The Cisco Catalyst SD-WAN Solution

The Cisco Catalyst SD-WAN Solution

Table 1: Feature History

Feature Name	**Release Information**	**Feature Description**
Support for the TLS 1.3 Protocol for Cisco Catalyst SD-WAN Control Connections	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature adds support for the Transport Layer Security (TLS) 1.3 protocol for Cisco Catalyst SD-WAN control connections.

Cisco Catalyst SD-WAN Solution

The Need for Cisco Catalyst SD-WAN Solution

Legacy networking technology has become increasingly expensive and complex, and it cannot scale to meet the needs of today's multisite enterprises. The Cisco Catalyst SD-WAN Solution, which is based on time-tested and proven elements of networking, offers an elegant, software-based solution that reduces the costs of running enterprise networks and provides straightforward tools to simplify the provisioning and management of large and complex networks that are distributed across multiple locations and geographies. Built in to the Cisco Catalyst SD-WAN Solution are inherent authentication and security processes that ensure the safety and privacy of the network and its data traffic.

Cisco Catalyst SD-WAN Solution represents an evolution of networking from an older, hardware-based model to a secure, software-based, virtual IP fabric. Cisco Catalyst SD-WAN fabric, also called an *overlay network*, forms a software overlay that runs over standard network transport services, including the public Internet, MPLS, and broadband. The overlay network also supports next-generation software services, thereby accelerating your shift to cloud networking.

Challenges in Legacy Network Design

The traditional approach to network design cannot scale to meet today's needs for four fundamental reasons:

- Cost: Legacy networks run on expensive hardware such as routers and switches, which require time-consuming configuration and maintenance. In addition, these networks require expensive transport connections or carrier circuits to secure and segment the network.
- Complexity: Legacy networks operate on the old model of a distributed control plane, which means that every node in the network must be configured with routing and security rules. Remote site management, change control, and network maintenance represent major logistical challenges.
- Lengthy installation times: Legacy networks that run on dedicated carrier circuits depend on the carrier to install new circuits, which can take several months. This can dramatically delay the launch of new branch locations.
- Control: Legacy networks that run on carrier circuits sacrifice control to the ISP, from network design to configuration to monitoring. Requesting changes from the ISP also requires extra time and is prone to communication errors.

Cost and complexity become even more prohibitive for legacy networks in the face of today's requirements, including:

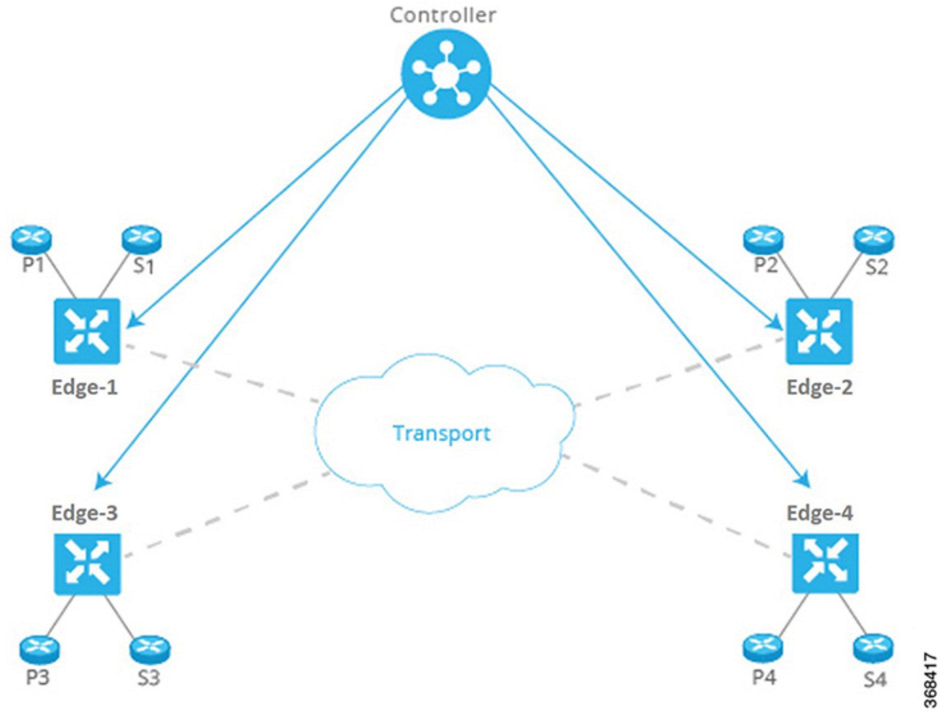
- Rigorous end-to-end security
- Disparate transport networks
- High-bandwidth cloud applications that are hosted in multiple data centers
- Ongoing increase in the number of mobile end users
- Any-to-any connectivity over fluid topologies
- Unique needs of particular businesses

Cisco Catalyst SD-WAN Solution

The Cisco Catalyst SD-WAN solution is a Software-Defined WAN (SD-WAN). As with all SD-WANs, it is based on the same routing principles that allowed the Internet to scale during the 1990s and 2000s. What separates Cisco Catalyst SD-WAN from other SD-WANs is that it reimagines the WAN for a new generation of enterprise networks, separating the data plane from the control plane and virtualizing much of the routing that used to require dedicated hardware.

The virtualized network runs as an overlay on cost-effective hardware, whether physical routers or virtual devices. Centralized controllers, called Cisco SD-WAN Validators, oversee the control plane of the fabric, efficiently managing provisioning, maintenance, and security for the entire Cisco Catalyst SD-WAN overlay network. Another device, called the Cisco SD-WAN Validator, automatically authenticates all other Cisco vEdge devices when they join the Cisco Catalyst SD-WAN overlay network.

Figure 1: Components of the Cisco Catalyst SD-WAN Solution



This division of labor allows each networking layer to focus on what it does best. The control plane manages the rules for the routing traffic through the overlay network, and the data plane passes the actual data packets among the network devices. The control plane and data plane form the warp and weft of a flexible, robust fabric that you weave according to your needs, on your schedule, over existing circuits.

Cisco SD-WAN Manager provides a simple, yet powerful, set of graphical dashboards for monitoring network performance on all devices in the overlay network, from a centralized monitoring station. In addition, Cisco SD-WAN Manager provides centralized software installation, upgrade, and provisioning, whether for a single device or as a bulk operation for many devices simultaneously.

Cisco Catalyst SD-WAN is ideally suited to the needs of cloud networking. Cisco Catalyst SD-WAN virtual IP fabric supports software services that streamline and optimize cloud networking, allowing you to take full advantage of the power of the overlay network for individual cloud applications.

Note

- Cisco SD-WAN Controllers are purpose-built, custom stacks. Although open-source Linux components are used, our custom operating system stacks bear no resemblance to the open-source Linux components used. The Linux components are not subject to the same hardening requirements as the custom operating system stacks that they are used in.
- The root access is disabled on Cisco SD-WAN Controllers and cannot be accessed from the user space.
- We meet compliance standards and requirements, such as, FedRAMP, FIPS, and CC. This compliance should be considered as proof of the security validation of our operating systems.
- We follow a secure development lifecycle outlined here.
- We also follow a well-defined process run by the Cisco Product Security Incident Response Team (PSIRT) to address any new exploits or attacks, such as, CVE.
- If you are still concerned about the platform security of Cisco SD-WAN Controllers, we recommend that you conduct an independent penetration testing through third parties.

The Virtual IP Fabric

The complexity in legacy enterprise networks stems from three main sources:

- There is no clear separation between entities that exchange data traffic and the transport network that binds these entities together. That is, there is no clear separation between hosts, devices, and servers on the service side of the network and the interconnects between routers on the transport side of the network.
- Policy and control decisions are embedded at every hop across the enterprise network.
- Security is a time-intensive, manual process, and security management must be implemented either at every node in the network or by using centralized security servers to manage group keys.

Cisco Catalyst SD-WAN uses time-tested and proven elements of networking in innovative ways to build the secure, virtual IP fabric. These networking elements include:

- Using routing and routing advertisements to establish and maintain the flow of traffic throughout the network.
- Layer 3 segmentation, sometimes called virtual routing and forwarding (VRF), to isolate different flows of traffic. This is useful to separate traffic from different customers or different business organizations within an enterprise.
- Peer-to-peer concepts to set up and maintain bidirectional connections between pairs of protocol entities
- Authentication and encryptions
- Policies for routing and data traffic

With five simple steps, Cisco Catalyst SD-WAN virtual IP fabric transforms a complex legacy network into an easy-to-manage, scalable network:

- Step 1: Separate transport from the service side of the network
- Step 2: Centralize routing intelligence and enable segmentation

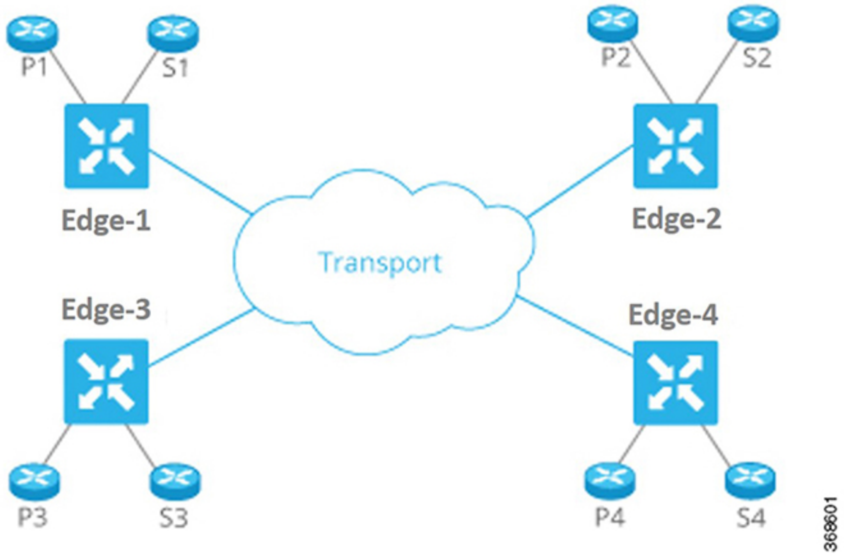
- Step 3: Secure the network automatically
- Step 4: Influence reachability through centralized policy
- Step 5: Simplify orchestration and provisioning

Step 1: Separate Transport from the Service Side of the Network

The job of the transport network is to carry packets from one transport router to another. The transport network needs to know only about the routes to follow to reach the next-hop or destination router. It need not know about the prefixes for nontransport routers, the routers that sit behind the transport routers in their local service networks.

Separating network transport from the service side of the network allows the network administrator to influence router-to-router communication independently of the communication between users or between hosts.

Figure 2: Transport Network Separated from Service Network



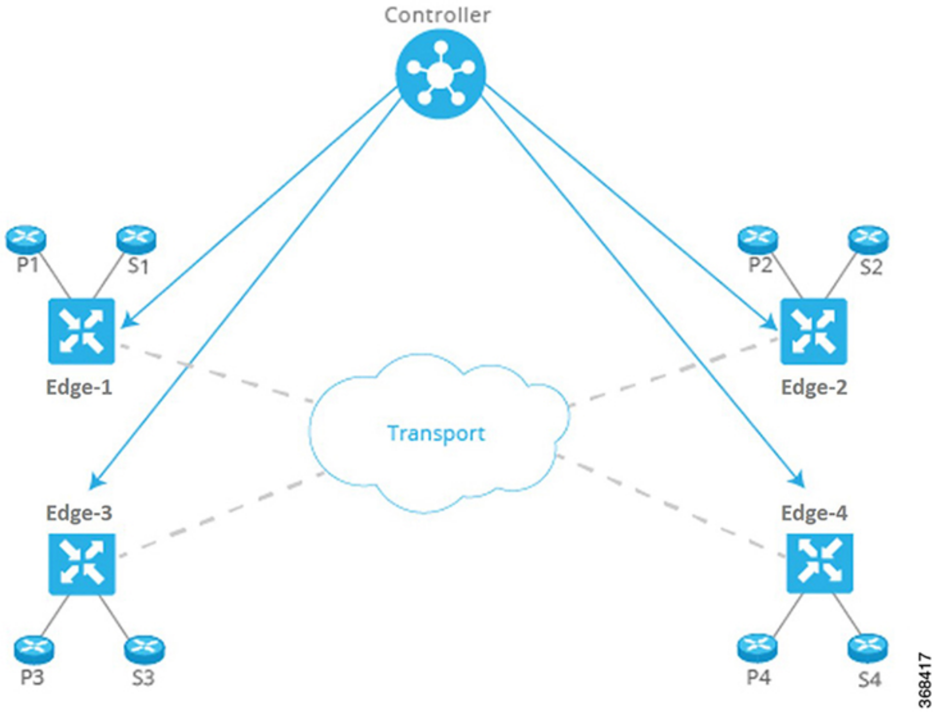
This approach has many benefits:

- The network administrator can choose transport circuits based on SLA and cost.
- The routing system can assign attributes to transport links for optimal routing, load balancing, and policy-based routing.

Step 2: Centralize Routing Intelligence and Enable Segmentation

Every router at the edge of a network has two sides for routing: one to the transport network and one to the service side of the network. To have any-to-any communication among all routers, all routers need to learn all prefixes. Traditionally, routers learn these prefixes using full-mesh IGP/BGP or by enabling routing on an overlay tunnel (for example, BGP or IGP over MPLS or GRE). Various techniques allow the scaling issues associated with full-mesh routing adjacencies to be mitigated or eliminated, such as employing a route reflector for BGP.

Figure 3: Centralizing Routing Intelligence with a Centralized Controller



The Cisco Catalyst SD-WAN fabric builds on the route reflector model by centralizing routing intelligence. Essentially, all prefixes learned from the service side on a router are advertised to a centralized controller, which then reflects the information to other routers over the network's control plane. The controllers do not handle any of the data traffic; they are involved only in control plane communication.

This approach has many benefits:

- The centralized controller can use inexpensive or commodity servers for control plane processing.
- The routers can use off-the-shelf silicon, allowing cost benefits from economies of scale.
- Scale challenges associated with full-mesh routing on the transport side of the network are eliminated.
- The network administrator can create multiple segments without the need for complex signaling protocols. For example, in the figure here, all Px prefixes can be part of one VPN, while all Sx prefixes can be part of a different VPN.

Note The centralized controller only “influences” routing on the routers. The controller does not participate in every flow going through the network, nor does it participate in routing on the service side. This design allows the routers to have local intelligence—enough intelligence to make local site decisions quickly.

Step 3: Secure the Network and Links Automatically

The Cisco Catalyst SD-WAN fabric identifies transport side links and automatically encrypts traffic between sites. The associated encryption keys are exchanged over a secure session with the centralized controller. Secure sessions with the controller are set up automatically using RSA and certificate infrastructure.

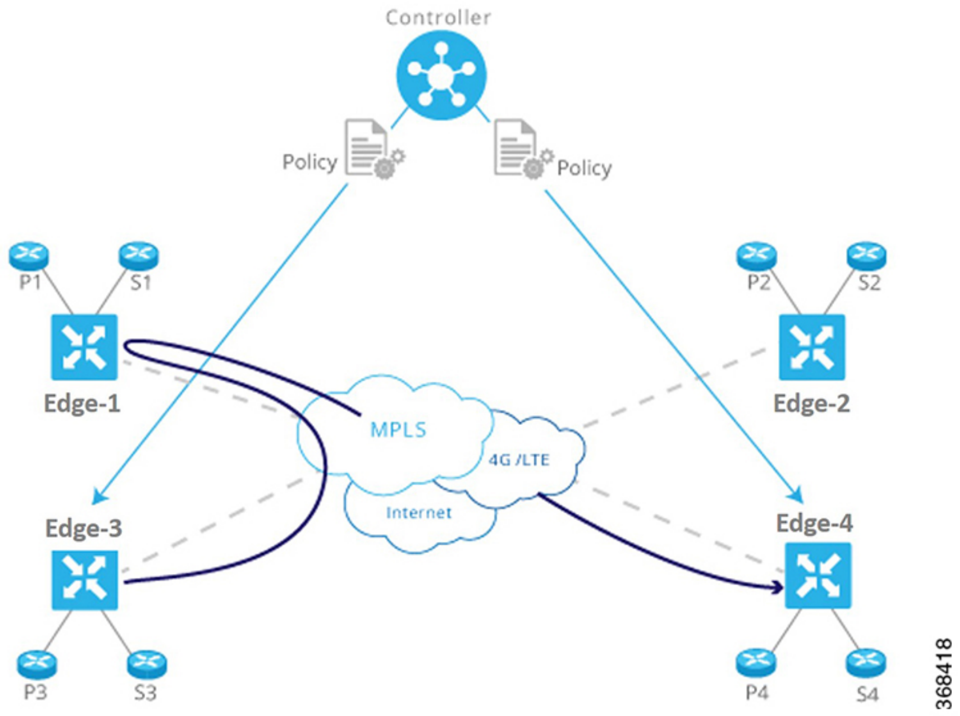
This approach has many benefits:

- The Cisco Catalyst SD-WAN fabric itself authenticates all devices participating in the network, which is an important step to secure the infrastructure.
- The fabric automatically exchanges encryption keys associated with the transport links, eliminating the hassle of configuring thousands of pair-wise keys.
- The fabric ensures that the network is not prone to attacks from the transport side.

Step 4: Influence Reachability through Centralized Policy

Policy configured on a centralized controller strongly influences how prefixes are advertised among the routers. For example, if all traffic between routers P3 and P4 in the figure here has to make a U-turn at router vEdge-1, the network administrator can apply a simple route policy on the centralized controller. The controller then passes the policy to the affected edge routers. The network administrator does not need to provision the policy on each individual router.

Figure 4: Policy Configured on a Centralized Controller



This approach has many benefits:

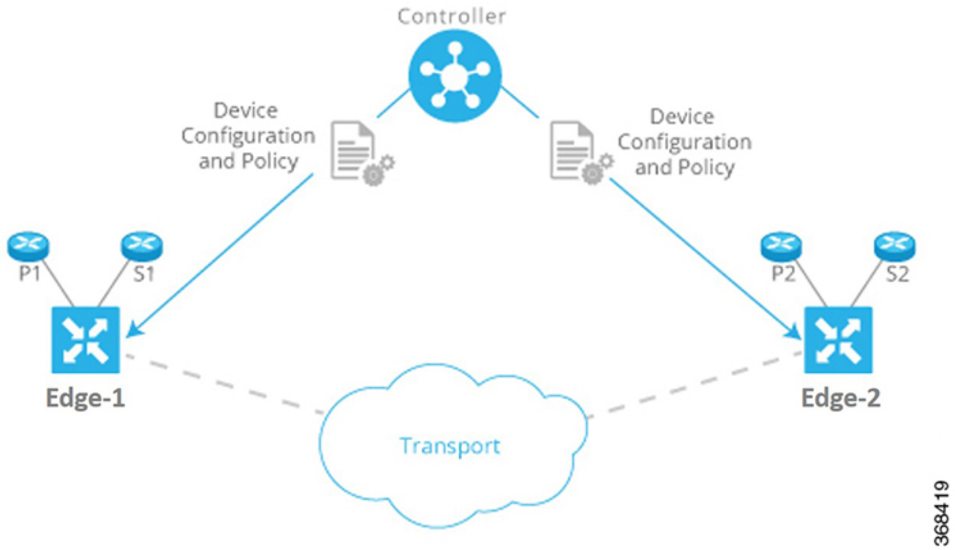
- The controller centrally influences access control, that is, which prefixes are allowed to talk to each other inside a VPN.

- The controller optimizes user experience by influencing transport link choice based on SLA or other attributes. The network administrator can color transport links (such as gold and bronze), and allow applications to map the colors to appropriate transport links.
- The network administrator can map business logic from a single centralized point.
- The network can react faster to planned and unexpected situations, such as routing all traffic from high-risk countries through an intermediate point.
- The network can centralize services such as firewalls, IDPs, and IDSs. Instead of distributing these services throughout the network at every branch and campus, the network administrator can centralize these functions, achieving efficiencies of scale and minimizing the number of touch points for provisioning.

Step 5: Simplify Provisioning and Management

Legacy network devices are provisioned and monitored manually through a CLI. Network administrators must type configurations line by line, and enter operational commands one at a time on individual devices in order to retrieve and read status information. This method is error prone and time consuming when provisioning and troubleshooting a network, and it can present serious difficulties when devices are in remote locations or when management ports are inaccessible.

Figure 5: Simplified Provisioning and Management of a Network by Cisco Catalyst SD-WAN


Controller
Device Configuration and Policy
Device Configuration and Policy
P1
S1
P2
S2
Edge-1
Edge-2
Transport
368419

Cisco Catalyst SD-WAN centralizes and significantly simplifies provisioning and management through Cisco SD-WAN Manager. Cisco SD-WAN Manager provides an easy-to-use, graphical dashboard from which you can monitor, configure, and maintain all Cisco vEdge devices and links in the overlay network. For example, the GUI dashboard provides a templated view of various configurations to ease provisioning a service, so all common elements, such as AAA and company-specific servers, can be pushed to multiple devices with a single click, from a single point.

This approach has many benefits:

- The network administrator provisions and manages the network as a whole, efficiently and easily, as opposed to a piece-meal approach that deals with individual devices one at a time.

- The network administrator has improved network visibility (for example, viewing network-wide VPN statistics) from a single point.
- Troubleshooting tasks are simplified and presented visually, instead of requiring network administrators to read lengthy configurations and output from individual devices.

Cisco Catalyst SD-WAN Components

Primary Cisco Catalyst SD-WAN Components

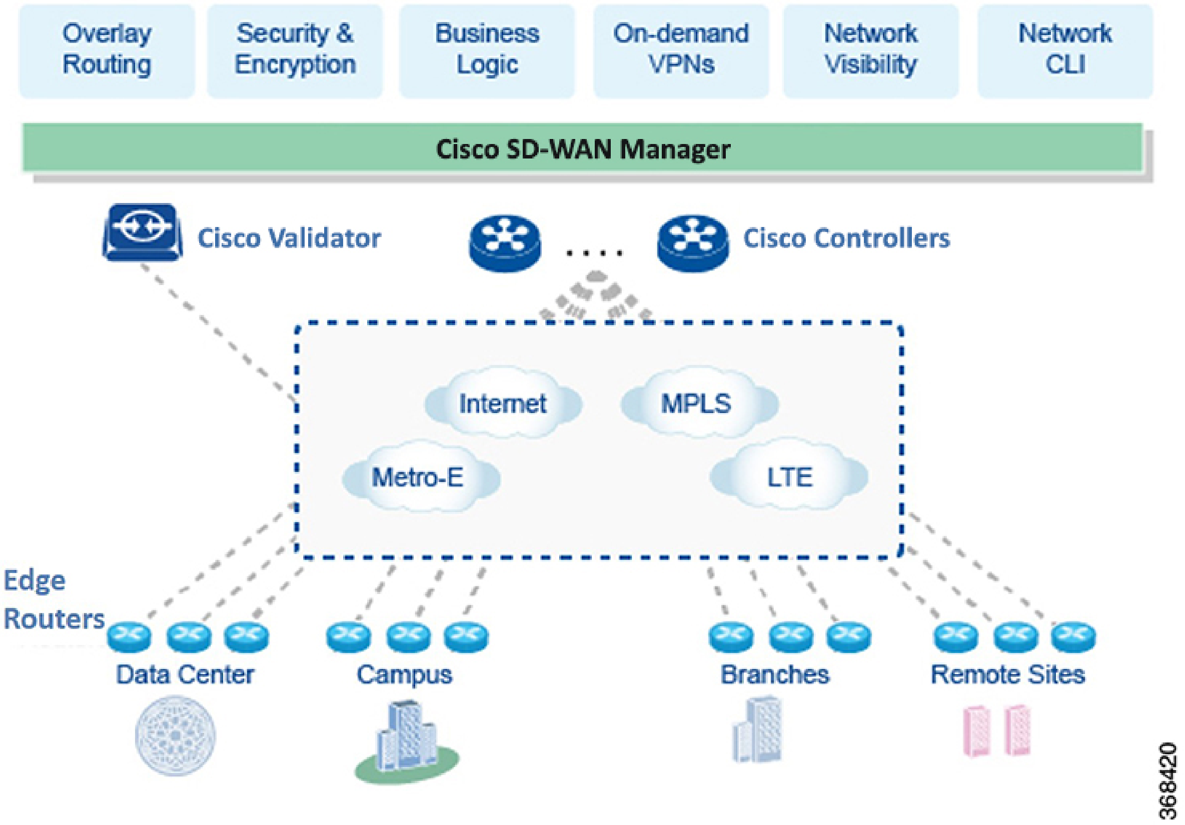
The secure, virtual IP fabric of Cisco Catalyst SD-WAN is made up of four fundamental components:

- **Cisco SD-WAN Manager**: Cisco SD-WAN Manager is a centralized network management system that lets you configure and manage the entire overlay network from a simple graphical dashboard.
- **Cisco SD-WAN Controller**: The Cisco SD-WAN Controller is the centralized brain of the Cisco Catalyst SD-WAN solution, controlling the flow of data traffic throughout the network. The Cisco SD-WAN Controller works with the Cisco SD-WAN Validator to authenticate Cisco vEdge devices as they join the network and to orchestrate connectivity among the edge routers.
- **Cisco SD-WAN Validator**: The Cisco SD-WAN Validator automatically orchestrates connectivity between edge routers and Cisco SD-WAN Controllers. If any edge router or Cisco SD-WAN Controller is behind a NAT, the Cisco SD-WAN Validator also serves as an initial NAT-traversal orchestrator.
- **Cisco IOS XE Catalyst SD-WAN and Cisco vEdge Devices**: The edge routers sit at the perimeter of a site (such as remote offices, branches, campuses, data centers) and provide connectivity among the sites. They are either hardware devices or software (Cloud router), that runs as a virtual machine. The edge routers handle the transmission of data traffic.

Of these four components, the edge router can be a Cisco Catalyst SD-WAN hardware device or software that runs as a virtual machine, and the remaining three are software-only components. The Cloud router, Cisco SD-WAN Manager, and Cisco SD-WAN Controller software runs on servers, and the Cisco SD-WAN Validator software runs as a process (daemon) on a edge router.

The figure below illustrates the components of Cisco Catalyst SD-WAN. The sections below describe each component in detail.

Figure 6: Components of Cisco Catalyst SD-WAN



Cisco Catalyst SD-WAN Manager

Cisco SD-WAN Manager is a centralized network management system. Cisco SD-WAN Manager dashboard provides a visual window into the network, and it allows you to configure and manage Cisco edge network devices. Cisco SD-WAN Manager software runs on a server in the network. This server is typically situated in a centralized location, such as a data center. It is possible for Cisco SD-WAN Manager software to run on the same physical server as Cisco SD-WAN Controller software.

You can use Cisco SD-WAN Manager to store certificate credentials, and to create and store configurations for all Cisco edge network components. As these components come online in the network, they request their certificates and configurations from Cisco SD-WAN Manager. When Cisco SD-WAN Manager receives these requests, it pushes the certificates and configurations to the Cisco edge network devices.

For Cloud routers, Cisco SD-WAN Manager can also sign certificates and generate bootstrap configurations, and it can decommission the devices.

Secure Communication with Devices and Controllers through a vmanage-admin Account

Cisco SD-WAN Manager communicates with edge devices and controllers using a secure channel—either a datagram transport layer security (DTLS) tunnel or transport layer security (TLS) tunnel. Within this secure channel, it communicates with the devices or controllers using the NETCONF protocol, within an SSH session. It uses an internal-use-only passwordless "vmanage-admin" user account on the device or controller. The vmanage-admin account is created during the initial device or controller setup. Cisco SD-WAN Manager uses this secure channel for monitoring, configuring, and managing each of the following:

- Edge devices
- Cisco SD-WAN Manager nodes in a cluster
- Cisco SD-WAN Validator
- Cisco SD-WAN Controllers

As noted, the vmanage-admin user accounts do not have any password associated with them, so Cisco SD-WAN Manager uses a passwordless procedure to log in to the account. To accomplish this, Cisco SD-WAN Manager generates an asymmetric encryption public-private key pair. During deployment of an edge device into the Cisco Catalyst SD-WAN fabric, or of a controller instance, Cisco SD-WAN Manager copies the public key that it has generated to the edge device or instance. It sends the public key using a proprietary protocol, within a secure channel—a DTLS or TLS tunnel.

The activity that Cisco SD-WAN Manager performs using the vmanage-admin account appears in syslog messages and in the output of certain **show** commands. The syslog messages are logged with the same level of detail as activities performed through any other user account. The level of syslog detail depends on the syslog configuration of the device.

Cisco SD-WAN Manager requires the vmanage-admin account on devices in the fabric in order to monitor, configure, and manage the devices. Removing, disabling, or altering this account on a device would prevent Cisco SD-WAN Manager from performing these activities, and is not supported.

Cisco Catalyst SD-WAN Controller

The Cisco SD-WAN Controller oversees the control plane of the Cisco Catalyst SD-WAN overlay network, establishing, adjusting, and maintaining the connections that form the Cisco Catalyst SD-WAN fabric.

The major components of the Cisco SD-WAN Controller are:

- Control plane connections: Each Cisco SD-WAN Controller establishes and maintains a control plane connection with each edge router in the overlay network. (In a network with multiple Cisco SD-WAN Controllers, a single Cisco SD-WAN Controller may have connections only to a subset of the edge routers, for load-balancing purposes.) Each connection, which runs as a DTLS tunnel, is established after device authentication succeeds, and it carries the encrypted payload between the Cisco SD-WAN Controller and the edge router. This payload consists of route information necessary for the Cisco SD-WAN Controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the Edge routers. The DTLS connection between a Cisco SD-WAN Controller and an edge router is a permanent connection. The Cisco SD-WAN Controller has no direct peering relationships with any devices that an edge router is connected to on the service side.
- OMP (Overlay Management Protocol): The OMP protocol is a routing protocol similar to BGP that manages the Cisco Catalyst SD-WAN overlay network. OMP runs inside DTLS control plane connections and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the Cisco SD-WAN Controller and the edge routers and carries only control plane information. The Cisco SD-WAN Controller processes the routes and advertises reachability information learned from these routes to other edge routers in the overlay network.
- Authentication: The Cisco SD-WAN Controller has pre-installed credentials that allow it to authenticate every new edge router that comes online. These credentials ensure that only authenticated devices are allowed access to the network.

- Key reflection and rekeying: The Cisco SD-WAN Controller receives data plane keys from an edge router and reflects them to other relevant edge routers that need to send data plane traffic.
- Policy engine: The Cisco SD-WAN Controller provides rich inbound and outbound policy constructs to manipulate routing information, access control, segmentation, extranets, and other network needs.
- Netconf and CLI: Netconf is a standards-based protocol used by Cisco SD-WAN Manager to provision a Cisco SD-WAN Controller. In addition, each Cisco SD-WAN Controller provides local CLI access and AAA.

The Cisco SD-WAN Controller maintains a centralized route table that stores the route information, called OMP routes, that it learns from the edge routers and from any other Cisco SD-WAN Controllers in the Cisco Catalyst SD-WAN overlay network. Based on the configured policy, the Cisco SD-WAN Controller shares this route information with the Cisco edge network devices in the network so that they can communicate with each other.

The Cisco SD-WAN Controller is a software that runs as a virtual machine on a server configured with ESXi or VMware hypervisor software. The Cisco SD-WAN Controller software image is a signed image that is downloadable from the Cisco Catalyst SD-WAN website. A single Cisco Catalyst SD-WAN root-of-trust public certificate is embedded into all Cisco SD-WAN Controller software images.

During the initial startup of a Cisco SD-WAN Controller, you enter minimal configuration information, such as the IP addresses of the controller and the Cisco SD-WAN Validator. With this information and the root-of-trust public certificate, the Cisco SD-WAN Controller authenticates itself on the network, establishes a DTLS control connection with the Cisco SD-WAN Validator, and receives and activates its full configuration from Cisco SD-WAN Manager if one is present in the domain. (Otherwise, you can manually download a configuration file or create a configuration directly on the Cisco SD-WAN Controller through a console connection.) The Cisco SD-WAN Controller is now also ready to accept connections from the edge routers in its domain.

To provide redundancy and high availability, a typical overlay network includes multiple Cisco SD-WAN Controllers in each domain. A domain can have up to 20 Cisco SD-WAN Controllers. To ensure that the OMP network routes remain synchronized, all the Cisco SD-WAN Controllers must have the same configuration for policy and OMP. However, the configuration for device-specific information, such as interface locations and addresses, system IDs, and host names, can be different. In a network with redundant Cisco SD-WAN Controllers, the Cisco SD-WAN Validator tells the Cisco SD-WAN Controllers about each other and tells each Cisco SD-WAN Controller which edge routers in the domain it should accept control connections from. (Different edge routers in the same domain connect to different Cisco SD-WAN Controllers, to provide load balancing.) If one Cisco SD-WAN Controller becomes unavailable, the other controllers automatically and immediately sustain the functioning of the overlay network.

Cisco Catalyst SD-WAN Validator

Cisco SD-WAN Validator automatically coordinates the initial bringup of Cisco SD-WAN Controllers and edge routers, and it facilities connectivity between Cisco SD-WAN Controllers and edge routers. During the bringup processes, the Cisco SD-WAN Validator authenticates and validates the devices wishing to join the overlay network. This automatic orchestration process prevents tedious and error-prone manual bringup.

Cisco SD-WAN Validator is the only Cisco vEdge device that is located in a public address space. This design allows the Cisco SD-WAN Validator to communicate with Cisco SD-WAN Controllers and edge routers that are located behind NAT devices, and it allows the Cisco SD-WAN Validator to solve any NAT-traversal issues of these Cisco vEdge devices.

The major components of the Cisco SD-WAN Validator are:

- Control plane connection: Each Cisco SD-WAN Validator has a persistent control plane connection in the form of a DTLS tunnel with each Cisco Catalyst SD-WAN Controller in its domain. In addition, the Cisco SD-WAN Validator uses DTLS connections to communicate with edge routers when they come online, to authenticate the router, and to facilitate the router's ability to join the network. Basic authentication of an edge router is done using certificates and RSA cryptography.
- NAT traversal: The Cisco SD-WAN Validator facilitates the initial orchestration between edge routers and Cisco SD-WAN Controllers when one or both of them are behind NAT devices. Standard peer-to-peer techniques are used to facilitate this orchestration.
- Load balancing: In a domain with multiple Cisco SD-WAN Controllers, the Cisco SD-WAN Validator automatically performs load balancing of edge routers across the Cisco SD-WAN Controllers when routers come online.

Cisco SD-WAN Validator is a software module that authenticates the Cisco SD-WAN Controllers and the edge routers in the overlay network and coordinates connectivity between them. It must have a public IP address so that all Cisco vEdge devices in the network can connect to it. (It is the only Cisco vEdge device that must have a public address.)

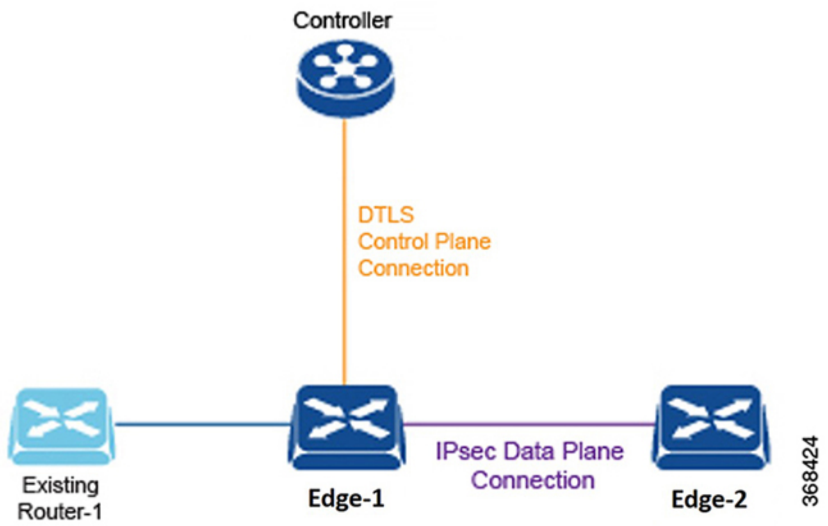
Cisco SD-WAN Validator orchestrates the initial control connection between Cisco SD-WAN Controllers and edge routers. It creates DTLS tunnels to the Cisco SD-WAN Controllers and edge routers to authenticate each node that is requesting control plane connectivity. This authentication behavior assures that only valid customer nodes can participate in the Cisco Catalyst SD-WAN overlay network. The DTLS connections with Cisco SD-WAN Controllers are permanent so that the Cisco SD-WAN Validator controller can inform the Cisco SD-WAN Controllers as edge routers join the network. The DTLS connections with edge routers are temporary; once the Cisco SD-WAN Validator has matched a edge router with a Cisco Catalyst SD-WAN Controller, there is no need for the Cisco SD-WAN Validator and the edge router to communicate with each other. The Cisco SD-WAN Validator shares only the information that is required for control plane connectivity, and it instructs the proper edge routers and Cisco SD-WAN Controllers to initiate secure connectivity with each other. The Cisco SD-WAN Validator maintains no state.

To provide redundancy for the Cisco SD-WAN Validator, you can create multiple Cisco SD-WAN Validator entities in the network and point all edge routers to those Cisco SD-WAN Validators. Each Cisco SD-WAN Validator maintains a permanent DTLS connection with each Cisco Catalyst SD-WAN Controller in the network. If one Cisco SD-WAN Validator becomes unavailable, the others are automatically and immediately able to sustain the functioning of the overlay network. In a domain with multiple Cisco SD-WAN Controllers, the Cisco SD-WAN Validator pairs a edge router with one of the Cisco SD-WAN Controllers to provide load balancing.

Cisco vEdge Devices and Cisco IOS XE Catalyst SD-WAN Devices

The edge router, whether a hardware or software device, is responsible for the data traffic sent across the network. When you place an edge router into an existing network, it appears as a standard router.

Figure 7: An Edge Router Placed into an Existing Network



To illustrate this, the figure here shows an edge router and an existing router that are connected by a standard Ethernet interface. These two routers appear to each other to be Layer 3 end points, and if routing is needed between the two devices, OSPF or BGP can be enabled over the interface. Standard router functions, such as VLAN tagging, QoS, ACLs, and route policies, are also available on this interface.

The components of an edge router are:

- DTLS control plane connection: Each edge router has one permanent DTLS connection to each Cisco SD-WAN Controller it talks to. This permanent connection is established after device authentication succeeds, and it carries encrypted payload between the edge router and the Cisco SD-WAN Controller. This payload consists of route information necessary for the Cisco SD-WAN Controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the edge routers.

- OMP (Overlay Management Protocol): As described for the Cisco SD-WAN Controller, OMP runs inside the DTLS connection and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the edge router and the Cisco SD-WAN Controller and carries only control information.

- Protocols: The edge router supports standard protocols, including OSPF, BGP, VRRP, and BFD.

- Routing Information Base (RIB): Each edge router has multiple route tables that are populated automatically with direct interface routes, static routes, and dynamic routes learned via BGP and OSPF. Route policies can affect which routes are stored in the RIB.

- Forwarding Information Base (FIB): This is a distilled version of the RIB that the CPU on the edge router uses to forward packets.

- Netconf and CLI: Netconf is a standards-based protocol used by Cisco SD-WAN Manager to provision a edge router. In addition, each edge router provides local CLI access and AAA.

- Key management: Edge routers generate symmetric keys that are used for secure communication with other edge routers, using the standard IPsec protocol.

- Data plane: The edge router provides a rich set of data plane functions, including IP forwarding, IPsec, BFD, QoS, ACLs, mirroring, and policy-based forwarding.

The edge router has local intelligence to make site-local decisions regarding routing, high availability (HA), interfaces, ARP management, ACLs, and so forth. The OMP session with the Cisco SD-WAN Controller influences the RIB in the edge router, providing non-site-local routes and the reachability information necessary to build the overlay network.

The hardware edge router includes a Trusted Board ID chip, which is a secure cryptoprocessor that contains the private key and public key for the router, along with a signed certificate. All this information is used for device authentication. When you initially start up a edge router, you enter minimal configuration information, such as the IP addresses of the edge router and the Cisco SD-WAN Validator. With this information and the information on the Trusted Board ID chip, the edge router authenticates itself on the network, establishes a DTLS connection with the Cisco SD-WAN Controller in its domain, and receives and activates its full configuration from Cisco SD-WAN Manager if one is present in the domain. Otherwise, you can manually download a configuration file or create a configuration directly on the edge router through a console connection.

Cisco Catalyst SD-WAN Control Connections

The following sections provide information about Cisco Catalyst SD-WAN control connections.

Information About Cisco Catalyst SD-WAN Control Connections

Cisco Catalyst SD-WAN control connections refer to the communication channels that control and manage the operation of a Cisco Catalyst SD-WAN network. These connections are established between Cisco Catalyst SD-WAN control components (Cisco Catalyst SD-WAN Validator, Cisco Catalyst SD-WAN Controller, Cisco SD-WAN Manager) and Cisco IOS XE Catalyst SD-WAN devices.

Support for the TLS 1.3 Protocol

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, the control connections in Cisco Catalyst SD-WAN support the Transport Layer Security protocol version 1.3. The TLS 1.3 version provides stronger security than TLS 1.2, thus improving network performance and efficiency.

If the Cisco Catalyst SD-WAN Control components are using Cisco Catalyst SD-WAN Control Components Release 20.13.1 or later, and devices are using Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, they establish a TLS 1.3 connection between them. In the absence of a TLS 1.3 connection, these components negotiate and establish a connection using TLS 1.2.

Cipher Suites

For control connections, Cisco Catalyst SD-WAN automatically selects one of the following cipher suites:

- TLS-AES-256-GCM-SHA384
- TLS-AES-128-GCM-SHA256
- TLS-AES-128-CCM-8-SHA256
- TLS-AES-128-CCM-SHA256

Benefits of TLS 1.3 in Cisco Catalyst SD-WAN Control Connections

- TLS 1.3 provides stronger security compared to TLS 1.2.
- TLS 1.3 reduces the number of round trips that are required for the initial connection setup (handshake). This reduces latency, and speeds up the establishment of a secure connection, improving overall performance.

Verify Cisco Catalyst SD-WAN Control Connections

The following is a sample output from the **show sdwan control connections** command that displays the connection status, including the TLS version and selected cipher suite. This command displays the information about active control connections and control plane connections on Cisco IOS XE Catalyst SD-WAN devices.

In the following command output, the protocol version (TLS 1.3) and cipher suite are shown in bold.

```
Device# show sdwan control connections

LOCAL-COLOR- lte SYSTEM-IP- 12.16.255.19 PEER-PERSONALITY- vsmart


site-id 100
domain-id 1 protocol tls
protocol-version TLS1_3
cipher-name TLS_AES_256_GCM_SHA384 private-ip 10.0.5.19
private-port 23556
public-ip 10.0.5.19
public-port 23556
org-name vIPtela Inc Regression
state up [Local Err: NO_ERROR] [Remote Err: NO_ERROR] uptime 0:00:01:24
hello interval 1000
hello tolerance 12000
controller-grp-id 0 shared-region-id-set N/A peer-session-id 0xdba4a2f8
Tx Statistics- hello 86
connects 0
registers 0
register-replies 0
challenge 0
challenge-response 1
challenge-ack 0
teardown 0
teardown-all 0
vmanage-to-peer 0
register-to-vmanage 0 Rx Statistics-
hello 86
connects 0
registers 0
register-replies 0
challenge 1
challenge-response 0

challenge-ack 1
teardown 0
vmanage-to-peer 0
register-to-vmanage 0
```

This command displays information about control plane connection attempts initiated by the local device on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan control connection-history detail
```

```
LOCAL-COLOR- lte SYSTEM-IP- 0.0.0.0 PEER-PERSONALITY- vbond


site-id 0
domain-id 0 protocol dtls
protocol-version DTLS1_2
cipher-name ECDHE-RSA-AES256-GCM-SHA384
private-ip 10.0.12.26
private-port 12346
public-ip 10.0.12.26
public-port 12346
UUID/chassis-number eb8844be-f58f-4bd3-b8c2-4f8cbc78131c
state tear_down [Local Err: ERR_DISCONNECT_VBOND] [Remote Err: NO_ERROR] downtime
2023-10-13T20:06:44+0000
repeat count 0 previous downtime N/A
Tx Statistics- hello 17
connects 0
registers 2
register-replies 0
challenge 0
challenge-response 1
challenge-ack 0
teardown 1
teardown-all 0
vmanage-to-peer 0
register-to-vmanage 0 Rx Statistics-

hello 17
connects 0
registers 0
register-replies 2
challenge 1
challenge-response 0
challenge-ack 1
teardown 0
vmanage-to-peer 0
register-to-vmanage 0
```

This command displays information about control plane connection attempts initiated by a Cisco IOS XE Catalyst SD-WAN device toward Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller.

```
Device# show control connections detail""
------------------------------------------------------------------------------------------

 REMOTE-COLOR- lte SYSTEM-IP- 172.16.255.21   PEER-PERSONALITY- vedge
------------------------------------------------------------------------------------------
site-id             100
domain-id           1
protocol            tls
protocol-version    TLS1_2
cipher-name         ECDHE-RSA-AES256-GCM-SHA384
private-ip          10.0.111.1
private-port        46437
public-ip           10.0.111.1
public-port         46437
org-name            vIPtela Inc Regression
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:10:02
hello interval      1000
hello tolerance     12000
peer-session-id      0x00656994de

  Tx Statistics-
  --------------
    hello                   603
    connects                0
    registers               0
    register-replies        0
    challenge               1
    challenge-response      0
    challenge-ack           1
    teardown                0
    teardown-all            0
    vmanage-to-peer         1
    register-to-vmanage     0
    create-cert-reply       0

  Rx Statistics-
  --------------
    hello                   603
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      1
    challenge-ack           0
    teardown                0
    vmanage-to-peer         0
    register-to-vmanage     1
    create-cert             0

------------------------------------------------------------------------------------------

 REMOTE-COLOR- default SYSTEM-IP- 172.16.255.19   PEER-PERSONALITY- vsmart
------------------------------------------------------------------------------------------
site-id             100
domain-id           1
protocol            tls
protocol-version    TLS1_3
cipher-name         TLS_AES_256_GCM_SHA384
private-ip          10.0.5.19
private-port        23456
public-ip           10.0.5.19
public-port         23456
org-name            vIPtela Inc Regression
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:09:48
hello interval      1000
hello tolerance     12000
peer-session-id      0x00b6655c4d

  Tx Statistics-
  --------------
    hello                   589
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      1
    challenge-ack           0
    teardown                0
    teardown-all            0
    vmanage-to-peer         1
    register-to-vmanage     0
    create-cert-reply       0

  Rx Statistics-
  --------------
    hello                   589
    connects                0
    registers               0
    register-replies        0
    challenge               1
    challenge-response      0
    challenge-ack           1
    teardown                0
    vmanage-to-peer         0
    register-to-vmanage     1
    create-cert             0
```

Cisco Catalyst SD-WAN Solution

To streamline and optimize cloud networking, Cisco Catalyst SD-WAN offers next-generation software services that run on the secure, virtual IP fabric:

- **Cloud onRamp for SaaS**: Cloud onRamp for SaaS optimizes the performance of Software as a Service (SaaS) cloud applications. It provides clear visibility of the performance of individual applications and automatically chooses the best path for each one. Cloud onRamp calculates metrics about loss and latency using a formula customized for each application.
- **Cisco SD-WAN Analytics**: Cisco SD-WAN Analytics is a SaaS service hosted by Cisco Catalyst SD-WAN as part of the solution. It provides graphical representations of the performance of your entire overlay network over time and lets you drill down to the characteristics of a single carrier, tunnel, or application at a particular time.
- **Cisco Catalyst SD-WAN Portal**: Cisco Catalyst SD-WAN Portal is a cloud-infrastructure automation tool tailored for Cisco Catalyst SD-WAN, which provides a quick way to provision, monitor, and maintain Cisco SD-WAN Controllers on public cloud providers.

Cloud onRamp for SaaS

Enterprises have been adopting business critical SaaS applications including Microsoft Office365, Salesforce, Dropbox, and others. Enterprises use three primary methods to offer connectivity to SaaS applications for their users:

- Direct Internet Access (DIA) from a branch office.
- Internet access through gateways in regional facilities.
- Cloud exchange or direct connection through gateways in a Carrier Neutral Facility (CNF).

Latency and packet loss have a direct impact on the performance of applications and on end-user experience, but in many cases network administrators have limited or no visibility into the network performance characteristics between the end-user and SaaS applications. When path impairment occurs and application performance suffers, shifting traffic from a primary to an alternate path usually requires the network administrator to performa a set of complex, manual, time-consuming, and error-prone steps.

Cisco Catalyst SD-WAN Cloud onRamp for SaaS provides visibility and continuous monitoring of network performance characteristics. It makes real-time decisions by choosing the best performing path between the end-user and SaaS application for an optimal user experience. It automatically reacts to changes in network performance by intelligently re-routing application traffic away from any degraded network paths.

Cloud onRamp for SaaS supports all access methods for cloud-based SaaS applications, including DIA, internet access through a regional facility, and access through a CNF.

Cloud onRamp for SaaS calculates an application performance value called the Viptela Quality of Experience (vQoE) for enterprise cloud applications. The vQoE value weighs loss and latency using a formula customized for each application. For example, email applications tolerate latency better than video applications do, and video applications tolerate loss better than email does. The vQoE value ranges from zero to ten, with zero being the worst quality and ten being the best.

You enable Cloud onRamp for SaaS in Cisco SD-WAN Manager with a few clicks of the mouse, and then you access the Cloud onRamp dashboard in Cisco SD-WAN Manager for continuous visibility into the performance of individual applications.

Cisco Catalyst SD-WAN Analytics

Cisco SD-WAN Analytics offers visibility into the performance of applications and the network over time. Cisco SD-WAN Analytics is a SaaS service hosted by Cisco Catalyst SD-WAN as part of the solution. It provides graphical representations of your entire overlay network and lets you drill down to display the characteristics of a single carrier, tunnel, or application at a particular time.

The Cisco SD-WAN Analytics dashboard serves as an interactive overview of your network and an entrance point for more details. The dashboard by default displays information aggregated for the last 24 hours. When you drill down, you can select different time periods for different data sets to display. The dashboard displays data on application performance, WAN site usage, and carrier usage.

Cisco SD-WAN Analytics calculates application performance with the QoE value, which is customized for individual applications. This value ranges from zero to ten, with zero being the worst performance and ten being the best. Cisco SD-WAN Analytics calculates QoE based on latency, loss, and jitter, customizing the calculation for each application.

Cisco SD-WAN Analytics stores data over a long period of time, displays historical trend information, and offers insights that could be used for future planning.

It offers:

- Application visibility:
  - Best and worst performing applications: Display the best and worst performing applications and drill down to details at the site level.
  - Most bandwidth consuming applications: Display applications consuming the most bandwidth and drill down to sites and users.
- Network visiblity:
  - Network availability and circuit availability: Display network availability and correlate network and circuit availability.
  - Tunnel performance: Display key performance indicators such as loss, latency and jitter over various Cisco Catalyst SD-WAN tunnels.
  - Carrier usage views: Display providers and their network characteristics.

Cisco Catalyst SD-WAN Portal

Cisco Catalyst SD-WAN Portal is a cloud-infrastructure automation tool tailored for Cisco Catalyst SD-WAN, which provides a quick way to provision, monitor, and maintain Cisco SD-WAN Controllers on public cloud providers.

You can provision the following controllers using the Cisco Catalyst SD-WAN Portal:

- Cisco SD-WAN Manager
- Cisco Catalyst SD-WAN Validator
- Cisco Catalyst SD-WAN Controller

Note Beginning with Cisco vManage Release 20.9.1, a link to the Cisco Catalyst SD-WAN Portal is added from the Cisco Catalyst SD-WAN menu. From the Cisco Catalyst SD-WAN menu, click **SD-WAN Portal** to access the Cisco Catalyst SD-WAN Portal for provisioning, monitoring, and maintaining Cisco SD-WAN Controllers.

For more information on the Cisco Catalyst SD-WAN Portal, see the *Cisco Catalyst SD-WAN Portal Configuration Guide*.

Cisco SD-AVC

Beginning with the 18.4 release, Cisco Catalyst SD-WAN incorporates Cisco Software-Defined Application Visibility and Control (SD-AVC) to provide:

- Recognition of network application traffic for visibility, analytics, application-aware routing, and application-based policies, such as QoS and application-based firewall policy.
- Analytics at the network level.

Cisco SD-AVC operates on Cisco IOS XE Catalyst SD-WAN devices in the network, and the Cisco SD-AVC network service operates as a container within Cisco SD-WAN Manager.

Note All relevant Cisco SD-AVC functionality is accessed through the Cisco SD-WAN Manager interface. Cisco Catalyst SD-WAN does not support the use of a separate SD-AVC interface.

Cisco SD-WAN Manager Cluster

Cisco SD-AVC must operate on only one Cisco SD-WAN Manager instance. In a Cisco SD-WAN Manager cluster, enable Cisco SD-AVC on only one instance of Cisco SD-WAN Manager.

Work with Cisco Catalyst SD-WAN

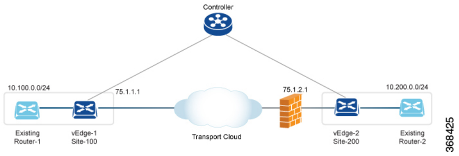
Build a Basic Overlay Network using Cisco vEdge Devices

Let's use a simple network design, one that has two vEdge routers and one Cisco SD-WAN Controllers, to illustrate how to form a functioning overlay network from Cisco vEdge components. In this topology, the Cisco SD-WAN Validator software has been enabled on one of the vEdge routers. Once you understand a simple network, you can start designing and building more complex topologies.

A Simple Network Topology

The following figure illustrates our simple topology. Here, we have two sites, Site-100 and Site-200. vEdge-1 is the edge device in Site-100, and vEdge-2 is the edge device at Site-200. At each local site, the vEdge router connects to an existing traditional router via a standard Ethernet interface. vEdge-2 is connected to the transport network through a NAT device that also has firewall functionality.

Figure 8: A Simple Network Topology



The goal of our design is to create a private network so that Router-1 and Router-2 can be next to each other from a Layer 3 perspective and so that hosts connected to each of these routers can communicate through the private network.

Construct a Basic Network

The following steps allow you to create the simple overlay network depicted in the topology above.

- Step 1: Perform initial bringup and basic configuration.
- Step 2: Enable host or service-side interfaces and routing.
- Step 3: Enable overlay routing over OMP.
- Step 4: Check the automatic setup of the IPsec data plane.
- Step 5: Enforce policies.

Let’s look at the steps in a bit more detail.

Step 1: Perform Initial Bring up and Basic Configuration

From the perspective of a network administrator, the initial bringup of the Cisco vEdge network components is a straightforward and simple process, involving creating the configurations for each of the network components and ensuring that a few key authentication-related files are in place. From the perspective of user, bringup entails simply powering up the vEdge router and plugging in a cable to connect the router to the network. The remainder of the bringup occurs automatically via a zero-touch-provisioning process.

The network administrator performs the following tasks as part of the initial bringup:

1. Configure the Cisco SD-WAN Validator function on one of the vEdge routers in the network. In our example, this is vEdge-1.
2. Optionally, configure a top-level Cisco SD-WAN Validator to act as a ZTP server. In this situation, a DNS server must be present in the enterprise network.
3. Ensure that a DHCP server is present in the enterprise network.
4. Install the signed certificate on Cisco SD-WAN Manager, and download that certificate to Cisco SD-WAN Manager orchestrator.
5. Install the vEdge router authorized serial number file on Cisco SD-WAN Manager, and then download it to the Cisco SD-WAN Controllers.

6. From Cisco SD-WAN Manager CLI, create a configuration for each Cisco Catalyst SD-WAN Controller and vEdge router in the overlay network:
   a. Configure a system IP address, which is similar to the router ID address on a traditional router, identifying the Cisco vEdge device with an address that is independent of any of the interfaces on the device. System IP addresses must be pre-allocated and must be unique across each vEdge router and Cisco Catalyst SD-WAN Controller. These addresses need not be routable through the network.
   b. Configure site IDs for the various sites in the overlay network. In our example, vEdge-1 is at site-100 and vEdge-2 is at site-200. The Cisco Catalyst SD-WAN Controller can be collocated at a site, or it can be in its own site.
   c. Configure domain IDs. This is an optional step to create clusters. For our example, configure the domain-ID as 1.
   d. Configure the IP address or DNS name for the Cisco SD-WAN Validator server and the Cisco Catalyst SD-WAN Controller.
   e. Configure WAN interfaces on vEdge-1 and vEdge-2. VPN 0 is the VPN reserved for WAN transport interfaces. IP addresses can be automatically obtained through DHCP. Alternatively, you can configure a default gateway and DNS explicitly.
   f. By default, DTLS and IPsec are enabled on the WAN interfaces.
   g. Save the configuration.

When the Cisco SD-WAN Controllers join the network, they are authenticated by the Cisco SD-WAN Validator, and when vEdge routers join the network, they are authenticated by both the Cisco SD-WAN Validator and the Cisco SD-WAN Controllers. These devices then connect to Cisco SD-WAN Manager, which downloads the configuration to them.

Example Configuration on vEdge-1:

```
system
  host-name vEdge-1
  system-ip 1.0.0.1
  domain-id 1
  site-id   100
  vbond 75.1.1.1  local
!
vpn 0
  interface ge 0/0
    ip address 75.1.1.1/24
    tunnel-interface
      color default
    no shutdown
  ip route 0.0.0.0/0 75.1.1.254
!
```

The remaining sections in this article describe how to configure other common functionality on vEdge routers and Cisco SD-WAN Controllers. Typically, you configure all functionality at one time, in the configuration that you create on Cisco SD-WAN Manager and that is downloaded to the device when it joins the overlay network. However, to highlight the different functionalities, this article describes the various portions of the configuration separately.

Step 2: Enable Host or Service-Side Interfaces and Routing

From Cisco SD-WAN Manager, you can also configure service-side interfaces and regular routing:

1. Configure interfaces on vEdge-1 towards the existing traditional router. Assign IP address and put the interface in a non-default VPN. In our example, this is VPN 1. Do the same on vEdge-2.
2. Configure OSPF or BGP on the vEdge routers towards the existing routers
3. Commit

To check for standard IP reachability, routes, and next hops at the local site, use the standard **ping**, **traceroute**, and various **show** commands on Cisco SD-WAN Manager or from the CLI of the device (if you have a direct connection to the device):

Example Configuration for the Host or Service-side VPN:

```
vpn 1
  router
    ospf
      redistribute omp
      area 0
        interface ge 0/1
        exit
      exit
    !
  !
  interface ge 0/1
    ip address 10.1.2.12/24
    no shutdown
!
```

Step 3: Enable Overlay Routing over OMP

All site-local routes are populated on the vEdge routers. Distributed these routes to the other vEdge routers this is done through the Cisco Catalyst SD-WAN Controller, via OMP.

1. If you are using BGP or if there are OSPF external LSAs, allow OMP to redistribute the BGP routes.
2. Re-advertise OMP routes into BGP or OSPF.
3. Commit.

Example Configuration of Overlay Routing over OMP:

```
omp
  advertise ospf external
!
```

At this point, vEdge-1 is able to learn about the prefixes from site-200, and vEdge-2 is able to learn about prefixes from site-100. Because all the prefixes are part of VPN 1, the hosts in site-100 and site-200 have reachability with one another. From a Cisco Catalyst SD-WAN overlay network point of view, this reachability is possible because vEdge-1 advertises a vRoute consisting of the address 10.100.0.0/24 and the TLOC color of default, which we write as {75.1.1.1, default }, to the Cisco Catalyst SD-WAN Controller. In turn, the Cisco Catalyst SD-WAN Controller advertises this vRoute to vEdge-2. The same process happens with prefix 10.200.0.0/24 on vEdge-2.

Step 4: Check the Automatic Setup of the IPsec Data Plane

For every TLOC on a vEdge router, the vEdge router advertises a symmetric key for encryption. The Cisco Catalyst SD-WAN Controller reflects this key automatically and advertises the TLOC with the symmetric key. A two-way IPsec SA is set up as a result (that is, there is a different key in each direction), and data traffic automatically starts to use this IPsec tunnel. Once a tunnel is up, BFD automatically starts on the tunnel. This is done to ensure fast data plane convergence in the event of a failure in the transport network.

The setup of the IPsec data plane happens automatically. No configuration is necessary. Multiple show commands are available to check the SAs and the state of the IPsec tunnel.

Step 5: Enforce Policies

As an optional step, you can create control and data plane policies on the Cisco Catalyst SD-WAN Controller and push them to the vEdge routers. As an example, if the network administrator wants to enforce a policy to divert traffic destined to { vEdge-2, prefix 10.200.0.0/24 } to go to another site say vEdge-3, a control plane policy can be created on the Cisco Catalyst SD-WAN Controller and pushed to the respective vEdge routers. The results of the policy are pushed to the vEdge routers, not the configuration itself.

Example Configuration of Policies:

```
policy
  lists
    site-list site-100
      site-id 100
    !
    prefix-list my-prefixes
      ip-prefix 10.200.0.0/24
    !
  control-policy TE-thru-vedge3
    sequence 10
      match route
        prefix-list my-prefixes
      !
      action accept
        set
          tloc 1.0.0.3 color default
        !
      !
      default action accept
    !
apply-policy
  site-list site-100
    control-policy TE-thru-vedge3 out
  !
!
```

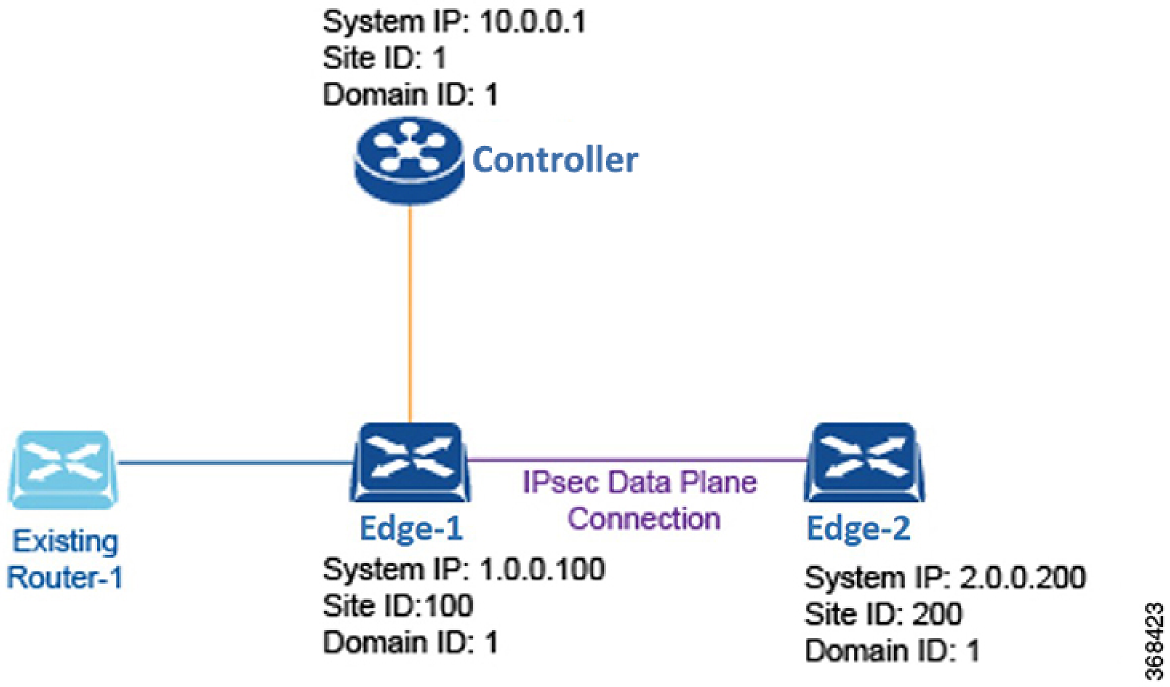
Advanced Options

Now that we have looked at basic routing, security, and policy, we can start adding various other elements to the network. You are encouraged to look at the *Software* category to add elements such as High Availability, Convergence, BFD, QoS, ACLs, segmentation, and advanced policy.

Cisco Catalyst SD-WAN Terminology

The following figure summarizes the terminology used to describe a Cisco Catalyst SD-WAN overlay network.

Figure 9: Terminology used in a Cisco Catalyst SD-WAN overlay network



Domain ID

A domain is a logical grouping of edge routers and Cisco SD-WAN Controllers that demarcate the span of control for the Cisco SD-WAN Controllers. Each domain is identified by a unique integer, called the domain ID. Currently, you can configure only one domain in a Cisco Catalyst SD-WAN overlay network.

Within a domain, edge routers can connect only with the Cisco SD-WAN Controllers in their own domain. The Cisco SD-WAN Validator is aware of which Cisco SD-WAN Controllers are in which domain, so that when new edge routers come up, the Cisco SD-WAN Validator can point those routers to the Cisco SD-WAN Controllers in the proper domain. However, the Cisco SD-WAN Validator is never a member of a domain.

Within a domain, there is full synchronization of routing information among the Cisco SD-WAN Controllers and edge routers, and there is scope for route aggregation and summarization. An organization can divide up its network into domains to serve desired business purposes. For example, domains can correspond to a large geographic area or to data centers so that each data center and the branches for which it is responsible are contained within a single domain.

OMP Routes

On Cisco SD-WAN Controllers and edge routers, OMP advertises to its peers the routes and services that it has learned from its local site, along with their corresponding transport location mappings, which are called Transport Locations (TLOCs). These routes are called OMP routes, to distinguish them from standard IP routes. It is through OMP routes that the Cisco SD-WAN Controllers learn the network topology and the available services.

Cisco Catalyst SD-WAN control plane architecture uses three types of OMP routes:

- OMP routes: Prefixes that establish reachability between end points that use the OMP-orchestrated transport network. OMP routes can represent services in a central data center, services at a branch office, or collections of hosts and other end points in any location of the overlay network. OMP routes require and resolve into TLOCs for functional forwarding. In comparison with BGP, an OMP route is the equivalent of a prefix carried in any of the BGP AFI/SAFI fields.
- TLOCs: Identifiers that tie an OMP route to a physical location. The TLOC is the only entity of the OMP routing domain that is visible to the underlying network, and it must be reachable via routing in the underlying network. A TLOC can be directly reachable via an entry in the routing table of the physical network, or it must be represented by a prefix residing on the outside of a NAT device and must be included in the routing table. In comparison with BGP, the TLOC acts as the next hop for OMP routes.
- Service routes: Identifiers that tie an OMP route to a service in the network, specifying the location of the service in the network. Services include firewalls, Intrusion Detection Systems (IDPs), and load balancers.

Note The maximum OMP routes supported are 140K on the C1131X_8PW devices. When there are more than 140K OMP routes, the device crashes due to the out of memory issue.

Site ID

A site is a particular physical location within the Cisco Catalyst SD-WAN overlay network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer, called a site ID. Each Cisco vEdge device at a site is identified by the same site ID. So within a data center, all the Cisco SD-WAN Controllers and any edge routers are configured with the same site ID. A branch office or local site typically has a single edge router, but if a second one is present for redundancy, both routers are configured with the same site ID.

System IP Address

Each edge router and Cisco Catalyst SD-WAN Controller is assigned a system IP address, which identifies the physical system independently of any interface addresses. This address is similar to the router ID on a regular router. The system IP address provides permanent network overlay addresses for edge routers and Cisco SD-WAN Controllers, and allows the physical interfaces to be renumbered as needed without affecting the reachability of the Cisco vEdge device. You write the system IP address as you would an IPv4 address, in decimal four-part dotted notation.

TLOC

A TLOC, or transport location, identifies the physical interface where a edge router connects to the WAN transport network or to a NAT gateway. A TLOC is identified by a number of properties, the primary of which is an IP address–color pair, which can be written as the tuple {IP-address, color}. In this tuple, IP address is the system IP address and color is a fixed text string that identifies a VPN or traffic flow within a VPN. OMP advertised TLOCs using TLOC routes.

Additional Information

For a description of the elements in a Cisco Catalyst SD-WAN overlay network, see *Components of the Cisco Catalyst SD-WAN Solution*. For an understanding of how you put together an overlay network using Cisco

Catalyst SD-WAN software and hardware, see *Constructing a Basic Network Using Cisco Catalyst SD-WAN Components*. For examples of how the components of the overlay network work, see the *Validated Examples*.