Cisco Catalyst 9800-L Wireless Controller

© 2023 Cisco and/or its affiliates. All rights reserved.

Contents

Product overview	4
Platform details	5
Ports	7
Power	9
SFPs supported	9
Product benefits	10
Specifications	13
Software requirements	16
Licensing	16
Warranty	19
Cisco environmental sustainability	20
Ordering information	20
Cisco Capital	21
Document history	22

© 2023 Cisco and/or its affiliates. All rights reserved.

Built from the ground up for intent-based networking



Figure 1.
Cisco Catalyst 9800-L

The Cisco Catalyst 9800-L is a fixed wireless controller with seamless software updates for small and midsize enterprises.

Built from the ground up for intent-based networking, the Cisco Catalyst 9800-L brings together Cisco IOS XE Software and Cisco RF excellence to create a best-in-class wireless experience for your evolving and growing organization.

The Cisco Catalyst 9800-L is feature rich and enterprise ready to power your business-critical operations and transform end-user experiences:

- Choose between copper and fiber uplinks. This choice gives you flexibility in your network.
- High availability and seamless software updates, enabled by hot and cold patching, keep your clients and services **always on** in planned and unplanned events.
- **Secure** the air, devices, and users with the Cisco Catalyst 9800-L. The wireless infrastructure becomes the strongest first line of defense, with Encrypted Traffic Analytics (ETA) and Software-Defined Access (SD-Access). The controller comes with built-in security: Secure Boot, runtime defenses, image signing, integrity verification, and hardware authenticity.
- Built on a modular operating system, the controller features open and programmable APIs that enable **automation** of day-0 to day-N network operations. Model-driven streaming telemetry provides deep insights into your **network and client health**.
- Cisco User Defined Network, a feature available in Cisco DNA Center, allows IT to give end users control of their very own wireless network partition on a shared network. End users can then remotely and securely deploy their devices on this network. Perfect for university dormitories or extended hospital stays, Cisco User Defined Network grants both device security and control, allowing each user to choose who can connect to their network.

© 2023 Cisco and/or its affiliates. All rights reserved.

- The Wi-Fi 6 readiness dashboard is a new dashboard in the Assurance menu of Cisco DNA Center. It will look through the inventory of all devices on the network and verify device, software, and client compatibility with the new Wi-Fi 6 standard. After upgrading, advanced wireless analytics will indicate performance and capacity gains as a result of the Wi-Fi 6 deployment. This is an incredible tool that will help your team define where and how the wireless network should be upgraded. It will also give you insights into the access point distribution by protocol (802.11 ac/n/abg), wireless airtime efficiency by protocol, and granular performance metrics.
- With Cisco In Service Software Upgrade (ISSU), network downtime during a software update or upgrade is a thing of the past. ISSU is a complete image upgrade and update while the network is still running. The software image—or patch—is pushed onto the wireless controller while traffic forwarding continues uninterrupted. All access point and client sessions are retained during the upgrade process. With just a click, your network automatically upgrades to the newest software.

Product overview

Table 1. Key features

Feature	Description
Maximum number of access points	250, 500 (with Performance license)
Maximum number of clients	5000, 10,000 (with Performance license)
Maximum throughput	5 Gbps, 10 Gbps **(with Performance license)
Maximum WLANs	4096
Maximum VLANs	4096
Fixed uplinks	2x 10G/Multigigabit copper or 2x 10G/Multigigabit fiber
Power supply	110W, 12V DC, AC/DC adapter
Maximum power consumption	9800-L-C: 86.9W (with 4.5W USB load) 9800-L-F: 84.5W (assumes 2pc 2.5W SFP and with 4.5W USB load)
Deployment modes	Centralized, Cisco FlexConnect, and fabric
Form factor	1RU; half-width chassis allows side-by-side installation in standard 19-in. rack
License	Smart License enabled
Software	Cisco IOS XE
Management	Cisco DNA Center, Cisco Prime Infrastructure, and third party (open standards APIs)
Interoperability	AireOS-based controllers

© 2023 Cisco and/or its affiliates. All rights reserved.

Feature	Description
Access points	Cisco Aironet 802.11ac Wave 1 and Wave 2 access points, Cisco Catalyst 9100 802.11ax access points

*For information on compatibility: Compatibility Guide

**With 1374 Byte size of packet

Always on

The Cisco Catalyst 9800-L provides seamless software updates for faster resolution of critical issues, the ability to introduce new access points with zero downtime, and flexible software upgrades. Stateful Switchover (SSO) with active standby and N+1 redundancy keeps your network, services, and clients always on, even in unplanned events.

Secure

Secure the air, devices, and users with the Cisco Catalyst 9800-L. Wireless infrastructure becomes the strongest first line of defense with Encrypted Traffic Analytics and SD-Access. The controller comes with built-in security: Secure Boot, runtime defenses, image signing, integrity verification, and hardware authenticity. Cisco Advanced Wireless Intrusion Prevention System (aWIPS) is a complete wireless security solution that uses the Cisco Unified Access infrastructure to detect, locate, mitigate, and contain wired and wireless rogues and threats.

Open and programmable

The Cisco Catalyst 9800-L controller is built on the Cisco IOS XE operating system, which offers a rich set of open standards-based programmable APIs and model-driven telemetry that provide an easy way to automate day-0 to day-N network operations.

Platform details

Physical dimensions

Table 2. Physical dimensions

Dimension	Value
Width	8.5 in. (21.59 cm)
Depth	9.06 in. (23.01 cm)
Height	1.58 in. (4.02 cm)
Weight	C9800-L-C: 3.95 lb. (1.79 kg) C9800-L-F: 4.01 lb. (1.82 kg)

© 2023 Cisco and/or its affiliates. All rights reserved.

Front panel

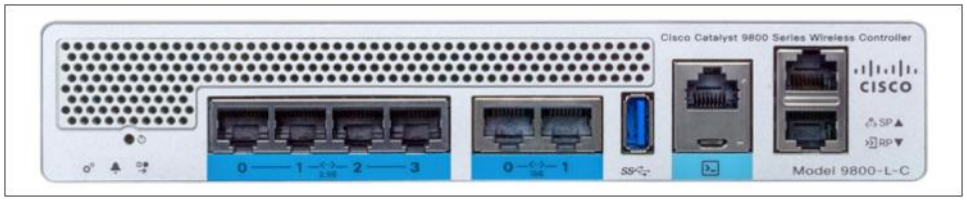


Figure 2.
Cisco Catalyst 9800-L-C front panel

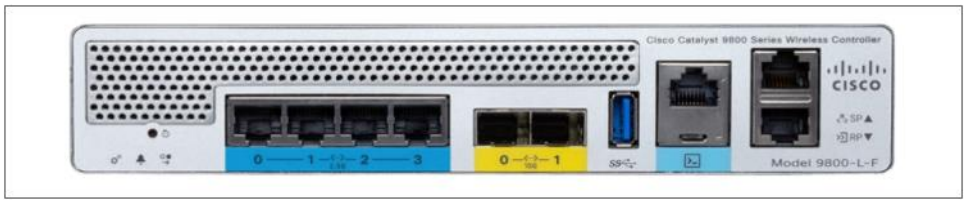


Figure 3.
Cisco Catalyst 9800-L-F front panel

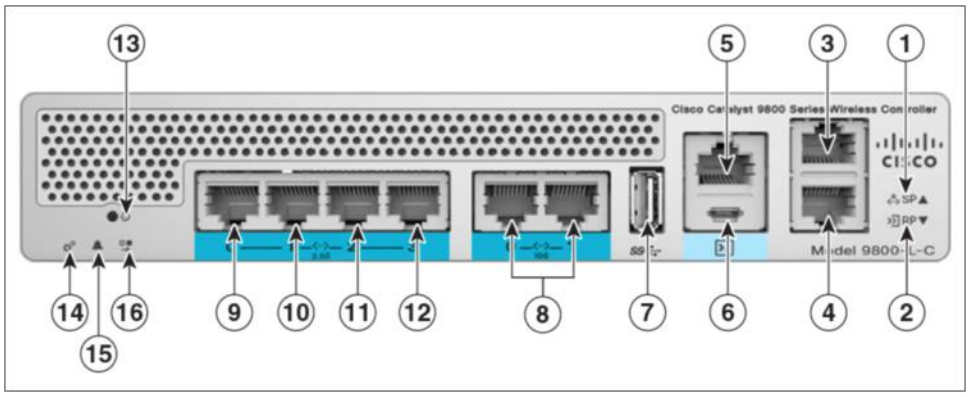


Figure 4.
Cisco Catalyst 9800-L -C front panel with components labeled

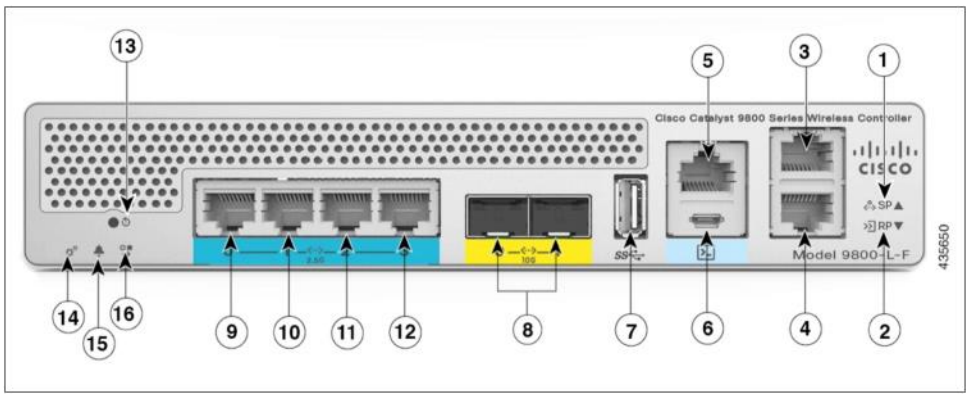


Figure 5.
Cisco Catalyst 9800-L-F front panel with components labeled

© 2023 Cisco and/or its affiliates. All rights reserved.

Table 3. Front panel components

Label	Description
1	Service port LED
2	Redundancy port LED
3	Service Port (SP) (RJ-45) for out-of-band management
4	Redundancy port
5	RJ-45 console port
6	Micro-B USB console
7	USB 3.0 port
8	2x 10G/Multigigabit copper (Figure 4) 2x 10G/Multigigabit fiber (Figure 5)
9-12	Quad RJ-45 2.5G/1G Multigigabit Ethernet ports
13	Reset button
14	System LED
15	Alarm LED
16	High availability LED

Ports

Table 4. Ports and their purpose

Port	Description
1x RJ-45 console port	Console port for out-of-band management.
1x Micro USB console port	Console port for out-of-band management.
1x USB 3.0 port	USB 3.0 port for plugging in external memory.
1x RJ-45 management port	Management port used for out-of-band management. Also known as the service port.
1x RJ-45 redundancy port	Redundancy port used for SSO.
4x 2.5G/1G and 2x 10G copper ports	Ports used for sending and receiving traffic between access points and controller, northbound traffic, in-band management traffic, and wireless client traffic. Must be connected to the switch.
4x 2.5G/1G copper and 2x 10G SFP+ fiber ports	Ports used for sending and receiving traffic between access points and controller, northbound traffic, in-band management traffic, and wireless client traffic. Must be connected to the switch.

The four data ports can operate in either 2.5 Gigabit Ethernet or 1 Gigabit Ethernet mode.

Note: 10-Mbps operation is not supported.

© 2023 Cisco and/or its affiliates. All rights reserved.

Front LEDs

Table 5. Front-panel LEDs and their purpose

LED	Color	Function
Power	Green	Green if all power rails are within spec
System status	Green	On: Cisco IOS XE boot is complete Blinking: Cisco IOS boot in progress
	Red	On: System crash Blinking: Secure Boot failure Off: ROMMON boot
High Availability (HA) port	Green	On: HA active Slow blink: HA standby hot
	Amber	Slow blink: Booted with HA standby cold Fast blink: HA maintenance
Alarm	Green	On: ROMMON boot complete Blinking: System upgrade in progress
	Amber	On: ROMMON boot and SYSTEM bootup Blinking: Temperature error and Secure Boot failure
Network link LED Indicator	Green	Solid green: Link Flashing green: Activity LED off: Link down

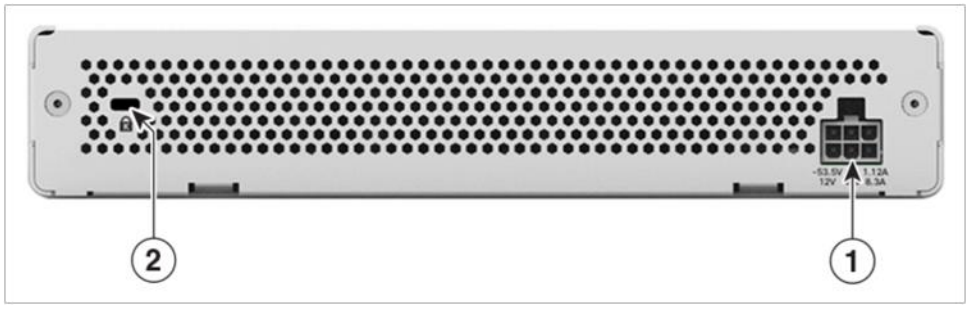


Figure 6.
Rear panel with components labeled

© 2023 Cisco and/or its affiliates. All rights reserved.

Table 6. Rear-panel components

Label	Description
1	Power adapter
2	Kensington lock

Power

The Cisco Catalyst 9800-L Wireless Controller is powered by a single output 12V DC, 110W 120/240V AC adapter (C9800-AC-110W) that is shipped by default.

SFPs supported

Table 7. SFPs supported

Type	Module supported
SFP supported on the C9800-L-F-K9 Model	GLC-BX-D
	GLC-BX-U
	GLC-SX-MMD
	GLC-ZX-SMD
	GLC-TE
	FINISAR-LR
	FINISAR-SR
	SFP-10G-LR
	SFP-10G-LR-S
	SFP-10G-LRM
	SFP-10G-LR-X
	SFP-10G-SR
	SFP-10G-SR-S
	SFP-10G-SR-X
	SFP-H10GB-CU1M
	SFP-H10GB-CU1.5M
	SFP-H10GB-CU2M
	SFP-H10GB-CU2.5M

© 2023 Cisco and/or its affiliates. All rights reserved.

Type	Module supported
	SFP-H10GB-CU3M
	SFP-H10GB-CU5M
	SFP-H10GB-ACU7M
	SFP-H10GB-ACU10M
SFP supported on the C9800-L-C-K9 Model	GLC-BX-D
	GLC-BX-U
	GLC-LH-SMD
	GLC-SX-MMD
	GLC-T
	GLC-TE
	GLC-ZX-SMD

Product benefits

Cisco IOS XE

The Cisco Catalyst 9800 Series opens a completely new paradigm in network configuration, operation, and monitoring through network automation. Cisco's automation solution is open, standards based, and extensible across the entire lifecycle of a network device. The various mechanisms that bring about network automation are outlined below, based on the device lifecycle.

- **Automated device provisioning:** This is the ability to automate the process of upgrading software images and installing configuration files on Cisco Catalyst access points when they are being deployed in the network for the first time. Cisco provides turnkey solutions with Plug and Play (PnP) capabilities that enable an effortless and automated deployment.
- **API-driven configuration:** Modern wireless controllers such the Cisco Catalyst 9800 Series support a wide range of automation features and provide robust open APIs over NETCONF and RESTCONF using YANG data models for external tools, both off-the-shelf and custom built, to automatically provision network resources.
- **Granular visibility:** Model-driven telemetry provides a mechanism to stream data from a switch to a destination. The data to be streamed is driven through subscription to a data set in a YANG model. The subscribed data set is streamed out to the destination at configured intervals. Additionally, Cisco IOS XE enables the push model, which provides near-real-time monitoring of the network, leading to quick detection and rectification of failures.
- **Seamless software upgrades and patching:** To enhance OS resilience, Cisco IOS XE supports patching, which provides fixes for critical bugs and security vulnerabilities between regular maintenance releases. This support allows customers to add patches without having to wait for the next maintenance release.

© 2023 Cisco and/or its affiliates. All rights reserved.

Security

- **Trustworthy systems:** Cisco Trust Anchor Technologies provide a highly secure foundation for Cisco products. With the Cisco Catalyst 9800 Series, these trustworthy systems enable hardware and software authenticity assurance for supply chain trust and strong mitigation against man-in-the-middle attacks on software and firmware. Trust Anchor capabilities include:
- **Image signing:** Cryptographically signed images provide assurance that the firmware, BIOS, and other software are authentic and unmodified. As the system boots, its software signatures are checked for integrity.
- **Secure Boot:** Cisco Secure Boot technology anchors the boot sequence chain of trust to immutable hardware, mitigating threats against a system's foundational state and the software that is to be loaded, regardless of a user's privilege level. It provides layered protection against the persistence of illicitly modified firmware.
- **Cisco Trust Anchor module:** A tamper-resistant, strong cryptographic, single-chip solution provides hardware authenticity assurance to uniquely identify the product so that its origin can be confirmed to Cisco, providing assurance that the product is genuine.
- **Cisco Wireless Intrusion Prevention System (WIPS):** WIPS offers advanced network security to detect, locate, mitigate, and contain any intrusion or threat on your wireless network. It can monitor and detect wireless network anomalies, unauthorized access, and RF attacks. A new, dedicated classification engine for rogues and aWIPS is built on Cisco DNA Center. A fully integrated stack for the WIPS solution includes Cisco DNA Center, Cisco Catalyst 9800 controller, Wave 2, and Cisco Catalyst 9100 Access Point. This new architecture provides improved detection and security, simplicity, ease of use, and reduced false positive alarms.

Resiliency and high availability

- **Stateful Switchover (SSO):** Stateful Switchover with an active standby and N+1 redundancy keeps your network, services, and clients always on, even in unplanned events.
- **Software Maintenance Upgrades (SMUs) and hot and cold patching:** Patching allows for a patch to be installed as a bug fix without bringing down the entire network and avoiding the need to requalify an entire software image. The SMU is a package that can be installed on a system to provide a patch fix or security resolution to a released image. SMUs allow you to address the network issue quickly while reducing the time and scope of the testing required. The Cisco IOS XE platform internally validates the SMU compatibility and does not allow you to install incompatible SMUs. All SMUs are integrated into the subsequent Cisco IOS XE Software maintenance releases.
- **Intelligent rolling access point upgrades and seamless multisite upgrades:** The Cisco Catalyst 9800 Series comes with intelligent rolling access point upgrades to simplify network operations. Multisite upgrades can now be done in stages, and access points can be upgraded intelligently without restarting the entire network.
- Standby Monitoring of Cisco Catalyst 9800 Wireless Controllers in HA mode enables monitoring the health of the system on standby controller in an HA pair using programmatic interfaces (NETCONF/YANG, RESTCONF) and CLIs without going through the active controller. **For more details refer technical documentation**.

© 2023 Cisco and/or its affiliates. All rights reserved.

- **In-Service Software Upgrade (ISSU):** ISSU is a complete image upgrade/update with zero downtime while the network is still on. The software image or a patch is pushed onto the wireless controller while traffic forwarding continues uninterrupted. All access point and client sessions are retained during the upgrade process. With just a click, your network automatically upgrades to the newest software. Your backup 9800 controller receives the new software that is pushed via the active 9800 controller. The backup 9800 controller becomes active and takes over your network, while your previously active 9800 turns into a backup 9800 controller and processes the software upgrade. Using an intelligent RF-based rolling access point upgrade, all access points are upgraded in a staggered fashion without impacting any wireless session. This procedure is carried out without any manual intervention natively from the controller and without the need for an external orchestrator or additional licenses.

Flexible NetFlow

- **Flexible NetFlow (FNF):** Cisco IOS Software FNF is the next generation in flow visibility technology, allowing optimization of the network infrastructure, reducing operating costs, and improving capacity planning and security incident detection with increased flexibility and scalability.

Application visibility and control

- **Next-Generation Network-Based Application Recognition (NBAR2):** NBAR2 enables advanced application classification techniques and accuracy, with up to 1400 predefined and well-known application signatures and up to 150 encrypted applications on the Cisco Catalyst 9800 Series. Some of the most popular applications included are Skype, Office 365, Microsoft Lync, Cisco WebEx, and Facebook. Many others are already predefined and easy to configure. NBAR2 provides the network administrator with an important tool to identify, control, and monitor end-user application usage while helping ensure a quality user experience and securing the network from malicious attacks. It uses FNF to report application performance and activities within the network to any supported NetFlow collector, such as Cisco Prime, Cisco Stealthwatch, or any compliant third-party tool.

Quality of service (QoS)

- **Superior QoS:** QoS technologies are a set of tools and techniques for managing network resources and are considered the key enabling technologies for the transparent convergence of voice, video, and data networks. QoS on the Cisco Catalyst 9800 Series consists of classification and marking, policing and markdown, and scheduling, shaping, and queuing functions. A modular QoS command-line framework provides consistent platform-independent and flexible configuration behavior. The Cisco Catalyst 9800 Series also supports 2-level hierarchical or nested policies.

Smart operation

- **Bluetooth ready:** The Cisco Catalyst 9800-L has hardware support to connect a Bluetooth dongle to the controller, enabling you to use this wireless interface as a management port. This port functions as an IP management interface and can be used for configuration and troubleshooting using the WebUI or Command-Line Interface (CLI), and to transfer images and configurations.
- **WebUI:** WebUI is an embedded GUI-based device-management tool that enables provisioning of the device, simplifying device deployment and manageability and enhancing the user experience. WebUI comes with the default image. There is no need to enable anything or install any license on the device. You can use WebUI to build a day-1 configuration and from then on monitor and troubleshoot the device without having to know how to use the CLI.

© 2023 Cisco and/or its affiliates. All rights reserved.

Specifications

Table 8. Specifications

Item	Specification	
Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave1 and Wave2, 802.11ax	
Wired, switching, and routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T, 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q VLAN tagging, IEEE 802.1AX Link Aggregation	
Data Requests For Comments (RFCs)	• RFC 768 UDP • RFC 791 IP • RFC 2460 IPv6 • RFC 792 ICMP • RFC 793 TCP • RFC 826 ARP • RFC 1122 Requirements for Internet Hosts • RFC 1519 CIDR • RFC 1542 BOOTP • RFC 2131 DHCP • RFC 5415 CAPWAP Protocol Specification • RFC 5416 CAPWAP Binding for 802.11	
Security standards	• Wi-Fi Protected Access (WPA) • IEEE 802.11i (WPA2, RSN) • Wi-Fi Protected Access 3 (WPA3) • RFC 1321 MD5 Message-Digest Algorithm • RFC 1851 ESP Triple DES Transform • RFC 2104 HMAC: Keyed-Hashing for Message Authentication • RFC 2246 TLS Protocol Version 1.0 • RFC 2401 Security Architecture for the Internet Protocol • RFC 2403 HMAC-MD5-96 within ESP and AH • RFC 2404 HMAC-SHA-1-96 within ESP and AH • RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV • RFC 2407 Interpretation for ISAKMP • RFC 2408 ISAKMP • RFC 2409 IKE • RFC 2451 ESP CBC-Mode Cipher Algorithms • RFC 3280 Internet X.509 PKI Certificate and CRL Profile • RFC 4347 Datagram Transport Layer Security • RFC 5246 TLS Protocol Version 1.2	

© 2023 Cisco and/or its affiliates. All rights reserved.

Item	Specification	
Encryption	• Wired Equivalent Privacy (WEP) RC4 40, 104 and 128 bits (both static and shared keys) • Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) • Data Encryption Standard (DES): DES-CBC, 3DES • Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit • DTLS: AES-CBC • IPsec: DES-CBC, 3DES, AES-CBC • 802.1AE MACsec encryption	
Authentication, Authorization, and Accounting (AAA)	• IEEE 802.1X • RFC 2548 Microsoft Vendor-Specific RADIUS Attributes • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS Authentication • RFC 2866 RADIUS Accounting • RFC 2867 RADIUS Tunnel Accounting • RFC 2869 RADIUS Extensions • RFC 3576 Dynamic Authorization Extensions to RADIUS • RFC 5176 Dynamic Authorization Extensions to RADIUS • RFC 3579 RADIUS Support for EAP • RFC 3580 IEEE 802.1X RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol (EAP) • Web-based authentication • TACACS support for management users	
Management	• Simple Network Management Protocol (SNMP) v1, v2c, v3 • RFC 854 Telnet • RFC 1155 Management Information for TCP/IP-Based Internets • RFC 1156 MIB • RFC 1157 SNMP • RFC 1213 SNMP MIB II • RFC 1350 TFTP • RFC 1643 Ethernet MIB • RFC 2030 SNTP • RFC 2616 HTTP • RFC 2665 Ethernet-Like Interface Types MIB • RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions • RFC 2819 RMON MIB • RFC 2863 Interfaces Group MIB • RFC 3164 Syslog • RFC 3414 User-Based Security Model (USM) for SNMPv3 • RFC 3418 MIB for SNMP • RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs • RFC 4741 Base NETCONF protocol • RFC 4742 NETCONF over SSH	

© 2023 Cisco and/or its affiliates. All rights reserved.

Item	Specification	
	• RFC 6241 Network Configuration Protocol (NETCONF) • RFC 6242 NETCONF over SSH • RFC 5277 NETCONF event notifications • RFC 5717 Partial Lock Remote Procedure Call • RFC 6243 With-Defaults capability for NETCONF • RFC 6020 YANG • Cisco private MIBs	
Management interfaces	• Web-based: HTTP/HTTPS • Command-line interface: Telnet, Secure Shell (SSH) Protocol, serial port • Cisco Prime Infrastructure	
Environmental conditions supported	Operating temperature: • 32° to 104°F (0° to 40°C) Note: The maximum temperature is derated by 1.0°C for every 1000 ft (305 m) of altitude above sea level. Nonoperating temperature: • -13° to 158°F (-25° to 70°C) Operating humidity: • 5% to 95% noncondensing Nonoperating humidity: • 0% to 95% noncondensing Altitude: • Operating altitude: 0 to 3000 m (0 to 10,000 ft) • Nonoperating altitude: 0 to 12,192 m (0 to 40,000 ft.) Electrical input: • AC input frequency range: 47 to 63 Hz • AC input range: 90 to 264 VAC Maximum power: • 9800-L-C max measured power = 86.9W (with 4.5W USB load) • 9800-L-F max measured power = 84.5W (assumes 2pc 2.5W SFP and with 4.5W USB load) Maximum heat dissipation: • 9800-L-C: 296.4 Btu/hr (with 4.5W USB load) • 9800-L-F: 288.2 Btu/hr (assumes 2pc 2.5W SFP and with 4.5W USB load) Sound power level measure: • Normal: 40 dBA at 25C • Maximum: 42.9 dBA at 40C Power adapter: • Input power: 100 to 240 VAC; 50/60 Hz	

© 2023 Cisco and/or its affiliates. All rights reserved.

Item	Specification	
Regulatory compliance	Safety: • UL/CSA 60950-1 • IEC/EN 60950-1 • AS/NZS 60950.1 • CAN/CSA-C22.2 No. 60950-1	
	EMC - Emissions: • FCC 47CFR15 • AS/NZS CISPR 22 • CISPR 22 • EN55022/EN55032 (EMI-1) • ICES-003 • VCCI • KN 32 (EMI-2) • CNS-13438	**Class A**
	EMC - Emissions: • EN61000-3-2 Power Line Harmonics (EMI-3) • EN61000-3-3 Voltage Changes, Fluctuations, and Flicker (EMI-3)	

Software requirements

The Cisco Catalyst 9800-L runs on Cisco IOS XE Software version 16.12.1 or later. This software release includes all the features listed earlier in the Product Benefits section.

Table 9 lists the minimum software requirements for the controller models.

Licensing

No licenses are required to boot up a **Cisco Catalyst 9800 Series Wireless Controller**. However, in order to connect any access points to the **controller**, Cisco DNA software subscriptions are required. To be able to connect to a Cisco Catalyst 9800 Series controller, each access point requires a Cisco DNA subscription license.

© 2023 Cisco and/or its affiliates. All rights reserved.

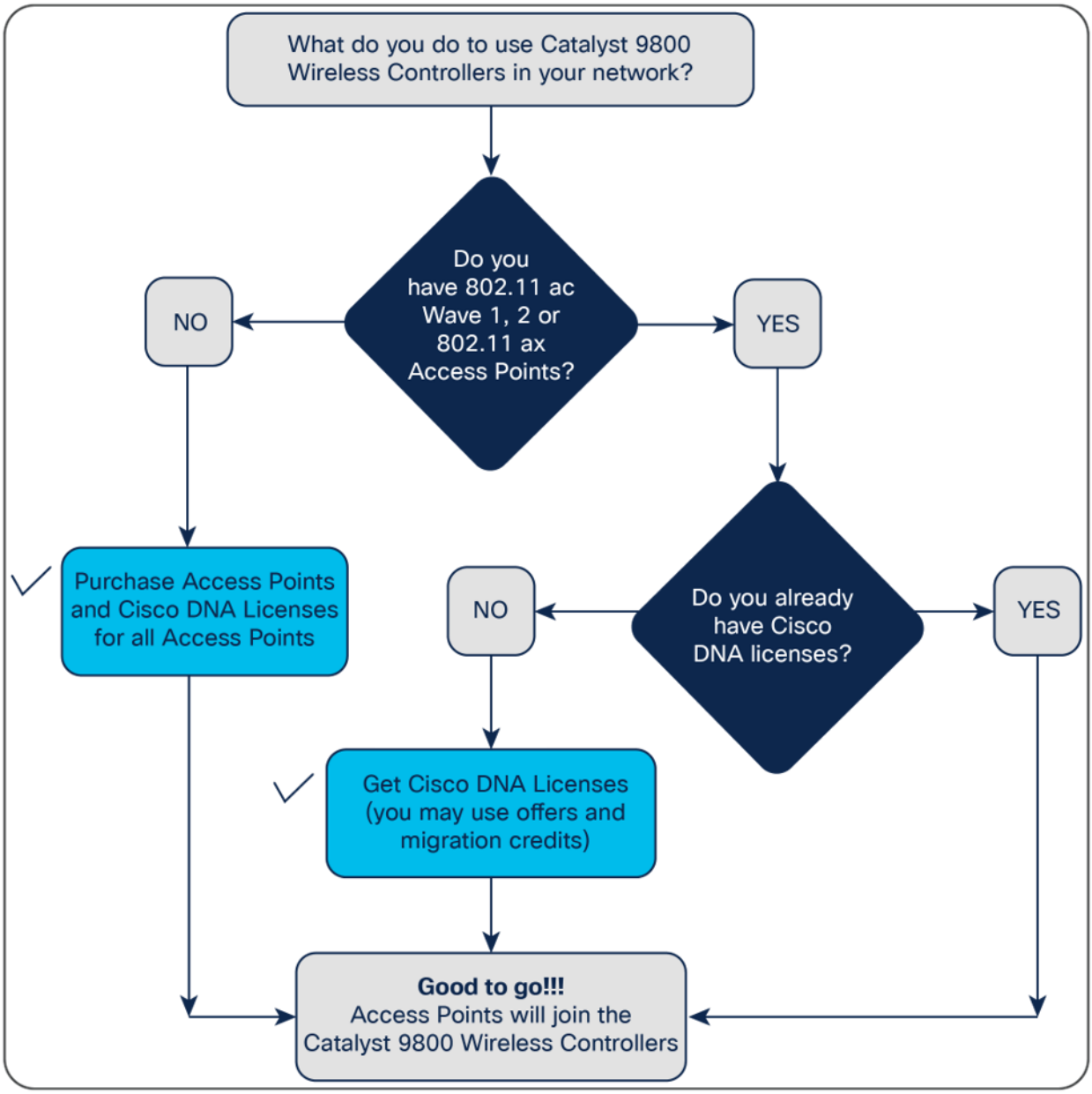


Figure 7.
Determining license requirements for access points connecting to Cisco Catalyst 9800 Series Wireless Controllers

Access points connecting to the Cisco Catalyst 9800 Series have new and simplified software subscription packages.

They can support both tiers of Cisco DNA software: Cisco DNA Essentials and Cisco DNA Advantage.

Cisco DNA software subscriptions provide Cisco innovations on the access point. They also include perpetual Network Essentials and Network Advantage licensing options, which cover wireless fundamentals such as 802.1X authentication, QoS, and PnP; telemetry and visibility; and single sign-on, as well as security controls.

Cisco DNA subscription software has to be purchased for a 3-, 5-, or 7-year subscription term. Upon expiration of the subscription, the Cisco DNA features will expire, whereas the Network Essentials and Network Advantage features will remain.

© 2023 Cisco and/or its affiliates. All rights reserved.

For the full feature list of Cisco DNA Software, including the perpetual Network Essentials and Network advantage, please see the feature matrix: https://www.cisco.com/c/m/en_us/products/software/dna-subscription-wireless/en-sw-sub-matrix-wireless.html?oid=porew018984.

Two modes of licensing are available:

- Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more convenient way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure- you control what users can access. With Smart Licensing you get:
  - Easy Activation: Smart licensing establishes a pool of software licenses that can be used across the entire organization-no more PAKs (Product Activation Keys).
  - Unified Management: Cisco License Central (CLC) provides a complete view into all of your Cisco Products and services in an easy-to-use portal, so you always know what you have and what you are using.
  - License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

    To use Smart Licensing, you must first set up a Smart Account on Cisco License Central.

    For a more detailed overview on Cisco Licensing, visit the Licensing Hub.
- Specific License Reservation (SLR) is a feature used in highly secure networks. It provides a method for customers to deploy a software license on a device (product instance) without communicating usage information to Cisco. There is no communication with Cisco or a satellite. The licenses are reserved for every controller. It is node-based licensing.

Four levels of license are supported on the **Cisco Catalyst 9800 Series Wireless Controllers.** The controllers can be configured to function at any one of the four levels.

- Cisco DNA Essentials: At this level the Cisco DNA Essentials feature set will be supported.
- Cisco DNA Advantage: At this level the Cisco DNA Advantage feature set will be supported.
- NE: At this level the Network Essentials feature set will be supported. This is available with Cisco DNA Essentials.
- NA: At this level the Network Advantage feature set will be supported. This is available with Cisco DNA Advantage.

For customers who purchase Cisco DNA Essentials, Network Essentials will be supported and will continue to function even after term expiration. And for customers who purchase Cisco DNA Advantage, Network Advantage will be supported and will continue to function even after term expiration.

Initial bootup of the controller will be at the Cisco DNA Advantage level.

For questions, contact the Cisco Catalyst 9800 Series Wireless Controllers Licensing mailer group at ask-catalyst9800licensing

The Cisco Catalyst 9800-L Wireless Controller has enhanced capability to increase performance through a Performance license. This Performance license allows customers to connect with 500 access points and 10,000 clients and gives a higher throughput.

© 2023 Cisco and/or its affiliates. All rights reserved.

Table 9. Comparison of the 9800-L with and without the Performance license

• Features	• 9800-L	• 9800-L with Performance License
• APs supported	• 250	• 500
• Clients supported	• 5000	• 10,000
• Throughput with IMIX	• 5 Gbps	• 5 Gbps
• Throughput without IMIX	• 5 Gbps	• 10 Gbps*

* With 1374-byte packet size

- Customer will have an option to select this Performance license while buying the 9800-L wireless controller or can order as spare.
- The Performance license is a perpetual license that is separate from the Cisco DNA license. They are also tracked by Smart Account.
- For High Availability deployments, Performance licenses must be brought on both controllers in the HA pair.

Managing licenses with Smart Accounts

Creating Smart Accounts by using the Cisco Smart Software Manager (SSM) enables you to order devices and licensing packages and also manage your software licenses from a centralized website. You can set up the Smart Account to receive daily email alerts and to be notified of expiring add-on licenses that you want to renew. A Smart Account is mandatory for Cisco Catalyst 9800 Series controllers. For more information on Smart Accounts, refer to https://www.cisco.com/go/smartaccounts.

Warranty

Find warranty information on Cisco.com at the Product Warranties page.

Cisco 1-year limited hardware warranty terms

The following are terms applicable to your hardware warranty. Your embedded software is subject to the Cisco General Terms and/or any Supplemental General Terms or specific software warranty terms for additional software products loaded on the device.

Duration of hardware warranty: One (1) year

Replacement, repair, or refund procedure for hardware: Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of the RMA request. Actual delivery times may vary depending on customer location.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

© 2023 Cisco and/or its affiliates. All rights reserved.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Table 10. Links to sustainability information

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance
Sustainability inquiries	Contact: csr_inquiries@cisco.com

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Ordering information

Table 11. Ordering information

Type	PID	Description
Controller	C9800-L-F-K9	Cisco Catalyst 9800-L (Fiber Uplink) Wireless Controller
	C9800-L-C-K9	Cisco Catalyst 9800-L (Copper Uplink) Wireless Controller
	LIC-C9800-DTLS-K9	Cisco Catalyst 9800 Series Wireless Controller DTLS License
	LIC-C9800L-PERF	Cisco C9800 Series Wireless Controller upgrade license
Accessories, spares	C9800L-RMNT=	Cisco Catalyst 9800 Series Wireless Controller Rack Mount Bracket
	C9800-AC-110W=	Cisco Catalyst Wireless Controller 110W AC Power Supply
	LIC-C9800L-PERF=	Cisco C9800 Series Wireless Controller upgrade license-Spare

© 2023 Cisco and/or its affiliates. All rights reserved.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation, and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services, and complementary third-party equipment in easy, predictable payments. Learn more.

© 2023 Cisco and/or its affiliates. All rights reserved.

Document history

New or Revised Topic	Described In	Date
SFPs supported – Revamped it completely with additional SFPs info for both copper and fiber versions of 9800L	SFPs supported	December 12, 2022
Changed the part name for rack mount bracket	Ordering Information	December 12, 2022
Added support for WPA3	Security Standards	December 12, 2022

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 **https://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/go/trademarks. 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. (1110R)

Printed in USA C78-742434-09 07/26

© 2023 Cisco and/or its affiliates. All rights reserved.