Cisco Catalyst CW9800M Wireless Controller

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

Product overview	3
Features	5
Ports	8
Power	9
SFPs supported	10
Benefits	12
Specifications	14
Software requirements	19
Licensing	19
Ordering information	20
Warranty	20
Cisco environmental sustainability	21
Cisco Capital	21

© 2026 Cisco and/or its affiliates. All rights reserved.

Product overview

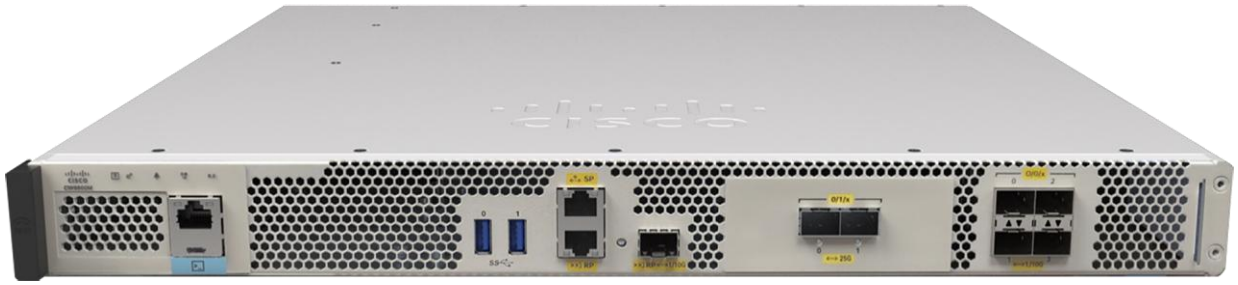


Figure 1.
Cisco Catalyst CW9800M wireless controller

Engineered from the ground up to be the most powerful and energy-efficient mid-sized wireless controller Cisco has ever developed, the Cisco Catalyst™ CW9800M Series wireless controller boasts up to a 53% increase in performance and consumes up to 18% less power compared to its predecessor. The Cisco Catalyst CW9800M has increased capacity to support 1000 more access points than the previous generation Catalyst 9800-40 while remaining a single-rack-unit design to save you space and provide greater flexibility in your datacenters. Together, these advancements, along with a host of innovative features, deliver a best-in-class wireless solution tailored to accommodate the dynamic and evolving needs of your organization.

The emergence of 6GHz Wi-Fi, along with the rise of new devices, cloud-based applications, smart workplaces, and IoT, calls for a new approach to network deployments, management, and troubleshooting. These new applications and increasing demands are met head-on by the powerful and efficient Cisco Catalyst CW9800 wireless controllers, which are engineered to address your most stringent needs and set the stage for the future.

The Cisco Catalyst CW9800 wireless controllers, built on Cisco IOS® XE, are specifically designed to thrive in dynamic environments, offering simplicity, security, and sustainability. In conjunction with the comprehensive suite of Cisco Catalyst solutions, the CW9800 wireless controllers deliver an unmatched wireless experience, catering to the growing demands of your organization. By integrating these controllers with Cisco Catalyst Center, you can harness applied AI for analytics and insights, automate intricate tasks, and enhance troubleshooting efficiency—helping ensure optimal user experiences and enabling you to focus on your organization's wider strategic objectives.

The Cisco Catalyst CW9800M is a high-performance wireless controller with the ability to support up to 3000 access points and 32,000 clients with up to 50 Gbps of maximum throughput. Additionally, it has 4 x 1Gpbs/10Gbps, and 2 x 25Gbps uplinks available to meet high throughput demands of 6GHz wireless. The Cisco Catalyst CW9800M is feature rich with high-performance capabilities to power your business-critical operations and transform user experiences:

© 2026 Cisco and/or its affiliates. All rights reserved.

- High availability and seamless software updates, enabled by hot patching, keep your clients and services always on in planned and unplanned events.
- Secure the airwaves, devices, and users with the Cisco Catalyst CW9800M. Wireless infrastructure becomes the strongest first line of defense with Cisco® Encrypted Traffic Analytics (ETA) and Software-Defined Access (SD-Access). Additionally, because the Cisco Catalyst CW9800M controllers are designed for Wi-Fi Protected Access 3 (WPA3) and beyond, security is front and center. This includes Secure Boot, runtime defenses, image signing, integrity verification, and hardware authenticity. The Catalyst CW9800M also supports hardware cryptographic offload to enable advanced encryption without any performance degradation.
- Built on a modular operating system, the CW9800M features open and programmable APIs that enable automation of day-0 to day-N network operations. Model-driven streaming telemetry provides deep insights into the health of your network and clients.
- Cisco User Defined Network Plus, 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 Plus provides advanced control, allowing each user to choose who can connect to their network.
- The CW9800 wireless controllers offer support for application hosting, enabling you to reduce your dependence on IoT overlay networks and consequently save on both CapEx and OpEx. With this feature, you can upload, deploy, and manage IOx applications directly on your Catalyst access points. It also provides third-party developers with the capability to create and run containerized applications using Docker, with access to designated CW9800 resources. This integration facilitates streamlined operations and enhances the overall efficiency of your network infrastructure.
- With Cloud Monitoring for Catalyst Wireless, you get a unified view of your Cisco infrastructure to help with troubleshooting including root cause analysis of network and client issues. Cloud monitoring is delivered through the Meraki dashboard, included in DNA Essentials and Advantage, and gives the ability to ensure the delivery of services while maximizing network performance and uptime. Additionally, because its cloud based, you access it anywhere. And best of all, it utilizes your existing hardware without the need for an immediate upgrade. Cloud monitoring for CW9800 wireless controllers will be available in a future software release.
- With Cisco In-Service Software Upgrade (ISSU), network downtime during a software update or upgrade is a thing of the past. ISSU performs 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Feature highlights

The Catalyst CW9800M boasts a fully programmable multicore network processor that improves access point scale by up to 50%, performance by up to 53%, and energy efficiency by 18% when compared to the Cisco Catalyst 9800-40. The CW9800M offers both RJ-45 and Small Form-Factor Pluggable (SFP) High Availability (HA) ports giving you the option of either 1Gbps or 10Gbps, depending on your requirements. Additionally, the CW9800M, supports 1000 more APs than the C9800-40 and in turn, 1000 more policy tags and site tags. This capability helps ensure greater flexibility and efficiency in managing expanding network environments with a more capable controller.

Features

Table 1. Key features

Metric	Value
Maximum number of access points	3000
Maximum number of clients	32,000
Maximum throughput	Up to 50 Gbps
Maximum WLANs	4096
Maximum VLANs	4096
Maximum site tags	3000
Maximum Flex APs per site	300
Maximum policy tags	3000
Maximum RF tags	3000
Maximum RF profiles	6000
Maximum policy profiles	1000
Maximum Flex profiles	3000
Fixed uplinks	4x 1/10Gbps + 2x 25Gbps
Redundant power supply	AC power supply
Maximum power consumption with modules	350W
Deployment modes	Centralized, Cisco FlexConnect®, and fabric wireless (SD-Access)
Form factor	1RU
License	Smart License enabled
Operating system	Cisco IOS XE

© 2026 Cisco and/or its affiliates. All rights reserved.

Metric	Value
Management	Integrated WebUI, Cisco Catalyst Center, and third party (open standards APIs)*
Policy engine	Cisco Identity Services Engine (ISE)*
Location platform	Cisco Spaces*
Access points	It supports Cisco Access Points from the following generations: Wi-Fi 5 Wave 2 (802.11ac Wave 2), Wi-Fi 6/6E (802.11ax), and Wi-Fi 7 (802.11be) Standard Power supported with Automated Frequency Coordination where applicable

*For information on compatibility, see the Compatibility Guide.

Always on

Seamless software updates enable faster resolution of critical issues, introduction of new access points with zero downtime, and flexible software upgrades. Stateful switchover (SSO) with 1:1 active standby and N+1 redundancy keeps your network, services, and clients always on, even in unplanned events. 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.

Secure

Secure airwaves, devices, and users with the Cisco Catalyst CW9800 wireless controller. Wireless infrastructure becomes the strongest first line of defense with ETA and SD-Access. The controller comes with built-in security: Secure Boot, runtime defenses, image signing, integrity verification, and hardware authenticity.

Open and programmable

The 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.

Details



Figure 2.
CW9800M

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 2. Physical dimensions

Dimension	Value
Width	17.3 inches (43.94 cm)
Depth	18.4 inches (46.74 cm)
Height	1.73 inches (4.39 cm)
Weight	20.5 lb (9.3 kg)

Front panel



Figure 3.
CW9800M Front panel

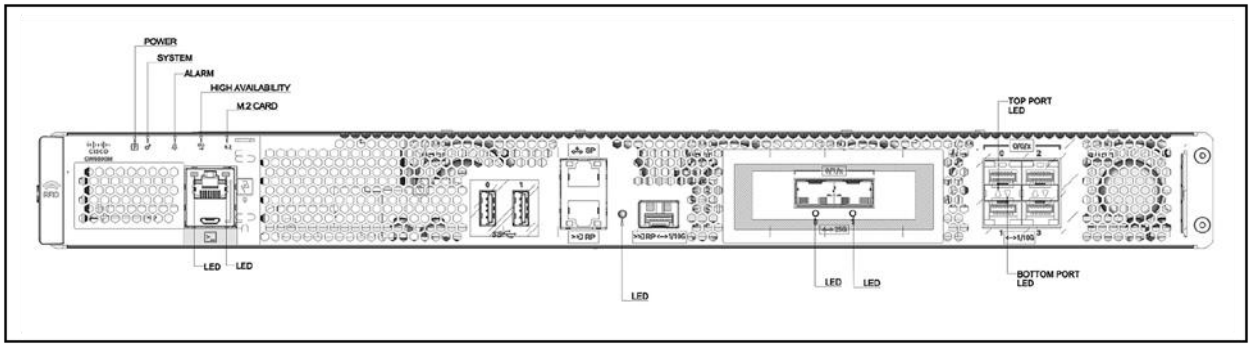


Figure 4.
CW9800M Front panel components

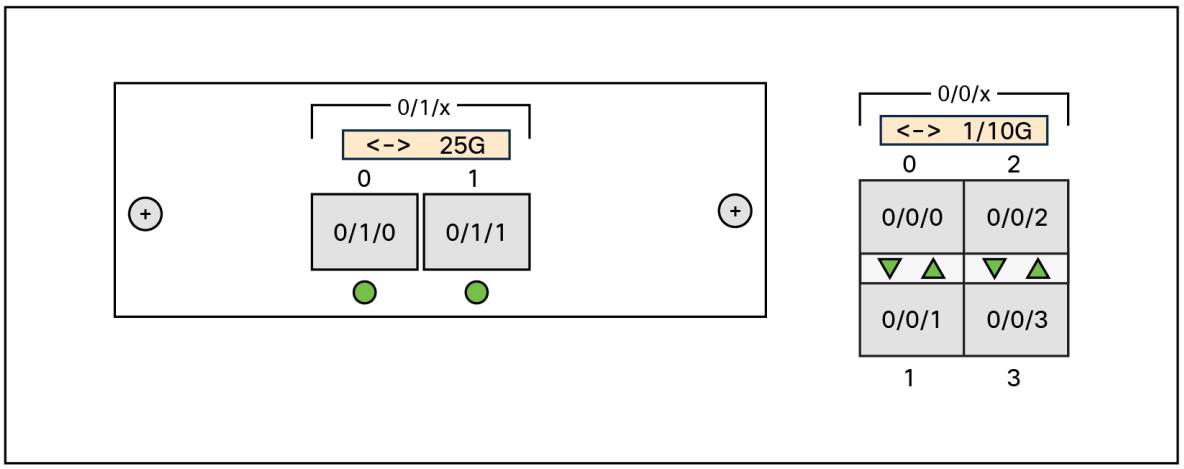


Figure 5.
CW9800M Uplinks

© 2026 Cisco and/or its affiliates. All rights reserved.

Ports

Table 3. Ports and their purposes

Port	Purpose
1x RJ-45 console port	Console port for out-of-band management
1x USB 3.0 console port	Console port for out-of-band management
2x USB 3.0 ports	USB 3.0 ports for plugging in external memory
1x RJ-45 management port	Management port for out-of-band management. Also known as the service port
1x RJ-45 redundancy port	Redundancy port used for SSO
1x SFP 10 Gbps Ethernet redundancy port	Redundancy port used for SSO; works with Cisco supported SFPs for RP port
Fixed uplink ports	4 x 1/10 Gbps SFP+ 2 x 25 Gbps SFP+

Front panel LEDs

Table 4. Front panel LEDs

LED	Color	Function
Power **PWR**	Green	Green if all power rails are within spec
STATUS **SYS**	Green	On: IOS boot is complete Blinking: IOS boot is in progress
	Amber	On: System crash Blinking: Secure Boot failure Off: ROMMON boot
ALARM **ALM**	Green	On: ROMMON boot is complete Blinking: System upgrade in progress
	Amber	On: ROMMON boot and SYSTEM bootup Blinking: Temperature error and secure boot failure
HIGH AVAILABILITY **HA**	Green	On: HA active Blinking: HA standby hot
	Amber	Slow blink: Booted with HA standby cold Fast blink: HA maintenance

© 2026 Cisco and/or its affiliates. All rights reserved.

LED	Color	Function
USB CON ENABLED **EN**	Green	When lit, USB console is enabled (RJ-45 console is disabled)
10/100/1000 RJ45 I/F **LINK**	Green	Solid green indicates link
10/100/1000 RJ45 I/F **ACTIVITY**	Green	Flashing green indicates activity
SSD Activity **SSD**	Green	Indicates active use of the hard disk SSD memory devices in the unit

Rear panel



Figure 6.
Rear panel

- The chassis has a front-to-rear airflow.
- Four internal fans draw cooling air in through the front of the chassis and across the internal components to maintain an acceptable operating temperature.
- The fans are located at the rear of the chassis.
- The fans are numbered from 0 to 3, right to left.

Power

The CW9800M controller ships with a single AC power supply unit.

The Power Entry Module (PEM) provides redundant power to the system, and the CW9800M can operate continuously with only a single PEM installed. The PEMs are hot-swappable, and replacement of a single PEM can be made without power interruption to the system. All external connections to the PEMs are made from the rear panel of the chassis, and they are removed or inserted from the rear. The main power switch for the unit is located directly next to the PEMs on the rear of the chassis.

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 5. Power supply options

Power supply condition	Green (OK) LED status	Amber (Fail) LED status
No AC power to all power supplies	Off	Off
Power supply failure (includes over voltage, over current, over temperature, and fan failure)	Off	Red for power supply failure Amber for fan failure
Power supply warning events in which the power supply continues to operate (high temperature, high power, and slow fan)	Off	1 Hz blinking

Note: Redundancy is supported with the same power supply types.

SFPs supported

- All 1, 10, and 25Gbps ports can be configured independently.
- Online Insertion and Removal (OIR) for SFP, SFP+, and SFP28.
- Modules are hot-swappable.

Table 6. SFPs supported

Type	Modules supported
Small Form-Factor Pluggable (SFP)	GLC-BX-D GLC-BX-U GLC-EX-SMD GLC-LH-SMD GLC-SX-MMD GLC-TE GLC-ZX-SMD
SFP (for RP ports)	GLC-SX-MMD GLC-LH-SMD SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S
Enhanced SFP (SFP+)	Finisar-LR (FTLX1471D3BCL) Finisar-SR (FTLX8574D3BC) SFP-10G-AOC10M SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M

© 2026 Cisco and/or its affiliates. All rights reserved.

Type	Modules supported
	SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-BXD-I SFP-10G-BXU-I SFP-10G-ER SFP-10G-LR SFP-10G-LR-S SFP-10G-LR-X SFP-10G-SR SFP-10G-SR-S SFP-10G-T-X (17.18.3+) SFP-H10GB-ACU10M SFP-H10GB-ACU7M SFP-H10GB-CU1-5M SFP-H10GB-CU1M SFP-H10GB-CU2-5M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M
SFP28	SFP-10/25G-CSR-S SFP-10/25G-LR-S SFP-25G-AOC10M SFP-25G-AOC1M SFP-25G-AOC2M SFP-25G-AOC3M SFP-25G-AOC5M SFP-25G-AOC7M SFP-25G-SR-S SFP-H25G-CU1M SFP-H25G-CU5M

© 2026 Cisco and/or its affiliates. All rights reserved.

Benefits

Cisco IOS XE 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 a device lifecycle.

- **Automated device provisioning:** This is the ability to automate the process of upgrading software images and installing configuration files on Cisco access points when they are being deployed in the network for the first time. Cisco provides turnkey solutions such as Plug and Play (PnP) that enable an effortless and automated deployment.
- **API-driven configuration:** Modern wireless controllers such the Cisco Catalyst CW9800M wireless controller supports a wide range of automation features and provide robust open APIs over Network Configuration Protocol (NETCONF) 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 wireless controller 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.

Always on

- **High availability:** Stateful switchover with 1:1 active standby and N+1 redundancy keeps your network, services, and clients always on, even in unplanned events.
- **Software maintenance upgrades (SMUs) with hot patching:** Patching allows for a patch to be installed as a bug fix without bringing down the entire network and eliminates 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's 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 Catalyst CW9800M wireless controller comes equipped 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

- Standby monitoring of Catalyst CW9800M wireless controller in high-availability mode enables you to monitor the health of the system on a standby controller in a high-availability pair using programmatic interfaces (NETCONF/YANG, RESTCONF) and Command-Line Interfaces (CLIs) without going through the active controller. For more details refer to the technical documentation.
- **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 CW9800 controller receives the new software that is pushed via the active CW9800 controller. The backup controller becomes active and takes over your network, while your previously active controller turns into a backup 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.

Security

- **Encrypted Traffic Analytics (ETA):** ETA is a unique capability for identifying malware in encrypted traffic coming from the access layer. Since more and more traffic is being encrypted, the visibility this feature provides related to threat detection is critical for keeping your network secure at different layers.
- **Trustworthy systems:** Cisco Trust Anchor Technologies provide a highly secure foundation for Cisco products. With the Catalyst CW9800M, these trustworthy systems help assure hardware and software authenticity 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 hardware solution uniquely identifies 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 Catalyst Center. A fully integrated stack for the WIPS solution includes Cisco Catalyst Center, a Cisco Catalyst 9800 series controller, Wave 2 or Cisco Catalyst 9100 Access Point. This new architecture provides improved detection and security, simplicity, and ease of use, and fewer false positive alarms.

Flexible NetFlow

- **Flexible NetFlow (FNF):** Cisco IOS 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, with up to 1400 predefined and well-known application signatures and up to 150 encrypted applications on the Catalyst CW9800M. Some of the most popular applications included are Skype, Office 365, Microsoft

© 2026 Cisco and/or its affiliates. All rights reserved.

Lync, Webex by Cisco, 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 Secure Network Analytics, or any compliant third-party tool.

Quality of service

- **Superior Quality of Service (QoS):** QoS technologies are 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 Catalyst CW9800M consists of classification of traffic based on packet data as well as application recognition and traffic control actions such as dropping, marking and policing. A modular QoS command-line framework provides consistent platform-independent and flexible configuration behavior. The CW9800M also supports policies at two levels of target: BSSID as well as client. Policy assignment can be granular down to the client level.

Smart operation

- **WebUI:** WebUI is an embedded GUI-based device-management tool that provides the ability to provision 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-0 and day-1 configuration and from then on monitor and troubleshoot the device without having to know how to use the CLI.

Specifications

Table 7. 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 Wave 2, 802.11ax, 802.11be
Wired, switching, and routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q VLAN tagging, IEEE 802.1AX Link Aggregation
Data standards	• RFC 768 User Datagram Protocol (UDP) • RFC 791 IP • RFC 2460 IPv6 • RFC 792 Internet Control Message Protocol (ICMP) • RFC 793 TCP • RFC 826 Address Resolution Protocol (ARP) • RFC 1122 Requirements for Internet Hosts • RFC 1519 Classless Interdomain Routing (CIDR) • RFC 1542 Bootstrap Protocol (BOOTP) • RFC 2131 Dynamic Host Configuration Protocol (DHCP) • RFC 5415 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol • RFC 5416 CAPWAP Binding for 802.11
Security standards	• IEEE 802.11i (WPA2, RSN) • Wi-Fi Protected Access 3 (WPA3) • RFC 1321 MD5 Message-Digest Algorithm

© 2026 Cisco and/or its affiliates. All rights reserved.

Item	Specification
	• RFC 1851 Encapsulating Security Payload (ESP) Triple DES (3DES) 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 8446 TLS Protocol Version 1.3 • RFC 2407 Interpretation for Internet Security Association Key Management Protocol (ISAKMP) • RFC 2408 ISAKMP • RFC 2409 Internet Key Exchange (IKE) • RFC 2451 ESP CBC-Mode Cipher Algorithms • RFC 3280 Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile • RFC 4347 Datagram Transport Layer Security (DTLS) • RFC 5246 TLS Protocol Version 1.2 • RFC 8446 TLS Protocol Version 1.3
Encryption standards	• Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with CBC 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

© 2026 Cisco and/or its affiliates. All rights reserved.

Item	Specification
Authentication, Authorization, and Accounting (AAA)	• IEEE 802.1X • RFC 2548 Microsoft Vendor-Specific RADIUS Attributes • RFC 2716 Point-to-Point Protocol (PPP) Extensible Authentication Protocol (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 standards	• 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 Trivial File Transfer Protocol (TFTP) • RFC 1643 Ethernet MIB • RFC 2030 Simple Network Time Protocol (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 Remote Monitoring (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 • RFC 6241 NETCONF • RFC 6242 NETCONF over SSH • RFC 5277 NETCONF event notifications

© 2026 Cisco and/or its affiliates. All rights reserved.

Item	Specification
	• 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 • SNMP • NETCONF
Hard Disk Drives (HDD)	• SATA Solid-State Drive (SSD) • 240 GB of memory
Environmental conditions supported	Operating temperature: • Normal: 0° to 40° C (32° to 104° F) • Short term:0° to 50° C (32° to 122° F) Nonoperating temperature: • -40° to 65° C (-104° to 149° F) Operating humidity: • Normal: 10% to 90% noncondensing • Short term: 5% to 90% noncondensing Nonoperating temperature humidity: • 5% to 93% at 82° F (28° C) Operating altitude: • Appliance operating: 0 to 3000 m (0 to 10,000 ft) • Appliance nonoperating: 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 with AC PEM • DC input range: -40 to -72 VDC with DC PEM Maximum power with modules: 350W Heat dissipation: 1194 BTU/hr Sound power level measure: • Sound power level is 73.5 (dBA) under normal operating conditions

© 2026 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 EMC – Emissions: • EN61000-3-2 Power Line Harmonics (EMI-3) • EN61000-3-3 Voltage Changes, Fluctuations, and Flicker (EMI-3) EMC – Immunity: • IEC/EN61000-4-2 Electrostatic Discharge Immunity • IEC/EN61000-4-3 Radiated Immunity • IEC/EN61000-4-4 EFT-B Immunity (AC Power Leads) • IEC/EN61000-4-4 EFT-B Immunity (DC Power Leads) • IEC/EN61000-4-4 EFT-B Immunity (Signal Leads) • IEC/EN61000-4-5 Surge AC Port • IEC/EN61000-4-5 Surge DC Port • IEC/EN61000-4-5 Surge Signal Port • IEC/EN61000-4-6 Immunity to Conducted Disturbances • IEC/EN61000-4-8 Power Frequency Magnetic Field Immunity • IEC/EN61000-4-11 Voltage Dips, Short Interruptions, and Voltage Variations • K35 (EMI-2) EMC (ETSI/EN) • EN 300 386 Telecommunications Network Equipment (EMC) (EMC-3) • EN55022 Information Technology Equipment (Emissions) • EN55024/CISPR 24 Information Technology Equipment (Immunity) • EN50082-1/EN61000-6-1 Generic Immunity Standard (EMC-4)

© 2026 Cisco and/or its affiliates. All rights reserved.

Software requirements

The Catalyst CW9800M runs on Cisco IOS XE Software Release 17.14.1 or later.

Licensing

No licenses are required to boot up a CW9800 wireless controller. However, to connect any access points to the controller, either a Cisco DNA software subscription or Cisco Networking subscription is required. To be entitled to connect to a CW9800 controller, each access point requires a subscription license. For more details on Cisco Networking Subscription for Wi-Fi 7 access points, read the datasheet: https://www.cisco.com/c/en/us/products/collateral/networking/software/networking-subscription-ds.html

For the full feature list of Cisco DNA Software for previous-gen access points, 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.

  Four levels of license are supported on the **Cisco Catalyst CW9800 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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@cisco.com.

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 the Catalyst CW9800 controllers. For more information on Smart Accounts, refer to https://www.cisco.com/go/smartaccounts.

Ordering information

Table 8. Ordering information

Type	Product ID	Description
Wireless controller	CW9800M	Cisco Catalyst CW9800M wireless controller
Accessories, spares	PWR-CH1-750WACR	Cisco Catalyst wireless controller 750W AC Power Supply
	PWR-CH1-750WACR	Cisco CW9800 750W AC power supply
	PWR-CH1-950WDCR	Cisco CW9800 950W DC power supply
	PWR-750WACR-RED	Cisco CW9800 750W AC Redundant power supply

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 EULA and/or any SEULA 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 Return Materials Authorization (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.

© 2026 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 "Environmental Sustainability" section of the CSR Report) are provided in the following table.

Table 9. 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.

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 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.

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 C78-4269840-04 09/26

© 2026 Cisco and/or its affiliates. All rights reserved.