CISCO VALIDATED PROFILE

Access Switching Retail & Enterprise Vertical Profile

April 2017

Table of Contents

Profile Introduction

The Enterprise market segment is divided into five broader verticals: Retail & Enterprise, Financial, Healthcare, Education, and Government. This document focuses on a typical Retail & Enterprise deployment profile, and you can use it as reference validation document for Retail and Enterprise Network deployments.

The following sections describe the key considerations for Retail and Enterprise Verticals.

RETAIL SECURITY COMPLYING WITH PCI STANDARDS

In retail stores, network security is major area of consideration. Retail stores have to comply with PCI standards, which include using end-to-end Cisco TrustSec for securing station to data-center links.

Cisco TrustSec with the Identity features helps to achieve advanced security, to prevent credit card theft, and to secure credit card transactions.

Network Edge Authentication Topology (NEAT) enables extended secure access in areas outside the wiring closet (such as conference rooms). NEAT allows you to configure a switch to act as a supplicant to another switch.

OPTIMIZED NETWORK

Optimizing the existing network using technologies such as Private VLAN helps with effective IP address use, as well as providing the required network segmentation in order to meet the needs of the Enterprise segment for conference rooms, etc.

You provision the network by using the Auto SmartPort configuration, which has built-in macros for devices such as Cisco IP phone, Cisco IP video surveillance cameras, etc. Auto SmartPort macros dynamically configure ports based on the device type connected on the port.

NETWORK MANAGEMENT

From security and compliance perspective, retail networks require monitoring capabilities in order to keep track of network events and traffic types. SNMP and NetFlow are used to track and test network/traffic activities.

SYSTEM RESILIENCY

This Retail & Enterprise Vertical Profile serves as a guide for deploying a resilient and efficient network by touching on the challenges of security, performance, and using special services in order to provide a better user experience. Table 1 lists the key areas on which the Retail & Enterprise profile focuses.

NETWORK SERVICES

Enterprise network architectures largely use multicast protocols. Proper classification and traffic prioritization helps in reducing the latency of time-sensitive traffic. Custom QoS and Cisco Auto QoS help in achieving this demand. When it comes to cost reduction, EnergyWise can be one of the important tools for driving the relevant energy policies, enabling power savings after business hours.

Cisco Application Visibility and Control (AVC) provides application-level classification and monitoring on a Cisco network. AVC allows the network administrator to upgrade protocol packs, and custom application services help network administrators to customize the discovery of protocols and monitor the customized applications.

Table 1 *Retail profile feature summary*

Deployment areas	Features
Security	MAB, dot1x, Cisco TrustSec security group tagging, SG ACL, ACL, OGACL, MACsec, ASP, CISP/NEAT
Optimized network	Video content delivery (L2/L3 multicast), AutoQoS, private VLAN
Network planning & trouble-shooting	NetFlow, SPAN, Wireshark, stack merged logs (radio active tracing)
Network management	Cisco Prime Infrastructure, WebUI, SNMP
System resiliency	SSO, VSS, HSRP, stack, Flexlinks, RapidPVST
Network services	OSFP, EIGRP, BGP, EnergyWise, AVC

Network Profile

Based on the research and customer feedback and configuration samples, the retail deployments are usually self-contained, flat networks with minimal vertical or horizontal requirements.

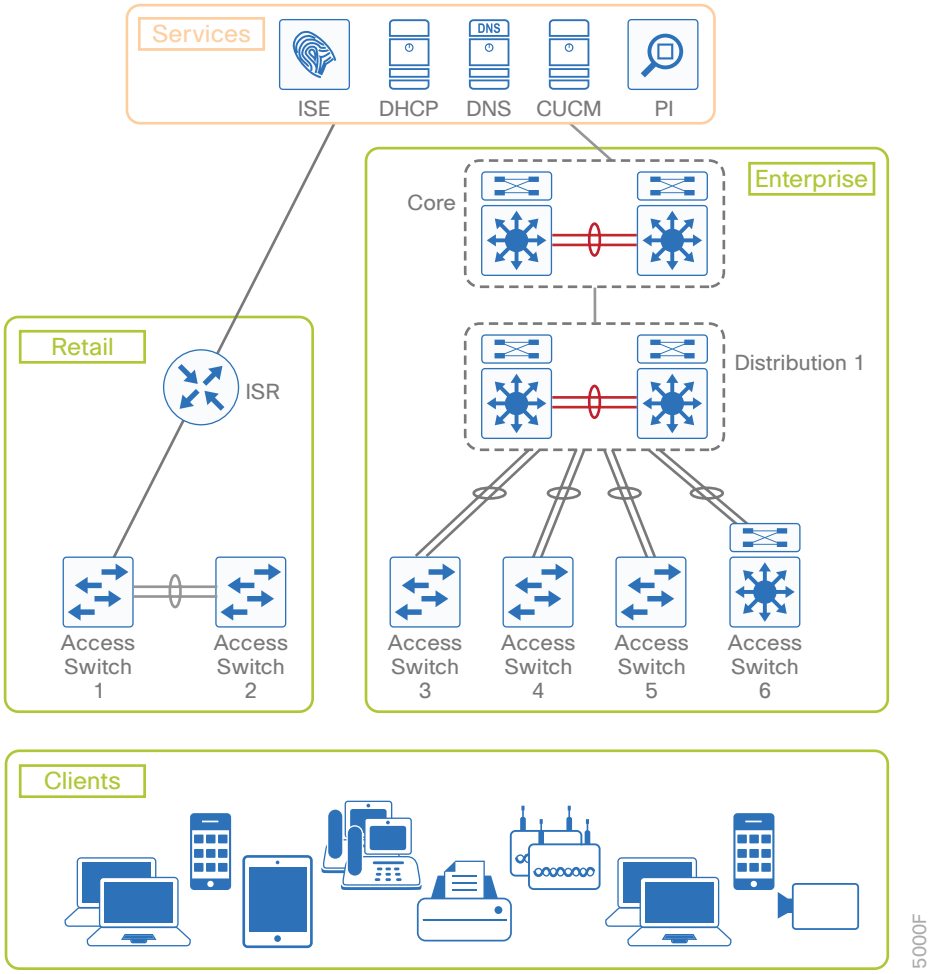
Based on customer deployment feedback, the enterprise deployments use Cisco Catalyst 2k/3k/4k as an access switch in each building connected to a Catalyst 4500 in the distribution layer and Catalyst 6500 in the core layer.

The following diagram shows the Retail infrastructure and enterprise network that is used for the validation of the Retail & Enterprise 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 requirements.

Figure 1 *Retail/Enterprise Vertical Profile: topology overview*



Site-1 (the left-portion of the topology) represents the retail deployment where a Catalyst 3850 is used as an access switch along with Cisco Integrated Servers Routers (ISRs) that are used for routing and WAN services.

Site-2 (the right-portion) represents the Enterprise deployment with Catalyst 2k/3k/4k used as an access switch, connected to a Catalyst 4500 in the distribution layer and a Catalyst 6500 in the core layer.

HARDWARE & FEATURE SPECIFICATIONS

This section details the 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 Deployment layer, Platforms, and the vertical features deployed. The scale of these configured features, the test environment, the list of endpoints, and the hardware/software versions in the network topology are defined later in this document.

Disclaimer

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

Table 2 *Feature summary with hardware and PIN*

Deployment layer (PIN)	Platforms	Critical vertical features
Access	Switch-1: C3850 2M stack Switch-2: C3650 2M stack Switch-3: C2960X/XR 4M stack Switch-4: 3750X 5Mstack Switch-5: C4900M/C4948E Switch-6: Cat4k Sup7E/7L-E/8L-E Switch-7: WS-C3650-24PDM Switch-7: C2960L	802.1x, MAB, AAA, Radius, TrustSec, ASP AutoQoS DHCP snooping, DAI, ARP ACL, Port Security, Storm Control, IPSG ACL (Ipv4) L2-EtherChannel SNMP Multicast–Ipv4, IGMP/MLD Snooping SPAN, Wireshark, FNF Private VLAN EnergyWise, POE (endpoints) AVC CISP/NEAT
Distribution	Cat4k VSS–Sup7E/8E Cat4500X VSS	DHCP Multicast–Ipv4 OSPF EIGRP VSS L3 EtherChannel
WAN	ISR	OSPF, BFD
Core	Cat6k	OSPF EIGRP BGP L3 EtherChannel Multicast

Hardware Profile

Table 3 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end Retail 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	Description
Cisco Prime	Version 3.1.4 DP6	For network management
Cisco ISE	Version 1.3, 2.1	For security policy management
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
Cisco UCS server	ESXi 5.5.0	To manage and host the virtual machines
Ixia	IxNetwork 7.5	Generate traffic streams and to emulate dot1x clients
Cisco Unified IP Phones 796x, 796x, 9971	Cisco IP phones	Endpoints
Windows laptops	Windows 7/8	Endpoints
MacBook Pro	OSX 10.10.x	Endpoints
IP camera	Cisco	Endpoints

TEST ENVIRONMENT

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

Disclaimer

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

Table 4 *Retail Profile: feature scale*

Feature	Scale
EtherChannels	6-8
VLANs	1k
STP	64 instances
MAC Learning	2k MAC addresses
Storm-Control (bcast)	286 interfaces
Ipv4 ACLs/ACEs(DACL)	20 ACLs (10 Cisco ACEs per ACL)
Static routes	100 Ipv4
SSH server	All switches
NTP client	All switches
SPAN/RSPAN/ERSPAN	4/4/2
Stacking	2 up to 9 members
802.1Q VLAN trunking	50 trunks
SVI	64
IGMP snooping	500 groups
NetFlow	6 monitors + 2k flows
QoS	40 classes + 11 policy-maps + 38 policers
SNMP	Cisco Prime/MIB walks
DHCP snooping	600 clients
IP phones/PCs	48
IPDT	Enabled on interface and vlan
Dot1x clients	500 (real+emulation)
MAB clients	48 phones
v4 clients	500
MLD snooping	200 groups
EnergyWise	50 (phones+cameras+PCs+printers)
AVC flows	20

Use Case Scenarios

TEST METHODOLOGY

The use cases listed in Table 5 are executed using the topology shown in Figure 1, along with the test environment (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 image with existing configuration that comprises the use cases and relevant traffic profiles. 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/leaks are monitored during the validation phase. Furthermore, to test the robustness of the software release and platform under test, typical networks events are triggered during the use-case execution process.

USE CASES

Table 5 describes the use cases that are executed on the Retail & Enterprise 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 and troubleshooting, simplified management, and system health monitoring, along with system and network resiliency.

Table 5 *List of use-case scenarios*

No.	TAG	Use cases
System upgrade		
1	Upgrade/downgrade operation (Access/Distribution)	Network administrator should be able to perform production network upgrade/downgrade between releases seamlessly. ▪ All of the configuration should be migrated seamlessly during the upgrade/downgrade operation. ▪ SW Install, Clean, Expand, ISSU
Security		
2	End-user security (Access)	Network admin wants to deploy security in a phased manner using the monitor mode for open access and monitor for any possible failures and remedy them before enforcement. ▪ 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-Host, Multi-Auth

Table 5 continued

3	Permit/deny for point of sale devices (Access)	Network admin wants to deploy authorized differentiated access in a phased manner using the low impact mode. ▪ 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-Host, Multi-Auth ▪ AuthZ> Pre-AuthACL, dACL
4	TrustSec (dynamic and static) (Access/Distribution)	Network admin enables TrustSec features to enable the secure tagging in the retail branch. ▪ Static SGT tagging. ▪ Dynamic SGT tagging ▪ SGACL
5	Auto smart ports (Access)	Network admin should be able to enable auto smart ports to allow the configuration per port, based on the device connected. ▪ Auto smart port for Cisco devices like IP phones, IP camera, laptops etc.
6	ACL (Access/Distribution)	Network admin to deploy input/output PACL, RACL, OGACL, and VACL with large number of ACEs for various traffic patterns (v4/v6) in 3-tier route-access network. Network admin to apply the ACL for Telnet, SSH, and SNMP access to unauthorized networks/users.
7	Guest-access (Access)	Network admin wants to provide temporary guest access CWA. ▪ CWA–Self Register Guest Portal
8	Encryption (Access/Distribution)	Network admin wants to deploy MACsec (SAP/MKA) for encryption on uplinks in large enterprise network
9	BYOD (Access)	Network admin wants to provide only Internet access to employees' personal devices–BYOD Dot1x, WebAuth
10	CISF/IPV6 FHS (Access)	Network admin wants to protect confidential data on the enterprise wired network and secure the network against attacks. ▪ IPSG, DHCP snooping, DAI, storm control ▪ DHCP/DHCP v6 server ▪ FHS
11	CISP/NEAT (Access)	Enterprise IT admin deploys NEAT to control/restrict the MAC addresses getting access to the network and prevent man-in-the-middle attacks

Table 5 continued

Network services		
12	Multicast data/video (Access/Distribution)	Network admin wants to enable and deploy multicast services. ▪ V4 Multicast ▪ L3/L2 Multicast video delivery using PIM-SM, SSM, IGMP/MLD Snooping
13	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, laptops, etc.
14	OSPF and BGP (Access/Distribution)	Network admin wants to enable routing services. ▪ OSPFv2 and OSPFv3 ▪ BGP
15	EnergyWise (Access)	Enable network admins to measure and manage energy use in the network by implementing energy saving policies for various endpoints (phones, cameras, PCs) & scenarios (shutdown/sleep/hibernate, activity check).
16	QoS (Access/Distribution)	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
17	AVC	Network admin wants to enable AVC over the network for better user experience and monitoring ▪ Protocol discovery ▪ Application Visibility: Skype, Facebook, Jabber, Lync, etc ▪ QoS-Classification: classify the traffic using the policy defined on the interface. ▪ Network admin performs Protocol Pack upgrade without taking downtime and uses the new available protocol discovery. Admin configures new custom apps to mark organizational internal traffic specified in the device configuration.

Table 5 continued

Monitoring & troubleshooting		
18	SPAN, Wireshark (Access/Distribution)	Network admin should be able to troubleshoot the network by capturing and analyzing the traffic. ▪ SPAN, Remote-SPAN, ER-SPAN ▪ Wireshark–Control Plane Capturing
19	NetFlow (Access/Distribution)	Enable IT admins to determine network resource usage, capacity planning by monitoring IP traffic flows using Flexible NetFlow. ▪ Traffic types: L2, IPv4 ▪ Prime Collector, Live Action
20	Private VLAN (Access/Distribution)	Network admin to deploy Private VLAN for efficient IP aggregation ▪ Primary VLAN, Secondary VLAN ▪ Isolate port, Community port on the physical interface depending on the connected end points
Simplified management		
21	Prime-Manage-Monitor	Network admin wants to manage and monitor all the devices in the network using Cisco Prime Infrastructure.
22	Prime-SWIM	Network admin should be able to manage images on network devices using Cisco Prime Infrastructure for upgrade/downgrade.
23	Prime-Template	Network admin wants to configuration deployment using Cisco Prime Infrastructure. ▪ Import and deploy customer specific configuration templates ▪ Schedule configuration for immediate or later deployment ▪ Simplify configuration using config-templates
24	Prime-Troubleshooting	Simplify network troubleshooting and debugging for IT admins ▪ Monitor & troubleshoot end-end deployment via maps & topologies ▪ Monitor network for alarms, syslogs and traps ▪ Troubleshoot network performance using traffic flow monitoring.
25	WebUI-Day0 Wizard	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

Table 5 continued

26	WebUI-Configuration	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
27	WebUI-Monitoring	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
28	WebUI-System Management	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.
29	WebUI–Image deployment	Network admin should be able to upgrade/downgrade images on the access devices using WebUI.
30	WebUI–AVC	Network admin to monitor AVC using WebUI. ▪ Allows admin to configure AVC using WebUI management ▪ Allows admin to monitor AVC using graphical charts for monitoring and per-interface statistics
System health monitoring		
31	System health (Access/Distribution)	Monitor system health for CPU usage, memory consumption, and memory leaks during longevity.

Table 5 continued

System & network resiliency, robustness		
32	System resiliency (Access/Distribution)	Verify system level resiliency during the following events: ▪ Active switch failure ▪ Standby/Member switch failure ▪ EtherChannel member link flaps ▪ Stack power failure ▪ VSL link failure ▪ Stack merged logs with radio active tracing.
33	Typical deployment events, triggers (Access/Distribution)	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 ▪ VSL link flap

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.