Validated Profile: Retail (Non-Fabric and SD-WAN) Vertical

June 16, 2026

Note: For the Cisco Validated Profile for Cloud Managed Retail, refer to Validated Profile: Cloud Managed Retail Vertical.

Document purpose and usage

This document presents a Cisco Validated Profile (CVP) for retail enterprise networks built on Cisco Catalyst SD-WAN overlay architecture and Cisco Catalyst Center using a non-SD-Access (non-fabric) architecture.

This CVP:

- Provides a high-level, validated reference architecture for retail deployments that leverage Cisco Catalyst Center and Cisco Catalyst SD-WAN overlay architecture.
- Illustrates how Cisco Catalyst Center supports centralized visibility, automation, and lifecycle management across distributed retail sites.
- Describes how Cisco Catalyst SD-WAN overlay architecture enables reliable, scalable WAN connectivity between retail locations and central services.
- Establishes a common architectural baseline that engineers can adapt to different retail scales and operational models.

Deployment engineers can use the theoretical and practical sections of this document to understand service requirements and make informed decisions during network deployment and configuration.

This document guides customers and partners through the overall design approach and validated capabilities of the retail solution. Later sections address detailed design considerations, configurations, and operational workflows.

Target audience

This document targets deployment engineers, network architects, operations teams, and Cisco partners who plan, deploy, and manage retail networks using Cisco Catalyst Center and Cisco Catalyst SD-WAN overlay architecture.

Introduction

Retail enterprises typically operate large numbers of geographically distributed locations. Each location supports business-critical applications such as point-of-sale systems, inventory management, employee services, guest access, and IoT devices. Retail stores may also provide third-party vendor access (extranet) and host affiliate stores within their premises. These environments require a network architecture that is scalable, resilient, centrally managed, and operationally simple, while still allowing flexibility at individual store locations.

This Cisco Validated Profile describes a retail network solution built on Cisco Catalyst Center and Cisco Catalyst SD-WAN overlay architecture, using a non-SD-Access (traditional campus) design model. The solution enables centralized management and assurance while supporting local switching and site-specific operational requirements common in retail deployments.

Cisco Catalyst Center acts as the centralized management and automation platform for the retail network. It provides device discovery, Plug and Play onboarding, template-based configuration, software image lifecycle management, and end-to-end assurance for both wired and wireless infrastructure. These capabilities ensure consistent policy enforcement and operational visibility across all retail locations.

Cisco Catalyst SD-WAN overlay architecture provides the WAN connectivity foundation, enabling secure and resilient communication between retail stores, data centers, and cloud services. It improves application performance, simplifies branch connectivity, and supports rapid expansion as retailers add new locations.

Wireless connectivity plays a critical role in retail environments. Wireless mobility enables seamless and fast roaming throughout the store, which streamlines inventory management workflows, improves employee productivity, and enhances the overall customer experience. Centralized wireless management with local data switching supports overlapping IP address schemes, efficient WAN utilization, and consistent wireless policy enforcement across sites.

Network security remains a foundational requirement in retail environments to protect both business operations and customer data. This solution incorporates industry-standard security mechanisms, including:

Wired network security using IEEE 802.1X and MAC Authentication Bypass (MAB)

Wireless security features such as access point authentication, rogue access point detection, and guest wireless access controls

High availability ensures uninterrupted retail operations. The solution uses multiple redundancy and resiliency mechanisms—including switch stacking, Hot Standby Router Protocol (HSRP), StackWise Virtual Link (SVL), WAN path redundancy, wireless controller Stateful Switchover (SSO), and N+1 high availability models—to minimize service disruption during component failures.

Cisco Spaces integrates with the retail network to provide real-time location visibility and analytics across distributed store locations. By leveraging location telemetry from the wireless infrastructure, Cisco Spaces enables retailers to gain insights into in-store movement patterns and device presence without impacting network operations.

Capabilities such as heatmaps, dwell-time analytics, and location-based telemetry help retailers assess customer and device traffic patterns, understand space utilization, and evaluate the impact of network services on in-store experiences.

By combining location data from Cisco Spaces with Catalyst Center assurance, administrators can correlate application performance and connectivity events, which enables enhanced root cause analysis and improved operational workflows for both network and application issues.

This solution overview establishes a validated architectural foundation for retail deployments. Subsequent sections cover detailed architecture, topology, scale characteristics, and operational workflows.

Traditional networks versus Catalyst Center and SD-WAN

- Retail organizations often build traditional retail networks using site-specific designs that rely heavily on manual configuration and localized operational processes. As organizations scale to hundreds or thousands of stores, they find this approach increasingly difficult to manage and maintain.
- In contrast, a modern retail architecture using Cisco Catalyst Center and Cisco Catalyst SD-WAN overlay architecture offers a centrally managed, policy-driven approach to network deployment and operations. Catalyst Center enables consistent configuration, visibility, and assurance across campus and branch infrastructure, while SD-WAN provides a scalable and resilient WAN foundation that connects distributed retail locations to data centers and cloud services.
- By integrating campus, wireless, and WAN domains under a common operational framework, retail organizations reduce complexity, improve consistency, and gain end-to-end visibility across their environments.

Challenges in traditional retail networks

Retail organizations face increasing pressure to modernize their distributed store infrastructure while delivering secure, seamless, and personalized digital experiences across all customer touchpoints.

Traditional retail networks often present challenges, such as:

- Fragmented infrastructure across thousands of geographically distributed stores creates operational silos.
- Manual configurations cause inconsistent policies, configuration drift, and a higher risk of errors.
- Limited visibility prevents IT teams from monitoring application performance and user experience across in-store, data center, and cloud systems.
- Growing cybersecurity threats, particularly at the branch edge, expose stores to the internet.
- The increasing demand for real-time data and insights challenges retailers to optimize store operations, inventory workflows, and customer engagement.

These challenges hinder retail IT teams from operating efficiently and responding quickly to business and operational needs.

Why Cisco Catalyst SD-WAN overlay architecture

Cisco Catalyst SD-WAN overlay architecture provides an enterprise-grade WAN architecture overlay that facilitates digital and cloud transformation for enterprises. It integrates routing, security, centralized policy enforcement, and orchestration into large-scale networks. The solution offers multitenancy, cloud delivery, high automation, security, scalability, and application-awareness with rich analytics. Cisco Catalyst SD-WAN technology solves the common challenges of traditional WAN deployments. This technology provides several key benefits:

- Centralized management: Centralized network and policy management simplifies operations, which reduces change control and deployment times.
- Transport-independent overlay: A transport-independent overlay extends to the data center, branch, and cloud. Organizations can mix MPLS and low-cost broadband in an active/active fashion, which optimizes capacity and reduces bandwidth costs.
- Deployment flexibility: The separation of the control plane and data plane allows organizations to deploy control components on-premises or in the cloud. IT teams can deploy Cisco WAN Edge routers physically or virtually anywhere in the network.
- Robust security: The solution incorporates comprehensive security, including strong data encryption, end-to-end network segmentation, and certificate-based identity for routers and control components using a zero-trust security model. It also provides control plane protection, application firewalls, and integration with Cisco Umbrella and other network services.
- Seamless cloud connectivity: The solution facilitates seamless connectivity to the public cloud and extends the WAN edge to the branch.
- Application-aware policies: The solution recognizes applications and enforces real-time service-level agreements (SLAs) through application-aware policies.
- SaaS optimization: Dynamic optimization of SaaS applications improves performance for users.
- Rich analytics: Rich analytics provide visibility into applications and infrastructure, which enables rapid troubleshooting and assists in forecasting for effective resource planning.

Retailers must secure every part of the network that handles or stores payment card information to meet the Payment Card Industry Data Security Standard (PCI DSS). Key aspects include:

- **Network segmentation and traffic inspection**: Retailers must secure and segment network portions that pass or store payment card data to minimize the PCI scope. We recommend deploying zone-based firewalls at the store level to inspect traffic.
- **SD-WAN security features for PCI compliance**: Cisco SD-WAN supports PCI compliance through features such as IPsec encrypted tunnels, secure segmentation via VPNs and firewall zones, enterprise firewalls with application awareness, and intrusion prevention systems (IPS/IDS). These features ensure transport security, segmentation, perimeter control, and attack prevention in alignment with PCI requirements.
- **Certified SD-WAN controllers**: Cisco Catalyst SD-WAN controllers maintain PCI-DSS certification. They provide a secure infrastructure with features such as single sign-on, multi-factor authentication, audit logging, vulnerability scanning, and encrypted control plane communication. This certification simplifies the compliance journey for customers.
- **Segmentation best practices**: Retailers should segment point-of-sale (PoS) traffic from management and other non-PoS applications to reduce PCI scope and risk. Organizations achieve this through network addressing and segmentation strategies, including inline or redirection interception methods for traffic optimization and security.

In summary, organizations achieve PCI compliance in retail SD-WAN deployments by combining secure network segmentation, encrypted transport, enterprise-grade firewall and IPS capabilities, and certified SD-WAN controllers while adhering to Cisco's PCI design and implementation best practices.

Cisco Catalyst SD-WAN overlay architecture addresses five major use cases:

- Secure Automated WAN: The solution secures connectivity between remote offices, data centers, and public or private clouds over a transport-independent network.
- Application Performance Optimization: The solution improves the application experience for users at remote offices.
- Secure Direct Internet Access: The solution locally offloads internet traffic at the remote office.
- Remote Store Security: The solution provides WAN access and helps stores meet compliance demands on-site while offering constant protection against cyber threats, ranging from customer online shopping to multicloud SaaS environments.
- Multicloud Connectivity: The solution connects remote offices to cloud (SaaS and IaaS) applications over an optimal path and through regional colocation or exchange points where administrators can apply security services.

For more information, refer to Cisco Catalyst SD-WAN Data Sheet.

Why Catalyst Center

Cisco Catalyst Center serves as the central management and automation platform for the retail network and simplifies operations across wired and wireless domains.

Cisco Catalyst Center provides several key benefits for retail deployments:

- **Automates day-0 through day-n operations**: This reduces manual effort and operational overhead.
- **Enforces consistent policies and configurations**: The platform ensures uniformity across all retail sites.
- **Provides comprehensive assurance and visibility**: IT teams gain deep insights into device health, client experience, and network services.
- **Accelerates troubleshooting and root cause analysis**: The platform uses correlated telemetry and insights to resolve issues quickly.

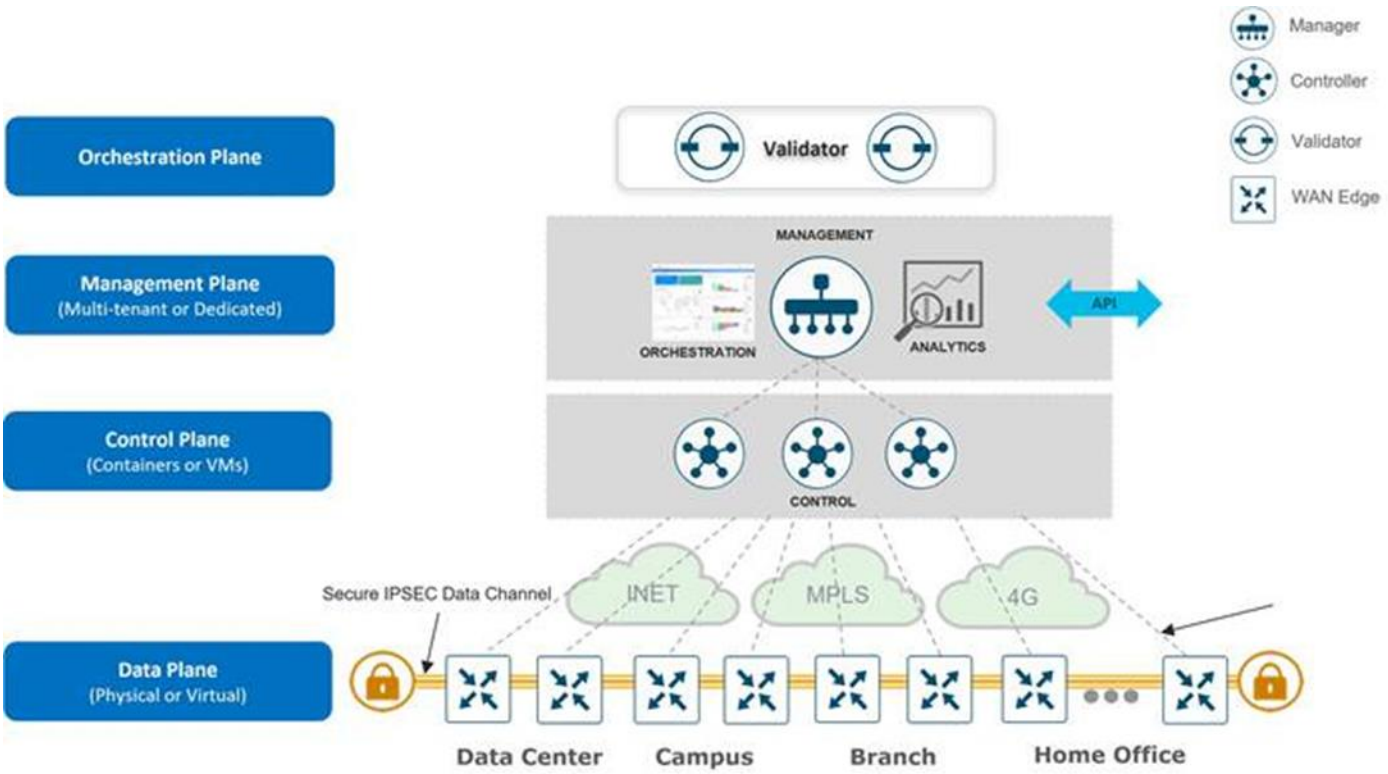
By combining Cisco Catalyst Center with Cisco Catalyst SD-WAN overlay architecture and integrated ecosystem components, retail IT teams operate their networks more efficiently and support evolving business requirements.

For more information, refer to Cisco Catalyst Center Data Sheet.

Cisco Catalyst SD-WAN components

The Cisco Catalyst SD-WAN solution separates its orchestration, management, control, and data planes. The orchestration plane automates the onboarding process for routers into the SD-WAN overlay. The management plane handles central configuration and monitoring. The control plane builds and maintains the network topology and determines traffic flow. Finally, the data plane forwards packets based on decisions from the control plane.

The Cisco Catalyst SD-WAN solution includes four primary components: the SD-WAN Manager (management plane), the SD-WAN Controller (control plane), the SD-WAN Validator (orchestration plane), and the WAN Edge router (data plane).



- **SD-WAN manager**: This software-based, centralized network management system provides a GUI that allows administrators to monitor, configure, and maintain all Cisco Catalyst SD-WAN devices and their connected links in the underlay and overlay networks. It offers a unified management dashboard for Day 0, Day 1, and Day 2 operations. Please consult this Data Sheet for a complete summary of recommended computing resources for Cisco Catalyst SD-WAN control components for software version 20.15.
- **SD-WAN controller**: This software-based component manages the centralized control plane of the SD-WAN network. It maintains a secure connection to each WAN Edge router and distributes routes and policy information via the Overlay Management Protocol (OMP), acting as a route reflector. It also orchestrates secure data plane connectivity between WAN Edge routers by reflecting crypto key information, which facilitates a highly scalable, IKE-less architecture.
- **SD-WAN validator**: This software-based component authenticates WAN Edge devices and orchestrates connectivity between the SD-WAN Controller, Manager, and WAN Edge routers. It also enables communication between devices located behind Network Address Translation (NAT).
- **WAN Edge routers**: These devices, available as hardware appliances or software-based routers, reside at a physical site or in the cloud and provide secure data plane connectivity among sites over one or

more WAN transports. They handle traffic forwarding, security, encryption, quality of service (QoS), and routing protocols such as BGP and OSPF.

Cisco Catalyst Center

Cisco Catalyst Center connects, secures, and automates retail network operations across wired and wireless infrastructure. In non-SD-Access retail environments, Catalyst Center simplifies the management of Cisco Catalyst switches, routers, wireless controllers, and access points, ensuring a consistent and reliable network experience across distributed store locations.

Catalyst Center provides enterprise-scale visibility and operational control for users, applications, and connected devices within retail stores, regional sites, and corporate locations. It enables retail IT teams to manage network lifecycle operations and monitor service health across both wired and wireless domains without requiring a fabric-based architecture.

Catalyst Center integrates automation, analytics, and policy enforcement to support these capabilities:

- Streamlining day-0 through day-n network operations.
- Providing visibility into client health, application performance, and network services.
- Integrating with Cisco and third-party platforms to support operational workflows.
- Managing centralized security policies and monitoring compliance across retail sites.
- Optimizing infrastructure efficiency, including Power over Ethernet (PoE) for in-store devices.

Organizations can deploy Cisco Catalyst Center as either a physical or virtual appliance, which provides the flexibility to align with specific retail infrastructure, scale, and operational requirements.

Refer to the Cisco Catalyst Center Data Sheet for a complete list of supported platforms and scale specifications. You can find Cisco Catalyst Center installation guides here.

Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) acts as a centralized network access control and policy platform that provides visibility, control, and consistent enforcement for users and devices accessing the retail network. In retail environments, ISE secures access across wired and wireless networks by validating user and device identity and applying access policies based on role, device type, and location.

ISE supports common retail use cases such as employee access, guest Wi-Fi, point-of-sale (POS) systems, IoT devices, and third-party vendor access. By integrating identity and posture information, ISE helps retail organizations enforce zero-trust principles and reduces the risk of unauthorized or non-compliant devices accessing critical business systems.

In non-SD-Access retail deployments, ISE integrates with Cisco Catalyst Center, wireless controllers, switches, and routers to provide these capabilities:

- Centralizes authentication, authorization, and accounting (AAA).
- Enforces policies using 802.1X, MAC Authentication Bypass (MAB), and web authentication.
- Controls access based on roles and segments the network using VLANs and downloadable ACLs.
- Manages guest access services with self-registration and sponsor workflows.
- Profiles and identifies devices for POS, scanners, cameras, and IoT endpoints.

ISE supports both standalone and distributed architectures, which allows retail organizations to scale from small deployments to environments with hundreds of thousands of endpoints. Retailers deploy distributed ISE nodes to ensure high availability, resiliency, and geographic scale, which proves essential for large retail footprints.

Organizations deploy ISE with multiple personas (Administration, Policy Service, and Monitoring) across dedicated or combined nodes, depending on scale and availability requirements. The *Cisco Identity Services Engine Administrator Guide* documents deployment guidance and sizing recommendations.

Refer to the Cisco Identity Services Engine Administrator Guide for information on ISE deployment models. For more ISE deployment and scale details, refer to the ISE Performance and Scalability Guide.

Cisco Catalyst 9000 Series switches

Cisco Catalyst 9000 Series switches provide a flexible, secure, and scalable switching foundation for retail networks. These switches support distributed branch and campus environments and deliver high-performance wired connectivity for store endpoints, such as point-of-sale (POS) systems, kiosks, digital signage, access points, cameras, and IoT devices.

In retail deployments, Catalyst 9000 switches support non-SD-Access architectures and integrate tightly with Cisco Catalyst Center to centralize configuration, monitoring, and assurance. This integration ensures consistent policy enforcement and operational visibility across thousands of geographically distributed retail locations.

Catalyst 9000 Series switches offer these key capabilities in retail environments:

- Stacking and redundant power supplies ensure high availability for always-on store operations.
- Integrated security features like 802.1X, MAC Authentication Bypass (MAB), and downloadable ACLs enforce role-based access control.
- Power over Ethernet (PoE and PoE+) powers wireless access points, cameras, and IoT devices.
- Telemetry and streaming data provide real-time visibility and assurance through Catalyst Center.
- Flexible form factors accommodate access, aggregation, and distribution layers in store, branch, and campus locations.

Cisco Catalyst 9000 Series switches serve as a critical component of the retail network, as they enable secure and reliable wired connectivity while simplifying operations and lifecycle management through automation.

Cisco Catalyst 9000 series switching offers flexible and highly scalable design options. For detailed platform specifications and capabilities, refer to the Cisco Catalyst 9000 Series data sheets.

Cisco Catalyst Wireless LAN Controller and Access Point

Cisco Catalyst 9800 Series Wireless LAN Controllers (WLCs) and Catalyst 9100 Series Access Points (APs) provide a secure, resilient, and highly scalable wireless foundation for retail environments. This solution supports seamless wireless connectivity across stores, campuses, and branch locations, enabling reliable access for employees, guests, IoT devices, and retail applications.

In retail deployments, Catalyst 9800 WLCs operate in non-SD-Access (non-fabric) mode and integrate tightly with Cisco Catalyst Center to simplify wireless design, provisioning, monitoring, and assurance. This integration enforces consistent wireless policy and provides operational visibility across geographically distributed retail locations.

Catalyst wireless solutions offer these key capabilities for retail environments:

- High-performance Wi-Fi connectivity: Supports point-of-sale (POS) systems, inventory scanners, mobile devices, digital signage, and customer guest access.
- Seamless and fast roaming: Improves employee mobility and enhances the customer experience across store floors.
- High availability: Utilizes Stateful Switchover (SSO) and N+1 redundancy models to ensure uninterrupted wireless services.
- Advanced wireless security: Includes access point authentication, rogue detection, and encrypted control and data planes.
- Telemetry and assurance: Integrates with Catalyst Center for proactive monitoring, client health visibility, and faster troubleshooting.

Cisco designed the Catalyst 9100 Series access points, including Wi-Fi 6 and Wi-Fi 6E models, for high-density retail environments. These access points integrate with Cisco Spaces to enable location-based services and analytics.

For detailed platform specifications and capabilities, refer to the Cisco Catalyst 9800 Series Wireless Controller and Catalyst 9100 Series Access Point data sheets.

Cisco Catalyst 9800 Series

Cisco Catalyst 9100 Series

Cisco Access Point and Wireless Controller Selector

Architecture overview

Solution components

Cisco built the retail architecture on an integrated networking and management stack designed for non-SD-Access deployments. The solution combines centralized management, secure connectivity, and scalable WAN transport to support geographically distributed retail locations.

The solution includes these key components:

- **Cisco Catalyst Center**: Centralizes automation, assurance, and visibility across wired and wireless networks.
- **Cisco Catalyst SD-WAN overlay architecture**: Provides resilient, secure, and scalable WAN connectivity between retail stores, data centers, and cloud services.
- **Cisco Catalyst 9000 Series switches**: Enable campus and branch wired access.
- **Cisco Catalyst 9800 Series Wireless LAN Controllers and Catalyst 9100 Series Access Points**: Deliver enterprise-grade wireless connectivity.
- **Cisco Identity Services Engine (ISE)**: Manages network access control and policy enforcement.
- **Cisco Secure Firewall (Firepower)**: Secures branch and edge environments.
- **Cisco ThousandEyes and Cisco Spaces**: Provide application assurance, visibility, and location-based analytics.

These components deliver a unified, policy-driven architecture that simplifies deployment and operations across large-scale retail environments.

Operational planes

The retail network architecture uses four logical planes to enable scalability, security, and operational efficiency:

- **Management plane**
  Cisco Catalyst Center, Cisco Catalyst SD-WAN overlay architecture, and integrated tools provide centralized orchestration, monitoring, assurance, and lifecycle management.
- **Control plane**
  The network manages routing, signaling, and sessions across wired, wireless, and WAN domains, including SD-WAN control and policy distribution.
- **Data plane**
  The infrastructure transports user, application, and device traffic across LAN, WLAN, and WAN environments using traditional IP forwarding.
- **Policy plane**
  Cisco ISE, firewall policies, and SD-WAN security capabilities drive identity-based access control, segmentation, and security policy enforcement.

This separation of planes enables centralized control and visibility while the network maintains simple and efficient packet forwarding at retail sites.

Network architecture

Retail deployments typically consist of distributed store locations connected to centralized data centers and cloud services over a secure WAN. Each store operates as a non-fabric site using traditional Layer 2 and Layer 3 designs, while benefiting from centralized policy and automation.

The architecture includes these key characteristics:

- **Non-SDA campus and branch design**: The network uses traditional VLANs, routing, and high availability mechanisms.
- **Centralized policy and configuration management**: Catalyst Center manages policies and configurations across all stores.
- **SD-WAN-based WAN connectivity**: This provides path optimization, application-aware routing, and resilience.
- **Integrated wireless architecture**: This supports employee, guest, and IoT connectivity.
- **End-to-end visibility**: The solution provides comprehensive monitoring across LAN, WLAN, and WAN domains.

This architecture enables consistent deployment patterns while allowing flexibility to accommodate varying store sizes and connectivity requirements.

High availability and resiliency

High availability is a critical requirement for retail environments, where network downtime can directly impact store operations, revenue, and customer experience. The retail architecture achieves resiliency through a combination of redundant hardware, resilient network design, and intelligent software mechanisms across campus, wireless, and WAN domains.

These capabilities provide high availability:

- **Campus and branch resiliency**
  Retail and campus networks use switch stacking, StackWise Virtual, and redundant uplinks to eliminate single points of failure and ensure continuous wired connectivity.
- **Wireless high availability**
  Stateful Switchover (SSO) and N+1 redundancy for Catalyst 9800 Wireless LAN Controllers enable seamless client continuity and fast recovery if a controller fails.
- **WAN resiliency with Cisco Catalyst SD-WAN overlay architecture**
  Retail sites connect to multiple WAN transports, which allows for intelligent path selection and fast failover. The control plane continuously monitors device and link health, while the data plane uses rapid failure detection mechanisms to reroute traffic with minimal disruption.
- **WAN resiliency using TLOC extension**

The TLOC (Transport Locator) extension in Cisco SD-WAN provides WAN resiliency by enabling redundancy and load sharing of transport links between WAN Edge routers at a site. This feature proves particularly useful in retail SD-WAN deployments where a single WAN Edge router cannot connect directly to multiple transports, or where IT teams want to minimize the cost and management overhead of additional devices like switches.

TLOC extension allows a WAN Edge router to access the transport connected to a neighboring WAN edge router through a TLOC-extension interface. This extends transport connectivity and provides redundancy for both control plane (DTLS/TLS) and data plane (IPsec/GRE) connections.

- **Centralized and distributed fault tolerance**
  Cisco deploys Catalyst SD-WAN components with geographic redundancy to support disaster recovery and business continuity. Management components operate in primary and secondary models to ensure service availability during site-level failures.

- **Security continuity at the edge**
  Distributed security enforcement at the branch edge ensures that security policies remain active and enforced even during WAN or upstream outages.
- Integrated Security Cisco SD-WAN edge routers in retail environments deliver comprehensive on-premises security through integrated NGFW, IPS, AMP, TLS decryption, and segmentation. They seamlessly integrate with cloud security services like Cisco Umbrella and SASE to protect users and data across distributed locations and cloud applications. This combination ensures secure WAN access, compliance with industry standards, and protection against evolving cyber threats both on-premises and in the cloud.

Together, these capabilities ensure the uninterrupted operation of critical retail services such as point-of-sale (POS) systems, inventory management, employee mobility, and guest Wi-Fi, while allowing retail IT teams to maintain consistent availability across thousands of distributed locations.

Wireless architecture

Wireless connectivity anchors the retail architecture, enabling mobility for store associates, customers, and connected devices.

Catalyst 9800 WLCs and Catalyst 9100 APs deliver these capabilities:

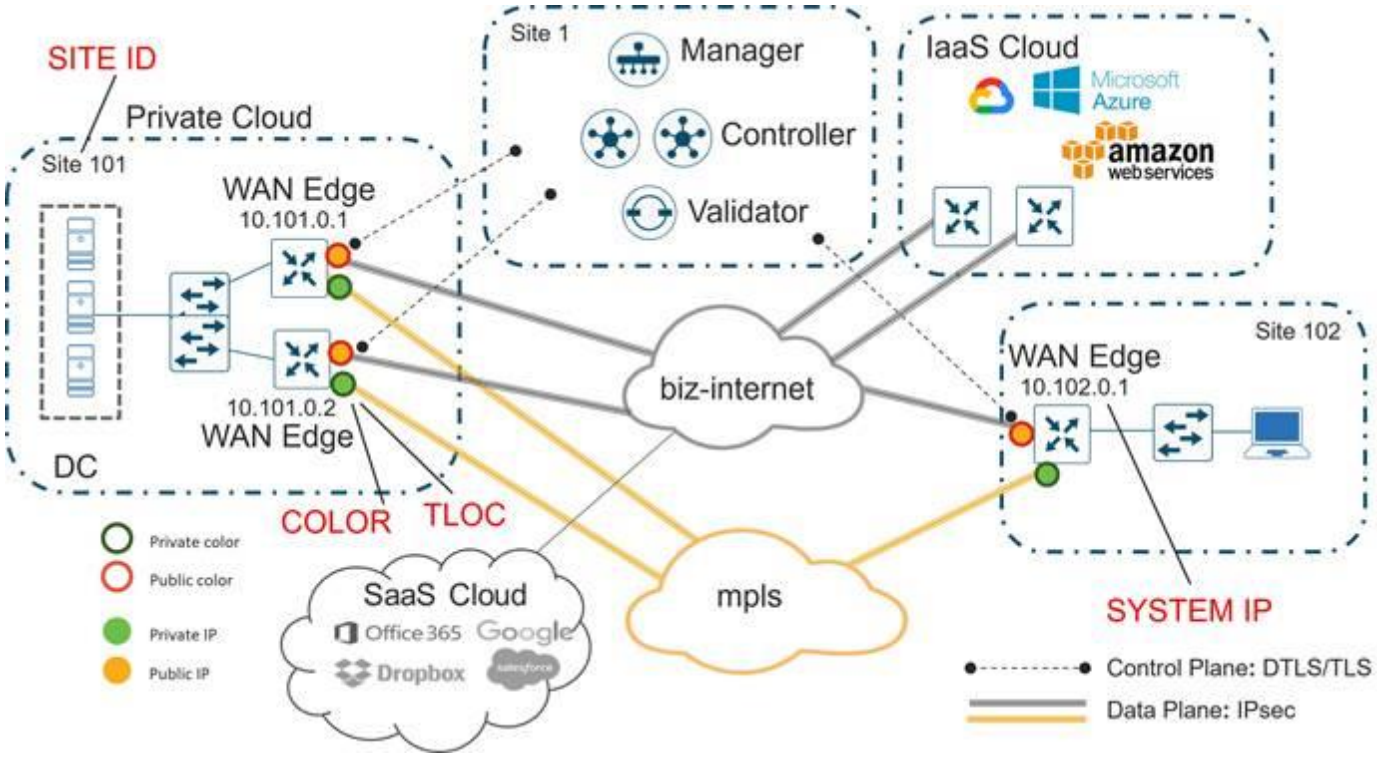
- Centralize wireless policy and image management
- Enable seamless roaming across store environments
- Provide secure employee and guest wireless access
- Integrate with Cisco Spaces for location analytics and insights
- Deliver telemetry and assurance via Catalyst Center

Wireless deployments operate in non-fabric mode and integrate natively with the broader campus and WAN architecture.

For more information, refer to the Cisco Solutions Offerings.

Cisco Catalyst SD-WAN solution constructs

This diagram demonstrates several aspects of the Cisco Catalyst SD-WAN solution. This sample topology connects two WAN Edge sites, each directly to a private MPLS transport and a public internet transport. The cloud-based SD-WAN Controllers, the SD-WAN Validator, and the SD-WAN Manager communicate directly through internet transport. Additionally, the topology provides cloud access to SaaS and IaaS applications.



WAN Edge routers form a permanent DTLS or TLS control connection to the SD-WAN Controllers and connect to both SD-WAN Controllers over each transport. The routers also form a permanent DTLS or TLS control connection to the SD-WAN Manager, but only over one of the transports. WAN Edge routers communicate securely with other WAN Edge routers using IPsec tunnels over each transport. The system enables the Bidirectional Forwarding Detection (BFD) protocol by default, which runs over each of these tunnels to detect loss, latency, jitter, and path failures.

Site ID – A unique identifier for a site in the SD-WAN overlay network with a numeric value between 1 and 4,294,967,295. It identifies the source location of an advertised prefix. Configure this ID on every WAN Edge device, including control components, and ensure it remains the same for all WAN Edge devices residing at the same site. A site could be a data center, branch office, campus, or similar location. By default, the system does not form IPsec tunnels between WAN Edge routers within the same site that share the same site-id.

System IP – A persistent, system-level IPv4 address that uniquely identifies the device independently of any interface addresses. It functions like a router ID, so you do not need to advertise or define it within the underlay. Assign this to the system interface that resides in VPN 0. As a best practice, assign this system IP address to a loopback interface and advertise it in any service VPN. You can then use it as a source IP address for SNMP and logging to correlate network events with SD-WAN Manager information easily.

Organization Name – You assign this to the entire SD-WAN overlay. This field is case-sensitive and must match the organization name configured on all SD-WAN devices in the overlay. The system uses it to define the Organization Unit (OU) field during the Certificate Authentication process when you bring an SD-WAN device into the overlay network.

Public and Private IP Addresses –

Private IP Address – On WAN Edge routers, the interface assigns this IP address to the SD-WAN device. This represents the pre-NAT address, which can be a public or private address (RFC 1918).

Public IP Address – The SD-WAN Validator detects this Post-NAT address. This address can be either a public (routably) or a private address (RFC 1918). In the absence of NAT, the private and public IP addresses of the SD-WAN device remain the same.

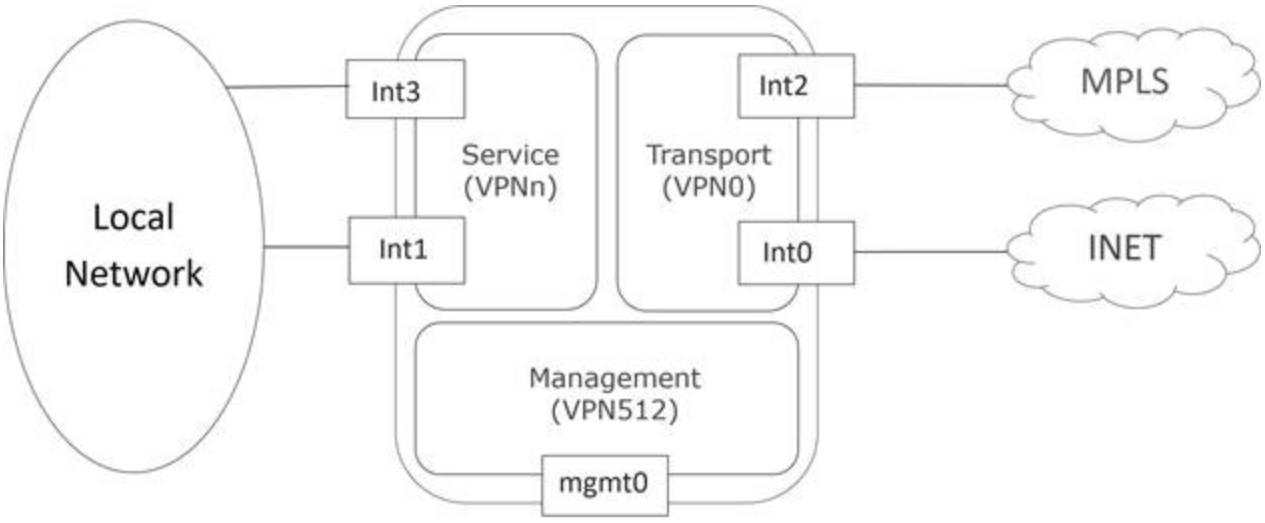
TLOC – The "Transport Locator" (TLOC) acts as the attachment point where a WAN Edge router connects to the WAN transport network. A three-tuple uniquely identifies and represents a TLOC: System IP, link color, and Encapsulation (GRE/IPSec).

Color – This applies to WAN Edge routers, SD-WAN Managers, and Controllers to help identify an individual TLOC; the system assigns different color labels to different TLOCs. The sample SD-WAN topology uses a public color called "biz-internet" for the internet transport TLOC and a private color called "mpls" for the other transport TLOC.

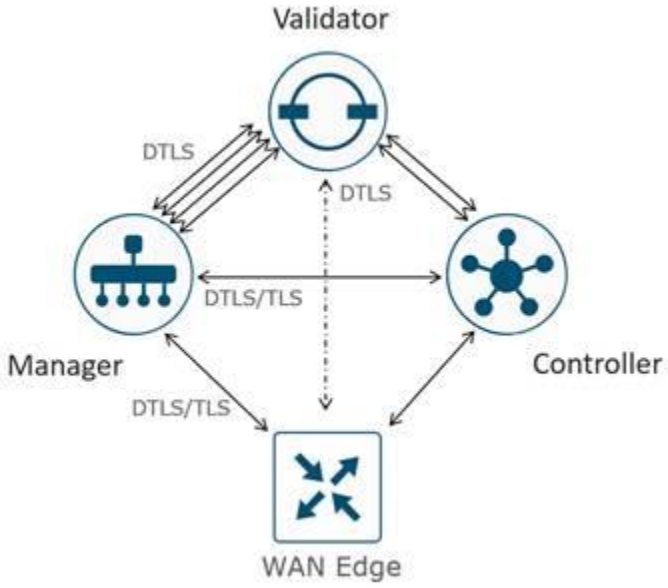
Overlay Management Protocol (OMP) – This core routing protocol of Cisco Catalyst SD-WAN overlay architecture, which features a structure similar to BGP, manages the SD-WAN overlay network. The protocol runs between SD-WAN Controllers and between SD-WAN Controllers and WAN Edge routers, where routers exchange control plane information, such as route prefixes, next-hop routes, crypto keys, and policy information, over a secure DTLS or TLS connection. The SD-WAN Controller acts like a BGP route reflector; it receives routes from WAN Edge routers, processes and applies any policy to them, and then advertises them to other WAN Edge routers in the overlay network.

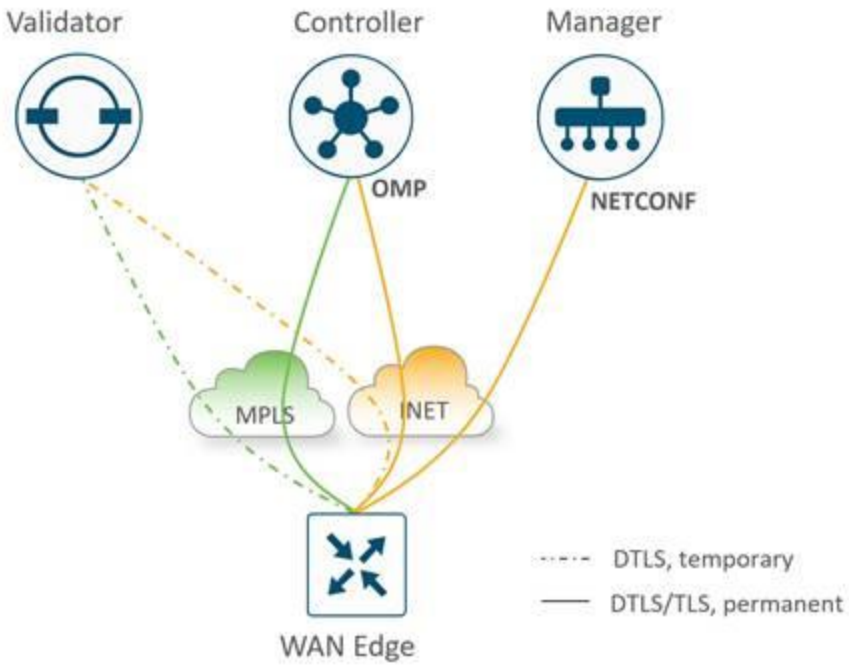
Virtual private networks (VPNs) – In the Cisco Catalyst SD-WAN overlay, VPNs provide segmentation, similar to VRFs (Virtual Routing and Forwarding). Each VPN remains isolated, and each possesses its own forwarding table. Administrators explicitly configure an interface or sub-interface under a single VPN, and it cannot belong to more than one VPN. The system uses labels in OMP route attributes and packet encapsulation to identify the VPN to which a packet belongs. Two main VPNs exist by default in WAN Edge devices and control components: VPN 0 and VPN 512. VPN 0 functions as a transport VPN; it contains the interfaces that connect to the WAN transports and initiates secure DTLS/TLS connections to the control components. VPN 512 functions as the management VPN; it carries out-of-band management traffic to and from the Cisco Catalyst SD-WAN devices.

The figure demonstrates VPNs on a WAN Edge router. Int0 and Int2 belong to the transport VPN; Int1 and Int3 belong to the service VPN, which attaches to the local network at the site; and the mgmt0 port belongs to VPN 512.



Control Connections – The Cisco Catalyst SD-WAN Manager and Controllers initially contact and authenticate to the SD-WAN Validator, forming persistent DTLS connections, and subsequently establish and maintain persistent DTLS/TLS connections with each other. WAN Edge devices onboard similarly but drop the transient SD-WAN Validator connection and maintain DTLS/TLS connections with the SD-WAN Manager and Controllers. The diagrams illustrate various control connections between controllers and WAN edge devices.





For more detail about Cisco Catalyst SD-WAN Architecture and components, refer to the Cisco Catalyst SD-WAN Design Guide.

Compatibility matrix

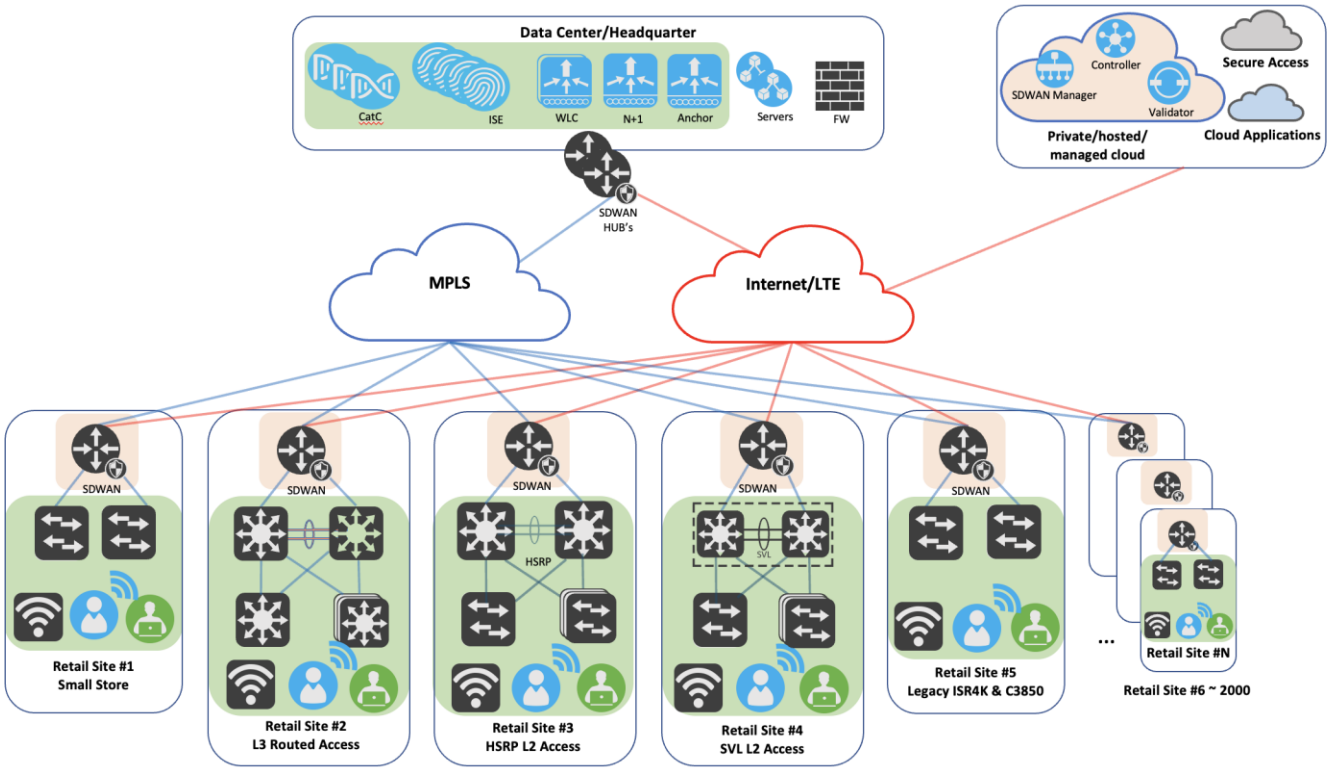
Cisco Catalyst Center supports Cisco enterprise switching, routing, and mobility products. Refer to the compatibility matrix for a complete list of supported Cisco products, which is updated regularly.

Cisco Catalyst Center Compatibility Matrix

SDWAN Compatibility Matrix

Retail profile deployment

This section provides design guidance for retail spaces, demonstrating how Cisco Catalyst Center and Catalyst SD-WAN create simple, secure, and flexible networks. These topologies, use cases, and solutions address standard deployment requirements for retail organizations.



Retail branch deployment types

Retail networks typically include multiple store formats with varying scales, availability, and service needs. These branch types map common store sizes and functions to validated Cisco architectures.

VPN requirements:

- Retailers typically deploy up to four Service VPNs: VPN 10 (Employee), VPN 20 (POS), VPN 30 (Monitoring), and VPN 40 (Guest).
- Small branches require VPN 10 and VPN 40 only when they include a secured kiosk with employee access.

Small retail sites

Characteristics:

- Small footprint stores, kiosks, pop-up locations, or limited-service outlets.
- Support for up to 50 users or devices, primarily POS terminals, handheld scanners, and a small number of employee devices.
- Limited application services with basic employee and guest wireless access.

Topology and design:

- A single WAN router (Catalyst 8200/8300 or ISR 1100 Series) connects via one or two WAN circuits (MPLS or internet/LTE).

- A Catalyst 9300 serves as a Layer 2 access switch.
- A centralized wireless controller (9800) resides at the HQ/Data Center.
- APs operate in FlexConnect mode to ensure local switching and survivability.
- The system locally switches guest and employee traffic, with optional central anchoring for guest traffic.
- The configuration supports Ethernet LAN connectivity for up to eight devices.
- The design enables local internet breakout with NAT on the directly connected transport.
- Security features incorporate an enterprise firewall with application awareness, IPS, URL filtering, AMP, and DNS/web-layer security.
- Retailers may provide guest Wi-Fi where cost-effective.
- The design provides limited transport redundancy via a single WAN circuit.
- Cisco SD-WAN Manager provides centralized management and policy enforcement.

Medium and standard retail sites

Characteristics:

- Full-service retail stores accommodate higher device density.
- These stores support POS systems, employee devices, inventory systems, cameras, and guest Wi-Fi.
- These environments require moderate bandwidth and network redundancy.

Topology and design:

- A single WAN router (Catalyst 8300 Series) manages dual WAN circuits (MPLS + internet or dual internet).
- Multiple Catalyst 9300 switches provide Layer 3 routed access.
- A Catalyst 9300/9500 switch pair forms the distribution layer.
- A centralized 9800 WLC resides at the HQ/Data Center.
- The design uses a mix of central switching and FlexConnect, depending on application requirements.
- The network provides Ethernet LAN connectivity for up to eight devices, including computers, POS terminals, WLAN APs, and video surveillance.
- The architecture achieves N+1 WAN transport redundancy.
- Local internet breakout uses NAT and SIG tunnels for cloud security.
- Security features include an enterprise firewall, IPS, URL filtering, AMP, DNS security, and integration with Cisco Umbrella SIG.
- Dual internet circuits and SIG tunnel health checks ensure high availability.
- Cisco SD-WAN Manager provides centralized policy enforcement and monitoring.

Large retail sites, distribution centers, and warehouses

Characteristics:

- These sites handle high device density and business-critical operations.
- Warehouses, distribution centers, or super-large retail locations define this category.
- They support hundreds of devices, including scanners, cameras, and automation systems.
- This design suits logistics-heavy retail environments.

Topology and design:

- Dual Catalyst 8300 Series routers provide redundant WAN connectivity.
- Multiple Catalyst 9300 stacks provide Layer 2 access switching.
- A Catalyst 9300 and 9500 pair forms the distribution layer.
- Administrators configure HSRP at the distribution layer to ensure load sharing and resiliency.
- A centralized 9800 WLC manages APs using FlexConnect.
- The network provides Ethernet LAN connectivity for up to eight devices.
- The architecture achieves N+2 WAN transport redundancy.
- Local internet breakout uses NAT, SIG integration, and advanced security features.
- Security features include an enterprise firewall with application awareness, IPS, URL filtering, AMP, DNS/web-layer security, TLS/SSL decryption, and zero-trust authentication.
- Multiple WAN transports and cellular backup ensure high availability.
- Cisco SD-WAN Manager provides centralized management and policy enforcement.

Superstore

Characteristics:

- Large to super-large retail sites require modern switching capabilities.
- These environments prioritize simplified operations and faster convergence.
- StackWise Virtual (SVL) simplifies the distribution layer by acting as a single logical switch.
- This approach enables faster failover and reduces operational complexity.
- These designs fit newer retail builds or network refresh projects.

Topology and design:

- Dual Catalyst 8300 Series routers provide redundant WAN links.
- Catalyst 9300 stacks provide Layer 2 access switching.
- Catalyst 9500 SVL (StackWise Virtual) forms the distribution layer.
- A centralized 9800 WLC resides at the HQ/Data Center.
- FlexConnect APs ensure network survivability.

These definitions align with Cisco's validated profiles and design case studies for SD-WAN deployments in retail verticals. They differentiate architectures clearly based on router count, WAN circuits, throughput, device support, and use case criticality.

Site communication and address translation considerations

Retail and enterprise deployments, especially those resulting from mergers and acquisitions, frequently encounter overlapping IP address spaces across sites. In these scenarios, multiple locations use identical internal (service-side) subnets, which prevents direct routing across the WAN overlay without address translation.

To solve this, the Cisco Catalyst SD-WAN fabric implements Service-Side NAT (inside NAT) to ensure address uniqueness when users access shared or centralized services.

SSNAT-based design

- WAN edge devices (cEdges) perform Service-side NAT. They translate traffic from overlapping local subnets into unique, non-overlapping addresses before forwarding it across the SD-WAN overlay toward shared services, such as data centers, private cloud, or SaaS via centralized egress.
- Unlike traditional SNAT for internet breakout, this model focuses on translating internal (LAN/service-side) subnets to ensure reachability to common service endpoints across sites with duplicate addressing.
- The system assigns a unique NAT pool or prefix to each site (or group of sites), which ensures that traffic entering the overlay remains globally unique and allows for deterministic routing.
- Services route return traffic back based on the translated (NATed) address, and the originating WAN edge performs reverse translation to deliver traffic to the correct local subnet.

Key considerations:

- **Deterministic NAT mapping**: Assign each site a unique, non-overlapping NAT pool or prefix to prevent return traffic ambiguity and ensure consistent routing.
- **Policy-based NAT control**: Apply NAT policies selectively only to traffic destined for shared services where overlap occurs. Bypass NAT for non-overlapping or intra-site traffic to preserve visibility and simplify troubleshooting.
- **Routing alignment**: The SD-WAN overlay (OMP routes) advertises translated prefixes rather than original overlapping subnets to service nodes to maintain consistency.
- **Symmetry enforcement**: Ensure that forward and return paths traverse the same WAN edge to maintain NAT state and prevent session drops.
- **Segmentation awareness (VPN/VRF)**: Align NAT policies with SD-WAN VPN segmentation. Because overlapping subnets may exist in the same or different VPNs, scope NAT behavior accordingly.
- **Logging and observability**: Enable flow logging, NAT translation visibility, and telemetry on WAN edges to trace original-to-translated IP mappings for troubleshooting and audit purposes.
- S**calability and pool design**: Plan NAT pools carefully to accommodate growth, such as onboarding newly acquired sites, without requiring redesigns.
- **Operational consistency**: Centralized policy definition via Cisco Catalyst SD-WAN controllers (vManage) ensures consistent deployment and reduces configuration drift across edges.

This service-side NAT approach enables organizations to integrate overlapping networks seamlessly during mergers and acquisitions. It allows continued access to shared services without requiring immediate IP readdressing while maintaining scalable and predictable network operations.

Business outcomes and challenges

Retail networks operate as highly distributed, diverse, and complex systems that support a wide range of business-critical applications across thousands of locations. These environments demand high levels of security, resiliency, and regulatory compliance to maintain consistent performance and operational efficiency.

To achieve business outcomes, such as uninterrupted store operations, secure customer transactions, and improved customer experiences, retailers must incorporate core network capabilities that address operational challenges and evolving business demands. These sections outline the critical network capabilities that support modern retail organizations at scale.

Large-scale multisite deployments

Retail networks typically span hundreds to thousands of geographically distributed sites. This scale makes traditional box-by-box or site-by-site management operationally inefficient and difficult to manage. Maintaining consistent configurations, policies, and software versions across such a vast footprint challenges network teams, especially when stores lack local IT support.

Automation solves these challenges for modern retail deployments. By leveraging centralized orchestration and policy-driven workflows, retail organizations deploy complex site architectures rapidly and consistently. This strategy minimizes manual configuration, reduces errors, and lowers operational overhead. It enables network teams to scale efficiently while maintaining reliability, security, and consistency across all retail locations.

Automation and monitoring

Large retail organizations with global footprints require networks that support rapid site bring-up and centralized management without local IT resources. Retail environments need solutions that enable remote deployment, configuration, and ongoing operations to support lean, efficient IT models.

Network automation and continuous assurance reduce operational complexity and minimize time spent on deployment and troubleshooting. Centralized automation, real-time monitoring, and proactive analytics allow retail IT teams to accelerate rollouts, maintain consistent policies across locations, and resolve issues quickly before they impact store operations or customer experiences.

Security challenges in retail

Retailers prioritize security as a critical pillar of modern networks, as they must protect sensitive business and customer data while maintaining regulatory compliance. Retail organizations mitigate an expanding threat landscape by implementing robust security controls, enforcing consistent policies, and continuously assessing risk across distributed store environments.

Cisco security capabilities integrated with Catalyst Center and Cisco Catalyst SD-WAN overlay architecture enable retail customers to adopt flexible security deployment models based on their operational and compliance requirements. On-premises security solutions provide greater control, customization, and compliance for environments handling sensitive data, while cloud-based security services offer scalability, advanced threat protection, and operational efficiency. In many retail deployments, a hybrid security approach delivers the best balance by combining local enforcement at the branch edge with cloud-based inspection and intelligence.

Retail Chief Information Security Officers (CISOs) identify cybersecurity as a top concern. The growth of digital storefronts, guest Wi-Fi, IoT devices, and hybrid workforce models significantly increases the attack surface across retail networks. An integrated, defense-in-depth security architecture helps retail

organizations reduce risk, respond faster to threats, and maintain secure, reliable operations without compromising the customer experience.

The need for guest user isolation

Retail environments provide guest network access to customers using diverse personal devices, some of which may be unmanaged or potentially compromised. To protect business-critical systems and sensitive data, the network isolates guest traffic from corporate resources and inspects it continuously.

The retail network architecture enforces strict separation of guest traffic across wired and wireless access. The system directs all guest traffic to a firewall in a demilitarized zone (DMZ) as the first point of network access, which enables centralized policy enforcement, threat inspection, and secure internet breakout. This approach delivers guest connectivity safely without increasing the risk to internal retail systems while maintaining a seamless experience for customers.

Compliance and regulatory requirements

Retail organizations handle large volumes of sensitive data, including payment card information, customer data, and operational systems that must comply with strict regulatory and security requirements. As retail networks evolve toward highly distributed, cloud-connected environments, maintaining consistent compliance across thousands of store locations becomes increasingly critical.

Cisco Catalyst SD-WAN overlay architecture helps retail customers meet industry and regulatory compliance requirements by providing secure connectivity, centralized policy enforcement, and continuous visibility across branch, data center, and cloud environments. The solution supports compliance with widely adopted industry standards relevant to retail deployments, such as PCI-DSS for payment card security, SOC2/SOC3, and multiple ISO information security standards.

Key compliance capabilities for retail SD-WAN deployments:

- **Data protection and encryption**

  Encrypted IPsec tunnels protect all sensitive data in transit between retail stores, data centers, and cloud services, which ensures the confidentiality and integrity of transactional and operational data.

- **Traffic segmentation and isolation**

  VPNs and firewall zones isolate payment systems, corporate traffic, IoT devices, and guest access, which reduces the attack surface and supports PCI-DSS requirements.

- **Integrated firewall and threat protection**

  Stateful firewall services with application awareness, along with intrusion prevention and detection capabilities, inspect traffic and prevent security threats at the branch edge.

- **Centralized policy management and auditing**

  Centralized configuration management ensures consistent security baselines across all retail locations. Role-based access control (RBAC), audit logging, and secure change tracking support operational governance and compliance audits.

- **Continuous monitoring and validation**

  Ongoing visibility, vulnerability assessments, and regular internal and external audits help retail organizations maintain compliance and adapt to evolving regulatory requirements.

- **Cloud security integration**

  Native integration with cloud-based security services and Secure Service Edge (SSE) solutions enforces consistent policies and protects against threats for SaaS and cloud applications commonly used in retail environments.

- **Compliance enforcement in Cisco Catalyst SD-WAN management**

  Cisco Catalyst SD-WAN overlay architecture aligns configurations with required industry certifications, which simplifies compliance management across large-scale retail deployments.

Supported standards and certifications:

Cisco Catalyst SD-WAN overlay architecture helps retail organizations meet key industry standards, such as:

- PCI-DSS for payment card data security
- SOC2 and SOC3 for security and operational controls
- ISO 27001, 27701, 27017, and 27018 for information security and privacy management
- C5 and ENS certifications for cloud security assurance

By combining strong encryption, segmentation, centralized management, and integrated security services, Cisco Catalyst SD-WAN overlay architecture enables retail organizations to maintain compliance, protect sensitive data, and support secure omnichannel operations at scale.

User experience business outcomes

SD-WAN deployment improves retail customer experience in several key ways:

1. **Cisco accelerates deployment and scaling**.

   Cisco Customer Experience services drive a smooth transformation by prioritizing setup and transition at the first retail locations, then scaling SD-WAN quickly across all sites. Teams categorize sites, create templates, define global policies, and enable the right security architecture to prevent major roadblocks and deliver successful rollout. This approach can reduce total operating costs by up to 38% over five years. 1

2. **Cisco improves application performance and visibility.**

   Cisco Catalyst SD-WAN overlay architecture improves application performance by reducing packet loss, jitter, and delay. It uses application-aware routing to send traffic over WAN links that meet specific SLA policies. Integration with ThousandEyes expands visibility across internet, cloud, and SaaS applications, helping teams resolve issues faster and manage performance more effectively in retail environments that rely on dependable connectivity. 2, 3

3. R**etailers create better in-store experiences.**

   Retailers such as Woolworths use Cisco Catalyst SD-WAN overlay architecture and digital network architecture to build connected store experiences. These solutions improve software compliance, increase connected devices per store, and provide real-time access to customer insights. As a result, stores increase shopping lane availability and gain a flexible, scalable foundation for continued innovation. 4

4. **Cisco strengthens secure, reliable connectivity.**

   SD-WAN enables secure direct internet access (DIA) at branch locations, which reduces latency and improves application performance by removing backhaul through central data centers. Embedded Cisco Catalyst SD-WAN security features, plus integration with Cisco Umbrella Cloud, protect retail networks and provide resilient connectivity for customers and store associates. 2

5. **Cisco boosts associate and customer engagement.**

   Cisco solutions equip store associates with mobile tools and real-time information, which improves productivity and effectiveness. Associates deliver better service and more personalized shopping experiences, supporting stronger sales growth and higher customer satisfaction. 5

Cisco Catalyst SD-WAN overlay architecture improves retail user experience by accelerating rollout, optimizing application performance, strengthening security, and enabling reliable, real-time connectivity and insights for both customers and store associates.

High sensitivity to quality of service (QoS)

Besides managing security, compliance, and availability, organizations must prevent slow, inconsistent network performance because it reduces customer satisfaction and drives financial losses. On trading floors, where even small delays disrupt operations, organizations need low latency and consistent QoS to meet business requirements.

Operational

Maximize productivity, simplify digital transformation initiatives, manage reputation effectively, and enhance brand value.

Centralized and consistent policy management

As endpoint connections grow exponentially and large retail organizations expand worldwide, security teams must manage policies across multiple geographic regions. Local laws often shape these rules, which increases management complexity. Teams need to simplify user and device grouping so they can manage security policies more intuitively.

Acquisitions integration

To realize full collaboration and value from an acquisition, organizations must integrate both companies' systems and streamline redundant operations. Teams usually start with network integration, but they must secure that process to avoid introducing new vulnerabilities.

Solutions to retail challenges and business outcomes

The solutions discussed here help meet the business requirements defined for retail network deployment.

Retail

Modern IT infrastructure management relies on two essential components: automation and monitoring. Organizations use automation to handle tasks such as software deployment, configuration management, system provisioning, and workflow orchestration. By automating repetitive and time-consuming tasks, organizations improve efficiency, reduce errors, and free up human resources to focus on more strategic activities. Monitoring, on the other hand, empowers IT teams to continuously observe and analyze the performance and health of IT systems, networks, applications, and services.

Cisco Catalyst SD-WAN Manager serves as a key component of the Cisco Catalyst SD-WAN solution. It plays a crucial role in simplifying network operations by providing centralized management and control of the SD-WAN infrastructure. Cisco Catalyst SD-WAN Manager simplifies network operations in several key ways:

Centralized management

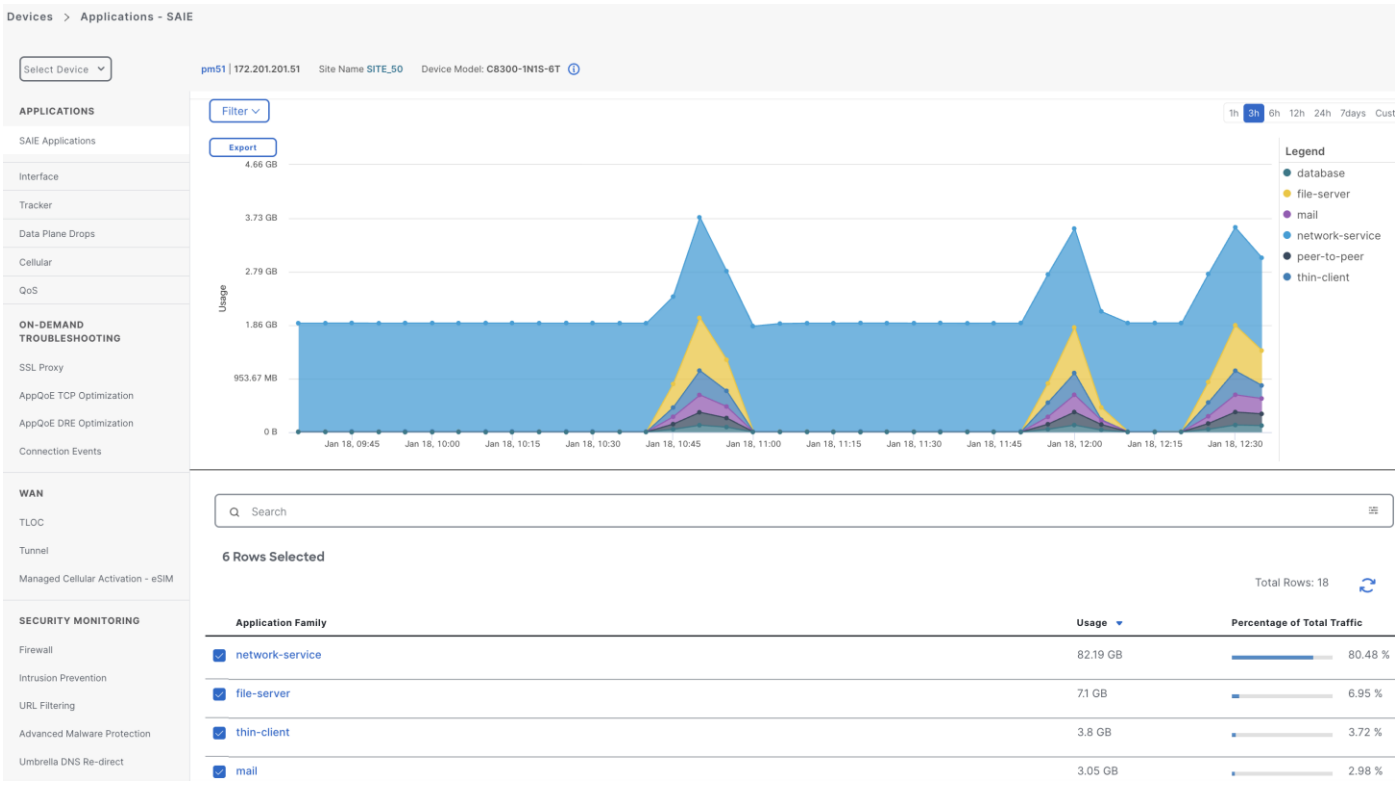
Cisco Catalyst SD-WAN Manager gives network administrators a single-pane-of-glass view of the entire SD-WAN network, making it easier to configure, monitor, and manage network resources. By centralizing management, it eliminates the need to access and manage individual network devices, simplifying network administration significantly.

Automation and orchestration

Cisco Catalyst SD-WAN Manager empowers administrators to automate and orchestrate network operations by defining and enforcing network policies from a central location. This approach eliminates manual configuration on individual devices, reduces the risk of human error, and ensures consistent policy enforcement across the entire network.

Application visibility and control

Cisco Catalyst SD-WAN Manager gives administrators deep visibility into network traffic and application performance. Administrators can use this visibility to identify and prioritize critical applications, ensuring they receive the necessary network resources. This capability improves application performance and user experience, making network operations simpler and more efficient.

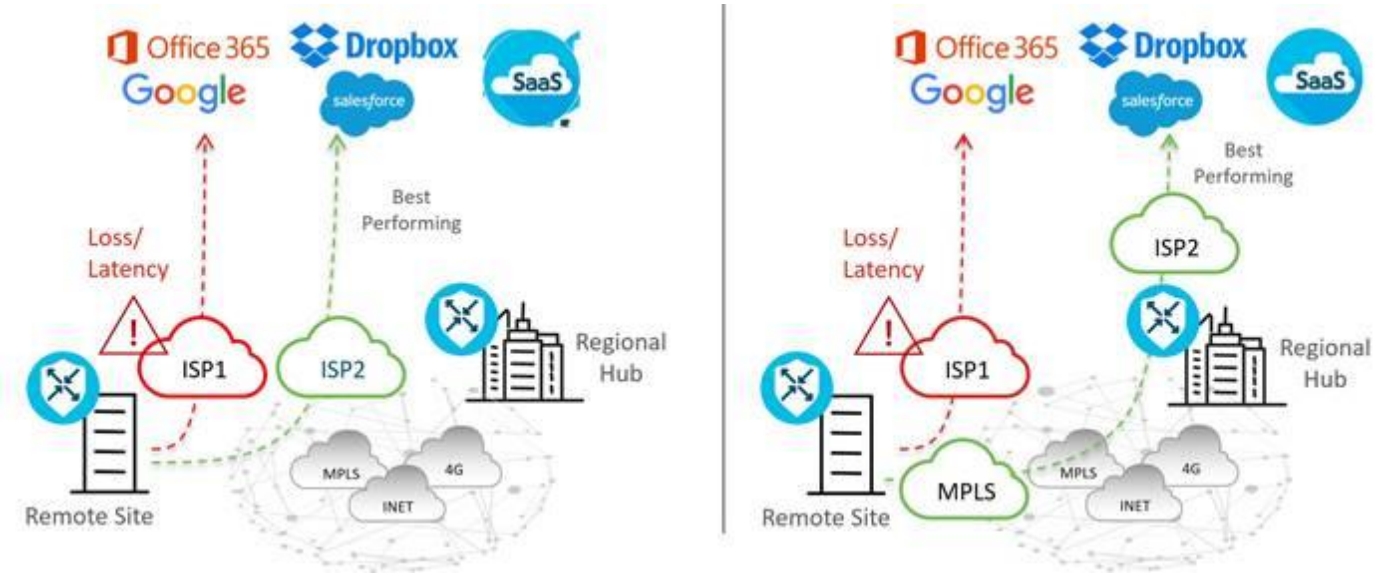


Application experience

Software-as-a-Service (SaaS): Traditionally, branches accessed SaaS applications such as Salesforce, Box, and Office 365 through centralized data centers, which increased application latency and created an unpredictable user experience. As SD-WAN evolved, organizations gained additional network paths to access SaaS applications, including Direct Internet Access and access through regional gateways or colocation sites. However, network administrators often have limited or no visibility into SaaS application performance from remote sites, making it difficult to choose the best network path to optimize the end-user experience. Additionally, when network changes or impairments occur, administrators may have no easy way to move affected applications to an alternate path.

Cloud onRamp for SaaS solves these challenges by allowing administrators to easily configure access to SaaS applications, either directly from the internet or through gateway locations. It continuously probes, measures, and monitors the performance of each path to each SaaS application, and automatically selects the best-performing path based on loss and delay. When impairment occurs, Cloud onRamp for SaaS dynamically and intelligently moves SaaS traffic to the updated optimal path.

Beyond these core benefits, Cisco has introduced several new features to strengthen the integration between SD-WAN Cloud onRamp for SaaS and Office 365. These enhancements give users more insightful metrics, greater control over traffic flow for individual Office 365 applications, and automatic remediation of suboptimal performance by factoring in Microsoft telemetry metrics.



Zero-touch provisioning

Cisco Catalyst SD-WAN Manager supports zero-touch provisioning, enabling organizations to deploy new SD-WAN devices without manual configuration. This capability significantly reduces deployment time and minimizes the need for on-site technical expertise. On the backend, integration with Cisco's Plug and Play portal further streamlines the onboarding of edge locations.

LAN automation

Cisco LAN Automation simplifies network operations by freeing IT staff from time-consuming, repetitive configuration tasks and building a standard, error-free underlay network. It accelerates underlay network deployment by eliminating the need for traditional network planning and implementation processes.

Cisco LAN Automation delivers these key benefits:

Zero-touch provisioning

Cisco LAN Automation dynamically discovers, onboards, and automates network devices from their factory-default state to fully integrated network participants, requiring no manual intervention.

End-to-end topology

Cisco LAN Automation dynamically discovers new network systems and their physical connectivity, then models and programs them into the network. It automates Layer 3 IP addressing and routing protocols to dynamically build end-to-end routing topologies.

Resilience

Cisco LAN Automation integrates system and network configuration parameters that optimize forwarding topologies and redundancy. It enables system-level redundancy and automates best practices to deliver resiliency during both planned and unplanned network outages.

Security

Cisco LAN Automation applies Cisco-recommended network access and infrastructure protection parameters from the initial deployment, building security into the network from day one.

Compliance

Cisco LAN Automation eliminates human errors, misconfigurations, and inconsistent rules and settings that drain IT resources. During new system onboarding, it enforces compliance across the network infrastructure by automating globally managed parameters directly from Cisco Catalyst Center.

Troubleshooting using iCAP

Smaller retail branches often lack an onsite network support team, making troubleshooting significantly more difficult.

Intelligent Capture capability of Cisco Catalyst Center addresses this challenge by establishing a direct communication link between Cisco Catalyst Center and access points (APs) in Cisco Non SD-Access Wireless environments. Through this link, Cisco Catalyst Center receives packet capture data, AP and client statistics, and spectrum data. This direct connection also gives administrators access to AP data that wireless controllers alone cannot provide.

Plug and Play (PnP) and Return Material Authorization (RMA)

Cisco Catalyst Center helps network administrators automate the deployment of Catalyst 9000 series switches at branch or campus locations using built-in Plug-and-Play (PnP) functionality. This feature allows switches, routers, and wireless access points to onboard to the network automatically. A built-in agent on each device connects to Cisco Catalyst Center and downloads the required software and configuration, eliminating the need for manual setup.

Managing device replacements across an enterprise network with hundreds or thousands of devices can be a complex and error-prone process. Administrators must identify replacement hardware with the correct software version and manually replicate configurations, which increases the risk of copy-paste errors and misconfigurations. Cisco Catalyst Center simplifies this process by providing a complete workflow that guides administrators through identifying, configuring, and replacing network device hardware quickly and accurately.

For detailed information, refer to Network Device Onboarding.

For more information on Cisco Catalyst SD-WAN Plug-n-Play deployment of edge devices, refer to Onboard a cEdge Device with PnP Process and Cisco Plug and Play Support Guide for Cisco SD-WAN Products.

Software upgrade and image management

Network administrators can use the Cisco Catalyst Center Software Image Management (SWIM) solution to automate software upgrades for Catalyst 9000 series switches at branch or campus locations. SWIM also helps administrators standardize software images across all network devices.

Cisco Catalyst Center stores all unique software images organized by image type and version for every device in the network. Administrators can view, import, and delete software images, and push them directly to network devices. They can also schedule software upgrades for a later time. For detailed information, refer to Software Image Management.

Cisco Catalyst SD-WAN Manager allows administrators to centrally upgrade software on Catalyst SD-WAN edge devices in the overlay network and reboot them with the new software. Administrators can perform upgrades on a single device or multiple devices simultaneously. SD-WAN Manager also provides dedicated workflows to upgrade SD-WAN Controller and SD-WAN Validator instances. For detailed information, refer to SD-WAN Software Image Management.

Security solution architecture

Organizations can address security challenges by implementing comprehensive measures such as robust encryption protocols, regular security audits, and proactive threat monitoring to protect against cyber threats and data breaches.

This solution combines built-in security features with the integration of Cisco ISE and Cisco Catalyst Center to deliver highly secure and segmented systems.

Cisco ISE gathers real-time contextual information from networks, users, and devices to support Cisco Catalyst Assurance. This integration simplifies the advanced security requirements of retail organizations that need to prevent fraud and protect confidential data. It streamlines network access provisioning, accelerates security operations, and consistently enforces security policies across the entire network.

Cisco Group-Based Policy (GBP) and identity-based access control features, including IEEE 802.1X/MAC Authentication Bypass, site-level MACsec encryption, and FQDN-based certificates, help retail organizations meet their specific security needs.

Retail organizations face strict security and compliance requirements. Cisco Catalyst SD-WAN overlay architecture meets these needs by delivering comprehensive security capabilities, including robust segmentation, strong encryption, zero trust security, advanced threat protection, continuous monitoring and management, compliance and audit support, and seamless integration with existing security infrastructure. By adopting these security measures, retail organizations can build a secure, resilient, and compliant network environment that protects sensitive data, maintains customer and stakeholder trust, and supports their overall business objectives.

Cisco Catalyst SD-WAN delivers security measures at every level:

Control plane

Cisco Catalyst SD-WAN fabric applies a zero-trust security model to its control plane, authenticating and authorizing all fabric elements before granting them access to the network. This model uses digital certificates to establish the identity of each fabric element during authentication. These certificates create secure TLS or DTLS control channels between controllers and between WAN Edge routers and their respective controllers. TLS and DTLS encrypt all control traffic over these connections using the Advanced Encryption Standard (AES-256) algorithm. AES-256-GCM also provides integrity verification, ensuring that no one tampers with the traffic. WAN Edge devices must appear on an authorization list before the network admits them.

Data plane

Cisco Catalyst SD-WAN overlay architecture secures the data plane by enforcing authentication through a key exchange model and an enhanced version of the Encapsulating Security Payload (ESP) protocol. This enhanced ESP version also protects data packet payloads by encrypting them using the AES-GCM-256 cipher.

Management plane

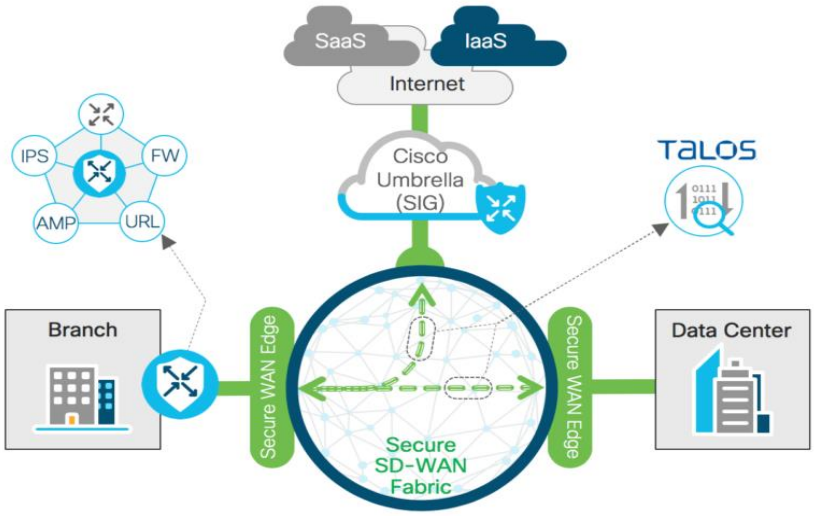
Cisco Catalyst SD-WAN overlay architecture secures the management plane through Role-Based Access Control (RBAC) and Access Control Lists (ACLs) that restrict which users and devices can access SD-WAN Manager based on their source IP addresses.

Cisco Catalyst SD-WAN Manager delivers a comprehensive security framework tailored to the needs of retail organizations. It combines strong encryption, multi-factor authentication, role-based access control,

and integration with external identity provider (IDP) solutions to keep the management plane secure and resilient. These capabilities help retail organizations protect sensitive data, meet regulatory compliance requirements, and maintain high levels of network performance and reliability. By using Cisco Catalyst SD-WAN Manager, retail customers can manage their networks with confidence, knowing they have a robust security foundation supporting them.

Branch users and devices

Cisco Catalyst SD-WAN overlay architecture protects branch users and devices against threats such as DDoS attacks, unauthorized access, viruses, malware, and ransomware. Cisco SD-WAN branch routers include embedded security features such as Zone-Based Firewall, IPS/IDS, URL Filtering, Advanced Malware Protection (AMP), SSL/TLS Proxy, and DNS/Web-Layer Security with Umbrella Integration to defend against these threats.



For detailed information on Catalyst SD-WAN security, refer to this link.

Firewall integration

Firewall peers commonly support internet access, access to data center prefixes, WAN connectivity, and Inter-VN communication. In most deployments, network administrators place endpoints, users, or devices that need to communicate directly with each other in the same overlay virtual network. Some networks require VN-to-VN communication, though this need arises less frequently. Companies typically encounter VN-to-VN requirements during mergers, or within corporate, government, or similar multi-tenant environments where each agency, tenant, or division must maintain its own VN space.

A firewall performs stateful inspection for inter-VN communication and delivers Intrusion Prevention System (IPS) capabilities, advanced malware protection (AMP), granular Application Visibility and Control (AVC), and even URL filtering. Firewalls such as Cisco ASA and Cisco Firepower Threat Defense (FTD) also generate rich reports detailing traffic source, destination, usernames, groups, and firewall actions, and they reliably log every permit and drop.

AI endpoint analytics

Cisco AI Endpoint Analytics, our next-generation artificial intelligence endpoint visibility solution, gathers deeper context from your network and IT ecosystem to make all endpoints visible and searchable. It detects and reduces the number of unknown endpoints in your enterprise through these techniques:

- Deep packet inspection (DPI) gathers deeper endpoint context by scanning and interpreting the applications and communication protocols of IT, Building Automation, and Healthcare endpoints.
- Machine learning (ML) automatically groups endpoints that share common attributes and helps IT administrators label them. The solution then anonymously shares these unique labels with other organizations as suggestions, wherever similar groups of unknown endpoints appear. This approach reduces unknown endpoints and groups them under newer labels.
- Integrations with Cisco and third-party products supply additional network and non-network context, which the solution uses to profile endpoints.

In summary, Cisco AI Endpoint Analytics reduces or eliminates the first hurdle many of our customers face when implementing security policies: achieving high-fidelity endpoint visibility. Cisco offers this solution as a new application in Cisco Catalyst Center Release 2.1.2.x and higher. Customers who subscribe at the Cisco Catalyst Advantage level or higher gain access to Cisco AI Endpoint Analytics. This short technology primer examines Cisco AI Endpoint Analytics and explains how Cisco customers benefit from it.

AI Endpoint Analytics Catalyst Center Guide

Cisco Secure Network Analytics service

The Cisco Secure Network Analytics service on Catalyst Center, working alongside Cisco Secure Network Analytics, monitors all network traffic in real time. The service automatically provisions network elements based on best practices, so they send data to Cisco Secure Network Analytics, which expands your visibility and strengthens your malware detection capabilities.

For more information about how the Cisco Secure Network Analytics service integrates with Cisco Catalyst Center, refer to the Cisco AI Endpoint Analytics: A New Path Forward White Paper.

End-to-end encryption

Retail customers need to encrypt the data traversing their networks, and certain deployments must meet privacy, data confidentiality, or regulatory requirements. Retail organizations sometimes demand Layer 2 encryption within the corporate network and require Layer 3 encryption across the WAN. MACsec delivers encryption on the MAC layer.

Network segmentation

Network segmentation protects critical retail business assets, reduces risk, and helps organizations meet regulatory requirements such as PCI-DSS. In retail environments, segmentation isolates payment systems, corporate users, IoT devices, and guest access while preserving centralized visibility and policy control.

In a non-SD-Access retail architecture, network teams implement segmentation through VPNs and Virtual Routing and Forwarding (VRF) instances on Cisco Catalyst SD-WAN routers, combined with firewall policies and centralized orchestration. Cisco Catalyst Center and Cisco Catalyst SD-WAN management platforms deliver consistent configuration, visibility, and policy enforcement across all retail locations.

Historically, network engineers achieved segmentation by dividing flat networks into smaller broadcast domains using VLANs. As retail networks expanded geographically, VLAN-based segmentation became difficult to scale and manage across distributed sites.

To overcome this challenge, modern retail networks widely adopt Layer 3 segmentation using VRFs and VPNs. Each VPN or VRF maintains its own routing and forwarding tables, which inherently isolate traffic domains. Firewall policies and security inspection tightly control communication between segments, permitting only explicitly authorized traffic.

Macro segmentation

Macro segmentation offers a common and effective approach for retail deployments, where SD-WAN VPNs mapped to VRFs isolate different classes of users and devices. This model strongly separates traffic while supporting centralized management and scalable deployment across thousands of stores.

In retail environments, macro segmentation typically isolates endpoints and services based on business function. Centralized SD-WAN and Catalyst Center workflows consistently deploy these segments across branch and data center sites.

Typical retail segmentation model

A retail deployment may define multiple VPNs/VRFs to enforce strict traffic separation, including:

- **Employee VPN**

  Serves internal corporate users and grants access to business applications.

- **POS VPN**

  Supports point-of-sale systems and payment devices that handle retail transactions, helping the organization meet PCI-DSS compliance.

- **Monitoring VPN**

  Carries logging, telemetry, and in-band management traffic such as syslog, SNMP, and monitoring tool data.

- **Guest VPN**

  Provides isolated internet-only access for customer guest Wi-Fi, while firewalls or cloud security services securely inspect and route the traffic.

- **Infrastructure VPN**

  Connects network infrastructure components such as access points, switches, and management interfaces, enabling secure device communication and control.

By default, these VPNs remain strictly separated. Centralized security and firewall policies explicitly control any required inter-VPN communication.

Benefits of VPN-based segmentation for retail

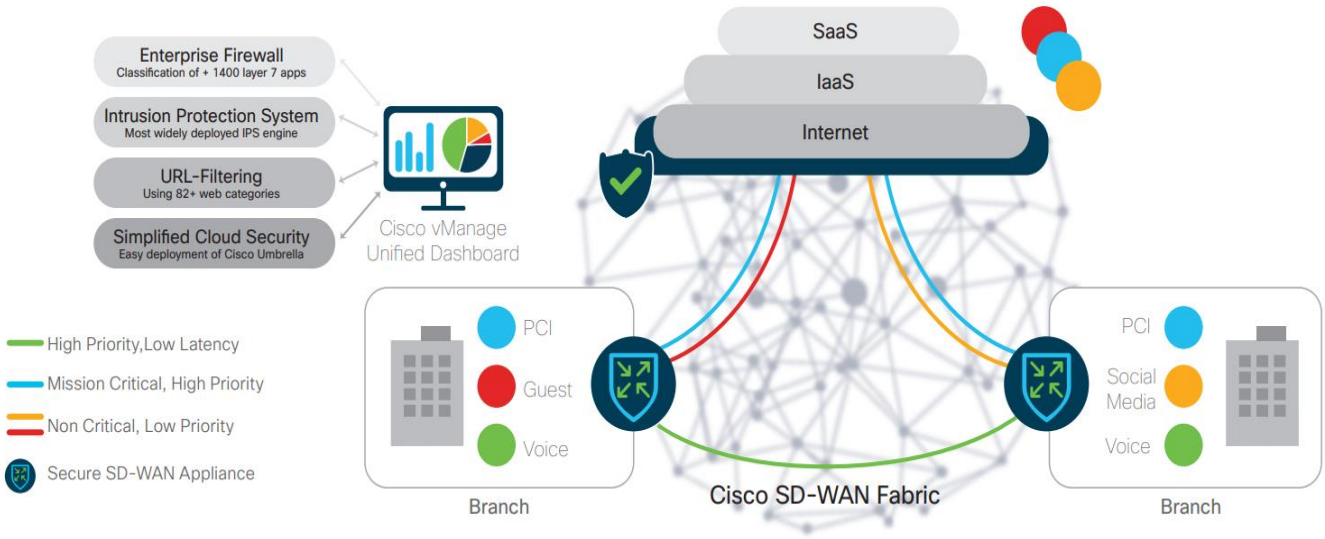
Strong isolation of sensitive payment and business traffic

- Simplified, scalable segmentation across thousands of stores
- Centralized policy enforcement and visibility
- Alignment with regulatory and compliance requirements
- Reduced operational complexity compared to site-specific VLAN designs

This segmentation approach enables retail organizations to maintain a secure, compliant, and scalable network architecture while supporting evolving store technologies and digital experiences.

In the Cisco Catalyst SD-WAN overlay network, VRFs divide the network into different segments. The router performs segmentation at its edges and carries the segmentation information in the packets in the form of an identifier. A separate routing table holds all prefixes belonging to a single VRF. This provides Layer 3 isolation required for the various segments in the network. In addition, the Cisco Catalyst SD-WAN Controller maintains the VRF context of each prefix. Separate routing tables provide isolation on a single node. Cisco Catalyst SDWAN allows application of granular policies on a per segment (VRF) basis – this includes Security, QoS, App Aware Routing, Topology (Hub/Spoke, Full Mesh, Partial Mesh and so on).

Detailed information on Catalyst SD-WAN Segmentation is available here.



Cisco Catalyst SD-WAN Manager provides network administrators with tools to implement and manage network segmentation. Cisco Catalyst SD-WAN Manager uses several features and techniques to achieve segmentation.

Security policies for firewall integration

Implement security policies to control traffic within segments. Use firewall rules, access control lists (ACLs), and other security measures to regulate traffic flow between segments.

Third party integration – Forescout with ISE

Integrating Cisco ISE with Forescout enhances network security by combining identity-based access control with comprehensive device visibility and management. This integration lets organizations enforce policies more effectively across their network infrastructure, strengthening both control and security posture.

- **Define Groups**: Use Cisco Catalyst Center to create logical groups for protected applications/services and endpoints based on their access requirements.
- **Traffic Observation**: Catalyst Center observes traffic patterns between these groups, giving you visibility into communication flows for effective policy management.
- **Leverage ISE Infrastructure**: Integrate with Cisco ISE to use its geo-resilient deployment capabilities, ensuring continuous service availability across locations.
- **SGT Data Sharing**: Cisco ISE shares Security Group Tag (SGT) data through pxGrid, enabling seamless integration with security applications and optimizing policy enforcement.
- **Optimized Policy Management**: Together, Catalyst Center and ISE deliver automation and identity-driven policies, letting you adjust policies dynamically based on real-time context such as user identity and device type.

This integrated approach boosts security and operational efficiency by leveraging Cisco's network and security infrastructure to manage policies comprehensively and maintain traffic visibility.

Forescout's pxGrid Plugin integrates with your existing Cisco ISE (Identity Services Engine) deployments, so you can benefit from Forescout visibility and assessment for policy decisions while continuing to use ISE as an enforcement point. The pxGrid Plugin enables Forescout Platform policies to detect ISE-related properties on endpoints and to apply Cisco ISE Adaptive Network Control (ANC) policies, including policies that assign Security Groups to devices.

Cisco also calls this plugin the Forescout Cisco pxGrid Plugin.

To use the plugin effectively, you should understand Cisco ISE concepts, functionality, and terminology, and you should know how Forescout Platform policies and other basic features work.

The plugin uses certificates to communicate securely with Cisco ISE.

A Forescout Platform policy or manual action instructs ISE to apply an ANC (Adaptive Network Control) policy to devices that the operator selects or that meet Forescout Platform policy conditions.

ISE then applies a Security Group to the devices that match the ANC policy.

You configure Cisco switches to allow or deny resource access for specific Security Group Tags (SGTs).

For more information on the pxGrid plugin for Cisco ISE, refer to:

https://docs.forescout.com/bundle/pxgrid-1-2-2-h/page/c-about-the-pxgrid-plugin.html

Configuring Cisco ISE for the pxGrid plugin can be done from the Cisco ISE UI.

https://docs.forescout.com/bundle/pxgrid-1-2-2-h/page/c-configure-cisco-ise-for-the-plugin.html#t_pxgrid_12_h_configure_cisco_ise_for_the_pxgrid_plugin

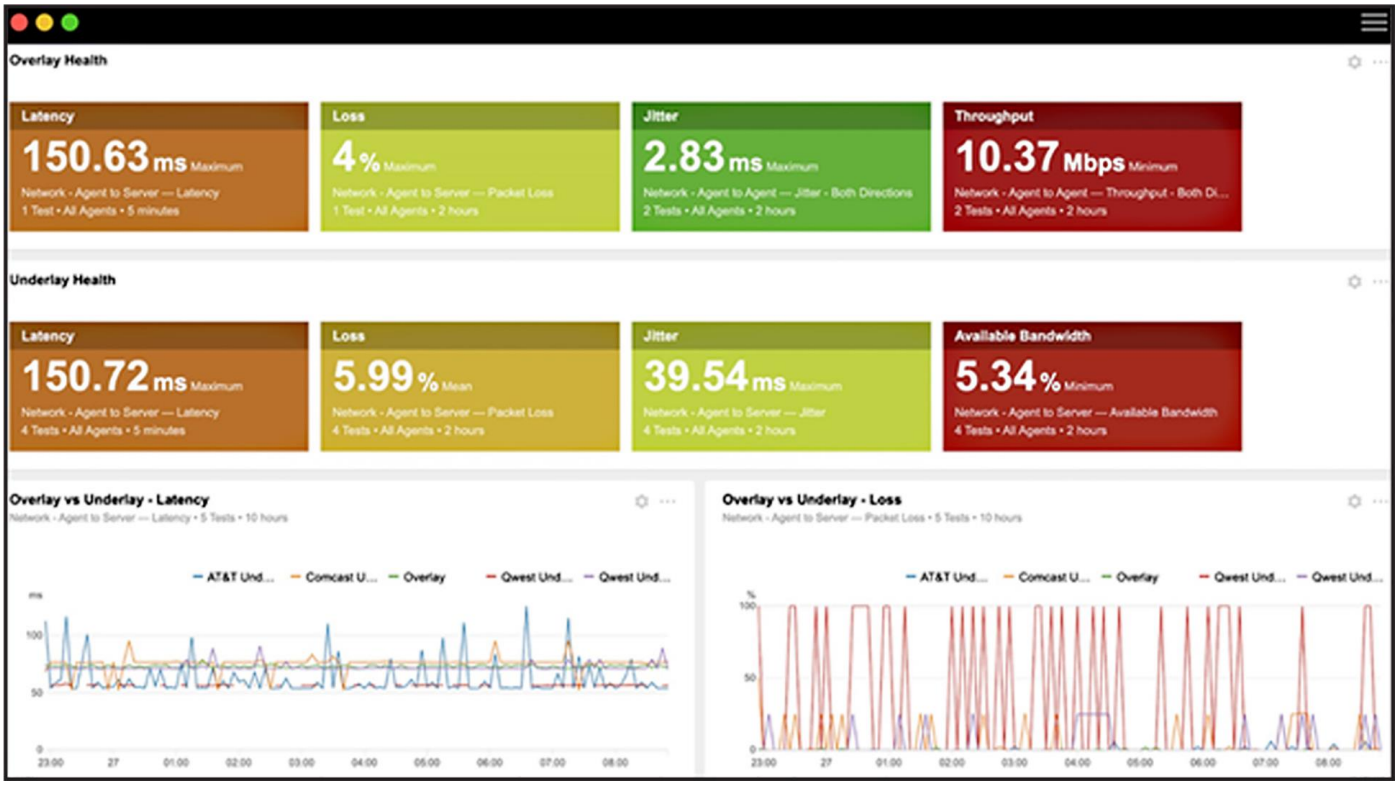
Assurance and user experience monitoring

Assurance and Visibility

Cisco Catalyst SD-WAN overlay architecture offers a unified interface that combines assurance and management capabilities, giving customers a comprehensive, near real-time view of network and application health, configurations, and security status. The unified dashboard streamlines administrative tasks, reduces operational complexity, and strengthens network oversight and governance for our customers. By leveraging Cisco Catalyst SD-WAN Analytics, customers synthesize extensive telemetry data, blending application performance insights with network conditions in an intuitive, simplified dashboard. This advanced analytics capability not only improves network visibility but also establishes historical benchmarks, helping our customers quickly pinpoint the root cause of any issue. As a result, NetOps and SecOps teams gain actionable intelligence, full-context alerts, and detailed security insights that enable them to safeguard their networks against evolving cyber threats.

Integrating Cisco Catalyst SD-WAN overlay architecture with ThousandEyes brings end-to-end visibility into application delivery and network performance beyond traditional enterprise network boundaries. This integration delivers the only SD-WAN solution with turnkey ThousandEyes vantage points, providing an optimal application experience over any network. Enterprises and other organizations can deploy ThousandEyes agents faster through Catalyst SD-WAN Manager integration, quickly pinpoint the source of issues, reach resolution faster, and manage the performance of what matters most.

For more information, refer to *Cisco Catalyst SD-WAN Assurance and Visibility*.

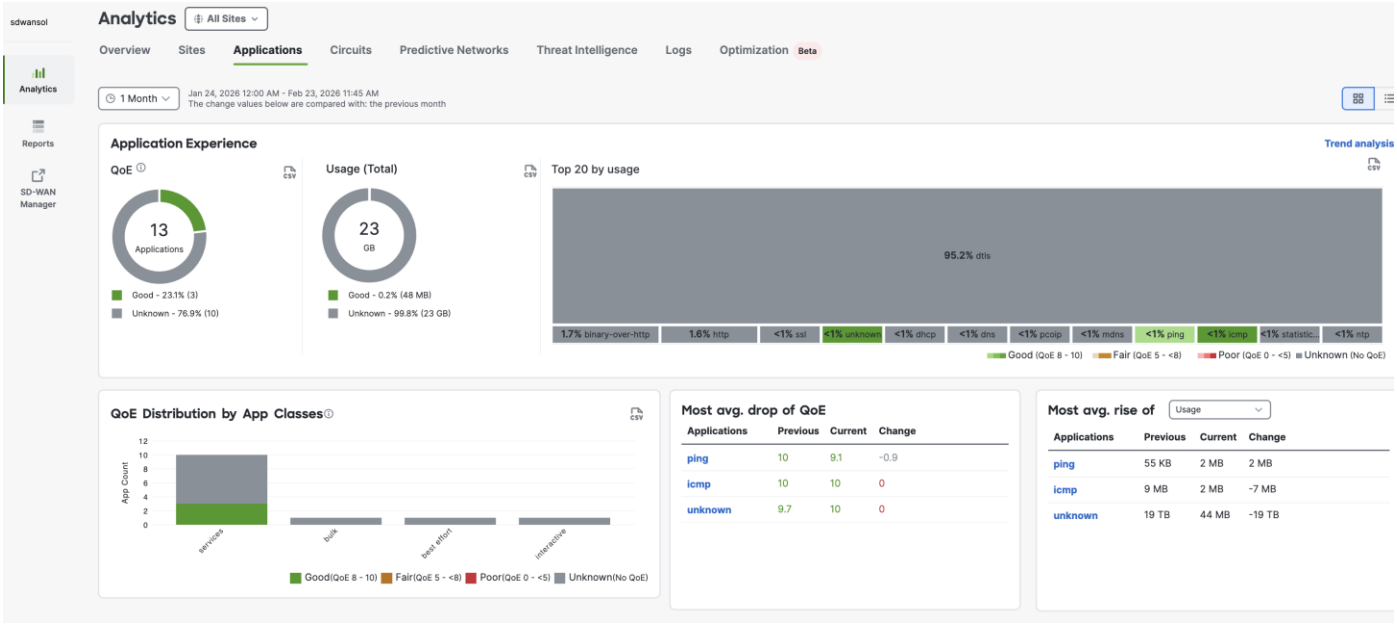


Cisco Catalyst Center manages your network by automating network devices and services, and it also delivers network assurance and analytics capabilities. Cisco Catalyst Center collects telemetry from network devices, Cisco ISE, users/endpoints, applications, and other integrations across the network.

Cisco Catalyst Center Network Analytics correlates data from various sources to help administrators and operators gain comprehensive network insight into:

- **Device 360/client 360**: View device or client connectivity, including topology, throughput, and latency across different times and applications.
- **Network time travel**: Go back in time to see what caused a network issue.
- **Application experience**: Gain comprehensive visibility and performance control over the applications critical to your core business on a per-user basis.
- **Network analytics**: Receive recommended corrective actions for issues the system finds in the network. These actions can include guided remediation, where the engine provides the steps a network administrator performs.

Cisco Catalyst Center Assurance is explained in detail in *Cisco Catalyst Center Assurance: Unlocking the Power of Data*.



ThousandEyes integration

Retail organizations depend heavily on cloud and SaaS applications such as POS backends, inventory systems, loyalty platforms, and collaboration tools. To ensure consistent application performance across thousands of geographically distributed stores, these organizations need deep visibility that extends beyond the enterprise network into the Internet, ISP, and SaaS provider domains.

ThousandEyes enables IT organizations to troubleshoot application and user experience issues by giving them end-to-end, hop-by-hop visibility across the enterprise network, service provider networks, and public cloud or SaaS environments. This visibility matters especially in retail, where a localized ISP issue or SaaS degradation can directly disrupt store operations and customer experience.

End-to-end visibility across campus, WAN, and internet

Integrating Cisco Catalyst Center, Cisco Catalyst SD-WAN, and ThousandEyes creates a comprehensive observability framework for retail networks:

- **Inside the store and campus**

  Cisco Catalyst Center provides assurance for wired and wireless infrastructure, endpoint health, and user experience within the store environment.

- **Across the WAN**

Cisco Catalyst SD-WAN delivers application-aware routing, path optimization, and telemetry across MPLS, broadband, and LTE or 5G transport links.

- **Across the internet and SaaS providers**

  ThousandEyes extends visibility beyond the enterprise edge, offering hop-by-hop path analysis across ISPs, cloud networks, and SaaS providers.

This combined approach helps IT teams rapidly identify the source of an issue, including:

- Store LAN or Wi-Fi conditions
- WAN transport degradation
- ISP routing problems
- Cloud or SaaS service outages

ThousandEyes integration with Cisco Catalyst Center

Cisco Catalyst Center enables on-premises ThousandEyes visibility within retail stores and campus environments by supporting the native deployment of ThousandEyes Enterprise Agents on Cisco Catalyst 9000 switches.

Cisco Catalyst Center uses the App Hosting framework on Cisco Catalyst 9000 platforms to centrally deploy, manage, and monitor ThousandEyes Enterprise Agents as containerized applications. This approach eliminates the need for dedicated appliances or external probes at retail locations and allows IT teams to extend application and network visibility directly from the access and distribution layers of the network.

Administrators can use the guided App Hosting workflows in Cisco Catalyst Center to:

- onboard supported Catalyst 9000 switches for application hosting
- allocate CPU, memory, and storage resources for the ThousandEyes agent
- deploy and activate ThousandEyes Enterprise Agents at scale, and

- monitor application health and lifecycle centrally from Catalyst Center.

This deployment model simplifies operations in retail environments where stores often operate with minimal local IT support and require standardized, repeatable deployment methods across hundreds or thousands of locations.

Enhanced retail visibility from the network edge:

By running ThousandEyes Enterprise Agents directly on Catalyst 9000 switches, retail organizations gain first-hop visibility into application performance and user experience from the exact point where users, POS systems, and IoT devices connect to the network.

This deployment enables you to:

- monitor SaaS applications used in stores in real time, such as point-of-sale (POS), inventory, loyalty, and payment systems
- detect last-mile ISP and broadband issues that impact store operations
- correlate wired and wireless network health with end-to-end application performance, and
- isolate root causes faster across campus, WAN, ISP, and cloud domains.

Cisco Catalyst Center correlates assurance data from the LAN and WLAN with ThousandEyes path and application telemetry. This integration provides a single operational view that helps IT teams quickly determine whether issues originate inside the store, across the WAN, or beyond the enterprise boundary.

For additional details, refer to the *Cisco ThousandEyes Enterprise Agent Deployment Guide on Catalyst 9000 Switching Platforms*.

ThousandEyes integration with Cisco Catalyst SD-WAN overlay architecture

ThousandEyes helps IT organizations troubleshoot application and user experience issues by providing hop-by-hop visibility across enterprise, ISP, and SaaS provider networks. When you combine ThousandEyes with the network and user health insights from Cisco Catalyst Center, you gain access to comprehensive diagnostics. This integration helps you quickly understand the impact and root cause of application performance issues. You can use the guided workflows in Cisco Catalyst Center to deploy ThousandEyes agents quickly and at scale.

For more information, refer to the *Cisco Catalyst Center and ThousandEyes Integration Guide*.

You can natively deploy the Cisco ThousandEyes Enterprise Agent as a container application on supported Cisco IOS XE Catalyst SD-WAN devices to integrate Cisco Catalyst SD-WAN with Cisco ThousandEyes. You can install and activate the Cisco ThousandEyes Enterprise Agent using Cisco Catalyst SD-WAN Manager. This integration provides granular insights into network and application performance with full hop-by-hop path analysis across the internet and helps you isolate fault domains for faster troubleshooting and resolution.

Refer to the *Cisco Catalyst SD-WAN ThousandEyes Integration Guide* for steps to configure Catalyst SD-WAN edge device integration with Cisco ThousandEyes.

Multicast design for video surveillance and digital signage

Retail environments rely heavily on high-bandwidth media applications, such as IP-based video surveillance and digital signage. Both use cases use one-to-many traffic patterns, which makes multicast a critical design component for efficient network utilization.

Multicast optimizes the delivery of media streams by sending a single copy of traffic across the network and replicating the copy only where needed. This optimization reduces bandwidth consumption compared to traditional unicast delivery, especially in large-scale retail deployments with many endpoints.

Video surveillance

For video surveillance deployments:

IP cameras generate continuous video streams that multiple systems—such as network video recorders (NVRs), monitoring stations, and analytics platforms—receive and process.

The network uses multicast to distribute these streams to multiple receivers without duplicating traffic across the WAN.

The system segments traffic within a dedicated virtual routing and forwarding (VRF) instance, such as an IoT VRF, to ensure isolation and policy control.

Digital signage

For digital signage:

The data center centrally hosts advertisement and promotional content and distributes the content to retail stores.

Multicast streams live or scheduled content to multiple locations simultaneously.

This approach avoids redundant unicast streams and ensures efficient WAN bandwidth utilization.

Multicast architectural considerations

Cisco Catalyst SD-WAN extends multicast capabilities across the WAN to replicate traffic efficiently at branch edges.

The network uses protocols such as Protocol Independent Multicast (PIM) and Internet Group Management Protocol (IGMP) for multicast routing and group membership management.

Policy-based traffic prioritization ensures that media streams do not affect business-critical applications.

Administrators can use multicast group segmentation to deliver region-specific or store-specific content.

This unified multicast design delivers surveillance and digital signage traffic efficiently while maintaining segmentation, performance, and operational simplicity across distributed retail sites.

Operational benefits for retail organizations

Deploying ThousandEyes Enterprise Agents through Cisco Catalyst Center and Cisco Catalyst SD-WAN provides these retail-specific benefits:

- eliminating the need for additional hardware in stores
- enabling centralized, policy-driven deployment at scale
- reducing operational complexity and on-site troubleshooting
- isolating issues faster across access, WAN, and cloud, and

- improving visibility for customer-facing and revenue-critical applications.

A three-node SD-WAN Manager cluster can manage up to 4,000 devices and can tolerate the failure of one node.

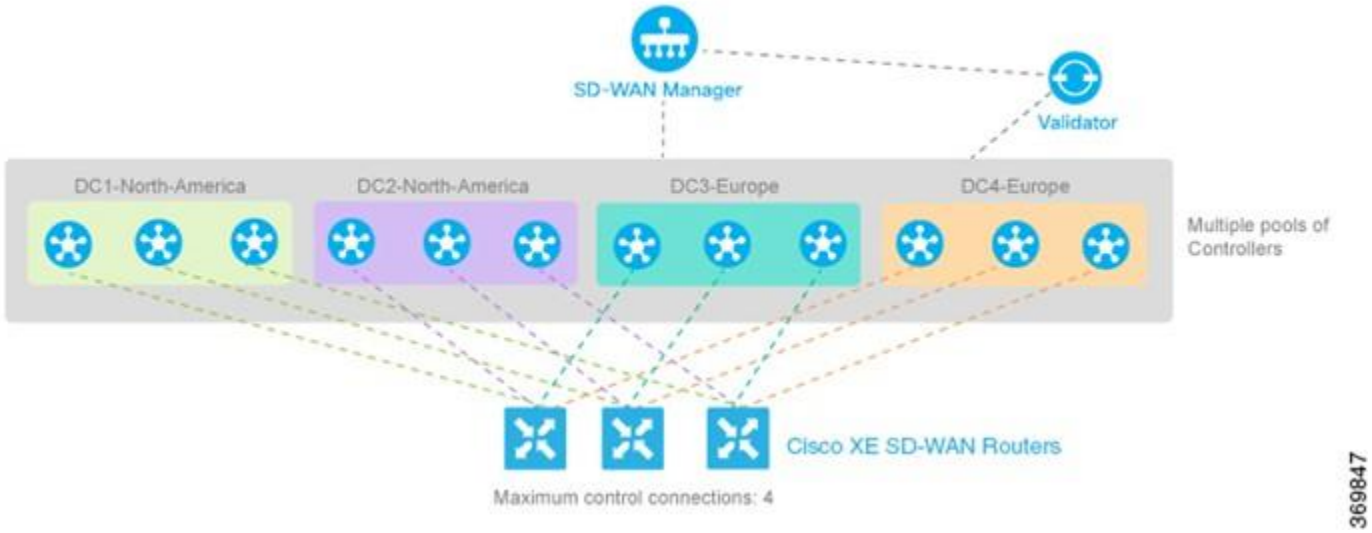
SD-WAN Manager maintains configuration and statistics databases for all routers. The system replicates these databases between the cluster members to ensure fault tolerance. If one of the SD-WAN Manager instances fails, the two remaining instances provide the redundancy you need to continue managing the SD-WAN routers.

The configuration and statistics databases must run on all three SD-WAN Manager instances, but you can separate these databases. For example, in a cluster of six SD-WAN Manager instances, three instances can maintain the configuration database, and the other three instances can maintain the statistics database. Managing statistics when you enable deep packet inspection (DPI) can impose a heavy load on an SD-WAN Manager instance. By using a cluster, you can separate this responsibility from other services.

For more details, refer to the *Cisco Catalyst SD-WAN High Availability Design Guide*.

Multiple data centers

If the preferred data center experiences an outage, Cisco Catalyst SD-WAN automatically redirects traffic to the other data center, ensuring continuous access to applications and data.



Cisco Catalyst Center disaster recovery

Retail organizations have a low tolerance for management, control, or data plane failures. Cisco Catalyst Center supports both intra-cluster and inter-cluster resiliency. The disaster recovery implementation in Cisco Catalyst Center consists of three components: the main site, the recovery site, and the witness site. At any given time, the main and recovery sites operate in either active or standby roles.

The active site manages your network, while the standby site maintains a continuously updated copy of the data and managed services from the active site. If the active site fails, Cisco Catalyst Center automatically initiates a failover to designate the standby site as the new active site.

For more information, refer to the *Cisco Catalyst Center Disaster Recovery Application Guide*.

For more information, refer to the *Cisco Catalyst SD-WAN Disaster Recovery Deployment Guide*.

Resilient network architecture

StackWise Virtual (SVL), like its predecessor Virtual Switching System (VSS), simplifies Layer 2 operations. This technology virtualizes two physical switches into a single logical switch from a control and management plane perspective. SVL eliminates the need for spanning tree, first-hop redundancy protocols, and multiple configuration touchpoints.

Layer 3 routed access moves the Layer 2 and Layer 3 boundary from the distribution layer to the access layer. Shifting this boundary eliminates the need for the distribution and collapsed core layers to service Layer 2 adjacency and Layer 2 redundancy.

While StackWise Virtual simplifies operations for control plane protocols and physical adjacencies, it requires additional protocols to solve Layer 2 challenges. When you use StackWise Virtual in a Layer 3 routed network, you can lose a redundant IGP or EGP control plane instance.

Apart from conventional resiliency methods like stacking and StackWise Virtual, regional hubs and campus headquarters in retail organizations often require protection from building failures. This protection ensures that connectivity to data centers for payment gateways and other critical applications remains available.

High availability

Retail organizations achieve high availability (HA) in Cisco Catalyst SD-WAN deployments through hardware redundancy, comprehensive network design, and software mechanisms that ensure rapid recovery from failures:

- **Comprehensive network design**

  Distribute redundant Cisco Catalyst SD-WAN Validators and Controllers geographically and connect them through different transport networks. Configure local site routers to connect to multiple transport networks.

- **Disaster recovery**

  Deploy Cisco Catalyst SD-WAN Manager—which is stateful and cannot operate in active-active mode—in a primary and secondary model across two data centers. The system replicates data automatically, and you can manually trigger a failover to the secondary cluster. This disaster recovery solution supports various cluster sizes and deployment models.

These elements collectively provide retail organizations with a resilient, scalable, and manageable SD-WAN solution that ensures continuous network service availability and rapid recovery from failures.

Controller redundancy

Cisco Catalyst SD-WAN supports the clustering of SD-WAN Manager instances. You must use a minimum of three nodes to form a cluster. Each node within a cluster shares a configuration and statistics database. A single SD-WAN Manager instance can manage up to 2,000 Cisco Catalyst SD-WAN routers. A three-node SD-WAN Manager cluster can manage up to 4,000 devices and can tolerate the failure of one node.

SD-WAN Manager maintains configuration and statistics databases for all routers. The system replicates the configuration and statistics databases between the cluster members to ensure fault tolerance. If one of the SD-WAN Manager instances fails, the two remaining instances provide the redundancy you need to continue managing the Cisco Catalyst SD-WAN routers.

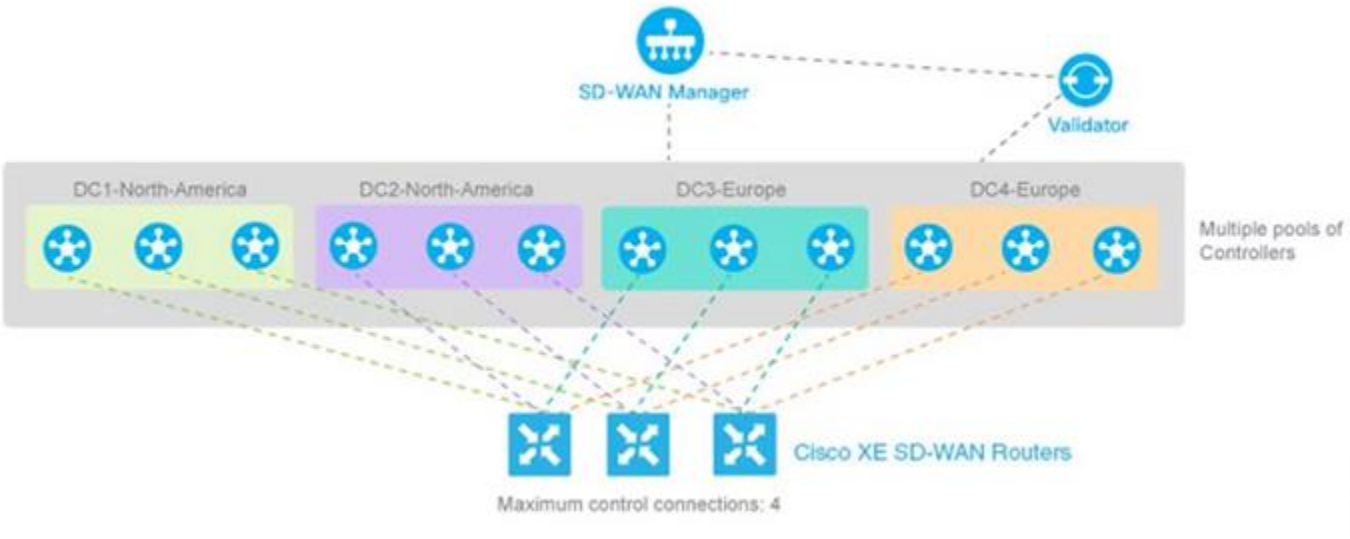
The configuration and statistics databases must run on all three SD-WAN Manager instances, but you can separate them. For example, in a cluster of six SD-WAN Manager instances, three instances can maintain the configuration database, and the other three instances can maintain the statistics database. Managing

statistics when you enable deep packet inspection (DPI) can impose a heavy load on an SD-WAN Manager instance. By using a cluster, you can separate this responsibility from other services.

For details about designing controller redundancy in Cisco Catalyst SD-WAN networks, refer to the *Cisco Catalyst SD-WAN High Availability Design Guide*.

Active-active data centers

If retail organizations have multiple data centers, you can configure Cisco Catalyst SD-WAN edge locations to maintain active-active connections to each data center. In this configuration, the network prefers routes from one data center over the other for data plane traffic during normal conditions. If the preferred data center experiences an outage, Cisco Catalyst SD-WAN automatically redirects traffic to the other data center, which ensures continuous access to applications and data.



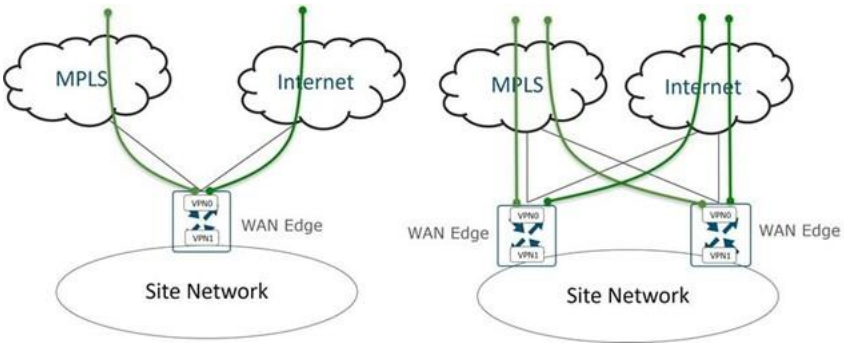
WAN redundancy

Multiple connections: Branches have multiple WAN connections, which ensures continuous connectivity even if one or more links fail. Cisco Catalyst SD-WAN dynamically routes traffic based on link performance and availability.

Edge device redundancy

Dual edge devices: As an option, some branches can deploy dual WAN Edge devices in an active-active or active-standby configuration to enhance local redundancy. TLOC extensions extend the WAN circuits to peer routers at the same site, which offers transport-level redundancy on both WAN Edge routers.

Transport options from WAN Edge in Cisco Catalyst SD-WAN:



Catalyst Center high availability

The high availability (HA) framework in Cisco Catalyst Center reduces downtime from failures and makes your network more resilient. The HA framework achieves this by synchronizing changes across your cluster nodes in near real-time, which provides redundancy for your network. Cisco Catalyst Center supports a three-node cluster configuration to provide both software and hardware HA.

Refer to the *Cisco Catalyst Center High Availability Guide* for configuration steps.

Cisco ISE high availability

A standalone deployment uses a single Cisco Identity Services Engine (ISE) node. This node runs the Administration, Policy Service, and Monitoring personas. A distributed deployment uses more than one Cisco ISE node. To support failover and improve performance, you can deploy multiple Cisco ISE nodes in a distributed architecture. In a distributed deployment, the system centralizes administration and monitoring activities and distributes processing across the Policy Service nodes.

Refer to the *Cisco Identity Services Engine High Availability Configuration Guide* for setup instructions.

Cisco wireless LAN controller redundancy

The high availability stateful switchover (SSO) capability on the wireless controller enables the access point (AP) to establish a CAPWAP tunnel with the active wireless controller. The active wireless controller then shares a mirror copy of the AP and client database with the standby wireless controller.

During a switchover (when the active controller fails and the standby controller takes control), joined APs do not enter the discovery state, and clients do not disconnect. The AP maintains only one CAPWAP tunnel at a time with an active wireless controller.

The system centralizes and synchronizes all control plane activities between the active and standby units. The active controller centrally manages all control and management communication. The standby unit transparently switches network control data traffic to the active unit for centralized processing.

Refer to the *Cisco Catalyst 9800 Series Wireless LAN Controller High Availability Guide* for configuration steps.

Large-scale multisite deployments and centralized policy management

A large-scale, multisite deployment implements a system, application, or infrastructure across multiple locations. Organizations adopt this approach to support widespread operations across various regions. This design provides the flexibility, resilience, and scalability you need to meet modern business requirements. Centralizing policy management helps you achieve consistent, end-to-end policy control.

Multiple Cisco Catalyst Center clusters to a single Cisco ISE cluster

Global deployments often require you to deploy multiple Cisco Catalyst Center clusters to accommodate scale, network latency, and compliance requirements. You can integrate multiple Cisco Catalyst Center

clusters with a single Cisco ISE deployment to centralize and standardize authentication, authorization, and security group policies across your enterprise.

Large retail organizations can benefit from integrating multiple Cisco Catalyst Center clusters with a single Cisco ISE deployment. Cisco Catalyst Center supports multiple clusters per Cisco ISE deployment to maximize Cisco ISE utilization and provide a centralized policy management plane.

For more information, refer to Support for Multiple Cisco Catalyst Center Clusters with a Single Cisco ISE System.

Refer to the *Cisco Catalyst Center and Cisco ISE Integration Guide* for detailed deployment steps.

Centralized policy management

Retail networks face rapid growth in endpoints, including POS devices, inventory scanners, IoT sensors, and customer devices that connect to guest Wi-Fi. Managing security, access, and traffic policies consistently across thousands of distributed stores is a significant challenge.

Cisco Catalyst Center, integrated with Cisco ISE and Cisco Catalyst SD-WAN, provides a centralized framework to define, propagate, and enforce policies consistently across your network.

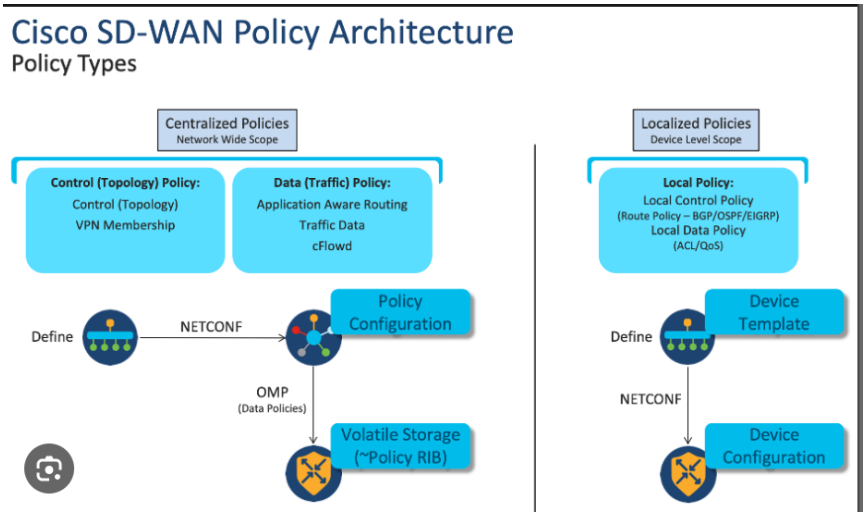
You can use this integration to:

- securely onboard retail endpoints, including BYOD devices, IoT sensors, and POS systems, using Cisco ISE and Cisco Catalyst Center to ensure they meet security posture requirements and receive appropriate access permissions
- assign security tags or policy identifiers to endpoints to enforce traffic segmentation, QoS, firewall rules, and access controls from end to end
- author policies once and replicate them across multiple clusters to ensure uniform security and operational standards across all retail locations
- monitor group and device interactions using traffic and security analytics to identify unauthorized or anomalous behavior, and
- define and enforce application-aware routing, VPN segmentation, QoS, and security policies across all branch and WAN sites using Cisco Catalyst SD-WAN Manager.

Policy examples for retail networks

You can implement these policy examples to secure your retail network:

- isolate POS traffic from guest Wi-Fi and corporate applications using VPN segmentation
- prioritize inventory management and IoT traffic using QoS policies
- restrict guest Wi-Fi traffic to internet access and inspect traffic using branch firewalls
- enforce PCI-DSS and other compliance standards for payment and sensitive customer data, and
- centralize logging and monitoring for audits, compliance, and troubleshooting.



Control policies

Cisco Catalyst SD-WAN control policies define how the network routes and manages traffic. These policies enable network administrators to optimize performance, enforce security, and ensure compliance with organizational requirements. Network administrators can implement these Cisco Catalyst SD-WAN control policies to define how sites connect with each other:

- traffic engineering policies
- VPN membership policies
- topology policies, and
- traffic filtering policies.

You can use control policies to implement hub-and-spoke, full-mesh, and partial or regional mesh topologies. For more details, refer to the *Cisco Catalyst SD-WAN Control Policy Configuration Guide*.

Traffic steering

You can use policies to define how the network steers traffic. You can create policies that direct specific types of traffic over specific links or paths. For example, you can send critical business application traffic over a high-performance link and direct guest traffic over a lower-cost link.

Traffic steering in Cisco Catalyst SD-WAN prioritizes traffic and routes packets through the most appropriate paths based on performance, cost, and security requirements. You can implement traffic steering for retail customers using these Cisco Catalyst SD-WAN features:

- application-aware routing
- policy-based routing
- dynamic path selection
- quality of service (QoS), and
- service level agreements (SLAs).

Application-aware routing

The Application-Aware Routing (AAR) feature in Cisco Catalyst SD-WAN helps retail organizations ensure that critical applications receive the necessary performance, security, and reliability. You can use these features to implement AAR for retail customers:

- application identification
- performance monitoring and SLAs
- traffic policies and path selection
- QoS and prioritization, and
- continuous monitoring and adjustments.

These policies enable WAN Edge devices to dynamically select the best path for application traffic based on application performance requirements:

- SLA compliance: Ensure that applications meet predefined performance metrics.
- Application prioritization: Prioritize traffic based on application type, such as voice over IP (VoIP) or video conferencing.

For more information, refer to the *Cisco Catalyst SD-WAN Application-Aware Routing Deployment Guide*.

When you enable Enhanced AAR on WAN Edge devices, you accelerate the detection of tunnel performance issues.

Benefits of enhanced AAR

- **Improved PfR metrics measurements**: The system introduces inline data to measure loss, latency, and jitter more accurately. Inline data refers to traffic that Cisco IOS XE Catalyst SD-WAN devices process and inspect directly at the network edge. Instead of routing all traffic to a central location for analysis and security checks, inline data enables real-time inspection and decision-making at the network edge.
- **Fast route detection and SLA enforcement**: The system reduces the poll interval to a minimum of 10 seconds. This reduction enables Cisco IOS XE Catalyst SD-WAN devices to quickly detect slow circuit degradation. If a circuit fails to meet the SLA threshold, the system swiftly switches tunnels out of SLA forwarding to maintain network performance. SLA forwarding enables the Cisco Catalyst SD-WAN solution to dynamically route network traffic based on predefined performance criteria.
- **Faster SLA switchover times**
- **SLA dampening**: The system uses dampening to ensure a smooth transition back to SLA forwarding. Before the system applies SLA forwarding again, the tunnel undergoes dampening to prevent disruptions and instabilities, which minimizes negative effects on network performance.
- **Enhanced measurements**: The system uses improved methods to measure loss, latency, and jitter.

For more information, refer to the *Cisco Catalyst SD-WAN Application-Aware Routing Deployment Guide*.

Custom applications in retail networks

Many retail organizations use internal or proprietary applications that require specific handling. You can classify these applications as custom applications on WAN Edge devices and apply policies to provide preferential treatment. Cisco Catalyst SD-WAN uses Software-Defined Application Visibility and Control (SD-AVC) capabilities to identify these applications. For more information, refer to the *Cisco Catalyst SD-WAN Custom Application Guide*.

Security policies for custom applications

You can create policies to enforce security rules and restrictions. These policies implement firewall rules, access control lists, or VPN policies to protect the network and sensitive data.

Isolation of guest users

Retail networks often serve many guest devices in stores, such as customer smartphones that connect to Wi-Fi. To protect the corporate network and sensitive data, you must securely isolate and manage guest traffic across all stores.

In a Cisco Catalyst SD-WAN retail network with wireless managed by Cisco Catalyst Center, you can centrally isolate and anchor guest traffic to ensure secure and consistent delivery:

- **Guest network segmentation**: The system places guest traffic from all store locations into a dedicated VPN or overlay network on WAN Edge routers, which logically separates guest traffic from corporate, POS, and inventory traffic.
- **Traffic inspection at the edge**: The network directs all guest traffic to a firewall in the branch DMZ, which inspects and filters the traffic before it reaches the internet. This firewall inspection prevents unauthorized access to sensitive retail systems.
- **Guest anchor wireless controllers**: To simplify deployment across multiple stores, guest Wi-Fi can use a centralized anchor wireless controller (WLC). Access points (APs) in each store tunnel guest traffic back to the anchor WLC at a regional or centralized site, which enables:
  - consistent guest subnet usage across all stores
  - centralized policy enforcement for guest access, and
  - simplified IP management without requiring per-store subnets.
- **Centralized management with Cisco Catalyst Center**: Cisco Catalyst Center automates provisioning and policy propagation for guest networks and anchored WLCs, which enables new store locations to adopt the same guest network configuration with minimal manual effort.
- **Scalable multisite deployment**: The network securely aggregates and tunnels guest traffic from multiple retail sites to the anchor WLC, which maintains isolation and enables centralized monitoring and analytics.
- **Reliable end-user experience**: Despite strict isolation, guests receive reliable, high-speed Wi-Fi across all stores, which supports customer engagement applications and in-store digital experiences.

Benefits for retail environments

Benefits for retail environments include:

- protecting POS, inventory, and corporate networks from guest devices
- centralizing guest network management and policy enforcement
- providing a consistent guest experience across all store locations, and

- simplifying multisite deployments using a guest anchor WLC and SD-WAN automation.

From a Cisco ISE perspective, you can use these options to isolate guest environments for retail customers:

- a separate Policy Service Node (PSN) hosted in the DMZ for guest users, or
- a dedicated PSN for guest users.

By implementing separate authentication and authorization for guest users, you fully isolate the guest network from the control plane, data plane, and policy plane. This isolation secures the guest network from other retail users, devices, and resources.

Service chaining

Cisco Catalyst SD-WAN service chaining in the retail vertical automatically inserts network and security services into the data traffic path. This capability supports use cases such as:

- redirecting specific traffic flows through firewalls, load balancers, WAN optimization appliances, or web proxies to meet security and performance requirements
- ensuring compliance with regulatory standards by directing sensitive traffic, such as PCI-DSS traffic, through centralized or regional security services, and
- automating service insertion with centralized policies and templates to simplify deployment and management compared to traditional WAN environments.

In retail environments, you can use SD-WAN service chaining to secure and optimize traffic between distributed store locations and corporate data centers or cloud services. For example, the network can route traffic from stores through security virtual network functions (VNFs) or physical appliances in a service chain before the traffic reaches applications, which ensures secure and compliant access.

Additionally, Cisco Catalyst SD-WAN in retail environments supports intelligent path selection, automatic traffic steering based on application needs, and local internet breakout for cloud applications, which improves performance and the customer experience. The centralized control policy creates secure IPsec VPN tunnels between headquarters and stores. This configuration enables centralized policy enforcement and allows local breakout for guest Wi-Fi and SaaS access.

Retail enterprises use SD-WAN service chaining and related capabilities to:

- secure and optimize connectivity for point-of-sale (POS) systems and inventory management
- enforce security centrally with flexible traffic routing
- provide resilient connectivity with multipath broadband and cellular backup, and
- simplify VPN deployment and management through cloud orchestration.

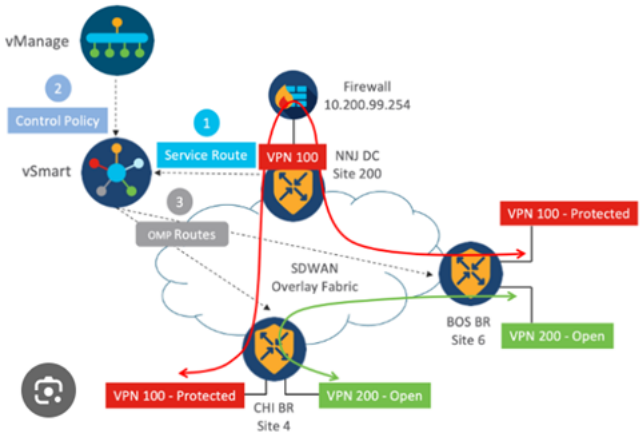
These features collectively enable retail enterprises to deliver secure, high-performance, and compliant network services across distributed store locations with centralized control and automation.

This design enables you to insert services—such as firewalls, intrusion detection systems, or intrusion prevention systems—on demand when traffic flows match specific criteria.

For more details, refer to the *Cisco Catalyst SD-WAN Service Chaining Deployment Guide*.

Refer to the *Cisco Catalyst SD-WAN Service Chaining Configuration Guide* for setup steps.

Service Insertion Example – Firewall Service



Configure NNJ DC to advertise the availability of the Firewall service to the vSmart controller via service VPN feature template.

Build and activate a centralized control policy to insert the Firewall service into traffic path bi-directionally between CHI and BOS sites in VPN 100.

vSmart controller modifies the OMP routes in VPN 100 for CHI and BOS to set the next hop to NNJ TLOC with the Firewall service label before advertises them to CHI and BOS accordingly.

Quality of service

Quality of service (QoS) enables retail organizations to ensure that critical applications—such as point-of-sale (POS) systems, inventory management, and voice over IP (VoIP) services—receive the necessary bandwidth and prioritization. By prioritizing critical applications, you ensure that these services receive the necessary network resources.

Cisco Catalyst SD-WAN enables you to apply granular QoS policies at a per-VPN or segment level, and use advanced adaptive per-tunnel QoS capabilities. You can define QoS policies to prioritize specific types of traffic over others. For example, the network can give higher priority to real-time applications, such as VoIP or video conferencing, to ensure low latency and minimal packet loss. You can use Cisco Catalyst SD-WAN Manager to monitor the QoS for each site.

Refer to the *Cisco Catalyst SD-WAN Quality of Service Configuration Guide* for detailed configuration steps.

Apart from standard QoS tasks—such as traffic classification, marking, policing, queuing, scheduling, and bandwidth allocation—you can use these features to implement advanced QoS for retail organizations using Cisco Catalyst SD-WAN.

Per-tunnel QoS

You can apply per-tunnel QoS only to hub-and-spoke network topologies. Per-tunnel QoS on a hub enables you to shape tunnel traffic to individual spokes. This feature also differentiates individual data flows that traverse the tunnel or the spoke for policing.

Benefits of per-tunnel QoS

- **Session-group configuration**: You can configure a QoS policy based on session groups to regulate traffic from the hub to spokes at a per-spoke level.
- **Overrun prevention**: The hub cannot send excessive traffic to a small spoke and overrun it.
- **Automatic queue setup**: The system automatically sets up the maximum outbound bandwidth and QoS queue when each spoke sends an Overlay Management Protocol (OMP) message to register.
- **Resource protection**: You can limit the amount of outbound hub bandwidth that a greedy spoke can consume to prevent the traffic from monopolizing hub resources and starving other spokes.

- **Multiple policies support**: The system supports multiple policies (MPoL), which enables underlay and TLOC extension traffic to coexist with overlay tunnel traffic.

Refer to the *Cisco Catalyst SD-WAN Per-Tunnel Quality of Service Configuration Guide* for detailed configuration and monitoring steps.

Adaptive QoS

This feature enables WAN interface shapers and per-tunnel shapers at the enterprise edge to adapt to the available WAN bandwidth. This adaptation controls differentiated packet drops at the enterprise edge and reduces or prevents packet drops in the network core.

This capability enables WAN Edge routers to dynamically adjust shaper parameters based on the actual available internet bandwidth in both directions, which the system periodically computes. This configuration allows you to configure a QoS policy on the spoke toward the hub and ensures better control of application performance at the enterprise edge even when bandwidth fluctuates. The feature adapts the aggregate tunnel shape to provide effective bandwidth between the spoke and the hub.

Refer to the *Cisco Catalyst SD-WAN Adaptive Quality of Service Configuration Guide* for detailed configuration and monitoring steps.

Per-VPN QoS

When a WAN Edge device receives traffic belonging to different VPNs from the branch network, you can configure a QoS policy to limit the bandwidth that traffic belonging to each VPN or group of VPNs can use.

Refer to the *Cisco Catalyst SD-WAN Per-VPN Quality of Service Configuration Guide* for detailed configuration and monitoring steps.

Benefits of per-VPN QoS

- T**raffic control**: You can control bandwidth consumption and traffic throughput based on the VPN to which the traffic belongs.
- **Resource allocation**: A greedy VPN cannot use outbound bandwidth beyond the allocated limit, which prevents it from starving other VPNs.
- **Service classification**: You can configure different classes of service for each VPN on a single WAN interface.

High sensitivity to QoS with application policy

Retail organizations use stringent application service level agreements (SLAs) to maintain application availability. A slow or QoS-disparate network can lead to a poor application experience, which can disrupt store operations that are sensitive to delays.

Cisco Catalyst Center includes advancements that help large and global retail organizations manage and scale application policies for deployment. When building the Cisco Non SD-Access fabric, you can deploy a tiered, Cisco-recommended or customized QoS policy to both the wired and wireless infrastructures. This application policy uses the DiffServ model, where the system categorizes applications in application sets and divides them into business-relevance categories based on administrator preference.

The controller-based application recognition feature in Cisco Catalyst Center uses the NBAR2 Deep Packet Inspection (DPI) capabilities that the system uses for endpoint analytics. This capability enables Cisco Catalyst Center to learn applications directly from packets in transit across the network. This integration enables the system to learn applications from the Cisco NBAR2 Cloud, Microsoft Office 365, and Infoblox.

The system can learn the fully qualified domain names (FQDN) and URL information of applications and use this data to update application sets within QoS policies. This capability enables you to immediately deploy these application policies at scale anywhere in the network.

Cisco Catalyst Center also gathers telemetry based on how these application policies operate, which enables administrators to modify and redeploy policies at scale across the network. Viewing application operations helps you understand the user experience and resolve issues before an end user reports them. This method helps you identify the root cause of issues quickly.

Because application QoS policies correctly classify and mark all application traffic, any device can process the traffic appropriately from end to end across the network, the WAN, the cloud, or the data center.

Refer to the *Cisco SD-Access Application Policies Configuration Guide* for detailed steps.

Application visibility and control features

The system uses deep packet inspection (DPI) and Network-Based Application Recognition (NBAR) to identify and prioritize traffic based on specific applications, including custom applications in retail networks.

Cisco Catalyst SD-WAN provides application visibility and control (AVC) capabilities for retail organizations. These features enable retail customers to monitor, manage, and optimize their network traffic effectively, ensuring that critical applications receive the necessary resources.

You can implement and use AVC in Cisco Catalyst SD-WAN using these features:

- application recognition
- performance monitoring
- traffic analytics
- policy enforcement, and
- real-time reporting and alerts.

Integrated security and cloud services

To protect and optimize your retail network, you can implement these integrated services:

- **Security services**: The network uses security services—such as stateful firewalls, intrusion prevention systems, Advanced Malware Protection, and secure web gateways—to protect applications and the network from threats.
- **Cloud integration**: Cisco Catalyst SD-WAN integrates with cloud providers—such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud—to simplify branch office connections to cloud resources.
- **Multi-cloud connectivity**: This connectivity enables you to connect to multiple cloud providers and manage traffic efficiently.
- **Policy-based routing**: Administrators can define routing policies to control how the network routes and manages traffic, ensuring that critical applications receive the appropriate prioritization.

Managing configuration compliance and auditing

Role-based access control

Role-based access control (RBAC) for Cisco Catalyst SD-WAN Manager secures and simplifies network management for retail organizations. By implementing RBAC, you can manage user access, enforce security policies, and maintain compliance with regulatory requirements to safeguard critical network infrastructure and data.

Refer to the *Cisco Catalyst SD-WAN Manager Configuration Guide* for more information on RBAC.

Cisco Catalyst SD-WAN supports single sign-on (SSO) integration with up to three identity providers (IdPs) to provide different levels of access for SSO users of Cisco Catalyst SD-WAN Manager. Refer to the *Cisco Catalyst SD-WAN Single Sign-On Integration Guide* for more information on IdP integration.

Cisco Catalyst Center enables you to assign permissions to users based on a local, RADIUS, or TACACS database. You can assign users one of these roles and grant them access to specific applications within Cisco Catalyst Center:

- **Administrator (SUPER-ADMIN-ROLE)**: Users with this role have full access to all Cisco Catalyst Center functions. They can create other user profiles with various roles, including the SUPER-ADMIN-ROLE.
- **Network Administrator (NETWORK-ADMIN-ROLE)**: Users with this role have full access to all network-related Cisco Catalyst Center functions. They cannot access system-related functions, such as backup and restore.
- **Observer (OBSERVER-ROLE)**: Users with this role have view-only access to Cisco Catalyst Center functions. They cannot access functions that configure or control Cisco Catalyst Center or its managed devices.

Refer to the "Manage Users" section in the *Cisco Catalyst Center Administrator Guide* for detailed information on user management.

You can configure Cisco Catalyst Center with RADIUS external authentication using a Cisco ISE server to manage the controller. Refer to the *Cisco Catalyst Center and Cisco ISE Integration Guide* for configuration steps.

Audit logs

Cisco Catalyst SD-WAN audit logs offer several benefits for retail customers, enabling you to:

- maintain regulatory compliance
- monitor network security
- perform forensic analysis
- ensure accountability and transparency
- gain operational insights into configuration changes
- validate network policies
- receive alerts and notifications, and
- drive continuous improvement.

Overall, audit logs in Cisco Catalyst SD-WAN provide retail customers with essential capabilities to maintain security, compliance, operational efficiency, and proactive risk management within their network infrastructure.

Refer to the *Cisco Catalyst SD-WAN Monitor and Maintain Guide* for more information on audit logs and steps to export them to an external server.

Audit logs capture information about the applications running on Cisco Catalyst Center. These logs also capture device public key infrastructure (PKI) notifications. You can use the information in these audit logs to troubleshoot issues involving applications or device CA certificates.

Audit logs also record system events, including when and where they occurred and which users initiated them. The system logs configuration changes to separate files for auditing.

Refer to the " Audit Logs" section in the *Cisco Catalyst Center Administrator Guide* for detailed information and instructions on how to check the audit logs.

Configuration compliance

Configuration compliance helps retail customers ensure network security, adhere to regulatory requirements, and maintain operational consistency. Cisco Catalyst SD-WAN provides several key capabilities to achieve configuration compliance:

- template-based configurations
- version control and rollback, and
- the capability to lock the router CLI after Cisco Catalyst SD-WAN Manager manages the device.

Compliance checks help you identify intent deviations or out-of-band changes in the network that users inject or reconfigure. A network administrator can identify devices in Cisco Catalyst Center that do not meet compliance requirements for various aspects, such as software images, PSIRTs, and network profiles. You can automate compliance checks or perform them on demand using scheduling options.

Refer to the *Cisco Catalyst Center Compliance User Guide* for detailed information on how to enable and manage compliance for network devices.

Configuration drift

Compliance mandates often require retail organizations to archive configurations for all network devices. Cisco Catalyst Center supports configuration drift monitoring, which highlights the current configuration of every device and enables you to view configuration changes on a specific device over the past 30 days.

Wireless design

Retail networks rely on reliable wireless connectivity to support in-store operations, including point-of-sale (POS) systems, inventory management, employee devices, and guest Wi-Fi. In non-SD-Access retail deployments, the architecture uses Cisco Catalyst 9800 Series Wireless LAN Controllers (WLCs) at the corporate headquarters or data center. Cisco Catalyst Center centrally manages these controllers, while you deploy access points (APs) at remote store sites.

The retail wireless design includes these key components:

- **Centralized controller deployment**: You deploy all wireless controllers at the data center or corporate headquarters. This centralized deployment enables you to manage APs and wireless policies across hundreds or thousands of retail locations using Cisco Catalyst Center.
- **Wireless FlexConnect at remote sites**: FlexConnect APs provide wireless services under remote control from the headquarters or data center over the WAN. FlexConnect APs can:
  - switch client traffic locally at the store to improve performance, and
  - resynchronize with the headquarters WLC when the network restores connectivity, which ensures uninterrupted wireless service.
- **Centralized management with Cisco Catalyst Center**: Cisco Catalyst Center provides a centralized dashboard to provision, monitor, and manage all WLCs and APs across retail locations. Cisco Catalyst Center automates AP onboarding, firmware updates, configuration deployment, and policy consistency across sites.
- **High availability and resiliency**: Redundant WLCs at the headquarters or data center support stateful switchover (SSO) and N+1 configurations. FlexConnect APs automatically fail over between controllers to maintain continuous connectivity.
- **Guest and employee traffic segmentation**: The controller segments wireless traffic from APs, and the Cisco Catalyst SD-WAN or campus edge enforces security policies. Employee devices, POS terminals, and guest Wi-Fi operate on separate VLANs or VPNs to maintain security and regulatory compliance.
- **Multisite deployment**: Cisco Catalyst Center enables centralized orchestration for consistent wireless configurations and policies across all retail locations, which reduces manual work and deployment errors.
- **End-to-end assurance**: Integrating wireless telemetry and analytics with Cisco Catalyst Center provides real-time visibility into client health, AP performance, and wireless service quality. This visibility helps you troubleshoot issues and maintain service quality.

Wireless deployments in retail environments provide these benefits:

- providing consistent wireless performance across all stores
- centralizing management for large-scale retail environments
- supporting remote sites with FlexConnect to eliminate the need for local WLCs
- ensuring high availability and resiliency for business-critical wireless services
- segmenting employee, POS, and guest traffic securely, and
- accelerating deployments and policy propagation for new store locations.

Refer to the *Cisco Wireless Deployment Guide* for more information.

Migration to SD-WAN

To migrate from traditional routing to Cisco Catalyst SD-WAN, you must plan and execute several key steps. This process ensures an efficient transition while enhancing network capabilities and security. You can use this outline to manage the migration process.

Refer to the *Cisco Catalyst SD-WAN Migration Guide* for detailed planning and migration methodologies.

Assessment and planning

Network audit: Conduct a comprehensive audit of the existing network infrastructure, including hardware, software, and configurations.

Traffic analysis: Analyze traffic patterns, application dependencies, and performance requirements to identify critical applications and their network paths.

Risk assessment: Evaluate potential risks and challenges associated with the migration process, such as downtime, data integrity, and compliance requirements.

Design and architecture

SD-WAN solution design: Develop a detailed design plan to implement Cisco Catalyst SD-WAN based on your requirements.

Topology mapping: Define the new SD-WAN topology, including the deployment of WAN Edge routers and controllers, such as Cisco SD-WAN Controller and Cisco SD-WAN Manager.

Security integration: Integrate security measures—such as firewall policies, VPN configurations, and encryption protocols—to protect data during the migration.

Implementation phases

Pilot deployment: Deploy a pilot SD-WAN environment in a controlled setting to validate the design, functionality, and performance before full-scale deployment.

Phased rollout: Implement Cisco Catalyst SD-WAN gradually across different branches, starting with less critical locations to refine processes and resolve early challenges.

Configuration migration: Migrate existing routing configurations to SD-WAN templates and policies to ensure consistency and compliance with business requirements.

Testing and validation: Test Cisco Catalyst SD-WAN functionality thoroughly, including failover scenarios, application performance, and security measures.

Integration and optimization

Network convergence: Integrate Cisco Catalyst SD-WAN with existing network infrastructure to ensure reliable connectivity and interoperability between legacy systems and SD-WAN components.

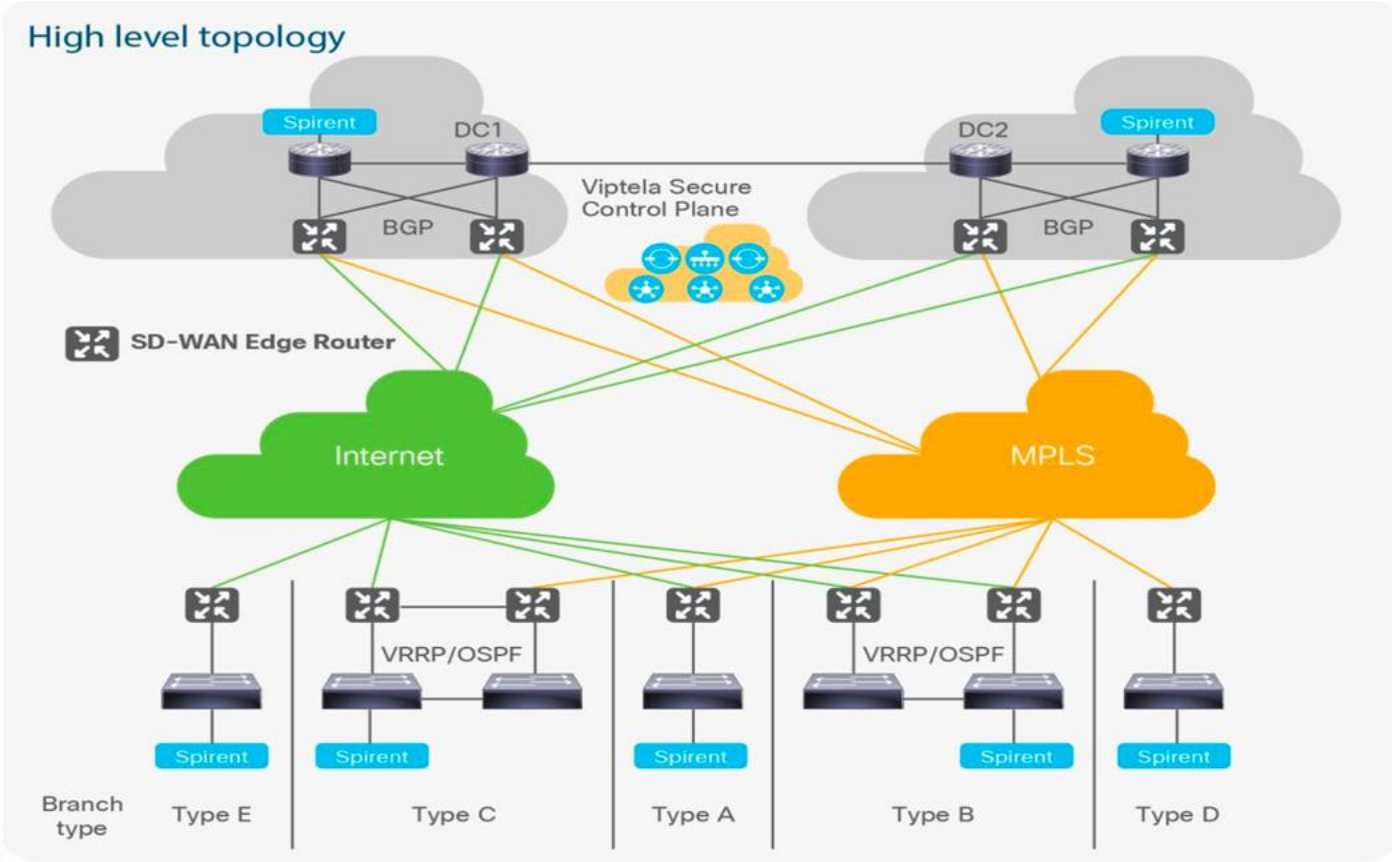
Performance optimization: Fine-tune SD-WAN policies and QoS settings to optimize application performance, prioritize critical traffic, and improve overall network efficiency.

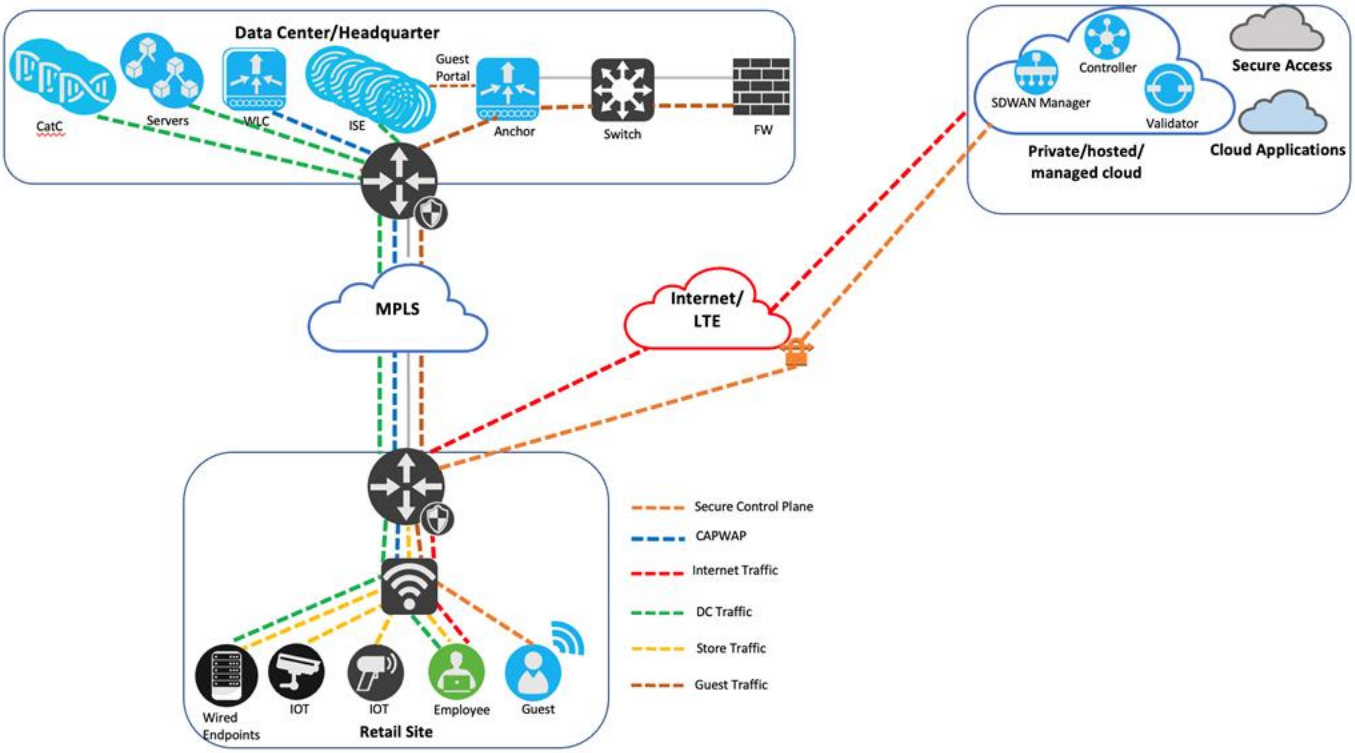
Monitoring and management: Use centralized monitoring and management tools, such as Cisco SD-WAN Manager, to monitor network health, analyze performance metrics, and resolve issues.

Validated solution use cases and topology

Topology

These validated use cases serve as templates to help you design and build your retail network infrastructure. The figures show the logical topology of the solution test bed.





Solution use cases

These validated designs help you build a network infrastructure that meets your requirements.

Day 0 and Day 1 network bringup and site connectivity

Retail networks must support the rapid, repeatable deployment of new stores, distribution centers, and corporate locations while minimizing manual configuration and onsite effort. Cisco Catalyst Center and Cisco Catalyst SD-WAN provide centralized automation and orchestration to accelerate Day 0 and Day 1 operations across large-scale retail environments.

New site bringup (greenfield deployments)

You can use these platforms to deploy new retail sites—including stores, campuses, and distribution centers—to:

- provision wired, wireless, and WAN devices automatically using zero-touch provisioning (ZTP), Plug and Play (PnP), and bootstrap workflows
- discover devices, visualize topologies, and manage inventory automatically
- provision switch, router, and SD-WAN configurations centrally using standardized templates
- establish secure and reliable connectivity between headquarters, branches, data centers, and cloud services
- support flexible WAN transport options, including MPLS, broadband internet, LTE or 5G, and direct internet access (DIA), and
- enable SaaS and cloud application access directly from branch locations.

Wireless network deployment

You can simplify and scale wireless deployments across retail locations to:

- upload floor maps and associate them with Cisco Catalyst Center sites
- onboard access points using Plug and Play and assign them to the correct site and floor map
- provision centralized and FlexConnect wireless profiles from headquarters-based or data center-based Cisco Catalyst 9800 Series Wireless LAN Controllers
- deploy SSIDs, wireless policies, and RF profiles consistently across thousands of stores
- enable guest wireless access with traffic segmentation and secure internet breakout, and
- implement N+1 wireless LAN controller (WLC) designs to improve scalability and high availability.

Brownfield site expansion and upgrades

You can modernize existing retail sites with minimal disruption to:

- migrate brownfield stores and campuses to centralized management using Cisco Catalyst Center and Cisco Catalyst SD-WAN Manager
- introduce new wired, wireless, and WAN services while preserving existing connectivity
- standardize configurations and reduce drift using Day 0 configuration templates, and
- integrate legacy infrastructure into a centrally managed operational model.

Centralized automation and policy consistency

You can maintain operational consistency across all retail locations to:

- apply standardized wired, wireless, and WAN configuration templates across multiple sites
- integrate with Cisco Identity Services Engine (ISE) to authenticate devices and clients across wired, wireless, and SD-WAN environments
- manage network inventory, software images, and lifecycle operations from a centralized management dashboard, and
- accelerate the onboarding of new stores using predefined site profiles and reusable configuration policies.

Managing Day N network operations

Retail networks operate on a massive scale and require continuous optimization, security enforcement, and lifecycle management without disrupting store operations. Cisco Catalyst Center and Cisco Catalyst SD-WAN provide centralized visibility, automation, and assurance to manage Day N operations across wired, wireless, and WAN domains.

Lifecycle and software management

You can simplify ongoing network lifecycle operations across all retail locations to:

- manage software images centrally for switches, routers, and wireless controllers using Software Image Management (SWIM)
- schedule and automate upgrades for:
- campus and branch switches, including stacks and StackWise Virtual deployments
- Cisco Catalyst 9800 Series Wireless LAN Controllers (physical and virtual) with stateful switchover (SSO), and
- access points using rolling upgrade workflows
- generate upgrade reports and compliance status across the retail network

- support brownfield device migrations and refresh cycles with minimal service disruption, and
- manage software upgrades and maintenance for Cisco Catalyst SD-WAN using Cisco Catalyst SD-WAN Manager.

Refer to the *Cisco Catalyst Center Install and Upgrade Guides* for installation instructions.

Configuration and change management

You can maintain configuration consistency while enabling controlled changes to:

- deploy and modify wired, wireless, and SD-WAN configurations using reusable templates
- track configuration changes and drift across devices and sites
- perform Day N configuration updates, including:
  - device credentials and password changes
  - certificate renewals and third-party root CA updates, and
  - AAA service updates, including Cisco ISE PSN migrations
- integrate with IT Service Management (ITSM) platforms, such as ServiceNow, for automated change control workflows, approvals, scheduling, and audit tracking, and
- log and audit all configuration and software changes for governance and compliance.

Wireless operations

You can manage wireless services across retail locations to:

- manage and operate wireless services across retail sites from a centralized controller at the data center or headquarters
- modify wireless network settings, profiles, tags, and AP zones to adapt to changing business and store requirements
- create, update, and scale enterprise, BYOD, and guest SSIDs consistently across branches
- onboard wireless clients using enterprise SSIDs for branch employees and internal users
- provide guest wireless access using a centralized web authentication portal with a controlled onboarding experience
- enforce guest SSID traffic segmentation, including anchoring guest traffic to a centralized firewall using Multisite Remote Border
- manage both centralized and FlexConnect wireless deployments through Cisco Catalyst Center
- apply quality of service (QoS) policies for employee, BYOD, and guest wireless clients using AP groups and policy profiles
- onboard new access points using Plug and Play (PnP) for simplified Day N expansion
- support AP refresh and RMA workflows with automated reprovisioning to preserve configuration and policy consistency, and
- update AP locations and reprovision devices as store layouts or floor maps change.

Security and access control operations

You can maintain a strong security posture throughout Day N operations to:

- manage wired and wireless authentication policies, including 802.1X, MAC Authentication Bypass (MAB), and preshared keys (PSK)

- monitor threats, rogue access points, and adaptive wireless intrusion prevention system (aWIPS) events
- configure and maintain guest Wi-Fi access with traffic segmentation
- implement role-based access control (RBAC) updates to align with evolving operational and compliance requirements, and
- perform security scans and receive security advisories for network devices.

The security dashboard in Cisco Catalyst SD-WAN Manager provides comprehensive monitoring and management of security features across the SD-WAN fabric. The dashboard offers a graphical view of packets that the firewall inspects or drops, signature violations for the intrusion prevention system (IPS), and files that the system transfers with their disposition for Advanced Malware Protection (AMP). This dashboard enables you to monitor overall security health and traffic statistics in real time or over selected time periods.

Inventory and asset management

You can maintain an accurate and up-to-date network inventory to:

- discover devices using Plug and Play, IP address scanning, or Cisco Discovery Protocol (CDP)
- manage device lifecycle events, including Return Material Authorization (RMA) and hardware replacement
- move devices between sites and locations as retail stores evolve, and
- run compliance checks to ensure alignment with standard configurations.

Monitoring, assurance, and telemetry

You can gain continuous visibility into network health and performance to:

- monitor system health and utilization across sites, devices, and services
- track wired and wireless client counts, performance, and experience
- monitor critical network services, such as AAA, DHCP, and DNS
- enable real-time streaming telemetry for detailed performance analytics, and
- configure alerts and notifications for incident detection and response.

Segmentation and security policy use cases

Retail networks must securely support diverse users, devices, and applications—including employees, POS systems, guests, IoT devices, and vendors—across thousands of geographically distributed locations. Cisco Catalyst Center and Cisco Catalyst SD-WAN consistently segment traffic, enforce policies centrally, and integrate security across the retail environment.

Network segmentation and policy enforcement

You can use Cisco Catalyst SD-WAN and Cisco Catalyst Center to:

- implement macro segmentation using VPNs and virtual network constructs to isolate traffic domains, such as employee, point-of-sale (POS), guest, vendor, and IoT and monitoring systems
- enforce consistent segmentation policies across branches, campuses, data centers, and the cloud using encrypted SD-WAN overlays
- support operational scalability to add new segments and update policies without reconfiguring each site
- apply policy-based routing (PBR) and topology control to steer traffic based on the application, user role, or destination

- optimize performance for business-critical retail applications—such as POS transactions, inventory systems, analytics platforms, and video services—by controlling traffic paths and latency-sensitive flows, and
- enable direct internet access (DIA) for retail sites while maintaining segmentation and security controls.

Secure access and identity-based policies

You can use Cisco Catalyst Center and Cisco Identity Services Engine (ISE) to:

- securely onboard wired and wireless clients for centralized authentication and authorization
- enforce role-based access policies aligned with user personas, such as employees, guests, contractors, vendors, and IoT devices
- support employee mobility and remote access with secure, reliable connectivity to retail applications from any location, and
- integrate external AAA systems for role-based administrative access and audit logging.

Threat protection and traffic inspection

You can protect your network from security threats to:

- isolate untrusted or guest traffic by steering the traffic through centralized firewalls or demilitarized zones (DMZs) using Cisco Catalyst SD-WAN service chaining
- implement zone-based firewall (ZBFW) policies on WAN Edge devices to control and inspect traffic flows
- enable intrusion detection and prevention (IDS or IPS) capabilities within the SD-WAN fabric to protect against cyber threats
- deploy Unified Threat Defense (UTD) mechanisms to safeguard retail networks across branches and headquarters, and
- integrate Secure Service Edge (SSE) and cloud security services to enhance threat protection and policy enforcement.

Encryption, certificates, and compliance

You can secure data and maintain regulatory compliance to:

- ensure secure connectivity across all retail locations using encrypted SD-WAN overlays
- implement MACsec to protect data integrity and confidentiality on critical wired links
- manage the certificate lifecycle by rolling out trusted and third-party certificate authorities (CAs), and rotating or revoking certificates across devices and controllers, and
- support PCI DSS-compliant retail environments by enforcing segmentation and encryption for payment-related traffic.

Visibility, monitoring, and incident response

You can monitor network operations and respond to security incidents to:

- integrate Cisco Secure Network Analytics for network threat detection, behavioral analysis, and automated threat response
- monitor and audit policy changes, deployments, and enforcement status centrally
- generate real-time alerts for policy violations, non-compliant endpoints, and rogue clients and access points using Cisco Catalyst Center Intelligent Capture, and
- isolate rogue or compromised WAN Edge devices or sites by revoking certificates in Cisco Catalyst SD-WAN Manager.

System and network robustness, resilience, and performance

Retail networks must operate continuously despite WAN impairments, device failures, and operational churn. Cisco Catalyst Center, Cisco Catalyst wireless solutions, Cisco Catalyst SD-WAN, and Cisco Identity Services Engine (ISE) work together to maintain network resilience, performance, and stability across campuses, branches, and data centers.

System and network resilience

You can use this architecture to:

- validate end-to-end resilience across wireless, campus switching, WAN, and identity services during planned and unplanned events
- ensure rapid recovery from device, link, and service failures with minimal impact on user connectivity and the application experience, and
- maintain configuration and policy continuity during Return Material Authorization (RMA) hardware replacement and device recovery workflows.

Wireless and WAN resilience

To maintain wireless and WAN operations, the network can:

- verify wireless service continuity during wireless controller failover, stateful switchover (SSO) events, or individual access point failures, and
- ensure reliable client connectivity when remote sites experience WAN outages or degraded links, or when the network restores WAN connectivity after an outage.

Campus and local device resilience

You can configure the network to:

- validate end-to-end resilience across wireless, campus switching, WAN, and identity services during planned and unplanned events
- prevent failures at the access or distribution layer from cascading into service-wide outages, and
- maintain configuration and policy continuity during Return Material Authorization (RMA) hardware replacement and device recovery workflows.

Identity and policy services resilience

To maintain identity and policy services, Cisco Identity Services Engine (ISE) and Cisco Catalyst Center can:

- enforce policies continuously during Cisco ISE Policy Service Node (PSN) failures, Policy Administration Node (PAN) failovers, PSN reassignments, node changes, or Cisco ISE software upgrades, and
- maintain uninterrupted authentication and authorization services for wired and wireless clients.

Network resilience and impairment handling

To handle network impairments, Cisco Catalyst SD-WAN and Cisco Catalyst Center can:

- monitor and mitigate WAN impairments—such as latency, packet loss, and jitter—across geographically distributed retail sites
- adapt to degraded network conditions automatically to maintain application availability and the user experience, and

- preserve service continuity during node failures in clustered wireless controllers, Cisco Catalyst SD-WAN controllers, and management platforms.

Performance and longevity

You can optimize network performance and longevity to:

- ensure consistent application performance by using intelligent path selection, routing traffic dynamically during link degradation, and routing SaaS and internet-bound traffic directly from branch locations
- apply quality of service (QoS) to prioritize critical retail applications, such as point-of-sale (POS) systems, inventory management, and real-time analytics
- validate long-term infrastructure stability by performing continuous soak and churn testing, multi-layer performance testing across campus, WAN, wireless, and identity domains, and regular access point (AP) and client performance testing using tools such as Intelligent Capture (iCAP), and
- sustain network longevity despite ongoing changes in devices, users, policies, and application workloads.

Monitoring and troubleshooting with assurance and analytics

Cisco Catalyst Center provides a centralized assurance and analytics platform to support Day N network operations across campus, WAN, and wireless domains. This platform provides continuous visibility into network health, the user experience, and application performance across retail locations.

Centralized visibility and health monitoring

You can use the assurance dashboards to:

- monitor the overall state of the network—including wired and wireless users, devices, and services—from a centralized dashboard
- gain real-time visibility into network health, device status, and service availability, including Cisco Identity Services Engine (ISE), Cisco Catalyst Center, wireless controllers, and SD-WAN controllers
- detect and track severe, critical, and ongoing issues across sites with contextual impact analysis and guided remediation recommendations, and
- identify failures—such as device outages, site disconnections, or control plane disruptions—and their effect on users and applications.

User, device, and application experience

To monitor and analyze user and device experiences, you can:

- obtain a comprehensive view of individual devices, wired users, and wireless users, including connectivity, authentication status, and performance history
- monitor detailed application usage and performance using Application Visibility and Control (AVC)
- perform deep traffic analysis and reporting using Network-Based Application Recognition (NBAR), Flexible NetFlow (FNF), and cFlowd to gain granular insights into application behavior and bandwidth consumption, and
- use historical insights to analyze user experience trends across branch, campus, and headquarters environments.

Cisco Catalyst SD-WAN Manager also provides deep visibility into network traffic and application performance. This visibility enables administrators to identify and prioritize critical applications, which ensures that these applications receive the necessary network resources and simplifies network operations.

Advanced analytics and observability

To gain deep insights into your network, you can:

- integrate ThousandEyes agents on network devices to gain end-to-end visibility into WAN paths, cloud services, SaaS applications, and internet dependencies
- perform continuous testing and analytics to validate application performance and SLA compliance, and
- correlate application performance metrics with network events to identify the root cause of issues quickly.

Troubleshooting and optimization

To resolve issues quickly, you can use Cisco Catalyst Center to:

- access devices using SSH directly from the dashboard
- compare historical and current configurations to identify changes
- run path trace analysis to identify connectivity issues
- analyze device health metrics, such as high CPU or memory utilization, and
- review audit logs for configuration, public key infrastructure (PKI), and application-related issues.

Troubleshooting and root cause analysis

To identify and resolve network and client connectivity issues, you can:

- troubleshoot connectivity issues using integrated assurance tools, such as Network-Wide Path Insights (NWPI), Underlay Measurement and Tracing Services (UMTS), path trace and end-to-end flow visualization, or the Machine Reasoning Engine for automated issue detection and remediation guidance, and
- analyze policy, configuration, and control plane events in conjunction with client and application telemetry to reduce the mean time to resolution (MTTR).

Location analytics and in-store visibility

Location analytics provides retailers with insights into customer behavior, foot traffic patterns, and in-store engagement. This integration connects Cisco wireless infrastructure with analytics platforms to deliver real-time and historical insights.

Architecture overview

The location analytics architecture uses these components and processes:

- Cisco access points collect client telemetry, including Wi-Fi and Bluetooth Low Energy (BLE) presence data
- access points forward this telemetry data to Cisco Catalyst Center for processing and aggregation, and
- integrations with analytics platforms, such as Cisco Spaces, enable advanced visualization and insights.

Key capabilities

The location analytics solution enables you to:

- track the real-time location of devices within store premises
- generate heatmaps that show customer dwell times and movement patterns
- analyze zone-based traffic in areas such as entrances, aisles, and checkout counters, and
- generate historical reports to optimize business operations.

Integration workflow

The system integrates wireless telemetry with location analytics through these steps:

- access points detect client devices using probe requests and association data
- access points forward this telemetry data to Cisco Catalyst Center
- Cisco Catalyst Center integrates with location analytics platforms using APIs, and
- the system processes and visualizes data in dashboards for business and IT stakeholders.

Business outcomes

Implementing location analytics helps you:

- optimize store layouts based on customer movement patterns
- improve staffing decisions using footfall analytics
- measure campaign effectiveness using dwell times and engagement metrics, and
- enhance the customer experience using data-driven insights.

Visualizing operational data

We recommend including dashboards and heatmap visualizations in this section to show real-world usage and provide operational clarity.

Scale

Solution test verified the scale numbers listed in this table on a 112-core second-generation Catalyst Center appliance. For the software and hardware capacity, refer to the Cisco Catalyst Center Data Sheet.

Catalyst Center scale

Catalyst Center	Value
Device inventory	10,000
Number of sites (Area, Building, Floor	10,000
Number of WLCs	4000
Number of APs	25,000
Number of sensors	3200
Network profiles	50
Number of SSIDs	200
Number of endpoints	300,000
Number of syslogs	10,000
Number of SNMP traps	10,000
ISE support	9 node cluster (1 PAN + 1 MNT + 6 PSN)

For detailed Cisco Catalyst Center scale considerations, refer to appliance scale.

Throughput performance varies depending on the combination of enabled features and the multidimensional deployment.

SD-WAN scale

SD-WAN controller	Value
SD-WAN Manager device inventory	12,500 (6 node cluster)
SD-WAN policy scale (# of lines)	60,000

cEdge	Branch (8200)	Hub 8500-20X6C
BFD IPSEC tunnels	100	10,000
VRFs	5	64
DPI flows	50,000	2,000,000
OMP routes	1000	300,000

cEdge	Branch (8200)	Hub 8500-20X6C
Multicast PIM neighbors	10	10
Maximum NAT sessions	20,000	2,000,000
FW sessions	4000	2,000,000

For detailed Cisco Catalyst SD-WAN scale considerations and sizing of SD-WAN Manager, SD-WAN Controller, SD-WAN Validator, refer to the scale matrix.

Hardware and software matrix

This table lists the hardware and software used to test the solution. For a complete list of hardware that the Cisco Catalyst Center solution supports, refer to the Cisco Catalyst Center Compatibility Matrix.

Also refer to Cisco Catalyst SD-WAN Control Components Compatibility Matrix as needed.

Role	Model name	Hardware platform	Software release	
Cisco Catalyst Center Controller	DN3-HW-APL-XL	Catalyst Center appliance 3-node cluster	2.3.7.9	2.3.7.10
Cisco Catalyst Center on ESXi (1,2)	DNA-SW-OVA	Catalyst Center on ESXi	2.3.7.9	2.3.7.10
Identity Management, RADIUS server	SNS-3695-K9	Secure Network Server for Cisco Identity Services Engine (ISE) application (large)	3.4 Patch 4	Cisco ISE 3.4 Patch 4
Cisco wireless controller	C9800-80-K9	C9800-80-K9	17.12.5, 17.17.1	17.15.4, 17.18.2, 17.18.3
Cisco wireless controller	C9800-CL	Virtual wireless controller	17.12.5, 17.17.1	17.15.4, 17.18.2, 17.18.3
Cisco SD-WAN cEdge router	C8500-12X4QC	Cisco SD-WAN Edge platform	17.12.5a	17.12.5a
Cisco SD-WAN cEdge router	C8300-2N2S-4T2X	Cisco SD-WAN Edge platform	17.12.5a	17.12.5a
Remote site switch	C9500-24Y4C C9300-48P, T, U C9300-24U, UX	Cisco Catalyst 9300/9500	17.9.6a, 17.12.5, 17.15.3	17.12.6, 17.15.4d, 17.18.3
Remote site switch (legacy)	ISR4451 Cisco Catalyst 3850	Cisco Integrated Service Router Cisco Catalyst 3850	17.12.5a 16.12.13	17.12.5a 16.12.13
Cisco Spaces	Cisco Spaces Connector	Virtual connector	location-3.1.0.127, iot-services-3.1.3.44	location-3.2.3.11, iot-services-3.2.0.3
Ekahau	—	Ekahau Artificial Intelligence (AI) Pro software	11.0.2.219	11.0.2.219

References and best practices

Cisco Catalyst 9800 Series Wireless Configuration Best Practices

Cisco Catalyst Center User Role Permissions

Implement Disaster Recovery

Support for Multiple Cisco Catalyst Center Clusters with a Single Cisco ISE System

Cisco Catalyst Center Release Notes

Cisco Catalyst Center Security Best Practices Guide

Cisco Catalyst SD-WAN Design Guide

Cisco Catalyst SD-WAN End-to-End Deployment Guide

Cisco Catalyst SD-WAN: Application-Aware Routing Deployment Guide

Cisco Catalyst SD-WAN: Enabling Direct Internet Access

Zscaler Internet Access (ZIA) and Cisco Catalyst SD-WAN