

is – iz

- isakmp am-disable (Deprecated), on page 2
- isakmp disconnect-notify (Deprecated), on page 3
- isakmp enable (Deprecated), on page 4
- isakmp identity (Deprecated), on page 5
- isakmp ipsec-over-tcp (Deprecated), on page 7
- isakmp keepalive, on page 8
- isakmp nat-traversal (Deprecated), on page 10
- isakmp policy authentication, on page 12
- isakmp policy encryption (Deprecated), on page 14
- isakmp policy group (Deprecated), on page 16
- isakmp policy hash (Deprecated), on page 18
- isakmp policy lifetime (Deprecated), on page 20
- isakmp reload-wait (Deprecated), on page 22
- isis priority, on page 23
- isis protocol shutdown, on page 27
- isis retransmit-interval, on page 31
- isis retransmit-throttle-interval, on page 35
- isis tag, on page 39
- is-type, on page 43
- issuer (Deprecated), on page 47
- issuer-name, on page 49

isakmp am-disable (Deprecated)

To disable inbound aggressive mode connections, use the **isakmp am-disable** command in global configuration mode. To enable inbound aggressive mode connections, use the **no** form of this command.

isakmp am-disable
no isakmp am-disable

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is enabled.

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	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp am-disable** command replaced it.

Examples

The following example, entered in global configuration mode, disables inbound aggressive mode connections:

```
ciscoasa(config)# isakmp am-disable
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp disconnect-notify (Deprecated)

To enable disconnect notification to peers, use the **isakmp disconnect-notify** command in global configuration mode. To disable disconnect notification, use the **no** form of this command.

isakmp disconnect-notify
no isakmp disconnect-notify

Syntax Description

This command has no arguments or keywords.

Command Default

The default value 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	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp disconnect-notify** command replaced it.

Examples

The following example, entered in global configuration mode, enables disconnect notification to peers:

```
ciscoasa(config)# isakmp disconnect-notify
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp enable (Deprecated)

To enable ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA, use the **isakmp enable** command in global configuration mode. To disable ISAKMP on the interface, use the **no** form of this command.

isakmp enable *interface-name*
no isakmp enable *interface-name*

Syntax Description

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP negotiation.

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	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp enable** command replaced it.

Examples

The following example, entered in global configuration mode, shows how to disable ISAKMP on the inside interface:

```
ciscoasa(config)# no isakmp enable
 inside
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp identity (Deprecated)

To set the Phase 2 ID to be sent to the peer, use the **isakmp identity** command in global configuration mode. To return to the default setting, use the **no** form of this command.

isakmp identity { **address** | **hostname** | **key-id** *key-id-string* | **auto** }
no isakmp identity { **address** | **hostname** | **key-id** *key-id-string* | **auto** }

Syntax Description

address	Uses the IP address of the host exchanging ISAKMP identity information.
auto	Determines ISKMP negotiation by connection type; IP address for the preshared key or certificate DN for certificate authentication.
hostname	Uses the fully qualified domain name of the host exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
key-id *key_id_string*	Specifies the string used by the remote peer to look up the preshared key.

Command Default

The default ISAKMP identity is the **isakmp identity hostname** command.

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	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp identity** command replaced it.

Examples

The following example, entered in global configuration mode, enables ISAKMP negotiation on the interface for communicating with the IPsec peer, depending on connection type:

```
ciscoasa(config)# isakmp identity auto
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.

Command	Description
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp ipsec-over-tcp (Deprecated)

To enable IPsec over TCP, use the **isakmp ipsec-over-tcp** command in global configuration mode. To disable IPsec over TCP, use the **no** form of this command.

isakmp ipsec-over-tcp [**port** *port1...port10*]
no isakmp ipsec-over-tcp [**port** *port1...port10*]

Syntax Description

port *port1...port10*	(Optional) Specifies the ports on which the device accepts IPsec over TCP connections. You can list up to 10 ports. Port numbers can be in the range of 1-65535. The default port number is 10000.

Command Default

The default value 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	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp ipsec-over-tcp** command replaces it.

Examples

This example, entered in global configuration mode, enables IPsec over TCP on port 45:

```
ciscoasa(config)# isakmp ipsec-over-tcp port 45
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp keepalive

To configure IKE keepalives, use the **isakmp keepalive** command in tunnel-group ipsec-attributes configuration mode. To return the keepalive parameters to enabled with default threshold and retry values, use the **no** form of this command.

isakmp keepalive [**threshold** *seconds* | *infinite*] [**retry** *seconds*] [**disable**]
no isakmp keepalive [**threshold** *seconds* | *infinite*] [**retry** *seconds*] [**disable**]

Syntax Description

disable	Disables IKE keepalive processing, which is enabled by default.
infinite	The ASA never initiates keepalive monitoring.
retry *seconds*	Specifies the interval in seconds between retries after a keepalive response has not been received. The range is 2-10 seconds. The default is 2 seconds.
threshold *seconds*	Specifies the number of seconds that the peer can idle before beginning keepalive monitoring. The range is 10-3600 seconds. The default is 10 seconds for a LAN-to-LAN group, and 300 second for a remote access group.

Command Default

The default for a remote access group is a threshold of 300 seconds and a retry of 2 seconds.

For a LAN-to-LAN group, the default is a threshold of 10 seconds and a retry of 2 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
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

In every tunnel group, IKE keepalives are enabled by default with default threshold and retry values. You can apply this attribute only to IPsec remote access and IPsec LAN-to-LAN tunnel group types.

Examples

The following example entered in tunnel-group ipsec-attributes configuration mode, configures IKE DPD, establishes a threshold of 15, and specifies a retry interval of 10 for the IPsec LAN-to-LAN tunnel group with the IP address 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
```

```
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
ciscoasa(config-tunnel-ipsec)#
```

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 ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

isakmp nat-traversal (Deprecated)

To enable NAT traversal globally, check that ISAKMP is enabled (you can enable it with the **isakmp enable** command) in global configuration mode and then use the **isakmp nat-traversal** command. If you have enabled NAT traversal, you can disable it with the **no** form of this command.

isakmp nat-traversal *natkeepalive*
no isakmp nat-traversal *natkeepalive*

Syntax Description

natkeepalive	Sets the NAT keepalive interval, from 10 to 3600 seconds. The default is 20 seconds.

Command Default

By default, NAT traversal (**isakmp nat-traversal** command) 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	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp nat-traversal** command replaced it.

Usage Guidelines

Network Address Translation (NAT), including Port Address Translation (PAT), is used in many networks where IPsec is also used, but there are a number of incompatibilities that prevent IPsec packets from successfully traversing NAT devices. NAT traversal enables ESP packets to pass through one or more NAT devices.

The ASA supports NAT traversal as described by Version 2 and Version 3 of the IETF "UDP Encapsulation of IPsec Packets" draft, available at http://www.ietf.org/html.charters/ipsec-charter.html , and NAT traversal is supported for both dynamic and static crypto maps.

This command enables NAT-T globally on the ASA. To disable in a crypto-map entry, use the **crypto map set nat-t-disable** command.

Examples

The following example, entered in global configuration mode, enables ISAKMP and then enables NAT traversal with an interval of 30 seconds:

```
ciscoasa(config)# isakmp enable
ciscoasa(config)# isakmp nat-traversal 30
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy authentication

To specify an authentication method within an IKE policy, use the **isakmp policy authentication** command in global configuration mode. To remove the ISAKMP authentication method, use the **clear configure** command.

isakmp policy *priority* **authentication** { **crack** | **pre-share** | **rsa-sig** }

Syntax Description

crack	Specifies IKE Challenge/Response for Authenticated Cryptographic Keys (CRACK) as the authentication method.
pre-share	Specifies preshared keys as the authentication method.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
rsa-sig	Specifies RSA signatures as the authentication method. RSA signatures provide non-repudiation for the IKE negotiation. This means you can prove to a third party whether or not you had an IKE negotiation with the peer.

Command Default

The default ISAKMP policy authentication is the **pre-share** option.

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	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

IKE policies define a set of parameters for IKE negotiation. If you specify RSA signatures, you must configure the ASA and its peer to obtain certificates from a certification authority (CA). If you specify preshared keys, you must separately configure these preshared keys within the ASA and its peer.

Examples

The following example, entered in global configuration mode, sets the authentication method of RSA signatures to be used within the IKE policy with the priority number of 40:

```
ciscoasa(config)# isakmp policy 40 authentication rsa-sig
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy encryption (Deprecated)

To specify the encryption algorithm to use within an IKE policy, use the **isakmp policy encryption** command in global configuration mode. To reset the encryption algorithm to the default value, use the **no** form of this command.

isakmp policy *priority* **encryption** { **aes** | **aes-192** | **aes-256** | **des** | **3des** }
no isakmp policy *priority* **encryption** { **aes** | **aes-192** | **aes-256** | **des** | **3des** }

Syntax Description

3des	Specifies that the triple DES encryption algorithm be used in the IKE policy.
aes	Specifies that the encryption algorithm to use in the IKE policy is AES with a 128-bit key.
aes-192	Specifies that the encryption algorithm to use in the IKE policy is AES with a 192-bit key.
aes-256	Specifies that the encryption algorithm to use in the IKE policy is AES with a 256-bit key.
des	Specifies that the encryption algorithm to use in the IKE policy is 56-bit DES-CBC.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Command Default

The default ISAKMP policy encryption is **3des**.

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	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp policy encryption** command replaced it.

Examples

The following example, entered in global configuration mode, sets 128-bit key AES encryption as the algorithm to be used within the IKE policy with the priority number of 25:

```
ciscoasa(config)# isakmp policy 25 encryption aes
```

The following example, entered in global configuration mode, sets the 3DES algorithm to be used within the IKE policy with the priority number of 40:

```
ciscoasa(config)# isakmp policy 40 encryption 3des
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy group (Deprecated)

To specify the Diffie-Hellman group for an IKE policy, use the **isakmp policy group** command in global configuration mode.To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

isakmp policy *priority* **group** { **1** | **2** | **5** }
no isakmp policy *priority* **group**

Syntax Description

group 1	Specifies that the 768-bit Diffie-Hellman group be used in the IKE policy. This is the default value.
group 2	Specifies that the 1024-bit Diffie-Hellman group 2 be used in the IKE policy.
group 5	Specifies that the 1536-bit Diffie-Hellman group 5 be used in the IKE policy.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Command Default

The default is group 2.

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	—	—

Command History

Release	Modification
7.0(1)	This command was added. Group 7 was added.
7.2(1)	This command was deprecated. The **crypto isakmp policy group** command replaced it.

Usage Guidelines

IKE policies define a set of parameters to use during IKE negotiation.

There are three group options: 768-bit (DH Group 1), 1024-bit (DH Group 2), and 1536-bit (DH Group 5). The 1024-bit and 1536-bit Diffie-Hellman Groups provide stronger security, but require more CPU time to execute.



Note The Cisco VPN Client Version 3.x or higher requires ISAKMP policy to have DH group 2 configured. (If you have DH group 1 configured, the Cisco VPN Client cannot connect.)AES support is available on ASAs licensed for VPN-3DES only. Due to the large key sizes provided by AES, ISAKMP negotiation should use Diffie-Hellman (DH) group 5 instead of group 1 or group 2. This is done with the **isakmp policy priority group 5** command.

Examples

The following example, entered in global configuration mode, sets group 2, the 1024-bit Diffie Hellman, to use for the IKE policy with the priority number of 40:

```
ciscoasa(config)# isakmp policy 40 group   2
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy hash (Deprecated)

To specify the hash algorithm for an IKE policy, use the **isakmp policy hash** command in global configuration mode.To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

isakmp policy *priority* **hash** { **md5** | **sha** }
no isakmp policy *priority* **hash**

Syntax Description

md5	Specifies that MD5 (HMAC variant) be used as the hash algorithm in the IKE policy.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
sha	Specifies that SHA-1 (HMAC variant) be used as the hash algorithm in the IKE policy.

Command Default

The default hash algorithm is SHA-1.

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	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp policy hash** command replaces it.

Usage Guidelines

IKE policies define a set of parameters to be used during IKE negotiation.

There are two hash algorithm options: SHA-1 and MD5. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.

Examples

The following example, entered in global configuration mode, specifies that the MD5 hash algorithm be used within the IKE policy, with the priority number of 40:

```
ciscoasa(config)# isakmp policy 40 hash    md5
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.

Command	Description
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy lifetime (Deprecated)

To specify the lifetime of an IKE security association before it expires, use the **isakmp policy lifetime** command in global configuration mode. To reset the security association lifetime to the default value of 86,400 seconds (one day), use the **no** form of this command .

isakmp policy *priority* **lifetime** *seconds*
no isakmp policy *priority* **lifetime**

Syntax Description

priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
seconds	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2147483647 seconds. Use 0 seconds for an infinite lifetime.

Command Default

The default value is 86,400 seconds (one day).

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	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp policy lifetime** command replaced it.

Usage Guidelines

When IKE begins negotiations, it seeks to agree upon the security parameters for its own session. Then the security association at each peer refers to the agreed-upon parameters. The peers retain the security association until the lifetime expires. Before a security association expires, subsequent IKE negotiations can use it, which can save time when setting up new IPsec security associations. The peers negotiate new security associations before current security associations expire.

With longer lifetimes, the ASA sets up future IPsec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default, but you can specify an infinite lifetime if the peer does not propose a lifetime.

Note If the IKE security association is set to an infinite lifetime, but the peer proposes a finite lifetime, then the negotiated finite lifetime from the peer is used.

Examples

The following example, entered in global configuration mode, sets the lifetime of the IKE security association to 50,4000 seconds (14 hours) within the IKE policy with the priority number of 40:

```
ciscoasa(config)# isakmp policy 40 lifetime 50400
```

The following example, entered in global configuration mode, sets the IKE security association to an infinite lifetime.

```
ciscoasa(config)# isakmp policy 40 lifetime 0
```

Related Commands

clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp reload-wait (Deprecated)

To enable waiting for all active sessions to voluntarily terminate before rebooting the ASA, use the **isakmp reload-wait** command in global configuration mode. To disable waiting for active sessions to terminate and to proceed with a reboot of the ASA, use the **no** form of this command.

isakmp reload-wait
no isakmp reload-wait

Syntax Description

This command has no arguments or keywords.

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	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp reload-wait** command replaced it.

Examples

The following example, entered in global configuration mode, tells the ASA to wait until all active sessions have terminated before rebooting:

```
ciscoasa(config)# isakmp reload-wait
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isis priority

To configure the priority of designated ASAs on an interface, use the **isis priority** command in interface isis configuration mode. To reset the default priority, use the **no** form of this command.

isis priority *number-value* [**level-1** | **level-2**]
no isis priority [**level-1** | **level-2**]

Syntax Description

number-value	Sets the priority of a router. The range is 0 to 127.
level-1	(Optional) Sets the priority for Level 1 independently.
level-2	(Optional) Sets the priority for Level 2 independently.

Command Default

The default is 64.

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 isis Configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command sets the priority that is used to determine which ASA on a LAN will be the designated router or DIS. The priorities are advertised in the hello packets. The ASA with the highest priority becomes the DIS.

Note In IS-IS there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If an ASA with a higher priority comes on line, it takes over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.

Examples

The following example shows Level 1 routing given priority by setting the priority level to 80. This ASA is now more likely to become the DIS:

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis priority 80 level-1
```

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.

isis protocol shutdown

To disable the IS-IS protocol so that it cannot form adjacencies on a specified interface and place the IP address of the interface into the LSP that is generated by the ASA, use the **isis protocol shutdown** command in interface isis configuration mode. To reenable the IS-IS protocol, use the **no** form of this command.

isis protocol shutdown
no isis protocol shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

This command has 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 isis configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command lets you disable the IS-IS protocol for a specified interface without removing the configuration parameters. The IS-IS protocol does not form any adjacencies for the interface for which this command has been configured, and the IP address of the interface is put into the LSP that is generated by the ASA. Use the **protocol shutdown** command if you do not want IS-IS to form any adjacency on any interface and to clear the IS-IS LSP database.

Examples

The following example disables the IS-IS protocol on GigabitEthernet 0/0:

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis protocol shutdown
```

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.

Command	Description
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.
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.

Command	Description
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.
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.

Command	Description
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.

isis retransmit-interval

To configure the amount of time between retransmission of each IS-IS LSP, use the **isis retransmit-interval** command in interface isis configuration mode. To restore the default value, use the **no** form of this command.

isis retransmit-interval *seconds*
no isis retransmit-interval *seconds*

Syntax Description

seconds	(Optional) The time between retransmission of each LSP. The number should be greater than the expected round-trip delay between any two routers on the attached network. The range is 0 to 65535.

Command Default

The default is 5.

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 isis configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

Make sure the *seconds* argument is conservative, otherwise needless retransmission results. This command has no effect on LAN (multi-point) interfaces.

Examples

The following example configures GigabitEthernet 0/0 for retransmission of each IS-IS LSP every 60 seconds for a large serial line:

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis retransmit-interval 60
```

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.

Command	Description
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.
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.

Command	Description
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.
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.

Command	Description
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.

isis retransmit-throttle-interval

To configure the amount of time between retransmissions of each IS-IS LSP on an interface, use the **isis retransmit-throttle-interval** command in interface isis configuration mode. To restore the default value, use the **no** form of this command.

isis retransmit-throttle-interval *milliseconds*
no isis retransmit-throttle-interval

Syntax Description

milliseconds	(Optional) The minimum delay between LSP retransmission on the interface. The range is 0 to 65535.

Command Default

The delay is determined by the **isis lsp-interval** command.

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 isis configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command can be useful in very large networks with many LSPs and many interfaces as a way of controlling LSP retransmission traffic. This command controls the rate at which LSPs can be resent on the interface.

This command is distinct from the rate at which LSPs are sent on the interface (controlled by the **isis lsp-interval** command) and the period between retransmissions of a single LSP (controlled by the **isis retransmit-interval** command). You can use these commands in combination to control the offered load of routing traffic from one ASA to its neighbors.

Examples

The following example configures GigabitEthernet 0/0 to limit the rate of LSP retransmissions to one every 300 milliseconds:

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis retransmit-throttle-interval 300
```

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.

isis tag

To set a tag on the IP address configured for an interface when this IP prefix is put into an IS-IS LSP, use the **isis tag** command in interface isis configuration mode. To stop tagging the IP address, use the **no** form of this command.

isis tag *tag-number*
no isis tag *tag-number*

Syntax Description

tag-number	The number that serves as a tag on an IS-IS route. The range is 1 to 4294967295.

Command Default

No route tag is associated for IP addresses configured for the interface.

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 isis configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

No action occurs on a tagged route until the tag is used, for example, to redistribute routes or summarize routes. Configuring this command triggers the ASA to generate new LSPs because the tag is a new piece of information in the packet.

Examples

The following example configures GigabitEthernet 0/0 to have a tag of 100:

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis tag 100
```

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.

Command	Description
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.
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.

Command	Description
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.
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.

Command	Description
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.

is-type

To configure the routing level for an instance of the IS-IS routing process, use the **is-type** command in router isis configuration mode. To reset the default value, use the **no** form of this command.

isis type [**level-1** | **level 1-2** | **level-2-only**
no isis type [**level-1** | **level 1-2** | **level-2-only**

Syntax Description

level-1	(Optional) Indicates intra-area routing. This ASA only learns about destinations inside its area. Level 2 (inter-area) routing is performed by the closest Level 1-2 ASA.
level-1-2	(Optional) The ASA performs both Level 1 and Level 2 routing. This ASA runs two instances of the routing process. It has one link-state packet database (LSDB) for destinations inside the area (Level 1 routing) and runs a shortest path first (SPF) calculation to discover the area topology. It also has another LSDB with link-state packets (LSPs) of all other backbone (Level 2) routers, and runs another SPF calculation to discover the topology of the backbone, and the existence of all other areas.
level-2-only	(Optional) Indicates inter-area routing. This ASA is part of the backbone and does not communicate with Level 1-only ASAs in its own area.

Command Default

In conventional IS-IS configurations, the ASA acts as both a Level 1 (intra-area) and a Level 2 (inter-area) router.

In multi-area IS-IS configurations, the first instance of the IS-IS routing process configured is by default a Level 1-2 (intra-area and inter-area) router. The remaining instances of the IS-IS process configured by default are Level 1 routers.

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 isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

We highly recommend that you configure the type of IS-IS routing process. If you are configuring multi-area IS-IS, you must configure the type of the router, or allow it to be configured by default. By default, the first instance of the IS-IS routing process that you configure using the **router isis** command is a Level 1-2 router.

If only one area is in the network, there is no need to run both Level 1 and Level 2 routing algorithms. If IS-IS is used for Connectionless Network Service (CLNS) routing (and there is only one area), Level 1 only must

be used everywhere. If IS-IS is used for IP routing only (and there is only one area), you can run Level 2 only everywhere. Areas you add after the Level 1-2 area exists are by default Level 1 areas.

If the router instance has been configured for Level 1-2 (the default for the first instance of the IS-IS routing process), you can remove Level 2 (inter-area) routing for the area using the **is-type** command. You can also use the **is-type** command to configure Level 2 routing for an area.

Examples

The following example specifies an area router:

```
ciscoasa#
router isis
ciscoasa(config-router)#
is-type level-2-only
```

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.

Command	Description
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.
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.

Command	Description
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.
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.

issuer (Deprecated)

Note The last supported release of this command was Version 9.5(1).

To specify the security device that is sending assertions to a SAML-type SSO server, use the **issuer** command in webvpn-sso-saml configuration mode for that specific SAML type. To remove the issuer name, use the **no** form of this command.

issuer*identifier*
no issuer [*identifier*]

Syntax Description

identifier	Specifies a security device name, usually the hostname of the device. An identifier must be less than 65 alphanumeric characters.

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
Webvpn-sso-saml configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.5(2)	This command was deprecated.

Usage Guidelines

SSO support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SAML POST-type SSO server and the SiteMinder-type of SSO server.

This command applies only to SAML-type SSO Servers.

Examples

The following example specifies the issuer name for a security device named asa1.example.com:

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# issuer asa1.example.com
ciscoasa(config-webvpn-sso-saml#
```

Related Commands

Command	Description
assertion-consumer-url	Specifies the URL that the security device uses to contact the SAML-type SSO server assertion consumer service.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
trustpoint	Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion.

issuer-name

To specify the issuer name DN of all issued certificates, use the **issuer-name** command in local certificate authority (CA) server configuration mode. To remove the subject DN from the certificate authority certificate, use the **no** form of this command.

issuer-name*DN-string*
no issuer-name *DN-string*

Syntax Description

DN-string	Specifies the distinguished name of the certificate, which is also the subject name DN of the self-signed CA certificate. Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains a comma. An issuer name must be less than 500 alphanumeric characters.

Command Default

The default issuer name is cn=*hostame.domain-name*, for example cn=asa.example.com.

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
Ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.3(1)	This command was added.
8.0(2)	Support for quotation marks was added to retain commas in *DN-string* values.

Usage Guidelines

This command specifies the issuer name that appears on any certificate created by the local CA server. Use this optional command if you want the issuer name to be different from the default CA name.

Note This issuer name configuration cannot be changed after you have enabled the CA server and generated the certificate by issuing the **no shutdown** command.

Examples

The following example configures certificate authentication:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# issuer-name cn=asa-ca.example.com,ou=Eng,o=Example,c="cisco systems, inc.”
```

```
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to ca server configuration mode commands, which allow you to configure and manage the local CA.
keysize	Specifies the size of the public and private keys generated at certificate enrollment.
lifetime	Specifies the lifetime of the CA certificate and issued certificates.
show crypto ca server	Displays the characteristics of the local CA.
show crypto ca server cert-db	Displays local CA server certificates.