Validated Profile: Cisco SD-Access Healthcare Vertical

Revised: December 20, 2023

Solution Overview

The purpose of this document is to provide guidance for a typical healthcare deployment profile using Cisco DNA Center and Cisco SD-Access and serve as a validation reference.

Significant changes have been taking place in the healthcare industry, such as exponential growth in telehealth and virtual care, the sudden increases in remote workforces, increased security concerns, fast-evolving primary care models, shifts in care delivery sites, and the prioritization of worker safety and wellness.

The following sections describe the key considerations for a large, evolving healthcare network that needs to meet today's healthcare requirements.

Service and Network Resiliency

The healthcare system requires strict network- and service-level resiliency, as it cannot afford to have long downtimes. Network-level resiliency can be achieved with a robust fabric network design that includes dual fabric borders nodes, dual fabric control plane nodes, dual anchor borders and control plane nodes, dual wireless controllers, fabric switches with either hardware stacking or StackWise Virtual, dual multicast rendezvous-points (RP), and dual fabric transit control plane nodes (where applicable). Service-level resiliency is achieved by deploying the following:

- A Cisco DNA Center three-node cluster.
- A distributed Cisco Identity Services Engine (ISE) cluster with multiple Policy Administration Nodes (PAN), Monitoring Nodes (MNT), as well as active and standby Platform Exchange Grid (pxGrid) and Policy Service Nodes (PSN).

Network Expansion

A healthcare network typically comprises of several large-scale campus sites and many small-scale branch or clinic sites. For a major health service provider, its clinical sites can number in the hundreds or even thousands. The surge in demand for telehealth and virtual care is matched by a corresponding rise in demand for the dynamic deployment of new clinic sites and the expansion of existing campus and clinic sites.

Cisco DNA Center provides ample support for flexible site additions and site expansion. The LAN Automation feature provides a zero-touch plug-and-play workflow to discover new devices and automate the creation of the underlying Layer 3 unicast and multicast network that connects to the existing network in a multitier fashion. Once in inventory, these newly discovered devices are ready to be provisioned with AAA configurations and added into a fabric with a fabric role. Cisco DNA Center also offers another unique zero-touch plug-and-play workflow that brings extended node devices into the Cisco SD-Access fabric site. The end-to-end workflow starts from discovery and continues through to IP address assignment, base provisioning, and fabric provisioning. Cisco SD-Access Extended Nodes increase the reach of a healthcare network by providing connectivity to uncarpeted spaces such as hospital parking lots or warehouses. They also greatly increase port density without the need to add additional fabric edge switches. Cisco DNA Center has the option to configure border nodes at a central location in order to provide internet access for the new sites via Cisco SD-Access Transit. When this option is enabled, all traffic from local sites that's destined for the internet will be forwarded to the local site border, then to the central campus site border. The traffic then exits the fabric domain. This not only provides an option to enforce security policies in a centralized location, but it also offers flexibility and reduces operational overhead for new site deployment, especially in scaled environments.

Network Services

Anchored Services: The design of a large hospital's network is very similar to that of most large campus networks, with a few differences. The main purpose of a hospital is to provide services to patients and guests. At any time, the hospital is likely to have

extensive guest services across all of its sites. Securely and reliably handling all of the wireless guests across multiple sites is an operational challenge. Another difference is that hospital networks contain massive amounts of medical devices such as monitors, pumps, medical-grade stations, servers, and imaging equipment. These devices could be located in different locations, but may need to be in the same subnet for L2 adjacency and managed in a unified manner from both the control and data plane points of view. Typically, any endpoint that is bound to its individual fabric site receives IP addresses from the local site address pool, and all traffic is directed via local site borders. This adds complexity for address management and policy enforcement for each managed site.

Cisco DNA Center provides the Multisite Remote Border solution, which can simplify the extension of a subnet between sites. This solution offers a simple and consistent anchored service for a particular Virtual Network (VN), the anchored VN, for both wired and wireless endpoints across sites. For anchored services, traffic for all of the endpoints that belong to the anchored VN at each dispersed site will be aggregated and tunneled back to a central location (the Anchor Border at the Anchor site) over Virtual Extensible LAN (VXLAN). This allows a single subnet to be deployed for clients across different sites. With this simplified and centralized subnet structure, the Multisite Remote Border solution facilitates service deployment and provides a clean and secure segmentation for anchored traffic in a multisite healthcare environment.

Multicast Services: Most healthcare networks need to accommodate a large number and variety of devices that service medical staff and patients, such as medical-grade computers, monitors, security cameras, and image analysis equipment. Data generated by these devices needs to be stored both locally and on remote hospital medical servers. This data must be accessible at any moment and in real time. Different types of servers—electronic medical records servers, medical image processing servers, medical billing servers—are often located in a dedicated medical server room in the main campus or main headquarter site of large healthcare organizations or medical research centers. These servers distribute mission-critical and time-sensitive data to multiple endpoints across distributed campus sites. Enabling multicast will offer optimal bandwidth and CPU utilization for data communications between medical servers and endpoint devices.

Cisco DNA Center provides a rich multicast solution that offers both PIM Any-Source Multicast (PIM-ASM) and PIM Source-Specific Multicast (PIM-SSM) in both the overlay and the underlay. This solution offers two different transport methods for multicast forwarding, tailored for different customer network design at a per-VN basis. The first method is head-end replication (that is, ingress replication), which offers a clean, overlay-only multicast forwarding solution (as it does not require multicast in the underlay network). The second method is native multicast, which offers the most scalable bandwidth and CPU efficiency wherever multicast replication is done throughout the underlay network.

Silent Medical Device Handling: Every day, thousands of medical devices connect to a healthcare network. Among these devices, some endpoints fall into the silent host category. These endpoints generally require the receipt of an Address Resolution Protocol (ARP) broadcast packet to come out of silence. Cisco DNA Center provides the Layer 2 flooding capability to support these silent hosts. Layer 2 flooding enables the flooding of broadcast, link-local multicast, and ARP traffic for a given overlay subnet. It maps the overlay subnet to a dedicated multicast group in the underlay, encapsulates the targeted traffic in a fabric VXLAN, and sends the traffic to the destination's underlay multicast group. It makes use of PIM-ASM in the underlay, which can be set up automatically using the Cisco DNA Center LAN Automation workflow or configured manually later in the deployment process. This provides great flexibility to a healthcare network by accommodating a variety of medical devices with different embedded capabilities.

Security and Network Segmentation

The healthcare system needs to protect the personal medical records and financial information of its patients. In the US, hospitals and medical centers are required to have HIPAA-compliant wired and wireless networks that can provide complete and constant visibility into their network traffic. These networks must protect sensitive data and medical devices such as electronic medical records (EMR) servers, vital sign monitors, and nurse workstations so that a malicious device cannot compromise the network. In other regions in the world, similar medical record privacy and security regulations are already in place.

Within the Cisco SD-Access architecture, Cisco DNA Center and Cisco ISE work in unison to provide the automation for planning, configuration, segmentation, identity, and policy services. Cisco ISE is responsible for device profiling, identity services, policy services, and the dynamic exchange of information with Cisco DNA Center.

The Cisco SD-Access solution addresses the need for complete data and control plane isolation between patient/visitor devices and medical/research facility devices by using macrosegmentation. By putting devices into different overlay Virtual Networks (VNs), healthcare facilities can achieve complete data isolation and provide security among different departments and users.

Cisco SD-Access can further address the need for more granular data plane isolation between endpoints within the same VN by using microsegmentation via Scalable Group Tags (SGTs) for Group-Based Policy (GBP). Cisco DNA Center allows IT administrators to create groups, place employees and devices in those groups by their roles, and define policies that control how these groups can interact with one another.

Network Assurance and Analytics

Network administrators should be able to efficiently manage and monitor their networks to quickly respond to the dynamic needs of a healthcare system. To improve the performance of a network, its devices, and its applications, a deployment should use telemetry to proactively predict network-related and security-related risks. Cisco DNA Assurance, with the use of Cisco AI Network Analytics, collects telemetry data, monitors the performance and health of network devices, flags any issues that it detects, and offers remediation steps.

With network assurance, administrators can monitor the overall health of network devices and connected endpoints (both wired and wireless). Endpoint and application assurance can be used to determine the individual health of the devices, endpoints, and their applications. With this deeper level of analytics, administrators can identify the individual issues that the network elements are facing, such as the connectivity issues a wireless laptop or medical device is having with a wireless network.

Endpoints Analytics

Modern security threats seek vulnerable points of entry to exploit a network's valuable enterprise information. Once an entry point has been breached, lateral movement from device to device can take place in mere seconds. Granular network segmentation, such as that enabled by Cisco's SD-Access solution, is the preferred method to prevent this kind of threat. Healthcare networks are populated by a wide variety of devices in multiple locations, which makes finding and identifying all of the devices in a network time-consuming and tedious. Cisco's Endpoint Analytics addresses this issue by identifying devices by type, manufacturer, model, OS type, communication protocols, and ports, using passive network telemetry monitoring and deep packet inspection to scan the network and allow an administrator to create profiling rules to classify devices based on those attributes. Coupled with machine learning, Cisco DNA Center can detect spoofed endpoints and help an admin take the appropriate action.

Further, Cisco DNA Center will share the endpoint classification attributes with Cisco ISE. When new devices onboard through identity-based authentication, they can be automatically identified by manufacturer and type and added to the appropriate group. Defining and enforcing security policies is easier when these policies are applied to groups rather than to individual endpoints. Group-based policy can easily be updated to adapt to new circumstances, such as security breakage by endpoints, and applied globally to the entire network.

Group-Based Policy Analytics

Understanding device types is the foundation for creating logical groups of access-control policies. Group-Based Policy Analytics (GBPA) provides a holistic view of traffic patterns that shows how groups (SGTs) are communicating with each other. With this information, an admin can map ports and protocols to device groups and use deep packet inspection to provide an early threat warning system by identifying malware in traffic. Devices that suspiciously start using different ports or protocols to communicate can be isolated. For example, if a device is identified as a medical device and suddenly starts sending streams of traffic to a compliance-critical medical record server, GBPA can be used to identify the anomaly. After viewing the abnormal traffic pattern, the administrator can change the policy to block the device until IT can investigate the cause.

Hardware and Software Specifications

This solution has been tested with the hardware and software listed in the following table. For a complete list of supported hardware, refer to the Cisco Software-Defined Access Compatibility Matrix.

Role	Model Name	Hardware Platform	Software Version	Software Version
Cisco DNA Center Controller	DN2-HW-APL-XL	Cisco DNA Center Appliance 3-Node Cluster	Cisco DNA Center 2.3.3.7	Cisco DNA Center 2.3.5.5
Identity Management, RADIUS Server	ISE-VM-K9	Cisco Identity Services Engine Virtual Appliance	Cisco Identity Services Engine 3.0, Patch 6 or 3.1 Patch 3	Cisco Identity Services Engine 3.2 Patch 2
	SNS-3695-K9	Secure Network Server for ISE Applications (large)		
Cisco SD-Access Fabric Control Plane Node	ASR1001-X	Cisco 1000 Series Aggregation Services Routers	17.6.6a, 17.9.4a	17.6.6a, 17.9.4a
	C9500-24Y4C C9500-24Q C9300-48P C9300-24P	Cisco Catalyst 9300/9500 Series Switches	17.6.6a, 17.9.4a	17.6.6a, 17.9.4a
Cisco SD-Access Fabric Border Node	C9500-24Y4C C9500-40X C9500-12Q C9500-24Q C9300-48P C9300-24P	Cisco Catalyst 9300/9500 Series Switches	17.6.6a, 17.9.4a	17.6.6a, 17.9.4a
Cisco SD-Access Fabric Edge Node	C9300-48P C9300-24P C9404R	Cisco Catalyst 9300 Series Switches	17.6.6a, 17.9.4a	17.6.6a, 17.9.4a
Cisco SD-Access Wireless Controller	C9800-80-K9	Cisco Catalyst 9800-80 Wireless Controller	17.6.6a, 17.9.4a	17.6.6a, 17.9.4a
Cisco SD-Access Extended Node	IE-3300-8P2S	Cisco Catalyst IE3300 Rugged Series	17.6.6a	17.6.6a
	IE-4010-4S24P	Cisco Catalyst IE4010 Rugged Series	15.2(7)E4	15.2(7)E4
	WS-C3560CX	Cisco Catalyst 3560-CX Switch Family	15.2(7)E6	15.2(7)E6

Role	Model Name	Hardware Platform	Software Version	Software Version
Cisco SD-Access Policy Extended Node	IE-3400H-16T	Cisco Catalyst IE3400 Rugged Series	17.6.6a	17.6.6a
	C9300-48P	Cisco Catalyst 9000 Series Switches	17.6.6a	17.6.6a

Solution Use Case Scenarios

The following use cases were executed for the Cisco SD-Access Healthcare Vertical profile. To view the logical topology of the Cisco SD-Access Healthcare Vertical solution test bed, see the figure provided in Topology, on page 8.

- Implement intent-based networking using Cisco DNA Center:
  - Administrators can design a global network hierarchy, configure global and site-level network settings, and provision devices automatically.
  - Administrators can deploy the main campus with dual borders and dual control plane nodes for redundancy and scale considerations.
  - Administrators can flexibly expand campus and branch sites by leveraging automation to onboard new devices:
    - Onboard fabric edges using zero-touch plug-and-play LAN automation.
    - Onboard classic extended nodes into the fabric for IoT device connection using zero-touch plug-and-play.
    - Onboard policy extended nodes into the fabric with direct support of SGT and enhanced traffic enforcement.
  - Administrators can provision a large number of small clinic branch sites automatically with different border options:
    - Fabric-in-a-box (FiaB) with embedded wireless enabled and hardware stacking.
    - Dual colocated border and control plane nodes with either an embedded or standalone wireless controller.
  - Distributed campus sites can connect using Cisco SD-Access Transit for shared data center and internet services.
- Integration of multiple Cisco DNA Center instances with a single Cisco ISE cluster:
  - Administrators can centrally manage virtual networks, scalable group tags, access contracts, and security policies on the Author node, and automatically synchronize with Reader nodes.
  - Administrators can perform role changes (like promoting the Author node) on different Cisco DNA Center instances without breaking the consistency of policy objects.
  - Policy enforcement verification and Change of Authority (CoA) can be successfully be deployed to devices in an environment with multiple Cisco DNA Center instances using Cisco ISE.
- Implement multitier security to protect sensitive medical data:
  - Administrators can segment users, guests, and IoT/medical devices into the appropriate logical network to limit the movement of threats around your network.
  - Administrators can enable closed authentication onboarding (dot1x) or MAC Authentication Bypass (MAB) for wired and wireless endpoints to prevent unauthorized access.

- Administrators can create groups, place users and endpoints in these groups (based on their identities), and define group-based policies that control traffic between groups.
- Administrators can implement a high scale of access control policies for hospital campuses, and Security Group ACLs (SGACL) are properly installed on edge devices when clients are onboarding.
- Administrators can monitor Cisco DNA Center activities using audit logs which record system events that occurred, when and where they occurred, and the users that initiated them.
- Administrators should be able to create granular role-based users with different privileges to access Cisco DNA Center.

- Service and network resiliency:
  - High Availability can be achieved throughout the network with dual Cisco SD-Access borders and dual control plane nodes, a border SVL and border/edge stack, and dual transit control planes in the transit network. Failover and recovery after a network failure should result in little or no interruption of traffic flows.
  - Administrators should be able to configure Cisco DNA Center in 3-node High Availability mode. When services or a node fails in a Cisco DNA Center cluster, the system should recover without any user intervention.
  - Cisco ISE's distributed deployment model should be recovered after a PAN, PSN, or pxGrid service failover.
  - Administrators can implement a critical VLAN for fabric edges when Cisco ISE is unreachable.
  - Administrators can schedule a backup of Cisco DNA Center's configuration and data for a particular time or initiate a backup on demand. Administrators can then restore the backup file in order to restore a previous Cisco DNA Center configuration.

- Simplified management:
  - Cisco DNA Center provides the central management of device inventory and allows users to view device information such as IP address, installed software version, provision status, and inventory insights.
  - Administrators can use the Software Image Management (SWIM) functionality in Cisco DNA Center to upgrade switches, routers, extended nodes, and wireless controllers to the selected golden image.
  - Cisco DNA Center's fabric border and control plane RMA workflow makes device replacement seamless.
  - The optimization of site border L3 handoff VLAN consumption gives administrators flexibility when assigning VLANs in a scaled multisite environment.
  - LAN automation with an overlapping pool option provides significant IP address optimization by allowing the underlay network to reuse the same address across different fabric sites.

- Network services:
  - Administrators can implement Multisite Remote Border at a central location to provide guest services to wireless endpoints across fabric sites. Guest traffic is isolated within a guest VN and tunneled to anchoring borders for internet access.
  - The Multisite Remote Border solution can use the same subnet for wired endpoints across multiple fabric sites.
  - The anchor site, with dual anchor borders/CP in different locations, can be implemented to provide redundancy when network failure occurs.
  - Multicast service enabled at main campus sites and remote sites can be configured with various design options:
    - RP is outside the Cisco SD-Access fabric, reachable from fabric borders.
    - PIM-ASM is enabled for multicast service in overlay virtual networks.

        - PIM-SSM is enabled for native multicast in underlay network.
        - Borders at the main campus fabric site can serve distributed campus sites for multicast service via the Cisco SD-Access Transit network.
        - Multicast sources in server rooms are connected to edge and border nodes using trunks with multicast receivers across different fabric sites.
    - Administrators can enable L2 flooding to handle silent medical devices as well as broadcast, unknown unicast, and multicast (BUM) traffic within fabric sites.

- Monitor a network and its clients using Cisco DNA Assurance and Analytics:
    - Administrators can use Assurance to monitor network health and identify network issues. Assurance can report issues triggered by various network failures including link down, AP down, and switch stack member down.
    - Administrators can use Assurance to monitor the health of wired and wireless clients and identify client onboarding issues.
    - Administrators can enable Telemetry Data Logger (TDL)-based assurance for better scale and performance when reporting client health.
    - Administrators can monitor a large number of concurrent endpoints, with Assurance charts displaying information for 100,000 concurrent endpoints and 250,000 transient endpoints.
    - Administrators can use Cisco AI Endpoint Analytics to identify and profile endpoints and IoT devices.
    - Administrators can monitor wireless network performance using wireless sensors.
    - Administrators can enable application telemetry and use Assurance to monitor application health for latency, jitter, and packets drops.
    - Administrators can visualize communications between existing endpoints to assess the need for and the impact of introducing new access controls.
    - Administrators can use Cisco AI Endpoint Analytics to detect spoofed endpoints (based on endpoints classification and behavioral model learning) and take the appropriate action.
    - Administrators can use GBPA capabilities to view traffic patterns and protocols, as well as create and implement microsegmentation policies to allow or disallow traffic flows.

Solution Environment

Topology

The test topology for the Cisco SD-Access Healthcare Vertical solution includes two Cisco DNA Center three-node clusters, which manage hospital region 1 and region 2 respectively. They are configured as Multiple Cisco DNA Center and integrated with the same distributed ISE cluster. The Cisco-distributed ISE cluster deployment includes two Policy Administration Nodes (PAN), two Monitoring Nodes (MnT), pxGrid, and multiple Policy Service Nodes (PSN).

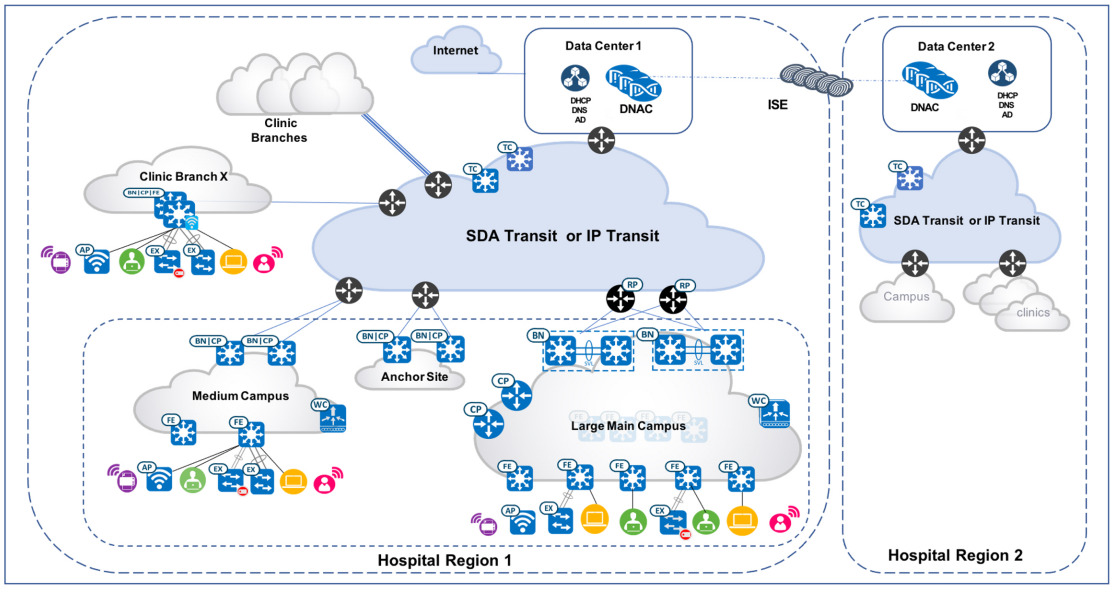
Each Cisco DNA Center cluster manages a fabric consisting of one large-scale hospital main campus site, one medium-scale campus site, one Anchor Site, and 500 small-scale clinic branch sites with Fabric-in-a-box (FiaB). Cisco SD-Access transit is deployed to connect distributed campuses. Remote clinic branches are connected to the main campus via IP networks. Figure 1 illustrates the logical topology of the Cisco SD-Access Healthcare Vertical solution test bed.

The fabric's sites are described below:

- The Large Campus Main site has dual borders, dual dedicated control plane nodes, dual WLC, and 100 fabric edges.
- The Medium site has dual colocated border and control plane nodes, WLC, fabric edges, and extended nodes.
- The Small sites have FiaB on hardware stacking with embedded WLC and extended nodes.
- The Anchor Site has dual colocated anchor borders and control plane nodes and provide anchored service across multiple fabric sites.
- Cisco SD-Access Transit is implemented with dual transit control plane nodes. Main Campus site borders are configured to provide internet access to other campus sites via Cisco SD-Access Transit.

In the following deployment example, Cisco SD-Access multicast with external RP is configured and the server room that resides within the fabric is deployed across multiple campus sites. The large fabric site deploys native multicast to achieve the best possible network performance. The smaller fabric site deploys headend multicast to simplify site management.

Figure 1: Solution Test Logical Topology



Scale

Solution test verified the scale numbers listed in the following table. To view the scale numbers for the Cisco DNA Center appliance, see the Cisco DNA Center Data Sheet.

Category	Value
Device inventory	5,000
Number of devices per fabric site	100
Multiple Cisco DNA Center appliances	2
Number of buildings and floors	2000
Number of VNs per fabric site	64

Category	Value
Number of IP pools per fabric site	500
Number of WLCs per fabric site	2
Number of fabric sites	502
Number of APs in inventory	13000
Number of endpoints	100,000 (50,000 wired, 50,000 wireless)
Number of SSIDs	10
Number of SGTs	4000

Solution Key Notes

This section describes the key technical notes for the Cisco SD-Access Healthcare Vertical profile's solution validation.

Incremental Site Deployment and Expansion

Healthcare networks naturally have a high number of sites, and the demand for network expansion to new locations is constant. Cisco DNA Center automation workflows provide a cost-effective, flexible, and scalable solution to deploy new fabric sites with Cisco SD-Access enabled in multiple locations. The Cisco SD-Access Healthcare Vertical solution executed the following workflows to expand new Cisco SD-Access sites:

- **Main Site provides internet access and shared services to distributed campuses via Cisco SD-Access Transit**: Newly deployed fabric sites need to be able to reach the following domains: shared service (such as Cisco DNA Center, Cisco ISE cluster, DNS, AD and DHCP servers), service within the same VN across fabric sites, and internet access. Cisco DNA Center provides an optimized and scalable solution with Cisco SD-Access Transit, which seamlessly enable full reachability for the new fabric site.
    - **Enable internet access for new fabric sites:** In a typical large medical deployment, the Headquarters or Main Campus sites access the internet via borders that are connected directly to the internet or through data center firewalls. To simplify new fabric deployment, Cisco DNA Center provides the following option in the border configuration workflow: `This site provides internet access to other sites through SDA Transit`. By checking this check box, the local site border will act as the default gateway—not just for the local site, but also for all other fabric sites connected via Cisco SD-Access Transit within the same fabric domain. In large healthcare deployments, just like any large campus, the site borders in the Main Campus site are configured with the following option selected: `This site provides internet access to other sites through SDA Transit`. For any new fabric site that is deployed, it will immediately be able to route any unknown traffic or internet access via the site border in the Main Campus site. The following two figures illustrate the GUI workflow and packet flow showing the Main Campus site providing the internet access to distributed sites.

Figure 2: Provide Internet Access for Remote Sites GUI

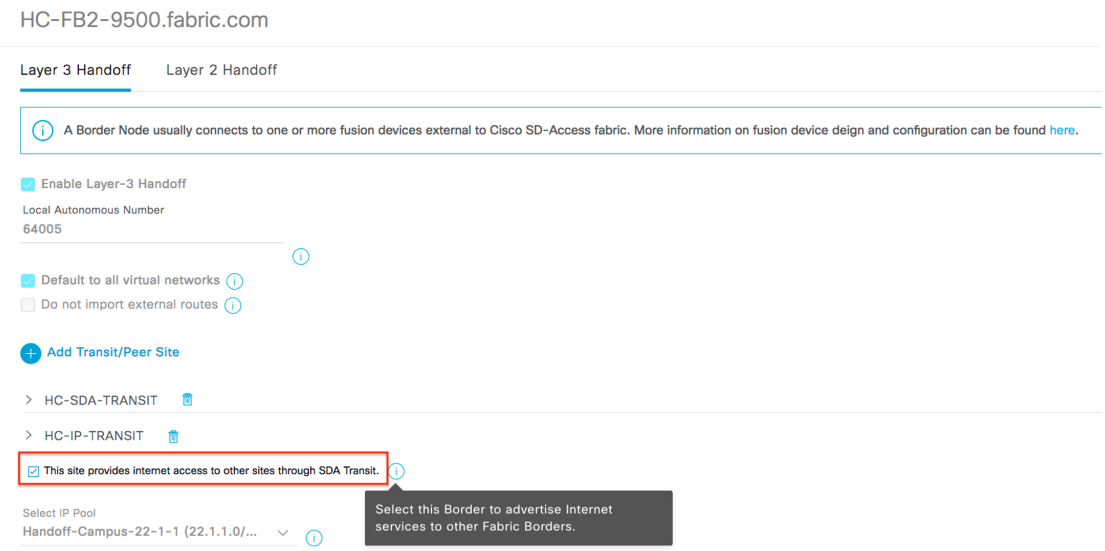
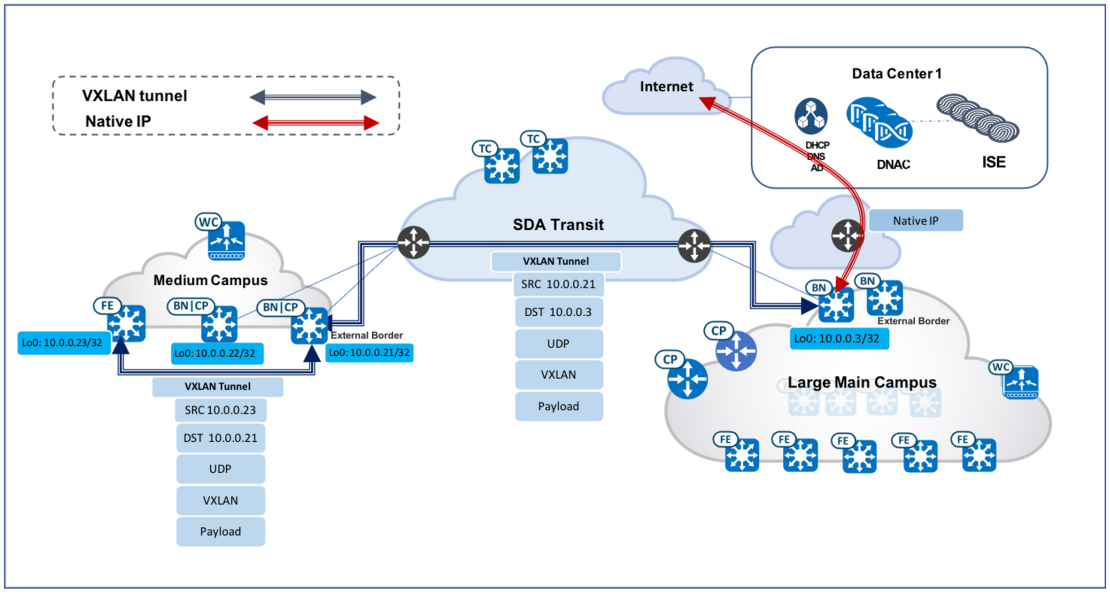


Figure 3: Packet Flow of Internet Access in Distributed Campus Site Via Cisco SD-Access Transit



- **Enable Cisco SD-Access Transit:** When setting up site borders for a new campus site, enable Cisco SD-Access Transit and specify Transit Control Plane Nodes. For a generic workflow that enables Cisco SD-Access, refer to Cisco Software-Defined Access for Distributed Campus Prescriptive Deployment Guide. Transit Control Plane nodes take care of interfabric communication and associate the aggregate prefixes with a border node's RLOC. Site-local Control Plane nodes take care of intrafabric communication and associate the endpoint identity (EID) with a fabric edge node. Intersite data traffic is encapsulated between sites using the fabric VXLAN encapsulation carrying macro (VN) and micro (SGT) policy constructs. With Cisco SD-Access Transit enabled, newly deployed fabric sites can communicate across sites for services within the same VN. These new sites can also access shared services at a central fabric site through proper route leaking between VNs.

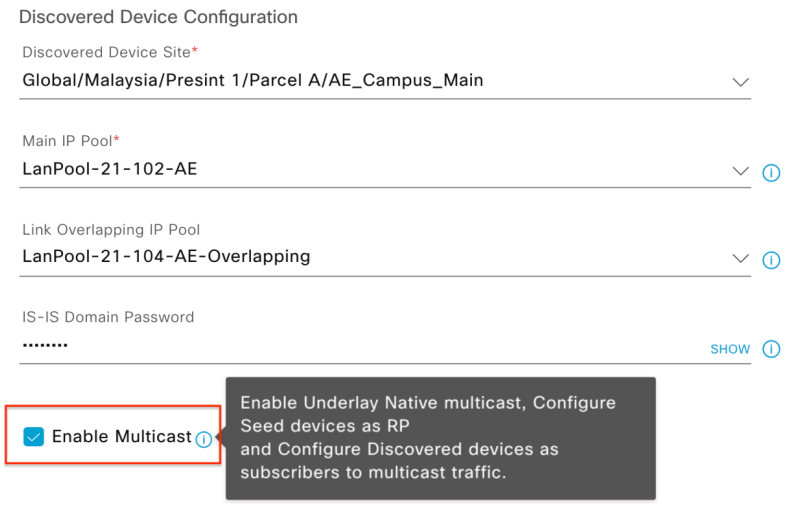
- **Uncarpeted space expansion**: Healthcare has undergone dramatic changes at care delivery sites, especially while dealing with COVID-19. As a result, healthcare systems have been moving medical services to outdoor spaces like parking lots and warehouses. Cisco SD-Access extended nodes enable mobility by offering a Layer 2 port extension and increasing the port density to existing fabric edge nodes, while also providing segmentation and group-based polices to the endpoints connected to these switches. Cisco DNA Center provides a zero-touch plug-and-play automated workflow to discover, provision, and add extended nodes to the fabric.

  Cisco DNA Center has two different support options for extended nodes: classic extended nodes (ENs) and policy extended nodes (PENs). In addition to the operation and management provided by classic extended nodes, PENs directly support SGT policy enforcement with SGACLs. This local support of SGACLs provides direct east-west traffic enforcement on PENs.

  Extended nodes are connected to a single fabric edge switch through an 802.1Q trunk port. This port can be deployed as an EtherChannel if two or more links are aggregated at the upstream fabric edge. Cisco DNA Center automates the trunk and the creation of the EtherChannel. After extended nodes have been onboarded through the workflow, endpoints (including fabric-mode APs and other Power over Ethernet (PoE) devices) can connect directly to the extended node, expanding the wired and wireless services to uncarpeted spaces as needed. For Cisco SD-Access extended node deployment details, see the Cisco Extended Enterprise Non-Fabric and SD-Access Fabric Design Guide.

- **Underlay multicast enablement**: Enabling multicast in the physical underlay network is essential to future fabric multicast service deployment. We highly recommend that you enable underlay multicast during the LAN Automation workflow. This workflow provides the option to automate the underlay PIM-ASM configuration for new devices. The workflow creates a Loopback60000 on seed devices and uses this address as the default RP for the underlay multicast network. The following figure shows the GUI screen from which you can enable underlay multicast in the LAN Automation workflow.

Figure 4: Enable Underlay Multicast in LAN Automation



Anchored Services for Wired and Wireless Hospital Endpoints

Healthcare customers often need to manage extensive guest services across all of their sites. Guest endpoints (which are bound to each individual fabric site) typically get IP addresses from the local site address pool and direct all traffic towards the local site borders. This adds complexity for address management and policy enforcement across multiple sites. To address this challenge, Cisco DNA Center provides the Multisite Remote Border solution that utilizes VN anchors. This solution allows traffic from a VN at multiple sites to be aggregated back to a central location (an anchor site) using a single common subnet, rather than having to define and use per-site subnets for that VN. With a simplified and centralized subnet structure, VN anchors facilitate guest service deployments across multisites. They also provide consistent and secure segmentation for guest traffic in large-scale healthcare environments.

Using anchored service, traffic for all of the endpoints belonging to the anchored VN at each site is aggregated and tunneled back to the central anchor border residing at the anchor site over VXLAN. While an anchor site functions very much like a traditional fabric site, it forms a virtual fabric site serving a particular VN. This virtual fabric site has its own site border and control plane (anchor border and CP), which are located at the anchor site. What is special about the anchor site is that the edges and wireless controller for this site are dispersed across multiple fabric sites.

Multisite Remote Border is enabled on a per-VN basis. For an anchored VN (such as Guest_VN), all edges at anchoring sites use the anchor CP/border for control and data plane communication. Wireless controllers at the anchoring sites communicate with the anchor CP for wireless endpoint registration. For nonanchored traditional VNs, edges and wireless controllers use their own site-local CP/border for control and data plane communication. Like other RLOCs of devices operating in a fabric role, the Loopback 0 address of the anchor border/CP node must be reachable via a /32 route in the global routing table of the edge nodes residing at the anchoring sites.

When a wireless guest has Multisite Remote Border enabled, the guest endpoint joins the guest SSID, completes Central Web Authentication (CWA) via Cisco ISE, and is then associated with the anchored guest VN. Guest traffic is tunneled to the anchored border and makes its way to the internet through a firewall. The first figure shows the Cisco DNA Center GUI screens from which you can enable Multisite Remote Border. The second figure illustrates the packet flow of both an anchored and unanchored VN.

Figure 5: Enable VN Anchoring

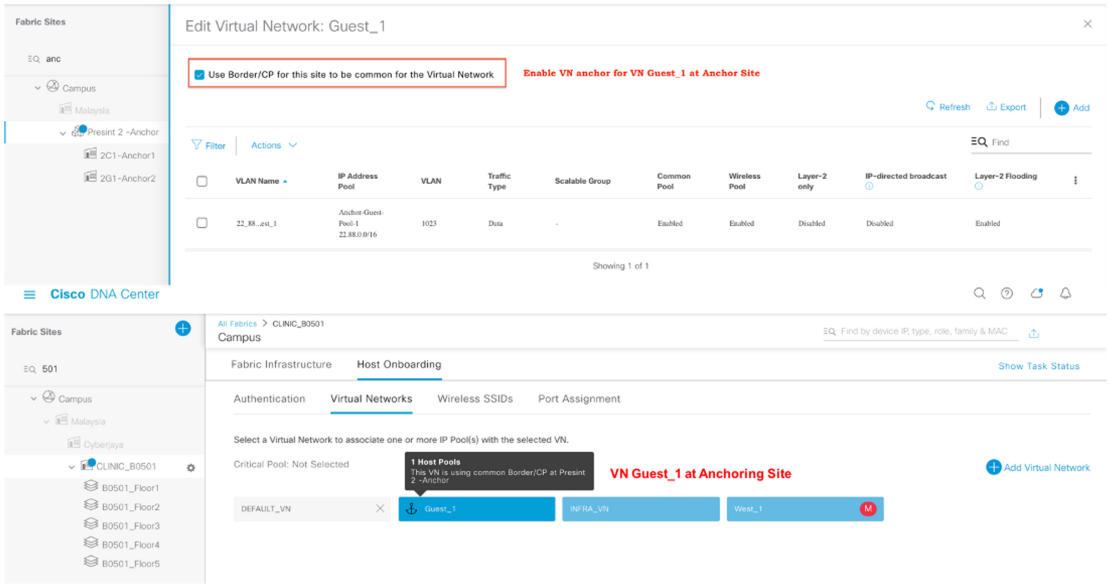
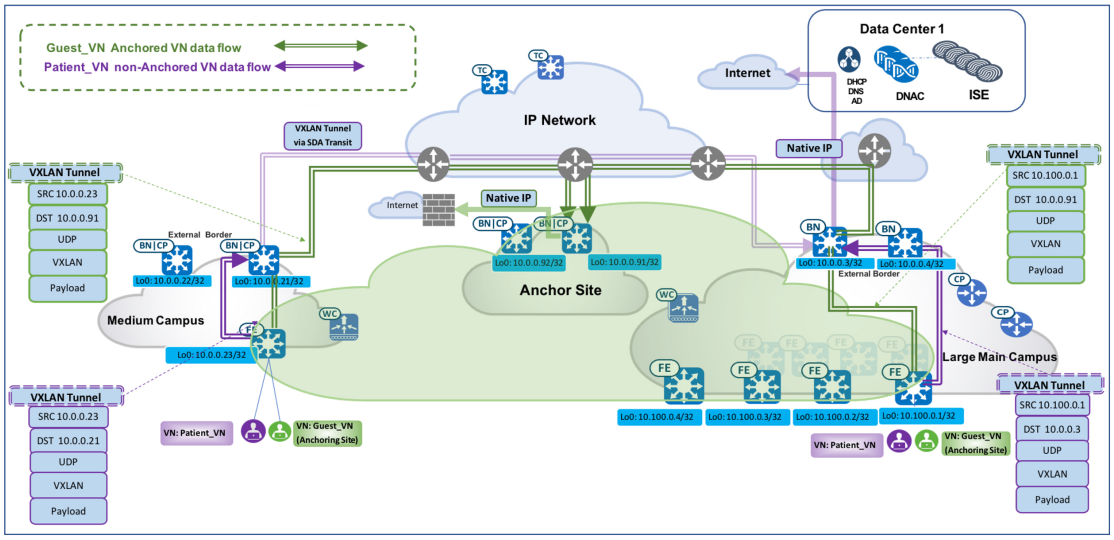


Figure 6: Data Packet Flow for an Anchored and Non-Anchored VN



Medical Server Room: Multicast Across Multiple Sites

Cisco SD-Access supports Multicast PIM Any-Source Multicast (PIM-ASM) and PIM Source-Specific Multicast (PIM-SSM) in both the virtual overlay network and physical underlay network. The multicast source can either be outside of the fabric domain (typically in the data center) or within the fabric overlay (typically connected directly to an edge node or extended node). Multicast receivers are usually connected directly to edge nodes or extended nodes across all fabric sites.

Cisco DNA Center offers two different multicast forwarding methods, tailored for different customer network designs on a per-VN basis. The first method is headend multicast (or ingress replication), which offers a clean overlay-only multicast forwarding solution as it does not require multicast in the underlay network. The second method is native multicast, which offers the most scalable bandwidth and CPU efficiency as the multicast replication is done throughout the underlay network.

Note Even though multicast forwarding is enabled on a per-VN basis, the two forwarding methods are mutually exclusive within a given fabric site.

The Cisco SD-Access Healthcare Vertical design has validated the following use case scenario, which demonstrates a multicast deployment in a large-scale multisite hospital network using Cisco DNA Center. In this scenario, a medical server room is connected to a fabric edge in the overlay at the Large Main Campus site. The servers in the server room are the multicast sources and could be in different VNs, servicing different medical audiences such as patients, administrators, medical staff, or medical school interns. The receivers are located across distributed campus sites. In Figure 7, multicast receivers reside in the hospital's Large Main Campus site as well as its Medium Campus site. The Rendezvous Point (RP) is placed outside of the fabric, so it can consistently serve both existing and newly-deployed fabric sites.

Multicast use cases cover the following requirements:

- Multiple servers (multicast sources) in different VNs are connected to a single fabric edge via the trunk port at the Large Main Campus site.
- Multicast receivers from the same Campus site where the multicast source resides are deployed.
- Multicast receivers from campus sites different from the one where the multicast source resides are deployed.

- Cisco SD-Access Transit is deployed across distributed campus sites.
- The multicast RP is located outside of the fabric.

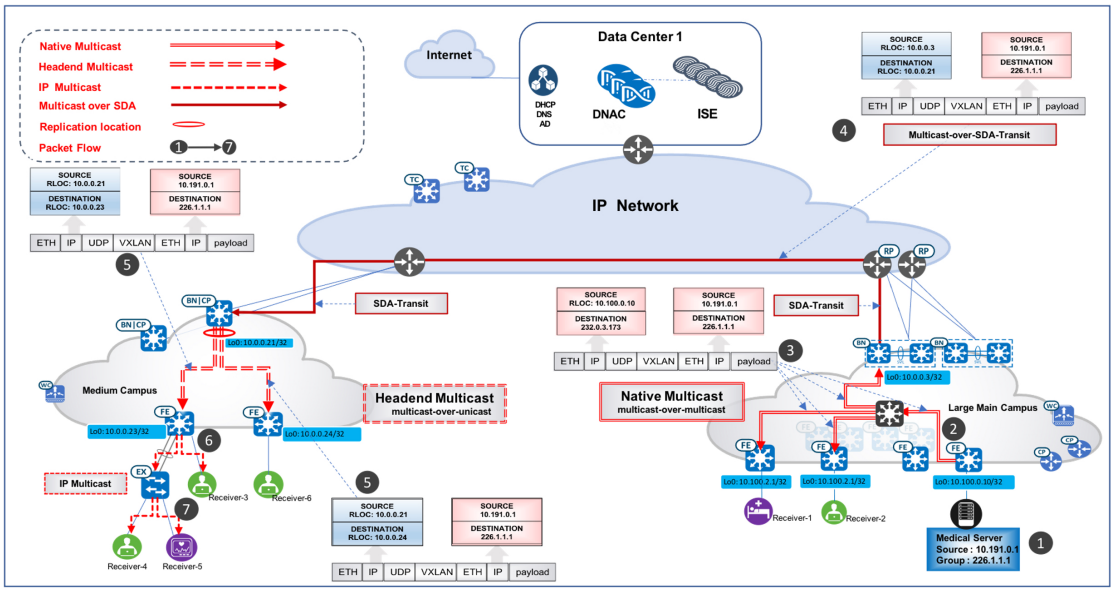
The following solutions have been validated and fulfill these requirements:

- **Deploy trunk port for server connection**: The fabric host onboarding port-assignment workflow provides the option to configure the connected device type as the trunk. As a result, the switch port on the edge or extended node is configured as the trunk. This allows the servers in the server room to connect to fabric edges with different VLAN tags.
- **Deploy multicast with headend replication (PIM-ASM in overlay)**: As mentioned earlier, headend replication for multicast runs on the overlay network and performs multicast-in-unicast encapsulations. In this service room case, the distributed site border will be the First Hop Router (FHR) and replicate each multicast packet in the overlay (S, G). It sends packets via unicast over the VXLAN tunnel (FHR_RLOC, LHR_RLOC) to all Last Hop Routers (LHR) which have the interested subscribers. For a small campus site, the edges are often directly connected to the fabric borders. With its lean and simple topology, this option is ideal for small fabric sites as it doesn't add too much bandwidth overhead on the site borders (FHR). It also has significantly less operational overhead, as it does not require the setup of underlay multicast.

  In a case where there are multiple receivers connected to an extended node (with the IGMP snooping function enabled by default), extended nodes complete packet replication on all the ports where the receivers are connected. Figure 7 illustrates the detailed packet data path in the small fabric site using headend replication as the transport option.
- **Deploy native multicast (PIM-ASM in overlay, PIM-SSM in underlay)**: Native multicast does not rely on the FHR to replicate packets. The entire underlay, including intermediate nodes, is participating in packet replication. Packets get replicated wherever there is a branch-out point on the underlay Source Specific Multicast (SSM) tree. In other words, packets get replicated at the closest node to the receivers and are replicated only when it is necessary. This option is ideal for large campus sites, as it provides the most bandwidth and CPU efficiency for the FHR and the rest of the network.

  Native multicast requires PIM-SSM for the underlay multicast transport and performs multicast-over-multicast encapsulations at the FHR. In this particular server room case, as multicast sources (medical servers) are connected to the edge, the fabric edge is the FHR. When the FHR receives the multicast packet on the overlay (S_overlay, G_overlay), it tunnels this packet as the payload in underlay multicast packets (S_underlay, G_underlay). From there, it uses the underlay SSM tree to complete packet replication. Figure 7 illustrates the detailed packet data path in the Main Campus site using Native Multicast as the transport option.
- **Multicast Across Fabric Sites via SD-Access Transit**: Distributed healthcare campus sites communicate with the RP and Multicast source through Cisco SD-Access Transit. PIM packets are first sent to the local campus site borders and are then tunneled to the Main Campus site borders via VXLAN. The Main Campus site border then forwards the PIM packets to the RP (outside of the fabric, in this case) through IP transit or forwards it to the edge where the source (medical server) is located through VXLAN. Multicast data forwarding across sites uses Cisco SD-Access Transit as well. Figure 7 depicts the detailed multicast data packet path sourced from the Medical Server within the Large Main Campus site, with the receivers at both the Large Main Campus site and the Medium Campus site.

Figure 7: Multicast Data Packet Path Across Cisco SD-Access Multisites: Server Room on Fabric Edge



Migration to Telemetry-Based Assurance

Healthcare organizations manage a large number of medical devices and users. Checkup rooms, treatment rooms, and consulting rooms are equipped with many device terminals and monitors. For fabric-wired endpoints, Cisco DNA Center typically uses inventory and SNMP-based polling methods to retrieve, monitor, and report the health data that's provided in Cisco DNA Assurance health pages. Starting with version 2.1.2.0, Cisco DNA Center leverages telemetry over NETCONF to support assurance data collection. This new method, Telemetry Data Logger (TDL)-based wired assurance, is recommended for monitoring wired client health as it provides better scale and performance and more real-time status reporting. The Cisco SD-Access Healthcare Vertical has successfully migrated from inventory to TDL-based assurance for 50,000 wired fabric clients in the current Cisco DNA Center release.

Migrating to TDL-based assurance on fabric devices also enables Power Over Ethernet (PoE) telemetry and analytics in the network. The following categories can be monitored for PoE-capable devices in the Cisco DNA Assurance PoE page: PoE Operational State Distribution, PoE Powered Device Distribution, Power Load Distribution, and PoE Insights. This information offers comprehensive insights into the power distribution and power usage details for all PoE devices across all sites in the network.

Related Cisco SD-Access Documentation

- Cisco SD-Access Solution Design Guide (CVD)
- Cisco Software-Defined Access for Distributed Campus Prescriptive Deployment Guide
- Cisco Extended Enterprise Non-Fabric and SD-Access Fabric Design Guide
- Cisco Software-Defined Access Compatibility Matrix

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

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

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.