CISCO VALIDATED PROFILE

Access Switching Healthcare Profile

April 2017

Table of Contents

Profile Introduction 1

- Security 1
- Network Services 1
- Network Segmentation 1
- Efficient Network Management 1
- System & Network Resiliency 1

Network Profile 3

- Hardware & Feature Specifications 4
- Test Environment 6

Use Case Scenarios 9

- Test Methodology 9
- Use Cases 9

Appendix A 14

Profile Introduction

The Enterprise market segment can be divided into five broader verticals: Healthcare, Educational, Financial, Retail and Government. This document focuses on a typical Healthcare deployment profile, and you can use it as a reference validation document for Hospital or Medical Center deployment.

The following sections describe the key considerations for the Healthcare Vertical.

SECURITY

The healthcare system needs to protect patient personal medical records and financial information. Security-rich features such as dot1x, MAB, Guest-access (centralized), CISF (Catalyst Integrated Security Features), and Cisco TrustSec (CTS) are deployed to provide identity-based services securely.

NETWORK SERVICES

The healthcare system must enable traditional and specialized resources in order to provide reliable access and faster delivery of electronic medical records (EMRs), electronic health records (EHRs), and medical and diagnostic lab reports needed for the collaborated care services. Network services such as video delivery and Quality of Experience with Custom QoS and Auto QoS are deployed to allow collaborated care services between lab, doctors, nurses, caregivers, and patient facilities. MPLS VPNs provides a secure, flexible, and scalable way to form logical segmentation. Multicast VPNs allows transport of IPv4 multicast over the Unicast MPLS VPN backbone encapsulated in GRE tunnels.

NETWORK SEGMENTATION

Optimizing the existing network using technologies such as VRF-Lite, GRE, Private VLAN, and MPLS VPN helps in effective IP address use, as well as providing the required network segmentation to meet healthcare system needs, such as separation among medical staff, medical equipment, and DMZ servers while providing VPN and guest access services.

EFFICIENT NETWORK MANAGEMENT

Network administrators should be able to efficiently manage and monitor their networks to quickly respond to the dynamic needs of the healthcare system. 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.

SYSTEM & NETWORK RESILIENCY

The healthcare system and hospital emergency departments cannot afford to have larger downtimes, which calls for strict system and network level resiliency. Stack HA, EtherChannel link-level resiliency BFD, Virtual Switching System (VSS), First-Hop Redundancy Protocol (FHRP) and Gateway Load Balancing Protocol (GLBP) help in meeting such demands at different levels of the network.

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

Table 1 *Healthcare profile feature summary*

Deployment areas	Features
Security	Dot1x, MAB, CISF, ACL, guest access, Cisco TrustSec
Network services	Multicast, Multicast over GRE, Multicast VPN, QoS, AutoQoS
Network segmentation	VRF-Lite, GRE, Private-VLAN, MPLS VPN
Network planning & troubleshooting	NetFlow, SPAN, Wireshark
Efficient network management	Cisco Prime Infrastructure, WebUI
System & network resiliency	EtherChannel, BFD, Stack HA, FHRP, GLBP, VSS

Network Profile

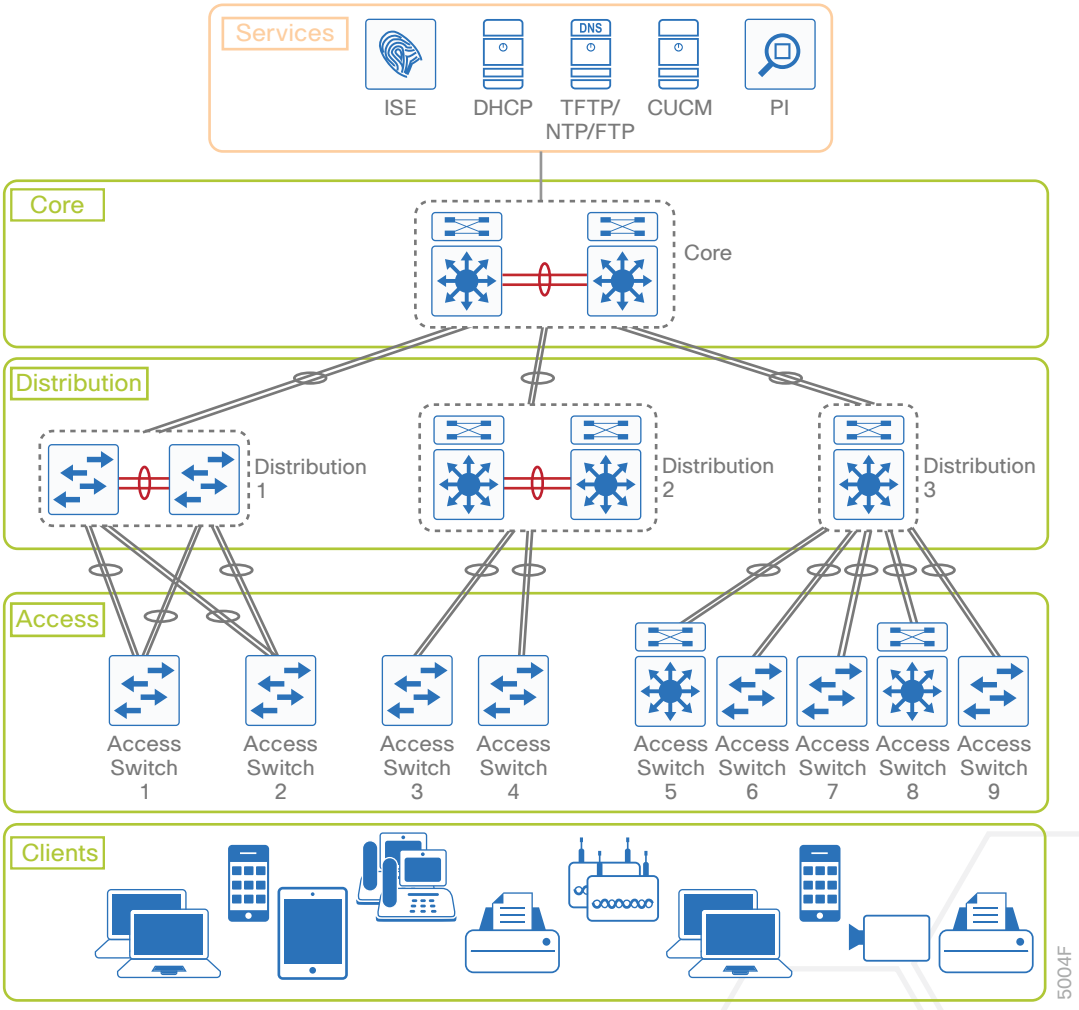
Based on the research, customer feedback, and configuration samples, the Healthcare Vertical Profile is designed with the three tier architecture with Hybrid (L2/L3) access.

Figure 1 shows the topology that is used for the validation of the Healthcare 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 *Healthcare Vertical Profile: topology overview*



Site-1 (the left-portion of the topology) represents a block of a Hospital deployment where a Cisco Catalyst 3850 and 3650 are deployed in access layer. The 3850 in the distribution layer is 10G.

Site-2 (the middle portion of the topology) represents another block of the Hospital deployment, where a 3850 and 3650 are in the access layer and a 4500 is in the distribution layer.

Site-3 (the right portion of the topology) represents another block of Hospital deployment with Cat4KSUP7E/7LE, 2960X, 3560CX, Cat4KSUP8E/8LE and C2960-L in the access layer and a Catalyst 4500 in the distribution layer. All sites use common Cat6500 in the core layer. Based on the size of the campus, its geographical location and user-scale, there might be more distribution switches connecting to the core layer.

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 endpoints 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 3-M stack Switch2: C3650 3-M stack Switch3: C3850 7-M stack Switch4: C3650 3-M stack Switch5: Cat4K- SUP7E/7LE Switch6: 2960X 4-M stack Switch7: C3560CX 4-M Stack Switch8: Cat4K-SUP8E/8LE Switch9: C2960-L	802.1x, MAB, CWA, AAA, Radius Custom IPv4 Ingress/Egress QoS DHCP snooping, DAI, ARP ACL, Port Security, Storm Control, IPSG IPv4 Input/output ACL L3-EtherChannel CTS manual (no-encap) SNMP Multicast–PIM-SM, PIM-SSM(IGMPv3), PIM-DM, IGMP Snooping Static route VRF-Lite Private-Vlan SPAN, R-SPAN, FNF Named VLAN ERSPAN OSPF MCASToGRE LDP BGP MPLS BFD L3VPN MVPN
Distribution	Dist1: WS-3850-48XS,WS-3850-48XS Dist2: Cat4K-VSS (SUP8E) Dist3: Cat4K-SUP8E/8LE	VSS OSPF, BGP Static route Multicast–PIM-SM, PIM-SSM, PIM-DM L3 EtherChannel CTS manual (no-encap) DHCP HSRP, GLBP MCASToGRE LDP, MPLS, L3VPN, MVPN BFD
Core	Core1: Cat6K-VSS	OSPF Multicast L3 EtherChannel LDP BGP MPLS BFD L3VPN

Hardware Profile

Table 3 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end Healthcare 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 DP7	For network management
Cisco ISE	Version 2.1	Radius server used for authentication, authorization
CUCM	Version 10.1	CUCM server for managing IP Phones
Cisco UCS Server	ESXi 5.5.0	To manage and host the virtual machines
Ixia	IxNetwork and IxExplorer version 7.5.1	Generate traffic streams, emulate clients, emulate HTTP traffic
Cisco Unified IP Phones 7945, 7960	Cisco IP phones	Endpoints
Windows laptops	Windows 7/8	Endpoints
Printer	NA	Endpoints
IP camera	NA	Endpoints
PC with Cisco AnyConnect	Windows 7/8	Endpoints
MacBook Pro laptops	OSX 10.10.x	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 respective 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 *Healthcare Profile: feature scale*

Feature	Scale
EtherChannels	6-8
VLANs	1k
STP	64
MAC Learning	1k MAC addresses
Storm Control (bcast)	128 interfaces
IPv4 ACLs/ACEs(RACL/PACL)	20 ACLs (10 Cisco ACEs per ACL)
Static routes	16 IPv4
SSH server	All switches
NTP client	All switches
SPAN/RSPAN	2/2
Stacking	3 up to 9 members
802.1Q VLAN trunking	6 trunks
SVI	64
IGMP Snooping	300 groups
NetFlow	6 monitors+2k flows
QoS	40 classes+11 policy-maps+38 policers
SNMP	PI/MIB walks
DHCP Snooping	600 clients
IP phones (MAB Clients)	50 phones per switch stack
WebAuth Clients	10 PCs (real+emulation)
IPDT	Enabled on interface and vlan
Dot1x Clients	500 (real+emulation) Per Switch stack
MAB Clients	50 phones per switch stack
WebAuth Clients	20 PCs (real+emulation)
Port-Security	128 Interfaces
IPv4 Clients	50 per switch stack
EtherChannels	6-8
Multicast	1k mcast groups
VRF-Lite	15
GRE Tunnels	5
Private VLAN	Community group–3 or 4 , promiscuous port–1, isolated port–2
BFD	20
MCASToGRE tunnels	10
MPLS VRF	20

Table 4 continued

MPLS Label Scale	1k
MPLS IPv4 VPN Routes	1k
MVPN VRF	10
MVPN Groups	1k
LDP sessions	6
BGP Sessions	5

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 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 image with existing 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/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 were executed on the Healthcare 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, optimizing network & traffic, 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 (Access/Distribution)	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, Archive Download
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	ACL (Access/Distribution)	Network admin to deploy input/output PACL, RACL and VACL with large number of ACEs for various traffic patterns (IPv4)

Table 5 continued

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-Host, Multi-Auth ▪ AuthZ : dACL, Dynamic VLAN ▪ Clients spread across open, closed and low impact modes ▪ Critical VLAN ▪ Reauthentication timers
5	Auth-Manager Mode (legacy) (Access)	Network admin wants to deploy end-point/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, Host Mode : Multi-Domain ▪ Dot1x, MAB: PCs, Phones. Host mode: Single Host, Multi-Host, Multi-Auth ▪ AuthZ : dACL, Dynamic VLAN ▪ Clients spread across open, closed and low impact modes ▪ Critical VLAN ▪ Reauthentication timers
6	Guest-Access (Access)	Network admin wants to provide temporary guest access CWA ▪ CWA–Self Register Guest Portal
Network Segmentation		
7	VRF-Lite (Access/Distribution)	Network admin to provide VPN connectivity and optimize the use of IP address, using the VRF-Lite ▪ VRF routing using overlapped IP addresses
8.	GRE (Access/Distribution)	Network admin to provide logical isolation between the VPNs and share dedicated network resources using GRE to provide Guest and Partner access. ▪ Path Isolation between the VPNs using GRE tunnels.
9	Private VLAN (Access/Distribution)	Network admin to deploy Private VLAN for efficient IP address aggregation ▪ Primary VLAN, Secondary VLAN ▪ Isolate port, Community port, Promiscuous port on the physical interface depending on the connected endpoints
10	MPLS VPN	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

Table 5 continued

Network services		
11	Multicast VPN	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
12	MCASToGRE	Network admin want to configure network to use point-to-point GRE tunnels to send Protocol Independent Multicast (PIM) and multicast traffic between source and receivers separated by an IP cloud that is not configured for IP multicast routing. ▪ IPv4 Multicast over GRE Tunnels ▪ PIM-SSM and PIM-SM modes
13	Multicast Video (Access/Distribution)	Network admin wants to enable and deploy multicast services. ▪ V4 & V6 Multicast ▪ L2/L3 Multicast video delivery using PIM-SM, PIM-SSM, IGMP/MLD Snooping ▪ PIM-SM with static RP, auto RP, PIM-SSM with static RP
14	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 ▪ AutoQoS on certain ports that are connected to endpoints
Monitoring & troubleshooting		
15	NetFlow (Access/Distribution)	Enable IT admins to determine network resource usage and capacity planning by monitoring L2/IPv4 traffic flows using Flexible NetFlow ▪ Traffic types: L2, IPv4 ▪ FNFv9, IPFIX-v10 ▪ Prime Collector
16	SPAN, Wireshark (Distribution/Access)	Network admin should be able to troubleshoot the network by capturing and analyzing the traffic. ▪ SPAN, Wireshark–Dataplane & Control Plane Capturing
Simplified management		
17	Prime-Manage-Monitor	Network admin wants to manage and monitor all the devices in the network using Cisco Prime Infrastructure.

Table 5 continued

18	Prime-SWIM	Network admin should be able to manage images on network devices using Cisco Prime Infrastructure for upgrade/downgrade.
19	Prime-Template	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
20	Prime-Troubleshooting	Simple 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
21	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
22	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 ▪ Implement Quality-of-Service using Cisco-recommended AutoQoS
23	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.
24	WebUI-System Management	Network admin routinely perform 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.

Table 5 continued

System health monitoring		
25	System Health (Access/Distribution)	Monitor system health for CPU usage, memory consumption, and memory leaks during longevity
System & network resiliency, robustness		
26	System Resiliency (Access/Distribution)	Verify system level resiliency during the following events: ▪ Active switch failure ▪ Standby/Member switch failure ▪ Etherchannel LACP rate fast ▪ EtherChannel member link flaps
27	Network Resiliency (Access/Distribution)	High availability of the network during system failures using: ▪ Bidirectional Forwarding Detection ▪ VSS/FHRP ▪ GLBP
28	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

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.