Validated Profile: Financial Vertical

Revised: December 20, 2023

Solution Overview

This guide focuses on creation and validation of Cisco SD-Access and Cisco SD-WAN-based deployment for a large-scale financial vertical. This deployment uses an Independent-Domain model, where the Cisco SD-WAN controller and Cisco DNA Center are independently managed and not integrated. This guide can be used as a reference document for finance network deployments.

Financial organizations operate hundreds of branches throughout the world, ranging from small ATMs to large corporate offices. While each site has its own special requirements, the financial vertical needs standardized and secure network connectivity, simplified network operations and maintenance, highly failure-resilient systems, and a consistent policy implementation across the entire organization.

Using features such as Cisco DNA Center three-node high availability and disaster recovery for resiliency, the resulting solution provides high uptimes, lower operating costs, streamlined workflows, performance optimization, and secure end-to-end connectivity.

System and Network Resiliency

The financial vertical solution can handle failures at multiple layers, from low-level device and link failures, to controller failures, to even data center outages. Cisco DNA Center provides system resiliency with features such as high availability and disaster recovery. Cisco SD-Access and SD-WAN also offer network resiliency with support of dual SD-Access borders, dual Cisco SD-WAN WAN edges, fabric nodes with stacks and StackWise Virtual Link (SVL), and wireless controllers in SSO and N+1.

Security

The solution leverages the built-in security features as well as the integration of Cisco ISE and Cisco DNA Center to provide highly secure and segmented systems.

Cisco ISE is the policy engine that simplifies the delivery of security to the network and provides support for Group-Based Policy (GBP). Cisco GBP dynamically organizes endpoints into logical groups, using scalable group tags (SGTs). SGTs are assigned based on business decisions using a richer context than simply an IP address. SGTs are easier to understand and manage. The number of group-based rules is dramatically less than an equivalent set of rules based on IP addresses. Cisco ISE also performs AAA functions with network devices and end clients.

Cisco DNA Center scales the network and still restricts access to critical applications in the fabric while improving situational awareness on the network. After Cisco ISE is integrated with Cisco DNA Center, Cisco DNA Center retrieves the Group-Based Policy from Cisco ISE to protect applications from unauthorized endpoints and clients. Cisco ISE gathers real-time contextual information from networks, users, and devices for Cisco DNA Assurance. This integration simplifies the advanced security needs of the financial institution that strives to prevent fraud and protect confidential data. The integration facilitates the provisioning of network access, accelerates security operations, and consistently enforces policy anywhere in the network.

Cisco GBP and the identity-based access control features (IEEE 802.1X/MAC authentication bypass, site-level MACsec encryption, FQDN-based certificates) help achieve the security needs of the financial vertical.

Network Segmentation

Network segmentation is essential for protecting critical business assets. Cisco DNA Center provides a simplified approach, called *macrosegmentation*, to protect data between virtual networks (VNs). Cisco DNA Center also provides the framework for deploying *microsegmentation* using group-based access control for endpoints within VNs.

The concept of network segmentation is not new, but it has evolved significantly over recent years. Initially, network segmentation was defined as the process of breaking up one *flat* network or broadcast domain into smaller segments with virtual LANs (VLANs).

As requirements were established to extend network segments across organizations regardless of location, the concept of VN or Virtual Routing and Forwarding (VRF) instances was used to implement Layer 3 isolation between network segments.

Isolation is inherent, as each VRF maintains its own routing and forwarding, thereby creating a virtual network. Isolation is attained because routes contained in one VRF are not present in another, thereby limiting communications between them. With Cisco GBP, segmentation is no longer performed based on VLANs or VRFs with IP addressing and routing. Instead, Cisco GBP relies on the use of role- or group-based membership, regardless of IP addressing, to create policies that allow segmentation of the network.

Simplify Network Operations

Cisco DNA Center provides an intent-based solution to automate workflows such as network device provisioning, software image management (SWIM), and inventory management. Cisco DNA Center also pushes the organization's intent as policies across all sites. The solution allows Switch Virtual Interface (SVI) number reuse for the Layer 3 connections between the fabric borders and gateways and provides the framework for administrators to standardize SVI assignments in each border. Cisco DNA Center also provides actionable information about the network's health using Assurance, such as Assurance dashboards for network, client, and critical issues. The capability to drill down to a single device or client simplifies the troubleshooting process.

Robust Network and Connectivity

Cisco SD-WAN is an overlay WAN architecture that connects multiple sites through a single fabric. The Cisco SD-WAN architecture consists of separate orchestration, management, control, and data planes. The Cisco vBond controller provides for the automatic onboarding of the SD-WAN routers into the SD-WAN overlay. The Cisco vManage controller is responsible for central configuration and monitoring. The Cisco vSmart controller is responsible for the centralized control plane of the SD-WAN network. The WAN edge establishes secure data-plane connectivity with other WAN edges.

The Cisco SD-WAN edges connect to SD-Access sites across the Cisco SD-WAN fabric using Cisco SD-Access IP transit to maintain a standard and secure connectivity throughout the network. In the Independent-Domain deployment model, Cisco vManage and Cisco DNA Center do not communicate with each other. Cisco SD-Access VNs are connected to Cisco SD-WAN virtual private networks (VPNs) using VRF-Lite. This allows the VN from two SD-Access sites to communicate across Cisco SD-WAN. External Border Gateway Protocol (eBGP) is configured between SD-WAN WAN edges and Cisco SD-Access borders to exchange routes within the VN/VPN.

Centralized Policy Management

There are differences in numbers between Cisco DNA Center systems endpoint scale and Cisco ISE scale. With multiple geographic and distant branches and sites worldwide, large Cisco ISE deployments, such as in the financial vertical, can benefit by integrating multiple Cisco DNA Center clusters with a single Cisco ISE. Cisco supports multiple Cisco DNA Center clusters per Cisco ISE deployment to better utilize Cisco ISE and also provides a centralized policy management plane for multiple Cisco DNA Centers. In a multiple Cisco DNA Center deployment, the first Cisco DNA Center system serves as the *author* node for Group-Based Access Policy. The author node manages scalable groups, access contracts, policies, and VNs. Creation, modification, or deletion of these policy and security elements is only possible on the author node. Additional *reader* nodes are independent systems that manage separate sets of network devices. The reader node does not manage local VNs or Group-Based Access Policy. Reader nodes only have read-only visibility of VNs and scalable groups.

Network Services

Trading floor architectures largely use multicast protocols for their data and video feed services. Cisco DNA Center and Cisco SD-WAN provide the framework to enable multicast from hubs to branches.

Hardware and Software Specifications

The solution is tested with the hardware and software listed in the following table. For the complete list of hardware supported, see the Cisco Software-Defined Access Compatibility Matrix.

Table 1: Hardware and Software Profile Summary

Role	Hardware Platform	Software Release	Software Release
Cisco DNA Center Controller	DN2-HW-APL-L, DN2-HW-APL-XL	2.3.3.7	2.3.5.5
Cisco Identity Service Management, RADIUS Server	Physical/Virtual Appliance	3.0 Patch 6, 3.1 Patch 3	3.2 Patch 2
Cisco SD-WAN NMS Controller	vManage	20.6.1	20.6.1
Cisco SD-Access Control Plane Node	C9500	17.6.6a	17.6.6a, 17.9.4a
Cisco SD-Access Fabric Border Node	C9500	17.6.6a	17.6.6a, 17.9.4a
Cisco SD-Access Fabric Edge Node	C9200, C9300	17.6.6a	17.6.6a, 17.9.4a
Cisco Wireless Controller	AireOS C9800-40	8.10MR8 17.6.6a	8.10MR9 17.6.6a, 17.9.4a
Cisco SD-WAN WAN Edge	ASR1002-X, ISR4331	17.6.5a	17.6.5a
Cisco Stealthwatch Controller	Physical/Virtual Appliance	7.1.2	7.3.2

Solution Use Case Scenarios

The following use cases were validated on the financial vertical profile using the topology defined in Topology.

- Implement intent-based networking using Cisco DNA Center and Cisco SD-Access.
  - Administrators should be able to automate and simplify network device provisioning.
  - Administrators should be able to maintain and monitor inventory and resolve problems easily.
  - Administrators should be able to use Cisco DNA Center SWIM to upgrade multiple devices, such as switches, routers, and wireless controllers.
- Integrate multiple Cisco DNA Centers with a single Cisco ISE.
  - Administrators should be able to create, modify, and delete intent-based policy on the Author node and automatically synchronize to the Reader node.
  - Administrators should be able to request promotion to the Author node from the Cisco DNA Center Reader node.

- Connect multiple geographic and distant sites using Cisco SD-WAN.
    - Administrators should be able to configure Cisco SD-WAN to connect between campus and branches.
    - Administrators should be able to configure the Cisco SD-WAN WAN edge to connect to the SD-Access fabric via IP transit.
    - Administrators should be able to configure inline SGT propagation on the Cisco SD-WAN WAN edge to maintain end-to-end using Cisco TrustSec.
    - Administrators should be able to use Cisco SD-WAN vManage to upgrade the Cisco SD-WAN WAN edge image.

- System and network resiliency.
    - The network should recover from device or link failure automatically with minimal impact on existing applications, traffic, and users.
    - Administrators should be able to configure Cisco DNA Center in three-node HA mode. In case of services or node failure in Cisco DNA Center, the system should recover without user intervention.
    - Administrators should be able to configure disaster recovery in Cisco DNA Centers that reside in different data centers. In case of multiple node failures or irrecoverable network issues, Cisco disaster recovery should trigger automatic failover to Cisco DNA Center in a different data center.
    - Administrators should be able to upgrade or perform maintenance activities with Cisco DNA Center disaster recovery configured.
    - Administrators should be able to fail over to the standby Cisco DNA Center.
    - Administrators should be able to configure multiple Policy Administration Node (PAN), Policy Service Node (PSN), and Cisco Platform Exchange Grid (pxGrid) in a Cisco ISE distributed deployment.
    - Administrators should be able to upgrade to a major release or apply new patches to a Cisco ISE distributed deployment without impacting users and devices.
    - Administrators should be able to back up, one time or on schedule, Cisco DNA Center controller configuration and data.
    - Administrators should be able to restore Cisco DNA Center controller configuration and data.

- Configure integrated network intent across the entire organization.
    - Administrators should be able to create VNs across the organization to achieve consistent macrosegmentation.
    - Administrators should be able to apply multiple SGTs for a single VN and create group-based access policy for microsegmentation traffic within a VN.
    - Administrators should be able to configure dot1x authentication for wired and wireless clients.
    - Administrators should be able add or remove new groups of users via an add/remove VN, and then associate or disassociate the IP pool to the VN.

- Configure enhanced security to protect sensitive financial data.
    - To prevent unauthorized access, administrators should be able to enable Closed Auth Onboarding (dot1x) for wired and wireless devices and users.
    - Administrators should be able to configure secure site-level fabric traffic with MACsec.
    - To provide tighter security, administrators on Cisco DNA Center should be able to apply trusted CA FQDN-based certificates.

    - Administrators should be able to integrate Stealthwatch with Cisco DNA Center for threat detection, threat containment, and SSA for ETA automation.
    - Administrators should be able to create granular role-based users and use audit logging to monitor Cisco DNA Center activities.
    - Administrators should be able to audit policy changes, deployment of policy changes, status of deployment, the user who initiate the changes, and when.

- Monitor network and client health using Assurance and analytics.
    - Network administrators should be able to monitor the state of the network, wired users, and wireless users from a single pane of glass.
    - Network administrators should be able to examine severe, critical, and other ongoing issues with the network and devices and follow the suggested actions in Assurance to resolve the issues.
    - Network administrators should be able to monitor the health of the wired and wireless users and devices connected to the network.
    - Network administrators should be able to look at a single device, wired user, or wireless user and retrieve detailed information.
    - Network administrators should be able to see detailed application data usage.
    - Network administrators should be able to use sensors to monitor wireless network health.

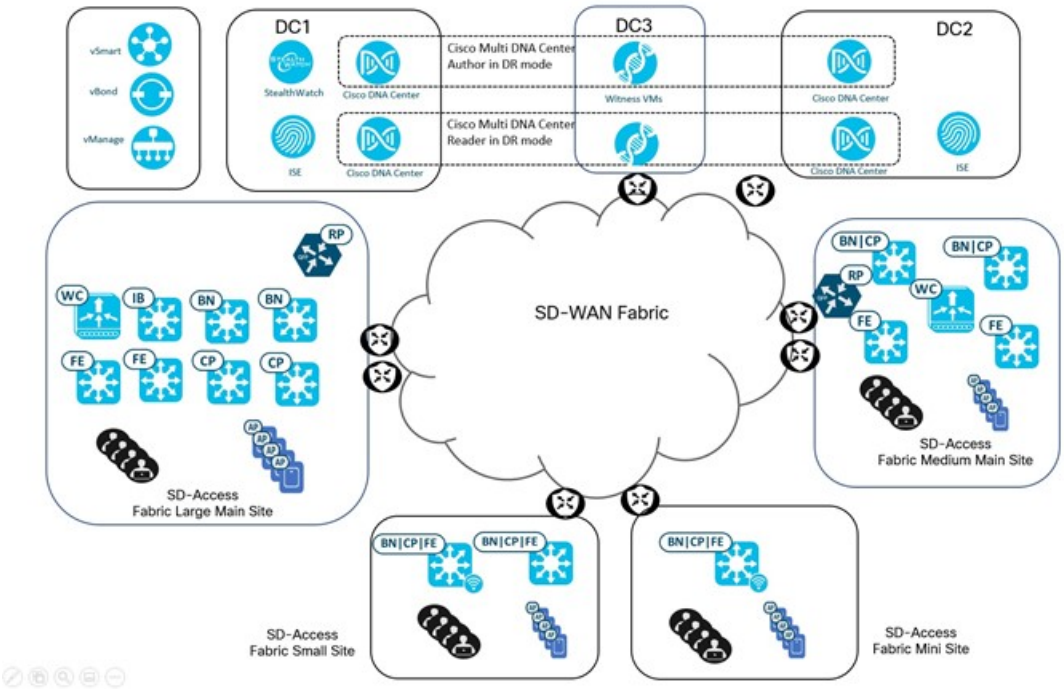
Topology

The test topology for the financial vertical includes four Cisco DNA Centers. They are deployed across multiple data centers and configured with Cisco DNA Center disaster recovery. Data center 1 has the main Cisco DNA Center cluster. Data center 2 has the recovery Cisco DNA Center cluster for Cisco DNA Center disaster recovery. Data center 3 houses the witnesses. Each data center has two Cisco DNA Center deployments, one as multiple Cisco DNA Center Authors and another as a Reader. Cisco ISE Policy Administration Node (PAN) and Policy Service Node (PSN) are distributed across Data center 1 and Data center 2. Cisco SD-WAN controllers are in Data center 1. There are multiple fabric sites connected via Cisco SD-WAN WAN edge over the SD-WAN fabric. The sites are described as follows:

- The larger main site has dual borders, dual non-collocated CPs, and wireless LAN controllers. The medium main site has dual borders, collocated CPs, and wireless LAN controllers.
- The small sites have dual fabric-in-a-box with embedded wireless LAN controllers.
- The mini sites have fabric-in-a-box with embedded wireless LAN controllers.
- All fabric sites have SD-Access multicast with ASM overlay, SSM underlay, and native multicast. External RPs are in the main sites. Between the main sites, MSDP peering is used to communicate site-specific multicast sources.

The following figure illustrates the logical topology of the solution test bed.

Figure 1: Solution Test Topology



Scale

Solution test verified the scale numbers listed in the following table. For the hardware capacity, see the Cisco DNA Center Data Sheet.

Category	Value
Device inventory	2000
Number of devices per fabric site	1 to 500
Number of VNs per site	3 to 64
Number of WLCs per site	2 per HA
Number of fabric sites	450
Number of APs per site	Up to 1000
Number of endpoints	100,000 (60,000 wireless, 20,000 guest, 20,000 wired)
Number of SSIDs	4
Number of SGTs	500
Traffic profile	Unicast and multicast

Solution Key Notes

This section describes technical notes that are useful for deploying the solution.

Multiple Cisco DNA Center

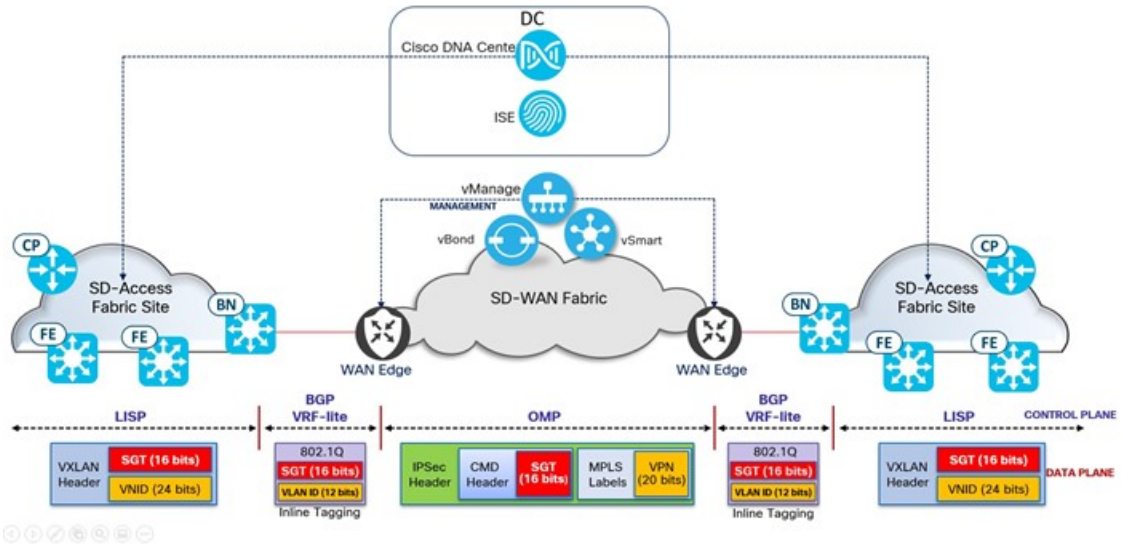
Large Cisco ISE deployments, such as the financial vertical, can benefit by integrating multiple Cisco DNA Center clusters with a single Cisco ISE. Cisco DNA Center supports multiple Cisco DNA Center clusters per Cisco ISE deployment to better utilize Cisco ISE and provide a centralized policy management plane for multiple Cisco DNA Centers. For more information, see Support for Multiple Cisco DNA Center Clusters with a Single Cisco ISE System.

- The multiple Cisco DNA Center package is not bundled with the release software image and must be downloaded separately.
- The first Cisco DNA Center integrated with Cisco ISE becomes the Author node. The Author node is the source of truth for all SD-Access policy information. Changing the Author node is not recommended; therefore, decide which Cisco DNA Center is the Author node during bring-up.
- Subsequent integrations of Cisco DNA Centers (up to three) to Cisco ISE become Reader nodes. It is best to add a newly deployed Cisco DNA Center as a Reader node. If there is any existing policy data, do not integrate that node with Cisco ISE.
- All Cisco DNA Centers in a multiple Cisco DNA Center deployment must run the same version of software.

Cisco SD-WAN

With fabric sites and branches throughout the world, Cisco SD-WAN provides a robust transport for connectivity between Cisco SD-Access site underlay and overlay. Using inline SGT tagging, SGTs are maintained end to end, allowing for consistent policy enforcement throughout the domain and at the fabric edges. The following figure shows the SD-Access SD-WAN integration with inline SGT tagging.

Figure 2: SD-Access SD-WAN Integration with Inline SGT



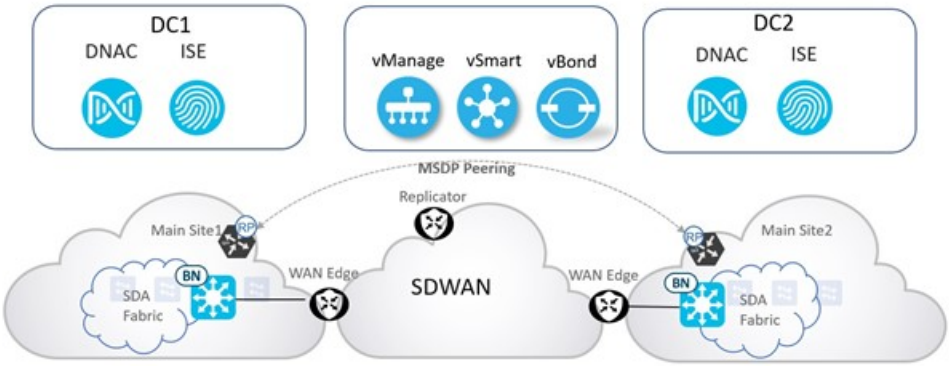
- After Cisco SD-WAN controllers are up and WAN edges are onboarded and managed by the Cisco SD-WAN controller, integration with the Cisco SD-Access network is achieved via IP transit L3 handoff on the fabric borders with VRF lite and eBGP.

- Layer 3 MTU alignment between fabric borders and the WAN edge is confirmed to consistently ensure end-to-end large packet forwarding.
- Enabling TrustSec with **cts manual** causes the interface to flap momentarily.
- If the SD-Access border is a Cisco Catalyst switch, configuring **cts manual** followed by **policy static sgt <sgt number> trusted** on the SD-Access border switchport enables CTS on all VLANs of the trunk link. On the SD-WAN edge, **cts manual** is configured on the parent physical interface and **cts manual** followed by **policy static sgt <sgt number> trusted** is configured on the subinterfaces. The <*sgt number*> is the SGT value to apply to untagged or untrusted incoming traffic.

Layer 3 Multicast from Hubs to Branches

Trading floor architectures use multicast protocols for data and video feed services. Cisco DNA Center and Cisco SD-WAN provide the framework to enable multicast from hubs to branches. The following figure shows the Layer 3 multicast topology.

Figure 3: Solution Test Multicast Topology



The financial vertical has native multicast enabled on the main, small, and mini sites. SD-Access native multicast relies on Source Specific Multicast (SSM) in the underlay; therefore, SSM configurations are configured on the fabric nodes, intermediate nodes, and SD-WAN WAN edges. Multicast Rendezvous Point (RP) is external to the SD-Access fabric. MSDP peering is enabled to communicate site-specific multicast sources to remote multicast RP. A replicator is configured in the SD-WAN WAN edge.

Multicast is enabled on the service VPN subinterfaces of the SD-WAN WAN edges, which are in turn connected to the underlay network in the fabric borders. This topology ensures complete end-to-end native multicast configuration throughout the fabric nodes and SD-WAN WAN edges.

Telemetry

Cisco DNA Center uses telemetry to collect device and client data and provides network health information in Assurance.

- To enable the telemetry connection, devices are discovered with NETCONF.
- For devices that are already discovered without NETCONF, they are rediscovered with NETCONF, followed by an **Update the Telemetry Settings with Force** option.
- When Cisco DNA Center uses the FQDN certificate to collect device telemetry, devices must run Cisco IOS 17.5.1.

Role-Based Access Control and Audit Log

Financial organizations need granular access control based on roles. Cisco DNA Center supports role-based access control (RBAC) to define custom roles that permit or restrict user access to certain functions. For more information, see Cisco DNA Center User Role Permissions. Cisco DNA Center generates event-based audit logs that can be used to monitor user activity.

- Only a SUPER-ADMIN-ROLE user can define custom roles. By default, Cisco DNA Center comes with an admin role that already has these permissions.
- Audit logs are filtered by date and time.
- Audit logs are published on external log servers for further processing and storage.

Cisco DNA Center Disaster Recovery

Network resiliency is important to the financial sector. Cisco DNA Center disaster recovery provides data center failure protection. For more information, see Implement Disaster Recovery.

- The same security certificate is installed on both the main and recovery sites.
- With an FQDN-based certificate, the system name must be the same on both the main and recovery sites.
- Cisco DNA Center disaster recovery maintains the complete event history on its GUI. Notifications are enabled for email, log server, and web server.
- The Cisco DNA Center Security Best Practices Guide describes the best practices for setting up disaster recovery. The guide also explains which TCP and UDP ports must unblocked if the main and recovery sites are across a firewall.
- Cisco DNA Center disaster recovery works with a round-trip time (RTT) delay of 350 ms.
- Assurance data is not replicated across the clusters. Devices start sending Assurance data to new, active Cisco DNA Center clusters after failover has completed.

References

- Cisco SD-Access Solution Design Guide (Cisco Validated Design)
- Cisco DNA Center User Role Permissions
- Implement Disaster Recovery
- Support for Multiple Cisco DNA Center Clusters with a Single Cisco ISE System
- Cisco DNA Center Release Notes

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2021–2023 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.