Wireless Healthcare Vertical

April 2016

Table of Contents

Profile Introduction

The Enterprise market segment can be divided into five broader verticals: Education, Healthcare, Retail, Service Provider, and Government. This document focuses on a typical Healthcare deployment profile, and you can use it as a reference validation document.

Healthcare network environments combine the technology requirements of a specialized set of demands that include security needs, enhanced network services, efficient network management, seamless mobility, network high availability, and location services.

The following sections describe the challenges specific to these environments.

SECURITY

Healthcare providers need to protect personal, patients', 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

Healthcare infrastructures must enable traditional and specialized resources in order to provide accessibility and speed. Network services such as video delivery, BYOD, PTT, AVC, and Quality of Experience with custom QoS are deployed.

EFFICIENT NETWORK MANAGEMENT

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.

MOBILITY

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

HIGH AVAILABILITY

Healthcare 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.

LOCATION SERVICES

Connected Mobility Experience (CMX) can be used to manage and monitor location of patients and the medical devices.

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

Table 1 *Healthcare Profile feature summary*

| Deployment areas	Features
Security	Rogue detection and containment
	Intrusion Prevention (WDS/wIPS)
	Dot1x
	Guest Access (CWA, LWA)
Network services	Video Content Delivery (L2/L3 Multicast)
	BYOD
	Push-To-Talk
	AVC
	Custom QoS
Network planning & troubleshooting	NetFlow
	RF Sniffer
Efficient network management	Cisco Prime Infrastructure, WebUI
Mobility	Fast roaming OKC, CCKM
	802.11 r/k/v
	Fast SSID
High availability	Client SSO
	N+1 Redundancy
Location services	Cisco Connect Mobility Experience (CMX) Location Analytics

Network Profile

Based on the research, customer feedback, and configuration samples, the Healthcare 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 Healthcare Network Two-Tier design that is used for the validation of the Healthcare Vertical Profile.

The topology represents a typical Healthcare deployment with a Cisco Catalyst 6500 collapsed core in the distribution 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/distribution layer.

Figure 1 *Healthcare Vertical Profile: topology overview*
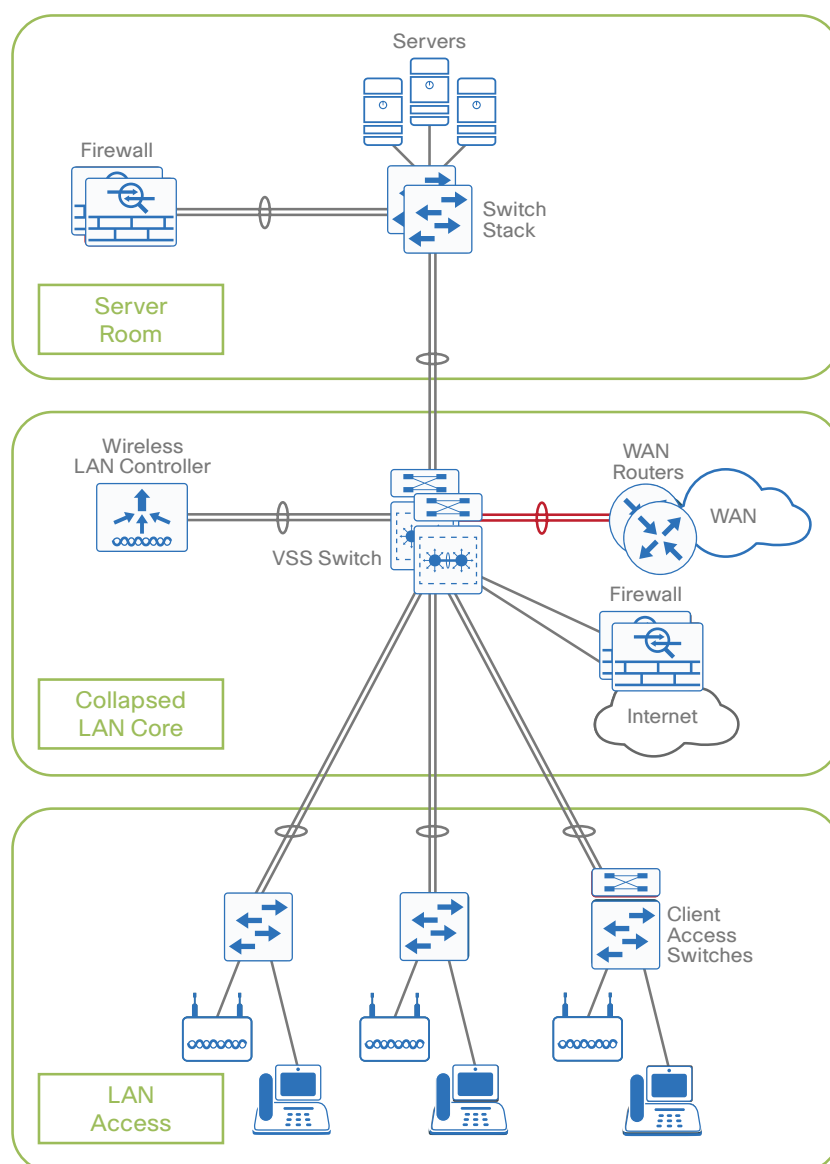
HARDWARE PROFILE

Table 2 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end Healthcare 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
Cisco Prime	Version 3.0	For Network Management
Cisco ISE	Version 1.3/1.4	Radius Server used for authentication, authorization,
CUCM	Version 10.1	CUCM Server for managing IP phones
CMX	Version 10.2.1	Location Services
DNS/AD Server	Windows 8 Enterprise Server	Windows External server for DNS and Active Directory management
APIC-EM Plug-n-Play	Version 1.0.1	For Day0 Config and Image Management
Cisco UCS Server	ESXi 5.5	To manage and host the virtual machines
Ixia	IxNetwork/ixExplorer	Generate traffic streams and to emulate dot1x clients
Ixia Veriwave	Veriwave	Wireless Endpoints with scale.
Vocera Badge	Paging device	Endpoints
Spectra Link	SIP Phone	Endpoints
Cisco Unified IP Phones 796x, 796x, 9971	Cisco IP phones	Endpoints
Laptops	Windows 8, 10	Endpoints
Macbook	Mac OSX	Endpoints for SDG
IP camera		Endpoints
Wireless printers		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 respective feature.

Table 3   *Healthcare Profile: feature scale*

Feature	Scale
Access points	800 APs (WLC–5520), 400 APs (WLC–5508)
Clients	10K clients (WLC–5520), 5K Clients (WLC–5508)
WLANs	450
AP groups	500
Wireless interface	500
Trap Receivers	6
IPv4 ACLs	64
IPv6 ACLs	64
Mobility groups	10
IGMP snooping	300 groups
NetFlow	6 monitors+2k flows
SNMP	PI/MIB walks

Use Case Scenarios

TEST METHODOLOGY

The use cases listed in Table 4 below are executed using the Topology defined in Figure 1, along with the Test environment already explained in Table 3.

With respect to the Longevity for this profile setup, CPU and memory use is monitored overnight and during the weekends, along with any mem-leak checks. 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 Healthcare Vertical Profile. These Use cases are divided into buckets of technology areas to see the complete coverage of the deployment scenarios.

These technology buckets comprises of System Upgrade, Security, Network Services, Monitoring & Trouble-shooting, simplified management, system health monitoring along with system and network resiliency.

Table 4 *List of use case scenarios*

No.	Focus area	Use cases
System upgrade		
1	Upgrade	Network Administrator should be able to perform WLC upgrade and down-grade between releases seamlessly. · All of the configuration should be migrated seamlessly during the up-grade/downgrade operation · SW Install, Clean, Expand
Security		
2	On-Wire Attacks	Network admin wants to detect and mitigate on-wire attacks. · Rogue on wired detection, containment.
3	Over-the-Air Attacks	Network admin wants to detect and mitigate wireless thread. · Adaptive wIPS · Enhanced Local Mode (ELM) wIPS
4	Guest-Access	Network admin wants to provide temporary guest access using the LWA and CWA. · LWA—Custom/Default Pages · CWA—Self Register Guest Portal

Table 4 continued

Network services		

5	Multicast Video	Network admin wants to enable and deploy multicast services.
		
		  • V4 & V6 Multicast
		
		  • L3/L2 Multicast video delivery using PIM-SM, SSM, IGMP/MLD Snooping

6	Multicast Voice	Hospital staffs page nurses and doctors on duty.
		
		  • Vocera badge
		
		  • Spectra Link

7	Custom QoS	Network admin needs to enhance user experience by ensuring traffic and application delivery using custom QoS policies.
		
		  • Traffic types: VOIP, Video, Call Control, Transactional Data, Bulk Data, Scavenger
		
		  • Policing Ingress and Priority & BW Management in Egress

8	Location	Hospital staffs should be able to track newborn babies, patients, and medical devices on the floor.
		
		  • Hyper location with Halo
		
		  • RFID

9	Plug-n-Play	Simplify network provisioning of new switches by Zero-Touch-Deployment for Day0 using NG-PNP app via APIC-EM for image and config management.
Monitoring & troubleshooting		
10	Client Troubleshooting	Network admin should be able to troubleshoot client connectivity issue. • Service Assurance

11	NetFlow	Enable IT admins to determine network resource usage and capacity planning by monitoring IP traffic flows using Flexible NetFlow.
		
		  • Traffic Types: L2, IPv4, IPv6
		
		  • Lancope
		
		  • Prime Collector, Live Action

Simplified management		
12	Prime-Manage-Monitor	Network admin wants to manage and monitor all the devices in the network using Cisco Prime Infrastructure
13	Prime-SWIM	Network admin should be able to manage images on network devices using Cisco Prime Infrastructure for upgrade/downgrade.

Table 4 continued

14	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
15	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
System health monitoring		
16	System Health	Monitor system health for CPU usage, memory consumption, and memory leaks during longevity
System & network resiliency, robustness		
17	System Resiliency	Verify system level resiliency during the following events: • Active WLC failure • Standby WLC failure • RP link flaps • Power failure • LAG failure • AP Failure
18	Network Resiliency	High availability of the network during system failures using: • VSS
19	Negative Events, Triggers	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 • Burst client association • Radius failure • DHCP failure

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.

Cisco Validated Profile

B-875CVP-1 04/16