CHAPTER 6

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. If you have both fiber and copper Ethernet ports (for example, on the 4GE SSM for the ASA 5510 and higher series adaptive security appliance), this chapter describes how to configure the interface media type.

- In single context mode, complete the procedures in this chapter and then continue your interface configuration in Chapter 8, "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 7, "Adding and Managing Security Contexts," and finally configure the interface parameters within each context according to Chapter 8, "Configuring Interface Parameters."

Note To configure interfaces for the ASA 5505 adaptive security appliance, see Chapter 5, "Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance."

The security appliance interfaces do not support jumbo frames.

This chapter includes the following sections:

Configuring and Enabling RJ-45 Interfaces

This section describes how to configure Ethernet settings for physical interfaces with an RJ-45 connector, and how to enable the interface. It includes the following topics:

RJ-45 Interface Overview

This section describes the RJ-45 interface, and includes the following topics:

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.

Connector Types

The ASA 5550 adaptive security appliance and the 4GE SSM for the ASA 5510 and higher adaptive security appliance include two connector types: copper RJ-45 and fiber SFP. RJ-45 is the default. If you want to configure the security appliance to use the fiber SFP connectors, see the "Configuring and Enabling Fiber Interfaces" section on page 6-3.

Auto-MDI/MDIX Feature

For RJ-45 interfaces on the ASA 5500 series adaptive 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.

Configuring the RJ-45 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
hostname(config-if)#
```

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

The physical interface types include the following:

- **ethernet**

- **gigabitethernet**
- **management** (ASA 5500 only)

For the PIX 500 series security appliance, enter the type followed by the port number, for example, **ethernet0**.

For the ASA 5500 series adaptive security appliance, enter the type followed by *slot*/*port*, for example, **gigabitethernet0/1** or **ethernet 0/1**.

The ASA 5500 management interface is a Fast Ethernet interface designed for management traffic only, and is specified as **management0/0**. You can, however, use it for through traffic if desired (see the **management-only** command). In transparent firewall mode, you can use the management interface (for management purposes) in addition to the two interfaces allowed for through traffic. You can also add subinterfaces to the management interface to provide management in each security context for multiple context mode.

Note In transparent firewall mode, the management interface updates the MAC address table in the same manner as a data interface; therefore you should not connect both a management and a data interface to the same switch unless you configure one of the switch ports as a routed port (by default Cisco Catalyst switches share a MAC address for all VLAN switch ports). Otherwise, if traffic arrives on the management interface from the physically-connected switch, then the 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.

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

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

The **auto** setting is the default. The **speed nonegotiate** command disables link negotiation.

Step 3 (Optional) To set the duplex, 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 and Enabling Fiber Interfaces

This section describes how to configure Ethernet settings for physical interfaces, and how to enable the interface. By default, the connectors used on the 4GE SSM or for built-in interfaces in slot 1 on the ASA 5550 adaptive security appliance are the RJ-45 connectors. To use the fiber SFP connectors, you must set the media type to SFP. The fiber interface 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.

This section includes the following topics:

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.

Configuring the Fiber Interface

To enable the interface, set the media type, or to set negotiation settings, perform the following steps:

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

```
hostname(config)# interface gigabitethernet 1/port
hostname(config-if)#
```

The fiber interfaces are available in slot 1 only.

Step 2 To set the media type to SFP, enter the following command:

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

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

Step 3 (Optional) To disable link negotiation, enter the following command:

```
hostname(config-if)# speed nonegotiate
```

The default is **no speed nonegotiate**, which sets the speed to 1000 Mbps and enables link negotiation for flow-control parameters and remote fault information. The **speed nonegotiate** command disables link negotiation.

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 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 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

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

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 8-2 or the "Automatically Assigning MAC Addresses to Context Interfaces" section on page 7-11). 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 RJ-45 Interfaces" section on page 6-1 or the "Configuring and Enabling Fiber Interfaces" section on page 6-3), 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_interface
```

See the "Configuring and Enabling RJ-45 Interfaces" section for a description of the physical interface ID.

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

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

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

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

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

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

Changing the Active Interface

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

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

For example:

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

To change the active interface, enter the following command:

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

where the **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

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

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 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

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 RJ-45 Interfaces" section on page 6-1, the "Configuring and Enabling Fiber Interfaces" section on page 6-3, or the "Configuring a Redundant Interface" section on page 6-5).

Maximum Subinterfaces

To determine how many subinterfaces are allowed for your platform, see the "Supported Feature Licenses Per Model" section on page 3-1.

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 8-1 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 | redundant number}.subinterface
hostname(config-subif)#
```

See the "Configuring and Enabling RJ-45 Interfaces" section for a description of the physical interface ID.

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

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

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

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

The following command adds a subinterface to a redundant interface:

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

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

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

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

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