CISCO VALIDATED PROFILE

Access Switching Government Profile

April 2017

Table of Contents

Profile Introduction

The Enterprise market segment can be divided into five broader verticals: Government, Financial, Health, Retail, and Government. This document covers the Government branch vertical.

This document focuses on a typical Government branch deployment profile, and network administrators can use it to design a resilient and an efficient government branch infrastructure.

The following section describes the focuses of the Government profile.

SECURITY

Security is one of the main concerns of any Government branch deployment. Special care must be taken to protect data and transactions and even to monitor and authenticate the devices that are being used within the Government branch office.

This Government CVP also covers the supported FIPS compliance scenarios.

SPECIALIZED SERVICES

Network services such as video delivery (Multicast video and data) and Quality of Experience with custom QoS and Auto QoS are deployed.

The Cisco Application Visibility and Control (AVC) solution provides application-level classification and monitoring of the network. It also allows the network administrators to upgrade protocol packs and create their own custom applications that can be monitored.

MIGRATION TO IPV6

Devices increasingly run on IPv6, while network infrastructures are likely to continue on IPv4.

Dual Stack deployment with features such as IPv6 access, IPv6 FHS, and IPv6 Multicast are enabled for this Government vertical guide.

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.

SYSTEM AND NETWORK RESILIENCY

Government branch offices would require a robust network with strict system and network level resiliency. Stack HA, EtherChannel link resiliency, and HSRP/VRRP would help in designing a network that is stable and provides high-availability.

PRICE-PERFORMANCE AND SCALABILITY

Various models of Cisco Catalyst 3850/3650 with high-port density, POE-enabled ports with EnergyWise-capable services are deployed.

The following table lists the key areas on which the Government profile focuses.

Table 1 *Government Profile feature summary*

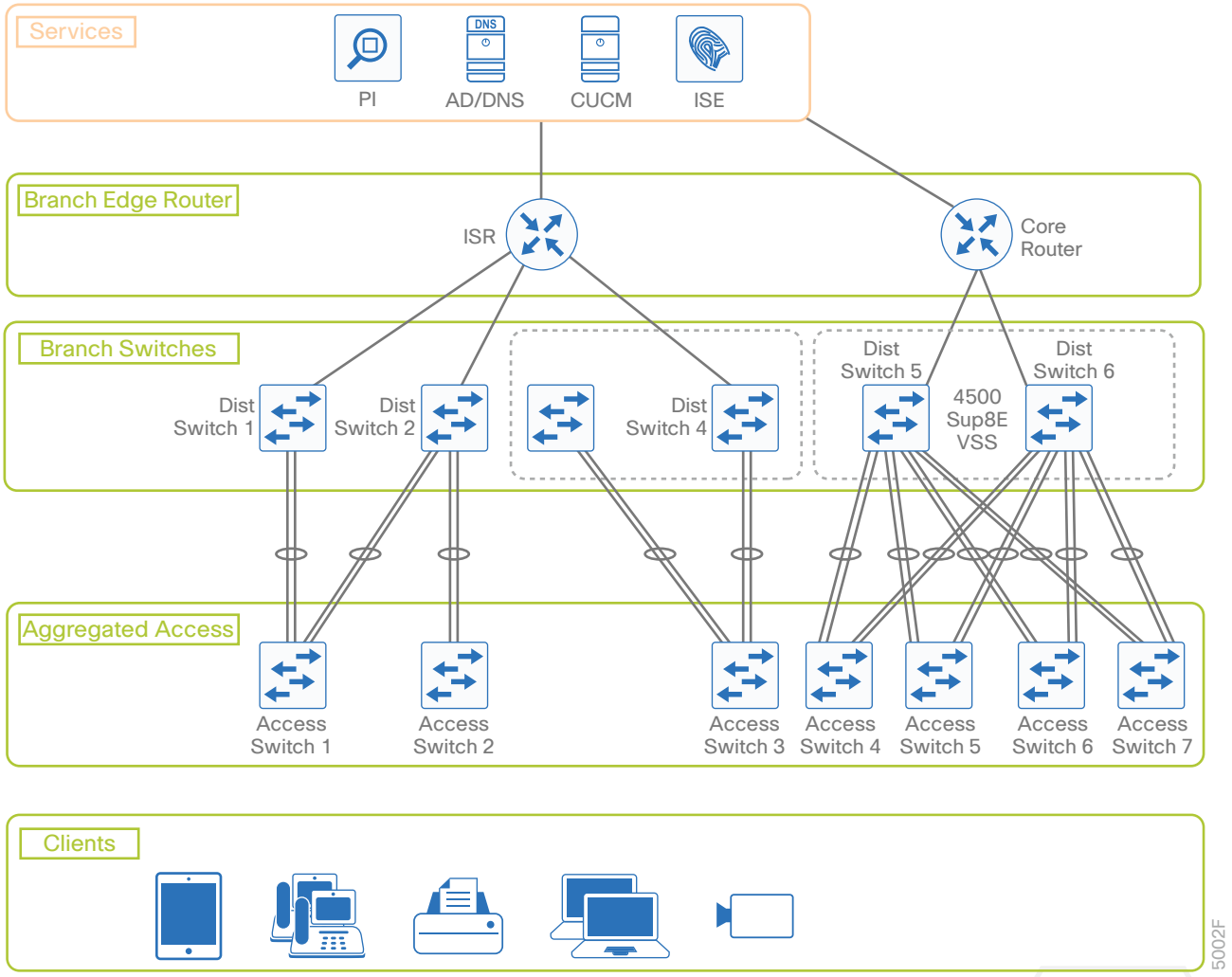
Deployment areas	Features
Security	MAB, dot1x, Guest Access (CWA), CISF, IPv6 FHS FIPS ACL, PACL, dACL, V6VACL, MACsec uplink
Network services	Video content delivery (L2/L3 Multicast), Custom QoS, AutoQoS, AVC
IPv6 migration	Dual Stack, V6 multicast, IPv6 FHS and Security
Network planning & troubleshooting	NetFlow, SPAN, Flow SPAN R-SPAN, ER-SPAN, Wireshark
Efficient network management	Cisco Prime Infrastructure, WebUI
System and Network resiliency	EtherChannel, HSRP/VRRP, VRRPv3
Price-performance	EnergyWise, PoE, high-port density, mGIG chassis, collapsible core/distribution at smaller sites

Network Profile

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

TOPOLOGY DIAGRAM

Figure 1 *Government Branch Profile: topology overview*



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

HARDWARE & FEATURE SPECIFICATIONS

This section of the guide 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	Platforms	Critical vertical features
Access	Switch1: C3850 3-M stack Switch2: C3650 6-M stack Switch3: C3650-12X48UR Switch4: C4503-E Sup 8-E Switch5: C3750x 5-M stack Switch6: C2960x 4-M stack Switch7: C2960L-24PS-LL	IPv4/V6- Dual Stack Web Auth, 802.1x, MAB, AAA, Radius Custom QoS Ingress/Egress, AutoQoS DHCP snooping, DAI, Port Security, Storm Control, IPSG IPv6 FHS ACL (IPv4/IPv6) EtherChannel EnergyWise, POE (endpoints) SNMP Multicast–IPv4/v6, IGMP/MLD Snooping Radioactive tracing for V6 Multicast SPAN, FNF Private-VLAN Static Routes OSPF, EIGRP V6VACL EtherChannel rate fast AVC BFD FIPS

Table 2 continued

Distribution	Switch1: WS-C3850 3-M stack Switch2: WS-C3650 6-M stack Switch3: C3650-12X48UZ Switch4: C3850-48XS-F Switch5: WS-C4507R+E Sup8-E Switch6: WS-3750X 2-M Stack	HSRP/VRRP VRRPv3 EIGRP OSPF Multicast–IPv4/v6 PIM SSM/SM EtherChannel (L2/L3) Ether Channel rate fast SNMP BFD Custom QoS Ingress/Egress Static Routes
Branch Edge	ISR3945	OSPF Multicast EtherChannel

Hardware Profile

Table 3 defines the set of relevant hardware, servers, test equipment and endpoints that are used to complete the end-to-end Government branch 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 DP6	For network management
Cisco ISE	Version 2.1 Patch1	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
Cisco UCS Server	ESXi 5.5.0	To manage and host the virtual machines
Ixia	IxNetwork and IxExplorer version 6.40	Generate traffic streams and to emulate dot1x clients
Cisco Unified IP Phones 796x, 796x, 9971	Cisco IP phones	Endpoints
Lenovo laptops	Windows 8	Endpoints
IP camera	Sony and Cisco	Endpoints
MacBook Pro laptops	OSX 10.10.x	Endpoints
Printer	Epson	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 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 *Government Profile: feature scale*

Feature	Scale
EtherChannels	8
VLANs	1k
MAC Learning	1k MAC addresses
Storm Control (bcast/unicast/mcast)	128 interfaces
Ipv4 ACLs/ACEs(RACL/PACL)	20 ACLs (10 Cisco ACEs per ACL)
Ipv6 ACLs/ACEs	10 ACLs (10 ACEs per ACL)
SSH server	All switches
NTP client	All switches
Stacking	3M–6M Stack
SVI	64
IGMP Snooping	100 groups
NetFlow	6 monitors+2k flows
QoS	40 classes+11 policy-maps+38 policers
SNMP	PI/MIB walks
DHCP Snooping	500 clients
IP Phones/PCs	20
Dot1x clients	500 (real+emulation) per switch stack
MAB clients	50 phones per switch stack
WebAuth clients	10 PCs
EnergyWise clients	10 (phones+cameras+PCs+printers)
Port-Security	128 interfaces
Dual Stack v4+v6 clients	50 per switch stack
OSPF sessions/routes	4-5 sessions/1k routes
OSPFv3 sessions/routes	4-5 sessions/1k routes
HSRP	50 groups
VRRPV3	50 groups
V6VACL	2 ACL (100 ACEs per ACL)
AVC Flows	20
BFD	6 sessions

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 already explained 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 network events are triggered during the use-case execution process.

USE CASES

Table 5 describes the use cases that were executed on the Government 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, 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 (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

Table 5 continued

Security		
2	Closed-mode (Access)	Network admin wants to secure the network in a closed mode. ▪ Secure endpoints using dot1x, mab ▪ Secure end users using dot1x ▪ PC behind the Phone: AuthC > Dot1x for the PC and MAB for the Phone, HostMode > Multi-Domain ▪ Dot1x, MAB : PCs, phones. Hostmode: Single Host, Multi-Host, Mutli-Auth ▪ AuthZ > Pre-AuthACL, dACL, dVLAN
3	Guest-access (Access)	Network admin wants to provide temporary guest access using CWA. ▪ CWA–Self Register Guest Portal
4	ACLS (Access)	Network admin to deploy input/output PACL, RACL and VACL with large number of ACEs for various traffic patterns (v4/v6) in 3-tier route-access network. ▪ ACL ▪ PACL ▪ dACL ▪ IPV6 VACL Network admin to apply the ACL for telnet, SSH, SNMP to block unauthorized networks/users
5	CISF (Access)	Network admin to secure the L2 access against MITM, DOS attacks using the CISF (Cisco Integrated Security Features) ▪ Port Security, IPSG, DAI, DHCP snooping
6	IPv6 fhs (Access)	Network admin to secure the ipv6 network against mitm, dos attacks by providing control-plane and data-plane filtering using ipv6 fhs (first-hop-security) ▪ ipv6-snooping, nd inspection, ra guard, source, & destination guard, dhcpv6 guard
7	FIPS (Access)	Network admin to ensure FIPS is enabled on all of the network devices and all security encapsulations are working as expected ▪ Enable FIPS ▪ SSH and SSHv2 ▪ IKEv1 and IKEv2 encapsulations and crypto maps

Table 5 continued

Network services		
8	Multicast data and video (Access/distribution)	Network admin wants to enable and deploy multicast services. ▪ V4 & V6 multicast ▪ L3/L2 multicast video delivery using PIM-SM, SSM, IGMP/MLD Snooping ▪ Use radio active tracing for debugging (tracking specific MAC addresses) IPv6 multicast traffic flows
9	EnergyWise (Access)	Enable network admins to measure and manage energy usage in the network by implementing energy saving policies for various endpoints (phones, cameras, PCs) and scenarios (shutdown/sleep/hibernate, wake-on-LAN)
10	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, etc.
11	Custom 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
12	AVC monitoring (Access)	Network admin wants to enable AVC to enhance user experience and monitoring. ▪ Protocol Discovery ▪ AVC protocol classification with Active Switchover ▪ Protocol pack upgrade ▪ Custom Applications ▪ Using WebUI and CLI interface
Monitoring & troubleshooting		
13	SPAN, R-SPAN, ERSPAN, Wireshark (Access/distribution)	Network admin should be able to troubleshoot the network by capturing and analyzing the traffic. ▪ SPAN, Remote-SPAN ▪ Encapsulated Remote Span (ERSPAN) ▪ Wireshark–Dataplane & Control Plane Capturing
14	NetFlow (Access)	Enable IT admins to determine network resource usage and capacity planning by monitoring IP traffic flows using Flexible NetFlow. ▪ Traffic types: IPv4, IPv6 ▪ FNFv9 ▪ Prime Collector

Table 5 continued

Simplified management		
15	Prime-Manage-Monitor	Network admin wants to manage and monitor all the devices in the network using Cisco Prime Infrastructure.
16	Prime-SWIM	Network admin should be able to manage images on network devices using Cisco Prime Infrastructure for upgrade/downgrade.
17	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
18	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
19	Web-UI Day0	Simplify network setup with WebUI Day0 config manager ▪ 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
20	Web-UI 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.
21	Web-UI 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.
System health monitoring		
22	System health (access/distribution)	Monitor system health for CPU usage, memory consumption, and memory leaks during longevity

Table 5 continued

System & network resiliency, robustness		
23	System resiliency (Access/distribution)	Verify system level resiliency during the following events: ▪ Active switch failure ▪ Standby/Member switch failure ▪ EtherChannel member link flaps (ether-channel rate fast) ▪ Stack power failure ▪ BFD for faster link-state detection
25	Network resiliency (Access/distribution)	High availability of the network during system failures using: ▪ Redundancy protocols–HSRP/VRRP, VRRPv3 ▪ Redundant link failures
26	Deployment and operational events (Access)	Verify that the system holds well and recovers to working condition after the following negative 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.