

System Commands

- admin-tech-on-failure (system), on page 1
- console-baud-rate, on page 2
- control-session-pps (system), on page 3
- controller-group-list (system), on page 3
- device-groups (system), on page 4
- enable-ipv6-unique-local-address , on page 4
- gps-location (system), on page 5
- logging, on page 8
- max-omp-sessions (system), on page 10
- organization-name (system), on page 11
- overlay-id (system), on page 11
- port-hop (system), on page 12
- port-offset (system), on page 13
- site-id (system), on page 13
- sp-organization-name (system), on page 14
- statistics table interface collection-interval, on page 15
- system-ip (system), on page 15
- system overlay-id, on page 16
- track-transport (system), on page 17
- track-default-gateway (system), on page 17
- upgrade-confirm (system), on page 18
- vbond (system), on page 19

admin-tech-on-failure (system)

When a Cisco device reboots, it collects system status information in a compressed tar file to aid in troubleshooting and diagnostics. This tar file, which is saved in the user's home directory, contains the output of various commands and the contents of various files on the local device, including syslog files, files for each process (daemon) running on the device, core files, and configuration rollback files. For aid in troubleshooting, send the tar file to Cisco customer support.

To configure a device to collect system status information in an admin-tech file when the device reboots, use the **admin-tech-on-failure** command in system configuration mode. To delete the system status information from the admin tech file, use the no form of this command.

admin-tech-on-failure

no admin-tech-on-failure

Syntax Description

This comand has no keywords or arguments.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example configures the device to collect system status information in an admin-tech file when the device reboots:

```
Router(config)# system
Router(config-system)# admin-tech-on-failure
!
```

console-baud-rate

To change the baud rate of the console connection on a Cisco IOS XE Catalyst SD-WAN device, use the **console-baud-rate** command in system configuration mode. To delete the configured baud rate, use the **no** form of this command.

console-baud-rate *rate*

no console-baud-rate

Syntax Description

rate	Specifies the baud rate, in baud or bits per second (bps). Each signal carries only one bit, so the baud rate is equal to the bits-per-second rate. Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Starting from Cisco vManage Release 20.3.1, the default value is 9600 on Cisco IOS XE Catalyst SD-WAN devices.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example changes the console baud rate to 57600:

```
Device(config)# system
Device(config-system)# console-baud-rate 57600
```

control-session-pps (system)

To police the flow of DTLS control session traffic, use the **control-session-pps** command in system configuration mode. To delete the control session traffic rate, use the no form of this command.

control-session-pps *site-id*

no control-session-pps

Syntax Description

rate	Sets the maximum rate of DTLS control session traffic in packets per second (pps). Range: 1 - 65535 pps Default: 300 pps

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example changes the maximum control session traffic rate to 250 pps:

```
Router(config)# system
Router(config-system)# control-session-pps 250
```

controller-group-list (system)

To list the controller groups to which a router belongs, use the **controller-group-list** command in system configuration mode. A router can form control connections only with the Cisco Catalyst SD-WAN Controllers that are in the same controller group. To delete the control connections from the Cisco Catalyst SD-WAN Controllers, use the no form of this command.

controller-group-list *list-of-controller-groups*

no controller-group-list *list-of-controller-groups*

Syntax Description

list-of-controller-groups	Specifies an identifier of one or more Cisco Catalyst SD-WAN Controllerr groups to which a router belongs. You configure this identifier on the Cisco Catalyst SD-WAN Controllers, using the **system controller-group-id** command. The number of controller groups cannot exceed the maximum number of control connections configured on the router.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example allows a router to establish control connections to the Cisco Catalyst SD-WAN Controllers in groups 1 and 2:

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

device-groups (system)

To configure one or more groups to which a device belongs, use the **device-groups** command in system configuration mode. To delete the groups to which a device belongs, use the no form of this command.

device-groups *group-name*

no device-groups *group-name*

Syntax Description

group-name	Name of one or more groups to which the device belongs. When specifying multiple group names, enclose the names in square brackets. When a group name contains spaces, enclose it in quotation marks (" ").

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example adds a router to two groups: London and the United Kingdom:

```
Router(config)# system
Router(config-system)# device-groups London ["United Kingdom"]
```

enable-ipv6-unique-local-address

To enable the IPv6 Unique Local Addresses (ULA), use the **enable-ipv6-unique-local-address** command in system configuration mode. To disable these addresses, use the no form of this command.

enable-ipv6-unique-local-address

no enable-ipv6-unique-local-address

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example enables the IPv6 Unique Local Address:

```
Router(config)# system
Router(config-system)# enable-ipv6-unique-local-address
```

gps-location (system)

To configure the location and the geofencing boundary for a device and to enable SMS alerts for boundary violations, use the **gps-location** command in system configuration mode. To disable geofencing, use the **no** form of this command.

gps-location [**latitude** *decimal-number*] [**longitude** *decimal-number*] [**auto-detect-geofencing-location**] [**geo-fencing-enable** [**geo-fencing-config** [**geo-fencing-range** *meters*] [**sms** [[**sms-enable**] **mobile-number** *mobile-number*]]]]

no gps-location

Syntax Description

latitude *decimal-number*	(Optional) Specifies the latitude coordinates of a device in decimal degrees. Range: -90.0 - 90.0 **Note** For configuring the **gps-location** command for geofencing, the **latitude**, **longitude**, and **geo-fencing-enable** parameters are mandatory. Although the syntax allows you to configure **latitude**, **longitude**, and **geo-fencing-enable** parameters in separate **gps-location** commands, we recommend that all three be configured within a single command. All three have to be configured with **geo-fencing-enable** configured last. A single command reduces the risk of configuration errors by keeping corequisite parameters close together, and single-command syntax ensures that **geo-fencing-enable** is configured last. **Note** Deconfigure the **latitude**, **longitude**, and **geo-fencing-enable** parameters by using the **no gps-location** command. You can configure a maximum of six digits to the right of the decimal point.

longitude *decimal-number*	(Optional) Specifies the longitude coordinates of a device in decimal degrees. Range: -180.0 - 180.0 **Note** For configuring the **gps-location** command for geofencing, the **latitude**, **longitude**, and **geo-fencing-enable** parameters are mandatory. Although the syntax allows you to configure **latitude**, **longitude**, and **geo-fencing-enable** parameters in separate **gps-location** commands, we recommend that all three be configured within a single command. All three have to be configured with **geo-fencing-enable** configured last. A single command reduces the risk of configuration errors by keeping corequisite parameters close together, and single-command syntax ensures that **geo-fencing-enable** is configured last. **Note** Deconfigure the **latitude**, **longitude**, and **geo-fencing-enable** parameters by using the **no gps-location** command. You can configure a maximum of six digits to the right of the decimal point.
auto-detect-geofencing-location	(Optional) Enables automatic detection of a device where the device determines its own location. You can choose either to specify latitude and longitude parameters, or configure the **auto-detect-geofencing-location** parameter. **Note** Do not configure latitude and longitude coordinates when enabling **auto-detect-geofencing-location**. This field allows you to configure geofencing with the last-known valid GPS coordinates of the device, instead of mandating latitude and longitude coordinates for GPS location. The last-known GPS coordinates are persistent across boot cycles and are periodically updated as the location of the device changes. If no historically valid last-known GPS coordinates are available, the device rejects the automatic detection configuration.
geo-fencing-config	(Optional) Allows you to configure geofencing parameters.
geo-fencing-range *meters*	(Optional) Specifies the radius from the base target location in meters. Default geofencing range is 100 meters. Configurable ranges of values is 100 to 10,000 meters.
sms	(Optional) Provides SMS notification options.

sms-enable	(Optional) Enables registration of end-user mobile numbers for receiving SMS alerts. An SMS alert is delivered when a device is determined to be outside the configured geofencing radius of its target location. **Note** The presence of a SIM card is mandatory in the LTE PIM module for receiving SMS alerts.
mobile-number *mobile-number*	(Optional) Specifies the mobile numbers for sending SMS alerts. Mobile numbers must start with a + sign, include a country code, an area code, with no spaces between the country code and the area code, and the remaining digits. You can configure a maximum of four mobile numbers for receiving SMS alerts.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Additional parameters qualified: • **geo-fencing enable** • **geo-fencing config** • **geo-fencing range** • **sms** • **sms-enable** • **mobile-number**
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Additional parameter qualified: **auto-detect-geofencing-location**

Usage Guidelines

Note In Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and earlier releases, geofencing parameters such as, **latitude**, **longitude**, and **geo-fence range** are not reconfigurable once configured. You need to first disable geofencing and then reenable geofencing again with the updated parameters.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, **latitude**, **longitude**, and **geo-fence range** are all reconfigurable.

Provide **latitude** and **longitude** coordinates as close as possible to the intended installation location of the device. This is necessary because of inherent inaccuracies of GPS and fluctuations over time.

Whenever there are too many **Device Location Inside** and **Device Location Outside** notifications generated for the device on Cisco SD-WAN Manager when the device is in a static installation environment, we suggest picking a higher value for the **geo-fence-range** parameter to account for GPS fluctuations.

Examples

The following examples set the geographical coordinates of a device:

```
Device(config)# system
Device(config-system)# gps-location latitude 37.317342 longitude -122.218170
```

```
Device(config)# system
Device(config-system)# gps-location longitude 91.1 latitude 11.0
```

The following example shows enabling and configuring geofencing with a geofence range of 1000 meters.

```
Device(config-system)# gps-location geo-fencing-enable
Device(config-system)# gps-location geo-fencing-config
Device(conf-geo-fencing-config)# geo-fencing-range 1000
```

The following example shows enabling SMS and adding a mobile number for receiving SMS alerts.

```
Device(conf-geo-fencing-config)# sms sms-enable mobile-number +1214343789
Device(config-mobile-number-+1214343789)#
```

The following example shows configuring a device without the **auto-detect-geofencing-location** parameter:

```
Device(config)# system
Device(config-system)# gps-location latitude 37.439917 longitude -121.886471
```

You need to configure latitude and longitude coordinates when not enabling the **auto-detect-geofencing-location** parameter.

The following example shows enabling a device using the **auto-detect-geofencing-location** parameter:

```
Device(config)# system
Device(config-system)# no gps-location latitude
Device(config-system)# no gps-location longitude
Device(config-system)# gps-location auto-detect-geofencing-location
```

You should not configure latitude and longitude coordinates when enabling the **auto-detect-geofencing-location** parameter.

logging

To set system logging parameters use the **logging** command in global configuration mode. To remove logging parameters, use the **no** form of this command.

logging { **IP address** | **console** | **event** | **host** | **persistent** | **tls-profile** | **string** | **discriminator** | **file** | **monitor** | **snmp-trap** | **trap** | **buffered** | **esm** | **history** | **origin-id** | **source-interface** }
no logging { **IP address** | **console** | **event** | **host** | **persistent** | **tls-profile** | **string** | **discriminator** | **file** | **monitor** | **snmp-trap** | **trap** | **buffered** | **esm** | **history** | **origin-id** | **source-interface** }

Syntax Description

ip address	IP address of the host that will receive the system logging (syslog) messages.

console	Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels.
event	Logs interface events.
host	Logs messages to a UNIX syslog server host.
persistent	Allows writing logged messages to files on the routers flash disk.
tls-profile	Profile used for secure syslog messages with TLSv1.1 or TLSv1.2.
string	Includes the custom string in the session ID tag. Custom string in the s_id="custom_string" tag.
discriminator	(Optional) Specifies a message discriminator for the session. Name of the message discriminator.
file	Stores log messages in a file in flash memory on a standalone switch or, a switch stack, on the active switch.
monitor	Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels.
snmp-trap	Logs SNMP-trap notifications.
trap	Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels.
buffered	Logs messages to an internal buffer on the switch or on a standalone switch or, a switch stack, on the active switch.
esm	syslog filter modules, which are Tool Command Language (Tcl) script files stored locally or on a remote device.
history	Changes the default level of syslog messages stored in the history file and sent to the SNMP server. By default, warnings, errors, critical, alerts, and emergencies messages are sent.
origin-id	Adds an origin identifier to system logging messages sent to remote hosts.
source-interface	Specifies the source IPv4 or IPv6 address of system logging packets.

Command Default

Logging to the console is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Logging events can be configured and stored on local flash of router or sent out via syslog or snmp-trap.

Example

The following example shows setting the TLS-version of profile1 to TLSv1.1

```
Device(config)# logging tls-profile profile1 tls-version TLSv1.1
```

The following example shows how to log interface events

```
Device(config)# logging event link-status default
```

max-omp-sessions (system)

To configure the maximum number of OMP sessions that a device can establish with Cisco Catalyst SD-WAN Controllers, use the **max-omp-sessions** command in system configuration mode.

max-omp-sessions *number*

Syntax Description

name	Specifies the maximum number of OMP sessions that a device can establish with Cisco Catalyst SD-WAN Controllers. These connections are DTLS or TLS control plane tunnels. Range: 0–100

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A Cisco IOS XE Catalyst SD-WAN device establishes a single OMP session with each Cisco Catalyst SD-WAN Controller. Even when a device has multiple tunnel connections with the same Cisco Catalyst SD-WAN Controller, because all the tunnels have the same IP address, this group of tunnels is effectively a single OMP session. When **max-omp-sessions** is configured (without affinity), the devices establish OMP peering with Cisco Catalyst SD-WAN Controllers having higher System-IP.

In an overlay network with redundant Cisco Catalyst SD-WAN Controllers, configure the maximum number of OMP sessions to manage the scale of the overly network, by limiting the number of Cisco Catalyst SD-WAN Controllers that an individual device can establish control connections with.

This command provides system-wide control over the maximum number of control connections that a device can establish to Cisco Catalyst SD-WAN Controllers. To configure the number of control connections allowed on an individual tunnel interface, include the **max-control-connections** command when configuring the tunnel interface in VPN 0. The maximum number of OMP sessions configured on the router becomes the default value for the maximum number of control connections allowed on the tunnel interfaces of a device.

Examples

The following example changes the maximum number of Cisco Catalyst SD-WAN Controller connections to 8:

```
Router(config)# system
Router(config-system)# max-omp-sessions 8
```

organization-name (system)

To configure the name of your organization, use the **organization-name** command in system configuration mode. To delete the organization name configuration, use the no form of this command.

organization-name *name*

no organization-name

Syntax Description

name	Configures the name of your organization. The name is case-sensitive. It must be identical on all the devices in your overlay network, and it must match the name in the certificates for all Cisco IOS XE Catalyst SD-WAN devices.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, the size limit of the organization name must be within the range 1 to 128.

Examples

The following example configures an organization name:

```
Router(config)# system
Router(config-system)# organization-name Cisco
```

overlay-id (system)

To configure the overlay id of a device in Cisco SD-WAN overlay netowrk, use the **overlay-id** command in system configuration mode. To delete the overlay id, use the no form of this command.

overlay-id *overlay-id*

no overlay-id

Syntax Description

overlay-id	Specifies the overlay id of a device. Range: Range: 0 - 4294967295 (2^{32} – 1) Default: 1

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example sets the overlay Id of a device:

```
Router(config)# system
Router(config-system)# overlay-id 42000
```

port-hop (system)

To establish DTLS connections with other Cisco IOS XE Catalyst SD-WAN devices when a connection attempt is unsuccessful (on Cisco IOS XE Catalyst SD-WAN devices, Cisco SD-WAN Manager servers, and Cisco Catalyst SD-WAN Controllers), use the **port-hop** command in system configuration mode. To disable port hopping on the Cisco IOS XE Catalyst SD-WAN device, or if global port hopping is enabled, to disable port hopping on an individual TLOC, use the no form of this command.

port-hop

no port-hop

Syntax Description

This comand has no keywords or arguments.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For a Cisco IOS XE Catalyst SD-WAN device that is behind a NAT device or for an individual tunnel interface (TLOC) on the device, rotate through a pool of preselected OMP port numbers, known as base ports. By default, port hopping is enabled on Cisco IOS XE Catalyst SD-WAN devices and on all tunnel interfaces on Cisco IOS XE Catalyst SD-WAN devices, and it's disabled on Cisco SD-WAN Manager servers and Cisco Catalyst SD-WAN Controllers.

There are five base ports: 12346, 12366, 12386, 12406, and 12426. These port numbers determine the ports used for connection attempts. The first connection attempt is made on port 12346. If the first connection doesn't succeed after about 1 minute, port 12366 is tried. After about 2 minutes, port 12386 is tried; after about 5 minutes, port 12406; after about 6 minutes, port 12426 is tried. Then the cycle returns to port 12346.

If you have configured a port offset with the **port-offset** command, the five base ports are a function of the configured offset. For example, with a port offset of 2, the five base ports are 12348, 12368, 12388, 12408, and 12428. Cycling through these base ports happens in the same way as if you hadn't configured an offset.

Examples

The following example enables port hopping:

```
Router(config)# system
Router(config-system)# port-hop
!
```

port-offset (system)

To offset the base port numbers to be used for the TLOC when multiple Cisco devices are present behind a single NAT device, use the **port-offset** command in system configuration mode. Each device must have a unique port number so that overlay network traffic can be correctly delivered. To delete the port offset value, use the no form of this command.

port-offset *number*

no port-offset

Syntax Description

number	Specifies offset value from the default base port numbers, which are 12346, 12366, 12386, 12406, and 12426. Range: 0-19 Default: 0

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example configures a port offset value:

```
Router(config)# system
Router(config-system)# port-offset 1
```

site-id (system)

To configure the identifier of a site in the Cisco SD-WAN overlay network, such as a branch, campus, or data center, in which devices and controllers reside, use the **site-id** command in system configuration mode. To delete the site id of a device, use the no form of this command.

site-id *site-id*

no site-id

Syntax Description

site-id	Numeric identifier of the site in the Cisco SD-WAN overlay network. The site ID must be the same for all routers that reside in the same site. Range: 0 - 4294967295 (2^{32} – 1) Default: 101

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example configures the site id of a device to 50:

```
Router(config)# system
Router(config-system)# site-id 50
```

sp-organization-name (system)

To configure the name of your service provider for a Cisco Catalyst SD-WAN Validator or Cisco Catalyst SD-WAN Controller that is part of a software multitenant architecture, use the **sp-organization-name** command in system configuration mode. To delete the service provider organization name configuration, use the no form of this command.

sp-organization-name *name*

no sp-organization-name

Syntax Description

name	Configures the name of your service provider. The name is case-sensitive. It must be identical on all the devices in your overlay network, and it must match the name in the certificates for all Cisco IOS XE Catalyst SD-WAN devices.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, the size limit of the organization name must be within the range 1 to 128.

Examples

The following example configures a service provider organization name:

```
Router(config)# system
Router(config-system)# sp-organization-name My Phone Company Inc
```

statistics table interface collection-interval

To set the interface statistics collection interval in Cisco IOS XE Catalyst SD-WAN, use the **statistics table interface collection-interval** command in global configuration mode.

statistics table interface collection-interval *interval-time*

Syntax Description

interval-time	Specify the data collection interval for interface statistics as 1 (minute).

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 26.1.1	This command was introduced.

Examples

The following is an example of how to set the interface statistics collection interval on a WAN edge device:

```
Device(config)# statistics
Device(config-statistics)# table interface
Device(config-table-interface)# collection-interval 1
```

system-ip (system)

To configure a system IP address of a device, use the **system-ip** command in system configuration mode. To delete the system IP address of a device, use the no form of this command.

system-ip *ipv4-address*

no system-ip

Syntax Description

ipv4-address	Specifies an IPv4 address in decimal four-part dotted notation. Enter the address, and the prefix length (/32) is implicit. The system IP address can be any IPv4 address except for 0.0.0.0/8, 127.0.0.0/8, 224.0.0.0/4, 240.0.0.0/4 and later. Each device in the overlay network must have a unique system IP address. You can't use the same address for another interface in VPN 0.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The system IP address is a persistent IP address that identifies the Cisco device. It's similar to a router ID on a regular router, which is the address used to identify the router from which packets originated. The system IP address is used internally as the loopback address of the device in the transport VPN (VPN 0).



Note This IP address isn't the same as a loopback address that you configure for an interface.

On a router, the system IP address is used as the router ID for BGP or OSPF. If you configure a router ID for either of these protocols and it's different from the system IP address, the router ID takes precedence.

Examples

The following example sets the system IP address of a device:

```
Router(config)# system
Router(config-system)# system-ip 172.16.255.11
```

system overlay-id

To set an overlay-id, use the **system overlay-id** command in global configuration mode. To remove the overlay-id, use the **no** form of this command.

system overlay-id *ID*
no system overlay-id *ID*

Syntax Description

ID	Specifies the ID number 0-4294967295.

Command Default

Default overlay-id is set to 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The overlay-id command is used to determine whether devices belong to specific SD-WAN topologies or overlay.

Example

The following example shows how to configure an overlay-id of 2335.

```
Device(config)# system overlay-id 2335
```

track-transport (system)

To check whether the routed path between the local device and a Cisco Catalyst SD-WAN Validator is available by using ICMP probes at regular interval of 3s, use the **track-transport** command in system configuration mode. To delete the regular monitoring of the DTLS connection to the Cisco Catalyst SD-WAN Validator, use the no form of this command. By default, transport checking is enabled.

track-transport

no track-transport

Syntax Description

This comand has no keywords or arguments.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example explicitly configures regular monitoring of the DTLS connection to the Cisco Catalyst SD-WAN Validator:

```
Router(config)# system
Router(config-system)# track-transport
Router(config-system)# commit
Commit complete.
```

track-default-gateway (system)

For a static default route, to determine whether the next hop is reachable before adding that route to the device's route table, use the **track-default-gateway** command in system configuration mode. To disable the device from determining whether the next hop for a default static route is reachable before placing the deafault static route in the local route table, use the no form of the command. By default, this command is enabled.

track-default-gateway

no track-default-gateway

Syntax Description

This comand has no keywords or arguments.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

With gateway tracking enabled, the software sends ARP messages every 10 seconds to the next hop of a default static route. If the software receives an ARP response, it places the default static route into the local route table. After 10 consecutive ARP responses are missed, the default static route is removed from the route table. The software continues to periodically send ARP messages, and as soon as it once again receives an ARP responses, the default static route is added back to the route table.

Examples

The following example configures the device to determine whether the next hop for a default static route is reachable before placing the static route in the local route table:

```
Router(config)# system
Router(config-system)# track-default-gateway
```

upgrade-confirm (system)

To configure the time limit for confirming that a software upgrade is successful, use the **upgrade-confirm** command in system configuration mode. It's recommended that you configure this on all Cisco IOS XE Catalyst SD-WAN devices. To disable the time limit configuration set for successful software upgrade, use the no form of this command.

upgrade-confirm *minutes*

no upgrade-confirm

Syntax Description

minutes	Specifies how long to wait for the **request software sdwan upgrade-confirm** command to be issued before reverting to the previous software image if a software upgrade fails. Range: 5-60 minutes Default: None

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

By default, software upgrade confirmation isn't enabled. When you enable the confirmation, the device waits for the amount of time you configure. If the device doesn't get booted up within that time, the device reverts to the previous image.

When the upgrade-confirm is enabled, the devices can still revert to the previous image if the control-connections fail to boot up.

After you issue the **request software sdwan software install** command to upgrade the software and then log in to the device after the reboot completes, enter the **request software sdwan upgrade-confirm** command within the configured time limit to confirm that the software upgrade is successful. If you do not, the system automatically reverts to the previous software image.

Examples

The following example sets the upgrade confirmation time to 5 minutes:

After a software upgrade, when the system reboots and restarts, if you don't issue a **request software sdwan upgrade-confirm** command within 5 minutes (either from the CLI or from the Cisco SD-WAN Manager), the system automatically reverts to the software image that was running before the upgrade:

```
Router(config)# system
Router(config-system)# upgrade-confirm 5
!
```

vbond (system)

To configure the IP address and other information related to the Cisco Catalyst SD-WAN Validator, use the **vbond** command in system configuration mode. To remove the Cisco Catalyst SD-WAN Validator configuration from the device, use the no form of this command.

vbond *dns-name ip-address* [**local**] [**port** *port-number*] [**ztp-server**]

no vbond [**local**] [**port** *port-number*]

Syntax Description

dns-name	Specifies the DNS name that points to a Cisco Catalyst SD-WAN Validator or to a number of Cisco Catalyst SD-WAN Validators. The addresses can be resolved to Cisco Catalyst SD-WAN Validators configured with IPv4 addresses, IPv6 addresses, or with both IPv4 and IPv6 adresses.
ip-address	Specifies IPv4 or IPv6 address of the Cisco Catalyst SD-WAN Validator, in decimal four-part dotted notation. You can configure one IP address, and it must be a public IP address.
local	Designates the Cisco IOS XE Catalyst SD-WAN device to be a Cisco Catalyst SD-WAN Validator in the overlay network domain. If you configure the **local** option, you can omit the DNS name, or IP address of the Cisco Catalyst SD-WAN Validator as long as one of the interfaces in VPN 0 has a routable public IP address.
port-number	Specifies the port number to use to connect to the Cisco Catalyst SD-WAN Validator. If you omit this option, the local system first tries port 12346 on the Cisco Catalyst SD-WAN Validator. If this port is not available, the system then tries port 12366 and then port 12388, rotating through these three port numbers until one is available. If you do not want to rotate through these three port numbers, configure the port number to connect to the Cisco Catalyst SD-WAN Validator. Range: 1-65535 Default: 12346
ztp-server	Designates the local Cisco IOS XE Catalyst SD-WAN device to be the zero-touch-provisioning (ZTP) server in the overlay network domain. Such a Cisco Catalyst SD-WAN Validator acts as an enterprise ZTP server, and provides the devices in your domain with the IP address of your enterprise Cisco Catalyst SD-WAN Validator and with the enterprise root CA chain. You must load two files onto your enterprise ZTP server–the authorized serial number file of the device that you received and your enterprise root CA chain, which must be signed by Symantec.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

If you have configured an IP address for the Cisco Catalyst SD-WAN Validator, to change the address, you must delete the address and then configure the new address. Doing this causes all the existing device connections to the other devices in the network to go down. The devices come back up after you commit the configuration with the new IP address. To avoid this problem, we recommend that you always use a DNS name for your Cisco Catalyst SD-WAN Validators, and then make changes to the DNS devices instead of on the Cisco IOS XE Catalyst SD-WAN devices and Cisco Catalyst SD-WAN Controllers directly.

Examples

The following example configures the port number of a device used to connect to the Cisco Catalyst SD-WAN Validator:

```
Router(config)# system
Router(config-system)# vbond 192.0.2.4 port 12346
```