

Wireless Education Profile

Cisco Catalyst 9800 Controllers

Cisco Validated Profile (CVP)

March 2021

Contents

- Profile introduction 3**
 - Security 3
 - Specialized services 3
 - Migration to IPv6 3
 - Mobility 3
 - High availability 3
 - Efficient network management 3
 - Performance and scalability 4
- Network profile 5**
 - Topology diagram 5
 - Hardware profile 6
 - Test environment 7
- Use case scenarios 8**
 - Test methodology 8
 - Use cases 8
- Appendix A 11**

Profile introduction

The Enterprise market segment can be divided into six broader verticals: Education/Large Enterprise, Healthcare, Retail, Service Provider, Financial, and Government. This document focuses on a typical Education deployment profile utilizing the Cisco next generation C9800 Wireless controller, and you can use it as a reference validation document for a University/Large Enterprise profile.

Education network environments combine the technology requirements of large enterprises with a specialized set of demands that includes security needs, enhanced network services, seamless mobility, network high availability, and efficient network management. The following sections describe the challenges specific to these environments.

This document is based on the test results up to release 17.6.1 for the C9800 Wireless Controller platforms validation.

Security

Universities need to protect personal, academic, and copyrighted information with security-rich features such as rogue detection/containment, Intrusion Prevention (WDS/wIPS), DOT1X, and guest-access (centralized and local web-auth).

Specialized services

Educational infrastructures must enable traditional and specialized resources to provide accessibility and speed. Network services such as video delivery, RLAN Support, BYOD, AVC, NetFlow, mDNS/SDG, Quality of Experience with custom QoS, Flexible Radio Assignment (FRA), and Client Aware FRA are deployed.

Migration to IPv6

Devices increasingly run on IPv6, while network infrastructures are likely to continue on IPv4. Dual Stack deployments with features such as IPv6 access and IPv6 Multicast are enabled for this Education vertical guide.

Mobility

Seamless mobility for large number of clients is essential to supporting uninterrupted voice and data services. Fast roaming such as CCKM, 802.11 r/k/v, Selective Roaming, and Optimized Roaming are enabled for this vertical.

High availability

Education infrastructures cannot afford downtime in their networks. The network should be able to sustain catastrophic events such as AP or Controller outage. Self-healing RF network and Client SSO are deployed.

Efficient network management

Network administrators should be able to efficiently manage and monitor their networks. The administrators could use Cisco-provided tools such as Cisco Prime Infrastructure and WebUI to quickly deploy, manage, monitor, and troubleshoot the end-to-end network. DNA Center is incorporated for automated network provisioning of WLC and APs.

Performance and scalability

Universities and colleges face tight IT budgets and steep technology demands. Various models of Wireless Controller (C9900-40/80) and 802.11AC/AX Access Point (AP1832, AP1852, AP2800, AP3800, AP9120AX, AP9130AX) can meet the demand for both scalability and performance. This includes handling of high-density scenarios of large number of clients per AP and large-scale client mobility on the wireless controllers.

The following table summarizes key areas on which this Education profile focuses.

Table 1. Education profile feature summary

Deployment Areas	Features
Security	Rogue Detection/Classification/Containment Intrusion Prevention (WDS/wIPS) Dot1x Authentication Guest Access: Local Web AUTH, Central Web AUTH BYOD Identity Pre-Shared-Key
Network services	Video Content Delivery (L2/L3 Multicast) mDNS/SDG Application, Visibility, and Control (AVC) Custom QoS Bandwidth Limiting per WLAN or per user Load Balancing/Band Steering Client Profiling DHCP or HTTP Trustsec (SGT/SGT-ACL)
IPv6 migration	Dual Stack, IPv6 security, CAPWAPv6
Mobility	Fast roaming OKC, CCKM L2/L3 roaming 802.11 r/k/v Selective Roaming Optimized Roaming IRCM Edu-Roam
High availability	AP/Client SSO N+1 Redundancy In-Service Software Upgrades (ISSU) Rolling Upgrades Hot/Cold Software Patches
Location services	Cisco Connect Mobility Experience (CMX) Location Analytics DNASpaces RFIDs BLE Probing
Network planning & troubleshooting	NetFlow RF Sniffer Wireless Service Assurance Sensor
Efficient network management	Cisco Prime Infrastructure

	WebUI DNA Center
Licensing	Smart License

Network profile

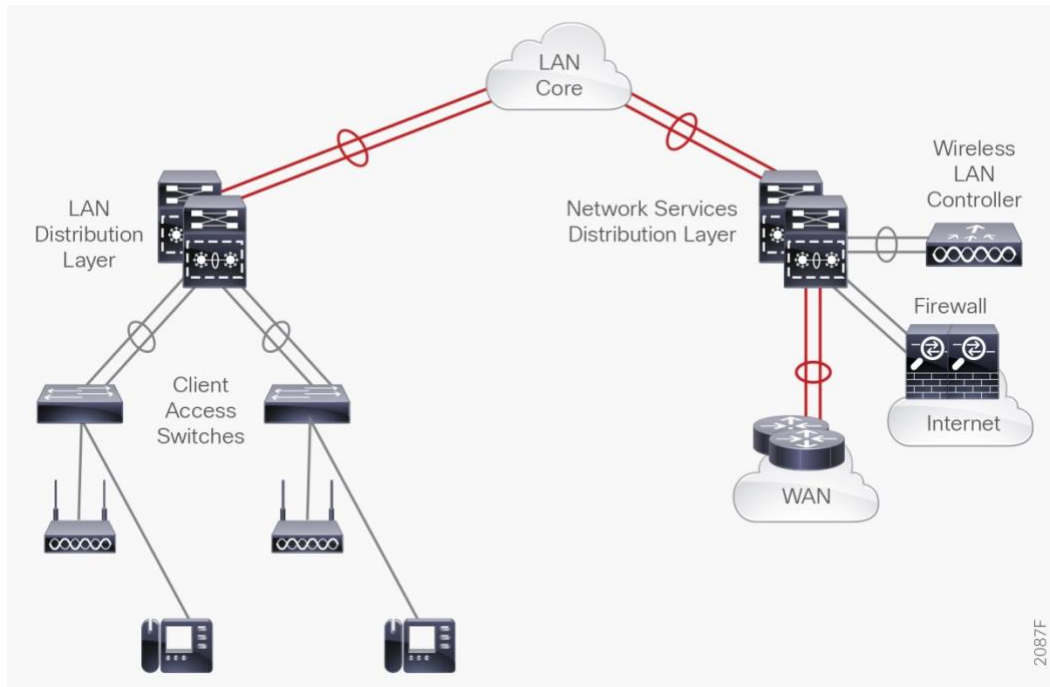
Based on the research, customer feedback, and configuration samples, the Education Vertical Profile is designed with a deployment topology that is generic and can easily be modified to fit any specific deployment scenario.

Topology diagram

Figure 1 shows the University Campus three-tiers design that is used for the validation of the Education Vertical Profile.

The topology represents a typical University Campus deployment with a Cisco Catalyst 6500/Cisco Nexus 7K in the distribution layer and a Cisco Catalyst 6500/Cisco Nexus 7K in the core layer. Based on the size of the campus (both its geographical location and user-scale), there might be more distribution switches connecting to the core layer. Also, depending on AP/client scale, different C9800 Wireless Controllers models can be utilized. For the Education profile, the primary validation centered on the C9800-80, C9800-40 and C9800-CL models, although all models are supported.

Figure 1. Education vertical profile: topology overview



Hardware profile

Table 2 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end Education Vertical Profile deployment.

The list of hardware, along with the relevant software versions and the role of these devices, complement the actual physical topology defined in Figure 1.

Table 2. Hardware profile of servers and endpoints

VM and HW	Software Versions	Description
C9800 Wireless Controller	17.3.x, 17.6.1	Cisco Next generation Wireless Controller: 9800-80, 9800-40, 9800-CL
Cisco Prime	Version 3.10 & 3.9 MR1	For Network Management
Cisco ISE	Version 2.4/ 2.6/ 2.7/3.0	Radius Server used for authentication, authorization
Free Radius	Version 3.0	Radius Server used for authentication, authorization
CUCM	Version 11	CUCM Server for managing IP phones
Cisco CMX	Version 10.6.2/3	Location Services
Cisco DNAC Spaces	Version 2.3.0/1	Location Services
DNS/AD Server	Windows 2012	Windows External server for DNS and Active Directory management
APIC-EM Plug-n-Play	Version 2.0	For Day0 Config and Image Management
Cisco UCS Server	ESXI 6.0/6.5/6.7	To manage and host the virtual machines
Ixia	IxNetwork and IxExplorer	Generate traffic streams and to emulate dot1x clients
Ixia Veriwave	Veriwave	Wireless endpoints with scale
Cisco Unified IP Phones 796x, 9971, 925, 8821	Cisco IP phones	Endpoints
Laptops	Windows 8, Windows 10, Chromebook	Endpoints: Google, HP, Samsug, Dell Inspiron/Latitude\XPS, Lenovo, Surface Pro
Macbook	Mac OSX	Endpoints for SDG: Macbook Pro, Air
Casting	Apple TV 3 rd & 4 th Generation, ChromeCast, Roku	SDG server
Smartphone/Tablet	Multiple versions	Endpoints (iPhone6/6s/7/8/10/XR/11, iPad, iPad Pro, iPad Mini, Samsung Note 8/10/20, Samsung Galaxy S7/8/9/10,21, Nexus, LG)
IP camera	Samsung, Netgear	Endpoints
Printer	HP, Epson, Samsung	Endpoints
Gaming	Xbox, PlayStation	Endpoints

Test environment

This section describes the features and the relevant scales at which the features are deployed across the physical topology. Table 3 lists the scale for each feature.

Table 3. Education profile: feature scale

Feature	Scale
Wireless Controller*	C9800-40, C9800-80, C9800-CL
Access Points*	AP1540, AP1560, AP1570, AP1800i, AP1810, AP1810w, AP1815i, AP1815w, AP1815m, AP1830, AP1840, AP1850, AP2800, AP3800, AP4800, AP9105, AP9115, AP9117, AP9120, AP9124i, AP9124D, AP9130, IW3700, IW6300, ESW6300 (16.12.x and 17.3.x releases also include AP1700, AP2700, AP3700, AP1530, AP1570 testing)
Modes	Flex, Local, Fabric and Mesh mode APs
Clients	80% as baseline for Wireless Controller maximum capacity + 20% Clients from each use case
WLANs	1000
AP Join Profiles	50
Site Tags	200
APs per Site Tag	800 (Local), 100 (Flex)
RF Tags / Profiles	100 / 200
Policy Tags / Profiles	2000 / 1024
Flex Profiles	200
Rogue APs	80% of platform support
Rogue Clients	80% of platform support
AAA Servers	3
RFIDs	80% of platform support
VLANs	1000
VLAN Groups	100
Wireless interface	5
Trap receivers	6
IPv4 ACLs	200
IPv6 ACLs	200
Mobility Groups	1
Mobility Group Members	20
IGMP snooping	300 groups
SNMP	PI/MIB walks

* Note: Please refer to the supported hardware matrix for each release.

Use case scenarios

Test methodology

The use cases listed in Table are executed using the topology defined in Figure 1, along with the Test environment shown in Table 3.

The System Under Test is loading up with 80% system capacity as the baseline at all time. The remaining 20% will be used for each use case to establish scale and stress condition for the system under test.

With respect to the longevity for this profile setup, Radio Crashes, Device Core-Dump, CPU and memory usage are monitored for 7 days. In order to test the robustness, certain negative events would be triggered during the use-case testing.

Use cases

Table 4 describes the use cases that were executed on the Educational Vertical Profile. These use cases are divided into buckets of technology areas to show the complete coverage of the deployment scenarios.

These technology buckets are composed of system upgrade, security, network services, monitoring & troubleshooting, simplified management, and system health monitoring along with system and network resiliency.

Table 4. List of use case scenarios

No.	Focus Area	Use Cases
System upgrade/downgrade		
1	Upgrade/Downgrade	Network administrator should be able to perform C9800 WLC upgrade and downgrade between releases seamlessly <ul style="list-style-type: none">All of the configuration should be migrated seamlessly during the upgrade/downgrade operationSW Install, Remove Inactive, Activate, Commit
2	DNAC-SWIM	Network admin should be able to manage images on network devices using DNAC for upgrade/downgrade
3	In-Service Upgrade	Network Administrator should be able to perform C9800 WLC ISSU upgrade between releases seamlessly. <ul style="list-style-type: none">All of the configurations should be migrated seamlessly during the upgrade operationWLC GUI and DNAC Driven ISSU.ISSU supported on all major releases (17.3.x-17.3.x) and between major releases (ie, 17.3.x to 17.6.x)
4	AP Service/Device Pack Upgrade	Network Administrator should be able to upgrade APs using service packs or device packs without requiring a new wireless controller release (when available). <ul style="list-style-type: none">Access Point (AP) fixes and updates using an AP Service Pack (APSP)Support for new AP models using an AP Device Pack (APDP)Rolling AP upgrade
Security		
5	Over-the-Air Attacks	Network admin wants to detect and mitigate wireless thread <ul style="list-style-type: none">Adaptive WIPS using DNACRogue APs and rogue clientsRogue Containment

No.	Focus Area	Use Cases
6	Guest-Access	Network admin wants to provide temporary guest access using the LWA and CWA. <ul style="list-style-type: none"> • LWA—Custom/Default Pages • EWA—External Web Server • CWA—Self Register Guest Portal • Wired Guest • UDN - Edu-Roam
7	Device Onboarding	Faculty and Student can bring their own devices to onboard using self-portal registration or through hotspot
8	AP 802.1X	Configure 802.1X authentication between a lightweight access point and a Cisco switch to prevent unauthorized AP
Network services		
9	Multicast Video	Network admin wants to enable and deploy multicast services <ul style="list-style-type: none"> • V4 & V6 Multicast • L3/L2 Multicast video delivery using PIM-SM, SSM, IGMP/MLD Snooping
10	mDNS/SDG	Network admin enables the mDNS/SDG services on wired networks so that teachers can access IT-maintained Apple TVs and printers and students can access only the printers <ul style="list-style-type: none"> • mDNS Filtering – SSID, AP Name, AP Location • Micro-Location Services
11	Custom QoS	Network admin needs to enhance user experience by ensuring traffic and application delivery using custom QoS policies <ul style="list-style-type: none"> • Traffic types: VOIP, Video, Call Control, Transactional Data, Bulk Data, Scavenger • SSID and client policies on wireless QOS targets • Marking, Policing of wireless traffic • Auto QOS: Predefined profiles which can be further modified by the customer • Bidirectional Rate Limiting
12	Application Visibility and Control	Network admin wants to monitor application based statistics reporting per wlan and per client in their network Mark, Drop, Rate Limit an application
Client Mobility		
13	Mobility	Seamless mobility for a large number of clients with uninterrupted voice and data services <ul style="list-style-type: none"> • L2/L3 Roaming • Fast Roaming with CCKM, 802.11 r/k/v • OKC Roaming • Optimized Roaming • Selective Roaming
14	IRCM Mobility	Seamless Mobility for clients between eWLC and AireOS WLCs with uninterrupted voice and data services. <ul style="list-style-type: none"> • L2/L3 Roaming • Fast Roaming
15	Guest Anchor	Anchor/Foreign relationship with Anchor located on AireOS or eWLC WLCs. <ul style="list-style-type: none"> • IRCM (AireOS as Guest Anchor) • eWLC as Guest Anchor
Monitoring & troubleshooting		
14	Client Troubleshooting	Network admin should be able to troubleshoot client connectivity issues <ul style="list-style-type: none"> • Service Assurance (iCAP, RA Tracing, DNAC Assurance) • WLC embedded packet captures filtered via ACL and inner filter

No.	Focus Area	Use Cases
15	NetFlow	Enable IT admins to determine network resource usage and capacity planning by monitoring IP traffic flows using Flexible NetFlow. <ul style="list-style-type: none"> Traffic Types: L2, IPv4, IPv6 Prime Collector, Live Action Encrypted Traffic Analytics (ETA)
16	Wireless Network Assurance	360 views for Client, AP, WLC, and Switch
Simplified management		
17	Prime-Manage-Monitor	Network admin wants to manage and monitor all the devices in the network using Cisco Prime Infrastructure
16	Prime-Template	Network admin wants to configure deployment using Cisco Prime Infrastructure <ul style="list-style-type: none"> Import and deploy customer-specific configuration templates Schedule configuration for immediate or later deployment Simplify configuration using configuration-templates
19	Prime-Troubleshooting	Simplify network troubleshooting and debugging for IT admins <ul style="list-style-type: none"> Monitor & troubleshoot end-end deployment via maps & topologies Monitor network for alarms, syslogs and traps Troubleshoot network performance using traffic flow monitoring
20	DNA Center	Admin should have the ability to use Automation for their network provisioning via the DNAC including Plug and Play onboarding of wireless controllers and access points.
System health monitoring		
21	System Health	Monitor system health for CPU usage, memory consumption, and memory leaks during longevity
System & network resiliency, robustness		
22	High Density/Stress	High client associations/disassociations/roams in Classroom, Town hall, Auditorium, or special events
23	System Resiliency	Verify system level resiliency during the following events: <ul style="list-style-type: none"> Active WLC failure Standby WLC failure RMI/RP link flaps Power failure LAG failure AP Failure
24	Negative Events, Triggers	Verify that the system holds well and recovers to working condition after the following events are triggered: <ul style="list-style-type: none"> Config Changes—Add/Remove config snippets, Default-Interface configs Link Flaps, SVI Flaps RMI, Gateway reachability. Clear Counters, Clear ARP, Clear Routes, Clear access-sessions, Clear multicast routes IGMP/MLD Join, Leaves Burst client association Radius failure DHCP failure WLAN Flaps Manual wireless client deauthentication and traffic verification following subsequent authentication VLAN pooling and Dirty VLAN recovery

Appendix A

Cisco Catalyst 9800 Series Configuration Best Practices can be found at the following location:

<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html>

IOS-XE Wireless Feature List Per Release

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214855-ios-xe-wireless-feature-list-per-release.html>




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)