



Interfaces

The following topics explain how to configure the interfaces on your FTD device.

- [About FTD Interfaces, on page 1](#)
- [Guidelines and Limitations for Interfaces, on page 5](#)
- [Configure a Physical Interface, on page 6](#)
- [Configure Bridge Groups, on page 10](#)
- [Configure VLAN Subinterfaces and 802.1Q Trunking, on page 14](#)
- [Configure Passive Interfaces, on page 19](#)
- [Configure Advanced Interface Options, on page 22](#)
- [Add Interfaces to the FTDv, on page 26](#)
- [Configure Hardware Bypass for Power Failure \(ISA 3000\), on page 27](#)
- [Monitoring Interfaces, on page 29](#)
- [Examples for Interfaces, on page 30](#)

About FTD Interfaces

FTD includes data interfaces as well as a Management/Diagnostic interface.

When you attach a cable to an interface connection (physically or virtually), you need to configure the interface. At minimum, you need to name the interface and enable it for it to pass traffic. If the interface is a member of a bridge group, this is sufficient. For non-bridge group members, you also need to give the interface an IP address. If you intend to create VLAN subinterfaces rather than a single physical interface on a given port, you would typically configure the IP addresses on the subinterface, not on the physical interface. VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs, which is useful when you connect to a trunk port on a switch. You do not configure IP addresses on passive interfaces.

The interface list shows the available interfaces, their names, addresses, modes, and states. You can change the state of an interface, on or off, directly in the list of interfaces. The list shows the interface characteristics based on your configuration. Use the open/close arrow on a bridge group interface to view the member interfaces, which also appear by themselves in the list. For information on how these interfaces map to virtual interfaces and network adapters, see [How VMware Network Adapters and Interfaces Map to the FTD Physical Interfaces](#).

The following topics explain the limitations of configuring interfaces through the FDM as well as other interface management concepts.

Interface Modes

You can configure one of the following modes for each interface:

Routed

Each Layer 3 routed interface requires an IP address on a unique subnet. You would typically attach these interfaces to switches, a port on another router, or to an ISP/WAN gateway.

Passive

Passive interfaces monitor traffic flowing across a network using a switch SPAN (Switched Port Analyzer) or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This function provides the system visibility within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted.

BridgeGroupMember

A bridge group is a group of interfaces that the FTD device bridges instead of routes. All interfaces are on the same network. The bridge group is represented by a Bridge Virtual Interface (BVI) that has an IP address on the bridge network.

You can route between routed interfaces and BVIs, if you name the BVI. In this case, the BVI acts as the gateway between member interfaces and routed interfaces. If you do not name the BVI, traffic on the bridge group member interfaces cannot leave the bridge group. Normally, you would name the interface so that you can route member interfaces to the internet.

One use for a bridge group in routed mode is to use extra interfaces on the FTD device instead of an external switch. You can attach endpoints directly to bridge group member interfaces. You can also attach switches to add more endpoints to the same network as the BVI.

Management/Diagnostic Interface

The physical port labeled Management (or for the FTDv, the Management0/0 virtual interface) actually has two separate interfaces associated with it.

- Management virtual interface—This IP address is used for system communication. This is the address the system uses for Smart Licensing and to retrieve database updates. You can open management sessions to it (FDM and CLI). You must configure a management address, which is defined on **System Settings > Management Interface**.
- Diagnostic virtual interface—You can use this interface to send syslog messages to an external syslog server. Configuring an IP address for the Diagnostic interface is optional. The main reason to configure the interface is if you want to use it for syslog messages. This interface appears, and is configurable, on the **Device > Interfaces** page. The Diagnostic interface only allows management traffic, and does not allow through traffic.

(Hardware devices.) One way to configure Management/Diagnostic is to not wire the physical port to a network. Instead, configure the Management IP address only, and configure it to use the data interfaces as the gateway for obtaining updates from the internet. Then, open the inside interfaces to HTTPS/SSH traffic (by default, HTTPS is enabled) and open the FDM using the inside IP address (see [Configuring the Management Access List](#)).

For the FTDv, the recommended configuration is to attach Management0/0 to the same network as the inside interface, and use the inside interface as the gateway. Do not configure a separate address for Diagnostic.

Recommendations for Configuring a Separate Management Network

(Hardware devices.) If you want to use a separate management network, wire the physical Management interface to a switch or router.

For FTDv, attach Management0/0 to a separate network from any of the data interfaces. If you are still using the default IP addresses, you will need to change either the management IP address or the inside interface IP address, as they are on the same subnet.

Then, configure the following:

- Select **Device > System Settings > Management Interface** and configure IPv4 or IPv6 addresses (or both) on the attached network. If you want to, you can configure a DHCP server to provide IPv4 addresses to other endpoints on the network. If there is a router with a route to the internet on the management network, use that as the gateway. Otherwise, use the data interfaces as the gateway.
- Configure an address for the Diagnostic interface (on **Device > Interfaces**) only if you intend to send syslog messages through the interface to a syslog server. Otherwise, do not configure an address for Diagnostic; it is not needed. Any IP address you configure must be on the same subnet as the management IP address and cannot be in the DHCP server pool. For example, if you use 192.168.45.45 as the management address, and 192.168.45.46-192.168.45.254 as the DHCP pool, you can configure Diagnostic using any address from 192.168.45.1 to 192.168.45.44.

Limitations for Management/Diagnostic Interface Configuration for a Separate Management Network

If you wire the physical Management interface, or for FTDv, you attach Management0/0 to a separate network, ensure that you follow these limitations:

- If you want a DHCP server on the management network, configure it on the Management interface (**Device > System Settings > Management Interface**). You cannot configure a DHCP server on the Diagnostic interface.
- If there is another DHCP server on the management network, disable it or the DHCP server running on Management. As a rule, a given subnet should have no more than one DHCP server.
- If you configure addresses for both Management and Diagnostic, ensure that they are on the same subnet.
- (Hardware devices only.) You can use the data interfaces as the management gateway even if you configure an IP address for Diagnostic. But Diagnostic will not use the data interfaces as a gateway. If you need a path from Diagnostic to other networks, another router on the management network needs to route the traffic originating from the Diagnostic IP address. If necessary, configure static routes for the Diagnostic interface (select **Device > Routing**).

Security Zones

Each interface can be assigned to a single security zone. You then apply your security policy based on zones. For example, you can assign the inside interface to the inside zone; and the outside interface to the outside zone. You can configure your access control policy to enable traffic to go from inside to outside, but not from outside to inside, for example.

Each zone has a mode, either routed or passive. This relates directly to the interface mode. You can add routed and passive interfaces only to the same mode security zone.

For bridge groups, you add member interfaces to the zones, you cannot add the Bridge Virtual Interface (BVI).

You do not include the Management/Diagnostic interface in a zone. Zones apply to data interfaces only.

You can create security zones on the **Objects** page.

IPv6 Addressing

You can configure two types of unicast addresses for IPv6:

- Global—The global address is a public address that you can use on the public network. For a bridge group, you configure the global address on the Bridge Virtual Interface (BVI), not on each member interface. You cannot specify any of the following as a global address.
 - Internally reserved IPv6 addresses: fd00::/56 (from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
 - An unspecified address, such as ::/128
 - The loopback address, ::1/128
 - multicast addresses, ff00::/8
 - Link-local addresses, fe80::/10
- Link-local—The link-local address is a private address that you can only use on the directly-connected network. Routers do not forward packets using link-local addresses; they are only for communication on a particular physical network segment. They can be used for address configuration or for the Network Discovery functions such as address resolution and neighbor discovery. In a bridge group, enabling IPv6 on the BVI automatically configures link-local addresses for each bridge group member interface. Each interface must have its own address because the link-local address is only available on a segment, and is tied to the interface MAC address.

At a minimum, you need to configure a link-local address for IPv6 to operate. If you configure a global address, a link-local address is automatically configured on the interface, so you do not also need to specifically configure a link-local address. If you do not configure a global address, then you need to configure the link-local address, either automatically or manually.

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.

Guidelines and Limitations for Interfaces

The following topics cover some of the limitations for interfaces.

Limitations for Interface Configuration

When you use the FDM to configure the device, there are several limitations to interface configuration. If you need any of the following features, you must use the FMC to configure the device.

- Routed firewall mode only is supported. You cannot configure transparent firewall mode interfaces.
- You can configure passive interfaces, but not ERSPAN interfaces.
- You cannot configure interfaces to be inline (in an inline set), or inline tap, for IPS-only processing. IPS-only mode interfaces bypass many firewall checks and only support IPS security policy. In comparison, Firewall mode interfaces subject traffic to firewall functions such as maintaining flows, tracking flow states at both IP and TCP layers, IP defragmentation, and TCP normalization. You can also optionally configure IPS functions for this firewall mode traffic according to your security policy.
- You cannot configure EtherChannel or redundant interfaces.
- You can only add one bridge group.
- You cannot configure PPPoE for IPv4. If the Internet interface is connected to a DSL, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address, you must use the FMC instead of the FDM.
- For the Firepower 1010, you can configure and use the Power over Ethernet (PoE) ports as regular Ethernet ports, but you cannot enable or configure any PoE-related properties.
- For the ASA 5515-X, 5525-X, 5545-X, and 5555-X, and the Firepower 2100 series, you can install an optional network interface module. Modules are only discovered during bootstrap (that is, initial installation or reimage, or when switching between local/remove management). The FDM sets the correct defaults for speed and duplex for these interfaces. If you replace an optional module with one that changes the speed/duplex options for the interfaces, without changing the total number of interfaces available, reboot the device so that the system recognizes the correct speed/duplex values for the replaced interfaces. From an SSH or Console session with the device, enter the **reboot** command. Then, in the FDM, edit each physical interface that had capability changes and select valid speed and duplex options, as the system does not automatically correct your original settings. Deploy your changes right away to ensure correct system behavior.



Note Replacing a module with one that changes the total number of interfaces, or removing interfaces that were referred to by other objects, can result in unexpected problems. If you need to make this kind of change, please first remove all references to the interfaces you will remove, such as security zone membership, VPN connections, and so forth. We also suggest you do a backup prior to making the change.

- For the FTDv devices, you cannot add or remove interfaces without reinitializing the device as described in [Add Interfaces to the FTDv, on page 26](#). However, if you simply replace interfaces with ones that

have different speed/duplex capabilities, reboot the device so that the system recognizes the new speed/duplex values. From the CLI console, enter the **reboot** command. Then, in the FDM, edit each interface that had capability changes and select valid speed and duplex options, as the system does not automatically correct your original settings. Deploy your changes right away to ensure correct system behavior.

Maximum Number of VLAN Subinterfaces by Device Model

The device model limits the maximum number of VLAN subinterfaces that you can configure. Note that you can configure subinterfaces on data interfaces only, you cannot configure them on the management interface.

The following table explains the limits for each device model.

Model	Maximum VLAN Subinterfaces
Firepower 1010	60
Firepower 1120	512
Firepower 1140	1024
Firepower 2100	1024
FTDv	50
ASA 5508-X	50
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	25

Configure a Physical Interface

At minimum, you must enable a physical interface to use it. You would also typically name it and configure IP addressing. You would not configure IP addressing if you intend to create VLAN subinterfaces, if you are configuring a passive mode interface, or if you intend to add the interface to a bridge group.



Note To configure physical interfaces as passive interfaces, see [Configure a Physical Interface in Passive Mode, on page 21](#).

You can disable an interface to temporarily prevent transmission on the connected network. You do not need to remove the interface's configuration.

Procedure

- Step 1** Click **Device**, then click the link in the **Interfaces** summary.
- The interface list shows the available interfaces, their names, addresses, and states.
- Step 2** Click the edit icon (🔗) for the physical interface you want to edit.
- You cannot edit an interface that you are using as the failover or stateful failover link in a high availability configuration.
- Step 3** Set the following:

The screenshot shows the 'Edit Physical Interface' configuration window for Ethernet1/2. The window has a blue header with the title 'Ethernet1/2 Edit Physical Interface' and a close button. Below the header, there are three main sections: 'Interface Name', 'Mode', and 'Status'. The 'Interface Name' field contains 'inside'. The 'Mode' dropdown is set to 'Routed'. The 'Status' toggle is turned on. Below these fields is a note: 'Most features work with named interfaces only, although some require unnamed interfaces.' There is also a 'Description' text area. Below the description are three tabs: 'IPv4 Address' (selected), 'IPv6 Address', and 'Advanced'. Under the 'IPv4 Address' tab, there is a 'Type' dropdown set to 'Static'. Below that are two sections: 'IP Address and Subnet Mask' with fields for '10.99.10.1' and '24', and 'Standby IP Address and Subnet Mask' with fields for '10.99.10.2' and '24'. At the bottom right of the window are 'CANCEL' and 'OK' buttons.

- a) Set the **Interface Name**.


Set the name for the interface, up to 48 characters. Alphabetic characters must be lower case. For example, **inside** or **outside**. Without a name, the rest of the interface configuration is ignored. Unless you configure subinterfaces, the interface should have a name.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

b) Choose the **Mode**.

- **Routed**—Routed mode interfaces subject traffic to all firewall functions, including maintaining flows, tracking flow states at both IP and TCP layers, IP defragmentation, and TCP normalization, and your firewall policies. This is the normal interface mode.
- **Passive**—Passive interfaces monitor traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This function provides the system visibility within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted. If you select this mode, do not following the rest of this procedure. Instead, see [Configure a Physical Interface in Passive Mode, on page 21](#). Note that you cannot configure IP addresses on passive interfaces.

If you later add this interface to a bridge group, the mode will automatically change to **BridgeGroupMember**. Note that you cannot configure IP addresses on bridge group member interfaces.

c) Set the **Status** slider to the enabled setting ()

If you intend to configure subinterfaces for this physical interface, you are probably done. Click **Save** and continue with [Configure VLAN Subinterfaces and 802.1Q Trunking, on page 14](#). Otherwise, continue.

Note Even when configuring subinterfaces, it is valid to name the interface and supply IP addresses. This is not the typical setup, but if you know that is what you need, you can configure it.

d) (Optional) Set the **Description**.

The description can be up to 200 characters on a single line, without carriage returns.

Step 4 Click the **IPv4 Address** tab and configure the IPv4 address.

Select one of the following options from the **Type** field:

- **DHCP**—Choose this option if the address should be obtained from the DHCP server on the network. You cannot use this option if you configure high availability. Change the following options if necessary:
 - **Route Metric**—If you obtain the default route from the DHCP server, the administrative distance to the learned route, between 1 and 255. The default is 1.
 - **Obtain Default Route**—Whether to get the default route from the DHCP server. You would normally select this option, which is the default.
- **Static**—Choose this option if you want to assign an address that should not change. Type in the interface's IP address and the subnet mask for the network attached to the interface. For example, if you attach the 10.100.10.0/24 network, you could enter 10.100.10.1/24. Ensure that the address is not already used on the network.

If you configured high availability, and you are monitoring this interface for HA, also configure a standby IP address on the same subnet. The standby address is used by this interface on the standby device. If

you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes. See [Configuring the DHCP Server](#).

Step 5 (Optional.) Click the **IPv6 Address** tab and configure the IPv6 address.

- **State**—To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, select **Enabled**. The link local address is generated based on the interface MAC addresses (*Modified EUI-64* format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

- **Address Auto Configuration**—Select this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the FTD device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

- **Static Address/Prefix**—If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see [IPv6 Addressing, on page 4](#).

If you want to use the address as link local only, select the **Link - Local** option. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feec:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Standby IP Address**—If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.
- **Suppress RA**—Whether to suppress router advertisements. The FTD can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the FTD device to supply the IPv6 prefix (for example, the outside interface).

Step 6 (Optional.) [Configure Advanced Options, on page 24.](#)

The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 7 Click **OK**.

What to do next

- Add the interfaces to the appropriate security zones. See [Configuring Security Zones](#).

Configure Bridge Groups

A bridge group is a virtual interface that groups one or more interfaces. The main reason to group interfaces is to create a group of switched interfaces. Thus, you can attach workstations or other endpoint devices directly to the interfaces included in the bridge group. You do not need to connect them through a separate physical switch, although you can also attach a switch to a bridge group member.

The group members do not have IP addresses. Instead, all member interfaces share the IP address of the Bridge Virtual Interface (BVI). If you enable IPv6 on the BVI, member interfaces are automatically assigned unique link-local addresses.

You enable and disable the member interfaces individually. Thus, you can disable any unused interfaces without needing to remove them from the bridge group. The bridge group itself is always enabled.

You typically configure a DHCP server on the bridge group interface (BVI), which provides IP addresses for any endpoints connected through member interfaces. However, you can configure static addresses on the endpoints connected to the member interfaces if you prefer. All endpoints within the bridge group must have IP addresses on the same subnet as the bridge group IP address.

Guidelines and Limitations

- You can add one bridge group.
- You cannot configure bridge groups on Firepower 2100 series or FTDv devices.
- For the ISA 3000 and Firepower 1010, the device comes pre-configured with bridge group BVI1, named **inside**, which includes all data interfaces except for the **outside** interface. Thus, the device is pre-configured with one port used for linking to the Internet or other upstream network, and all other ports enabled and available for direct connections to endpoints. If you want to use an inside interface for a new subnet, you must first remove the needed interfaces from BVI1.

Before you begin

Configure the interfaces that will be members of the bridge group. Specifically, each member interface must meet the following requirements:

- The interface must have a name.


- The interface cannot have any IPv4 or IPv6 addresses defined for it, either static or served through DHCP. If you need to remove the address from an interface that you are currently using, you might also need to remove other configurations for the interface, such as static routes, DHCP server, or NAT rules, that depend on the interface having an address.
- You must remove the interface from its security zone (if it is in a zone), and delete any NAT rules for the interface, before you can add it to a bridge group.

Procedure


Step 1 Click **Device**, then click the link in the **Interfaces** summary.

The interface list shows the available interfaces, their names, addresses, and states. If there is already a bridge group, it is a folder. Click the open/close arrow to view the member interfaces. Member interfaces also appear separately in the list.

Step 2 Do one of the following:

- Click the edit icon () for the BV11 bridge group.
- Select **Add Bridge Group Interface** from the gear drop-down list to create a new group.

Note You can have a single bridge group. If you already have a bridge group defined, you should edit that group instead of trying to create a new one. If you need to create a new bridge group, you must first delete the existing bridge group.

- Click the delete icon () for the bridge group if you no longer need it. When you delete a bridge group, its members become standard routed interfaces, and any NAT rules or security zone membership are retained. You can edit the interfaces to give them IP addresses. If you want to add them to a new bridge group, first you need to remove the NAT rules and remove the interface from its security zone.

Step 3 Configure the following:

The screenshot shows a dialog box titled "Add Bridge Group Interface". At the top, there is a blue header bar with a question mark icon and a close button. Below the header, the "Bridge Group Name" field contains the text "inside_bvi". A note below this field states: "Most features work with named interfaces only, although some require unnamed interfaces." The "Description" field is empty. Below the description, there are four tabs: "Bridge Group Specific" (which is selected), "IPv4 Address", "IPv6 Address", and "Advanced". Under the "Bridge Group Members" section, there is a plus icon to add members and a list containing "inside". At the bottom right, there are "CANCEL" and "OK" buttons.

a) (Optional) Set the **Interface Name**.

Set the name for the bridge group, up to 48 characters. Alphabetic characters must be lower case. For example, **inside** or **outside**. Set the name if you want this BVI to participate in routing between it and other named interfaces.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

b) (Optional) Set the **Description**.

The description can be up to 200 characters on a single line, without carriage returns.

c) Edit the **Bridge Group Members** list.

You can add up to 64 interfaces or subinterfaces to a single bridge group.

- Add an interface—Click the plus icon (+), click one or more interfaces, and then click **OK**.
- Remove an interface—Mouse over an interface and click the **x** on the right side.

Step 4 Click the **IPv4 Address** tab and configure the IPv4 address.

Select one of the following options from the **Type** field:

- **Static**—Choose this option if you want to assign an address that should not change. Type in the bridge group's IP address and the subnet mask. All attached endpoints will be on this network. For models with a pre-configured bridge group, the default for the BVI1 "inside" network is 192.168.1.1/24 (i.e. 255.255.255.0). Ensure that the address is not already used on the network.

If you configured high availability, and you are monitoring this interface for HA, also configure a standby IP address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes. See [Configuring the DHCP Server](#).

- **Dynamic (DHCP)**—Choose this option if the address should be obtained from the DHCP server on the network. This is not the typical option for bridge groups, but you can configure it if needed. You cannot use this option if you configure high availability. Change the following options if necessary:
 - **Route Metric**—If you obtain the default route from the DHCP server, the administrative distance to the learned route, between 1 and 255. The default is 1.
 - **Obtain Default Route**—Whether to get the default route from the DHCP server. You would normally select this option, which is the default.

Step 5 (Optional.) Click the **IPv6 Address** tab and configure the IPv6 address.

- **State**—To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, select **Enabled**. The link local address is generated based on the interface MAC addresses (*Modified EUI-64* format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

- **Static Address/Prefix**—If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see [IPv6 Addressing, on page 4](#).

If you want to use the address as link local only, select the **Link - Local** option. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feec:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Standby IP Address**—If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.
- **Suppress RA**—Whether to suppress router advertisements. The FTD device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the FTD device to supply the IPv6 prefix (for example, the outside interface).

Step 6 (Optional.) [Configure Advanced Options, on page 24.](#)

You configure most advanced options on bridge group *member* interfaces, but some are available for the bridge group interface.

The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 7 Click **OK**.

What to do next

- Ensure that all member interfaces that you intend to use are enabled.
- Configure a DHCP server for the bridge group. See [Configuring the DHCP Server](#).
- Add the member interfaces to the appropriate security zones. See [Configuring Security Zones](#).
- Ensure that policies, such as identity, NAT, and access, supply the required services for the bridge group and member interfaces.

Configure VLAN Subinterfaces and 802.1Q Trunking

VLAN subinterfaces let you divide a physical 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 devices.

Create subinterfaces if you attach the physical interface to a trunk port on a switch. Create a subinterface for each VLAN that can appear on the switch trunk port. If you attach the physical interface to an access port on the switch, there is no point in creating a subinterface.

Guidelines and Limitations

- 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. Because the physical interface must be enabled for the subinterface to pass traffic, ensure that the physical interface does not pass traffic by not naming the interface. If you want to let the physical interface pass untagged packets, you can name the interface as usual.
- You cannot configure IP addresses on bridge group member interfaces, although you can modify advanced settings as needed.
- All subinterfaces on the same parent interface must be either bridge group members or routed interfaces; you cannot mix and match.


- FTD does not support the Dynamic Trunking Protocol (DTP), so you must configure the connected switch port to trunk unconditionally.
- You might want to assign unique MAC addresses to subinterfaces defined on the FTD device, because they use the same burned-in MAC address of the parent interface. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses, which can avoid traffic disruption in certain instances on the FTD device.


Procedure

Step 1 Click **Device**, then click the link in the **Interfaces** summary.

The interface list shows the available interfaces, their names, addresses, and states.

Step 2 Do one of the following:

- Select **Add Subinterface** from the gear drop-down list to create a new subinterface.
- Click the edit icon () for the subinterface you want to edit.

If you no longer need a subinterface, click the delete icon () for the subinterface to delete it.

Step 3 Set the **Status** slider to the enabled setting ()

Step 4 Configure the parent interface, name, and description:

?
×
Add Subinterface

Parent Interface	Subinterface Name	Mode	Status
Ethernet1/1 ▼	engineering	Routed ▼	<input checked="" type="checkbox"/>

Most features work with named interfaces only, although some require unnamed interfaces.

Description

VLAN ID	Subinterface ID
200	200

1 - 4094

IPv4 Address IPv6 Address Advanced

Type
 Static ▼

IP Address and Subnet Mask
 10.10.10.1 / 24
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask
 10.10.10.2 / 24
e.g. 192.168.5.16

CANCEL
OK

- a) Choose the **Parent Interface**.

The parent interface is the physical interface to which you want to add the subinterface. You cannot change the parent interface after you create the subinterface.

- b) Set the **Subinterface Name**, up to 48 characters.

Alphabetic characters must be lower case. For example, **inside** or **outside**. Without a name, the rest of the interface configuration is ignored.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

- c) Set the **Mode** to **Routed**.

If you later add this interface to a bridge group, then the mode will automatically change to **BridgeGroupMember**. Note that you cannot configure IP addresses on bridge group member interfaces.

d) (Optional) Set a **Description**.

The description can be up to 200 characters on a single line, without carriage returns.

e) Set the **VLAN ID**.

Enter the VLAN ID between 1 and 4094 that will be used to tag the packets on this subinterface.

f) Set the **Subinterface ID**.

Enter the subinterface ID as an integer between 1 and 4294967295. This ID is appended to the interface ID; for example Ethernet1/1.100. You can match the VLAN ID for convenience, but it is not required. You cannot change the ID after you create the subinterface.

Step 5 Click the **IPv4 Address** tab and configure the IPv4 address.

Select one of the following options from the **Type** field:

- **DHCP**—Choose this option if the address should be obtained from the DHCP server on the network. You cannot use this option if you configure high availability. Change the following options if necessary:
 - **Route Metric**—If you obtain the default route from the DHCP server, the administrative distance to the learned route, between 1 and 255. The default is 1.
 - **Obtain Default Route**—Whether to get the default route from the DHCP server. You would normally select this option, which is the default.
- **Static**—Choose this option if you want to assign an address that should not change. Type in the interface's IP address and the subnet mask for the network attached to the interface. For example, if you attach the 10.100.10.0/24 network, you could enter 10.100.10.1/24. Ensure that the address is not already used on the network.

If you configured high availability, and you are monitoring this interface for HA, also configure a standby IP address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes. See [Configuring the DHCP Server](#).

Step 6 (Optional.) Click the **IPv6 Address** tab and configure the IPv6 address.

- **State**—To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, select **Enabled**. The link local address is generated based on the interface MAC addresses (*Modified EUI-64* format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

- **Address Auto Configuration**—Select this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6

address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the FTD device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

- **Static Address/Prefix**—If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see [IPv6 Addressing, on page 4](#).

If you want to use the address as link local only, select the **Link - Local** option. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Standby IP Address**—If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.
- **Suppress RA**—Whether to suppress router advertisements. The FTD can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the FTD device to supply the IPv6 prefix (for example, the outside interface).

Step 7 (Optional.) [Configure Advanced Options, on page 24](#).

The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 8 Click **OK**.

What to do next

- Add the subinterfaces to the appropriate security zones. See [Configuring Security Zones](#).

Configure Passive Interfaces

Passive interfaces monitor traffic flowing across a network using a switch SPAN (Switched Port Analyzer) or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This function provides the system visibility within the network without being in the flow of network traffic.

When configured in a passive deployment, the system cannot take certain actions such as blocking traffic. Passive interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted.

You use a passive interface to monitor the traffic on the network to gather information about the traffic. For example, you can apply intrusion policies to identify the types of threats that afflict the network, or to see the URL categories for the web requests users are making. You can implement various security policies and rules to see what the system would do if deployed actively, so that it could drop traffic based on your access control and other rules.

However, because passive interfaces cannot impact traffic, there are many configuration limitations. These interfaces are merely letting the system peek at the traffic: no packets that enter a passive interface ever leave the device.

The following topics explain more about passive interfaces and how to configure them.

Why Use Passive Interfaces?

The main purpose of passive interfaces is to provide a simple demonstration mode. You can set up the switch to monitor a single source port, then use a workstation to send test traffic that is monitored by the passive interface. Thus, you can see how the FTD system evaluates connections, identifies threats, and so forth. Once you are satisfied with how the system performs, you can then deploy it actively in your network and remove the passive interface configuration.

However, you can also use passive interfaces in a production environment to provide the following services:

- Pure IDS deployment—If you do not want to use the system as a firewall or IPS (intrusion prevention system), you can deploy it passively as an IDS (intrusion detection system). In this deployment method, you would use an access control rule to apply an intrusion policy to all traffic. You would also have the system monitor multiple source ports on the switch. Then, you would be able to use the dashboards to monitor the threats seen on the network. However, in this mode, the system can do nothing to prevent these threats.
- Mixed deployment—You can mix active routed interfaces with passive interfaces on the same system. Thus, you can deploy the FTD device as a firewall in some networks, while configuring one or more passive interfaces to monitor traffic in other networks.

Limitations for Passive Interfaces

Any physical interface that you define as a passive mode interface has the following restrictions:

- You cannot configure subinterfaces for the passive interface.
- You cannot include the passive interface in a bridge group.
- You cannot configure IPv4 or IPv6 addresses on the passive interface.
- You cannot select the Management Only option for a passive interface.

- You can include the interface in a passive mode security zone only, you cannot include it in a routed security zone.
- You can include passive security zones in the source criteria of access control or identity rules. You cannot use passive zones in the destination criteria. You also cannot mix passive and routed zones in the same rule.
- You cannot configure management access rules (HTTPS or SSH) for a passive interface.
- You cannot use passive interfaces in NAT rules.
- You cannot configure static routes for passive interfaces. You also cannot use a passive interface in the configuration of a routing protocol.
- You cannot configure a DHCP server on a passive interface. You also cannot use a passive interface to obtain DHCP settings through auto configuration.
- You cannot use a passive interface in a syslog server configuration.
- You cannot configure any type of VPN on a passive interface.

Configure the Switch for a Hardware FTD Passive Interface

A passive interface on a hardware FTD device works only if you configure the network switch correctly. The following procedure is based on a Cisco Nexus 5000 series switch. If you have a different type of switch, the commands might be different.

The basic idea is to configure a SPAN (Switched Port Analyzer) or mirror port, connect the passive interface to that port, and configure a monitoring session on the switch to send copies of traffic from one or more source ports to the SPAN or mirror port.

Procedure

Step 1 Configure a port on the switch as a monitor (SPAN or mirror) port.

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

Step 2 Define a monitoring session to identify the ports to monitor.

Ensure that you define the SPAN or mirror port as the destination port. In the following example, two source ports are monitored.

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

Step 3 (Optional.) Verify the configuration using **show monitor session** command.

The following example shows the brief output for session 1.

```
switch# show monitor session 1 brief
  session 1
-----
type           : local
state          : up
source intf    :
  rx           : Eth1/7      Eth1/8
  tx           : Eth1/7      Eth1/8
  both        : Eth1/7      Eth1/8
source VSANs   :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

- Step 4** Physically connect the cable from the FTD passive interface to the destination port on the switch. You can configure the interface in passive mode either before or after you make the physical connection. See [Configure a Physical Interface in Passive Mode, on page 21](#).

Configure the VLAN for a FTDv Passive Interface

A passive interface on a FTDv device works only if you configure the VLAN on the virtual network correctly. Ensure that you do the following:

- Connect the FTDv interface to a VLAN that you have configured in promiscuous mode. Then, configure the interface as explained in [Configure a Physical Interface in Passive Mode, on page 21](#). The passive interface will see a copy of all traffic on the promiscuous VLAN.
- To the same VLAN, connect one or more endpoint devices, such as virtual Windows systems. You can use a single device if there is a connection from the VLAN to the Internet. Otherwise, you need at least two devices so that you can pass traffic between them. To get data for URL categories, you need to have an Internet connection.



Configure a Physical Interface in Passive Mode

You can configure an interface in passive mode. When acting passively, the interface simply monitors the traffic from the source ports in a monitoring session configured on the switch itself (for hardware devices) or on the promiscuous VLAN (for FTDv). For detailed information on what you need to configure in the switch or virtual network, see the following topics:

- [Configure the Switch for a Hardware FTD Passive Interface, on page 20](#)
- [Configure the VLAN for a FTDv Passive Interface, on page 21](#)

Use passive mode when you want to analyze the traffic coming through the monitored switch ports without impacting the traffic. For an end-to-end example of using passive mode, see [How to Passively Monitor the Traffic on a Network](#).

Procedure

- Step 1** Click **Device**, then click the link in the **Interfaces** summary.
- The interface list shows the available interfaces, their names, addresses, and states.
- Step 2** Click the edit icon () for the physical interface you want to edit.
- Pick a currently-unused interface. If you intend to convert an in-use interface to a passive interface, you need to first remove the interface from any security zone and remove all other configurations that use the interface.
- Step 3** Set the **Status** slider to the enabled setting ().
- Step 4** Configure the following:
- **Interface Name**—The name for the interface, up to 48 characters. Alphabetic characters must be lower case. For example, monitor.
 - **Mode**—Select **Passive**.
 - (Optional.) **Description**—The description can be up to 200 characters on a single line, without carriage returns.
- Note** You cannot configure IPv4 or IPv6 addresses. On the Advanced tab, you can change the MTU, duplex, and speed settings only.
- Step 5** Click **OK**.
-

What to do next

Creating a passive interface is not sufficient for populating the dashboards with information about the traffic seen on the interface. You must also do the following. The use case covers these steps. See [How to Passively Monitor the Traffic on a Network](#).

- Create a passive security zone and add the interface to it. See [Configuring Security Zones](#).
- Create access control rules that use the passive security zone as the source zone. Typically, you would apply intrusion policies in these rules to implement IDS (intrusion detection system) monitoring. See [Configuring the Access Control Policy](#).
- Optionally, create SSL decryption and identity rules for the passive security zone, and enable the Security Intelligence policy.

Configure Advanced Interface Options

Advanced options include setting the MTU, hardware settings, management only, MAC address, and other settings.

About MAC Addresses

You can manually configure Media Access Control (MAC) addresses to override the default.

For a high availability configuration, you can configure both the active and standby MAC address for an interface. 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.

Default MAC Addresses

Default MAC address assignments depend on the type of interface.

- Physical interfaces—The physical interface uses the burned-in MAC address.
- Subinterfaces—All subinterfaces of a physical interface use the same burned-in MAC address. You might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses, which can avoid traffic disruption in certain instances on the FTD.

About the MTU

The MTU specifies the maximum frame *payload* size that the FTD device can transmit on a given Ethernet interface. The MTU value is the frame size *without* Ethernet headers, VLAN tagging, or other overhead. For example, when you set the MTU to 1500, the expected frame size is 1518 bytes including the headers, or 1522 when using VLAN. Do not set the MTU value higher to accommodate these headers.

Path MTU Discovery

The FTD device supports Path MTU Discovery (as defined in RFC 1191), which lets all devices in a network path between two hosts coordinate the MTU so they can standardize on the lowest MTU in the path.

MTU and Fragmentation

For IPv4, if an outgoing IP packet is larger than the specified MTU, it is fragmented into 2 or more frames. Fragments are reassembled at the destination (and sometimes at intermediate hops), and fragmentation can cause performance degradation. For IPv6, packets are typically not allowed to be fragmented at all. Therefore, your IP packets should fit within the MTU size to avoid fragmentation.

For UDP or ICMP, the application should take the MTU into account to avoid fragmentation.



Note The FTD device can receive frames larger than the configured MTU as long as there is room in memory.

MTU and Jumbo Frames

A larger MTU lets you send larger packets. Larger packets might be more efficient for your network. See the following guidelines:

- Matching MTUs on the traffic path—We recommend that you set the MTU on all FTD interfaces and other device interfaces along the traffic path to be the same. Matching MTUs prevents intermediate devices from fragmenting the packets.

- Accommodating jumbo frames—A jumbo frame is an Ethernet packet larger than the standard maximum of 1522 bytes (including Layer 2 header and VLAN header), up to 9216 bytes. You can set the MTU to 9000 bytes or higher to accommodate jumbo frames. The maximum depends on the model.



Note Increasing the MTU assigns more memory for jumbo frames, which might limit the maximum usage of other features, such as access rules. If you increase the MTU above the default 1500 on ASA 5500-X series devices or FTDv, you must reboot the system. If the device is configured for high availability, you must also reboot the standby device. You do not need to reboot other models, where jumbo frame support is always enabled.

Configure Advanced Options

Advanced interface options have default settings that are appropriate for most networks. Configure them only if you are resolving networking problems, or if you configure high availability.

The following procedure assumes the interface is already defined. You can also edit these settings while initially editing or creating the interface.

Limitations

- For bridge groups, you configure most of these options on the member interfaces. Except for DAD attempts and Enable for HA Monitoring, these options are not available for the Bridge Virtual Interface (BVI).
- You cannot set MTU, duplex, or speed for the Management interface on a Firepower 1000 or 2100 device.
- For passive interfaces, you can set the MTU, duplex, and speed only. You cannot make the interface management only.


Procedure

Step 1

Click **Device**, then click the link in the **Interfaces** summary.

The interface list shows the available interfaces, their names, addresses, and states.

Step 2

Click the edit icon () for the interface you want to edit.

Step 3

Click **Advanced Options**.

Step 4

Select **Enable for HA Monitoring** if you want the health of the interface to be a factor when the system decides whether to fail over to the peer unit in a high availability configuration.

This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.

Step 5

To make a data interface management only, select **Management Only**.

A management only interface does not allow through traffic, so there is very little value in setting a data interface as management only. You cannot change this setting for the Management/Diagnostic interface, which is always management only.

Step 6 Change the **MTU** (maximum transmission unit) to the desired value.

The default MTU is 1500 bytes. The minimum and maximum depend on your platform. Set a high value if you typically see jumbo frames on your network.

Note If you increase MTU above 1500 on ASA 5500-X series devices, ISA 3000 series devices, or the FTDv, you must reboot the device. If the device is configured for high availability, you must also reboot the standby device. You do not need to reboot other models, where jumbo frame support is always enabled.

Step 7 (Physical interface only.) Modify the speed and duplex settings.

The default is that the interface negotiates the best duplex and speed with the interface at the other end of the wire, but you can force a specific duplex or speed if necessary. The options listed are only those supported by the interface. Before setting these options for interfaces on a network module, please read [Limitations for Interface Configuration, on page 5](#).

- **Duplex**—Choose **Auto**, **Half** or **Full**. SFP interfaces only support **Full** duplex.
- **Speed**—Choose a speed (varies depending on the model), or **Auto**.

Step 8 Modify the **IPv6 Configuration** settings.

- **Enable DHCP for IPv6 address configuration**—Whether to set the Managed Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain addresses, in addition to the derived stateless autoconfiguration address.
- **Enable DHCP for IPv6 non-address configuration**—Whether to set the Other Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address.
- **DAD Attempts**—How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless autoconfiguration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

Step 9 (Optional, recommended for subinterfaces and high availability units.) Configure the MAC address.

By default, the system uses the MAC address burned into the network interface card (NIC) for the interface. Thus, all subinterfaces on an interface use the same MAC address, so you might want to create unique addresses per subinterface. Manually configured active/standby MAC addresses are also recommended if you configure high availability. Defining the MAC addresses helps maintain consistency in the network in the event of failover.

- **MAC Address**—The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 00C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)
- **Standby MAC Address**—For use with high availability. 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.

Step 10 Click **OK**.

Add Interfaces to the FTDv

When you deploy the FTDv, you assign interfaces to the virtual machine. Then, from within the FDM, you configure those interfaces using the same methods you would use for a hardware device.

However, you cannot add more virtual interfaces to the virtual machine and then have the FDM automatically recognize them. If you need more physical-interface equivalents for the FTDv, you basically have to start over. You can either deploy a new virtual machine, or you can use the following procedure.



Caution Adding interfaces to a virtual machine requires that you completely wipe out the FTDv configuration. The only part of the configuration that remains intact is the management address and gateway settings.

Before you begin

Do the following in the FDM:

- Examine the FTDv configuration, and make notes on settings that you will want to replicate in the new virtual machine.
- Choose **Devices > Smart License > View Configuration**, and disable all feature licenses.

Procedure

Step 1 Power off the FTDv.

Step 2 Using the virtual machine software, add the interfaces to the FTDv.

For VMware, virtual appliances use vmxnet3 (10 Gbit/s) interfaces by default. You can also use ixgbe (10 Gbit/s) interfaces.

Important FTDv on VMware now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. If you are using e1000 interfaces, we strongly recommend you switch. The vmxnet3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance.

Step 3 Power on the FTDv.

Step 4 Open the FTDv console, delete the local manager, then enable the local manager.

Deleting the local manager, then enabling it, resets the device configuration and gets the system to recognize the new interfaces. The management interface configuration does not get reset. The following SSH session shows the commands.

```
> show managers
Managed locally.

> configure manager delete
```

```
If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled

> show managers
No managers configured.

> configure manager local
>
```

- Step 5** Open a browser session to the FDM, complete the device setup wizard, and configure the device. See [Complete the Initial Configuration Using the Setup Wizard](#).

Configure Hardware Bypass for Power Failure (ISA 3000)

You can enable hardware bypass so that traffic continues to flow between an interface pair during a power outage. Supported interface pairs are copper interfaces GigabitEthernet 1/1 and 1/2; and GigabitEthernet 1/3 and 1/4. If you have a fiber Ethernet model, only the copper Ethernet pair (GigabitEthernet 1/1 and 1/2) supports hardware bypass.

When hardware bypass is active, traffic passes between these interface pairs at layer 1. Both the FDM and the FTD CLI will see the interfaces as being down. No firewall functions are in place, so make sure you understand the risks of allowing traffic to pass through the device.

We suggest that you disable TCP sequence number randomization (as described in this procedure). By default, the ISA 3000 rewrites the initial sequence number (ISN) of TCP connections passing through it to a random number. When hardware bypass is activated, the ISA 3000 is no longer in the data path and does not translate the sequence numbers. The receiving client receives an unexpected sequence number and drops the connection, so the TCP session needs to be re-established. Even with TCP sequence number randomization disabled, some TCP connections will have to be re-established because of the link that is temporarily down during the switchover.

In CLI Console or an SSH session, use the **show hardware-bypass** command to monitor the operational status.

Before you begin

For hardware bypass to work:

- You must place the interface pairs in the same bridge group.
- You must attach the interfaces to access ports on the switch. Do not attach them to trunk ports.

Procedure

- Step 1** Click **Device**, then click the link in the Interfaces summary.
- The **Hardware Bypass** section at the top of the page shows the current configuration on the allowed interface pairs for this device.

However, you must ensure the pairs are configured in the same bridge group before you can enable hardware bypass.

Step 2 To enable or disable automatic hardware bypass on a given pair, move the slider for the pair in the **Bypass When Power Down** column.

The change is not immediate. You must deploy the configuration.

Step 3 (Optional) To manually enable or disable hardware bypass on a pair.

For example, you might want to test the system, or temporarily bypass the device for some reason. Note that you must deploy the configuration to change the state of hardware bypass; simply changing the settings is not sufficient.

When you manually enable/disable hardware bypass, you will see the following syslog messages, where *pair* is 1/1-1/2 or 1/3-1/4.

- %FTD-6-803002: no protection will be provided by the system for traffic over GigabitEthernet *pair*
- %FTD-6-803003: User disabled bypass manually on GigabitEthernet *pair*

- a) Move the slider for the pair to the enabled or disabled state in the **Bypass Immediately** column.
- b) Click the **Deploy Changes** icon in the upper right of the web page and deploy the change.

In CLI Console or an SSH session, use the **show hardware-bypass** command to monitor the operational status.

Step 4 (Optional.) Create the FlexConfig object and policy needed to disable TCP sequence number randomization.

- a) Click **View Configuration** in **Device > Advanced Configuration**.
- b) Click **FlexConfig > FlexConfig Objects** in the Advanced Configuration table of contents.
- c) Click the + button to create a new object.
- d) Enter a name for the object. For example, **Disable_TCP_Randomization**.
- e) In the **Template** editor, enter the commands to disable TCP sequence number randomization.

The command is **set connection random-sequence-number disable**, but you must configure it for a specific class within a policy map. By far, the easiest approach is to disable random sequence numbers globally, which requires the following commands:

```
policy-map global_policy
  class default_class
    set connection random-sequence-number disable
```

- f) In the **Negate Template** editor, enter the lines required to undo this configuration.

For example, if you disable TCP sequence number randomization globally, the negate template would be the following:

```
policy-map global_policy
  class default_class
    set connection random-sequence-number enable
```

- g) Click **OK** to save the object.

You now need to add the object to the FlexConfig policy. Creating the object is not enough.

- h) Click **FlexConfig Policy** in the table of contents.
- i) Click + in the Group List.

- j) Select the `Disable_TCP_Randomization` object and click **OK**.

The preview should update with the commands in the template. Verify you are seeing the expected commands.

- k) Click **Save**.

You can now deploy the policy.

Monitoring Interfaces

You can view some basic information about interfaces in the following areas:

- **Device.** Use the port graphic to monitor the current state of the interfaces. Mouse over a port to see its IP addresses and enabled and link statuses. The IP addresses can be statically assigned or obtained using DHCP.

Interface ports use the following color coding:

- **Green**—The interface is configured, enabled, and the link is up.
 - **Gray**—The interface is not enabled.
 - **Orange/Red**—The interface is configured and enabled, but the link is down. If the interface is wired, this is an error condition that needs correction. If the interface is not wired, this is the expected status.
- **Monitoring > System.** The **Throughput** dashboard shows information on traffic flowing through the system. You can view information on all interfaces, or you can select a specific interface to examine.
 - **Monitoring > Zones.** This dashboard shows statistics based on security zones, which are composed of interfaces. You can drill into this information for more detail.

Monitoring Interfaces in the CLI

You can also open the CLI console or log into the device CLI and use the following commands to get more detailed information about interface-related behavior and statistics.

- **show interface** displays interface statistics and configuration information. This command has many keywords you can use to get to the information you need. Use `?` as a keyword to see the available options.
- **show ipv6 interface** displays IPv6 configuration information about the interfaces.
- **show bridge-group** displays information about Bridge Virtual Interfaces (BVI), including member information and IP addresses.
- **show conn** displays information about the connections currently established through the interfaces.
- **show traffic** displays statistics about traffic flowing through each interface.
- **show ipv6 traffic** displays statistics about IPv6 traffic flowing through the device.
- **show dhcpd** displays statistics and other information about DHCP usage on the interfaces, particularly about the DHCP servers configured on interfaces.

Examples for Interfaces

The use case chapter includes the following interface-related examples:

- [How to Configure the Device in FDM](#)
- [How to Add a Subnet](#)
- [How to Passively Monitor the Traffic on a Network](#)