Hardware Bypass Mode

This chapter describes how the Cisco ISA 3000 Industrial Security Appliance is able to operate in bypass mode. Bypass mode is defined as the copper ports are able to continue with an end to end connection, bypassing the Cisco ISA 3000 in the event of loss of power. This functionality is programmable. The Software will be responsible turning off bypass mode once the system has booted up.

The chapter contains the following sections:

- Hardware Bypass Scenarios, page 5-1
- Hardware Bypass and Firewall Mode Compatibility, page 5-2
- Port Bypass LEDs, page 5-3
- Event Messages, page 5-3
- CLI Interface Commands, page 5-3

Hardware Bypass Scenarios

The hardware bypass feature lets traffic pass freely between the following interface pairs in the event of a power outage:

- Gigabitethernet 1/1 and 1/2
- Gigabitethernet 1/3 and 1/4

The hardware bypass behavior is configurable. For details, see the ASA general operations configuration guide for your software version:


You can configure the hardware bypass behavior for each pair of interfaces for the following events:

- Power down
- Power up to system operational

You can also manually enable or disable hardware bypass.

Power down means reloading or restarting the Cisco ISA 3000 via power cycle or a complete loss of power. This will bypass the ISA data ports if it has been configured to do so. If you configure the hardware bypass to continue after power up, all the traffic can pass from the internal port to the external port and vice versa. When power is restored, the system software will monitor the boot up progress and only disable the bypass when the system is ready (Firewall is ready to process packets).
Power up means after power is restored, the system will continue in bypass mode in the data ports according to the user configuration. All the traffic can pass from internal port to external port and vice versa until the user manually disables the bypass. An event/trap will be sent to the management system to indicate the system still continues in bypass mode after power is restored.

If you manually enable hardware bypass, the system will enable bypass mode and all Firewall/VPN or IPS function will not take effect until the user issues a command to disable the bypass. A critical event will be sent to the management system to indicate no protection will be provided by the system. The user has to consider whether bypass feature is enabled or not while configuring other features.

---

**Note**

There will be a warning message when the user attempts to modify the system configuration (e.g. firewall rules) to notify the user that all changes will not take effect unless bypass is disabled.

**Note**

Never configure the system with fail over and bypass together. Cisco does not support this configuration.

---

**Caution**

Reload on the system is not a software reset, it is a hardware reset. This equals a power rest to the bypass mode. This means that after a software update, and you reload the system with sticky set, it will stay in bypass mode.

**Caution**

When the device is in bypass mode, each segment can only be 50 meters to support a typical reach of 100 meters end to end of the connected networking equipment.

---

**Hardware Bypass and Firewall Mode Compatibility**

---

**Note**

You can only configure the Hardware Bypass in Transparent Firewall mode.

Transparent mode is like a layer 2 switch in bridge mode. There are no IP addresses for interfaces, and only one IP address is assigned for a bridged interface. Neighbor devices do not know the existence of the device. You can configure bypass.

Routed mode operates in layer 3 router mode. Each interface has IP addresses assigned and other typical layer 3 attributes are assigned. With two subnets active, you can’t put the box into bypass mode.
Port Bypass LEDs

Each port is equipped with a bi-colored (Green and Amber) LED which indicates the port status. The LED states are shown below:

<table>
<thead>
<tr>
<th>LED</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Ports</td>
<td>Bypass Mode Indicator</td>
<td>Off — No link</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Steady on — Link is up</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Flashing — Transmitting and Receiving data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amber — Fault, implies no link</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port 1&amp;2 or 3&amp;4 LEDs flashing amber together — Those two ports are in bypass mode and the system is up.</td>
</tr>
</tbody>
</table>

Event Messages

The user will receive warning messages via syslog and snmp.

For details on messaging, see the ASA Syslog Guide

CLI Interface Commands

This command is used to show the status of hardware bypass.

```
ISA3000# show hardware-bypass
```

<table>
<thead>
<tr>
<th>Status</th>
<th>Powerdown</th>
<th>Powerup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabitethernet 1/1-1/2</td>
<td>Enable/Disable</td>
<td>Enable/Disable</td>
</tr>
<tr>
<td>Gigabitethernet 1/3-1/4</td>
<td>Enable/Disable</td>
<td>Enable/Disable</td>
</tr>
</tbody>
</table>

This command is used to enable or disable the bypass mode during power down and power up. In this example, sticky means hardware bypass is enabled on power down and the device will keep it enabled even after software comes up.

```
ISA3000(config)#[no] hardware-bypass gigabitethernet {1/1-1/2|1/3-1/4} [sticky]
```

When hardware bypass is enabled, traffic continuous to flow on the bypass port pair even the system loses power.

This command is used to enable hardware bypass mode with manual option:

```
ISA3000# hardware-bypass manual gigabitethernet 1/1-1/2
```

This command is used to enable sticky power down & up:

```
ISA3000# hardware-bypass GigabitEthernet 1/1-1/2 [sticky]
```

This command is used to bring the system out of bypass mode when the SFR module is ready:

```
ISA3000# hardware-bypass boot-delay module-up sfr
```

See the ASA command reference for more information
Manually Enabling and Disabling Hardware Bypass

This command is used to enable/disable the bypass feature when the Cisco ISA 3000 is up and running. This does not depend on the power down or power up option.

ISA3000#[no] hardware-bypass manual gigabitethernet {1/1-1/2|1/3-1/4}

When hardware bypass is enabled with the manual option, after a reload the bypass state will follow the power down and power up behavior that has been configured.