

CISCO VALIDATED PROFILE

Access Switching Finance Profile

April 2017

Table of Contents

Profile Introduction	1
Foundational Security.....	1
Advanced Security	1
Network Services.....	1
Optimized Network & Traffic	1
Network Programmability	1
Efficient Network Management	2
System & Network Resiliency.....	2
Network Profile	3
Topology Diagram	3
Hardware & Feature Specifications	4
Key Vertical Features.....	4
Hardware Profile	7
Test Environment	7
Use Case Scenarios	9
Test Methodology	9
Use Cases	9
Appendix A	16

Profile Introduction

The Enterprise market segment can be divided into five broader verticals: Education, Financial, Health, Retail, and Government. This document focuses on a typical Finance deployment profile, and you can use it as reference validation document for Finance Network deployments.

The following sections describe some of the key considerations for the Finance Vertical.

FOUNDATIONAL SECURITY

Security is an integral requirement when it comes to the financial institutions. To safeguard the network at the foundational level, the following features are employed to protect against MITM (Man-in-the-Middle) and DOS (Denial-of-Service) attacks—ACL, CISF (Catalyst Integrated Security Features), IPv6 FHS, Guest Access (Web-auth).

ADVANCED SECURITY

Cisco TrustSec (CTS), along with the Identity features (dot1x/MAB), helps to achieve the advanced security needs of the financial institution that strives to prevent identity theft and frauds and to protect confidential data. CTS uses the software-defined segmentation technology to simplify the provisioning of network access, accelerate security operations, and consistently enforce policy anywhere in the network, along with MACSEC encryption and EAP-TLS.

NETWORK SERVICES

Trading floor architectures largely use Multicast protocols for the data/video feed services. Proper classification and traffic prioritization helps in reducing the latency of time-sensitive traffic in the Financial Institution. Custom and AutoQoS help in achieving this demand. When it comes to cost reduction, EnergyWise can be one of the important tools for driving the relevant energy policies to have power savings after business hours.

OPTIMIZED NETWORK & TRAFFIC

Optimizing the existing network using the technologies such as VRF-Lite and Private VLAN helps in effective IP address use, as well as providing the required network segmentation to meet some of the needs of the Financial Institution, such as VPN and isolating DMZ servers from each other. WCCP helps in transparently intercepting and redirecting the network traffic for application acceleration and WAN optimization.

NETWORK PROGRAMMABILITY

When network administrators need to deploy equipment from different network vendors or have to deal with different platforms within the same vendor, the operational expenses related to configuring, monitoring, and troubleshooting network devices in such network is a significant expense. Model-based management using Netconf/Restconf-Yang provides a standard programmatic interface that can enable efficient configuration management. With respect to simplified device deployment, the network-based boot-loader Preboot eXecution Environment (iPXE) helps to automatically boot up image from network based on DHCP options.

EFFICIENT NETWORK MANAGEMENT

The network administrators should be able to efficiently manage and monitor their networks to quickly respond to the dynamic needs of the financial institution. 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

Financial institutions and trade floors cannot afford to have larger downtimes, which calls for strict system and network-level resiliency. Stack HA, EtherChannel link level resiliency, VSS, and HSRP help meet such demands at different levels of the network.

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

Table 1 Finance Profile feature summary

Deployment areas	Features
Foundational security	CISF, IPv6 FHS, ACL, Guest Access
Advanced security	Cisco TrustSec (CTS), Dot1x, MAB, MAC-SEC, EAP-TLS
Network services	Multicast, QoS, EnergyWise, CoPP, OSPF, BGP, VNET
Optimized network & traffic	VRF-Lite, Private-VLAN, WCCP, QinQ
Programmability	Netconf-Yang/Restconf-Yang, iPXE
Efficient network management	Cisco Prime Infrastructure, WebUI
System & network resiliency	EtherChannel, Stack HA, VSS, HSRP

Network Profile

Based on the research, customer feedbacks and configuration samples, this Finance Vertical Profile is designed with the three-tier architecture, along with both L2 and routed access.

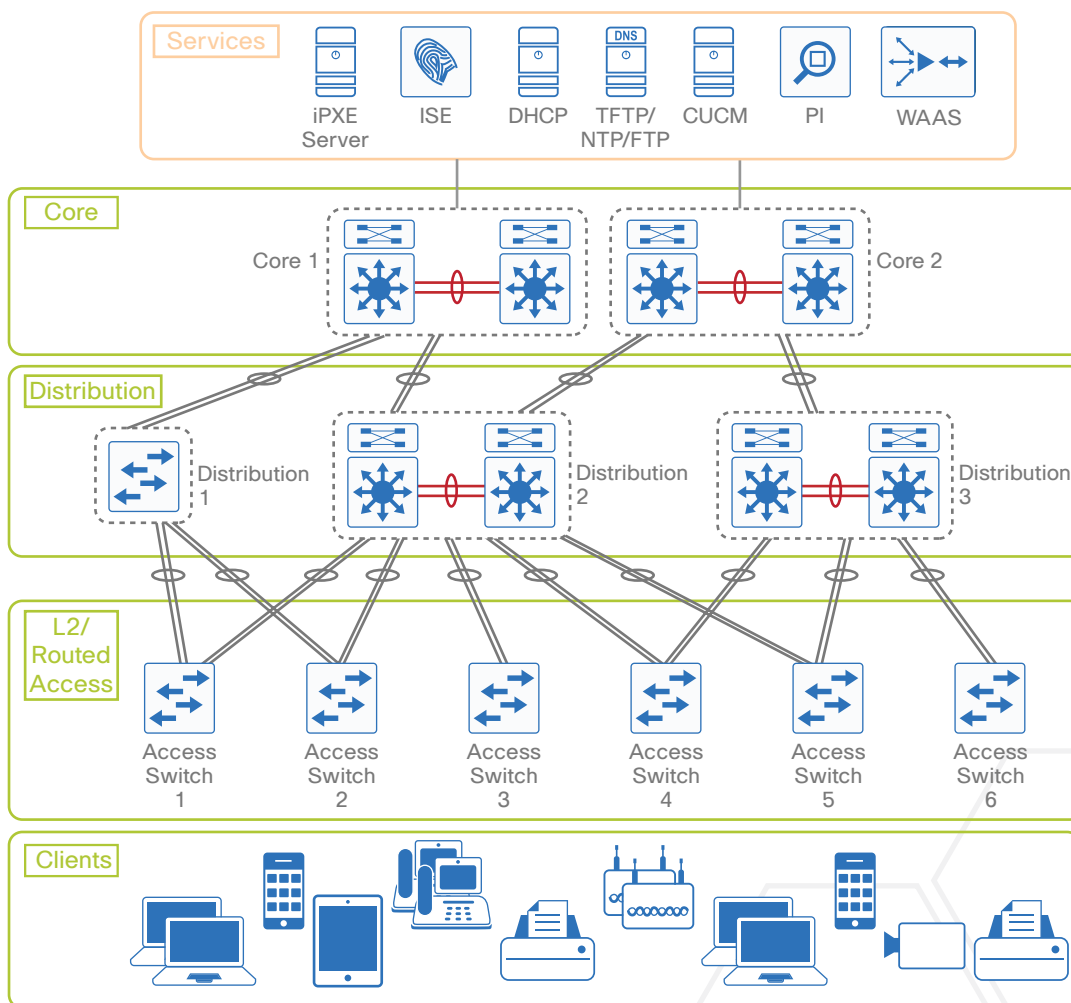
TOPOLOGY DIAGRAM

Figure 1 shows the topology that is used for the validation of this Finance 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 Finance Vertical Profile: topology overview



HARDWARE & FEATURE SPECIFICATIONS

This section of the guide describes the 3-D feature matrix where the typical 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 6-M stack (mixed stack - WS-C3850-12X48U) Switch2: C3650 5-M stack (mixed stack - WS-C3650-8X24UQ-E) Switch3: SUP8E/8LE Switch4: 2960X/2960XR stack Switch5: 3750X stack Switch6: WS-C3560CX, 2960L	V4/V6- Dual Stack 802.1x, MAB, CWA, AAA, Radius Custom IPv4/IPv6 Ingress/Egress QoS DHCP snooping, DAI, ARP ACL, Port Security, Storm Control, IPSG IPv6 FHS IPv4/IPv6 Input/Output ACL L3-EtherChannel CTS manual (no-encap) EnergyWise, POE (endpoints) Downshift - MGig Visibility (100m) MACSEC uplink (SAP/MKA) MACSEC downlink (MKA) EAP-TLS SNMP IPv6 VACL SGACL logging & monitoring BFD Multicast-PIM-SM, PIM-SSM(IGMPv3), PIM-DM, IGMP Snooping Static IP-SGT, Subnet-SGT Vlan-SGT, Port-SGT and Static SGACL Dynamic SGT/SGACL/CoA SXP Netconf-Yang (model-based management) Restconf-Yang (model-based management) iPX boot Static route VRF-Lite Private-Vlan WCCP SPAN, R-SPAN, FNF OSPF VNET trunk

Table 2 continued

Distribution	Dist1: WS-3850-48XS Dist2: Cat4K-VSS (SUP8E/ SUP7E) Dist3: 4500X-VSS	VSS OSPF Static route MACSEC uplink (SAP/MKA) EAP-TLS Multicast-PIM-SM, PIM-SSM, PIM-DM L3 EtherChannel CTS manual (no-encap) Static IP-SGT, Subnet-SGT Vlan-SGT, Port-SGT and Static SGACL SXP VRF-Lite SNMP IPv6/IPv4 Ingress/Egress QoS IPv6/IPv4 input/output ACL VNET trunk
Core	Core1: Cat6K-VSS Core2: Nexus7K-VSS	OSPF BGP Multicast L3 EtherChannel VNET trunk

HARDWARE PROFILE

Table 3 defines the set of hardware, servers, test equipment, and endpoints that are used to complete the end-to-end Financial 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
iPXE Server	Ubuntu 16.04 LTS	iPXE Server
Cisco UCS Server	ESXi 5.5.0	To manage and host the virtual machines
Ixia	IxNetwork, IxLoad	Generate traffic streams, emulate clients, emulate HTTP traffic
Cisco Unified IP Phones 7945, 7960	Cisco IP phones	Endpoints
Windows Laptops	Windows 7/8	Endpoints
PC with Cisco AnyConnect	Windows 7/8	Endpoints
MacBook Pro laptops	OSX 10.10.x	Endpoints
Printer	NA	Endpoints
IP camera	NA	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 Finance Profile: feature scale

Feature	Scale
EtherChannels	6-8
VLANs	1k
STP	64
MAC Learning	2k at access/10K at distribution
Storm Control (bcast)	128 interfaces
IPv4 ACLs/ACEs(RACL/PACL)	20 ACLs (10 Cisco ACEs per ACL)
IPv6 ACLs/ACEs(RACL/VACL)	13 ACLs (10 Cisco ACEs per ACL)
Static routes	16 IPv6/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	Cisco Prime/MIB walks
DHCP Snooping	600 clients
IPDT	Enabled on interface and vlan
Dot1x Clients	500 (real+emulation)
IP Phones (MAB Clients)	50 Phones per switch stack
WebAuth Clients	20 PCs (Real+Emulation)
EnergyWise Clients	50 (Phones)
Port-Security	128 Interfaces
V6 Clients	50 (real+emulation)
SGT/DGT	100 bindings
Multicast	1k mcast groups
VNET	16
VRF-Lite	3
Private VLAN	Community group-3 or 4 , promiscuous port-1, isolated port-2
WCCP	2 cache engines, 1000 http pkts/sec
OSPFv2	5 to 10 sessions
OSPFv3	5 to 10 sessions
BGP	2 sessions
OSPFv2 routes	2k
OSPFv3 routes	2k
BGP routes	50K
HSRP	100 groups (mix of IPv4 and IPv6)

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

USE CASES

Table 5 describes the typical use cases that were executed on the Financial 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)	<p>Network administrator should be able to perform switch upgrade and downgrade between releases seamlessly.</p> <ul style="list-style-type: none"> ▪ All of the configuration should be migrated seamlessly during the upgrade/downgrade operation. ▪ SW Install, Clean, Expand, ISSU
Security		
2	CISF (Access)	<p>Network admin to secure the L2 access against MITM, DOS attacks using the CISF (Cisco Integrated Security Features)</p> <ul style="list-style-type: none"> ▪ PortSecurity, IPSG, DAI, DHCP snooping
3	IPv6 FHS (Access)	<p>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)</p> <ul style="list-style-type: none"> ▪ IPv6-Snooping, ND Inspection, RA guard, Source & Destination guard, DHCPv6 guard
4	ACL (Access)	<p>Network admin to deploy input/output PACL, RACL and VACL with large number of ACEs for various traffic patterns (v4/v6) in 3-tier routed-access finance network</p>
5	IBNS 2.0 Mode (eEdge// new-style) (Access)	<p>Network admin wants to deploy endpoint/end-users security using MAB/Dot1x with IBNS 2.0 Mode (eEdge/new-style).</p> <ul style="list-style-type: none"> ▪ PC behind the Phone: AuthC > Dot1x for the PC and MAB for the Phone, Host mode : Multi-Domain ▪ Dot1x, MAB : PCs, phones. Hostmode: Single Host, Multi-Host, Multi-Auth ▪ AuthZ : dACL, Dynamic VLAN ▪ Clients spread across open, closed and low impact modes ▪ Critical VLAN ▪ Reauthentication timers ▪ CDP Bypass ▪ Multiple clients login/logoff ▪ End point profiling-BYOD ▪ Auto Identity: Monitor/Low impact/Close Modes.

Table 5 continued

6	Auth-Manager Mode (legacy) (Access)	<p>Network admin wants to deploy End-Point/End-users security using MAB/Dot1x with Auth-Manager Mode (legacy).</p> <ul style="list-style-type: none"> ▪ 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, Multi-Auth ▪ AuthZ : dACL, Dynamic VLAN ▪ Clients spread across open, closed and low impact modes ▪ Critical VLAN ▪ Reauthentication timers ▪ CDP Bypass ▪ Multiple clients login/logoff ▪ Endpoint profiling–BYOD
7	Guest-Access (Access)	<p>Network admin wants to provide temporary guest access CWA.</p> <ul style="list-style-type: none"> ▪ CWA–Self Register Guest Portal
8	TrustSec (static) (Access/Distribution)	<p>Network admin to deploy TrustSec using static SGT/SGACL</p> <ul style="list-style-type: none"> ▪ Static SGT/SGACL with different bindings (ip, vlan, subnet, port) with inline tagging (v4)–across L3 EtherChannel with CTS dot1x/manual
9	TrustSec (dynamic) (Access/Distribution)	<p>Network admin to deploy TrustSec using dynamic SGT/SGACL</p> <ul style="list-style-type: none"> ▪ Dynamic SGT/SGACL/CoA with inline tagging (v4) along with SGACL logging and monitoring–across L3 EtherChannel with CTS dot1x/manual. Dynamic clients using Dot1x/MAB with dVLAN/dACL, along with monitor, low-impact and closed mode sessions at access layer. Use Radio active tracing capability for CoA for debuggability purposes.
10	TrustSec (dynamic over SXP) (Access/Distribution)	<p>Network admin to deploy TrustSec using dynamic over SXP</p> <ul style="list-style-type: none"> ▪ Dynamic SGT/SGACL over SXP (v4/v6)–across L3 EtherChannel with CTS dot1x/manual. Dynamic clients using Dot1x/MAB with dVLAN/dACL
11	Encryption (Access/ Distribution)	<p>Network admin to deploy encryption using MACsec on uplink and downlink</p> <ul style="list-style-type: none"> ▪ Uplink encryption using MACsec uplink (SAP/MKA) on the L3 Ether-channel mGig downshift link ▪ Downlink encryption using MACsec downlink (MKA) ▪ Device certificates are carried using EAP-TLS

Table 5 continued

Optimizing network & traffic		
12	VRF-Lite (Access/Distribution)	Network admin to provide VPN connectivity and optimize the usage of IP address, using the VRF-Lite <ul style="list-style-type: none"> ▪ VRF routing using overlapped IP addresses
13	Private VLAN (Access/Distribution)	Network admin to deploy Private VLAN for efficient IP address aggregation <ul style="list-style-type: none"> ▪ Primary VLAN, Secondary VLAN ▪ Isolate port, Community port, Promiscuous port on the physical interface depending on the connected end points
14	WCCP (Access/Distribution)	Network admin to deploy WCCP to transparently intercept and redirect the network traffic for application acceleration and WAN optimization <ul style="list-style-type: none"> ▪ WCCP redirection into separate CEs (cache engines) based on service groups
15	Q-in-Q (Access/Distribution)	Network admin to segregate or bundle customer traffic into fewer VLANs or different VLANs by adding another layer of 802.1Q tags <ul style="list-style-type: none"> ▪ Unmapped C-VLANs switching in Q-in-Q network ▪ VLAN traffic flow over Q-in-Q link with LACP fast convergence.
Network services		
16	Multicast Data/Video (Access/Distribution)	Network admin wants to enable and deploy multicast services. <ul style="list-style-type: none"> ▪ 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
17	OSPF and BGP (Access/Distribution)	Network admin wants to enable routing services. <ul style="list-style-type: none"> ▪ OSPFv2 and OSPFv3 ▪ BGP
18	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, activity check)

Table 5 continued

19	QoS (Access/Distribution)	<p>Network Admin needs to enhance user experience by ensuring traffic and application delivery using custom QoS policies for trusted/untrusted interfaces.</p> <ul style="list-style-type: none"> ▪ Traffic Types: VOIP, Video, Call Control, Transactional Data, Bulk Data, Scavenger ▪ Policing Ingress and Priority & BW Management in Egress ▪ AutoQoS on certain ports which are connected to end points
20	Control Plane Policing (CoPP) (Access)	<p>Network admin uses CoPP to protect the control and management planes and ensure routing stability, reachability, and packet delivery.</p> <ul style="list-style-type: none"> ▪ QoS and Policy maps to filter and rate-limit the traffic
21	VNET(Access/Distribution/ Core)	<p>Network admin flexibility to transport multi-VRF traffic on each routed physical interface/uplink.</p> <ul style="list-style-type: none"> ▪ VRF routing with VNET trunk.
Programmability		
22	Model-based Management (Access/Distribution)	<ul style="list-style-type: none"> ▪ Network admin to use model based management (Netconf/Restconf-Yang) to do the configuration management.
23	iPXE boot (Access/Distribution)	<p>Network admin to use network-based bootloader,iPXE, to set up in such a way that the new devices deployed on the network can be automatically booted up with the image from the network (HTTP/TFTP) using values from DHCP options</p>
Monitoring & troubleshooting		
24	NetFlow (Access/Distribution)	<p>Enable IT admins to determine network resource usage, capacity planning by monitoring SGT/DGT traffic flows using Flexible NetFlow</p> <ul style="list-style-type: none"> ▪ Traffic Types: L2, IPv4, IPv6 ▪ FNFv9, IPFIX-v10 ▪ Prime Collector
Simplified management		
25	Prime-Manage-Monitor	<p>Network admin wants to manage and monitor all the devices in the network using Cisco Prime Infrastructure.</p>
26	Prime-SWIM	<p>Network admin should be able to manage images on network devices using Cisco Prime Infrastructure for upgrade/downgrade.</p>

Table 5 continued

27	Prime-Template	<p>Network admin wants to deploy configuration using Cisco Prime Infrastructure.</p> <ul style="list-style-type: none"> ▪ Import and deploy customer specific configuration templates. ▪ Schedule configuration for immediate or later deployment ▪ Simplify configuration using config-templates
28	Prime-Troubleshooting	<p>Simple network troubleshooting and debugging for IT admins.</p> <ul style="list-style-type: none"> ▪ Monitor & troubleshoot end-end deployment via maps & topologies ▪ Monitor network for alarms, syslog and traps ▪ Troubleshoot network performance using traffic flow monitoring.
29	WebUI-Day0 Wizard	<p>Network admin deploys 3850 in the access layer site (Day 0).</p> <ul style="list-style-type: none"> ▪ 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
30	WebUI-Configuration	<p>Network admin to be able to configure the system (Day N)</p> <ul style="list-style-type: none"> ▪ 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, IPv6 FHS ▪ Implement Quality-of-Service using Cisco-recommended Auto-QoS
31	WebUI-Monitoring	<p>Network admin should be able to monitor the health of the system.</p> <ul style="list-style-type: none"> ▪ Monitor the health of the system in terms of the CPU utilization and memory consumption of the switch. ▪ Flexible enough to look for the system health during a particular time range

Table 5 continued

32	WebUI-System Management	<p>Network admin routinely performs the task of Asset Management.</p> <ul style="list-style-type: none"> ▪ 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.
System health monitoring		
33	System Health (Access/Distribution)	Monitor system health for CPU usage, memory consumption, and memory leaks during longevity
System & network resiliency, robustness		
34	System Resiliency (Access/Distribution)	<p>Verify system level resiliency during the following events:</p> <ul style="list-style-type: none"> ▪ Active switch failure ▪ Standby/Member switch failure ▪ EtherChannel member link flaps
35	Network Resiliency (Distribution)	<p>High availability of the network during system failures using:</p> <ul style="list-style-type: none"> ▪ VSS ▪ HSRP
36	Typical Deployment Events, Triggers (Access/Distribution)	<p>Verify that the system holds well and recovers to working condition after the following events are triggered:</p> <ul style="list-style-type: none"> ▪ 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.

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.

© 2017 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)