Release Notes for Cisco 8000 Series Routers, IOS XR Release 7.3.1

Revised: July 31, 2024

Cisco 8200 and 8800 Series Routers

Note This software release has reached end-of-life status. For more information see the End-of-Life and End-of-Sale Notices.

What's New in Cisco IOS XR Release

Cisco is continuously enhancing the product with every release and this section covers a brief description of key features and enhancements. It also includes links to detailed documentation, where available.

Table 1: New Hardware

Feature	Description
New and Parity Optics	
Cisco QDD-400-AOC cables	This release introduces a new active optic cable (AOC) that can operate over multimode fiber. These cables are suitable for short distances and offer a flexible way to connect within racks and across racks. This cable supports length of 3, 5, 7, 10, 15, 20, 25 and 30 meters. meters. The AOC cable PIDs are - QDD-400-AOC3M, QDD-400-AOC5M, QDD-400-AOC7M, QDD-400-AOC10M, QDD-400-AOC15M, QDD-400-AOC20M, QDD-400-AOC25M, and QDD-400-AOC30M. For more information, see Cisco Optics-to-Device Compatibility Matrix
Cisco QSFP-40G-LR4-S (S-Class)	The Cisco 40GBASE-LR4 QSFP module supports link lengths of up to 10 kilometer over a standard pair of G.652 single-mode fiber with duplex LC connectors. The QSFP-40G-LR4-S module supports 40GBASE Ethernet rate only. Cisco QSFP-40G-LR4 optic is a new optic supported on Cisco 8000 series routers. The PID is: • QSFP-40G-LR4-S
QSFP-40G-SR4	Cisco QSFP-40G-SR4 optic is a new optic supported on Cisco 8000 series routers. This optic is supported in Native and 4x10G breakout modes.The PID is: • QSFP-40G-SR4

Feature	Description
Cisco QSFP-100G-AOC cables	This release introduces a new active optic cable (AOC) that can operate over multimode fiber. These cables are suitable for short distances and offer a flexible way to connect within racks and across racks. This cable supports length of 1, 2, 3, 5, 7, 10, 15, 20, 25 and 30 meters. The AOC cable PIDs are - QSFP-100G-AOC1M, QSFP-100G-AOC2M, QSFP-100G-AOC3M, QSFP-100G-AOC5M, QSFP-100G-AOC7M, QSFP-100G-AOC10M, QSFP-100G-AOC15M, QSFP-100G-AOC20M, QSFP-100G-AOC25M, and QSFP-100G-AOC30M.
QDD-2x100G-LR4-S	Cisco QDD-2x100G-LR4-S is a new optic supported on Cisco 8000 series routers.
Cisco QSFP-H40G-AOC cables	This release introduces a new active optic cable (AOC) that can operate over multimode fiber. These cables are suitable for short distances and offer a flexible way to connect within racks and across racks. This cable supports length of 1, 2, 3, 5, 7, 10, 15, 20, 25 and 30 meters. The AOC cable PIDs are - QSFP-H40G-AOC1M, QSFP-H40G-AOC2M, QSFP-H40G-AOC3M, QSFP-H40G-AOC5M, QSFP-H40G-AOC7M, QSFP-H40G-AOC10M, QSFP-H40G-AOC15M, QSFP-H40G-AOC20M, QSFP-H40G-AOC25M, QSFP-H40G-AOC25M, and QSFP-H40G-AOC30M.
Cisco QSFP-4X10G-LR	The Cisco QSFP-4X10G-LR-S QSFP module supports link lengths of up to 10km on G.652 Single-Mode Fiber (SMF). It enables high-bandwidth 40G optical links over 12-fiber parallel fiber terminated with MPO/MTP multifiber female connectors. It can also be used in a 4x10G mode for interoperability with 10GBASE-LR interfaces up to 10km. Cisco QSFP-4X10G-LR is an existing optic. The optic is now supported on Cisco 8000 series routers. The PID is: • QSFP-4X10G-LR-S

Table 2: New Software

Feature	Description
System Setup	
Enhanced Login Banner	To comply with US DoD, an option to enable display of login banner is introduced. The login banner provides information such as number of successful and unsuccessful login attempts, time stamp, login method, and so on. The login-history command is introduced.

Feature	Description
Secure Zero Touch Provisioning	This feature allows devices in the network to establish a secure connection with the ZTP server and authenticate information using a three-step validation process involving validation of the network device, the ZTP server, and onboarding information. This eliminates security risks or malicious actions during remote provisioning. The **ztp secure-mode enable** command is introduced.
Software Installation	
Install Cisco RPM Directly from TAR File	Cisco RPMs can be installed from one of these sources - repository name, repository URL or a local file path. Previously, to install RPMs from a TAR file, you had to manually extract the TAR file and specify the path to the locally extracted file to install the RPM. This feature extends support to install the RPM directly from the TAR file. Bug fix RPMs are available as TAR files on the Software Download page. The RPMs can be installed from the TAR file using CLI or Yang data model.
Support ZTP Initialization File in Golden ISO (GISO)	With this feature, an initialization file (ztp.ini) for ZTP is provided when building a golden ISO (GISO). This file defines the ZTP configuration. During a reload operation or when ZTP is initiated manually, ZTP runs with the custom .ini file that was previously used in the configuration.
BGP	
128-way ECMP	This feature enables the router to support up to 128 parallel multipaths to a destination. In this release, in additon to the existing support for 128 parellel multipaths, one backup multipath is supported.
Advertising IPv4 NLRI with IPv6 Next Hops in MP-BGP Networks	This feature allows the MP-BGP peers to dynamically exchange IPv4 NLRI and VPN-IPv4 NLRI with an IPv6 next hop. This feature introduces **ipv4 forwarding-enable** command.
BGP Labeled Unicast MPLS IP POP Support	This feature is based on the BGP Labeled Unicast feature. This feature enables a router to send IPv4 unicast traffic to the destination from BGP label unicast using implicit NULL.
BGP Slow Peer Automatic Isolation from Update Group	A slow peer cannot keep up with the rate at which the router generates BGP update messages over a period of time, in an update group. This feature automatically detects a slow peer in an update group and moves it to a new update group. The feature is enabled on the router, by default. New commands introduced in this release: • **slow-peer detection enable** • **clear bgp slow-peers** Updated commands in this release: • **slow-peer detection disable**
BGP-eBGP Security GSTM	The Generalized TTL Security Mechanism (GTSM) is designed to protect a router's IP-based control plane from CPU-utilization based attacks. This feature enables the router to accept only IP packets with a TTL count that is equal to the maximum TTL value. New command introduced: • **ttl-security**

Feature	Description
Support for Increased Number of BGP Peers	This feature is now enhanced to support 750 IPv4 and 750 IPv6 BGP peers.
Segment Routing	
BFD-triggered TI-LFA	Topology-Independent Loop-Free Alternate (TI-LFA) uses segment routing to provide link, node, and Shared Risk Link Groups (SRLG) protection in topologies where other fast reroute techniques cannot provide protection. BFD-triggered TI-LFA allows you to obtain link, node, and SRLG protection by using the Bidirectional Forwarding Detection (BFD) protocol.
Link Delay Measurement using TWAMP Light Encoding	The PM for link delay uses the IP/UDP packet format defined in RFC 5357 (TWAMP-Light) for probes. Two-Way Active Measurement Protocol (TWAMP) adds two-way or round-trip measurement capabilities. TWAMP employs time stamps applied at the echo destination (reflector) to enable greater accuracy.
SR OAM for SR Policy (Policy Name / Binding SID / Custom label stack)	This feature extends SR OAM ping and traceroute function for an SR policy (or binding SID)-LSP end-point combination. This addresses the limitations of the Nil-FEC LSP Ping and Traceroute function which cannot perform a ping operation to a segment list that is not associated with an installed SR policy. Also, it cannot validate egress device-specific SR policies.
Segment Routing Data Plane Monitoring	Traffic black holes in MPLS networks could be difficult to detect and isolate. They can be caused by user configuration, out-of-sync neighbors, or incorrect data-plane programming. Segment Routing Data Plane Monitoring (SR DPM) provides a scalable solution to address data-plane consistency verification and traffic black hole detection. SR DPM validates the actual data plane status of all FIB entries associated with SR IGP prefix SIDs.
Segment Routing Flexible Algorithm	The Segment Routing architecture associates prefix-SIDs to an algorithm that defines how the path is computed. This feature allows for user-defined algorithms where the IGP computes paths based on a combination of metric type and constraint. An operator can assign custom SR prefix-SIDs to realize forwarding beyond link-cost-based SPF. As a result, this feature provides a traffic-engineered path computed automatically by the IGP to any destination reachable by the IGP. This release supports the following functionality: • TI-LFA (IS-IS/OSPF) • Microloop Avoidance (IS-IS) • Inter-AS Support (IS-IS) • SID Redistribution (IS-IS) • Metric minimization—avoidance, multi-plane, delay (IS-IS/OSPF) • Affinity include (IS-IS/OSPF) • Affinity exclude (IS-IS/OSPF)
Routing	

Feature	Description
Support for a Configurable Knob to Reject ISIS PDU on Layer 2 Interfaces	This feature enables you to use Layer 2 ACL to drop ISIS packets from certain ISIS destination MAC addresses. Dropping ISIS packets allows you to isolate a particular node from ISIS domain. This feature enables you to utilize the network bandwidth efficiently. This feature introduces the **ethernet-services access-list isis-drop-all-l2-pdus** command
System Security	
Collect Filesystem Inventory	With this feature, a snapshot of the filesystem metadata such as when the file was created, modified, or accessed is collected at each configured interval. In addition to displaying the changes that the file underwent as compared to the previous snapshot, the inventory helps in maintaining data integrity of all the files in the system.
Ed25519 Public-Key Signature Algorithm Support for SSH	This algorithm is now supported on Cisco IOS XR 64-bit platforms when establishing SSH sessions. It is a modern and secure public-key signature algorithm that provides several benefits, particularly resistance against several side-channel attacks. Prior to this release, DSA, ECDSA, and RSA public-key algorithms were supported. This command is modified for this feature: ssh server algorithms host-key
IMA Optimization	Integrity Measurement Architecture (IMA) is a Linux-based utility that attests and appraises the integrity of a system security, at runtime. In this release, IMA introduces the following IMA optimization aspects: • Incremental IMA that collects IMA events selectively and progressively instead of collecting all the IMA events at the same time. You can define the start of an IMA sequence, which consists of start event, start sequence number, and start time. • SUDI Signature - provides the hardware root of trust to the dossier that is collected by the system.
Password Masking	With this feature, when you key in a password or secret, it is not displayed on the screen. This enhances security. The feature is enabled by default. The following options are added to the **username** command: • **masked-password** • **masked-secret**
Retrieve CRL through the HTTP Proxy Server	CRL contains the serial numbers of the third-party certificates that are invalidated by the issuing Certificate Authority. In the event that the CRL Distribution point (CDP) is not directly reachable, you can fetch the CRL through the http proxy server using the newly introduced crypto ca http-proxy command. Command modified for this feature: crypto ca crl request
SSD Encryption	This feature enables trust and security in the system's steady state by encrypting data at the disk level. The encrypted data can be accessed *only* with a specific key stored in the TAm.

Feature	Description
Support for Ed25519 Public-Key Signature System	This feature allows you to generate and securely store crypto key pair for the Ed25519 public-key signature algorithm on Cisco IOS XR 64-bit platforms. This signature system provides fast signing, fast key generation, fool proof session keys, collision resilience, and small signatures. The feature also facilitates integration of Cisco IOS XR with Cisco Crosswork Trust Insights. Commands introduced for this feature are: • crypto key generate ed25519 • crypto key zeroize ed25519 • show crypto key mypubkey ed25519 Commands modified for this feature are: • ca-keypair • keypair
User Configurable Maximum Authentication Attempts for SSH	This feature allows you to set a limit on the number of user authentication attempts allowed for SSH connection, using the three authentication methods that are supported by Cisco IOS XR. The limit that you set is an overall limit that covers all the authentication methods together. If the user fails to enter the correct login credentials within the configured number of attempts, the connection is denied and the session is terminated. This command is introduced for this feature: ssh server max-auth-limit
Verify Authenticity of RPM Packages Using Fingerprint	This feature helps in verifying the authenticity of an installable package. A Known Good Value (KGV) is calculated and published for each package. The installed and running software is compared with the KGV to determine whether the package is genuine or not. These two values are displayed only in the Yang model output. No CLI commands are provided to view these values.
X.509v3 Certificate-based Authentication for SSH	This feature adds new public-key algorithms that use X.509v3 digital certificates for SSH authentication. These certificates use a chain of signatures by a trusted certification authority to bind a public key to the digital identity of the user who is authenticating with the SSH server. These certificates are tough to falsify and are therefore used for identity management and access control across many applications and networks. Commands introduced for this feature are: ssh server certificate ssh server trustpoint This command is modified for this feature: ssh server algorithms host-key
System Monitoring	

Feature	Description
Graceful Handling of Out of Resource (OOR) Situations	This feature enables you to resend any traffic that was dropped during an OOR situation. This enables better monitoring and management of failed traffic. Commands introduced and modified are: • oor hw • show controllers npu resources • show logging
Licensing	
Software Innovation Access (SIA) Entitlement	SIA license grants you access to the latest software upgrades which contain new features, bug fixes, and security enhancements for devices on your network. Also, it enables the consumption of Advanced and Essential Right-to-Use (RTU) licenses on your device, and allows portability of these RTU licenses from one device to another.
Specific License Reservation	Specific License Reservation (SLR) allows customers in highly secure networks to utilize smart licenses without communicating the license information to the Cisco Smart Software manager (CSSM).
System Management	
ITU-T G.8275.1 profile support	This feature supports the architecture defined in ITU-T G.8275 for systems requiring accurate phase and time synchronisation, phase or time-of-day synchronization is required, and where each network device participates in the PTP protocol. Support of this capability is extended on the Cisco 8000 Series router, in this release.
Support for Frequency Synchronization	Based on the ITU-T G.8262 recommendations, precision frequency is enabled on timing devices to deliver frequency synchronization for bandwidth, frequency accuracy, holdover, and noise generation. This support allows for correct network operations when synchronous equipment is timed from either another synchronous equipment clock or a higher-quality clock.
Support for ITU-T G.8263 standard for secondary clock with ITU-T G.8265.1 profile	ITU-T G.8263 is a performance compliance standard for secondary clocks configured with ITU-T G.8265.1 profiles. These clocks drive frequency synchronization based on the PTP packets received at the secondary devices, from traceable primary devices.
Support for ITU-T G.8264 Standard	The Ethernet Synchronization Message Channel (ESMC) protocol is specified in the ITU-T G.8264 performance compliance standard. It provides recommendations on synchronizing clock frequency across a network over an Ethernet port, along with the ability to select quality levels. The G.8264 standard provides a new extended Quality Level (QL) of Type Length Value (TLV). As Ethernet equipment gradually replace SONET and SDH equipment in service provider networks, frequency synchronization provides high-quality clock synchronization over Ethernet ports.
Support for Precision Time Protocol (PTP)	Precision Time Protocol (PTP) is based on the IEEE 1588-2008 clock synchronization standard and enables clocks in a distributed system to be synched with highly precise clocks. The precision in time synchronization is achieved through packets that are transmitted and received in a session between the primary clock and secondary clock. PTP also ensures that the best clock is selected as a timing source (the primary clock) and all other clocks are synchronized with the primary clock.
Telemetry	

Feature	Description
AI-driven telemetry (ADT)	This feature leverages machine learning to detect and retrieve important network-state changes on the router. Relevant data is filtered and exported to the network management system for analysis or troubleshooting purposes. ADT significantly simplifies the configuration of streaming telemetry, and you are no longer required to manually choose sensor paths or tune the cadence at which counters have to be collected.
Hardware Timestamp	This feature synchronises the timestamp for accurate calculation of data rate from the router, wherein the counters are read from the hardware. The counters are updated only when the collector reads the counters from hardware, irrespective of the number of times the MDT client polls data. With hardware timestamping in rate computation while streaming periodic statistics, the spikes due to the inconsistent timestamp from cache files is resolved.

Streaming Digital Optical Monitoring (DOM) data from the router	This feature streams fiber optic transceiver parameters such as optical input or output levels, temperature, laser bias current, supply voltage, receiver power, bias threshold, etc., in real-time. This helps network operators to easily locate a fiber link failure, thereby simplifying the maintenance process, and improving overall system reliability.
	Sensor paths introduced for this feature are:
	`Cisco-IOS-XR-dwdm-ui-oper:dwdm/ports/port/info/optics-info`
	`Cisco-IOS-XR-controller-optics-oper:optics-oper/optics-ports/optics-port/optics-info`

Programmability	
Unified NETCONF V1.0 and V1.1	Cisco IOS XR supports NETCONF 1.0 and 1.1 programmable management interfaces. With this release, a client can choose to establish a NETCONF 1.0 or 1.1 session using a separate interface for both these formats. This enhancement provides a secure channel to operate the network with both interface specifications.
Interfaces	
Ethernet Link OAM	This feature allow Service Providers to monitor the quality of the connections on a MAN or WAN. Service providers can monitor specific events, and take actions on events. Ethernet link OAM operates on a single, physical link and it can be configured to monitor either side or both sides of that link.
GRE Tunnel	Generic Routing Encapsulation (GRE) provides a simple approach to transporting packets of one protocol over another protocol using encapsulation. This capability is now extended to the Cisco 8000 Series Routers. This feature supports: • Unidirectional GRE encapsulation • Unidirectional GRE decapsulation And introduces the following commands: • **show interface tunnel accounting (encap)** • **show interface tunnel accounting (decap)**

Feature	Description
Generic UDP Encapsulation	This feature enables you to add an additional header to the packets to identify or authenticate the data using UDP. Encapsulating packets in UDP leverages the use of the UDP source port to provide entropy to Equal Cost Multi-Path (ECMP) hashing and provides significant performance benefits for load-balancing. This command is introduced for this feature: **decapsulate gue**
Outer-header hashing support for MPLSoGRE and IPoGRE traffic	This feature allows load-balancing of GRE traffic in transit routers. A transit node distributes incoming GRE traffic evenly across all available ECMP links in a GRE tunnel topology. A hashing function uses GRE outer and inner header tuples such as source IP, destination IP, protocol, and router ID to determine traffic entropy. This capability is now extended to the Cisco 8000 Series Routers.
SPAN to File - PCAPng File Format	PCAPng is the next generation of packet capture format that contains a dump of data packets captured over a network and stored in a standard format. The PCAPng file contains different types of information blocks, such as the section header, interface description, enhanced packet, simple packet, name resolution, and interface statistics. These blocks can be used to rebuild the captured packets into recognizable data. The PCAPng file format: • Provides the capability to enhance and extend the existing capabilities of data storage over time • Allows you to merge or append data to an existing file. • Enables to read data independently from network, hardware, and operating system of the machine that made the capture.
IP Addresses and Services	
ACLs on BVI	This feature allows traffic filtering by configuring ACLs on Bridge Virtual Interfaces (BVIs). A single configuration can be applied for multiple interfaces that are part of the BVI. You can therefore, filter traffic for a group of interfaces with a particular purpose.
Configuration Status of Cisco Express Forwarding (CEF) Hardware Modules	This feature enables you to view pending actions, such as a reload or commit, that is applicable to the CEF hardware-modules. The show hw-module profile cef command is introduced for this feature.
Hybrid ACLs	You can apply compression levels for object-group ACLs and attach up to 4000 ACEs per line card in the ingress direction. This leads to optimal TCAM space usage and resources utilization. The commands modified are: • ipv4 access-group • ipv6 access-group
MPLS	

Feature	Description
LDP Over RSVP LSR Support	With this feature, users can transport LDP traffic over an RSVP TE network automatically, through a targeted LDP session. The automatic configuration for LDP over RSVP TE supports 1000 TE tunnels.
MPLS Static Forwarding Over A BVI	The router can receive MPLS L2VPN traffic from an L2 bridge domain, and forward the L3 (customer) traffic over an egress BVI, using an MPLS static LSP. For the incoming L2VPN traffic, the BVI serves as an L3 gateway. Since the router can perform switching for L2 traffic and routing for incoming L3 MPLS traffic, it enhances flexibility for transporting MPLS traffic.
Multicast	
Multicast Route Statistics	When enabled, this feature provides statistics on the number of packets received for a multicast route. This information may be useful for monitoring and billing purposes.
Netflow	
sFlow support on L2 Interfaces	In this release, support for ingress sFlow on a L2 interface is introduced. Support for sFlow existed in earlier releases.
Modular QoS	
QoS Behavior for Generic Routing Encapsulation (GRE) Tunnels: Default Marking	With the support for GRE encapsulation and decapsulation tunnel interfaces, there are some important updates to QoS behavior for GRE tunnels. These updates are applicable for default packet marking and involve Type of Service (ToS) and MPLS experimental bits.
QoS Behavior for Generic Routing Encapsulation (GRE) Tunnels: Explicit Marking	With the support for GRE encapsulation and decapsulation tunnel interfaces, there are some important updates to QoS behavior for GRE tunnels. These updates are applicable for explicit packet marking and involve QoS behavior during ingress and egress.
Hardware Installation	
Grace Period Before Route Processor Shutdown after Ejector Lever is Unlatched	Unlatching the ejector lever of the Route Processor (RP) card that is in operational state, triggered a graceful shutdown of the RP. With this release, the RP card is enabled with a grace period of 15 seconds before it shuts down. In the event the ejector lever is unlatched, or for any other reason, you have 15 seconds to relatch the ejector lever and return the RP back to its operational state.
MIB Locator	
IOS XR MIB Locator	An interface to view, search, and download platform MIBs.
Compatibility Matrix	
Cisco IOS XR – Product Compatibility	An intuitive interface, connecting an IOS XR product series to various product models, architectures, and supported releases.

For a complete list of supported hardware and ordering information, see the Cisco 8000 Series Data Sheet.

Release 7.3.1 Packages

The Cisco IOS XR software is composed of a base image (ISO) that provides the XR infrastructure. The ISO image is made up of a set of packages (also called RPMs). These packages are of three types:

- A mandatory package that is included in the ISO
- An optional package that is included in the ISO
- An optional package that is not included in the ISO

Visit the Cisco Software Download page to download the Cisco IOS XR software images.

To determine the Cisco IOS XR Software packages installed on your router, log in to the router and enter the **show install active** command:

To know about all the RPMs installed including XR, OS and other components use the **show install active all** command.

The software modularity approach provides a flexible model that allows you to install a subset of IOS XR packages on devices based on your individual requirements. All critical components are modularized as packages so that you can select the features that you want to run on your router.

Note The above show command output displays mandatory packages that are installed on the router. To view the optional and bug fix RPM packages, first install the package and use the **show install active summary** command.

Caveats Specific to Cisco 8000 Series Routers

This section lists the open bugs for Cisco 8000 Series Routers

Table 3: Cisco 8000 Series Router Specific Bug

Bug ID	Headline
CSCvx19378	On Cisco 8000 routers, software downgrade from 7.3.15 to 7.0.14 fails with an error 'No such file or directory'

Determine Software Version

Log in to the router and enter the **show version** command:

```
RP/0/RP0/CPU0# show version
Mon Mar  1 03:53:38.590 UTC
Cisco IOS XR Software, Version 7.3.1 LNT
Copyright (c) 2013-2021 by Cisco Systems, Inc.

Build Information:
Built By     : ingunawa
Built On     : Fri Feb 26 04:56:31 UTC 2021
Build Host   : iox-ucs-020
Workspace    : /auto/srcarchive17/prod/7.3.1/8000/ws
Version      : 7.3.1
```

```
Label         : 7.3.1

cisco 8000 (Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz)
cisco 8202-SYS (Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz) processor with 32GB of memory
R11 uptime is 45 minutes
```

Determine Firmware Support

Log in to the router and enter **show fpd package** command:

Cisco 8200 Series Router

```
RP/0/RP0/CPU0# show fpd package
Mon Mar  1 04:03:36.411 UTC

================================ ============================================
                                        Field Programmable Device Package
                                 ============================================
                                           Req      SW       Min Req   Min Req
Card Type            FPD Description       Reload   Ver      SW Ver   Board Ver
================== ========================= ====== ======= ======== =========
------------------------------------------------------------------------------
8202                 Bios                   YES     1.22    1.22     0.0
                     BiosGolden             YES     1.22    1.15     0.0
                     BmcFitGolden           YES     3.00    0.240    0.0
                     BmcFitPrimary          YES     3.00    3.00     0.0
                     BmcFpga                YES     1.01    1.01     0.0
                     BmcFpgaGolden          YES     1.01    0.86     0.0
                     BmcTamFw               YES     5.06    5.06     0.0
                     BmcTamFwGolden         YES     5.06    5.05     0.0
                     BmcUbootGolden         YES     1.02    0.15     0.0
                     BmcUbootPrimary        YES     1.02    1.02     0.0
                     IoFpga                 YES     1.01    1.01     0.0
                     IoFpgaGolden           YES     1.01    0.33     0.0
                     MiFpga                 YES     1.00    1.00     0.0
                     MiFpgaGolden           YES     1.00    0.02     0.0
                     SsdIntelS3520          YES     1.21    1.21     0.0
                     SsdIntelS4510          YES    11.20   11.20     0.0
                     SsdMicron5100          YES     7.01    7.01     0.0
                     SsdMicron5300          YES     0.01    0.01     0.0
                     x86Fpga                YES     1.02    1.02     0.0
                     x86FpgaGolden          YES     1.02    0.48     0.0
                     x86TamFw               YES     5.06    5.06     0.0
                     x86TamFwGolden         YES     5.06    5.05     0.0
------------------------------------------------------------------------------
PSU2KW-ACPE          PO-PrimMCU             NO     17.54   17.54     0.0
------------------------------------------------------------------------------
PSU2KW-ACPI          PO-PrimMCU             NO     17.56   17.56     0.0
------------------------------------------------------------------------------
PSU2KW-DCPE          PO-PrimMCU             NO      1.07    1.07     0.0
------------------------------------------------------------------------------
PSU2KW-DCPI          PO-PrimMCU             NO      1.07    1.07     0.0
```

Cisco 8800 Series Router

```
RP/0/RP0/CPU0# show fpd package
Mon Mar  1 04:31:34.268 UTC

================================ ============================================
                                        Field Programmable Device Package
```

Card Type	FPD Description	Req Reload	SW Ver	Min Req SW Ver	Min Req Board Ver
88-LC0-36FH	Bios	YES	0.09	0.09	0.1
	BiosGolden	YES	0.09	0.09	0.1
	EthSwitch	YES	1.02	1.02	0.0
	EthSwitchGolden	YES	1.02	0.07	0.0
	IoFpga	YES	0.127	0.127	0.1
	IoFpgaGolden	YES	0.127	0.127	0.1
	PwrSeqZone0_0	YES	0.03	0.03	0.10
	PwrSeqZone1_0	YES	0.03	0.03	0.10
	PwrSeqZone2_0	YES	0.03	0.03	0.10
	PwrSeqZone2_1	YES	0.03	0.03	0.10
	PwrSeqZone3_0	YES	0.03	0.03	0.10
	PwrSeqZone3_1	YES	0.03	0.03	0.10
	PwrSeqZone3_2	YES	0.03	0.03	0.10
	PwrSeqZone3_3	YES	0.03	0.03	0.10
	SsdIntelS3520	YES	1.21	1.21	0.0
	SsdIntelS4510	YES	11.20	11.20	0.0
	SsdMicron5100	YES	7.01	7.01	0.0
	SsdMicron5300	YES	0.01	0.01	0.0
	x86Fpga	YES	0.33	0.33	0.1
	x86FpgaGolden	YES	0.33	0.33	0.1
	x86TamFw	YES	6.05	6.05	0.1
	x86TamFwGolden	YES	6.05	6.05	0.1
88-LC0-36FH-M	Bios	YES	0.09	0.09	0.1
	BiosGolden	YES	0.09	0.09	0.1
	EthSwitch	YES	1.02	1.02	0.0
	EthSwitchGolden	YES	1.02	0.07	0.0
	IoFpga	YES	0.127	0.127	0.1
	IoFpgaGolden	YES	0.127	0.127	0.1
	PwrSeqZone0_0	YES	0.04	0.04	0.1
	PwrSeqZone0_0	YES	0.03	0.03	0.20
	PwrSeqZone1_0	YES	0.04	0.04	0.1
	PwrSeqZone1_0	YES	0.03	0.03	0.20
	PwrSeqZone2_0	YES	0.04	0.04	0.1
	PwrSeqZone2_0	YES	0.03	0.03	0.20
	PwrSeqZone2_1	YES	0.04	0.04	0.1
	PwrSeqZone2_1	YES	0.03	0.03	0.20
	PwrSeqZone3_0	YES	0.04	0.04	0.1
	PwrSeqZone3_0	YES	0.03	0.03	0.20
	PwrSeqZone3_1	YES	0.04	0.04	0.1
	PwrSeqZone3_1	YES	0.03	0.03	0.20
	PwrSeqZone3_2	YES	0.04	0.04	0.1
	PwrSeqZone3_2	YES	0.03	0.03	0.20
	PwrSeqZone3_3	YES	0.04	0.04	0.1
	PwrSeqZone3_3	YES	0.03	0.03	0.20
	SsdIntelS3520	YES	1.21	1.21	0.0
	SsdIntelS4510	YES	11.20	11.20	0.0
	SsdMicron5100	YES	7.01	7.01	0.0
	SsdMicron5300	YES	0.01	0.01	0.0
	x86Fpga	YES	0.33	0.33	0.1
	x86FpgaGolden	YES	0.33	0.33	0.1
	x86TamFw	YES	6.05	6.05	0.1
	x86TamFwGolden	YES	6.05	6.05	0.1
8800-LC-36FH	Bios	YES	1.22	1.22	0.0
	BiosGolden	YES	1.22	1.15	0.0
	EthSwitch	YES	1.02	1.02	0.0
	EthSwitchGolden	YES	1.02	0.07	0.0
	IoFpga	YES	1.12	1.12	0.0

	IoFpgaGolden	YES	1.12	0.08	0.0
	SsdIntelS3520	YES	1.21	1.21	0.0
	SsdIntelS4510	YES	11.20	11.20	0.0
	SsdMicron5100	YES	7.01	7.01	0.0
	SsdMicron5300	YES	0.01	0.01	0.0
	x86Fpga	YES	1.01	1.01	0.0
	x86FpgaGolden	YES	1.01	0.33	0.0
	x86TamFw	YES	5.06	5.06	0.0
	x86TamFwGolden	YES	5.06	5.05	0.0
8800-LC-48H	Bios	YES	1.22	1.22	0.0
	BiosGolden	YES	1.22	1.15	0.0
	EthSwitch	YES	1.02	1.02	0.0
	EthSwitchGolden	YES	1.02	0.07	0.0
	IoFpga	YES	1.12	1.12	0.0
	IoFpgaGolden	YES	1.12	0.08	0.0
	SsdIntelS3520	YES	1.21	1.21	0.0
	SsdIntelS4510	YES	11.20	11.20	0.0
	SsdMicron5100	YES	7.01	7.01	0.0
	SsdMicron5300	YES	0.01	0.01	0.0
	x86Fpga	YES	1.01	1.01	0.0
	x86FpgaGolden	YES	1.01	0.33	0.0
	x86TamFw	YES	5.06	5.06	0.0
	x86TamFwGolden	YES	5.06	5.05	0.0
8800-RP	Bios	YES	1.22	1.22	0.0
	BiosGolden	YES	1.22	1.15	0.0
	BmcFitGolden	YES	3.00	0.240	0.0
	BmcFitPrimary	YES	3.00	3.00	0.0
	BmcFpga	YES	1.02	1.02	0.0
	BmcFpgaGolden	YES	1.02	0.19	0.0
	BmcTamFw	YES	5.06	5.06	0.0
	BmcTamFwGolden	YES	5.06	5.05	0.0
	BmcUbootGolden	YES	1.02	0.15	0.0
	BmcUbootPrimary	YES	1.02	1.02	0.0
	EthSwitch	YES	1.01	1.01	0.0
	EthSwitchGolden	YES	1.01	0.07	0.0
	SsdIntelS3520	YES	1.21	1.21	0.0
	SsdIntelS4510	YES	11.20	11.20	0.0
	SsdMicron5100	YES	7.01	7.01	0.0
	SsdMicron5300	YES	0.01	0.01	0.0
	TimingFpga	YES	1.02	1.02	0.0
	TimingFpgaGolden	YES	1.02	0.11	0.0
	x86Fpga	YES	1.05	1.05	0.0
	x86FpgaGolden	YES	1.05	0.24	0.0
	x86TamFw	YES	5.06	5.06	0.0
	x86TamFwGolden	YES	5.06	5.05	0.0
8804-FAN	FtFpga	NO	1.00	1.00	0.0
	FtFpgaGolden	NO	1.00	0.16	0.0
8804-FC0	IoFpga	YES	0.12	0.12	0.0
	IoFpgaGolden	YES	0.12	0.12	0.0
8808-FAN	FtFpga	NO	1.00	1.00	0.0
	FtFpgaGolden	NO	1.00	0.16	0.0
8808-FC	IoFpga	YES	1.02	1.02	0.0
	IoFpgaGolden	YES	1.02	0.05	0.0
8808-FC0	IoFpga	YES	0.12	0.12	0.0
	IoFpgaGolden	YES	0.12	0.12	0.0
8812-FAN	FtFpga	NO	1.00	1.00	0.0

```
                    FtFpgaGolden              NO      1.00    0.16    0.0
-------------------------------------------------------------------------------
8812-FC             IoFpga                    YES     1.02    1.02    0.0
                    IoFpgaGolden              YES     1.02    0.05    0.0
                    Retimer                   YES     3.00    3.00    0.0
-------------------------------------------------------------------------------
8818-FAN            FtFpga                    NO      1.00    1.00    0.0
                    FtFpgaGolden              NO      1.00    0.16    0.0
-------------------------------------------------------------------------------
8818-FC             IoFpga                    YES     1.02    1.02    0.0
                    IoFpgaGolden              YES     1.02    0.05    0.0
                    Retimer                   YES     3.00    3.00    0.0
-------------------------------------------------------------------------------
8818-FC0            IoFpga                    YES     0.12    0.12    0.0
                    IoFpgaGolden              YES     0.12    0.12    0.0
-------------------------------------------------------------------------------
PSU-4.8KW-DC100     PO-PrimMCU                NO     34.238  34.238   0.0
-------------------------------------------------------------------------------
PSU6.3KW-20A-HV     DT-LogicMCU               NO      1.00    1.00    0.0
                    DT-PrimMCU                NO      1.00    1.00    0.0
                    DT-SecMCU                 NO      1.00    1.00    0.0
-------------------------------------------------------------------------------
PSU6.3KW-HV         AB-LogicMCU               NO      3.08    3.08    0.0
                    AB-PrimMCU                NO      3.08    3.08    0.0
                    AB-SecMCU                 NO      3.06    3.06    0.0
                    DT-LogicMCU               NO      4.11    4.11    0.0
                    DT-PrimMCU                NO      4.01    4.01    0.0
                    DT-SecMCU                 NO      4.00    4.00    0.0
-------------------------------------------------------------------------------
PWR-4.4KW-DC-V3     DT-LogicMCU               NO      3.02    3.02    0.0
                    DT-Prim1MCU               NO      3.01    3.01    0.0
                    DT-Prim2MCU               NO      3.01    3.01    0.0
                    DT-Sec1MCU                NO      3.01    3.01    0.0
                    DT-Sec2MCU                NO      3.01    3.01    0.0
```

Supported Transceiver Modules

To determine the transceivers that Cisco hardware device supports, refer to the Transceiver Module Group (TMG) Compatibility Matrix tool.

Other Important Information

- The warning message that the smart licensing evaluation period has expired is displayed in the console every hour. There is, however, no functionality impact on the device. The issue is seen on routers that don't have the Flexible Consumption licensing model enabled. To stop the repetitive messaging, register the device with the smart licensing server and enable the Flexible Consumption model. Later load a new registration token.

  To register the device with the smart licensing server, see the Registering and Activating Your Router.

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.