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 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

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 1/1	Management 1/2	Configurable for Through Traffic	Subinterfaces Allowed
Firepower 1000	—	**Yes**	—	**Yes**	**Yes**
Secure Firewall 1200	—	**Yes**	—	**Yes**	**Yes**
Secure Firewall 3100	—	**Yes**	—	**Yes**	**Yes**
Secure Firewall 4200	—	**Yes**	**Yes**	**Yes**	**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**
ISA 3000	—	**Yes**	—	—	—
ASAv	**Yes**	—	—	**Yes**	—

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)) 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 device models, you can create subinterfaces of the Management interface and allocate a Management subinterface to each context. However, ASA models 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.

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.
- 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 (ISA 3000)—Enabled. However, for traffic to pass through the EtherChannel, the channel group physical interfaces must also be enabled.
- EtherChannel port-channel interfaces (Other 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.

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)
- (Secure Firewall 1200/3100/4200) Enable pause frames for flow control
- (Secure Firewall 3100/4200) Set Forward Error Correction

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:

- **ethernet**

  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 speed (varies depending on the model).

speed {**auto** | *speed* | **nonegotiate** | **sfp-detect**}

Example:

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

For Firepower 1100 fiber interfaces, **speed nonegotiate** sets the speed to 1000 Mbps and disables link negotiation for flow-control parameters and remote fault information. For the Secure Firewall 1200/3100/4200, see the **negotiate-auto** command.

(Secure Firewall 1200/3100/4200 only) Choose **sfp-detect** to detect the speed of the installed SFP module and use the appropriate speed. Duplex is always full, and auto-negotiation is always enabled. This option is useful if you later change the network module to a different model, and want the speed to update automatically.

Step 3 (Secure Firewall 1200/3100/4200) Set auto-negotiation.

negotiate-auto

Auto-negotiation is set separately from the speed.

Example:

```
ciscoasa(config-if)# negotiate-auto
```

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

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

SFP interfaces only support full duplex.

Example:

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

Step 5 (Optional) (Secure Firewall 3100/4200) Set Forward Error Correction (FEC) for 25 Gbps and higher interfaces.

fec {**auto** | **cl108-rs** | **cl74-fc** | **cl91-rs** | **disable**}

For an EtherChannel member interface, you must configure FEC before you add it to the EtherChannel. The setting chosen when you use **auto** depends on the transceiver type and whether the interface is fixed (built-in) or on a network module.

Note If an interface is removed from the EtherChannel, after rebooting your ASA, the FEC and auto-negotiation configuration will be changed. You need to manually configure the FEC and auto-negotiation once again because this is an expected behaviour.

Table 2: Default FEC for Auto Setting

Transceiver Type	Fixed Port Default FEC (Ethernet 1/9 through 1/16)	Network Module Default FEC
25G-SR	cl108-rs	cl108-rs
25G-LR	cl108-rs	cl108-rs
10/25G-CSR	cl108-rs	cl74-fc
25G-AOC*x*M	cl74-fc	cl74-fc
25G-CU2.5/3M	Auto-Negotiate	Auto-Negotiate
25G-CU4/5M	Auto-Negotiate	Auto-Negotiate
25/50/100G	cl91-rs	cl91-rs

Step 6 (Optional) (Secure Firewall 1200/3100/4200) Enable pause (XOFF) frames for flow control on Gigabit and higher interfaces:

flowcontrol send on

Example:

```
ciscoasa(config-if)# flowcontrol send on
```

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If the ASA port experiences congestion (exhaustion of queuing resources on the internal switch) and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

Note The ASA supports transmitting pause frames so that the remote peer can rate-control the traffic.

However, receiving of pause frames is not supported.

The internal switch has a global pool of 8000 buffers of 250 bytes each, and the switch allocates buffers dynamically to each port. A pause frame is sent out every interface with flowcontrol enabled when the buffer usage exceeds the global high-water mark (2 MB (8000 buffers)); and a pause frame is sent out of a particular interface when its buffer exceeds the port high-water mark (.3125 MB (1250 buffers)). After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark (1.25 MB globally (5000 buffers); .25 MB per port (1000 buffers)). The link partner can resume traffic after receiving an XON frame.

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

Step 7 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 Virtual, ISA 3000)

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.

This procedure only applies to the ISA 3000 and the ASA virtual. Other models support jumbo frames by default.

Jumbo frames are not supported on the ASAv5 and ASAv10 with less than 8GB RAM.

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
```

Manage the Network Module for the Secure Firewall 3100/4200

If you install a network module before you first power on the firewall, no action is required; the network module is enabled and ready for use.

If you need to make changes to your network module installation after initial bootup, then see the following procedures.

Configure Breakout Ports

You can configure 10GB breakout ports for each 40GB or higher interface. This procedure tells you how to break out and rejoin the ports. breakout ports can be used just like any other physical Ethernet port, including being added to EtherChannels.

If an interface is already in use in your configuration, you will have to manually remove any configuration related to interfaces that will no longer be present.

Before you begin

- You must use a supported breakout cable. See the hardware installation guide for more information.
- For clustering or failover, make sure the cluster/failover link is not using the parent interface (for breaking out) or the child interface (for rejoining); you cannot make changes to the interface if it is in use for the cluster/failover link.

Procedure

Step 1 Break out 10GB ports from a 40GB or higher interface.

breakout *slot port*

For example, to break out the Ethernet2/1 40GB interface, you would specify **2** for the *slot* and **1** for the *port*. The resulting child interfaces will be identified as Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3, and Ethernet2/1/4.

For clustering or failover, perform this step on the control node/active unit; the interface changes are replicated to the other nodes.

Example:

```
ciscoasa(config)# breakout 2 1
ciscoasa(config)# breakout 2 2
ciscoasa(config)# breakout 2 3
ciscoasa(config)# breakout 2 4
```

Step 2 Rejoin the breakout ports to restore the interface.

no breakout *slot port*

For clustering or failover, perform this step on the control node/active unit; the module state is replicated to the other nodes.

You must rejoin all child ports for the interface.

Example:

```
ciscoasa(config)# no breakout 2 1
```

Add a Network Module

To add a network module to a firewall after initial bootup, perform the following steps. Adding a new module requires a reload. For clustering or failover, zero downtime is not supported, so make sure to perform this procedure during a maintenance window.

Procedure

Step 1 Install the network module according to the hardware installation guide. You can install the network module while the firewall is powered on.

For clustering or failover, install the network module on all nodes.

Step 2 Reload the firewall; see Reload the ASA.

For clustering or failover, reload all nodes. Because nodes with different network modules cannot join the cluster/failover pair, you need to reload all nodes with the new module before they can reform the cluster/failover pair.

Step 3 Enable the network module.

no netmod 2 disable

For clustering or failover, perform this step on the control node/active unit; the module state is replicated to the other nodes.

Example:

```
ciscoasa(config)# no netmod 2 disable
```

Hot Swap the Network Module

You can hot swap a network module for a new module of the same type without having to reload. However, you must shut down the current module to remove it safely. This procedure describes how to shut down the old module, install a new module, and enable it.

For clustering or failover, you cannot disable a network module if the cluster control link/failover link is on the module.

Procedure

Step 1 For clustering or failover, perform the following steps.

- **Clustering**—Ensure the unit you want to perform the hot swap on is a data node (see Change the Control Node); then disable clustering on the node. See Become an Inactive Node or Deactivate a Node.

  If the cluster control link is on the network module, you must leave the cluster. See Leave the Cluster. Disabling the network module with an active cluster control link is not allowed.

- **Failover**—Ensure the unit you want to perform the hot swap on is the standby node. See Force Failover.

  If the failover link is on the network module, you must disable failover. See Disable Failover. Disabling the network module with an active failover link is not allowed.

Step 2 Disable the network module.

netmod 2 disable

Example:

```
ciscoasa(config)# netmod 2 disable
```

Step 3 Replace the network module according to the hardware installation guide. You can replace the network module while the firewall is powered on.

Step 4 Enable the network module.

no netmod 2 disable

Example:

```
ciscoasa(config)# no netmod 2 disable
```

Step 5 For clustering or failover, perform the following steps.

- **Clustering**—Add the node back to the cluster. See Rejoin the Cluster.
- **Failover**—If you disabled failover, then reform failover.

Replace the Network Module with a Different Type

If you replace a network module with a different type, then a reload is required. If the new module has fewer interfaces than the old module, you will have to manually remove any configuration related to interfaces that will no longer be present. For clustering or failover, zero downtime is not supported, so make sure to perform this procedure during a maintenance window.

Procedure

Step 1 Disable the network module.

netmod 2 disable

For clustering or failover, perform this step on the control node/active unit; the module state is replicated to the other nodes. Do not save the configuration; when you reload, the module will be enabled using the saved configuration.

Example:

```
ciscoasa(config)# netmod 2 disable
```

Step 2 Replace the network module according to the hardware installation guide. You can replace the network module while the firewall is powered on.

For clustering or failover, install the network module on all nodes.

Step 3 Reload the firewall; see Reload the ASA.

For clustering or failover, reload all nodes. Because nodes with different network modules cannot join the cluster/failover pair, you need to reload all nodes with the new module before they can reform the cluster/failover pair.

Step 4 If you saved the configuration before reloading, you will have to reenable the module.

Remove the Network Module

If you want to permanently remove the network module, follow these steps. Removing a network module requires a reload. For clustering or failover, zero downtime is not supported, so make sure to perform this procedure during a maintenance window.

Before you begin

For clustering or failover, make sure the cluster/failover link is not on the network module; you cannot remove the module in this case.

Procedure

Step 1 Disable the network module and save the configuration.

netmod 2 disable

write memory

For clustering or failover, perform this step on the control node/active unit; the module state is replicated to the other nodes.

Example:

```
ciscoasa(config)# netmod 2 disable
ciscoasa(config)# write memory
```

Step 2 Remove the network module according to the hardware installation guide. You can remove the network module while the firewall is powered on.

For clustering or failover, remove the network module on all nodes.

Step 3 Reload the firewall; see Reload the ASA.

For clustering or failover, reload all nodes. Because nodes with different network modules cannot join the cluster/failover pair, you need to reload all nodes without the module before they can reform the cluster/failover pair.

Monitoring Interfaces

See the following commands.

Note For Firepower and Secure Firewall models, 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**

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 3: History for Interfaces

Feature Name	Releases	Feature Information
Support for Secure Firewall 1200 Series	9.22(1)	Features such as flow control, FEC, detect SFP, and auto-negotiation are supported.
Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to cl108-rs from cl74-fc for 25 GB+ SR, CSR, and LR transceivers	9.18(3) / 9.19(1)	When you set the FEC to Auto on the Secure Firewall 3100 fixed ports, the default type is now set to cl108-rs instead of cl74-fc for 25 GB SR, CSR, and LR transceivers. New/Modified commands: **fec**
Pause Frames for Flow Control for the Secure Firewall 3100	9.18(1)	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. New/Modified commands: **flowcontrol send on**
Breakout ports for the Secure Firewall 3130 and 3140	9.18(1)	You can now configure four 10GB breakout ports for each 40GB interface on the Secure Firewall 3130 and 3140. New/Modified commands: **breakout**
Support for hot swapping the network module for the Secure Firewall 3100	9.17(1)	You can add or remove the network module on the Secure Firewall 3100 while the firewall is powered up. To replace a module with another module of the same type, you do not need to reboot. After initial bootup, adding a module, permanently removing a module, or replacing a module with a new type requires a reboot. New/Modified commands: **netmod**
Support for Forward Error Correction for the Secure Firewall 3100	9.17(1)	Secure Firewall 3100 25 Gbps interfaces support Forward Error Correction (FEC). FEC is enabled by default and set to Auto. New/Modified commands: **fec**
Support for setting the speed based on the SFP for the Secure Firewall 3100	9.17(1)	The Secure Firewall 3100 supports speed detection for interfaces based on the SFP installed. Detect SFP is enabled by default. This option is useful if you later change the network module to a different model, and want the speed to update automatically. New/Modified commands: **speed sfp-detect**
Secure Firewall 3100 auto-negotiation can be enabled or disabled for 1Gigabit and higher interfaces.	9.17(1)	Secure Firewall 3100 auto-negotiation can be enabled or disabled separately from speed for 1Gigabit and higher interfaces. New/Modified commands: **negotiate-auto**

Feature Name	Releases	Feature Information
Speed auto-negotiation can be disabled on fiber interfaces on the Firepower 1100 and 2100	9.14(1)	You can now configure a Firepower 1100 or 2100 fiber interface to disable auto-negotiation. For 10GB interfaces, you can configure the speed down to 1GB without auto-negotiation; you cannot disable auto-negotiation for an interface with the speed set to 10GB. New/Modified commands: **speed nonegotiate**
Through traffic support on the Management 0/0 interface for the ASA virtual	9.6(2)	You can now allow through traffic on the Management 0/0 interface on the ASA virtual. Previously, only the ASA virtual on Microsoft Azure supported through traffic; now all ASA virtuals 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 ASA 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**.
Jumbo packet support for the ASA 5580	8.1(1)	The 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.