

Basic Interface Configuration

This chapter includes basic interface configuration including Ethernet settings and Jumbo frame configuration.

Note For multiple context mode, complete all tasks in this section in the system execution space. To change from the context to the system execution space, enter the **changeto system** command.

Note For the ASA Services Module interfaces, see the ASA Services Module quick start guide.

For the Firepower 2100 and Firepower 4100/9300 chassis, you configure basic interface settings in the FXOS operating system. See the configuration or getting started guide for your chassis for more information.

- About Basic Interface Configuration, on page 1
- Licensing for Basic Interface Configuration, on page 5
- Guidelines for Basic Interface Configuration, on page 5
- Default Settings for Basic Interface Configuration, on page 5
- Enable the Physical Interface and Configure Ethernet Parameters, on page 6
- Enable Jumbo Frame Support (ASA Models), on page 8
- Monitoring Interfaces, on page 10
- Examples for Basic Interfaces, on page 10
- History for Basic Interface Configuration, on page 11

About Basic Interface Configuration

This section describes interface features and special interfaces.

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.

Management Interface

The management interface, depending on your model, is a separate interface just for management traffic.

Management Interface Overview

You can manage the ASA by connecting to:

- Any through-traffic interface
- A dedicated Management *Slot*/*Port* interface (if available for your model)

You may need to configure management access to the interface according to Management Access.

Management *Slot*/*Port* Interface

The following table shows the Management interfaces per model.

Table 1: Management Interfaces Per Model

Model	Management 0/0	Management 0/1	Management 1/0	Management 1/1	Configurable for Through Traffic	Subinterfaces Allowed
Firepower 2100	—	—	—	**Yes**	— **Note** Technically, you can enable through traffic; however, the throughput of this interface is not adequate for data operations.	**Yes**
Firepower 4100/9300	N/A The interface ID depends on the physical mgmt-type interface that you assigned to the ASA logical device	—	—	—	—	**Yes**

Model	Management 0/0	Management 0/1	Management 1/0	Management 1/1	Configurable for Through Traffic	Subinterfaces Allowed
ASA 5506-X	—	—	—	**Yes**	—	—
ASA 5508-X	—	—	—	**Yes**	—	—
ASA 5512-X	**Yes**	—	—	—	—	—
ASA 5515-X	**Yes**	—	—	—	—	—
ASA 5516-X	—	—	—	**Yes**	—	—
ASA 5525-X	**Yes**	—	—	—	—	—
ASA 5545-X	**Yes**	—	—	—	—	—
ASA 5555-X	**Yes**	—	—	—	—	—
ASA 5585-X	**Yes**	**Yes**	**Yes** If you installed an SSP in slot 1, then Management 1/0 and 1/1 provide management access to the SSP in slot 1 only.	**Yes**	**Yes**	**Yes**
ISA 3000	—	—	—	**Yes**	—	—
ASASM	—	—	—	—	—	—
ASAv	**Yes**	—	—	—	**Yes**	—

Note If you installed a module, then the module management interface(s) provides management access for the module only. For models with software modules, the software module uses the same physical Management interface as the ASA.

Use Any Interface for Management-Only Traffic

You can use any interface as a dedicated management-only interface by configuring it for management traffic, including an EtherChannel interface (see the **management-only** command).

Management Interface for Transparent Mode

In transparent firewall mode, in addition to the maximum allowed through-traffic interfaces, you can also use the Management interface (either the physical interface, a subinterface (if supported for your model), or an EtherChannel interface comprised of Management interfaces (ASA 5585-X only)) as a separate management-only interface. You cannot use any other interface types as Management interfaces. For the

Firepower 4100/9300 chassis, the management interface ID depends on the mgmt-type interface that you assigned to the ASA logical device.

In multiple context mode, you cannot share any interfaces, including the Management interface, across contexts. To provide management per context on Firepower models and the ASA 5585-X, you can create subinterfaces of the Management interface and allocate a Management subinterface to each context. However, ASA models other than the ASA 5585-X do not allow subinterfaces on the Management interface, so per-context management for these models requires you to connect to a data interface. For the Firepower 4100/9300 chassis, the management interface and its subinterfaces are not recognized as specially-allowed management interfaces within the contexts; you must treat a management subinterface as a data interface in this case and add it to a BVI.

The management interface is not part of a normal bridge group. Note that for operational purposes, it is part of a non-configurable bridge group.

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 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 ASA 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 ASA 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.

No Support for Redundant Management Interfaces

Redundant interfaces do not support Management *slot*/*port* interfaces as members. You can, however, set a redundant interface comprised of non-Management interfaces as management-only.

Management Interface Characteristics for ASA Models

The Management interface for ASA 5500-X models except for the ASA 5585-X has the following characteristics:

- No through traffic support
- No subinterface support
- No priority queue support
- No multicast MAC support
- The software module shares the Management interface. Separate MAC addresses and IP addresses are supported for the ASA and module. You must perform configuration of the module IP address within the module operating system. However, physical characteristics (such as enabling the interface) are configured on the ASA.

Licensing for Basic Interface Configuration

Model	License Requirement
ASA 5585-X	Interface Speed for SSP-10 and SSP-20: • Base License—1-Gigabit Ethernet for fiber interfaces • 10 GE I/O License (Security Plus)—10-Gigabit Ethernet for fiber interfaces • (SSP-40 and SSP-60 support 10-Gigabit Ethernet by default.)

Guidelines for Basic Interface Configuration

Transparent Firewall Mode

For multiple context, transparent mode, each context must use different interfaces; you cannot share an interface across contexts.

Failover

You cannot share a failover or state interface with a data interface.

Additional Guidelines

Some management-related services are not available until a non-management interface is enabled, and the the ASA achieves a “System Ready” state. The ASA generates the following syslog message when it is in a “System Ready” state:

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

Default Settings for Basic Interface Configuration

This section lists default settings for interfaces if you do not have a factory default configuration.

Default State of Interfaces

The default state of an interface depends on the type and the context mode.

In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

In single mode or in the system execution space, 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.
- VLAN subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.
- VXLAN VNI interfaces—Enabled.
- EtherChannel port-channel interfaces (ASA models)—Enabled. However, for traffic to pass through the EtherChannel, the channel group physical interfaces must also be enabled.
- EtherChannel port-channel interfaces (Firepower models)—Disabled.



Note For the Firepower 4100/9300, you can administratively enable and disable interfaces in both the chassis and on the ASA. For an interface to be operational, the interface must be enabled in both operating systems. Because the interface state is controlled independently, you may have a mismatch between the chassis and the ASA.

Default Speed and Duplex

- By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.
- For fiber interfaces for the 5585-X, the speed is set for automatic link negotiation.

Default Connector Type

Some models include two connector types: copper RJ-45 and fiber SFP. RJ-45 is the default. You can configure the ASA to use the fiber SFP connectors.

Default MAC Addresses

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.

Enable the Physical Interface and Configure Ethernet Parameters

This section describes how to:

- Enable the physical interface
- Set a specific speed and duplex (if available)
- Enable pause frames for flow control

Before you begin

For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the **changeto system** command.

Procedure

Step 1 Specify the interface you want to configure:

interface *physical_interface*

Example:

```
ciscoasa(config)# interface gigabitethernet 0/0
```

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

The physical interface types include the following:

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

Enter the type followed by *slot*/*port*, for example, **gigabitethernet0/1**. A space is optional between the type and the slot/port.

Step 2 (Optional) Set the media type to SFP, if available for your model:

media-type sfp

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

Step 3 (Optional) Set the speed:

speed {**auto** | **10** | **100** | **1000** | **10000** | **nonegotiate**}

Example:

```
ciscoasa(config-if)# speed 100
```

For RJ-45 interfaces, the default setting is **auto**.

For SFP interfaces, the default setting is **no speed nonegotiate**, which sets the speed to the maximum speed (up to 1000 Mbps) and enables link negotiation for flow-control parameters and remote fault information. For 10GB interfaces, this option sets the speed down to 1000 Mbps. The **nonegotiate** keyword is the only keyword available for SFP interfaces. The **speed nonegotiate** command disables link negotiation.

Step 4 (Optional) Set the duplex for RJ-45 interfaces:

duplex {**auto** | **full** | **half**}

Example:

```
ciscoasa(config-if)# duplex full
```

The **auto** setting is the default. The duplex setting for an EtherChannel interface must be **full** or **auto**.

Step 5 (Optional) Enable pause (XOFF) frames for flow control on GigabitEthernet and TenGigabitEthernet interfaces:

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

Example:

```
ciscoasa(config-if)# flowcontrol send on 95 200 10000
```

If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue. Pause (XOFF) and XON frames are generated automatically by the NIC hardware based on the FIFO buffer usage. A pause frame is sent when the buffer usage exceeds the high-water mark. The default *high_water* value is 128 KB (10 GigabitEthernet) and 24 KB (1 GigabitEthernet); you can set it between 0 and 511 (10 GigabitEthernet) or 0 and 47 KB (1 GigabitEthernet). After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark. By default, the *low_water* value is 64 KB (10 GigabitEthernet) and 16 KB (1 GigabitEthernet); you can set it between 0 and 511 (10 GigabitEthernet) or 0 and 47 KB (1 GigabitEthernet). The link partner can resume traffic after receiving an XON, or after the XOFF expires, as controlled by the timer value in the pause frame. The default *pause_time* value is 26624; you can set it between 0 and 65535. If the buffer usage is consistently above the high-water mark, pause frames are sent repeatedly, controlled by the pause refresh threshold value.

When you use this command, you see the following warning:

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

To change the parameters without being prompted, use the **noconfirm** keyword.

Note Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

Step 6 Enable the interface:

no shutdown

Example:

```
ciscoasa(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.

Enable Jumbo Frame Support (ASA Models)

A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and VLAN header), 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 maximum use of other features, such as ACLs. Note that the ASA MTU sets the payload size not including the Layer 2 (14 bytes) and VLAN header (4 bytes), so the maximum MTU is 9198, depending on your model.



Note This procedure only applies to ASA hardware models. Firepower models support jumbo frames by default.

Before you begin

- In multiple context mode, set this option in the system execution space.
- Changes in this setting require you to reload the ASA.
- Be sure to set the MTU for each interface that needs to transmit jumbo frames to a higher value than the default 1500; for example, set the value to 9198 using the **mtu** command. In multiple context mode, set the MTU within each context.
- Be sure to adjust the TCP MSS, either to disable it for non-IPsec traffic (use the **sysopt connection tcpmss 0** command), or to increase it in accord with the MTU.

Procedure

Enable jumbo frame support:

jumbo-frame reservation

Examples

The following example enables jumbo frame reservation, saves the configuration, and reloads the ASA:

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

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

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

Monitoring Interfaces

See the following commands.

Note For the Firepower 2100 and the Firepower 4100/9300, some statistics are not shown using the ASA commands. You must view more detailed interface statistics using FXOS commands.

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

For the Firepower 2100, see also the following FXOS connect local-mgmt commands:

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

See the FXOS troubleshooting guide for more information.

- **show interface**

  Displays interface statistics.

- **show interface ip brief**

  Displays interface IP addresses and status.

Examples for Basic Interfaces

See the following configuration examples.

Physical Interface Parameters Example

The following example configures parameters for the physical interface in single mode:

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

Multiple Context Mode Example

The following example configures interface parameters in multiple context mode for the system configuration, and allocates the gigabitethernet 0/1.1 subinterface to contextA:

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

History for Basic Interface Configuration

Table 2: History for Interfaces

Feature Name	Releases	Feature Information
Through traffic support on the Management 0/0 interface for the ASAv	9.6(2)	You can now allow through traffic on the Management 0/0 interface on the ASAv. Previously, only the ASAv on Microsoft Azure supported through traffic; now all ASAvs support through traffic. You can optionally configure this interface to be management-only, but it is not configured by default. We modified the following command: **management-only**
Support for Pause Frames for Flow Control on Gigabit Ethernet Interfaces	8.2(5)/8.4(2)	You can now enable pause (XOFF) frames for flow control for Gigabit Ethernet interfaces on all models. We modified the following command: **flowcontrol**.
Support for Pause Frames for Flow Control on the ASA 5580 Ten Gigabit Ethernet Interfaces	8.2(2)	You can now enable pause (XOFF) frames for flow control. This feature is also supported on the ASA 5585-X. We introduced the following command: **flowcontrol**.

Feature Name	Releases	Feature Information
Jumbo packet support for the ASA 5580	8.1(1)	The Cisco ASA 5580 supports jumbo frames. 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 maximum use of other features, such as ACLs. This feature is also supported on the ASA 5585-X. We introduced the following command: **jumbo-frame reservation**.
Gigabit Ethernet Support for the ASA 5510 Security Plus License	7.2(3)	The ASA 5510 now supports GE (Gigabit Ethernet) for port 0 and 1 with the Security Plus license. If you upgrade the license from Base to Security Plus, the capacity of the external Ethernet0/0 and Ethernet0/1 ports increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the **speed** command to change the speed on the interface and use the **show interface** command to see what speed is currently configured for each interface.
Increased interfaces for the Base license on the ASA 5510	7.2(2)	For the Base license on the ASA 5510, the maximum number of interfaces was increased from 3 plus a management interface to unlimited interfaces.