CISCO VALIDATED PROFILE

Access Switching Education Profile

April 2017

Table of Contents

Profile Introduction

The Enterprise market segment can be divided into five broader verticals: Education, Financial, Health, Retail, and Government. This document focuses on a typical Education deployment profile, and you can use it as a reference validation document for a University or a K-12 Education profile.

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

SECURITY

Universities need to protect personal, academic, and copyrighted information. Security-rich features such as MAB, dot1x, guest-access (centralized and local web-auth), CISF, IPV6 First-Hop-Security (FHS) are deployed.

SPECIALIZED SERVICES

Educational infrastructures must enable traditional and specialized resources in order to provide accessibility and speed. Network services such as video delivery, SDG, Plug-n-Play, Auto-Conf, and Quality of Experience with custom QoS and Auto QoS are deployed.

The Application Visibility Control (AVC) with Domain Name System as an Authoritative Source (DNS-AS) feature provides a centralized means of controlling the identification and classification of trusted network traffic in an organization. DNS-AS can provide AVC on low-end platfroms on which NBAR is not supported.

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, IPv6 FHS, and IPv6 Multicast are enabled for this Education vertical guide.

EFFICIENT NETWORK MANAGEMENT

The Education infrastructures cannot afford downtime in their networks. The 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.

PRICE-PERFORMANCE AND SCALABILITY

Universities and colleges face tight IT budgets and steep technology demands. Various models of Cisco Catalyst 3850/3650/2960X/3750X/C3560CX/2960L with high-port density, POE-enabled ports with EnergyWise-capable services are deployed for the Educational vertical.

NETWORK SEGMENTATION

Optimizing the existing network using technologies such as VRF-Lite and MPLS VPN helps in effective IP address use, as well as providing the required network segmentation to meet universities' and schools' system needs, such as separation between teacher and student access, STEM departments' access or guest access, isolating them from each other. MPLS VPNs provide a secure, flexible, and scalable way to form logical segmentation. Multicast VPNs allow the transport of IPv4 Multicast (video conferencing) over the Unicast MPLS VPN backbone encapsulated in GRE tunnels.

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

Table 1 Education profile feature summary

Deployment areas	Features
Security	MAB, dot1x, guest access (CWA, LWA), CISF, IPv6 FHS, V6VACL
Network services	Video content delivery (L2/L3 multicast), SDG (mDNS), Plug-n-Play or Smart Install, Custom QoS, AutoQoS, AutoConf, DNS-AS
IPv6 migration	Dual Stack, V6 multicast, IPv6 FHS
Network planning & troubleshooting	NetFlow, SPAN, R-SPAN, ERSPAN, Wireshark
Efficient network management	Cisco Prime Infrastructure, WebUI
Price-performance	EnergyWise, PoE, high-port density, mGIG chassis, collapsible core/distribution at smaller sites
Network Segmentation	MPLS VPN, Multicast VPN

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. This profile caters both to the smaller K-12 and the larger University Campus deployments.

For K-12 deployments, due to the smaller geographical size, budget restrictions, and smaller scale, the Core is collapsed to the Distribution layer, and Cisco Catalyst 4500 (and in some cases Catalyst 3850) can be used as a combination of Distribution plus Core.

For larger University campus deployments—which cover larger geographical areas, larger scale, and heavier usage of resources—this design uses the classic 3-tier architecture of Access, Distribution, and Core. Please refer to the topology for further details.

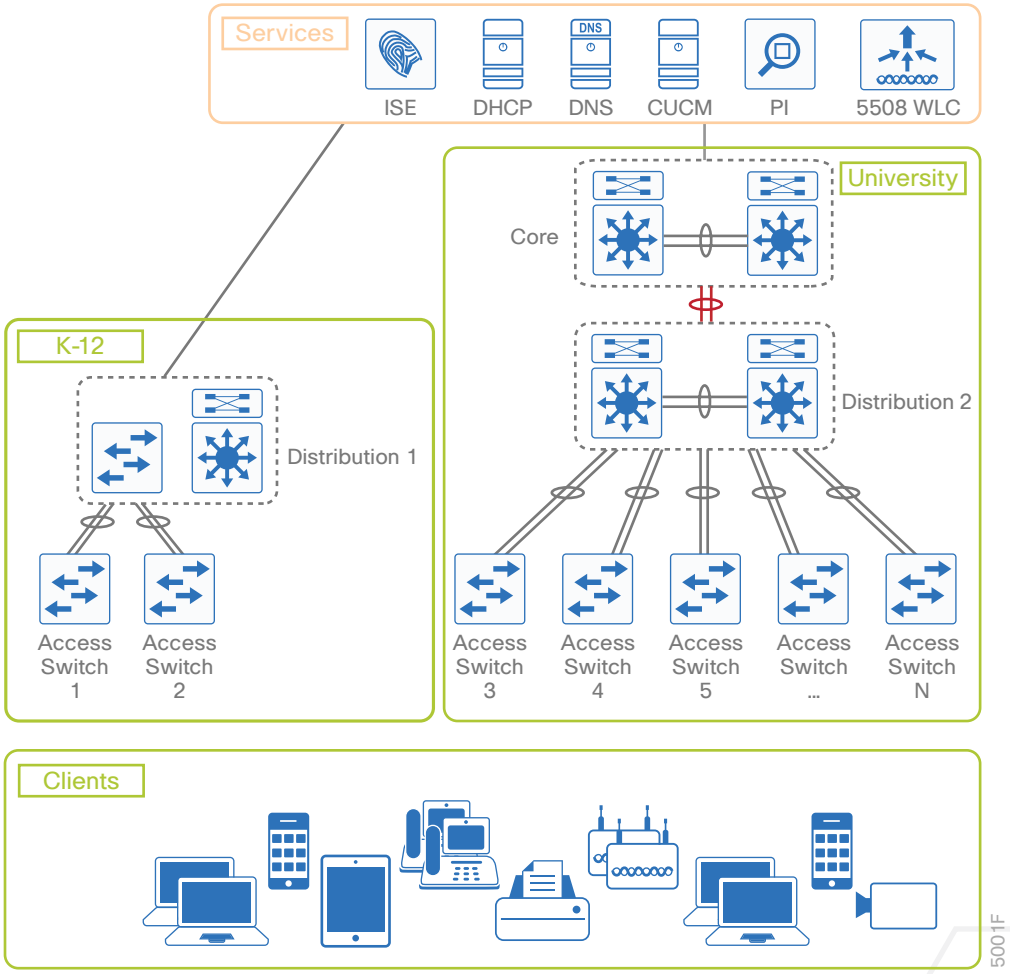
TOPOLOGY DIAGRAM

Figure 1 shows the "converged" K-12 and the University Campus that is used for the validation of the Education Vertical Profile.

Disclaimer

The links between the different network layers in the topology are mainly to facilitate this profile validation across different platform combinations, and the actual deployment could vary based on specific requirement

Figure 1 *Education Profile: vertical topology*



Site-1 (the left-portion of the topology) represents the K-12 deployment where a Catalyst 3K is used as a distribution switch along with Catalyst 4500s that are used as collapsed core/distribution.

Site-2 (the right portion of the topology) represents a typical University Campus deployment with a Catalyst 4500 in the distribution layer and a Catalyst 6500 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.

Disclaimer

The links between the different network layers in the topology are mainly to facilitate this profile validation across different platform combinations and the actual deployment could vary based on specific requirement

HARDWARE & FEATURE SPECIFICATIONS

This section describes the 3-D feature matrix where the hardware platforms are listed along with their place-in-network (PIN) and the relevant vertical features.

Key Vertical Features

Table 2 defines the 3-D hardware, PIN, and the features deployed. The scale of these configured features, the test environment, and the list of end-points and hardware/software versions of the network topology are defined later in this document.

Disclaimer

Refer to appropriate CCO documentation for release/feature support across different platforms.

Table 2 3-D feature summary with hardware and PIN

Deployment layer (PIN)	Platforms	Critical vertical features
Access	Switch1: C3850 5-M stack Switch2: C3650 5-M stack New-HW: WS-C3650-48FQM-ESwitch3: C3850 9-M stack Switch4: C3650 5-M stack Switch 5: C3560CX 3-M stack Switch 6: 3750X 6-M stack Switch 7: 2960X 4-M stack or 2960XR 2-M stack Switch 8: 2960L Switch 9: SUP8E Switch 10: SUP8LE	V4/V6- Dual Stack Web Auth, 802.1x, MAB, AAA, Radius Custom QoS Ingress/Egress, AutoQoS DHCP snooping, DAI, Port Security, Storm Control, IPSG IPv6 FHS ACL (IPv4/IPv6) V6VACL L2-EtherChannel EnergyWise, POE (endpoints) SNMP Multicast–IPv4/v6, IGMP/MLD Snooping Radioactive Tracing SDG SPAN, R-SPAN, ERSPAN, Wireshark, FNF DNS-AS OpenFlow1.3 Named VLAN OSPF LDP BGP MPLS BFD L3VPN MVPN
Distribution	Dist1: WS-3850-12XS 2-M stack, Cat4K(SUP7E) Dist2: Cat4K-VSS (SUP8E) or Cat4K-VSS (SUP7E)	VSS OSPF Multicast–IPv4/v6 PIM SSM/SM EtherChannel SNMP SDG Custom QoS Ingress/Egress FNF, NetFlow-lite
Core	Core1: Cat6K-VSS	BGP, OSPF Multicast EtherChannel LDP MPLS L3VPN BFD

Hardware Profile

Table 3 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end Education Vertical Profile deployment.

This 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 3 *Hardware profile of servers and endpoints*

VM and HW	Software versions	Description
Cisco Prime	Version 3.1.4 DP6	For network management
Cisco ISE	Version 2.1	Radius server used for authentication, authorization
CUCM	Version 10.1	CUCM server for managing IP phones
DNS/AD server	Windows 8 Enterprise Server	Windows external server for DNS and Active Directory management
APIC-EM Plug-n-Play	APIC-EM 1.2	For Day0 config and image management
Cisco UCS Server	ESXI 5.5.0	To manage and host the virtual machines
Ixia	IxNetwork 7.51.1014.17 EA-Patch1	Generate traffic streams and to emulate dot1x clients
Cisco Unified IP Phones 7960, 7945, 9971	Cisco IP phones	Endpoints
Windows laptops	Windows 7/8	Endpoints
MacBook Pro laptops	OSX 10.10.x	Endpoints for SDG
Apple TV	3rd Gen 2013, 7.0	SDG server
IP camera	NA	Endpoints
Printer	N/A	Endpoints

TEST ENVIRONMENT

This section describes the features and the relevant scales at which the features are deployed across the physical topology. Table 4 lists the scale for each feature.

Disclaimer

The table below captures a sample set of scale values used in one of the use cases. Refer to appropriate CCO documentation/datasheets for comprehensive scale data.

Table 4 *Education Profile: feature scale*

Feature	Scale
EtherChannels	6-8
VLANs	1k
STP	64
MAC Learning	2k MAC addresses
Storm Control (bcast)	128 interfaces
IPv4 ACLs/ACEs(RACL/PACL)	20 ACLs (10 Cisco ACEs per ACL), 10K ACE
IPv6 ACLs/ACEs	10 ACLs (10 ACEs per ACL), 10K ACE, 2V6ACL (10 ACEs per ACL)
Static routes	16 IPv4/IPv6
SSH server	All switches
NTP client	All switches
SPAN/RSPAN/ERSPAN	2/2/2
Stacking	3 up to 9 members
802.1Q VLAN trunking	6 trunks
SVI	80
IGMP/MLD Snooping	300 groups
NetFlow	6 monitors+10k flows
QoS	40 classes+11 policy-maps+38 policers
SNMP	Cisco PI/MIB walks
DHCP snooping	600 clients
IP phones (MAB clients)	50
IPDT	Enabled on interface and vlan
Dot1x clients	500 (real+emulation)
WebAuth clients	20 PCs (real+emulation)
EnergyWise clients	50 (phones+cameras+PCs+printers)
Port-security	128 Interfaces
SDG	20 ATVs (K12), 100ATVs+50 Printers (Univ) (real+emulation)
V6 clients	50 (real+emulation)
BFD	15
MPLS VRF	5
MPLS IPv4 VPN Routes	500
MPLS Label Scale	100
MVPN VRF	2
MVPN Groups	200
LDP Session	2
BGP Session	2
DNS-AS	10 applications

Use Case Scenarios

TEST METHODOLOGY

The use-cases listed in Table 5 are executed using the topology defined in Figure 1, along with the test environment already shown in Table 4.

Images are loaded on the devices under test via the tftp server using the Management interface.

To validate a new release, the network topology is upgraded with the new software while loading the complete configuration that comprises the use cases and relevant traffic profiles. Addition of new use cases acquired from the field or customer deployments are added on top of the existing configuration.

During each use-case execution, syslog is monitored closely across the devices for any relevant system events, errors, or alarms. With respect to longevity for this profile setup, CPU and memory usage are monitored during overnight runs as well as during the weekends, paying special attention systems memory usage and any memory leaks. Furthermore, to test the robustness of the software release and platform under test, specific negative events are triggered during the use-case execution process.

USE-CASES

Table 5 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. Use cases continuously evolve based on the feedback from the field.

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 5 *List of use case scenarios*

No.	Focus area	Use cases
System upgrade		
1	Upgrade (Distribution/Access)	Network administrator should be able to perform switch upgrade and downgrade between releases seamlessly. ▪ All of the configuration should be migrated seamlessly during the upgrade/downgrade operation ▪ SW Install, Clean, Expand
Security		
2	CISF (Access)	Network admin to secure the L2 access against MITM, DOS attacks using the CISF (Cisco Integrated Security Features) ▪ PortSecurity, IPSG, DAI, DHCP snooping
3	IPv6 FHS (Distribution/Access)	Network admin to secure the IPv6 network against MITM, DOS attacks by providing control-plane and data-plane filtering using IPv6 FHS (First-Hop-Security) ▪ IPv6 Snooping, ND Inspection, RA guard, Source & Destination Guard, DHCPv6 Guard
4	IBNS 2.0 Mode (eEdge/new-style) (Access)	Network admin wants to deploy endpoint/end-user security using MAB/Dot1x with IBNS 2.0 mode (eEdge/new-style). ▪ PC behind the Phone: AuthC > Dot1x for the PC and MAB for the Phone, Host Mode : Multi-Domain ▪ Dot1x, MAB : PCs, phones. Host mode: Single Host, Multi-Auth ▪ AuthZ > dACL, Dynamic VLAN
5	Auth-Manager Mode (legacy) (Access)	Network admin wants to deploy endpoint/end-users security using MAB/Dot1x with Auth-Manager Mode (legacy). ▪ PC behind the Phone: AuthC > Dot1x for the PC and MAB for the phone, HostMode : Multi-Domain ▪ Dot1x, MAB : PCs, phones. Hostmode: Single Host, Multi-Auth ▪ AuthZ--> dACL, Dynamic VLAN
6	Guest-Access (Access)	Network admin wants to provide temporary guest access using the LWA and CWA. ▪ LWA–Custom/Default Pages ▪ CWA–Self Register Guest Portal
7	ACL (Access)	Network admin to deploy input/output PACL, RACL, and VACL with large number of ACEs for various traffic patterns (v4/v6) in 3-tier route-access network ▪ ACL ▪ PACL ▪ IPV6 VACL

Table 5 continued

Network services		
8	Multicast Video (Distribution/Access)	Network admin wants to enable and deploy multicast services. ▪ V4 & V6 Multicast ▪ L3/L2 Multicast video delivery using PIM-SM, SSM, IGMP/MLD Snooping ▪ Enable radioactive tracing to see IGMP client join events on switch
9	EnergyWise (Distribution/Access)	Enable network admins to measure and manage energy usage in the network by implementing energy saving policies for various endpoints (phones, cameras, PCs) and scenarios (shutdown/sleep/hibernate, wake-on-LAN)
10	SDG (Distribution/Access)	Network admin enables the SDG services on wired networks so that teachers can access IT-maintained Apple TV and printers, and students can access only the printers.
11	Auto QoS (Access)	Network admin needs to enhance user experience by ensuring traffic and application delivery. ▪ AutoQoS for Cisco devices such as IP phones, IP cameras, etc.
12	Custom QoS (Distribution/Access)	Network admin needs to enhance user experience by ensuring traffic and application delivery using custom QoS policies for trusted/untrusted interfaces. ▪ Traffic types: VOIP, Video, Call Control, Transactional Data, Bulk Data, Scavenger ▪ Policing Ingress and Priority & BW Management in Egress
13	Custom QoS with DNS-AS	Network admin needs to enhance user experience by ensuring traffic and application delivery. ▪ Traffic types: Traffic from any application that generates DNS query ▪ Policing ingress and priority & BW Management in egress
14	Plug-n-Play (Distribution/Access)	Simplify network provisioning of new switches by Zero-Touch-Deployment for Day0 using NG-PNP app via APIC-EM for image and config management
15	Smart Install (Distribution/Access)	Simplify network provisioning of new switches by Zero-Touch-Deployment for Day0 using Smart Install
16	AutoConf (Access)	Simplified network deployment of IP phones, cameras, telepresence, access points, and other end units connected to a Catalyst switch for a network administrator
17	ASP (Access)	Enable ease-of-use feature (for example, ASP that enables admin to automatically detect the devices that are connected to configure the port using macros)

Table 5 continued

Network Segmentation		
18	MPLS VPN (Access)	Network admin is able to provide secure and scalable segmentation between the MPLS VPNs. VPNs are transported independently over MPLS core. ▪ MP-iBGP (PE), LDP (core) , OSPF/Static (CE-PE) ▪ BGP ECMP path
19	Multicast VPN (Access)	Enterprise network administrator wants to extend the reach of enterprise multicast applications using Multicast VPN (MVPN) over MPLS (L3VPN) environment. ▪ Default and Data MDTs ▪ VRF Multicast traffic (IPv4) using PIM-SM, PIM-SSM ▪ PIM-SM in the core
Monitoring and troubleshooting		
20	SPAN, Wireshark (Distribution/Access)	Network admin should be able to troubleshoot the network by capturing and analyzing the traffic. ▪ SPAN, Remote-SPAN, ERSPAN ▪ Wireshark–Dataplane & Control Plane Capturing
21	NetFlow (Distribution/Access)	Enable IT admins to determine network resource usage and capacity planning by monitoring IP traffic flows using Flexible NetFlow ▪ Traffic types: L2, IPv4, IPv6 ▪ FNFv9, IPFIX-v10 ▪ Prime Collector/LiveAction
Simplified management		
22	Prime-Manage-Monitor (Distribution/Access)	Network admin wants to manage and monitor all the devices in the network using Cisco Prime Infrastructure.
23	Prime-SWIM (Distribution/Access)	Network admin should be able to manage images on network devices using Cisco Prime Infrastructure for upgrade/downgrade.
24	Prime-Template (Distribution/Access)	Network admin wants to configure deployment using Cisco Prime Infrastructure. ▪ Import and deploy customer specific configuration templates ▪ Schedule configuration for immediate or later deployment ▪ Simplify configuration using config-templates
25	Prime-Troubleshooting (Distribution/Access)	Simplify network troubleshooting and debugging for IT admins ▪ Monitor & troubleshoot end-end deployment via maps & topologies ▪ Monitor network for alarms, syslog, and traps ▪ Troubleshoot network performance using traffic flow monitoring

Table 5 continued

26	WebUI-Day0 Wizard (Distribution/Access)	Network admin deploys 3850 in the access layer site (Day 0). ▪ Able to do basic settings in an Access deployment scenario where the switch is deployed in the access layer with a single uplink to peer with the distribution/gateway switch ▪ Goal is to configure the switch with necessary management configuration along with relevant switch and port level configurations that can provide connectivity to the end devices
27	WebUI-Configuration (Distribution/Access)	Network admin to be able to configure the system (Day N) ▪ Switch uplink/downlink interface configs and provisioning of spanning tree protocol ▪ Most commonly used system level services (DHCP, NTP, DNS, Time/Date, Telnet/SSH) ▪ Security features–ACL, Access-Session, Port-Security, IPv6 FHS ▪ Implement Quality-of-Service using Cisco-recommended Auto-QoS
28	WebUI-Monitoring (Distribution/Access)	Network admin should be able to monitor the health of the system. ▪ Monitor the health of the system in terms of the CPU utilization and memory consumption of the switch ▪ Have the flexibility to look for the system health during a particular time range ▪ Flexible enough to look for the system health during a particular time range
29	WebUI-System Management (Distribution/Access)	Network admin routinely performs the task of Asset Management. ▪ Includes the detailed hardware inventory information down to serial numbers, software versions, stack information, power usage, licensing information, etc. Furthermore, it is a common practice to generate system reports based on this for audit purposes.
System health monitoring		
30	System Health (Distribution/Access)	Monitor system health for CPU usage, memory consumption, and memory leaks during longevity

Table 5 continued

System & network resiliency, robustness		
31	System Resiliency (Distribution/Access)	Verify system level resiliency during the following events: ▪ Active switch failure ▪ Active SUP failure ▪ Standby/Member switch failure ▪ EtherChannel member link flaps
32	Network Resiliency (Distribution/Access)	High availability of the network during system failures using: ▪ VSS ▪ BFD
33	Typical Deployment Events, Triggers (Distribution/Access)	Verify that the system holds well and recovers to working condition after the following events are triggered: ▪ Config Changes–Add/Remove config snippets, Default-Interface configs ▪ Link Flaps, SVI Flaps ▪ Clear Counters, Clear ARP, Clear Routes, Clear access-sessions, Clear multicast routes ▪ IGMP/MLD Join, Leaves

Appendix A

You can find example configurations at the following location:

http://cvddocs.com/fw/cvpconfig

Please use the feedback form to send comments and suggestions about this guide.

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 www.cisco.com/go/offices.