Basic Interface Configuration for Firepower 1010 Switch Ports

You can configure each Firepower 1010 interface to run as a regular firewall interface or as a Layer 2 hardware switch port. This chapter includes tasks for starting your switch port configuration, including enabling or disabling the switch mode and creating VLAN interfaces and assigning them to switch ports. This chapter also describes how to customize Power over Ethernet (PoE) on supported interfaces.

About Firepower 1010 Switch Ports

This section describes the switch ports of the Firepower 1010.

Understanding Switch Ports and Interfaces

Ports and Interfaces

For each physical Firepower 1010 interface, you can set its operation as a firewall interface or as a switch port. See the following information about physical interface and port types as well as logical VLAN interfaces to which you assign switch ports:

- Physical firewall interface—In routed mode, these interfaces forward traffic between networks at Layer 3, using the configured security policy to apply firewall and VPN services. In transparent mode, these interfaces are bridge group members that forward traffic between the interfaces on the same network at Layer 2, using the configured security policy to apply firewall services. In routed mode, you can also use Integrated Routing and Bridging with some interfaces as bridge group members and others as Layer 3 interfaces. By default, the Ethernet 1/1 interface is configured as a firewall interface.
- Physical switch port—Switch ports forward traffic at Layer 2, using the switching function in hardware. Switch ports on the same VLAN can communicate with each other using hardware switching, and traffic is not subject to the ASA security policy. Access ports accept only untagged traffic, and you can assign

them to a single VLAN. Trunk ports accept untagged and tagged traffic, and can belong to more than one VLAN. By default, Ethernet 1/2 through 1/8 are configured as access switch ports on VLAN 1. You cannot configure the Management interface as a switch port.

- Logical VLAN interface—These interfaces operate the same as physical firewall interfaces, with the exception being that you cannot create subinterfaces, or EtherChannel interfaces. When a switch port needs to communicate with another network, then the ASA device applies the security policy to the VLAN interface and routes to another logical VLAN interface or firewall interface. You can even use Integrated Routing and Bridging with VLAN interfaces as bridge group members. Traffic between switch ports on the same VLAN are not subject to the ASA security policy, but traffic between VLANs in a bridge group are subject to the security policy, so you may choose to layer bridge groups and switch ports to enforce the security policy between certain segments.

Power Over Ethernet

Power over Ethernet+ (PoE+) is supported on Ethernet 1/7 and Ethernet 1/8 on the Firepower 1010.

Auto-MDI/MDIX Feature

For all switch ports, 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. 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.

Guidelines and Limitations for Switch Ports

Context Mode

The Firepower 1010 does not support multiple context mode.

Failover and Clustering

- No cluster support.
- Active/Standby failover support only.
- You should not use the switch port functionality when using Failover. Because the switch ports operate in hardware, they continue to pass traffic on both the active *and* the standby units. Failover is designed to prevent traffic from passing through the standby unit, but this feature does not extend to switch ports. In a normal Failover network setup, active switch ports on both units will lead to network loops. We suggest that you use external switches for any switching capability. Note that VLAN interfaces can be monitored by failover, while switch ports cannot. Theoretically, you can put a single switch port on a VLAN and successfully use Failover, but a simpler setup is to use physical firewall interfaces instead.
- You can only use a firewall interface as the failover link.

Logical VLAN Interfaces

- You can create up to 60 VLAN interfaces.
- If you also use VLAN subinterfaces on a firewall interface, you cannot use the same VLAN ID as for a logical VLAN interface.
- MAC Addresses:
  - Routed firewall mode—All VLAN interfaces share a MAC address. Ensure that any connected switches can support this scenario. If the connected switches require unique MAC addresses, you can manually assign MAC addresses. See Manually Configure the MAC Address.
  - Transparent firewall mode—Each VLAN interface has a unique MAC address. You can override the generated MAC addresses if desired by manually assigning MAC addresses. See Manually Configure the MAC Address.

Bridge Groups

You cannot mix logical VLAN interfaces and physical firewall interfaces in the same bridge group.

VLAN Interface and Switch Port Unsupported Features

VLAN interfaces and switch ports do not support:

- Dynamic routing
- Multicast routing
- Policy based routing
- Equal-Cost Multi-Path routing (ECMP)
- VXLAN
- EtherChannels
- Failover and state link
- Traffic zones
- Security group tagging (SGT)

Other Guidelines and Limitations

- You can configure a maximum of 60 named interfaces on the Firepower 1010.
- You cannot configure the Management interface as a switch port.

Default Settings

- Ethernet 1/1 is a firewall interface.
- Ethernet 1/2 through Ethernet 1/8 are switch ports assigned to VLAN 1.
- Default Speed and Duplex—By default, the speed and duplex are set to auto-negotiate.

Configure Switch Ports and Power Over Ethernet

To configure switch ports and PoE, complete the following tasks.

Enable or Disable Switch Port Mode

You can set each interface independently to be either a firewall interface or a switch port. By default, Ethernet 1/1 is a firewall interface, and the remaining Ethernet interfaces are configured as switch ports.

Procedure

Step 1 Enter interface configuration mode.

interface ethernet1/*port*

- *port*—Sets the port, 1 through 8.

You cannot set the Management 1/1 interface to switch port mode.

Example:

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

Step 2 Enable switch port mode.

switchport

If this interface is already in switchport mode, you are prompted for switch port parameters instead of changing the mode.

```
ciscoasa(config-if)# switchport
ciscoasa(config-if)# switchport ?
interface mode commands/options:
  access         Set access mode characteristics of the interface
  mode           Set trunking mode of the interface
  monitor        Monitor another interface
  protected      Configure an interface to be a protected port
  trunk          Set trunking characteristics of the interface
<cr>
ciscoasa(config-if)#
```

Step 3 Disable switch port mode.

no switchport

```
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# switchport ?

interface mode commands/options:
```

```
<cr>
```

Example

The following example sets Ethernet 1/3 and 1/4 to firewall mode:

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)#
```

Configure a VLAN Interface

This section describes how to configure VLAN interfaces for use with associated switch ports.

Procedure

Step 1 Add a VLAN interface.

interface vlan *id*

- *id*—Sets the VLAN ID for this interface, between 1 and 4070, excluding IDs in the range 3968 to 4047, which are reserved for internal use.

Example:

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)#
```

Step 2 (Optional) Disable forwarding to another VLAN.

no forward interface *vlan_id*

- *vlan_id*—Specifies the VLAN ID to which this VLAN interface cannot initiate traffic.

For example, you have one VLAN assigned to the outside for internet access, one VLAN assigned to an inside business network, and a third VLAN assigned to your home network. The home network does not need to access the business network, so you can use the **no forward interface** command on the home VLAN; the business network can access the home network, but the home network cannot access the business network.

Example:

```
ciscoasa(config-if)# no forward interface 200
ciscoasa(config-if)#
```

Configure Switch Ports as Access Ports

To assign a switch port to a single VLAN, configure it as an access port. Access ports accept only untagged traffic. By default, Ethernet 1/2 through Ethernet 1/8 switch ports are enabled and assigned to VLAN 1.

Note The device does not support Spanning Tree Protocol for loop detection in the network. Therefore you must ensure that any connection with the ASA does not end up in a network loop.

Procedure

Step 1 Enter interface configuration mode.

interface ethernet1/*port*

- *port*—Sets the port, 1 through 8.

Example:

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

Step 2 Assign this switch port to a VLAN.

switchport access vlan *number*

- *number*—Sets the VLAN ID, between 1 and 4070. The default is VLAN 1.

Example:

```
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)#
```

Step 3 (Optional) Set this switch port as protected, so you can prevent the switch port from communicating with other protected switch ports on the same VLAN.

switchport protected

You might want to prevent switch ports from communicating with each other if: the devices on those switch ports are primarily accessed from other VLANs; you do not need to allow intra-VLAN access; and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the **switchport protected** command to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.

Example:

```
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)#
```

Step 4 (Optional) Set the speed.

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

The default is **auto**.

Example:

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

Step 5 (Optional) Set the duplex.

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

The default is **auto**.

Example:

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

Step 6 Enable the switch port.

no shutdown

To disable the switch port, enter the **shutdown** command.

Example:

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

Example

The following example assigns Ethernet 1/3, Ethernet 1/4, and Ethernet 1/5 to VLAN 101, and sets Ethernet 1/3 and Ethernet 1/4 as protected:

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/4
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/5
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# no shutdown
```

Configure Switch Ports as Trunk Ports

This procedure describes how to create a trunk port that can carry multiple VLANs using 802.1Q tagging. Trunk ports accept untagged and tagged traffic. Traffic on allowed VLANs pass through the trunk port unchanged.

When the trunk receives untagged traffic, it tags it to the native VLAN ID so that the ASA can forward the traffic to the correct switch ports, or can route it to another firewall interface. When the ASA sends native VLAN ID traffic out of the trunk port, it removes the VLAN tag. Be sure to set the same native VLAN on the trunk port on the other switch so that the untagged traffic will be tagged to the same VLAN.

Procedure

Step 1 Enter interface configuration mode.

interface ethernet1/*port*

- *port*—Sets the port, 1 through 8.

Example:

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

Step 2 Make this switch port a trunk port.

switchport mode trunk

To restore this port to access mode, enter the **switchport mode access** command.

Example:

```
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)#
```

Step 3 Assign VLANs to this trunk.

switchport trunk allowed vlan *vlan_range*

- *vlan_range*—Sets the VLAN IDs between 1 and 4070. You can identify up to 20 IDs in one of the following ways:
  - A single number (n)
  - A range (n-x)
  - Numbers and ranges separated by commas, for example:

    5,7-10,13,45-100

  You can enter spaces instead of commas, but the command is saved to the configuration with commas.

  If you include the native VLAN in this command, it is ignored; the trunk port always removes the VLAN tagging when sending native VLAN traffic out of the port. Moreover, it will not receive traffic that still has native VLAN tagging.

Example:

```
ciscoasa(config-if)# switchport trunk allowed vlan 100,200,300
ciscoasa(config-if)#
```

Step 4 Set the native VLAN.

switchport trunk native vlan *vlan_id*

- *vlan_range*—Sets the VLAN ID between 1 and 4070. The default value is VLAN 1.

Each port can only have one native VLAN, but every port can have either the same or a different native VLAN.

Example:

```
ciscoasa(config-if)# switchport trunk native vlan 2
ciscoasa(config-if)#
```

Step 5 (Optional) Set this switch port as protected, so you can prevent the switch port from communicating with other protected switch ports on the same VLAN.

switchport protected

You might want to prevent switch ports from communicating with each other if: the devices on those switch ports are primarily accessed from other VLANs; you do not need to allow intra-VLAN access; and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the **switchport protected** command to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.

Example:

```
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)#
```

Step 6 (Optional) Set the speed.

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

The default is **auto**.

Example:

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

Step 7 (Optional) Set the duplex.

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

The default is **auto**.

Example:

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

Step 8 Enable the switch port.

no shutdown

To disable the switch port, enter the **shutdown** command.

Example:

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

Example

The following example sets Ethernet 1/6 as a trunk port with VLANs 20 through 30, and sets the native VLAN as 4:

```
ciscoasa(config)# interface ethernet1/6
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 20-30
ciscoasa(config-if)# switchport trunk native vlan 4
ciscoasa(config-if)# no shutdown
```

Configure Power Over Ethernet

Ethernet 1/7 and Ethernet 1/8 support Power over Ethernet (PoE) for devices such as IP phones or wireless access points. The Firepower 1010 supports both IEEE 802.3af (PoE) and 802.3at (PoE+). PoE+ uses Link Layer Discovery Protocol (LLDP) to negotiate the power level. PoE+ can deliver up to 30 watts to a powered device. Power is only supplied when needed.

If you shut down the interface, then you disable power to the device.

PoE is enabled by default on Ethernet 1/7 and Ethernet 1/8. This procedure describes how to disable and enable PoE and how to set optional parameters.

Procedure

Step 1 Enter interface configuration mode.

interface ethernet1/{**7** | **8**}

Example:

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)#
```

Step 2 Enable or disable PoE+.

power inline {**auto** | **never** | **consumption wattage** *milliwatts*}

- **auto**—Delivers power automatically to the powered device using a wattage appropriate to the class of the powered device. The Firepower 1010 uses LLDP to further negotiate the correct wattage.
- **never**—Disables PoE.
- **consumption wattage** *milliwatts*—Manually specified the wattage in milliwatts, from 4000 to 30000. Use this command if you want to set the watts manually and disable LLDP negotiation.

View the current PoE+ status using the **show power inline** command.

Example:

```
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)# show power inline
Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

Example

The following example manually sets the wattage for Ethernet 1/7 and sets the power to auto for Ethernet 1/8:

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

Monitoring Switch Ports

- **show interface**

  Displays interface statistics.

- **show interface ip brief**

  Displays interface IP addresses and status.

- **show switch vlan**

  Displays the VLAN–to–switch port association.

```
ciscoasa# show switch vlan
VLAN Name                   Status    Ports
```

```
---- --------------------- --------- --------------------
1    -                       down      Ethernet1/3,
                                       Ethernet1/4,
                                       Ethernet1/5,
                                       Ethernet1/6
                                       Ethernet1/7,
                                       Ethernet1/8
10   inside                  up        Ethernet1/1
20   outside                 up        Ethernet1/2
```

- **show switch mac-address-table**

  Shows the static and dynamic MAC address entries.

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds
  Mac Address  | VLAN |       Type       | Age | Port
-----------------------------------------------------
0c75.bd11.c504 | 0010 |     dynamic      | 330 | In0/0
885a.92f6.c6e3 | 0010 |     dynamic      | 330 | Et1/1
0c75.bd11.c504 | 0020 |     dynamic      | 330 | In0/0
885a.92f6.c45b | 0020 |     dynamic      | 330 | Et1/2
```

- **show arp**

  Shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds. Static ARP entries include a dash (-) instead of the age, and proxy ARP entries state “alias.” The following is sample output from the **show arp** command. The first entry is a dynamic entry aged 2 seconds. The second entry is a static entry, and the third entry is from proxy ARP.

```
ciscoasa# show arp
outside 10.86.194.61 0011.2094.1d2b 2
outside 10.86.194.1 001a.300c.8000 -
outside 10.86.195.2 00d0.02a8.440a alias
```

- **show power inline**

  Shows PoE+ status.

```
ciscoasa# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

Examples for Switch Ports

The following topics provide examples for configuring switch ports in routed and transparent mode.

Routed Mode Example

The following example creates two VLAN interfaces, and assigns two switchports to the inside interface, and one to the outside interface.

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Vlan20
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

Transparent Mode Example

The following example creates two VLAN interfaces in bridge group 1, and assigns two switchports to the inside interface, and one to the outside interface.

```
firewall transparent
!
interface BVI1
ip address 10.20.20.1 255.255.255.0
!
interface Vlan11
bridge-group 1
nameif inside
security-level 100
no shutdown
!
interface Vlan20
bridge-group 1
nameif outside
security-level 0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
```

```
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

Mixed Firewall Interface/Switch Port Example

The following example creates one VLAN interface for the inside interface, and two firewall interfaces for the outside and dmz.

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/4
nameif outside
security-level 0
ip address 10.12.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/5
nameif dmz
security-level 50
ip address 10.13.11.1 255.255.255.0
no shutdown
```

Integrated Routing and Bridging Example

The following example creates two bridge groups, with two VLAN interfaces (inside_1 and inside_2) in bridge group 1, and one (outside) in bridge group 2. A fourth VLAN interface is not part of a bridge group, and is a regular routed interface. Traffic between switch ports on the same VLAN are not subject to the ASA's security policy. But traffic between VLANs in a bridge group are subject to the security policy, so you may choose to layer bridge groups and switch ports to enforce the security policy between certain segments.

```
interface BVI1
nameif inside_bvi
security-level 100
ip address 10.30.1.10 255.255.255.0
!
interface BVI2
nameif outside_bvi
security-level 0
ip address 10.40.1.10 255.255.255.0
!
interface Vlan10
bridge-group 1
nameif inside_1
security-level 100
no shutdown
!
interface Vlan20
bridge-group 2
nameif outside
security-level 0
no shutdown
!
interface Vlan30
bridge-group 1
nameif inside_2
security-level 100
no shutdown
!
interface Vlan 100
nameif dmz
security-level 0
ip address 10.1.1.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/4
switchport
switchport access vlan 20
security-level 100
no shutdown
!
interface Ethernet1/5
switchport
switchport access vlan 100
no shutdown
!
interface Ethernet1/6
switchport
switchport access vlan 10
```

```
no shutdown
!
interface Ethernet1/7
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/8
switchport
switchport access vlan 100
no shutdown
```

Failover Example

The following example configures Ethernet 1/3 as the failover interface.

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0 standby 10.11.11.2
no shutdown
!
interface Vlan20
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0 standby 10.20.20.2
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
description LAN/STATE Failover Interface
no shutdown
!
failover
failover lan unit primary
failover lan interface folink Ethernet1/3
failover replication http
failover link folink Ethernet1/3
failover interface ip folink 10.90.90.1 255.255.255.0 standby 10.90.90.2
```

History for Switch Ports

Table 1: History for Switch Ports

Feature Name	Version	Feature Information
Firepower 1010 hardware switch support	9.13(1)	The Firepower 1010 supports setting each Ethernet interface to be a switch port or a firewall interface. New/Modified commands: **forward interface, interface vlan, show switch mac-address-table, show switch vlan, switchport, switchport access vlan, switchport mode, switchport trunk allowed vlan**
Firepower 1010 PoE+ support on Ethernet 1/7 and Ethernet 1/8	9.13(1)	The Firepower 1010 supports Power over Ethernet+ (PoE+) on Ethernet 1/7 and Ethernet 1/8. New/Modified commands: **power inline, show power inline**