area through auto-update timeout Commands

area

To create an OSPF v2 or OSPFv3 area, use the **area** command in router configuration mode. To remove the area, use the **no** form of this command.

area *area_id*

no area *area_id*

Syntax Description

area_id	The ID of the area being created. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—
IPv6 router configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	We introduced this command.
9.0(1)	Support for OSPFv3 was added.

Usage Guidelines

The area that you create does not have any parameters set. Use the related **area** commands to set the area parameters.

Examples

The following example shows how to create an OSPF area with an area ID of 1:

```
hostname(config-router)# area 1
hostname(config-router)#
```

Related Commands

Command	Description
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.

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

area authentication

To enable authentication for an OSPFv2 area, use the **area authentication** command in router configuration mode. To disable area authentication, use the **no** form of this command.

area *area_id* **authentication** [**message-digest**]

no area *area_id* **authentication** [**message-digest**]

Syntax Description

area_id	The identifier of the area for which authentication is to be enabled. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication for the area specified by the *area_id*.

Defaults

Area authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	We introduced this command.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

If the specified OSPFv2 area does not exist, it is created when this command is entered. Entering the **area authentication** command without the **message-digest** keyword enables simple password authentication. Including the **message-digest** keyword enables MD5 authentication.

Examples

The following example shows how to enable MD5 authentication for area 1:

```
hostname(config-router)# area 1 authentication message-digest
hostname(config-router)#
```

Related Commands

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

area default-cost

To specify a cost for the default summary route sent into a stub or NSSA, use the **area default-cost** command in router configuration mode or IPv6 router configuration mode. To restore the default cost value, use the **no** form of this command.

area *area_id* **default-cost** *cost*

no area *area_id* **default-cost** *cost*

Syntax Description

area_id	The identifier of the stub or NSSA whose default cost is being changed. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
cost	Specifies the cost for the default summary route that is used for a stub or NSSA. Valid values range from 0 to 65535

Defaults

The default value of *cost* is 1.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	•	—
IPv6 router configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	We introduced this command.
9.0(1)	Multiple context mode and OSPFv3 are supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Examples

The following example show how to specify a default cost for summary route sent into a stub or NSSA:

```
hostname(config-router)# area 1 default-cost 5
hostname(config-router)#
```

Related Commands

Command	Description
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area filter-list prefix

To filter prefixes advertised in Type 3 LSAs between OSPFv2 areas of an ABR, use the **area filter-list prefix** command in router configuration mode. To change or cancel the filter, use the **no** form of this command.

area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

no area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

Syntax Description

area_id	Identifies the area for which filtering is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
in	Applies the configured prefix list to prefixes advertised inbound to the specified area.
list_name	Specifies the name of a prefix list.
out	Applies the configured prefix list to prefixes advertised outbound from the specified area.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	We introduced this command.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Only Type 3 LSAs can be filtered. If an ASBR has been configured in the private network, then it sends Type 5 LSAs (describing private networks) that are flooded to the entire AS including the public areas.

Examples

The following example filters prefixes that are sent from all other areas to area 1:

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
hostname(config-router)#
```

Related Commands

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

area nssa

To configure an area as an NSSA, use the **area nssa** command in router configuration mode or IPv6 router configuration mode. To remove the NSSA designation from the area, use the **no** form of this command.

area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

no area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

Syntax Description

area_id	Identifies the area being designated as an NSSA. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
default-information-originate	Used to generate a Type 7 default into the NSSA area. This keyword only takes effect on an NSSA ABR or an NSSA ASBR.
metric *metric_value*	(Optional) Specifies the OSPF default metric value. Valid values range from 0 to 16777214.
metric-type {**1** | **2**}	(Optional) the OSPF metric type for default routes. Valid values are the following: • **1**—type 1 • **2**—type 2. The default value is 2.
no-redistribution	(Optional) Used when the router is an NSSA ABR and you want the **redistribute** command to import routes only into the normal areas, but not into the NSSA area.
no-summary	(Optional) Allows an area to be a not-so-stubby area but not have summary routes injected into it.

Defaults

The defaults are as follows:

- No NSSA area is defined.
- The **metric-type** is 2.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Router configuration	•	—	•	•	—
IPv6 router configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	We introduced this command.
9.0(1)	Multiple content mode and OSPFv3 are supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

If you configure one option for an area, and later specify another option, both options are set. For example, entering the following two command separately results in a single command with both options set in the configuration:

```
hostname(config-rtr)# area 1 nssa no-redistribution
hostname(config-rtr)# area area_id nssa default-information-originate
```

Examples

The following example shows how setting two options separately results in a single command in the configuration:

```
hostname(config-rtr)# area 1 nssa no-redistribution
hostname(config-rtr)# area 1 nssa default-information-originate
hostname(config-rtr)# exit
hostname(config-rtr)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

Related Commands

Command	Description
area stub	Defines the area as a stub area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area range (OSPFv2)

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no** form of this command.

area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

no area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

Syntax Description

address	IP address of the subnet range.
advertise	(Optional) Sets the address range status to advertise and generates Type 3 summary link-state advertisements (LSAs).
area_id	Identifies the area for which the range is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
mask	IP address subnet mask.
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Defaults

The address range status is set to advertise.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	We introduced this command.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

The **area range** command is used only with ABRs to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*. You can configure multiple **area range** commands for an area. In this way, OSPF can summarize addresses for many different sets of address ranges.

The **no area** *area_id* **range** *ip_address netmask* **not-advertise** command removes only the **not-advertise** optional keyword.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
hostname(config-router)#
```

Related Commands

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

area range (OSPFv3)

To consolidate and summarize OSPFv3 routes at an area boundary, use the **area range** command in IPv6 router configuration mode. To disable this function, use the **no** form of this command.

area *area_id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

no area *area_id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

Syntax Description

advertise	(Optional) Sets the range status to advertise and generates Type 3 summary link-state advertisements (LSAs).
area_id	Specifies the identifier of the area for which routes are to be summarized. You can specify the identifier as either a decimal number or an IPv6 prefix.
cost *cost*	(Optional) Specifies the metric or cost for this summary route, which is used during OSPF SPF calculations to detemine the shortest paths to the destination. Valid values range from 0 to 16777215.
ipv6-prefix	Specifies the IPv6 prefix.
not-advertise	(Optional) Sets the range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.
prefix-length	Specifies the IPv6 prefix length.

Defaults

The range status is set to advertise by default.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
IPv6 router configuration	•	—	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

The **area range** command is used only with ABRs. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each

IPv6 prefix and prefix length. This behavior is called *route summarization*. You can configure multiple **area range** commands for an area. In this way, OSPFv3 can summarize routes for many different sets of IPv6 prefixes and prefix lengths.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for IPv6 prefix 2000:0:0:4::2 with the prefix-length 2001::/64:

```
hostname(config-router)# area 1 range 2000:0:0:4::2/2001::/64
hostname(config-router)#
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode for OSPFv3.
show running-config ipv6 router	Displays the IPv6 commands in the global router configuration.

area stub

To define an area as a stub area, use the **area stub** command in router configuration mode or IPv6 router configuration mode. To remove the stub area, use the **no** form of this command.

area *area_id* **stub** [**no-summary**]

no area *area_id* **stub** [**no-summary**]

Syntax Description

area_id	Identifies the stub area. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
no-summary	Prevents an ABR from sending summary link advertisements into the stub area.

Defaults

The default behaviors are as follows:

- No stub areas are defined.
- Summary link advertisements are sent into the stub area.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—
IPv6 router configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	We introduced this command.
9.0(1)	Support for OSPFv3 was added.

Usage Guidelines

The command is used only on an ABR attached to a stub or NSSA.

There are two stub area router configuration commands: the **area stub** and **area default-cost** commands. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **area stub** command. Use the **area default-cost** command only on an ABR attached to the stub area. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Examples

The following example configures the specified area as a stub area:

```
hostname(config-rtr)# area 1 stub
hostname(config-rtr)#
```

Related Commands

Command	Description
area default-cost	Specifies a cost for the default summary route sent into a stub or NSSA.
area nssa	Defines the area as a not-so-stubby area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area virtual-link (OSPFv2)

To define an OSPF virtual link, use the **area virtual-link** command in router configuration mode. To reset the options or remove the virtual link, use the **no** form of this command.

area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key[0 | 8]** *key*] | [**message-digest-key** *key_id* **md5 [0 | 8]** *key*]]]]

no area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key [0 | 8]** *key*] | [**message-digest-key** *key_id* **md5 [0 | 8]** *key*]]]]

Syntax Description

area_id	Area ID of the transit area for the virtual link. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
authentication	(Optional) Specifies the authentication type.
authentication-key [0 | 8]*key*	(Optional) Specifies an OSPF authentication password for use by neighboring routing devices.
dead-interval *seconds*	(Optional) Specifies the interval before declaring a neighboring routing device is down if no hello packets are received; valid values are from 1 to 65535 seconds.
hello-interval *seconds*	(Optional) Specifies the interval between hello packets sent on the interface; valid values are from 1 to 65535 seconds.
md5 [0 | 8] *key*	(Optional) Specifies an alphanumeric key up to 16 bytes.
message-digest	(Optional) Specifies that message digest authentication is used.
message-digest-key *key_id*	(Optional) Enables the Message Digest 5 (MD5) authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
0	Specifies an unencrypted password will follow.
8	Specifies an encrypted password will follow.
null	(Optional) Specifies that no authentication is used. Overrides password or message digest authentication if configured for the OSPF area.
retransmit-interval *seconds*	(Optional) Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.
router_id	The router ID associated with the virtual link neighbor. The router ID is internally derived by each router from the interface IP addresses. This value must be entered in the format of an IP address. There is no default.
transmit-delay *seconds*	(Optional) Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds from 0 to 65535. The default is 5 seconds.

Note Single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported.

Defaults

The defaults are as follows:

- *area_id*: No area ID is predefined.
- *router_id*: No router ID is predefined.
- **hello-interval** *seconds*: 10 seconds.
- **retransmit-interval** *seconds*: 5 seconds.
- **transmit-delay** *seconds*: 1 second.
- **dead-interval** *seconds*: 40 seconds.
- **authentication-key [0 | 8]** *key*: No key is predefined.
- **message-digest-key** *key_id* **md5 [0 | 8]** *key*: No key is predefined.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	We introduced this command.

Usage Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes are detected, but more routing traffic ensues.

The setting of the retransmit interval should be conservative, or needless retransmissions occur. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

The specified authentication key is used only when authentication is enabled for the backbone with the **area** *area_id* **authentication** command.

The two authentication schemes, simple text and MD5 authentication, are mutually exclusive. You can specify one or the other or neither. Any keywords and arguments you specify after **authentication-key [0 | 8]** *key* or **message-digest-key** *key_id* **md5[0 | 8]** *key* are ignored. Therefore, specify any optional arguments before such a keyword-argument combination.

If the authentication type is not specified for an interface, the interface uses the authentication type specified for the area. If no authentication type has been specified for the area, the area default is null authentication.

Note Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID for a virtual link to be properly configured. Use the **show ospf** command to see the router ID.

Examples

The following example establishes a virtual link with MD5 authentication:

```
hostname(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5 8
sa5721bk47
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
show running-config router	Displays the commands in the global router configuration.

area virtual-link (OSPFv3)

To define an OSPFv3 virtual link, use the **area virtual-link** command in IPv6 router configuration mode. To reset the options or remove the virtual link, use the **no** form of this command.

area *area_id* **virtual-link** *router_id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [**ttl-security hops** *hop-count*]

no area *area_id* **virtual-link** *router_id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

Syntax Description

area_id	Specifies the area ID of the transit area for the virtual link. You can specify the identifier as either a decimal number or valid IPv6 prefix. Valid decimal values range from 0 to 4294967295.
dead-interval *seconds*	(Optional) Specifies the time in seconds that hello packets are not seen before a neighbor indicates that the router is down. The dead interval in an unsigned integer value. As with the hello interval, this value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 to 8192 seconds.
hello-interval *seconds*	(Optional) Specifies the time in seconds between hello packets that the ASA sends on the interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 to 8192 seconds.
retransmit-interval *seconds*	(Optional) Specifies the time in seconds between LSA retransmissions for adjacent routers that belong to the interface. The retransmission interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. Valid values range from 1 to 8192 seconds.
router_id	Specifies the router ID that is associated with the virtual link neighbor. The router ID appears in the **show ipv6 ospf** or **show ipv6 display** command.
transmit-delay *seconds*	(Optional) Specifies the estimated time in seconds that is required to send a link-state update packet on the interface. The integer value must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. Valid values range from 1 to 8192 seconds.
ttl-security hops *hop-count*	(Optional) Configures the time-to-live (TTL) security on a virtual link. Valid values for the hop count range from 1 to 254.

Note Single-digit passwords and passwords starting with a digit followed by a white space are no longer supported.

Defaults

The defaults are as follows:

- *area_id*: No area ID is predefined.
- *router_id*: No router ID is predefined.

- **hello-interval**: 10 seconds.
- **retransmit-interval**: 5 seconds.
- **transmit-delay**: 1 second.
- **dead-interval**: 40 seconds.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
IPv6 router configuration	•	—	•	—	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

In OSPFv3, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes are detected, but more routing traffic occurs.

The setting of the retransmission interval should be conservative, or unnecessary retransmissions occur. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

Note Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID for a virtual link to be correctly configured. Use the **show ipv6 ospf** command to obtain the router ID.

Examples

The following example establishes a virtual link in OSPFv3:

```
hostname(config-if)# ipv6 router ospf 1
hostname(config-rtr)# log-adjacency-changes
hostname(config-rtr)# area 1 virtual-link 192.168.255.1 hello interval 5
```

Related Commandsi

Command	Description
ipv6 router ospf	Enters router configuration mode for OSPFv3.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
show running-config ipv6 router	Displays the IPv6 commands in the global router configuration.

arp

To add a static ARP entry to the ARP table, use the **arp** command in global configuration mode. To remove the static entry, use the **no** form of this command.

arp *interface_name ip_address mac_address* [**alias**]

no arp *interface_name ip_address mac_address*

Syntax Description

alias	(Optional) Enables proxy ARP for this mapping. If the ASA receives an ARP request for the specified IP address, then it responds with the ASA MAC address. When the ASA receives traffic destined for the host belonging to the IP address, the ASA forwards the traffic to the host MAC address that you specify in this command. This keyword is useful if you have devices that do not perform ARP, for example. In transparent firewall mode, this keyword is ignored; the ASA does not perform proxy ARP.
interface_name	The interface attached to the host network.
ip_address	The host IP address.
mac_address	The host MAC address.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	**Modification**
7.0(1)	We introduced this command.

Usage Guidelines

Although hosts identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver. The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry times out before it can be updated.

A static ARP entry maps a MAC address to an IP address and identifies the interface through which the host is reached. Static ARP entries do not time out, and might help you solve a networking problem. In transparent firewall mode, the static ARP table is used with ARP inspection (see the **arp-inspection** command).

Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the ASA, such as management traffic.

Examples

The following example creates a static ARP entry for 10.1.1.1 with the MAC address 0009.7cbe.2100 on the outside interface:

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

Related Commands

Command	Description
arp timeout	Sets the time before the ASA rebuilds the ARP table.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

arp permit-nonconnected

To enable the ARP cache to also include non-directly-connected subnets, use the **arp permit-nonconnected** command in global configuration mode. To disable non-connected subnets, use the **no** form of this command.

arp permit-nonconnected

no arp permit-nonconnected

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:

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

Command History

Release	Modification
8.4(5), 9.0(1)	We introduced this command.

Usage Guidelines

The ASA ARP cache only contains entries from directly-connected subnets by default. This command lets you enable the ARP cache to also include non-directly-connected subnets. We do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attack against the ASA; a user on any interface could send out many ARP replies and overload the ASA ARP table with false entries.

You may want to use this feature if you use:

- Secondary subnets.
- Proxy ARP on adjacent routes for traffic forwarding.

Examples

The following example enables non-connected subnets:

```
hostname(config)# arp permit non-connected
```

Related Commands

Command	Description
arp	Adds a static ARP entry.

arp-inspection

To enable ARP inspection for transparent firewall mode, use the **arp-inspection** command in global configuration mode. To disable ARP inspection, use the **no** form of this command.

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

no arp-inspection *interface_name* **enable**

Syntax Description

enable	Enables ARP inspection.
flood	(Default) Specifies that packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, then the ASA drops the packet. **Note** The management-specific interface, if present, never floods packets even if this parameter is set to flood.
interface_name	The interface on which you want to enable ARP inspection.
no-flood	(Optional) Specifies that packets that do not exactly match a static ARP entry are dropped.

Defaults

By default, ARP inspection is disabled on all interfaces; all ARP packets are allowed through the ASA. When you enable ARP inspection, the default is to flood non-matching ARP packets.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configure static ARP entries using the **arp** command before you enable ARP inspection.

ARP inspection checks all ARP packets against static ARP entries (see the **arp** command) and blocks mismatched packets. This feature prevents ARP spoofing.

When you enable ARP inspection, the ASA compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.

- If there is a mismatch between the MAC address, the IP address, or the interface, then the ASA drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the ASA to either forward the packet out all interfaces (flood), or to drop the packet.

Note The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a "man-in-the-middle" attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can then intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, provided the correct MAC address and the associated IP address are in the static ARP table.

Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the ASA, such as management traffic.

Examples

The following example enables ARP inspection on the outside interface and sets the ASA to drop any ARP packets that do not match the static ARP entry:

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(config)# arp-inspection outside enable no-flood
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
clear configure arp-inspection	Clears the ARP inspection configuration.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

arp timeout

To set the time before the ASA rebuilds the ARP table, use the **arp timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command.

arp timeout *seconds*

no arp timeout *seconds*

Syntax Description

seconds	The number of seconds between ARP table rebuilds, from 60 to 4294967.

Defaults

The default value is 14,400 seconds (4 hours).

Command Modes

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

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

Command History

Release	Modification
7.0(1)	We introduced this command.

Usage Guidelines

Rebuilding the ARP table automatically updates new host information and removes old host information. You might want to reduce the timeout because the host information changes frequently.

Examples

The following example changes the ARP timeout to 5,000 seconds:

```
hostname(config)# arp timeout 5000
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.
show running-config arp timeout	Shows the current configuration of the ARP timeout.

asdm disconnect

To terminate an active ASDM session, use the **asdm disconnect** command in privileged EXEC mode.

asdm disconnect *session*

Syntax Description

session	The session ID of the active ASDM session to be terminated.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm disconnect** command to the **asdm disconnect** command.

Usage Guidelines

Use the **show asdm sessions** command to display a list of active ASDM sessions and their associated session IDs. Use the **asdm disconnect** command to terminate a specific session.

When you terminate an ASDM session, any remaining active ASDM sessions keep their associated session ID. For example, if there are three active ASDM sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM sessions keep the session IDs 0 and 2. The next new ASDM session in this example would be assigned a session ID of 1, and any new sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm sessions** commands display the active ASDM sessions before and after the **asdm disconnect** command is entered.

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm sessions

1 192.168.1.2
```

Related Commands

Command	Description
show asdm sessions	Displays a list of active ASDM sessions and their associated session ID.

asdm disconnect log_session

To terminate an active ASDM logging session, use the **asdm disconnect log_session** command in privileged EXEC mode.

asdm disconnect log_session *session*

Syntax Description

session	The session ID of the active ASDM logging session to be terminated.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **show asdm log_sessions** command to display a list of active ASDM logging sessions and their associated session IDs. Use the **asdm disconnect log_session** command to terminate a specific logging session.

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from the ASA. Terminating a log session may have an adverse effect on the active ASDM session. To terminate an unwanted ASDM session, use the **asdm disconnect** command.

Note Because each ASDM session has at least one ASDM logging session, the output for the **show asdm sessions** and **show asdm log_sessions** may appear to be the same.

When you terminate an ASDM logging session, any remaining active ASDM logging sessions keep their associated session ID. For example, if there are three active ASDM logging sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM logging sessions keep the session IDs 0 and 2. The next new ASDM logging session in this example would be assigned a session ID of 1, and any new logging sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm log_sessions** commands display the active ASDM sessions before and after the **asdm disconnect log_sessions** command is entered.

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm log_sessions

1 192.168.1.2
```

Related Commands

Command	Description
show asdm log_sessions	Displays a list of active ASDM logging sessions and their associated session ID.

asdm history enable

To enable ASDM history tracking, use the **asdm history enable** command in global configuration mode. To disable ASDM history tracking, use the **no** form of this command.

asdm history enable

no asdm history enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm history enable** command to the **asdm history enable** command.

Usage Guidelines

The information obtained by enabling ASDM history tracking is stored in the ASDM history buffer. You can view this information using the **show asdm history** command. The history information is used by ASDM for device monitoring.

Examples

The following example enables ASDM history tracking:

```
hostname(config)# asdm history enable
hostname(config)#
```

Related Commands

Command	Description
show asdm history	Displays the contents of the ASDM history buffer.

asdm image

To specify the location of the ASDM software image in flash memory, use the **asdm image** command in global configuration mode. To remove the image location, use the **no** form of this command.

asdm image *url*

no asdm image [*url*]

Syntax Description

url	Sets the location of the ASDM image in flash memory. See the following URL syntax: • **disk0:/**[*path/*]*filename* For the ASA 5500 series, this URL indicates the internal flash memory. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:/**[*path/*]*filename* For the ASA 5500 series, this URL indicates the external flash memory card. • **flash:/**[*path/*]*filename* This URL indicates the internal flash memory.

Defaults

If you do not include this command in your startup configuration, the ASA uses the first ASDM image it finds at startup. It searches the root directory of internal Flash memory and then external flash memory. The ASA then inserts the **asdm image** command into the running configuration if it discovered an image.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can store more than one ASDM software image in flash memory. If you enter the **asdm image** command to specify a new ASDM software image while there are active ASDM sessions, the new command does not disrupt the active sessions; active ASDM sessions continue to use the ASDM software image they started with. New ASDM sessions use the new software image. If you enter the **no asdm image** command, the command is removed from the configuration. However, you can still access ASDM from the ASA using the last-configured image location.

If you do not include this command in your startup configuration, the ASA uses the first ASDM image it finds at startup. It searches the root directory of internal flash memory and then external flash memory. The ASA then inserts the **asdm image** command into the running configuration if it discovered an image. Be sure to save the running configuration to the startup configuration using the **write memory** command. If you do not save the **asdm image** command to the startup configuration, every time you reboot, the ASA searches for an ASDM image and inserts the **asdm image** command into your running configuration. If you are using Auto Update, the automatic addition of this command at startup causes the configuration on the ASA not to match the configuration on the Auto Update Server. This mismatch causes the ASA to download the configuration from the Auto Update Server. To avoid unnecessary Auto Update activity, save the **asdm image** command to the startup configuration.

Examples

The following example sets the ASDM image to asdm.bin:

```
hostname(config)# asdm image flash:/asdm.bin
hostname(config)#
```

Related Commands

Command	Description
show asdm image	Displays the current ASDM image file.
boot	Sets the software image and startup configuration files.

asdm location

Caution Do not manually configure this command. ASDM adds **asdm location** commands to the running configuration and uses them for internal communication. This command is included in the documentation for informational purposes only.

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

Syntax Description

if_name	The name of the highest security interface. If you have multiple interfaces at the highest security, then an arbitrary interface name is chosen. This interface name is not used, but is a required parameter.
ip_addr	The IP address used internally by ASDM to define the network topology.
ipv6_addr/prefix	The IPv6 address and prefix used internally by ASDM to define the network topology.
netmask	The subnet mask for *ip_addr*.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm location** command to the **asdm location** command.

Usage Guidelines

Do not manually configure or remove this command.

asp load-balance per-packet

For multicore ASAs, to change the load balancing behavior, use the **asp load-balance per-packet** command in global configuration mode. To restore the default load-balancing mechanism, use the **no** form of this command.

asp load-balance per-packet

no asp load-balance per-packet

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the load-balancing mechanism favors many interfaces. The default behavior is to allow only one core to receive packets from an interface receive ring at a time.

Command Modes

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

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

Command History

Release	Modification
8.1(1)	We introduced this command.

Usage Guidelines

The default behavior is optimized for scenarios where packets are received uniformly on all interface rings. The per-packet behavior is optimized for scenarios where traffic is asymmetrically distributed on interface receive rings. Performance on the ASAs with multiple cores can vary depending on the number of processors, the number of interface receive rings, and the nature of the traffic passing through. Using the **asp load-balance per-packet** command allows multiple cores to work simultaneously on packets received from a single interface receive ring. This command provides for parallel processing if the packets received are spread over many independent connections. Note that this command can cause additional queuing overhead for packets from the same and related connections because these packets are processed by one core.

If the system drops packets, and the **show cpu** command output is far less than 100%, then this command may help your throughput if the packets belong to many unrelated connections. The CPU usage is a good indicator of how many cores are effectively being used.

For example on the ASA 5580-40, which includes 8 cores, if two cores are used, then the **show cpu** command output will be 25%; four cores will be 50%; and six cores will be 75%.

Examples

The following example enables per-packet load balancing:

```
hostname(config)# asp load-balance per-packet
```

Related Commands

Command	Description
show asp load-balance	Displays a histogram of the load balancer queue sizes.

asr-group

To specify an asymmetrical routing interface group ID, use the **asr-group** command in interface configuration mode. To remove the ID, use the **no** form of this command.

asr-group *group_id*

no asr-group *group_id*

Syntax Description

group_id	The asymmetric routing group ID. Valid values are from 1 to 32.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When Active/Active failover is enabled, you may encounter situations where load balancing causes the return traffic for outbound connections to be routed through an active context on the peer unit, in which the context for the outbound connection is in the standby group.

The **asr-group** command causes incoming packets to be reclassified with the interface of the same ASR group if a flow with the incoming interface cannot be found. If reclassification finds a flow with another interface, and the associated context is in standby state, then the packet is forwarded to the active unit for processing.

Stateful Failover must be enabled for this command to take effect.

You can view ASR statistics using the **show interface detail** command. These statistics include the number of ASR packets sent, received, and dropped on an interface.

Note No two interfaces in the same context should be configured in the same ASR group.

Examples

The following example assigns the selected interfaces to the asymmetric routing group 1.

Context ctx1 configuration:

```
hostname/ctx1(config)# interface Ethernet2
```

```
hostname/ctx1(config-if)# nameif outside
hostname/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
hostname/ctx1(config-if)# asr-group 1
```

Context ctx2 configuration:

```
hostname/ctx2(config)# interface Ethernet3
hostname/ctx2(config-if)# nameif outside
hostname/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
hostname/ctx2(config-if)# asr-group 1
```

Related Commands

Command	Description
interface	Enters interface configuration mode.
show interface	Displays interface statistics.

assertion-consumer-url

To identify the URL that the security device accesses to contact the assertion consumer service, use the **assertion-consumer-url** command in the webvpn configuration mode for that specific SAML-type SSO server. To remove the URL from the assertion, use the **no** form of this command.

assertion-consumer-url *url*

no assertion-consumer-url [*url*]

Syntax Description

url	Specifies the URL of the assertion consumer service used by the SAML-type SSO server. The URL must start with either http:// or https:// and must be less than 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Single sign-on (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.

If the URL begins with HTTPS, the requirement is to install the root certificate for the assertion consumer service SSL certificate.

Examples

The following example specifies the assertion consumer URL for a SAML-type SSO server:

```
hostname(config-webvpn)# sso server myhostname type saml-v1.1-post
hostname(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
hostname(config-webvpn-sso-saml#
```

Related Commands

Command	Description
issuer	Specifies the SAML-type SSO server security device name.
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 WebVPN SSO server.
trustpoint	Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion.

attribute

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

attribute *name value*

Syntax Description

name	Specifies a well-known attribute name, or an attribute that incorporates a "label" tag. The label tag corresponds to the endpoint ID that you configure for file, registry, process, antivirus, antispyware, and personal firewall endpoint attributes in the DAP record.
value	The value assigned to the AAA attribute.

Command Default

No default value or behaviors.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
DAP attributes configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use this command multiple times to enter multiple attribute value pairs.

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 selection attributes for a DAP record.

Examples

The following example assumes that ASA selects two DAP records if the authenticated user is a member of the SAP group and has antivirus software installed on the endpoint system. The endpoint ID for the antivirus software endpoint rule is *nav*.

The DAP records have the following policy attributes:

DAP Record 1	DAP Record 2
action = continue	action = continue
port-forward = enable hostlist1	url-list = links2
—	url-entry = enable

```
hostname # test dynamic-access-policy attributes
hostname(config-dap-test-attr)# attribute aaa.ldap.memberof SAP
hostname(config-dap-test-attr)# attribute endpoint.av.nav.exists true
hostname(config-dap-test-attr)# exit

hostname # test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable

hostname #
```

Related Commandsl

Command	Description
display	Displays current attribute lists.
dynamic-access-policy-record	Creates a DAP record.
test dynamic-access-policy attributes	Enters attributes.
test dynamic-access-policy execute	Executes the logic that generates the DAP and displays the resulting access policies to the console.

auth-cookie-name

To specify the name of an authentication cookie, use the **auth-cookie-name** command in aaa-server host configuration mode. This is an SSO with HTTP Forms command.

auth-cookie-name

Syntax Description

name	The name of the authentication cookie. The maximum name size is 128 characters.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The WebVPN server of the ASA uses an HTTP POST request to submit a single sign-on (SSO) authentication request to an SSO server. If authentication succeeds, the authenticating web server passes back an authentication cookie to the client browser. The client browser then authenticates to other web servers in the SSO domain by presenting the authentication cookie. The **auth-cookie-name** command configuresthe name of the authentication cookie to be used for SSO by the ASA.

A typical authentication cookie format is Set-Cookie: *cookie name*=*cookie value* [;*cookie attributes*]. In the following authentication cookie example, SMSESSION is the name that would be configured with the **auth-cookie-name** command:

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLDKTa8
ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw+MGiw0o8
8uHa2t4l+SillqfJvcpuXfiIAO06D/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5d
c/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;Pa
th=/
```

Examples

The following example specifies the authentication cookie name of SMSESSION for the authentication cookie received from a web server named example.com:

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# auth-cookie-name SMSESSION
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies that a username parameter must be submitted as part of the HTTP POST request used for SSO authentication.

authenticated-session-username

To specify which authentication username to associate with the session when double authentication is enabled, use the **authenticated-session-username** command in tunnel-group general-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

authenticated-session-username {**primary** | **secondary**}

no authenticated-session-username

Syntax Description

primary	Uses the username from the primary authentication server.
secondary	Uses the username from the secondary authentication server.

Defaults

The default value is **primary**.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

This command is meaningful only when double authentication is enabled. The **authenticated-session-username** command selects the authentication server from which the ASA extracts the username to associate with the session.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies the use of the username from the secondary authentication server for the connection:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-webvpn)# authenticated-session-username secondary
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the prefill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

authentication-attr-from-server

To specify which authentication server authorization attributes to apply to the connection when double authentication is enabled, use the **authentication-attr-from-server** command in tunnel-group general-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

authentication-attr-from-server {**primary** | **secondary**}

no authentication-attr-from-server

Syntax Description

primary	Uses the primary authentication server.
secondary	Uses the secondary authentication server.

Defaults

The default value is **primary**.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

This command is meaningful only when double authentication is enabled. The **authentication-attr-from-server** command selects the authentication server from which the ASA extracts the authorization attributes to be applied to the connection.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies that the authorization attributes to be applied to the connection must come from the secondary authentication server:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-webvpn)# authentication-attr-from-server secondary
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the prefill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

authentication-certificate

To request a certificate from a WebVPN client establing a connection, use the **authentication-certificate** command in webvpn configuration mode. To cancel the requirement for a client certificate, use the **no** form of this command.

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

Syntax Description

interface-name	The name of the interface used to establish the connection. Available interfaces names are: • **inside** Name of interface GigabitEthernet0/1 • **outside** Name of interface GigabitEthernet0/0

Defaults

If you omit the **authentication-certificate** command, client certificate authentication is disabled. If you do not specify an interface name with the **authentication-certificate** command, the default interface name is **inside**.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

For this command to take effect, WebVPN must already be enabled on the corresponding interface. An interface is configured and named with the **interface**, **IP address**, and **nameif** commands.

This command applies only to WebVPN client connections; however, the ability to specify client certificate authentication for management connections with the **http authentication-certificate** command is available on all platforms, including those that do not support WebVPN.

The ASA validates certificates using the PKI trustpoints. If a certificate does not pass validation, then one of the following actions occurs:

If:	Then:
The local CA embedded in the ASA is not enabled.	The ASA closes the SSL connection.
The local CA is enabled, and AAA authentication is not enabled.	The ASA redirects the client to the certificate enrollment page for the local CA to obtain a certificate.
Both the local CA and AAA authentication are enabled.	The client is redirected to a AAA authentication page. If configured, the client also is presented with a link to the enrollment page for the local CA.

Examples

The following example configures certificate authentication for WebVPN user connections on the outside interface:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-certificate outside
hostname(config-webvpn)#
```

Related Commands

Command	Description
authentication (tunnel-group webvpn configuration mode)	Specifies that the members of a tunnel group must use a digital certificate for authentication.
http authentication-certificate	Specifies authentication by means of certificate for ASDM management connections to the ASA.
interface	Configures the interface used to establish the connection
show running-config ssl	Displays the current set of configured SSL commands.
ssl trust-point	Configures the SSL certificate trustpoint.

authentication-exclude

To enable end users to browse to configured links without logging in to clientless SSL VPN, enter the **authentication-exclude** command in webvpn configuration mode. Use this command multiple times to permit acccess to multiple sites.

authentication-exclude *url-fnmatch*

Syntax Description

url-fnmatch	Identifies the link to exempt from the requirement to log in to a clientless SSL VPN.

Command Default

Disabled.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This feature is useful when you require some internal resources to be available for public use via SSL VPN.

You need to distribute information about the links to end users in an SSL VPN-mangled form, for example, by browsing to these resources using SSL VPN and copying the resulting URLs into the information about links that you distribute.

Examples

The following example shows how to exempt two sites from authentication requirements:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-exclude http://www.example.com/public/*
hostname(config-webvpn)# authentication-exclude *example.html
hostname(config-webvpn)# hostname #
```

authentication

To configure the authentication method for WebVPN and e-mail proxies, use the **authentication** command in various modes. To restore the default method, use the **no** form of this command. The ASA authenticates users to verify their identity.

authentication {[**aaa**] [**certificate**] [**mailhost**] [**piggyback**]}

no authentication [**aaa**] [**certificate**] [**mailhost**] [**piggyback**]

Syntax Description

aaa	Provides a username and password that the ASA checks with a previously configured AAA server.
certificate	Provides a certificate during SSL negotiation.
mailhost	Authenticates via the remote mail server for SMTPS only. For IMAP4S and POP3S, mailhost authentication is mandatory and not displayed as a configurable option.
piggyback	Requires that an HTTPS WebVPN session already exist. Piggyback authentication is available for e-mail proxies only.

Defaults

The following table shows the default authentication methods for WebVPN and e-mail proxies:

Protocol	Default Authentication Method
IMAP4S	Mailhost (required)
POP3S	Mailhost (required)
SMTPS	AAA
WebVPN	AAA

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—
Webvpn configuration	•		•		

Command History

Release	Modification
8.0(2)	This command was introduced.

Release	Modification
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group webvpn-attributes configuration mode for WebVPN.
8.0(2)	This command was modified to reflect changes to certificate authentication requirements.

Usage Guidelines

At least one authentication method is required. For WebVPN, for example, you can specify AAA authentication, certificate authentication, or both. You can enter these commands in either order.

WebVPN certificate authentication requires that HTTPS user certificates be required for the respective interfaces. That is, for this selection to be operational, before you can specify certificate authentication, you must have specified the interface in an **authentication-certificate** command.

If you enter this command in webvpn configuration mode, it is transformed into the same command in tunnel-group webvpn-attributes configuration mode.

For WebVPN, you can require both AAA and certificate authentication. In this case, users must provide both a certificate and a username and password. For e-mail proxy authentication, you can require more than one authentication method. Specifying the command again overwrites the current configuration.

Examples

The following example shows how to require that WebVPN users provide certificates for authentication:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication certificate
```

Related Commands

Command	Description
authentication-certificate	Requests a certificate from a WebVPN client establishing a connection.
show running-config	Displays the current tunnel group configuration.
clear configure aaa	Removes or resets the configured AAA values.
show running-config aaa	Displays the AAA configuration.

authentication eap-proxy

For L2TP over IPsec connections, to enable EAP and permit the ASA to proxy the PPP authentication process to an external RADIUS authentication server, use the **authentication eap-proxy** command in tunnel-group ppp-attributes configuration mode. To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication eap-proxy

no authentication eap-proxy

Syntax Description

This command has no keywords or arguments.

Defaults

By default, EAP is not a permitted authentication protocol.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel group type.

Examples

The following example entered in config-ppp configuration mode, permits EAP for PPP connections for the tunnel group named pppremotegrp:

```
hostname(config)# tunnel-group pppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group pppremotegrp ppp-attributes
hostname(config-ppp)# authentication eap
hostname(config-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.

Command	Description
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

authentication key eigrp

To enable authentication of EIGRP packets and specify the authentication key, use the **authentication key eigrp** command in interface configuration mode. To disable EIGRP authentication, use the **no** form of this command.

authentication key eigrp *as-number key* **key-id** *key-id*

no authentication key eigrp *as-number*

Syntax Description

as-number	The autonomous system number of the EIGRP process being authenticated. This must be the same value as configured for the EIGRP routing process.
key	Key to authenticate EIGRP updates. The key can contain up to 16 characters.
key-id *key-id*	Key identification value; valid values range from 1 to 255.

Defaults

EIGRP authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

You must configure both the **authentication mode eigrp** and the **authentication key eigrp** commands on an interface to enable EIGRP message authentication. Use the **show running-config interface** command to view the **authentication** commands configured on an interface.

Examples

The following examples shows EIGRP authentication configured on interface GigabitEthernet0/3:

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# authentication mode eigrp md5
hostname(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

Related Commands

Command	Description
authentication mode eigrp	Specifies the type of authentication used for EIGRP authentication.

authentication mode eigrp

To specify the type of authentication used for EIGRP authentication, use the **authentication mode eigrp** command in interface configuration mode. To restore the default authentication method, use the **no** form of this command.

authentication mode eigrp *as-num* **md5**

no authentication mode eigrp *as-num* **md5**

Syntax Description

as-num	The autonomous system number of the EIGRP routing process.
md5	Uses MD5 for EIGRP message authentication.

Defaults

No authentication is provided by default.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

You must configure both the **authentication mode eigrp** and the **authentication key eigrp** commands on an interface to enable EIGRP message authentication. Use the **show running-config interface** command to view the **authentication** commands configured on an interface.

Examples

The following examples shows EIGRP authentication configured on interface GigabitEthernet0/3:

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# authentication mode eigrp 100 md5
hostname(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

Related Commands

Command	Description
authentication key eigrp	Enables authentication of EIGRP packets and specifies the authentication key.

authentication ms-chap-v1

For L2TP over IPsec connections, to enable Microsoft CHAP, Version 1 authentication for PPP, use the **authentication ms-chap-v1** command in tunnel-group ppp-attributes configuration mode.To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command. To disable Microsoft CHAP, Version 1, use the **no** form of this command.

authentication ms-chap-v1

no authentication ms-chap-v1

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel-group type. This protocol is similar to CHAP, but more secure in that the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE.

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

authentication ms-chap-v2

For L2TP over IPsec connections, to enable Microsoft CHAP, Version 2 authentication for PPP, use the **authentication ms-chap-v1** command in tunnel-group ppp-attributes configuration mode. To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

```
authentication ms-chap-v2

no authentication ms-chap-v2
```

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel-group type.

This protocol is similar to CHAP but more secure in that the server stores and compares only encrypted passwords rather than clear text passwords as in CHAP. This protocol also generates a key for data encryption by MPPE.

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel group database or just the specified tunnel group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

authentication pap

For L2TP over IPsec connections, to permit PAP authentiation for PPP, use the **authentication pap** command in tunnel-group ppp-attributes configuration mode. To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication pap

no authentication pap

Syntax Description

This command has no keywords or arguments.

Defaults

By default, PAP is not a permitted authentication protocol.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel group type.

This protocol passes the clear text username and password during authentication and is not secure.

Examples

The following example entered in config-ppp configuration mode, permits PAP for PPP connections for a tunnel group named pppremotegrps:

```
hostname(config)# tunnel-group pppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group pppremotegrp ppp-attributes
hostname(config-ppp)# authentication pap
hostname(config-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.

Command	Description
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

authentication-certificate

To request a certificate from a WebVPN client establishing a connection, use the **authentication-certificate** command in webvpn configuration mode. To cancel the requirement for a client certificate, use the **no** form of this command.

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

Syntax Description

interface-name	The name of the interface used to establish the connection. Available interfaces names are: • **inside** Name of interface GigabitEthernet0/1 • **outside** Name of interface GigabitEthernet0/0

Defaults

If you omit the **authentication-certificate** command, client certificate authentication is disabled. If you do not specify an interface name with the **authentication-certificate** command, the default interface-name is **inside**.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

For this command to take effect, WebVPN must already be enabled on the corresponding interface. An interface is configured and named with the **interface**, **IP address**, and **nameif** commands.

This command applies only to WebVPN client connections; however, the ability to specify client certificate authentication for management connections with the **http authentication-certificate** command is available on all platforms, including the platforms that do not support WebVPN.

The ASA validates certificates with the PKI trustpoints. If a certificate does not pass validation, then one of the following actions occurs:

If:	Then:
The local CA embedded in the ASA is not enabled.	The ASA closes the SSL connection.
The local CA is enabled, and AAA authentication is not enabled.	The ASA redirects the client to the certificate enrollment page for the local CA to obtain a certificate.
Both the local CA and AAA authentication are enabled.	The client is redirected to a AAA authentication page. If configured, the client also is presented with a link to the enrollment page for the local CA.

Examples

The following example configures certificate authentication for WebVPN user connections on the outside interface:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-certificate outside
hostname(config-webvpn)#
```

Related Commands

Command	Description
authentication (tunnel-group webvpn configuration mode)	Specifies that the members of a tunnel group must use a digital certificate for authentication.
http authentication-certificate	Specifies authentication by means of certificate for ASDM management connections to the ASA.
interface	Configures the interface used to establish the connection.
show running-config ssl	Displays the current set of configured SSL commands.
ssl trust-point	Configures the SSL certificate trustpoint.

authentication-port

To specify the port number used for RADIUS authentication for this host, use the **authentication-port** command in aaa-server configuration host configuration mode. To remove the authentication port specification, use the **no** form of this command.

authentication-port *port*

no authentication-port

Syntax Description

port	A port number, in the range 1-65535, for RADIUS authentication.

Defaults

By default, the device listens for RADIUS on port 1645 (in compliance with RFC 2058). If the port is not specified, the RADIUS authentication default port number 1645 is used.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Semantic change to the command to support the specification of server ports on a per-host basis for server groups that contain RADIUS servers.

Usage Guidelines

This command specifies the destination TCP/UDP port number of the remote RADIUS server hosts to which you want to assign authentication functions. If your RADIUS authentication server uses a port other than 1645, you must configure the ASA for the appropriate port before starting the RADIUS service with the **aaa-server** command.

This command is valid only for server groups that are configured for RADIUS.

Examples

The following example configures a RADIUS AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry interval of 7 seconds, and configures authentication port 1650.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa authentication	Enables or disables LOCAL, TACACS+, or RADIUS user authentication on a server designated by the **aaa-server** command or by ASDM user authentication.
aaa-server host	Enters aaa-server host configuration mode, so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

authentication-server-group (imap4s, pop3s, smtps)

To specify the set of authentication servers to use for e-mail proxies, use the **authentication-server-group** command in various modes. To remove authentication servers from the configuration, use the **no** form of this command.

authentication-server-group *group_tag*

no authentication-server-group

Syntax Description

group_tag	Identifies the previously configured authentication server or group of servers.

Defaults

No authentication servers are configured by default.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The ASA authenticates users to verify their identity.

If you configure AAA authentication, you must configure this attribute as well. Otherwise, authentication always fails.

Use the **aaa-server** command to configure authentication servers.

Examples

The following example shows how to configure an IMAP4S e-mail proxy to use the set of authentication servers named “IMAP4SSVRS”:

```
hostname(config)# imap4s
hostname(config-imap4s)# authentication-server-group IMAP4SSVRS
```

Related Commands

Command	Description
aaa-server host	Configures authentication, authorization, and accounting servers.

authentication-server-group (tunnel-group general-attributes)

To specify the AAA server group to use for user authentication for a tunnel group, use the **authentication-server-group** command in tunnel-group general-attributes configuration mode. To return this attribute to the default, use the **no** form of this command.

authentication-server-group [(*interface_name*)] *server_group* [**LOCAL**]

no authentication-server-group [(*interface_name*)] *server_group*

Syntax Description

interface_name	(Optional) Specifies the interface at which the IPsec tunnel terminates.
LOCAL	(Optional) Requires authentication with the local user database if all of the servers in the server group have been deactivated due to communication failures.
server_group	Identifies the previously configured authentication server or group of servers.

Defaults

The default setting for the server-group in this command is **LOCAL**.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
8.0(2)	This command was enhanced to allow per-interface authentication for IPsec connections.

Usage Guidelines

You can apply this attribute to all tunnel-group types.

Use the **aaa-server** command to configure authentication servers and the **aaa-server-host** command to add servers to a previously configured AAA server group.

Examples

The following example entered in config-general configuration mode, configures an authentication server group named aaa-server456 for an IPsec remote access tunnel group named remotegrp:

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
aaa-server	Creates a AAA server group and configures AAA server parameters that are group-specific and common to all group hosts.
aaa-server host	Adds servers to a previously configured AAA server group and configures host-specific AAA server parameters.
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.

authorization-required

To require users to authorize successfully prior to connecting, use the **authorization-required** command in various modes. To remove the attribute from the configuration, use the **no** form of this command.

authorization-required

no authorization-required

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
7.2(1)	Replaced the webvpn configuration mode with the imap4s, pop3s, and smtps configuration modes.

Examples

The following example, entered in global configuration mode, requires authorization based on the complete DN for users connecting through a remote access tunnel group named remotegrp. The first command configures the tunnel-group type as ipsec_ra (IPsec remote access) for the remote group named remotegrp. The second command enters tunnel-group general-attributes configuration mode for the specified tunnel group, and the last command specifies that authorization is required for the named tunnel group.

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
authorization-dn-attributes	Specifies the primary and secondary subject DN fields to use as the username for authorization.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

authorization-server-group

To specify the set of authorization servers to use with WebVPN and e-mail proxies, use the **authorization-server-group** command in various modes. To remove authorization servers from the configuration, use the **no** form of this command.

authorization-server-group *group_tag*

no authorization-server-group

Syntax Description

group_tag	Identifies the previously configured authorization server or group of servers. Use the **aaa-server** command to configure authorization servers.

Defaults

No authorization servers are configured by default.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.

Usage Guidelines

The ASA uses authorization to verify the level of access to network resources that users are permitted.

If you enter this command in webvpn configuration mode, it is transformed into the same command in tunnel-group general-attributes mode.

When VPN authorization is defined as LOCAL, the attributes configured in the default group policy DfltGrpPolicy are enforced.

Examples

The following example shows how to configure POP3S e-mail proxy to use the set of authorization servers named “POP3Spermit”:

```
hostname(config)# pop3s
hostname(config-pop3s)# authorization-server-group POP3Spermit
```

The following example entered in tunnel-general configuration mode, configures an authorization server group named “aaa-server78” for an IPsec remote-access tunnel group named “remotegrp”:

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-server-group aaa-server78
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
aaa-server host	Configures authentication, authorization, and accounting servers.
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.

auth-prompt

To specify or change the AAA challenge text for through-the-ASA user sessions, use the **auth-prompt** command in global configuration mode. To remove the authentication challenge text, use the **no** form of this command.

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

Syntax Description

accept	If a user authentication via Telnet is accepted, displays the prompt *string*.
prompt	The AAA challenge prompt string follows this keyword.
reject	If a user authentication via Telnet is rejected, displays the prompt *string*.
string	A string of up to 235 alphanumeric characters or 31 words, limited by whichever maximum is first reached. Special characters, spaces, and punctuation characters are permitted. Entering a question mark or pressing the **Enter** key ends the string. (The question mark appears in the string.)

Defaults

If you do not specify an authentication prompt:

- FTP users see `FTP authentication`.
- HTTP users see `HTTP Authentication`.
- Telnet users see no challenge text.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Minor semantic changes.

Usage Guidelines

The **auth-prompt** command lets you specify the AAA challenge text for HTTP, FTP, and Telnet access through the ASA when requiring user authentication from TACACS+ or RADIUS servers. This text is primarily for cosmetic purposes and displays above the username and password prompts that users see when logging in.

If user authentication occurs from Telnet, you can use the **accept** and **reject** options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

If the AAA server authenticates the user, the ASA displays the **auth-prompt accept** text, if specified, to the user; otherwise, it displays the **reject** text, if specified. Authentication of HTTP and FTP sessions displays only the challenge text at the prompt. The **accept** and **reject** text do not appear.

Note Microsoft Internet Explorer displays up to 37 characters in an authentication prompt. Telnet and FTP display up to 235 characters in an authentication prompt.

Examples

The following example sets the authentication prompt to the string “Please enter your username and password.”:

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

After this string is added to the configuration, users see the following:

```
Please enter your username and password
User Name:
Password:
```

For Telnet users, you can also provide separate messages to display when the ASA accepts or rejects the authentication attempt; for example:

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

The following example sets the authentication prompt for a successful authentication to the string, “You’re OK.”

```
hostname(config)# auth-prompt accept You’re OK.
```

After successfully authenticating, the user sees the following message:

```
You’re OK.
```

Related Commands

Command	Description
clear configure auth-prompt	Removes the previously specified authentication prompt challenge text and reverts to the default value, if any.
show running-config auth-prompt	Displays the current authentication prompt challenge text.

auto-signon

To configure the ASA to automatically pass user login credentials for clientless SSL VPN connections on to internal servers, use the **auto-signon** command in any of three modes: webvpn configuration, webvpn group configuration, or webvpn username configuration mode. To disable auto-signon to a particular server, use the **no** form of this command with the original **ip**, **uri**, and **auth-type** arguments. To disable auto-signon to all servers, use the **no** form of this command without arguments.

auto-signon allow {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ftp** | **ntlm** | **all**}

no auto-signon [**allow** {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ftp** | **ntlm** | **all**}]

Syntax Description

all	Specifies both the NTLM and HTTP Basic authentication methods.
allow	Enables authentication to a particular server.
auth-type	Enables selection of an authentication method.
basic	Specifies the HTTP Basic authentication method.
ftp	Ftp and cifs authentication type.
ip	Specifies that an IP address and mask identifies the servers to be authenticated to.
ip-address	In conjunction with *ip-mask*, identifies the IP address range of the servers to be authenticated to.
ip-mask	In conjunction with *ip-address*, identifies the IP address range of the servers to be authenticated to.
ntlm	Specifies the NTLMv1 authentication method.
resource-mask	Identifies the URI mask of the servers to be authenticated to.
uri	Specifies that a URI mask identifies the servers to be authenticated to.

Defaults

By default, this feature is disabled for all servers.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration (global)	•	—	•	—	—
Webvpn group policy configuration	•	—	•	—	—
Webvpn username configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.
8.0(1)	NTLMv2 support was added. The **ntlm** keyword includes both NTLMv1 and NTLMv2.

Usage Guidelines

The **auto-signon** command is a single sign-on method for clientless SSL VPN users. It passes the login credentials (username and password) to internal servers for authentication using NTLM authentication, HTTP Basic authentication, or both. Multiple auto-signon commands can be entered and are processed according to the input order (early commands take precedence).

You can use the auto-signon feature in three modes: webvpn configuration group-policy, webvpn configuration, or webvpn username configuration mode. The typical precedence behavior applies, where username supersedes group, and group supersedes global. The mode you choose depends on the desired scope of authentication:

Mode	Scope
Webvpn configuration	All WebVPN users globally
Webvpn group configuration	A subset of WebVPN users defined by a group policy
Webvpn username configuration	An individual WebVPN user

Examples

The following example configures auto-signon for all clientless users, using NTLM authentication, to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255:

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
```

The following example configures auto-signon for all clientless users, using HTTP Basic authentication, to servers defined by the URI mask https://*.example.com/*:

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

The following example configures auto-signon for clientless users ExamplePolicy group policy, using either HTTP Basic or NTLM authentication, to servers defined by the URI mask https://*.example.com/*:

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

The following example configures auto-signon for a user named Anyuser, using HTTP Basic authentication, to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255:

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
basic
```

Related Commands

Command	Description
show running-config webvpn auto-signon	Displays auto-signon assignments of the running configuration.

auto-summary

To enable the automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in router configuration mode. To disable route summarization, use the **no** form of this command.

auto-summary

no auto-summary

Syntax Description

This command has no arguments or keywords.

Defaults

Route summarization is enabled for RIP Version 1, RIP Version 2, and EIGRP.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	Support for EIGRP was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables.

RIP Version 1 always uses automatic summarization. You cannot disable automatic summarization for RIP Version 1.

If you are using RIP Version 2, you can turn off automatic summarization by specifying the **no auto-summary** command. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is disabled, subnets are advertised.

EIGRP summary routes are given an administrative distance value of 5. You cannot configure this value.

Only the **no** form of this command appears in the running configuration.

Examples

The following example disables RIP route summarization:

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
hostname(config-router)# no auto-summary
```

The following example disables automatic EIGRP route summarization:

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# no auto-summary
```

Related Commands

Command	Description
clear configure router	Clears all **router** commands and router configuration mode commands from the running configuration.
router eigrp	Enables the EIGRP routing process and enters EIGRP router configuration mode.
router rip	Enables the RIP routing process and enters RIP router configuration mode.
show running-config router	Displays the **router** commands and router configuration mode commands in the running configuration.

auto-update device-id

To configure the ASA device ID for use with an Auto Update Server, use the **auto-update device-id** command in global configuration mode. To remove the device ID, use the **no** form of this command.

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

Syntax Description

hardware-serial	Uses the hardware serial number of the ASA to uniquely identify the device.
hostname	Uses the hostname of the ASA to uniquely identify the device.
ipaddress [*if_name*]	Uses the IP address of the ASA to uniquely identify the ASA. By default, the ASA uses the interface used to communicate with the Auto Update Server. If you want to use a different IP address, specify the *if_name* option.
mac-address [*if_name*]	Uses the MAC address of the ASA to uniquely identify the ASA. By default, the ASA uses the MAC address of the interface used to communicate with the Auto Update Server. If you want to use a different MAC address, specify the *if_name* option.
string *text*	Specifies the text string to uniquely identify the device to the Auto Update Server.

Defaults

The default ID is the hostname.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the device ID to the serial number:

```
hostname(config)# auto-update device-id hardware-serial
```

Related Commands

auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-at

To schedule a specific time for the ASA to poll the Auto Update Server, use the **auto-update poll-at** command in global configuration mode. To remove all specified scheduling times for the ASA to poll the Auto Update Server, use the **no** form of this command.

auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

no auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

Syntax Description

days-of-the-week	Any single day or combination of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday. Other possible values are daily (Monday through Sunday), weekdays (Monday through Friday) and weekend (Saturday and Sunday).
randomize *minutes*	Specifies the period to randomize the poll time following the specified start time. from from 1 to 1439 minutes.
retry_count	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
retry_period	Specifies how long to wait between connection attempts. The default is 5 minutes. The range is from 1 and 35791 minutes.
time	Specifies the time in the format HH:MM at which to start the poll. For example, 8:00 is 8:00 AM and 20:00 is 8:00 PM.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **auto-update poll-at** command specifies a time at which to poll for updates. If you enable the **randomize** option, the polling occurs at a random time within the range of the first *time* option and the specified number of minutes. The **auto-update poll-at** and **auto-update poll-period** commands are mutually exclusive. Only one of them can be configured.

Examples

In the following example, the ASA polls the Auto Update Server every Friday and Saturday night at a random time between 10:00 p.m. and 11:00 p.m. If the ASA is unable to contact the server, it tries two more times every 10 minutes.

```
hostname(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
hostname(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
management-access	Enables access to an internal management interface on the ASA.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-period

To configure how often the ASA checks for updates from an Auto Update Server, use the **auto-update poll-period** command in global configuration mode. To reset the parameters to the defaults, use the **no** form of this command.

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

Syntax Description

poll_period	Specifies how often, in minutes, to poll an Auto Update Server, between 1 and 35791. The default is 720 minutes (12 hours).
retry_count	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
retry_period	Specifies how long to wait, in minutes, between connection attempts, between 1 and 35791. The default is 5 minutes.

Defaults

The default poll period is 720 minutes (12 hours).

The default number of times to try reconnecting to the Auto Update Server if the first attempt fails is 0.

The default period to wait between connection attempts is 5 minutes.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **auto-update poll-at** and **auto-update poll-period** commands are mutually exclusive. Only one of them can be configured.

Examples

The following example sets the poll period to 360 minutes, the retries to 1, and the retry period to 3 minutes:

```
hostname(config)# auto-update poll-period 360 1 3
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update server

To identify the Auto Update Server, use the **auto-update server** command in global configuration mode. To remove the server, use the **no** form of this command.

auto-update server *url* [**source** *interface*] [*verify-certificate*]

no auto-update server *url* [**source** *interface*] [*verify-certificate*]

Syntax Description

source *interface*	Specifies which interface for the source IP address to use when sending requests to the Auto Update Server.
url	Specifies the location of the Auto Update Server using the following syntax: **http**[**s**]**:**[[*user:password@*]*location* [:*port*]] **/** *pathname*
verify_certificate	Verifies the certificate returned by the Auto Update Server.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The command was modified to add support for multiple servers.

Usage Guidelines

The ASA periodically contacts the Auto Update Server for any configuration, operating system, and ASDM updates.

You can configure multiple servers to work with auto-update. When checking for updates, a connection is made to the first server, but if that fails, then the next server is contacted. This process continues until all the servers have been tried. If all of them fail to connect, then a retry starting with the first server is attempted if the auto-update poll period has been configured to retry the connection.

For auto-update functionality to work correctly, you must use the **boot system configuration** command and ensure that it specifies a valid boot image. In addition, you must use the **asdm image** command with auto-update to update the ASDM software image.

If the interface specified in the **source** *interface* argument is the same interface specified with the **management-access** command, requests to the Auto Update Server are sent over the VPN tunnel.

Examples

The following example sets the Auto Update Server URL and specifies the interface as outside:

```
hostname(config)# auto-update server http://10.1.1.1:1741/ source outside
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
management-access	Enables access to an internal management interface on the ASA.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update timeout

To set a timeout period in which to contact the Auto Update Server, use the **auto-update timeout** command in global configuration mode. To remove the timeout, use the **no** form of this command.

auto-update timeout [*period*]

no auto-update timeout [*period*]

Syntax Description

period	Specifies the timeout period in minutes between 1 and 35791. The default is 0, which means there is no timeout. You cannot set the timeout to 0; use the **no** form of the command to reset it to 0.

Defaults

The default timeout is 0, which sets the ASA to never time out.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

A timeout condition is reported with syslog message 201008.

If the Auto Update Server has not been contacted for the timeout period, the ASA stops all traffic going through it. Set a timeout to ensure that the ASA has the most recent image and configuration.

Examples

The following example sets the timeout to 24 hours:

```
hostname(config)# auto-update timeout 1440
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.

clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.