

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 | <i>ip-address</i> | (Optional) IP address used in replies to DNS queries. |
|--------------------|-------------------|---|
|--------------------|-------------------|---|

| Defaults | No default behavior or values |
|----------|-------------------------------|
|----------|-------------------------------|

| 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 Release 12.2(28)SB. |

Usage Guidelines

DNS spoofing allows a router 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 router forwards DNS queries to the real DNS servers.

The router 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 router specified by the **hostname** command, with no default domain appended. For example, in the following configuration:

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

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 router will respond to a DNS query with an IP address of 192.168.15.1:

```
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 Virtual Private Network (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 <i>vrf-name</i> | (Optional) The <i>vrf-name</i> 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. |
| <i>view-name</i> | 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.

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 be configured (by using the **restrict name-group** and **restrict source access-group** 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. |
| 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 router 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. |

| Command | Description |
|-------------------------------------|--|
| 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

| | |
|-----------------------|---|
| <i>view-list-name</i> | 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 <i>vrf-name</i> argument specifies a name for the VRF table. |
| <i>name</i> | Domain name. Do not include the initial period that separates an unqualified name from the domain name. |

Defaults

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 <i>vrf-name</i> 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 the IP Domain Naming System (DNS)-based host name-to-address translation, use the **ip domain lookup** command in global configuration mode. To disable the DNS, use the **no** form of this command.

ip domain lookup

no ip domain lookup

Syntax Description

This command has no arguments or keywords.

Defaults

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-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. |

Usage Guidelines

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

Examples

The following example enables the IP DNS-based host name-to-address translation:

```
ip domain lookup
```

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 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 **no** form of this command.

ip domain name [**vrf** *vrf-name*] *name*

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

Syntax Description

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

Defaults

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 <i>vrf-name</i> 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 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

| | |
|---------------|---|
| <i>number</i> | Number of times to retry sending a DNS query to the DNS server. The range is from 0 to 100; the default is 2. |
|---------------|---|

Defaults

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.

Defaults

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 | <i>seconds</i> | Time, in seconds, to wait for a response to a DNS query. The range is from 0 to 3600; the default is 3. |
|---------------------------|----------------|---|

| | |
|-----------------|----------------------------|
| Defaults | <i>seconds</i> : 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 seconds 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 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

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

Defaults

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. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

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 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 <i>vrf-name</i> | (Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The <i>vrf-name</i> argument specifies a name for the VRF table. |
| <i>server-address1</i> | IPv4 or IPv6 addresses of a name server. |
| <i>server-address2...server-address6</i> | (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 <i>vrf-name</i> 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. |

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). |

logging (DNS)

To enable logging of a system message logging (syslog) message each time the Domain Name System (DNS) view is used, use the **logging** command in DNS view configuration mode. To disable logging of a syslog message each time the DNS view is used, use the **no** form of this command.

logging

no logging

Syntax Description This command has no arguments or keywords.

Command Default No syslog message is logged when the DNS view is used.

Command Modes DNS view configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.4(9)T | This command was introduced. |

Usage Guidelines This command enables the logging of syslog messages for the DNS view. To display the logging setting for a DNS view, use the **show ip dns view** command.

Examples The following example shows how to enable logging of a syslog message each time the DNS view named user3 that is associated with the VRF vpn32 is used:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# logging
```

| Related Commands | 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. |
| | 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. |

restrict authenticated

To specify that a Domain Name System (DNS) view list member cannot be used to respond to an incoming DNS query if the DNS view and the DNS client have not been authenticated, use the **restrict authenticated** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict authenticated

no restrict authenticated

Syntax Description This command has no arguments or keywords.

Command Default When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the DNS view and the DNS client have been authenticated.

Command Modes DNS view list member configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.4(9)T | This command was introduced. |

Usage Guidelines This command restricts the DNS view list member from responding to an incoming DNS query unless the Cisco IOS software has verified the authentication status of the client. The view list member is rejected, and the view-selection process proceeds to the next view in the view list, if the client is not authenticated. The router that is running Split DNS determines the query client authentication status by calling any DNS client authentication functions that have been registered with Split DNS.

A client can be authenticated within a Cisco IOS environment by various methods, such as Firewall Authentication Proxy, 802.1x, and wireless authentication. Some DNS authentication functions might inspect only the source IP address or MAC address and the VRF information, while other functions might inspect the source IP address or MAC address, the VRF information, and the DNS view name.



Note

In Cisco IOS Release 12.4(9)T, none of these authentication methods are implemented by any Cisco IOS authentication subsystems. As a result, if a DNS view is configured to be restricted based on client authentication, the Cisco IOS software will not use that view whenever the view is considered for handling a query. In future Cisco IOS releases, authentication subsystems will implement client authentication functions and enable them to be registered on a router running Split DNS. This will enable the Cisco IOS software to support authentication-based use restrictions on DNS views. This command is provided now for backward compatibility when DNS authentication functions are implemented.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the query source IP address (configured by using the **restrict source access-group** command) or the query hostname (configured by using the **restrict name-group** command).

**Note**

If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source VRF of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.

Examples

The following example shows how to create the DNS view list userlist5 so that it contains the two DNS views:

```
Router(config)# ip dns view-list userlist5
Router(cfg-dns-view-list)# view vrf vpn101 user1 20
Router(cfg-dns-view-list-member)# exit
Router(cfg-dns-view-list)# view vrf vpn201 user2 35
Router(cfg-dns-view-list-member)# restrict authenticated
```

Both view list members are restricted from responding to an incoming DNS query unless the query is from the same VRF as the VRF with which the view is associated.

The first view list member (the view named user1 and associated with the VRF vpn101) has no further restrictions placed on its use.

The second view list member (the view named user2 and associated with the VRF vpn201) is further restricted from responding to an incoming DNS query unless the Cisco IOS software can verify the authentication status of the client.

Related Commands

| Command | Description |
|-------------------------------------|---|
| 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. |

restrict name-group

To specify that a Domain Name System (DNS) view list member cannot be used to respond to a DNS query unless the query hostname matches a permit clause in a particular DNS name list and none of the deny clauses, use the **restrict name-group** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict name-group *name-list-number*

no restrict name-group *name-list-number*

| | | |
|---------------------------|-------------------------|--|
| Syntax Description | <i>name-list-number</i> | Integer from 1 to 500 that identifies an existing DNS name list. |
|---------------------------|-------------------------|--|

| | |
|------------------------|---|
| Command Default | When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the query hostname matches a permit clause in a particular DNS name list. |
|------------------------|---|

| | |
|----------------------|------------------------------------|
| Command Modes | DNS view list member configuration |
|----------------------|------------------------------------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.4(9)T | This command was introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | <p>This command restricts the DNS view list member from responding to an incoming DNS query if a permit clause in the specified DNS name list specifies a regular expression that matches the query hostname. The view list member is rejected, and the view-selection process proceeds to the next view in the view list, if an explicit deny clause in the name list (or the implicit deny clause at the end of the name list) matches the query hostname. To configure a DNS name list, use the ip dns name-list command.</p> <p>A DNS view list member can also be restricted from responding to an incoming DNS query based on the source IP address of the incoming DNS query. To configure this type of restriction, use the restrict source access-group command.</p> |
|-------------------------|---|



| | |
|-------------|---|
| Note | If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source VRF of the query and all configured usage restrictions are met by the query. |
|-------------|---|

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.



| | |
|-------------|--|
| Note | The <i>name-list-number</i> argument referenced in this command is configured using the ip dns name-list command. The DNS name list is referred to as a “name list” when it is defined and as a “name group” when it is referenced in other commands. |
|-------------|--|

Examples

The following example shows how to specify that DNS view user3 associated with the global VRF, when used as a member of the DNS view list userlist5, cannot be used to respond to an incoming DNS query unless the query hostname matches the DNS name list identified by the number 1:

```
Router(config)# ip dns view-list userlist5
Router(cfg-dns-view-list)# view user3 40
Router(cfg-dns-view-list-member)# restrict name-group 1
```

Related Commands

| Command | Description |
|-------------------------------------|---|
| 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 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. |

restrict source access-group

To specify that a Domain Name System (DNS) view list member cannot be used to respond to a DNS query unless the source IP address of the DNS query matches a standard access control list (ACL), use the **restrict source access-group** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

```
restrict source access-group {acl-name | acl-number}
```

```
no restrict source access-group {acl-name | acl-number}
```

| Syntax Description | | |
|--------------------|-------------------|---|
| | <i>acl-name</i> | String (not to exceed 64 characters) that specifies a standard ACL. |
| | <i>acl-number</i> | Integer from 1 to 99 that specifies a standard ACL. |

Command Default When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the source IP address of the DNS query belongs to a particular standard ACL.

Command Modes DNS view list member configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.4(9)T | This command was introduced. |

Usage Guidelines This command restricts the DNS view list member from responding to an incoming DNS query if the query source IP address matches the specified standard ACL. To configure a standard ACL, use the **access-list** (IP standard) command.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the the query hostname. To configure this type of restriction, use the **restrict name-group** command.



Note

If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source Virtual Private Network (VPN) routing and forwarding (VRF) instance of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.



Note

The *acl-name* or *acl-number* argument referenced in this command is configured using the **access-list** command. The access list is referred to as a “access list” when it is defined and as a “access group” when it is referenced in other commands.

Examples

The following example shows how to specify that DNS view user4 associated with the global VRF, when used as a member of the DNS view list userlist7, cannot be used to respond to an incoming DNS query unless the query source IP address matches the standard ACL number 6:

```
Router(config)# ip dns view-list userlist7
Router(cfg-dns-view-list)# view user4 40
Router(cfg-dns-view-list-member)# restrict source access-group 6
```

Related Commands

| Command | Description |
|----------------------------------|---|
| access-list (IP standard) | Creates a standard ACL that defines the specific host or subnet for host-specific PAM. |
| 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 view-list | Displays information about a particular DNS view list or about all configured DNS view lists. |

show ip ddns update

To display information about the Dynamic Domain Name System (DDNS) updates, use the **show ip ddns update** command in privileged EXEC mode.

```
show ip ddns update [interface-type number]
```

| | |
|---------------------------|---|
| Syntax Description | <i>interface-type number</i> (Optional) Displays DDNS updates configured on an interface. |
|---------------------------|---|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| 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. | |

| | |
|-----------------|---|
| Examples | The following output shows the IP DDNS update method on loopback interface 100 and the destination: |
|-----------------|---|

```
Router# show ip ddns update

Dynamic DNS Update on Loopback100:
Update Method Name      Update Destination
testing                 10.1.2.3
```

| 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. |

show ip ddns update method

To display information about the Dynamic Domain Name System (DDNS) update method, use the **show ip ddns update method** command in privileged EXEC mode.

```
show ip ddns update method [method-name]
```

| | |
|---------------------------|--|
| Syntax Description | <i>method-name</i> (Optional) Name of the update method. |
|---------------------------|--|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| 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. | |

Examples The following is sample output from the **show ip ddns update method** command:

```
Router# show ip ddns update method

Dynamic DNS Update Method: test
  Dynamic DNS update in IOS internal name cache
```

| 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. |
| | show ip ddns update | Displays information about the DDNS updates. |
| | show ip host-list | Displays the assigned hosts in a list. |
| | update dns | Dynamically updates a DNS with A and PTR RRs for some address pools. |

show ip dns name-list

To display a particular Domain Name System (DNS) name list or all configured DNS name lists, use the **show ip dns name-list** command in privileged EXEC mode.

```
show ip dns name-list [name-list-number]
```

| | |
|---------------------------|---|
| Syntax Description | <i>name-list-number</i> (Optional) Integer from 1 to 500 that identifies a DNS name list. |
|---------------------------|---|

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.4(9)T | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | Display a DNS name list to view the ordered list of pattern-matching rules it defines. Each rule in the name list specifies a regular expression and the type of action to be taken if the query hostname matches that expression. |
|-------------------------|--|

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

| | |
|-----------------|---|
| Examples | The following is sample output from the show ip dns name-list command: |
|-----------------|---|

```
Router# show ip dns name-list

ip dns name-list 1
  deny WWW.EXAMPLE1.COM
  permit WWW.EXAMPLE.com

ip dns name-list 2
  deny WWW.EXAMPLE2.COM
  permit WWW.EXAMPLE3.COM
```

Table 25 describes the significant fields shown for each DNS name list in the display.

Table 25 *show ip dns name-list Field Descriptions*

| Field | Description |
|-----------|---|
| name-list | Integer that identifies the DNS name list. Configured using the ip dns name-list command. |
| deny | Regular expression, case-insensitive, to be compared to the DNS query hostname. If the DNS query hostname matches this expression, the name list matching will terminate immediately and the name list will be determined to have not matched the hostname. A deny clause is configured by using the ip dns name-list command. |
| permit | Regular expression in domain name format (a sequence of case-insensitive ASCII labels separated by dots), case-insensitive, and to be compared to the DNS query hostname. If the DNS query hostname matches this expression, the name list matching will terminate immediately and the name-list will be determined to have matched the hostname. A permit clause is configured by using the ip dns name-list command. |

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. |

show ip dns primary

To display the authority record parameters configured for the Domain Name System (DNS) server, use the **show ip dns primary** command in user EXEC or privileged EXEC mode.

show ip dns primary

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 12.0 | This command was introduced. |

Examples The following example shows how to configure the router as a DNS server and then display the authority record parameters for the DNS server:

```
Router(conf)# ip dns server
Router(conf)# ip dns primary example.com soa ns1.example.com mb1.example.com
Router(conf)# ip host example.com ns ns1.example.com
Router(conf)# ip host ns1.example.com 209.165.201.1
Router(conf)# exit
Router# show ip dns primary
Primary for zone example.com:
  SOA information:
    Zone primary (MNAME): ns1.example.com
    Zone contact (RNAME): mb1.example.com
    Refresh (seconds):    21600
    Retry (seconds):      900
    Expire (seconds):     7776000
    Minimum (seconds):    86400
```

[Table 26](#) describes the significant fields shown in the display.

Table 26 *show ip dns primary Field Descriptions*

| Field | Description |
|----------------------|--|
| Zone primary (MNAME) | Authoritative name server. |
| Zone contact (RNAME) | DNS mailbox of administrative contact. |
| Refresh (seconds) | Refresh time in seconds. This time interval that must elapse between each poll of the primary by the secondary name server. |
| Retry (seconds) | 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. |

Table 26 *show ip dns primary Field Descriptions (continued)*

| Field | Description |
|-------------------|---|
| Expire (seconds) | Authority expire time in seconds. The secondary expires its data if it cannot reach the primary name server within this time interval. |
| Minimum (seconds) | Minimum Time to Live (TTL) in seconds for zone information. Other servers should cache data from the name server for this length of time. |

Related Commands

| Command | Description |
|-----------------------|---|
| ip dns primary | Configures router authority parameters for the DNS name server, for the DNS name server. |
| ip dns server | Enables the DNS server on the 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 statistics

To display packet statistics for the Domain Name System (DNS) server, use the **show ip dns statistics** command in user EXEC or privileged EXEC mode.

show ip dns statistics

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC (>)
Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.4(20)T | This command was introduced. |

Usage Guidelines Use this command to display the number of DNS requests received and dropped by the DNS server and the number of DNS responses sent by the DNS server.

Examples The following is sample output from the **show ip dns statistics** command:

```
Router# show ip dns statistics

DNS requests received = 818725 ( 818725 + 0 )
DNS requests dropped = 0 ( 0 + 0 )
DNS responses replied = 0 ( 0 + 0 )

Forwarder queue statistics:
Current size = 0
Maximum size = 400
Drops = 804613

Director queue statistics:
Current size = 0
Maximum size = 0
Drops = 0
```

Table 27 describes the significant fields shown in the display.

Table 27 *show ip dns statistics Field Descriptions*

| Field | Description |
|-----------------------|--|
| DNS requests received | Total number of DNS requests received by the DNS server. Additional details are displayed in parenthesis: <ul style="list-style-type: none"> • Number of UDP packets received • Number of TCP packets received |
| DNS requests dropped | Total number of DNS requests discarded by the DNS server. Additional details are displayed in parenthesis: <ul style="list-style-type: none"> • Number of UDP packets dropped • Number of TCP packets dropped |
| DNS responses replied | Total number of DNS responses sent by the DNS server. Additional details are displayed in parenthesis: <ul style="list-style-type: none"> • Number of UDP packets dropped • Number of TCP packets dropped |
| Current size | Displays the current size of the queue counter. |
| Maximum size | Displays the maximum size of the queue counter reached since the reload. <p>Note Whenever you change the queue size, the Maximum size counter will be reset to zero.</p> |
| Drops | Displays the number of packets dropped when a queue function fails. <p>Note Whenever you change the queue size, the Drops counter will be reset to zero.</p> |

show ip dns view

To display configuration information about a Domain Name System (DNS) view or about all configured DNS views, including the number of times the DNS view was used, the DNS resolver settings, the DNS forwarder settings, and whether logging is enabled, use the **show ip dns view** command in privileged EXEC mode.

```
show ip dns view [vrf vrf-name] [default | view-name]
```

Syntax Description

| | |
|----------------------------|---|
| vrf <i>vrf-name</i> | (Optional) The <i>vrf-name</i> argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view. Default is the global VRF (that is, the VRF whose name is a NULL string). |
| 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 | (Optional) Specifies that the DNS view is unnamed. By default all configured DNS views are displayed. |
| <i>view-name</i> | (Optional) Name of the DNS view whose information is to be displayed. Default is all configured DNS views. |
| 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 Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Display DNS view information to view its DNS resolver settings, DNS forwarder settings, and whether logging is enabled.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

Because different DNS views can be associated with the same VRF, omitting both the **default** keyword and the *view-name* argument causes this command to display information about all the views associated with the global or named VRF.

Examples

The following is sample output from the **show ip dns view** command:

```
Router# show ip dns view

DNS View default parameters:
Logging is on (view used 102 times)
DNS Resolver settings:
```

```
Domain lookup is enabled
Default domain name: example.com
Domain search list: example1.com example2.com example3.com
Domain name for multicast lookups: 192.0.2.10
Lookup timeout: 7 seconds
Lookup retries: 5
Domain name-servers:
    192.168.2.204
    192.168.2.205
    192.168.2.206
Round-robin'ing of IP addresses is enabled
DNS Server settings:
Forwarding of queries is enabled
Forwarder addresses:
    192.168.2.11
    192.168.2.12
    192.168.2.13
Forwarder source interface: FastEthernet0/1

DNS View user5 parameters:
Logging is on (view used 10 times)
DNS Resolver settings:
    Domain lookup is enabled
    Default domain name: example5.net
    Domain search list:
    Lookup timeout: 3 seconds
    Lookup retries: 2
    Domain name-servers:
        192.168.2.104
        192.168.2.105
DNS Server settings:
    Forwarding of queries is enabled
    Forwarder addresses:
        192.168.2.204

DNS View user1 vrf vpn101 parameters:
Logging is on (view used 7 times)
DNS Resolver settings:
    Domain lookup is enabled
    Default domain name: example1.com
    Domain search list:
    Lookup timeout: 3 seconds
    Lookup retries: 2
    Domain name-servers:
        192.168.2.100
DNS Server settings:
    Forwarding of queries is enabled
    Forwarder addresses:
        192.168.2.200 (vrf vpn201)
```

Table 28 describes the significant fields shown for each DNS view in the display.

Table 28 *show ip dns view Field Descriptions*

| Field | Description |
|-----------------------------------|---|
| Logging | Logging of a system message logging (syslog) message each time the DNS view is used. Configured using the logging command. Note If logging is enabled for a DNS view, the show ip dns view command output includes the number of times the DNS view has been used in responding to DNS queries. |
| Domain lookup | DNS lookup to resolve hostnames for internally generated queries. Enabled or disabled using the domain lookup command. |
| Default domain name | Default domain to append to hostnames without a dot. Configured using the domain name command. |
| Domain search list | List of domain names to try for hostnames without a dot. Configured using the domain list command. |
| Domain name for multicast lookups | IP address to use for multicast address lookups. Configured using the domain multicast command. |
| Lookup timeout | Time (in seconds) to wait for DNS response after sending or forwarding a query. Configured using the domain timeout command. |
| Lookup retries | Number of retries when sending or forwarding a query. Configured using the domain retry command. |
| Domain name-servers | Up to six name servers to use to resolve domain names for internally generated queries. Configured using the domain name-server command. |
| Resolver source interface | Source interface to use to resolve domain names for internally generated queries. Configured using the ip domain lookup source-interface global command. |
| Round robin'ing of IP addresses | Round-robin rotation of the IP addresses associated with the hostname in cache each time hostnames are looked up. Enabled or disabled using the domain round-robin command. |
| Forwarding of queries | Forwarding of incoming DNS queries. Enabled or disabled using the dns forwarding command. |
| Forwarder addresses | Up to six IP address to use to forward incoming DNS queries. Configured using the dns forwarder command. |
| Forwarder source-interface | Source interface to use to forward incoming DNS queries. Configured using the dns forwarding source-interface command. |

show ip dns view-list

To display information about a Domain Name System (DNS) view list or about all configured DNS view lists, use the **show ip dns view-list** command in privileged EXEC mode.

```
show ip dns view-list [view-list-name]
```

| | | |
|---------------------------|-----------------------|---|
| Syntax Description | <i>view-list-name</i> | (Optional) Name of the DNS view list. Default is all configured DNS view lists. |
|---------------------------|-----------------------|---|

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.4(9)T | This command was introduced. |

Usage Guidelines If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

IP DNS view lists are defined by using the **ip dns view-list** command.

To display information about how DNS view lists are applied, use the **show running-config** command:

- The default DNS view list, if configured, is listed in the default DNS view information (in the **ip dns view default** command information, as the argument for the **ip dns server view-group** command).
- Any DNS view lists attached to interfaces are listed in the information for each individual interface (in the **interface** command information for that interface, as the argument for the **ip dns view-group** command).

Examples

The following is sample output from the **show ip dns view-list** command:

```
Router# show ip dns view-list

View-list userlist1:
  View user1 vrf vpn101:
    Evaluation order: 10
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
  View user2 vrf vpn102:
    Evaluation order: 20
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
  View user3 vrf vpn103:
    Evaluation order: 30
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
View-list userlist2:
  View user1 vrf vpn101:
    Evaluation order: 10
    Restrict to ip dns name-list: 151
  View user2 vrf vpn102:
```

```

Evaluation order: 20
Restrict to ip dns name-list: 151
View user3 vrf vpn103:
Evaluation order: 30
Restrict to ip dns name-list: 151

```

Table 29 describes the significant fields shown for each DNS view list in the display.

Table 29 *show ip dns view-list Field Descriptions*

| Field | Description |
|------------------|--|
| View-list | A DNS view list name. Configured using the ip dns view command. |
| View | A DNS view that is a member of this DNS view list. If the view is associated with a VRF, the VRF name is also displayed. Configured using the ip dns view-list command. |
| Evaluation order | Indication of the order in which the DNS view is checked, relative to other DNS views in the same DNS view list. Configured using the view command. |
| Restrict | Usage restrictions for the DNS view when it is a member of this DNS view list. Configured using the restrict name-group command or the restrict source access-group command. |

Related Commands

| Command | Description |
|---------------------------------|--|
| debug ip dns view-list | Enables debugging output for DNS view list events. |
| interface | Configures an interface type and enter interface configuration mode so that the specific interface can be configured. |
| 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-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 running-config | Displays the contents of the currently running configuration file of your routing device. |

show ip host-list

To display the assigned hosts in a list, use the **show ip host-list** command in privileged EXEC mode.

```
show ip host-list [host-list-name]
```

| | |
|---------------------------|--|
| Syntax Description | <i>host-list-name</i> (Optional) Name assigned to the list of hosts. |
|---------------------------|--|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| 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. | |

Examples The following is sample output from the **show ip host-list** command example for the abctest group:

```
Router# show ip host-list abctest
```

```
Host list: abctest
ddns.abc.test
10.2.3.4
ddns2.unit.test
10.3.4.5
ddns3.com
10.3.3.3
e.org
1.org.2.org
3.com
10.5.5.5 (VRF: def)
```

| Related Commands | Command | Description |
|-------------------------|----------------------------------|--|
| | debug dhcp | Displays debugging information about the DHCP client and monitors the status of DHCP packets. |
| | debug ip ddns update | Enables debugging for DDNS updates. |
| | debug ip dhcp server | Enables DHCP server debugging. |
| | host (host-list) | Specifies a list of hosts that will receive DDNS updates of A and PTR RRs. |
| | ip ddns update hostname | Enables a host to be used for DDNS updates of A and PTR RRs. |
| | ip ddns update method | Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates. |
| | ip dhcp client update dns | Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client. |
| | ip dhcp-client update dns | Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client. |

| Command | Description |
|-----------------------------------|--|
| ip dhcp update dns | Enables DDNS updates of A and PTR RRs for most address pools. |
| ip host-list | Specifies a list of hosts that will receive DDNS updates of A and PTR RRs. |
| show ip ddns update | Displays information about the DDNS updates. |
| show ip ddns update method | Displays information about the DDNS update method. |
| update dns | Dynamically updates a DNS with A and PTR RRs for some address pools. |

update dns

To dynamically update the Domain Name System (DNS) with address (A) and pointer (PTR) Resource Records (RRs) for some address pools, use the **update dns** command in global configuration mode. To disable dynamic updates, use the **no** form of this command.

update dns [**both** | **never**] [**override**] [**before**]

no update dns [**both** | **never**] [**override**] [**before**]

Syntax Description

| | |
|-----------------|--|
| both | (Optional) Dynamic Host Configuration Protocol (DHCP) server will perform Dynamic DNS (DDNS) updates for both PTR (reverse) and A (forward) RRs associated with addresses assigned from an address pool. |
| never | (Optional) DHCP server will not perform DDNS updates for any addresses assigned from an address pool. |
| override | (Optional) DHCP server will perform DDNS updates for PTR RRs associated with addresses assigned from an address pool, even if the DHCP client has specified in the fully qualified domain name (FQDN) option that the server should not perform updates. |
| before | (Optional) DHCP server will perform DDNS updates before sending the DHCP ACK back to the client. The default is to perform updates after sending the DHCP ACK. |

Defaults

No updates are performed.

Command Modes

DHCP pool 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

If you configure the **update dns both override** command, the DHCP server will perform DDNS updates for both PTR and A RRs associated with addresses assigned from an address pool, even if the DHCP client specified in the FQDN that the server should not.

If the server is configured using this command with or without any of the other 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 act as though it were configured to update both A and PTR records on behalf of the client.

Examples

The following example shows how to configure the DHCP to never update the A and PTR RRs:

```
update dns never
```

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. |

view (DNS)

To access or create the specified Domain Name System (DNS) view list member in the DNS view list and then enter DNS view list member configuration mode, use the **view** command in DNS view list configuration mode. To remove the specified DNS view list member from the DNS view list, use the **no** form of this command.

```
view [vrf vrf-name] {default | view-name} order-number
```

```
no view [vrf vrf-name] {default | view-name} order-number
```

| Syntax Description | |
|----------------------------|---|
| vrf <i>vrf-name</i> | <p>(Optional) The <i>vrf-name</i> argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view. Default is the global VRF (that is, the VRF whose name is a NULL string).</p> <p>Note If the named VRF does not exist, a warning is displayed but the view is added to the view list anyway. The specified VRF can be defined after the view is added as a member of the view list (and after the view itself is defined).</p> <p>Note More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the default keyword) and the VRF with which it is associated.</p> |
| default | <p>Specifies that the DNS view is unnamed.</p> <p>Note More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the default keyword) and the VRF with which it is associated.</p> |
| <i>view-name</i> | <p>String (not to exceed 64 characters) that identifies the name of an existing DNS view.</p> <p>Note If the specified view does not exist, a warning is displayed but the default view list member is added anyway. The specified view can be defined after it is added as a member of DNS view list.</p> <p>Note More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the default keyword) and the VRF with which it is associated.</p> |
| <i>order-number</i> | <p>Integer from 1 to 2147483647 that specifies the order in which the DNS view is checked, with respect to other DNS views in the same DNS view list.</p> <p>Tip If the <i>order-number</i> values for the DNS views within a DNS view list are configured with large intervals between them (for example, by specifying <i>order-number</i> values such as 10, 20, and 30), additional DNS views can be inserted into the view list quickly without affecting the existing ordering or views in the view list. That is, adding a new view to the view list—or changing the ordering of existing views within the view list—does not require that existing views in the view list be removed from the view list and then added back to the list with new <i>order-number</i> values.</p> |

Command Default No DNS view is accessed or created.

Command Modes DNS view list configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.4(9)T | This command was introduced. |

Usage Guidelines This command enters DNS view list member configuration mode—for the specified view list member—so that usage restrictions can be configured for that view list member. If the DNS view list member does not exist yet, the specified DNS view is added to the DNS view list along with the value that indicates the order in which the view list member is to be checked (relative to the other DNS views in the view list) whenever the router needs to determine which DNS view list member to use to address a DNS query.



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.



Note The parameters {**default** | *view-name*} and [**vrf** *vrf-name*] identify an existing DNS view, as defined by using the **ip dns view** command. 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.

The **view** command can be entered multiple times to specify more than one DNS view in the DNS view list.

To display information about a DNS view list, use the **show ip dns view-list** command.

Subsequent Operations on a DNS View List Member

After you use the **view** command to define a DNS view list member and enter DNS view list member configuration mode, you can use any of the following commands to configure usage restrictions for the DNS view list member:

- **restrict authenticated**
- **restrict name-group**
- **restrict source access-group**

These optional, additional restrictions are based on query source authentication, the query hostname, and the query source host IP address, respectively. If none of these optional restrictions are configured for the view list member, the only usage restriction on the view list member is the usage restriction based on its association with a VRF.

Reordering of DNS View List Members

To provide for efficient management of the order of the members in a view list, each view list member definition includes the specification of the position of that member within the list. That is, the order of the members within a view list is defined by explicit specification of position values rather than by the order in which the individual members are added to the list. This enables you to add members to an existing view list or reorder the members within an existing view list without having to remove all the view list members and then redefine the view list membership in the desired order:

Examples

The following example shows how to add the view user3 to the DNS view list userlist5 and assign this view member the order number 40 within the view list. Next, the view user2, associated with the VRF vpn102 and assigned the order number 20 within the view list, is removed from the view list.

```
Router(config)# ip dns view-list userlist5
Router(cfg-dns-view-list)# view user3 40
Router(cfg-dns-view-list-member)# exit
Router(cfg-dns-view-list)# no view vrf vpn102 user2 20
```

Related Commands

| Command | Description |
|-------------------------------------|---|
| 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. |
| 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. |