Starting Interface Configuration (ASA 5505)

This chapter includes tasks for starting your interface configuration for the ASA 5505, including creating VLAN interfaces and assigning them to switch ports.

For ASA 5510 and higher configuration, see the "Feature History for ASA 5505 Interfaces" section on page 10-13.

This chapter includes the following sections:

Information About ASA 5505 Interfaces

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

Understanding ASA 5505 Ports and Interfaces

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

- Physical switch ports—The ASA 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 10-4 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 ASA applies the security policy to the traffic and routes or bridges between the two VLANs.

Maximum Active VLAN Interfaces for Your License

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

- Base license—3 active VLANs. The third VLAN can only be configured to initiate traffic to one other VLAN. See Figure 10-1 for more information.
- Security Plus license—20 active VLANs.

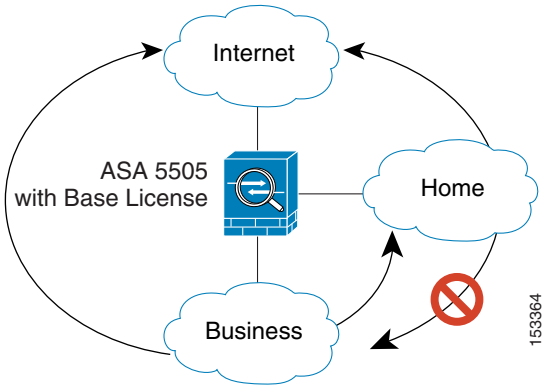
In transparent firewall mode, you can configure the following VLANs depending on your license:

- Base license—2 active VLANs in 1 bridge group.
- Security Plus license—3 active VLANs: 2 active VLANs in 1 bridge group, and 1 active VLAN for the failover link.

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

With the Base license in routed mode, the third VLAN can only be configured to initiate traffic to one other VLAN. See Figure 10-1 for an example network where the Home VLAN can communicate with the Internet, but cannot initiate contact with Business.

Figure 10-1 ASA 5505 with Base License

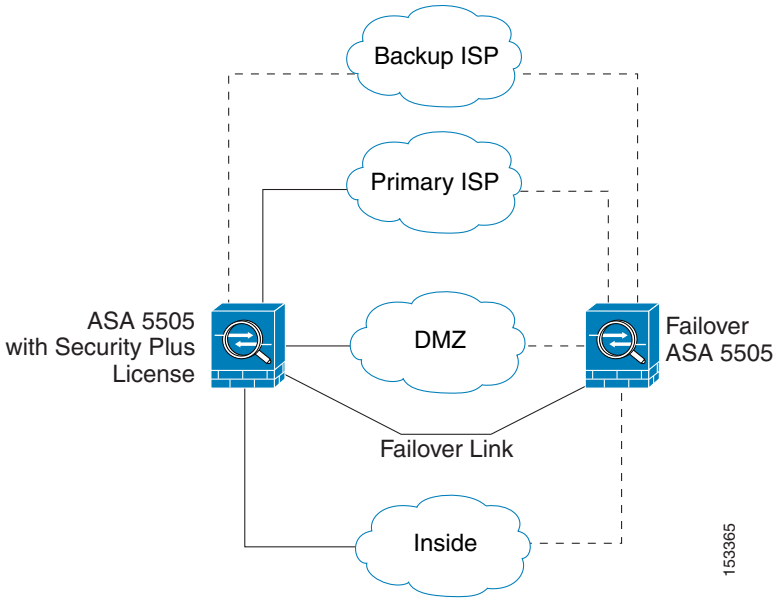


With the Security Plus license, you can configure 20 VLAN interfaces in routed mode, including a VLAN interface for failover and a VLAN interface as a backup link to your ISP. You can configure the backup interface to not pass through traffic unless the route through the primary interface fails. You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

Note The ASA 5505 supports Active/Standby failover, but not Stateful Failover.

See Figure 10-2 for an example network.

Figure 10-2 ASA 5505 with Security Plus License



VLAN MAC Addresses

- Routed firewall mode—All VLAN interfaces share a MAC address. Ensure that any connected switches can support this scenario. If the connected switches require unique MAC addresses, you can manually assign MAC addresses. See the "Configuring the MAC Address, MTU, and TCP MSS" section on page 11-10.
- Transparent firewall mode—Each VLAN has a unique MAC address. You can override the generated MAC addresses if desired by manually assigning MAC addresses. See the "Configuring the MAC Address, MTU, and TCP MSS" section on page 12-13.

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 ASA does not supply power to the switch ports.

If you shut down the switch port using the **shutdown** command, you disable power to the device. Power is restored when you enable the port using the **no shutdown** command. See the "Configuring and Enabling Switch Ports as Access Ports" section on page 10-7 for more information about shutting down a switch port.

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

Monitoring Traffic Using SPAN

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

See the **switchport monitor** command in the command reference for more information.

Auto-MDI/MDIX Feature

All ASA 5505 interfaces include 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. You cannot disable Auto-MDI/MDIX.

Licensing Requirements for ASA 5505 Interfaces

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

Guidelines and Limitations

Context Mode Guidelines

The ASA 5505 does not support multiple context mode.

Firewall Mode Guidelines

- In transparent mode, you can configure up to eight bridge groups. Note that you must use at least one bridge group; data interfaces must belong to a bridge group.
- Each bridge group can include up to four VLAN interfaces, up to the license limit.

Failover Guidelines

Active/Standby failover is only supported with the Security Plus license. Active/Active failover is not supported.

IPv6 Guidelines

Supports IPv6.

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 State of Interfaces

Interfaces have the following default states:

- Switch ports—Disabled.

- VLANs—Enabled. However, for traffic to pass through the VLAN, the switch port must also be enabled.

Default Speed and Duplex

By default, the speed and duplex are set to auto-negotiate.

Starting ASA 5505 Interface Configuration

This section includes the following topics:

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 10-6.

Step 2 Configure and enable switch ports as access ports. See the "Configuring and Enabling Switch Ports as Access Ports" section on page 10-7.

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 10-9.

Step 4 Complete the interface configuration according to Chapter 11, "Completing Interface Configuration (Routed Mode)," or Chapter 12, "Completing Interface Configuration (Transparent Mode)."

Configuring VLAN Interfaces

This section describes how to configure VLAN interfaces. For more information about ASA 5505 interfaces, see the "Information About ASA 5505 Interfaces" section on page 10-1.

Guidelines

We suggest that you finalize your interface configuration before you enable Easy VPN.

Detailed Steps

	Command	Purpose
Step 1	**interface vlan** *number* **Example:** `ciscoasa(config)# interface vlan 100`	Adds a VLAN interface, where the *number* is between 1 and 4090. To remove this VLAN interface and all associated configuration, enter the **no interface vlan** command. Because this interface also includes the interface name configuration, and the name is used in other commands, those commands are also removed.
Step 2	(Optional for the Base license) **no forward interface vlan** *number* **Example:** `ciscoasa(config-if)# no forward interface vlan 101`	Allows this interface to be the third VLAN by limiting it from initiating contact to one other VLAN. The *number* specifies the VLAN ID to which this VLAN interface cannot initiate traffic. With the Base license, you can only configure a third VLAN if you use this command to limit it. For example, you have one VLAN assigned to the outside for Internet access, one VLAN assigned to an inside business network, and a third VLAN assigned to your home network. The home network does not need to access the business network, so you can use the **no forward interface** command on the home VLAN; the business network can access the home network, but the home network cannot access the business network. If you already have two VLAN interfaces configured with a **nameif** command, be sure to enter the **no forward interface** command before the **nameif** command on the third interface; the ASA does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505. **Note** If you upgrade to the Security Plus license, you can remove this command and achieve full functionality for this interface. If you leave this command in place, this interface continues to be limited even after upgrading.

What to Do Next

Configure the switch ports. See the "Configuring and Enabling Switch Ports as Access Ports" section on page 10-7 and the "Configuring and Enabling Switch Ports as Trunk Ports" section on page 10-9.

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 10-9. If you have a factory default configuration, see the "ASA 5505 Default Configuration" section on page 3-20 to check if you want to change the default interface settings according to this procedure.

For more information about ASA 5505 interfaces, see the "Information About ASA 5505 Interfaces" section on page 10-1.

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

Detailed Steps

	Command	Purpose
Step 1	**interface ethernet0/***port* **Example:** `ciscoasa(config)# interface ethernet0/1`	Specifies the switch port you want to configure, where *port* is 0 through 7.
Step 2	**switchport access vlan** *number* **Example:** `ciscoasa(config-if)# switchport access vlan 100`	Assigns this switch port to a VLAN, where *number* is the VLAN ID, between 1 and 4090. See the "Configuring VLAN Interfaces" section on page 10-6 to configure the VLAN interface that you want to assign to this switch port. To view configured VLANs, enter the **show interface** command. **Note** You might assign multiple switch ports to the primary or backup VLANs if the Internet access device includes Layer 2 redundancy.
Step 3	(Optional) **switchport protected** **Example:** `ciscoasa(config-if)# switchport protected`	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 **switchport protected** command to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.
Step 4	(Optional) **speed** {**auto** | **10** | **100**} **Example:** `ciscoasa(config-if)# speed 100`	Sets the speed. The **auto** setting is the default. If you set the speed to anything other than **auto** on PoE ports Ethernet 0/6 or 0/7, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.
Step 5	(Optional) **duplex** {**auto** | **full** | **half**} **Example:** `ciscoasa(config-if)# duplex full`	Sets the duplex. The **auto** setting is the default. If you set the duplex to anything other than **auto** on PoE ports Ethernet 0/6 or 0/7, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.
Step 6	**no shutdown** **Example:** `ciscoasa(config-if)# no shutdown`	Enables the switch port. To disable the switch port, enter the **shutdown** command.

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 10-9.
- To complete the interface configuration, see Chapter 11, "Completing Interface Configuration (Routed Mode)," or Chapter 12, "Completing Interface Configuration (Transparent Mode)."

Configuring and Enabling Switch Ports as Trunk Ports

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

To create an access port, where an interface is assigned to only one VLAN, see the "Configuring and Enabling Switch Ports as Access Ports" section on page 10-7.

Guidelines

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

Detailed Steps

	Command	Purpose
Step 1	**interface ethernet0/***port* **Example:** `ciscoasa(config)# interface ethernet0/1`	Specifies the switch port you want to configure, where *port* is 0 through 7.
Step 2	To assign VLANs to this trunk, do one or more of the following:	
	switchport trunk allowed vlan *vlan_range* **Example:** `ciscoasa(config)# switchport trunk allowed vlan 100-200`	Identifies one or more VLANs that you can assign to the trunk port, where the *vlan_range* (with VLANs between 1 and 4090) can be identified in one of the following ways: • A single number (n) • A range (n-x) • Separate numbers and ranges by commas, for example: 5,7-10,13,45-100 You can enter spaces instead of commas, but the command is saved to the configuration with commas. You can include the native VLAN in this command, but it is not required; the native VLAN is passed whether it is included in this command or not.

	Command	Purpose
	switchport trunk native vlan *vlan_id* **Example:** `ciscoasa(config-if)# switchport trunk native vlan 100`	Assigns a native VLAN to the trunk, where the *vlan_id* is a single VLAN ID between 1 and 4090. Packets on the native VLAN are not modified when sent over the trunk. For example, if a port has VLANs 2, 3 and 4 assigned to it, and VLAN 2 is the native VLAN, then packets on VLAN 2 that egress the port are not modified with an 802.1Q header. Frames which ingress (enter) this port and have no 802.1Q header are put into VLAN 2. Each port can only have one native VLAN, but every port can have either the same or a different native VLAN.
Step 3	**switchport mode trunk** **Example:** `ciscoasa(config-if)# switchport mode trunk`	Makes this switch port a trunk port. To restore this port to access mode, enter the **switchport mode access** command.
Step 4	(Optional) **switchport protected** **Example:** `ciscoasa(config-if)# switchport protected`	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 **switchport protected** command to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.
Step 5	(Optional) **speed** {**auto** | **10** | **100**} **Example:** `ciscoasa(config-if)# speed 100`	Sets the speed. 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 6	(Optional) **duplex** {**auto** | **full** | **half**} **Example:** `ciscoasa(config-if)# duplex full`	Sets the duplex. 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 7	**no shutdown** **Example:** `ciscoasa(config-if)# no shutdown`	Enables the switch port. To disable the switch port, enter the **shutdown** command.

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 ASA 5505 Interfaces

This section includes the following topics:

Access Port Example

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

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

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

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

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

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

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

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
```

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

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

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

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

Trunk Port Example

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

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

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

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

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

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

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

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

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
```

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

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

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

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

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

Where to Go Next

Complete the interface configuration according to Chapter 11, "Completing Interface Configuration (Routed Mode)," or Chapter 12, "Completing Interface Configuration (Transparent Mode)."

Feature History for ASA 5505 Interfaces

Table 10-1 lists the release history for this feature.

Table 10-1 Feature History for Interfaces

Feature Name	Releases	Feature Information
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.
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. We introduced the following command: **switchport trunk native vlan**.