5 or SHA1 authentication
		LDRA forwards DHCPv6 messages between clients and servers when they are not on the same IPv6 link, allowing relay agent information to be inserted by an access node that performs a link-layer bridging (non-routing) function.

Service and Support

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. Our innovative services are delivered through a unique combination of people, processes, tools, and partners and focus on helping you increase operation efficiency and improve your data center network. Cisco Advanced Services use an architecture-led approach to help you align your data center infrastructure with your business goals and provide 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 diagnostic information and real-time alerts for your Cisco Nexus 7000 Series and 7700 Series Switches. Spanning the entire network lifecycle, Cisco Services offerings help increase 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.

Cisco Capital Financing to Help You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive.

We can help you reduce CapEx, accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital financing is available in more than 100 countries. Learn more.

For More Information

For more information about the Cisco Nexus 7000 Series and & Nexus 7700 Series Switches, visit the product homepage at http://www.cisco.com/go/nexus or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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 C25-736957-00 03/16