dh – dm

dhcp-client broadcast-flag

To allow the ASA to set the broadcast flag in the DHCP client packet, use the **dhcp-client broadcast-flag** command in global configuration mode. To disallow the broadcast flag, use the **no** form of this command.

dhcp-client broadcast-flag
no dhcp-client broadcast-flag

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the broadcast flag is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

If you enable the DHCP client for an interface using the **ip address dhcp** command, then you can use this command to set the broadcast flag to 1 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1.

If you enter the **no dhcp-client broadcast-flag** command, the broadcast flag is set to 0, and the DHCP server unicasts the reply packets to the client with the offered IP address.

The DHCP client can receive both broadcast and unicast offers from the DHCP server.

Examples

The following example enables the broadcast flag:

```
ciscoasa(config)# dhcp-client broadcast-flag
```

Related Commands

Command	Description
ip address dhcp	Enables the DHCP client for an interface.
interface	Enters interface configuration mode so you can set the IP address.
dhcp-client client-id	Sets DHCP request packet option 61 to include the interface MAC address.

Command	Description
dhcp-client update dns	Enables DNS updates for the DHCP client.

dhcp-client client-id

To force a MAC address to be stored inside a DHCP request packet for option 61 instead of the default internally generated string, use the **dhcp-client client-id** command in global configuration mode. To disallow the MAC address, use the **no** form of this command.

dhcp-client client-id interface *interface_name*
no dhcp-client client-id interface *interface_name*

Syntax Description

interface *interface_name*	Specifies the interface on which you want to enable the MAC address for option 61.

Command Default

By default, an internally-generated ASCII string is used for option 61.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

If you enable the DHCP client for an interface using the **ip address dhcp** command, some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. Use the **dhcp-client client-id** command to include the interface MAC address for option 61.

Examples

The following example enables the MAC address for option 61 for the outside interface:

```
ciscoasa(config)# dhcp-client client-id interface outside
```

Related Commands

Command	Description
ip address dhcp	Enables the DHCP client for an interface.
interface	Enters interface configuration mode so you can set the IP address.
dhcp-client broadcast-flag	Sets the broadcast flag in the DHCP client packet.

Command	Description
dhcp-client update dns	Enables DNS updates for the DHCP client.

dhcp client route distance

To configure an administrative distance for routes learned through DHCP, use the **dhcp client route distance** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

dhcp client route distance *distance*
no dhcp client route distance *distance*

Syntax Description

distance	The administrative distance to apply to routes learned through DHCP. Valid values are from 1 to 255.

Command Default

Routes learned through DHCP are given an administrative distance of 1 by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **dhcp client route distance** command is checked only when a route is learned from DHCP. If the **dhcp client route distance** command is entered after a route is learned from DHCP, the administrative distance specified does not affect the existing learned route. Only routes learned after the command was entered have the specified administrative distance.

You must specify the **setroute** option in the **ip address dhcp** command to obtain routes through DHCP.

If DHCP is configured on multiple interfaces, you must use the **dhcp client route distance** command on each of the interfaces to indicate the priority of the installed routes.

Examples

The following example obtains the default route through DHCP on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the backup route obtained through DHCP on GigabitEthernet0/3 is used. The backup route is assigned an administrative distance of 254.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

Related Commands

Command	Description
dhcp client route track	Associates routes learned through DHCP with a tracking entry object.
ip address dhcp	Configures the specified interface with an IP address obtained through DHCP.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

dhcp client route track

To configure the DHCP client to associate added routes with a specified tracked object number, use the **dhcp client route track** command in interface configuration mode. To disable DHCP client route tracking, use the **no** form of this command.

dhcp client route track *number*
no dhcp client route track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **dhcp client route track** command is checked only when a route is learned from DHCP. If the **dhcp client route track** command is entered after a route is learned from DHCP, the existing learned routes are not associated with a tracking object. You must put the following two commands in the correct order. Make sure that you always enter the **dhcp client route track** command first, followed by the **ip address dhcp setroute** command, If you have already entered the **ip address dhcp setroute** command, then remove it and reenter it in the order previously described. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option in the **ip address dhcp** command to obtain routes through DHCP.

If DHCP is configured on multiple interfaces, you must use the **dhcp client route distance** command on each of the interfaces to indicate the priority of the installed routes.

Examples

The following example obtains the default route through DHCP on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the backup route obtained through DHCP on GigabitEthernet0/3 is used. The backup route is assigned an administrative distance of 254.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

Related Commands

Command	Description
dhcp client route distance	Assigns an administrative distance to routes learned through DHCP.
ip address dhcp	Configures the specified interface with an IP address obtained through DHCP.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

dhcp-client update dns

To configure the update parameters that the DHCP client passes to the DHCP server, use the **dhcp-client update dns** command in global configuration mode. To remove the parameters that the DHCP client passes to the DHCP server, use the **no** form of this command.

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

Syntax Description

both	The client requests that the DHCP server update both the DNS A and PTR resource records.
none	The client requests that the DHCP server perform no DDNS updates.
server	Specifies the DHCP server to receive the client requests.

Command Default

By default, the ASA requests that the DHCP server perform PTR RR updates only. The client does not send the FQDN option to the server.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can also be entered in interface configuration mode, but it is not hyphenated. See the **dhcp client update dns** command. When entered in interface mode, the **dhcp client update dns** command overrides settings configured by this command in global configuration mode.

Examples

The following example configures the client to request that the DHCP server update neither the A and the PTR RRs:

```
ciscoasa(config)# dhcp-client update dns server none
```

The following example configures the client to request that the server update both the A and PTR RRs:

ciscoasa(config)# **dhcp-client update dns server both**

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.
ddns update	Associates a DDNS update method with a ASA interface or a DDNS update hostname.
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

dhcp-network-scope

To specify the range of IP addresses the DHCP server should use to assign addresses to users of this group policy, use the **dhcp-network-scope** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

dhcp-network-scope { *ip_address* | **none** }
no dhcp-network-scope

Syntax Description

ip_address	Specifies a routeable address on the same subnet as the desired pool, but not within the pool. The DHCP server determines which subnet this IP address belongs to and assigns an IP address from that pool.
none	Sets the DHCP scope to a null value, thereby allowing no IP addresses. Prevents inheriting a value from a default or specified group policy.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same subnet identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group.

If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address.

To specify a scope, enter a routeable address on the same subnet as the desired pool, but not within the pool. The DHCP server determines which subnet this IP address belongs to and assigns an IP address from that pool.

We recommend using the IP address of an interface whenever possible for routing purposes. For example, if the pool is 10.100.10.2-10.100.10.254, and the interface address is 10.100.10.1/24, use 10.100.10.1 as the DHCP scope. Do not use the network number. You can use DHCP for IPv4 addressing only. If the address you choose is not an interface address, you might need to create a static route for the scope address.

This command allows inheritance of a value from another group policy. To prevent inheriting a value, use the **dhcp-network-scope none** command.

Examples

The following example shows how to set an IP subnetwork of 10.10.85.1 for the group policy named First Group:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# dhcp-network-scope 10.10.85.1
```

dhcp-server

To configure support for DHCP servers that assign IP addresses to clients as a VPN tunnel is established, use the **dhcp-server** command in tunnel-group general-attributes configuration mode. To return this command to the default, use the **no** form of this command.

dhcp-server [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]
[**no**] **dhcp-server** [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]

Syntax Description

ip1	Address of a DHCP server
ip2-ip10	(Optional) Addresses of additional DHCP servers. Up to ten may be specified in the same command or spread over multiple commands.
link-selection	(Optional) Specifies that the ASA should send DHCP suboption 5, the Link Selection Suboption for the Relay Information Option 82, defined by RFC 3527. This should only be used with servers that support this RFC.
subnet-selection	(Optional) Specifies that the ASA should send DHCP Option 118, the IPv4 Subnet Selection Option, defined by RFC 3011. This should only be used with servers that support this RFC.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(5)	The **link-selection** and **subnet-selection** keywords were added.

Usage Guidelines

You can apply this attribute to remote access tunnel group types only.

Examples

The following command, entered in config-general configuration mode, adds three DHCP servers (dhcp1, dhcp2, and dhcp3) to the IPsec remote access tunnel group “remotegrp”:

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# dhcp-server dhcp1 dhcp2 dhcp3
ciscoasa(config-tunnel-general)
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

dhcpd address

To define the IP address pool used by the DHCP server, use the **dhcpd address** command in global configuration mode. To remove an existing DHCP address pool, use the **no** form of this command.

dhcpd address *ip_address 1* [- *ip_address 2*] *interface_name*
no dhcpd address *interface_name*

Syntax Description

interface_name	Interface to which the address pool is assigned. In transparent mode, specify a bridge group member interface. In routed mode, specify a routed interface or a BVI; do not specify the bridge group member interface.
ip_address1	Start address of the DHCP address pool.
ip_address2	End address of the DHCP address pool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	You can now configure this command on a BVI in routed mode when using Integrated Routing and Bridging.

Usage Guidelines

The address pool of an ASA DHCP server must be within the same subnet of the ASA interface on which it is enabled, and you must specify the associated ASA interface using *interface_name*.

The size of the address pool is limited to 256 addresses per pool on the ASA. If the address pool range is larger than 253 addresses, the netmask of the ASA interface cannot be a Class C address (for example, 255.255.255.0) and needs to be something larger, for example, 255.255.254.0.

DHCP clients must be physically connected to the subnet of the ASA DCHP server interface.

The **dhcpd address** command cannot use interface names with a “-” (dash) character because this character is interpreted as a range specifier instead of as part of the object name.

The **no dhcpd address** *interface_name* command removes the DHCP server address pool that you configured for the specified interface.

See the CLI configuration guide for information about how to implement the DHCP server feature in the ASA.

Examples

The following example shows how to configure an address pool and DNS server for the DHCP clients on the DMZ interface of the ASA:

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 209.165.200.226
ciscoasa(config)# dhcpd enable dmz
```

The following example shows how to configure a DHCP server on the inside interface. The **dhcpd address** command assigns a pool of 10 IP addresses to the DHCP server on that interface.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd enable	Enables the DHCP server on the specified interface.
show dhcpd	Displays DHCP binding, statistical, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd auto_config

To enable the ASA to automatically configure DNS, WINS and domain name values for the DHCP server based on the values obtained from an interface running a DHCP or PPPoE client, or from a VPN server, use the **dhcpd auto_config** command in global configuration mode. To discontinue the automatic configuration of DHCP parameters, use the **no** form of this command.

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]
no dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

Syntax Description

client_if_name	Specifies the interface running the DHCP client that supplies the DNS, WINS, and domain name parameters.
interface *if_name*	Specifies the interface to which the action will apply.
vpnclient-wins-override	Overrides the interface DHCP or PPPoE client WINS parameter with the vpnclient parameter.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you specify DNS, WINS, or domain name parameters using the CLI commands, then the CLI-configured parameters overwrite the parameters obtained by automatic configuration.

Examples

The following example shows how to configure DHCP on the inside interface. The **dhcpd auto_config** command is used to pass DNS, WINS, and domain information obtained from the DHCP client on the outside interface to the DHCP clients on the inside interface.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd auto_config outside
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd enable	Enables the DHCP server on the specified interface.
show ip address dhcp server	Displays detailed information about the DHCP options provided by a DHCP server to an interface acting as a DHCP client.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd dns

To define the DNS servers for DHCP clients, use the **dhcpd dns** command in global configuration mode. To clear defined servers, use the **no** form of this command.

dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]
no dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

Syntax Description

dnsip1	Specifies the IP address of the primary DNS server for the DHCP client.
dnsip2	(Optional) Specifies the IP address of the alternate DNS server for the DHCP client.
interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dhcpd dns** command lets you specify the IP address or addresses of the DNS server(s) for the DHCP client. You can specify two DNS servers. The **no dhcpd dns** command lets you remove the DNS IP address(es) from the configuration.

Examples

The following example shows how to configure an address pool and DNS server for the DHCP clients on the DMZ interface of the ASA.

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 192.168.1.2
ciscoasa(config)# dhcpd enable dmz
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.

Command	Description
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
dhcpd enable	Enables the DHCP server on the specified interface.
dhcpd wins	Defines the WINS servers for DHCP clients.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd domain

To define the DNS domain name for DHCP clients, use the **dhcpd domain** command in global configuration mode. To clear the DNS domain name, use the **no** form of this command.

dhcpd domain *domain_name* [**interface** *if_name*]
no dhcpd domain [*domain_name*] [**interface** *if_name*]

Syntax Description

domain_name	Specifies the DNS domain name (example.com).
interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dhcpd domain** command lets you specify the DNS domain name for the DHCP client. The **no dhcpd domain** command lets you remove the DNS domain server from the configuration.

Examples

The following example shows how to configure the domain name supplied to DHCP clients by the DHCP server on the ASA:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.

Command	Description
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd enable

To enable the DHCP server, use the **dhcpd enable** command in global configuration mode. To disable the DHCP server, use the **no** form of this command.

dhcpd enable *interface*
no dhcpd enable *interface*

Syntax Description

interface	Specifies the interface on which to enable the DHCP server.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The DHCP server provides network configuration parameters to DHCP clients. Support for the DHCP server within the ASA means that the ASA can use DHCP to configure connected clients. The **dhcpd enable** *interface* command lets you enable the DHCP daemon to listen for the DHCP client requests on the DHCP-enabled interface. The **no dhcpd enable** command disables the DHCP server feature on the specified interface.

Note For multiple context mode, you cannot enable the DHCP server on an interface that is used by more than one context (a shared VLAN).

When the ASA responds to a DHCP client request, it uses the IP address and subnet mask of the interface at which the request was received as the IP address and subnet mask of the default gateway in the response.

Note The ASA DHCP server daemon does not support clients that are not directly connected to an ASA interface.

See the CLI configuration guide for information about how to implement the DHCP server feature in the ASA.

Examples

The following example shows how to enable the DHCP server on the inside interface:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
debug dhcpd	Displays debugging information for the DHCP server.
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
show dhcpd	Displays DHCP binding, statistical, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd lease

To specify the DHCP lease length, use the **dhcpd lease** command in global configuration mode. To restore the default value for the lease, use the **no** form of this command.

dhcpd lease *lease_length* [**interface** *if_name*]
no dhcpd lease [*lease_length*] [**interface** *if_name*]

Syntax Description

interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
lease_length	Specifies the length of the IP address lease, in seconds, granted to the DHCP client from the DHCP server. Valid values are from 300 to 1048575 seconds.

Command Default

The default *lease_length* is 3600 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dhcpd lease** command lets you specify the length of the lease, in seconds, that is granted to the DHCP client. This lease indicates how long the DHCP client can use the assigned IP address that the DHCP server granted.

The **no dhcpd lease** command lets you remove the lease length that you specified from the configuration and replaces this value with the default value of 3600 seconds.

Examples

The following example shows how to specify the length of the lease of DHCP information for DHCP clients:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd option

To configure DHCP options, use the **dhcpd option** command in global configuration mode. To clear the option, use the **no** form of this command.

dhcpd option *code* { **ascii** *string* } | { **ip** *IP_address* [*IP_address*] } | { **hex** *hex_string* } [**interface** *if_name*]
no dhcpd option *code* [**interface** *if_name*]

Syntax Description

ascii *string*	Specifies that the option parameter is an ASCII character string without spaces.
code	Specifies a number representing the DHCP option being set. Valid values are 0 to 255 with several exceptions. See the Usage Guidelines section for the list of DHCP option codes that are not supported.
hex *hex_string*	Specifies that the option parameter is a hexadecimal string with an even number of digits and no spaces. You do not need to use a 0x prefix.
interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
ip	Specifies that the option parameter is an IP address. You can specify a maximum of two IP addresses with the **ip** keyword.
IP_address	Specifies a dotted-decimal IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can use the **dhcpd option** command to provide TFTP server information to Cisco IP Phones and routers.

When a DHCP option request arrives at the ASA DHCP server, the ASA places the value or values that are specified by the **dhcpd option** command in the response to the client.

The **dhcpd option 66** and **dhcpd option 150** commands specify TFTP servers that Cisco IP Phones and routers can use to download configuration files. Use these commands as follows:

- **dhcpd option 66 ascii** *string*, where *string* is either the IP address or hostname of the TFTP server. Only one TFTP server can be specified for option 66.
- **dhcpd option 150 ip** *IP_address* [*IP_address*], where *IP_address* is the IP address of the TFTP server. You can specify a maximum of two IP addresses for option 150.

Note The **dhcpd option 66** command only takes an **ascii** parameter, and the **dhcpd option 150** only takes an **ip** parameter.

Use the following guidelines when specifying an IP address for the **dhcpd option 66 | 150** commands:

- If the TFTP server is located on the DHCP server interface, use the local IP address of the TFTP server.
- If the TFTP server is located on a less secure interface than the DHCP server interface, then general outbound rules apply. Create a group of NAT, global, and access list entries for the DHCP clients, and use the actual IP address of the TFTP server.
- If the TFTP server is located on a more secure interface, then general inbound rules apply. Create a group of static and access list statements for the TFTP server and use the global IP address of the TFTP server.

For information about other DHCP options, see RFC 2132.

Note The ASA does not verify that the option type and value that you provide match the expected type and value for the option code as defined in RFC 2132. For example, you can enter the **dhcpd option 46 ascii hello** command, and the ASA accepts the configuration although option 46 is defined in RFC 2132 as a single-digit, hexadecimal value.

You cannot configure the following DHCP options with the **dhcpd option** command:

Option Code	Description
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER

Option Code	Description
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

Examples

The following example shows how to specify a TFTP server for DHCP option 66:

```
ciscoasa(config)# dhcpd option 66 ascii MyTftpServer
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd ping_timeout

To change the default timeout for DHCP ping, use the **dhcpd ping_timeout** command in global configuration mode. To return to the default value, use the **no** form of this command.

dhcpd ping_timeout *number* [**interface** *if_name*]
no dhcpd ping_timeout [**interface** *if_name*]

Syntax Description

interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
number	The timeout value of the ping, in milliseconds. The minimum value is 10, the maximum is 10000. The default is 50.

Command Default

The default number of milliseconds for *number* is 50.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To avoid address conflicts, the DHCP server sends two ICMP ping packets to an address before assigning that address to a DHCP client. The ASA waits for both ICMP ping packets to time out before assigning an IP address to a DHCP client. For example, if the default value is used, the ASA waits for 1500 milliseconds (750 milliseconds for each ICMP ping packet) before assigning an IP address.

A long ping timeout value can adversely affect the performance of the DHCP server.

Examples

The following example shows how to use the **dhcpd ping_timeout** command to change the ping timeout value for the DHCP server:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd reserve-address

To reserve a DHCP address for an interface, use the **dhcpd reserve-address** command in global configuration mode. To remove an existing DHCP address reservation, use the **no** form of this command.

dhcpd reserve-address *ip_address mac_address if_name*
no dhcpd reserve_address *ip_address mac_address if_name*

Syntax Description

ip_address	The IP address from the address pool assigned to the DHCP client, based on the client's MAC address.
mac_address	The client MAC address.
if_name	The interface on which you want to reserve an IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was added.

Usage Guidelines

The reserved address must come from the configured address pool, and the address pool must be on the same subnet as the ASA interface. In transparent mode, specify a bridge group member interface. In routed mode, specify a routed interface or a BVI; do not specify the bridge group member interface.

Examples

The following example shows how to use the **dhcpd reserve-address** command to assign a specific address from the address pool to client based on the client's MAC address:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd enable inside
ciscoasa(config)# dhcpd reserve-address 10.0.1.109 030c.f142.4cde inside
```

Related Commands

Command	Description
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.

Command	Description
dhcpd enable	Enables the DHCP server on the specified interface.
show dhcpd	Displays DHCP binding, statistical, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd update dns

To enable a DHCP server to perform DDNS updates, use the **dhcpd update dns** command in global configuration mode. To disable DDNS by a DHCP server, use the **no** form of this command.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]
no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

Syntax Description

both	Specifies that the DHCP server updates both A and PTR DNS RRs.
interface	Specifies the ASA interface to which the DDNS updates apply.
override	Specifies that the DHCP server overrides DHCP client requests.
srv_ifc_name	Specifies an interface to apply this option to.

Command Default

By default, the DHCP server performs PTR RR updates only.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

DDNS updates the name-to-address and address-to-name mapping maintained by DNS. Updates are performed in conjunction with a DHCP server. The **dhcpd update dns** command enables updates by the server.

Name and address mapping is contained in two types of RRs:

- The A resource record contains domain name-to IP-address mapping.
- The PTR resource record contains IP address- to-domain name mapping.

DDNS updates can be used to maintain consistent information between the A and PTR RR types.

Using the **dhcpd update dns** command, the DHCP server can be configured to perform both A and PRT RR updates or PTR RR updates only. It can also be configured to override update requests from the DHCP client.

Examples

The following example configures the DDNS server to perform both A and PTR updates and override requests from the DHCP client:

```
ciscoasa(config)# dhcpd update dns both override
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.
ddns update	Associates a DDNS update method with an ASA interface or a DDNS update hostname.
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

dhcpd wins

To define the WINS server IP addresses for DHCP clients, use the **dhcpd wins** command in global configuration mode. To remove the WINS server IP addresses from the configuration, use the **no** form of this command.

dhcpd wins *server1* [*server2*] [**interface** *if_name*]
no dhcpd wins [*server1* [*server2*]] [**interface** *if_name*]

Syntax Description

interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
server1	Specifies the IP address of the primary Microsoft NetBIOS name server (WINS server).
server2	(Optional) Specifies the IP address of the alternate Microsoft NetBIOS name server (WINS server).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dhcpd wins** command lets you specify the addresses of the WINS servers for the DHCP client. The **no dhcpd wins** command removes the WINS server IP addresses from the configuration.

Examples

The following example shows how to specify WINS server information that is sent to DHCP clients:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
dhcpd dns	Defines the DNS servers for DHCP clients.
show dhcpd	Displays DHCP binding, statistical, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcprelay enable

To enable the DHCP relay agent, use the **dhcprelay enable** command in global configuration mode. To disable the DHCP relay agent, use the **no** form of this command.

dhcprelay enable *interface_name*
no dhcprelay enable *interface_name*

Syntax Description

interface_name	Name of the interface on which the DHCP relay agent accepts client requests.

Command Default

The DHCP relay agent is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The DHCP relay agent allows DHCP requests to be forwarded from a specified ASA interface to a specified DHCP server.

For the ASA to start the DHCP relay agent with the **dhcprelay enable** *interface_name* command, you must have a **dhcprelay server** command already in the configuration. Otherwise, the ASA displays an error message similar to the following:

```
DHCPRA: Warning - There are no DHCP servers configured!
No relaying can be done without a server!
Use the 'dhcprelay server <server_ip> <server_interface>' command
```

You cannot enable DHCP relay under the following conditions:

- You cannot enable DHCP relay and the DHCP relay server on the same interface.
- You cannot enable DCHP relay and a DHCP server (**dhcpd enable**) on the same interface.
- The DHCP relay agent cannot be enabled if the DHCP server is also enabled.
- For multiple context mode, you cannot enable DHCP relay on an interface that is used by more than one context (a shared VLAN).

The **no dhcprelay enable** *interface_name* command removes the DHCP relay agent configuration for the interface that is specified by the *interface_name* argument only.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the ASA, client requests on the inside interface of the ASA, and a timeout value up to 90 seconds:

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

The following example shows how to disable the DHCP relay agent:

```
ciscoasa(config)# no dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
debug dhcp relay	Displays debugging information for the DHCP relay agent.
dhcprelay server	Specifies the DHCP server to which the DHCP relay agent forwards DHCP requests.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay information trust-all

To configure a specified interface as trusted, use the **dhcprelay information trust-all** command in global configuration mode.

dhcprelay information trust-all

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

This command configures a given interface as trusted. To view the interface-specific trusted configuration, use the **show running-config dhcprelay interface** command in interface configuration mode. To configure a given interface as trusted in interface configuration mode, use the **dhcprelay information trusted** command. To view a given interface as trusted in global configuration mode, use the **show running-config dhcprelay** command.

Examples

The following example shows how to configure a specified interface as trusted in global configuration mode:

```
ciscoasa(config-if)# interface vlan501
ciscoasa(config-if)# nameif inside
ciscoasa(config)# dhcprelay information trust-all
ciscoasa(config)# show running-config dhcprelay
dhcprelay information trust-all
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.

Command	Description
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay information trusted

To configure a specified interface as trusted, use the **dhcprelay information trusted** command in interface configuration mode.

dhcprelay information trusted

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

This command configures a given interface as trusted. To view the interface-specific trusted configuration, use the **show running-config dhcprelay interface** command in interface configuration mode. To configure a given interface as trusted in global configuration mode, use the **dhcprelay information trust-all** command. To view a given interface as trusted in global configuration mode, use the **show running-config dhcprelay** command.

Examples

The following example shows how to configure a specified interface as trusted:

```
ciscoasa(config-if)# interface gigabitEthernet 0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay information trusted
ciscoasa(config)# show running-config dhcprelay
interface gigabitEthernet 0/0
nameif inside
dhcprelay information trusted
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.

Command	Description
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay server (global)

To specify the DHCP server to which DHCP requests are forwarded, use the **dhcpreplay server** command in global configuration mode. To remove the DHCP server from the DHCP relay configuration, use the **no** form of this command.

dhcprelay server [*interface_name*]
no dhcprelay server [*interface_name*]

Syntax Description

interface_name	Specifies the name of the ASA interface on which the DHCP server resides.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The DHCP relay agent allows DHCP requests to be forwarded from a specified ASA interface to a specified DHCP server. You can add up to ten DHCP relay servers per interface. You must add at least one **dhcprelay server** command to the ASA configuration before you can enter the **dhcprelay enable** command. You cannot configure a DHCP client on an interface that has a DHCP relay server configured.

The **dhcprelay server** command opens UDP port 67 on the specified interface and starts the DHCP relay task as soon as the **dhcprelay enable** command is added to the configuration.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the ASA, client requests on the inside interface of the ASA, and a timeout value of up to 90 seconds:

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay server (interface)

To specify the DHCP relay interface server to which DHCP requests are forwarded, use the **dhcpreplay server** command in interface configuration mode. To remove the DHCP relay interface server from the DHCP relay configuration, use the **no** form of this command.

dhcprelay server ip_address
no dhcprelay server ip_address

Syntax Description

ip_address	Specifies the IP address of the DHCP relay interface server to which the DHCP relay agent forwards client DHCP requests.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

The DHCP relay agent allows DHCP requests to be forwarded from a specified ASA interface to a specified DHCP server. You can add up to four DHCP relay servers per interface. You must add at least one **dhcprelay server** command to the ASA configuration before you can enter the **dhcprelay enable** command. You cannot configure a DHCP client on an interface that has a DHCP relay server configured.

The **dhcprelay server** command opens UDP port 67 on the specified interface and starts the DHCP relay task as soon as the **dhcprelay enable** command is added to the configuration.

In the interface configuration mode, you can use the **dhcprelay server** *ip_address* command to configure a DHCP relay server (called a helper) address on a per-interface basis. This means that when a DHCP request is received on an interface and it has helper addresses configured, then the request is forwarded to only those servers.

When you use the **no dhcprelay server** *ip_address* command, the interface stops forwarding DHCP packets to that server and removes the DHCP relay agent configuration for the DHCP server that is specified by the *ip_address* argument only.

This command takes precedence over a DHCP relay server that has been configured in global configuration mode. This means that the DHCP relay agent forwards the client discovery message first to the DHCP relay interface server, then to the DHCP global relay server.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP relay interface server with an IP address of 10.1.1.1 on the outside interface of the ASA, client requests on the inside interface of the ASA, and a timeout value of up to 90 seconds:

```
ciscoasa(config)# interface vlan 10
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay server 10.1.1.1
ciscoasa(config-if)# exit
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay enable inside
dhcprelay timeout 90
interface vlan 10
nameif inside
dhcprelay server 10.1.1.1
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay server (vti tunnel)

To reach a dhcp relay server through a VTI tunnel interface, use the **dhcpreplay server** command in global configuration mode.

dhcprelay server *ip_address vti-ifc-name*

Syntax Description

ip_address	Specifies the IP address of the DHCP relay server that forwards client DHCP requests.
vti-ifc-name	Specify the name of the VTI interface that you want the DHCP relay agent forward the DHCP packets to the DHCP server.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.14(1)	This command was added.

Usage Guidelines

The DHCP relay agent allows DHCP requests to be forwarded from a specified ASA interface to a specified DHCP server. However, the relay agent could be configured only on physical interfaces. As VTI interface was a logical interface, the DHCP relay requests could not be forwarded through it.

From ASA 9.14(1), using this command, the DHCP relay server can forward the packets through a VTI tunnel interface.

Examples

The following example shows how to configure the DHCP relay agent on a VTI tunnel. First, create a VTI tunnel:

```
ciscoasa(config)# interface Tunnel100
ciscoasa(config-if)# nameif vti
ciscoasa(config-if)# ip address 10.1.1.10 255.255.255.0
ciscoasa(config-if)# tunnel source interface outside
ciscoasa(config-if)# tunnel destination 192.168.2.111
ciscoasa(config-if)# tunnel mode ipsec ipv4
ciscoasa(config-if)# tunnel protection ipsec profile PROFILE1
```

Now, configure the DHCP relay server with the tunnel name:

```
ciscoasa(config)# dhcprelay server 192.168.3.112 vti
```

dhcprelay setroute

To set the default gateway address in the DHCP reply, use the **dhcprelay setroute** command in global configuration mode. To remove the default router, use the **no** form of this command.

dhcprelay setroute *interface*
no dhcprelay setroute *interface*

Syntax Description

interface	Configures the DHCP relay agent to change the first default IP address (in the packet sent from the DHCP server) to the address of *interface*.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command causes the default IP address of the DHCP reply to be substituted with the address of the specified ASA interface. The **dhcprelay setroute** *interface* command lets you enable the DHCP relay agent to change the first default router address (in the packet sent from the DHCP server) to the address of *interface*.

If there is no default router option in the packet, the ASA adds one containing the address of *interface*. This action allows the client to set its default route to point to the ASA.

When you do not configure the **dhcprelay setroute** *interface* command (and there is a default router option in the packet), it passes through the ASA with the router address unaltered.

Examples

The following example shows how to set the default gateway in the DHCP reply from the external DHCP server to the inside interface of the ASA:

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay setroute inside
ciscoasa(config)# dhcprelay enable inside
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay server	Specifies the DHCP server that the DHCP relay agent forwards DHCP requests to.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay timeout

To set the DHCP relay agent timeout value, use the **dhcprelay timeout** command in global configuration mode. To restore the timeout value to its default value, use the **no** form of this command.

dhcprelay timeout *seconds*
no dhcprelay timeout

Syntax Description

seconds	Specifies the number of seconds that are allowed for DHCP relay address negotiation.

Command Default

The default value for the DHCP relay timeout is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dhcprelay timeout** command lets you set the amount of time, in seconds, allowed for responses from the DHCP server to pass to the DHCP client through the relay binding structure.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the ASA, client requests on the inside interface of the ASA, and a timeout value up to 90 seconds:

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.

Command	Description
dhcprelay server	Specifies the DHCP server to which the DHCP relay agent forwards DHCP requests.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dialog

To customize dialog box messages displayed to WebVPN users, use the **dialog** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

dialog { **title** | **message** | **border** } **style** *value*
no dialog { **title** | **message** | **border** } **style** *value*

Syntax Description

border	Specifies a change to the border.
message	Specifies a change to the message.
style	Specifies a change to the style.
title	Specifies a change to the title.
value	The actual text or or CSS parameters to display (the maximum is 256 characters).

Command Default

The default title style is background-color:#669999;color:white.

The default message style is background-color:#99CCCC;color:black.

The default border style is border:1px solid black;border-collapse:collapse.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid CSS parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

- The RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma-separated entry indicates the level of intensity of each color to combine with the others.
- The HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the dialog box message, changing the foreground color to blue:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# dialog message style color:blue
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

diameter

To create a custom Diameter attribute-value pair (AVP) for use in a Diameter inspection class or policy map, use the **diameter** command in global configuration mode. To remove an existing custom AVP, use the **no** form of this command.

diameter avp *name* **code** *value* **data-type** *type* [**vendor-id** *id_number*] [**description** *text*]
no diameter avp *name* **code** *value* **data-type** *type* [**vendor-id** *id_number*] [**description** *text*]

Syntax Description

name	The name of the custom AVP you are creating, up to 32 characters. You would refer to this name on the **match avp** command in a Diameter inspection policy map or class map.
code *value*	The custom AVP code value, from 256-4294967295. You cannot enter a code and vendor-id combination that is already defined in the system.
data-type *type*	The data type of the AVP. You can define AVP of the following types. If the new AVP is of a different type, you cannot create a custom AVP for it. • **address**—For IP addresses. • **diameter-identity**—Diameter identity data. • **diameter-uri**—Diameter uniform resource identifier (URI). • **float32**—32-bit floating point number. • **float64**—64-bit floating point number. • **int32**—32-bit integer. • **int64**—64-bit integer. • **octetstring**—Octet string. • **time**—Time value. • **uint32**—32-bit unsigned integer. • **uint64**—64-bit unsigned integer.
vendor-id *id_number*	(Optional.) The ID number of the vendor who defined the AVP, from 0-4294967295. For example, the 3GPP vendor ID is 10415, the IETF is 0.
description *text*	(Optional.) A description of the AVP, up to 80 characters. Enclose the description in quotation marks if you include spaces.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

As new attribute-value pairs (AVP) are defined and registered, you can create custom Diameter AVP to define them and use them in your Diameter inspection policy map. You would get the information you need to create the AVP from the RFC or other source that defines the AVP.

Create custom AVP only if you want to use them in a Diameter inspection policy map or class map for AVP matching.

Examples

The following example shows how to create a custom AVP and then use it in a Diameter inspection policy map.

```
ciscoasa(config)# diameter avp eg_custom_avp code 9999 data-type int32

ciscoasa(config)# policy-map type inspect diameter avp-filter-pmap

asa3(config-pmap)# match avp eg_custom_avp
```

Related Commands

Command	Description
class-map type inspect diameter	Creates a Diameter inspection class map.
match avp	Matches Diameter attribute-value pairs (AVP).
policy-map type inspect diameter	Creates a Diameter inspection policy map.

dir

To display the directory contents, use the **dir** command in privileged EXEC mode.

dir [**/all**] [**all-filesystems**] [**/recursive**] [**disk0:** | **flash: | system:**] [*path*]

Syntax Description

/all	(Optional) Displays all files.
/recursive	(Optional) Displays the directory contents recursively.
all-filesystems	(Optional) Displays the files of all filesystems.
disk0:	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
flash:	(Optional) Displays the directory contents of the default flash partition.
path	(Optional) Specifies a specific path.
system:	(Optional) Displays the directory contents of the file system.

Command Default

If you do not specify a directory, the directory is the current working directory by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dir** command without keywords or arguments displays the directory contents of the current directory.

Examples

The following example shows how to display the directory contents:

```
ciscoasa# dir
Directory of disk0:/
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

The following example shows how to display recursively the contents of the entire file system:

```
ciscoasa# dir /recursive disk0:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

The following example shows how to display the contents of the flash partition:

```
ciscoasa# dir flash:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
pwd	Displays the current working directory.
mkdir	Creates a directory.
rmdir	Removes a directory.

director-localization

To enable director localization to improve performance and reduce round-trip time latency for inter-site clustering for data centers, use the **director-localization** command in cluster group configuration mode. To disable director localization, use the **no** form of this command.

director-localization
no director-localization

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

New connections are typically load-balanced and owned by cluster members within a given site. However, the ASA assigns the director role to a member at any site. Director localization enables additional director roles: a local director at the same site as the owner, and a global director that can be at any site. Keeping the owner and director at the same site improves performance. Also, if the original owner fails, the local director chooses a new connection owner at the same site. The global director is used if a cluster member receives packets for a connection that is owned on a different site.

Set the site ID for the cluster member in the bootstrap configuration.

The following traffic types do not support localization: NAT or PAT traffic; SCTP-inspected traffic; Fragmentation owner query.

Examples

The following example enables director localization for cluster1:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# director-localization
ciscoasa(cfg-cluster)# enable noconfirm
```

Related Commands

Command	Description
cluster group	Enters cluster group configuration mode.
show asp table cluster chash	Shows local cHash tables.
show conn	The conn flag "l" indicates the stub flow is local director "Yl" or local backup "yl".
site-id	Sets the cluster unit site ID for use with inter-site clustering.

disable (cache)

To disable caching for WebVPN, use the **disable** command in cache configuration mode. To reenable caching, use the **no** version of this command.

disable
no disable

Command Default

Caching is enabled with default settings for each cache attribute.

Command Modes

The following table shows the modes in which you enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cache Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Caching stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. It reduces traffic between WebVPN and both the remote servers and end-user browsers, with the result that many applications run much more efficiently.

Examples

The following example shows how to disable caching, and then how to reenable it.

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# disable
ciscoasa(config-webvpn-cache)# no disable
ciscoasa(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters webvpn cache configuration mode.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.

Command	Description
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum size of an object to cache.

disable (privileged EXEC)

To exit privileged EXEC mode and return to unprivileged EXEC mode, use the **disable** command in privileged EXEC mode.

disable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **enable** command to enter privileged mode. The **disable** command allows you to exit privileged mode and returns you to an unprivileged mode.

Note If you are logged into the ASA with a username, then entering **disable** will change your user identity to the default enable_1 username.

Examples

The following example shows how to enter privileged mode:

```
ciscoasa
>
enable
ciscoasa#
```

The following example shows how to exit privileged mode:

```
ciscoasa#

disable
ciscoasa
>
```

Related Commands

Command	Description
enable	Enables privileged EXEC mode.

disable service-settings (Deprecated)

To disable the service settings on IP phones when using the Phone Proxy feature, use the **disable service-settings** command in phone-proxy configuration mode. To preserve the settings on the IP phones, use the **no** form of this command.

disable service-settings
no disable service-settings

Syntax Description

There are no arguments or keywords for this command.

Command Default

The service settings are disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

By default, the following settings are disabled on the IP phones:

- PC Port
- Gratuitous ARP
- Voice VLAN access
- Web Access
- Span to PC Port

To preserve the settings configured on the CUCM for each IP phone configured, configure the **no disable service-settings** command.

Examples

The following example shows how to preserve the settings of the IP phones that use the Phone Proxy feature on the ASA:

```
ciscoasa
(config-phone-proxy)# no disable service-settings
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.
show phone-proxy	Displays Phone Proxy specific information.

display

To display attribute value pairs that the ASA writes to the DAP attribute database, enter the **display** command in dap test attributes mode.

display

Command Default

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dap test attributes	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Normally the ASA retrieves user authorization attributes from the AAA server and retrieves endpoint attributes from Cisco Secure Desktop, Host Scan, CNA or NAC. For the test command, you specify the user authorization and endpoint attributes in this attributes mode. The ASA writes them to an attribute database that the DAP subsystem references when evaluating the AAA selection attributes and endpoint select attributes for a DAP record. The **display** command lets you display these attributes to the console.

Related Commands

Command	Description
attributes	Enters attributes configuration mode, in which you can set attribute value pairs.
dynamic-access-policy-record	Creates a DAP record.
test dynamic-access-policy attributes	Enters attributes submode.
test dynamic-access-policy execute	Executes the logic that generates DAP and displays the resulting access policies to the console.

distance

To define the administrative distance assigned to routes discovered by the IS-IS protocol, use the **distance** command in router isis configuration mode. To remove the distance command from the configuration file and restore the system to its default condition in which the software removes a distance definition, use the **no** form of this command.

distance*weight***ip**
no distance *weight* **ip**

Syntax Description

weight	The administrative distance to be assigned to IS-IS routes. The range is 1 to 255.
ip	The distance applied for IP-derived routes.

Command Default

The default is 115.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

An administrative distance is a number from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored. Weight values are subjective; no quantitative method exists for choosing weight values.

Use the **distance** command to configure the administrative distances applied to IS-IS routes when they are inserted into the Routing Information Base (RIB), and influence the likelihood of these routes being preferred over routes to the same destination addresses discovered by other protocols.

Examples

In the following example, a distance of 20 is assigned to all ISIS routes:

```
ciscoasa(config)#
router isis
ciscoasa(config-router)#
distance 20 ip
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

distance bgp

To configure the administrative distance for BGP routes, use the distance bgp command in address family configuration mode. To return the administrative distance to the default value, use the no form of this command.

distancebgp*external-distanceinternal-distancelocal-distance*
no distance bgp

Syntax Description

external-distance	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.
internal-distance	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.
local-distance	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.

Command Default

The following values are used if this command is not configured or if the no form is entered:

external-distance: 20 internal-distance: 200 local-distance: 200

Note Routes with a distance of 255 are not installed in the routing table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The distance bgp command is used to configure a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255.

In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.

Caution Changing the administrative distance of internal BGP routes is considered dangerous and is not recommended. Improper configuration can introduce routing table inconsistencies and break routing.

The distance bgp command replaces the distance mbgp command.

Examples

In the following example, the external distance is set to 10, the internal distance is set to 50, and the local distance is set to 100:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47
ciscoasa(config-router-af)# distance bgp 10 50 100
ciscoasa(config-router-af)# end
```

distance eigrp

To configure the administrative distances of internal and external EIGRP routes, use the **distance eigrp** command in router configuration mode. To restore the default values, use the **no** form of this command.

distanceeigrp*internal-distanceexternal-distance*
no distance eigrp

Syntax Description

external-distance	Administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. Valid values are from 1 to 255.
internal-distance	Administrative distance for EIGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system. Valid values are from 1 to 255.

Command Default

The default values are as follows:

- *external-distance* is 170
- *internal-distance* is 90

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Because every routing protocol has metrics based on algorithms that are different from the other routing protocols, it is not always possible to determine the “best path” for two routes to the same destination that were generated by different routing protocols. Administrative distance is a route parameter that the ASA uses to select the best path when there are two or more different routes to the same destination from two different routing protocols.

If you have more than one routing protocol running on the ASA, you can use the **distance eigrp** command to adjust the default administrative distances of routes discovered by the EIGRP routing protocol in relation to the other routing protocols. <xref> lists the default administrative distances for the routing protocols supported by the ASA.

Table 1: Default Administrative Distances

Route Source	Default Administrative Distance
Connected interface	0
Static route	1
EIGRP summary route	5
Internal EIGRP	90
OSPF	110
RIP	120
EIGRP external route	170
Unknown	255

The **no** form of the command does not take any keywords or arguments. Using the **no** form of the command restores the default administrative distance for both internal and external EIGRP routes.

Examples

The following example uses the **distance eigrp** command to set the administrative distance of all EIGRP internal routes to 80 and all EIGRP external routes to 115. Setting the EIGRP external route administrative distance to 115 would give routes discovered by EIGRP to a specific destination preference over the same routes discovered by RIP but not by OSPF.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.7.0
ciscoasa(config-router)# network 172.16.0.0

ciscoasa(config-router)# distance eigrp 90 115
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

distance ospf (ipv6 router ospf)

To define OSPFv3 route administrative distances based on route type, use the **distance** command in ipv6 router ospf configuration mode. To restore the default values, use the **no** form of this command.

distance [**ospf** { **external** | **intra-area** / **inter-area** }] *distance*
no distance [**ospf** { **external** | **intra-area** / **inter-area** }] *distance*

Syntax Description

distance	Specifies the administrative distance. Valid values range from 10 to 254.
external	(Optional) Specifies external type 5 and type 7 routes for OSPFv3 routes.
inter-area	(Optional) Specifies the inter-area routes for OSPFv3 routes.
intra-area	(Optional) Specifies the intra-area routes for OSPFv3 routes.
ospf	(Optional) Specifies the administrative distance for OSPFv3 routes.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to set the administrative distance for OSPFv3 routes.

Examples

The following example sets the administrative distance for external type 5 and type 7 routes for OSPFv3 to 200:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# distance ospf external 200
```

Related Commands

Command	Description
default-information originate	Generates a default external route into an OSPFv3 routing domain.

Command	Description
redistribute	Redistributes IPv6 routes from one routing domain into another routing domain.

distance ospf (router ospf)

To define OSPFv2 route administrative distances based on route type, use the **distance ospf** command in router ospf configuration mode. To restore the default values, use the **no** form of this command.

distance ospf [**intra-area** *d1*] [**inter-area** *d2*] [**external** *d3*]
no distance ospf

Syntax Description

d1, *d2*, and *d3*	Specifies the distance for each route type. Valid values range from 1 to 255.
external	(Optional) Sets the distance for routes from other routing domains that are learned by redistribution.
inter-area	(Optional) Sets the distance for all routes from one area to another area.
intra-area	(Optional) Sets the distance for all routes within an area.

Command Default

The default values for *d1*, *d2*, and *d3* are 110.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router ospf configuratio	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must specify at least one keyword and argument. You can enter the commands for each type of administrative distance separately, however they appear as a single command in the configuration. If you reenter an administrative distance, the administrative distance for only that route type changes; the administrative distances for any other route types remain unaffected.

The **no** form of the command does not take any keywords or arguments. Using the **no** form of the command restores the default administrative distance for all of the route types. If you want to restore the default administrative distance for a single route type when you have multiple route types configured, you can do one of the following:

- Manually set that route type to the default value.
- Use the **no** form of the command to remove the entire configuration and then reenter the configurations for the route types that you want to keep.

Examples

The following example sets the administrative distance of external routes to 150:

```
ciscoasa(config-router)# distance ospf external 105
ciscoasa(config-router)#
```

The following example shows how entering separate commands for each route type appears as a single command in the router configuration:

```
ciscoasa(config-rtr)# distance ospf intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf intra-area 105
ciscoasa(config-rtr)# distance ospf external 105
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
ciscoasa(config)#
```

The following example shows how to set each administrative distance to 105, and then change only the external administrative distance to 150. The **show running-config router ospf** command shows how only the external route type value changed, while the other route types retained the value previously set.

```
ciscoasa(config-rtr)# distance ospf external 105 intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf external 150
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
ciscoasa(config)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode for OSPFv2.
show running-config router	Displays the OSPFv2 commands in the global router configuration.

distribute-list

To filter networks received or transmitted in Open Shortest Path First (OSPF) updates, use the distribute-list command in the router ospf configuration mode. To change or cancel the filter, use the no form of this command.

distribute-list *access-list name* [**in** | **out**] [**interface** *if_name*]
no distribute-list *access-list name* [**in** | **out**]

Syntax Description

access-list name	Standard IP access list name. The list defines which networks are to be received and which are to be suppressed in routing updates.
in	Applies the access list or route-policy to incoming routing updates.
out	Applies the access list or route-policy to outgoing routing updates.The out keyword is available only in router configuration mode.
interface *if_name*	(Optional) The interface on which to apply the routing updates. Specifying an interface causes the access list to be applied only to routing updates received on that interface.

Command Default

Networks are not filtered.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router ospf Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

If no interface is specified, the access list will be applied to all incoming updates.

Examples

The following example filters OSPF routing updates received on the outside interface. It accepts routes in the 10.0.0.0 network and discards all others.

```
ciscoasa(config)# access-list ospf_filter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ospf_filter deny any
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ospf_filter in interface outside
```

Related Commands

Command	Description
distribute-list in	Filters incoming routing updates.
router ospf	Enters router configuration mode for the OSPF routing process.
show running-config router	Displays the commands in the global router configuration.

distribute-list in (address-family)

To filter routes or networks received in incoming Border Gateway Protocol (BGP) updates; use the distribute-list in command in address-family configuration mode. You can access the address-family configuration mode by first entering the **router bgp** command. To delete the distribute list and remove it from the running configuration file, use the no form of this command.

distribute-list { *acl-name* | **prefix** *list-name* } **in**
no distribute-list { *acl-name* | **prefix** *list-name* } **in**

Syntax Description

acl-name	Standard IP access list name. The access list defines which networks are to be received and which are to be suppressed in routing updates.
prefix list-name	Name of a prefix list. The prefix list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching prefixes.

Command Default

If this command is configured without a predefined access list or prefix list, the distribute list will default to permitting all traffic.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The distribute-list in command is used to filter incoming BGP updates. An access list or prefix list must be defined prior to configuration of this command. Standard and expanded access lists are supported. IP prefix lists are used to filter based on the bit length of the prefix. An entire network, subnet, supernet, or single host route can be specified. Prefix list and access list configuration is mutually exclusive when configuring a distribute list. The session must be reset with the clear bgp command before the distribute list will take effect.

Examples

In the following example, a prefix list and distribute list are defined to configure the BGP routing process to accept traffic from only network 10.1.1.0/24, network 192.168.1.0, and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
ciscoasa(config)# ip prefix-list RED permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list RED permit 10.108.0.0/16
ciscoasa(config)# ip prefix-list RED permit 192.168.1.0/24
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list prefix RED in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

In the following example, an access list and distribute list are defined to configure the BGP routing process to accept traffic from only network 192.168.1.0 and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.1.0 255.255.255.0

ciscoasa(config)# access-list distribute-list-acl permit 10.108.0.0 255.255.0.0

ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list distribute-list-acl in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

Related Commands

Command	Description
clear bgp	Resets BGP connections using hard or soft reconfigurations.
ip prefix-list	Creates a prefix list or adds a prefix list entry.

distribute-list in (router)

To filter incoming routing updates, use the **distribute-list in** command in router configuration mode. To remove the filtering, use the **no** form of this command.

distribute-list *acl* **in** [**interface** *if_name*]
no distribute-list *acl* **in** [**interface** *if_name*]

Syntax Description

acl	Name of a standard access list.
interface *if_name*	(Optional) The interface on which to apply the incoming routing updates. Specifying an interface causes the access list to be applied only to routing updates received on that interface.

Command Default

Networks are not filtered in incoming updates.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

If no interface is specified, the access list will be applied to all incoming updates.

Examples

The following example filters RIP routing updates received on the outside interface. It accepts routes in the 10.0.0.0 network and discards all others.

```
ciscoasa(config)# access-list ripfilter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ripfilter deny any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter in interface outside
```

The following example filters EIGRP routing updates received on the outside interface. It accepts routes in the 10.0.0.0 network and discards all others.

```
ciscoasa(config)# access-list eigrp_filter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list eigrp_filter deny any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter in interface outside
```

Related Commands

Command	Description
distribute-list out	Filters outgoing routing updates.
router eigrp	Enters router configuration mode for the EIGRP routing process.
router rip	Enters router configuration mode for the RIP routing process.
show running-config router	Displays the commands in the global router configuration.

distribute-list out (address-family)

To suppress networks from being advertised in outbound Border Gateway Protocol (BGP) updates, use the distribute-list out command in address-family configuration mode. You can access the address-family configuration mode by first entering the **router bgp** command. To delete the distribute list and remove it from the running configuration file, use the no form of this command.

distribute-list { *acl-name* | **prefix** *list-name* } **out** [*protocol process-number* | **connected** | **static**]
no distribute-list { *acl-name* | **prefix** *list-name* } **out** [*protocol process-number* | **connected** | **static**]

Syntax Description

acl-name	Standard IP access list name. The access list defines which networks are to be received and which are to be suppressed in routing updates.
prefix list-name	Name of a prefix list. The prefix list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching prefixes.
protocol process-number	Specifies the routing protocol to apply the distribution list. BGP, EIGRP, OSPF, and RIP are supported. The process number is entered for all routing protocols, except RIP. The process number is a value from 1 to 65.
connected	Specifies peers and networks learned through connected routes.
static	Specifies peers and networks learned through static routes.

Command Default

If this command is configured without a predefined access list or prefix list, the distribute list will default to permitting all traffic.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The distribute-list out command is used to filter outbound BGP updates. An access list or prefix list must be defined prior to configuration of this command. Only standard access lists are supported.

IP prefix lists are used to filter based on the bit length of the prefix. An entire network, subnet, supernet, or single host route can be specified. Prefix list and access list configuration is mutually exclusive when configuring a distribute list. The session must be reset with the clear bgp command before the distribute list will take effect.

Entering a protocol and/or process-number arguments causes the distribute list to be applied to only routes derived from the specified routing process. Addresses not specified in the distribute-list command will not be advertised in outgoing routing updates after a distribute list is configured.

To suppress networks or routes from being received in inbound updates, use the distribute-list in command.

Examples

In the following example, a prefix list and distribute list are defined to configure the BGP routing process to advertise only network 192.168.0.0. An outbound route refresh is initiated to activate the distribute-list.

```
ciscoasa(config)# ip prefix-list BLUE permit 192.168.0.0/16
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list prefix BLUE out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

In the following example, an access list and a distribute list are defined to configure the BGP routing process to advertise only network 192.168.0.0. An outbound route refresh is initiated to activate the distribute-list.

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.0.0 255.255.0.0
ciscoasa(config)# access-list distribute-list-acl deny 0.0.0.0 0.0.0.0
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list distribute-list-acl out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

Related Commands

Command	Description
clear bgp	Resets BGP connections using hard or soft reconfigurations.
ip prefix-list	Creates a prefix list or adds a prefix list entry.

distribute-list out (router)

To filter outgoing routing updates, use the **distribute-list out** command in router configuration mode. To remove the filtering, use the **no** form of this command.

distribute-list *acl* **out** [**interface** *if_name*] [**eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]
no distribute-list *acl* **out** [**interface** *if_name*] [**eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

Syntax Description

acl	Name of a standard access list.
connected	(Optional) Filters only connected routes.
eigrp *as_number*	(Optional) Filters only EIGRP routes from the specified autonomous system number. The *as_number* argument is the autonomous system number of the EIGRP routing process on the ASA.
interface *if_name*	(Optional) The interface on which to apply the outgoing routing updates. Specifying an interface causes the access list to be applied only to routing updates received on that interface.
ospf *pid*	(Optional) Filters only OSPF routes discovered by the specified OSPF process.
rip	(Optional) Filters only RIP routes.
static	(Optional) Filters only static routes.

Command Default

Networks are not filtered in sent updates.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The **eigrp** keyword was added.

Usage Guidelines

If no interface is specified, the access list will be applied to all outgoing updates.

Examples

The following example prevents the 10.0.0.0 network from being advertised in RIP updates sent out of any interface:

```
ciscoasa(config)# access-list ripfilter deny 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ripfilter permit any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter out
```

The following example prevents the EIGRP routing process from advertising the 10.0.0.0 network on the outside interface:

```
ciscoasa(config)# access-list eigrp_filter deny 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list eigrp_filter permit any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter out interface outside
```

Related Commands

Command	Description
distribute-list in	Filters incoming routing updates.
router eigrp	Enters router configuration mode for the EIGRP routing process.
router rip	Enters router configuration mode for the RIP routing process.
show running-config router	Displays the commands in the global router configuration.