CHAPTER 5

Configuring Ethernet Settings and Subinterfaces

This chapter describes how to configure and enable physical Ethernet interfaces 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 7, "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 6, "Adding and Managing Security Contexts," and finally configure the interface parameters within each context according to Chapter 7, "Configuring Interface Parameters."

Note To configure interfaces for the ASA 5505 adaptive security appliance, see Chapter 4, "Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance."

This chapter includes the following sections:

Configuring and Enabling RJ-45 Interfaces

This section describes how to configure Ethernet settings for physical interfaces, and how to enable the interface. By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through it or through a subinterface. For multiple context mode, if you allocate a physical interface 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 also enable the 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.

The ASA 5550 adaptive security appliance and the 4GE SSM for the ASA 5510 and higher adaptive security appliance includes 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 5-3.

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.

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
```

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

The physical interface types include the following:

- **ethernet**
- **gigabitethernet**

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**. Interfaces that are built into the chassis are assigned to slot 0, while interfaces on the 4GE SSM are assigned to slot 1.

The ASA 5500 series adaptive security appliance also includes the following type:

- **management**

  The 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 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.

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 for a physical interface, 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, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through it or through a subinterface. For multiple context mode, if you allocate a physical interface 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 also enable the interface in the system configuration according to this procedure.

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.

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
```

The 4GE SSM interfaces are assigned to slot 1, as shown in the interface ID in the syntax (the interfaces built into the chassis are assigned to slot 0).

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
```

For fiber Gigabit Ethernet interfaces, 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 for a physical interface, 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 VLAN Subinterfaces and 802.1Q Trunking

This section describes how to configure and enable a VLAN subinterface. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk.

You must enable the physical interface before any traffic can pass through an enabled subinterface (see the "Configuring and Enabling RJ-45 Interfaces" section on page 5-1 or the "Configuring and Enabling Fiber Interfaces" section on page 5-3). For multiple context mode, if you allocate a subinterface to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration with this procedure.

Subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. 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 you can assign unique interfaces to each context.

To determine how many subinterfaces are allowed for your platform, see Appendix A, "Feature Licenses and Specifications."

Note If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Because the physical interface must be enabled for the subinterface to pass traffic, ensure that the physical interface does not pass traffic by leaving out the **nameif** command. If you want to let the physical interface pass untagged packets, you can configure the **nameif** command as usual. See the "Configuring Interface Parameters" section on page 7-1 for more information about completing the interface configuration.

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.subinterface
```

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

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

For example, enter the following command:

```
hostname(config)# interface gigabitethernet0/1.100
```

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 security appliance changes the old ID.

Step 3 To enable the subinterface, enter the following command:

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

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.