



# CHAPTER 9

## 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 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 1-1.

---

This chapter includes the following sections:

- [Information About Interfaces](#), page 9-1
- [Licensing Requirements for Interfaces](#), page 9-6
- [Guidelines and Limitations](#), page 9-7
- [Default Settings](#), page 9-7
- [Starting Interface Configuration \(ASA 5510 and Higher\)](#), page 9-8
- [Starting Interface Configuration \(ASA 5505\)](#), page 9-15
- [Completing Interface Configuration \(All Models\)](#), page 9-20
- [Allowing Same Security Level Communication](#), page 9-31
- [Enabling Jumbo Frame Support \(ASA 5580, Multiple Mode\)](#), page 9-32
- [Monitoring Interfaces](#), page 9-32
- [Feature History for Interfaces](#), page 9-33

## Information About Interfaces

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

- [ASA 5505 Interfaces](#), page 9-2
- [Auto-MDI/MDIX Feature](#), page 9-4
- [Security Levels](#), page 9-5

- [Dual IP Stack](#), page 9-5
- [Management Interface \(ASA 5510 and Higher\)](#), page 9-6

## ASA 5505 Interfaces

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

- [Understanding ASA 5505 Ports and Interfaces](#), page 9-2
- [Maximum Active VLAN Interfaces for Your License](#), page 9-2
- [VLAN MAC Addresses](#), page 9-4
- [Power Over Ethernet](#), page 9-4

### Understanding ASA 5505 Ports and Interfaces

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

- Physical switch ports—The 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 9-4](#) 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 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 9-1](#) for more information.
- Security Plus license—20 active VLANs.

**Note**

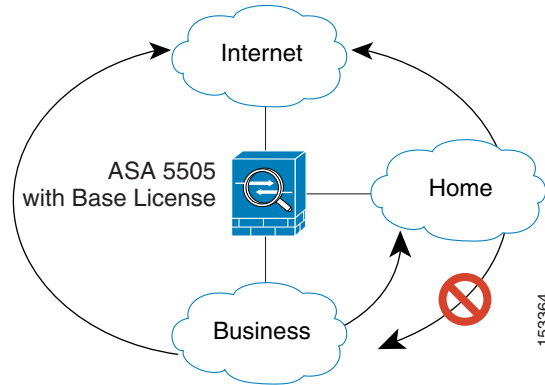
---

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 9-1](#) for an example network where the Home VLAN can communicate with the Internet, but cannot initiate contact with Business.

**Figure 9-1** 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.

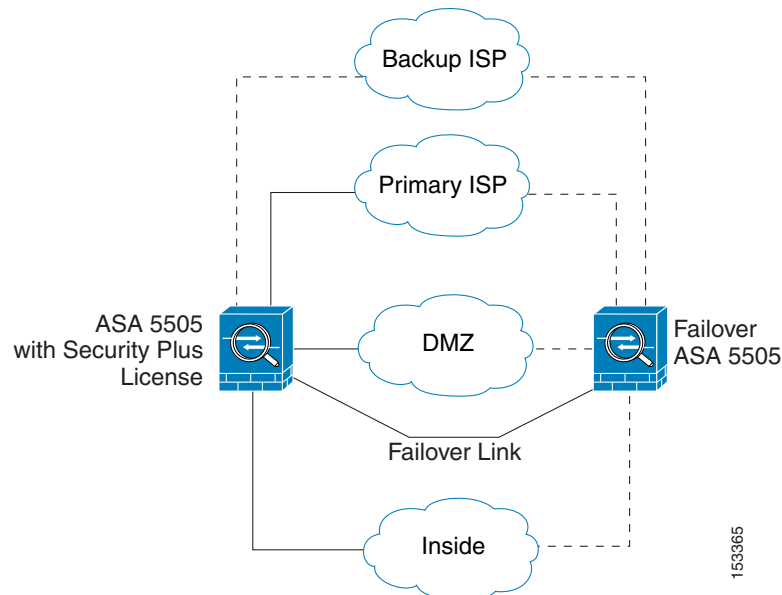


**Note**

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

See [Figure 9-2](#) for an example network.

**Figure 9-2** 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 Advanced Interface Parameters” section on page 9-25](#).
- 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 Advanced Interface Parameters” section on page 9-25](#).

## 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 security appliance does not supply power to the switch ports.

If you shut down the switch port, you disable power to the device. Power is restored when you enable the port. See the [“Configuring and Enabling Switch Ports as Access Ports” section on page 9-18](#) for more information about shutting down a switch port.

## 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.

You can only enable SPAN monitoring using the Command Line Interface tool by entering the **switchport monitor** command. See the **switchport monitor** command in the *Cisco ASA 5500 Series Command Reference* for more information.

## ASA 5580 Interfaces

The ASA 5580 security appliance supports multiple types of Ethernet interfaces including Gigabit Ethernet and 10-Gigabit Ethernet speeds, and copper and fiber connectors. See the *Cisco ASA 5580 Adaptive Security Appliance Getting Started Guide* for detailed information about the interface adapters available for the ASA 5580 security appliance, and which slots support each adapter type.

## Auto-MDI/MDIX Feature

For RJ-45 interfaces on the ASA 5500 series security appliance, 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. 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.

## 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 9-31](#) 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 9-31](#)), 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 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.

- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- **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 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 a Fast Ethernet interface designed for management traffic only. You can, however, use it for through traffic if desired. 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 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 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
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 9-8](#).

Then, configure the logical interface parameters in the context execution space according to the [“Completing Interface Configuration \(All Models\)” section on page 9-20](#).

## Firewall Mode Guidelines

Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA 5510 and higher 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.

## Failover Guidelines

Do not finish configuring failover interfaces with the procedures in [“Completing Interface Configuration \(All Models\)” section on page 9-20](#). See the [“Failover Link Configuration” section on page 17-10](#) and [“State Link Configuration” section on page 17-11](#) 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 8-3](#).

## Model Guidelines

Subinterfaces are not available for the ASA 5505 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 1-1](#).

## 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 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 security appliance and the 4GE SSM for the ASA 5510 and higher security appliance include two connector types: copper RJ-45 and fiber SFP. RJ-45 is the default. You can configure the 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. If you are not already in the system execution space, in the Configuration > Device List pane, double-click **System** under the active device IP address.

For ASA 5505 configuration, see the “[Starting Interface Configuration \(ASA 5505\)](#)” section on [page 9-15](#).

This section includes the following topics:

- [Task Flow for Starting Interface Configuration](#), page 9-9
- [Configuring a Redundant Interface](#), page 9-11
- [Enabling the Physical Interface and Configuring Ethernet Parameters](#), page 9-9
- [Configuring VLAN Subinterfaces and 802.1Q Trunking](#), page 9-14

- [Assigning Interfaces to Contexts and Automatically Assigning MAC Addresses \(Multiple Context Mode\)](#), page 9-15

## 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. If you are not already in the System configuration mode, in the Configuration > Device List pane, double-click **System** under the active device IP address.
- Step 2** Enable the physical interface, and optionally change Ethernet parameters. See the “[Enabling the Physical Interface and Configuring Ethernet Parameters](#)” section on page 9-9.
- Physical interfaces are disabled by default.
- Step 3** (Optional) Configure redundant interface pairs. See the “[Configuring a Redundant Interface](#)” section on page 9-11.
- 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 9-14.
- 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 9-15.
- Step 6** Complete the interface configuration according to the “[Completing Interface Configuration \(All Models\)](#)” section on page 9-20.
- 

## 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. If you are not already in the System configuration mode, in the Configuration > Device List pane, double-click **System** under the active device IP address.

### Detailed Steps

- 
- Step 1** Depending on your context mode:
- For single mode, choose the **Configuration > Device Setup > Interfaces** pane.

- For multiple mode in the System execution space, choose the **Configuration > Context Management > Interfaces** pane.

By default, all physical interfaces are listed.

**Step 2** Click a physical interface that you want to configure, and click **Edit**.

The Edit Interface dialog box appears.

**Step 3** To enable the interface, check the **Enable Interface** check box.

**Step 4** To add a description, enter text in the Description field.

The description can be up to 240 characters on a single line, without carriage returns. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.

**Step 5** (Optional) To set the media type, duplex, and speed, or for the ASA 5580 10 Gigabit Ethernet interface, enable pause frames for flow control, click **Configure Hardware Properties**.

- If you have an ASA 5550 adaptive security appliance or a 4GE SSM, you can choose either **RJ-45** or **SFP** from the Media Type drop-down list.

RJ-45 is the default.

- To set the duplex for RJ-45 interfaces, choose **Full**, **Half**, or **Auto**, depending on the interface type, from the Duplex drop-down list.
- To set the speed, choose a value from the Speed drop-down list.

The speeds available depend on the interface type. For SFP interfaces, you can set the speed to Negotiate or Nonnegotiate. Negotiate (the default) enables link negotiation, which exchanges flow-control parameters and remote fault information. Nonnegotiate does not negotiate link parameters. For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. See the “[Auto-MDI/MDIX Feature](#)” section on page 9-4.

- For the ASA 5580 10 Gigabit Ethernet interfaces, to enable pause (XOFF) frames for flow control on 10 Gigabit Ethernet interfaces, check the **Enable Pause Frame** check box.

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 Watermark. The default 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 Watermark. By default, the 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 Pause Time value in the pause frame. The default value is 26624; you can set it between 0 and 65535. If the buffer usage is consistently above the High Watermark, pause frames are sent repeatedly, controlled by the pause refresh threshold value.

To change the default values for the Low Watermark, High Watermark, and Pause Time, uncheck the **Use Default Values** check box.



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

- Click **OK** to accept the Hardware Properties changes.

**Step 6** Click **OK** to accept the Interface changes.

---

## What to Do Next

Optional Tasks:

- Configure redundant interface pairs. See the “[Configuring a Redundant Interface](#)” section on page 9-11.
- Configure VLAN subinterfaces. See the “[Configuring VLAN Subinterfaces and 802.1Q Trunking](#)” section on page 9-14.

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 9-15.
- For single context mode, complete the interface configuration. See the “[Completing Interface Configuration \(All Models\)](#)” section on page 9-20.

## 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 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 9-11](#)
- [Changing the Active Interface, page 9-13](#)

## 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 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 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 9-9).
- 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.
- 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 Advanced Interface Parameters”](#) section on page 9-25 or the [“Assigning Interfaces to Contexts and Automatically Assigning MAC Addresses \(Multiple Context Mode\)”](#) section on page 9-15). 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 in the Configuration > Device Setup > Interfaces pane.
- For multiple context mode, complete this procedure in the system execution space. If you are not already in the System configuration mode, in the Configuration > Device List pane, double-click **System** under the active device IP address.



### 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** Depending on your context mode:
- For single mode, choose the **Configuration > Device Setup > Interfaces** pane.
  - For multiple mode in the System execution space, choose the **Configuration > Context Management > Interfaces** pane.
- Step 2** Click **Add > Redundant Interface**.
- The Add Redundant Interface dialog box appears.
- Step 3** In the Redundant ID field, enter an integer between 1 and 8.
- Step 4** From the Primary Interface drop-down list, choose the physical interface you want to be primary.

Be sure to pick an interface that does not have a subinterface and that has not already been allocated to a context.

- Step 5** From the Secondary Interface drop-down list, choose the physical interface you want to be secondary.
- Step 6** If the interface is not already enabled, check the **Enable Interface** check box.  
The interface is enabled by default. To disable it, uncheck the check box.
- Step 7** To add a description, enter text in the Description field.  
The description can be up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.
- Step 8** Click **OK**.  
You return to the Interfaces pane.
- 

## What to Do Next

Optional Task:

- Configure VLAN subinterfaces. See the [“Configuring VLAN Subinterfaces and 802.1Q Trunking” section on page 9-14](#).

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 9-15](#).
- For single context mode, complete the interface configuration. See the [“Completing Interface Configuration \(All Models\)” section on page 9-20](#).

## 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 in the Tools > Command Line Interface tool:

```
show interface redundant $number$  detail | grep Member
```

For example:

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

To change the active interface, enter the following command:

```
redundant-interface redundant $number$  active-member  $physical\_interface$ 
```

where the **redundant $number$**  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 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 9-6](#).
- **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 not configuring a name for the interface. If you want to let the physical or redundant interface pass untagged packets, you can configure the name as usual. See the [“Completing Interface Configuration \(All Models\)” section on page 9-20](#) for more information about completing the interface configuration.

### Prerequisites

For multiple context mode, complete this procedure in the system execution space. If you are not already in the System configuration mode, in the Configuration > Device List pane, double-click **System** under the active device IP address.

### Detailed Steps

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

- 
- Step 1** Depending on your context mode:
- For single mode, choose the **Configuration > Device Setup > Interfaces** pane.
  - For multiple mode in the System execution space, choose the **Configuration > Context Management > Interfaces** pane.
- Step 2** Click **Add > Interface**.  
The Add Interface dialog box appears.
- Step 3** From the Hardware Port drop-down list, choose the physical interface to which you want to add the subinterface.
- Step 4** If the interface is not already enabled, check the **Enable Interface** check box.  
The interface is enabled by default. To disable it, uncheck the check box.
- Step 5** In the VLAN ID field, enter the VLAN ID between 1 and 4095.  
Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. For multiple context mode, you can only set the VLAN in the system configuration.
- Step 6** In the Subinterface ID field, enter the subinterface ID as an integer between 1 and 4294967293.

The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it.

**Step 7** (Optional) In the Description field, enter a description for this interface.

The description can be up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.

**Step 8** Click **OK**.

You return to the Interfaces pane.

---

### 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 9-15.
- For single context mode, complete the interface configuration. See the [“Completing Interface Configuration \(All Models\)”](#) section on page 9-20.

## 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 11, “Configuring Security Contexts”](#):

- To assign interfaces to contexts, see the [“Configuring Security Contexts”](#) section on page 11-16.
- (Optional) To automatically assign unique MAC addresses to context interfaces, see the [“Automatically Assigning MAC Addresses”](#) section on page 11-18.

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 Advanced Interface Parameters”](#) section on page 9-25.

### What to Do Next

Complete the interface configuration. See the [“Completing Interface Configuration \(All Models\)”](#) section on page 9-20.

## Starting Interface Configuration (ASA 5505)

This section includes tasks for starting your interface configuration for the ASA 5505 security appliance, including creating VLAN interfaces and assigning them to switch ports. See the [“Understanding ASA 5505 Ports and Interfaces”](#) section on page 9-2 for more information.

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

This section includes the following topics:

- [Task Flow for Starting Interface Configuration, page 9-16](#)
- [Configuring VLAN Interfaces, page 9-16](#)
- [Configuring and Enabling Switch Ports as Access Ports, page 9-18](#)
- [Configuring and Enabling Switch Ports as Trunk Ports, page 9-19](#)

## 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 9-16](#).
  - Step 2** Configure and enable switch ports as access ports. See the [“Configuring and Enabling Switch Ports as Access Ports” section on page 9-18](#).
  - 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 9-19](#).
  - Step 4** Complete the interface configuration according to the [“Completing Interface Configuration \(All Models\)” section on page 9-20](#).
- 

## 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 9-2](#).

### Detailed Steps

**Note**

If you enabled Easy VPN, you cannot add or delete VLAN interfaces, nor can you edit the security level or interface name. We suggest that you finalize your interface configuration before you enable Easy VPN.

---

- 
- Step 1** Choose the **Configuration > Device Setup > Interfaces** pane.
  - Step 2** On the Interfaces tab, click **Add**.  
The Add Interface dialog box appears with the General tab selected.
  - Step 3** In the Available Switch Ports pane, choose a switch port, and click **Add**.  
You see the following message:  
*“switchport is associated with name interface. Adding it to this interface, will remove it from name interface. Do you want to continue?”*  
Click **OK** to add the switch port.  
You will always see this message when adding a switch port to an interface; switch ports are assigned to the VLAN 1 interface by default even when you do not have any configuration.  
Repeat for any other switch ports that you want to carry this VLAN.



---

**Note** Removing a switch port from an interface essentially just reassigns that switch port to VLAN 1, because the default VLAN interface for switch ports is VLAN 1.

---

**Step 4** Click the **Advanced** tab.



---

**Note** You receive an error message about setting the IP address. You can either set the IP address and other parameters now, or you can finish configuring the VLAN and switch ports by clicking **Yes**, and later set the IP address and other parameters according to the [“Completing Interface Configuration \(All Models\)”](#) section on page 9-20.

---

**Step 5** In the VLAN ID field, enter the VLAN ID for this interface, between 1 and 4090.

If you do not want to assign the VLAN ID, ASDM assigns one for you randomly.

**Step 6** (Optional for the Base license) To allow this interface to be the third VLAN by limiting it from initiating contact to one other VLAN, in the Block Traffic From this Interface to drop-down list, choose the VLAN 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 this option 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 name, be sure to configure this setting before setting the name on the third interface; the security appliance does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505 security appliance.



---

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

To configure the MAC address and MTU, see the [“Configuring Advanced Interface Parameters”](#) section on page 9-25.

---

**Step 7** Click **OK**.

---

## What to Do Next

Configure the switch ports. See the [“Configuring and Enabling Switch Ports as Access Ports”](#) section on page 9-18 and the [“Configuring and Enabling Switch Ports as Trunk Ports”](#) section on page 9-19.

## 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 9-19](#). If you have a factory default configuration, see the [“ASA 5505 Default Configuration” section on page 1-2](#) 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 9-2](#).

**Caution**

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

### Detailed Steps

**Step 1** Choose the **Configuration > Device Setup > Interfaces** pane.

**Step 2** Click the **Switch Ports** tab.

**Step 3** Click the switch port you want to edit.

The Edit Switch Port dialog box appears.

**Step 4** To enable the switch port, check the **Enable SwitchPort** check box.

**Step 5** In the Mode and VLAN IDs area, click the **Access** radio button.

**Step 6** In the VLAN ID field, enter the VLAN ID associated with this switch port. The VLAN ID can be between 1 and 4090.

By default, the VLAN ID is derived from the VLAN interface configuration you completed in [“Configuring VLAN Interfaces” section on page 9-16](#) (on the Configuration > Device Setup > Interfaces > Interfaces > Add/Edit Interface dialog box). You can change the VLAN assignment in this dialog box. Be sure to apply the change to update the VLAN configuration with the new information. If you want to specify a VLAN that has not yet been added, we suggest you add the VLAN according to the [“Configuring VLAN Interfaces” section on page 9-16](#) rather than specifying it in this dialog box; in either case, you need to add the VLAN according to the [“Configuring VLAN Interfaces” section on page 9-16](#) and assign the switch port to it.

**Step 7** (Optional) To prevent the switch port from communicating with other protected switch ports on the same VLAN, check the **Isolated** check box.

This option prevents the switch port from communicating with other protected switch ports on the same VLAN. 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 Protected option 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 8** (Optional) From the Duplex drop-down list, choose **Full**, **Half**, or **Auto**.

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 9** (Optional) From the Speed drop-down list, choose **10**, **100**, or **Auto**.

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 10** Click **OK**.

---

## 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 9-19](#).

To complete the interface configuration, see the [“Completing Interface Configuration \(All Models\)” section on page 9-20](#).

## Configuring and Enabling Switch Ports as Trunk Ports

This procedure tells 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 9-18](#).

For more information about ASA 5505 interfaces, see the [“ASA 5505 Interfaces” section on page 9-2](#).

## Detailed Steps

---

**Step 1** Choose the **Configuration > Device Setup > Interfaces** pane.

**Step 2** Click the **Switch Ports** tab.

**Step 3** Click the switch port you want to edit.  
The Edit Switch Port dialog box appears.

**Step 4** To enable the switch port, check the **Enable SwitchPort** check box.

**Step 5** In the Mode and VLAN IDs area, click the **Trunk** radio button.

**Step 6** In the VLAN IDs field, enter the VLAN IDs associated with this switch port, separated by commas. The VLAN ID can be between 1 and 4090.

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

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

If the VLANs are already in your configuration, after you apply the change, the Configuration > Device Setup > Interfaces > Interfaces tab shows this switch port added to each VLAN. If you want to specify a VLAN that has not yet been added, we suggest you add the VLAN according to the [“Configuring VLAN Interfaces” section on page 9-16](#) rather than specifying it in this dialog box; in either case, you need to add the VLAN according to the [“Configuring VLAN Interfaces” section on page 9-16](#) and assign the switch port to it.

**Step 7** To configure the native VLAN, check the **Configure Native VLAN** check box, and enter the VLAN ID in the Native VLAN ID field. The VLAN ID can be 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.

**Step 8** (Optional) To prevent the switch port from communicating with other protected switch ports on the same VLAN, check the **Isolated** check box.

This option prevents the switch port from communicating with other protected switch ports on the same VLAN. 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 Protected option 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 9** (Optional) From the Duplex drop-down list, choose **Full**, **Half**, or **Auto**.

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 10** (Optional) From the Speed drop-down list, choose **10**, **100**, or **Auto**.

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 11** Click **OK**.

## What to Do Next

To complete the interface configuration, see the [“Completing Interface Configuration \(All Models\)” section on page 9-20](#).

# 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. In the Configuration > Device List pane, double-click the context name under the active device IP address.

This section includes the following topics:

- [Configuring General Interface Parameters, page 9-21](#)
- [Configuring Advanced Interface Parameters, page 9-25](#)
- [Configuring IPv6 Addressing, page 9-26](#)
- [Configuring the Link-Local Address on an Interface \(Transparent Firewall Mode\), page 9-30](#)

## Task Flow for Completing Interface Configuration

- 
- Step 1** Complete the procedures in the “[Starting Interface Configuration \(ASA 5510 and Higher\)](#)” section on page 9-8 or the “[Starting Interface Configuration \(ASA 5505\)](#)” section on page 9-15.
- Step 2** (Multiple context mode) In the Configuration > Device List pane, double-click the context name under the active device IP address.
- Step 3** Configure general interface parameters, including the interface name, security level, and IPv4 address. See the “[Configuring General Interface Parameters](#)” section on page 9-21.
- 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 9-22). 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 Management IP Address for Transparent Firewall Mode](#)” section on page 8-1.
- Step 4** (Optional) Configure the MAC address and the MTU. See the “[Configuring Advanced Interface Parameters](#)” section on page 9-25.
- Step 5** (Optional) Configure IPv6 addressing. See the “[Configuring IPv6 Addressing](#)” section on page 9-26
- 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 9-22). This section includes how to set the link-local address in transparent mode, but this task is usually not required. To set the global management address for transparent mode, see the “[Configuring the Management IP Address for Transparent Firewall Mode](#)” section on page 8-1.
- 

## 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 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 9-5.
- 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 “[Failover Link Configuration](#)” section on page 17-10 and “[State Link Configuration](#)” section on page 17-11 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 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 security appliance or context management IP address, see the [“Configuring the Management IP Address for Transparent Firewall Mode”](#) section on page 8-1. 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 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 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 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 9-8 or the [“Starting Interface Configuration \(ASA 5505\)”](#) section on page 9-15.
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, in the Configuration > Device List pane, double-click the context name under the active device IP address.

## Detailed Steps

- 
- Step 1** Choose the **Configuration > Device Setup > Interfaces** pane.  
For the ASA 5505, the Interfaces tab shows by default.
- Step 2** Choose the interface row, and click **Edit**.  
The Edit Interface dialog box appears with the General tab selected.
- Step 3** In the Interface Name field, enter a name up to 48 characters in length.
- Step 4** In the Security level field, enter a level between 0 (lowest) and 100 (highest).  
See the [“Security Levels”](#) section on page 9-5 for more information.
- Step 5** (Optional) To set this interface as a management-only interface, check the **Dedicate this interface to management-only** check box.  
Through traffic is not accepted on a management-only interface. For the ASA 5510 and higher, see the [“Information About the Management Interface”](#) section on page 9-22 for more information.
- Step 6** If the interface is not already enabled, check the **Enable Interface** check box.
- Step 7** To set the IP address, one of the following options.

**Note**

For use with failover, you must set the IP address and standby address manually; DHCP and PPPoE are not supported. Set the standby IP addresses on the Configuration > Device Management > High Availability > Failover > Interfaces tab

In transparent firewall mode, do not set the IP address for each interface, but rather set it for the whole 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, click the **Use Static IP** radio button and enter the IP address and mask.
- To obtain an IP address from a DHCP server, click the **Obtain Address via DHCP** radio button.
  - a. (Optional) To force a MAC address to be stored inside a DHCP request packet for option 61 instead of the default internally-generated string, click the **Use MAC Address** radio button.

Some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned.

- b. (Optional) To obtain the default route from the DHCP server, check **Obtain Default Route Using DHCP**.
- c. (Optional) To assign an administrative distance to the learned route, enter a value between 1 and 255 in the DHCP Learned Route Metric field. If this field is left blank, the administrative distance for the learned routes is 1.
- d. (Optional) To enable tracking for DHCP-learned routes, check **Enable Tracking for DHCP Learned Routes**. Set the following values:

Track ID—A unique identifier for the route tracking process. Valid values are from 1 to 500.

Track IP Address—Enter the IP address of the target being tracked. Typically, this would be the IP address of the next hop gateway for the route, but it could be any network object available off of that interface.

**Note**

Route tracking is only available in single, routed mode.

SLA ID—A unique identifier for the SLA monitoring process. Valid values are from 1 to 2147483647.

Monitor Options—Click this button to open the Route Monitoring Options dialog box. In the Route Monitoring Options dialog box you can configure the parameters of the tracked object monitoring process.

- e. (Optional) To renew the lease, click **Renew DHCP Lease**.
- (Single, routed mode only) To obtain an IP address using PPPoE, check **Use PPPoE**.
    - a. In the Group Name field, specify a group name.
    - b. In the PPPoE Username field, specify the username provided by your ISP.
    - c. In the PPPoE Password field, specify the password provided by your ISP.
    - d. In the Confirm Password field, retype the password.
    - e. For PPP authentication, click either the **PAP**, **CHAP**, or **MSCHAP** radio button.

PAP passes cleartext username and password during authentication and is not secure. With CHAP, the client returns the encrypted [challenge plus password], with a cleartext username in response to the server challenge. CHAP is more secure than PAP, but it does not encrypt data. MSCHAP is similar to CHAP but is more secure because the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. MSCHAP also generates a key for data encryption by MPPE.

- f. (Optional) To store the username and password in Flash memory, check the **Store Username and Password in Local Flash** check box.

The security appliance stores the username and password in a special location of NVRAM. If an Auto Update Server sends a **clear configure** command to the security appliance, and the connection is then interrupted, the security appliance can read the username and password from NVRAM and re-authenticate to the Access Concentrator.

- g. (Optional) To display the PPPoE IP Address and Route Settings dialog box where you can choose addressing and tracking options, click **IP Address and Route Settings**. See the “[PPPoE IP Address and Route Settings](#)” section on page 9-24 for more information.

**Step 8** (Optional) In the Description field, enter a description for this interface.

The description can be up to 240 characters on a single line, without carriage returns. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.



**Note** (ASA 5510 and higher) For information about the Configure Hardware Properties button, see the “[Enabling the Physical Interface and Configuring Ethernet Parameters](#)” section on page 9-9.

**Step 9** Click **OK**.

## What to Do Next

- (Optional) Configure the MAC address and MTU. See the “[Configuring Advanced Interface Parameters](#)” section on page 9-25.
- (Optional) Configure IPv6 addressing. See the “[Configuring IPv6 Addressing](#)” section on page 9-26

## PPPoE IP Address and Route Settings

The Configuration > Interfaces > Add/Edit Interface > General > PPPoE IP Address and Route Settings > PPPoE IP Address and Route Settings dialog box lets you choose addressing and tracking options for PPPoE connections.

### Fields

- IP Address area—Lets you choose between Obtaining an IP address using PPP or specifying an IP address, and contains the following fields:
  - Obtain IP Address using PPP—Select to enable the security appliance to use PPP to get an IP address.
  - Specify an IP Address—Specify an IP address and mask for the security appliance to use instead of negotiating with the PPPoE server to assign an address dynamically.

- Route Settings Area—Lets you configure route and tracking settings and contains the following fields:
  - Obtain default route using PPPoE—Sets the default routes when the PPPoE client has not yet established a connection. When using this option, you cannot have a statically defined route in the configuration.
  - PPPoE learned route metric—Assigns an administrative distance to the learned route. Valid values are from 1 to 255. If this field is left blank, the administrative distance for the learned routes is 1.
  - Enable tracking—Check this check box to enable route tracking for PPPoE-learned routes.




---

**Note** Route tracking is only available in single, routed mode.

---

- Primary Track—Select this option to configure the primary PPPoE route tracking.
- Track ID—A unique identifier for the route tracking process. Valid values are from 1 to 500.
- Track IP Address—Enter the IP address of the target being tracked. Typically, this would be the IP address of the next hop gateway for the route, but it could be any network object available off of that interface.
- SLA ID—A unique identifier for the SLA monitoring process. Valid values are from 1 to 2147483647.
- Monitor Options—Click this button to open the Route Monitoring Options dialog box. In the Route Monitoring Options dialog box you can configure the parameters of the tracked object monitoring process.
- Secondary Track—Select this option to configure the secondary PPPoE route tracking.
- Secondary Track ID—A unique identifier for the route tracking process. Valid values are from 1 to 500.

## Configuring Advanced Interface Parameters

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

### 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 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 11-2](#) 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” section on page 11-18](#) 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.

## Detailed Steps

- 
- Step 1** Choose the **Configuration > Device Setup > Interfaces** pane.  
For the ASA 5505, the Interfaces tab shows by default.
- Step 2** Choose the interface row, and click **Edit**.  
The Edit Interface dialog box appears with the General tab selected.
- Step 3** Click the **Advanced** tab.
- Step 4** To set the MTU or to enable jumbo frame support (ASA 5580 only), enter the value in the MTU field, between 300 and 65,535 bytes.  
The default is 1500 bytes.
- For the ASA 5580 in single mode—If you enter a value for any interface that is greater than 1500, then you enable jumbo frame support automatically for all interfaces. If you set the MTU for all interfaces back to a value under 1500, then jumbo frame support is disabled.
  - For the ASA 5580 in multiple mode—If you enter a value for any interface that is greater than 1500, then be sure to enable jumbo frame support in the system configuration. See the [“Enabling Jumbo Frame Support \(ASA 5580, Multiple Mode\)”](#) section on page 9-32.




---

**Note** Enabling or disabling jumbo frame support requires you to reboot the security appliance.

---

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. Jumbo frames require extra memory to process, and assigning more memory for jumbo frames might limit the maximum use of other features, such as access lists.

- Step 5** To manually assign a MAC address to this interface, enter a MAC address in the Active Mac Address field in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 00C.F142.4CDE.
- Step 6** If you use failover, enter the standby MAC address in the Standby Mac Address field. 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 9-26

## Configuring IPv6 Addressing

This section describes how to configure IPv6 addressing. For more information about IPv6, see 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 Management IP Address for Transparent Firewall Mode” section on page 8-1](#). If you do not configure a management address, you can configure the link-local addresses in transparent mode according to the [“Configuring the Link-Local Address on an Interface \(Transparent Firewall Mode\)” section on page 9-30](#).

### 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.

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 on 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:

```
%PIX|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 addresses associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

The 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 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:

```
%PIX|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.

## Restrictions

The security appliance does not support IPv6 anycast addresses.

## Detailed Steps

- 
- Step 1** Choose the **Configuration > Device Setup > Interfaces** pane.
- Step 2** Choose an interface, and click **Edit**.
- The Edit Interface dialog box appears with the General tab selected.
- Step 3** Click the **IPv6** tab.
- Step 4** (Optional) To enforce the use of Modified EUI-64 format interface identifiers in IPv6 addresses on a local link, check the **Enforce EUI-64** check box.
- If the interface identifiers do not conform to the modified EUI-64 format, an error message appears. See the [“Information About Modified EUI-64 Interface IDs”](#) section on page 9-28 for more information.
- Step 5** Configure the global IPv6 address using one of the following methods.



**Note** If you do not want to configure a global IPv6 address, you can configure the link-local addresses either automatically by checking the **Enable IPv6** check box, or manually by entering a value in the Link-local address field in the Interface IPv6 Addresses area. A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. See the [“IPv6 Addresses”](#) section on page B-5 for more information about IPv6 addressing.

If you configure a global IPv6 address (or manually configure a link-local address), checking or unchecking the **Enable IPv6** check box does not affect how IPv6 operates; IPv6 continues to be enabled.

- Stateless autoconfiguration—In the Interface IPv6 Addresses area, check the **Enable address autoconfiguration** check box.

Enabling stateless autoconfiguration on the interface configures IPv6 addresses based upon 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.

- Manual configuration—To manually configure a global IPv6 address:
  - a. In the Interface IPv6 Addresses area, click **Add**.  
The Add IPv6 Address for Interface dialog box appears.
  - b. In the Address/Prefix Length field, enter the global IPv6 address and the IPv6 prefix length. For example, 2001:0DB8::BA98:0:3210/48. See the “IPv6 Addresses” section on page B-5 for more information about IPv6 addressing.
  - c. (Optional) To use the Modified EUI-64 interface ID in the low order 64 bits of the address, check the **EUI-64** check box.
  - d. Click **OK**.

**Step 6** (Optional) In the top area, customize the IPv6 configuration by configuring the following options:

- DAD Attempts—This setting configures the number of consecutive neighbor solicitation messages that are sent on an interface while DAD is performed on IPv6 addresses. Valid values are from 0 to 600. A zero value disables DAD processing on the specified interface. The default is one message.
- NS Interval—Enter the neighbor solicitation message interval. The neighbor solicitation message requests the link-layer address of a target node. Valid values are from 1000 to 3600000 milliseconds. The default is 1000 milliseconds.
- Reachable Time—Enter the amount of time in seconds that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred. Valid values are from 0 to 3600000 milliseconds. The default is zero. A configured time enables the detection of unavailable neighbors. Shorter times enable detection more quickly; however, very short configured times are not recommended in normal IPv6 operation.
- RA Lifetime—Enter the amount of time that IPv6 router advertisement transmissions are considered valid. Valid values are from 0 to 9000 seconds. The default is 1800 seconds. Router advertisement transmissions include a preference level and a lifetime field for each advertised router address. These transmissions provide route information and indicate that the router is still operational to network hosts.
- RA Interval—Enter the interval between IPv6 router advertisement transmissions. Valid values are from 3 to 1800 seconds. The default is 200 seconds. To list the router advertisement transmission interval in milliseconds, check the **RA Interval in Milliseconds** check box. Valid values are from 500 to 1800000 milliseconds.
- To allow the generation of addresses for hosts, make sure that the Suppress RA check box is unchecked. This is the default setting if IPv6 unicast routing is enabled. To prevent the generation of IPv6 router advertisement transmissions, check the **Suppress RA** check box.

**Step 7** (Optional) To configure which IPv6 prefixes are included in IPv6 router advertisements, complete the following.

By default, prefixes configured as addresses on an interface are advertised in router advertisements. If you configure prefixes for advertisement using this area, then only these prefixes are advertised.

- a. In the Interface IPv6 Prefixes area, click **Add**.  
The Add IPv6 Prefix for Interface dialog box appears.

- b. In the Address/Prefix Length field, enter the IPv6 address with the prefix length. To configure settings that apply to all prefixes, check the **Default Values** check box instead of entering an Address.
- c. (Optional) To indicate that the IPv6 prefix is not advertised, check the **No Advertisements** check box.
- d. (Optional) To indicate that the specified prefix is not used for on-link determination, check the **Off-link** check box.
- e. (Optional) To indicate to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration, check the **No Auto-Configuration** check box.
- f. In the Prefix Lifetime area, choose one of the following:
  - Lifetime Duration—Specify the following:
 

A valid lifetime for the prefix in seconds from the drop-down list. This setting is the amount of time that the specified IPv6 prefix is advertised as being valid. The maximum value represents infinity. Valid values are from 0 to 4294967295. The default is 2592000 (30 days).

A preferred lifetime for the prefix from the drop-down list. This setting is the amount of time that the specified IPv6 prefix is advertised as being preferred. The maximum value represents infinity. Valid values are from 0 to 4294967295. The default setting is 604800 (seven days).
  - Lifetime Expiration Date—Specify the following:
 

Choose a valid month and day from the drop-down list, and then enter a time in hh:mm format.

Choose a preferred month and day from the drop-down list, and then enter a time in hh:mm format.

**Step 8** Click **OK**.

You return to the Edit Interface dialog box.

**Step 9** Click **OK**.

You return to the Configuration > Device Setup > Interfaces pane.

## Configuring the Link-Local Address on an Interface (Transparent Firewall Mode)

If you only need to configure a link-local address and are not going to assign any other IPv6 addresses, you have the option of manually defining the link-local address.

To assign a link-local address to an interface, perform the following steps:

**Step 1** Choose the **Configuration > Device Setup > Interfaces** pane.

**Step 2** Select an interface, and click **Edit**.

The Edit Interface dialog box appears with the General tab selected.

**Step 3** Click the **IPv6** tab.

**Step 4** (Optional) To enforce the use of Modified EUI-64 format interface identifiers in IPv6 addresses on a local link, check the **Enforce EUI-64** check box.

If the interface identifiers do not conform to the modified EUI-64 format, an error message appears. See the [“Information About Modified EUI-64 Interface IDs”](#) section on page 9-28 for more information.

**Step 5** To set the link-local address, enter an address in the Link-local address field.

A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. See the “[IPv6 Addresses](#)” section on page B-5 for more information about IPv6 addressing.

**Step 6** Click **OK**.

---

## 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.

**Note**

If you enable NAT control, you do not need to configure NAT between same security level interfaces. See the “[NAT and Same Security Level Interfaces](#)” section on page 22-12 for more information on NAT and same security level interfaces.

---

### 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 security appliance.

---

### Restrictions

This feature is only available in routed firewall mode.

### Detailed Steps

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

- To enable interfaces on the same security level to communicate with each other, from the Configuration > Interfaces pane, check **Enable traffic between two or more interfaces which are configured with same security level**.
- To enable communication between hosts connected to the same interface, check **Enable traffic between two or more hosts connected to the same interface**.

## Enabling Jumbo Frame Support (ASA 5580, Multiple Mode)

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. In single mode, setting the MTU larger than 1500 bytes automatically enables jumbo frames.

### Detailed Steps

To enable jumbo frame support, choose the **Configuration > Context Management > Interfaces pane**, and click the **Enable jumbo frame support** check box.

**Note**

---

Changes in this setting require you to reboot the 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. See the [“Configuring Advanced Interface Parameters” section on page 9-25](#). Set the MTU within each context.

---

## Monitoring Interfaces

To monitor interfaces, see [Chapter 42, “Monitoring Interfaces.”](#)

# Feature History for Interfaces

Table 9-1 lists the release history for this feature.

**Table 9-1** Feature History for Interfaces

Feature Name	Releases	Feature Information
Increased VLANs	7.0(5)	Increased the following limits: <ul style="list-style-type: none"> <li>• ASA5510 Base license VLANs from 0 to 10.</li> <li>• ASA5510 Security Plus license VLANs from 10 to 25.</li> <li>• ASA5520 VLANs from 25 to 100.</li> <li>• ASA5540 VLANs from 100 to 200.</li> </ul>
Increased VLANs	7.2(2)	The maximum number of VLANs for the Security Plus license on the ASA 5505 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.  VLAN limits were also increased for the ASA 5510 security appliance (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 security appliance (from 100 to 150), the ASA 5550 security appliance (from 200 to 250).
Gigabit Ethernet Support for the ASA 5510 Security Plus License	7.2(3)	The ASA 5510 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 <b>speed</b> command to change the speed on the interface and use the <b>show interface</b> 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 using the <b>switchport trunk native vlan</b> command.

Table 9-1 Feature History for Interfaces (continued)

Feature Name	Releases	Feature Information
Gigabit Ethernet Support for the ASA 5510 Base License	7.2(4)/8.0(4)	The ASA 5510 security appliance now supports GE (Gigabit Ethernet) for port 0 and 1 in the Base license (support was previously added for the Security Plus license). 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 <b>speed</b> command to change the speed on the interface and use the <b>show interface</b> command to see what speed is currently configured for each interface.
Jumbo packet support for the ASA 5580	8.1(1)	The Cisco ASA 5580 supports jumbo frames when you enter the <b>jumbo-frame reservation</b> command. 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.  In ASDM, see Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced.
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 screens were modified: (Single Mode) Configuration > Device Setup > Interfaces > Add/Edit Interface > General, (Multiple Mode, System) Configuration > Interfaces > Add/Edit Interface.