



High Availability

The goal of any high availability solution is to ensure that all network services are resilient to failure. Such a solution aims to provide continuous access to network resources by addressing the potential causes of downtime through functionality, design, and best practices. The core of the Cisco Catalyst SD-WAN high availability solution is achieved through a combination of three factors:

- **Functional hardware device redundancy.** The basic strategy consists of installing and provisioning redundant hardware devices and redundant components on the hardware. These devices are connected by a secure control plane mesh of Datagram Transport Layer Security (DTLS) connections among themselves, which allows for rapid failover should a device fail or otherwise become unavailable. A key feature of the Cisco Catalyst SD-WAN control plane is that it is established and maintained automatically, by the Cisco IOS XE Catalyst SD-WAN devices and software themselves.
- **Robust network design.**
- **Software mechanisms ensure rapid recovery from a failure.** To provide a resilient control plane, the Cisco Catalyst SD-WAN Overlay Management Protocol (OMP) regularly monitors the status of all Cisco IOS XE Catalyst SD-WAN devices in the network and automatically adjusts to changes in the topology as devices join and leave the network. For data plane resiliency, the Cisco Catalyst SD-WAN software implements standard protocol mechanisms, specifically Bidirectional Forwarding Detection (BFD), which runs on the secure IPsec tunnels between routers.

Recovery from a failure is a function of the time it takes to detect the failure and then repair or recover from it. The Cisco Catalyst SD-WAN solution provides the ability to control the amount of time to detect a failure in the network. In most cases, repair of the failure is fairly instantaneous.

Hardware Support of High Availability

A standard best practice in any network setup is to install redundant hardware at all levels, including duplicate parallel routers and other systems, redundant fans, power supplies and other hardware components within these devices, and backup network connections. Providing high availability in the Cisco Catalyst SD-WAN solution is no different. A network design that is resilient in the face of hardware failure should include redundant Cisco SD-WAN Validators, Cisco SD-WAN Controllers, and routers and any available redundant hardware components.

Recovery from the total failure of a hardware component in the Cisco Catalyst SD-WAN overlay network happens in basically the same way as in any other network. A backup component has been preconfigured, and it is able to perform all necessary functions by itself.

Robust Network Design

In addition to simple duplication of hardware components, the high availability of a Cisco Catalyst SD-WAN network can be enhanced by following best practices to design a network that is robust in the face of failure. In one such network design, redundant components are spread around the network as much as possible. Design practices include situating redundant Cisco SD-WAN Validators and Cisco SD-WAN Controllers at dispersed geographical locations and connecting them to different transport networks. Similarly, the routers at a local site can connect to different transport networks and can reach these networks through different NATs and DMZs.

Software Support of High Availability

The Cisco Catalyst SD-WAN software support for high availability and resiliency in the face of failure is provided both in the control plane, using the standard DTLS protocol and the proprietary Cisco Catalyst SD-WAN Overlay Management Protocol (OMP), and in the data plane, using the industry-standard protocols BFD, BGP, OSPF, and VRRP.

Control Plane Software Support of High Availability

The Cisco Catalyst SD-WAN control plane operates in conjunction with redundant components to ensure that the overlay network remains resilient if one of the components fails. The control plane is built on top of DTLS connections between the Cisco devices, and it is monitored by the Cisco Catalyst SD-WAN OMP protocol, which establishes peering sessions (similar to BGP peering sessions) between pairs of Cisco SD-WAN Controllers and routers, and between pairs of Cisco SD-WAN Controllers. These peering sessions allow OMP to monitor the status of the Cisco devices and to share the information among them so that each device in the network has a consistent view of the overlay network. The exchange of control plane information over OMP peering sessions is a key piece in the Cisco Catalyst SD-WAN high availability solution:

- Cisco SD-WAN Controllers quickly and automatically learn when a Cisco SD-WAN Validator or a router joins or leaves the network. They can then rapidly make the necessary modifications in the route information that they send to the routers.
- Cisco SD-WAN Validator quickly and automatically learn when a device joins the network and when a Cisco SD-WAN Controller controller leaves the network. They can then rapidly make the necessary changes to the list of Cisco SD-WAN Controller IP addresses that they send to routers joining the network.
- Cisco SD-WAN Validators learn when a domain has multiple Cisco SD-WAN Controllers controllers and can then provide multiple Cisco SD-WAN Controller addresses to routers joining the network.
- Cisco SD-WAN Controllers learn about the presence of other Cisco SD-WAN Controllers, and they all automatically synchronize their route tables. If one Cisco SD-WAN Controller fails, the remaining systems take over management of the control plane, simply and automatically, and all routers in the network continue to receive current, consistent routing and TLOC updates from the remaining Cisco SD-WAN Controllers.

Let's look at the redundancy provided by each of the Cisco Catalyst SD-WAN hardware devices in support of network high availability.

Recovering from a Failure in the Control Plane

The combination of hardware component redundancy with the architecture of the Cisco Catalyst SD-WAN control plane results in a highly available network, one that continues to operate normally and without interruption when a failure occurs in one of the redundant control plane components. Recovery from the total failure of a Cisco SD-WAN Controller, Cisco SD-WAN Validator, or router in the Cisco Catalyst SD-WAN

overlay network happens in basically the same way as the recovery from the failure of a regular router or server on the network: A preconfigured backup component is able to perform all necessary functions by itself.

In the Cisco Catalyst SD-WAN solution, when a network device fails and a redundant device is present, network operation continues without interruption. This is true for all Cisco devices, Cisco SD-WAN Validators, Cisco SD-WAN Controllers, and routers. No user configuration is required to implement this behavior; it happens automatically. The OMP peering sessions running between Cisco devices ensure that all the devices have a current and accurate view of the network topology.

Let's examine failure recovery device by device.

Data Plane Software Support for High Availability

For data plane resiliency, the Cisco Catalyst SD-WAN software implements the standard BFD protocol, which runs automatically on the secure IPsec connections between routers. These IPsec connections are used for the data plane, and for data traffic, and are independent of the DTLS tunnels used by the control plane. BFD is used to detect connection failures between the routers. It measures data loss and latency on the data tunnel to determine the status of the devices at either end of the connection.

BFD is enabled, by default, on connections between Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices. BFD sends Hello packets periodically (by default, every 1 second) to determine whether the session is still operational. If a certain number of the Hello packets are not received, BFD considers that the link has failed and brings the BFD session down (the default dead time is 3 seconds). When BFD sessions go down, any route that points to a next hop over that IPsec tunnel is removed from the forwarding table (FIB), but it is still present in the route table (RIB).

In the Cisco Catalyst SD-WAN software, you can adjust the Hello packet and dead time intervals. If the timers on the two ends of a BFD link are different, BFD negotiates to use the lower value.

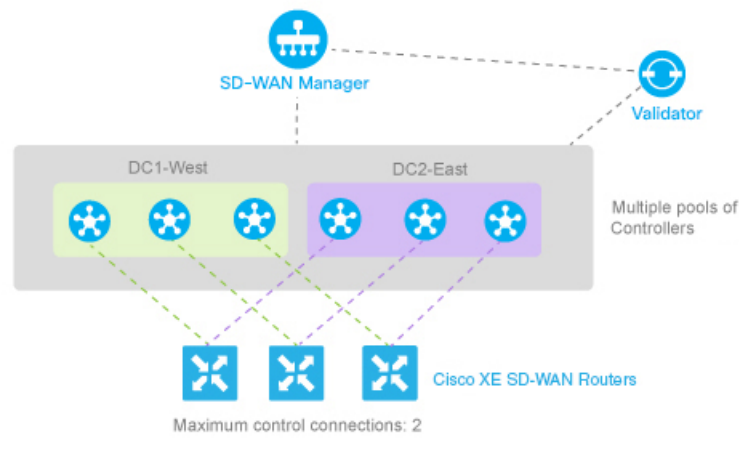
Using Affinity to Manage Network Scaling

In the Cisco Catalyst SD-WAN overlay network, all Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices establish control connections to Cisco SD-WAN Controllers, to ensure that the routers are always able to properly route data traffic across the network. As networks increase in size, with routers at thousands of sites and with Cisco SD-WAN Controllers in multiple data centers managing the flow of control and data traffic among routers, network operation can be improved by limiting the number of Cisco SD-WAN Controllers that a router can connect to. When data centers are distributed across a broad geography, network operation can also be better managed by having routers establish control connections only with the Cisco SD-WAN Controllers collocated in the same geographic region.

Establishing affinity between Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices allow you to control the scaling of the overlay network, by limiting the number of Cisco SD-WAN Controllers that a Cisco IOS XE Catalyst SD-WAN device can establish control connections (and form TLOCs) with. When you have redundant routers in a single data center, affinity allows you to distribute the Cisco IOS XE Catalyst SD-WAN device control connections across the Cisco SD-WAN Controllers.

Similarly, when you have multiple data centers in the overlay network, affinity allows you to distribute the control connections between edge devices and the Cisco SD-WAN Controller, across all data centers. This way, a Cisco IOS XE Catalyst SD-WAN device has controller redundancy and data center redundancy. If the link between a Cisco IOS XE Catalyst SD-WAN device and any one of the data centers goes down, the Cisco SD-WAN Controllers in the other data center are available to continue servicing the overlay network.

The following figure illustrates this scenario, showing three Cisco SD-WAN Controllers the two data centers. Each of the three Cisco IOS XE Catalyst SD-WAN devices establishes a control connection to one controller in the West data center and one in the East data center.



369846

You might think of the scenario in the figure above as one where there are redundant data centers in the same region of the world, such as in the same city, province, or country. For an overlay network that spans a larger geography, such as across a continent or across multiple continents, you can use affinity to limit the network scale either by restricting Cisco IOS XE Catalyst SD-WAN devices so that they connect only to local Cisco SD-WAN Controllers or by having

- [Cisco Catalyst SD-WAN Validator Redundancy, on page 4](#)
- [Cisco Catalyst SD-WAN Manager Server Redundancy, on page 5](#)
- [Cisco Catalyst SD-WAN Controller Redundancy, on page 9](#)
- [Cisco IOS XE Catalyst SD-WAN Device Redundancy, on page 10](#)
- [Configure Affinity Between Cisco Catalyst SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN Device, on page 11](#)

Cisco Catalyst SD-WAN Validator Redundancy

The Cisco SD-WAN Validator performs two key functions in the Cisco Catalyst SD-WAN overlay network:

- Authenticates and validates all Cisco SD-WAN Controllers and routers that attempt to join the Cisco Catalyst SD-WAN network.
- Orchestrates the control plane connections between the Cisco SD-WAN Controllers and routers, thus enabling Cisco SD-WAN Controller and routers to connect to each other in the Cisco Catalyst SD-WAN network.

The Cisco SD-WAN Validator runs as a VM on a network server.

Having multiple Cisco SD-WAN Validators ensures that one of them is always available whenever a Cisco device such as a router or a Cisco SD-WAN Controller is attempting to join the network.

Configuration of Redundant Cisco Catalyst SD-WAN Validators

A Cisco SD-WAN Controller learns that it is acting as a Cisco SD-WAN Validator from its configuration. In the **system vbond** configuration command, which defines the IP address (or addresses) of the Cisco SD-WAN Validator (or validators) in the Cisco Catalyst SD-WAN overlay network, you include the **local** option. In this command, you also include the local public IP address of the Cisco SD-WAN Validator, (Even though on Cisco IOS XE Catalyst SD-WAN device and Cisco SD-WAN Controllers you can specify an IP address

of Cisco SD-WAN Validator as a DNS name, on the Cisco SD-WAN Validator itself, you must specify it as an IP address.)

On Cisco SD-WAN Controllers, and Cisco IOS XE Catalyst SD-WAN devices, when the network has only a single Cisco SD-WAN Validator, you can configure the location of the Cisco SD-WAN Validator system either as an IP address or as the name of a DNS server (such as `vbond.cisco.com`). (Again, you configure this in the **system vbond** command.) When the network has two or more Cisco SD-WAN Validators and they must all be reachable, you should use the name of a DNS server. The DNS server then resolves the name to a single IP address that the Cisco SD-WAN Validator returns to the Cisco IOS XE Catalyst SD-WAN device. If the DNS name resolves to multiple IP addresses, the Cisco SD-WAN Validator returns them all to the Cisco IOS XE Catalyst SD-WAN device, and the router tries each address sequentially until it forms a successful connection.

Note that even if your Cisco Catalyst SD-WAN network has only a single Cisco SD-WAN Validator, it is recommended as a best practice that you specify a DNS name rather than an IP address in the **system vbond** configuration command, because this results in a scalable configuration. Then, if you add additional Cisco SD-WAN Validators to your network, you do not need to change the configurations on any of the routers or Cisco SD-WAN Controllers in your network.

Recovering from a Cisco Catalyst SD-WAN Validator Failure

In a network with multiple Cisco SD-WAN Validators, if one of them fails, the other Cisco SD-WAN Validators simply continue operating and are able to handle all requests by Cisco devices to join the network. From a control plane point of view, each Cisco SD-WAN Validator maintains a permanent DTLS connections to each of the Cisco SD-WAN Controllers in the network. (Note however, that there are no connections between the Cisco SD-WAN Validators themselves.) As long as one Cisco SD-WAN Validator is present in the domain, the Cisco Catalyst SD-WAN network is able to continue operating without interruption, because Cisco SD-WAN Controllers and routers are still able to locate each other and join the network.

Because Cisco SD-WAN Validators never participate in the data plane of the overlay network, the failure of any Cisco SD-WAN Validator has no impact on data traffic. Cisco SD-WAN Validators communicate with routers only when the routers are first joining the network. The joining router establishes a transient DTLS connection with a Cisco SD-WAN Validator to learn the IP address of a Cisco SD-WAN Controller. When the Cisco IOS XE Catalyst SD-WAN device configuration lists the Cisco SD-WAN Validator address as a DNS name, the router tries each of the Cisco SD-WAN Validators in the list, one by one, until it is able to establish a DTLS connection. This mechanism allows a router to always be able to join the network, even after one of a group of Cisco SD-WAN Validators has failed.

Cisco Catalyst SD-WAN Manager Server Redundancy

The Cisco SD-WAN Manager servers comprise a centralized network management system that enables configuration and management of the Cisco devices in the overlay network. It also provides a real-time dashboard into the status of the network and network devices. The Cisco SD-WAN Manager servers maintain permanent communication channels with all Cisco IOS XE Catalyst SD-WAN devices in the network. Over these channels, the Cisco SD-WAN Manager servers push out files that list the serial numbers of all valid devices, they push out the configuration of each device, and they push out new software images as part of a software upgrade process. From each network device, the Cisco SD-WAN Manager servers receive various status information that is displayed on the Cisco SD-WAN Manager **Monitor > Overview** page.



Note In Cisco vManage Release 20.6.1 and earlier releases, the status information is available on the **Dashboard > Main Dashboard** page.

A highly available Cisco Catalyst SD-WAN network contains three or more Cisco SD-WAN Manager servers in each domain. This scenario is referred to as a cluster of Cisco SD-WAN Manager servers, and each Cisco SD-WAN Manager server in a cluster is referred to as a Cisco SD-WAN Manager instance. Each Cisco SD-WAN Manager instance in a cluster can manage approximately 2000 devices, so a cluster of three Cisco SD-WAN Manager instances can manage up to 6000 devices. The Cisco SD-WAN Manager instances automatically load balances the devices that they manage. With three instances, the Cisco SD-WAN Manager cluster remains operational if one of the devices in that cluster fail.

For related information, see [Troubleshooting TechNotes](#).

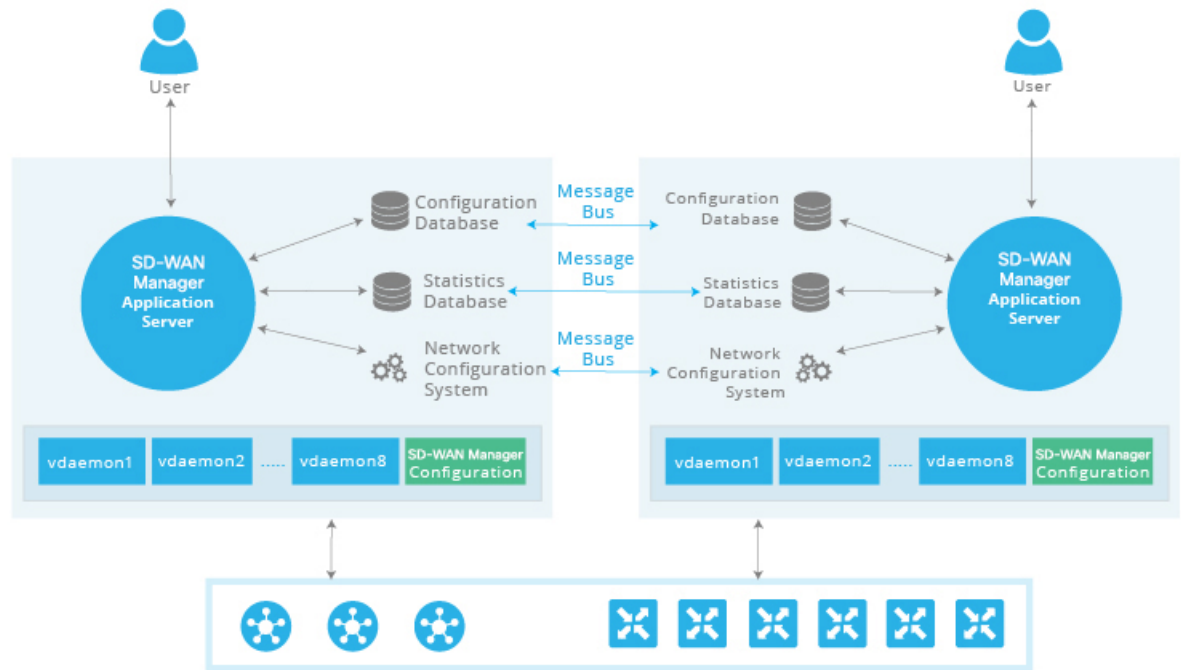
A Cisco SD-WAN Manager cluster consists of the following architectural components:

- Application server—This provides a web server for user sessions. Through these sessions, a logged-in user can view a high-level dashboard summary of networks events and status, and can drill down to view details of these events. A user can also manage network serial number files, certificates, software upgrades, device reboots, and configuration of the Cisco SD-WAN Manager cluster itself from the Cisco SD-WAN Manager application server.
- Configuration database—Stores the inventory and state and the configurations for all Cisco IOS XE Catalyst SD-WAN devices.
- Network configuration system—Stores all configuration information, policies, templates, certificates, and more.
- Statistics database—Stores the statistics information collected from all Cisco devices in the overlay network.
- Message bus—Communication bus among the different Cisco SD-WAN Manager instances. This bus is used to share data and coordinate operations among the Cisco SD-WAN Manager instances in the cluster.

The Statistics database and Configuration database services must run on an odd number of Cisco SD-WAN Manager instances, with a minimum of three. For these databases to be writeable, there must be a quorum of Cisco SD-WAN Manager instances running and they should be in sync. A quorum is a simple majority. For example, if you have a cluster of three Cisco SD-WAN Manager instances running these databases, then two must be running and in sync. Initially, all Cisco SD-WAN Manager instances run the same services. However, you can choose not to run some services on some instances. From the **Cluster Management** window, you can select the services that can run on each Cisco SD-WAN Manager instance. You can add a fourth Cisco SD-WAN Manager instance to load balance more Cisco IOS XE Catalyst SD-WAN devices. In such a case, disable the statistics database and configuration database on one of the instances Cisco SD-WAN Manager because those services need to run on an odd number of instances. Optionally, you can run the configuration database on a single instance to reduce the amount of information shared between the devices and reduce load.

The following figure shows the interaction between Cisco SD-WAN Manager instances in a cluster, although a minimum of three devices are required. The figure illustrates the Cisco SD-WAN Manager services that synchronize between the Cisco SD-WAN Manager instances. Also in this figure, you see that each Cisco SD-WAN Manager instance resides on a virtual machine (VM). The VM can have from one to eight cores,

with a Cisco Catalyst SD-WAN software process (vdaemon) running on each core. In addition, the VM stores the actual configuration for the Cisco SD-WAN Manager server itself.



The Cisco SD-WAN Manager cluster implements an active-active architecture in the following way:

- Each of the Cisco SD-WAN Manager instance in the cluster is an independent processing node.
- All Cisco SD-WAN Manager instances are active simultaneously.
- All user sessions to the application server are load balanced by using an external load balancer.
- All control sessions between the Cisco SD-WAN Manager application servers and the routers are load balanced. A single Cisco SD-WAN Manager instance can manage a maximum of about 2000 Cisco IOS XE Catalyst SD-WAN devices. However, all the controller sessions—the sessions between the Cisco SD-WAN Manager instances and the Cisco Catalyst SD-WAN Controllers, the sessions between the Cisco SD-WAN Manager instances and the Cisco Catalyst SD-WAN Validators are arranged in a full-mesh topology.
- The configuration and statistics databases can be replicated across Cisco SD-WAN Manager instances, and these databases can be accessed and used by all the Cisco SD-WAN Manager instances.
- If one of the Cisco SD-WAN Manager instances in the cluster fails or otherwise becomes unavailable, the network management services that are provided by the Cisco SD-WAN Manager server are still fully available across the network.

The message bus among the Cisco SD-WAN Manager instances in the cluster allows all the instances to communicate using an out-of-band network. This design, which leverages a third vNIC on the Cisco SD-WAN Manager VM, avoids using WAN bandwidth for management traffic.

You configure the Cisco SD-WAN Manager cluster from the Cisco SD-WAN Manager web application server. During the configuration process, you can configure each Cisco SD-WAN Manager instance that can run the following services:

- Application server—Each Cisco SD-WAN Manager server runs an application server instance.
- Configuration database—Within the Cisco SD-WAN Manager cluster, no more than three iterations of the configuration database can run.
- Load balancer—The Cisco SD-WAN Manager cluster requires a load balancer to distribute user login sessions among the Cisco SD-WAN Manager instances in the cluster. As mentioned, a single Cisco SD-WAN Manager instance can manage a maximum of about 2000 WAN edge devices.
- Messaging server—We recommend that you configure each Cisco SD-WAN Manager instance to run the message bus so that all the instances in the cluster can communicate with each other.
- Statistics database—Within a Cisco SD-WAN Manager cluster, no more than three iterations of the statistics database can run.
- Coordination server: It's used internally by the Messaging server.

The following are the design considerations for a Cisco SD-WAN Manager cluster:

- A Cisco SD-WAN Manager cluster should consist of a minimum of three Cisco SD-WAN Manager instances.
- The application server and message bus should run on all Cisco SD-WAN Manager instances.
- Within a cluster, a maximum of three instances of the configuration database and three instances of the statistics database can run. However, any individual Cisco SD-WAN Manager instance can run both, one, or none of these two databases.
- To provide the greatest availability, we recommend that you run the configuration and statistics databases on three Cisco SD-WAN Manager instances.

See the [Cluster Management](#) chapter in the *Cisco Getting Started Guide* for more information about deploying and managing the Cisco SD-WAN Manager instances of a cluster.

Cisco Catalyst SD-WAN Manager Backups

Cisco manages Cisco SD-WAN Manager by taking regular snapshots of the devices for recovery due to a catastrophic failure or corruption. The frequency and retention of these snapshots are set for each overlay. Generally, the snapshots are taken daily and retained for up to 10 days. For certain scheduled maintenance activities, such as the upgrade of the devices, another snapshot can be taken before the scheduled activity. In all other cases, it's your responsibility to take regular backups of the Cisco SD-WAN Manager configuration database and snapshots of the Cisco SD-WAN Manager virtual machine, and follow the example of frequency and retention that is followed by Cisco.

Cisco Catalyst SD-WAN Manager Database Backup

Although the Cisco SD-WAN Manager cluster provides high availability and a level of fault tolerance, regular backup of the configuration database should be taken and stored securely off-site. Cisco SD-WAN Manager doesn't have a mechanism of automating the collection of a configuration database backup on a schedule and copying it to another server. The greater the time between the backup and when it's needed for a recovery, the greater the risk that data might be lost. Perform configuration database backups often. Use the following command to create a configuration database backup file.


```
request nms configuration-db backup path <path>
```

Cisco Catalyst SD-WAN Controller Redundancy

Cisco Catalyst SD-WAN Controller Redundancy

The Cisco SD-WAN Controllers are the central orchestrators of the control plane. They have permanent communication channels with all the Cisco devices in the network. Over the DTLS connections between the Cisco SD-WAN Controllers and Cisco SD-WAN Validators and between pairs of Cisco SD-WAN Controllers, the devices regularly exchange their views of the network, to ensure that their route tables remain synchronized. The Cisco SD-WAN Controllers pass accurate and timely route information over DTLS connections to Cisco IOS XE Catalyst SD-WAN device.

A highly available Cisco Catalyst SD-WAN network contains two or more Cisco SD-WAN Controllers in each domain. A Cisco Catalyst SD-WAN domain can have up to 20 Cisco SD-WAN Controllers, and each router, by default, connects to two of them. When the number of Cisco SD-WAN Controllers in a domain is greater than the maximum number of controllers that a domain's routers are allowed to connect to, the Cisco Catalyst SD-WAN software load-balances the connections among the available Cisco SD-WAN Controllers.

While the configurations on all the Cisco SD-WAN Controllers must be functionally similar, the control policies must be identical. This is required to ensure that, at any time, all Cisco IOS XE Catalyst SD-WAN devices receive consistent views of the network. If the control policies are not absolutely identical, different Cisco SD-WAN Controllers might give different information to a Cisco IOS XE Catalyst SD-WAN device, and the likely result will be network connectivity issues.



Note To reiterate, the Cisco Catalyst SD-WAN overlay network works properly only when the control policies on all Cisco SD-WAN Controllers are identical. Even the slightest difference in the policies will result in issues with the functioning of the network.

To remain synchronized with each other, the Cisco SD-WAN Controllers establish a full mesh of DTLS control connections, as well as a full mesh of OMP sessions, between themselves. Over the OMP sessions, the Cisco SD-WAN Controllers advertise routes, TLOCs, services, policies, and encryption keys. It is this exchange of information that allows the Cisco SD-WAN Controllers to remain synchronized.

You can place Cisco SD-WAN Controllers anywhere in the network. For availability, it is highly recommended that the Cisco SD-WAN Controllers be geographically dispersed.

Each Cisco SD-WAN Controller establishes a permanent DTLS connection to each of the Cisco SD-WAN Validators. These connections allow the Cisco SD-WAN Validators to track which Cisco SD-WAN Controllers are present and operational. So, if one of the Cisco SD-WAN Controller fails, the Cisco SD-WAN Validator does not provide the address of the unavailable Cisco SD-WAN Controller to a router that is just joining the network.

To reiterate, the Cisco Catalyst SD-WAN overlay network works properly only when the control policies on all Cisco SD-WAN Controllers are identical. Even the slightest difference in the policies result in issues with the functioning of the network.

Recovering from a Cisco Catalyst SD-WAN Controller Failure

The Cisco SD-WAN Controllers are the primary controllers of the network. To maintain this control, they maintain permanent DTLS connections to all the Cisco SD-WAN Validators and Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices. These connections allow the Cisco SD-WAN Controllers to be constantly aware of any changes in the network topology. When a network has multiple Cisco SD-WAN Controllers:

- There is a full mesh of OMP sessions among the Cisco SD-WAN Controllers.
- Each Cisco SD-WAN Controller has a permanent DTLS connection to each Cisco SD-WAN Validator.
- The Cisco SD-WAN Controllers have permanent TLS or DTLS connections to the Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices.

If one of the Cisco SD-WAN Controllers fails, the other Cisco SD-WAN Controllers seamlessly take over handling control of the network. The remaining Cisco SD-WAN Controllers are able to work with Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices joining the network and are able to continue sending route updates to the routers. As long as one Cisco SD-WAN Controller is present and operating in the domain, the Cisco Catalyst SD-WAN network may continue operating without interruption.

Cisco IOS XE Catalyst SD-WAN Device Redundancy

The Cisco IOS XE Catalyst SD-WAN device is commonly used in two ways in the Cisco Catalyst SD-WAN network: to be the Cisco Catalyst SD-WAN routers at a branch site, and to create a hub site that branch routers connect to.

A branch site can have two or more Cisco IOS XE Catalyst SD-WAN devices for redundancy. Each of the router maintains the following connections:

- A secure control plane connection, via a TLS or DTLS connection, with one or more Cisco SD-WAN Controllers in its domain.
- A secure data plane connection with the other routers.

Because both the routers receive the same routing information from the Cisco SD-WAN Controllers, each one is able to continue to route traffic if one fails, even if they are connected to different transport providers.

When using Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices in a hub site, you can provide redundancy by installing two Cisco IOS XE Catalyst SD-WAN devices. The branch routers need to connect to each of the hub routers by using separate DTLS connections.

You can also have Cisco IOS XE Catalyst SD-WAN device provide redundancy by configuring up to tunnel interfaces on a single router. Each tunnel interface can go through the same or different firewalls, service providers, and network clouds, and each maintains a secure control plane connection, by means of a DTLS tunnel, with the Cisco SD-WAN Controllers in its domain.

Recovering from a Cisco IOS XE Catalyst SD-WAN Device Failure

The route tables on Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices are populated by OMP routes received from the Cisco SD-WAN Controllers. For a site or branch with redundant routers, the route tables on both routers remain synchronized, so if either of the routers fail, the other one continues to be able to route data traffic to its destination.

Configure Affinity Between Cisco Catalyst SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN Device

One way to manage network scale is to configure affinity between Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices. To do this, you place each Cisco SD-WAN Controller into a controller group, and then you configure which group or groups a Cisco IOS XE Catalyst SD-WAN device can establish control connections with. The controller groups are what establishes the affinity between Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN device.

Configure Controller Group Identifier on Cisco Catalyst SD-WAN Controllers

To participate in affinity, each Cisco SD-WAN Controller must be assigned a controller group identifier:

```
vSmart(config)#system controller-group-id number
```

The identifier number can be from 0 through 100.

For Cisco SD-WAN Controllers in the same data center, they can have the same controller group identifier or different identifiers:

- If the Cisco SD-WAN Controllers have the same controller group identifier, a Cisco IOS XE Catalyst SD-WAN device establishes a control connection to any one of them. If that Cisco SD-WAN Controller becomes unreachable, the router simply establishes a control connection with another one of the controllers in the data center. As an example of how this might work, if one Cisco SD-WAN Controller becomes unavailable during a software upgrade, the Cisco IOS XE Catalyst SD-WAN device immediately establishes a new TLOC with another Cisco SD-WAN Controller, and the router's network operation is not interrupted. This network design provides redundancy among Cisco SD-WAN Controllers in a data center.
- If the Cisco SD-WAN Controllers have different controller group identifiers, a Cisco IOS XE Catalyst SD-WAN device can use one controller as the preferred and the other as backup. As an example of how this might work, if you are upgrading the Cisco SD-WAN Controller software, you can upgrade one controller group at a time. If a problem occurs with the upgrade, a Cisco IOS XE Catalyst SD-WAN device establishes TLOCs with the Cisco SD-WAN Controllers in the second, backup controller group, and the router's network operation is not interrupted. When the Cisco SD-WAN Controller in the first group again becomes available, the Cisco IOS XE Catalyst SD-WAN device switches its TLOCs back to that controller. This network design, while offering redundancy among the Cisco SD-WAN Controllers in a data center, also provides additional fault isolation.

Configure Affinity on Cisco IOS XE Catalyst SD-WAN Device

For a Cisco IOS XE Catalyst SD-WAN device to participate in affinity, you configure the Cisco SD-WAN Controllers that the router is allowed to establish control connections with, and you configure the maximum number of control connections (or TLOCs) that the Cisco IOS XE Catalyst SD-WAN device itself, and that an individual tunnel on the router, is allowed to establish.

Configure Cisco Catalyst SD-WAN Controller Groups

Configuring the Cisco SD-WAN Controllers that the router is allowed to establish control connections is a two-part process:

- At the system level, configure a single list of the controller group identifiers that are present in the overlay network.
- For each tunnel interface, you can choose to restrict which controller group identifiers the tunnel interface can establish control connections with. To do this, configure an exclusion list.

At a system level, configure the identifiers of the Cisco SD-WAN Controller groups:

```
ISR4331(config)#system controller-group-list numbers
```

List the Cisco SD-WAN Controller group identifiers that any of the tunnel interfaces on the Cisco IOS XE Catalyst SD-WAN device might want to establish control connections with. It is recommended that this list contain the identifiers for all the Cisco SD-WAN Controller groups in the overlay network.

If you want a specific tunnel interface to establish control connections to only a subset of all the Cisco SD-WAN Controller groups, configure the group identifiers to exclude:

```
ISR4331(config-interface-GigabitEthernet0/0/1)#tunnel-interface exclude-controller-group-list numbers
```

```
ISR4331(config-sdwan)# interface GigabitEthernet0/0/1 tunnel-interface  
exclude-controller-group-list numbers
```

This command lists the identifiers of the Cisco SD-WAN Controller groups that this particular tunnel interface should not establish control connections with, when a Cisco SD-WAN Controller is available in configured controller groups. Ensure that the controller groups in this list are a subset of the controller groups that are configured with the **system controller-group-list** command.

To display the controller groups configured on a Cisco IOS XE Catalyst SD-WAN device, use the **show sdwan running-config system** command.

Configure Maximum Number of Control Connections

By default, the maximum number of control connections that each tunnel interface can establish is the same as the maximum number of OMP sessions that is configured on the Cisco IOS XE Catalyst SD-WAN device. The default value for MOS is 2.

Configuring the maximum number of control connections for a tunnel interface for a Cisco IOS XE Catalyst SD-WAN device is a two-part process:

- At the system level, configure the MOS that the Cisco IOS XE Catalyst SD-WAN device can establish to Cisco SD-WAN Controllers.
- If a tunnel interface needs to connect to a different number Cisco SD-WAN Controllers than the configured MOS value, configure the maximum number of control connections that the tunnel can establish to Cisco SD-WAN Controllers,



Note If MCC is not configured on a tunnel interface, its default value is the same as the MOS value.

Effectively, the maximum number of control connections a tunnel interface in a Cisco IOS XE Catalyst SD-WAN device can establish is determined by the following formula:

Max Control Connections for tunnel interface in VPN 0 = MIN(MOS, MCC)

To modify the maximum number of OMP sessions, enter the following command:

```
Device (Config)# system max-omp-sessions number
```

A Cisco IOS XE Catalyst SD-WAN device establishes OMP sessions as follows:

- The device, not the individual tunnel interfaces, establishes OMP sessions with Cisco SD-WAN Controllers.
- When different tunnel interfaces on a router connect to the same Cisco SD-WAN Controller, the device creates a single OMP session with the Cisco SD-WAN Controller and the different tunnel interfaces use this single OMP session.



Note When each tunnel interface connects to the same set of Cisco SD-WAN Controllers, a Cisco IOS XE Catalyst SD-WAN device has the total number of OMP sessions equal to the configured maximum number of OMP sessions. However, if each tunnel interface connects to a different Cisco SD-WAN Controller (because of an excluded controller list), the total number of OMP sessions on the device is higher than the configured maximum number of OMP sessions,

Use the following command to modify the maximum number of control connections for a tunnel interface:

```
Device (config)#sdwan interface interface-name tunnel-interface max-control-connections number
```

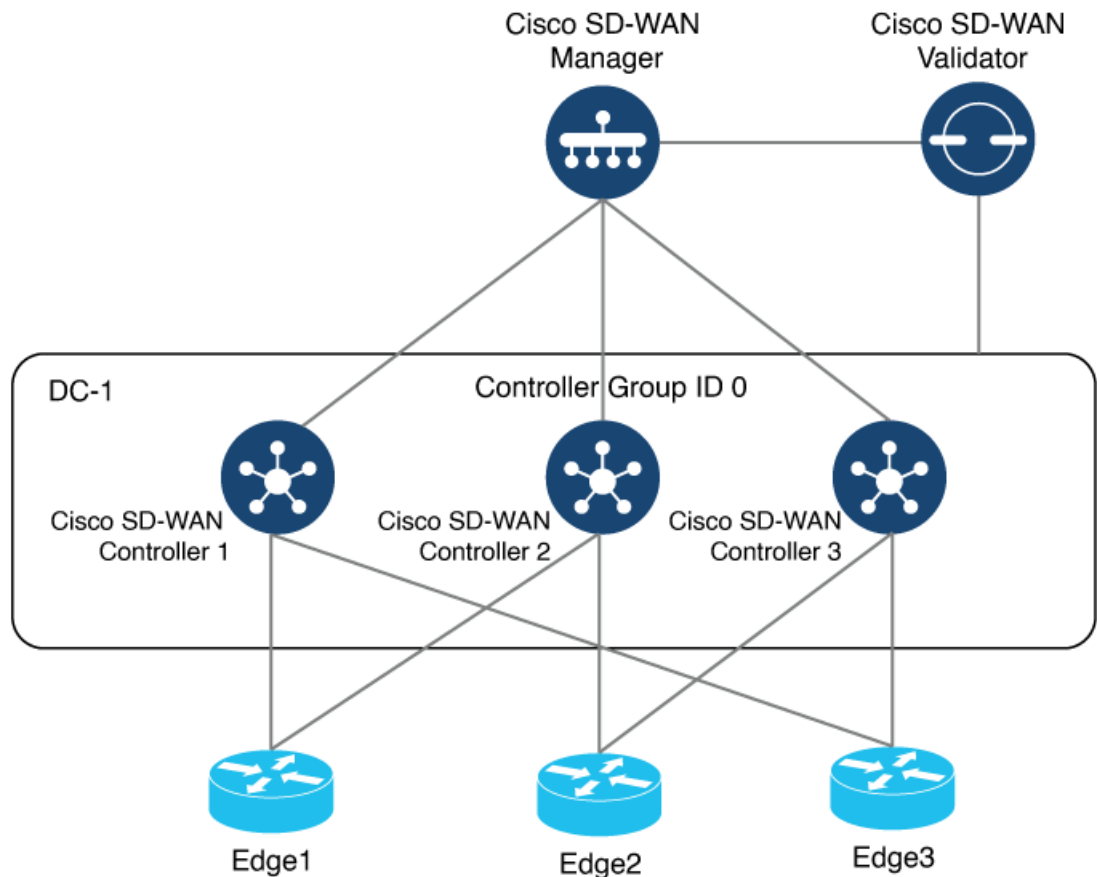
The number of control connections can be from 0 through 100. The default value is the maximum number of OMP sessions that is configured with the **system max-omp-sessions** command.

To display the actual number of control connections for each tunnel interface, use the **show sdwan control affinity config** command.

To display a list of the Cisco SD-WAN Controllers that each tunnel interface has established control connections with, use the **show sdwan control affinity status** command.

Configure Affinity for Cisco Catalyst SD-WAN Controllers on Single Data Center

In a Cisco Catalyst SD-WAN overlay network that has multiple Cisco SD-WAN Controllers, each tunnel interface in a Cisco IOS XE Catalyst SD-WAN device establishes control connections to two Cisco SD-WAN Controllers. This default behavior provides controller redundancy, so there is no need to configure affinity.



In the topology that is shown in the figure above, there are three Cisco SD-WAN Controllers in Data Center DC-1, all of which belong to default controller group 0. A Cisco IOS XE Catalyst SD-WAN device selects two Cisco SD-WAN Controllers, which are identified as its assigned Cisco SD-WAN Controllers. Each tunnel interface of the Cisco IOS XE Catalyst SD-WAN device connects to these assigned Cisco SD-WAN Controllers. When a tunnel interface connects to its assigned Cisco SD-WAN Controller, that tunnel interface is said to be in *equilibrium*.



Note If `exclude-controller-group-list` is configured on a tunnel interface, that tunnel interface may have different Cisco SD-WAN Controllers assigned to it.

However, if you want to connect the Cisco IOS XE Catalyst SD-WAN device only to a subset of the Cisco SD-WAN Controllers in a data center, you can use affinity. Place the Cisco SD-WAN Controllers in different controller groups, and then configure the Cisco IOS XE Catalyst SD-WAN device with a list of controller groups that it can connect to. This design provides redundant control connections to the Cisco SD-WAN Controller and provides fault isolation among the Cisco SD-WAN Controller groups in the same data center.

In the topology that is shown in the figure above, assume that you want edge devices to connect to Cisco SD-WAN Controllers as follows:

- Edge1 connects only to Cisco SD-WAN Controller 1 and Cisco SD-WAN Controller 2
- Edge2 connects only to Cisco SD-WAN Controller 2 and Cisco SD-WAN Controller 3

- Edge3 connects only to Cisco SD-WAN Controller 1 and Cisco SD-WAN Controller 3

To achieve these connections, configure Cisco SD-WAN Controller 1 with controller group ID 1:

```
vSmart(config)# system controller-group-id 1
```

To verify the configuration, use the **show running-config** command:

```
vSmart# show running-config system  
system  
description          "vSmart in data center 1"  
host-name            vSmart  
gps-location latitude 37.368140  
gps-location longitude -121.913658  
system-ip            172.16.255.19  
site-id              100  
controller-group-id 1  
organization-name    "Cisco"  
clock timezone       America/Los_Angeles
```

Use the following commands to configure the other Cisco SD-WAN Controllers:

```
vSmart2(config)# system controller-group-id 2
```

```
vSmart3(config)# system controller-group-id 3
```

In this example, each Cisco SD-WAN Controller in the data center is added to its own controller group. Alternatively, you can add multiple Cisco SD-WAN Controllers to the same controller group.



Note When Cisco SD-WAN Controllers are assigned to controller groups, we recommend that you assign controller groups for all Cisco SD-WAN Controllers in the overlay network.

Next, because you want Edge1 to connect only to Cisco SD-WAN Controller 2 and Cisco SD-WAN Controller 3, configure Edge1 as follows:

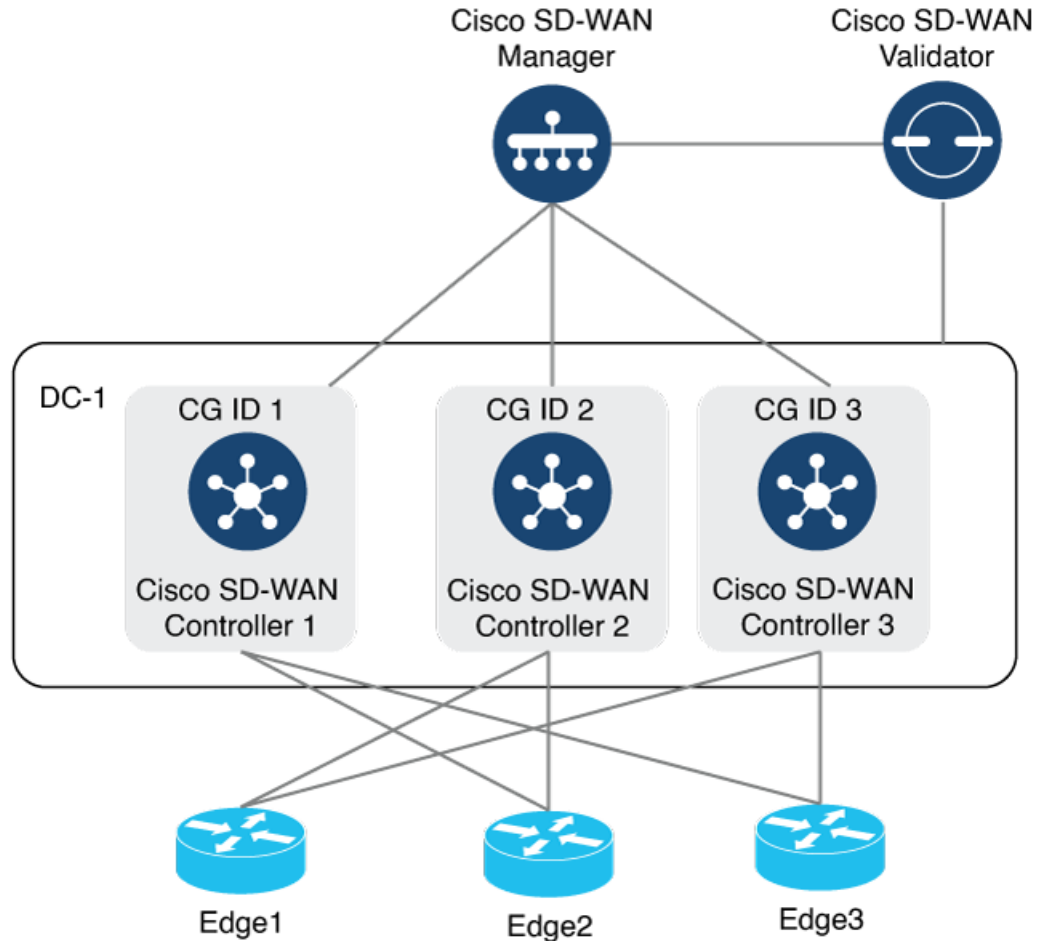
```
Edge1(config)# system controller-group-list 2 3
```

Configure Edge2 to connect only to Cisco SD-WAN Controller 1 and Cisco SD-WAN Controller 2:

```
Edge2(config)# system controller-group-list 1 2
```

Configure Edge3 to connect only to Cisco SD-WAN Controller 1 and Cisco SD-WAN Controller 3:

```
Edge3(config)# system controller-group-list 1 3
```

To display the control connections with the Cisco SD-WAN Controllers, use the **show sdwan control connections** command. The last column on the output, **Controller Group ID**, lists the Cisco SD-WAN Controller group that a router is in.

```
Edge1# show sdwan control connections
```

PEER TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER			PEER			LOCAL COLOR	PROXY	STATE	UPTIME	CONTROLLER
					PRIVATE IP	PORT	PUBLIC IP	PORT	ORGANIZATION	GROUP ID					
vsmart	tls	172.16.255.27	200	1	10.0.12.27	23456	10.0.12.27	23456	Cisco	default	No	up	0:00:18:34	3	
vsmart	tls	172.16.255.20	200	1	10.0.12.20	23456	10.0.12.20	23456	Cisco	default	No	up	0:00:18:33	2	
vmanage	tls	172.16.255.22	200	0	10.0.12.22	23656	10.0.12.22	23656	Cisco	default	No	up	0:00:18:34	0	

To display the maximum number of control connections allowed on the router, use the **show sdwan control local-properties** command. The last line of the output lists the maximum controllers. The following is the abbreviated output for this command:

```
Edge1# show sdwan control local-properties
personality                vedge
sp-organization-name       Cisco
organization-name          Cisco
root-ca-chain-status        Installed
root-ca-crl-status          Not-Installed

certificate-status           Installed
certificate-validity         Valid
...
```

INTERFACE REG	PUBLIC IPv4	PUBLIC PORT	PRIVATE IPv4	PRIVATE IPv6	PRIVATE PORT	VS/VM COLOR	STATE	MAX CNTRL	RESTRICT/ CONTROL/	LR/LB	LAST CONNECTION	SPI REMAINING	TIME	NAT TYPE	VM CON
										STUN			PRF		

GigabitEthernet1 Default	10.1.15.15	12386	10.1.15.15	::	12386	2/1	default	up	2	no/yes/no	No/No	0:00:47:59	0:11:11:43	N	5

These two commands display information about the control connections established by the affinity configuration. To see, for each interface, which controller groups are configured and which Cisco SD-WAN Controller the interface is connected to, use the **show sdwan control affinity config** command:

```
Edge1# show sdwan control affinity config

EFFECTIVE CONTROLLER LIST FORMAT - G(C),...      - Where G is the Controller Group ID
                                                C is the Required vSmart Count

CURRENT CONTROLLER LIST FORMAT   - G(c)s,...    - Where G is the Controller Group ID
                                                c is the current vSmart count
                                                s Status Y when matches, N when
does not match
```

INDEX	INTERFACE	VS COUNT	EFFECTIVE CONTROLLER LIST	CURRENT CONTROLLER LIST	LAST-RESORT EQUILIBRIUM INTERFACE
0	GigabitEthernet1 No	2	2(1),3(1)	2(1)Y,3(1)Y	Yes

The command output above shows that affinity is configured on interface GigabitEthernet1:

Table 1:

Field	Description
Effective Required VS Count	Shows that the interface is configured to create two control connections, and two control connections have been established.
Effective Controller List	Shows that affinity on the interface is configured to use one Cisco SD-WAN Controller from Controller Group 1, shown as 1(1), and one Cisco SD-WAN Controller from Controller Group 2, shown as 2(1). You configure the affinity controller identifiers with the controller-group-list command (at the system level) and, for the tunnel interface, the exclude-controller-group-list command.
Current Controller List	Lists the actual affinity configuration for the interface. The output here shows that the interface has two control connections with Cisco SD-WAN Controller in group 1 and another control connection. The “Y” indicates that the current and effective controller lists match each other.

Field	Description
Equilibrium	Indicates that the current controller lists match what is expected from the affinity configuration for that tunnel interface.

To determine the exact Cisco Catalyst SD-WAN Controllers with which the tunnel interface has established control connections, use the **show control affinity status** command:

```
Edge1# show sdwan control affinity status

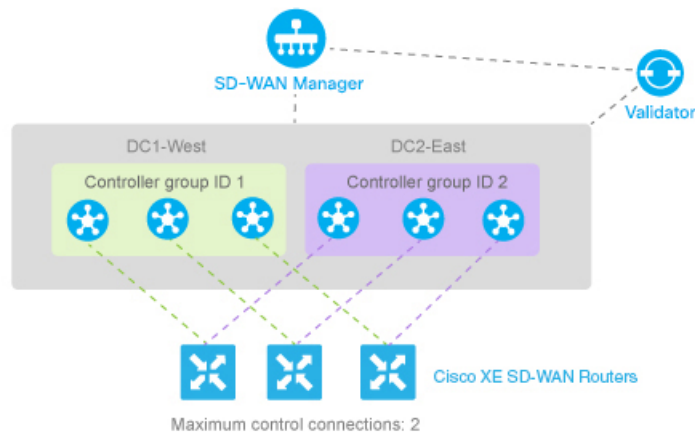
ASSIGNED CONNECTED CONTROLLERS - System IP( G),.. - System IP of the assigned vSmart
                                belongs to          G is the group ID to which the vSmart
UNASSIGNED CONNECTED CONTROLLERS - System IP( G),.. - System IP of the unassigned vSmart
                                belongs to          G is the group ID to which the vSmart

INDEX INTERFACE      ASSIGNED CONNECTED CONTROLLERS      UNASSIGNED CONNECTED CONTROLLERS
-----
0      GigabitEthernet1      172.16.255.20 (2),172.16.255.27 (3)
```

The command output above shows that interface **GigabitEthernet1** has control connections to two Cisco SD-WAN Controllers, 172.16.255.20, which is in group 1, and 172.16.255.27, which is in group 2. These Cisco SD-WAN Controllers are assigned for this device as indicated by the **Assigned Connected Controller** column. If the interface were connected to a Cisco SD-WAN Controller other than these two, it would be listed in the **Unassigned Connected Controllers** column and the tunnel interface would not be in equilibrium.

Configure Affinity for Cisco Catalyst SD-WAN Controllers on Two Data Centers

You can use affinity to enable redundancy among data centers, for a network design in which multiple Cisco SD-WAN Controllers are spread across two or more data centers. Then, if the link between a Cisco IOS XE Catalyst SD-WAN device and one of the data centers goes down, the Cisco SD-WAN Controllers in the second data center are available to continue servicing the overlay network. The figure below illustrates this scenario, showing three Cisco SD-WAN Controllers in each of two data centers. Each of the three Cisco IOS XE Catalyst SD-WAN devices establishes a control connection to one controller in the West data center and one in the East data center.



You configure the three Cisco SD-WAN Controllers in DC1-West with controller group identifier 1:

```
vSmart-DC1(config)# system controller-group-id 1
```

The three Cisco SD-WAN Controllers in DC2-East are in controller group 2:

```
vSmart-DC2(config)# system controller-group-id 2
```

We want all the Cisco IOS XE Catalyst SD-WAN devices to have a maximum of two OMP sessions, and we want each tunnel interface to have a maximum of two control connections and to not exclude any controller groups. So the only configuration that needs to be done on the routers is to set the controller group list. We want Cisco IOS XE Catalyst SD-WAN devices in the west to prefer Cisco Catalyst SD-WAN Controllers in DC1-West over DC2-East:

```
ISR4331-West(config)# system controller-group-list 1 2
```

Similarly, we want Cisco IOS XE Catalyst SD-WAN devices in the East to prefer DC2-East:

```
ISR4331-East(config)# system controller-group-list 2 1
```

The software evaluates the controller group list in order, so with this configuration, the Cisco IOS XE Catalyst SD-WAN devices-West prefer Cisco SD-WAN Controller group 1 (which is the West data center), and the Cisco IOS XE Catalyst SD-WAN devices - East prefer Cisco SD-WAN Controller group 2.

When a Cisco IOS XE Catalyst SD-WAN devices-West router needs to connect to only one Cisco SD-WAN Controller (based on configuration), it connects only to the West data center. If the router needs to connect to two Cisco SD-WAN Controllers, it connects to one Cisco SD-WAN Controller from the West data center and another Cisco SD-WAN Controller from the East data center.

You can fine-tune the controller group preference in other ways:

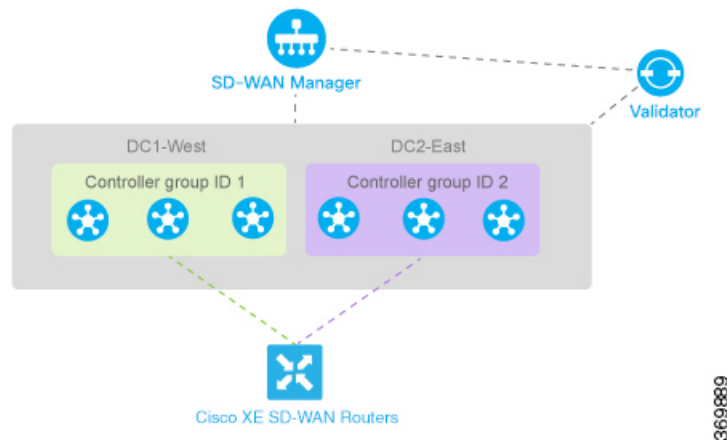
- Set the maximum number of OMP sessions allowed on the router to 1 (**system max-omp-sessions 1**). To illustrate how this works, let's look at a Cisco IOS XE Catalyst SD-WAN devices - West. The router has only one tunnel interface, and that interface creates one control connection to Cisco SD-WAN Controller list 1. If all the Cisco SD-WAN Controllers in this group become unavailable, or if the connection between the router that the DC1-West data center goes down, the tunnel interface establishes one control connection to Cisco SD-WAN Controller list 2, because this group is listed in the **system controller-group-list** command.
- Set the maximum number of control connections that the tunnel interface can establish to 1 (**sdwan interface interface-name tunnel-interface max-control-connections 1**). Because the software evaluates the controller group list in order, for a Cisco IOS XE Catalyst SD-WAN devices - West, this configuration

forces the tunnel interface to establish a control connection to Cisco SD-WAN Controller group 1. Again, if this controller group or data center becomes unreachable, the tunnel establishes a control connection with controller group 2, because this group is configured in the **system controller-group-list** command.

- Exclude the non-preferred Cisco SD-WAN Controller group for a particular tunnel. For example, for a Cisco IOS XE Catalyst SD-WAN devices -West to prefer controller group 1, you configure **sdwan interface interface-name tunnel-interface exclude-controller-group-list 2**. As with the above configurations, if this controller group or West data center becomes unreachable, the tunnel establishes a control connection with controller group 2, because this group is configured in the **system controller-group-list** command.

Configure Redundant Control Connections on Single Device

When a Cisco IOS XE Catalyst SD-WAN device has two tunnel connections and the network has two (or more) data centers, you can configure redundant control connections from the Cisco IOS XE Catalyst SD-WAN device to Cisco SD-WAN Controllers in two of the data centers. It is recommended that do this using the minimum number of OMP sessions—in this case, two. To do this, you configure one of the tunnel interfaces to go only to one of the data centers and the other to go only to the second. This configuration provides Cisco SD-WAN Controller redundancy with the minimum number of OMP sessions.



On the Cisco IOS XE Catalyst SD-WAN device router, define the controller group list and configure the maximum number of OMP sessions to be 2:

```
ISR4331(config)# system controller-group-list 1 2
ISR4331(config)# system max-omp-sessions 2
```

For one of the tunnels, you can use the default affinity configuration (that is, there is nothing to configure) to have this tunnel prefer a Cisco Catalyst SD-WAN Controller in group 1. You can also explicitly force this tunnel to prefer Cisco Catalyst SD-WAN Controller group 1:

```
ISR4331(config-tunnel-interface-1)# max-control-connections 1
```

You do not need to configure **exclude-controller-group-list 2**, because the software evaluates the controller group list in order, starting with group 1. However, you could choose to explicitly exclude Cisco SD-WAN Controller group 2.

Then, on the second tunnel, configure it to prefer a Cisco SD-WAN Controller in group 2. As with the other tunnel, you limit the maximum number of control connections to 1. In addition, you have to exclude controller group 1 for this tunnel.

```
ISR4331(config-tunnel-interface-2)# max-control-connections 1
ISR4331(config-tunnel-interface-2)# exclude-controller-group-list 1
```

Configure Control Plane and Data Plane High Availability Parameters

This topic discusses the configurable high availability parameters for the control plane and the data plane.

Control Plane High Availability

A highly available Cisco Catalyst SD-WAN network contains two or more Cisco SD-WAN Controllers in each domain. A Cisco Catalyst SD-WAN domain can have up to 20 Cisco SD-WAN Controllers, and each Cisco IOS XE Catalyst SD-WAN device, by default, connects to two of them. You change this value on a per-tunnel basis:

```
ISR4331(config)# sdwan interface interface-name tunnel-interface max-control-connections
number
```

When the number of Cisco SD-WAN Controllers in a domain is greater than the maximum number of controllers that a domain's Cisco IOS XE Catalyst SD-WAN devices are allowed to connect to, the Cisco Catalyst SD-WAN software load-balances the connections among the available Cisco SD-WAN Controllers.



Note To maximize the efficiency of the load-balancing among Cisco SD-WAN Controllers, use sequential numbers when assigning system IP addresses to the Cisco IOS XE Catalyst SD-WAN devices in the domain. One example of a sequential numbering schemes is 172.1.1.1, 172.1.1.2, 172.1.1.3, and so forth. Another is 172.1.1.1.1, 172.1.2.1, 172.1.3.1, and so forth.

Data Plane High Availability

BFD, which detects link failures as part of the Cisco Catalyst SD-WAN high availability solution, is enabled by default on all Cisco devices. BFD runs automatically on all IPsec data tunnels between Cisco IOS XE Catalyst SD-WAN devices. It does not run on the control plane (DTLS or TLS) tunnels that Cisco SD-WAN Controllers establish with all Cisco devices in the network.

You can modify the BFD Hello packet interval and the number of missed Hello packets (the BFD interval multiplier) before BFD declares that a link has failed.

Change the BFD Hello Packet Interval

BFD sends Hello packets periodically to detect faults on the IPsec data tunnel between two Cisco IOS XE Catalyst SD-WAN devices. By default, BFD sends these packets every 1000 milliseconds (that is, once per second). To change this interval on one or more traffic flow, use the **hello-interval** command:

```
ISR4331(config)#bfd color color hello-interval milliseconds
```

The interval can be a value from 100 to 300000 milliseconds (5 minutes).

Configure the interval for each tunnel connection, which is identified by a color. The color can be **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1**, **private2**, **public-internet**, **red**, or **silver**.

Change the BFD Packet Interval Multiplier

After BFD has not received a certain number of Hello packets on a link, it declares that the link has failed. This number of packets is a multiplier of the Hello packet interval time. By default, the multiplier is 7 for hardware routers and 20 for Cloud software routers. This means that if BFD has not received a Hello packet after 7 seconds, it considers that the link has failed and implements its redundancy plan.

To change the BFD packet interval multiplier, use the **multiplier** command:

```
ISR4331(config)#bfd color color multiplier integer
```

Multiplier range: 1 to 60 (integer)

You configure the multiplier for each tunnel connection, which is represented by a color.

Control PMTU Discovery

On each transport connection (that is, for each TLOC, or color), the Cisco Catalyst SD-WAN BFD software performs path MTU (PMTU) discovery, which automatically negotiates the MTU size in an effort to minimize or eliminate packet fragmentation on the connection. BFD PMTU discovery is enabled by default, and it is recommended that you use BFD PMTU discovery and not disable it. To explicitly enable it:

```
ISR4331(config)#bfd color color pmtu-discovery
```

With PMTU discovery enabled, the path MTU for the tunnel connection is checked periodically, about once per minute, and it is updated dynamically. With PMTU discovery enabled, 16 bytes might be required by PMTU discovery, so the effective tunnel MTU might be as low as 1452 bytes. From an encapsulation point of view, the default IP MTU for GRE is 1468 bytes, and for IPsec it is 1442 bytes because of the larger overhead. Enabling PMTU discovery adds to the overhead of the BFD packets that are sent between the Cisco IOS XE Catalyst SD-WAN devices, but does not add any overhead to normal data traffic.

If PMTU discovery is disabled, the expected tunnel MTU is 1472 bytes (tunnel MTU of 1500 bytes less 4 bytes for the GRE header, 20 bytes for the outer IP header, and 4 bytes for the MPLS header). However, the effective tunnel MTU might be 1468 bytes, because the software might sometimes erroneously add 4 bytes to the header.

Configure High Availability

CLI commands for configuring and monitoring high availability.

High Availability Configuration Commands

Use the following commands to configure high availability on a Cisco IOS XE Catalyst SD-WAN device:

```
bfd
  app-route
    multiplier number
    poll-interval milliseconds
  color color
    hello-interval milliseconds
    multiplier number
    pmtu-discovery
```

High Availability Monitoring Commands

show sdwan bfd sessions—Display information about the BFD sessions running on the local Cisco IOS XE Catalyst SD-WAN device.

Best Practices for Configuring Affinity

- In the **system controller-group-list** command on the Cisco IOS XE Catalyst SD-WAN device, list all the controller groups that are available in the overlay network. Doing so ensures that all the Cisco SD-WAN Controller in the overlay network are available for the affinity configuration, and provides additional redundancy if connectivity to the preferred group or groups is lost. You can manipulate the number of control connections and their priority with the maximum number of OMP sessions for the router, the maximum number of control connections for the tunnel, and the controller groups that the tunnel should not use (**exclude-controller-group-list** command).

Listing all controller groups in the **system controller-group-list** command provides an additional layer of redundancy in situations where the Cisco IOS XE Catalyst SD-WAN device site is experiencing connectivity problems with the Cisco SD-WAN Controllers in the controller group list.

To illustrate, consider a network with three controller groups (1, 2, and 3), and in which the controller group list on a Cisco IOS XE Catalyst SD-WAN device includes only groups 1 and 2 as preferred groups. In this scenario, if the router learns from the Cisco SD-WAN Validator that the Cisco SD-WAN Controllers in groups 1 and 2 are operational, but the router is unable to establish a connection to either device, it loses connectivity to the overlay network. However, if the controller group list contains all three controller groups and group 3 is set up as a less preferred (excluded) group, the router still normally prefers groups 1 and 2, but would fall back and connect to the controllers in group 3 if it cannot connect to group 1 or group 2.

- The controller groups listed in the **exclude-controller-group-list** command must be a subset of the controller groups configured for the entire router, in the **system controller-group-list** command.
- When a data center has multiple Cisco SD-WAN Controllers that use the same controller group identifier, and when the overlay network has two or more data centers, it is recommended that the number of Cisco SD-WAN Controllers in each of the controller groups be the same. For example, if Data Center 1 has three Cisco SD-WAN Controllers, all with the same group identifier (let's say, 1), Data Center 2 should also have three Cisco SD-WAN Controllers, all with the same group identifier (let's say, 2), and any additional data centers should also have three Cisco SD-WAN Controllers.
- When a data center has Cisco SD-WAN Controllers in the same controller group, the hardware capabilities—specifically, the memory and CPU—on all the Cisco SD-WAN Controllers should be identical. More broadly, all the Cisco SD-WAN Controllers in the overlay network, whether in one data center or in many, should have the same hardware capabilities. Each Cisco SD-WAN Controller should have equal capacity and capability to handle a control connection from any of the Cisco IOS XE Catalyst SD-WAN devices in the network.
- When a router has two tunnel connections and the network has two (or more) data centers, it we recommend that you configure one of the tunnel interfaces to go to one of the data centers and the other to go to the second. This configuration provides Cisco SD-WAN Controller redundancy with the minimum number of OMP sessions.
- Whenever possible in your network design, you should leverage affinity configurations to create fault-isolation domains.

