



# I Commands

---

This chapter describes the Cisco NX-OS Layer 3 interfaces commands that begin with I.

# ip address

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

**ip address** *ip-address mask* [**secondary**]

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

Syntax Description		
<i>ip-address</i>		IPv4 address in the format <i>A.B.C.D</i> or <i>A.B.C.D/length</i> .
<i>mask</i>		Mask for the associated IP subnet.
<b>secondary</b>		(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

**Command Default** No IP address is defined for the interface.

**Command Modes** Interface configuration mode  
Subinterface configuration mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

## Usage Guidelines



**Note** Before you use this command, make sure that you use the **no switchport** command on the interface to use the Layer 3 features.

An interface can have one primary IP address and one secondary IP address.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command.

The optional **secondary** keyword allows you to specify a secondary IP address. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts, Address Resolution Protocol (ARP) requests, and interface routes are handled in the IP routing table.



**Note** When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that the secondary address of an interface falls into the same OSPF area as the primary addresses.

**Examples** This example shows how to configure the IP address 192.168.0.27 as the primary address and 192.168.0.5 as the secondary address for Ethernet interface 1/5:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 192.168.0.27 255.255.255.0
switch(config-if )# ip address 192.168.0.5 255.255.255.0 secondary
switch(config-if)#
```

Related Commands	Command	Description
	<b>copy running-config startup-config</b>	Saves the configuration change to the startup configuration file.
	<b>no switchport</b>	Enables an interface for Layer 3 configuration.
	<b>show ip interface</b>	Displays interfaces configured for IPv4.

# ip arp

To configure a static Address Resolution Protocol (ARP) entry, use the **ip arp** command. To remove a static ARP entry, use the **no** form of this command.

**ip arp** *ip-address mac-address*

**no ip arp** *ip-address*

Syntax Description	<i>ip-address</i>	IPv4 address, in <i>A.B.C.D</i> format.
	<i>mac-address</i>	MAC address in one of the following formats: <ul style="list-style-type: none"> <li>• E.E.E</li> <li>• EE-EE-EE-EE-EE-EE</li> <li>• EE:EE:EE:EE:EE:EE</li> <li>• EEEE.EEEE.EEEE</li> </ul>

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

**Usage Guidelines** Use this command on Layer 3 interfaces and Layer 3 subinterfaces.

**Examples** This example shows how to configure a static ARP entry on interface Ethernet 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip arp 192.0.2.1 0150.5a03.efab
switch(config-if)#
```

This example shows how to configure a static ARP entry on a subinterface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# interface ethernet 1/1.1
switch(config-subif)# ip arp 192.0.2.1 0150.5a03.efab
switch(config-subif)#
```

Related Commands	Command	Description
	show ip arp	Displays ARP entries.

# ip arp gratuitous

To enable gratuitous Address Resolution Protocol (ARP), use the **ip arp gratuitous** command. To disable gratuitous ARP, use the **no** form of this command.

**ip arp gratuitous {request | update}**

**no ip arp gratuitous {request | update}**

Syntax Description	request	update
	Enables sending gratuitous ARP requests when a duplicate address is detected.	Enables ARP cache updates for gratuitous ARP.

**Command Default** Enabled

**Command Modes** Interface configuration mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

**Examples** This example shows how to disable a gratuitous ARP request on interface Ethernet 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip arp gratuitous
switch(config-if)#
```

Related Commands	Command	Description
	<b>ip arp</b>	Configures a static ARP entry.
	<b>show ip arp</b>	Displays ARP configuration information.

# ip arp timeout

To configure an Address Resolution Protocol (ARP) timeout, use the **ip arp timeout** command. To revert to the default value, use the **no** form of this command.

**ip arp timeout** *timeout-value*

**no ip arp timeout**

<b>Syntax Description</b>	<i>timeout-value</i>	Time (in seconds) that an entry remains in the ARP cache. Valid values are from 60 to 28800, and the default is 1500.				
<b>Command Default</b>	1500 seconds					
<b>Command Modes</b>	Global configuration mode					
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>6.0(2)N1(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	6.0(2)N1(1)	This command was introduced.	
Release	Modification					
6.0(2)N1(1)	This command was introduced.					
<b>Examples</b>	<p>This example shows how to configure the ARP timeout value to 120 seconds:</p> <pre>switch(config)# ip arp timeout 120 switch(config)#</pre> <p>This example shows how to revert to the default ARP timeout value of 1500 seconds:</p> <pre>switch(config)# no ip arp timeout switch(config)#</pre>					
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show running-config</b> <b>arp all</b></td> <td>Displays the ARP configuration, including the default configurations.</td> </tr> </tbody> </table>	Command	Description	<b>show running-config</b> <b>arp all</b>	Displays the ARP configuration, including the default configurations.	
Command	Description					
<b>show running-config</b> <b>arp all</b>	Displays the ARP configuration, including the default configurations.					

# ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** 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 mode  
Subinterface configuration mode

---

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

---



---

**Usage Guidelines** An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.

A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

If a directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts that are intended for the subnet to which that interface is attached are broadcast on that subnet.

If the **no ip directed-broadcast** command has been configured for an interface, directed broadcasts that are destined for the subnet to which that interface is attached are dropped, rather than being broadcast.



**Note**

Because directed broadcasts, and particularly ICMP-directed broadcasts, have been abused by malicious persons, we recommend that you disable the **ip directed-broadcast** command on any interface where directed broadcasts are not needed. We also recommend that you use access lists to limit the number of broadcast packets.

---



---

**Examples** This example shows how to enable forwarding of IP directed broadcasts on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
```

```
switch(config-if)# ip directed-broadcast
switch(config-if)#
```

Related Commands	Command	Description
	<b>show ip interface</b>	Displays IP information for an interface.

## interface ethernet (Layer 3)

To configure a Layer 3 Ethernet IEEE 802.3 routed interface, use the **interface ethernet** command.

```
interface ethernet [chassis_ID] slot/port[.subintf-port-no]
```

Syntax Description	
<i>chassis_ID</i>	(Optional) Fabric Extender chassis ID. The chassis ID is from 100 to 199. <b>Note</b> This argument is not optional when addressing the host interfaces of a Cisco Nexus 2000 Series Fabric Extender.
<i>slot</i>	Slot from 1 to 3. The following list defines the slots available: <ul style="list-style-type: none"> <li>Slot 1 includes all the fixed ports. A Fabric Extender only has one slot.</li> <li>Slot 2 includes the ports on the upper expansion module (if populated).</li> <li>Slot 3 includes the ports on the lower expansion module (if populated).</li> </ul>
<i>port</i>	Port number within a particular slot. The port number is from 1 to 128.
.	(Optional) Subinterface separator.
<i>subintf-port-no</i>	(Optional) Port number for the subinterface. The range is from 1 to 48.

**Command Default** None

**Command Modes** Global configuration mode  
Interface configuration mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

**Usage Guidelines** You must use the **no switchport** command in the interface configuration mode to configure the interface as a Layer 3 routed interface. When you configure the interface as a Layer 3 interface, all Layer 2-specific configurations on this interface are deleted.

Use the **switchport** command to convert a Layer 3 interface into a Layer 2 interface. When you configure the interface as a Layer 2 interface, all Layer 3-specific configurations on this interface are deleted.

### Examples

This example shows how to enter interface configuration mode for a Layer 3 Ethernet interface 1/5:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

This example shows how to enter interface configuration mode for a host interface on a Fabric Extender:

```
switch(config)# interface ethernet 101/1/1
switch(config-if)# no switchport
```

```
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

This example shows how to configure a Layer 3 subinterface for Ethernet interface 1/5 in the global configuration mode:

```
switch(config)# interface ethernet 1/5.2
switch(config-if)# no switchport
switch(config-subif)# ip address 10.1.1.1/24
switch(config-subif)#
```

This example shows how to configure a Layer 3 subinterface in interface configuration mode:

```
switch(config)# interface ethernet 1/5
switch(config-if)# interface ethernet 1/5.1
switch(config-if)# no switchport
switch(config-subif)# ip address 10.1.1.1/24
switch(config-subif)#
```

This example shows how to convert a Layer 3 interface to a Layer 2 interface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)# switchport
switch(config-if)#
```

#### Related Commands

Command	Description
<b>bandwidth</b>	Sets the bandwidth parameters for an interface.
<b>delay</b>	Configures the interface throughput delay value.
<b>encapsulation</b>	Sets the encapsulation type for an interface.
<b>inherit</b>	Assigns a port profile to an interface.
<b>interface vethernet</b>	Configures a virtual Ethernet interface.
<b>ip address</b>	Sets a primary or secondary IP address for an interface.
<b>no switchport</b>	Configures an interface as a Layer 3 interface.
<b>service-policy</b>	Configures a service policy for an interface.
<b>show fex</b>	Displays all configured Fabric Extender chassis connected to the switch.
<b>show interface ethernet</b>	Displays various parameters of an Ethernet IEEE 802.3 interface.

# ip local-proxy-arp

To enable the local proxy Address Resolution Protocol (ARP) feature, use the **ip local-proxy-arp** command. To disable this feature, use the **no** form of this command.

**ip local-proxy-arp**

**no ip local-proxy-arp**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Disabled

**Command Modes** Interface configuration mode  
Subinterface configuration mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

**Usage Guidelines** Before the local proxy ARP feature can be used, you must enable the IP proxy ARP feature by using the **ip proxy-arp** command. The IP proxy ARP feature is disabled by default.



**Note**

This command is not applicable to Layer 3 loopback interfaces.

**Examples** This example shows how to enable the local proxy ARP:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip arp local-proxy-arp
switch(config-if)#
```

Related Commands	Command	Description
	<b>copy running-config startup-config</b>	Saves the configuration to the startup configuration file.
	<b>ip proxy-arp</b>	Enables proxy ARP on an interface.
	<b>show ip arp</b>	Displays ARP configuration information.

# interface loopback

To create a loopback interface and enter interface configuration mode, use the **interface loopback** command. To remove a loopback interface, use the **no** form of this command.

**interface loopback** *number*

**no interface loopback** *number*

<b>Syntax Description</b>	<i>number</i>	Interface number; valid values are from 0 to 1023.
---------------------------	---------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Global configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.0(2)N1(1)	This command was introduced.

<b>Usage Guidelines</b>	<p>Use the <b>interface loopback</b> command to create or modify loopback interfaces.</p> <p>From the loopback interface configuration mode, the following parameters are available:</p> <ul style="list-style-type: none"> <li>• <b>description</b>—Provides a description of the purpose of the interface.</li> <li>• <b>ip</b>—Configures IP features, such as the IP address for the interface, Address Resolution Protocol (ARP) attributes, load balancing, Unicast Reverse Path Forwarding (RPF), or IP Source Guard.</li> <li>• <b>logging</b>—Configures logging of events.</li> <li>• <b>shutdown</b>—Shuts down traffic on the interface.</li> </ul>
-------------------------	---

This command does not require a license.

<b>Examples</b>	This example shows how to create a loopback interface:
-----------------	--

```
switch(config)# interface loopback 50
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show interface loopback</b>	Displays information about the traffic on the specified loopback interface.

# interface port-channel

To create an EtherChannel interface and enter interface configuration mode, use the **interface port-channel** command. To remove an EtherChannel interface, use the **no** form of this command.

```
interface port-channel channel-number[.subintf-channel-no]
```

```
no interface port-channel channel-number[.subintf-channel-no]
```

Syntax Description		
<i>channel-number</i>	Channel number that is assigned to this EtherChannel logical interface. The range is from 1 to 4096.	
.	(Optional) Subinterface separator.	
	<b>Note</b> Applies to Layer 3 interfaces.	
<i>subintf-channel-no</i>	(Optional) Port number of the EtherChannel subinterface. The range is from 1 to 4093.	
	<b>Note</b> Applies to Layer 3 interfaces.	

**Command Default** None

**Command Modes** Global configuration mode  
Interface configuration mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

**Usage Guidelines** A port can belong to only one channel group.

When you use the **interface port-channel** command for Layer 2 interfaces, follow these guidelines:

- If you are using Cisco Discovery Protocol (CDP), you must configure it only on the physical interface and not on the EtherChannel interface.
- If you do not assign a static MAC address on the EtherChannel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.
- The MAC address of the EtherChannel is the address of the first operational port added to the channel group. If this first-added port is removed from the channel, the MAC address comes from the next operational port added, if there is one.

You must use the **no switchport** command in interface configuration mode to configure the EtherChannel interface as a Layer 3 interface. When you configure the interface as a Layer 3 interface, all Layer 2-specific configurations on this interface are deleted.

Use the **switchport** command to convert a Layer 3 EtherChannel interface into a Layer 2 interface. When you configure the interface as a Layer 2 interface, all Layer 3-specific configurations on this interface are deleted.

You can configure one or more subinterfaces on a port channel made from routed interfaces.

### Examples

This example shows how to create an EtherChannel group interface with channel-group number 50:

```
switch(config)# interface port-channel 50
switch(config-if)#
```

This example shows how to create a Layer 3 EtherChannel group interface with channel-group number 10:

```
switch(config)# interface port-channel 10
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.1/24
switch(config-if)#
```

This example shows how to configure a Layer 3 EtherChannel subinterface with channel-group number 1 in interface configuration mode:

```
switch(config)# interface port-channel 10
switch(config-if)# no switchport
switch(config-if)# interface port-channel 10.1
switch(config-subif)# ip address 192.0.2.2/24
switch(config-subif)#
```

This example shows how to configure a Layer 3 EtherChannel subinterface with channel-group number 20.1 in global configuration mode:

```
switch(config)# interface port-channel 20.1
switch(config-subif)# ip address 192.0.2.3/24
switch(config-subif)#
```

### Related Commands

Command	Description
<b>encapsulation</b>	(Layer 3 interfaces) Sets the encapsulation type for an interface.
<b>ip address</b>	(Layer 3 interfaces) Sets a primary or secondary IP address for an interface.
<b>no switchport</b>	(Layer 3 interfaces) Configures an interface as a Layer 3 interface.
<b>show interface</b>	Displays configuration information about interfaces.
<b>show lacp</b>	Displays LACP information.
<b>show port-channel summary</b>	Displays information about the EtherChannels.
<b>vtp (interface)</b>	Enables VLAN Trunking Protocol (VTP) on an interface.

# ip port-unreachable

To enable the generation of ICMP port unreachable messages, use the **ip port-unreachable** command. To disable this function, use the **no** form of this command.

**ip port-unreachable**

**no ip port-unreachable**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** Enabled

---

**Command Modes** Interface configuration mode  
Subinterface configuration mode

---

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

---



---

**Examples** This example shows how to enable the generation of ICMP port unreachable messages, as appropriate, on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip port-unreachable
```

---

Related Commands	Command	Description
	<b>ip unreachable</b>	Sends ICMP unreachable messages.

---

# ip proxy-arp

To enable proxy Address Resolution Protocol (ARP) on an interface, use the **ip proxy-arp** command. To disable proxy ARP on the interface, use the **no** form of this command.

**ip proxy-arp**

**no ip proxy-arp**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Disabled

**Command Modes** Interface configuration mode  
Subinterface configuration mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

**Examples** This example shows how to enable proxy ARP:

```
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip proxy-arp
switch(config-if)#
```

Related Commands	Command	Description
	<b>copy running-config startup-config</b>	Saves the configuration to the startup configuration file.
	<b>show ip arp</b>	Displays ARP configuration information.

## ip tcp path-mtu-discovery

To enable path maximum transmission unit (MTU) discovery on an IPv4 interface, use the **ip tcp path-mtu discovery** command. To disable this feature, use the **no** form of this command.

**ip tcp path-mtu discovery**

**no ip tcp path-mtu discovery**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** Disabled

---

**Command Modes** Interface configuration mode

---

Release	Modification
6.0(2)N1(1)	This command was introduced.

---



---

**Examples** This example shows how to enable path MTU discovery for IPv4:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip tcp path-mtu-discovery
switch(config-if)#
```

---

Command	Description
<b>show ip arp</b>	Displays ARP configuration information.

---

## ip tcp synwait-time

To set a period of time that the Cisco NX-OS software waits while attempting to establish a TCP connection before it times out, use the **ip tcp synwait-time** command. To restore the default time, use the **no** form of this command.

**ip tcp synwait-time** *seconds*

**no ip tcp synwait-time**

<b>Syntax Description</b>	<i>seconds</i>	Time, in seconds, that the software waits while attempting to establish a TCP connection. It can be an integer from 5 to 300 seconds.
---------------------------	----------------	---

<b>Command Default</b>	5 seconds
------------------------	-----------

<b>Command Modes</b>	Global configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.0(2)N1(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to configure the switch software to continue attempting to establish a TCP connection for 10 seconds:

```
switch# configure terminal
switch(config)# ip tcp synwait-time 10
Setting syn time to 10 seconds
switch(config)#
```

This example shows how to disable TCP synchronization on interfaces:

```
switch# configure terminal
switch(config)# no ip tcp synwait-time
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>show running-config</b>

# ip unreachable

To enable the generation of ICMP unreachable messages, use the **ip unreachable** command. To disable this function, use the **no** form of this command.

**ip unreachable**

**no ip unreachable**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** Enabled

---

**Command Modes** Interface configuration mode  
Subinterface configuration mode

---

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

---



---

**Examples** This example shows how to enable the generation of ICMP unreachable messages on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip unreachable
```

---

Related Commands	Command	Description
	<b>ip port-unreachable</b>	Sends ICMP port unreachable messages.

---

# ip wccp

To enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **ip wccp** command. To disable the service group, enter the **no** form of this command.

```
ip wccp {service-number | web-cache} [service-list service-access-list] [mode {open | closed}]
[redirect-list access-list] [password [0-7] password]
```

```
no ip wccp {service-number | web-cache} [service-list service-access-list] [mode {open | closed}]
[redirect-list access-list] [password [0-7] password]
```

Syntax Description		
<i>service-number</i>		Dynamic service identifier. The service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256.
<b>web-cache</b>		Specifies the web-cache well-known service.
<b>service-list</b> <i>service-access-list</i>		(Optional) Identifies a named extended IP access list that defines the packets that matches the service. This keyword is required only when the service is defined as closed mode.
<b>mode</b>		(Optional) <a href="#">Need description.</a>
<b>open</b>		(Optional) Identifies the service as open. This is the default service mode.
<b>closed</b>		(Optional) Identifies the service as closed.
<b>redirect-list</b> <i>access-list</i>		(Optional) Specifies the access list that controls traffic redirected to this service group. The <i>access-list</i> argument should consist of a string with a maximum of 64 characters (name or number) that specifies the access list.
<b>password</b> [0-7] <i>password</i>		(Optional) Specifies the message digest algorithm 5 (MD5) authentication for messages that are received from the service group. Messages that are not accepted by the authentication are discarded. The encryption type can be any value between 0 and 7 (inclusive). 0 specifies that the password is not yet encrypted. 7 specifies that the password is proprietary. The <i>password</i> argument can be up to eight characters in length.

**Command Default** WCCP services are not enabled on the router.

**Command Modes** Global configuration mode

Command History	Release	Modification
	7.0(0)N1(1)	This command was introduced.

**Usage Guidelines** The optional **redirect-list** *access-list* keyword and option instruct the router to use an access list to control the traffic that is redirected to the cache engines of the service group by the service name that you specify. The *access-list* argument specifies either a number from 1 to 99 to represent a standard or

extended access-list number or a name to represent a named standard or extended access list. The access list itself specifies the traffic that is permitted to be redirected. The default is for no **redirect-list** to be configured (all traffic is redirected).

The **service-list** keyword can only be used for closed mode services. When a WCCP service is configured as closed, WCCP discards packets that do not have a client application registered to receive the traffic. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

The password can be up to seven characters. When user designates a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

### Examples

This example shows how to configure a router to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

Prompts need to be added.

```
switch(config)# access-list 100 deny ip any host 10.168.196.51
access-list 100 permit ip any any
ip wccp web-cache redirect-list 100
interface ethernet 1/1
ip wccp web-cache redirect in
```

The following example shows how to configure a closed WCCP service:

```
ip wccp 99 service-list access1 mode closed
```

### Related Commands

Command	Description
<b>show ip wccp</b>	Specifies packet redirection on an inbound interface.

# ip wccp redirect

To enable packet redirection on an outbound or inbound interface using the Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command. To disable WCCP redirection, use the **no** form of this command.

```
ip wccp {service-number | web-cache} redirect {in}
```

```
no ip wccp {service-number | web-cache} redirect {in}
```

Syntax Description		
	<i>service-number</i>	Dynamic service identifier. The service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256.
	<b>web-cache</b>	Specifies the web-cache well-known service.
	<b>in</b>	Specifies packet redirection on an inbound interface.

**Command Default** Redirection checking on the interface is disabled.

**Command Modes** Interface configuration mode

Command History	Release	Modification
	7.0(0)N1(1)	This command was introduced.

**Usage Guidelines** Configure WCCP in the incoming direction on the inside interface by entering the **ip wccp redirect in** command on the router interface that faces the cache.

You can also include a redirect list when you configure a service group. The specified redirect list denies packets and prevents redirection. See the **ip wccp** command for configuration of the redirect list and service group.

The **ip wccp redirect in** command allows you to configure WCCP redirection on an interface that receives the inbound network traffic. When you apply this command to an interface, all packets that arrive at the interfaces are compared against the criteria that is defined by the specified service. If the packets match the criteria, they are redirected.

**Examples** This example shows how to configure a session in which HTTP traffic that arrives on Ethernet interface 0/1 is redirected to a Cisco cache engine:

```
switch(config)# ip wccp web-cache
switch(config)# interface ethernet 1/1
switch(config-if)# ip wccp web-cache redirect in
```

Related Commands	Command	Description
	<b>show ip interface</b>	Displays the usability status of the interfaces that are configured for IP.
	<b>show ip wccp</b>	Displays the WCCP statistics.

# ipv6 nd

To configure IPv6 neighbor discovery (ND), use the **ipv6 nd** command. To remove the IPv6 ND configuration, use the **no** form of this command.

```
ipv6 nd { hop-limit hop-limit | managed-config-flag | mtu | ns-interval ns-interval |
other-config-flag | prefix { A:B::C:D/LEN | default { 0-4294967295 | infinite { infinite
[no-autoconfig | no-onlink | off-link]} | no-advertise } } | ra-interval ra-interval | ra-lifetime
ra-lifetime | reachable-time reachable-time | redirects | retrans-timer retrans-timer |
suppress-ra [mtu] }
```

```
no ipv6 nd { hop-limit hop-limit | managed-config-flag | mtu mtu-size | ns-interval ns-interval |
other-config-flag | prefix { A:B::C:D/LEN | default { 0-4294967295 | infinite { infinite
[no-autoconfig | no-onlink | off-link]} | no-advertise } } | ra-interval ra-interval | ra-lifetime
ra-lifetime | reachable-time reachable-time | redirects | retrans-timer retrans-timer |
suppress-ra [mtu] }
```

## Syntax Description

<b>hop-limit</b>	Specifies the hop limit in the IPv6 header.
<i>hop-limit</i>	Hop limit. The range is from 0 to 255.
<b>managed-config-flag</b>	Informs hosts to use stateful address autoconfiguration to obtain address information.
<b>mtu</b>	Specifies the maximum transmission unit (MTU) size.
<i>mtu-size</i>	MTU size. The range is from 1280 to 65535.
<b>ns-interval</b>	Specifies the retransmission interval between sending the neighbor-solicitation messages.
<i>ns-interval</i>	Interval in milliseconds. The range is from 1000 to 3600000.
<b>other-config-flag</b>	Informs hosts to use stateful autoconfiguration to obtain nonaddress-related information.
<b>prefix</b>	Specifies the IPv6 prefix to advertise in the router-advertisement message.
<b>A:B::C:D/LEN</b>	Specifies the IPv6 address prefix.
<b>default</b>	Specifies the prefix default parameters.
<b>0-4294967295</b>	Specifies the valid value for the lifetime.
<b>infinite</b>	Specifies the indefinite lifetime.
<b>no-autoconfig</b>	(Optional) Specifies not to use the prefix for autoconfiguration.
<b>no-onlink</b>	(Optional) Specifies not to use the prefix for the onlink determination.
<b>off-link</b>	Indicates that the prefix is offlink.
<b>no-advertise</b>	Specifies not to advertise the prefix.
<b>ra-interval</b>	Specifies the interval between sending the router-advertisement message.
<i>ra-interval</i>	Router-advertisement message interval. The range is from 4 to 1800.
<b>ra-lifetime</b>	Specifies the router lifetime of a default router.
<i>ra-lifetime</i>	Router-advertisement message lifetime. The range is from 4 to 1800. The value for the default router cannot be 0.
<b>reachable-time</b>	Specifies the advertised time when a node considers a neighbor is up after receiving a reachability confirmation.
<i>reachable-time</i>	Reachable time. The range is from 0 to 3600000.

<b>redirects</b>	Enables sending ICMPv6 redirect messages.
<b>retrans-timer</b>	Specifies the advertised time between NS messages.
<b>retrans-timer</b>	Time between messages. The range is from 0 to 4294967295.
<b>suppress-ra</b>	Disables sending router-advertisement messages.

**Defaults**

hop-limit-64  
 mtu-1500  
 ns-interval-1000  
 ra-interval-600  
 reachable-time-0  
 retrans-timer-0

**Command Modes**

Interface configuration mode

**Command History**

Release	Modification
6.0(2)N1(1)	This command was introduced.

**Usage Guidelines**

This command does not require a license.

**Examples**

This example shows how to configure IPv6 neighbor discovery:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ipv6 nd
switch(config-if)# ipv6 nd reachable time 30
```

This example shows how to remove IPv6 neighbor discovery:

```
switch(config-if)# no ipv6 nd reachable time 30
switch(config-if)#
```

**Related Commands**

Command	Description
<b>show ipv6 nd interface</b>	Displays neighbor discovery interface information.