Split DNS

First Published: June 19, 2006
Last Updated: June 19, 2006

The Split DNS feature enables a Cisco router to respond to Domain Name System (DNS) queries using a specific configuration and associated host table cache that are selected based on certain characteristics of the queries. In a Split DNS environment, multiple DNS databases can be configured on the router, and the Cisco IOS software can be configured to choose one of these DNS name server configurations whenever the router must respond to a DNS query by forwarding or resolving the query.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Split DNS" section on page 102.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Split DNS

No special equipment or software is needed to use the Split DNS feature. To use Split DNS to forward incoming DNS queries, you must have a client that issues DNS queries, a DNS caching name server on which the Split DNS features are to be configured, and a back-end DNS name server. Both of the DNS name server components reside in a Cisco router running the Cisco IOS DNS subsystem software. An example of this basic topology is illustrated in Figure 1 on page 4.

Restrictions for Split DNS

Data Link Layer Redirection

The DNS forwarding functionality provided by Split DNS to the DNS server subsystem of the Cisco IOS software is available only for DNS packets that are directed to one of the IP addresses of the router that serves as the DNS caching name server. Split DNS does not support processing of packets intercepted at the data link layer (Layer 2) and then redirected to the DNS caching name server.

Information About Split DNS

To configure the Split DNS feature, you should understand the following concepts.

Split DNS Feature Overview

The Split DNS feature enables a Cisco router to answer DNS queries using the internal DNS hostname cache specified by the selected virtual DNS name server or, for queries that cannot be answered from the information in the hostname cache, direct queries to specific, back-end DNS servers. The virtual DNS name server is selected based on certain characteristics of each query. Split DNS commands are used to configure a customer premise equipment (CPE) router that serves as the DNS server and forwarder for queries from hosts and as the DNS server and resolver for queries originated by the router itself.

The following sections summarize Split DNS features:

Split DNS Use to Respond to DNS Queries: Benefits

The following sections describe the primary Split DNS features:

- Selection of Virtual DNS Caching Name Server Configurations, page 3
- Ability to Offload Internet Traffic from the Corporate DNS Server, page 3
- Compatibility with NAT and PAT, page 3

Selection of Virtual DNS Caching Name Server Configurations

To configure a Split DNS environment, configure multiple DNS databases on the router and then configure the router to choose one of these virtual DNS server configurations whenever the router must respond to a DNS query by looking up or forwarding the query. The router that acts as the DNS forwarder or resolver is configured with multiple virtual DNS caching name server configurations, each associated with restrictions on the types of DNS queries that can be handled using that name server. The router can be configured to select a virtual forwarding or resolving DNS server configuration based on any combination of the following criteria:

- Query source port
- Query source interface Virtual Private Network (VPN) routing and forwarding (VRF) instance
- Query source authentication
- Query source IP address
- Query hostname

When the router must respond to a query, the Cisco IOS software selects a DNS name server by comparing the characteristics of the query to a list of name servers and their configured restrictions. After the appropriate name server is selected, the router addresses the query using the associated host table cache or forwarding parameters that are defined for that virtual name server.

Ability to Offload Internet Traffic from the Corporate DNS Server

When deployed in an enterprise network that supports many remote hosts with Internet VPN access to the central site, the Split DNS features of the Cisco IOS software enable the router to be configured to direct Internet queries to the Internet service provider (ISP) network, thus reducing the load on the corporate DNS server.

Compatibility with NAT and PAT

Split DNS is compatible with Network Address Translation (NAT) and Cisco IOS Port Address Translation (PAT) upstream interfaces. If NAT or PAT is enabled on the CPE router, DNS queries are translated (by address translation or port translation) to the appropriate destination address, such as an ISP DNS server or a corporate DNS server. When using split tunneling, the remote router routes the Internet-destined traffic directly, not forwarding it over the encrypted tunnel. With a remote client that uses split tunneling, it is possible for the router to direct DNS queries destined for the corporate DNS server to the pushed DNS server list from the central site if the tunnel is up and to direct DNS queries destined for the ISP DNS server to the outside public interface address if the tunnel is down.

Note Split tunneling requires additional security and firewall configuration to ensure the security of the remote site.

Split DNS Operation

A basic network topology for using Split DNS is illustrated in Figure 1. The network diagram shows a CPE router that connects to both an ISP DNS name server and a corporate DNS name server. The diagram also shows three of the CPE client machines that access the router.

Figure 1 A Basic Network Topology for Split DNS

The following sections summarize the network activities in a basic Split DNS environment:

- CPE Router Configuration, page 4
- DNS Query Issued by a CPE Client, page 5
- Virtual DNS Name Server Selection, page 5
- Response to the Client-issued DNS Query, page 5

CPE Router Configuration

Configuration of the CPE router consists of defining DNS caching name server configurations and defining sets of rules for selecting one of the configurations to use for a given DNS query.

- Each DNS caching name server definition specifies an internal DNS hostname cache, DNS forwarding parameters, and DNS resolving parameters.
- Each set of configuration-selection rules consist of a list of name server configurations, with usage restrictions attached to each configuration in the list. The router can be configured with a default set of selection rules, and any router interface can be configured to use a set of selection rules.

DNS Query Issued by a CPE Client

The CPE client can issue DNS queries that request access to the Internet or to the corporate site. The basic network topology in Figure 1 on page 4 shows a CPE router that receives incoming DNS queries from three clients, through interfaces that are enabled with NAT. The three client machines represent typical users of a corporate network:

- PC of a remote teleworker accessing noncorporate Internet sites
- Home PC that is being used by a family member of a home teleworker
- PC of a worker at the corporate site

The clients access the corporate network through a VPN tunnel that originates at the corporate VPN gateway and terminates in the CPE router.

Note The advantage of establishing the VPN tunnel from the corporate access system to the CPE router (rather than the endpoint client system) is that every other computer on the home LAN can also use the same tunnel, making it unnecessary to establish multiple tunnels (one for each system). In addition, the client system end user can use the tunnel when accessing corporate systems, without having to explicitly bring the tunnel up and down each time.

Virtual DNS Name Server Selection

Given an incoming DNS query, the Cisco IOS software uses either the default selection rules or the interface-specific selection rules (depending on the interface on which the query arrived) to select one of the DNS name server configurations in the list. To make the selection, the Cisco IOS software matches the query characteristics to the usage restrictions for each DNS name server configuration in the list. The selected configuration specifies both a host table cache and forwarding parameters, and the router uses this information to handle the query.

Response to the Client-issued DNS Query

The router handles the DNS query using the parameters specified by the selected DNS name server configuration:

1. If the query can be answered using the information in the internal DNS hostname cache specified by the selected virtual DNS name server, the router responds to the query.
2. If the query cannot be answered from the information in the hostname cache but DNS forwarding is enabled for the selected virtual DNS name server, the router sends the query to each of the configured DNS forwarders.
3. If no DNS forwarders are configured for the selected configuration, the router forwards the query using the name servers configured for the virtual DNS name server. For the three client machines (shown in Figure 1 on page 4) that request Internet access or access to the corporate site, the CPE router can forward those DNS queries to the appropriate DNS servers as follows:
   - An Internet access request from the PC of the remote teleworker would be forwarded to the ISP DNS name server.
   - Similarly, an Internet access request from the PC of the family member of the home teleworker also would be forwarded to the ISP DNS name server.
   - A DNS request for access to the corporate site from a worker, though, would be forwarded to the corporate DNS name server.

4. If no domain name servers are configured for the virtual DNS name server, the router forwards the query to the limited broadcast address (255.255.255.255) so that the query is received by all hosts on the local network segment but not forwarded by routers.

DNS Views

A DNS view is a set of parameters that specify how to handle a DNS query. A DNS view defines the following information:

- Association with a VRF
- Option to write to system message logging (syslog) output each time the view is used
- Parameters for resolving internally generated DNS queries
- Parameters for forwarding incoming DNS queries
- Internal host table for answering queries or caching DNS responses

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 following sections describe DNS views in further detail.

View Use Is Restricted to Queries from the Associated VRF

A DNS view is always associated with a VRF, whether it is the global VRF (the VRF whose name is a NULL string) or a named VRF. The purpose of this association is to limit the use of the view to handling DNS queries that arrive on an incoming interface matches a particular VRF:

- The global VRF is the default VRF that contains routing information for the global IP address space of the provider network. Therefore, a DNS view that is associated with the global VRF can be used only to handle DNS queries that arrive on an incoming interface in the global address space.
- A named VRF contains routing information for a VPN instance on a router in the provider network. A DNS view that is associated with a named VRF can be used only to handle DNS queries that arrive on an incoming interface that matches the VRF with which the view is associated.

Note Additional restrictions (described in the "DNS View Lists" section on page 7) can be placed on a view after it has been defined. Also, a single view can be referenced multiple times, with different restrictions added in each case. However, because the association of a DNS view with a VRF is specified in the DNS view definition, the *VRF-specific view-use limitation* is a characteristic of the DNS view definition itself and cannot be separated from the view.

Parameters for Resolving Internally Generated DNS Queries

The following parameters define how to resolve internally generated DNS queries:

- Domain lookup—Enabling or disabling of DNS lookup to resolve hostnames for internally generated queries.
- Default domain name—Default domain to append to hostnames without a dot.
- Domain search list—List of domain names to try for hostnames without a dot.
- Domain name for multicast lookups—IP address to use for multicast address lookups.
- Lookup timeout—Time (in seconds) to wait for a DNS response after sending or forwarding a query.
- Lookup retries—Number of retries when sending or forwarding a query.
- Domain name servers—List of name servers to use to resolve domain names for internally generated queries.
- Resolver source interface—Source interface to use to resolve domain names for internally generated queries.
- Round-robin rotation of IP addresses—Enabling or disabling of the use of a different IP address associated with the domain name in cache each time hostnames are looked up.

Parameters for Forwarding Incoming DNS Queries

The following parameters define how to forward incoming DNS queries:

- Forwarding of queries—Enabling or disabling of forwarding of incoming DNS queries.
- Forwarder addresses—List of IP addresses to use to forward incoming DNS queries.
- Forwarder source interface—Source interface to use to forward incoming DNS queries.

DNS View Lists

A DNS view list is an ordered list of DNS views in which additional usage restrictions can be specified for any individual member in the list. The scope of these optional usage restrictions is limited to a specific member of a specific DNS view list. When the router must respond to a DNS query, the Cisco IOS software uses a DNS view list to select the DNS view that will be used to handle 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.

Order in Which to Check the Members of a DNS View List

When a DNS view list is used to select a DNS view for handling a given DNS query, the Cisco IOS software checks each member of the view list—in the order specified by the list—and selects the first view list member whose restrictions permit the view to be used with the query that needs to be handled.

Usage Restrictions Defined for a DNS View in the View List

A DNS view list member can be configured with usage restrictions defined using access control lists (ACLs) that specify rules for selecting that view list member based on the query hostname or the query source host IP address. The two types of ACLs supported by the Split DNS view list definition are described in the "DNS Name Groups" section on page 8.

Note Multiple DNS view lists can be defined so that, for example, a given DNS view can be associated with different restrictions in each list. Also, different DNS view lists can include different DNS views.

Selection of the DNS View List

When the router that is acting as the DNS caching name server needs to respond to a DNS query, the Cisco IOS software uses a DNS view list to determine which DNS view can be used to handle the query:

- If the router is responding to an incoming query that arrives on an interface for which a DNS view list is configured, the *interface-specific DNS view list* is used.
- If the router is responding to an incoming query that arrives on an interface for which no specific DNS view list is configured, the *default DNS view list* is used.

If the router is responding to an internally generated query, no DNS view list is used to select a view; the *global DNS view* is used to handle the query.

The assignment of a DNS view list as the default or to an interface is described in the "DNS View Groups" section on page 9.

Selection of a DNS View List Member

The view list members are compared, each in turn, to the characteristics of the DNS query that the router is responding to:

1. If the query is from a different VRF than the view, the view cannot be used to address the query, so the view-selection process moves on to the next member of the view list.
2. The specification of additional view-use restrictions is an optional setting for any view list member.

   If the query list *does not* specify additional restrictions on the view, the view will be used to address the query, so the view-selection process is finished.

   If the view list *does* specify additional restrictions on the view, the query is compared to those restrictions:

   - If the query characteristics fail any view-use restriction, the view cannot be used to address the query, so the view-selection process moves on to the next member of the view list.
   - If the query characteristics pass all the view-use restrictions, the view will be used to address the query. The view-selection process is finished.
3. If the view-selection process reaches the end of the selected DNS view list without finding a view list member that can handle the query, the router discards the query.

The first DNS view list member that is found to have restrictions that match the query characteristics is used to handle the query.

DNS Name Groups

The Split DNS feature supports two types of ACLs that can be used to restrict the use of a DNS view. A DNS name list or a standard IP ACL (or both) can be applied to a DNS view list member to specify view-use restrictions in addition to the VRF-specific restriction that is a part of the view definition itself.

Note In this context, the term “group” is used to refer to the specification of a DNS name list or a standard IP ACL as a usage restriction on a view list member.

DNS View Usage Restrictions Based on the Query Hostame

A DNS name list is a named set of hostname pattern-matching rules, with each rule specifying the type of action to be performed if a query hostname matches the text string pattern in the rule. In order for a query hostname to match a name list, the hostname must match a rule that explicitly permits a matching pattern but the hostname cannot match any rules that explicitly deny a matching pattern.

DNS View Usage Restrictions Based on the Query Source IP Address

A standard IP ACL is a numbered or named set of host IP address-matching rules, with each rule specifying the type of action to be performed if an IP address matches the text string pattern in the rule. The Split DNS feature supports the use of a standard ACL as a view-use restriction based on the query source IP address. In order for a source IP address to match a name list, the IP address must match a rule that explicitly permits a matching pattern but the IP address cannot match any rules that explicitly deny a matching pattern.

DNS View Groups

The Split DNS feature provides two ways to specify the DNS view list that the Cisco IOS software is to use to select the DNS view that will be used to handle an incoming DNS query. For a query that arrives on an interface that is configured to use a particular DNS view list, the interface-specific DNS view list is used. Otherwise, the default DNS view list is used.

Note In this context, the term “group” refers to the specification of a DNS view list as an interface-specific DNS view list or the default view list for the router.

Interface-specific View Lists

A DNS view list can be attached to a router interface. When an incoming DNS query arrives on that interface, the Cisco IOS software uses that view list to select a DNS view to use to handle the query.

Default DNS View List

A DNS view list can be configured as the default DNS view list for the router. When an incoming DNS query arrives on an interface that is not configured to use a specific view list, the Cisco IOS software uses the default view list to select the DNS view to use to handle the query.

Router Response to DNS Queries in a Split DNS Environment

By introducing support of DNS views—and the ability to configure the router to select from a list of appropriate views for a given DNS query—the Split DNS feature enables different hosts and subsystems to use different virtual DNS caching name servers, each with their own, separate DNS cache and each accessible from a single router that acts as the DNS forwarder and resolver. Thus, each DNS view defines a different DNS database on a single router. Furthermore, because the Split DNS feature separates the configuration of DNS query forwarding and resolving parameters, it is a simple matter to configure the router to respond more freely to queries from internal clients while limiting response to queries from external clients.

The following sections provide detailed descriptions of how the router responds to DNS queries in a Split DNS environment.

Response to Incoming DNS Queries per the Forwarding Parameters of the Selected DNS View

Given an incoming DNS query, the Cisco IOS software uses the DNS view list configured for that interface to select the DNS view list to use to handle the query. If no view list is configured for the interface, the default DNS view list is used instead.

Using the configured or default view list, the router software selects the first view list member that is associated with the same VRF as the query and whose usage restrictions match the query characteristics. After the DNS view is selected, the router handles the query according to the parameters configured in the selected view.

1. The router uses the DNS view list that is specified for the interface on which the DNS query arrives:
   a. If a DNS view list is attached to the interface, the router uses the specified DNS view list.
   b. If no DNS view list is attached to the interface, the router uses the default DNS view list.
2. The router uses the DNS view list to select a DNS view to use to address the query. Each view list member is checked, in the order defined by the view list, as follows:
   a. If the view list member is associated with a different VRF from that of the incoming interface for the DNS query that needs to be resolved, the view-selection process moves on to the next member of the view list.
   b. If all the usage restrictions on the view list member match the other characteristics of the DNS query to be resolved, the view is selected to handle the query.

      Otherwise, the view-selection process moves on to the next member of the view list.

      If no member of the default DNS view list is qualified to address the query, the router does nothing further with the query.
3. The router attempts to respond to the query using the parameters specified by the selected DNS view:
   a. The Cisco IOS software looks in the hostname cache associated with the view. If the query can be answered from that information, the router responds to the query.
   b. If the query cannot be answered using the hostname cache, the Cisco IOS software checks whether the DNS forwarding of queries is enabled for the view. If DNS forwarding is enabled, the router sends the query to each of the configured DNS forwarders.
   c. If no DNS forwarders are configured for the view, the router forwards the query using the configured domain name servers.
   d. If no domain name servers are configured for the view, the router forwards incoming DNS queries to the limited broadcast address (255.255.255.255) so that the queries are received by all hosts on the local network segment but not forwarded by routers.

Response to Internally Generated DNS Queries per the Resolving Parameters of the Default Global DNS View

Given an internally generated DNS query to resolve, the Cisco IOS software uses the default DNS view to handle the query:

- When a hostname must be resolved for a query that does not specify a VRF, the router uses the unnamed DNS view associated with the global VRF (the default VRF that contains routing information for the global IP address space of the provider network).
- When a hostname must be resolved for a Cisco IOS command that specifies a VRF to use, the router uses the unnamed DNS view associated with that VRF.

The router attempts to respond to the query using the DNS resolving parameters specified by that view:

1. If the query specifies an unqualified hostname, the Cisco IOS software completes the hostname using the domain name list or the default domain specified by the view.
2. The Cisco IOS software looks in the hostname cache associated with the view. If the query can be answered from that information, the router responds to the query.
3. Otherwise, because the query cannot be answered using the hostname cache, the Cisco IOS software checks whether the DNS forwarding of queries is enabled for the view. If so, the router sends the query to each of the configured name servers, using the timeout period and number of retries specified for the view.
4. Otherwise, the router does not respond to the query.

How to Configure Split DNS

This section describes the following tasks:

Enabling Split DNS Debugging Output

Enabling a Split DNS **debug** command enables output to be written at every occurrence of a DNS name list event, a DNS view event, or a DNS view list event. The router continues to generate such output until you enter the corresponding **no debug** command. You can use the output from the Split DNS **debug** commands to diagnose and resolve internetworking problems associated with Split DNS operations.

Note By default, the network server sends the output from the **debug** commands to the console. Sending output to a terminal (virtual console) produces less overhead than sending it to the console. Use the **terminal monitor** privileged EXEC command to send output to a terminal. For more information about redirecting **debug** command output, see the "Using Debug Commands" chapter of the *Cisco IOS Debug Command Reference*.

A DNS name list event can be of any of the following:

- The addition or removal of a DNS name list entry (a hostname pattern and action to perform on an incoming DNS query for a hostname that matches the pattern).
- The removal of a DNS name list.

A DNS view event can be any of the following:

- The addition or removal of a DNS view definition.
- The addition or removal of a DNS forwarding name server setting for a DNS view.
- The addition or removal of a DNS resolver setting for a DNS view.
- The enabling or disabling of logging of a syslog message each time a DNS view is used.

A DNS view list event can be any of the following:

- The addition or removal of a DNS view list definition.
- The addition or removal of a DNS view list member (a DNS view and the relative order in which it is to be checked in the view list) to or from a DNS view list.
- The setting or clearing of a DNS view list assignment as the default view list for the router or to a specific interface on the router.

Perform this optional task if you want to enable the writing of an event message to syslog output for DNS name list events, view events, or view list events:

SUMMARY STEPS

1. **enable**
2. **debug ip dns name-list**
3. **debug ip dns view**
4. **debug ip dns view-list**
5. **show debugging**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip dns name-list** **Example:** `Router# debug ip dns name-list`	(Optional) Enables the writing of DNS name list event messages. • Debugging output for DNS name lists is disabled by default. • To disable debugging output for DNS name list events, use the **no** form of this command.
Step 3	**debug ip dns view** **Example:** `Router# debug ip dns view`	(Optional) Enables the writing of DNS view event messages. • Debugging output for DNS views is disabled by default. • To disable debugging output for DNS view events, use the **no** form of this command.
Step 4	**debug ip dns view-list** **Example:** `Router# debug ip dns view-list`	(Optional) Enables the writing of DNS view list event messages. • Debugging output for DNS view lists is disabled by default. • To disable debugging output for DNS view list events, use the **no** form of this command.
Step 5	**show debugging** **Example:** `Router# show debugging`	Displays the state of each debugging option.

Defining a DNS Name List

Perform this optional task if you need to define a DNS name list. A DNS name list is a list of hostname pattern-matching rules that could be used as an optional usage restriction on a DNS view list member.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ip dns name-list** *name-list-number* [{**deny** | **permit**} *pattern*]
4. **ip dns name-list** *name-list-number* {**deny** | **permit**} *pattern*
5. **exit**
6. **show ip dns name-list** [*name-list-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no ip dns name-list** *name-list-number* [{**deny** | **permit**} *pattern*] **Example:** `Router(config)# no ip dns name-list 500`	(Optional) Clears any previously defined DNS name list. • To clear only an entry in the list, specify the deny or permit clause. • To clear the entire list, omit any clauses.
Step 4	**ip dns name-list** *name-list-number* {**deny** | **permit**} *pattern* **Example:** `Router(config)# ip dns name-list 500 deny .*.example.com`	Creates a new entry in the specified DNS name list. • The *pattern* argument specifies a regular expression that will be compared to the query hostname. For a detailed description of regular expressions and regular expression pattern-matching characters, see the appendix titled "Regular Expressions" in the *Cisco IOS Terminal Services Configuration Guide*. • The **deny** keyword specifies that any name matching the specified pattern immediately terminates matching the name list with a negative result. The **permit** keyword specifies that any name matching the specified pattern immediately terminates matching the name list with a positive result. • Enter this command multiple times as needed to create multiple deny and permit clauses. • To apply a DNS name list to a DNS view list member, use the **restrict name-group** command.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 6	**show ip dns name-list** [*name-list-number*] **Example:** `show ip dns name-list`	Displays a particular DNS name list or all configured name lists.

Defining a DNS View

Perform this task to define a DNS view. A DNS view definition can be used to respond to either an incoming DNS query or an internally generated DNS query.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dns view** [**vrf** *vrf-name*] {**default** | *view-name*}
4. [**no**] **logging**
5. [**no**] **domain lookup**
6. **domain name** *domain-name*
   or
   domain list *domain-name*
7. **domain name-server** *name-server-ip-address*
   or
   domain name-server interface *interface*
8. **domain multicast** *domain-name*
9. **domain retry** *number*
10. **domain timeout** *seconds*
11. [**no**] **dns forwarding**
12. **dns forwarder** [**vrf** *vrf-name*] *forwarder-ip-address*
13. **dns forwarding source-interface** *interface*
14. **end**
15. **show ip dns view** [**vrf** *vrf-name*] [**default** | *view-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dns view** [**vrf** *vrf-name*] {**default** | *view-name*} **Example:** `Router(config)# ip dns view vrf vpn101 user3`	Defines a DNS view and enters DNS view configuration mode.

	Command or Action	Purpose

Step 4	`[no] logging`
	
	Example:
	`Router(cfg-dns-view)# logging`
		(Optional) Enables or disables logging of a syslog message each time the DNS view is used.
		
		Note View-specific event logging is disabled by default.

Step 5	`[no] domain lookup`
	
	Example:
	`Router(cfg-dns-view)# domain lookup`
		(Optional) Enables or disables DNS-based hostname-to-address translation for internally generated DNS queries handled using the DNS view.
		
		Note The domain lookup capability is enabled by default.

Step 6	**domain name** *domain-name*
	
	or
	
	domain list *domain-name*
	
	Example:
	`Router(cfg-dns-view)# domain name example.com`
	
	or
	
	Example:
	`Router(cfg-dns-view)# domain list example1.com`
		(Optional) Defines a default domain name to be used by this DNS view to complete unqualified hostnames when addressing DNS queries.
		
		or
		
		(Optional) Defines a list of domain names to be used by this DNS view to complete unqualified hostnames when addressing DNS queries.
		
		• The router attempts to respond to the query using the parameters specified by the selected DNS view. First, the Cisco IOS software looks in the hostname cache associated with the view. If the query can be answered from that information, the router responds to the query. Otherwise, because the query cannot be answered using the hostname cache, the router forwards the query using the configured domain name servers.
		• If the router is using this view to handle a DNS query for an unqualified hostname and domain lookup is enabled for the view, the Cisco IOS software appends a domain name (either a domain name from the domain name list or the default domain name) in order to perform any of the following activities:
		– Looking up the hostname in the name server cache.
		– Forwarded the query to other name servers (whether to the hosts specified as DNS forwarders in the selected view or to the limited broadcast address).
		• You can specify a single, default domain name, an ordered list of domain names, or both. However, the default domain name is used only if the domain list is empty.

	Command or Action	Purpose

Step 7	**domain name-server** *name-server-ip-address*
	
	or
	
	domain name-server interface *interface*
	
	Example:
	`Router(cfg-dns-view)# domain name-server 192.168.2.124`
	
	or
	
	Example:
	`Router(cfg-dns-view)# domain name-server interface FastEthernet0/1`
		(Optional) Defines a list of name servers to be used by this DNS view to resolve internally generated DNS queries.
		
		or
		
		(Optional) Defines an interface on which to acquire (through DHCP or PPP interaction on the interface) the IP address of a DNS server to add to the list of DNS name servers to be used by this DNS view to resolve internally generated DNS queries.
		
		• If both of these commands are configured, DHCP or PPP interaction on the interface causes another IP address to be added to the list.

Step 8	**domain multicast** *domain-name* **Example:** `Router(cfg-dns-view)# domain multicast www.example8.com`	(Optional) Specifies the IP address to use for multicast lookups handled using the DNS view.
Step 9	**domain retry** *number* **Example:** `Router(cfg-dns-view)# domain retry 4`	(Optional) Defines the number of times to perform a retry when using this DNS view to send or forward DNS queries. **Note** The number of retries is 2 by default.
Step 10	**domain timeout** *seconds* **Example:** `Router(cfg-dns-view)# domain timeout 5`	(Optional) Defines the number of seconds to wait for a response to a DNS query sent or forwarded when using this DNS view. **Note** The time to wait is 3 seconds by default.
Step 11	[**no**] **dns forwarding** **Example:** `Router(cfg-dns-view)# dns forwarding`	(Optional) Enables or disables forwarding of incoming DNS queries handled using the DNS view. **Note** The query forwarding capability is enabled by default.
Step 12	**dns forwarder** [**vrf** *vrf-name*] *forwarder-ip-address* **Example:** `Router(cfg-dns-view)# dns forwarder 192.168.3.240`	Defines a list of name servers to be used by this DNS view to forward incoming DNS queries. • If no forwarding name servers are defined, then the configured list of domain name servers is used instead. • If no name servers are configured either, then queries are forwarded to the limited broadcast address.
Step 13	**dns forwarding source-interface** *interface* **Example:** `Router(cfg-dns-view)# dns forwarding source-interface FastEthernet0/0`	Defines the interface on which to forward queries when this DNS view is used.

	Command or Action	Purpose
Step 14	**end** **Example:** `Router(cfg-dns-view)# end`	Returns to privileged EXEC mode.
Step 15	**show ip dns view** [**vrf** *vrf-name*] [**default** | *view-name*] **Example:** `Router# show ip dns view vrf vpn101 user3`	Displays information about a particular DNS view, a group of views (with the same view name or associated with the same VRF), or all configured DNS views.

Defining Static Entries in the Hostname Cache for a DNS View

Typically, it is easier to refer to network devices by symbolic names rather than numerical addresses (services such as Telnet can use hostnames or addresses). Hostnames and IP addresses can be associated with one another through static or dynamic means. Manually assigning hostnames-to-address mappings is useful when dynamic mapping is not available.

Perform this optional task if you need to define static entries in the DNS hostname cache for a DNS view.

SUMMARY STEPS

1. **enable**
2. **clear host** [**view** *view-name* | **vrf** *vrf-name* | **all**] {*hostname* | *****}
3. **configure terminal**
4. **ip host** [**vrf** *vrf-name*] [**view** *view-name*] *hostname* {*ip-address1* [*ip-address2...ip-address8*] | **additional** *ip-address9* [*ip-address10...ip-addressn*]}
5. **exit**
6. **show hosts** [**vrf** *vrf-name*] [**view** *view-name*] [**all** | *hostname*] [**summary**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear host** [**view** *view-name* | **vrf** *vrf-name* | **all**] {*hostname* | *****} **Example:** `Router# clear host all *`	(Optional) Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all configured views. • Use the **view** keyword and *view-name* argument to specify the DNS view whose hostname cache is to be cleared. Default is the default DNS view associated with the specified or global VRF. • Use the **vrf** keyword and *vrf-name* argument to specify the VRF associated with the DNS view whose hostname cache is to be cleared. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view. • Use the **all** keyword to specify that hostname-to-address mappings are to be deleted from the hostname cache of every configured DNS view. • Use the *hostname* argument to specify the name of the host for which hostname-to-address mappings are to be deleted from the specified hostname cache. • Use the ***** keyword to specify that all the hostname-to-address mappings are to be deleted from the specified hostname cache.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**ip host** [**vrf** *vrf-name*] [**view** *view-name*] *hostname* {*ip-address1* [*ip-address2*...*ip-address8*] | **additional** *ip-address9* [*ip-address10*...*ip-addressn*]} **Example:** `Router(config)# ip host vrf vpn101 view user3 www.example.com 192.168.2.111 192.168.2.112`	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view. • 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. • Use the *hostname* argument to specify the name of the host for which hostname-to-address mappings are to be added to the specified hostname cache. • To bind more than eight addresses to a hostname, you can use the ip host command again and use the **additional** keyword.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 6	**show hosts** [**vrf** *vrf-name*] [**view** *view-name*] [**all** | *hostname*] [**summary**] **Example:** `Router# show hosts vrf vpn101 view user3 www.example.com`	(Optional) 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. • 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. • Use the **all** keyword if the specified hostname cache information is to be displayed for all configured DNS views. • Use the *hostname* argument if the specified name cache information displayed is to be limited to entries for a particular hostname.

Defining a DNS View List

Perform this task to define an ordered list of DNS views with optional, additional usage restrictions for each view list member. The router uses a DNS view list to select the DNS view that will be used to handle a DNS query.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dns view-list** *view-list-name*
4. **view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number*
5. **restrict name-group** *name-list-number*
6. **restrict source access-group** *acl-number*
7. **exit**
8. **end**
9. **show ip dns view-list** *view-list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dns view-list** *view-list-name* **Example:** `Router(config)# ip dns view-list userlist5`	Defines a DNS view list and enters DNS view list configuration mode.
Step 4	**view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number* **Example:** `Router(cfg-dns-view-list)# view vrf vpn101 user5 10`	Defines a DNS view list member and enters DNS view list member configuration mode.
Step 5	**restrict name-group** *name-list-number* **Example:** `Router(cfg-dns-view-list-member)# restrict name-group 500`	(Optional) Specifies that this DNS view list member cannot be used to respond to a DNS query unless the query hostname matches a permit clause in the specified DNS name list and none of the deny clauses. • To define a DNS name list entry, use the **ip dns name-list** command.
Step 6	**restrict source access-group** *acl-number* **Example:** `Router(cfg-dns-view-list-member)# restrict access-group 99`	(Optional) Specifies that this DNS view list member cannot be used to respond to a DNS query unless the source IP address of the DNS query matches the specified standard ACL. • To define a standard ACL entry, use the **access-list** command.
Step 7	**exit** **Example:** `Router(cfg-dns-view-list-member)# exit`	Exits DNS view list member configuration mode. • To add another view list member to the list, go to Step 4.
Step 8	**end** **Example:** `Router(cfg-dns-view-list)# end`	Returns to privileged EXEC mode.
Step 9	**show ip dns view-list** *view-list-name* **Example:** `Router# show ip dns view-list userlist5`	Displays information about a particular DNS view list or all configured DNS view lists.

Modifying a DNS View List

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 perform either of the following tasks without having to remove all the view list members and then redefine the view list membership in the desired order:

- Adding a Member to a DNS View List Already in Use, page 22
- Changing the Order of the Members of a DNS View List Already in Use, page 23

Adding a Member to a DNS View List Already in Use

Perform this optional task if you need to add another member to a DNS view list that is already in use.

For example, suppose the DNS view list named userlist5 is already defined and in use as a default view list or as an interface-specific view list. Assume that the list consists of the following members:

- DNS view user1 with position number 10
- DNS view user2 with position number 20
- DNS view user3 with position number 30

If you need to add DNS view user4 as the second member of the list, add that view to the list with a position number value from 11 to 19. You do not need to remove the three existing members and then add all four members to the list in the desired order.

SUMMARY STEPS

1. **enable**
2. **show ip dns view-list** *view-list-name*
3. **configure terminal**
4. **ip dns view-list** *view-list-name*
5. **view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number*
6. **end**
7. **show ip dns view-list** *view-list-name*

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**show ip dns view-list** *view-list-name* **Example:** `Router# show ip dns view-list userlist5`	Displays information about a particular DNS view list or all configured DNS view lists.

	Command or Action	Purpose
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**ip dns view-list** *view-list-name* **Example:** `Router(config)# ip dns view-list userlist5`	Defines a DNS view list and enters DNS view list configuration mode.
Step 5	**view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number* **Example:** `Router(cfg-dns-view-list)# view user4 15`	Defines a DNS view list member and enters DNS view list member configuration mode.
Step 6	**end** **Example:** `Router(cfg-dns-view-list-member)# end`	Returns to privileged EXEC mode.
Step 7	**show ip dns view-list** *view-list-name* **Example:** `Router# show ip dns view-list userlist5`	Displays information about a particular DNS view list or all configured DNS view lists.

Changing the Order of the Members of a DNS View List Already in Use

Perform this optional task if you need to change the order of the members of a DNS view list that is already in use.

For example, suppose the DNS view list named userlist5 is already defined and in use as a default view list or as an interface-specific view list. Assume that the list consists of the following members:

- DNS view user1 with position number 10
- DNS view user2 with position number 20
- DNS view user3 with position number 30

If you want to move DNS view user1 to the end of the list, remove that view from the list and then add it back to the list with a position number value greater than 30. You do not need to remove the three existing members and then add the members back to the list in the desired order.

SUMMARY STEPS

1. **enable**
2. **show ip dns view-list** *view-list-name*
3. **configure terminal**
4. **ip dns view-list** *view-list-name*
5. **no view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number*
6. **view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number*

7. **end**
8. **show ip dns view-list** *view-list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip dns view-list** *view-list-name* **Example:** `Router# show ip dns view-list userlist5`	Displays information about a particular DNS view list or all configured DNS view lists.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**ip dns view-list** *view-list-name* **Example:** `Router(config)# ip dns view-list userlist5`	Defines a DNS view list and enters DNS view list configuration mode.
Step 5	**no view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number* **Example:** `Router(cfg-dns-view-list)# no view user1 10`	Removes a DNS view list member from the list.
Step 6	**view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number* **Example:** `Router(cfg-dns-view-list)# view user1 40`	Defines a DNS view list member and enters DNS view list member configuration mode.
Step 7	**end** **Example:** `Router(cfg-dns-view-list-member)# end`	Returns to privileged EXEC mode.
Step 8	**show ip dns view-list** *view-list-name* **Example:** `Router# show ip dns view-list userlist5`	Displays information about a particular DNS view list or all configured DNS view lists.

Specifying the Default DNS View List for the Router's DNS Server

Perform this task to specify the default DNS view list for the router's DNS server. The router uses the default DNS view list to select a DNS view to use to handle an incoming DNS query that arrives on an interface for which no interface-specific DNS view list has been defined.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dns server view-group** *view-list-name*
4. **exit**
5. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dns server view-group** *name-list-number* **Example:** `Router(config)# ip dns server view-group 500`	Configures the default DNS view list for the router's DNS server.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 5	**show running-config** **Example:** `Router# show running-config`	Displays information about how DNS view lists are applied. The default DNS view list, if configured, is listed in the default DNS view information as the argument for the **ip dns server view-group** command.

Specifying a DNS View List for a Router Interface

Perform this optional task if you need to specify a DNS view list for a particular router interface. The router uses that view list to select a DNS view to use to handle a DNS query that arrives on that interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface*
4. **ip dns view-group** *view-list-name*
5. **end**
6. **show running-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface` *interface* **Example:** `Router(config)# interface ATM2/0`	Configures an interface type and enter interface configuration mode so that the specific interface can be configured.
Step 4	`ip dns view-group` *view-list-name* **Example:** `Router(config-if)# ip dns view-group userlist5`	Configures the DNS view list for this interface on the router.

Step 5	`end`
	
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 6	`show running-config`
	
	Example:
	`Router# show running-config`
		Displays information about how DNS view lists are applied. Any DNS view lists attached to interfaces are listed in the information for each individual interface, as the argument for the **ip dns view-group** command.

Configuration Examples for Split DNS

This section provides the following configuration examples:

- Split DNS View Limited to Queries from a Specific VRF: Example, page 27
- Split DNS View with Dynamic Name Server Configuration: Example, page 27
- Split DNS View with Statically Configured Hostname Cache Entries: Example, page 28

Split DNS View Limited to Queries from a Specific VRF: Example

The following example shows how to define two different VRFs and then define two different DNS views that are associated with those VRFs:

```
ip vrf vpn101
 description VRF vpn101 for example purposes
 rd 10:112
 exit
!
ip vrf vpn102
 description VRF vpn102 for example purposes
 rd 10:128
 exit
!
ip dns view vrf vpn101
 .
 .
 .
exit
!
ip dns view vrf vpn102 user1
 .
 .
 .
exit
```

The two DNS views are both named user1, but each view is associated with a different VRF.

- The default DNS view associated with VRF vpn101 is limited to handling DNS queries from VRF vpn101 only. This view will be used by the resolver for commands which specify a VRF, such as **ping vrf vpn101 www.example.com**.
- The DNS view user1 associated with VRF vpn102 is limited to handling DNS queries from VRF vpn102 only. This view will only be used if specified inside a DNS view list that is configured for use by the DNS server globally or for a specific interface.

The two DNS views in this example can be configured with the same DNS resolving and forwarding parameters, or they can be configured with different DNS resolving and forwarding parameters.

Split DNS View with Dynamic Name Server Configuration: Example

The following example shows how to populate the list of resolving name servers for the default DNS view in the global namespace with three statically defined IP addresses. The example also shows how to configure the router to be able to dynamically acquire, through DHCP or PPP interaction on FastEthernet slot 0, port 1, name server IP addresses to add to the list of resolving name servers for that view:

```
ip dns view default
 domain lookup
 domain name-server 192.168.2.204
 domain name-server 192.168.2.205
 domain name-server 192.168.2.206
```

```
 domain name-server interface FastEthernet0/0
```

Split DNS View with Statically Configured Hostname Cache Entries: Example

The following example shows how to statically add three hostname-to-address mappings for the host www.example.com in the DNS hostname cache for the DNS view user5 that is associated with VRF vpn101:

```
clear host all *
 ip host vrf vpn101 view user5 www.example.com 192.168.2.10 192.168.2.20 192.168.2.30
 exit
show hosts vrf vpn101 view user5
```

Note It does not matter whether the VRF vpn101 has been defined. The hostname cache for this DNS view will be automatically created, and the hostname will be added to the cache.

Split DNS View with Round-Robin Rotation of Hostname Cache Entries: Example

When resolving DNS queries using a DNS view for which the hostname cache contains hostnames that are associated with multiple IP addresses, the router sends those queries to the first associated IP address in the hostname cache. By default, the other associated addresses in the hostname cache are used only in the event of host failure.

The round-robin rotation of hostname cache entries specifies that each time a hostname in the internal cache is accessed, the list of IP addresses associated with that hostname should be rotated such that the second IP address in the list becomes the first one and the first one is moved to the end of the list. For a more detailed description of round-robin functionality, see the description of the **ip domain round-robin** command in the *Cisco IOS IP Addressing Services Command Reference*.

The following example shows how to define the hostname www.example.com with three IP addresses and then enable round-robin rotation for the default DNS view associated with the global VRF. Each time that hostname is referenced internally or queried by a DNS client sending a query to the Cisco IOS DNS server on this system, the order of the IP addresses associated with the host www.example.com will be changed. Because most client applications look only at the first IP address associated with a hostname, this results in different clients using each of the different addresses and thus distributing the load among the three different IP addresses.

```
ip host view www.example.com 192.168.2.10 192.168.2.20 192.168.2.30
!
ip dns view default
 domain lookup
 domain round-robin
```

Split DNS Configuration of ACLs That Can Limit DNS View Use: Example

The following example shows how to configure one DNS name list and one standard IP ACL:

- A DNS name list is a list of hostname pattern-matching rules that can be used to restrict the use of a DNS view list member.
- A standard IP ACL is a list of IP addresses that can be used to restrict the use of a DNS view list member.

Both types of lists can be used to limit the types of DNS queries that a DNS view is allowed to handle.

```
! Define a DNS name-list
!
ip dns name-list 151 deny .*.example1.net
! (Note: The view fails this list if the query hostname matches this)
!
ip dns name-list 151 permit .*.example1.com
ip dns name-list 151 permit www.example1.org
! (Note: All other access implicitly denied)
!
! Define a standard IP ACL
!
access-list 71 deny 192.168.2.64 0.0.0.63
! (Note: The view fails this list if the query source IP matches this)
!
access-list 71 permit 192.168.2.128 0.0.0.63
! (Note: All other access implicitly denied)
```

Using this configuration example, suppose that the first member of a DNS view list is configured to use DNS name list 151 as a usage restriction. Then, if the router were to use that DNS view list to select the DNS view to use to handle a given DNS query, the view-selection steps would begin as follows:

1. If the DNS query is for a hostname that matches the string *.example1.net, the first DNS view list member is immediately rejected and the view-selection process moves on to the second member of DNS view list.
2. If the DNS query is for a hostname that matches the string *.example1.com, the first DNS view list member is selected to handle the query.
3. If the DNS query is for a hostname that matches the string www.example1.org, the first DNS view list member is selected to handle the query. Otherwise, the first DNS view list member is rejected and the view-selection process moves on to the second member of DNS view list.

Continuing to use this configuration example, suppose that this same DNS view list member is also configured to use standard IP ACL 71 as a usage restriction. Then, even if the *query hostname* matched DNS name list 151, the *query source IP address* would have to match standard IP ACL 71 before that view would be selected to handle the query. To validate this second usage restriction, the DNS view-selection steps would continue as follows:

1. If the DNS query source IP address matches 192.168.2.64, the first DNS view list member is selected to handle the query.
2. If the DNS query source IP address matches 192.168.2.128, the first DNS view list member is selected to handle the query. Otherwise, the first DNS view list member is rejected and the view-selection process moves on to the second member of the DNS view list.

Split DNS View Lists Configured with Different View-use Restrictions: Example

The following example shows how to define two DNS view lists, userlist1 and userlist2. Both view lists comprise the same three DNS views:

- DNS view user1 that is associated with the usergroup10 VRF
- DNS view user2 that is associated with the usergroup20 VRF
- DNS view user3 that is associated with the usergroup30 VRF

Both view lists contain the same DNS views, specified in the same order:

```
ip dns view-list userlist15
 view vrf usergroup100 user1 10
  restrict name-group 121
  exit
view vrf usergroup200 user2 20
  restrict name-group 122
  exit
view vrf usergroup300 user3 30
  restrict name-group 123
  exit
!
exit
ip dns view-list userlist16
 view vrf usergroup100 user1 10
  restrict name-group 121
  restrict source access-group 71
  exit
 view vrf usergroup200 user2 20
  restrict name-group 122
  restrict source access-group 72
  exit
 view vrf usergroup300 user3 30
  restrict name-group 123
  restrict source access-group 73
  exit
exit
```

The two DNS view lists differ, though, in the usage restrictions placed on their respective view list members. DNS view list userlist15 places only query hostname restrictions on its members while view list userlist16 restricts each of its members on the basis of the query hostname and the query source IP address:

- Because the members of userlist15 are restricted only based on the VRF from which the query originates, userlist15 is typical of a view list that can be used to select a DNS view for handling DNS requests from internal clients.
- Because the members of userlist16 are restricted not only by the query VRF and query hostname but also by the query source IP address, userlist16 is typical of a view list that can be used to select a DNS view for handling DNS requests from external clients.

Split DNS Configuration of Default and Interface-specific View Lists: Example

The following example shows how to configure the default DNS view list and two interface-specific view lists:

```
ip dns server view-group userlist1
!
interface FastEthernet 0/0
```

```
 ip dns view-group userlist2
 exit
!
interface FastEthernet 0/1
 ip dns view-group userlist3
 exit
```

The Cisco IOS software uses the DNS view list named userlist1 to select the DNS view to use to respond to incoming queries that arrive on router interfaces that are not configured to use a specific view list. View list userlist1 is configured as the default DNS view list for the router.

The Cisco IOS software uses the DNS view list named userlist2 to select the DNS view to use for incoming queries that arrive on port 0 of the FastEthernet card in slot 0.

The Cisco IOS software uses the DNS view list named userlist3 to select the DNS view to use for incoming queries that arrive on port 1 of the FastEthernet card in slot 0.

Additional References

The following sections provide references related to the Split DNS feature.

Related Documents

Related Topic	Document Title
IP addressing services configuration tasks	*Cisco IOS IP Addressing Services Configuration Guide*, Release 12.4T
IP addressing services commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*, Release 12.4T
How MPLS VPNs in a Cisco IOS network use VRFs to deploy scalable Layer 3 VPN backbone services: • Definition of a VRF • VRF-aware DNS configuration tasks: Defining VPN routing instances and creating VRFs for each VPN	"Part 1: Basic MPLS" of the *Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4: • "Multiprotocol Label Switching Overview" chapter • "Configuring Multiprotocol Label Switching" chapter
VRF-aware DNS configuration tasks: Enabling VRF-aware DNS, mapping VRF-specific hostnames to IP addresses, configuring a static entry in a VRF-specific hostname cache, and verifying the hostname cache entries in the VRF table VRF-aware DNS commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*VRF-Aware DNS*, Release 12.4(4)T
All **debug** commands: Using **debug** commands, conditionally triggered debugging, **debug** commands, X.25 cause and diagnostic codes, and ISDN switch types, codes, and values	*Cisco IOS Debug Command Reference*, Release 12.4T

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

New Commands

- **debug ip dns name-list**
- **debug ip dns view**
- **debug ip dns view-list**
- **dns forwarder**
- **dns forwarding**
- **dns forwarding source-interface**

- domain list
- domain lookup
- domain multicast
- domain name
- domain name-server
- domain name-server interface
- domain retry
- domain round-robin
- domain timeout
- ip dns name-list
- ip dns server view-group
- ip dns view
- ip dns view-group
- ip dns view-list
- logging (DNS)
- restrict authenticated
- restrict name-group
- restrict source access-group
- show ip dns name-list
- show ip dns view
- show ip dns view-list
- view (DNS)

Modified Commands

- clear host
- ip host
- show hosts

clear host

To delete hostname-to-address mapping entries from one or more hostname caches, use the **clear host** command in privileged EXEC mode.

clear host [**view** *view-name* | **vrf** *vrf-name* | **all**] {*hostname* | *****}

Syntax Description

view *view-name*	(Optional) The *view-name* argument specifies the name of the Domain Name System (DNS) view whose hostname cache is to be cleared. Default is the default DNS view associated with the specified or global Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the VRF associated with the DNS view whose hostname cache is to be cleared. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view.
all	(Optional) Specifies that hostname-to-address mappings are to be deleted from the hostname cache of every configured DNS view.
hostname	Name of the host for which hostname-to-address mappings are to be deleted from the specified hostname cache.
*****	Specifies that all the hostname-to-address mappings are to be deleted from the specified hostname cache.

Command Default

No hostname-to-address mapping entries are deleted from any hostname cache.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.4(4)T	The **vrf** keyword, *vrf-name* argument, and **all** keyword were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.

Usage Guidelines

This command clears the specified hostname cache entries in running memory, but it does not remove the entries from NVRAM.

Entries can be removed from the hostname caches for a DNS view name, from the hostname caches for a VRF, or from all configured hostname caches. To remove entries from hostname caches for a particular DNS view name, use the **view** keyword and *view-name* argument. To remove entries from the hostname caches for a particular VRF, use the **vrf** keyword and *vrf-name* argument. To remove entries from all configured hostname caches, use the **all** keyword.

To remove entries that provide mapping information for a single hostname, use the *hostname* argument. To remove all entries, use the ***** keyword.

To display the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views, use the **show hosts** command.

To define static hostname-to-address mappings in the DNS hostname cache for a DNS view, use the **ip host** command.

Examples

The following example shows how to clear all entries from the hostname cache for the default view in the global address space:

```
Router# clear host all *
```

The following example shows how to clear entries for the hostname www.example.com from the hostname cache for the default view associated with the VPN named vpn101:

```
Router# clear host vrf vpn101 www.example.com
```

The following example shows how to clear all entries from the hostname cache for the view named user2 in the global address space:

```
Router# clear host view user2 *
```

Related Commands

Command	Description
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a 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.

debug ip dns name-list

To enable debugging output for Domain Name System (DNS) name list events, use the **debug ip dns name-list** command in privileged EXEC mode. To disable debugging output for DNS name list events, use the **no** form of this command.

debug ip dns name-list

no debug ip dns name-list

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging output is disabled for DNS name lists.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command enables the writing of DNS name list event messages to system message logging (syslog) output. A DNS name list event can be either of the following:

- The addition or removal of a DNS name list entry (a hostname pattern and action to perform on an incoming DNS query for a hostname that matches the pattern). To add or remove a DNS name list entry, use the **ip dns name-list** command.
- The removal of a DNS name list.

Note The addition of a DNS name list is reported as an addition of a name list entry.

To display which debugging options are enabled (DNS name list, DNS view, or DNS view list), use the **show debugging** command. To display the syslog history statistics and buffer contents, use the **show logging** command. To display a particular DNS name list or all configured name lists, use the **show ip dns name-list** command.

Examples

The following sample output from the **debug ip dns name-list** command shows the hostname pattern www.example.com being added to DNS name list 1 as a permit clause. Next, the hostname patterns www.example1.com and www.example2.com are added to DNS name list 2 as deny clauses and permit clauses, respectively. Finally, the hostname pattern www.example1.com is removed from DNS name list 2.

```
Router# debug ip dns name-list

DNS Name-list debugging is on
.
```

```
.
.
Router# show debugging

DNS Name-list debugging is on
.
.
.
Router# show logging
.
.
.
*May 16 14:54:44.326: DNS_NAMELIST: adding permit 'WWW.EXAMPLE' to name-list 1
*May 16 14:54:44.910: DNS_NAMELIST: adding deny 'WWW.EXAMPLE1.COM' to name-list 2
*May 16 14:54:45.202: DNS_NAMELIST: adding permit 'WWW.EXAMPLE2.COM' to name-list 2
*May 16 19:32:20.881: DNS_NAMELIST: removing 'WWW.EXAMPLE1.COM' from name-list 2
```

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.
show debugging	Displays the state of each debugging option.
show ip dns name-list	Displays a particular DNS name list or all configured name lists.
show logging	Displays the contents of logging buffers.

debug ip dns view

To enable debugging output for Domain Name System (DNS) view events, use the **debug ip dns view** command in privileged EXEC mode. To disable debugging output for a DNS view, use the **no** form of this command.

debug ip dns view

no debug ip dns view

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging output is disabled for DNS views.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command enables the writing of DNS view event messages to system message logging (syslog) output. A DNS view event can be any of the following:

- The addition or removal of a DNS view definition.
- The addition or removal of a DNS forwarding name server setting for a DNS view.
- The addition or removal of a DNS resolver setting for a DNS view.
- The enabling or disabling of logging of a syslog message each time a DNS view is used.

To display which debugging options are enabled (DNS name list, DNS view, or DNS view list), use the **show debugging** command. To show the syslog history statistics and buffer contents, use the **show logging** command.

Examples

The following sample output from the **debug ip dns view** command shows the default DNS view being configured:

```
Router# debug ip dns view

DNS View debugging is on
.
.
.
Router# show debugging

DNS View debugging is on
.
.
.
```

```
Router# show logging
.
.
.
DNS_VIEW: creating view view1
DNS_VIEW: Clearing logging in view default
DNS_VIEW: Setting domain lookup in view default
DNS_VIEW: Setting domain name to cisco.com in view default
DNS_VIEW: Setting  domain list example1.com in view default
DNS_VIEW: Setting  domain list example1.com example2.com in view default
DNS_VIEW: Setting  domain list example1.com example2.com example3.com in view default
DNS_VIEW: Setting domain multicast to 192.0.2.10 in view default
DNS_VIEW: Setting domain lookup in view default
DNS_VIEW: Setting domain timeout to 7 in view default
DNS_VIEW: Setting domain retry to 7 in view default
DNS_VIEW: Setting  domain name-server 192.0.2.204 192.0.2.205 in view default
DNS_VIEW: Setting  domain name-server 192.0.2.204 192.0.2.205 192.0.2.206 in view default
DNS_VIEW: Setting domain name-server interface FastEthernet0/1 in view default
DNS_VIEW: Setting domain round-robin to 4 in view default
DNS_VIEW: Setting dns forwarding in view default
DNS_VIEW: Setting  dns forwarder 192.0.2.11 in view default
DNS_VIEW: Setting  dns forwarder 192.0.2.11 192.0.2.12 in view default
DNS_VIEW: Setting  dns forwarder 192.0.2.11 192.0.2.12 192.0.2.13 in view default
```

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 debugging	Displays the state of each debugging option.
show logging	Displays the contents of logging buffers.

debug ip dns view-list

To enable debugging output for Domain Name System (DNS) view list events, use the **debug ip dns view-list** command in privileged EXEC mode. To disable debugging output for a DNS view list, use the **no** form of this command.

debug ip dns view-list

no debug ip dns view-list

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging output is disabled for DNS view lists.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command enables the writing of DNS view list event messages to system message logging (syslog) output. A DNS view list event can be any of the following:

- The addition or removal of a DNS view list definition. To add or remove a DNS view list definition, use the **ip dns view-list** command.
- The addition or removal of a DNS view list member (a DNS view and the relative order in which it is to be checked in the view list) to or from a DNS view list. To add or remove a DNS view list member, use the **view** command.
- The setting or clearing of a DNS view list assignment as the default view list (using the **ip dns server view-group** command) or to an interface (using the **ip dns view-group** command).

To show which debugging options are enabled (DNS name list, DNS view, or DNS view list), use the **show debugging** command. To show the syslog history statistics and buffer contents, use the **show logging** command.

Examples

The following sample output from the **debug ip dns vies-list** command shows the addition of the DNS view list definition named userlist5. Next, five DNS views are added as members of the DNS view list.

```
Router# debug ip dns view-list

DNS View-list debugging is on
.
.
.
Router# show debugging

DNS View-list debugging is on
```

```
.
.
.
Router# show logging

*May 16 23:31:17.491: DNS_VIEWLIST: creating view-list userlist5
*May 16 23:31:17.711: DNS_VIEWLIST: adding member user1 vrf vpn101 order 10 to view-list
userlist5
*May 16 23:31:18.583: DNS_VIEWLIST: adding member user2 vrf vpn102 order 20 to view-list
userlist5
*May 16 23:31:19.851: DNS_VIEWLIST: adding member user3 vrf vpn103 order 30 to view-list
userlist5
*May 16 23:31:21.007: DNS_VIEWLIST: adding member user4 vrf vpn204 order 45 to view-list
userlist5
*May 16 23:31:22.199: DNS_VIEWLIST: adding member default order 60 to view-list userlist5
```

Related Commands

Command	Description
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 debugging	Displays the state of each debugging option.
show logging	Displays the contents of logging buffers.
view	Enters DNS view list member configuration mode so that usage restrictions can be configured for the view list member.

dns forwarder

To add an address to the end of the ordered list of IP addresses for a Domain Name System (DNS) view to use when forwarding incoming DNS queries, use the **dns forwarder** command in DNS view configuration mode. To remove an IP address from the list, use the **no** form of this command.

dns forwarder [**vrf** *vrf-name*] *forwarder-ip-address*

no dns forwarder [**vrf** *vrf-name*] *forwarder-ip-address*

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance of the *forwarder-ip-address*. **Note** If no VRF is specified, the default is the global VRF.
forwarder-ip-address	IP address to use when forwarding DNS queries handled using the DNS view.

Command Default

Provided that DNS forwarding (configured by using the **dns forwarding** command) is enabled and the interface to use when forwarding incoming DNS queries is configured (if using the **dns forwarding source-interface** command) and not shut down, incoming DNS queries handled using the DNS view are forwarded to one of the DNS forwarding name servers.

If no forwarding name servers are configured for the DNS view, the router uses any configured domain name server addresses.

If there are no domain name server addresses configured either, the router forwards incoming DNS queries to the limited broadcast address (255.255.255.255) so that the queries are received by all hosts on the local network segment but not forwarded by routers.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command can be entered multiple times to specify a maximum of six forwarding name servers. After six forwarding name servers have been specified, additional forwarding name servers cannot be specified unless an existing entry is removed.

To display the list of DNS forwarding name server addresses configured for the DNS view, use the **show ip dns view** command.

Note DNS resolving name servers and DNS forwarding name servers are configured separately. The **domain name-server** and **domain name-server interface** commands are used to specify the DNS resolving name servers (the ordered list of IP addresses to use when *resolving internally generated DNS queries* handled using the DNS view). The **dns forwarder** command specifies the forwarder addresses (the

ordered list of IP addresses to use when *forwarding incoming DNS queries* handled using the DNS view).

Versions of Cisco IOS prior to Release 12.4(9)T used the resolving name server list for both resolving internal DNS queries and forwarding DNS queries received by the DNS server. For backward compatibility, if there are no forwarding name servers configured, the resolving name server list will be used instead.

Examples

The following example shows how to add three IP addresses to the list of forwarder addresses for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# dns forwarder 192.0.2.0
Router(cfg-dns-view)# dns forwarder 192.0.2.1
Router(cfg-dns-view)# dns forwarder 192.0.2.2
```

The following example shows how to add the IP address 192.0.2.3 to the list of forwarder addresses for the DNS view named user1 that is associated with the VRF vpn32, with the restriction that incoming DNS queries will be forwarded to 192.0.2.3 only if the queries are from the VRF named vpn1:

```
Router(config)# ip dns view vrf vpn32 user1
Router(cfg-dns-view)# dns forwarder vrf vpn1 192.0.2.3
```

Related Commands

Command	Description
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 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.
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.

dns forwarding

To enable forwarding of incoming Domain Name System (DNS) queries handled using the DNS view, use the **dns forwarding** command in DNS view configuration mode. To disable forwarding and revert to the default configuration, use the **no** form of this command.

dns forwarding

no dns forwarding

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is inherited from the global setting configured using the **ip domain lookup** global command. However, the **dns forwarding** DNS view command does not have a reciprocal side effect on the setting configured by the **ip domain lookup** global command.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command enables forwarding of incoming DNS queries handled using the DNS view.

To display the DNS forwarding setting for a DNS view, use the **show ip dns view** command.

If you configure **no domain lookup** for a DNS view while **dns forwarding** has not been disabled for that view, then the **dns forwarding** setting will appear in the **show ip dns view** command output in order to make it clear that DNS forwarding is still enabled.

If you configure the **no ip domain lookup** global command, however, the **no dns forwarding** setting is automatically configured also, in order to be backward compatible with the global command form.

Note DNS lookup and DNS forwarding are configured separately. The **domain lookup** command enables the resolution of internally generated DNS queries handled using the DNS view. The **dns forwarding** command enables the forwarding of incoming DNS queries handled using the DNS view.

By default, both domain lookup and DNS forwarding are both enabled for a view. If you then configure **no domain lookup**, DNS forwarding is still enabled. However, if you instead uses the older Cisco IOS command **no ip domain lookup** to disable domain lookup for the global default view, then DNS forwarding is disabled automatically. This is done for backward compatibility with the functionality of the **no ip domain lookup** global command.

Examples

The following example shows how to enable forwarding of incoming DNS queries handled using the DNS view named user3 that is associated with the VRF vpn32:

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

Related Commands

Command	Description
domain lookup	Enables the IP DNS-based hostname-to-address translation for internally generated DNS queries handled using the DNS view.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
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.

dns forwarding source-interface

To specify the interface to use when forwarding incoming Domain Name System (DNS) queries handled using the DNS view, use the **dns forwarding source-interface** command in DNS view configuration mode. To remove the specification of the source interface for a DNS view to use when forwarding DNS queries, use the **no** form of this command.

dns forwarding source-interface *interface*

no dns forwarding source-interface

Syntax Description

interface	Router interface to use when forwarding DNS queries.

Command Default

No interface is specified for forwarding incoming DNS queries handled using the DNS view, so the router selects the appropriate source IP address automatically, according to the interface used to send the packet, when the query is forwarded.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command specifies the interface to use when forwarding incoming DNS queries handled using the DNS view.

To display the interface configured by this command, use the **show ip dns view** command.

Tip To list all the interfaces configured on the router or access server, use the **show interfaces** command with the **summary** keyword. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *interface* argument in the **dns forwarding source-interface** command.

Examples

The following is sample output from the **show interfaces** command used with the **summary** keyword:

```
Router# show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface              IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
```

```
* FastEthernet0/0          0     0     0     0     0     0     0     0     0
  FastEthernet0/1          0     0     0     0     0     0     0     0     0
  ATM2/0                   0     0     0     0     0     0     0     0     0
  Ethernet3/0              0     0     0     0     0     0     0     0     0
  Ethernet3/1              0     0     0     0     0     0     0     0     0
  Ethernet3/2              0     0     0     0     0     0     0     0     0
  Ethernet3/3              0     0     0     0     0     0     0     0     0
  ATM6/0                   0     0     0     0     0     0     0     0     0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown
```

The following example shows how to configure FastEthernet slot 0, port 1 as the interface to be used to forward DNS queries for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# dns forwarder source-interface FastEthernet0/1
```

Related Commands

Command	Description
dns forwarding	Enables forwarding of incoming DNS queries by the DNS view.
show interfaces	Display statistics for all interfaces configured on the router or access server.
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.

domain list

To add a domain name to the end of the ordered list of domain names used to complete unqualified hostnames (names without a dotted-decimal domain name) in Domain Name System (DNS) queries handled using the DNS view, use the **domain list** command in DNS view configuration mode. To remove a name from the domain search list, use the **no** form of this command.

domain list *domain-name*

no domain list *domain-name*

Syntax Description

domain-name	Domain name to add or delete from the domain search list.
	Note Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No domain list is defined for the DNS view.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command adds a domain name to the end of the domain search list for the DNS view.

Note The **domain list** and **domain name** commands are similar, except that the **domain list** command can be used to define a list of domain names for the view, each to be tried in turn. If DNS lookup is enabled for the DNS view but the domain search list (specified using the **domain list** command) is empty, the default domain name (specified by using the **domain name** command) is used instead. If the domain search list is not empty, the default domain name is not used.

To display the list of domain names used to complete unqualified hostnames in DNS queries received by a DNS view, use the **show hosts** command or the **show ip dns view** command.

Examples

The following example shows how to add two domain names to the list for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain list example1.com
Router(cfg-dns-view)# domain list example1.org
```

The following example shows how to add two domain names to the list for the DNS view and then delete one of the domain names from the list:

```
Router(cfg-dns-view)# domain list example2.com
```

```
Router(cfg-dns-view)# domain list example2.org
Router(cfg-dns-view)# no domain list example2.net
```

Related Commands

Command	Description
domain name	Specifies a single default domain name to use to complete unqualified hostnames in internally generated DNS queries 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.
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.

domain lookup

To enable the IP Domain Name System (DNS)-based hostname-to-address translation for internally generated DNS queries handled using the DNS view, use the **domain lookup** command in DNS view configuration mode. To disable domain lookup for hostname resolution, use the **no** form of this command.

domain lookup

no domain lookup

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is inherited from the global setting configured using the **ip domain lookup** global command. However, the **domain lookup** DNS view command does not have a reciprocal side effect on the setting configured by the **ip domain lookup** global command.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command enables DNS-based hostname-to-address translation for internally generated DNS queries handled using the DNS view.

To display the DNS lookup setting for a DNS view, use the **show ip dns view** command.

If you configure **no dns forwarding** for a DNS view while **domain lookup** has not been disabled for that view, then the **domain lookup** setting will appear in the **show ip dns view** command output in order to make it clear that domain lookup is still enabled.

If you configure the **no ip domain lookup** global command, however, the **no domain lookup** setting is automatically configured also, in order to be backward compatible with the global command form.

Note DNS lookup and DNS forwarding are configured separately. The **domain lookup** command enables the resolution of internally generated DNS queries handled using the DNS view. The **dns forwarding** command enables the forwarding of incoming DNS queries handled using the DNS view.

By default, both domain lookup and DNS forwarding are both enabled for a view. If you then configure **no domain lookup**, DNS forwarding is still enabled. However, if you instead uses the older Cisco IOS command **no ip domain lookup** to disable domain lookup for the global default view, then DNS forwarding is disabled automatically. This is done for backward compatibility with the functionality of the **no ip domain lookup** global command.

Examples

The following example shows how to enable IP DNS-based hostname-to-address translation in the DNS view named user3 that is associated with the VRF vpn32:

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

Related Commands

Command	Description
dns forwarding	Enables forwarding of incoming DNS queries by 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.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
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.

domain multicast

To configure the domain name to be used when performing multicast address lookups for internally generated Domain Name System (DNS) queries handled using the DNS view, use the **domain multicast** command in DNS view configuration mode. To remove the specification of the domain name for multicast address lookups, use the **no** form of this command.

domain multicast *domain-name*

no domain multicast

Syntax Description

domain-name	Domain name to be used when performing multicast address lookups.

Command Default

No IP address is specified for performing multicast address lookups for the DNS view.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command configures the domain name to be used when performing multicast address lookups for internally generated DNS queries handled using the DNS view.

To display the domain name for multicast address lookups, use the **show ip dns view** command.

Examples

The following example shows how to configure the domain name www.example.com as the domain name to be used when performing multicast lookups for internally generated DNS queries handled using the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain multicast www.example.com
```

Related Commands

Command	Description
ip domain multicast	Changes the domain prefix used by Cisco IOS software for DNS-based SSM mapping.
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.

domain name

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

domain name *domain-name*

no domain name

Syntax Description

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

Command Default

No default domain name is defined for the DNS view.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command configures the default domain name used to complete unqualified hostnames in DNS queries handled using the DNS view.

Note The **domain list** and **domain name** commands are similar, except that the **domain list** command can be used to define a list of domain names for the view, each to be tried in turn. If DNS lookup is enabled for the DNS view but the domain search list (specified using the **domain list** command) is empty, the default domain name (specified by using the **domain name** command) is used instead. If the domain search list is not empty, the default domain name is not used.

To display the default domain name configured for a DNS view, use the **show hosts** command or the **show ip dns view** command.

Examples

The following example shows how to define example.com as the default domain name for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain name example.com
```

Related Commands

Command	Description
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.
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.
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.

domain name-server

To add a name server to the list of Domain Name System (DNS) name servers to be used for a DNS view to resolve internally generated DNS queries, use the **domain name-server** command in DNS view configuration mode. To remove a DNS name server from the list, use the **no** form of this command.

domain name-server *name-server-ip-address*

no domain name-server *name-server-ip-address*

Syntax Description

name-server-ip-address	IP address of a DNS name server.

Command Default

No IP address is explicitly added to the list of resolving name servers for this view, although an IP address can be added to the list if dynamic name server acquisition is enabled. If the list of resolving name servers is empty, the router will send the query to the limited broadcast address 255.255.255.255 when this view is used.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command can be entered multiple times to specify a maximum of six resolving name servers. After six resolving name servers have been specified, additional resolving name servers cannot be specified unless an existing entry is removed.

This method of explicitly populating the list of resolving name servers is useful in an enterprise network where the population of available DNS servers is relatively static. In an Internet service provider (ISP) environment, where primary and secondary DNS server addresses can change frequently, the router can learn a DNS server address through either DHCP or PPP on the interface. To configure the dynamic acquisition of DNS resolving name server addresses, use the **domain name-server interface** command. Regardless of the method or methods used to populate the list of DNS resolving name servers for the view, no more than six resolving name servers are maintained for the view.

To display the list of DNS resolving name server IP addresses configured for a DNS view, use the **show hosts** command or the **show ip dns view** command.

Note The DNS resolving name servers and DNS forwarding name servers are configured separately. The **domain name-server** and **domain name-server interface** commands are used to specify the DNS resolving name servers (the ordered list of IP addresses to use when *resolving internally generated DNS queries* for the DNS view). The **dns forwarder** command specifies the forwarder addresses (the ordered list of IP addresses to use when *forwarding incoming DNS queries* for the DNS view).

If there is no DNS forwarder configuration in a view, then the domain name server list will be used when forwarding DNS queries. This is done for backward compatibility with the **ip name-server** global command.

Examples

The following example shows how to specify the hosts at 192.0.2.111 and 192.0.2.112 as the name servers for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain name-server 192.0.2.111
Router(cfg-dns-view)# domain name-server 192.0.2.112
```

Related Commands

Command	Description
dns forwarder	Specifies the ordered list of IP addresses to use when forwarding incoming 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.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
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.
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.

domain name-server interface

To specify the interface on which the router can learn (through either DHCP or PPP) Domain Name System (DNS) a resolving name server address for the DNS view, use the **domain name-server interface** command in DNS view configuration mode. To remove the definition of the interface, use the **no** form of this command.

domain name-server interface *interface*

no domain name-server interface *interface*

Syntax Description

interface	Interface on which to acquire the IP address of a DNS name server that the DNS view can use to resolve internally generated DNS queries. The interface must connect to another router on which the DHCP agent or the PPP agent has been configured to allocate the IP address of the DNS server.

Command Default

No interface is used to acquire the DHCP or PPP address to be used for a DNS view to resolve internally generated DNS queries.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command specifies the interface from which to acquire (through DHCP or PPP interaction on the interface) the IP address of a DNS server to add to the list of DNS name servers used to resolve internally generated DNS queries for the DNS view.

The dynamic acquisition of DNS resolving name server addresses is useful in an Internet service provider (ISP) environment, where primary and secondary DNS server addresses can change frequently. To explicitly populate the list of resolving name servers in an enterprise network where the population of available DNS servers is relatively static, use the **domain name-server** command. Regardless of the method or methods used to populate the list of DNS resolving name servers for the view, no more than six resolving name servers are maintained for the view.

Note The DNS resolving name servers and DNS forwarding name servers are configured separately. The **domain name-server** and **domain name-server interface** commands are used to specify the DNS resolving name servers (the ordered list of IP addresses to use when *resolving internally generated DNS queries* for the DNS view). The **dns forwarder** command specifies the forwarder addresses (the ordered list of IP addresses to use when *forwarding incoming DNS queries* for the DNS view).

If there is no DNS forwarder configuration in a view, then the domain name server list will be used when forwarding DNS queries. This is done for backward compatibility with the **ip name-server** global command.

To display information about the setting configured by the **domain name-server interface** command, use the **show running-config** command. The interface on which to acquire the IP address of a DNS server to add to the list of DNS name servers, if configured, is listed in the default DNS view information (in the **ip dns view default** command information, as the argument for the **domain name-server interface** command).

Tip To list all the interfaces configured on the router or access server, use the **show interfaces** command with the **summary** keyword. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *interface* argument in the **domain name-server interface** command.

Examples

The following is sample output from the **show interfaces** command used with the **summary** keyword:

```
Router# show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface              IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
* FastEthernet0/0          0     0    0     0     0    0     0    0    0
  FastEthernet0/1          0     0    0     0     0    0     0    0    0
  ATM2/0                   0     0    0     0     0    0     0    0    0
  Ethernet3/0              0     0    0     0     0    0     0    0    0
  Ethernet3/1              0     0    0     0     0    0     0    0    0
  Ethernet3/2              0     0    0     0     0    0     0    0    0
  Ethernet3/3              0     0    0     0     0    0     0    0    0
  ATM6/0                   0     0    0     0     0    0     0    0    0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown
```

The following example shows how to specify a list of name servers for the DNS view named user3 that is associated with the VRF vpn32. First, the list of name server addresses is cleared, then five DNS server IP addresses are added to the list. Finally, FastEthernet slot 0, port 0 is specified as the interface on which to acquire, by DHCP or PPP interaction, a sixth DNS server IP address.

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# no domain name-server
Router(cfg-dns-view)# domain name-server 192.0.2.001
Router(cfg-dns-view)# domain name-server 192.0.2.002
Router(cfg-dns-view)# domain name-server 192.0.2.003
Router(cfg-dns-view)# domain name-server 192.0.2.004
Router(cfg-dns-view)# domain name-server 192.0.2.005
Router(cfg-dns-view)# domain name-server interface FastEthernet0/0
```

Related Commands

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.
show interfaces	Display statistics for all interfaces configured on the router or access server.

Command	Description
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.
show running-config	Displays the contents of the currently running configuration file of your routing device.

domain retry

To configure the number of retries to perform when sending or forwarding Domain Name System (DNS) queries handled using the DNS view, use the **domain retry** command in DNS view configuration mode. To remove the specification of the number of retries for a DNS view, use the **no** form of this command.

domain retry *number*

no domain retry

Syntax Description

number	Number of times to retry sending or forwarding a DNS query. The range is from 0 to 100.

Command Default

number: 2 times

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command configures the number of retries to perform when sending or forwarding DNS queries handled using the DNS view.

To display the number of retries configured for the DNS view, use the **show ip dns view** command.

Examples

The following example shows how to configure the router to send out or forward ten DNS queries from the DNS view named user3 that is associated with the VRF vpn32 before giving up:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain retry 10
```

Related Commands

Command	Description
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.

domain round-robin

To enable round-robin rotation of multiple IP addresses associated with a name in the hostname cache used by the DNS view, use the **domain round-robin** command in DNS view configuration mode. To disable round-robin functionality for the DNS view, use the **no** form of this command.

domain round-robin

no domain round-robin

Syntax Description

This command has no arguments or keywords.

Command Default

Round-robin rotation of multiple IP addresses associated with a name in the hostname cache is disabled for the DNS view.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command enables round-robin rotation such that each time a hostname in the internal cache is accessed, the system returns the next IP address in the cache, rotated such that the second IP address in the list becomes the first one and the first one is moved to the end of the list. For a more detailed description of round-robin functionality, see the description of the **ip domain round-robin** global command in the *Cisco IOS IP Addressing Services Command Reference*.

To display the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views, use the **show hosts** command. To define static hostname-to-address mappings in the global hostname cache or VRF hostname cache for the specified DNS view, use the **ip host** command. To display the round-robin setting for the DNS view, use the **show ip dns view** command.

Examples

The following example shows how to define the hostname www.example.com with three IP addresses and then enable round-robin rotation for the default DNS view associated with the global VRF. Each time that hostname is referenced internally or queried by a DNS client sending a query to the Cisco IOS DNS server on this system, the order of the IP addresses associated with the host www.example.com will be changed. Because most client applications look only at the first IP address associated with a hostname, this results in different clients using each of the different addresses and thus distributing the load among the three different IP addresses.

```
Router(config)# ip host view www.example.com 192.168.2.100 192.168.2.200 192.168.2.250
Router(config)# ip dns view default
Router(cfg-dns-view)# domain lookup
Router(cfg-dns-view)# domain round-robin
```

Related Commands

Command	Description
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip domain round-robin	Enables round-robin functionality on DNS servers.
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.
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.

domain timeout

To configure the number of seconds to wait for a response to a Domain Name System (DNS) query sent or forwarded by the DNS view, use the **domain timeout** command in DNS view configuration mode. To remove the specification of the number of seconds for a DNS view to wait, use the **no** form of this command.

domain timeout *seconds*

no domain timeout

Syntax Description

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

Command Default

number: 3 seconds

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command configures the number of seconds to wait for a response to a DNS query sent or forwarded by the DNS view.

To display the number of seconds configured for the DNS view, use the **show ip dns view** command.

Examples

The following example shows how to configure the router to wait 8 seconds for a response to a DNS query received in the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain timeout 8
```

Related Commands

Command	Description
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 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 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.

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 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.
show running-config	Displays the contents of the currently running configuration file of your routing device.

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 *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.

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.
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.

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).

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.
show running-config	Displays the contents of the currently running configuration file of your routing device.

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 hostname 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 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.
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	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*	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 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*	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*	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 Release 12.2(33)SRA.

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 thhe **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:

```
Router(config)# ip host www.example1.com 192.0.2.141 192.0.2.241
Router(config)# ip host www.example2.com 192.0.2.242
Router(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:

```
Router(config)# ip host vrf vpn101 view user3 www.example1.com 192.0.2.141 192.0.2.241
Router(config)# ip host vrf vpn101 view user3 www.example2.com 192.0.2.242
Router(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.

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

name-list-number	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

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.

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.

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 *name-list-number* 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

acl-name	String (not to exceed 64 characters) that specifies a standard ACL.
acl-number	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 hosts

To 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 Domain Name System (DNS) view or for all configured DNS views, use the **show hosts** command in privileged EXEC mode.

show hosts [**vrf** *vrf-name*] [**view** *view-name*] [**all** | *hostname*] [**summary**]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache entries are to be displayed. 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 DNS view whose hostname cache information is to be displayed. Default is the default (unnamed) 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.
all	(Optional) The specified hostname cache information is to be displayed for all configured DNS views. This is the default.
hostname	(Optional) The specified hostname cache information displayed is to be limited to entries for a particular hostname. Default is the hostname cache information for all hostname entries in the cache.
summary	(Optional) The specified hostname cache information is to be displayed in brief summary format. Disabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2T	This command was updated to support the Cisco modem user interface feature.
12.4(4)T	The **vrf**, **all**, and **summary** keywords and *vrf-name* and *hostname* arguments were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.

Usage Guidelines

This command 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.

If you specify the **show hosts** command without any optional keywords or arguments, only the entries in the global hostname cache will be displayed.

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 hosts** command with no parameters specified:

```
Router# show hosts

Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 192.0.2.220
Host Flag Age Type Address(es)
EXAMPLE1.CISCO.COM (temp, OK) 1 IP 192.0.2.10
EXAMPLE2.CISCO.COM (temp, OK) 8 IP 192.0.2.50
EXAMPLE3.CISCO.COM (temp, OK) 8 IP 192.0.2.115
EXAMPLE4.CISCO.COM (temp, EX) 8 IP 192.0.2.111
EXAMPLE5.CISCO.COM (temp, EX) 0 IP 192.0.2.27
EXAMPLE6.CISCO.COM (temp, EX) 24 IP 192.0.2.30
```

The following is sample output from the **show hosts** command that specifies the VRF vpn101:

```
Router# show hosts vrf vpn101

Default domain is example.com
Domain list: example1.com, example2.com, example3.com
Name/address lookup uses domain service
Name servers are 192.0.2.204, 192.0.2.205, 192.0.2.206

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                      Port  Flags      Age Type   Address(es)
user                      None  (perm, OK)  0   IP    192.0.2.001
www.example.com           None  (perm, OK)  0   IP    192.0.2.111
                                                      192.0.2.112
```

Table 1 describes the significant fields shown in the display.

Table 1 show hosts Field Descriptions

Field	Description
Default domain	Default domain name to be used to complete unqualified names if no domain list is defined.
Domain list	List of default domain names to be tried in turn to complete unqualified names.
Name/address lookup	Style of name lookup service.
Name servers	List of name server hosts.
Host	Learned or statically defined hostname. Statically defined hostname-to-address mappings can be added to the DNS hostname cache for a DNS view by using the **ip hosts** command.

Table 1 show hosts Field Descriptions (continued)

Field	Description
Port	TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command.
Flags	Indicates additional information about the hostname-to-IP address mapping. Possible values are as follows: • temp—A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity. • perm—A permanent entry is entered by a configuration command and is not timed out. • OK—Entries marked OK are believed to be valid. • ??—Entries marked ?? are considered suspect and subject to revalidation. • EX—Entries marked EX are expired.
Age	Number of hours since the software last referred to the cache entry.
Type	Type of address. For example, IP, Connectionless Network Service (CLNS), or X.121. If you have used the **ip hp-host global** configuration command, the **show hosts** command will display these hostnames as type HP-IP.
Address(es)	IP address of the host. One host may have up to eight addresses.

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.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.

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

name-list-number	(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 2 describes the significant fields shown for each DNS name list in the display.

Table 2 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 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 *vrf-name*	(Optional) The *vrf-name* 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.
view-name	(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.

To display information about the setting configured by the **domain name-server interface** command, use the **show running-config** command. The interface on which to acquire the IP address of a DNS server to add to the list of DNS name servers, if configured, is listed in the default DNS view information (in the **ip dns view default** command information, as the argument for the **domain name-server interface** command).

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:
    192.0.2.204
    192.0.2.205
    192.0.2.206
  Round-robin'ing of IP addresses is enabled
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.0.2.11
    192.0.2.12
    192.0.2.13
  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:
    192.0.2.104
    192.0.2.105
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.0.2.204

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:
    192.0.2.100
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.0.2.200 (vrf vpn201)
```

Table 3 describes the significant fields shown for each DNS view in the display.

Table 3 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-interfac**e 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.

Related Commands

Command	Description
debug ip dns view	Enables debugging output for DNS view events.
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.
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 running-config	Displays the contents of the currently running configuration file of your routing device.

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

view-list-name	(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 4 describes the significant fields shown for each DNS view list in the display.

Table 4 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.

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 *vrf-name*	(Optional) The *vrf-name* 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** 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). **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.
default	Specifies that the DNS view is unnamed. **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.
view-name	String (not to exceed 64 characters) that identifies the name of an existing DNS view. **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. **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.
order-number	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. **Tip** If the *order-number* values for the DNS views within a DNS view list are configured with large intervals between them (for example, by specifying *order-number* 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 *order-number* values.

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.

Feature Information for Split DNS

Table 5 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 5 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 5 Feature Information for Split DNS

Feature Name	Releases	Feature Information
Split DNS	12.4(9)T	The Split DNS feature introduces the configuration of multiple DNS databases on a router and the ability of the router to select one of these DNS server configurations based on certain characteristics of the DNS query that the router is handling. The Cisco router attempts to answer a DNS query by using the internal DNS hostname cache specified by the selected virtual DNS name server. If the DNS query cannot be answered from the information in the hostname cache, the router directs the query to specific, back-end DNS servers.

Glossary

AAA—authentication, authorization, and accounting.

ACL—access control list. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

access control list—*See* ACL.

address resolution—Generally, a method for resolving differences between computer addressing schemes. Address resolution usually specifies a method for mapping network layer (Layer 3) addresses to data link layer (Layer 2) addresses.

authentication—In security, the verification of the identity of a person or a process.

bridge—Device that connects and passes packets between two network segments that use the same communications protocol. Bridges operate at the data link layer (Layer 2) of the OSI reference model. In general, a bridge filters, forwards, or floods an incoming frame based on the MAC address of that frame. *See also* relay.

broadcast address—A special address reserved for sending a message to all stations.

CE router—Customer edge router, an edge router in the C network, defined as a C router which attaches directly to a P router.

client—Any host requesting configuration parameters.

C network—Customer (enterprise or service provider) network.

CPE—customer premises equipment.

C router—Customer router, a router in the C network.

DDR—dial-on-demand routing. Technique whereby a router can automatically initiate and close a circuit-switched session as transmitting stations demand. The router spoofs keepalives so that end stations treat the session as active. DDR permits routing over ISDN or telephone lines using an external ISDN terminal adapter or modem.

DHCP—Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DNS—Domain Name System. System used on the Internet for translating names of network nodes into addresses.

DNS name group—Association of a DNS view list member with a restriction that limits the view to handling DNS queries whose queried domain name matches a DNS name list. *See also* DNS source access group.

DNS name list—A named set of a domain name pattern-matching rules, with each rule specifying the type of action to be performed on a DNS query if a queried domain name matches the text string pattern.

DNS proxy—Feature that allows a router to act as a proxy for devices on the LAN by sending its own LAN address to devices that request DNS server IP addresses and forwarding DNS queries to the real DNS servers after the WAN connection is established.

DNS server view group—A DNS view list that has been configured as the default DNS view list for the router. The Cisco IOS software uses the default DNS view list to determine which DNS view to use to handle resolution of incoming DNS queries that arrive on an interface not configured with a DNS view list. *See also* DNS view group.

DNS source access group—Association of a DNS view list member with a restriction that limits the view to handling DNS queries whose source IP address matches a standard access control list (ACL).*See also* DNS name group.

DNS spoofing—Scheme used by 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 hostname other than its own but will respond to the DNS query with the IP address of the incoming interface when queried for its own hostname.

The hostname used in the DNS query is defined as the exact configured hostname of the router specified by the **hostname** command, with no default domain appended.

DNS view—A named set of virtual DNS servers. Each DNS view is associated with a VRF and is configured with DNS resolver and forwarder parameters.

DNS view group—Association of a DNS view list with a router interface. The Cisco IOS software uses this view list to determine which DNS view to use to handle resolution of incoming DNS queries that arrive on that interface. *See also* DNS server view group.

DNS view list—A named set of DNS views that specifies the order in which the view list members should be checked and specifies usage restrictions for each view list member.

DNS view list member—A named set of DNS views that specifies the order in which the view list members should be checked and specifies usage restrictions for each view list member.

domain—On the Internet, a portion of the naming hierarchy tree that refers to general groupings of networks based on organization type or geography.

domain name—The style of identifier—a sequence of case-insensitive ASCII labels separated by dots—defined for subtrees in the Internet Domain Name System (R1034) and used in other Internet identifiers, such as hostnames, mailbox names, and URLs.

enterprise network—Large and diverse network connecting most major points in a company or other organization. Differs from a WAN in that it is privately owned and maintained.

gateway—In the IP community, an older term referring to a routing device. Today, the term router is used to describe nodes that perform this function, and gateway refers to a special-purpose device that performs an application-layer conversion of information from one protocol stack to another. *Compare with* router.

ISP—Internet service provider. Company that provides Internet access to other companies and individuals.

LAN—local-area network. High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies. *Compare with* MAN and WAN.

MAN—metropolitan-area network. Network that spans a metropolitan area. Generally, a MAN spans a larger geographic area than a LAN, but a smaller geographic area than a WAN. *Compare with* LAN and WAN.

MPLS—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

multicast address—Single address that refers to multiple network devices. *Synonymous with* group address.

name caching—Method by which remotely discovered hostnames are stored by a router for use in future packet-forwarding decisions to allow quick access.

name resolution—Generally, the process of associating a name with a network location.

name server—Server connected to a network that resolves network names into network addresses.

namespace—Commonly distributed set of names in which all names are unique.

PE router—Provider edge router, an edge router in the P network, defined as a P router which attaches directly to a C router.

P network—MPLS-capable service provider core network. P routers perform MPLS.

P router—Provider router, a router in the P network.

relay—OSI terminology for a device that connects two or more networks or network systems. A data link layer (Layer 2) relay is a bridge; a network layer (Layer 3) relay is a router. *See also* bridge *and* router.

router—Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information. Occasionally called a gateway (although this definition of gateway is becoming increasingly outdated). *Compare with* gateway. *See also* relay.

server—Any host providing configuration parameters.

spoofing—Scheme used by routers to cause a host to treat an interface as if it were up and supporting a session. The router spoofs replies to keepalive messages from the host in order to convince that host that the session still exists. Spoofing is useful in routing environments, such as DDR, in which a circuit-switched link is taken down when there is no traffic to be sent across it in order to save toll charges.

SSM—Source Specific Multicast. A datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is the core networking technology for the Cisco implementation of the IP Multicast Lite suite of solutions targeted for audio and video broadcast application environments.

tunnel—Secure communication path between two peers, such as two routers.

VPN—Virtual Private Network. Framework that consists of multiple peers transmitting private data securely to one another over an otherwise public infrastructure. A VPN protects inbound and outbound network traffic by using protocols that tunnel and encrypt all data at the IP level. This framework permits networks to extend beyond their local topology, while remote users are provided with the appearance and functionality of a direct network connection. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

VRF—VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router. Each VPN instantiated on the PE router has its own VRF.

WAN—wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs. *Compare with* LAN *and* MAN.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.