



CHAPTER 7

Configuring Interfaces in Single Mode

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. For each interface (physical, redundant, or subinterface), you must also configure a name, security level, and IP address (routed mode only).



Note

To configure interfaces for the ASA 5505 adaptive security appliance, see [Chapter 9, “Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance.”](#)

To configure interfaces in multiple context mode, see [Chapter 8, “Configuring Interfaces in Multiple Mode.”](#)

This chapter includes the following sections:

- [Interface Overview, page 7-1](#)
- [Configuring an Interface \(Single Mode\), page 7-5](#)
- [Enabling Same Security Level Communication \(Single Mode\), page 7-9](#)
- [PPPoE IP Address and Route Settings, page 7-9](#)

Interface Overview

This section describes physical interfaces, redundant interfaces, and subinterfaces, and includes the following topics:

- [Physical Interface Overview, page 7-1](#)
- [Redundant Interface Overview, page 7-2](#)
- [VLAN Subinterface and 802.1Q Trunking Overview, page 7-3](#)
- [Default State of Interfaces, page 7-4](#)
- [Default Security Level, page 7-4](#)

Physical Interface Overview

This section describes physical interfaces, and includes the following topics.

- [Default Physical Interface Settings, page 7-2](#)
- [Connector Types, page 7-2](#)
- [Auto-MDI/MDIX Feature, page 7-2](#)

Default Physical Interface Settings

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.

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.

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.

Redundant Interface Overview

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

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

- [Redundant Interfaces and Failover Guidelines, page 7-2](#)
- [Redundant Interface MAC Address, page 7-3](#)
- [Physical Interface Guidelines for Use in a Redundant Interface, page 7-3](#)

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; 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 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 an Interface \(Single Mode\)”](#) section on page 7-5 or the [“Configuring Security Contexts”](#) section on page 10-16). When the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.

Physical Interface Guidelines for Use in a Redundant Interface

Follow these guidelines when adding member interfaces:

- Both member interfaces must be of the same physical type. For example, both must be Ethernet.
- When you add a physical interface to the redundant interface, the name, IP address, and security level is removed.



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.
- If you shut down the active interface, then the standby interface becomes active.

VLAN Subinterface and 802.1Q Trunking 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 section includes the following topics:

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

Maximum Subinterfaces

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

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 naming it. If you want to let the physical or redundant interface pass untagged packets, you can configure the name command as usual.

Default State of Interfaces

Interfaces have the following default states:

- Physical interfaces—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

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.

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 [“Enabling Same Security Level Communication \(Single Mode\)” section on page 7-9](#) 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 between same security interfaces, 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).

For some 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 some 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 between same security interfaces, you can configure **established** commands for both directions.

Configuring an Interface (Single Mode)

To configure an interface, perform the following steps. For overview information, see the “[Interface Overview](#)” section on page 7-1.



Note

If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and Stateful Failover communications. See [Chapter 15, “High Availability.”](#) to configure the failover and state links. You can, however, set physical interface properties such as the speed and duplex using this procedure.

Step 1

Go to the Configuration > Device Setup > Interfaces pane.

By default, all physical interfaces are listed. You can edit a physical interface, or you can add a subinterface or redundant interface.

- To edit a physical interface or any other existing interface, choose the interface row, and click **Edit**. The Edit Interface dialog box appears with the General tab selected.
- To add and configure a subinterface, perform the following steps:
 - a. Click **Add > Interface**. The Add Interface dialog box appears with the General tab selected.
 - b. From the Hardware Port drop-down list, choose the physical interface to which you want to add the subinterface.
 - c. 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.
 - d. 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.
 - e. Continue configuring the interface by following [Step 2](#).
- To add and configure a redundant interface, perform the following steps:

- a. Click **Add > Redundant Interface**.

The Add Redundant Interface dialog box appears with the General tab selected.

- b. In the Redundant ID field, enter an integer between 1 and 8.
- c. 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.
- d. From the Secondary Interface drop-down list, choose the physical interface you want to be secondary.
- e. Continue configuring the interface by following [Step 2](#).

Step 2 In the Interface Name field, enter a name up to 48 characters in length.

Step 3 In the Security level field, enter a level between 0 (lowest) and 100 (highest).

See the [“Default Security Level” section on page 7-4](#) for more information.

Step 4 (Optional) To set this interface as a management-only interface, check **Dedicate this interface to management-only**.

Through traffic is not accepted on a management-only interface.

Step 5 If the interface is not already enabled, check **Enable Interface**.

Step 6 To set the IP address, follow these guidelines:

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 [Management IP Address](#) pane. To set the IP address of the Management interface or subinterface, use this procedure.



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.

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.

Use one of the following options to set the IP address:

- To set the IP address manually, click **Use Static IP** and enter the IP address and mask.
- To obtain an IP address from a DHCP server, click **Obtain Address via DHCP**.
 - a. (Optional) To obtain the default route from the DHCP server, check **Obtain Default Route Using DHCP**.

- b. (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.
- c. (Optional) To renew the lease, click **Renew DHCP Lease**.
- 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.

- 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 PAP, CHAP, or MSCHAP.

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 **Store Username and Password in Local Flash**.

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 7-9 for more information.

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. 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 (Optional) To set the media type, duplex, and speed, click the **Configure Hardware Properties** button.

- a. 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.

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

- c. To set the speed, choose a value from the Speed drop-down list.

The speeds available depend on the interface type. For fiber 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. 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.

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

Step 9 (Optional) To set the MTU or to enable jumbo frame support (ASA 5580 only), click the **Advanced** tab and enter the value in the MTU field, between 300 and 65,535 bytes.

The default is 1500 bytes. For the ASA 5580, 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.



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

Step 10 (Optional) To manually assign a MAC address to this interface, on the Advanced tab 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 000C.F142.4CDE.

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.

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 field, then it is used regardless of the member interface MAC addresses.

You might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

Step 11 Click **OK**.

Enabling Same Security Level Communication (Single Mode)

By default, interfaces on the same security level cannot communicate with each other. Allowing communication between same-security interfaces lets you 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).

**Note**

If you enable NAT control, you do not need to configure NAT between same security level interfaces.

If you enable same security interface communication, you can still configure interfaces at different security levels as usual.

You can also enable communication between hosts connected to the same interface.

- 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**.

PPPoE IP Address and Route Settings

The PPPoE IP Address and Route Settings dialog lets you choose addressing and tracking options for PPPoE connections.

See the “[Configuring an Interface \(Single Mode\)](#)” section on page 7-5 for more information about using PPPoE for an interface.

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 checkbox 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.