



CHAPTER 8

Configuring Interfaces

This chapter describes how to configure interfaces, including Ethernet parameters, switch ports (for the ASA 5505), VLAN subinterfaces, and IP addressing.

The procedure to configure interfaces varies depending on several factors: the ASA 5505 vs. other models; routed vs. transparent mode; and single vs. multiple mode. This chapter describes how to configure interfaces for each of these variables.



Note

If your adaptive security appliance has the default factory configuration, many interface parameters are already configured. This chapter assumes you do *not* have a factory default configuration, or that if you have a default configuration, that you need to change the configuration. For information about the factory default configurations, see the [“Factory Default Configurations”](#) section on page 2-1.

This chapter includes the following sections:

- [Information About Interfaces](#), page 8-1
- [Licensing Requirements for Interfaces](#), page 8-6
- [Guidelines and Limitations](#), page 8-7
- [Default Settings](#), page 8-8
- [Starting Interface Configuration \(ASA 5510 and Higher\)](#), page 8-9
- [Starting Interface Configuration \(ASA 5505\)](#), page 8-16
- [Completing Interface Configuration \(All Models\)](#), page 8-23
- [Allowing Same Security Level Communication](#), page 8-30
- [Enabling Jumbo Frame Support \(ASA 5580\)](#), page 8-31
- [Monitoring Interfaces](#), page 8-32
- [Configuration Examples for Interfaces](#), page 8-32
- [Feature History for Interfaces](#), page 8-34

Information About Interfaces

This section describes adaptive security appliance interfaces and includes the following topics:

- [ASA 5505 Interfaces](#), page 8-2
- [Auto-MDI/MDIX Feature](#), page 8-5

- [Security Levels](#), page 8-5
- [Dual IP Stack](#), page 8-6
- [Management Interface \(ASA 5510 and Higher\)](#), page 8-6

ASA 5505 Interfaces

This section describes the ports and interfaces of the ASA 5505 adaptive security appliance and includes the following topics:

- [Understanding ASA 5505 Ports and Interfaces](#), page 8-2
- [Maximum Active VLAN Interfaces for Your License](#), page 8-2
- [VLAN MAC Addresses](#), page 8-4
- [Power over Ethernet](#), page 8-4

Understanding ASA 5505 Ports and Interfaces

The ASA 5505 adaptive security appliance supports a built-in switch. There are two kinds of ports and interfaces that you need to configure:

- **Physical switch ports**—The adaptive security appliance has 8 Fast Ethernet switch ports that forward traffic at Layer 2, using the switching function in hardware. Two of these ports are PoE ports. See the [“Power over Ethernet” section on page 8-4](#) for more information. You can connect these interfaces directly to user equipment such as PCs, IP phones, or a DSL modem. Or you can connect to another switch.
- **Logical VLAN interfaces**—In routed mode, these interfaces forward traffic between VLAN networks at Layer 3, using the configured security policy to apply firewall and VPN services. In transparent mode, these interfaces forward traffic between the VLANs on the same network at Layer 2, using the configured security policy to apply firewall services. See the [“Maximum Active VLAN Interfaces for Your License”](#) section for more information about the maximum VLAN interfaces. VLAN interfaces let you divide your equipment into separate VLANs, for example, home, business, and Internet VLANs.

To segregate the switch ports into separate VLANs, you assign each switch port to a VLAN interface. Switch ports on the same VLAN can communicate with each other using hardware switching. But when a switch port on VLAN 1 wants to communicate with a switch port on VLAN 2, then the adaptive security appliance applies the security policy to the traffic and routes or bridges between the two VLANs.

Maximum Active VLAN Interfaces for Your License

In transparent firewall mode, you can configure the following VLANs depending on your license:

- Base license—2 active VLANs.
- Security Plus license—3 active VLANs, one of which must be for failover.

In routed mode, you can configure the following VLANs depending on your license: Base license

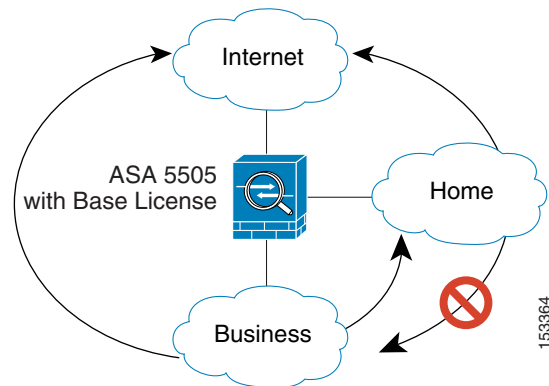
- Base license—3 active VLANs. The third VLAN can only be configured to initiate traffic to one other VLAN. See [Figure 8-1](#) for more information.
- Security Plus license—20 active VLANs.

**Note**

An *active VLAN* is a VLAN with a **nameif** command configured.

With the Base license, the third VLAN can only be configured to initiate traffic to one other VLAN. See [Figure 8-1](#) for an example network where the Home VLAN can communicate with the Internet, but cannot initiate contact with Business.

Figure 8-1 ASA 5505 Adaptive Security Appliance with Base License



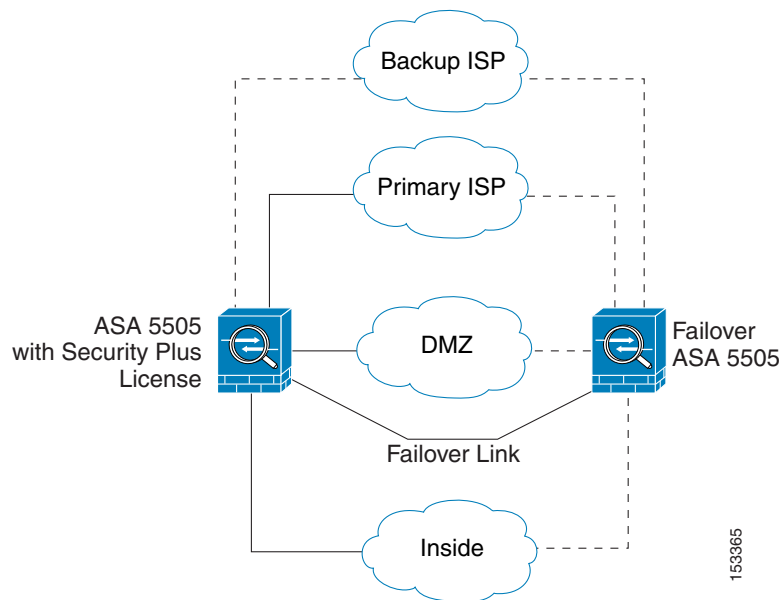
With the Security Plus license, you can configure 20 VLAN interfaces, including a VLAN interface for failover and a VLAN interface as a backup link to your ISP. You can configure the backup interface to not pass through traffic unless the route through the primary interface fails. You can configure trunk ports to accommodate multiple VLANs per port.

**Note**

The ASA 5505 adaptive security appliance supports Active/Standby failover, but not Stateful Failover.

See [Figure 8-2](#) for an example network.

Figure 8-2 ASA 5505 Adaptive Security Appliance with Security Plus License



VLAN MAC Addresses

- Routed firewall mode—All VLAN interfaces share a MAC address. Ensure that any connected switches can support this scenario. If the connected switches require unique MAC addresses, you can manually assign MAC addresses. See the [“Configuring the MAC Address”](#) section on page 8-26.
- Transparent firewall mode—Each VLAN has a unique MAC address. You can override the generated MAC addresses if desired by manually assigning MAC addresses. See the [“Configuring the MAC Address”](#) section on page 8-26.

Power over Ethernet

Ethernet 0/6 and Ethernet 0/7 support PoE for devices such as IP phones or wireless access points. If you install a non-PoE device or do not connect to these switch ports, the adaptive security appliance does not supply power to the switch ports.

If you shut down the switch port using the **shutdown** command, you disable power to the device. Power is restored when you enable the port using the **no shutdown** command. See the [“Configuring and Enabling Switch Ports as Access Ports”](#) section on page 8-18 for more information about shutting down a switch port.

To view the status of PoE switch ports, including the type of device connected (Cisco or IEEE 802.3af), use the **show power inline** command.

Monitoring Traffic Using SPAN

If you want to monitor traffic that enters or exits one or more switch ports, you can enable SPAN, also known as switch port monitoring. The port for which you enable SPAN (called the destination port) receives a copy of every packet transmitted or received on a specified source port. The SPAN feature lets you attach a sniffer to the destination port so you can monitor all traffic; without SPAN, you would have to attach a sniffer to every port you want to monitor. You can only enable SPAN for one destination port.

See the **switchport monitor** command in the *Cisco ASA 5500 Series Command Reference* for more information.

Auto-MDI/MDIX Feature

For RJ-45 interfaces, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase.

For the ASA 5510 and higher, either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

For Gigabit Ethernet, when the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

For the ASA 5505, you cannot disable Auto-MDI/MDIX.

Security Levels

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See the [“Allowing Same Security Level Communication” section on page 8-30](#) for more information.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

If you enable communication for same security interfaces (see the [“Allowing Same Security Level Communication” section on page 8-30](#)), there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some application inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
 - NetBIOS inspection engine—Applied only for outbound connections.
 - SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the adaptive security appliance.
- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

If you enable communication for same security interfaces, you can filter traffic in either direction.

- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

If you enable communication for same security interfaces, you can configure **established** commands for both directions.

Dual IP Stack

The adaptive security appliance supports the configuration of both IPv6 and IPv4 on an interface. You do not need to enter any special commands to do so; simply enter the IPv4 configuration commands and IPv6 configuration commands as you normally would. Make sure you configure a default route for both IPv4 and IPv6.

Management Interface (ASA 5510 and Higher)

The management interface is designed for management traffic only, and is specified as **managementslot/port** in commands. You can, however, use it for through traffic if desired (see the **management-only** command). In transparent firewall mode, you can use the management interface (for management purposes) in addition to the two interfaces allowed for through traffic. You can also add subinterfaces to the management interface to provide management in each security context for multiple context mode.



Note

In transparent firewall mode, the management interface updates the MAC address table in the same manner as a data interface; therefore you should not connect both a management and a data interface to the same switch unless you configure one of the switch ports as a routed port (by default Cisco Catalyst switches share a MAC address for all VLAN switch ports). Otherwise, if traffic arrives on the management interface from the physically-connected switch, then the adaptive security appliance updates the MAC address table to use the *management* interface to access the switch, instead of the data interface. This action causes a temporary traffic interruption; the adaptive security appliance will not re-update the MAC address table for packets from the switch to the data interface for at least 30 seconds for security reasons.

Licensing Requirements for Interfaces

The following table shows the licensing requirements for VLANs:

Model	License Requirement
ASA 5505	Base License: 3 (2 regular zones and 1 restricted zone that can only communicate with 1 other zone) Security Plus License: 20
ASA 5510	Base License: 50 Security Plus License: 100
ASA 5520	Base License: 150
ASA 5540	Base License: 200

Model	License Requirement
ASA 5550	Base License: 250
ASA 5580	Base License: 250

The following table shows the licensing requirements for VLAN trunks:

Model	License Requirement
ASA 5505	Base License: None. Security Plus License: 8.
All other models	N/A

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

- In multiple context mode, configure the physical interfaces in the system execution space according to the [“Starting Interface Configuration \(ASA 5510 and Higher\)”](#) section on page 8-9.
- Then, configure the logical interface parameters in the context execution space according to the [“Completing Interface Configuration \(All Models\)”](#) section on page 8-23.

Firewall Mode Guidelines

- Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA 5510 and higher adaptive security appliance, you can use the Management 0/0 or 0/1 interface (either the physical interface or a subinterface) as a third interface for management traffic. The mode is not configurable in this case and must always be management-only.
- Intra-interface communication is only available in routed firewall mode.

Failover Guidelines

Do not finish configuring failover interfaces with the procedures in [“Completing Interface Configuration \(All Models\)”](#) section on page 8-23. See the [“Configuring Active/Standby Failover”](#) section on page 59-7 or the [“Configuring Active/Active Failover”](#) section on page 58-8 to configure the failover and state links. In multiple context mode, failover interfaces are configured in the system configuration.

IPv6 Guidelines

- Supports IPv6.
- In transparent mode on a per interface basis, you can only configure the link-local address; you configure the global address as the management address for the entire unit, but not per interface. Because configuring the management global IP address automatically configures the link-local addresses per interface, the only IPv6 configuration you need to perform is to set the management IP address according to the [“Configuring the IPv6 Address”](#) section on page 7-14.

Model Guidelines

Subinterfaces are not available for the ASA 5505 adaptive security appliance.

Default Settings

This section lists default settings for interfaces if you do not have a factory default configuration. For information about the factory default configurations, see the [“Factory Default Configurations” section on page 2-1](#).

Default Security Level

The default security level is 0. If you name an interface “inside” and you do not set the security level explicitly, then the adaptive security appliance sets the security level to 100.



Note

If you change the security level of an interface, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

Default State of Interfaces

The default state of an interface depends on the type and the context mode.

In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

In single mode or in the system execution space, interfaces have the following default states:

- Physical interfaces and switch ports—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces or VLANs—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Default Speed and Duplex

- By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.
- The fiber interface for the ASA 5550 and the 4GE SSM has a fixed speed and does not support duplex, but you can set the interface to negotiate link parameters (the default) or not to negotiate.
- For fiber interfaces for the ASA 5580, the speed is set for automatic link negotiation.

Default Connector Type

The ASA 5550 adaptive security appliance and the 4GE SSM for the ASA 5510 and higher adaptive security appliance include two connector types: copper RJ-45 and fiber SFP. RJ-45 is the default. You can configure the adaptive security appliance to use the fiber SFP connectors.

Default MAC Addresses

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

Starting Interface Configuration (ASA 5510 and Higher)

This section includes tasks for starting your interface configuration for the ASA 5510 and higher.

**Note**

For multiple context mode, complete all tasks in this section in the system execution space. To change from the context to the system execution space, enter the **changeto system** command.

For ASA 5505 configuration, see the “[Starting Interface Configuration \(ASA 5505\)](#)” section on page 8-16.

This section includes the following topics:

- [Task Flow for Starting Interface Configuration](#), page 8-9
- [Configuring a Redundant Interface](#), page 8-12
- [Enabling the Physical Interface and Configuring Ethernet Parameters](#), page 8-10
- [Configuring VLAN Subinterfaces and 802.1Q Trunking](#), page 8-14
- [Assigning Interfaces to Contexts and Automatically Assigning MAC Addresses \(Multiple Context Mode\)](#), page 8-16

Task Flow for Starting Interface Configuration

To start configuring interfaces, perform the following steps:

-
- Step 1** (Multiple context mode) Complete all tasks in this section in the system execution space. To change from the context to the system execution space, enter the **changeto system** command.
- Step 2** Enable the physical interface, and optionally change Ethernet parameters. See the “[Enabling the Physical Interface and Configuring Ethernet Parameters](#)” section on page 8-10.
- Physical interfaces are disabled by default.
- Step 3** (Optional) Configure redundant interface pairs. See the “[Configuring a Redundant Interface](#)” section on page 8-12.
- A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic.
- Step 4** (Optional) Configure VLAN subinterfaces. See the “[Configuring VLAN Subinterfaces and 802.1Q Trunking](#)” section on page 8-14.
- Step 5** (Multiple context mode only) Assign interfaces to contexts and automatically assign unique MAC addresses to context interfaces. See the “[Assigning Interfaces to Contexts and Automatically Assigning MAC Addresses \(Multiple Context Mode\)](#)” section on page 8-16.
- Step 6** Complete the interface configuration according to the “[Completing Interface Configuration \(All Models\)](#)” section on page 8-23.
-

Enabling the Physical Interface and Configuring Ethernet Parameters

This section describes how to:

- Enable the physical interface
- Set a specific speed and duplex (if available)
- Enable pause frames for flow control (ASA 5580 10 Gigabit Ethernet only).

Prerequisites

For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the **changeto system** command.

Detailed Steps

Step 1 To specify the interface you want to configure, enter the following command:

```
hostname(config)# interface physical_interface
hostname(config-if)#
```

where the *physical_interface* ID includes the type, slot, and port number as *type[slot]port*.

The physical interface types include the following:

- **ethernet**
- **gigabitethernet**
- **tengigabitethernet**
- **management**

Enter the type followed by *slot/port*, for example, **gigabitethernet0/1** or **ethernet 0/1**.

Step 2 (Optional) To set the media type to SFP, if available for your model, enter the following command:

```
hostname(config-if)# media-type sfp
```

To restore the default RJ-45, enter the **media-type rj45** command.

Step 3 (Optional) To set the speed, enter the following command:

```
hostname(config-if)# speed {auto | 10 | 100 | 1000 | nonegotiate}
```

For copper interfaces, the default setting is **auto**.

For SFP interfaces, the default setting is **no speed nonegotiate**, which sets the speed to the maximum speed and enables link negotiation for flow-control parameters and remote fault information. The **nonegotiate** keyword is the only keyword available for SFP interfaces. The **speed nonegotiate** command disables link negotiation.

Step 4 (Optional) To set the duplex for copper interfaces, enter the following command:

```
hostname(config-if)# duplex {auto | full | half}
```

The **auto** setting is the default.

Step 5 (Optional; ASA 5580 only) To enable pause (XOFF) frames for flow control on 10 Gigabit Ethernet interfaces, enter the following command:

```
hostname(config-if)# flowcontrol send on [low_water high_water pause_time] [noconfirm]
```

If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue. Pause (XOFF) and XON frames are generated automatically by the NIC hardware based on the FIFO buffer usage. A pause frame is sent when the buffer usage exceeds the high-water mark. The default *high_water* value is 128 KB; you can set it between 0 and 511. After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark. By default, the *low_water* value is 64 KB; you can set it between 0 and 511. The link partner can resume traffic after receiving an XON, or after the XOFF expires, as controlled by the timer value in the pause frame. The default *pause_time* value is 26624; you can set it between 0 and 65535. If the buffer usage is consistently above the high-water mark, pause frames are sent repeatedly, controlled by the pause refresh threshold value.

When you use this command, you see the following warning:

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

To change the parameters without being prompted, use the **noconfirm** keyword.



Note Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

Step 6 To enable the interface, enter the following command:

```
hostname(config-if)# no shutdown
```

To disable the interface, enter the **shutdown** command. If you enter the **shutdown** command, you also shut down all subinterfaces. If you shut down an interface in the system execution space, then that interface is shut down in all contexts that share it.

What to Do Next

Optional Tasks:

- Configure redundant interface pairs. See the [“Configuring a Redundant Interface”](#) section on page 8-12.
- Configure VLAN subinterfaces. See the [“Configuring VLAN Subinterfaces and 802.1Q Trunking”](#) section on page 8-14.

Required Tasks:

- For multiple context mode, assign interfaces to contexts and automatically assign unique MAC addresses to context interfaces. See the [“Assigning Interfaces to Contexts and Automatically Assigning MAC Addresses \(Multiple Context Mode\)”](#) section on page 8-16.
- For single context mode, complete the interface configuration. See the [“Completing Interface Configuration \(All Models\)”](#) section on page 8-23.

Configuring a Redundant Interface

A logical redundant interface consists of a pair of physical interfaces: an active and a standby interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the adaptive security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired.

This section describes how to configure redundant interfaces and includes the following topics:

- [Configuring a Redundant Interface, page 8-12](#)
- [Changing the Active Interface, page 8-14](#)

Configuring a Redundant Interface

This section describes how to create a redundant interface. By default, redundant interfaces are enabled.

Guidelines and Limitations

- You can configure up to 8 redundant interface pairs.
- All adaptive security appliance configuration refers to the logical redundant interface instead of the member physical interfaces.
- Redundant interface delay values are configurable, but by default the adaptive security appliance will inherit the default delay values based on the physical type of its member interfaces.
- The only configuration available to physical interfaces that are part of a redundant interface pair are physical parameters (set in the [“Enabling the Physical Interface and Configuring Ethernet Parameters”](#) section on page 8-10), the **description** command, and the **shutdown** command. You can also enter run-time commands like **default** and **help**.
- If you shut down the active interface, then the standby interface becomes active.

For failover, follow these guidelines when adding member interfaces:

- If you want to use a redundant interface for the failover or state link, then you must configure the redundant interface as part of the basic configuration on the secondary unit in addition to the primary unit.
- If you use a redundant interface for the failover or state link, you must put a switch or hub between the two units; you cannot connect them directly. Without the switch or hub, you could have the active port on the primary unit connected directly to the standby port on the secondary unit.
- You can monitor redundant interfaces for failover using the **monitor-interface** command; be sure to reference the logical redundant interface name.
- When the active interface fails over to the standby interface, this activity does not cause the redundant interface to appear to be failed when being monitored for device-level failover. Only when both physical interfaces fail does the redundant interface appear to be failed.

Redundant Interface MAC Address

The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses (see the [“Configuring the MAC Address”](#) section on page 8-26 or the [“Assigning Interfaces to Contexts and](#)

[Automatically Assigning MAC Addresses \(Multiple Context Mode\)](#)” section on page 8-16). When the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.

Prerequisites

- Both member interfaces must be of the same physical type. For example, both must be Ethernet.
- You cannot add a physical interface to the redundant interface if you configured a name for it. You must first remove the name using the **no nameif** command.
- For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the **changeto system** command.



Caution

If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

Detailed Steps

You can configure up to 8 redundant interface pairs. To configure a redundant interface, perform the following steps:

Step 1 To add the logical redundant interface, enter the following command:

```
hostname(config)# interface redundant number
hostname(config-if)#
```

where the *number* argument is an integer between 1 and 8.

Step 2 To add the first member interface to the redundant interface, enter the following command:

```
hostname(config-if)# member-interface physical_interface
```

See the [“Enabling the Physical Interface and Configuring Ethernet Parameters”](#) section for a description of the physical interface ID.

After you add the interface, any configuration for it (such as an IP address) is removed.

Step 3 To add the second member interface to the redundant interface, enter the following command:

```
hostname(config-if)# member-interface physical_interface
```

Make sure the second interface is the same physical type as the first interface.

To remove a member interface, enter the **no member-interface** *physical_interface* command. You cannot remove both member interfaces from the redundant interface; the redundant interface requires at least one member interface.

Examples

The following example creates two redundant interfaces:

```
hostname(config)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1
hostname(config-if)# interface redundant 2
hostname(config-if)# member-interface gigabitethernet 0/2
hostname(config-if)# member-interface gigabitethernet 0/3
```

What to Do Next

Optional Task:

- Configure VLAN subinterfaces. See the “[Configuring VLAN Subinterfaces and 802.1Q Trunking](#)” section on page 8-14.

Required Tasks:

- For multiple context mode, assign interfaces to contexts and automatically assign unique MAC addresses to context interfaces. See the “[Assigning Interfaces to Contexts and Automatically Assigning MAC Addresses \(Multiple Context Mode\)](#)” section on page 8-16.
- For single context mode, complete the interface configuration. See the “[Completing Interface Configuration \(All Models\)](#)” section on page 8-23.

Changing the Active Interface

By default, the active interface is the first interface listed in the configuration, if it is available. To view which interface is active, enter the following command:

```
hostname# show interface redundantnumber detail | grep Member
```

For example:

```
hostname# show interface redundant1 detail | grep Member
Members GigabitEthernet0/3 (Active), GigabitEthernet0/2
```

To change the active interface, enter the following command:

```
hostname# redundant-interface redundantnumber active-member physical_interface
```

where the **redundantnumber** argument is the redundant interface ID, such as **redundant1**.

The *physical_interface* is the member interface ID that you want to be active.

Configuring VLAN Subinterfaces and 802.1Q Trunking

Subinterfaces let you divide a physical or redundant interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or adaptive security appliances. This feature is particularly useful in multiple context mode so that you can assign unique interfaces to each context.

Guidelines and Limitations

- Maximum subinterfaces—To determine how many VLAN subinterfaces are allowed for your platform, see the “[Licensing Requirements for Interfaces](#)” section on page 8-6.
- Preventing untagged packets on the physical interface—If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. This property is also true for the active physical interface in a redundant interface pair. Because the physical or redundant interface must be enabled for the subinterface to pass traffic, ensure that the physical or redundant interface does not pass traffic by leaving out the **nameif**

command. If you want to let the physical or redundant interface pass untagged packets, you can configure the **nameif** command as usual. See the “[Completing Interface Configuration \(All Models\)](#)” section on page 8-23 for more information about completing the interface configuration.

Prerequisites

For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the **changeto system** command.

Detailed Steps

To add a subinterface and assign a VLAN to it, perform the following steps:

Step 1 To specify the new subinterface, enter the following command:

```
hostname(config)# interface {physical_interface | redundant number}.subinterface  
hostname(config-subif)#
```

See the “[Enabling the Physical Interface and Configuring Ethernet Parameters](#)” section for a description of the physical interface ID.

The **redundant number** argument is the redundant interface ID, such as **redundant 1**.

The *subinterface* ID is an integer between 1 and 4294967293.

The following command adds a subinterface to a Gigabit Ethernet interface:

```
hostname(config)# interface gigabitethernet 0/1.100
```

The following command adds a subinterface to a redundant interface:

```
hostname(config)# interface redundant 1.100
```

Step 2 To specify the VLAN for the subinterface, enter the following command:

```
hostname(config-subif)# vlan vlan_id
```

The *vlan_id* is an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information.

You can only assign a single VLAN to a subinterface, and you cannot assign the same VLAN to multiple subinterfaces. You cannot assign a VLAN to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the **no** option; you can enter the **vlan** command with a different VLAN ID, and the adaptive security appliance changes the old ID.

What to Do Next

- For multiple context mode, assign interfaces to contexts and automatically assign unique MAC addresses to context interfaces. See the “[Assigning Interfaces to Contexts and Automatically Assigning MAC Addresses \(Multiple Context Mode\)](#)” section on page 8-16.
- For single context mode, complete the interface configuration. See the “[Completing Interface Configuration \(All Models\)](#)” section on page 8-23.

Assigning Interfaces to Contexts and Automatically Assigning MAC Addresses (Multiple Context Mode)

To complete the configuration of interfaces in the system execution space, perform the following tasks that are documented in [Chapter 5, “Configuring Multiple Context Mode”](#):

- To assign interfaces to contexts, see the [“Configuring a Security Context”](#) section on page 5-17.
- (Optional) To automatically assign unique MAC addresses to context interfaces, see the [“Automatically Assigning MAC Addresses to Context Interfaces”](#) section on page 5-22.

The MAC address is used to classify packets within a context. If you share an interface, but do not have unique MAC addresses for the interface in each context, then the destination IP address is used to classify packets. Alternatively, you can manually assign MAC addresses within the context according to the [“Configuring the MAC Address”](#) section on page 8-26.

What to Do Next

Complete the interface configuration. See the [“Completing Interface Configuration \(All Models\)”](#) section on page 8-23.

Starting Interface Configuration (ASA 5505)

This section includes tasks for starting your interface configuration for the ASA 5505 adaptive security appliance, including creating VLAN interfaces and assigning them to switch ports. See the [“Understanding ASA 5505 Ports and Interfaces”](#) section on page 8-2 for more information.

For ASA 5510 and higher configuration, see the [“Starting Interface Configuration \(ASA 5510 and Higher\)”](#) section on page 8-9.

This section includes the following topics:

- [Task Flow for Starting Interface Configuration](#), page 8-16
- [Configuring VLAN Interfaces](#), page 8-17
- [Configuring and Enabling Switch Ports as Access Ports](#), page 8-18
- [Configuring and Enabling Switch Ports as Trunk Ports](#), page 8-20

Task Flow for Starting Interface Configuration

To configure interfaces in single mode, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Configure VLAN interfaces. See the “Configuring VLAN Interfaces” section on page 8-17. |
| Step 2 | Configure and enable switch ports as access ports. See the “Configuring and Enabling Switch Ports as Access Ports” section on page 8-18. |
| Step 3 | (Optional for Security Plus licenses) Configure and enable switch ports as trunk ports. See the “Configuring and Enabling Switch Ports as Trunk Ports” section on page 8-20. |
| Step 4 | Complete the interface configuration according to the “Completing Interface Configuration (All Models)” section on page 8-23. |
-

Configuring VLAN Interfaces

This section describes how to configure VLAN interfaces. For more information about ASA 5505 interfaces, see the [“ASA 5505 Interfaces”](#) section on page 8-2.

Detailed Steps

- Step 1** To add a VLAN interface, enter the following command:

```
hostname(config)# interface vlan number
```

Where the *number* is between 1 and 4090.

For example, enter the following command:

```
hostname(config)# interface vlan 100
```

To remove this VLAN interface and all associated configuration, enter the **no interface vlan** command. Because this interface also includes the interface name configuration, and the name is used in other commands, those commands are also removed.

- Step 2** (Optional for the Base license) To allow this interface to be the third VLAN by limiting it from initiating contact to one other VLAN, enter the following command:

```
hostname(config-if)# no forward interface vlan number
```

Where *number* specifies the VLAN ID to which this VLAN interface cannot initiate traffic.

With the Base license, you can only configure a third VLAN if you use this command to limit it.

For example, you have one VLAN assigned to the outside for Internet access, one VLAN assigned to an inside business network, and a third VLAN assigned to your home network. The home network does not need to access the business network, so you can use the **no forward interface** command on the home VLAN; the business network can access the home network, but the home network cannot access the business network.

If you already have two VLAN interfaces configured with a **nameif** command, be sure to enter the **no forward interface** command before the **nameif** command on the third interface; the adaptive security appliance does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505 adaptive security appliance.



Note If you upgrade to the Security Plus license, you can remove this command and achieve full functionality for this interface. If you leave this command in place, this interface continues to be limited even after upgrading.

What to Do Next

Configure the switch ports. See the [“Configuring and Enabling Switch Ports as Access Ports”](#) section on page 8-18 and the [“Configuring and Enabling Switch Ports as Trunk Ports”](#) section on page 8-20.

Configuring and Enabling Switch Ports as Access Ports

By default (with no configuration), all switch ports are shut down, and assigned to VLAN 1. To assign a switch port to a single VLAN, configure it as an access port. To create a trunk port to carry multiple VLANs, see the [“Configuring and Enabling Switch Ports as Trunk Ports”](#) section on page 8-20. If you have a factory default configuration, see the [“ASA 5505 Default Configuration”](#) section on page 2-2 to check if you want to change the default interface settings according to this procedure.

For more information about ASA 5505 interfaces, see the [“ASA 5505 Interfaces”](#) section on page 8-2.



Caution

The ASA 5505 adaptive security appliance does not support Spanning Tree Protocol for loop detection in the network. Therefore you must ensure that any connection with the adaptive security appliance does not end up in a network loop.

Detailed Steps

Step 1 To specify the switch port you want to configure, enter the following command:

```
hostname(config)# interface ethernet0/port
```

Where *port* is 0 through 7. For example, enter the following command:

```
hostname(config)# interface ethernet0/1
```

Step 2 To assign this switch port to a VLAN, enter the following command:

```
hostname(config-if)# switchport access vlan number
```

Where *number* is the VLAN ID, between 1 and 4090. See the [“Configuring VLAN Interfaces”](#) section on page 8-17 to configure the VLAN interface that you want to assign to this switch port. To view configured VLANs,



Note You might assign multiple switch ports to the primary or backup VLANs if the Internet access device includes Layer 2 redundancy.

Step 3 (Optional) To prevent the switch port from communicating with other protected switch ports on the same VLAN, enter the following command:

```
hostname(config-if)# switchport protected
```

You might want to prevent switch ports from communicating with each other if the devices on those switch ports are primarily accessed from other VLANs, you do not need to allow intra-VLAN access, and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the **switchport protected** command to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.

Step 4 (Optional) To set the speed, enter the following command:

```
hostname(config-if)# speed {auto | 10 | 100}
```

The **auto** setting is the default. If you set the speed to anything other than **auto** on PoE ports Ethernet 0/6 or 0/7, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.

Step 5 (Optional) To set the duplex, enter the following command:

```
hostname(config-if)# duplex {auto | full | half}
```

The **auto** setting is the default. If you set the duplex to anything other than **auto** on PoE ports Ethernet 0/6 or 0/7, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.

Step 6 To enable the switch port, enter the following command:

```
hostname(config-if)# no shutdown
```

To disable the switch port, enter the **shutdown** command.

Examples

The following example configures five VLAN interfaces, including the failover interface which is configured using the **failover lan** command:

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
```

```
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

What to Do Next

If you want to configure a switch port as a trunk port, see the [“Configuring and Enabling Switch Ports as Trunk Ports”](#) section on page 8-20.

To complete the interface configuration, see the [“Completing Interface Configuration \(All Models\)”](#) section on page 8-23.

Configuring and Enabling Switch Ports as Trunk Ports

This procedure describes how to create a trunk port that can carry multiple VLANs using 802.1Q tagging. Trunk mode is available only with the Security Plus license.

To create an access port, where an interface is assigned to only one VLAN, see the [“Configuring and Enabling Switch Ports as Access Ports”](#) section on page 8-18.

For more information about ASA 5505 interfaces, see the [“ASA 5505 Interfaces”](#) section on page 8-2.

Detailed Steps

-
- Step 1** To specify the switch port you want to configure, enter the following command:

```
hostname(config)# interface ethernet0/port
```

Where *port* is 0 through 7. For example, enter the following command:

```
hostname(config)# interface ethernet0/1
```

- Step 2** To assign VLANs to this trunk, enter one or more of the following commands.

- To assign native VLANs, enter the following command:

```
hostname(config-if)# switchport trunk native vlan vlan_id
```

where the *vlan_id* is a single VLAN ID between 1 and 4090.

Packets on the native VLAN are not modified when sent over the trunk. For example, if a port has VLANs 2, 3 and 4 assigned to it, and VLAN 2 is the native VLAN, then packets on VLAN 2 that egress the port are not modified with an 802.1Q header. Frames which ingress (enter) this port and have no 802.1Q header are put into VLAN 2.

Each port can only have one native VLAN, but every port can have either the same or a different native VLAN.

- To assign VLANs, enter the following command:

```
hostname(config-if)# switchport trunk allowed vlan vlan_range
```

where the *vlan_range* (with VLANs between 1 and 4090) can be identified in one of the following ways:

A single number (n)

A range (n-x)

Separate numbers and ranges by commas, for example:

5,7-10,13,45-100

You can enter spaces instead of commas, but the command is saved to the configuration with commas.

You can include the native VLAN in this command, but it is not required; the native VLAN is passed whether it is included in this command or not.

This switch port cannot pass traffic until you assign at least one VLAN to it, native or non-native.

Step 3 To make this switch port a trunk port, enter the following command:

```
hostname(config-if)# switchport mode trunk
```

To restore this port to access mode, enter the **switchport mode access** command.

Step 4 (Optional) To prevent the switch port from communicating with other protected switch ports on the same VLAN, enter the following command:

```
hostname(config-if)# switchport protected
```

You might want to prevent switch ports from communicating with each other if the devices on those switch ports are primarily accessed from other VLANs, you do not need to allow intra-VLAN access, and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the **switchport protected** command to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.

Step 5 (Optional) To set the speed, enter the following command:

```
hostname(config-if)# speed {auto | 10 | 100}
```

The **auto** setting is the default.

Step 6 (Optional) To set the duplex, enter the following command:

```
hostname(config-if)# duplex {auto | full | half}
```

The **auto** setting is the default.

Step 7 To enable the switch port, enter the following command:

```
hostname(config-if)# no shutdown
```

To disable the switch port, enter the **shutdown** command.

Examples

The following example configures seven VLAN interfaces, including the failover interface which is configured using the **failover lan** command. VLANs 200, 201, and 202 are trunked on Ethernet 0/1.

```
hostname(config)# interface vlan 100  
hostname(config-if)# nameif outside  
hostname(config-if)# security-level 0
```

```
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 201
hostname(config-if)# nameif dept1
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 202
hostname(config-if)# nameif dept2
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.3.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200-202
hostname(config-if)# switchport trunk native vlan 5
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

What to Do Next

To complete the interface configuration, see the [“Completing Interface Configuration \(All Models\)” section on page 8-23](#).

Completing Interface Configuration (All Models)

This section includes tasks to complete the interface configuration for all models.



Note

For multiple context mode, complete the tasks in this section in the context execution space. Enter the **changeto context name** command to change to the context you want to configure.

This section includes the following topics:

- [Entering Interface Configuration Mode, page 8-24](#)
- [Configuring General Interface Parameters, page 8-24](#)
- [Configuring the MAC Address, page 8-26](#)
- [Configuring IPv6 Addressing, page 8-27](#)

Task Flow for Completing Interface Configuration

-
- Step 1** Complete the procedures in the [“Starting Interface Configuration \(ASA 5510 and Higher\)” section on page 8-9](#) or the [“Starting Interface Configuration \(ASA 5505\)” section on page 8-16](#).
- Step 2** (Multiple context mode) Enter the **changeto context name** command to change to the context you want to configure.
- Step 3** Enter interface configuration mode. See the [“Entering Interface Configuration Mode” section on page 8-24](#).
- Step 4** Configure general interface parameters, including the interface name, security level, and IPv4 address. See the [“Configuring General Interface Parameters” section on page 8-24](#).
- For transparent mode, you do not configure IP addressing per interface, except for the management-only interface (see the [“Information About the Management Interface” section on page 8-25](#)). You do need to configure the other parameters in this section, however. To set the global management address for transparent mode, see the [“Configuring the IPv4 Address” section on page 7-14](#).
- Step 5** (Optional) Configure the MAC address. See the [“Configuring the MAC Address” section on page 8-26](#).
- Step 6** (Optional) Configure IPv6 addressing. See the [“Configuring IPv6 Addressing” section on page 8-27](#).
- For transparent mode, you do not configure IP addressing per interface, except for the management-only interface (see the [“Information About the Management Interface” section on page 8-25](#)). To set the global management address for transparent mode, see the [“Configuring the IPv6 Address” section on page 7-14](#).
-

Entering Interface Configuration Mode

The procedures in this section are performed in interface configuration mode.

Prerequisites

For multiple context mode, complete this procedure in the context execution space. Enter the **changeto context name** command to change to the context you want to configure.

Detailed Steps

If you are not already in interface configuration mode, enter the mode by using the **interface** command.

- For the ASA 5510 and higher:

```
hostname(config)# interface {{redundant number| physical_interface} [.subinterface] |
mapped_name}
hostname(config-if)#
```

The **redundant number** argument is the redundant interface ID, such as **redundant 1**.

See the “[Enabling the Physical Interface and Configuring Ethernet Parameters](#)” section for a description of the physical interface ID.

Append the *subinterface* ID to the physical or redundant interface ID separated by a period (.).

In multiple context mode, enter the *mapped_name* if one was assigned using the **allocate-interface** command.

- For the ASA 5505:

```
hostname(config)# interface vlan number
hostname(config-if)#
```

Configuring General Interface Parameters

This procedure describes how to set the name, security level, IPv4 address and other options.

For the ASA 5510 and higher, you must configure interface parameters for the following interface types:

- Physical interfaces
- VLAN subinterfaces
- Redundant interfaces

For the ASA 5505, you must configure interface parameters for the following interface types:

- VLAN interfaces

Guidelines and Limitations

- For the ASA 5550 adaptive security appliance, for maximum throughput, be sure to balance your traffic over the two interface slots; for example, assign the inside interface to slot 1 and the outside interface to slot 0.
- For information about security levels, see the “[Security Levels](#)” section on page 8-5.

- If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and Stateful Failover communications. See the [“Configuring Active/Standby Failover” section on page 59-7](#) or the [“Configuring Active/Active Failover” section on page 58-8](#) to configure the failover and state links.
- In routed firewall mode, set the IP address for all interfaces.
- In transparent firewall mode, do not set the IP address for each interface, but rather set it for the whole adaptive security appliance or context. The exception is for the Management 0/0 or 0/1 management-only interface, which does not pass through traffic. To set the transparent firewall mode whole adaptive security appliance or context management IP address, see the [“Setting the Management IP Address for a Transparent Firewall” section on page 7-12](#). To set the IP address of the Management 0/0 or 0/1 interface or subinterface, use this procedure.

Restrictions

PPPoE is not supported in multiple context mode or transparent firewall mode.

Information About the Management Interface

The ASA 5510 and higher adaptive security appliance includes a dedicated management interface called Management 0/0 or Management 0/1, depending on your model, which is meant to support traffic to the adaptive security appliance. However, you can configure any interface to be a management-only interface. Also, for Management 0/0 or 0/1, you can disable management-only mode so the interface can pass through traffic just like any other interface.

Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA 5510 and higher adaptive security appliance, you can use the Management 0/0 or 0/1 interface (either the physical interface or a subinterface) as a third interface for management traffic. The mode is not configurable in this case and must always be management-only.

Prerequisites

- Complete the procedures in the [“Starting Interface Configuration \(ASA 5510 and Higher\)” section on page 8-9](#) or the [“Starting Interface Configuration \(ASA 5505\)” section on page 8-16](#).
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the **changeto context name** command.
- Enter interface configuration mode according to the [“Entering Interface Configuration Mode” section on page 8-24](#).

Detailed Steps

Step 1 To name the interface, enter the following command:

```
hostname(config-if)# nameif name
```

The *name* is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value. Do not enter the **no** form, because that command causes all commands that refer to that name to be deleted.

Step 2 To set the security level, enter the following command:

```
hostname(config-if)# security-level number
```

Where *number* is an integer between 0 (lowest) and 100 (highest).

Step 3 To set the IP address, enter one of the following commands.



Note For use with failover, you must set the IP address and standby address manually; DHCP and PPPoE are not supported.

In transparent firewall mode, do not set the IP address for each interface, but rather set it for the whole adaptive security appliance or context. The exception is for the Management 0/0 or 0/1 management-only interface, which does not pass through traffic.

- To set the IP address manually, enter the following command:

```
hostname(config-if)# ip address ip_address [mask] [standby ip_address]
```

where the *ip_address* and *mask* arguments set the interface IP address and subnet mask.

The **standby ip_address** argument is used for failover. See the “[Configuring Active/Standby Failover](#)” section on page 59-7 or the “[Configuring Active/Active Failover](#)” section on page 58-8 for more information.

- To obtain an IP address from a DHCP server, enter the following command:

```
hostname(config-if)# ip address dhcp [setroute]
```

where the **setroute** keyword lets the adaptive security appliance use the default route supplied by the DHCP server.

Reenter this command to reset the DHCP lease and request a new lease.

If you do not enable the interface using the **no shutdown** command before you enter the **ip address dhcp** command, some DHCP requests might not be sent.

- To obtain an IP address from a PPPoE server, see [Chapter 68, “Configuring the PPPoE Client.”](#) PPPoE is not supported in multiple context mode.

Step 4 (Optional) To set an interface to management-only mode so that it does not pass through traffic, enter the following command:

```
hostname(config-if)# management-only
```

See the “[Information About the Management Interface](#)” section on page 8-25 for more information.

What to Do Next

- (Optional) Configure the MAC address. See the “[Configuring the MAC Address](#)” section on page 8-26.
- (Optional) Configure IPv6 addressing. See the “[Configuring IPv6 Addressing](#)” section on page 8-27.

Configuring the MAC Address

This section describes how to configure MAC addresses for interfaces.

Information About MAC Addresses

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address. A redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. If you assign a MAC address to the redundant interface using this command, then it is used regardless of the member interface MAC addresses.

In multiple context mode, if you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the adaptive security appliance easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See the [“How the Security Appliance Classifies Packets”](#) section on page 5-3 for more information. You can assign each MAC address manually, or you can automatically generate MAC addresses for shared interfaces in contexts. See the [“Automatically Assigning MAC Addresses to Context Interfaces”](#) section on page 5-22 to automatically generate MAC addresses. If you automatically generate MAC addresses, you can use this procedure to override the generated address.

For single context mode, or for interfaces that are not shared in multiple context mode, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

Prerequisites

Enter interface configuration mode according to the [“Entering Interface Configuration Mode”](#) section on page 8-24.

Detailed Steps

To assign a private MAC address to this interface, enter the following command:

```
hostname(config-if)# mac-address mac_address [standby mac_address]
```

The *mac_address* is in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE is entered as 000C.F142.4CDE.

The first two bytes of a manual MAC address cannot be A2 if you also want to use auto-generated MAC addresses.

For use with failover, set the **standby** MAC address. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

What to Do Next

(Optional) Configure IPv6 addressing. See the [“Configuring IPv6 Addressing”](#) section on page 8-27.

Configuring IPv6 Addressing

This section describes how to configure IPv6 addressing. For more information about IPv6, see the [“Information About IPv6 Support”](#) section on page 19-9 and the [“IPv6 Addresses”](#) section on page B-5.

For transparent mode, use this section for the Management 0/0 or 0/1 interface. To configure the global IPv6 management address for transparent mode, see the [“Configuring the IPv6 Address”](#) section on page 7-14.

Information About IPv6 Addressing

When you configure an IPv6 address on an interface, you can assign one or several IPv6 addresses to the interface at one time, such as an IPv6 link-local address and a global address. However, at a minimum, you must configure a link-local address.

Every IPv6-enabled interface must include at least one link-local address. When you configure a global address, a link-local address is automatically configured on the interface, so you do not also need to specifically configure a link-local address. These link-local addresses can only be used to communicate with other hosts on the same physical link.



Note

If you want to only configure the link-local addresses, see the **ipv6 enable** (to auto-configure) or **ipv6 address link-local** (to manually configure) command in the *Cisco ASA 5500 Series Command Reference*.

When IPv6 is used over Ethernet networks, the Ethernet MAC address can be used to generate the 64-bit interface ID for the host. This is called the EUI-64 address. Because MAC addresses use 48 bits, additional bits must be inserted to fill the 64 bits required. The last 64 bits are used for the interface ID. For example, FE80::/10 is a link-local unicast IPv6 address type in hexadecimal format.

Information About Duplicate Address Detection

During the stateless autoconfiguration process, duplicate address detection (DAD) verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection is performed first on the new link-local address. When the link local address is verified as unique, then duplicate address detection is performed all the other IPv6 unicast addresses on the interface.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state. An interface returning to an administratively up state restarts duplicate address detection for all of the unicast IPv6 addresses on the interface.

When a duplicate address is identified, the state of the address is set to DUPLICATE, the address is not used, and the following error message is generated:

```
%ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
```

If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. However, all configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

The adaptive security appliance uses neighbor solicitation messages to perform duplicate address detection. By default, the number of times an interface performs duplicate address detection is 1.

Information About Modified EUI-64 Interface IDs

RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture requires that the interface identifier portion of all unicast IPv6 addresses, except those that start with binary value 000, be 64 bits long and be constructed in Modified EUI-64 format. The adaptive security appliance can enforce this requirement for hosts attached to the local link.

When this command is enabled on an interface, the source addresses of IPv6 packets received on that interface are verified against the source MAC addresses to ensure that the interface identifiers use the Modified EUI-64 format. If the IPv6 packets do not use the Modified EUI-64 format for the interface identifier, the packets are dropped and the following system log message is generated:

```
%ASA-3-325003: EUI-64 source address check failed.
```

The address format verification is only performed when a flow is created. Packets from an existing flow are not checked. Additionally, the address verification can only be performed for hosts on the local link. Packets received from hosts behind a router will fail the address format verification, and be dropped, because their source MAC address will be the router MAC address and not the host MAC address.

Prerequisites

Enter interface configuration mode according to the [“Entering Interface Configuration Mode”](#) section on page 8-24.

Restrictions

The adaptive security appliance does not support IPv6 anycast addresses.

Detailed Steps

	Command	Purpose
Step 1	Do one of the following:	
	ipv6 address autoconfig Example: hostname(config-if)# ipv6 address autoconfig	Enables stateless autoconfiguration on the interface. Enabling stateless autoconfiguration on the interface configures IPv6 addresses based on prefixes received in Router Advertisement messages. A link-local address, based on the Modified EUI-64 interface ID, is automatically generated for the interface when stateless autoconfiguration is enabled.
	ipv6 address ipv6-prefix/prefix-length [eui-64] Example: hostname(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48	Assigns a global address to the interface. When you assign a global address, the link-local address is automatically created for the interface. Use the optional eui-64 keyword to use the Modified EUI-64 interface ID in the low order 64 bits of the address. See the “IPv6 Addresses” section on page B-5 for more information about IPv6 addressing.
Step 2	(Optional) ipv6 nd suppress-ra Example: hostname(config-if)# ipv6 nd suppress-ra	Suppresses Router Advertisement messages on an interface. By default, Router Advertisement messages are automatically sent in response to router solicitation messages. You may want to disable these messages on any interface for which you do not want the adaptive security appliance to supply the IPv6 prefix (for example, the outside interface).

	Command	Purpose
Step 3	(Optional) <code>ipv6 nd dad attempts value</code> Example: <pre>hostname(config-if)# ipv6 nd dad attempts 3</pre>	Changes the number of duplicate address detection attempts. The <i>value</i> argument can be any value from 0 to 600. Setting the <i>value</i> argument to 0 disables duplicate address detection on the interface. By default, the number of times an interface performs duplicate address detection is 1. See the “Information About Duplicate Address Detection” section on page 8-28 for more information.
Step 4	(Optional) <code>ipv6 nd ns-interval value</code> Example: <pre>hostname(config-if)# ipv6 nd ns-interval 2000</pre>	Changes the neighbor solicitation message interval. When you configure an interface to send out more than one duplicate address detection attempt with the <code>ipv6 nd dad attempts</code> command, this command configures the interval at which the neighbor solicitation messages are sent out. By default, they are sent out once every 1000 milliseconds. The <i>value</i> argument can be from 1000 to 3600000 milliseconds. Note Changing this value changes it for all neighbor solicitation messages sent out on the interface, not just those used for duplicate address detection.
Step 5	(Optional) <code>ipv6 enforce-eui64 if_name</code> Example: <pre>hostname(config)# ipv6 enforce-eui64 inside</pre>	Enforces the use of Modified EUI-64 format interface identifiers in IPv6 addresses on a local link. The <i>if_name</i> argument is the name of the interface, as specified by the <code>nameif</code> command, on which you are enabling the address format enforcement. See the “Information About Modified EUI-64 Interface IDs” section on page 8-29 for more information.

Allowing Same Security Level Communication

By default, interfaces on the same security level cannot communicate with each other, and packets cannot enter and exit the same interface. This section describes how to enable inter-interface communication when interfaces are on the same security level, and how to enable intra-interface communication.

Information About Inter-Interface Communication

Allowing interfaces on the same security level to communicate with each other provides the following benefits:

- You can configure more than 101 communicating interfaces.
If you use different levels for each interface and do not assign any interfaces to the same security level, you can configure only one interface per level (0 to 100).
- You want traffic to flow freely between all same security interfaces without access lists.

If you enable same security interface communication, you can still configure interfaces at different security levels as usual.

Information About Intra-Interface Communication

Intra-interface communication might be useful for VPN traffic that enters an interface, but is then routed out the same interface. The VPN traffic might be unencrypted in this case, or it might be reencrypted for another VPN connection. For example, if you have a hub and spoke VPN network, where the security appliance is the hub, and remote VPN networks are spokes, for one spoke to communicate with another spoke, traffic must go into the security appliance and then out again to the other spoke.

**Note**

All traffic allowed by this feature is still subject to firewall rules. Be careful not to create an asymmetric routing situation that can cause return traffic not to traverse the adaptive security appliance.

Restrictions

Intra-interface communication is only available in routed firewall mode. Inter-interface communication is available in both routed and transparent mode.

Detailed Steps

To enable interfaces on the same security level so that they can communicate with each other, enter the following command:

```
hostname(config)# same-security-traffic permit inter-interface
```

(Routed mode only) To enable communication between hosts connected to the same interface, enter the following command:

```
hostname(config)# same-security-traffic permit intra-interface
```

To disable these settings, use the **no** form of the command.

Enabling Jumbo Frame Support (ASA 5580)

A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. You can enable support for jumbo frames for all interfaces by increasing the amount of memory to process Ethernet frames. Assigning more memory for jumbo frames might limit the maximum use of other features, such as access lists.

**Note**

Other platform models do not support jumbo frames.

Prerequisites

In multiple context mode, set this option in the system execution space.

Detailed Steps

To enable jumbo frame support for the ASA 5580 adaptive security appliance, enter the following command:

```
hostname(config)# jumbo-frame reservation
```

To disable jumbo frames, use the **no** form of this command.

**Note**

Changes in this setting require you to reboot the adaptive security appliance.

Be sure to set the MTU for each interface that needs to transmit jumbo frames to a higher value than the default 1500; for example, set the value to 9000 using the **mtu** command. See the [“Configuring the MAC Address” section on page 8-26](#). In multiple context mode, set the MTU within each context.

Examples

The following example enables jumbo frame reservation, saves the configuration, and reloads the adaptive security appliance:

```
hostname(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

hostname(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
hostname(config)# reload
Proceed with reload? [confirm] Y
```

Monitoring Interfaces

To monitor interfaces, enter one of the following commands:

Command	Purpose
<code>show interface</code>	Displays interface statistics.
<code>show interface ip brief</code>	Displays interface IP addresses and status.

Configuration Examples for Interfaces

This section includes examples for interface configuration and includes the following topics:

- [Physical Interface Parameters Example, page 8-32](#)
- [Subinterface Parameters Example, page 8-33](#)
- [Multiple Context Mode Examples, page 8-33](#)
- [ASA 5505 Example, page 8-33](#)

Physical Interface Parameters Example

The following example configures parameters for the physical interface in single mode:

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# speed 1000
```

```
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

Subinterface Parameters Example

The following example configures parameters for a subinterface in single mode:

```
hostname(config)# interface gigabitethernet 0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# mac-address 000C.F142.4CDE standby 020C.F142.4CDE
hostname(config-subif)# no shutdown
```

Multiple Context Mode Examples

The following example configures interface parameters in multiple context mode for the system configuration, and allocates the gigabitethernet 0/1.1 subinterface to contextA:

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet 0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# no shutdown
hostname(config-subif)# context contextA
hostname(config-ctx)# ...
hostname(config-ctx)# allocate-interface gigabitethernet 0/1.1
```

The following example configures parameters in multiple context mode for the context configuration:

```
hostname/contextA(config)# interface gigabitethernet 0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
hostname/contextA(config-if)# no shutdown
```

ASA 5505 Example

The following example configures three VLAN interfaces for the Base license. The third home interface cannot forward traffic to the business interface.

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
```

```

hostname(config-if)# nameif business
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

```

Feature History for Interfaces

Table 8-1 lists the release history for this feature.

Table 8-1 Feature History for Interfaces

Feature Name	Releases	Feature Information
Increased VLANs	7.0(5)	<p>Increased the following limits:</p> <ul style="list-style-type: none"> ASA5510 Base license VLANs from 0 to 10. ASA5510 Security Plus license VLANs from 10 to 25. ASA5520 VLANs from 25 to 100. ASA5540 VLANs from 100 to 200.
Increased interfaces for the Base license on the ASA 5510	7.2(2)	<p>For the Base license on the ASA 5510, the maximum number of interfaces was increased from 3 plus a management interface to unlimited interfaces.</p>
Increased VLANs	7.2(2)	<p>The maximum number of VLANs for the Security Plus license on the ASA 5505 adaptive security appliance was increased from 5 (3 fully functional; 1 failover; one restricted to a backup interface) to 20 fully functional interfaces. In addition, the number of trunk ports was increased from 1 to 8. Now there are 20 fully functional interfaces, you do not need to use the backup interface command to cripple a backup ISP interface; you can use a fully-functional interface for it. The backup interface command is still useful for an Easy VPN configuration.</p> <p>VLAN limits were also increased for the ASA 5510 adaptive security appliance (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 adaptive security appliance (from 100 to 150), the ASA 5550 adaptive security appliance (from 200 to 250).</p>

Table 8-1 Feature History for Interfaces (continued)

Feature Name	Releases	Feature Information
Gigabit Ethernet Support for the ASA 5510 Security Plus License	7.2(3)	The ASA 5510 adaptive security appliance now supports GE (Gigabit Ethernet) for port 0 and 1 with the Security Plus license. If you upgrade the license from Base to Security Plus, the capacity of the external Ethernet0/0 and Ethernet0/1 ports increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the speed command to change the speed on the interface and use the show interface command to see what speed is currently configured for each interface.
Native VLAN support for the ASA 5505	7.2(4)/8.0(4)	You can now include the native VLAN in an ASA 5505 trunk port. The following command was introduced: switchport trunk native vlan .
Jumbo packet support for the ASA 5580	8.1(1)	The Cisco ASA 5580 supports jumbo frames. A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. You can enable support for jumbo frames for all interfaces by increasing the amount of memory to process Ethernet frames. Assigning more memory for jumbo frames might limit the maximum use of other features, such as access lists. The following command was introduced: jumbo-frame reservation .
Increased VLANs for the ASA 5580	8.1(2)	The number of VLANs supported on the ASA 5580 are increased from 100 to 250.
Support for Pause Frames for Flow Control on the ASA 5580 10 Gigabit Ethernet Interfaces	8.2(2)	You can now enable pause (XOFF) frames for flow control. The following command was introduced: flowcontrol .

