Configuring DNS

The Domain Name System (DNS) is a distributed database in which you can map host names to IP addresses through the DNS protocol from a DNS server. Each unique IP address can have an associated host name. The Cisco IOS XE software maintains a cache of host-name-to-address mappings for use by the **connect**, **telnet**, and **ping** EXEC commands, and related Telnet support operations. This cache speeds the process of converting names to addresses.

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.

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 Configuring DNS

To use DNS, you must have a DNS name server on your network.

Information About DNS

DNS Overview

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The global naming scheme of the Internet, the DNS, accomplishes this task. This service is enabled by default. The following sections summarize DNS concepts and function:

Host Names for Network Devices

Each unique IP address can have an associated host name. DNS uses a hierarchical scheme for establishing host names for network nodes. This allows local control of the segments of the network through a client-server scheme. The DNS system can locate a network device by translating the host name of the device into its associated IP address.

Domains Names for Groups of Networks

IP defines a naming scheme that allows a device to be identified by its location in the IP. This is a hierarchical naming scheme that provides for *domains*. On the Internet, a domain is a portion of the naming hierarchy tree that refers to general groupings of networks based on organization type or geography. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco is a commercial organization that the IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, the File Transfer Protocol (FTP) system, for example, is identified as *ftp.cisco.com*.

Name Servers

To keep track of domain names, IP has defined the concept of a *name server*. Name servers are programs that have complete information about their namespace portion of the domain tree and may also contain pointers to other name servers that can be used to lead to information from any other part of the domain tree. Name servers know the parts of the domain tree for which they have complete information. A name server may also store information about other parts of the domain tree. To map domain names to IP addresses, you must first identify the host names, then specify a name server, and enable the DNS service.

Cache

To speed the process of converting names to addresses, the name server maintains a database, called a *cache*, of host-name-to-address mappings for use by the **connect**, **telnet**, and **ping** EXEC commands, and related Telnet support operations. The cache stores the results from previous responses. Upon receiving a client-issued DNS query, it will check this local storage to see if the answer is available locally.

Name Resolvers

Name resolvers are programs that extract information from name servers in response to client requests. Resolvers must be able to access at least one name server. The resolver either uses that name server's information to answer a query directly or pursues the query using referrals to other names servers. A resolver will typically be a system routine that is directly accessible to user programs. Therefore, no protocol is necessary between the resolver and the user program.

Zones

The domain namespace is divided into areas called zones that are points of delegation in the DNS tree. A zone contains all domains from a certain point downward, except those for which other zones are authoritative.

Authoritative Name Servers

A name server is said to be an authority for the parts of the domain tree for which it has complete information. A zone usually has an authoritative name server, often more than one. An authoritative name server has been configured with host table information or has acquired host table information though a zone transfer (the action that occurs when a secondary DNS server starts up and updates itself from the primary server).

DNS Operation

Within an organization, you can have many name servers, but Internet clients can query only those that the root name servers know. The other name servers answer internal queries only.

A name server handles client-issued queries to the DNS server for locally defined hosts within a particular zone as follows:

- An authoritative name server responds to DNS user queries for a domain name that is under its zone of authority by using the permanent and cached entries in its own host table. If the query is for a domain name that is under its zone of authority but for which it does not have any configuration information, the authoritative name server simply replies that no such information exists..
- A name server that is not configured as the authoritative name server responds to DNS user queries by using information that it has cached from previously received query responses. If no device is configured as the authoritative name server for a zone, queries to the DNS server for locally defined hosts will receive nonauthoritative responses.

Name servers answer DNS queries (forward incoming DNS queries or resolve internally generated DNS queries) according to the forwarding and lookup parameters configured for the specific domain.

DNS Security

An alternating sequence of DNS public key (DNSKEY) RR sets and Delegation Signer (DS) RR sets forms a chain of signed data, with each link in the chain vouching for the next. A DNSKEY RR is used to verify the signature covering a DS RR and allows the DS RR to be authenticated. The DS RR contains a hash of another DNSKEY RR and this new DNSKEY RR is authenticated by matching the hash in the DS RR.

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
- 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 depends on the memory of Cisco device. Configuring a large number of DNS views and view lists uses more device memory, and configuring a large number of views in the view lists uses more device processor time. For optimum performance, configure views and view list members that are required to support your Split DNS query forwarding or query resolution needs.

Restricted View Use Queries from the Associated VRF

A DNS view is always associated with a VRF— the global VRF or a named VRF, so as to limit the view usage in handling DNS queries that arrive on an interface matching a particular VRF:

- A DNS view that is associated with the global VRF can be used only to handle DNS queries that arrive on an interface in the global address space.
- A DNS view that is associated with a named VRF can be used only to handle DNS queries that arrive on an interface that matches the VRF with which the view is associated.

Note Additional restrictions (described in DNS Views) 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

- 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.
- 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 device with the split DNS feature to forward DNS queries, the device 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 device 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 device. Configuring a larger number of DNS views and view lists uses more device memory, and configuring a larger number of views in the view lists uses more device 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 device 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 device 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 device 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 device 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 device 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 device 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 device.

Interface-specific View Lists

A DNS view list can be attached to a device 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 device. 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.

How to Configure DNS

Mapping Host Names to IP Addresses

Perform this task to associate host names with IP addresses.

A name server is used to keep track of information associated with domain names. A name server can maintain a database of host name-to-address mappings. Each name can map to one or more IP addresses. In order to use this service to map domain names to IP addresses, you must specify a name server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip host** *name* [*tcp-port-number*] *address1* [*address2 ... address8*] [*mx* ns srv]
4. Do one of the following:
   - **ip domain name** *name*
   - **ip domain list** *name*
5. **ip name-server** *server-address1* [*server-address2 ... server-address6*]
6. **ip domain lookup**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**ip host** *name* [*tcp-port-number*] *address1* [*address2 ... address8*] [*mx* ns srv]
	Example:
	`Device(config)# ip host cisco-rtp 192.168.0.148`
	`Device(config)# ip host test mx 1 mx_record`
	`Device(config)# ip host test ns ns_record`
	`Device(config)# ip host test srv 0 0 0 srv_record`
		Defines a static host name-to-address mapping in the host name cache.
		• Typically, it is easier to refer to network devices by symbolic names rather than numerical addresses (services such as Telnet can use host names or addresses). Host names and IP addresses can be associated with one another through static or dynamic means.
		• Manually assigning host names to addresses is useful when dynamic mapping is not available.

	Command or Action	Purpose
		• Mail exchanger (mx) identifies the mail server that is responsible for handling e-mails for a given domain name. • Name server (ns) state the authoritative name servers for the given domain. • Service (srv) records specifies the location of a service.

Step 4	Do one of the following:
	• **ip domain name** *name*
	• **ip domain list** *name*
	Example:
	`Device(config)# ip domain name cisco.com`
	Example:
	`Device(config)# ip domain list cisco1.com`
		(Optional) Defines a default domain name that the Cisco IOS XE software will use to complete unqualified host names.
		or
		(Optional) Defines a list of default domain names to complete unqualified host names.
		• You can specify a default domain name that the Cisco IOS XE software will use to complete domain name requests. You can specify either a single domain name or a list of domain names. Any host name that does not contain a complete domain name will have the default domain name you specify appended to it before the name is looked up.
		Note If there is no domain list, the domain name that you specified with the **ip domain name** global configuration command is used. If there is a domain list, the default domain name is not used. The **ip domain list** command is similar to the **ip domain name** command, except that with the **ip domain list** command you can define a list of domains, each to be tried in turn until the system finds a match.

Step 5	**ip name-server** *server-address1* [*server-address2 ... server-address6*] **Example:** `Device(config)# ip name-server 172.16.1.111 172.16.1.2`	Specifies one or more hosts that supply name information. • Specifies one or more hosts (up to six) that can function as a name server to supply name information for DNS.
Step 6	**ip domain lookup** **Example:** `Device(config)# ip domain lookup`	(Optional) Enables DNS-based address translation. • DNS is enabled by default. Use this command if DNS has been disabled.

What to do next

The name lookup system can be statically configured using the commands described in this task. Some other functions in Cisco IOS XE, such as DHCP can dynamically modify the state of the name lookup system. Use the **show hosts** command to display the cached host names and the DNS configuration.

Disabling DNS Queries for ISO CLNS Addresses

Perform this task to disable DNS queries for ISO CLNS addresses.

If your device has both IP and ISO Connectionless Network Service (ISO CLNS) enabled and you want to use ISO CLNS network service access point (NSAP) addresses, you can use the DNS to query these addresses, as documented in RFC 1348. This feature is enabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ip domain lookup nsap**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no ip domain lookup nsap** **Example:** `Device(config)# no ip domain lookup nsap`	Disables DNS queries for ISO CLNS addresses.

Verifying DNS

Perform this task to verify your DNS configuration.

SUMMARY STEPS

1. **enable**
2. **ping** *host*
3. **show hosts**
4. **debug ip domain**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**ping** *host* **Example:** `Device# ping cisco-rtp`	Diagnoses basic network connectivity. • After the DNS configuration is set, you can verify the DNS server by using a hostname to ping or telnet to a device.
Step 3	**show hosts** **Example:** `Device# show hosts`	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses. • After a name is resolved using DNS, use the **show hosts** command to view the cached hostnames and the DNS configuration.
Step 4	**debug ip domain** **Example:** `Device# debug ip domain`	Enables DNS debugging and displays DNS debugging information. • To view more DNS debugging options such as DNS server response debugging and so on, use the question mark (?) online help function.

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**] **dns trust** *name*
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** [**vrf** *vrf-name*] *name-server-ip-address*
   - **domain name-server interface** *interface*

8. **domain multicast** *domain-name*
9. [**no**] **dns forwarding**
10. **dns forwarder** [**vrf** *vrf-name*] *forwarder-ip-address*
11. **dns forwarding source-interface** *interface*
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dns view** [**vrf** *vrf-name*] {**default** | *view-name*} **Example:** `Device(config)# ip dns view vrf vpn101 user3`	Defines a DNS view and enters DNS view configuration mode.
Step 4	[**no**] **dns trust** *name* **Example:** `Device(cfg-dns-view)# dns trust name`	(Optional) Enables or disables storage of trusted keys in a view and enters DNS view configuration mode. The dns trust key enables the DNS security feature.
Step 5	[**no**] **domain lookup** **Example:** `Device(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:
	`Device(cfg-dns-view)# domain name example.com`
	Example:
	`Device(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 device 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 device responds to the

	Command or Action	Purpose

		query. Otherwise, because the query cannot be answered using the hostname cache, the device forwards the query using the configured domain name servers.
		• If the device 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.

Step 7	Do one of the following:
	• **domain name-server** [**vrf** *vrf-name*] *name-server-ip-address*
	• **domain name-server interface** *interface*
	Example:
	`Device(cfg-dns-view)# domain name-server 192.168.2.124`
	Example:
	`Device(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. The IP address of the name server can be an IPv4 or IPv6 address, and the IP address can be associated with a Virtual Private Network (VPN) routing and forwarding (VRF) instance.
		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:** `Device(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	[**no**] **dns forwarding** **Example:**	(Optional) Enables or disables forwarding of incoming DNS queries handled using the DNS view.

	Command or Action	Purpose
	`Device(cfg-dns-view)# dns forwarding`	**Note** The query forwarding capability is enabled by default.
Step 10	**dns forwarder** [**vrf** *vrf-name*] *forwarder-ip-address* **Example:** `Device(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. • The forwarder IP address can be an IPv4 or IPv6 address. • 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 11	**dns forwarding source-interface** *interface* **Example:** `Device(cfg-dns-view)# dns forwarding source-interface FastEthernet0/0`	Defines the interface on which to forward queries when this DNS view is used.
Step 12	**end** **Example:** `Device(cfg-dns-view)# end`	Returns to privileged EXEC mode.

Verifying DNS Views

Perform this task to verify the DNS configuration.

SUMMARY STEPS

1. **enable**
2. **show ip dns view** [**vrf** *vrf-name*] [**default** | *view-name*]
3. **show ip dns server** [**vrf** *vrf-name*] [**default** | *view-name*]
4. **clear ip dns servers**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show ip dns view** [**vrf** *vrf-name*] [**default** | *view-name*] **Example:** `Device# 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.
Step 3	**show ip dns server** [**vrf** *vrf-name*] [**default** | *view-name*] **Example:** `Device# show ip dns server vrf vpn101 user3`	Displays information from name server cache.
Step 4	**clear ip dns servers**	Cleans up server from name server cache.

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 device 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. **ip dns name-list** [*number*] [*permit/deny*] [*name*]
5. **view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number*
6. **restrict name-group** *name-list-number*
7. **restrict source access-group** *acl-number*
8. **exit**
9. **end**
10. **show ip dns view-list** *view-list-name*
11. **show ip dns name-list** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip dns view-list** *view-list-name* **Example:** `Device(config)# ip dns view-list userlist5`	Defines a DNS view list and enters DNS view list configuration mode.
Step 4	**ip dns name-list** [*number*] [*permit/deny*] [*name*] **Example:** `Device(config)# ip dns name-list 10`	Defines a DNS name list and enters DNS name list configuration mode.
Step 5	**view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number* **Example:** `Device(cfg-dns-view-list)# view vrf vpn101 user5 10`	Defines a DNS view list member and enters DNS view list member configuration mode.
Step 6	**restrict name-group** *name-list-number* **Example:** `Device(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 7	**restrict source access-group** *acl-number* **Example:** `Device(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 8	**exit** **Example:** `Device(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 9	**end** **Example:** `Device(cfg-dns-view-list)# end`	Returns to privileged EXEC mode.
Step 10	**show ip dns view-list** *view-list-name* **Example:** `Device# 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 11	**show ip dns name-list** *number* **Example:** `Device# show ip dns name-list 5`	Displays information about a particular DNS name list or all configured DNS name 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show ip dns view-list** *view-list-name* **Example:** `Device# 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:** `Device# configure terminal`	Enters global configuration mode.
Step 4	**ip dns view-list** *view-list-name* **Example:** `Device(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:** `Device(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:** `Device(cfg-dns-view-list-member)# end`	Returns to privileged EXEC mode.
Step 7	**show ip dns view-list** *view-list-name* **Example:** `Device# 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip dns view-list** *view-list-name* **Example:** `Device# 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:** `Device# configure terminal`	Enters global configuration mode.
Step 4	**ip dns view-list** *view-list-name* **Example:** `Device(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:** `Device(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:** `Device(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:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(cfg-dns-view-list-member)# end`	
Step 8	**show ip dns view-list** *view-list-name* **Example:** `Device# 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 Device

Perform this task to specify the default DNS view list for the device's DNS server. The device 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dns server view-group** *name-list-number* **Example:** `Device(config)# ip dns server view-group 500`	Configures the default DNS view list for the device's DNS server.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

	Command or Action	Purpose
Step 5	**show running-config** **Example:** `Device# 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 Device Interface

Perform this optional task if you need to specify a DNS view list for a particular device interface. The device 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface* **Example:** `Device(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:** `Device(config-if)# ip dns view-group userlist5`	Configures the DNS view list for this interface on the device.
Step 5	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# end`	
Step 6	**show running-config** **Example:** `Device# 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dns view** [**vrf** *vrf-name*] {**default**	*view-name*} **Example:** `Device(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.
Step 4	**domain resolver source-interface** *interface-type number* **Example:** `Device(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:**	(Optional) Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# end`	

Configuration Examples for DNS

Example: Creating a Domain List with Alternate Domain Names

The following example establishes a domain list with several alternate domain names:

```
ip domain list csi.com
ip domain list telecomprog.edu
ip domain list merit.edu
```

Example: Mapping Host Names to IP Addresses

The following example configures the host-name-to-address mapping process. IP DNS-based translation is specified, the addresses of the name servers are specified, and the default domain name is given.

```
! IP DNS-based host name-to-address translation is enabled
ip domain lookup
! Specifies hosts 192.168.1.111 and 192.168.1.2 as name servers
ip name-server 192.168.1.111 192.168.1.2
! Defines cisco.com as the default domain name the device uses to complete
! Set the name for unqualified host names
ip domain name cisco.com
```

Example: Customizing DNS

The following example shows the ip dns servers.

```
show ip dns server

   IP             VRF      TTL(s)   RTT(ms)  RTO(ms)  EDNS  DNSSEC  RECURSION
-------------------------------------------------------------------------------
2::1              red      628      1451     1451      Yes     Yes     Yes
172.168.10.1               875      1787     1787      Yes     Yes     Yes
2.2.2.1           red      606      1447     1447      Yes     Yes     Yes
1::1                       207      300      300       Yes     Yes     Yes
1.1.1.1                    179      242      242       Yes     Yes     Yes
```

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

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.

Additional References for Configuring DNS

Related Documents

Related Topic	Document Title
Master Command List	Cisco IOS Master Command List
IP Addressing Services Command Reference	Cisco IOS IP Addressing Services Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 1348	DNS NSAP Resource Records

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Configuring 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 Configuring DNS

Feature Name	Releases	Feature Configuration Information
Configuring DNS	Cisco IOS XE Release 2.1	The Domain Name System (DNS) is a distributed database in which you can map host names to IP addresses through the DNS protocol from a DNS server. Each unique IP address can have an associated host name. The Cisco IOS XE software maintains a cache of host name-to-address mappings. This cache speeds the process of converting names to addresses.
	Cisco IOS XE Release 3.13S	The following commands were introduced or modified: **debug ip domain**, **debug ip domain replies**.
	Cisco IOS XE Release 3.16S	The following commands were introduced or modified: **dns trust**, **clear ip dns servers**.