CISCO VALIDATED PROFILE

# Wireless Government 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 Government deployment profile, and you can use it to design a resilient and an efficient government branch infrastructure.

The following sections describe the focus of the Government Profile.

## SECURITY

Security-rich features such as rogue detection/containment, Intrusion Prevention (WDS/wIPS), DOT1X, ACL, and guest-access (centralized and local web-auth) are deployed.

## SPECIALIZED SERVICES

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

## 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 and IPv6 Multicast are enabled for this Government vertical guide.

## 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

Government 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.

## 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.

## PERFORMANCE AND SCALABILITY

Governments face tight IT budgets and steep technology demands. Various models of Wireless Controller (WLC 5520, WLC 8540) and 802.11AC Access Point (AP1832, AP1852, and AP3700) can meet the demand for both scalability and performance.

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

*Table 1* *Government Profile Feature Summary*

| Deployment areas | Features |
|---|---|
| Security | Rogue detection and containment<br>Intrusion Prevention (WDS/wIPS)<br>Dot1x Authentication<br>Guest Access: Local WebAuth, Central WebAuth |
| Network services | Video Content Delivery (L2/L3 Multicast)<br>Application, Visibility, and Control (AVC)<br>Custom QoS |
| IPv6 migration | Dual Stack, IPv6 security |
| Mobility | Fast roaming OKC, CCKM<br>802.11 r/k/v<br>Fast SSID |
| High availability | Client SSO<br>N+1 Redundancy |
| Network planning & trouble-shooting | NetFlow<br>RF Sniffer |
| Efficient network management | Cisco Prime Infrastructure<br>WebUI |
| Performance and scalability | High Performance/Capacity Wireless Controller and Wave 2 Access Points. |

# Network Profile

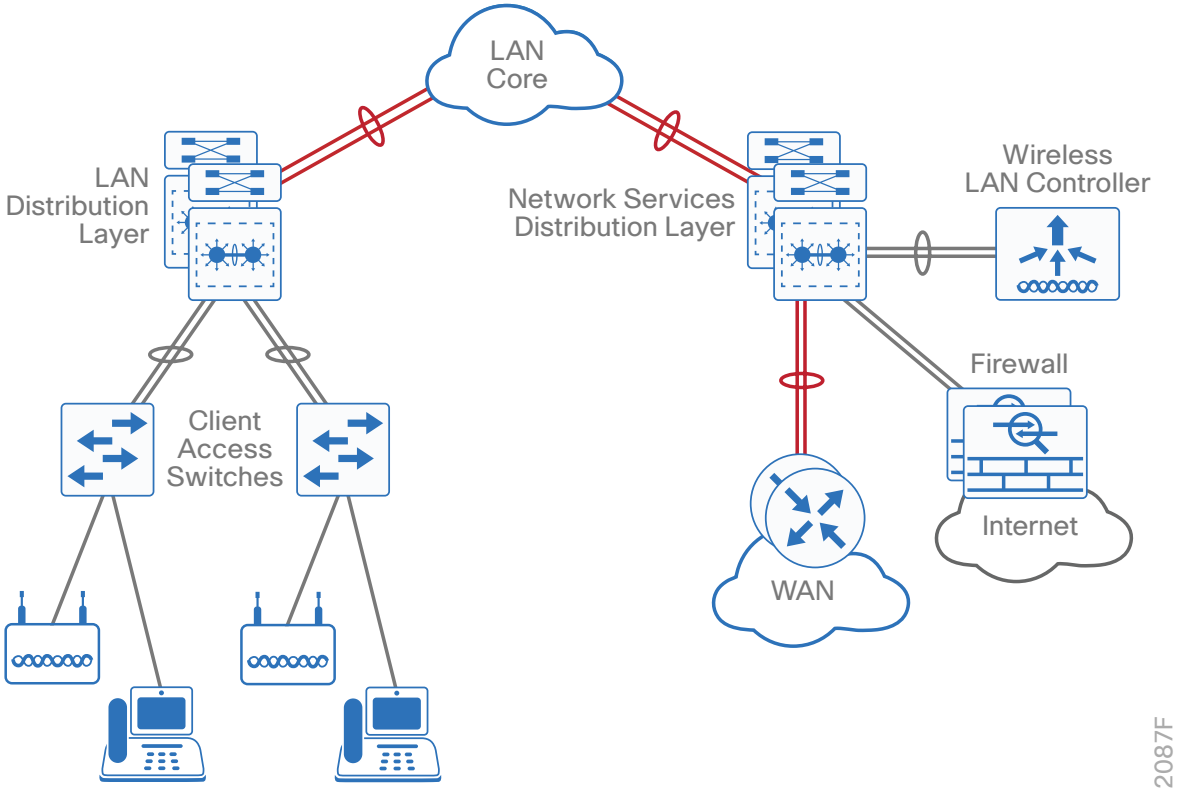
Based on the research, customer feedback, and configuration samples, the Government Vertical Profile is designed with a deployment topology that is generic and can easily be modified to fit any specific deployment scenario.

## TOPOLOGY DIAGRAM

Figure 1 shows the University Campus three-tiers design that is used for the validation of the Government Vertical Profile.

The topology represents a typical University Campus deployment with a Cisco Catalyst 4500/Catalyst 6500 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.

*Figure 1* *Government 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 Government 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 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 |
| DNS/AD Server | Windows 8 Enterprise Server | Windows External server for DNS and Active Directory management |
| APIC-EM<br>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. |
| Cisco Unified IP Phones 796x, 796x, 9971 | Cisco IP phones | Endpoints |
| Laptops | Windows 8, Windows 10 | Endpoints |
| Macbook | Mac OSX | Endpoints for SDG |
| Apple iPhone/iPad | | 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* *Government Profile: feature scale*

| Feature | Scale |
|---|---|
| Access points | 800 APs (WLC-5520 (real and simulated) |
| Clients | 10K clients (WLC-5520) (real and simulated) |
| 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 shown in Table 3.

With respect to the Longevity for this profile setup, CPU and Memory use are 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 Governmental 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 & trouble-shooting, simplified management, and 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.<br>▪ All of the configuration should be migrated seamlessly during the up-grade/downgrade operation.<br>▪ SW Install, Clean, Expand |
| Security | | |
| 2 | On-Wire Attacks | Network admin wants to detect and mitigate on-wire attacks.<br>▪ Rogue on wired detection, containment |
| 3 | Over-the-Air Attacks | Network admin wants to detect and mitigate wireless thread.<br>▪ Adaptive wIPS<br>▪ Enhanced Local Mode (ELM) wIPS |
| 4 | Guest-Access | Network admin wants to provide temporary guest access using the LWA and CWA.<br>▪ LWA–Custom/Default Pages<br>▪ CWA–Self Register Guest Portal |

*Table 4 continued*

| | | |
|---|---|---|
| Network services | | |
| 5 | Multicast Video | Network admin wants to enable and deploy multicast services.<br>▪ V4 & V6 Multicast<br>▪ L3/L2 Multicast video delivery using PIM-SM, SSM, IGMP/MLD Snooping |
| 6 | Custom QoS | Network admin needs to enhance user experience by ensuring traffic and application delivery using custom QoS policies.<br>▪ Traffic types: VOIP, Video, Call Control, Transactional Data, Bulk Data, Scavenger<br>▪ Policing Ingress and Priority & BW Management in Egress |
| 7 | 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 configuration management. |
| Monitoring & troubleshooting | | |
| 8 | Client Troubleshooting | Network admin should be able to troubleshoot client connectivity issue.<br>▪ Service Assurance |
| 9 | NetFlow | Enable IT admins to determine network resource usage and capacity planning by monitoring IP traffic flows using Flexible NetFlow.<br>▪ Traffic Types: L2, IPv4, IPv6<br>▪ Lancope<br>▪ Prime Collector, Live Action |
| Simplified management | | |
| 10 | Prime-Manage-Monitor | Network admin wants to manage and monitor all the devices in the network using Cisco Prime Infrastructure. |
| 11 | Prime-SWIM | Network admin should be able to manage images on network devices using Cisco Prime Infrastructure for upgrade/downgrade. |
| 12 | Prime-Template | Network admin wants to configuration deployment using Cisco Prime Infrastructure.<br>▪ Import and deploy customer specific configuration templates.<br>▪ Schedule configuration for immediate or later deployment<br>▪ Simplify configuration using config-templates |

*Table 4 continued*

| | | |
|---|---|---|
| 13 | Prime-Troubleshooting | Simplify network troubleshooting and debugging for IT admins.<br>▪ Monitor & troubleshoot end-end deployment via maps & topologies<br>▪ Monitor network for alarms, syslogs and traps<br>▪ Troubleshoot network performance using traffic flow monitoring. |
| System health monitoring | | |
| 14 | System Health | Monitor system health for CPU usage, memory consumption, and memory leaks during longevity |
| System & network resiliency, robustness | | |
| 15 | System Resiliency | Verify system-level resiliency during the following events:<br>▪ Active WLC failure<br>▪ Standby WLC failure<br>▪ RP link flaps<br>▪ Power failure<br>▪ Partial LAG failure<br>▪ AP Failure |
| 16 | Network Resiliency | High availability of the network during system failures using:<br>▪ VSS |
| 17 | Negative Events, Triggers | Verify that the system holds well and recovers to working condition after the following events are triggered:<br>▪ Config Changes–Add/Remove config snippets, Default-Interface configs<br>▪ Link Flaps, SVI Flaps<br>▪ Clear Counters, Clear ARP, Clear Routes, Clear access-sessions, Clear multicast routes<br>▪ IGMP/MLD Join, Leaves<br>▪ Burst client association<br>▪ Radius failure<br>▪ DHCP failure<br>▪ WLAN Flaps |

# 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.