CISCO VALIDATED PROFILE

Wireless
SP WiFi 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 Service Providers (SPs) deployment profile, and you can use it as a reference validation document.

SPs seek new ways to accommodate the surge in mobile data traffic and the variety of smart, portable devices coming onto their networks. As mobile devices proliferate, so do the opportunities to strengthen relationships with customers by delivering a superior subscriber or end-user experience. Fixed and mobile operators are therefore looking at both licensed and unlicensed Wi-Fi technologies to meet the demand and to expand customer footprint. Trusted Wi-Fi hotspots can be integrated into the existing SP policy and accounting infrastructure, thereby allowing the SP to maintain subscriber accountability. At the same time, traffic from these trusted Wi-Fi hotspots can be integrated into the existing packet core of the SP by using the standard Proxy Mobilize IPv6 (PMIPv6) interface to provide IP mobility across Wi-Fi and 4G networks to enhance subscriber experience.

Service Providers' network environments combine the technology requirements of a specialized set of demands that includes security, enhanced network services, efficient network management, location services, and network high availability. The following sections describe the challenges specific to these environments.

SECURITY

Security is one of the most important requirements for Service Providers. Security-rich features such as Intrusion Prevention (WDS/wIPS), Rogue detection/containment, TACACS+, Dot1x, and guest-access (centralized and local web-auth) are deployed.

SPECIALIZED SERVICES

Often the cable operators are leveraging Wi-Fi as an access technology for Wi-Fi offload. Service provider features such as Hotspot 2.0, EoGRE, PMIPv6, Custom QoS (Air Time Fairness, Bandwidth Contract), AVC, and NetFlow 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.

HIGH AVAILABILITY

Service Providers' 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

Service Providers should be able to efficiently and accurately locate devices in order to deliver customed information to them. SPs can use connected Mobility Experience (CMX) Connect, CMX Presence Analytics, and BLE Beacon to manage and monitor location and deliver customed information to the devices.

PERFORMANCE AND SCALABILITY

Service Providers require high performance and a scalable controller to manage their large customer base. Various models of Wireless Controller (WLC 8510, WLC 8540) and 802.11AC Access Point (AP1852, AP2700, AP3700) can meet the demand for both scalability and performance.

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

Table 1 SP Profile feature summary

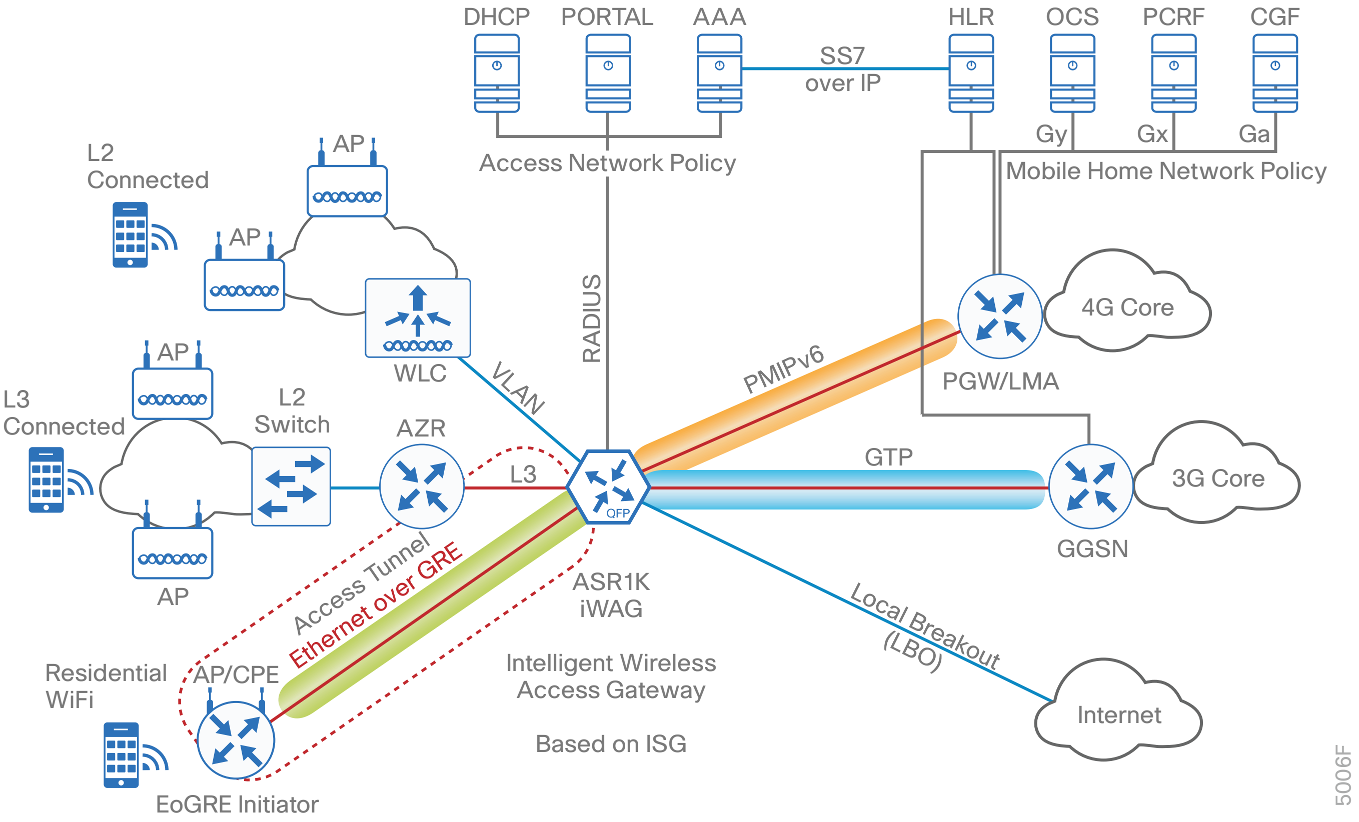
Deployment areas	Features
Security	Rogue detection and containment Intrusion Prevention (WDS/wIPS) Dot1x, EAP-SIM, EAP-AKA Guest Access (CWA, LWA)
Network services	Video Content Delivery BYOD QoS ATF AVC,
SP services	HotSpot 2.0 EoGRE PMIPv6 Flex Locally Switched/Central Auth
Mobility	Fast roaming OKC, CCKM 802.11 r/k/v Fast SSID
Network planning & troubleshooting	NetFlow RF Sniffer
Location services	CMX Presence CMX Connect BLE Beacon
Efficient network management	Cisco Prime Infrastructure, WebUI
Performance and scalability	High capacity WLCs (WLC-8510, WLC-8540), High performance APs (AP3700, AP2700, AP1852)

Network Profile

Based on the research, customer feedback, and configuration samples, the Service Providers 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 SP 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 Service Providers Vertical Profile deployment.

The list of hardware, along with the relevant software versions and the role of these devices, complement the actual physical topology that is 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	Version 1.3/1.4	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	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, ATA	Endpoints
Cisco Unified IP Phones 796x, 796x, 9971	Cisco IP phones	Endpoints
Laptops	Windows 8, 10	Endpoints
Macbook	Mac OSX	Endpoints for SDG
Apple iPad, iPhone	Apple iOS	Endpoints
Android Phone, Tablet	Android	Endpoints
IP camera		Endpoints
Printer		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   *SP WiFi Profile: feature scale*

Feature	Scale
Access points	5000 APs (WLC-8510 or WLC-8540) (Real and simulated)
Clients	50K Clients (Real and simulated)
WLANs	450
AP groups	500
Wireless interface	500
Trap receivers	6
IPv4 ACLs	64
IPv6 ACLs	64
Mobility 2oups	10
IGMP snooping	300 groups
NetFlow	6 monitors+2k flows
SNMP	PI/MIB walks

The following table describes the WAN characteristic under different test conditions with various scales. The recommendation (per Design and confirmed with Product Management) is 24 kbps/AP, but we tested at 12.8 kbps, which was in some of the deployment guides.

Table 4   *WAN Link Matrix*

Num APs	Link Bandwidth (kbps)	WAN Link RTT (ms)	MTU (Bytes)	Flex AVC	Test Scenario
1	15	300	1500	Enabled	Twenty-five clients sending traffic on Local Switch WLAN, Flex AVC enabled, wIPs, rogue detection on all APs and Clean Air
5	64	300	1500	Disable	Local Switch WLAN, wIPs, rogue detection on all APs and Clean Air
40	512	300	1000	Disable	WAN link with smaller MTU size, Local Switch WLAN, wIPs, rogue detection on all APs and Clean Air
50	640	300	576	Disable	WAN link with smaller MTU size, Local Switch WLAN, wIPs, rogue detection on all APs and Clean Air
6	128	300	1500	Disable	L2 intra-controller roaming on two APs in same FlexConnect Group with one hundred clients

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 Tables 3 and 4.

With respect to the longevity for this profile setup, the CPU and memory usage are monitored overnight and during the weekends, along with any memory-leak checks. In order to test the robustness, certain negative events would be triggered during the use-case testing.

USE CASES

Table 5 describes the Use Cases that were executed on the Service Providers 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, location, mobility, 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	Network administrator should be able to perform WLC 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	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 5 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, IGMP/MLD Snooping
6	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 ▪ Policing Ingress and Priority & BW Management in Egress ▪ Air Time Fairness
7	Location	Connect Experiences ▪ Hyper location with Halo ▪ RFID ▪ Hotspot 2.0
8	WiFi Offload	Service providers use Wi-Fi to offload 4G network. ▪ PMIPv6 ▪ EoGRE
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 issues. ▪ SPAN, Remote-SPAN ▪ Wireshark–Dataplane & Control Plane Capturing
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 5 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.

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.