CHAPTER 11

# Completing Interface Configuration (Routed Mode)

This chapter includes tasks to complete the interface configuration for all models in routed firewall mode. This chapter includes the following sections:

**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.

## Information About Completing Interface Configuration in Routed Mode

This section includes the following topics:

### 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 11-15 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 ACL to the interface.

  If you enable communication for same security interfaces (see the "Allowing Same Security Level Communication" section on page 11-15), 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 ASA.
- 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 (IPv4 and IPv6)

The ASA 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.

# Licensing Requirements for Completing Interface Configuration in Routed Mode

| Model | License Requirement |
|---|---|
| ASA 5505 | VLANs:<br>Routed Mode:<br>Base License: 3 (2 regular zones and 1 restricted zone that can only communicate with 1 other zone)<br>Security Plus License: 20<br>Transparent Mode:<br>Base License: 2 active VLANs in 1 bridge group.<br>Security Plus License: 3 active VLANs: 2 active VLANs in 1 bridge group, and 1 active VLAN for the failover link.<br>VLAN Trunks:<br>Base License: None.<br>Security Plus License: 8. |

| Model | License Requirement |
|---|---|
| ASA 5510 | VLANs[1]:<br>Base License: 50<br>Security Plus License: 100<br>Interface Speed:<br>Base License—All interfaces Fast Ethernet.<br>Security Plus License—Ethernet 0/0 and 0/1: Gigabit Ethernet; all others Fast Ethernet.<br>Interfaces of all types[2]:<br>Base License: 364<br>Security Plus License: 564 |
| ASA 5520 | VLANs[1]:<br>Base License: 150.<br>Interfaces of all types[2]:<br>Base License: 764 |
| ASA 5540 | VLANs[1]:<br>Base License: 200<br>Interfaces of all types[2]:<br>Base License: 964 |
| ASA 5550 | VLANs[1]:<br>Base License: 400<br>Interfaces of all types[2]:<br>Base License: 1764 |

| Model | License Requirement |
|---|---|
| ASA 5580 | VLANs[1]:<br>Base License: 1024<br>Interfaces of all types[2]:<br>Base License: 4612 |
| ASA 5512-X | VLANs[1]:<br>Base License: 50<br>Security Plus License: 100<br>Interfaces of all types[2]:<br>Base License: 716<br>Security Plus License: 916 |
| ASA 5515-X | VLANs[1]:<br>Base License: 100<br>Interfaces of all types[2]:<br>Base License: 916 |
| ASA 5525-X | VLANs[1]:<br>Base License: 200<br>Interfaces of all types[2]:<br>Base License: 1316 |
| ASA 5545-X | VLANs[1]:<br>Base License: 300<br>Interfaces of all types[2]:<br>Base License: 1716 |
| ASA 5555-X | VLANs[1]:<br>Base License: 500<br>Interfaces of all types[2]:<br>Base License: 2516 |
| ASA 5585-X | VLANs[1]:<br>Base and Security Plus License: 1024<br>Interface Speed for SSP-10 and SSP-20:<br>Base License—1-Gigabit Ethernet for fiber interfaces<br>10 GE I/O License (Security Plus)—10-Gigabit Ethernet for fiber interfaces<br>(SSP-40 and SSP-60 support 10-Gigabit Ethernet by default.)<br>Interfaces of all types[2]:<br>Base and Security Plus License: 4612 |

[1] For an interface to count against the VLAN limit, you must assign a VLAN to it. For example:

```
interface gigabitethernet 0/0.100
  vlan 100
```

2. The maximum number of combined interfaces; for example, VLANs, physical, redundant, bridge group, and EtherChannel interfaces. Every **interface** command defined in the configuration counts against this limit. For example, both of the following interfaces count even if the GigabitEthernet 0/0 interface is defined as part of port-channel 1:
**interface gigabitethernet 0/0**
and
**interface port-channel 1**

| Model | License Requirement |
|---|---|
| ASA SM | VLANs:<br>Base License: 1000 |

# Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

### Context Mode Guidelines

- For the ASA 5510 and higher in multiple context mode, configure the physical interfaces in the system execution space according to Chapter 9, "Starting Interface Configuration (ASA 5510 and Higher)." Then, configure the logical interface parameters in the context execution space according to this chapter. For the ASASM in multiple context mode, configure switch ports and VLANs on the switch, and then assign VLANs to the ASASM according to Chapter 2, "Configuring the Switch for Use with the ASA Services Module."

  The ASA 5505 does not support multiple context mode.
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to the "Configuring Multiple Contexts" section on page 6-15.
- PPPoE is not supported in multiple context mode.

### Firewall Mode Guidelines

Supported in routed firewall mode. For transparent mode, see Chapter 12, "Completing Interface Configuration (Transparent Mode)."

### Failover Guidelines

Do not finish configuring failover interfaces with the procedures in this chapter. See Chapter 7, "Configuring Failover," to configure the failover and state links. In multiple context mode, failover interfaces are configured in the system configuration.

### IPv6 Guidelines

Supports IPv6.

### VLAN ID Guidelines for the ASASM

You can add any VLAN ID to the configuration, but only VLANs that are assigned to the ASA by the switch can pass traffic. To view all VLANs assigned to the ASA, use the **show vlan** command.

If you add an interface for a VLAN that is not yet assigned to the ASA by the switch, the interface will be in the down state. When you assign the VLAN to the ASA, the interface changes to an up state. See the **show interface** command for more information about interface states.

# 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 3-18.

### 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 ASA 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 for the ASASM

- In single mode or in the system execution space, VLAN interfaces are enabled by default.
- 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.

### Jumbo Frame Support

By default, the ASASM supports jumbo frames. Just configure the MTU for the desired packet size according to the "Configuring the MAC Address, MTU, and TCP MSS" section on page 11-10.

# Completing Interface Configuration in Routed Mode

This section includes the following topics:

- Task Flow for Completing Interface Configuration, page 11-7
- Configuring General Interface Parameters, page 11-7
- Configuring the MAC Address, MTU, and TCP MSS, page 11-10
- Configuring IPv6 Addressing, page 11-12
- Allowing Same Security Level Communication, page 11-15

# Task Flow for Completing Interface Configuration

**Step 1** Set up your interfaces depending on your model:

- ASA 5510 and higher—Chapter 9, "Starting Interface Configuration (ASA 5510 and Higher)."
- ASA 5505—Chapter 10, "Starting Interface Configuration (ASA 5505)."
- ASASM—Chapter 2, "Configuring the Switch for Use with the ASA Services Module."

**Step 2** (Multiple context mode) Allocate interfaces to the context according to the "Configuring Multiple Contexts" section on page 6-15.

**Step 3** (Multiple context mode) Enter the **changeto context** *name* command to change to the context you want to configure. Configure general interface parameters, including the interface name, security level, and IPv4 address. See the "Configuring General Interface Parameters" section on page 11-7.

**Step 4** (Optional) Configure the MAC address and the MTU. See the "Configuring the MAC Address, MTU, and TCP MSS" section on page 11-10.

**Step 5** (Optional) Configure IPv6 addressing. See the "Configuring IPv6 Addressing" section on page 11-12.

**Step 6** (Optional) Allow same security level communication, either by allowing communication between two interfaces or by allowing traffic to enter and exit the same interface. See the "Allowing Same Security Level Communication" section on page 11-15.

# 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
- EtherChannel interfaces

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

- VLAN interfaces

## Guidelines and Limitations

- For the ASA 5550, 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.
- If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and Stateful Failover communications. See Chapter 7, "Configuring Failover," to configure the failover and state links.

## Restrictions

- PPPoE is not supported in multiple context mode.
- PPPoE and DHCP are not supported on the ASASM.

## Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5510 and higher—Chapter 9, "Starting Interface Configuration (ASA 5510 and Higher)."
  - ASA 5505—Chapter 10, "Starting Interface Configuration (ASA 5505)."
  - ASASM—Chapter 2, "Configuring the Switch for Use with the ASA Services Module."
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to the "Configuring Multiple Contexts" section on page 6-15.
- 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.

## Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | For the ASA 5510 and higher:<br>**interface** {{**redundant** *number* \| **port-channel** *number* \| *physical_interface*}[.*subinterface*] \| *mapped_name*}<br>For the ASA 5505 or ASASM:<br>`ciscoasa(config)#` **interface** {**vlan** *number* \| *mapped_name*}<br>**Example:**<br>`ciscoasa(config)# interface gigabitethernet 0/0` | If you are not already in interface configuration mode, enters interface configuration mode.<br>The **redundant** *number* argument is the redundant interface ID, such as **redundant 1**.<br>The **port-channel** *number* argument is the EtherChannel interface ID, such as **port-channel 1**.<br>See the "Enabling the Physical Interface and Configuring Ethernet Parameters" section for a description of the physical interface ID.<br>Append the *subinterface* ID to the physical or redundant interface ID separated by a period (.).<br>In multiple context mode, enter the *mapped_name* if one was assigned using the **allocate-interface** command. |
| **Step 2** | **nameif** *name*<br>**Example:**<br>`ciscoasa(config-if)# nameif inside` | Names the interface.<br>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 3** | Do one of the following: | |

| | Command | Purpose |
|---|---|---|
| | **ip address** *ip_address* [*mask*] [**standby** *ip_address*]<br>**Example:**<br>`ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2` | Sets the IP address manually.<br>**Note** For use with failover, you must set the IP address and standby address manually; DHCP and PPPoE are not supported.<br>The *ip_address* and *mask* arguments set the interface IP address and subnet mask.<br>The **standby** *ip_address* argument is used for failover. See the "Configuring Active/Standby Failover" section on page 7-26 or the "Configuring Active/Active Failover" section on page 7-30 for more information. |
| | **ip address dhcp** [**setroute**]<br>**Example:**<br>`ciscoasa(config-if)# ip address dhcp` | Obtains an IP address from a DHCP server.<br>The **setroute** keyword lets the ASA use the default route supplied by the DHCP server.<br>Reenter this command to reset the DHCP lease and request a new lease.<br>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 9, "Configuring the PPPoE Client," in the VPN configuration guide. | PPPoE is not supported in multiple context mode. |
| **Step 4** | **security-level** *number*<br>**Example:**<br>`ciscoasa(config-if)# security-level 50` | Sets the security level, where *number* is an integer between 0 (lowest) and 100 (highest). See the "Security Levels" section on page 11-1. |
| **Step 5** | (Optional)<br>**management-only**<br>**Example:**<br>`ciscoasa(config-if)# management-only` | Sets an interface to management-only mode so that it does not pass through traffic.<br>By default, Management interfaces are configured as management-only. To disable this setting, enter the **no management-only** command.<br>(ASA 5512-X through ASA 5555-X) You cannot disable **management-only** on the Management 0/0 interface.<br>The **management-only** command is not supported for a redundant interface. |

## Example

The following example configures parameters for VLAN 101:

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

The following example configures parameters in multiple context mode for the context configuration. The interface ID is a mapped name.

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

### What to Do Next

- (Optional) Configure the MAC address and the MTU. See the "Configuring the MAC Address, MTU, and TCP MSS" section on page 11-10.
- (Optional) Configure IPv6 addressing. See the "Configuring IPv6 Addressing" section on page 11-12.

## Configuring the MAC Address, MTU, and TCP MSS

This section describes how to configure MAC addresses for interfaces, how to set the MTU, and set the TCP MSS.

### 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.

For the ASASM, all VLANs use the same MAC address provided by the backplane.

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.

For an EtherChannel, all interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. The port-channel interface uses the lowest numbered channel group interface MAC address as the port-channel MAC address. Alternatively you can manually configure a MAC address for the port-channel interface. In multiple context mode, you can automatically assign unique MAC addresses to interfaces, including an EtherChannel port interface. We recommend manually, or in multiple context mode, automatically configuring a unique MAC address in case the group channel interface membership changes. If you remove the interface that was providing the port-channel MAC address, then the port-channel MAC address changes to the next lowest numbered interface, thus causing traffic disruption.

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 ASA 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 ASA Classifies Packets" section on page 6-3 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 6-24 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.

### Information About the MTU and TCP MSS

See the "Controlling Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size" section on page 9-8.

### Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5510 and higher—Chapter 9, "Starting Interface Configuration (ASA 5510 and Higher)."
  - ASA 5505—Chapter 10, "Starting Interface Configuration (ASA 5505)."
  - ASASM—Chapter 2, "Configuring the Switch for Use with the ASA Services Module."
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to the "Configuring Multiple Contexts" section on page 6-15.
- 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.
- To increase the MTU above 1500, enable jumbo frames on supported models according to the "Enabling Jumbo Frame Support (Supported Models)" section on page 9-35. Jumbo frames are supported by default on the ASASM; you do not need to enable them.

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | For the ASA 5510 and higher:<br>**interface** {{**redundant** *number* \| **port-channel** *number* \| *physical_interface*}[**.***subinterface*] \| *mapped_name*}<br>For the ASA 5505 or ASASM:<br>`ciscoasa(config)#` **interface** {**vlan** *number* \| *mapped_name*}<br>**Example:**<br>`ciscoasa(config)# interface vlan 100` | If you are not already in interface configuration mode, enters interface configuration mode.<br>The **redundant** *number* argument is the redundant interface ID, such as **redundant 1**.<br>The **port-channel** *number* argument is the EtherChannel interface ID, such as **port-channel 1**.<br>See the "Enabling the Physical Interface and Configuring Ethernet Parameters" section for a description of the physical interface ID.<br>Append the *subinterface* ID to the physical or redundant interface ID separated by a period (.).<br>In multiple context mode, enter the *mapped_name* if one was assigned using the **allocate-interface** command. |
| **Step 2** | **mac-address** *mac_address* [**standby** *mac_address*]<br>**Example:**<br>`ciscoasa(config-if)# mac-address 000C.F142.4CDE` | Assigns a private MAC address to this interface. 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.<br>The first two bytes of a manual MAC address cannot be A2 if you also want to use auto-generated MAC addresses.<br>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. |

| | Command | Purpose |
|---|---|---|
| **Step 3** | **mtu** *interface_name bytes*<br>**Example:**<br>`ciscoasa(config)# mtu inside 9200` | Sets the MTU between 300 and 65,535 bytes. The default is 1500 bytes.<br>**Note** When you set the MTU for a redundant or port-channel interface, the ASA applies the setting to all member interfaces.<br>For models that support jumbo frames, if you enter a value for any interface that is greater than 1500, then you need to enable jumbo frame support. See the "Enabling Jumbo Frame Support (Supported Models)" section on page 9-35. |
| **Step 4** | **sysopt connection tcpmss** [**minimum**] *bytes*<br>**Example:**<br>`ciscoasa(config)# sysopt connection tcpmss 8500`<br>`ciscoasa(config)# sysopt connection tcpmss minimum 1290` | Sets the maximum TCP segment size in bytes, between 48 and any maximum number. The default value is 1380 bytes. You can disable this feature by setting bytes to **0**.<br>For the **minimum** keyword, sets the maximum segment size to be no less than *bytes*, between 48 and 65535. The minimum feature is disabled by default (set to 0). |

### What to Do Next

(Optional) Configure IPv6 addressing. See the "Configuring IPv6 Addressing" section on page 11-12.

# Configuring IPv6 Addressing

This section describes how to configure IPv6 addressing. For more information about IPv6, see the "IPv6 Addresses" section on page 49-5.

This section includes the following topics:

- Information About IPv6, page 11-12
- Configuring a Global IPv6 Address, page 11-13
- Configuring IPv6 Neighbor Discovery, page 11-15

## Information About IPv6

This section includes information about how to configure IPv6, and includes the following topics:

- IPv6 Addressing, page 11-12
- Modified EUI-64 Interface IDs, page 11-13

### IPv6 Addressing

You can configure two types of unicast addresses for IPv6:

- Global—The global address is a public address that you can use on the public network.
- Link-local—The link-local address is a private address that you can only use on the directly-connected network. Routers do not forward packets using link-local addresses; they are only for communication on a particular physical network segment. They can be used for address configuration or for the ND functions such as address resolution and neighbor discovery.

At a minimum, you need to configure a link-local address for IPv6 to operate. If 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. If you do not configure a global address, then you need to configure the link-local address, either automatically or manually.

**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 command reference.

### 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 ASA can enforce this requirement for hosts attached to the local link.

When this feature 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.

## Configuring a Global IPv6 Address

To configure a global IPv6 address, perform the following steps.

**Note** Configuring the global address automatically configures the link-local address, so you do not need to configure it separately.

### Restrictions

The ASA does not support IPv6 anycast addresses.

### Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5510 and higher—Chapter 9, “Starting Interface Configuration (ASA 5510 and Higher).”
  - ASA 5505—Chapter 10, “Starting Interface Configuration (ASA 5505).”
  - ASASM—Chapter 2, “Configuring the Switch for Use with the ASA Services Module.”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to the “Configuring Multiple Contexts” section on page 6-15.
- 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.

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | For the ASA 5510 and higher:<br>`interface {{redundant number \| port-channel number \| physical_interface}[.subinterface] \| mapped_name}`<br>For the ASA 5505 or ASASM:<br>`ciscoasa(config)# interface {vlan number \| mapped_name}`<br>**Example:**<br>`ciscoasa(config)# interface gigabitethernet 0/0` | If you are not already in interface configuration mode, enters interface configuration mode.<br>The **redundant** *number* argument is the redundant interface ID, such as **redundant 1**.<br>The **port-channel** *number* argument is the EtherChannel interface ID, such as **port-channel 1**.<br>See the "Enabling the Physical Interface and Configuring Ethernet Parameters" section for a description of the physical interface ID.<br>Append the *subinterface* ID to the physical or redundant interface ID separated by a period (.).<br>In multiple context mode, enter the *mapped_name* if one was assigned using the **allocate-interface** command. |
| **Step 2** | Do one of the following: | |
| | `ipv6 address autoconfig`<br>**Example:**<br>`ciscoasa(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.<br>**Note** Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the ASA does send Router Advertisement messages in this case. See the **ipv6 nd suppress-ra** command to suppress messages. |
| | `ipv6 address ipv6-address/prefix-length [standby ipv6-address]`<br>**Example:**<br>`ciscoasa(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.<br>**standby** specifies the interface address used by the secondary unit or failover group in a failover pair.<br>See the "IPv6 Addresses" section on page 49-5 for more information about IPv6 addressing. |

| | Command | Purpose |
|---|---|---|
| | **ipv6 address** *ipv6-prefix/prefix-length* **eui-64**<br>**Example:**<br>`ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98::/48 eui-64` | Assigns a global address to the interface by combining the specified prefix with an interface ID generated from the interface MAC address using the Modified EUI-64 format. When you assign a global address, the link-local address is automatically created for the interface.<br>You do not need to specify the standby address; the interface ID will be generated automatically.<br>See the "IPv6 Addresses" section on page 49-5 for more information about IPv6 addressing. |
| **Step 3** | (Optional)<br>**ipv6 enforce-eui64** *if_name*<br>**Example:**<br>`ciscoasa(config)# ipv6 enforce-eui64 inside` | Enforces the use of Modified EUI-64 format interface identifiers in IPv6 addresses on a local link.<br>The *if_name* argument is the name of the interface, as specified by the **nameif** command, on which you are enabling the address format enforcement.<br>See the "Modified EUI-64 Interface IDs" section on page 11-13 for more information. |

## Configuring IPv6 Neighbor Discovery

See Chapter 31, "Configuring IPv6 Neighbor Discovery," to configure IPv6 neighbor discovery.

# 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 ACLs.

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

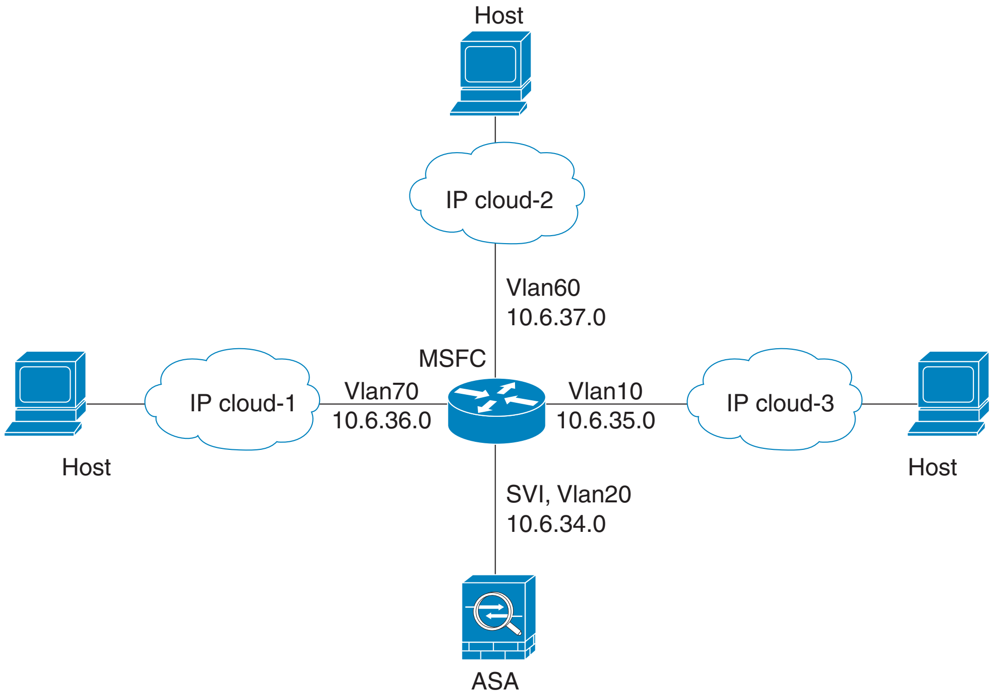
### Information About Intra-Interface Communication

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 ASA is the hub, and remote VPN networks are spokes, for one spoke to communicate with another spoke, traffic must go into the ASA 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 ASA.

For the ASASM, before you can enable this feature, you must first correctly configure the MSFC so that packets are sent to the ASA MAC address instead of being sent directly through the switch to the destination host. Figure 11-1 shows a network where hosts on the same interface need to communicate.

***Figure 11-1 Communication Between Hosts on the Same Interface***



The following sample configuration shows the Cisco IOS **route-map** commands used to enable policy routing in the network shown in Figure 11-1:

```
route-map intra-inter3 permit 0
    match ip address 103
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
    match ip address 102
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
    match ip address 101
    set interface Vlan20
    set ip next-hop 10.6.34.7
```

### Detailed Steps

| Command | Purpose |
|---|---|
| **`same-security-traffic permit inter-interface`** | Enables interfaces on the same security level so that they can communicate with each other. |
| **`same-security-traffic permit intra-interface`** | Enables communication between hosts connected to the same interface. |

# Turning Off and Turning On Interfaces

This section describes how to turn off and on an interface.

All interfaces are enabled by default. In multiple context mode, if you disable or reenable the interface within a context, only that context interface is affected. But if you disable or reenable the interface in the system execution space, then you affect that interface for all contexts.

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | `ciscoasa(config)#` **`interface`** `{`**`vlan`** *`number`* `\|` *`mapped_name`*`}`<br>**Example:**<br>`ciscoasa(config)# interface vlan 100` | If you are not already in interface configuration mode, enters interface configuration mode.<br>In multiple context mode, enter the *mapped_name* if one was assigned using the **allocate-interface** command. |
| **Step 2** | **`shutdown`**<br>**Example:**<br>`ciscoasa(config-if)# shutdown` | Disables the interface. |
| **Step 3** | **`no shutdown`**<br>**Example:**<br>`ciscoasa(config-if)# no shutdown` | Reenables the interface. |

# Monitoring Interfaces

To monitor interfaces, enter one of the following commands:

| Command | Purpose |
|---|---|
| **`show interface`** | Displays interface statistics. |
| **`show interface ip brief`** | Displays interface IP addresses and status. |

# Configuration Examples for Interfaces in Routed Mode

This section includes the following topics:

- ASA 5505 Example, page 11-18

## 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.

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

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif business
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

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

# Feature History for Interfaces in Routed Mode

Table 11-1 lists the release history for this feature.

*Table 11-1 Feature History for Interfaces*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Increased VLANs | 7.0(5) | Increased the following limits:<br>• ASA5510 Base license VLANs from 0 to 10.<br>• ASA5510 Security Plus license VLANs from 10 to 25.<br>• ASA5520 VLANs from 25 to 100.<br>• ASA5540 VLANs from 100 to 200. |
| Increased VLANs | 7.2(2) | The maximum number of VLANs for the Security Plus license on the ASA 5505 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.<br>VLAN limits were also increased for the ASA 5510 (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 (from 100 to 150), the ASA 5550 (from 200 to 250). |
| Gigabit Ethernet Support for the ASA 5510 Security Plus License | 7.2(3) | The ASA 5510 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.<br>We introduced the following command: **switchport trunk native vlan**. |

*Table 11-1 Feature History for Interfaces (continued)*

| Feature Name | Releases | Feature Information |
|---|---|---|
| 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 ACLs.<br>We introduced the following command: **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. |
| IPv6 support for transparent mode | 8.2(1) | IPv6 support was introduced for transparent firewall mode. |
| 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.<br>We introduced the following command: **flowcontrol**. |