Revised: August 4, 2026

Cisco Catalyst SD-WAN Terminology

Cisco SD-WAN Terminology

Defines terminology specific to Cisco Catalyst SD-WAN, enabling readers to understand key concepts and terms used in the SD-WAN environment.

Cisco Catalyst SD-WAN is a centrally managed, secure virtual network that connects users, sites, applications, data centers, and cloud environments across internet, MPLS, cellular, and other WAN transports.

This document defines terminology used in Cisco Catalyst SD-WAN. It focuses on terms that are specific to Cisco Catalyst SD-WAN, or whose meaning is distinct in an SD-WAN environment.

adaptive QoS

QoS behavior that adjusts available bandwidth and scheduling when a transport's usable capacity changes, which is especially useful for variable-bandwidth links.

advisory

A centralized notification about a security vulnerability, field notice, or product-lifecycle condition that may affect devices in the SD-WAN environment. Advisories help operators assess exposure and plan remediation or replacement.

alarm

A notification that an SD-WAN condition may require attention or corrective action. Alarms are raised for conditions such as device or control-connection failures, tunnel degradation, threshold violations, certificate issues, and component health problems. An alarm can remain active until the underlying condition clears or an operator acknowledges it, depending on the alarm type.

application-aware routing (AAR)

Policy-based path selection that chooses a tunnel according to the application and measured path quality. AAR can move traffic when loss, latency, or jitter no longer meets the application's SLA class.

application list

A reusable set of recognized applications or application families used as a policy match condition. Application lists help apply the same steering, QoS, security, or SaaS optimization behavior consistently.

application quality of experience (AppQoE)

The group of WAN-optimization capabilities that improve application performance over high-latency, lossy, or bandwidth-constrained paths.

AppNav-XE

The traffic-classification and service-steering component used to direct selected flows to AppQoE optimization services.

audit log

A history of administrative and configuration activity in SD-WAN Manager. Audit entries identify who performed an operation and when; supported workflows can also compare the current and previous versions of a template configuration.

automated certificate management

The SD-WAN Manager workflow for enrolling, renewing, distributing, and monitoring certificates used by control components and edge devices. Supported deployments can automate enrollment through protocols such as EST or SCEP.

autonomous mode

The Cisco IOS XE operating mode in which a router operates as a conventional, independently managed Cisco IOS XE Catalyst SD-WAN device rather than as a controller-managed SD-WAN edge. Supported platforms can require a mode change when migrating into or out of the SD-WAN fabric.

backup and restore

The operational workflow for protecting and recovering Cisco SD-WAN Manager configuration and database information. Backups support recovery from data loss, failed changes, or disaster-recovery events.

bidirectional forwarding detection (BFD)

The protocol used across SD-WAN data-plane tunnels to detect path failure and measure loss, latency, and jitter. Its results support rapid convergence, tunnel health monitoring, and application-aware routing.

bootstrap configuration

A generated configuration package used to start an edge device and direct it toward the services required to join the fabric. It commonly includes organization, validator, system, and WAN transport information.

border router

An MRF edge device that connects a regional overlay to the core region and forwards inter-region traffic. Border routers participate in both the assigned region and region 0.

centralized control policy

A policy that matches and changes OMP routing information as it is received or advertised by controllers. It can alter reachability or topology without requiring a separate routing policy on every edge device.

centralized data policy

A centrally defined policy that is installed on edge devices to act on data traffic. It can match traffic and then steer, drop, accept, mark, mirror, or redirect it.

centralized policy

Policy administered centrally and distributed through the control system. It can influence route advertisement, topology, segmentation, traffic steering, application paths, and service insertion across many sites.

certificate revocation

The process of invalidating a previously trusted device or component certificate. Cisco SD-WAN Manager can use certificate-revocation information from a certificate authority to prevent a revoked identity from participating in the fabric.

Cisco Catalyst SD-WAN

A software-defined WAN solution that separates network control from packet forwarding and builds a centrally managed, secure overlay across one or more transport networks.

Cisco Catalyst SD-WAN Analytics

A cloud-hosted analytics service that retains and correlates telemetry about applications, sites, carriers, and tunnels for historical trends, capacity planning, and root-cause analysis. Earlier documentation calls it Cisco vAnalytics.

Cisco Catalyst SD-WAN control components

The software components that manage, control, and help authenticate the fabric: Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco Catalyst SD-WAN Validator.

Cisco Catalyst SD-WAN fabric

The complete SD-WAN system: control components, edge devices, secure control connections, overlay routes, data-plane tunnels, and the policies that govern connectivity. The fabric is also called the overlay network.

Cisco Catalyst SD-WAN Portal

A cloud-infrastructure automation service used to provision, monitor, and maintain Cisco-hosted SD-WAN control components. Earlier documentation may call it the Cisco Self-Service Portal.

Cisco SD-WAN Controller

The control-plane component that maintains secure sessions with edge devices and distributes OMP routing, policy, and security information. It influences how traffic is forwarded but does not carry customer data traffic. Earlier documentation calls it Cisco vSmart Controller.

Cisco SD-WAN edge device

A physical or virtual router at a branch, campus, data center, colocation facility, or cloud location. It connects local networks to the SD-WAN fabric, forms control connections, establishes data-plane tunnels, and enforces forwarding and security policies. The terms *WAN edge* and *edge router* are also used.

Cisco SD-WAN Manager

The centralized management system for configuring, monitoring, maintaining, and troubleshooting the SD-WAN fabric. It also manages items such as device onboarding, certificates, software images, policies, and configuration workflows. Earlier documentation calls it Cisco vManage.

Cisco SD-WAN Manager cluster

Multiple Cisco SD-WAN Manager nodes operating together to distribute management services and improve scale and availability. Cluster health depends on the state and compatibility of its nodes and services.

Cisco SD-WAN Validator

The orchestration component that authenticates devices during fabric bring-up, introduces edge devices to the appropriate controllers, and assists with NAT traversal. Its connection to an edge device is generally needed for onboarding rather than for ongoing data forwarding. Earlier documentation calls it Cisco vBond Orchestrator.

Cisco Software-Defined Application Visibility and Control (SD-AVC)

The application-recognition and analytics capability used by the fabric for application visibility, application-aware routing, QoS, and application-based security policy.

CLI add-on template

A supplemental template for adding small sets of supported CLI configuration that are not represented by standard feature templates. It extends a device-template configuration and is not intended to replace the full template model.

Cloud Hub

An SD-WAN design that uses a cloud provider's backbone as underlay transport to connect branches, data centers, and cloud networks.

Cloud Interconnect

A Cloud OnRamp capability that automates site-to-site and site-to-cloud connectivity over a supported, cloud-agnostic interconnect provider.

Cloud OnRamp

The family of SD-WAN capabilities for automating or optimizing connectivity to SaaS applications, public-cloud workloads, colocation facilities, and cloud interconnect providers.

Cloud OnRamp for Colocation

A design that aggregates branch access to cloud and internet services through regional colocation facilities, where shared network and security services can be hosted.

Cloud OnRamp for IaaS

The earlier term for automated SD-WAN connectivity to infrastructure-as-a-service environments. For newer designs, Cisco documentation directs customers toward Cloud OnRamp for Multicloud.

Cloud OnRamp for Multicloud

The current model for automating SD-WAN connectivity to public-cloud networks and supported interconnect services across multiple cloud providers.

Cloud OnRamp for SaaS

A capability that continuously measures available paths to supported or custom SaaS applications and steers application traffic to the better-performing path.

cluster persona

The role assigned to an Cisco SD-WAN Manager cluster node that determines which services run on that server. Persona-based deployment simplifies adding and scaling cluster nodes.

configuration conversion

The workflow for moving a device from an older template-based configuration model to configuration groups while preserving supported settings.

configuration group

A reusable, intent-based configuration model that combines profiles, parcels, and device-specific values and applies them consistently to a group of devices.

control connection

An authenticated, encrypted DTLS or TLS session used between SD-WAN components. Control connections carry management and control-plane information, not customer application traffic.

controller configuration consistency

A validation and deployment process that helps ensure SD-WAN Controllers operate with consistent configuration. The workflow can validate, apply, and, when needed, roll back a change across the controller set.

controller group

A logical grouping of SD-WAN Controllers used to distribute control connections and provide redundancy. Edge devices can prefer controllers in one group and move to an alternate controller or group when necessary.

controller mode

The Cisco IOS XE operating mode in which a supported router participates in the Catalyst SD-WAN fabric and is centrally managed through Cisco SD-WAN Manager. Earlier documentation may call this SD-WAN mode.

control plane

The part of the solution that exchanges routes, transport locations, security information, and policy. Cisco SD-WAN Controller and edge devices exchange this information using OMP; controllers do not forward customer data traffic.

core region (region 0)

The MRF backbone containing border routers that interconnect regional overlays. It can use a transport design different from those of the individual regions.

custom application

A customer-defined application identity used when built-in recognition does not adequately identify an internal or specialized application.

data plane

The part of the solution that forwards customer traffic between edge devices, normally through encrypted IPsec tunnels. Path selection and forwarding take place on the edge devices.

data redundancy elimination (DRE)

An AppQoE capability that recognizes repeated byte patterns and avoids transmitting the same data repeatedly across the WAN, reducing bandwidth consumption.

day-0 configuration

The initial configuration that gives a new device enough identity, WAN connectivity, and controller information to begin onboarding. It is applied before the full operational configuration is deployed.

device-specific variable

A value supplied separately for each device when a template or configuration group is deployed, such as an interface address, site ID, or hostname. It allows a shared configuration design to contain unique device values.

device template

The classic SD-WAN configuration model that assembles feature templates and device-specific values into a complete configuration for one or more edge devices. Customers encounter device templates in deployments that predate or have not migrated to configuration groups.

device version compliance

An Cisco SD-WAN Manager check that identifies software versions that are outside the supported compatibility range. It can warn about or block a manager upgrade when incompatible edge-device versions remain in the overlay.

direct internet access (DIA)

A design in which selected branch traffic exits directly to the internet rather than being backhauled through a data center. SD-WAN policy can combine DIA with application steering and local or cloud-delivered security.

disaster recovery

A deployment and workflow for restoring SD-WAN management after a major site or system failure, commonly by maintaining primary and secondary Cisco SD-WAN Manager environments and replicating required data between them.

domain ID

An integer that identifies the SD-WAN domain—the logical scope in which edge devices and controllers exchange control information. A device forms controller relationships within its domain; the validator itself is not a domain member.

dynamic on-demand tunnel

A direct tunnel created only when matching traffic needs it. It combines a scalable hub-and-spoke baseline with temporary direct spoke-to-spoke paths.

enhanced application-aware routing

An AAR mode that improves how the edge device evaluates and switches paths, helping avoid unnecessary changes while responding more effectively to degraded application paths.

enterprise certificate

A certificate issued by an enterprise or supported certificate authority to establish the identity and trust of an SD-WAN component or edge device. Certificate identity must be consistent with the fabric's authentication settings.

enterprise firewall with application awareness

An edge security capability that can enforce firewall policy using recognized application identity in addition to addresses, ports, zones, and protocols.

event

A time-stamped record of a state change or operational occurrence in the SD-WAN environment. Events help reconstruct what happened before, during, or after an incident, but an event does not necessarily indicate a fault or require action.

feature profile

A reusable collection of related configuration within a configuration group, commonly organized by system, transport, service, policy, or security function.

feature template

A reusable configuration element in the classic template model that represents a particular device function, such as system settings, a VPN, an interface, routing, or security. Multiple feature templates are combined in a device template.

forward error correction (FEC)

A loss-recovery technique that adds parity packets to a traffic stream so the receiver can reconstruct some missing packets without retransmission. It is useful for loss-sensitive real-time applications.

full-mesh topology

An overlay design in which sites form direct data-plane tunnels to one another. It provides direct paths but can create more tunnel state as the number of sites grows.

high availability

A design that uses redundant control components, edge devices, connections, or services so the SD-WAN environment can continue operating when an element fails.

hosted edge service

An application or service, such as an IOx application, that runs on a supported SD-WAN edge platform. Cisco SD-WAN Manager can display its device association, version, health, and operational state.

hub-and-spoke topology

An overlay design in which spoke sites communicate through designated hub sites instead of forming direct tunnels to every other spoke. Centralized policy is commonly used to create the topology.

IPsec data-plane tunnel

An encrypted tunnel between edge-device TLOCs that carries customer traffic. The fabric distributes the information needed to establish these tunnels automatically.

localized policy

A policy that operates on an individual edge device, commonly for site-specific access control, route policy, QoS, or traffic handling. It does not change OMP advertisements at the controller.

log

A detailed record generated by an SD-WAN component or edge device for operations, troubleshooting, security analysis, or audit. Logs provide lower-level context than alarms and events and may be viewed in Cisco SD-WAN Manager or forwarded to an external logging system.

management region

An MRF construct that provides controlled connectivity to shared management resources without treating the management network as an ordinary user region.

management VPN (VPN 512)

The out-of-band management routing context used on platforms that support it. It is separate from both the transport VPN and customer service VPNs.

Multi-Region Fabric (MRF)

A hierarchical architecture that divides a large overlay into regional overlays and a core region. It reduces control and tunnel scale while providing governed connectivity between regions. Earlier documentation may call it Hierarchical SD-WAN.

NAT DIA

Direct internet access that uses address translation on the edge device for branch internet egress.

NAT DIA fallback

Policy behavior that sends traffic to an alternate route or site when the local NAT DIA path is unavailable.

network hierarchy

A model in Cisco SD-WAN Manager that organizes the fabric by geographic or operational levels, such as regions, areas, and sites. The hierarchy helps administrators assign resources, configurations, and operational views consistently.

Network-Wide Path Insight (NWPI)

A troubleshooting capability that traces a selected flow across the SD-WAN overlay and correlates the path with device, tunnel, policy, application, and service information.

NWPI trace

A live or simulated investigation of how a selected flow is handled from source to destination. Trace views and the insight summary help identify the point at which forwarding, policy, or path health differs from expectations.

OMP graceful restart

A resiliency mechanism that lets an edge device continue forwarding with cached OMP information for a limited period if its control connection is interrupted.

OMP route or vRoute

An enterprise prefix advertised through OMP together with the transport information needed to reach it. Unlike a conventional IP route, an OMP route resolves through a TLOC, which acts as its overlay next hop.

organization name

A case-sensitive name shared by the control components and edge devices in the same fabric. It forms part of the trust and authentication context; a mismatch can prevent control connections from forming.

overlay bring-up

The process of establishing a working fabric, including deploying control components, establishing trust, installing certificates, configuring system properties, and onboarding edge devices.

overlay management protocol (OMP)

The SD-WAN control protocol that runs between controllers and edge devices. OMP distributes overlay prefixes, TLOCs, services, policy attributes, and security information needed to build and operate the fabric.

overlay network

The logical network formed between SD-WAN edge devices. It carries enterprise traffic through encrypted tunnels and operates independently of the transports underneath it.

packet duplication

A loss-protection technique that sends copies of selected packets over more than one tunnel. The receiver keeps the first usable copy, improving resilience at the cost of additional bandwidth.

parcel

A modular configuration unit inside a feature profile. Parcels represent individual features or subfeatures that can be assembled into a configuration-group design.

per-tunnel QoS

Quality-of-service treatment applied separately to SD-WAN tunnels, allowing traffic scheduling to reflect the bandwidth or characteristics of different WAN transports.

policy group

A reusable model that combines supported policy and configuration profiles so a consistent operational intent can be assigned to multiple devices.

Predictive Path Recommendation (PPR)

An analytics capability that evaluates historical and expected path performance against application SLAs and recommends a better path before users are affected.

preferred color

A policy preference for one or more transport colors. Traffic uses an acceptable preferred transport when available and follows the policy's fallback behavior when it is not.

private color

A TLOC color normally used for a private transport, such as MPLS, where addresses are expected to be reachable within the private underlay. Private colors influence how the fabric attempts to form tunnels.

protocol pack

An update package for application recognition. Protocol-pack management lets customers update application signatures independently of a full device software upgrade, subject to compatibility requirements.

public color

A TLOC color whose transport address is expected to be reachable through a public network and may be translated by NAT. Public colors allow tunnel formation between compatible public transports.

Quick Connect

A guided SD-WAN Manager workflow for onboarding supported IOS XE edge devices. It creates basic Day-0 profiles, adds the device to the WAN transport, and helps establish its control and data-plane connections.

region

A logical part of a Multi-Region Fabric. Edge devices form direct tunnels within their region; traffic between different regions normally crosses border routers in the core region.

remote access

The SD-WAN capability for onboarding and applying policy to remote-user connectivity so remote users can securely reach private applications and other permitted resources.

report

A generated or scheduled summary of SD-WAN information over a selected period, such as device availability, application usage, network performance, security activity, or energy consumption. Reports are intended for operational review, capacity planning, compliance, and communication with stakeholders.

resource ID

An identifier allocated to an object in the network hierarchy, such as a region or site. Resource management helps prevent conflicting identifiers and simplifies consistent device deployment.

restrict

A tunnel-interface setting that limits data-plane tunnel formation to remote TLOCs of the same color. It is commonly used to keep traffic for a private transport on that transport.

route aggregation in MRF

The summarization of regional routes by border routers or transport gateways. It reduces the number of routes distributed across the core and improves control-plane scale.

route leaking

The intentional sharing of selected routes between otherwise isolated service VPNs or VRFs. It is used when segments need limited connectivity without removing their overall separation.

router affinity

An MRF preference that influences which border routers an edge device uses, helping distribute connections and create predictable primary and backup relationships.

route redistribution

The controlled exchange of routes between OMP and routing protocols used at a local site. It is how prefixes learned from a connected network, static routing, OSPF, BGP, or another supported protocol enter or leave the overlay.

safety barrier

A protective controller mechanism that monitors resource use such as CPU, memory, and disk. When a threshold is exceeded, it raises alarms and can restrict services that might worsen the resource condition.

secondary region

An additional regional association that gives selected devices alternate regional connectivity, commonly for resiliency or shared-service access.

secure internet gateway (SIG) integration

The redirection of branch internet and SaaS traffic from SD-WAN to a cloud-delivered security service, using centrally managed tunnels and policy.

secure service edge (SSE) integration

Integration between SD-WAN and cloud-delivered security services for protected access to internet, SaaS, and private applications.

segmentation

The isolation of users, applications, or business functions into separate service VPNs or VRFs. Segment identity is preserved across the overlay, while the underlay remains unaware of the customer segments.

service chain

An ordered path through one or more network services. Service chaining is the policy-driven process of sending selected traffic through that ordered path.

service insertion

Policy-based redirection of selected traffic to a network or security service, such as a firewall. The service can be located at another site, in a colocation facility, or in a supported cloud interconnect design.

service route

An OMP advertisement that identifies a network service and where it is available. It allows policy to steer selected traffic through services such as firewalls or other inspection functions.

service VPN or service VRF

A segmented routing context for customer users, applications, or services. Service routes are carried across the overlay while remaining isolated from other service VPNs unless policy explicitly permits connectivity.

site

A physical location or logical deployment unit, such as a branch, campus, data center, or cloud location. A site can contain one or more edge devices.

site ID

An integer that identifies a site in the overlay. Redundant edge devices at the same site use the same site ID, allowing the fabric and policy system to treat them as one location.

SLA class

A reusable set of acceptable loss, latency, and jitter thresholds. AAR compares tunnel measurements with these thresholds when choosing a path for matched application traffic.

software-defined cloud interconnect (SDCI)

A partner-delivered, software-controlled interconnect used with Cloud OnRamp to provision private or optimized connectivity between SD-WAN sites and cloud networks.

software maintenance upgrade (SMU)

A targeted patch package that fixes a specific software defect or security issue without requiring customers to wait for the next full IOS XE release.

software upgrade workflow

A guided Cisco SD-WAN Manager process for selecting images, checking devices, scheduling an upgrade, activating software, and monitoring results across edge devices or control components.

subregion

A further division within an MRF region used to control topology and scale at a finer level.

system IP address

A persistent, IPv4-formatted identifier assigned to an edge device or controller. It behaves like a router ID and is independent of interface addressing, so interface addresses can change without changing the device's overlay identity. It does not need to be a routable address.

TCP optimization

An AppQoE capability that improves TCP performance across WAN paths by optimizing the behavior of TCP sessions between sites.

TLOC color

A label that characterizes a WAN transport, such as mpls, biz-internet, or lte. Color is part of a TLOC and is used by policy, tunnel formation, and path selection; it does not have to match a provider's service name.

TLOC extension

A design in which one edge device uses a transport circuit connected to another edge device at the same site. It lets both devices use both WAN circuits without physically connecting every circuit to every router.

TLOC route

An OMP advertisement that describes a transport locator and its attributes, including how the transport attachment can be reached. TLOC routes allow edge devices to build the overlay topology and establish data-plane tunnels.

transport gateway

An edge-device role that extends connectivity between separate SD-WAN networks or transports. It exchanges routes and forwards traffic between the connected domains while preserving SD-WAN policy control.

transport locator (TLOC)

The overlay next hop that identifies an edge device's attachment to a WAN transport. A TLOC is commonly represented by the tuple {system IP address, color, encapsulation}. OMP uses TLOCs to associate reachable service-side prefixes with usable transport paths.

transport VPN (VPN 0 or global VRF)

The routing context that contains WAN-facing interfaces and provides underlay reachability for control connections and data-plane tunnels. It is deliberately separated from enterprise service networks.

underlay health visibility

Monitoring that exposes the condition and performance of the provider or physical networks beneath the SD-WAN overlay. It helps distinguish an underlay problem from overlay routing, policy, or application issues.

underlay network

The physical or provider networks that give SD-WAN endpoints basic IP reachability. Examples include internet, MPLS, broadband, and cellular services. SD-WAN can measure these transports and steer overlay traffic without requiring the provider network to understand enterprise routes.

unified threat defense (UTD)

The integrated edge security framework used to enable capabilities such as intrusion prevention, URL filtering, and malware protection on supported Cisco IOS XE Catalyst SD-WAN devices.

upgrade matrix

A Cisco compatibility resource that shows supported software upgrade paths, prerequisites, and release combinations for Cisco IOS XE Catalyst SD-WAN devices and control components.

vQoE score

The application-specific quality score used by Cloud OnRamp for SaaS. It weighs measurements such as loss and latency according to the application's sensitivity; a higher score represents a better path.

WAN Insights

The predictive analysis used to forecast WAN path behavior and support path recommendations from historical performance data.

zero-touch provisioning (ZTP)

An onboarding method in which a supported edge device can authenticate, contact provisioning services, and receive the information needed to join the fabric with minimal on-site configuration.

Current and earlier product names

Maps current and legacy product names to help readers navigate Cisco Catalyst SD-WAN environments.

Customers may encounter the following names in older documentation, user interfaces, APIs, command output, and support material.

The table below shows the earlier name and the current name.

Earlier name	Current name
Cisco SD-WAN solution	Cisco Catalyst SD-WAN
Cisco vManage	Cisco SD-WAN Manager
Cisco vAnalytics	Cisco Catalyst SD-WAN Analytics
Cisco vSmart Controller	Cisco SD-WAN Controller
Cisco vBond Orchestrator	Cisco SD-WAN Validator
Cisco Controllers	Cisco Catalyst SD-WAN Control Components
Cisco Self-Service Portal	Cisco Catalyst SD-WAN Portal
Cisco Cloud-Delivered SD-WAN	Cisco Cloud-Delivered Catalyst SD-WAN
Hierarchical SD-WAN	Multi-Region Fabric