

ip dhcp-client network-discovery through ip nat sip-sbc

- ip dhcp-client network-discovery, on page 3
- ip dhcp-client update dns, on page 5
- ip dhcp drop-inform, on page 7
- ip dhcp-relay information option server-override, on page 8
- ip dhcp-relay source-interface, on page 10
- ip dhcp-server, on page 11
- ip dhcp-server query lease, on page 13
- ip dns name-list, on page 14
- ip dns primary, on page 16
- ip dns server, on page 18
- ip dns server queue limit, on page 19
- ip dns server view-group, on page 20
- ip dns spoofing, on page 22
- ip dns view, on page 23
- ip dns view-group, on page 27
- ip dns view-list, on page 29
- ip domain list, on page 32
- ip domain lookup, on page 34
- ip domain multicast, on page 36
- ip domain name, on page 37
- ip domain recursive, on page 39
- ip domain retry, on page 40
- ip domain round-robin, on page 41
- ip domain timeout, on page 42
- ip gratuitous-arps, on page 43
- ip host, on page 44
- ip host-list, on page 49
- ip hostname strict, on page 50
- ip local-proxy-arp, on page 52
- ip mobile arp, on page 53
- ip name-server, on page 55

- ip nat, on page 57
- ip nat create flow-entries, on page 59
- ip nat enable, on page 61
- ip nat inside destination, on page 62
- ip nat inside source, on page 64
- ip nat log translations flow-export, on page 70
- ip nat log translations syslog, on page 72
- ip nat outside source, on page 73
- ip nat piggyback-support, on page 77
- ip nat pool, on page 78
- ip nat service, on page 81
- ip nat service dns-reset-ttl, on page 86
- ip nat service enable-sym-port, on page 88
- ip nat service gatekeeper, on page 90
- ip nat service ipsec-esp enable, on page 91
- ip nat service pptp, on page 92
- ip nat settings gatekeeper-size, on page 93
- ip nat settings mode, on page 94
- ip nat settings pap, on page 95
- ip nat settings pool watermark, on page 98
- ip nat settings redundancy optimized-data-sync, on page 99
- ip nat settings scale bind, on page 101
- ip nat settings support mapping outside, on page 102
- ip nat sip-sbc, on page 103

ip dhcp-client network-discovery

To control the sending of Dynamic Host Configuration Protocol (DHCP) Inform and Discover messages, use the **ip dhcp-client network-discovery**command in global configuration mode. To change or disable DHCP message control, use the **no** form of this command.

ip dhcp-client network-discovery informs *number-of-messages* **discovers** *number-of-messages* **period** *seconds*
no ip dhcp-client network-discovery informs *number-of-messages* **discovers** *number-of-messages* **period** *seconds*

Syntax Description

informs *number-of-messages*	Number of DHCP Inform messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.
discovers *number-of-messages*	Number of DHCP Discover messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.
period *seconds*	Timeout period for retransmission of DHCP Inform and Discover messages. Valid periods are from 3 to 15 seconds. Default is 15 seconds.

Command Default

0 DHCP Inform and Discover messages (network discovery is disabled when both the **informs** and **discovers**keywords are set to 0); 15-second timeout period.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip dhcp-client network-discovery**command allows peer routers to dynamically discover Domain Name System (DNS) and NetBIOS name server information configured on a DHCP server using PPP IP Control Protocol (IPCP) extensions. Setting the number of DHCP Inform or Discover messages to 1 or 2 determines how many times the system sends a DHCP Inform or Discover message before stopping network discovery, as follows:

- When the number of DHCP Inform messages is set to 1, once the first Inform messages is sent the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends a DHCP Discover message when the number of Discover messages is not set to 0. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

- When the number of DHCP Inform messages is set to 2, once the first Inform messages is sent, the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends another DHCP Inform message. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

Network discovery also stops when the DHCP server responds to DHCP Inform and Discover messages before the configured number of messages and timeout period are exceeded.

Setting the number of messages to 0 disables sending of DHCP Inform and Discover messages, and is the same as entering the **no ip dhcp-client network-discovery** command. When the **ip dhcp-client network-discovery**command is disabled, the system falls back to the static configurations made using the **async-bootp dns-server** and **async-bootp nb-server** global configuration commands or, as a last resort, to a DNS server address assigned with the **ip name-server** command.

Examples

The following example sets two DHCP Inform and Discovery messages and a timeout period of 12 seconds:

```
ip dhcp-client network-discovery informs 2 discovers 2 period 12
```

Related Commands

Command	Description
async-bootp	Configures extended BOOTP requests for asynchronous interfaces as defined in RFC 1084.
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip dhcp-client update dns

To enable Dynamic Domain Name System (DDNS) updates of address (A) Resource Records (RRs) using the same hostname passed in the hostname and fully qualified domain name (FQDN) options by a client, use the **ip dhcp-client update dns** command in global configuration mode. To disable dynamic updates, use the **no** form of this command.

ip dhcp-client update dns [**server** {**both** | **none**}]
no ip dhcp client update dns

Syntax Description

server	(Optional) Enables the Dynamic Host Control Protocol (DHCP) server to perform DDNS updates of forward or A RRs in the primary DNS server, unless the DHCP server reports in the ACK FQDN option that it has overridden the client request and updated this information previously. The keywords are as follows: • **both** --Enables the DHCP server to perform DDNS updates on both A (forward) and PTR (reverse) RRs in the primary DNS server unless the DHCP server has specified in the DHCP ACK FQDN option that it has overridden the client request and has updated the information previously. **Note** If the **both** keyword is specified, it means that the client will include an FQDN option specifying the S flag. This instructs the server that it should attempt to dynamically update both the A and PTR RRs. • **none** --On the client side, specifies that the DHCP client should include the FQDN option, however, it should not attempt any DDNS updates. On the server side, specifies that the client will include an FQDN option specifying the "N" flag. The server will not perform any DDNS updates for the client. The server can, of course, override this and do the updates anyway. **Note** If the **none** keyword is not specified, the FQDN option will result in the server updating the PTR RR and neither the server nor the client will update the A RR.

Command Default

No default behavior.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

Commands that are configured in interface configuration mode override the commands configured using global configuration mode. The **ip dhcp client update dns** command (no hyphen) is the interface configuration command.

If you specify the **both** and **none** keywords, the DHCP client will update both the A and PTR RRs, and the DHCP server will not perform any updates. The DHCP server can override the DHCP client using the **ip dhcp update dns override** command.

If you specify the **none** and **both** keywords (in this order), the DHCP client will not perform any updates and the server will update both the A and PTR RRs.

There are two parts to the DDNS update configuration on the client side. First, if the **ip ddns update method** command is configured on the client, which specifies the DDNS-style updates, then the client will be trying to generate or perform A updates. If the **ip ddns update method ddns both** command is configured, then the client will be trying to update both A and PTR RRs.

Second, the only way for the client to communicate with the server, with reference what updates it is generating or expecting the server to generate, is to include an FQDN option when communicating with the server. Whether or not this option is included is controlled on the client side by the **ip dhcp-client update dns** command in global configuration mode or the **ip dhcp client update dns** command in interface configuration mode.

If the FQDN option is included in the DHCP interaction, then the client may instruct the server to update "reverse" (the default), "both", or "none." Obviously, if the **ip ddns update method** command is configured with the **ddns both** keyword combination, then the FQDN option configuration should reflect an IP DHCP client update DNS server none, but you have to configure the system correctly.

Even if the client instructs the server to update both or update none, the server can override the client request and do whatever it was configured to do anyway. If there is an FQDN option in the DHCP interaction as above, then the server can communicate to the client that it was overridden, in which case the client will not perform the updates because it knows that the server has done the updates. Even if the server is configured to perform the updates after sending the ACK (the default), it can still use the FQDN option to instruct the client what updates it will be performing and thus the client will not do the same types of updates.

If the server is configured with the update dns command with or without any keywords, and if the server does not see an FQDN option in the DHCP interaction, then it will assume that the client does not understand DDNS and will automatically act as though it were configured to update both A and PTR RRs on behalf of the client.

Examples

The following example shows how to configure the DHCP server to perform A and PTR RR updates:

```
ip dhcp-client update dns server both
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

ip dhcp drop-inform

To drop DHCPINFORM messages, use the **ip dhcp drop-inform** command in global configuration mode. To send DHCPINFORM messages, use the **no** form of this command.

ip dhcp drop-inform
no ip dhcp drop-inform

Syntax Description

This command has no arguments or keywords.

Command Default

DHCPINFORM messages are not dropped.

Command Modes

Global configuration

Command History

Release	Modification
15.5(2)S	This command was introduced.

Usage Guidelines

This command implements DHCPINFORM as per the specifications given in RFC 2131.

If a client has obtained a network address through some other means (e.g., manual configuration), it may use a DHCPINFORM request message to obtain specific configuration parameters from the server.

Examples

The command in the following example drops DHCPINFORM messages:

```
Router(config)# ip dhcp drop-inform
```

ip dhcp-relay information option server-override

To enable the system to globally insert the server ID override and link selection suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp-relay information option server-override** command in global configuration mode. To disable inserting the server ID override and link selection suboptions into the DHCP relay agent information option, use the **no** form of this command.

ip dhcp-relay information option server-override
no ip dhcp-relay information option server-override

Syntax Description

This command has no arguments or keywords.

Command Default

The server ID override and link selection suboptions are not inserted into the DHCP relay agent information option.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp-relay information option server-override** command adds the following suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- Server ID override suboption
- Link selection suboption

When this command is configured, the gateway address (giaddr) will be set to the IP address of the outgoing interface, which is the interface that is reachable by the DHCP server.

If the **ip dhcp relay information option server-id-override** command is configured on an interface, it overrides the global configuration on that interface only.

Examples

In the following example, the DHCP relay will insert the server ID override and link selection suboptions into the relay information option of the DHCP packet. The loopback interface IP address is configured to be the source IP address for the relayed messages.

```
Device(config)# ip dhcp-relay information option server-override
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface Loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay information option server-id-override	Enables the system to insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

ip dhcp-relay source-interface

To globally configure the source interface for the relay agent to use as the source IP address for relayed messages, use the **ip dhcp-relay source-interface** command in global configuration mode. To remove the source interface configuration, use the **no** form of this command.

ip dhcp-relay source-interface *type number*
no ip dhcp-relay source-interface *type number*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

Command Default

The source interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp-relay source-interface** command allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface) for the relay agent to use as a source IP address for relayed messages.

If the **ip dhcp-relay source-interface** global configuration command is configured and the **ip dhcp relay source-interface** command is also configured, the **ip dhcp relay source-interface** command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

Examples

In the following example, the loopback interface IP address is configured to be the source IP address for the relayed messages:

```
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay source-interface	Configures the source interface for the relay agent to use as the source IP address for relayed messages.

ip dhcp-server

To use specific Dynamic Host Configuration Protocol (DHCP) servers on your network for address allocation, use the **ip dhcp-server** command in global configuration mode. To remove specific DHCP servers from being used on your network, use the **no** form of this command.

ip dhcp-server [**vrf** *vrf-name*] {*server-ip-address* | *server-name*}
no ip dhcp-server [**vrf** *vrf-name*] {*server-ip-address* | *server-name*}

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the virtual routing and forwarding (VRF) instance with which the DHCP server is associated. A VRF must be specified only if the DHCP server interface is associated with a VRF. The **ip dhcp-server vrf** command form can be used only when the device is used as an Intelligent Services Gateway (ISG) for sending lease queries. For basic DHCP client configuration (enabled using the command **ip address dhcp**), the **vrf** keyword is not needed.
server-ip-address	IP address of the DHCP server.
server-name	Name of the DHCP server.

Command Default

The IP limited broadcast address of 255.255.255.255 is used for transactions if no DHCP server is specified. This default setting allows automatic detection of DHCP servers.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.13	This command was integrated into Cisco IOS XE Release 3.13. The **vrf** *vrf-name* keyword-argument pair was added.

Usage Guidelines

A DHCP server temporarily allocates network addresses to clients through the access server on an as-needed basis. While the client is active, the address is automatically renewed in a minimum of 20-minute increments. When the user terminates the session, the interface connection is terminated so that network resources can be quickly reused. You can specify up to ten servers on the network.

In normal situations, if a SLIP or PPP session fails (for example, if a modem line disconnects), the allocated address will be reserved temporarily to preserve the same IP address for the client when dialed back into the server. This way, the session that was accidentally terminated can often be resumed.

To use the DHCP proxy-client feature, enable your access server to be a proxy-client on asynchronous interfaces by using the **ip address-pool dhcp-proxy-client** command. If you want to use specific DHCP servers on your network, use the **ip dhcp-server** command to define up to ten specific DHCP servers.



Note To facilitate transmission, configure intermediary devices (or access servers with router functionality) to use an IP helper address whenever the DHCP server is not on the local LAN and the access server is using broadcasts to interact with the DHCP server.

The **ip address-pool dhcp-proxy-client** command initializes proxy-client status to all interfaces defined as asynchronous on the access server. To selectively disable proxy-client status on a single asynchronous interface, use the **no peer default ip address** interface command.

Examples

The following command specifies a DHCP server with the IP address of 172.24.13.81:

```
ip dhcp-server 172.24.13.81
```

Related Commands

Command	Description
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
show cot dsp	Displays information about the COT DSP configuration or current status.

ip dhcp-server query lease

To change the default global retransmission scheme for Dynamic Host Configuration Protocol (DHCP) lease query packets, use the **ip dhcp-server query lease**command in global configuration mode. To remove this retransmission scheme and return to the default behavior, use the **no** form of this command.

ip dhcp-server query lease {**retries** *number* | **timeout** *seconds*}
no ip dhcp-server query lease {**retries** *number* | **timeout** *seconds*}

Syntax Description

retries *number*	The number of times the DHCP lease is transmitted following a timeout for an authoritative reply. The range is from 0 to 5. The default is 2 retries. A value of 0 means no retransmission (a single failure).
timeout *seconds*	The number of seconds to wait for a reply to a query. The range is from 1 to 60 seconds. The default is 5 seconds

Command Default

retries *number* : 2**timeout** *seconds*: 5

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The DHCP Lease Query protocol is a lightweight mechanism to query a DHCP server for certain information related to IP addresses leased from the DHCP server.

You can specify which DHCP servers to query by using the **ip dhcp-server** global configuration command. You can specify up to 10 servers on the network. Use the **ip dhcp-server query lease**global configuration command to change the default global retransmission scheme for lease query packets.

Examples

In the following example, the time to wait for a reply to a lease query is set to 15 seconds:

```
ip dhcp-server query lease timeout 15
```

In the following example, the retry number is set to 0, which means that only a single DHCP lease query will be transmitted for each DHCP server; no retries will be attempted.

```
ip dhcp-server query lease retries 0
```

Related Commands

Command	Description
ip dhcp-server	Specifies which DHCP server to use on your network.

ip dns name-list

To add a hostname pattern-matching rule to the end of a Domain Name System (DNS) name list, use the **ip dns name-list** command in global configuration mode. To remove a rule from a DNS name list or to remove an entire name-list, use the **no** form of this command.

ip dns name-list *name-list-number* {**deny** | **permit**} *pattern*
no ip dns name-list *name-list-number* [{**deny** | **permit**} *pattern*]

Syntax Description

name-list-number	Integer from 1 to 500 that identifies the DNS name list.
deny	Specifies that any name matching the specified pattern immediately terminates matching the name list with a negative result.
permit	Specifies that any name matching the specified pattern immediately terminates matching the name list with a positive result.
pattern	Regular expression, case-insensitive, to be compared to the a DNS query hostname.

Command Default

No DNS name list is defined or modified. The access list defaults to an implicit **deny .*** clause. The access list is always terminated by an implicit **deny .*** clause.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command adds a hostname pattern-matching rule to the end of the specified DNS name list. A DNS name list is identified by a unique *name-list-number* value and defines an ordered list of hostname pattern-matching rules that the Cisco IOS software can use to match hostnames in a DNS query.

If the DNS name list does not exist yet, it is automatically created.

When a DNS name list is used to determine if a DNS view list member can be used to handle an incoming DNS query, the individual deny and permit clauses function as follows:

- If the query hostname matches the pattern in a deny clause, the DNS view is rejected; the view-selection process moves on to the next member of the DNS view list.
- If the query hostname matches the pattern in a permit clause, the DNS view is selected to handle the query; the view-selection process is finished.
- There is an implicit deny statement at the end of the access list. If the view-selection process reaches the end of the DNS name list without either a deny clause that causes the view to be rejected or a permit clause that causes the view to be selected, the DNS view is rejected; the view-selection process moves onto the next member of the DNS view list.

For any DNS name list number, the **ip dns name-list** command can be entered multiple times to specify any number of pattern-matching rules in a single name list.

To display a particular DNS name list or all configured name lists, use the **show ip dns name-list** command.

Use of Pattern Matching Characters to Specify the Hostname Pattern

Any rule in a DNS name list can include Cisco regular expression pattern-matching characters in the regular expression that defines the hostname pattern. For a detailed description of regular expressions and regular expression pattern-matching characters, see the *Cisco IOS Terminal Services Configuration Guide* .

Use of a DNS Name List Definition

A DNS name list can be referenced by a DNS view list (accessed by using the **ip dns view-list** command), within a DNS view list member definition (accessed by using the **view** command) that has been configured to deny or permit the use of that DNS view for handling a given DNS query based on whether the destination hostname adheres to a particular DNS name list. To configure this type of usage restriction on the view list member, use the **restrict name-group** command.

Examples

The following example shows how to configure DNS name list number 9 so that the name list will be matched if the query hostname matches either www.example2.com or *.example3.com:

```
Router(config)# ip dns name-list 9 permit www.example2.com

Router(config)# ip dns name-list 9 permit .*.example3.org
```

Related Commands

Command	Description
debug ip dns name-list	Enables debugging output for DNS name list events.
ip dns name-list	Defines a list of pattern-matching rules in which each rule permits or denies the use of a DNS view list member to handle a DNS query based on whether the query hostname matches the specified regular expression.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
show ip dns name-list	Displays a particular DNS name list or all configured name lists.
view	Enters DNS view list member configuration mode so that usage restrictions can be configured for the view list member.

ip dns primary

To configure the router as authoritative for a zone, use the **ip dns primary** command in global configuration mode. To configure the router as nonauthoritative for a zone, use the **no** form of this command.

ip dns primary *domain-name* **soa** *primary-server-name mailbox-name* [*refresh-interval* [*retry-interval* [*expire-ttl* [*minimum-ttl*]]]]
no ip dns primary *domain-name*

Syntax Description

domain-name	Name of the Domain Name System (DNS).
soa	Start of authority record parameters.
primary-server-name	Authoritative name server.
mailbox-name	DNS mailbox of administrative contact.
refresh-interval	(Optional) Refresh time in seconds. This time interval must elapse between each poll of the primary by the secondary name server. The range is from 0 to 4294967295. The default is 21600 (6 hours).
retry-interval	(Optional) Refresh retry time in seconds. This time interval must elapse between successive connection attempts by the secondary to reach the primary name server in case the first attempt failed. The range is from 0 to 4294967295. The default is 900 (15 minutes).
expire-ttl	(Optional) Authority expire time in seconds. The secondary expires its data if it cannot reach the primary name server within this time interval. The range is from 0 to 4294967295. The default is 7776000 (90 days).
minimum-ttl	(Optional) Minimum Time to Live (TTL) in seconds for zone information. Other servers should cache data from the name server for this length of time. The range is from 0 to 4294967295. The default is 86400 (1 day).

Command Default

No authority record parameters are configured for the DNS name server, so queries to the DNS server for locally defined hosts will not receive authoritative responses from this server.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use this command to configure the router as an authoritative name server for the host table, or zone file, of a DNS domain. The primary name server name and a DNS mailbox name are required authority record parameters. Optionally, you can override the default values for the polling refresh interval, the refresh retry interval, the authority expire time, and the minimum TTL for zone information.

To display the authoritative name server configuration for the router, use the **show ip dns primary** command.

Examples

The following example shows how to configure the router as the primary DNS server authoritative for the example.com domain, or zone:

```
Router(config)# ip dns primary example.com soa ns1.example.com mb1.example.com
 10800
 900
 5184000
 172800
```

In the above example, the DNS domain name of the router is ns1.example.com, and the administrative contact for this zone is mb1@example.com. The refresh time is 3 hours, the refresh retry time is 15 minutes, the authority expire time is 60 days, and the minimum TTL is 2 days.

Related Commands

Command	Description
ip dns server	Enables the DNS server on a router.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
show ip dns primary	Displays the authoritative name server configuration for the router.

ip dns server

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

ip dns server
no ip dns server

Syntax Description

This command has no arguments or keywords.

Command Default

The DNS server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use this command to enable the DNS server as needed.

Examples

In the following example, the DNS server is enabled:

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

ip dns server queue limit

To configure a limit to the size of the queues used by the Domain Name System (DNS) server processes, use the **ip dns server queue limit**command in global configuration mode. To remove any limit on the queue, use the **no** form of this command.

ip dns server queue limit forwarder *queue-size-limit*
no ip dns server queue limit forwarder

Syntax Description

forwarder	Sets the queue limit for the forwarder queue.
queue-size-limit	Specifies the maximum size to be used for the queue. Valid range is from 0 to 1000000. Value 0 indicates no limit.

Command Default

The queue limit is set to 0, indicating there is no limit on the queue.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.4(24)T	The **director** keyword was removed.

Usage Guidelines

When a DNS query is forwarded to another nameserver for resolution, some memory space is held for the corresponding DNS query until an appropriate response is received or until there is a timeout. If the queries are being received at a very high rate, this may result in the free I/O memory getting exhausted.

Use the **ip dns server queue limit** command to set a limit to the size of the queue.

Examples

The following example shows how to set the limit to the forwarder queue used by the DNS server:

```
Router(config)# ip dns server queue limit forwarder 10
Router(config)#
```

Related Commands

Command	Description
show ip dns statistics	Displays packet statistics for the DNS server.

ip dns server view-group

To specify the default Domain Name System (DNS) server view list for the router, use the **ip dns server view-group** command in global configuration mode. To remove this definition, use the **no** form of this command.

ip dns server view-group *view-list-name*
no ip dns server view-group

Syntax Description

view-list-name	Name of a DNS view list. **Note** If the specified view list does not exist, a warning is displayed but the default view list setting is configured anyway. The specified view list can be defined after the default DNS server view list is configured.

Command Default

No default DNS view list is configured; incoming queries arriving on an interface not assigned a specific DNS view list will be handled using the global default view.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command configures the router to use the specified DNS server view list as the default DNS view list. The default DNS view list is used to determine which DNS view the router will use to handle a given incoming DNS query that arrives on an interface that is not configured with a DNS view list. The router checks these types of DNS queries against the DNS view list entries (in the order specified in the DNS view list) and uses the first DNS view list member whose restrictions allow the view to handle that query.

To specify that the router uses a particular DNS view list to choose the DNS view to use to handle incoming DNS queries that arrives on a specific interface, use the **ip dns view-group** command.

Note The *view-list-name* argument referenced in this command is configured using the **ip dns view-list** command. The DNS view list is referred to as a "view list" when it is defined and as a "view group" when it is referenced in other commands.

Examples

The following example shows how to configure the DNS name list userlist1 as the default name list:

```
Router(config)# ip dns server view-group userlist1
```

Related Commands

Command	Description
ip dns view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming DNS queries that arrive on a specific interface.
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

ip dns spoofing

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

ip dns spoofing [*ip-address*]
no ip dns spoofing [*ip-address*]

Syntax Description

ip-address	(Optional) IP address used in replies to DNS queries. **Note** You can specify an IPv4 or IPv6 address for DNS spoofing.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS 12.2(28)SB.
15.4(1)T	This command was modified. An IPv6 address can be specified for the *ip-address* argument.

Usage Guidelines

DNS spoofing allows a device to act as a proxy DNS server and "spoof" replies to any DNS queries using either the configured IP address in the **ip dns spoofing** command or the IP address of the incoming interface for the query. This functionality is useful for devices where the interface toward the ISP is not up. Once the interface to the ISP is up, the device forwards DNS queries to the real DNS servers.

The device will respond to the DNS query with the configured IP address when queried for any host name other than its own but will respond to the DNS query with the IP address of the incoming interface when queried for its own host name.

The host name used in the DNS query is defined as the exact configured host name of the device specified by the **hostname** command, with no default domain appended. For example, consider the following configuration:

```
ip domain name cisco.com
hostname host1
```

Here, the system would respond with a DNS spoofing reply if queried for "host1" but not for "host1.cisco.com".

Examples

In the following example, the device will respond to a DNS query with an IP address of 192.168.15.1:

```
Device(config)# ip dns spoofing 192.168.15.1
```

ip dns view

To access or create the Domain Name System (DNS) view of the specified name associated with the specified VPN routing and forwarding (VRF) instance and then enter DNS view configuration mode so that forwarding and routing parameters can be configured for the view, use the **ip dns view** command in global configuration mode. To remove the definition of the specified DNS view and then return to global configuration mode, use the **no** form of this command.

ip dns view [**vrf** *vrf-name*] {**default***view-name*}
no ip dns view [**vrf** *vrf-name*] {**default***view-name*}

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the VRF associated with the DNS view. Default is to associate the DNS view with the global VRF (that is, the VRF whose name is a NULL string). **Note** If the named VRF does not exist, a warning is displayed but the view is created anyway. The specified VRF can be defined after the DNS view is configured. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
default	Refers to the unnamed DNS view.
view-name	String (not to exceed 64 characters) that specifies the name of the DNS view. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.

Command Default

No new DNS view is accessed or created.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enters DNS view configuration mode--for the specified DNS view--so that forwarding parameters, resolving parameters, and the logging setting can be configured for that view. If the specified DNS view does not exist yet, it is automatically created.

Note The maximum number of DNS views and view lists supported is not specifically limited but is dependent on the amount of memory on the Cisco router. Configuring a larger number of DNS views and view lists uses more router memory, and configuring a larger number of views in the view lists uses more router processor time. For optimum performance, configure no more views and view list members than needed to support your Split DNS query forwarding or query resolution needs.

The default view associated with the unnamed global VRF exists by default. This is the view that is referenced by using the **ip dns view** command without specifying a VRF and specifying the **default** keyword instead of a *view-name* argument. The default DNS view cannot be removed.

Different DNS views can be associated with the same VRF.

To enable debugging output for DNS view events, use the **debug ip dns view** command.

To display information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used, use the **show ip dns view** command.

When you configure the **ip dns view ezvpn-internal-view** command, the command removes all saved configurations from the running configuration. This is because **ezvpn-internal-view** is a reserved DNS view for use on Easy VPN hardware clients, and is not intended to be modified. The configurations are removed when a Network Extension Mode (NEM) hardware client establishes an IPsec tunnel to the NEM server. The configuration remains until the IPsec tunnel is formed.

Subsequent Operations on a DNS View Definition

After you use the **ip dns view** command to define a DNS view and enter DNS view configuration mode, you can configure DNS forwarder parameters, DNS resolution parameters, and system message logging for the view.

To configure the Cisco IOS DNS forwarder functionality, use the following commands:

- **dns forwarder**
- **dns forwarding**
- **dns forwarding source interface**

To configure the Cisco IOS DNS resolver functionality, use the following commands:

- **domain list**
- **domain lookup**
- **domain multicast**
- **domain name**
- **domain name-server**
- **domain name-server interface**
- **domain retry**
- **domain round-robin**
- **domain timeout**

To enable logging of a system message logging (syslog) message each time the DNS view is used, use the **logging** command.

Use of a DNS View Definition

After a DNS view is configured, the view can be added to a DNS view list (by using the **ip dns view-list** command) and usage restrictions for that view within that view list can configured (by using the **restrict name-group** and **restrict source access-grou**p commands).

Examples

The following example shows how to define the default DNS view in the global address space. This DNS view exists by default, and it is the view that has been in use since before the Split DNS feature was implemented.

```
Router(config)# ip dns view default
```

The following example shows how to define the default DNS view associated with VRF vpn101, creating the view if it does not already exist:

```
Router(config)# ip dns view vrf vpn101 default
```

The following example shows how to define the DNS view user2 in the global address space, creating the view if it does not already exist:

```
Router(config)# ip dns view user2
```

The following example shows how to define the DNS view user2 associated with VRF vpn101, creating the view if it does not already exist:

```
ip dns view vrf vpn101 user2
```

Related Commands

Command	Description
debug ip dns view	Enables debugging output for DNS view events.
dns forwarder	Specifies the ordered list of IP addresses to use when forwarding incoming DNS queries handled using the DNS view.
dns forwarding	Enables forwarding of incoming DNS queries by the DNS view.
dns forwarding source-interface	Specifies the interface to use when forwarding incoming DNS queries handled using the DNS view.
domain list	Defines the ordered list of default domain names to use to complete unqualified hostnames in internally generated DNS queries handled using the DNS view.
domain lookup	Enables the IP DNS-based hostname-to-address translation for internally generated DNS queries handled using the DNS view.
domain multicast	Specifies the IP address to use for multicast lookups handled using the DNS view.
domain name	Specifies a single default domain name to use to complete unqualified hostnames in internally generated DNS queries handled using the DNS view.

Command	Description
domain name-server	Specifies the ordered list of IP addresses to use when resolving internally generated DNS queries handled using the DNS view.
domain name-server interface	Specifies the interface from which the device can learn (through either DHCP or PPP interaction on the interface) a DNS resolving name server address for the DNS view.
domain retry	Specifies the number of times to retry sending or forwarding a DNS query handled using the DNS view.
domain round-robin	Enables round-robin rotation of multiple IP addresses in the global or VRF-specific DNS hostname cache during the TTL of the cache each time DNS lookup is performed to resolve an internally generated DNS query handled using the DNS view.
domain timeout	Specifies the amount of time to wait for a response to a sent or forwarded DNS query handled using the DNS view.
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
logging	Enables logging of a syslog message each time the DNS view is used.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

ip dns view-group

To attach a Domain Name System (DNS) view list to the interface, use the **ip dns view-group** command in interface configuration mode. To disable the attachment of a DNS view list to an interface, use the **no** form of this command.

ip dns view-group *view-list-name*
no ip dns view-group *view-list-name*

Syntax Description

view-list-name	Name of an existing DNS view list. **Note** If the specified view list does not exist, a warning is displayed and the view list setting is not configured for the interface.

Command Default

No DNS view list is attached to the interface. If a default DNS view list is configured, that view list is used to handle incoming DNS queries. If no view list has been configured either on this specific interface or for the system, incoming DNS queries are handled using the default global view.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command configures the router to use the specified DNS view list to choose which DNS view to use to handle incoming DNS queries that arrive on the interface.

Only one DNS view list can be assigned to a given interface. However, a single DNS view list can be assigned to any number of interfaces so that the same ordered list of DNS views (along with the restrictions specified in the view list) can be checked by multiple interfaces.

A DNS view list can also be configured as the default DNS view list (by using the **ip dns server view-group** command) to determine which DNS view the router will use to handle a given incoming DNS query that arrives on an interface that is not configured with a DNS view list.



Note The *view-list-name* argument referenced in this command is configured using the **ip dns view-list** command. The DNS view list is referred to as a "view list" when it is defined and as a "view group" when it is referenced in other commands.

When an incoming DNS query is received through the interface, the Cisco IOS software will check the members of the DNS view list--in the order specified in the view list--to determine if the usage restrictions on any view list member allow the view to be used to forward the incoming query:

- Each DNS view list member is checked, in the order specified by the list.

- The first DNS view in the view list with configured usage restrictions (based on the query destination hostname or the query source IP address) that allow its use for the query will be used to forward the incoming query.

If the hostname cache for the view contains the information needed to answer the query, the router will respond to the query with the hostname IP address in that internal cache. Otherwise, provided DNS forwarding is enabled for the DNS view, the router will forward the query to the configured name servers (each in turn, until a response is received), and the response will be both added to the hostname cache and sent back to the originator of the query.

- If no DNS view in the DNS view list is qualified to handle the query, the router drops the query.

Examples

The following example shows how to configure the router so that each time a DNS query arrives through interface ethernet0 the usage restrictions for the members of the DNS view list userlist2 are checked in the order specified by the view list definition. The router uses the first view list member whose usage restrictions allow that DNS view to forward the query.

```
Router(config)# interface ethernet0

Router(config-if)# ip dns view-group userlist2
```

Related Commands

Command	Description
interface	Selects an interface to configure.
ip dns server view-group	Specifies the DNS view list to use to determine which DNS view to use handle incoming queries that arrive on an interface not configured with a DNS view list.
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

ip dns view-list

To access or create the Domain Name System (DNS) view list of the specified name and then enter DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS view members, use the **ip dns view-list** command in global configuration mode. To remove the definition of the specified DNS view list, use the **no** form of this command.

ip dns view-list *view-list-name*
no dns view-list *view-list-name*

Syntax Description

view-list-name	Text string (not to exceed 64 characters) that uniquely identifies the DNS view list to be created.

Command Default

No DNS view list is accessed or created.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enters DNS view list configuration mode--for the specified view list--so that individual view list members (DNS views and their order numbers within the view list) can be accessed in, added to, or deleted from that view list. If the specified DNS view list does not exist yet, it is automatically created.

Note The maximum number of DNS views and view lists supported is not specifically limited but is dependent on the amount of memory on the Cisco router. Configuring a larger number of DNS views and view lists uses more router memory, and configuring a larger number of views in the view lists uses more router processor time. For optimum performance, configure no more views and view list members than needed to support your Split DNS query forwarding or query resolution needs.

To display information about a specific DNS view list or all currently configured DNS view lists, use the **show ip dns view-list** command.

Subsequent Operations on a DNS View List

After you use the **ip dns view-list** command to define a DNS view list and enter DNS view list configuration mode, you can use the **view** command to access a view list member or add a DNS view as a new view list member at the end of the list. Each view list member specifies a DNS view and a value that indicates the relative order for checking that view when the DNS view list is used. to determine if it can be used to address a DNS query.

For any DNS view list member, you can use the **restrict authenticated**, **restrict name-group**, and **restrict source access-group** commands to configure usage restrictions for the DNS view list member. These restrictions are based on query source authentication, the query hostname, and the query source host IP address, respectively.

Purpose of a DNS View List

When a DNS view list is used to select a DNS view to use to handle a given DNS query, the Cisco IOS software checks each DNS view in the DNS view list--in the order specified in the view list--to determine if the usage restrictions for that view allow the view to be used to address that particular DNS query.

The first DNS view with configured usage restrictions that allow its use for the DNS query will be used to resolve or forward the query. That is, the router will use the configuration parameters for that DNS view to either respond to the query (by using the name cache belonging to the DNS view) or forward the query to the configured name servers. If no DNS view in the view list is qualified to handle the query, the router does not send or forward the query.

Note Multiple DNS view list definitions enable you to use the same DNS view, but with different restrictions, depending on the source of the DNS query being processed. For example, in one DNS view list a particular DNS view could be used with very few usage restrictions, while in another DNS view list the same DNS view could be used with more usage restrictions.

Use of a DNS View List for DNS Queries Incoming from a Particular Interface

Use the **ip dns view-group** command to configure the router to use a particular DNS view list to determine which DNS view to use to handle incoming DNS queries that arrive on that interface. Only one DNS view list can be assigned to a given interface. However, a single DNS view list can be assigned to any number of interfaces so that the same ordered list of DNS views (along with the restrictions specified in the view list) can be checked by multiple interfaces.

Use of a DNS View List as the Default DNS View List

Use the **ip dns server view-list** command to configure the default DNS view list. The router uses the default DNS view list to determine which DNS view to use to handle incoming DNS queries that arrive on an interface that is not configured with a DNS view list.

Examples

The following example shows how to remove the DNS view user1 from the DNS view list userlist5 and then add the view back to the view list, but with a different position indicator specified for that member within the view list. A usage restriction is also added to the view list member user1.

```
Router(config)# ip dns view-list userlist5

Router(cfg-dns-view-list)# no view user1 30

Router(cfg-dns-view-list)# view user1 10

Router(cfg-dns-view-list)# restrict name-group 7
```

Related Commands

Command	Description
debug ip dns view-list	Enables debugging output for DNS view list events.
ip dns server view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming queries that arrive on an interface not configured with a DNS view list.

Command	Description
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.
ip dns view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming DNS queries that arrive on a specific interface.
restrict authenticated	Restricts the use of the DNS view list member to DNS queries for which the DNS query host can be authenticated.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.
view	Enters DNS view list member configuration mode so that usage restrictions can be configured for the view list member.

ip domain list

To define a list of default domain names to complete unqualified names, use the **ip domain list** command in global configuration mode. To delete a name from a list, use the no form of this command.

ip domain list [**vrf** *vrf-name*] *name*
no ip domain list [**vrf** *vrf-name*] *name*

Syntax Description

vrf *vrf-name*	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
name	Domain name. Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No domain names are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The syntax of the command changed from **ip domain-list** to **ip domain list**.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If there is no domain list, the domain name that you specified with the **ip domain name** global configuration command is used. If there is a domain list, the default domain name is not used. The **ip domain list** command is similar to the **ip domain name** command, except that with the **ip domain list**command you can define a list of domains, each to be tried in turn until the system finds a match.

If the **ip domain list vrf** command option is specified, the domain names are only used for name queries in the specified VRF.

The Cisco IOS software will still accept the previous version of the command, **ip domain-list**.

Examples

The following example shows how to add several domain names to a list:

```
ip domain list company.com
ip domain list school.edu
```

The following example shows how to add several domain names to a list in vpn1 and vpn2:

```
ip domain list vrf vpn1 company.com
ip domain list vrf vpn2 school.edu
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain lookup

To enable IP Domain Name System (DNS)-based hostname-to-address translation, use the **ip domain lookup** command in global configuration mode. To disable DNS-based hostname-to-address translation, use the **no** form of this command.

ip domain lookup [**nsap** | **recursive** | [**vrf** *vrf-name*] [**source-interface** *interface-type interface-number*]]
no ip domain lookup [**nsap** | **recursive** | [**vrf** *vrf-name*] [**source-interface** *interface-type interface-number*]]

Syntax Description

nsap	(Optional) Enables IP DNS queries for Connectionless Network Service (CLNS) and Network Service Access Point (NSAP) addresses.
recursive	(Optional) Enables IP DNS recursive lookup.
vrf *vrf-name*	(Optional) Defines a Virtual Routing and Forwarding (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
source-interface	(Optional) Specifies the source interface for the DNS resolver.
interface-type interface-number	(Optional) The type of interface and the interface number.

Command Default

IP DNS-based hostname-to-address translation is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2	This command was modified. The syntax of the command changed from **ip domain-lookup** to **ip domain lookup**.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The **nsap** keyword was added.
Cisco IOS XE Release 3.10S	This command was modified. The **vrf** keyword and the *vrf-name* argument were added.

Release	Modification
Cisco IOS XE Dublin 17.12.1	In previous releases, the **ip domain lookup source-interface** configuration would be removed if the configured source-interface went down or if the interface experienced flap. The removal of the configuration was done programmatically without admin notification. Starting from the Cisco IOS XE Dublin 17.12.x release, the configuration remains intact when the configured interface goes down or experiences a flap.

Usage Guidelines

If the **ip domain lookup** command is enabled on a device, and you execute the **show tcp brief** command, the output may be displayed very slowly. With both IP and ISO CLNS enabled on a device, the **ip domain lookup nsap** command allows you to discover a CLNS address without having to specify a full CLNS address, given a hostname. The **ip domain lookup** command is useful for the **ping** (ISO CLNS) command, and for CLNS Telnet connections.

When configuring the **ip domain lookup source-interface** command, the user must ensure that the interface is in an up state for DNS functionality to work correctly. If the interface is in a down state or if the interface is removed, DNS queries that rely on this configuration will not work as expected.

Examples

The following example shows how to configure IP DNS-based hostname-to-address translation:

```
Device> enable
Device# configure terminal
Device(config)# ip domain lookup
Device(config)# end
```

The following example shows how to configure IP DNS-based hostname-to-address translation for a specified VRF and interface:

```
Device> enable
Device# configure terminal
Device(config)# ip domain lookup vrf RED source-interface ethernet 1/2
Device(config)# end
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
show tcp brief	Displays a concise description of TCP connection endpoints.

ip domain multicast

To create a domain prefix for Domain Name Service (DNS)-based Source Specific Multicast (SSM) mapping, use the **ip domain multicast** command in global configuration mode. To revert to the default domain prefix, use the **no** form of this command.

ip domain multicast *domain-prefix*
no ip domain multicast *domain-prefix*

Syntax Description

domain-prefix	Name of the domain prefix to be used for DNS-based SSM mapping.

Command Default

By default, the ip-addr.arpa domain is used as the domain prefix.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

When a device attempts DNS-based SSM mapping for an IP group address (G = G1.G2.G3.G4), the device queries the domain name server for IP address resource records (DNS record type ‘A’) for the domain G4.G3.G2.G1 *domain-prefix*.

Examples

The following example shows you how to create a domain prefix for DNS-based SSM mapping:

```
ip domain multicast ssm-map.cisco.com
```

Related Commands

Command	Description
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain name

To define a default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name), use the **ip domain name** command in global configuration mode. To disable use of the Domain Name System (DNS), use the noform of this command.

ip domain name [**vrf** *vrf-name*] *name*
no ip domain name [**vrf** *vrf-name*] *name*

Syntax Description

vrf *vrf-name*	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
name	Default domain name used to complete unqualified hostnames. Do not include the initial period that separates an unqualified name from the domain name.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The syntax of the command changed from **ip domain-name**to **ip domain name**.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Any IP hostname that does not contain a domain name (that is, any name without a dot) will have the dot and cisco.com appended to it before being added to the host table.

If the **ip domain name vrf** command option is specified, the domain names are only used for name queries in the specified VRF.

The Cisco IOS software will still accept the previous version of the command, which is **ip domain-name**.

Examples

The following example shows how to define cisco.com as the default domain name:

```
ip domain name cisco.com
```

The following example shows how to define cisco.com as the default domain name for vpn1:

```
ip domain name vrf vpn1 cisco.com
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain recursive

To enable recursive DNS querying for a device, use the **ip domain recursive** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip domain recursive {**allow-soa** | **retry** *maximum-referral-value*}
no ip domain recursive {**allow-soa** | **retry** *maximum-referral-value*}

Syntax Description

allow-soa	Treats a recursive DNS query response from an authoritative name server containing a start of authority (SOA) record as a referral.
retry *maximum-referral-value*	Configures the maximum number of retries for a DNS recursive query. The default value is 10.

Command Default

Recursive DNS querying is disabled for a device.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.12S	This command was introduced in a release earlier than Cisco IOS XE Release 3.12S.

Usage Guidelines

Examples

The following example shows you how to enable recursive DNS querying for a device and set a value for the maximum number of retries for a DNS recursive query:

```
Device> enable
Device# configure terminal
Device(config)# ip domain recursive retry 11
Device(config)# end
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain multicast	Creates a domain prefix for DNS-based SSM mapping.
ip domain retry	Specifies the number of times to retry sending DNS queries.

ip domain retry

To specify the number of times to retry sending Domain Name System (DNS) queries, use the **ip domain retry**command in global configuration mode. To return to the default behavior, use the no form of this command.

ip domain retry *number*
no ip domain retry *number*

Syntax Description

number	Number of times to retry sending a DNS query to the DNS server. The range is from 0 to 100; the default is 2.

Command Default

number : 2 times

Command Modes

Global configuration

Command History

Release	Modification
12.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **ip domain retry** command is not configured, the Cisco IOS software will only send DNS queries out twice.

Examples

The following example shows how to configure the router to send out 10 DNS queries before giving up:

```
ip domain retry 10
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified host names.
ip domain lookup	Enables the IP DNS-based host name-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain round-robin

To enable round-robin functionality on DNS servers, use the **ip domain round-robin**command in global configuration mode. To disable round-robin functionality, use the no form of the command.

ip domain round-robin
no ip domain round-robin

Syntax Description

This command has no arguments or keywords.

Command Default

Round robin is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In a multiple server configuration without the DNS round-robin functionality, the first host server/IP address is used for the whole time to live (TTL) of the cache, and uses the second and third only in the event of host failure. This behavior presents a problem when a high volume of users all arrive at the first host during the TTL time. The network access server (NAS) then sends out a DNS query; the DNS servers reply with a list of the configured IP addresses to the NAS. The NAS then caches these IP addresses for a given time (for example, five minutes). All users that dial in during the five minute TTL time will land on one host, the first IP address in the list.

In a multiple server configuration with the DNS round-robin functionality, the DNS server returns the IP address of all hosts to rotate between the cache of host names. During the TTL of the cache, users are distributed among the hosts. This functionality distributes calls across the configured hosts and reduces the amount of DNS queries.

Examples

The following example allows a Telnet to www.company.com to connect to each of the three IP addresses specified in the following order: the first time the Telnet command is given, it would connect to 10.0.0.1; the second time the command is given, it would connect to 10.1.0.1; and the third time the command is given, it would connect to 10.2.0.1. In each case, the other two addresses would also be tried if the first one failed; this is the normal operation of the Telnet command.

```
ip host www.server1.com 10.0.0.1 10.1.0.1 10.2.0.1
ip domain round-robin
```

ip domain timeout

To specify the amount of time to wait for a response to a DNS query, use the **ip domain timeout**command in global configuration mode. To return to the default behavior, use the no form of this command.

ip domain timeout *seconds*
no ip domain timeout *seconds*

Syntax Description

seconds	Time, in seconds, to wait for a response to a DNS query. The range is from 0 to 3600; the default is 3.

Command Default

seconds : 3 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **ip domain timeout** command is not configured, the Cisco IOS software will only wait 3 seconds for a response to a DNS query.

Examples

The following example shows how to configure the router to wait 50 seonds for a response to a DNS query:

```
ip domain timeout 50
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified host names.
ip domain lookup	Enables the IP DNS-based host name-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip gratuitous-arps

To enable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in an address pool if the transmission has been disabled, use the **ip gratuitous-arps** command in global configuration mode. To disable the transmission, use the **no**form of this command.

ip gratuitous-arps [**non-local**]
no ip gratuitous-arps

Syntax Description

non-local	(Optional) Sends gratuitous ARP messages if a client receives an IP address from a non-local address pool. Gratuitous ARP messages for locally originated peer addresses are not sent by default.

Command Default

Gratuitous ARP messages are not sent out when the client receives the address from the local address pool.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2T	The **non-local** keyword was added and the default behavior of the command changed.
12.4(2)T	The name of this command was changed from **no ip gratuitous-arps** to **ip gratuitous-arps**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

A Cisco router will send out a gratuitous ARP message out of all interfaces when a client connects and negotiates an address over a PPP connection. However, by default, gratuitous ARP messages are not sent out when the client receives the address from the local address pool. The **ip gratuitous-arps non-local** command option is the default form and is not saved in the running configuration.

Cisco 10000 Series Router

To maximize the performance of the router, disable gratuitous ARP requests using the **no ip gratuitous-arps** command.

Examples

The following example enables the sending of gratuitous ARP messages if the transmission has been disabled:

```
ip gratuitous-arps
```

ip host

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

ip host [**vrf** *vrf-name*] [**view** *view-name*] {*hostname* | **t** *modem-telephone-number*} [*tcp-port-number*] {*ip-address1* [*ip-address2* . . . *ip-address8*] | **additional** *ip-address9* [*ip-address10* . . . *ip-addressn*] | [**mx** *preference mx-server-hostname* | **ns** *nameserver-hostname* | **srv** *priority weight port target*]}
no ip host [**vrf** *vrf-name*] [**view** *view-name*] {*hostname* | **t** *modem-telephone-number*} [*tcp-port-number*] {*ip-address1* [*ip-address2* . . . *ip-address8*] **additional** *ip-address9* [*ip-address10* . . . *ip-addressn*] | [**mx** *preference mx-server-hostname* | **ns** *nameserver-hostname* | **srv** *priority weight port target*]}

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VRF) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache is to store the mappings. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
view *view-name*	(Optional) The *view-name* argument specifies the name of the DNS view whose hostname cache is to store the mappings. Default is the default DNS view associated with the specified or global VRF. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
hostname	Name of the host. The first character can be either a letter or a number. If you use a number, the types of operations you can perform (such as ping) are limited.
t *modem-telephone-number*	Modem telephone number that is mapped to the IP host address for use in Cisco modem user interface mode. You must enter the letter "t" before the telephone number. **Note** This argument is not relevant to the Split DNS feature.
tcp-port-number	(Optional) TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command. The default is Telnet (port 23).
ip-address1	Associated host IP address. **Note** You can specify an IPv4 or IPv6 address for the host IP address and additional IP addresses.

ip-address2 ...ip-address8	(Optional) Up to seven additional associated IP addresses, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.
additional *ip-address9*	The *ip-address9* argument specifies an additional IP address to add to the hostname cache. **Note** The use of the optional additional keyword enables the addition of more than eight IP addresses to the hostname cache.
ip-address10 ...ip-addressn	(Optional) Additional associated IP addresses, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.
mx *preference mx-server-hostname*	(Optional) Mail Exchange (MX) resource record settings for the host: • *preference* --The order in which mailers select MX records when they attempt mail delivery to the host. The lower this value, the higher the host is in priority. Range is from 0 to 65535. • *mx-server-hostname* --The DNS name of the Simple Mail Transfer Protocol (SMTP) server where the mail for a domain name should be delivered. An MX record specifies how you want e-mail to be accepted for the domain specified in the *hostname* argument. **Note** You can have several MX records for a single domain name, and they can be ranked in order of preference.
ns *nameserver-hostname*	(Optional) Name Server (NS) resource record setting for the host: • *nameserver-hostname* --The DNS name of the machine that provides domain service for the particular domain. Machines that provide name service do not have to reside in the named domain. An NS record lists the name of the machine that provides domain service for the domain indicated by the *hostname* argument. **Note** For each domain you must have at least one NS record. NS records for a domain must exist in both the zone that delegates the domain and in the domain itself.

srv *priority weight port target*	(Optional) Server (SRV) resource record settings for the host: • *priority* --The priority to give the record among the owner SRV records. Range is from 0 to 65535. • *weight* --The load to give the record at the same priority level. Range is from 0 to 65535. • *port* --The port on which to run the service. Range is from 0 to 65535. • *target* --Domain name of host running on the specified port. The use of SRV records enables administrators to use several servers for a single domain, to move services from host to host with little difficulty, and to designate some hosts as primary servers for a service and others as backups. Clients ask for a specific service or protocol for a specific domain and receive the names of any available servers.

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The **mx** keyword and the *preference* and *mx-server-hostname* arguments were added.
12.0(7)T	The **srv** keyword and the *priority*, *weight*, *port*, and *target* arguments were added.
12.2(1)T	The **ns** keyword and the *nameserver-hostname* argument were added.
12.4(4)T	The capability to map a modem telephone number to an IP host was added for the Cisco modem user interface feature.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS 12.2(33)SRA.
12.2SX	This command is integrated into Cisco IOS 12.2SX.
15.4(1)T	This command was modified. An IPv6 address can be specified for the *ip-address* argument, and the **additional** *ip-address* keyword-argument pair.

Usage Guidelines

This command adds the specified hostname-to-IP address mappings as follows:

- If no VRF name and no DNS view name is specified, the mappings are added to the global hostname cache.
- Otherwise, the mappings are added to the DNS hostname cache for a specific DNS view:
  - If only a DNS view name is specified, the specified mappings are created in the view-specific hostname cache.

- If only a VRF name is specified, the specified mappings are created in the VRF-specific hostname cache for the default view.
- If both a VRF name and a DNS view name are specified, the specified mappings are created in the VRF-specific hostname cache for the specified view.

If the specified VRF does not exist yet, a warning is displayed and the entry is added to the hostname cache anyway.

If the specified view does not exist yet, a warning is displayed and the entry is added to the hostname cache anyway.

If the hostname cache does not exist yet, it is automatically created.

To specify the machine that provides domain service for the domain, use the **ns** keyword and the *nameserver-hostname* argument

To specify where the mail for the host is to be sent, use the **mx** keyword and the *preference* and *mx-server-hostname* arguments.

To specify a host that offers a service in the domain, use the **srv** keyword and the *priority*, *weight*, *port*, and *target* arguments.

To display the display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views, use the **show hosts** command.



Note If a global or VRF-specific DNS hostname cache contains hostnames that are associated with multiple IP addresses, round-robin rotation of the returned addresses can be enabled on a DNS view-specific basis (by using the **domain round-robin** command).

Examples

The following example shows how to add three mapping entries to the global hostname cache and then remove one of those entries from the global hostname cache:

```
Device(config)# ip host www.example1.com 192.0.2.141 192.0.2.241

Device(config)# ip host www.example2.com 192.0.2.242

Device(config)# no ip host www.example1.com 192.0.2.141
```

The following example shows how to add three mapping entries to the hostname cache for the DNS view user3 that is associated with the VRF vpn101 and then remove one of those entries from that hostname cache:

```
Device(config)# ip host vrf vpn101 view user3 www.example1.com 192.0.2.141 192.0.2.241

Device(config)# ip host vrf vpn101 view user3 www.example2.com 192.0.2.242

Device(config)# no ip host vrf vpn101 view user3 www.example1.com 192.0.2.141
```

Related Commands

Command	Description
clear host	Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all DNS views.
domain round-robin	Enables round-robin rotation of multiple IP addresses in the global or VRF-specific DNS hostname cache during the TTL of the cache each time DNS lookup is performed to resolve an internally generated DNS query handled using the DNS view.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

ip host-list

To specify a list of hosts that will receive Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs) and to enter host-list configuration mode, use the **ip host-list**command in global configuration mode. To disable the host list, use the **no** form of this command.

ip host-list *host-list-name* [**vrf** *vrf-name*]
no ip host-list *host-list-name* [**vrf** *vrf-name*]

Syntax Description

host-list-name	List of servers that will receive DDNS updates.
vrf *vrf-name*	(Optional) Identifies the virtual routing and forwarding (VRF) table. The *vrf-name* argument identifies the address pool to which the VRF is associated.

Command Default

No IP host list is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

The interface configuration overrides the global configuration.

Examples

The following example shows how to configure a list of hosts:

```
ip host-list test
 host vrf testgroup
```

Related Commands

Command	Description
host (host-list)	Specifies a list of hosts that will receive DDNS updates of A and PTR RR.

ip hostname strict

To ensure that Internet hostnames comply with Section 2.1 of RFC 1123, use the **ip hostname strict** command in global configuration mode. To remove the restriction on hostnames, use the **no** form of this command.

ip hostname strict
no ip hostname strict

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default, that is, characters that are not specified in Section 2.1 of RFC 1123 are allowed in hostnames.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2SR	This command was introduced.

Usage Guidelines

Section 2.1 of RFC 1123 specifies the following rules for hostnames:

- A hostname is composed of one or more labels, separated by periods.
- Each label is composed of one or more of the following characters: letters (A-Z, a-z), digits (0-9), and the hyphen (-). No other characters are allowed.
- Alphabetic characters in hostnames can be either uppercase or lowercase, in any combination.
- A hyphen cannot be the first character of any label.
- The most significant label (also described as the top-level domain or TLD), that is, the group of characters that follow the final dot of the domain name, must contain at least one letter or hyphen, and must have least two characters.
- A hostname, including the periods, cannot have more than 255 characters. However, hostnames should not exceed 63 characters because conforming applications might be unable to handle hostnames longer than that.

The following hostnames comply with Section 2.1 of RFC 1123:

- • Name.Example.COM
  • XX
  • 3.example.org
  • 4-.5.9.1.6.US

The following hostnames do not comply with Section 2.1 of RFC 1123:

- • Name.Example.a The TLD “a” is too short.
  • Name.-e.com A label cannot start with “-”.
  • Name_Example.Example.COM “_” is not a valid character.
  • Name.Example..com A label must be at least one character.
  • Example.com. A label must be at least one character.

When the **ip hostname strict** command is configured on a router, any hostname configured on the router must comply with Section 2.1 of RFC 1123, including the following configurations:

- • Router(config)# **hostname router1**
  • Router(config)# **ip domain name domainname1.com**
  • Router(config)# **ip domain list list1.com**
  • Router(config)# **ip host host.example.com 10.0.0.1**
  • Router(config)# **ipv6 host a.example.com 1000::1**

When the **ip hostname strict** command is not configured on a router, characters that are not specified in Section 2.1 of RFC 1123 are allowed in hostnames.

Examples

The following example shows how to specify compliance with Section 2.1 of RFC 1123 for hostnames.

```
Router(config)# ip hostname strict
```

Related Commands

Command	Description
hostname	Defines the hostname for a network server.
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain name	Defines a default domain name to complete unqualified hostnames.
ip host	Defines static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view.
ipv6	Defines a static hostname-to-address mapping in the hostname cache.

ip local-proxy-arp

To enable the local proxy Address Resolution Protocol (ARP) feature, use the **ip local-proxy-arp** command in interface configuration mode. 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

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5c)EX	This command was introduced on the Catalyst 6500 series switches.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E on the Catalyst 6500 series switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The local proxy ARP feature allows the Multilayer Switching Feature Card (MSFC) to respond to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, the MSFC responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the Catalyst 6500 series switch on which they are connected.

Before the local proxy ARP feature can be used, the IP proxy ARP feature must be enabled. The IP proxy ARP feature is enabled by default.

Internet Control Message Protocol (ICMP) redirects are disabled on interfaces where the local proxy ARP feature is enabled.

Examples

The following example shows how to enable the local proxy ARP feature:

```
ip local-proxy-arp
```

ip mobile arp

To enable local-area mobility, use the **ip mobile arp** command in interface configuration mode. To disable local-area mobility, use the **no** form of this command.

ip mobile arp [**timers** *keepalive hold-time*] [**access-group** *access-list-numbername*]
no ip mobile arp

Syntax Description

timers	(Optional) Sets local-area mobility timers.
keepalive	(Optional) Frequency, in minutes, at which the Cisco IOS software sends unicast Address Resolution Protocol (ARP) messages to a relocated host to verify that the host is present and has not moved. The default value is 5.
hold-time	(Optional) Hold time, in minutes. This is the length of time the software considers that a relocated host is present without receiving some type of ARP broadcast or unicast from the host. Normally, the hold time should be at least three times greater than the keepalive time. The default value is 15.
access-group	(Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.
access-list-number	(Optional) Number of a standard IP access list. The range is from 1 to 99. Only hosts with addresses permitted by this access list are accepted for local-area mobility.
name	(Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Command Default

Local-area mobility is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 2.5.1	This command was integrated into Cisco IOS XE Release 2.5.1. VRF-awareness for local-area mobility is available in this release.

Usage Guidelines

Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces only.

To create larger mobility areas, you must first redistribute the mobile routes into your Interior Gateway Protocol (IGP). The IGP must support host routes. You can use Enhanced IGRP, Open Shortest Path First (OSPF), or

Intermediate System-to-Intermediate System (IS-IS); you can also use Routing Information Protocol (RIP), but RIP is not recommended. The mobile area must consist of a contiguous set of subnets.

Using an access list to control the list of possible mobile nodes is strongly encouraged. Without an access list, misconfigured hosts can be mistaken for mobile nodes and disrupt normal operations.

Examples

The following example shows how to configure local-area mobility on Ethernet interface 0:

```
access-list 10 permit 10.92.37.114
 interface ethernet 0
 ip mobile arp access-group 10
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
default-metric (BGP)	Sets default metric values for the BGP, OSPF, and RIP routing protocols.
default-metric (OSPF)	Sets default metric values for OSPF.
default-metric (RIP)	Sets default metric values for RIP.
network (BGP)	Specifies the list of networks for the BGP routing process.
network (IGRP)	Specifies a list of networks for the IGRP or Enhanced IGRP routing process.
network (RIP)	Specifies a list of networks for the RIP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
router eigrp	Configures the IP Enhanced IGRP routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process for IP.
router ospf	Configures an OSPF routing process.

ip name-server

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

ip name-server [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]
no ip name-server [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]

Syntax Description

vrf *vrf-name*	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
server-address1	IPv4 or IPv6 addresses of a name server.
server-address2...server-address6	(Optional) IP addresses of additional name servers (a maximum of six name servers).

Command Default

No name server addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(2)T	Support for IPv6 addresses was added.
12.0(21)ST	Support for IPv6 addresses was added.
12.0(22)S	Support for IPv6 addresses was added.
12.2(14)S	Support for IPv6 addresses was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following example shows how to specify IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers:

```
ip name-server 172.16.1.111 172.16.1.2
```

This command will be reflected in the configuration file as follows:

```
ip name-server 172.16.1.111
ip name-server 172.16.1.2
```

The following example shows how to specify IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers for vpn1:

```
Router(config)# ip name-server vrf vpn1 172.16.1.111 172.16.1.2
```

The following example shows how to specify IPv6 hosts 3FFE:C00::250:8BFF:FEE8:F800 and 2001:0DB8::3 as the name servers:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800 2001:0DB8::3
```

This command will be reflected in the configuration file as follows:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800
ip name-server 2001:0DB8::3
```

Related Commands

Command	Description
ip domain-lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain-name	Defines a default domain name to complete unqualified hostnames (names without a dotted decimal domain name).

ip nat

To designate that traffic originating from or destined for the interface is subject to Network Address Translation (NAT), to enable NAT logging, or to enable static IP address support, use the **ip nat**command in interface configuration mode. To prevent the interface from being able to translate or log, use the **no** form of this command.

ip nat [{**inside** | **outside**} | **log** | **translations** | **syslog** | **allow-static-host**]
no ip nat [{**inside** | **outside**} | **log** | **translations** | **syslog** | **allow-static-host**]

Syntax Description

inside	(Optional) Indicates that the interface is connected to the inside network (the network subject to NAT translation).
outside	(Optional) Indicates that the interface is connected to the outside network.
log	(Optional) Enables NAT logging.
translations	(Optional) Enables NAT logging translations.
syslog	(Optional) Enables syslog for NAT logging translations.
allow-static-host	(Optional) Enables static IP address support for NAT translation.

Command Default

Traffic leaving or arriving at this interface is not subject to NAT.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(2)XE	The **allow-static-host** keyword was added.
12.3(7)T	This command was implemented in Cisco IOS Release 12.3(7)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Only packets moving between inside and outside interfaces can be translated. You must specify at least one inside interface and outside interface for each border router where you intend to use NAT.

When static IP address support is enabled with the **ip nat allow-static-host**command, Cisco IOS software will provide a working IP address within the Public Wireless LAN to users configured with a static IP address.

Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 172.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 172.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

The following example enables static IP address support for the router at 192.168.196.51:

```
interface ethernet 1
 ip nat inside
ip nat allow-static-host
ip nat pool pool1 172.1.1.1 171.1.1.10 netmask 255.255.255.0 accounting WLAN-ACCT
ip nat inside source list 1 pool net-208
access-list 1 deny ip 192.168.196.51
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat create flow-entries

To enable flow cache entries in Network Address Translation (NAT), use the **ip nat create flow-entries** command in global configuration mode. To disable flow cache entries in NAT, use the **no** form of this command.

ip nat create flow-entries
no ip nat create flow-entries

Syntax Description

This command has no arguments or keywords.

Command Default

Flow cache entries are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Usage Guidelines

Note Disabling flow cache entries will result in lesser performance as this functionality does multiple database searches to find the most specific translation to use.

By default, Network Address Translation (NAT) creates a session (which is a 5-tuple entry) for every translation. A session is also called a flow cache entry.

Standard NAT and carrier-grade NAT (CGN) translation modes support the disabling of flow cache entries. You can disable flow cache entries in dynamic and static NAT/CGN configurations. Instead of creating sessions, dynamic and static NAT translations can translate a packet from the binding (or bindings, if both inside and outside bindings are available). A binding or a half entry is an association between a local IP address and a global IP address.

Disabling flow cache entries for dynamic and static translations saves memory usage and provides more scalability for your NAT translations.

Note Port Address Translation (PAT) or interface overload does not support disabling of flow cache entries.

Examples

The following example shows how to disable flow cache entries in a dynamic NAT configuration:

```
Device# configure terminal
Device(config)# ip nat pool net-208 172.16.233.208 172.16.233.223 prefix-length 28
Device(config)# access-list 1 permit 192.168.34.0 0.0.0.255
Device(config)# ip nat inside source list 1 pool net-208
Device(config)# no ip nat create flow-entries
```

The following example shows how to enable flow cache entries in a static CGN configuration:

```
Device# configure terminal
Device(config)# ip nat settings mode cgn
Device(config)# ip nat inside source static 192.168.2.1 192.168.34.2
Device(config)# ip nat create flow-entries
```

Related Commands

Command	Description
access-list (IP Extended)	Defines an extended IP access list.
access-list (IP Standard)	Defines a standard IP access list.
ip nat inside source	Enables NAT of the inside source address.
ip nat settings mode cgn	Enables CGN operating mode.

ip nat enable

To configure an interface connecting Virtual Private Networks (VPNs) and the Internet for Network Address Translation (NAT), use the **ip nat enable**command in interface configuration mode.

ip nat enable
no ip nat enable

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example show how to configure an interface connecting VPNs and the Internet for NAT translation:

```
interface Ethernet0/0
 ip vrf forwarding vrf1
 ip address 192.168.122.1 255.255.255.0
 ip nat enable
```

Related Commands

Command	Description
ip nat pool	Defines a pool of IP addresses for Network Address Translation.
ip nat source	Enables Network Address Translation on a virtual interface without inside or outside specification.

ip nat inside destination

To enable the Network Address Translation (NAT) of a globally unique outside host address to multiple inside host addresses, use the **ip nat inside destination**command inglobal configuration mode. This command is primarily used to implement TCP load balancing by performing destination address rotary translation. To remove the dynamic association to a pool, use the **no** form of this command.

ip nat inside destination list {*access-list-numbername*} **pool** *name* [**redundancy** *redundancy-id* **mapping-id** *map-id*]
no ip nat inside destination list

Syntax Description

list *access-list-number*	Specifies the standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
list *name*	Specifies the name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
pool *name*	Specifies the name of the pool from which global IP addresses are allocated during dynamic translation.
redundancy *redundancy-id*	Specifies the NAT redundancy operation.
mapping-id *map-id*	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.

Command Default

No inside destination addresses are translated.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.3(7)T	This command was modified. The **mapping-id** *map-id* keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The **redundancy** *redundancy-id* keyword and argument pair was added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

To implement TCP load balancing, you must configure NAT to use rotary pools as specified with the **ip nat pool** command and the **rotary** keyword.

Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Examples

The following example shows how to define a virtual address with connections that are distributed among a set of real hosts. The rotary pool defines the addresses of the real hosts. The access list defines the virtual address. If a translation does not already exist, TCP packets from serial interface 0 (the outside interface) whose destination matches the access list are translated to an address from the rotary pool.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0/0/0
 ip address 192.168.15.129 255.255.255.240
 ip nat outside
!
interface GigabitEthernet 0/0/1
 ip address 192.168.15.17 255.255.255.240
 ip nat inside
!
access-list 2 permit 192.168.15.1
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat inside source

To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** command in global configuration mode. To remove the static translation, or the dynamic association to a pool, use the **no** form of this command.

Dynamic NAT
ip nat inside source {**list** {*access-list-number access-list-name*} | **route-map** *name*} {**interface** *type number* | **pool** *name* [**redundancy** *rg-id* **mapping-id** *mapping-id*]} [**no-payload**] [**overload**] [**c**] [**vrf** *name* [**match-in-vrf**]] [**oer**] [**portmap** *name*]
no ip nat inside source {**list** {*access-list-number access-list-name* } | **route-map** *name*} {**interface** *type number* | **pool** *name* [**redundancy** *rg-id* **mapping-id** *mapping-id*]} [**no-payload**] [**overload**] [**reversible**] [**vrf** *name* [**match-in-vrf**]] [**oer**] [**portmap** *name*]

Static NAT
ip nat inside source static {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*} [**extendable**] [**no-alias**] [**no-payload**] [**route-map** *name* [**reversible**]] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**reversible**][**vrf** *name* [**match-in-vrf**] [**forced**] [**garp-interface**]]
no ip nat inside source static {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*} [**extendable**] [**no-alias**] [**no-payload**] [**route-map** *name* [**reversible**]] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**vrf** *name* [**match-in-vrf**] [**forced**] [**garp-interface**]]

Port Static NAT
ip nat inside source static {**tcp** | **udp**} {*local-ip local-port global-ip global-port* [**extendable**] [**forced**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**route-map** *name* [**reversible**]] [**vrf** *name* [**match-in-vrf**]] | **interface** *global-port*}
no ip nat inside source static {**tcp** | **udp**} {*local-ip local-port global-ip global-port* [**extendable**] [**forced**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**route-map** *name* [**reversible**]] [**vrf** *name* [**match-in-vrf**]] | **interface** *global-port*}

Network Static NAT
ip nat inside source static network *local-network global-network mask* [**extendable**] [**forced**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**vrf** *name* [**match-in-vrf**]]
no ip nat inside source static network *local-network global-network mask* [**extendable**] [**forced**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}] [**vrf** *name* [**match-in-vrf**]]

Syntax Description

list *access-list-number*	Specifies the number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *access-list-name*	Specifies the name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
route-map *name*	Specifies the named route map.
interface	Specifies an interface for the global address.

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
pool *name*	Specifies the name of the pool from which global IP addresses are allocated dynamically.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
redundancy	(Optional) Establishes NAT redundancy.
group-name	(Optional) Redundancy group name.
rg-id	(Optional) Redundancy group ID.
mapping-id *mapping-id*	(Optional) Specifies the mapping ID to be associated to NAT high-availability redundancy.
overload	(Optional) Enables the device to use one global address for many local addresses. When overloading is configured, the TCP or UDP port number of each inside host distinguishes between the multiple conversations using the same local IP address.
reversible	(Optional) Enables outside-to-inside initiated sessions to use route maps for destination-based NAT.
vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
match-in-vrf	(Optional) Enables NAT inside and outside traffic in the same VRF.
oer	(Optional) Allows Optimized Edge Routing (OER) to operate NAT and control traffic class routing.
portmap *name*	(Optional) Specifies the port map to be associated for NAT.
static	Sets up a single static translation.
esp *local-ip*	Establishes the IPsec Encapsulating Security Payload (ESP) (tunnel mode) support.
local-ip	Local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
global-ip	Globally unique IP address of an inside host as it appears to the outside network.
extendable	(Optional) Extends the translation.
forced	(Optional) Forcefully deletes an entry and its children from the configuration.
no-alias	(Optional) Prohibits an alias from being created for the global address.
tcp	Establishes the TCP protocol.

udp	Establishes the UDP protocol.
local-port	Local TCP or UDP port. The range is from 1 to 65535.
global-port	Global TCP or UDP port. The range is from 1 to 65535.
network *local-network*	Specifies the local subnet translation.
global-network	Global subnet translation.
mask	IP network mask to be used with subnet translations.
garp-interface	Initiates GARP messages request.

Command Default

No NAT translation of inside source addresses occurs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include the ability to use route maps with static translations, and the **route-map** *name* keyword-argument pair was added. This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the **redundancy** *group-name* keyword-argument pair was added. This command was modified to enable the translation of the IP header address only, and the **no-payload** keyword was added.
12.2(13)T	This command was modified. The **interface** keyword was added for static translations. The **vrf** *name* keyword-argument pair was added.
12.4(3)T	This command was modified. The **reversible** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified. The **oer** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRE	This command was modified. The **vrf** *name* keyword-argument pair was removed from Cisco 7600 series routers.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.3(2)T	This command was modified. The *rg-id* argument and the **mapping-id** *mapping-id* keyword-argument pair were added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Release	Modification
Cisco IOS XE Fuji Release 16.7.1	This command was modified. The **reversible** keyword was added to Static NAT configuration.
Cisco IOS XE 17.13.1a	This command was modified. The **garp-interface** keyword was added to Static NAT configuration to initiate GARP messages on the BD-VIF interface.

Usage Guidelines

The optional keywords of the **ip nat inside source** command can be entered in any order.

For information about the limitations when the **ip nat inside source** command was integrated into Cisco IOS XE Release 2.5, see the Cisco IOS XE 2 Release Notes.

This command has two forms: the dynamic and the static address translation. The form with an access list establishes the dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Packets that enter the device through the inside interface and packets sourced from the device are checked against the access list for possible NAT candidates. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form with the keyword **static** establishes a single static translation.

Note When a session is initiated from outside with the source IP as the outside global address, the device is unable to determine the destination VRF of the packet. Use the **match-in-vrf** keyword to enable the IP alias installation to work correctly when routing NAT inside and outside traffic in the same VRF.

Note When you configure NAT with a VRF-enabled interface address that acts as the global address, you must configure the **ip nat inside source static no-alias** command. If the **no-alias** keyword is not configured, Telnet to the VRF-enabled interface address fails.

Note Enabling or Initiating GARP for NAT Mapping as a feature using the **ip nat inside source static** command with the '**garp-interface**' option is only applicable to BD-VIF (Bridge Domain-Virtual Interface) interfaces. These interfaces bridge virtualized networks to the ACI fabric, offering essential connectivity for NAT mapping configuration and GARP notifications.

Examples

The following example shows how to translate between inside hosts addressed from either the 192.0.2.0 or the 198.51.100.0 network to the globally unique 203.0.113.209/28 network:

```
ip nat pool net-209 203.0.113.209 203.0.113.222 prefix-length 28
ip nat inside source list 1 pool net-209
!
interface ethernet 0
 ip address 203.0.113.113 255.255.255.240
 ip nat outside
!
```

```
interface ethernet 1
 ip address 192.0.2.1 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.0.2.1 255.255.255.0
access-list 1 permit 198.51.100.253 255.255.255.0
```

The following example shows how to translate the traffic that is local to the provider's edge device running NAT (NAT-PE):

```
ip nat inside source list 1 interface ethernet 0 vrf vrf1 overload
ip nat inside source list 1 interface ethernet 0 vrf vrf2 overload
!
ip route vrf vrf1 10.0.0.1 10.0.0.1 192.0.2.1
ip route vrf vrf2 10.0.0.1 10.0.0.1 192.0.2.1
!
access-list 1 permit 10.1.1.1 0.0.0.255
!
ip nat inside source list 1 interface ethernet 1 vrf vrf1 overload
ip nat inside source list 1 interface ethernet 1 vrf vrf2 overload
!
ip route vrf vrf1 10.0.0.1 10.0.0.1 198.51.100.1 global
ip route vrf vrf2 10.0.0.1 10.0.0.1 198.51.100.1 global
access-list 1 permit 10.1.1.0 0.0.0.255
```

The following example shows how to translate sessions from outside to inside networks:

```
ip nat pool POOL-A 10.1.10.1 10.1.10.126 255.255.255.128
ip nat pool POOL-B 10.1.20.1 10.1.20.126 255.255.255.128
ip nat inside source route-map MAP-A pool POOL-A reversible
ip nat inside source route-map MAP-B pool POOL-B reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.128 0.0.0.127
ip access-list extended ACL-B
 permit ip any 10.1.20.128 0.0.0.127
!
route-map MAP-A permit 10
 match ip address ACL-A
!
route-map MAP-B permit 10
 match ip address ACL-B
!
```

The following example shows how to configure the route map R1 to allow outside-to-inside translation for static NAT:

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.128 0.0.0.127
route-map R1 permit 10
 match ip address ACL-A
```

The following example shows how to configure NAT inside and outside traffic in the same VRF:

```
interface Loopback1
 ip vrf forwarding forwarding1
 ip address 192.0.2.11 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
```

```
interface Ethernet0/0
 ip vrf forwarding forwarding2
 ip address 192.0.2.22 255.255.255.0
 ip nat outside
 ip virtual-reassembly
ip nat pool MYPOOL 192.0.2.5 192.0.2.5 prefix-length 24
ip nat inside source list acl-nat pool MYPOOL vrf vrf1 overload
!
!
ip access-list extended acl-nat
 permit ip 192.0.2.0 0.0.0.255 any
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear ip nat translation	Clears dynamic NAT translations from the translation table.
interface	Configures an interface type and enters interface configuration mode.
ip access-list	Defines an IP access list or object group access control list by name or number.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
ip route vrf	Establishes static routes for a VRF instance.
ip vrf forwarding	Associates a VRF instance with a diameter peer.
match ip-address	Distributes any routes that have a destination network number address that is permitted by a standard access list, an extended access list, or a prefix list, or performs policy routing on packets.
permit	Sets conditions in a named IP access list or object group access control list that will permit packets.
route-map	Defines the conditions for redistributing routes from one routing protocol into another routing protocol, or enables policy routing.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat log translations flow-export

To enable the high-speed logging of Network Address Translation (NAT) translations by using a flow exporter, use the **ip nat log translations flow-export** command in global configuration mode. To disable the logging of NAT translations by using a flow exporter, use the **no** form of this command.

ip nat log translations flow-exportv9 udp {**destination** *IPv4address-port* | **ipv6-destination** *ipv6address-port*}[**vrf** *vrf-name* | **source** *interface-name interface-number* | **bind-only**]
no ip nat log translations flow-export

Syntax Description

v9	Specifies the flow exporter Version 9 format.
udp	Specifies the UDP protocol.
destination	Specifies the destination IPv4 address for which translations will be logged.
ipv6-destination	Specifies the destination address for which translations will be logged.
hostname	Name or IPv4 address of the destination.
local-udp-port	Local UDP port number. Valid values are from 1 to 65335.
bind-only	(Optional) Logs only NAT binding translations.
source *interface-type interface-number*	(Optional) Specifies the source interface for which translations will be logged.
vrf *vrf-name*	(Optional) Specifies the destination VRF for which translations will be logged.

Command Default

Logging is disabled for all NAT translations.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **bind-only** keyword was added.

Release	Modification
Cisco IOS XE Everest Release 16.6.1	This command was modified. The following keywords were added: • **ipv6-destination** • **vrf**

Usage Guidelines

The volume of data that is logged for NAT bindings translations is significantly reduced when you enable the **bind-only** keyword.

NAT binding is a one-to-one association between a local IP address and a global IP address. When you configure the **ip nat log translations flow-export** command without the **bind-only** keyword, translations for both NAT bindings and NAT sessions are logged. Sessions are identified by the 5-tuple (the source IP address, the destination IP address, the protocol, the source port, and the destination port) information. Sessions are normally created and destroyed at a much faster rate than bindings and, as a result, configuring the **bind-only** keyword can significantly reduce the volume of translation logs.

The **bind-only** keyword is most useful for dynamic NAT configurations without the overload configuration. Overload configurations (also known as Port Address Translation [PAT]) generally produce only sessions and no bindings. Thus, configuring the **bind-only** keyword is not very useful for PAT users.

Examples

The following example shows how to enable translation logging for a specific destination and source interface:

```
Device(config)# ip nat log translations flow-export v9 udp destination 10.10.0.1 1020 source
 gigabithethernet 0/0/1
```

This example shows how to enable high-speed logging using an IPv6 address

```
Device(config)# ip nat log translations flow-export v9 udp ipv6-destination 2001::06 5050
source GigabitEthernet 0/0/0
```

This example shows how to enable high-speed logging using an IPv6 address for a VRF

```
Device(config)# ip nat log translations flow-export v9 udp ipv6-destination 2001::06 5050
vrf hslvrf source GigabitEthernet 0/0/0
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
show ip nat translations	Displays active NAT translations.

ip nat log translations syslog

To enable the high-speed logging of Network Address Translation (NAT) translations to the syslog, use the **ip nat log translation syslog** command in global configuration mode. To disable the logging of NAT translations, use the **no** form of this command.

ip nat log translations syslog [**bind-only**]
no ip nat log translations

Syntax Description

bind-only	(Optional) Logs only NAT binding translations.

Command Default

Logging is disabled for all NAT translations.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **bind-only** keyword was added.

Usage Guidelines

The volume of data that is logged for NAT bindings translations is significantly reduced when you enable the **bind-only** keyword.

NAT binding is a one-to-one association between a local IP address and a global IP address. When you configure the **ip nat log translations syslog** command without the **bind-only** keyword, translations for both NAT bindings and NAT sessions are logged. Sessions are identified by the 5-tuple (the source IP address, the destination IP address, the protocol, the source port, and the destination port) information. Sessions are normally created and destroyed at a much faster rate than bindings and, as a result, configuring the **bind-only** keyword can significantly reduce the volume of translation logs.

The **bind-only** keyword is most useful for dynamic NAT configurations without the overload configuration. Overload configurations (also known as Port Address Translation [PAT]) generally produce only sessions and no bindings. Thus, configuring the **bind-only** keyword is not very useful for PAT users.

Examples

The following example shows how to log only NAT bindings translations to the syslog:

```
Device(config)# ip nat log translations syslog bind-only
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
show ip nat translations	Displays active NAT translations.

ip nat outside source

To enable Network Address Translation (NAT) of the outside source address, use the **ip nat outside source** command in global configuration mode. To remove the static entry or the dynamic association, use the **no** form of this command.

Dynamic NAT
ip nat outside source {**list** {*access-list-number access-list-name*} | **route-map** *name*} **pool** *pool-name* [**redundancy** *rg-id* **mapping-id** *mapping-id*] [**vrf** *name*] [**add-route**] [**no-payload**]
no ip nat outside source {**list** {*access-list-number access-list-name*} | **route-map** *name*} **pool** *pool-name* [**redundancy** *rg-id* **mapping-id** *mapping-id*] [**vrf** *name*] [**add-route**] [**no-payload**]

Static NAT
ip nat outside source static *global-ip local-ip* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]
no ip nat outside source static *global-ip local-ip* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]

Port Static NAT
ip nat outside source static {**tcp** | **udp**} *global-ip global-port local-ip local-port* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]
no ip nat outside source static {**tcp** | **udp**} *global-ip global-port local-ip local-port* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]

Network Static NAT
ip nat outside source static network *global-network local-network mask* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]
no ip nat outside source static network *global-network local-network mask* [**vrf** *name* [**match-in-vrf**]] [**add-route**] [**extendable**] [**no-alias**] [**no-payload**] [**redundancy** {*group-name* | *rg-id* **mapping-id** *mapping-id*}]

Syntax Description

list *access-list-number*	Specifies the number of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
list *access-list-name*	Specifies the name of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
route-map *name*	Specifies a named route map.
pool *pool-name*	Specifies the name of the pool from which global IP addresses are allocated.
add-route	(Optional) Adds a static route for the outside local address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
vrf *name*	(Optional) Associates the NAT rule with a particular VPN routing and forwarding (VRF) instance.

static	Sets up a single static translation.
global-ip	Globally unique IP address assigned to a host on the outside network by its owner. The address was allocated from the globally routable network space.
local-ip	Local IP address of an outside host as it appears to the inside network. The address was allocated from the address space routable on the inside (RFC 1918, *Address Allocation for Private Internets*).
match-in-vrf	(Optional) Matches the incoming VRF.
extendable	(Optional) Extends the transmission.
no-alias	(Optional) Prohibits an alias from being created for the local address.
redundancy	(Optional) Enables the NAT redundancy operation.
group-name	(Optional) Redundancy group name.
rg-id	(Optional) Redundancy group ID.
mapping-id *mapping-id*	(Optional) Specifies the mapping ID to be associated to NAT high-availability redundancy.
tcp	Establishes the TCP.
udp	Establishes the UDP.
global-port	Port number assigned to a host on the outside network by its owner.
local-port	Port number of an outside host as it appears to the inside network.
static network	Sets up a single static network translation.
global-network	Globally unique network address assigned to a host on the outside network by its owner. The address is allocated from a globally routable network space.
local-network	Local network address of an outside host as it appears to the inside network. The address is allocated from an address space that is routable on the inside network.
mask	Subnet mask for the networks that are translated.

Command Default

No translation of source addresses coming from the outside to the inside network occurs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.

Release	Modification
12.2(4)T	This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the **redundancy** *group-name* keyword-argument pair was added. This command was modified to enable the translation of the IP header address only, and the **no-payload** keyword was added.
12.2(13)T	This command was modified. The **vrf** *name* keyword-argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.3(2)T	This command was modified. The *rg-id* argument and the **mapping-id** *mapping-id* keyword-argument pair were added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

The optional keywords of the **ip nat outside source** command except for the **vrf** *name* keyword can be entered in any order.

For information about the limitations when this command was integrated into Cisco IOS XE Release 2.5, see the Cisco IOS XE 2 Release Notes.

You can use NAT to translate inside addresses that overlap with outside addresses. Use this command if your IP addresses in the stub network happen to be legitimate IP addresses belonging to another network, and you need to communicate with those hosts or devices.

This command has two general forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool that is named by using the **ip nat pool** command.

Alternatively, the syntax form with the **static** keyword establishes a single static translation.

The **match-in-vrf** keyword is supported with the **ip nat outside source static** command. The **match-in-vrf** keyword is not supported with the dynamic NAT configuration.

When you configure the **ip nat outside source static** command to add static routes for static outside local addresses, there is a delay in the translation of packets and packets are dropped. To avoid dropped packets, configure either the **ip nat outside source static add-route** command or the **ip route** command.

Examples

The following example shows how to translate between inside hosts addressed from the 10.114.11.0 network to the globally unique 10.69.233.208/28 network. Further, packets from outside hosts addressed from the 10.114.11.0 network (the true 10.114.11.0 network) are translated to appear to be from the 10.0.1.0/24 network.

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 10.114.11.39 255.255.255.0
 ip nat inside
!
access-list 1 permit 10.114.11.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear ip nat translation	Clears dynamic NAT from the translation table.
interface	Configures an interface type and enters interface configuration mode.
ip address	Sets a primary or secondary IP address for an interface.
ip nat	Designates the traffic originating from or destined for the interface as subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
ip route	Establishes static routes.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NATs.

ip nat piggyback-support

To enable a Network Address Translation (NAT) optimized Session Initiation Protocol (SIP) media path, use the **ip nat piggyback-support** commandinglobal configuration mode.

ip nat piggyback-support sip {**all-messages** | **sdp-only**} **router** *router-id* [**authentication** *authentication-key*]
no ip nat piggyback-support sip {**all-messages** | **sdp-only**} **router** *router-id* [**authentication** *authentication-key*]

Syntax Description

sip	SIP protocol algorithm.
all-messages	Establishes piggybacking in all messages except Session Description Protocol (SDP).
sdp-only	Establishes piggybacking in SDP only.
router *router-id*	Piggyback router ID number.
authentication *authentication-key*	(Optional) Specifies the MD5 authentication key.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Examples

The following example shows how to configure a NAT optimized SIP media path with SDP:

```
ip nat piggyback-support sip sdp-only router 100 authentication md5-key
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat pool

To define a pool of IP addresses for Network Address Translation (NAT) translations, use the **ip nat pool** command in global configuration mode. To remove one or more addresses from the pool, use the **no** form of this command.

ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**add-route**] [**type** {**match-host** | **rotary**}] [**accounting** *list-name*] [**arp-ping**] [**no-alias**] [**nopreservation**]
no ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**add-route**] [**type** {**match-host** | **rotary**}] [**accounting** *list-name*] [**arp-ping**] [**no-alias**] [**nopreservation**]

Syntax Description

name	Name of the pool.
start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.
netmask *netmask*	Specifies the network mask that indicates the address bits that belong to the network and subnetwork fields and the ones that belong to the host field. • Specify the network mask of the network to which the pool addresses belong.
prefix-length *prefix-length*	Specifies the number that indicates how many bits of the address is dedicated for the network.
add-route	(Optional) Specifies that a route is added to the NAT Virtual Interface (NVI) for the global address.
type	(Optional) Indicates the type of pool.
match-host	(Optional) Specifies that the host field of an IP address must remain the same after translation.
rotary	(Optional) Specifies that the range of addresses in the address pool identifies the real inside hosts among which TCP load distribution will occur.
accounting *list-name*	(Optional) Specifies the RADIUS profile name that matches the RADIUS configuration in the router.
arp-ping	(Optional) Determines static IP client instances and restarts the NAT entry timer.
no-alias	(Optional) Specifies to not create an alias for the address pool.
nopreservation	(Optional) Enables all IP addresses in the pool to be used for dynamic translation.

Command Default

No pool of addresses is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.3(2)XE	This command was modified. The **accounting** keyword and the *list-name* argument were added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was modified. The **add-route** keyword was added.
12.4(6)T	This command was modified. The **arp-ping** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. The **nopreservation** keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. The **accounting** keyword and the *list-name* argument were removed.
15.2(4)M	This command was modified. The **no-alias** keyword was added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

This command defines a pool of addresses by specifying the start address, the end address, and either network mask or prefix length.

When you enable the **no-alias** keyword, IP aliases are not created for IP addresses mentioned in the NAT pool.

Using the **nopreservation** keyword with the **prefix-length** or the **netmask** keyword disables the default behavior, which is known as IP address reservation. The **no** form of the command with the **nopreservation** keyword enables the default behavior and reserves the first IP address in the NAT pool, making the IP address unavailable for dynamic translation.

Examples

The following example shows how to translate between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 10.69.233.208/28 network:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
```

```
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

The following example shows how to add a route to the NVI interface for the global address:

```
ip nat pool NAT 192.168.25.20 192.168.25.30 netmask 255.255.255.0 add-route
ip nat source list 1 pool NAT vrf group1 overload
```

Related Commands

Command	Description
access-list	Defines a standard IP access list.
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets a primary or secondary IP address for an interface.
ip nat	Designates that traffic originating from or destined for an interface is subject to NAT.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat service	Enables a port other than the default port.
ip nat source	Enables NAT on a virtual interface without inside or outside specification.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat service

To specify a port other than the default port, use the **ip nat service**command in global configuration mode. To disable the port, use the **no** form of this command.

ip nat service dns-v6 {**H225** | **allow-h323-even-rtp-ports** | **allow-h323-keepalive** | **allow-sip-even-rtp-ports** | **allow-skinny-even-rtp-ports** | **fullrange** {**tcp** | **udp**} **port** *port-number* | **list** {*access-list-numberaccess-list-name*} {**ESP spi-match** | **IKE preserve-port** | **ftp tcp port** *port-number*} | **alg** {**tcp** | **udp**} **dns** | **allow-multipart** | **mgcp** | **enable-mib** | **nbar** | **port-randomization** | **ras** | **rtsp** | **sip** {**tcp** | **udp**} **port** *port-number* | **skinny tcp port** *port-number*}
no ip nat service dns-v6 {**H225** | **allow-h323-even-rtp-ports** | **allow-h323-keepalive** | **allow-sip-even-rtp-ports** | **allow-skinny-even-rtp-ports** | **fullrange** {**tcp** | **udp**} **port** *port-number* | **list** {*access-list-numberaccess-list-name*} {**ESP spi-match** | **IKE preserve-port** | **ftp tcp port** *port-number*} | **alg** {**tcp** | **udp**} **dns** | **allow-multipart** | **mgcp** | **enable-mib** | **nbar** | **port-randomization** | **ras** | **rtsp** | **sip** {**tcp** | **udp**} **port** *port-number* | **skinny tcp port** *port-number*}

Syntax Description

H225	Specifies the H.323 to H.225 protocol.
allow-h323-even-rtp-ports	Specifies the even-numbered Real-time Transport Protocol (RTP) ports for the H.323 protocol.
allow-h323-keepalive	Specifies the H.323 keepalive.
allow-sip-even-rtp-ports	Specifies the even-numbered RTP ports for the Session Initiation Protocol (SIP).
allow-skinny-even-rtp-ports	Specifies the even-numbered RTP ports for the skinny protocol.
fullrange	Specifies all the available ports. The range is from 1024 to 65535.
tcp	Specifies the TCP protocol. A maximum of 16 TCP ports can be configured.
udp	Specifies the UDP protocol. A maximum of 16 UDP ports can be configured.
port *port-number*	Specifies the port other than the default port in the range from 1 to 65533.
list *access-list-number*	Specifies the standard access list number in the range from 1 to 199.
access-list-name	Name of a standard IP access list.
ESP	Specifies the Security Parameter Index (SPI) matching IPsec pass-through.
spi-match	Specifies the SPI matching IPsec pass-through. The ESP endpoints must also have SPI matching enabled.
IKE	Preserves the Internet Key Exchange (IKE) port, as required by some IPsec servers.
preserve-port	Preserves the UDP port in IKE packets.
ftp	Specifies FTP.

alg {**tcp** | **upd**} **dns**	Enables Domain Name System (DNS) processing with an Application-Level Gateway (ALG) for either TCP or UDP.
allow-multipart	Enables SIP multipart processing.
mgcp	Specifies the Media Gateway Control Protocol (MGCP).
enable-mib	Enables NAT MIB support.
nbar	Enables network-based application recognition (NBAR).
port-randomization	Specifies that ports are allocated randomly for Network Address Translation (NAT), instead of sequentially.
ras	Specifies the H.323-Registration, Admission, and Status (RAS) protocol.
rtsp	Specifies the Real Time Streaming Protocol (RTSP). This protocol is enabled by default on port 554 and requires NBAR.
sip	Specifies SIP. This protocol is enabled by default on port 5060.
skinny	Specifies the skinny protocol.
dns-v6	Specifies if IPv6 DNS packets should be processed by ALG.

Command Default

DNS ALG processing is enabled for TCP and UDP. H.323 even-numbered RTP port allocation is enabled. Port randomization is disabled. RTSP is enabled and requires NBAR. Skinny even-numbered RTP port allocation is enabled. UDP SIP even-numbered RTP port allocation is enabled. UDP SIP is enabled on port 5060. UDP SIP multipart processing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	This command was modified. The **skinny** keyword was added.
12.2(8)T	This command was modified. The **sip** keyword was added.
12.2(15)T	This command was modified. The **ESP**and **spi-match**keywords were added to enable SPI matching on outside IPsec gateways. The **ike** and **preserve-port** keywords were added to enable outside IPsec gateways that require IKE source port 500.
12.3(7)T	This command was modified. The **rtsp** and **mgcp** keywords were added.
12.3(11)T	This command was modified. The **allow-sip-even-rtp-ports**keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4	This command was modified. The **nbar** keyword was added.

Release	Modification
12.4(24)T	This command was modified. The **port-randomization** keyword was added.
15.0(1)M	This command was modified. The **alg**, **dns**, and **allow-multipart** keywords were added.
15.0(1)M2	This command was modified. The **enable-mib** keyword was added.
15.1(1)T2	This command was modified. The **tcp** keyword used along with the **sip** keyword was removed.
15.0(1)M3	This command was modified. The **enable-mib** keyword was removed.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
16.7.1	This command was modified. The **dns-v6** keyword is added.
16.8.1	This command was modified. The **fullrange** keyword is enhanced to configure the local port with a global port in the high range (1024-65535).

Usage Guidelines

A host with an FTP server using a port other than the default port can have an FTP client using the default FTP control port. When a port other than the default port is configured for an FTP server, Network Address Translation (NAT) prevents FTP control sessions that are using port 21 for that particular server. If an FTP server uses the default port and a port other than the default port, both ports need to be configured using the **ip nat service** command.

NAT listens on the default port of the Cisco CallManager to translate the skinny messages. If the Cisco CallManager uses a port other than the default port, that port needs to be configured using the **ip nat service** command.

Use the **no ip nat service H225** command to disable support of H.225 packets by NAT.

Use the **no ip nat service allow-h323-even-rtp-ports**command to force odd-numbered RTP port allocation for H.323.

Use the **no ip nat service allow-sip-even-rtp-ports**command to force odd-numbered RTP port allocation for SIP.

Use the **no ip nat service allow-skinny-even-rtp-ports**command to force odd-numbered RTP port allocation for the skinny protocol.

Use the **no ip nat service rtsp** command to disable support of RTSP packets by NAT. RSTP uses port 554.

By default SIP is enabled on port 5060; therefore NAT-enabled devices interpret all packets on this port as SIP call messages. If other applications in the system use port 5060 to send packets, the NAT service may corrupt the packet as it attempts to interpret the packet as a SIP call message.

A NAT-enabled Cisco device that is running Cisco IOS Release 12.3(7)T or a later release may experience an increase in CPU usage when upgrading from a previous release. RTSP and MGCP NAT ALG support was added in Cisco IOS Release 12.3(7)T, which requires NBAR. You can use the **no ip nat service nbar** command to disable NBAR processing, which can decrease the CPU utilization rate.



Note If the **no ip nat service nbar** command is not specified during the startup of the router, results in the crashing of the router, when loading the configuration from the TFTP during the booting process.

The **port-randomization** keyword can be used to prevent a security threat caused by the possibility of of predicting the next port number that NAT will allocate. This security threat is described in the Cisco Security Advisory titled Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks . Port randomization has the following limitations:

- It cannot be used with certain other NAT features, including port map, full-range, and Secure Network Address Translation (SNAT).
- It is supported only for the port in the Layer 4 header of the packet.

Use the **ip nat service allow-multipart** command to enable the processing of SIP multipart Session Description Protocol (SDP) packets.

NAT MIB support is turned off by default to avoid breakpoint exception crashes. To enable NAT MIB support, use the **enable-mib** keyword.

Examples

The following example shows how to configure the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example shows how to configure the standard FTP port 21 and the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 21
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example shows how to configure the 20002 port of the Cisco CallManager:

```
ip nat service skinny tcp port 20002
```

The following example shows how to configure TCP port 500 of the third-party concentrator:

```
ip nat service list 10 IKE preserve-port
```

The following example shows how to configure SPI matching on the endpoint routers:

```
ip nat service list 10 ESP spi-match
```

The following example shows how to configure local port translating to the global port in the high range:

```
ip nat service fullrange udp port 53
ip nat service fullrange udp port 123
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.

Command	Description
ip nat outside source	Enables NAT of the outside source address.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat service dns-reset-ttl

To reset the time-to-live (TTL) value of Domain Name System (DNS) resource records that pass through Network Address Translation (NAT) to zero, use the **ip nat service dns-reset-ttl** command in global configuration mode. To prevent the TTL value of DNS resource records (RRs) from being set to zero, use the **no** form of this command.

ip nat service dns-reset-ttl
no ip nat service dns-reset-ttl

Syntax Description

This command has no arguments or keywords.

Command Default

The TTL value is set to zero for DNS RRs that pass through NAT.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.

Usage Guidelines

RFC 2694, *DNS extensions to Network Address Translators (DNS_ALG)*, states that the TTL value supplied in original RRs for static address assignments is left unchanged. For dynamic address assignments, the DNS application-level gateway (ALG) modifies the TTL value to zero, so that RRs are used only for transactions in progress and are not cached. RFC 2181, *Clarifications to the DNS Specification*, requires all RRs in an RRset (RRs with the same name, class, and type, but with different RDATA) to have the same TTL value. If the TTL value of an RR is set to zero, all other RRs within the same RRset are adjusted by the DNS ALG to be zero.

The **ip nat service dns-reset-ttl** command allows you to modify the behavior of the DNS ALG. The TTL values of all DNS RRs that pass through NAT are set to zero by default, and DNS servers or clients cannot cache temporarily assigned RRs. Use the **no ip nat service dns-reset-ttl** command to prevent the TTL value from being set to zero.

Use a TTL value of zero to prevent nonauthoritative servers from caching DNS RRs, when changing the IP address of a server. A nonzero value for DNS RRs enables remote name servers to cache the DNS RR information for a longer period of time, thereby reducing the number of queries for the RR and lengthening the amount of time required to proliferate RR changes simultaneously.

Examples

The following example shows how to prevent DNS RRs that pass through NAT from having their TTL values set to zero:

```
Router(config)# no ip nat service dns-reset-ttl
```

The following example shows how to set the value of DNS RRs that pass through NAT to zero:

```
Router(config)# ip nat service dns-reset-ttl
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip dns primary	Configures the router as authoritative for a zone.
ip dns server	Enables a DNS server on a router.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip name-server	Specifies the address of one or more name servers to be used for name and address resolution.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT; enables NAT logging; or enables static IP address support.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Specifies a port other than the default port for NAT.
show ip dns primary	Displays the authority record parameters configured for the DNS server.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat service enable-sym-port

To enable the endpoint agnostic port allocation, use the **ip nat service enable-sym-port** command in global configuration mode. To disable the endpoint agnostic port allocation, use the no form of this command.

ip nat service enable-sym-port
no ip nat service enable-sym-port

Syntax Description

This command has no arguments or keywords.

Command Default

If you do not issue this command, the endpoint agnostic port allocation is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use the **ip natserviceenable-sym-port** command to enable the endpoint agnostic port allocation, which is also known as symmetric port allocation.

Note Use this command before you enable Network Address Translation (NAT). If you enable the symmetric port database after creating entries in the NAT database, then corresponding entries are not added to the symmetric port database.

Examples

In the following example, an access list is created and the inside source address is translated using NAT. The endpoint agnostic port allocation is enabled after the inside source address is translated.

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# access list 1 permit 172.18.192.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface Ethernet 0/0
Router(config)# ip nat service enable-sym-port
Router(config)# end
```

Following are the list of entries which are made to the SymmetricPort (Sym Port) table, debugs, and Symmetric DB (Sym DB) when the command is issued and when the command is not entered:

```
NAT Symmetric Port Database: 1 entries
public ipaddr:port [tableid] | port# [refcount][syscount] | localaddr:localport [flags]
172.18.192.69:1024 [0] | 1025 [1] [0] | 172.18.192.69:1024 [0]
Sample SymPort Debugs:
If SymDB is not enabled or initiated:
NAT-SymDB: DB is either not enabled or not initiated.
If an entry needs to be inserted into SymDB:
NAT-SymDB: insert 172.18.192.69 1024 0
172.18.192.69 is the local address, 1024 is the local port, and 0 is the tableid
If SymDB lookup found an entry:
NAT-SymDB: [0] Entry was found for 172.18.192.69 -> 10.10.10.1: wanted 1024 got 1025
```

```
172.18.192.69 is the local address, 10.10.10.1 is the global address, 1024 is the requested
 port, and 1025 is the allocated port
If entry was deleted from SymDB:
NAT-SymDB: deleting entry 172.18.192.69:1024
172.18.192.69 is the local address, 1024 is the local port.
```

Related Commands

Command	Description
show ip nat translations	Displays the list of translations entries.
show ip nat statistics	Displays the entries in the symmetric port database

ip nat service gatekeeper

To prevent non-NAT packet flows from using excessive CPU for NAT translation, use the **ip nat service gatekeeper** command in global configuration mode. To disable the gatekeeper, use the **no** form of this command.

ip nat service gatekeeper
no ip nat service gatekeeper

Syntax Description

This command has no arguments or keywords.

Command Default

NAT gatekeeper is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)	This command was introduced from Cisco IOS Release 12.2.

Examples

The following example shows how to configure the gatekeeper for NAT:

```
Device(config)# ip nat service gatekeeper
Device(config)# end
Gatekeeper on
```

The following example shows how to disable the gateekeeper for NAT:

```
Device(config)# no ip nat service gatekeeper
Device(config)# end
Gatekeeper off
```

ip nat service ipsec-esp enable

To enable IPsec packet processing using ESP, use the **ip nat service ipsec-esp enable** command in global configuration mode. To disable IPsec packet processing using ESP, use the **no** form of this command.

ip nat service ipsec-esp enable
noip nat service ipsec-esp enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default IPsec packet processing using ESP is turned off.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.5(2)S	This command was introduced.

Examples

The following example shows how to use this command to enable IPsec packet processing using ESP:

```
Router(config)#  ip nat service ipsec-esp enable
```

ip nat service pptp

To enable Point-to-Point Tunneling Protocol (PPTP) application-layer gateway (ALG) translation for an application, use the **ip nat service pptp** command in global configuration mode. To disable the PPTP ALG translation for an application, use **no** form of this command.

ip nat service pptp
no ip nat service pptp

Syntax Description

This command has no arguments or keywords.

Command Default

PPTP ALG translation is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

PPTP ALG translation is enabled by default, when Network Address Translation (NAT) is configured.

Only Port Address Translation (PAT), also known as overload, uses the PPTP ALG. In static and dynamic NAT translations, the PPTP traffic is translated without the requirement of an ALG. PAT maps multiple unregistered internal addresses to only one or a few external addresses by using port numbers.

The following example shows how to disable PPTP ALG translation:

```
Device(config)# no ip nat service pptp
```

Related Commands

ip nat service	Specifies a port other than the default port.

ip nat settings gatekeeper-size

To configure cache for NAT, use **ip nat settings** *gatekeeper-size* command in global configuration mode. To disable the mode, use the **no** form of this command.

ip nat settings gatekeeper-size *gatekeeper-size*
no ip nat settings gatekeeper-size *gatekeeper-size*

Syntax Description

gatekeeper-size	Specifies the cache size.

Command Default

NAT gatekeeper is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2 SRA	This command was introduced from Cisco IOS Release 12.2 SRA.

Usage Guidelines

The extended mode for NAT allows the NAT gatekeeper to cache the source and the destination addresses. You can specify the required cache size based on the requirement when there is a non-NAT traffic on a NAT interface.

Examples

The following example shows how to configure the cache size for NAT gatekeeper:

```
Device(config)# ip nat settings gatekeeper-size 1024
Device(config)# end
```

ip nat settings mode

To enable the Network Address Translation (NAT) operating mode, use the **ip nat settings mode** command in global configuration mode. To disable the NAT operating mode, use the **no** form of this command.

ip nat settings mode {**cgn** | **default**}
no ip nat settings mode

Syntax Description

cgn	Enables the Carrier Grade NAT (CGN) operating mode.
default	Enables the default NAT operating mode.

Command Default

The default NAT operating mode is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.

Usage Guidelines

In CGN mode, the **ip nat inside destination** command is not supported.

Note We recommend the use of CGN mode for environments in which outside mapping translations are not required, but a large number of inside mappings are required.

Examples

The following example shows how to enable the CGN mode:

```
Router(config)# ip nat settings mode cgn
```

Related Commands

Command	Description
ip nat inside destination	Enables NAT of a globally unique outside host address to multiple inside host addresses.
ip nat settings support mapping outside	Configures NAT outside mapping support.

ip nat settings pap

To configure Network Address Translation (NAT) paired-address-pooling configuration mode, use the **ip nat settings pap** command in global configuration mode. To remove NAT paired-address-pooling configuration mode, use the **no** form of this command.

ip nat settings pap [**limit** {**1000** | **120** | **250** | **30** | **500** | **60**}] [**bpa**] [**set-size** *set-size*] [**step-size** *step-size*] [**single-set**]
no ip nat settings pap

Syntax Description

limit	(Optional) Limits the number of local addresses that you can use per global address.
1000	(Optional) Configures a limit of 1000 local addresses per global address by using an average of 64 ports.
120	(Optional) Configures a limit of 120 local addresses per global address by using an average of 512 ports. This is the default.
250	(Optional) Configures a limit of 250 local addresses per global address by using an average of 256 ports.
30	(Optional) Configures a limit of 30 local addresses per global address by using an average of 2048 ports.
500	(Optional) Configures a limit of 500 local addresses per global address by using an average of 128 ports.
60	(Optional) Configures a limit of 60 local addresses per global address by using an average of 1024 ports.
bpa	(Optional) Configures bulk logging and port-block allocation for carrier-grade NAT (CGN).
set-size *set-size*	(Optional) Configures the number of ports in each port block. Valid values for the *set-size* argument are 1024, 128, 2048, 256, 512, and 64. The default is 512.
step-size *step-size*	(Optional) Configures the step size for a port block. Valid values for the *step-size* argument are 1, 2, 4, and 8.
single-set	(Optional) Configures a single port set.

Command Default

Standard NAT configuration mode is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
Cisco IOS XE Release 3.10S	This command was modified. The **bpa** and **single-set** keywords and the **set-size** *set-size* and **step-size** *step-size* keyword-argument pairs were introduced.

Usage Guidelines

The ability of NAT to consistently represent a local IP address as a single global IP address is termed paired-address pooling. A local address is any address that appears on the inside of a network and a global address is any address that appears on the outside of the network.

If you change NAT configuration mode to paired-address-pooling configuration mode and vice versa, all existing NAT sessions are removed.

Paired-address pooling is supported only on Port Address Translation (PAT).

When you use the **no** form of this command, both paired-address pooling and bulk logging and port-block allocation modes are removed.

Bulk logging and port-block allocation mode allocates a block of ports for translation instead of allocating individual ports. This reduces the volume of messages logged through high-speed logging (HSL). The reduction of HSL messages is accomplished by dynamically allocating (based on data traffic) a block of global ports instead of a single global port to users.



Note Bulk logging and port-block allocation mode can be enabled only in carrier-grade NAT (CGN) mode. When you change any bulk logging and port-block allocation commands, all existing translations are torn down.

Bulk logging and port-block allocation uses a scattered port set method where a start port, a step value, and number of ports are used for bulk allocation of ports. For example, if the starting port number is 4000, the step value is 4,and the number of ports is 512, then the step value of 4 is added to 4000 to get the second port, again 4 is added to 4004 to get the third port and so on, till you have 512 ports in the port-set.

Port-set size determines the number of ports allocated in each port block. The step size is the number that is added to the previous port in a block to get the next port. The **single-set** keyword limits the number of port-sets to one per user

The default port size can differ based on the paired-address pooling limit that is configured .The following table provides information of the default port size when various paired-address pooling limit is configured:

Table 1: Default Port Size based on Paired-Address Pooling Support

Paired-Address Pooling	Default Port Set Size	Maximum Port Step Size
1000	64 ports	16
120	512 ports	8
250	256 ports	4
30	2048 ports	2
500	128 ports	8
60	1024 ports	4

Valid values available for the *set-size* argument are based on the configured paired-address pooling limit. The following table provides the paired-address pooling limit and the available set sizes:

Table 2: Paired-Address Pooling Limit and Available Set Sizes

Paired-Address Pooling Limit	Set Size
1000	1024, 128, 2048, 256, 512, and 64
120	1024, 2048, and 512
250	1024, 2048, 256, and 512
30	2048
500	1024, 128, 2048, 256, and 512
60	1024 and 2048

Valid values available for the *step-size* argument are based on the configured set-size. The following table provides the set size and the available step sizes:

Table 3: Port-Set Sizes and Available Step Sizes

Set-size	Step Size
1024	1, 2, and 4
2048	1 and 2
512	1, 2, 4, and 8

Examples

The following example shows how to configure paired-address-pooling mode:

```
Device# configure terminal
Device(config)# ip nat settings pap
```

The following example shows how to configure paired-address pooling limit and bulk logging and port-block allocation:

```
Device# configure terminal
Device(config)# ip nat settings mode cgn
Device(config)# ip nat settings mode pap limit 1000 2048 step-size 2 single-set
```

Related Commands

Command	Description
ip nat settings mode	Enables the default NAT operating mode.
ip nat settings mode cgn	Enables CGN operating mode.

ip nat settings pool watermark

To enable the configuration of threshold limits for address pool, use the **ip nat settings pool watermark** command in global configuration mode. To disable the threshold limit, use the **no** form of this command..

ip nat settings pool watermark high*number in percentage*
[low*number in percentage*]
no ip nat settings scale bind

Syntax Description:

This command has no arguments or keywords

Command Default

If the threshold limits are not configured, syslogs are generated after the address pool is exhausted.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8 Release	This command was introduced.

Examples

The following example shows how to enable threshold levels:

```
Device# configure terminal
Device(config)# ip nat settings pool watermark high 80 low 50
```

ip nat settings redundancy optimized-data-sync

To enable optimization of NAT entries synchronization in a high-availability setup, use the **ip nat settings redundancy optimized-data-sync** command in global configuration mode.

To disable the optimization of data synchronization, use the **no** form of this command.

ip nat settings redundancy optimized-data-sync
no ip nat settings redundancy optimized-data-sync



Note The feature enabled by the **ip nat settings redundancy optimized-data-sync** command is supported in Autonomous mode and is compatible with both classic NAT and CGN operational modes, but not in SD-WAN environments.

Syntax Description

redundancy optimized-data-sync	Specifies the optimization of data synchronization for NAT entries in high-availability configurations to reduce system load during the synchronization process.

Command Default

By default, the optimization of NAT entries synchronization in a redundant setup is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.15.1a	This command was introduced.

Usage Guidelines

This command is applicable specifically for B2B (box-to-box) high-availability deployments and is used to reduce the system load during the synchronization process of NAT entries between two high-availability peers.

To maintain service continuity and data integrity, it is critical to ensure full synchronization of control and data TCP connections to the standby router before performing a switchover.

After applying optimized data synchronization, it is important to verify that active and standby sessions are consistent, especially for redundancy group 1, and address any discrepancies promptly to maintain the accuracy of NAT session states.

The cooperation of this feature with the NAT gatekeeper is necessary to manage the NAT resources and synchronization correctly.

The **preempt** CLI option within the redundancy group configuration should be avoided with NAT, as it can lead to unpredictable behavior without providing any tangible benefits.

Even during standby reloads, redundancy sessions are expected to sync, maintaining consistency in redundancy capabilities.

Any inconsistencies between active and standby sessions, particularly after a reload with the optimized data sync feature, need to be promptly addressed to ensure the accurate state of NAT sessions. When the data link

on the standby router is shut down, sessions should not falsely display as synced, to prevent misinterpretation of the redundancy state.

Furthermore, upon the removal of the optimized-data-sync configuration, the synced sessions should become visible on the active router, confirming that the optimization feature has been deactivated.



Note For the feature to function correctly from the Cisco IOS XE 17.15.1a release, the **ip nat settings redundancy optimized-data-sync** command must be configured on both the active and standby routers. It is not supported to configure this command on only one router in a redundant pair. Furthermore, a system reload may be required for the command to take effect if it is configured or changed.

Examples

The following example shows how to enable optimized data synchronization for NAT entries in a high-availability setup:

```
Device# configure terminal
Device(config)# ip nat settings redundancy optimized-data-sync
```

ip nat settings scale bind

To configure CGN NAT to scale to a higher number of translations on ESP200, use the **ip nat settings scale bind** command in global configuration mode. To remove increased scaling on ESP200, use the **no** form of this command.

ip nat settings scale bind
no ip nat settings scale bind

Syntax Description:

This command has no arguments or keywords

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Usage Guidelines

The **ip nat settings scale bind** command must be configured before NAT is configured. If the **ip nat settings scale bind** is configured after NAT is configured, the router must be restarted for the changes to take effect.

Note We recommend the use of CGN mode for environments in which outside mapping translations are not required, but a large number of inside mappings are required.

Command History

Release	Modification
Cisco IOS XE Polaris 16.8	This command was introduced.

Examples

The following example shows how to use **ip nat settings scale bind** command:

```
Device# configure terminal
Device(config)# ip nat settings scale bind
```

ip nat settings support mapping outside

To configure the Network Address Translation (NAT) outside mapping support, use the **ip nat settings support mapping outside** command in global configuration mode. To remove all existing outside mapping configuration, use the **no** form of this command.

ip nat settings support mapping outside
no ip nat settings support mapping outside

Syntax Description

This command has no arguments or keywords.

Command Default

NAT outside mapping is supported by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.

Usage Guidelines

If you have configured NAT in the default mode, use the **ip nat settings mode cgn** command to change your NAT configuration to Carrier Grade NAT (CGN) mode. While changing your NAT configuration to CGN mode, use the **ip nat settings support mapping outside** command to remove all existing outside mapping configurations and to prevent the addition of outside mappings to the configuration.

Examples

The following example shows how to configure NAT outside mapping:

```
Router(config)# ip nat settings support mapping outside
```

Related Commands

Command	Description
ip nat settings mode	Enables the NAT operating mode.

ip nat sip-sbc

To configure a Cisco IOS hosted Network Address Translation (NAT) traversal for Session Border Controller (SBC), use the **ip nat sip-sbc** command in global configuration mode. To disable the Cisco IOS hosted NAT traversal for SBC, use the **no** form of this command.

Syntax Description

proxy	Configures the address or port which the inside phones refer to, and configures the outside proxy's address or port that the NAT SBC translates the destination IP address or port.
inside-address	Sets the Proxy's private IP address, which is configured on the inside phones.
inside-port	Sets the Proxy's private port.
outside-address	Sets the Proxy's public address, which is the actual proxy's address that NAT SBC changes the destination address to.
outside -port	Sets the Proxy's port.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
call-id-pool *pool-name*	(Optional) Specifies a dummy pool name from which the inside to outside SIP signaling packets' call ID is translated to a 1:1 maintained association rather than using the regular NAT pool.
override address	(Optional) Specifies the default override address mode.
override none	(Optional) Specifies that no override will be configured.
override port	(Optional) Specifies override port mode.
mode allow -flow-around	(Optional) Configures Real-Time Transport Protocol (RTP) for flow around for traffic between phones in the inside domain.
mode allow-flow-through *pool-name*	(Optional) Configures Real-Time Transport Protocol (RTP) for flow through for traffic between phones in the inside domain.
session -timeout *seconds*	(Optional) Configures the timeout duration for NAT entries pertaining to SIP signaling flows.
session-timeout nat-default	(Optional) Allows the default timeout to return to the NAT default timeout value of 5 minutes.
none	(Optional) Prevents modification of the out > in destination L3/L4 to the L3/L4 as saved in the sbc_appl_data of the door or NAT entry.
vrf -list vrf-name	(Optional) Defines SIP SBC VPN Routing and Forwarding (VRF) list names.
no	(Optional) Removes a name from the VRF list.

registration-throttle	(Optional) Defines the registration throttling parameter.
inside-timeout *seconds*	Timeout in seconds in the range of 1-536870.
outside-timeout *seconds*	Timeout in seconds in the range of 1-536870.
exit	(Required) Exit from SBC VRF configuration mode.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(15)T	The **allow-flow-through** and **registration-throttle** sub commands were added.

Usage Guidelines

The **proxy** keyword configures the address or port, which the inside phones refer to, and it configures the outside proxy's address or port that the NAT SBC translates the destination IP address or port. This keyword installs an outside static port half-entry with OL as the inside address or port and OG as the outside address or port.

The **mode allow-flow-around** keyword enables the RTP to be flow around. This keyword is only applicable for traffic between phones in the inside domain.

The mode **allow-flow-through** keyword enables the RTP to be flow through. This keywordd is only applicable for traffic between phones in the inside domain.

The optional **vrf-list** keyword must be followed by a list of VRF names. After the outside static port entry is created, a static route is installed wit the destination IP address as OL and next hop as OG. The NAT entry created is associated with appropriate VRFs as configured by this command.

Examples

The following example shows how to configure a Cisco IOS hosted NAT traversal for SBC:

```
interface ethernet1/1
 ip nat inside
 ip forwarding A
!
interface ethernet1/2
 ip nat inside
 ip forwarding B
!
interface ethernet1/3
 ip nat outside
!
ip nat pool call-id-pool 1.1.1.1 1.1.1.100
ip nat pool outside-pool 2.2.2.1.1.1 2.2.2.1.1.10
ip nat pool inside-pool-A 169.1.1.1 169.1.1.10
ip nat pool inside-pool-B 170.1.1.1 170.1.1.10
ip nat inside source list 1 pool inside-pool-A vrf A overload
ip nat inside source list 2 pool inside-pool-B vrf B overload
ip nat outside list 3 pool outside-pool
ip nat inside source list 4 pool call-id-pool
!
access-list for VRF-A inside-phones
```

```
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 2 permit 172.1.1.0 0.0.0.255
!
access-=list for call-id-pool
access-list 4 permit 10.1.1.0 0.0.0.255
access-list 4 permit 20.1.1.0 0.0.0.255
!
ip nat sip-sbc
 proxy 200.1.1.1 5060 192.1.1.1 5060 protocol udp
 vrf-list
  vrf-name A
  vrf-name B
 call-id-pool call-id-pool
 session-timeout 300
 mode allow-flow-around
 override address
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.