



CHAPTER 4

Configuring Ethernet Settings, Redundant Interfaces, and Subinterfaces

This chapter describes how to configure and enable physical Ethernet interfaces, how to create redundant interface pairs, and how to add subinterfaces.

- In single context mode, complete the procedures in this chapter and then continue your interface configuration in [Chapter 6, “Configuring Interface Parameters.”](#)
- In multiple context mode, complete the procedures in this chapter in the system execution space, then assign interfaces and subinterfaces to contexts according to [Chapter 5, “Adding and Managing Security Contexts,”](#) and finally configure the interface parameters within each context according to [Chapter 6, “Configuring Interface Parameters.”](#)

This chapter includes the following sections:

- [Configuring and Enabling Interfaces, page 4-1](#)
- [Configuring a Redundant Interface, page 4-3](#)
- [Configuring VLAN Subinterfaces and 802.1Q Trunking, page 4-6](#)
- [Enabling Jumbo Frame Support, page 4-8](#)

Configuring and Enabling Interfaces

This section describes how to configure Ethernet settings for physical interfaces, and how to enable the interface. It includes the following topics:

- [Interface Overview, page 4-1](#)
- [Configuring the Interface, page 4-2](#)

Interface Overview

This section describes the interfaces available, and includes the following topics:

- [Ethernet Adapter Support, page 4-2](#)
- [Default State of Physical Interfaces, page 4-2](#)
- [Auto-MDI/MDIX Feature, page 4-2](#)

Ethernet Adapter Support

The ASA 5580 adaptive 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 5500 Series Adaptive Security Appliance Getting Started Guide* for detailed information about the interface adapters available for the ASA 5580 adaptive security appliance, and which slots support each adapter type.

Depending on the type of Ethernet interface, you might have different physical options to configure.

Default State of Physical Interfaces

By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through it (either alone or as part of a redundant interface pair), or through a subinterface. For multiple context mode, if you allocate an interface (physical, redundant, or subinterface) to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must first enable the physical interface in the system configuration according to this procedure.

By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.

For fiber interfaces, the speed is set for automatic link negotiation.

Auto-MDI/MDIX Feature

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

Configuring the Interface

To enable the interface, or to set a specific speed and duplex, perform the following steps:

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

```
hostname(config)# interface physical_interface slot/port
hostname(config-if)#
```

The physical interface types include the following:

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

The space is optional between the interface type and the *slot/port*. For example, both of these forms are accepted at the CLI, but the command is saved to the configuration without the space:

```
interface gigabitethernet 3/1
interface gigabitethernet3/1
```

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* for detailed information about the interface adapters available for the ASA 5580 adaptive security appliance, and which slots support each adapter type.

The management interfaces are built-in Gigabit Ethernet interfaces designed for management traffic only, and they are specified as **management0/0** and **management0/1**. You can, however, use the management interfaces for through traffic if desired (see the **management-only** command). Management interfaces are not designed to support maximum throughput, however, so for a high-traffic solution, use the Ethernet adapter interfaces for through traffic. In transparent firewall mode, you can use the management interfaces (for management purposes) in addition to the two interfaces allowed for through traffic. You can also add subinterfaces to the management interfaces to provide management in each security context for multiple context mode.



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

Step 2 (Optional) To set the speed for copper interfaces, enter the following command:

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

The default setting is **auto**.

Step 3 (Optional) To set the duplex for copper interfaces, enter the following command:

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

The **auto** setting is the default.

Step 4 To enable the interface, enter the following command:

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

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

Configuring a Redundant Interface

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. You can configure a redundant interface to increase the adaptive security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. You can configure up to 8 redundant interface pairs.

All adaptive security appliance configuration refers to the logical redundant interface instead of the member physical interfaces.

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

- [Redundant Interface Overview](#), page 4-4
- [Adding a Redundant Interface](#), page 4-5
- [Changing the Active Interface](#), page 4-6

Redundant Interface Overview

This section includes overview information about redundant interfaces, and includes the following topics:

- [Default State of Redundant Interfaces](#), page 4-4
- [Redundant Interfaces and Failover Guidelines](#), page 4-4
- [Redundant Interface MAC Address](#), page 4-4
- [Physical Interface Guidelines](#), page 4-5

Default State of Redundant Interfaces

When you add a redundant interface, it is enabled by default. However, the member interfaces must also be enabled to pass traffic.

Redundant Interfaces and Failover Guidelines

Follow these guidelines when adding member interfaces:

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

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 Interface Parameters”](#) section on page 6-2 or the [“Automatically Assigning MAC Addresses to Context Interfaces”](#) section on page 5-11). When the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.

Physical Interface Guidelines

Follow these guidelines when adding member interfaces:

- Both member interfaces must be of the same physical type. For example, both must be Ethernet.
- You cannot add a physical interface to the redundant interface if you configured a name for it. You must first remove the name using the **no nameif** command.



Caution

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

- The only configuration available to physical interfaces that are part of a redundant interface pair are physical parameters (set in the “[Configuring and Enabling Interfaces](#)” section on page 4-1), the **description** command, and the **shutdown** command. You can also enter run-time commands like **default** and **help**.
- If you shut down the active interface, then the standby interface becomes active.

Adding a Redundant Interface

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

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

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

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

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

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

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

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

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

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

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

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

Step 4 To enable the interface (if you previously disabled it), enter the following command:

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

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

The following example creates two redundant interfaces:

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

Changing the Active Interface

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

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

For example:

```
hostname# show interface redundant1 detail | grep Member
Members GigabitEthernet3/3(Active), GigabitEthernet3/2
```

To change the active interface, enter the following command:

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

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

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

Configuring VLAN Subinterfaces and 802.1Q Trunking

This section describes how to configure a subinterface, and includes the following topics:

- [Subinterface Overview, page 4-6](#)
- [Adding a Subinterface, page 4-7](#)

Subinterface Overview

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

This section includes the following topics:

- [Default State of Subinterfaces, page 4-7](#)
- [Maximum Subinterfaces, page 4-7](#)
- [Preventing Untagged Packets on the Physical Interface, page 4-7](#)

Default State of Subinterfaces

When you add a subinterface, it is enabled by default. However, the physical or redundant interface must also be enabled to pass traffic (see the “[Configuring and Enabling Interfaces](#)” section on page 4-1 or the “[Configuring a Redundant Interface](#)” section on page 4-3).

Maximum Subinterfaces

To determine how many subinterfaces are allowed for your platform, see [Appendix A, “Feature Licenses and Specifications.”](#)

Preventing Untagged Packets on the Physical Interface

If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. This property is also true for the active physical interface in a redundant interface pair. Because the physical or redundant interface must be enabled for the subinterface to pass traffic, ensure that the physical or redundant interface does not pass traffic by leaving out the **nameif** command. If you want to let the physical or redundant interface pass untagged packets, you can configure the **nameif** command as usual. See the “[Configuring Interface Parameters](#)” section on page 6-1 for more information about completing the interface configuration.

Adding a Subinterface

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

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

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

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

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

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

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

```
hostname(config)# interface gigabitethernet 3/1.100
```

The following command adds a subinterface to a redundant interface:

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

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

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

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

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

Step 3 To enable the subinterface (if you previously disabled it), enter the following command:

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

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

Enabling Jumbo Frame Support

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 the maximum use of other features, such as access lists.

To enable jumbo frame support, enter the following command:

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

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

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

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

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

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

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



Note

Be sure to set the MTU for each interface that needs to accept jumbo frames to a higher value than the default 1500; for example, set the value to 9000 using the **mtu** command. In multiple context mode, set the MTU within each context.