CISCO VALIDATED PROFILE

Access Switching Finance Vertical

April 2016

Table of Contents

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.

NETWORK SERVICES

Trading floor architectures largely uses 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.

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
Network services	Multicast, QoS, EnergyWise, CoPP, OSPF, BGP
Optimized network & traffic	VRF-Lite, Private-VLAN, WCCP, QinQ
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.

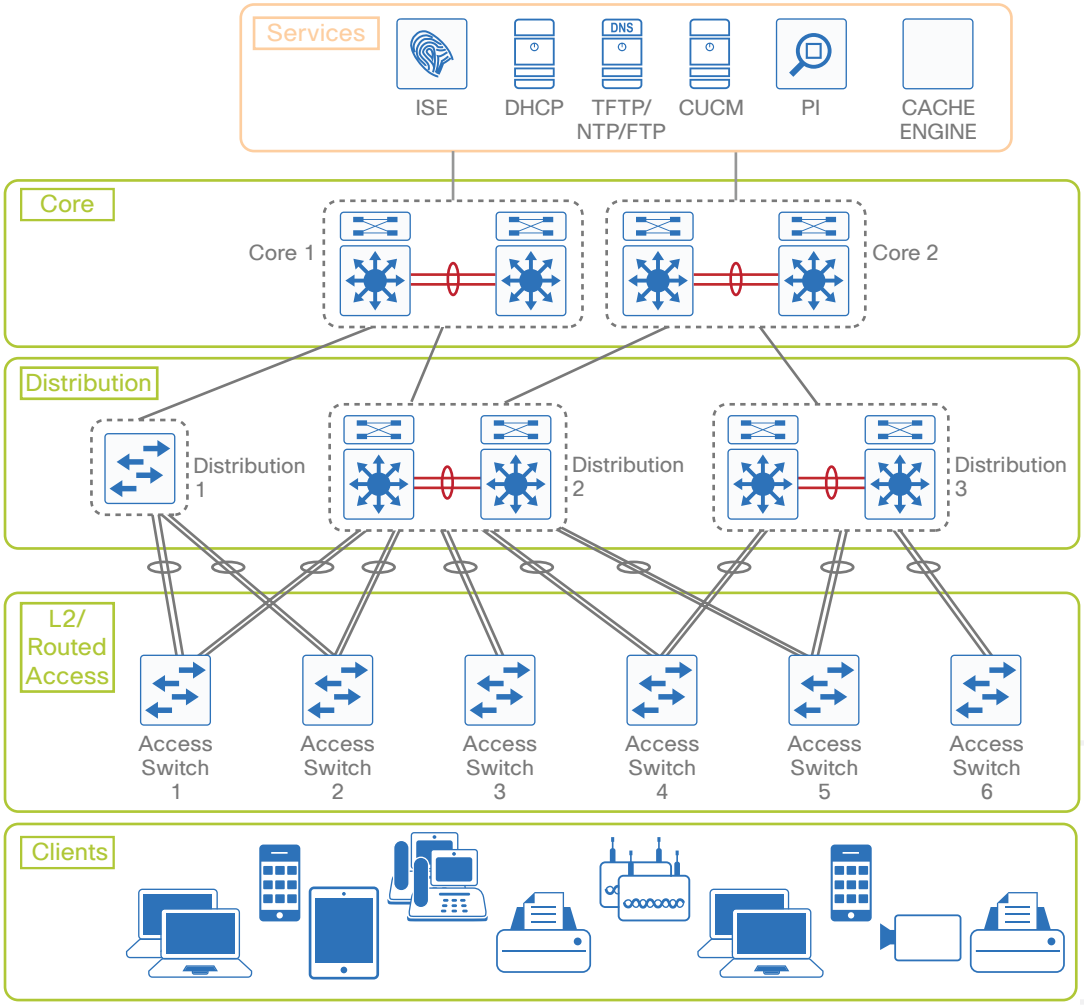
TOPOLOGY DIAGRAM

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 5-M stack Switch2: C3650 4-M stack Switch3: SUP8E/8LE Switch4: 2960X/2960XR stack Switch5: 3750X stack Switch6: WS-C3560CX	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) SNMP 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 SXP Static route VRF-Lite Private-Vlan WCCP SPAN, R-SPAN, FNF OSPF
Distribution	Dist1: WS-3850-48XS 2-M stack Dist2: Cat4K-VSS (SUP8E/SUP7E) Dist3: 4500X-VSS	VSS OSPF Static route 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
Core	Core1: Cat6K-VSS Core2: Nexus7K-VSS	OSPF BGP Multicast L3 EtherChannel

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 3.0 TP2	For network management
Cisco ISE	Version 1.3	Radius Server used for authentication, authorization,
CUCM	Version 10.1	CUCM Server for managing IP phones
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	10 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
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)	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, ISSU
Security		
2	CISF (Access)	Network admin to secure the L2 access against MITM, DOS attacks using the CISF (Cisco Integrated Security Features) ▪ PortSecurity, IPSG, DAI, DHCP snooping

Table 5 continued

3	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
4	ACL (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 routed-access finance network
5	IBNS 2.0 Mode (eEdge//new-style) (Access)	Network admin wants to deploy endpoint/end-users security using MAB/ Dot1x with IBNS 2.0 Mode (eEdge/new-style). ▪ 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.
6	Auth-Manager Mode (legacy) (Access)	Network admin wants to deploy End-Point/End-users security using MAB/ Dot1x with Auth-Manager Mode (legacy). ▪ 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

Table 5 continued

7	Guest-Access (Access)	Network admin wants to provide temporary guest access CWA. ▪ CWA–Self Register Guest Portal
8	TrustSec (static) (Access/Distribution)	Network admin to deploy TrustSec using static SGT/SGACL ▪ 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)	Network admin to deploy TrustSec using dynamic SGT/SGACL ▪ Dynamic SGT/SGACL with inline tagging (v4)–across L3 EtherChannel with CTS dot1x/manual. Dynamic clients using Dot1x/MAB with dV-LAN/dACL, along with Monitor, low-impact and closed mode sessions at access layer
10	TrustSec (dynamic over SXP) (Access/Distribution)	Network admin to deploy TrustSec using dynamic over SXP ▪ Dynamic SGT/SGACL over SXP (v4/v6)–across L3 EtherChannel with CTS dot1x/manual. Dynamic clients using Dot1x/MAB with dVLAN/dACL
Optimizing network & traffic		
11	VRF-Lite (Access/Distribution)	Network admin to provide VPN connectivity and optimize the usage of IP address, using the VRF-Lite ▪ VRF routing using overlapped IP addresses
12	Private VLAN (Access/Distribution)	Network admin to deploy Private VLAN for efficient IP address aggregation ▪ Primary VLAN, Secondary VLAN ▪ Isolate port, Community port, Promiscuous port on the physical interface depending on the connected end points
13	WCCP (Access/Distribution)	Network admin to deploy WCCP to transparently intercept and redirect the network traffic for application acceleration and WAN optimization ▪ WCCP redirection into separate CEs (cache engines) based on service groups
14	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 ▪ Unmapped C-VLANS switching in Q-in-Q network ▪ VLAN traffic flow over Q-in-Q link with LACP fast convergence.

Table 5 continued

Network services		
15	Multicast Data/Video (Access/Distribution)	Network admin wants to enable and deploy multicast services. ▪ 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
16	OSPF and BGP (Access/Distribution)	Network admin wants to enable routing services. ▪ OSPFv2 and OSPFv3 ▪ BGP
17	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)
18	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 ▪ AutoQoS on certain ports which are connected to end points
19	Control Plane Policing (CoPP) (Access)	Network admin uses CoPP to protect the control and management planes and ensure routing stability, reachability, and packet delivery. ▪ QoS and Policy maps to filter and rate-limit the traffic
Monitoring & troubleshooting		
20	NetFlow (Access/Distribution)	Enable IT admins to determine network resource usage, capacity planning by monitoring SGT/DGT traffic flows using Flexible NetFlow ▪ Traffic Types: L2, IPv4, IPv6 ▪ FNFv9, IPFIX-v10 ▪ Prime Collector
Simplified management		
21	Prime-Manage-Monitor	Network admin wants to manage and monitor all the devices in the network using Cisco Prime Infrastructure.

Table 5 continued

22	Prime-SWIM	Network admin should be able to manage images on network devices using Cisco Prime Infrastructure for upgrade/downgrade.
23	Prime-Template	Network admin wants to deploy configuration using Cisco Prime Infrastructure. ▪ Import and deploy customer specific configuration templates. ▪ Schedule configuration for immediate or later deployment ▪ Simplify configuration using config-templates
24	Prime-Troubleshooting	Simple network troubleshooting and debugging for IT admins. ▪ Monitor & troubleshoot end-end deployment via maps & topologies ▪ Monitor network for alarms, syslog and traps ▪ Troubleshoot network performance using traffic flow monitoring.
25	WebUI-Day0 Wizard	Network admin deploys 3850 in the access layer site (Day 0). ▪ 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
26	WebUI-Configuration	Network admin to be able to configure the system (Day N) ▪ 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
27	WebUI-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. ▪ Flexible enough to look for the system health during a particular time range

Table 5 continued

28	WebUI-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. Furthermore, it is a common practice to generate system reports based on this for audit purposes.
System health monitoring		
29	System Health (Access/Distribution)	Monitor system health for CPU usage, memory consumption, and memory leaks during longevity
System & network resiliency, robustness		
30	System Resiliency (Access/Distribution)	Verify system level resiliency during the following events: ▪ Active switch failure ▪ Standby/Member switch failure ▪ EtherChannel member link flaps
31	Network Resiliency (Distribution)	High availability of the network during system failures using: ▪ VSS ▪ HSRP
32	Typical Deployment Events, Triggers (Access/Distribution)	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

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.