

IP Commands

- access-class, on page 3
- address prefix, on page 4
- arp timeout, on page 4
- cdp enable, on page 5
- cdp run, on page 5
- default-router, on page 6
- dns-server, on page 6
- domain-name, on page 7
- ip address, on page 8
- ip address dhcp, on page 9
- ip arp proxy disable, on page 9
- ip bootp server, on page 10
- ip cef load-sharing algorithm, on page 11
- ip-clear-dont-fragment, on page 12
- ip community-list, on page 13
- ip dhcp client vendor-class, on page 15
- ip dhcp conflict logging, on page 16
- ip dhcp use, on page 17
- ip dhcp smart-relay, on page 18
- ip dhcp use hardware-address client-id, on page 19
- ip directed-broadcast, on page 19
- ip dns server, on page 20
- ip domain lookup, on page 21
- ip finger, on page 21
- ip helper-address, on page 22
- ip host, on page 22
- ip host *ip-address*, on page 23
- ip http authentication, on page 24
- ip http client source-interface, on page 25
- ip http secure-server, on page 25
- ip http server, on page 26
- ip http tls-version, on page 27
- ip icmp rate-limit unreachable, on page 27

- ip icmp redirect, on page 28
- ip igmp ssm-map query dns, on page 29
- ip load-sharing algorithm, on page 29
- ip mtu, on page 30
- ip multicast route-limit, on page 31
- ip name-server, on page 32
- ip pim, on page 33
- ip pim bsr-candidate, on page 33
- ip pim rp-address, on page 35
- ip pim rp-candidate, on page 35
- ip prefix-list, on page 37
- ip redirects, on page 37
- ip rcmd, on page 38
- ip rcmd rcp-enable, on page 39
- ip rcmd rsh-enable, on page 40
- ip route vrf, on page 40
- ip route, on page 41
- ip source-route, on page 42
- ip ssh version, on page 43
- ip tcp adjust-mss, on page 44
- ip tcp mss, on page 44
- ip unnumbered, on page 45
- ip virtual-reassembly, on page 45
- ipv6 access-class, on page 46
- ipv6 address, on page 47
- ipv6 address autoconfig, on page 48
- ipv6 address dhcp client request, on page 48
- ipv6 cef load-sharing algorithm, on page 48
- ipv6 dhcp client pd, on page 50
- ipv6 dhcp client vendor-class, on page 50
- ipv6 dhcp pool, on page 51
- ipv6 dhcp relay destination, on page 52
- ipv6 dhcp-relay option vpn, on page 52
- ipv6 dhcp server, on page 53
- ipv6 enable, on page 53
- ipv6 load-sharing algorithm, on page 54
- ipv6 nd other-config-flag, on page 55
- ipv6 nd prefix, on page 55
- ipv6 nd ra suppress, on page 56
- ipv6 nd router-preference, on page 57
- ipv6 redirects, on page 58
- ipv6 route, on page 58
- ipv6-strict-control, on page 59
- ipv6 unnumbered, on page 60
- lease, on page 61
- network (DHCP), on page 61

- option (DHCP), on page 62
- prefix-delegation, on page 63
- prefix-delegation pool, on page 63
- spt-only, on page 63
- vlan internal allocation policy, on page 64
- vendor-specific, on page 65
- vrf (DHCP pool), on page 65

access-class

To restrict incoming and outgoing connections between a particular VTY and the addresses in an access list, use the **access-class** command. To remove access restrictions, use the **no** form of this command.

access-class *access-list-name/number* { **in** | **out** }

no access-class *access-list-name* { **in** | **out** }

Syntax Description

access-list-name/number	You can either enter a name of the access-list or a number. Name of the IPv4 ACL class. The name can be a maximum of 64 alphanumeric characters. The name cannot contain a space or quotation mark. Number of an IP access list. This is a decimal number from 1 to 199 or from 1300 to 2699 .
in	Restricts incoming connections between a particular Cisco device and the addresses in the access list.
out	Restricts outgoing connections between a particular Cisco device and the addresses in the access list.

Command Default

None

Command Modes

Line configuration mode (config-line)

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `access-class` command.

Examples

This example shows how to configure an access class on a VTY line:

```
Device (config)# line vty 0 5
Device(config-line)# access-class TEST in
```

address prefix

To specify an address prefix for address assignment, use the **address prefix** command in interface configuration mode. To remove the address prefix, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE address prefix command.

Examples

The following example shows how to configure a pool called engineering with an IPv6 address prefix:

```
Device(config)# ipv6 dhcp pool engineering
Device(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite
```

arp timeout

To configure how long a dynamically learned IP address and its corresponding Media Control Access (MAC) address remain in the Address Resolution Protocol (ARP) cache, use the **arp timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

arp timeout *seconds*
no arp timeout

Syntax Description

seconds	Time (in seconds) that an entry remains in the ARP cache. The general recommended value for ARP timeout is the configured default value, which is 4 hours. If the network has frequent changes to cache entries, change the default to a shorter time period. As you reduce the ARP timeout, your network traffic increases. A low ARP timeout value might lead to network outage, and a value less than an hour (or 3600 seconds) will generate significantly increased traffic across the network. **Caution** We recommend that you set an ARP timeout value greater than 60 seconds.

Command Default

14400 seconds (4 hours)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For the usage guidelines, see arp timeout.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# arp timeout 7200
```

cdp enable

To enable Cisco Discovery Protocol on an interface, use the **cdp enable** command in interface configuration mode. To disable Cisco Discovery Protocol on an interface, use the **no**form of this command.

cdp enable
no cdp enable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled at the global configuration level and is supported on all interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see cdp enable.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# cdp enable
```

cdp run

To enable Cisco Discovery Protocol, use the **cdp run**command in global configuration mode. To disable Cisco Discovery Protocol, use the **no**form of this command.

cdp run
no cdp run

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled on all the platforms.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `cdp run` command.

Examples

In the following example, Cisco Discovery Protocol is enabled globally.

```
Device(config)# cdp run
```

default-router

To specify the default router list for a Dynamic Host Configuration Protocol (DHCP) client, use the **default-router** command in DHCP pool configuration mode. To remove the default router list, use the **no** form of this command.

default-router *address* [*address2* **. . .** *address8*]
no default-router

Syntax Description

address	Specifies the IP address of a router. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `default-router` command.

Examples

The following example specifies 10.1.19.15 as the IP address of the default router:

```
Device(config)# ip dhcp pool POOL1
Device(dhcp-config)# default-router 10.1.19.15
```

dns-server

To specify the Domain Name System (DNS) IP servers available to a Dynamic Host Configuration Protocol (DHCP) client, use the **dns-server** command in DHCP pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *address* [*address2* **. . .** *address8*]
no dns-server

Syntax Description

address	The IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line. The server addresses should be specified in the order of preference.

Command Default

If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Usage Guidelines

Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the domain name server of the client:

```
Device(config)# ip dhcp pool POOL1
Device(dhcp-config)# dns-server 10.12.1.99
```

domain-name

To specify the default domain for a Domain Name System (DNS) view to use to complete unqualified hostnames (names without a dotted-decimal domain name), use the **domain-name** command in DHCP pool configuration mode. To remove the specification of the default domain name for a DNS view, use the **no** form of this command.

domain-name *domain-name*
no domain-name

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No default domain name is defined for the DNS view.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `domain name` command.

Examples

The following example shows how to define dns1 as the default DNS view for the DHCP pool named POOL1.

```
Device(config)# ip dhcp pool POOL1
Device(dhcp-config)# domain-name dns1
```

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface or sub-interface configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address* [*mask*]
no ip address [*ip-address*] [*mask*]

Syntax Description

ip-address	IP address.
mask	(Optional) Mask for the associated IP subnet.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Sub-interface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see the Cisco IOS XE ip address command.

Examples

```
Device(config)# interface ATM 0/3/0.1 point-to-point

Device(config-if)# ip address 192.10.6.5

Device(config)# interface ATM 0/3/0.1

Device(config-subif)# ip address 10.0.0.0 255.255.255.252

Device(config)# interface Serial 0/1/0.2

Device(config-if)# ip address 10.1.1.1 255.255.255.0

Device(config)# interface Serial 0/0/1:5

Device(config-if)# ip address 10.1.1.1 255.255.255.0
```

```
Device(config)# interface MFR1

Device(config-if)# ip address 10.4.4.4 255.255.255.0
```

ip address dhcp

To acquire an IP address on an interface from the DHCP, use the **ip address dhcp**command in interface configuration mode. To remove any address that was acquired, use the **no** form of this command.

ip address dhcp [**client-id** *interface-type number*]
no ip address dhcp [**client-id** *interface-type number*]

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The **client-id** *interface-type number*option sets the client identifier to the hexadecimal MAC address of the named interface.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip address dhcp.

Examples

```
Device(config)# interface GigabitEthernet 1

Device(config-if)# ip address dhcp client-id GigabitEthernet 1
```

ip arp proxy disable

To globally disable proxy Address Resolution Protocol (ARP), use the **ip arp proxy disable** command in global configuration mode. To reenable proxy ARP, use the **no** form of this command.

ip arp proxy disable
no ip arp proxy disable

Syntax Description

This command has no arguments or keywords.

Command Default Proxy ARP is enabled.

Command Modes Global configuration

Command History

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

Usage Guidelines The **ip arp proxy disable** command overrides any proxy ARP interface configuration. The **default ip arp proxy** command returns proxy ARP to the default behavior, which is enabled.

Examples The following example disables proxy ARP:

```
Device(config)# ip arp proxy disable
```

The following example enables proxy ARP:

```
Device(config)# no ip arp proxy disable
```

ip bootp server

To enable the Bootstrap Protocol (BOOTP) service on your routing device, use the **ip bootp server** command in global configuration mode. To disable BOOTP services, use the **no** form of the command.

ip bootp server
no ip bootp server

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Global configuration

Command History

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

Usage Guidelines For usage guidelines, see the Cisco IOS XE `ip bootp server` command.

Examples In the following example, the BOOTP service is enabled and disabled on the router:

```
Device(config)# ip bootp server
Device(config)# no ip bootp server
```

ip cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm for IPv4, use the **ip cef load-sharing algorithm** command in global configuration mode. To return to the default universal load-balancing algorithm, use the **no** form of this command.

ip cef load-sharing algorithm { **universal** [*id*] | **include-ports** [**source** [*id*] | **destination** [*id*]] | **src-only** [*id*] }
no ip cef load-sharing algorithm

universal *[id]*	Sets the load-balancing algorithm to the universal algorithm that uses a source and destination IP. (This is set as default).
id	(Optional) Fixed identifier.
include-ports {**source** *[id]* | **destination***[id]*	Sets the load-balancing algorithm to include source port and destination port.
src-only *[id]*	Sets the load-balancing algorithm to include source-only port.

Command Default

The universal load-balancing algorithm is selected. If you do not configure the fixed identifier for a load-balancing algorithm, the router automatically generates a unique ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was modified. The **src-only** algorithm is added.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip cef load-sharing algorithm command.

You can enable **ECMP keying** to send the configurations for both IPv4 and IPv6.

Examples

The following example shows how to enable the CEF load-balancing algorithm for universal:

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm universal
```

The following example shows how to enable the IP CEF load-sharing algorithm to include source and destination ports algorithm:

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm include-ports source destination
Device(config)# commit
```

The following example shows how to enable CEF load-sharing algorithm to src-only port algorithm:

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm src-only [id]
Device(config)# commit
```

ip-clear-dont-fragment

ip clear-dont-fragment—Clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.

Note **ip clear-dont-fragment** clears the DF bit when there is fragmentation needed and the DF bit is set. For packets not requiring fragmentation, the DF bit is not affected.

The option to clear the Dont Fragment bit is available for Cisco SD-WAN tunnels interfaces only.

By default, the clearing of the DF bit is disabled.

vManage Feature Template

Configuration ▶ Templates ▶ Cellular Interface

Configuration ▶ Templates ▶ VPN Ethernet Interface

Configuration ▶ Templates ▶ VPN Interface DSL IPoE

Configuration ▶ Templates ▶ VPN Interface DSL PPPoA

Configuration ▶ Templates ▶ VPN Interface DSL PPPoE

Configuration ▶ Templates ▶ VPN Interface Multilink

Configuration ▶ Templates ▶ VPN Interface T1/E1

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE clear-dont-fragment

Example

This example shows how to clear the DF bit in IPv4 packets being sent out an interface:

```
Device# config-transaction
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip clear-dont-fragment
Device(config-if)#
```

ip community-list

To create a community list that you can use in a route map to filter BGP routes based on community values, use the **ip community-list** command in global configuration mode. It supports two types of community lists: **standard** and **expanded**.

Standard community list performs an exact match against the specified community values, while the expanded community list uses a regular expression to match community values.

To remove the community-list configuration, use the **no** form of this command.

ip { **community-list** | **community-list-deprecated** } { *standard-list-number* | **standard** *list-name* { **deny** | **permit** | **deny-v1 deny-list** | **permit-v1 permit-list** } [*community-number*] [*AA:NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**] [**gshut**] }

ip { **community-list** | **community-list-deprecated** } { *expanded-list-number* | **expanded** *list-name* { **deny** | **permit** | **deny-v1 deny-list** | **permit-v1 permit-list** } *regular-expression* }

no ip community-list { *standard-list-number* | **standard** *list-name* { **deny** | **permit** } [*community-number*] [*AA:NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**] }

community-list-deprecated	This keyword is provided for backward compatibility. Use this keyword instead of **community-list** if you are using Cisco Catalyst SD-WAN Manager Release 20.15.5 and later with Cisco IOS XE Catalyst SD-WAN devices running 17.14 or earlier.
standard-list-number	Standard community list defined with a number. Range: 1 to 99
standard *list-name*	Standard community list defined with a name.
deny	Exclude routes that match the BGP community attributes specified in this command.
permit	Include routes that match the BGP community attributes specified in this command.
deny-v1 deny-list	These keywords are provided for backward compatibility. Use these keywords instead of **deny** if you are using Cisco Catalyst SD-WAN Manager Release 20.15.1 to 20.15.4 with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier.
permit-v1 permit-list	These keywords are provided for backward compatibility. Use these keywords instead of **permit** if you are using Cisco Catalyst SD-WAN Manager Release 20.15.1 to 20.15.4 with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier.

community-number	Community value attached to a BGP route. It is used as a matching criterion to identify specific BGP routes that carry that particular tag, allowing you to either include or exclude those routes in a route map. Range: 1 to 4,294,967,200 A well-known community in a community list is a predefined community value used to tag routes with specific routing policies. Standard type is used to specify these well-known communities or community numbers.
AA:NN	Community value expressed in new format (Autonomous system:community number). Range: 1 to 65535:1 to 65535
internet **local-AS** **no-advertise** **no-export** **gshut**	A well-known community is a predefined community attribute used to tag routes with specific routing policies. • internet: Advertises the route to the internet community. • local-AS: Prevents the advertisement of a route outside local autonomous system • no-advertise: Prevents the advertisement of a route to any BGP peer. • no-export: Prevents the route from being advertised to external BGP peers. • gshut: Community of routes gracefully shut down.
expanded-list-number	Expanded community list defined with a number. Range: 100 to 500
expanded *list-name*	Expanded community list defined with a name.
regular-expression	Regex pattern used to match community values for flexible and complex filtering. Regular expressions are only supported with expanded community lists.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Route maps use community lists to match BGP community values to control route acceptance, preference, distribution, or advertisement.

If you are using Cisco Catalyst SD-WAN Manager Release 20.15.1 to 20.15.4 with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier, use the **permit-v1** and **permit-list** keywords for backward compatibility.

```
ip community-list standard TEST permit-v1 permit-list 10
```

If you are using Cisco Catalyst SD-WAN Manager Release 20.15.5 and later with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier, use the **deprecated** keyword for backward compatibility:

```
ip community-list-deprecated standard TEST permit 10
```

Examples

This example creates a standard BGP community list named COMMS that permits BGP routes with the community values 10:10 and 20:20. When a route-map uses this list in a **match** statement, the permit entry requires a BGP route to carry both community values **10:10** and **20:20** to satisfy the match condition. The route can also possess other community attributes; their presence does not prevent a match as long as **10:10** and **20:20** are both present. If a route contains only one of these two communities, it will not match this specific permit entry.

```
ip community-list standard COMMS permit 10:10 20:20
route-map TEST_COMM permit 10
 match community COMMS
```

When a route-map uses this list in an **exact-match** statement, the permit requires BGP route to carry exactly **10:10** and **20:20** community values to satisfy the **exact-match** condition. If a route contains more than these two communities, the match will be rejected.

```
ip community-list standard COMMS permit 10:10 20:20
route-map TEST_COMM permit 10
 match community COMMS exact-match
```

ip dhcp client vendor-class

By default the DHCP client carries PID (Product ID) of the device in option-124. This default behaviour can be overridden by configuring below CLI:

ip dhcp client vendor-class [**mac-address** | **ascii** | **hex** | **disable**]

Syntax Description

mac-address	The mac address of the device.
ascii	The user defined string in ascii format.
hex	The user defined string in hexadecimal format.
disable	Disables sending option-124 to DHCP messages.

Command Default

By default option-124 carries PID of the device.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

By default the DHCP client carries PID of the device in option-124. This default behaviour can be overridden by configuring the **ip dhcp client vendor-class** command.

Examples

The following example shows the configuration to override the decive PID with MAC address:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class mac-address
    !
```

The DHCP vendor-class option, overrides the Device PID with MAC Address.

The following example shows the configuration to override the device PID with user defined string in hex or in ascii format:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class hex aabbcc
    !
```

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class ascii cisco
    !
```

The following example shows the configuration to disable option-124 in DHCP messages:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class disable
    !
```

ip dhcp conflict logging

To enable conflict logging on a Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp conflict logging** command in global configuration mode. To disable conflict logging, use the **no** form of this command.

ip dhcp conflict logging

no ip dhcp conflict logging

This command has no arguments or keywords.

Command Default

Conflict logging is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command was introduced.

Usage Guidelines

A DHCP server database agent should be used to store automatic bindings. If a DHCP server database agent is not used, specify the **no ip dhcp conflict logging** command to disable the recording of address conflicts. By default, the DHCP server records DHCP address conflicts in a log file.

Example

The following example disables the recording of DHCP address conflicts:

```
Device(config)# no ip dhcp conflict logging
```

ip dhcp use

To control what information the Dynamic Host Configuration Protocol (DHCP) server accepts or rejects during address allocation, use the **ip dhcp use** command in global configuration mode.

To disable the use of Dynamic Host Configuration Protocol (DHCP) parameters during address allocation, use the no form of this command.

ip dhcp use { **class** | **vrf remote** }
no ip dhcp use class

Syntax Description

class	Specifies that the DHCP server use DHCP classes during address allocation.
vrf	Specifies whether the DHCP server ignores or uses the receiving VPN routing and forwarding (VRF) interface during address allocation.

Command Default

The DHCP server allocates addresses by default.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

When the Cisco IOS DHCP server code is allocating addresses, you can use the **ip dhcp use** command to either enable or disable the use of VRF configured on the interface, or to configure DHCP classes. If you use the **no ip dhcp use class** command, the DHCP class configuration is not deleted.

For usage guidelines, see Cisco IOS XE `ip dhcp use` command.

Examples

The following example shows how to configure the DHCP server to use the relay agent information option during address allocation:

```
Device(config)# ip dhcp use class
```

The following example shows how to configure the DHCP server to enable the use of the VRF configured on the interface during address allocation:

```
Device(config)# ip dhcp use vrf remote
```

The following example shows how to configure the DHCP server to disable the use of class during address allocation:

```
Device(config)# no ip dhcp use class
```

ip dhcp smart-relay

To allow the Cisco Dynamic Host Configuration Protocol (DHCP) relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server, use the **ip dhcp smart-relay** command in global configuration mode. To disable this smart-relay functionality and restore the default behavior, use the **no** form of this command.

ip dhcp smart-relay

no ip dhcp smart-relay

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was introduced.

Usage Guidelines

The DHCP relay agent attempts to forward the primary address as the gateway address. After three attempts and no response, the relay agent automatically switches to secondary addresses.

Example

The following example enables the DHCP relay agent to automatically switch to secondary address pools:

```
Device(config)# service dhcp
Device(config)# interface GigabitEthernet0/0
Device(config)# ip address 172.16.0.1 255.255.0.0
Device(config)# secondary ip address 192.168.255.254 255.255.0.0
Device(config)# ip helper-address 10.0.0.1
Device(config)# ip dhcp smart-relay
Device(config)# end
!
```

ip dhcp use hardware-address client-id

To set the hardware-address as a client-id on all dhcp requests, use the **ip dhcp use hardware-address client-id** command in global configuration mode. To remove the hardware-address as the client-id, use the **no** form of this command.

ip dhcp use hardware-address client-id
no ip dhcp use hardware-address client-id

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Subscriber-id, vrf-id, hardware-address can be used as client-id in DHCP requests. Use this **ip dhcp use hardware-address client-id** command to set the hardware-address as a client-id on all DHCP requests.

Examples

The following example shows how to set the client-id of dhcp requests to use the hardware-address.

```
Device(config)# ip dhcp use hardware-address client-id
```

Table 1: Related Commands

Commands	Description
ip dhcp use class	DHCP server to use the relay agent information option during address allocation.
ip dhcp use subscriber-id	DHCP server to use the subscriber-id information option during address allocation.
ip dhcp use vrf	DHCP server to use the VRF information option during address allocation.

ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** interface configuration command. To disable this function, use the **no** form of this command.

ip directed-broadcast

no ip directed-broadcast

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled; all IP directed broadcasts are dropped.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release Amsterdam 17.2.1v	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For the usage guidelines, see ip directed-broadcast.

Examples

```
csr8k(config)# interface GigabitEthernet 1.101
csr8k(config-if)# ip address 192.168.66.1
csr8k(config-if)# ip directed-broadcast
```

ip dns server

To enable the Domain Name System (DNS) server on a router, use the **ip dns server** command in global configuration mode. To disable the DNS server, use the **no** form of the command.

ip dns server
no ip dns server

Syntax Description

This command has no arguments or keywords.

Command Default

The DNS server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use this command to enable the DNS server as needed.

Examples

In the following example, the DNS server is enabled:

```
Device(config)# ip dns server
```

ip domain lookup

To enable the Domain Name Server (DNS) lookup feature, use the **ip domain-lookup** command. Use the **no** form of this command to disable this feature.

ip domain lookup
no ip domain lookup

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip domain lookup` command.

Examples

This example shows how to disable the DNS server lookup feature:

```
Device(config)# no ip domain-lookup
```

ip finger

To configure a system to accept Finger protocol requests (defined in RFC 742), use the **ip finger** command in global configuration mode. To disable this service, use the **no**form of this command.

ip finger
no ip finger

Command Default

Disabled

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 vManage CLI templates.

Examples

The following example disables the Finger protocol:

```
Device(config)# no ip finger
```

ip helper-address

To enable forwarding of User Datagram Protocol (UDP) broadcasts, including Bootstrap Protocol (BOOTP), received on an interface, use the **ip helper-address** command in interface configuration mode. To disable forwarding of broadcast packets to specific addresses, use the**no** form of this command.

ip helper-address *address*
no ip helper-address *address*

Syntax Description

address	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.

Command Default

UDP broadcasts are not forwarded.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

For the usage guidelines, see ip helper-address and dhcp-helper

DHCP helper addresses are not supported in VPN 0 / VPN 512.

Examples

The following example shows how to define an address that acts as a helper address:

```
Device(config)# interface GigabitEthernet 1.101
Device(config-if)# ip nbar protocol-discovery
Device(config-if)# ip helper-address 10.8.4.5
```

ip host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view, use the **ip host** command in global configuration mode. If the hostname cache does not exist yet, it is automatically created. To remove a hostname-to-address mapping, use the **no** form of this command.

ip host [**vrf** *vrf-name*] [*ip-address1* . . . [*ip-addressn*]]
no ip host [**vrf** *vrf-name*] [*ip-address1* . . . [*ip-addressn*]]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VRF) routing and forwarding (VRF) instance whose hostname cache is to store the mappings. Default is the global VRF (that is, the VRF whose name is a NULL string).

hostname	Name of the host. The first character can be either a letter or a number. If you use a number, the types of operations you can perform (such as ping) are limited.
ip-address1 . . . ip-addressn	Associated host IP address. You can specify an IPv4 or IPv6 address for the host IP address and additional IP addresses. (Optional) Additional associated IP addresses, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.

Command Default

No static hostname-to-address mapping is added to the DNS hostname cache.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip host` command.

For backward compatibility of Cisco Catalyst SD-WAN Manager Release 20.15.1 and later with devices running Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and earlier, when using CLI device templates or CLI add-on feature templates, use a different form of the **ip host** command. When pushing the CLI device templates or CLI add-on feature templates to the device in global configuration mode, use the following form of the **ip host** command with **ip-list** :

ip host *hostname* **ip-list** *ip-address*

The following example shows how to add a mapping entry to the hostname vbond.ubi.in and IPv4 address 10.0.0.0 with list of IP addresses associated with a hostname.

```
Device(config)# ip host vbond.ubi.in ip-list 10.0.0.0
```

Examples

The following example shows how to add two mapping entries to the hostname that is associated with the VRF 101 and then remove one of those entries from that hostname cache:

```
Device(config)# ip host vrf 101 test-1 192.0.2.141 192.0.2.241
Device(config)# no ip host vrf 101 test-1 192.0.2.141
```

ip host *ip-address*

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view, use the **ip host** command in global configuration mode. If the hostname cache does not exist yet, it is automatically created. To remove a hostname-to-address mapping, use the **no** form of this command.

ip host [*ip-address1* **. . .** [*ip-addressn*]]
no ip host [*ip-address1* **. . .** [*ip-addressn*]]

Syntax Description

ip-address1 **. . .***ip-addressn*	IP address of Cisco Catalyst SD-WAN Validator. You can specify an IPv4 or IPv6 address for the host IP address and additional IP addresses. (Optional) Additional associated IP addresses, delimited by a single space. You can configure a maximum of 24 IP addresses. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.

Command Default

No static hostname-to-address mapping is added to the DNS hostname cache.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to add two Cisco Catalyst SD-WAN Validator IP addresses as IP hosts, and how to remove one of them.

```
Device(config)# ip host 192.0.2.141 192.0.2.241

Device(config)# no ip host 192.0.2.141
```

ip http authentication

To specify a particular authentication method for HTTP server users, use the **ip http authentication** command in global configuration mode. To disable a configured authentication method, use the **no** form of this command.

ip http authentication local
no ip http authentication [**local**]

Syntax Description

local	Indicates that the login user name, password and privilege level access combination specified in the local system configuration (by the **username** global configuration command) should be used for authentication and authorization.

Command Default

The “enable” password is required when users (clients) connect to the HTTP server. Three command privilege levels exist on the router.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip http authentication` command.

Examples

The following example shows how to specify that the login user name, password and privilege level access combination specified in the local system configuration should be used for authentication and authorization.

```
Device(config)# ip http authentication local
```

ip http client source-interface

To enable HTTP client on your IP or IPv6 system, use the **ip http client** command in global configuration mode. To disable the HTTP client, use the **no** form of this command.

Supported Parameters

type	Name of the source interface.
number	Number of the source interface.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip http client source-interface command.

Example

```
Device(config)# ip http client source-interface GigabitEthernet0/0/2
```

ip http secure-server

To enable a secure HTTP (HTTPS) server, use the **ip http secure-server** command in global configuration mode. To disable an HTTPS server, use the **no** form of this command.

ip http secure-server
no ip http secure-server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTPS server is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip http secure-server` command.

Examples

In the following example the HTTPS server is disabled:

```
Device(config)# no ip http secure-server
```

ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, use the **ip http server**command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http server
no ip http server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTP server is disabled by default.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE`ip http server` command.

Examples

The following example shows how to disable the HTTP server:

```
Device(config)#no ip http server
```

ip http tls-version

To configure TLS version for HTTPS Server and HTTPS client sessions, use the **ip http tls-version** command in global configuration mode. To remove the configuration, use the **no** form of this command.

ip http tls-version *tls-version*
no ip http tls-version *tls-version*

Syntax Description

tls-version	Specifies TLS versions—TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

The **ip http tls-version** command allows you to set a particular version used for HTTP secure-server sessions. The underlying SSL infrastructure supports the option of specifying either all or only one TLS version. Hence the HTTPS provides the option to specify the individual version.

By default, three TLS versions used for HTTPS sessions are supported—TLSv1.2 and TLSv1.3. To enable a particular version use this command.

Examples

The following shows how to configure TLS version 1.0 for the HTTPS session:

```
Device(config)# ip http tls-version TLSv1.0
```

ip icmp rate-limit unreachable

To limit the rate at which Internet Control Message Protocol (ICMP) unreachable messages are generated for a destination, use the **ip icmp rate-limit unreachable** command in global configuration mode.

To use the default, use the **no** form of this command.

ip icmp rate-limit unreachable *ms*
no ip icmp rate-limit unreachable

Syntax Description

ms	The optional ms argument is a time limit in milliseconds (ms) in which one unreachable message is generated. The valid range is from 1 ms to 4294967295 ms. **Note** Counting begins as soon as this command is configured.

Command Default The default value is one ICMP destination unreachable message per 500 ms.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE ip icmp rate-limit unreachable command.

Examples The following example sets the rate of the ICMP destination unreachable message to one message every 10 ms:

```
Device(config)# ip icmp rate-limit unreachable 10
```

The following example turns off the previously configured rate limit:

```
Device(config)# no ip icmp rate-limit unreachable
```

ip icmp redirect

To control the type of Internet Control Message Protocol (ICMP) redirect message that is sent, use the **ip icmp redirect** command in global configuration mode. To set the value back to the default, use the **no**form of this command.

ip icmp redirect { **host** | **subnet** }
no ip icmp redirect

Syntax Description

host	Sends ICMP host redirects.
subnet	Sends ICMP subnet redirects.

Command Default The router will send ICMP subnet redirect messages.

Because the **ip icmp redirect subnet** command is the default, the command will not be displayed in the configuration.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1aexit	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE ip icmp redirect command.

Examples

The following example enables the router to send out ICMP host redirects:

```
Device(config)# ip icmp redirect host
```

The following example sets the value back to the default, which is subnet redirects:

```
Device(config)# ip icmp redirect subnet
```

ip igmp ssm-map query dns

To configure Domain Name System (DNS)-based Source Specific Multicast (SSM) mapping, use the **ip igmp ssm-map query dns** command in global configuration mode. To disable DNS-based SSM mapping, use the **no** form of this command.

ip igmp ssm-map query dns
no ip igmp ssm-map query dns

Syntax Description

This command has no arguments.

Command Default

This command is enabled by default when the **ip igmp ssm-map enable** command 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 vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip igmp ssm-map query dns command.

Examples

The following example shows how to disable DNS-based SSM mapping:

```
Device(config)# no ip igmp ssm-map query dns
```

ip load-sharing algorithm

To enable load balancing algorithm on an interface for IPv4, use the **ip load-sharing algorithm** command in Cisco Catalyst SD-WAN configuration mode. To disable load balancing algorithm on an interface, use the **no** form of this command.

ip load-sharing algorithm { **ip-and-ports** | **src-dst-ip** | **src-ip-only** }
no ip load-sharing algorithm { **ip-and-ports** | **src-dst-ip** | **src-ip-only** }

Syntax Description

ip-and-ports	Sets the load-balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.

src-dst-ip	Sets the load-balancing algorithm to the src-dst-ip algorithm that uses a source and destination ip.
src-ip-only	Sets the load-balancing algorithm to the src-ip algorithm that uses source ip.

Command Default

src-dst-ip algorithm is enabled by default.

Command Modes

SD-WAN configuration (config-sdwan)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

When the load-balancing algorithm is set to src-dst-ip mode, each router on the network can make a different load sharing decision for each source-destination address pair.

The ip-and-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not loadshared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams.

Examples

The following example shows how to enable load-balancing algorithm for source, destination ip and port:

```
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm ip-and-ports
```

The following example shows how to enable load balancing algorithm for source, destination ip:

```
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm src-dst-ip
```

The following example shows how to enable load balancing algorithm for source ip only:

```
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm src-ip-only
```

ip mtu

To set the maximum transmission unit (MTU) size of IP packets that are sent on an interface, use the **ip mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ip mtu *bytes*
no ip mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The default MTU value depends on the interface type.

Table 2: Default MTU Values by Interface Type

Interface Type	Default MTU (Bytes)
ATM	4470
Ethernet	1500
FDDI	4470
High-Speed Serial Interface High Speed Access (HSSI HSA)	4470
Serial	1500
Token Ring	4464
VRF-Aware Service Infrastructure (VASI)	9216

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see the IOS XE ip mtu command.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip mtu 1500
```

```
Device(config)# interface ATM 0/2/0.1 point-to-point
Device(config-if)# ip mtu 1500
```

ip multicast route-limit

To limit the number of multicast routes (mroutes) that can be added to a multicast routing table, use the **ip multicast route-limit**command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip multicast route-limit *limit*
no ip multicast route-limit *limit*

Syntax Description

limit	The number of mroutes that can be added. The range is from 1 to 2147483647. The default is 2147483647.

Command Default

limit : 2147483647

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **ip multicast route-limit** command limits the number of multicast routes that can be added to a router and generates an error message when the limit is exceeded.

For usage guidelines, see the Cisco IOS XE `ip multicast route-limit` command.

Examples

The following example shows how to set the mroute limit to 200,000:

```
Device(config-transaction)# ip multicast route-limit 200000
```

ip name-server

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** command in global configuration mode. To remove the addresses specified, use the **no** form of this command.

ip name-server [**vrf** *server-address*]
no ip name-server [**vrf** *server-address*]

Syntax Description

vrf	Defines a virtual private network's routing and forwarding instance (VRF) table.
server-address	IPv4 address of a name server.
server-ip-list	List of IPv4 addresses separated by a comma.

Command Default

No name server addresses are specified.

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 vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip name-server` command.

For backward compatibility of Cisco Catalyst SD-WAN Manager Release 20.12.1 with devices running Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, when using CLI device templates or CLI add on feature templates, use a different form of **ip name-server** command. If **ip name-server** command is configured in VRF, use the following form of the command:

ip name-server vrf *vrf* **server-ip-list** *list of DNS servers*

If **ip name-server** command is configured in a global mode, use **ip name-server no-vrf** *list of DNS servers*

Examples

The following example shows how to specify IPv4 host 10.0.0.0 as the name server:

```
Device(config)# ip name-server 10.0.0.0
```

ip pim

To enable Protocol Independent Multicast (PIM) on an interface, use the **ip pim** command in interface configuration or virtual network interface configuration mode. To disable PIM on the interface, use the **no** form of this command.

Supported Parameters

sparse-mode	Enables sparse mode of operation.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip pim command.

Examples

```
ip pim vrf 1 bsr-candidate GigabitEthernet5
ip pim vrf 1 rp-address 172.16.255.116
ip pim vrf 1 rp-candidate GigabitEthernet5 interval 10 priority 5

ip pim sparse-mode

spt-only
```

ip pim bsr-candidate

To configure a router to announce its candidacy as a bootstrap router (BSR), use the **ip pim bsr-candidate** command in global configuration mode. To remove this router as a BSR candidate, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority* [**accept-rp-candidate** [*acl-number acl-name*]]]]

no ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority* [**accept-rp-candidate** [*acl-number acl-name*]]]]

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to announce its candidacy as a BSR for the multicast virtual private network's (MVPN) multicast routing and forwarding instance (MVRF) specified for the *vrf-name* argument.

interface-type interface-number	Interface type and number of the router from which the BSR address is derived. This address is sent in BSR messages. **Note** This interface must be enabled for Protocol-Independent Multicast (PIM) using the **ip pim** command.
hash-mask-length	(Optional) Length of a mask (32 bits maximum) that is to be combined with the group address before the PIMv2 hash function is called. All the groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0.
priority	(Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The default priority is 0. The C-BSR with the highest priority value is preferred. **Note** The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate BSRs. This implementation predates RFC 5059, which specifies that 64 be used as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from RFC 5059. To comply with the default priority value specified in the RFC, you must explicitly set the priority value to 64.
accept-rp-candidate	(Optional) Specifies that the C-RP candidate is to be filtered.
acl-number	(Optional) Number of the access control list (ACL) to be used to filter C-RP advertisements. The range is 100 to 199 for standard ACL numbers and 2000 to 2699 for extended ACLs. **Note** You must have a valid standard or extended ACL in order to use an ACL in your configuration.
acl-name	(Optional) Name of the ACL to be used to filter C-RP advertisements. **Note** You must have a valid standard or extended ACL in order to use an ACL in your configuration.

Command Default

The router is not configured to announce itself as a candidate BSR.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip pim bsr-candidate command.

Examples

The following example shows how to configure the IP address of a router on GigabitEthernet interface 0/0 to be a BSR C-RP with a hash mask length of 0 and a priority of 192:

```
Device(config)# ip pim vrf 1 bsr-candidate GigabitEthernet 0/0 0 192
```

ip pim rp-address

To statically configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for multicast groups, use the **ip pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

Supported Parameters

vrf *vrf-name*	(Optional) Specifies that the static group-to-RP mapping be associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
rp-address	IP address of the RP to be used for the static group-to-RP mapping. This is a unicast IP address in four-part dotted-decimal notation.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip pim rp-address command.

Examples

```
ip pim vrf 1 bsr-candidate GigabitEthernet5
ip pim vrf 1 rp-address 172.16.255.116
ip pim vrf 1 rp-candidate GigabitEthernet5 interval 10 priority 5

ip pim sparse-mode

spt-only
```

ip pim rp-candidate

To configure a router to advertise itself to the bootstrap router (BSR) as a Protocol-Indepedenet Multicast (PIM) Version 2 (PIMv2) candidate rendezvous point (C-RP), use the **ip pim rp-candidate** command in global configuration mode. To remove this router as a C-RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-type interface-number* [**group-list** *access-list*] [**interval** *seconds*] [**priority** *value*]

no ip pim [**vrf** *vrf-name*] **rp-candidate**

Syntax Description

vrf *vrf-name*	(Optional) Configure the router to advertise itself to the BSR as PIMv2 C-RP for the multicast virtual private network's (MVPN) multicast routing and forwarding instance (MVRF) specified for the *vrf-name* argument.
interface-type interface-number	IP address associated with this interface type and number to be advertised as a C-RP address.
group-list *access-list*	(Optional) Specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists. **Note** You must have a valid standard or extended ACL in order to use an ACL in your configuration.
interval *seconds*	(Optional) Specifies the C-RP advertisement interval, in seconds. The range is from 1 to 16383. The default value is 60.
priority *value*	(Optional) Specifies the priority of the C-RP. The range is from 0 to 255. The default priority value is 0. The BSR C-RP with the lowest priority value is preferred. **Note** The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate RPs. This implementation predates the draft-ietf-pim-sm-bsr IETF draft, the first IETF draft to specify 192 as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from the IETF draft. To comply with the default priority value specified in the draft, you must explicitly set the priority value to 192.

Command Default

The router is not configured to announce itself to the BSR as a PIMv2 C-RP.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip pim rp-candidate command.

Examples

The following example shows how to configure a router to advertise itself as a C-RP to the BSR in its PIM domain. The standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Gigabit Ethernet interface 0/0. That RP is responsible for the groups with the prefix 239.

```
Device(config)# ip pim vrf 1 rp-candidate GigabitEthernet5 interval 10 priority 5
Device(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

ip prefix-list

To create a prefix list or to add a prefix list entry, use the **ip prefix-list** command in global configuration mode. To delete a prefix list entry, use the **no** form of this command.

ip prefix-list *list-name* **permit** *network / length*
no ip prefix-list *list-name* **permit** *network / length*

Syntax Description

list-name	Name to identify the prefix list. Do not use the words *detail* or *summary* as a list name because they are keywords in the **show ip prefix-list** command.
permit	Permits access for a matching condition.

Command Default

No prefix lists or prefix list entries are created.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip prefix-list` command.

Examples

In the following example, a prefix list is configured to permit the default route 10.0.0.0/8:

```
Device(config)# ip prefix-list TEST permit 10.0.0.0/8
```

ip redirects

To enable the task of sending Internet Control Message Protocol (ICMP) redirect messages if the software is forced to resend a packet through the same interface on which it was received, use the **ip redirects** command in interface configuration mode. To disable the task of sending redirect messages, use the **no** form of this command.

ip redirects
no ip redirects

Syntax Description

This command has no arguments or keywords.

Command Default

ICMP redirect messages are sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip redirects.

Examples

The following example shows how to enable the sending of ICMP redirect messages on GigabitEthernet interface 1:

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip redirects
```

The following example shows how to disable the sending of ICMP redirect messages on Tunnel interface 1:

```
Device(config)# interface Tunnel 1
Device(config-if)# no ip redirects
```

ip rcmd

To enable the IP remote command (rcmd) option, use the **ip rcmd** command in global configuration mode. To disable the IP remote command (rcmd) option, use the **no** form of this command.

ip rcmd { **domain-lookup** | **rcp-enable** | **rsh-enable** }
no ip rcmd { **domain-lookup** | **rcp-enable** | **rsh-enable** }

Syntax Description

domain-lookup Re-enables basic Domain Name System (DNS) security check for Remote Copy Protocol (RCP) and remote shell (rsh).

We recommend not including the ip **rcmd domain-lookup** command in a CLI add-on profile.

However, if you decide to use the **ip rcmd domain-lookup** command in a CLI add-on profile, do one of these to prevent an error:

- In the configuration group that you are using to push a configuration to the device, enable IP domain lookup.

  To do this: In the configuration group, open **System profile** > **Global** feature. Enable Domain Lookup.

- Alternatively, include the **ip domain lookup** command in the CLI add-on profile. This prevents the **ip rcmd domain-lookup** command from triggering an error.

  A simplified excerpt of a CLI add-on profile showing the two commands:

  ```
  ip domain lookup
  ip rcmd domain-lookup
  ```

  Note
  Executing the **show running-config** command on a device does not show the **ip domain lookup** command in the output even if it is configured. However, with the **all** keyword, the **show running-config all** command output does show the **ip domain lookup** command if configured.

rcp-enable	Allows remote users to copy files to and from the router using RCP.
rsh-enable	Allows remote users to execute commands on it using rsh.

Command Default

Domain-lookup is enabled.

rcp-enable is disabled.

rsh-enable is disabled.

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 abbreviation RCMD (remote command) is used to indicate both rsh and RCP. DNS lookup for RCMD is enabled by default and is performed as a basic security check. RCP-enable allows a remote user to execute RCP commands on the router. rsh, used as a client process, gives users the ability to remotely get router information, such as status, without the need to connect to the router and then disconnect. RSH-enable enables the router to receive rsh requests from remote users.

Examples

The following example shows how to enable RCP and rsh.

```
Device(config)# ip rcmd rcp-enable
Device(config)# ip rcmd rsh-enable
```

ip rcmd rcp-enable

To allow remote users to copy files to and from a router using Remote Copy Protocol (RCP), use the **ip rcmd rcp-enable** command in global configuration mode. To disable RCP on the device, use the **no** form of this command.

ip rcmd rcp-enable
no ip rcmd rcp-enable

Syntax Description

This command has no arguments or keywords.

Command Default

To ensure security, the router is not enabled for RCP by default.

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 vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip rcmd rcp-enable` command.

Examples

The following example shows how to enable RCP for copying files to and from a router:

```
Device(config)#ip rcmd rcp-enable
```

ip rcmd rsh-enable

To configure a router to allow remote users to execute commands on it using remote shell protocol (rsh), use the **ip rcmd rsh-enable** command in global configuration mode. To disable a router that is enabled for rsh, use the **no** form of this command.

ip rcmd rsh-enable
no ip rcmd rsh-enable

Syntax Description

This command has no arguments or keywords.

Command Default

To ensure security, the router is not enabled for rsh by default.

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 vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip rcmd rsh-enable` command.

Examples

The following example shows how to enable a router as an rsh server:

```
Device(config)# ip rcmd rsh-enable
```

ip route vrf

To establish static routes for a virtual private network's routing and forwarding (VRF) instance, use the **ip route vrf** command in global configuration mode. To disable static routes, use the **no** form of this command.

ip route vrf *vrf-name prefix mask* [*interface interface-number*] [*next-hop-address* [**tag** *tag*] [**track** *number*]]
no ip route vrf *vrf-name prefix mask* [*interface interface-number*] [*next-hop-address* [**tag** *tag*] [**track** *number*]]

Syntax Description

vrf-name	Name of the VRF for the static route.
prefix	IP route prefix for the destination, in dotted decimal format.
mask	Prefix mask for the destination, in dotted decimal format.

next-hop-address	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
interface	(Optional) Name of network interface to use.
interface-number	(Optional) Number identifying the network interface to use.
tag *tag*	(Optional) Specifies the label (tag) value that can be used for controlling redistribution of routes through route maps.
track *number*	(Optional) Associates a track object with this route. Valid values for the number argument range from 1 to 500.

Command Default

No default behavior or values.

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 vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameters qualified: prefix mask for destination address, next-hop address, interface type and number, tag.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip route vrf` command.

Examples

```
Device (config)# ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1 track 10
Device (config)# ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1 tag 2
Device (config)# ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1
Device (config)# ip route vrf 1 192.0.2.1 255.255.255.0 GigabitEthernet2
Device (config)# ip route vrf 1 192.0.2.1 255.255.255.0
```

ip route

To establish a static route, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

ip route *prefix mask* [*ip-address* | *interface-type-interface-number* [*ip-address*] | **Null0** *distance*] [**tag** *tag* | **track**]

no ip route *prefix mask* [*ip-address* | *interface-type-interface-number* [*ip-address*] | **Null0** *distance*] [**tag** *tag* | **track**]

Syntax Description

prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach the network.

interface-type interface-number	Network interface type and interface number. Valid values for the *number* argument range from 1 to 500.
track	(Optional) Associates a track object with this route.
tag *tag*	(Optional) Tag value that can be used as a match value for controlling redistribution through route maps.
Null0	Specifies null0 as the interface to prevent routing loops.
distance	(Optional) Administrative distance. The range is 1 to 255. The default administrative distance for a static route is 1.

Command Default

No static routes are established.

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 vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameters qualified: next-hop-address, Dialer, tag, track, Null0, distance.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip route`command.

Examples

The following example shows how to route packets for network 192.0.2.1 to a router at 198.51.100.1:

```
ip route 192.0.2.1 255.255.255.0 198.51.100.1
```

```
Device(config)# ip route 192.0.2.1 255.255.255.0 198.51.100.1 track <>
ip route 192.0.2.1 255.255.255.0 Dialer2 198.51.100.1 tag <>
ip route 192.0.2.1 255.255.255.0 198.51.100.1 tag <>
ip route 192.0.2.1 255.255.255.0 Dialer2 tag <>
ip route 192.0.2.1 255.255.255.0 Dialer2 198.51.100.1 <>
ip route 192.0.2.1 255.255.255.0 198.51.100.1 <>
ip route 192.0.2.1 255.255.255.0 Dialer2 <>
ip route 192.0.2.1 255.255.255.0 GigabitEthernet2 <>
ip route 192.0.2.1 255.255.255.0 <>
```

ip source-route

To allow the Cisco IOS software to handle IP datagrams with source-routing header options, use the **ip source-route** command in global configuration mode. To have the software discard any IP datagram containing a source-route option, use the **no** form of this command.

ip source-route
no ip source-route

Syntax Description

This command has no arguments or keywords.

Command Default 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 vManage CLI templates.

Examples

The following example shows how to disable the handling of IP datagrams with source-routing header options:

```
Device(config)# no ip source-route
```

ip ssh version

To specify the version of Secure Shell (SSH) to be run on a router, use the **ip ssh version**command in global configuration mode. To disable the version of SSH that is configured and to return to compatibility mode, use the **no** form of this command.

ip ssh version 2
no ip ssh version

Syntax Description

2	Router runs only SSH Version 2.

Command Default If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

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 vManage CLI templates.

Usage Guidelines Use this command with the keyword **2** to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

Examples

The following example shows that SSH Version 2 support is configured:

```
Router (config-transaction)# ip ssh version 2
```

The following example shows that SSH Version 2 configuration is removed:

```
Router (config-transaction)# no ip ssh version
```

ip tcp adjust-mss

To adjust the maximum segment size (MSS) value of TCP synchronize/start (SYN) packets that go through a router, use the **ip tcp adjust-mss** command in interface configuration mode. To return the MSS value to the default setting, use the **no** form of this command.

ip tcp adjust-mss *max-segment-size*
no ip tcp adjust-mss

Syntax Description

max-segment-size	Maximum segment size, in bytes. The range is from 500 to 1460.

Command Default

The MSS is determined by the originating host.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip tcp adjust-mss.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip tcp adjust-mss 1100
```

ip tcp mss

To enable a maximum segment size (MSS) for TCP connections originating or terminating on a router, use the **ip tcp mss** command in global configuration mode. To disable the configuration of the MSS, use the no form of this command.

ip tcp mss *bytes*
no ip tcp mss

Syntax Description

bytes	Maximum segment size for TCP connections in bytes. Valid values are from 0 to 10000.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip tcp mass` command.

Examples

The following example sets the MSS value at 1200:

```
Device(config)# ip tcp mss 1200
```

ip unnumbered

To enable IP processing on an interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command in interface configuration mode or subinterface configuration mode. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered *type*
no ip unnumbered

Syntax Description

type	Type of interface. For more information, use the question mark (**?**) online help function.

Command Default

Unnumbered interfaces are not supported.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip unnumbered command.

Examples

The following example shows how to configure GigabitEthernet 1 as an IP unnumbered interface.

```
Device(config)# interface Tunnel 1
Device(config-if)# ip unnumbered GigabitEthernet1
```

ip virtual-reassembly

ip virtual-reassemly command is used to enable a virtual packet reassembly on a Cisco IOS XE Catalyst SD-WAN device's interface. Virtual packet reassembly is a mechanism that helps in handling fragmented packets. To disable virtual reassembly, use the **no** form of this command.

ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]

no ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]

Syntax Description

max-reassemblies	(Optional) The number specifies the maximum number of IP packet reassemblies that can be held in the reassembly queue.
max-fragments	(Optional) The number specifies the upper limit on the number of fragments that can be created from a single IP packet.
timeout	(Optional) The timeout parameter defines the time window during which all fragments belonging to a particular IP packet are expected to arrive.
drop-fragments	(Optional) The drop-fragments parameter allows you to specify how the router should handle alone fragments that do not belong to any active reassembly process.

Command Default Disabled; all IP directed virtual fragmentation are dropped.

Command Modes Interface Configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Qualified for use in Cisco vManage CLI templates

Example

This example shows how to enable virtual reassemly:

```
Device# config-transaction
Device(config)#interface GigabitEthernet 3
Device(config-if)#ip virtual-reassembly max-reassemblies 3
Device(config-if)#ip virtual-reassembly max-reassemblies 3 max-fragments 60
```

ipv6 access-class

To create or configure an IPv6 access class to restrict incoming or outgoing traffic on a virtual terminal line (VTY), use the **ipv6 access-class** command. To remove the access class, use the **no** form of this command

ipv6 access-class *access-list-name*

no ipv6 access-class

Syntax Description

Syntax Description

access-list-name	Name of the IPv6 ACL class. The name can be a maximum of 64 characters. The name can contain characters, numbers, hyphens, and underscores. The name cannot contain a space or quotation mark.

Command Default

None

Command Modes

Line configuration mode (config-line)

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ipv6 access-class` command.

Examples

This example shows how to configure an access class on a VTY line:

```
Device(config)# line vty 0 4
Device(config-line)# ipv6 access-class TEST
```

ipv6 address

To configure an IPv6 address and enable IPv6 processing on an interface, use the **ipv6 address** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-address*
no ipv6 address *ipv6-address*

Syntax Description

ipv6-address	The IPv6 address to be used.

Command Default

No IPv6 addresses are defined for any interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see the Cisco IOS ipv6 address command.

Examples

```
Device(config)# interface GigabitEthernet 1.101
Device(config-if)# ipv6 address 2001:DB8::1
```

ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the **ipv6 address autoconfig** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 address autoconfig command.

Examples

The following example assigns the IPv6 address automatically:

```
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address autoconfig
```

ipv6 address dhcp client request

To configure an IPv6 client to request a vendor-specific option from a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp client request** command in interface configuration mode. To remove the request, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 address dhcp client request command.

Examples

The following example shows how to configure an interface to request vendor-specific options:

```
Device(config)# interface fastethernet 0/0
Device(config-if)# ipv6 address dhcp client request vendor
```

ipv6 cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm for IPv6, use the **ipv6 cef load-sharing algorithm** command in global configuration mode. To return to the default universal load-balancing algorithm, use the **no** form of this command.

ipv6 cef load-sharing algorithm { **universal** [*id*] | **include-ports** [**source** [*id*] | **destination** [*id*]] | **src-only** [*id*] }
no ipv6 cef load-sharing algorithm

universal*[id]*	Sets the load-balancing algorithm to the universal algorithm that uses a source and destination IP. (This is set as default).
id	(Optional) Fixed identifier.
include-ports {**source***[id]* | **destination***[id]*}	Sets the load-balancing algorithm to one that uses the source port and destination port.
src-only *[id]*	Sets the load-balancing algorithm to include source-only port.

Command Default

The universal load-balancing algorithm is selected. If you do not configure the fixed identifier for a load-balancing algorithm, the router automatically generates a unique ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was modified. The **src-only** algorithm is added.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 cef load-sharing algorithm command.

You can enable **ECMP keying** to send the configurations for both IPv4 and IPv6.

Examples

The following example shows how to enable the IPv6 CEF load-balancing algorithm for universal:

```
Device# config-transaction
Device (config-if)# ipv6 cef load-sharing algorithm universal
```

The following example shows how to enable the IPv6 CEF load-sharing algorithm for include-ports:

```
Device# config-transaction
Device(config)# ipv6 cef load-sharing algorithm include-ports source destination
```

The following example shows how to enable IPv6 CEF load-sharing algorithm to src-only port algorithm:

```
Device# config-transaction
Device(config)# ipv6 cef load-sharing algorithm src-only

Device(config)# commit
```

ipv6 dhcp client pd

To enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process and enable request for prefix delegation through a specified interface, use the **ipv6 dhcp client pd** command in interface configuration mode. To disable requests for prefix delegation, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 dhcp client pd command.

Examples

The following example enables prefix delegation:

```
Device(config-if)# ipv6 dhcp client pd dhcp-prefix
```

The following example configures a hint for prefix-delegating routers:

```
Device(config-if)# ipv6 dhcp client pd hint 2001:0DB8:1/48
```

ipv6 dhcp client vendor-class

By default the DHCP client carries PID (Product ID) of the device in option-16. This default behaviour can be overridden by configuring below CLI:

ipv6 dhcp client vendor-class [**mac-address** | **ascii** | **hex** | **disable**]

Syntax Description

mac-address	The mac address of the device.
ascii	The user defined string in ascii format.
hex	The user defined string in hexadecimal format.
disable	Disables sending option-16 to DHCP messages.

Command Default

By default option-16 carries PID of the device.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

By default the DHCP client carries PID of the device in option-16. This default behaviour can be overridden by configuring the **ipv6 dhcp client vendor-class** command.

Examples

The following example shows the configuration to override the decive PID with MAC address:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class mac-address
    !
```

The DHCPv6 vendor-class option, overrides the Device PID with MAC Address.

The following example shows the configuration to override the device PID with user defined string in hex or in ascii format:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class hex aabbcc
    !
```

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class ascii cisco
    !
```

The following example shows the configuration to disable option-16 in DHCP messages:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class disable
    !
```

ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 dhcp pool command.

Examples

The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode:

```
Device(config)# ipv6 dhcp pool cisco1
Device(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
Device(config-dhcpv6)# address prefix 2001:1000::0/64
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
Device(config)#ipv6 dhcp pool engineering
Device(config-dhcpv6)# link-address 2001:1001::0/64
Device(config-dhcpv6)# link-address 2001:1002::0/64
Device(config-dhcpv6)#
Device(config-dhcpv6)# address prefix 2001:1003::0/64
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Device(config)# ipv6 dhcp pool 350
Device(config-dhcpv6)# vendor-specific 9
Device(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Device(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
```

ipv6 dhcp relay destination

To specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol (DHCP) for IPv6 relay service on the interface, use the **ipv6 dhcp relay destination** command in interface configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 dhcp relay destination command.

Examples

The following example sets the relay destination address on Ethernet interface 4/3:

```
Device(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 4/3
```

The following example shows how to set the relay destination address on the Ethernet interface 4/3 on a Cisco CMTS router:

```
Device(config-if)# ipv6 dhcp relay destination 2001:db8:1234:5678:9abc:def1:2345:6789
ethernet 4/3
```

ipv6 dhcp-relay option vpn

To enable the DHCP for IPv6 relay VRF-aware feature, use the **ipv6 dhcp-relay option vpn** command in global configuration mode. To disable the feature, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 dhcp-relay option vpn command.

Examples

The following example enables the DHCPv6 relay VRF-aware feature globally on the router:

```
Device(config)# ipv6 dhcp-relay option vpn
```

ipv6 dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 service on an interface, use the **ipv6 dhcp server** in interface configuration mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 dhcp server command.

Examples

The following example enables DHCP for IPv6 for the local prefix pool named server1:

```
Device(config-if)# ipv6 dhcp server server1
```

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable**command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable
no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release Amsterdam 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **ipv6 enable**command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The no **ipv6 enable**command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

```
Device(config)# interface GigabitEthernet 1.101
Device(config-if)# ipv6 enable
```

ipv6 load-sharing algorithm

To enable load balancing algorithm on an interface for IPv6, use the **ipv6 load-sharing algorithm** command in Cisco Catalyst SD-WAN configuration mode. To disable load balancing algorithm on an interface, use the **no** form of this command.

ipv6 load-sharing algorithm { **ip-and-ports** | **src-dst-ip** | **src-ip-only** }
no ipv6 load-sharing algorithm { **ip-and-ports** | **src-dst-ip** | **src-ip-only** }

ip-and-ports	Sets the load-balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.
src-dst-ip	Sets the load-balancing algorithm to the src-dst-ip algorithm that uses a source and destination ip.
src-ip-only	Sets the load-balancing algorithm to the src-ip algorithm that uses source ip.

Command Default

src-dst-ip algorithm is enabled by default.

Command Modes

SD-WAN configuration (config-sdwan)

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

When the load-balancing algorithm is set to src-dst-ip mode, each router on the network can make a different load sharing decision for each source-destination address pair.

The ip-and-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not loadshared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams.

Examples

The following example shows how to enable load-balancing algorithm for source, destination ip and port:

```
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm ip-and-ports
```

The following example shows how to enable load balancing algorithm for source, destination ip:

```
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm src-dst-ip
```

The following example shows how to enable load balancing algorithm for source ip only:

```
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm src-ip-only
```

ipv6 nd other-config-flag

To set the "other stateful configuration" flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag** command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag
no ipv6 nd other-config-flag

Command Default

None

Command Modes

interface configuration (config-if)

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 setting of the "other stateful configuration" flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

Example

The following example configures the “other stateful configuration” flag in ipv6 router advertisements on GigabitEthernet 0/0/2.

```
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# ipv6 nd other-config-flag
```

Table 3: Related Commands

Command	Description
ipv6 nd managed-config-flag	Sets the “managed address configuration” flag in ipv6 router advertisements.

ipv6 nd prefix

To configure ipv6 prefixes that are included in IPv6 neighbor discovery router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix ipv6-prefix /prefix-length [**no-advertise**]
no ipv6 nd prefix ipv6-prefix /prefix-length [**no-advertise**]

Syntax Description

ipv6-prefix	Specifies the ipv6 network number to include the router advertisements (RA).
/ prefix-length	Specifies the length of the ipv6 prefix.

no-advertise	(Optional) specifies that the prefix is not advertised.

Command Default

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2,592,000 seconds (30 days) and a preferred lifetime of 604,800 seconds (7 days).

Command Modes

Interface configuration (config-if)

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 **ipv6 nd prefix** command allows control over individual parameters per prefix, including whether the prefix should be advertised or not.

Example

The following example includes the ipv6 prefix 2001:0DB8::/35 in router advertisements sent out GigabitEthernet 0/0/2.

```
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# ipv6 nd prefix 2001:0DB8::/35
```

ipv6 nd ra suppress

To suppress IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra suppress** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on an interface, use the **no** form of this command.

ipv6 nd ra suppress [**all**]
no ipv6 nd ra suppress [**all**]

Syntax Description

all	(optional) suppress all router advertisements (RAs) on an interface.

Command Default

IPv6 router advertisements are automatically sent on Ethernet and FDDI interfaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

Command Modes

Interface configuration (config-if)

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 **ipv6 nd ra suppress** command only suppresses periodic unsolicited RAs. It does not suppress RAs sent in response to a router solicitation. To suppress all RAs, including those sent in response to a router solicitation, use the **ipv6 nd ra suppress** command with the all keyword.

Example

The following example shows how to suppress IPv6 router advertisements on interface GigabitEthernet 0/0/2.

```
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# ipv6 nd ra suppress
```

Table 4: Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd router-preference

To configure a default router preference (DRP) for the router on a specific interface, use the **ipv6 nd router-preference** command in interface configuration mode. To return to the default DRP, use the **no** form of this command.

ipv6 nd router-preference { *high* | *medium* | *low* }
no ipv6 nd router-preference { *high* | *medium* | *low* }

Syntax Description

high	Preference for the router specified on an interface is high.
medium	Preference for the router specified on an interface is medium.
low	Preference for the router specified on an interface is low.

Command Default

Router Advertisements (RAs) are sent with the medium preference.

Command Modes

Interface configuration (config-if)

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

Router Advertisement messages are sent with the DRP configured by the **ipv6 nd router-preference** command. If no DRP is configured, Router Advertisements are sent with a medium preference. A DRP is useful when, for example, two routers on a link may provide equivalent, but not equal-cost, routing, and policy may dictate that hosts should prefer one of the routers.

Example

The following example configures a DRP of high for the router on GigabitEthernet 0/0/2.

```
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# ipv6 nd router-preference High
```

ipv6 redirects

To enable the sending of Internet Control Message Protocol (ICMP) IPv6 redirect messages if Cisco IOS software is forced to resend a packet through the same interface on which the packet was received, use the **ipv6 redirects** command in interface configuration mode. To disable the sending of redirect messages, use the **no** form of this command.

ipv6 redirects
no ipv6 redirects

Syntax Description This command has no arguments or keywords.

Command Default The sending of ICMP IPv6 redirect messages is enabled.

Command Modes Interface configuration (config-if)

Command History

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

Usage Guidelines

Examples The following example disables the sending of ICMP IPv6 redirect messages on Tunnel interface 1:

```
Device(config)# interface Tunnel 1
Device(config-if)# ipv6 unnumbered GigabitEthernet0/2.101
Device(config-if)# no ipv6 redirects
```

Related Commands

Command	Description
ipv6 icmp error-interval	Configures the interval for IPv6 ICMP error messages.

ipv6 route

To establish static IPv6 routes, use the **ipv6 route**command in global configuration mode. To remove a previously configured static route, use the **no** form of this command.

ipv6 route vrf *vrf-name ipv6-prefix/prefix-length*
no ipv6 route vrf *vrf-name ipv6-prefix/prefix-length*

Syntax Description

ipv6-prefix	The IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.

/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
vrf *vrf-name*	Specifies all virtual private network (VPN) routing/forwarding instance (VRF) tables or a specific VRF table for an IPv6 address.

Command Default

No static routes are established.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ipv6 route` command.

Examples

The following example configures a static route for use in a VRF for IPv6:

```
ipv6 route vrf TEST 2001:DB8::/32
```

ipv6-strict-control

To configure IPv6 as a default option on Cisco IOS XE Catalyst SD-WAN devices, Cisco SD-WAN Manager, and Cisco Catalyst SD-WAN Controller, use the **ipv6-strict-control** command in system configuration mode. To remove the option from the interface, use the **no** form of this command.

ipv6-strict-control { *true* | *false* }
no ipv6-strict-control

Syntax Description

true	Enables IPv6 as the default connection option for connecting to Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco IOS XE Catalyst SD-WAN devices.

Command Default

An IPv4 connection is defined for an interface.

Command Modes

System configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure IPv6 as a default connection option on a Cisco IOS XE Catalyst SD-WAN device to connect to Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller:

```
Device(config)# system
Device(config-system)# gps-location latitude 32.0
Device(config-system)# gps-location longitude -100.0
Device(config-system)# system-ip 10.16.255.14
Device(config-system)# domain-id 1
Device(config-system)# site-id 400
Device(config-system)# ipv6-strict-control true
Device(config-system)# admin-tech-on-failure
Device(config-system)# organization-name "Cisco"
Device(config-system)# vbond vbond
```

ipv6 unnumbered

To enable IPv6 processing on an interface without assigning an explicit IPv6 address to the interface, use the **ipv6 unnumbered**command in interface configuration mode. To disable IPv6 on an unnumbered interface, use the **no** form of this command.

ipv6 unnumbered *interface-type* **interface-number**
no ipv6 unnumbered

Syntax Description

interface-type	The interface type of the source address that the unnumbered interface uses in the IPv6 packets that it originates. The source address cannot be another unnumbered interface.
interface-number	The interface number of the source address that the unnumbered interface uses in the IPv6 packets that it originates.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

IPv6 packets that are originated from an unnumbered interface use the global IPv6 address of the interface specified in the **ipv6 unnumbered** command as the source address for the packets. The **ipv6 unnumbered**

interface command is used as a hint when doing source address selection; that is, when trying to determine the source address of an outgoing packet.

Examples

```
Device(config)# interface Tunnel 1
Device(config-if)# ipv6 unnumbered GigabitEthernet0/2.101
```

lease

To configure the duration of the lease for an IP address that is assigned from a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to a DHCP client, use the **lease** command in DHCP pool configuration mode. To restore the default value, use the no form of this command.

lease *days* [*hours* [*minutes*]]
no lease

Syntax Description

days	Specifies the duration of the lease in numbers of days.
hours	(Optional) Specifies the number of hours in the lease. A *days* value must be supplied before you can configure an *hours* value.
minutes	(Optional) Specifies the number of minutes in the lease. A *days* value and an *hours* value must be supplied before you can configure a *minutes* value.
infinite	Specifies that the duration of the lease is unlimited.

Command Default

1 day

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Examples

The following example shows a 365 day lease:

```
Device (config)# ip dhcp pool POOL1
Device(dhcp-config)# lease 365 0 0
```

network (DHCP)

To configure the network number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool primary subnet on a DHCP server, use the **network** command in DHCP pool configuration mode. To remove the subnet number and mask, use the **no** form of this command.

network *network-number* [*mask*]

Syntax Description

network-number	The IP address of the primary DHCP address pool.
mask	(Optional) The bit combination that renders which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host.

Command Default

This command is disabled by default.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `network (DHCP)` command.

Examples

The following example shows how to configure 255.255.255. 0 as the subnetwork number and mask of the DHCP pool named pool1.

```
Device(config)# ip dhcp pool pool1
Device(dhcp-config)# network 172.16.0.0 255.255.255.0
```

option (DHCP)

To configure DHCP server options, use the **option** command in DHCP pool configuration mode. To remove the options, use the **no** form of this command.

option *code* [**ip** *list-name*]
no option *code*

Syntax Description

code	Specifies the DHCP option code. The range is from 0 to 254.
ip *address*	Specifies an IP address. Up to eight IP addresses can be specified.
string	Hexadecimal value truncated to 180 characters entered. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period, colon, or white space.

Command Default

The default instance number is 0.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Examples

The following example shows how to configure DHCP option 150 for an IP list containing two IP addresses.

```
Device(config)# ip dhcp pool POOL1
Device(dhcp-config)# option 150 ip 10.10.10.1 10.10.10.2
```

prefix-delegation

To specify a manually configured numeric prefix to be delegated to a specified client (and optionally a specified identity association for prefix delegation [IAPD] for that client), use the **prefix-delegation** command in DHCP for IPv6 pool configuration mode. To remove the prefix, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE prefix-delegation command.

Examples

The following example configures an IAPD for a specified client:

```
Device(config)# prefix-delegation 2001:0DB8::/64 00030001000BBFAA2408
```

prefix-delegation pool

To specify a named IPv6 local prefix pool from which prefixes are delegated to Dynamic Host Configuration Protocol (DHCP) for IPv6 clients, use the **prefix-delegation pool** command in DHCP for IPv6 pool configuration mode. To remove a named IPv6 local prefix pool, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE prefix-delegation pool command.

Examples

The following example specifies that prefix requests should be satisfied from the pool called client-prefix-pool. The prefixes should be delegated with the valid lifetime set to 1800 seconds, and the preferred lifetime is set to 600 seconds:

```
Device(config)# prefix-delegation pool client-prefix-pool lifetime 1800 600
```

spt-only

To configure multicast routing in Cisco SD-WAN to use shortest-path first trees (SPT) only, use the **spt-only** command in VRF configuration mode. To disable SPT-only use the **no** form of this command.

spt-only

no spt-only

This command has no keywords or arguments.

Command Default

SPT-only is not configured.

Command Modes

VRF configuration (config-vrf-<vrf-id>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Enable spt-only on all Cisco IOS XE SD-WAN devices that have Cisco SD-WAN multicast overlay configured for the VRF.

Example

```
Device(config)# sdwan multicast address-family ipv4 vrf 1
Device(config-vrf-1)# spt-only
```

vlan internal allocation policy

To configure the allocation direction of the internal VLAN, use the **vlaninternalallocationpolicy** command in global configuration mode. To return the default setting, use the **no** form of this command to return.

vlan internal allocation policy ascending
no vlan internal allocation policy

Syntax Description

ascending	Allocates internal VLANs from 1006 to 4094.

Command Default

ascending

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 vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE vlan internal allocation policy command.

Examples

```
Device(config)# vlan internal allocation policy ascending
```

vendor-specific

To configures vendor-defined options for the IPv6 address pool, use the **vendor-specific** command in global configuration mode. To disable the feature, use the **no** form of this command.

vendor-specific *vendor-id*

Syntax Description

vendor-id	Specify an ID for the vendor.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example configures vendor-defined options for the IPv6 address pool:

```
Device(config)# vendor-specific 10
```

vrf (DHCP pool)

To associate the on-demand address pool with a VPN routing and forwarding instance (VRF) name, use the **vrf** command in DHCP pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*
no vrf *name*

Syntax Description

name	Name of the VRF to which the address pool is associated.

Command Default

No default behavior or values

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `vrf (DHCP Pool)` command.

Examples

The following example associates the address pool with a VRF named TEST:

```
Device(config)# ip dhcp pool POOL1
Device(dhcp-config)# vrf TEST
```