



IP Addressing Configuration Guide, Cisco IOS XE 17 (Cisco NCS 520 Series)

First Published: 2020-03-31

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1

Feature History 1

CHAPTER 2

DHCP Features Configuration 3

Limitations and Restrictions on the Cisco NCS 520 Router 3

DHCP Features 3

DHCP Server 4

DHCP Relay Agent 4

DHCP Snooping 4

Option-82 Data Insertion 5

Cisco IOS DHCP Server Database 8

DHCP Snooping Binding Database 8

Configuring DHCP Features 10

Default DHCP Configuration 10

DHCP Snooping Configuration Guidelines 11

Configuring the DHCP Server 12

Configuring the DHCP Relay Agent 12

Specifying the Packet Forwarding Address 13

Enabling DHCP Snooping and Option 82 14

Enabling the Cisco IOS DHCP Server Database 15

Enabling the DHCP Snooping Binding Database Agent 15

Stopping the Database Agent and Binding files 16

Clearing the Statistics of the DHCP Snooping Binding Database Agent 16

Deleting Binding Entries from the DHCP Snooping Binding Database 17

Disabling DHCP Snooping 17

Displaying DHCP Snooping Information 17

Pre-assigned Address Reserved in the DHCP Pool 17

Automatic Generation of Subscriber Identifier	18
DHCP Server Port-Based Address Allocation	18
Configuring DHCP Server Port-Based Address Allocation	19
Default Port-Based Address Allocation Configuration	19
Port-Based Address Allocation Configuration Guidelines	19
Enabling DHCP Server Port-Based Address Allocation	19
Pre-assigning IP Addresses	20
Removing an IP Address Reservation from a DHCP Pool	21
Automatic Generation of Subscriber Identifier	21
Disabling DHCP Port-Based Address Allocation	21
Displaying DHCP Server Port-Based Address Allocation	21

CHAPTER 3**Configuration of Dynamic ARP Inspection 23**

Dynamic ARP Inspection	23
Interface Trust States and Network Security	25
Rate Limiting of ARP Packets	26
Logging of Dropped Packets	26
Configuring Dynamic ARP Inspection	26
Default Dynamic ARP Inspection Configuration	26
Dynamic ARP Inspection Configuration Guidelines	27
Configuring Dynamic ARP Inspection in DHCP Environments	28
Example for Configuring Dynamic ARP Inspection	29
Disabling Dynamic ARP Inspection	29
Limiting the Rate of Incoming ARP Packets (optional)	30
Performing Validation Checks (optional)	31
Configuring the Log Buffer (optional)	32
Returning to the Default Log Buffer Settings	34
Displaying Dynamic ARP Inspection Information	34
Clearing or Displaying Dynamic ARP Inspection Statistics	35
Clearing or Displaying Dynamic ARP Inspection Logging Information	35



CHAPTER 1

Feature History

The following table lists the new and modified features supported in the IP Addressing Configuration Guide in Cisco IOS XE 17 releases, on Cisco NCS 520 Series Ethernet Access Device.

Feature	Description
Cisco IOS XE Amsterdam 17.3.1	
DHCP Snooping	The Dynamic Host Configuration Protocol (DHCP) Snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP Snooping binding database, DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. DHCP Snooping is used to differentiate untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another router. This feature is supported on the Cisco NCS 520 Router
Dynamic ARP Inspection	The dynamic Address Resolution Protocol (ARP) provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. Dynamic ARP inspection also determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, such as the DHCP Snooping binding database. This feature is supported on the Cisco NCS 520 Router



CHAPTER 2

DHCP Features Configuration

This chapter describes how to configure the DHCP server port-based address allocation features on the Router.

Table 1: Feature History

Feature Name	Release	Description
DHCP Snooping	Cisco IOS XE Amsterdam 17.3.1	The Dynamic Host Configuration Protocol (DHCP) Snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP Snooping binding database, DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. DHCP Snooping is used to differentiate untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another router. This feature is supported on the Cisco NCS 520 Router

- [Limitations and Restrictions on the Cisco NCS 520 Router](#) , on page 3
- [DHCP Features](#), on page 3
- [Configuring DHCP Features](#), on page 10
- [Displaying DHCP Snooping Information](#), on page 17
- [DHCP Server Port-Based Address Allocation](#), on page 18
- [Configuring DHCP Server Port-Based Address Allocation](#), on page 19

Limitations and Restrictions on the Cisco NCS 520 Router

- DHCP over xconnect and local connect is supported.
- DHCP smart relay supports a maximum of 16 local addresses configured on a BDI or an interface.

DHCP Features

DHCP is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts; only those hosts that are connected to the network consume IP addresses.

DHCP Server

The DHCP server assigns IP addresses from specified address pools on a switch or router to DHCP clients and manages them. If the DHCP server cannot give the DHCP client the requested configuration parameters from its database, it can forward the request to one or more secondary DHCP servers defined by the network administrator.

DHCP Relay Agent

A DHCP relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. Relay agents forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on egress interfaces.

DHCP relay is supported on these variants of the Cisco NCS 520 Series Ethernet Access Device:

- N520-4G4Z-A (Base)
- N520-X-4G4Z-A (Premium)
- N520-X-4G4Z-D (Premium)
- N520-20G4Z-A (Base)
- N520-20G4Z-D (Base)
- N520-X-20G4Z-A (Premium)
- N520-X-20G4Z-D (Premium)



Note DHCP option-82 is not supported, when the DHCP relay agent is enabled and by simultaneously disabling the DHCP snooping.

DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table. For more information about this database, see the [Displaying DHCP Snooping Information, on page 17](#).

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.



Note For DHCP snooping to function properly, all DHCP servers must be connected to the router through trusted interfaces.

An untrusted DHCP message is a message that is received from outside the network or firewall. When you use DHCP snooping in a service-provider environment, an untrusted message is sent from a device that is not in the service-provider network, such as a customer's switch. Messages from unknown devices are untrusted because they can be sources of traffic attacks.

The DHCP snooping binding database has the MAC address, the IP address, the lease time, the binding type, the bridge-domain number, and the interface information that corresponds to the local untrusted interfaces of a switch. It does not have information regarding hosts interconnected with a trusted interface.

In a service-provider network, a trusted interface is connected to a port on a device in the same network. An untrusted interface is connected to an untrusted interface in the network or to an interface on a device that is not in the network.

When a switch receives a packet on an untrusted interface and the interface belongs to a bridge-domain in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The router drops a DHCP packet when one of these situations occurs:

- A packet from a DHCP server, such as a DHCP OFFER, DHCP ACK, DHCP NAK, or DHCP REQUEST packet, is received from outside the network or firewall.
- A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.
- The switch receives a DHCP RELEASE or DHCP DECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.
- A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.

If the switch is an aggregation switch supporting DHCP snooping and is connected to an edge switch that is inserting DHCP option-82 information, the switch drops packets with option-82 information when packets are received on an untrusted interface. If DHCP snooping is enabled and packets are received on a trusted port, the aggregation switch does not learn the DHCP snooping bindings for connected devices and cannot build a complete DHCP snooping binding database.

When an aggregation switch can be connected to an edge switch through an untrusted interface and you enter the `ip dhcp snooping information option allowed-trust` global configuration command, the aggregation switch accepts packets with option-82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. The DHCP security features, such as dynamic ARP inspection, can still be enabled on the aggregation switch while the switch receives packets with option-82 information on ingress untrusted interfaces to which hosts are connected. The port on the edge switch that connects to the aggregation switch must be configured as a trusted interface.

Option-82 Data Insertion

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.



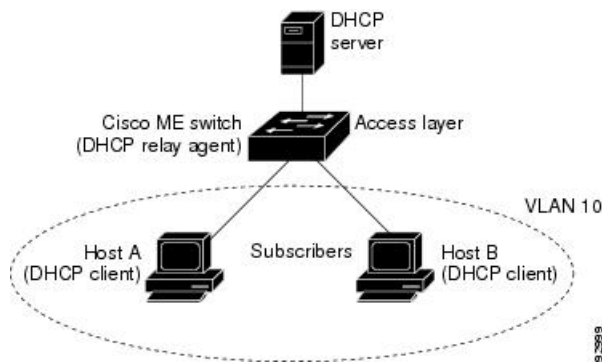
Note The DHCP option-82 feature is supported only when DHCP snooping is globally enabled and on the bridge-domains to which subscriber devices using this feature are assigned.



Note DHCP Client will not receive the IP address if DHCP server is connected via relay and when snooping is globally enabled along with BDI IP configured for snooping enabled BD.

Figure below is an example of a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the switch at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent (the Cisco Router) is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

Figure 1: DHCP Relay Agent in a Metropolitan Ethernet Network



When you enable the DHCP snooping information option 82 on the switch, this sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. By default, the remote-ID suboption is the switch MAC address, and the circuit-ID suboption is the port identifier from which the packet is received. You can also configure the remote ID and circuit ID. For information on configuring these suboptions, see the [Enabling DHCP Snooping and Option 82, on page 14](#).
- If the IP address of the relay agent is configured, the switch adds this IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82-capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.
- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

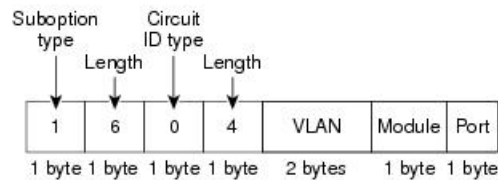
In the default suboption configuration, when the described sequence of events occurs, the values in these fields in figure below do not change:

- Circuit ID suboption fields
- Suboption type
- Length of the suboption type
- Circuit ID type
- Length of the circuit ID type
- Remote ID suboption fields
- Suboption type
- Length of the suboption type
- Remote ID type
- Length of the circuit ID type

Figure below shows the packet formats for the remote ID suboption and the circuit ID suboption when the default suboption configuration is used. The switch uses the packet formats when DHCP snooping is globally enabled and when the ip dhcp snooping information option global configuration command is entered.

Figure 2: Suboption Packet Formats

Circuit ID Suboption Frame Format



Remote ID Suboption Frame Format

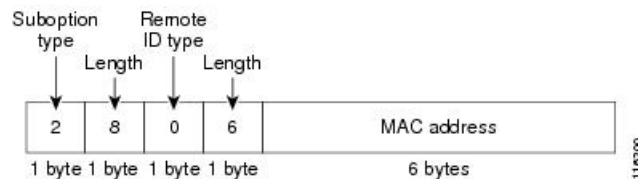


Figure below shows the packet formats for user-configured remote-ID and circuit-ID suboptions. The switch uses these packet formats when you globally enable DHCP snooping and enter the ip dhcp snooping information option format remote-id global configuration command and the ip dhcp snooping bridge-domain information option format-type circuit-id string interface configuration command.

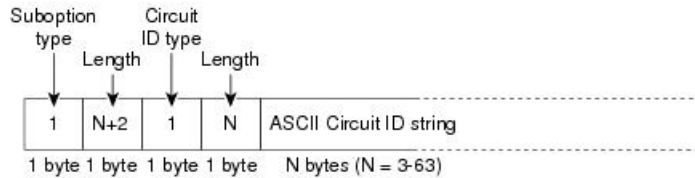
The values for these fields in the packets change from the default values when you configure the remote-ID and circuit-ID suboptions:

- Circuit-ID suboption fields
- The circuit-ID type is 1.

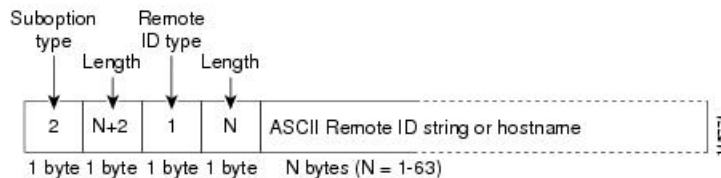
- The length values are variable, depending on the length of the string that you configure.
- Remote-ID suboption fields
- The remote-ID type is 1.
- The length values are variable, depending on the length of the string that you configure.

Figure 3: User-Configured Suboption Packet Formats

Circuit ID Suboption Frame Format (for user-configured string):



Remote ID Suboption Frame Format (for user-configured string):



Note In scenarios where **no ip dhcp snooping information option** is configured (i.e when the server does not support DHCP information option) then use **ip dhcp snooping track host** command. This is because the MAC to port mapping is only available in DHCP option 82. If the information options has been disabled then to know the MAC to port mapping **ip dhcp snooping track host** command must be enabled.

Cisco IOS DHCP Server Database

During the DHCP-based autoconfiguration process, the designated DHCP server uses the Cisco IOS DHCP server database. It has IP addresses, address bindings, and configuration parameters, such as the boot file.

An address binding is a mapping between an IP address and a MAC address of a host in the Cisco IOS DHCP server database. You can manually assign the client IP address, or the DHCP server can allocate an IP address from a DHCP address pool. For more information about manual and automatic address bindings, see the [IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S](#).

DHCP Snooping Binding Database

When DHCP snooping is enabled, the switch uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 8192 bindings.



Note DHCP snooping database read event will **not** retrieve entries for 10G and PC interface

Each database entry (*binding*) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the bridge-domain to which the interface belongs. The database agent stores the bindings in a file at a configured location. At the end of each entry is a *checksum* value that accounts for all the bytes associated with the entry. Each entry is 72 bytes, followed by a space and then the checksum value.

To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP inspection, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.

When reloading, the router reads the binding file to build the DHCP snooping binding database. The switch keeps the file current by updating it when the database changes.

When a router learns of new bindings or when it loses bindings, the router immediately updates the entries in the database. The router also updates the entries in the binding file. The frequency at which the file is updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.

This is the format of the file that has the bindings:

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-...-n>
END
```

Each entry in the file is tagged with a checksum value that the router uses to verify the entries when it reads the file. The *initial-checksum* entry on the first line distinguishes entries associated with the latest file update from entries associated with a previous file update.

This is an example of a binding file:

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
```

```

192.1.168.1 3 0003.47d8.c91f 2BB6488E Fa1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Fa1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Fa1/0/4 584a38f0

END

```

When the router starts and the calculated checksum value equals the stored checksum value, the router reads entries from the binding file and adds the bindings to its DHCP snooping binding database. The router ignores an entry when one of these situations occurs:

- The router reads the entry and the calculated checksum value does not equal the stored checksum value. The entry and the ones following it are ignored.
- An entry has an expired lease time (the router might not remove a binding entry when the lease time expires).
- The interface in the entry no longer exists on the system.
- The interface is a routed interface or a DHCP snooping-trusted interface.

Configuring DHCP Features

Default DHCP Configuration

Table below shows the default DHCP configuration.

Table 2: Default DHCP Configuration

Feature	Default Setting
DHCP server	Enabled in Cisco IOS software, requires configuration ¹
DHCP relay agent	Enabled ²
DHCP packet forwarding address	None configured
Checking the relay agent information	Enabled (invalid messages are dropped) ³
DHCP relay agent forwarding policy	Replace the existing relay agent information ⁴
DHCP snooping enabled globally	Disabled
DHCP snooping information option	Enabled
DHCP snooping option to accept packets on untrusted ingress interfaces ⁵	Disabled
DHCP snooping limit rate	None configured
DHCP snooping trust	Untrusted
DHCP snooping bridge-domain	Disabled
DHCP snooping MAC address verification	Enabled

Feature	Default Setting
Cisco IOS DHCP server binding database	Enabled in Cisco IOS software, requires configuration. Note The router gets network addresses and configuration parameters only from a device configured as a DHCP server.
DHCP snooping binding database agent	Enabled in Cisco IOS software, requires configuration. This feature is operational only when a destination is configured.

- ¹ The router responds to DHCP requests only if it is configured as a DHCP server.
- ² The router relays DHCP packets only if the IP address of the DHCP server is configured on the BDI of the DHCP client.
- ³ The router relays DHCP packets only if the IP address of the DHCP server is configured on the BDI of the DHCP client.
- ⁴ The router relays DHCP packets only if the IP address of the DHCP server is configured on the BDI of the DHCP client.
- ⁵ Use this feature when the router is an aggregation switch that receives packets with option-82 information from an edge switch.

DHCP Snooping Configuration Guidelines

- You must globally enable DHCP snooping on the router.
- DHCP snooping is not active until DHCP snooping is enabled on a bridge-domain.
- Before globally enabling DHCP snooping on the router, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- Before configuring the DHCP snooping information option on your router, be sure to configure the device that is acting as the DHCP server. For example, you must specify the IP addresses that the DHCP server can assign or exclude, or you must configure DHCP options for these devices.
- When configuring a large number of circuit IDs on a router, consider the impact of lengthy character strings on the NVRAM or the flash memory. If the circuit-ID configurations, combined with other data, exceed the capacity of the NVRAM or the flash memory, an error message appears.
- Before configuring the DHCP relay agent on your router, make sure to configure the device that is acting as the DHCP server. For example, you must specify the IP addresses that the DHCP server can assign or exclude, configure DHCP options for devices, or set up the DHCP database agent.
- If the DHCP relay agent is enabled but DHCP snooping is disabled, the DHCP option-82 data insertion feature is not supported.
- If a switch port is connected to a DHCP server, configure a port as trusted by entering the ip dhcp snooping trust interface configuration command.
- If a switch port is connected to a DHCP client, configure a port as untrusted by entering the no ip dhcp snooping trust interface configuration command.

Follow these guidelines when configuring the DHCP snooping binding database:

- Because both NVRAM and the flash memory have limited storage capacity, we recommend that you store the binding file on a TFTP server.
- For network-based URLs (such as TFTP and FTP), you must create an empty file at the configured URL before the router can write bindings to the binding file at that URL. See the documentation for your TFTP server to determine whether you must first create an empty file on the server; some TFTP servers cannot be configured this way.
- To ensure that the lease time in the database is accurate, we recommend that NTP is enabled and configured.
- If NTP is configured, the router writes binding changes to the binding file only when the router system clock is synchronized with NTP.
- Do not enter the `ip dhcp snooping information option allowed-untrusted` command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.

```
Router# show ip dhcp snooping binding
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
AA:00:11:13:00:01	40.0.0.2	117	dhcp-snooping	100	Port-channel100+Efp7

Configuring the DHCP Server

The router can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your router but are not configured. These features are not operational.

For procedures to configure the router as a DHCP server, see the [IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S](#).

Configuring the DHCP Relay Agent

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>service dhcp</code>	Enable the DHCP relay agent on your router. By default, this feature is enabled.
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	Verify your entries.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

What to do next

To disable the DHCP relay agent, use the **no service dhcp** global configuration command.

Specifying the Packet Forwarding Address

If the DHCP server and the DHCP clients are on different networks or subnets and the router is running the metro IP access image, you must configure the router with the **ip helper-address address** interface configuration command. The general rule is to configure the command on the Layer 3 interface closest to the client. The address used in the **ip helper-address** command can be a specific DHCP server IP address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables any DHCP server to respond to requests.



Note To remove the DHCP packet forwarding address, use the **no ip helper-address address** interface configuration command.

Beginning in privileged EXEC mode, follow these steps to specify the packet forwarding address:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface bridge-domain id	Create a switch virtual interface by entering a bridge-domain ID, and enter interface configuration mode.
Step 3	ip address ip-address subnet-mask	Configure the interface with an IP address and an IP subnet.
Step 4	ip helper-address address	Specify the DHCP packet forwarding address. The helper address can be a specific DHCP server address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables other servers to respond to DHCP requests. If you have multiple servers, you can configure one helper address for each server.
Step 5	end	Return to privileged EXEC mode.
Step 6	show running-config	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Enabling DHCP Snooping and Option 82

Beginning in the privileged EXEC mode, follow these steps to enable DHCP snooping on the switch:

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip dhcp snooping</code>	Enable DHCP snooping globally.
Step 3	<code>ip dhcp snooping bridge-domain id</code>	Enable DHCP snooping on a bridge-domain
Step 4	<code>ip dhcp snooping information option</code>	Enable the router to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. This is the default setting.
Step 5	<code>ip dhcp snooping information option format remote-id [string ASCII-string hostname]</code>	<p>(Optional) Configure the remote-ID suboption. You can configure the remote ID to be:</p> <ul style="list-style-type: none"> • String of up to 63 ASCII characters (no spaces) • Configured hostname for the router <p>Note If the hostname is longer than 63 characters, it is truncated to 63 characters in the remote-ID configuration.</p> <p>The default remote ID is the router MAC address.</p>
Step 6	<code>ip dhcp snooping information option allowed-untrusted</code>	<p>(Optional) If the router is acting as an aggregation switch connected to an edge switch, enable the router to accept incoming DHCP snooping packets with option-82 information from the edge switch.</p> <p>The default is disabled.</p> <p>Note Enter this command only on aggregation switches that are connected to trusted devices.</p>
Step 7	<code>interface interface-id</code>	Specify the interface to be configured, and enter interface configuration mode.
Step 8	<code>no shutdown</code>	Enable the port, if necessary. By default, UNIs and ENIs are disabled and NNIs are enabled.
Step 9	<code>ip dhcp snooping trust</code>	Configure the interface as trusted or untrusted. You can use the no keyword to configure an

	Command or Action	Purpose
		interface to receive messages from an untrusted client. The default is untrusted.
Step 10	ip dhcp snooping limit rate rate	(Optional) Configure the number of DHCP packets per second that an interface can receive. The range is 1 to 2048. By default, no rate limit is configured. Note We recommend an untrusted rate limit of not more than 100 packets per second. If you configure rate limiting for trusted interfaces, you might need to increase the rate limit if the port is a trunk port assigned to more than one bridge-domain on which DHCP snooping is enabled.
Step 11	exit	Return to global configuration mode.
Step 12	ip dhcp snooping verify mac-address	(Optional) Configure the router to verify that the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet. The default is to verify that the source MAC address matches the client hardware address in the packet.
Step 13	end	Return to privileged EXEC mode.
Step 14	show running-config	Verify your entries.
Step 15	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Enabling the Cisco IOS DHCP Server Database

For procedures to enable and configure the Cisco IOS DHCP server database, see the *IP Addressing: DHCP Configuration Guide*.

Enabling the DHCP Snooping Binding Database Agent

Beginning in privileged EXEC mode, follow these steps to enable and configure the DHCP snooping binding database agent on the router:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.

	Command or Action	Purpose
Step 2	<code>ip dhcp snooping database {flash:/filename ftp://user:password@host/filename http://[[username:password]@]{hostname host-ip}[/directory] /image-name.tar rcp://user@host/filename} tftp://host/filename</code>	Specify the URL for the database agent or the binding file by using one of these forms: <ul style="list-style-type: none"> • <code>flash:/filename</code> • <code>ftp://user:password@host/filename</code> • <code>http://[[username:password]@]{hostname host-ip}[/directory]/image-name.tar</code> • <code>rcp://user@host/filename</code> • <code>tftp://host/filename</code>
Step 3	<code>ip dhcp snooping database timeout seconds</code>	Specify when to stop the database transfer process after the binding database changes. The range is from 0 to 86400. Use 0 for an infinite duration. The default is 300 seconds (5 minutes).
Step 4	<code>ip dhcp snooping database write-delay seconds</code>	Specify the duration for which the transfer should be delayed after the binding database changes. The range is from 15 to 86400 seconds. The default is 300 seconds (5 minutes).
Step 5	<code>end</code>	Return to privileged EXEC mode.
Step 6	<code>ip dhcp snooping binding [ip-address mac-address dynamic static bridge-domain id interface interface]</code>	(Optional) Add binding entries to the DHCP snooping binding database. The <i>seconds</i> range is from 1 to 4294967295. Enter this command for each entry that you add. Note Use this command when you are testing or debugging the router.
Step 7	<code>show ip dhcp snooping database [detail]</code>	Display the status and statistics of the DHCP snooping binding database agent.
Step 8	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Stopping the Database Agent and Binding files

To stop using the database agent and binding files, use the `no ip dhcp snooping database` global configuration command. To reset the timeout or delay values, use the `ip dhcp snooping database timeout seconds` or the `ip dhcp snooping database write-delay seconds` global configuration command.

Clearing the Statistics of the DHCP Snooping Binding Database Agent

To clear the statistics of the DHCP snooping binding database agent, use the `clear ip dhcp snooping database statistics` privileged EXEC command. To renew the database, use the `renew ip dhcp snooping database` privileged EXEC command.

Deleting Binding Entries from the DHCP Snooping Binding Database

To delete binding entries from the DHCP snooping binding database, use the `no ip dhcp snooping binding mac-address bridge-domain id ip-address interface interface-id` privileged EXEC command. Enter this command for each entry that you delete.

Disabling DHCP Snooping

To disable DHCP snooping, use the `no ip dhcp snooping` global configuration command.

To disable DHCP snooping on a bridge-domain, use the `no ip dhcp snooping bridge-domain id` global configuration command.

To disable the insertion and removal of the option-82 field, use the `no ip dhcp snooping information option global` configuration command.

To configure an aggregation switch to drop incoming DHCP snooping packets with option-82 information from an edge switch, use the `no ip dhcp snooping information option allowed-untrusted` global configuration command.

Displaying DHCP Snooping Information

To display the DHCP snooping information, use one or more of the privileged EXEC commands as shown in below table:

Table 3: Commands for Displaying DHCP Information

Command	Purpose
<code>show ip dhcp snooping</code>	Displays the DHCP snooping configuration
<code>show ip dhcp snooping binding [ip-address / mac-address / dynamic static bridge-domain id interface interface]</code>	Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table. ⁶
<code>show ip dhcp snooping database</code>	Displays the DHCP snooping binding database status and statistics.

⁶ If DHCP snooping is enabled and an interface changes to the down state, the router does not delete the manually configured bindings.

Pre-assigned Address Reserved in the DHCP Pool

This example shows that the preassigned address was correctly reserved in the DHCP pool:

```
Router# show ip dhcp pool dhcppool
Pool dhcp pool:
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next) : 0 / 0
  Total addresses : 254
  Leased addresses : 0
  Excluded addresses : 4
  Pending event : none
```

```

1 subnet is currently in the pool:
Current index   IP address range      Leased/Excluded/Total
10.1.1.1       10.1.1.1 - 10.1.1.254  0 / 4 / 254
1 reserved address is currently in the pool
Address         Client
10.1.1.7       Et1/0

```

Automatic Generation of Subscriber Identifier

In this example, a subscriber identifier is automatically generated, and the DHCP server ignores any client identifier fields in the DHCP messages and uses the subscriber identifier instead. The subscriber identifier is based on the short name of the interface and the client preassigned IP address 10.1.1.7.

```

Router# show running config
Building configuration...
Current configuration : 4899 bytes
!
hostname router
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
 network 10.1.1.0 255.255.255.0
 address 10.1.1.7 client-id "Et1/0" ascii
#output truncated#

```

DHCP Server Port-Based Address Allocation

DHCP server port-based address allocation is a feature that enables DHCP to maintain the same IP address on an Ethernet switch port regardless of the attached device client identifier or client hardware address.

When Ethernet switches are deployed in the network, they offer connectivity to the directly connected devices. In some environments, such as on a factory floor, if a device fails, the replacement device must be working immediately in the existing network. With the current DHCP implementation, there is no guarantee that DHCP would offer the same IP address to the replacement device. Control, monitoring, and other software expect a stable IP address associated with each device. If a device is replaced, the address assignment should remain stable even though the DHCP client has changed.

When configured, the DHCP server port-based address allocation feature ensures that the same IP address is always offered to the same connected port even as the client identifier or client hardware address changes in the DHCP messages received on that port. The DHCP protocol recognizes DHCP clients by the client identifier option in the DHCP packet. Clients that do not include the client identifier option are identified by the client hardware address. When you configure this feature, the port name of the interface overrides the client identifier or hardware address and the actual point of connection, the switch port, becomes the client identifier.

In all cases, by connecting the Ethernet cable to the same port, the same IP address is allocated through DHCP to the attached device.

The DHCP server port-based address allocation feature is only supported on a Cisco IOS DHCP server and not a third-party server.

Configuring DHCP Server Port-Based Address Allocation

Before you begin

Default Port-Based Address Allocation Configuration

By default, DHCP server port-based address allocation is disabled.

Port-Based Address Allocation Configuration Guidelines

These are the configuration guidelines for DHCP port-based address allocation:

- Only one IP address can be assigned per port.
- Reserved addresses (preassigned) cannot be cleared by using the `clear ip dhcp binding` global configuration command.
- Preassigned addresses are automatically excluded from normal dynamic IP address assignment. Preassigned addresses cannot be used in host pools, but there can be multiple preassigned addresses per DHCP address pool.
- To restrict assignments from the DHCP pool to preconfigured reservations (unreserved addresses are not offered to the client and other clients are not served by the pool), you can enter the reserved-only DHCP pool configuration command.

Enabling DHCP Server Port-Based Address Allocation

Beginning in privileged EXEC mode, follow these steps to globally enable port-based address allocation and to automatically generate a subscriber identifier on an interface.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip dhcp use subscriber-id client-id</code>	Configure the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.
Step 3	<code>ip dhcp subscriber-id interface-name</code>	Automatically generate a subscriber identifier based on the short name of the interface. A subscriber identifier configured on a specific interface takes precedence over this command.
Step 4	<code>interface interface-id</code>	Specify the interface to be configured, and enter interface configuration mode.

	Command or Action	Purpose
Step 5	ip dhcp server use subscriber-id client-id	Configure the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Pre-assigning IP Addresses

After enabling DHCP port-based address allocation on the router, use the `ip dhcp pool global configuration` command to preassign IP addresses and to associate them to clients. To restrict assignments from the DHCP pool to preconfigured reservations, you can enter the reserved-only DHCP pool configuration command. Unreserved addresses that are part of the network or on pool ranges are not offered to the client, and other clients are not served by the pool. By entering this command, users can configure a group of switches with DHCP pools that share a common IP subnet and that ignore requests from clients of other switches.

Beginning in privileged EXEC mode follow these steps to preassign an IP address and to associate it to a client identified by the interface name.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip dhcp use subscriber-id client-id	Configure the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.
Step 3	ip dhcp subscriber-id interface-name	Automatically generate a subscriber identifier based on the short name of the interface. A subscriber identifier configured on a specific interface takes precedence over this command.
Step 4	interface <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 5	ip dhcp server use subscriber-id client-id	Configure the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Removing an IP Address Reservation from a DHCP Pool

To remove an IP address reservation from a DHCP pool, use the `no address ip-address client-id` string DHCP pool configuration command. To change the address pool to nonrestricted, enter the `no reserved-only` DHCP pool configuration command.

Automatic Generation of Subscriber Identifier

In this example, a subscriber identifier is automatically generated, and the DHCP server ignores any client identifier fields in the DHCP messages and uses the subscriber identifier instead. The subscriber identifier is based on the short name of the interface and the client preassigned IP address 10.1.1.7.

```
Router# show running config
Building configuration...
Current configuration : 4899 bytes
!
hostname router
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
 network 10.1.1.0 255.255.255.0
 address 10.1.1.7 client-id "Et1/0" ascii
#output truncated#
```

Disabling DHCP Port-Based Address Allocation

To disable DHCP port-based address allocation, use the `no ip dhcp use subscriber-id client-id global` configuration command. To disable the automatic generation of a subscriber identifier, use the `no ip dhcp subscriber-id interface-name global` configuration command. To disable the subscriber identifier on an interface, use the `no ip dhcp server use subscriber-id client-id interface` configuration command.

Displaying DHCP Server Port-Based Address Allocation

To display the DHCP server port-based address allocation information, use one or more of the privileged EXEC commands as shown in table below:

Table 4: Commands for Displaying DHCP Port-Based Address Allocation Information

Command	Purpose
<code>show interface <i>interface id</i></code>	Display the status and configuration of a specific interface.
<code>show ip dhcp pool</code>	Display the DHCP address pools.
<code>show ip dhcp binding</code>	Display address bindings on the Cisco IOS DHCP server.



CHAPTER 3

Configuration of Dynamic ARP Inspection

This chapter describes how to configure dynamic Address Resolution Protocol inspection (dynamic ARP inspection). This feature helps prevent malicious attacks on the router by not relaying invalid ARP requests and responses to other bridge-domains.

Table 5: Feature History

Feature Name	Release	Description
Dynamic ARP Inspection	Cisco IOS XE Amsterdam 17.3.1	The dynamic Address Resolution Protocol (ARP) provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. Dynamic ARP inspection also determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, such as the DHCP Snooping binding database. This feature is supported on the Cisco NCS 520 Router



Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

Restrictions

- Dynamic ARP inspection is supported only on bridge-domains; other interfaces such as VLANs are *not* supported.
- ARP packets with broadcast MAC address or router MAC address is only supported. Dynamic ARP inspection is *not* supported for unknown unicast ARP requests and ARP replies.
- [Dynamic ARP Inspection, on page 23](#)
- [Configuring Dynamic ARP Inspection, on page 26](#)
- [Displaying Dynamic ARP Inspection Information, on page 34](#)

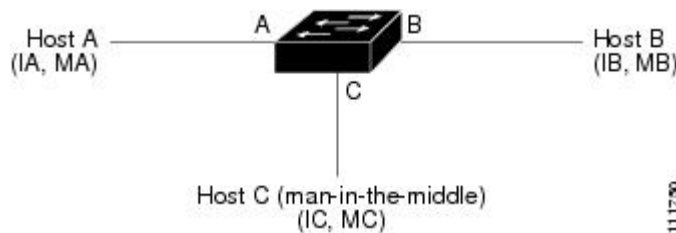
Dynamic ARP Inspection

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A but does not have the MAC address of

Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address. However, because ARP allows a gratuitous reply from a host even if an ARP request was not received, an ARP spoofing attack and the poisoning of ARP caches can occur. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host.

A malicious user can attack hosts, switches, and routers connected to your Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Figure below shows an example of ARP cache poisoning.

Figure 4: ARP Cache Poisoning



Hosts A, B, and C are connected to the switch on interfaces A, B and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, Host A uses IP address IA and MAC address MA. When Host A needs to communicate to Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. When the switch and Host B receive the ARP request, they populate their ARP caches with an ARP binding for a host with the IP address IA and a MAC address MA; for example, IP address IA is bound to MAC address MA. When Host B responds, the switch and Host A populate their ARP caches with a binding for a host with the IP address IB and the MAC address MB.

Host C can poison the ARP caches of the switch, Host A, and Host B by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB. This means that Host C intercepts that traffic. Because Host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. Host C has inserted itself into the traffic stream from Host A to Host B, the classic *man-in-the-middle* attack.

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The router performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets

Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the bridge-domains and on the router. If the ARP packet is received on a trusted interface, the router forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

You enable dynamic ARP inspection on a per-bridge-domain basis by using the **ip arp inspection bridge-domain** domain-id global configuration command.

You can configure dynamic ARP inspection to drop ARP packets when the IP addresses in the packets are invalid or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header. Use the **ip arp inspection validate [src-mac] [dst-mac] [ip]** global configuration command. For more information, see the [Performing Validation Checks \(optional\)](#).

Interface Trust States and Network Security

Dynamic ARP inspection associates a trust state with each interface on the router. Packets arriving on trusted interfaces bypass all dynamic ARP inspection validation checks, and those arriving on untrusted interfaces undergo the dynamic ARP inspection validation process.

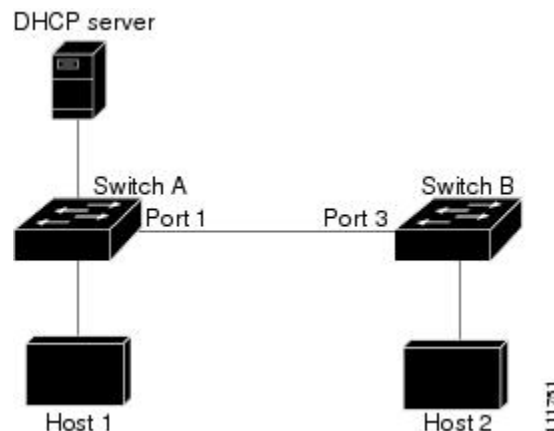
In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted. With this configuration, all ARP packets entering the network from a given switch bypass the security check. No other validation is needed at any other place in the bridge-domain or in the network. You configure the trust setting by using the **ip arp inspection trust interface** configuration command.



Note Use the trust state configuration carefully. Configuring interfaces as untrusted when they should be trusted can result in a loss of connectivity.

In the figure below, assume that both Switch A and Switch B are running dynamic ARP inspection on the bridge-domain that includes Host 1 and Host 2. If Host 1 and Host 2 acquire their IP addresses from the DHCP server connected to Switch A, only Switch A binds the IP-to-MAC address of Host 1. Therefore, if the interface between Switch A and Switch B is untrusted, the ARP packets from Host 1 are dropped by Switch B. Connectivity between Host 1 and Host 2 is lost.

Figure 5: ARP Packet Validation on a Bridge-Domain Enabled for Dynamic ARP Inspection



Configuring interfaces to be trusted when they are actually untrusted leaves a security hole in the network. If Switch A is not running dynamic ARP inspection, Host 1 can easily poison the ARP cache of Switch B (and Host 2, if the link between the switches is configured as trusted). This condition can occur even though Switch B is running dynamic ARP inspection.

Dynamic ARP inspection ensures that hosts (on untrusted interfaces) connected to a switch running dynamic ARP inspection do not poison the ARP caches of other hosts in the network. However, dynamic ARP inspection does not prevent hosts in other portions of the network from poisoning the caches of the hosts that are connected to a switch running dynamic ARP inspection.



Note Depending on the setup of the DHCP server and the network, it might not be possible to validate a given ARP packet on all switches in the bridge-domain.

Rate Limiting of ARP Packets

The switch CPU performs Dynamic ARP Inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial-of-service attack. By default, the rate for untrusted interfaces is 15 packets per second (pps). Trusted interfaces are not rate-limited. You can change this setting by using the `ip arp inspection limit` interface configuration command.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you intervene. You can use the `errdisable recovery` global configuration command to enable error disable recovery so that ports automatically emerge from this state after a specified timeout period.



Note You can configure a maximum of 1150 packets per second using the `ip arp inspection limit rate` command, although the range specified in the command is 0–2048 packets per second.

For configuration information, see the [Limiting the Rate of Incoming ARP Packets \(optional\)](#).

Logging of Dropped Packets

When the switch drops a packet, it places an entry in the log buffer and then generates system messages on a rate-controlled basis. After the message is generated, the switch clears the entry from the log buffer. Each log entry contains flow information, such as the receiving bridge-domain, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

You use the `ip arp inspection log-buffer` global configuration command to configure the number of entries in the buffer and the number of entries needed in the specified interval to generate system messages. You specify the type of packets that are logged by using the `ip arp inspection bridge-domain logging` global configuration command. For configuration information, see the [Configuring the Log Buffer \(optional\)](#), on page 32.

Configuring Dynamic ARP Inspection

Default Dynamic ARP Inspection Configuration

Table below shows the default dynamic ARP inspection configuration.

Table 6: Default Dynamic ARP Inspection Configuration

Feature	Default Setting
Dynamic ARP inspection	Disabled on all bridge-domains.
Interface trust state	All interfaces are untrusted.
Rate limit of incoming ARP packets	The rate is 15 pps on untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second. The rate is unlimited on all trusted interfaces. The burst interval is 1 second.
Validation checks	No checks are performed.
Log buffer	When dynamic ARP inspection is enabled, all denied or dropped ARP packets are logged. The number of entries in the log is 32. The number of system messages is limited to 5 per second. The logging-rate interval is 1 second.
Per-bridge-domain logging	All denied or dropped ARP packets are logged.

Dynamic ARP Inspection Configuration Guidelines

- A physical port can join an EtherChannel port channel only when the trust state of the physical port and the channel port match. Otherwise, the physical port remains suspended in the port channel. A port channel inherits its trust state from the first physical port that joins the channel. Consequently, the trust state of the first physical port need not match the trust state of the channel.

Conversely, when you change the trust state on the port channel, the switch configures a new trust state on all the physical ports that comprise the channel.

- The operating rate for the port channel is cumulative across all the physical ports within the channel. For example, if you configure the port channel with an ARP rate-limit of 400 pps, all the interfaces combined on the channel receive an aggregate 400 pps. The rate of incoming ARP packets on EtherChannel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on the channel-port members.

The rate of incoming packets on a physical port is checked against the port-channel configuration rather than the physical-ports configuration. The rate-limit configuration on a port channel is independent of the configuration on its physical ports.

If the EtherChannel receives more ARP packets than the configured rate, the channel (including all physical ports) is placed in the error-disabled state.

- Make sure to limit the rate of ARP packets on incoming trunk ports. Configure trunk ports with higher rates to reflect their aggregation and to handle packets across multiple dynamic ARP inspection-enabled bridge-domains. You also can use the `ip arp inspection limit none interface` configuration command to

make the rate unlimited. A high rate-limit on one bridge-domain can cause a denial-of-service attack to other bridge-domains when the software places the port in the error-disabled state.

- When you enable dynamic ARP inspection on the switch, policers that were configured to police ARP traffic are no longer effective. The result is that all ARP traffic is sent to the CPU.
- The **errdisable recovery cause arp-inspection interval** and **show ip arp inspection interfaces show errdisable recovery** commands are *not* supported on the router.

Configuring Dynamic ARP Inspection in DHCP Environments

This procedure shows how to configure dynamic ARP inspection when two switches support this feature. Host 1 is connected to Switch A, and Host 2 is connected to Switch B. Both switches are running dynamic ARP inspection on bridge-domain 1 where the hosts are located. A DHCP server is connected to Switch A. Both hosts acquire their IP addresses from the same DHCP server. Therefore, Switch A has the bindings for Host 1 and Host 2, and Switch B has the binding for Host 2.



Note Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses.

Beginning in privileged EXEC mode, follow these steps to configure dynamic ARP inspection. You must perform this procedure on both switches. This procedure is required.

Procedure

	Command or Action	Purpose
Step 1	show cdp neighbors	Verify the connection between the switches.
Step 2	configure terminal	Enter global configuration mode.
Step 3	ip arp inspection	Enables dynamic ARP inspection globally.
Step 4	ip arp inspection bridge-domain id	Enable dynamic ARP inspection on a per-bridge-domain basis. By default, dynamic ARP inspection is disabled on all bridge-domains. Specify the same bridge-domain ID for both switches.
Step 5	interface interface-id	Specify the interface connected to the other switch, and enter interface configuration mode.
Step 6	no shutdown	Enable the port, if necessary. By default, user network interfaces (UNIs) and enhanced network interfaces (ENIs) are disabled, and network node interfaces (NNIs) are enabled.

	Command or Action	Purpose
Step 7	ip arp inspection trust	<p>Configure the connection between the switches as trusted.</p> <p>By default, all interfaces are untrusted.</p> <p>The switch does not check ARP packets that it receives from the other switch on the trusted interface. It simply forwards the packets.</p> <p>For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the ip arp inspection bridge-domain logging global configuration command. For more information, see the Configuring the Log Buffer (optional), on page 32.</p>
Step 8	end	Return to privileged EXEC mode.
Step 9	show ip arp inspection interfaces show ip arp inspection bridge-domain id	Verify the dynamic ARP inspection configuration.
Step 10	show ip dhcp snooping binding	Verify the DHCP bindings.
Step 11	show ip arp inspection statistics bridge-domain id	Check the dynamic ARP inspection statistics.
Step 12	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Example for Configuring Dynamic ARP Inspection

This example shows how to configure dynamic ARP inspection on Switch A. You would perform a similar procedure on Switch B:

```
Router(config)# ip arp inspection bridge-domain 1
Router(config)# interface gigabitethernet0/1
Router(config-if)# ip arp inspection trust
```

Disabling Dynamic ARP Inspection

To disable dynamic ARP inspection, use the `no ip arp inspection bridge-domain` global configuration command.

To return the interfaces to an untrusted state, use the `no ip arp inspection trust` interface configuration command.

Limiting the Rate of Incoming ARP Packets (optional)

The switch CPU performs dynamic ARP inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial-of-service attack.

When the rate of incoming ARP packets exceeds the configured limit (1150 packets), the switch places the port in the error-disabled state. The port remains in that state until you enable error-disabled recovery so that ports automatically emerge from this state after a specified timeout period.



Note Unless you configure a rate limit on an interface (we recommend 1024 packets), changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the **no ip arp inspection** limit interface configuration command, the interface reverts to its default rate limit.

ARP inspection rate limit will not work for values above 1024.

For configuration guidelines for rate limiting trunk ports and EtherChannel ports, see the Dynamic ARP Inspection Configuration Guidelines.

Beginning in privileged EXEC mode, follow these steps to limit the rate of incoming ARP packets. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip arp inspection	Enables dynamic ARP inspection globally.
Step 3	interface interface-id	Specify the interface to be rate-limited, and enter interface configuration mode.
Step 4	no shutdown	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 5	ip arp inspection limit {rate pps [burst interval seconds] none}	<p>Limit the rate of incoming ARP requests and responses on the interface.</p> <p>The default rate is 15 pps on untrusted interfaces and unlimited on trusted interfaces. The burst interval is 1 second.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> For rate pps, specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 pps. (Optional) For burst intervalseconds, specify the consecutive interval in seconds, over which the interface is monitored for a high rate of ARP packets. The range is 1 to 15.

	Command or Action	Purpose
		<ul style="list-style-type: none"> For rate none, specify no upper limit for the rate of incoming ARP packets that can be processed.
Step 6	exit	Return to global configuration mode.
Step 7	exit	Return to privileged EXEC mode.
Step 8	copy running-config startup-config	<p>(Optional) Save your entries in the configuration file.</p> <p>Note To return to the default rate-limit configuration, use the <code>no ip arp inspection limit interface</code> configuration command. To disable error recovery for dynamic ARP inspection, use the <code>no errdisable recovery cause arp-inspection global</code> configuration command.</p>

Performing Validation Checks (optional)

Dynamic ARP inspection intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. You can configure the switch to perform additional checks on the destination MAC address, the sender and target IP addresses, and the source MAC address.

Beginning in privileged EXEC mode, follow these steps to perform specific checks on incoming ARP packets. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip arp inspection	Enables dynamic ARP inspection globally.
Step 3	ip arp inspection validate {[src-mac] [dst-mac] [ip]}	<p>Perform a specific check on incoming ARP packets. By default, no checks are performed.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> For src-mac, check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped. For dst-mac, check the destination MAC address in the Ethernet header against the

	Command or Action	Purpose
		<p>target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.</p> <ul style="list-style-type: none"> For ip, check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses. <p>You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command enables src and dst mac validations, and a second command enables IP validation only, the src and dst mac validations are disabled as a result of the second command.</p>
Step 4	exit	Return to privileged EXEC mode.
Step 5	show ip arp inspection bridge-domain id	Verify your settings.
Step 6	copy running-config startup-config	<p>(Optional) Save your entries in the configuration file.</p> <p>Note To disable checking, use the no ip arp inspection validate [src-mac] [dst-mac] [ip] global configuration command. To display statistics for forwarded, dropped, and MAC and IP validation failure packets, use the show ip arp inspection statistics privileged EXEC command.</p>

Configuring the Log Buffer (optional)



Note Log buffering is not currently supported.

When the switch drops a packet, it places an entry in the log buffer and then generates system messages on a rate-controlled basis. After the message is generated, the switch clears the entry from the log buffer. Each log entry contains flow information, such as the receiving bridge-domain, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

A log-buffer entry can represent more than one packet. For example, if an interface receives many packets on the same bridge-domain with the same ARP parameters, the switch combines the packets as one entry in the log buffer and generates a single system message for the entry.

If the log buffer overflows, it means that a log event does not fit into the log buffer, and the display for the **show ip arp inspection log** privileged EXEC command is affected. A -- in the display appears in place of all data except the packet count and the time. No other statistics are provided for the entry. If you see this entry in the display, increase the number of entries in the log buffer or increase the logging rate.

Beginning in privileged EXEC mode, follow these steps to configure the log buffer. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip arp inspection log-buffer {entries number logs number interval seconds}	<p>Configure the dynamic ARP inspection logging buffer.</p> <p>By default, when dynamic ARP inspection is enabled, denied or dropped ARP packets are logged. The number of log entries is 32. The number of system messages is limited to 5 per second. The logging-rate interval is 1 second.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> • For entries number, specify the number of entries to be logged in the buffer. The range is 0 to 1024. • For logs number interval seconds, specify the number of entries to generate system messages in the specified interval. <p>For logs number, the range is 0 to 1024. A 0 value means that the entry is placed in the log buffer, but a system message is not generated.</p> <p>For interval seconds, the range is 0 to 86400 seconds (1 day). A 0 value means that a system message is immediately generated (and the log buffer is always empty).</p> <p>An interval setting of 0 overrides a log setting of 0.</p> <p>The logs and interval settings interact. If the logs number X is greater than interval seconds Y, X divided by Y (X/Y) system messages are sent every second. Otherwise, one system message is sent every Y divided by X (Y/X) seconds.</p>

	Command or Action	Purpose
Step 3	ip arp inspection bridge-domain id logging {matchlog none} dhcp-bindings {all none permit}}	Control the type of packets that are logged per bridge-domain. By default, all denied or all dropped packets are logged. The term <i>logged</i> means the entry is placed in the log buffer and a system message is generated. The keywords have these meanings: <ul style="list-style-type: none"> • For dhcp-bindings all, log all packets that match DHCP bindings. • For dhcp-bindings none, do not log packets that match DHCP bindings. • For dhcp-bindings permit, log DHCP-binding permitted packets.
Step 4	exit	Return to privileged EXEC mode.
Step 5	show ip arp inspection log	Verify your settings.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Returning to the Default Log Buffer Settings

To return to the default log buffer settings, use the `no ip arp inspection log-buffer {entries | logs} global` configuration command.

To return to the default bridge-domain log settings, use the `no ip arp inspection bridge-domain id logging {dhcp-bindings}` global configuration command.

To clear the log buffer, use the `clear ip arp inspection log` privileged EXEC command.

Displaying Dynamic ARP Inspection Information

To display dynamic ARP inspection information, use the privileged EXEC commands described in table below.

Table 7: Commands for Displaying Dynamic ARP Inspection Information

Command	Description
<code>show ip arp inspection interfaces [interface-id]</code>	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.
<code>show ip arp inspection bridge-domain id</code>	Displays the configuration and the operating state of dynamic ARP inspection for the specified bridge-domain. If a range is specified, displays information for bridge domains with dynamic ARP inspection enabled (active).

Clearing or Displaying Dynamic ARP Inspection Statistics

To clear or display dynamic ARP inspection statistics, use the privileged EXEC commands in table below.

For the `show ip arp inspection statistics` command, the switch increments the number of forwarded packets for each ARP request and response packet on a trusted dynamic ARP inspection port. The switch increments the number of DHCP permitted packets for each packet that is denied by source MAC, destination MAC, or IP validation checks, and the switch increments the appropriate failure count.

Table 8: Commands for Clearing or Displaying Dynamic ARP Inspection Statistics

Command	Description
<code>clear ip arp inspection statistics</code>	Clears dynamic ARP inspection statistics.
<code>show ip arp inspection statistics bridge-domain id</code>	Displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, and DHCP permitted and denied packets for the specified bridge domain. If no bridge-domain is specified, the router displays information only for bridge domains with dynamic ARP inspection enabled (active).

Clearing or Displaying Dynamic ARP Inspection Logging Information

To clear or display dynamic ARP inspection logging information, use the privileged EXEC commands in table below:

Table 9: Commands for Clearing or Displaying Dynamic ARP Inspection Logging Information

Command	Description
<code>clear ip arp inspection log</code>	Clears the dynamic ARP inspection log buffer.
<code>show ip arp inspection log</code>	Displays the configuration and contents of the dynamic ARP inspection log buffer.

