Validated Profile: Healthcare (SD-WAN)

March 4, 2026

Document purpose and use

The purpose of this document is to outline a typical healthcare deployment profile that Cisco recommends. It provides guidelines for a typical fabric deployment that uses Cisco Catalyst SD-WAN and serves as a validation document you can refer to during the process. Deployment engineers can use this document's theoretical sections in conjunction with its practical sections to help understand the service requirements to make the best decisions for their network during deployment and configuration.

Target audience

The target audience for this healthcare profile is the technical staff that is responsible for engineering and operating the network, as well as the implementation teams.

Solution overview

Healthcare organizations run thousands of branches throughout the world, ranging from small clinic to large hospitals spanning across multiple regions. While each site has its own specific requirements, the healthcare network environments require a specialized set of demands that includes security, enhanced network services, efficient network management, seamless mobility, network high availability, and location services. The topics described in this document cover the key considerations for a large, evolving healthcare network that needs to meet today's requirements.

The Cisco Software Defined WAN (SD-WAN) offers on-prem, cloud-hosted, and cloud-delivered overlay WAN architecture that facilitates digital and cloud transformation for enterprises, with the cloud-hosted architecture being particularly pertinent to healthcare customer network profiles. It significantly drops WAN costs, reduces the time to deploy services, build application resiliency and provides a robust security architecture for hybrid networks.

Cisco SD-WAN solves many critical enterprise problems, including:

- Establishing transport-independent WAN for lower cost and higher diversity
- Providing secure control and data plane connectivity
- Meeting service-level agreements (SLAs) for business-critical and real-time applications
- Providing end-to-end segmentation for protecting critical enterprise compute resources
- Extending seamlessly into the private/public cloud
- Providing direct internet access from the branches with zone-based firewall

Cisco SD-WAN provides data plane and control plane separation by having controllers in the cloud (public or private).

This document covers the enterprise solution profile built for healthcare with the features described.

Security

The Cisco SD-WAN solution offers secure control and management communications between the routers and the control components. Data plane communication between the WAN Edge routers is encrypted and secured based on IPsec encapsulation.

Hybrid transport

There are two data centers in this profile with each data center having two SD-WAN routers. All of the data-center SD-WAN routers are connected to internet and Multiprotocol Label Switching (MPLS) transports.

The branches have a range of connectivity models.

- Hybrid Model: Dual transport internet and MPLS
- Single Site: Single transport, either to the internet or to MPLS
- Dual Site: Dual transport with tloc-extension

Segmentation and zone-based firewall

For segmentation and zone-based firewall (ZBFW), there can be multiple segments in the branches, and, with Cisco SD-WAN, a user is able to keep the segments separate within the branch and on the overlay. In this profile, four VPN segments have been defined.

- Sales VPN (VPN 2): For corporate sales employees and related devices

- Clinical VPN (VPN 3): Dedicated to clinical staff and healthcare operations, supporting critical healthcare applications
- Guest VPN (VPN 10): For guest Wi-Fi and visitor access, segregated from internal corporate traffic
- Research and Development (R&D) VPN (VPN 20): For research and development facilities and sensitive research operations
- Management (VPN511): For out of band management traffic

Zone-based firewall is deployed for the traffic from guest Wi-Fi VPN to DIA.

Policy-based hub-and-spoke topology

Centralized policies are deployed to establish a hub-and-spoke topology between the data centers and the branches.

One set of branches prefers the default route from Data Center 1 (DC-HUB-1), and another set of branches prefers the default from Data Center 2 (DR-Hub-1), as illustrated in the Topology diagram.

Quality of Service

Quality of Service (QoS) is configured on all devices. The WAN bandwidth is appropriately distributed between different types of applications. Voice is given dedicated bandwidth on WAN interfaces and placed in a Low Latency Queue. Other traffic classes share the remaining bandwidth among them based on weight assignment.

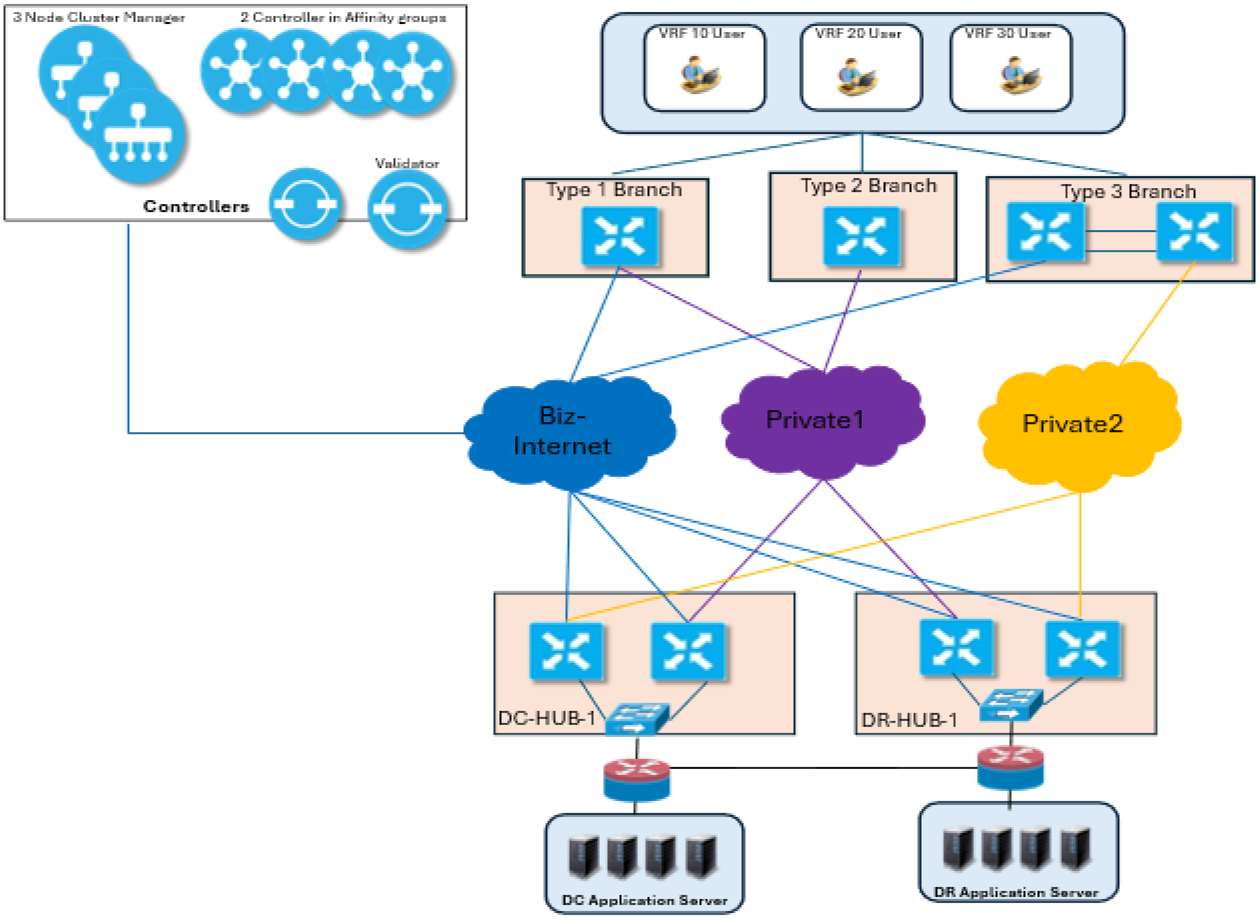
SLA based application-aware routing policies

Centralized routing policies for hybrid sites prioritize MPLS for voice traffic based on defined SLAs, while best-effort traffic is routed through the internet.

Dynamic Host Configuration Protocol servers for the branches

The WAN edge routers in the branches are configured to be Dynamic Host Configuration Protocol (DHCP) servers for some of the segments for allocating IP addresses to the clients.

Topology



Hardware details

Hardware device	Role	Number of tunnels
C8500-12X4QC	DC HUB	4000
ASR1002-HX	DR HUB	4000
ISR4451-X	T1 Spoke	8
ISR4461/K9	T2 Spoke	8
C8200-1N-4T	T3 Spoke	8
C8300-1N1S-4T2X	T3 Spoke	8

Key features in profile

Role	Features
Branch	QoS, DPI, ZBFW, NAT, BGP, OSPF, Multicast, Affinity, on-demand tunnel, VRF, SNMP
HUB	QoS, DPI, Multicast, Affinity, SNMP, VRF
SD-WAN Manager	Cluster, SDAVC, Feature Template, CLI Addon Template

Role	Features
SD-WAN Controller	Centralized Policy with HUB & Spoke, AAR, Affinity

Use cases

Flexible branch deployments

Flexible branch deployments in Cisco SD-WAN enable organizations to quickly and securely deploy and manage branch offices and remote sites with high efficiency and scalability. Key aspects include:

- Zero touch plug and play deployment
- Flexible deployment models
- Centralized management and analytics
- Hardware platforms for branches
- Scalability

Robust LAN segmentation for diverse users

Segmentation supports diverse scenarios such as separating lines of business, isolating guest users from authenticated users, segregating IoT or video surveillance traffic, and enforcing compliance with standards like HIPAA and PCI.

- End-to-end network segmentation using VRF
- Policy enforcement and security
- Centralized management

Reliable path monitoring and guaranteed application delivery

Cisco Application-Aware Routing (AAR) in Catalyst SD-WAN is a feature for the overlay that dynamically selects the best WAN path for application traffic based on real-time performance data and predefined Service Level Agreements (SLAs). It monitors key path characteristics such as packet loss, latency, and jitter using Bidirectional Forwarding Detection (BFD) probes and inline data, enabling optimized application delivery and reliable path monitoring.

In this profile, the app-route policy dynamically steers application traffic across the best available WAN transport (for example, MPLS, internet) based on application, DSCP, port, or prefix match and the real-time health and performance (SLA) of those paths.

Match criteria	SLA class	Preferred colors	Backup color(s)
dscp	Voice-And-Video_sclst	private1, private2	biz-internet
app-list	Transactional-Data_sclst	biz-internet, private1, private2	
source-ip	Default_sclst	private1, private2, biz-internet	

Note: Optionally, when Preferred Color Groups (PCG) is not selected, you can choose the preferred color group. Configure up to three levels of priority based on the color or path preference.

Secure remote access with on-demand tunnel

Secure remote access with On-Demand Tunnel (ODT) provides a controlled, temporary, and secure connection method for remote users to access network resources only when necessary.

In this profile, a dynamic ODT is established from single site WAN Edge to a hybrid-mode site over Biz-Internet for end-to-end unicast traffic.

Multicast support for critical healthcare operations

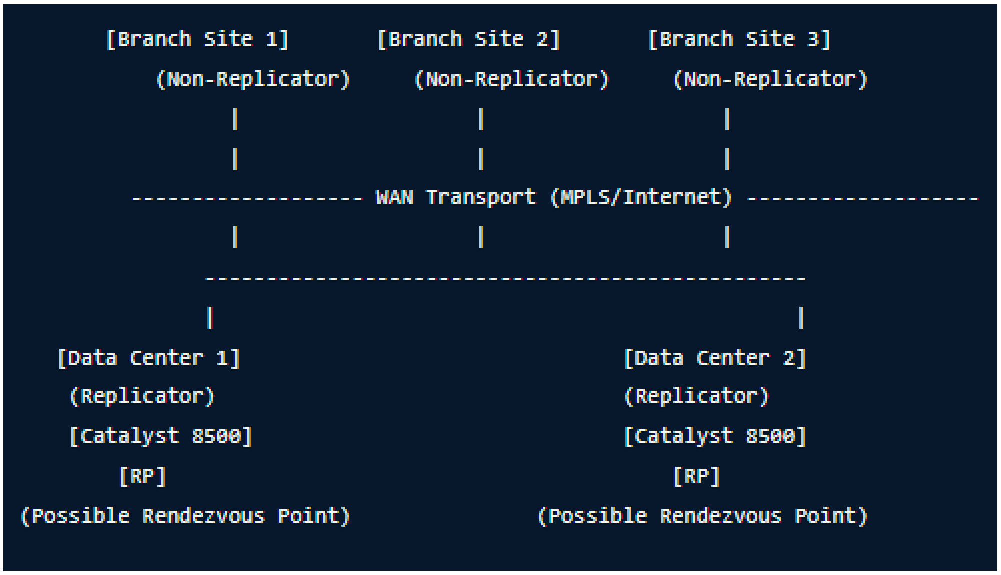
Multicast technology is essential in healthcare environments to efficiently deliver data streams such as patient monitoring, video conferencing, and real-time alerts to multiple recipients without overwhelming the network. Cisco SD-WAN multicast overlay routing extends native multicast capabilities by creating a secure and optimized multicast distribution tree over the SD-WAN fabric using the Overlay Management Protocol (OMP).

In this profile, the multicast source is located at the Hub (Data Center), and the multicast receivers are located at the branch sites. WAN Edge routers at the branch locations participate in the multicast domain, while the Catalyst 8500 WAN Edge routers at the data centers act as replicators.

In the data center, multicast routing is enabled in VRF 10 with PIM sparse mode configured on the service interface. The SSM range is defined as " PIM-SSM-Range" (239.232.0.0/16).

In the remote branches, IP multicast routing is enabled in VRF 10 using distributed mode. PIM sparse mode is configured on the LAN interface, with the SSM range defined by the prefix list " PIM-SSM-Range" (239.232.0.0/16).

With PIM Sparse Mode (PIM-SM/ASM), an RP is required. In this topology, the RP should be hosted on the hub/data-center side, with DC-HUB-1 as primary and DR-HUB-1 as backup for high availability. Configure the Rendezvous Points (RPs) on a stable hub-side Layer-3 interface (preferably a loopback) and ensure RP reachability from all branch multicast domains. The possible RPs are located within the data centers, as shown in the diagram.



```
       [Branch Site 1]       [Branch Site 2]       [Branch Site 3]
           (Non-Replicator)     (Non-Replicator)     (Non-Replicator)
                  |                   |                   |
                  |                   |                   |
         ------------------- WAN Transport (MPLS/Internet) -------------------
                  |                   |                   |
               -------------------------------------------------
                |                                               |
   [Data Center 1]                               [Data Center 2]
    (Replicator)                                 (Replicator)
    [Catalyst 8500]                              [Catalyst 8500]
        [RP]                                         [RP]
(Possible Rendezvous Point)               (Possible Rendezvous Point)
```

Note: Multicast traffic is supported only by Hub-to-Spoke tunnels and is not supported by ODT dynamically created between two branch sites through unicast traffic.

Troubleshooting

Cisco SD-WAN includes a robust built-in suite of troubleshooting capabilities designed to provide end-to-end visibility, control plane diagnostics, and data plane analysis, primarily managed by centralized Catalyst SD-WAN Manager. Some key capabilities include:

- Real-time Dashboard offers a single pane of glass for viewing the overall health of the SD-WAN fabric, including device status, tunnel health, and application performance.
- Path Visualization is a graphical tool that visualizes the path traffic takes across the overlay, helping to identify latency, jitter, or packet loss.
- Alarms and Events Real-time are categorized alerts for control, data, and management plane issues.
- Site Topology provides a map-based view of device connectivity.
- Built-in speed tests (site-to-site or internet) measure throughput and link capacity.
- Packet Capture and Trace features enable capturing packets (TCP dump/Wireshark) on specific interfaces or running Network-wide Path Insights (NWPI) to analyze drop points.

Table 1. Design considerations for scaling a 20.12.5/17.12.5 overlay

Devices	Factors	Maximum limit	Recommended
SD-WAN Manager	Cluster	6	• 6 Node Cluster for a 2501 to 12500 overlay scale • 3 Node Cluster for a scale 501 to 2500
	Instance Size	128 GB memory 64 vCPU 1 TB HDD	• With DPI enabled per instance: 64vCPU/128GB/1TB • Without DPI per instance: 32vCPU/64GB/500GB
SD-WAN Controller	Instance Size	8 vCPU, 16 GB memory	16GB Memory up to 1200 peers
	OMP Peers	1500	• Each controller with 750-1000 OMP peers • Affinity group enabled
	Affinity Group	63	6 groups for a large overlay with 12 vSmarts
	Maximum RIB OUT	90,000,000	• Per Controller max 90M RIB out • 2 OMP session per WAN edge • 2 Controller per Affinity Group
SD-WAN Validator	Edge device per validator	1500	1500
HUB	Tunnel scale	8000	8000
	Next hop scale	32,000	• 90% of next hop scale • Hub and spoke with tunnel group
	VPN scale	500	Next hop scale depends on the number of VPNs and the total number of branches connected to the HUB router. Example: 2 VPNs - Up to 4000 branch routers

Devices	Factors	Maximum limit	Recommended
			3 VPNs – Up to 2900 branch routers 4 VPNs – Up to 2150 branch routers
Spokes/Branches	Number of TLOC	8	2 TLOC per WAN Edge • One private WAN • One public WAN
	Number of service VPN (VRF)	500	3 VPNs