Split DNS

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, page 1
- Prerequisites for Split DNS, page 1
- Restrictions for Split DNS, page 2
- Information About Split DNS, page 2
- How to Configure Split DNS, page 12
- Configuration Examples for Split DNS, page 30
- Additional References, page 34
- Feature Information for Split DNS, page 35
- Glossary, page 36

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

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 the figure below.

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

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

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

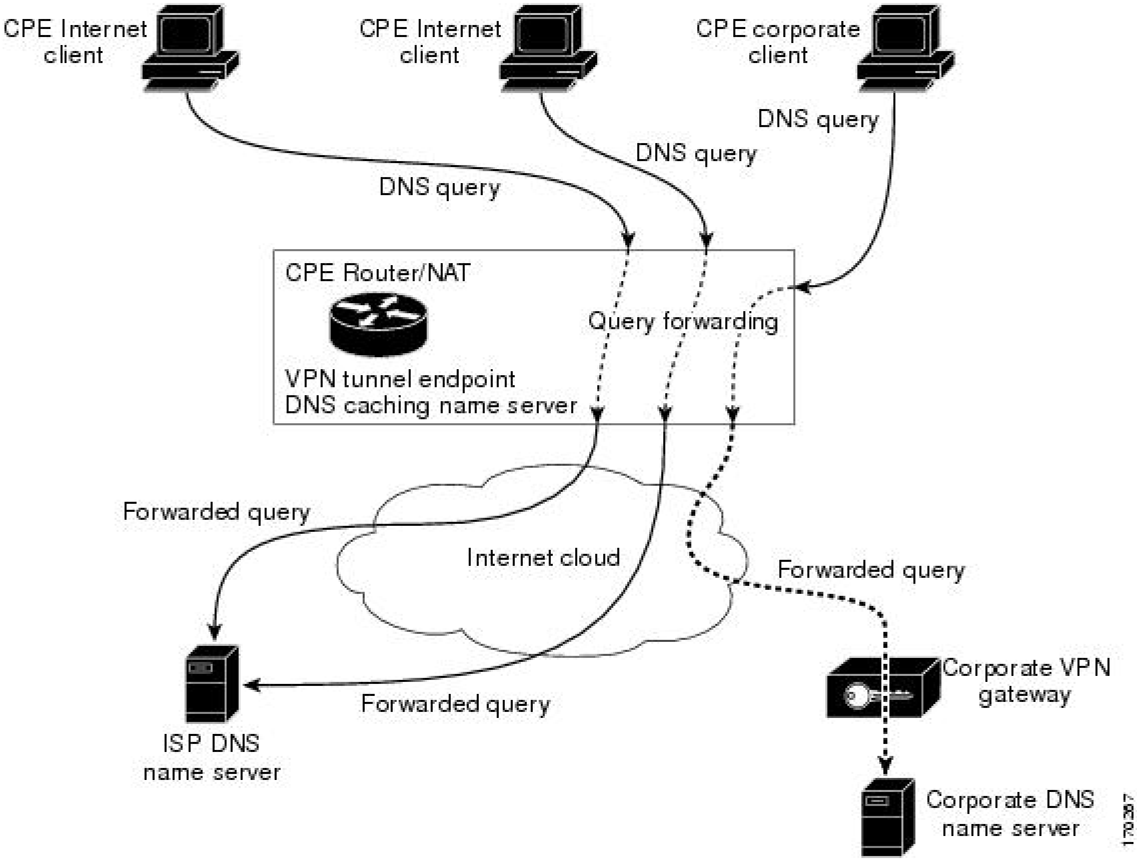
Split DNS is compatible with Network Address Translation (NAT) and Cisco IOS Port Address Translation (PAT) upstream interfaces. If NAT or PAT is enabled on the CPE router, DNS queries are translated (by address translation or port translation) to the appropriate destination address, such as an ISP DNS 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 the figure below. 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

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 the figure above 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 the figure above) 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 "DNS View Lists") 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.

Sometimes, when a source interface is configured on a router with the split DNS feature to forward DNS queries, the router does not forward the DNS queries through the configured interface. Hence, consider the following points while forwarding the DNS queries using the source interface:

- DNS queries are forwarded to a broadcast address when a forwarding source interface is configured and the DNS forwarder is not configured.
- The source IP address of the forwarded query should be set to the primary IP address of the interface configured, using the **dns forwarding source-interface** *interface* command. If no such configuration exists, then the source IP address of the forwarded DNS query will be the primary IP address of the

outgoing interface. DNS forwarding should be done only when the source interface configured for the DNS forwarding is active.

- The source IP address of the DNS query for the DNS resolver functionality is set using the **domain resolver source-interface** *interface-type number* command. If there is no DNS address configured, then queries will be broadcasted to the defined source interface. DNS resolving should be done only when the source interface configured for the DNS resolving is active. See "Specifying a Source Interface to Forward DNS Queries" for the configuration steps.

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 "DNS Name Groups".

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 "DNS View Groups".

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.
- 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 Hostname

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.

If the router receives a query other than a broadcast, it forwards the query as a broadcast under the VRF as defined in the interface view:

- If a device is acting as a forwarder.
- If at least one global name-server is configured.
- If the view to be used to service this query does not contain any of the following commands:
    - **dns forwarder** [**vrf** *vrf-name*] *forwarder-ip-address*
    - **dns forwarding source-interface** *interface*

- **domain name-server** *name-server-ip-address*
- **domain resolver source-interface** *interface-type number*

See "Specifying a DNS View List for a Router Interface" to specify a DNS view list for a particular router interface.

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:
    1. If a DNS view list is attached to the interface, the router uses the specified DNS view list.
    2. 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:
    1. 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.
    2. 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.

1. The router attempts to respond to the query using the parameters specified by the selected DNS view:
    1. 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.
    2. 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.
    3. If no DNS forwarders are configured for the view, the router forwards the query using the configured domain name servers.
    4. 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

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.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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. Do one of the following:
   - **domain name** *domain-name*
   -
   - **domain list** *domain- name*
7. Do one of the following:
   - **domain name-server** *name-server-ip-address*
   -
   - **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*}	Defines a DNS view and enters DNS view configuration mode.

	Command or Action	Purpose

	Example:
	`Router(config)# ip dns view vrf vpn101`
	`user3`	

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	Do one of the following:
	• **domain name** *domain-name*
	•
	• **domain list** *domain- name*
	Example:
	`Router(cfg-dns-view)# domain name example.com`
	Example:
	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	Do one of the following:
	• **domain name-server** *name-server-ip-address*
	•
	• **domain name-server interface** *interface*
	Example:
	`Router(cfg-dns-view)# domain name-server 192.168.2.124`
	Example:
	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.

	Command or Action	Purpose
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.

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

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

	Command or Action	Purpose

	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`
		• 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.

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`	(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.

	Command or Action	Purpose
	`name-group 500`	
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

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.
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.

	Command or Action	Purpose

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 DNS Server of the Router

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** *name-list-number*
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.

	Command or Action	Purpose
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.

Specifying a Source Interface to Forward DNS Queries

Perform this optional task if you need to specify a source interface to forward the DNS queries.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dns view** [**vrf** *vrf-name*] {**default** | *view-name*}
4. **domain resolver source-interface** *interface-type number*
5. **end**

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 vpn32 user3`
		Creates the DNS view of the specified name associated with the specified VRF instance and then enters DNS view configuration mode.

	Command or Action	Purpose
Step 4	**domain resolver source-interface** *interface-type number* **Example:** `Router(cfg-dns-view)# domain resolver source-interface fastethernet 0/0`	Sets the source IP address of the DNS queries for the DNS resolver functionality.

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

Configuration Examples for Split DNS

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

Related Documents

Related Topic	Document Title
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" module
DNS configuration tasks	"Configuring DNS" module
DNS commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*

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 Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Split DNS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: 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.