Cisco Catalyst 9800-CL Wireless Controller for Cloud

Built from the ground up for intent-based networking

Contents

Product overview

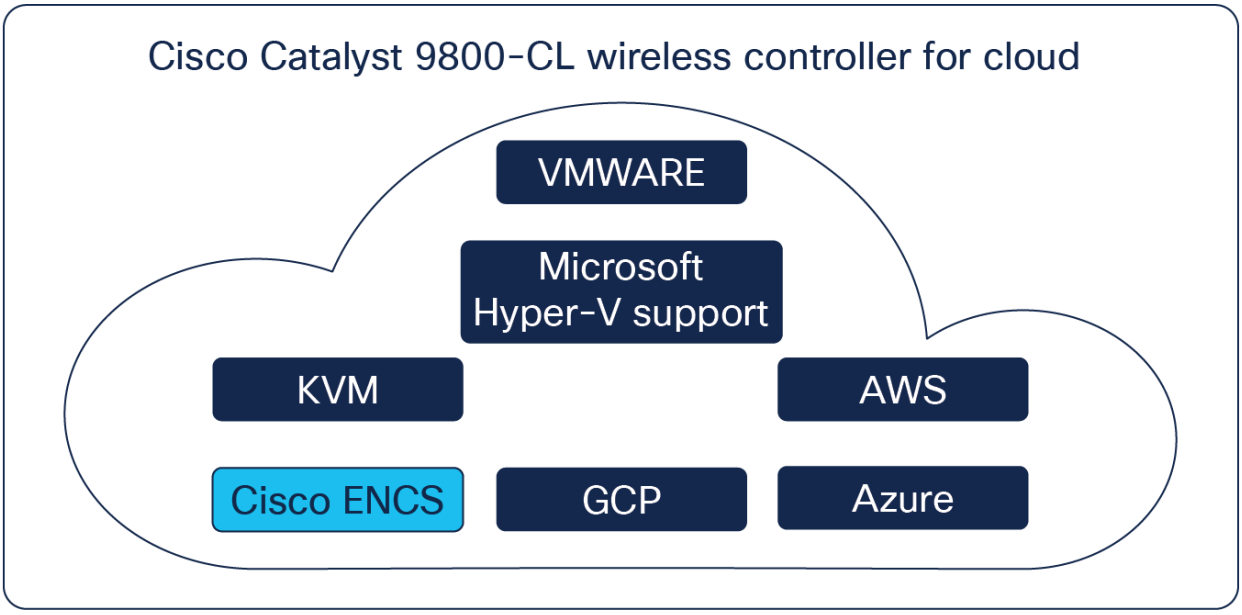

Figure 1.
Examples of compatible clouds

Built from the ground-up for the intent-based network, Cisco Catalyst 9800 Series Wireless Controllers are Cisco IOS XE based and integrate the RF excellence of Cisco Aironet access points, creating a best-in-class wireless experience for your evolving and growing organization. The 9800 Series is built on an open and programmable architecture with built-in security, streaming telemetry, and rich analytics.

The Cisco Catalyst 9800 Series Wireless Controllers are built on the three pillars of network excellence -always on, secure, and deployed anywhere - which strengthen the network by providing the best wireless experience without compromise, while saving time and money.

The Cisco Catalyst 9800-CL is the next generation of enterprise-class wireless controllers for cloud, with seamless software updates for distributed branches and midsize campuses to large enterprises and service providers.

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

- 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** air, devices, and users with the Cisco Catalyst 9800-CL. Wireless infrastructure becomes the strongest first line of defense with Cisco Encrypted Traffic Analytics (ETA) and Software-Defined Access (SD-Access). The controller comes with built-in security: runtime defenses, image signing and integrity verification.
- **Deploy anywhere** to enable wireless connectivity everywhere. Whether in a public or private cloud, the Cisco Catalyst 9800-CL best meets your organization's needs.
- Built on a modular operating system, the 9800-CL 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, 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.
- 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.

Cisco Catalyst 9800-CL for private cloud

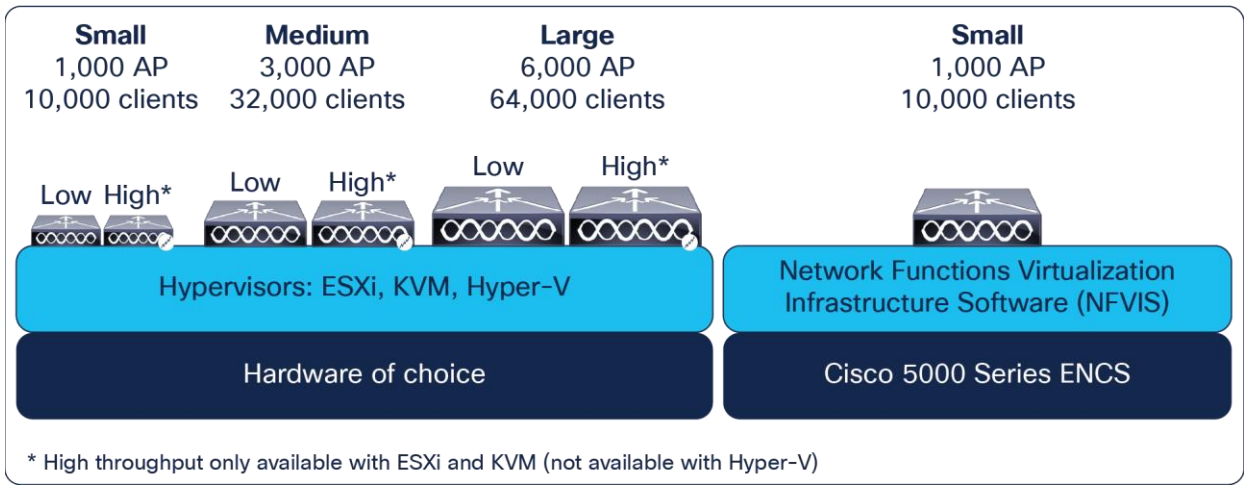

Figure 2.
Cisco Catalyst 9800-CL for private cloud

Key highlights

- VMware ESXi, KVM, Hyper-V, and Cisco NFVIS (on ENCS) supported
- Supports centralized, Cisco FlexConnect, mesh, and fabric (SD-Access) deployment modes
- Multiple scale and throughput* profiles with a single deployment package to best meet your organization's needs
    - **Small (low / high throughput):** Designed for distributed branches and small campuses supporting up to 1000 Access Points (APs) and 10,000 clients
    - **Medium (low / high throughput):** Designed for medium-sized campuses supporting up to 3000 APs and 32,000 clients
    - **Large (low / high throughput):** Designed for large enterprises and service providers supporting up to 6000 APs and 64,000 clients
- One deployment package for all the scale templates. Pick the deployment size and the throughput profile when you instantiate the Virtual Machine (VM)
- Supports up to 2.1 Gbps of throughput in a centralized wireless deployment (low-throughput profile without SR-IOV)
- With a high (enhanced) throughput profile, up to 5 Gbps can be reached on ESXi and KVM with the right set of network cards and resources (SR-IOV-enabled NIC card)
- An intuitive bootstrap wizard is available during the VM instantiation to boot the wireless controller with recommended parameters
- Optimize your branch by deploying the 9800-CL as a virtual machine on the Cisco 5000 Series Enterprise Network Compute System (ENCS) running Cisco NFVIS

* High-throughput profiles are only available with ESXi and KVM hypervisors.

Cisco Catalyst 9800-CL for public cloud

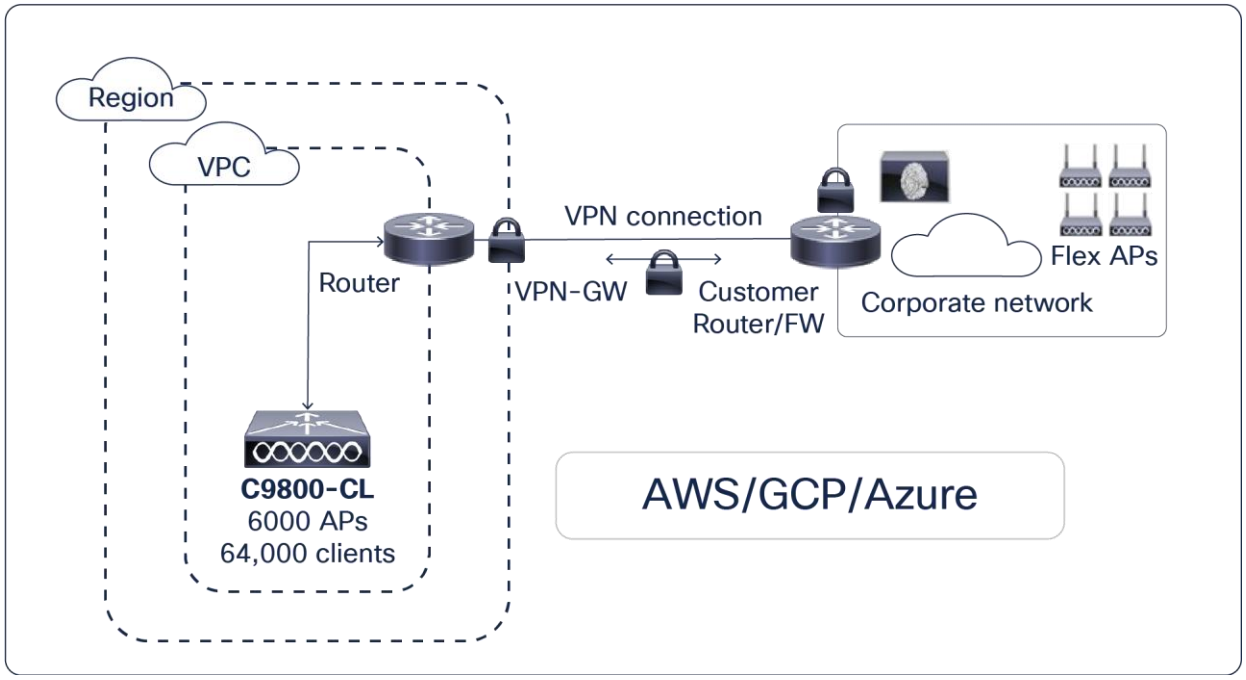

Figure 3.
Cisco Catalyst 9800-CL for public cloud

Key highlights

- Cisco Catalyst 9800-CL is available as an Infrastructure-as-a-Service (IaaS) solution on the Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure (Azure) Marketplaces
- Supported with managed VPN deployment mode till 17.7:
  - The 9800-CL should be instantiated within a Virtual Private Cloud (VPC)
  - A VPN tunnel has to be established from the customer site to AWS, GCP or Azure to enable communication between the Cisco access point and 9800-CL wireless controller
- Supported with Public IP for AP onboarding from 17.8
- Cisco FlexConnect central authentication and local switching
- Available on AWS GovCloud
- Supports up to 6000 access points and 64,000 clients
- Deploy a wireless controller instance in AWS using cloud-formation templates provided by Cisco (recommended) or by manually using the EC2 console
- Deploy a wireless controller in GCP and Azure using the guided workflow in the marketplace

Features

Table 1. Key features

Metric	Value
Maximum number of access points	Up to 6000
Maximum number of clients	64,000
Maximum throughput (low profile without SR-IOV)*	2.1 Gbps
Maximum throughput (high profile with SR-IOV)**	5 Gbps
Maximum WLANs	4096
Maximum VLANs	4096
Deployment modes	Centralized, Cisco FlexConnect, and fabric wireless (SD-Access)
License	Smart License enabled
Operating system	Cisco IOS XE Software
Management	Cisco DNA Center, Cisco Prime Infrastructure, integrated WebUI, and third party (open standards APIs)***
Interoperability	AireOS-based controllers***
Policy engine	Cisco Identity Services Engine***
Location platform	Cisco Connected Mobile Experiences (CMX), Cisco Spaces***
Access points	Aironet 802.11ac Wave 1 and Wave 2, Cisco Catalyst 9100 802.11ax access points

* For traffic with large (1374 bytes) packet size

** A high-throughput profile is supported on ESXi and KVM hypervisors only. Throughput numbers are with SR-IOV-enabled NICs.

*** For information on compatibility, visit: 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.

Secure

Secure air, devices, and users with the Cisco Catalyst 9800-CL. Wireless infrastructure becomes the strongest first line of defense with ETA and SD-Access. The controllers come with built-in security: runtime defenses, image signing, and integrity verification. 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.

Deploy anywhere

Whether in a public or private cloud, the Cisco Catalyst 9800-CL wireless controllers can be deployed anywhere for wireless everywhere. The 9800-CL meets the needs of your branch and campus network deployments.

Open and programmable

The controllers are 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.

Key specifications

Table 2. Key specifications

Metric	Private cloud				Public cloud		
	Ultra-low	**Small**	**Medium**	**Large**	**Small**	**Medium**	**Large**
Deployment modes supported	Cisco FlexConnect (local switching only), fabric (SD-Access)	Centralized, Cisco FlexConnect, fabric (SD-Access)	Centralized, Cisco FlexConnect, fabric (SD-Access)	Centralized, Cisco FlexConnect, fabric (SD-Access)	Cisco FlexConnect (local switching only)	Cisco FlexConnect (local switching only)	Cisco FlexConnect (local switching only)
vCPUs required* (Hyperthreading is not supported)	2	4 – low throughput 7 – high throughput	6 – low throughput 9 – high throughput	10 – low throughput 13 – high throughput	4 (required) 4 (available in public cloud)	6 (required) 8 (available in public cloud)	10 (required) 16 (available in public cloud)
Preferred mode for high throughput*	All traffic will be locally switched	SR-IOV	SR-IOV	SR-IOV	All traffic will be locally switched	All traffic will be locally switched	All traffic will be locally switched
NIC needed for SR-IOV	Intel x710 / Cisco Intel x710 adapter	Intel x710 / Cisco Intel x710 adapter	Intel x710 / Cisco Intel x710 adapter	Intel x710 / Cisco Intel x710 adapter	All traffic will be locally switched	All traffic will be locally switched	All traffic will be locally switched
Drivers needed for SR-IOV	ESXi – i40en KVM – i40e	ESXi – i40en KVM – i40e	ESXi – i40en KVM – i40e	ESXi – i40en KVM – i40e	All traffic will be locally switched	All traffic will be locally switched	All traffic will be locally switched
RAM required (GB)	6	8	16	32	8	16	32
Recommended hard disk space (GB)***	16	16	16	16	16	16	16
Hypervisors and cloud providers supported	ESXi 6.0/6.5/6.7, KVM, Hyper-V, NFVIS	ESXi 6.0/6.5/6.7, KVM, Hyper-V, NFVIS	ESXi 6.0/6.5/6.7, KVM, Hyper-V, NFVIS	ESXi 6.0/6.5/6.7, KVM, Hyper-V, NFVIS	AWS, GCP, Azure	AWS, GCP, Azure	AWS, GCP, Azure

Metric	Private cloud				Public cloud		
Maximum number of access points	100	1000	3000	6000	1000	3000	6000
Maximum number of clients	1000	10,000	32,000	64,000	10,000	32,000	64,000
Maximum throughput (low profile without SR-IOV)	All traffic will be locally switched	2.1 Gbps**	2.1 Gbps**	2.1 Gbps**	All traffic will be locally switched	All traffic will be locally switched	All traffic will be locally switched
Maximum throughput (high profile with SR-IOV)	All traffic will be locally switched	5 Gbps	5 Gbps	5 Gbps	All traffic will be locally switched	All traffic will be locally switched	All traffic will be locally switched
Maximum WLANs	4096	4096	4096	4096	4096	4096	4096
Maximum VLANs	4096	4096	4096	4096	4096	4096	4096
Maximum site tags	100	1000	3000	6000	1000	3000	6000
Maximum APs per site	100	100	100	100	100	100	100
Maximum policy tags	100	1000	3000	6000	1000	3000	6000
Maximum RF tags	100	1000	3000	6000	1000	3000	6000
Maximum RF profiles	200	2000	6000	12,000	2000	6000	12,000
Maximum policy profiles	1000	1000	1000	1000	1000	1000	1000
Maximum Flex profiles	100	1000	3000	6000	1000	3000	6000
vNIC adapters	ESXi: VMXNET3, E1000E, E1000 KVM: VIRTIO Hyper-V: NetVSC	ESXi: VMXNET3, E1000E, E1000 KVM: VIRTIO Hyper-V: NetVSC	ESXi: VMXNET3, E1000E, E1000 KVM: VIRTIO Hyper-V: NetVSC	ESXi: VMXNET3, E1000E, E1000 KVM: VIRTIO Hyper-V: NetVSC	–	–	–
Virtual switch	ESXi: vSwitch KVM: OVS Linux Bridge (brctl) Hyper-V: Hyper-V	ESXi: vSwitch KVM: OVS Linux Bridge (brctl) Hyper-V: Hyper-V	ESXi: vSwitch KVM: OVS Linux Bridge (brctl) Hyper-V: Hyper-V	ESXi: vSwitch KVM: OVS Linux Bridge (brctl) Hyper-V: Hyper-V	–	–	–

Metric	Private cloud				Public cloud		
	Virtual Switch	Virtual Switch	Virtual Switch	Virtual Switch			
VMware vMotion[***]	Yes	Yes	Yes	Yes	–	–	–
VMware Snapshot[***]	Yes	Yes	Yes	Yes	–	–	–
VMware Distributed Resource Scheduler[****]	Yes	Yes	Yes	Yes	–	–	–
VMware NIC Teaming[****]	Yes	Yes	Yes	Yes	–	–	–
Hyper-V Checkpoint	Yes	Yes	Yes	Yes	–	–	–
Hyper-V NIC Teaming	Yes	Yes	Yes	Yes	–	–	–
High availability	N+1	SSO, N+1	SSO, N+1	SSO, N+1	N+1	N+1	N+1
Cisco DNA support	Automation, Assurance	Automation, Assurance	Automation, Assurance	Automation, Assurance	–	–	–
mDNS gateway	–	Yes	Yes	Yes	–	–	–
Anchor controller	–	Yes	Yes	Yes	–	–	–
Foreign controller	–	Yes	Yes	Yes	–	–	–
Rogue detection / aWIPS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Client IPv6 support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Infrastructure IPv6 support	Yes	Yes	Yes	Yes	No	No	No
AP on board to WLC with Public IP [*****]	-	-	-	-	Yes	Yes	Yes

[*] A high-throughput profile is supported on ESXi and KVM hypervisors only.

[**] For traffic with large (1374 bytes) packet size.

[***] vMotion, Snapshot not supported in HA mode. Cloning from snapshots not supported.

[****] vMotion, DRS, Snapshots, and vNIC Teaming not supported when SR-IOV mode is enabled.

[*****] Starting 17.8

****** IOS-XE 17.13.1 release onwards, minimum disk space requirement is changed to 32GB for all the vWLC variants to support app-hosting.

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 9800-CL Wireless Controller for Cloud support 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 a 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 and cold 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 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-CL Wireless Controller for Cloud 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.
- **Standby monitoring of Cisco Catalyst 9800 Wireless Controllers in High-Availability (HA) mode:** This enables monitoring of the health of the system on a standby controller in a HA pair using programmatic interfaces (NETCONF/YANG, RESTCONF) and CLIs without going through the active controller. For more details refer to 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 AP/client sessions are retained during the upgrade process.

With just a click, your network automatically upgrades to the newest software. Your backup Catalyst 9800 controller receives the new software that is pushed via the active 9800 controller. The backup 9800 controller becomes active controller 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.

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. This feature is supported on private cloud deployments only.
- **Cisco Wireless Intrusion Prevention System (WIPS):** WIPS offers advanced network security to detect, locate, mitigate, and contain any intrusion and threat on your wireless network. It can monitor and detect wireless network anomalies, unauthorized access, and RF attacks. A new dedicated classification engine for rogue and aWIPS built on Cisco DNA Center. A fully integrated stack for WIPS solution includes Cisco DNA Center, Cisco Catalyst 9800 controller, Wave2, and Catalyst 9100 Access Points. This new architecture provides improved detection and security, simplicity and ease of use, and a reduction in false-positive alarms.
- **Trustworthy systems:** Cisco Trust Anchor Technologies provide a highly secure foundation for Cisco products. With the Cisco Catalyst 9800-CL, these trustworthy systems help assure 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.

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 Cisco Catalyst 9800-CL. 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 secure 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, Stealthwatch, 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 Cisco Catalyst 9800-CL 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 9800-CL, 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 3. Specifications

Item	Specification
Wireless standards	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 1 and Wave 2, 802.11ax
Wired, switching, and routing standards	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

Item	Specification
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 Encapsulating Security Payload (ESP) Triple DES (3DES) Transform • RFC 2104 HMAC: Keyed-Hashing for Message Authentication • RFC 2246 TLS Protocol Version 1.0 • 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
Encryption standards	• Static Wired Equivalent Privacy (WEP) RC4 40, 104 and 128 bits • 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 • 802.1AE MACsec encryption
Authentication, Authorization, and Accounting (AAA) standards	• 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

Item	Specification
	• 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 • 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

Software requirements

The Cisco Catalyst 9800-CL Wireless Controller for Cloud runs on Cisco IOS XE Software version 16.10.1 or later. This software release includes all the features listed earlier in the Platform Benefits section.

Table 4. Minimum software requirements

Model	Description	Minimum software requirement
C9800-CL-K9	Cisco Catalyst 9800-CL Wireless Controller for Cloud	Cisco IOS XE Software Release 16.10.1 High-throughput profiles supported from Release 17.3.1 onward

Licensing

No licenses are required to boot up and use 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 entitled to connect to a Cisco Catalyst 9800 Series controller, each access point requires a Cisco DNA subscription license. An active Cisco DNA license provides embedded Cisco Software Support (SWSS) coverage for access points. To be entitled to Return Materials Authorization (RMA) for access point hardware, customers will need Cisco Smart Net Total Care Service. To get Technical Assistance Center (TAC) support, and OS upgrades and updates on 9800-CL controllers, customers will need to purchase Cisco Software Support Service (SWSS).

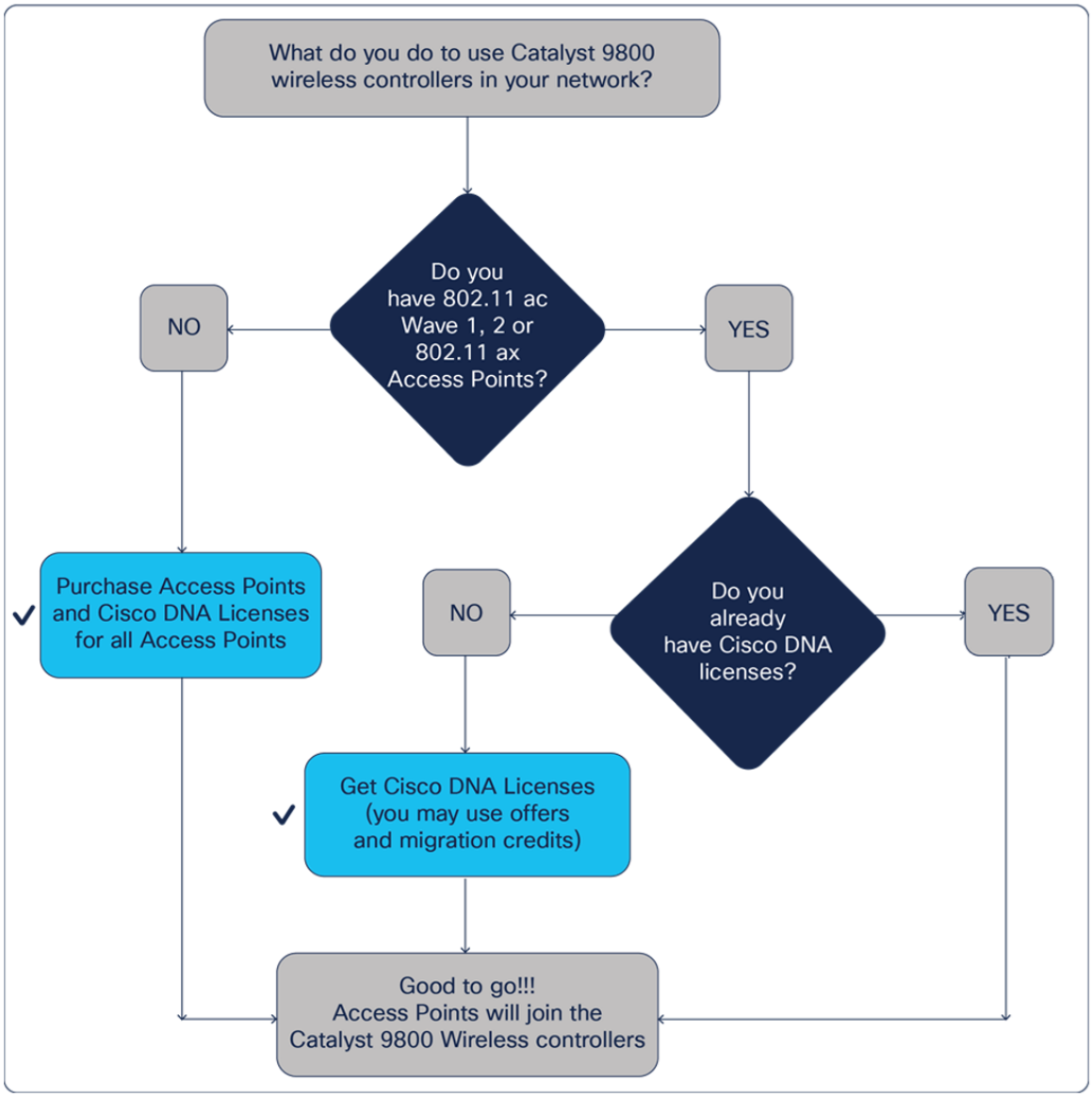

Figure 4.
Determining license requirements for access points connecting to Cisco Catalyst 9800 Series Wireless Controllers

APs connecting to Cisco Catalyst 9800 Series controllers 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 AP. 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.

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: My Cisco Entitlements (MCE) 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 Software Central (software.cisco.com).
  - For more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide
- 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.
- NA: At this level the Network Advantage feature set will be supported.

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.

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.

Note: If you are using a Cisco Catalyst 9800-CL Wireless Controller from or later than 17.7.1 release, you must complete RUM reporting and ensure that the ACK is made available on the product instance – at least once. This is to ensure that correct and up-to-date usage information is reflected in CSSM.

For more information, please visit: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-7/release-notes/rn-17-7-9800.html#Cisco_Concept.dita_36dcc319-36c4-4368-b1db-da5660b72211

Warranty

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

Your embedded software is subject to the Cisco General Terms (link available below) and/or any Supplemental General Terms or specific software warranty terms for additional software products loaded on the device.

Cisco environmental sustainabilityss

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 Table 5.

Table 5. 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 6. Ordering information

Type	Product ID	Description
Controller	**C9800-CL-K9**	Cisco Catalyst 9800-CL Wireless Controller for Cloud
	LIC-C9800-DTLS-K9	Cisco Catalyst 9800 Series Wireless Controller DTLS license

- Purchase the above SKU for software download and Cisco TAC support.
- The 9800-CL private cloud image for VMware ESXi, KVM, Hyper-V, and Cisco NFVIS on ENCS can be downloaded from software.cisco.com.
- The 9800-CL public cloud image for AWS can be subscribed and deployed from the AWS Marketplace.
- The 9800-CL public cloud image for GCP can be subscribed and deployed from the GCP Marketplace.
- The 9800-CL public cloud image for Azure can be subscribed and deployed from the Azure Marketplace.

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.

Document history

New or revised topic	Described In	Date
Cosmetic changes to various tables were made	Table 1, 2	November 15, 2018
Updated images were included	Image	November 15, 2018
Licensing information updated	Licensing	December xx, 2018
Cisco DNA Spaces name change	Updated product name to Cisco Spaces	10/18/22

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**.

Printed in USA C78-741546-13 11/24