Network Powered Lighting Configuration Guide, Cisco IOS XE 3.7.0EX (Catalyst 3850 Switches)

First Published: April 18, 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
Preface

- Document Conventions, page v
- Related Documentation, page vii
- Obtaining Documentation and Submitting a Service Request, page vii

Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)</td>
</tr>
<tr>
<td>bold font</td>
<td>Commands and keywords and user-entered text appear in bold font.</td>
</tr>
<tr>
<td>Italic font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.</td>
</tr>
<tr>
<td>Courier font</td>
<td>Terminal sessions and information the system displays appear in courier font.</td>
</tr>
<tr>
<td>Bold Courier font</td>
<td>Bold Courier font indicates text that the user must enter.</td>
</tr>
<tr>
<td>[x]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
</tbody>
</table>
### Document Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

### Reader Alert Conventions

This document may use the following conventions for reader alerts:

- **Note**: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

- **Tip**: Means *the following information will help you solve a problem*.

- **Caution**: Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

- **Timesaver**: Means *the described action saves time*. You can save time by performing the action described in the paragraph.

- **Warning**: IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS
Related Documentation

Note

Before installing or upgrading the switch, refer to the switch release notes.

- Cisco Catalyst 3850 Switch documentation, located at:
  http://www.cisco.com/go/cat3850_docs

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
PART

Network Powered Lighting

- Configuring COAP Proxy Server, page 3
- Autosmart Ports, page 15
- Configuring 2-event Classification, page 19
- Configuring Persistent POE, page 23
- Frequently Asked Questions, page 29
Configuring COAP Proxy Server

- Finding Feature Information, page 3
- Information about COAP Proxy Server, page 3
- Supported Hardware for COAP Proxy Server, page 4
- Configuring COAP Proxy Server, page 6
- Monitoring COAP Proxy Server, page 10
- Examples: COAP Proxy Server, page 11

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about COAP Proxy Server

The COAP protocol is designed for use with constrained devices. COAP works in the same way on constrained devices as HTTP works on servers in accessing information.

The comparison of COAP and HTTP is shown below:

- In the case of a webserver: HTTP is the protocol; TCP is the transport; and HTML is the most common information format transported.
- In case of a constrained device: COAP is the protocol; UDP is the transport; and JSON/link-format/ CBOR is the popular information format.

COAP provides a means to access and control device using a similar GET/POST metaphor and restful API as in HTTP.
Supported Hardware for COAP Proxy Server

COAP Proxy Server is supported on the following Catalyst 3850 Switch Models:

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Cisco IOS Image</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-C3850-24T-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48T-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-24P-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48P-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48F-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-24U-S</td>
<td>IP Base</td>
<td>Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply</td>
</tr>
<tr>
<td>WS-C3850-48U-S</td>
<td>IP Base</td>
<td>Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply</td>
</tr>
<tr>
<td>WS-C3850-12S-S</td>
<td>IP Base</td>
<td>Stackable 12 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-24S-S</td>
<td>IP Base</td>
<td>Stackable 24 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-12XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply</td>
</tr>
<tr>
<td>WS-C3850-16XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply. 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-S switch.</td>
</tr>
<tr>
<td>WS-C3850-24XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-32XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply. 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-S switch.</td>
</tr>
<tr>
<td>Switch Model</td>
<td>Cisco IOS Image</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>WS-C3850-48XS-S</td>
<td>IP Base</td>
<td>Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-48XS-F-S</td>
<td>IP Base</td>
<td>Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24XS-S</td>
<td>IP Base</td>
<td>Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24T-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48T-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-24P-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48P-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48F-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-3850-24U-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply</td>
</tr>
<tr>
<td>WS-3850-48U-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply</td>
</tr>
<tr>
<td>WS-C3850-12S-E</td>
<td>IP Services</td>
<td>Stackable, 2 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-24S-E</td>
<td>IP Services</td>
<td>Stackable, 24 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-12XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-16XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply. 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-E switch.</td>
</tr>
<tr>
<td>WS-C3850-24XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.</td>
</tr>
</tbody>
</table>
### Configuring COAP Proxy Server

To configure the COAP proxy server, you can configure the COAP Proxy and COAP Endpoints in the Configuration mode.

The commands are: **coap [proxy | endpoints]**.

### Configuring COAP Proxy

To start or stop the COAP proxy on the switch, perform the steps given below:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `coap proxy`
4. `security [none [[ipv4 | ipv6] {ip-address ip-mask/prefix} | list {ipv4-list name | ipv6-list-name}]] | dtls [id-trustpoint {identity-trustpoint label}] | [verification-trustpoint {verification-trustpoint} | [ipv4 | ipv6 {ip-address ip-mask/prefix} | list {ipv4-list name | ipv6-list-name}]]]
5. `max-endpoints {number}`
6. `port-unsecure` `{port-num}`
7. `port-dtls` `{port-num}`
8. `resource-directory [ ipv4 | ipv6 ] {ip-address} ]`
9. `list [ ipv4 | ipv6 ] {list-name}`
10. `start`
11. `stop`
12. `exit`
13. `end`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> coap proxy</td>
<td>Enters the COAP proxy sub mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# coap proxy</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> To stop the coap proxy and delete all configurations under coap proxy, use the <strong>no coap proxy</strong> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> security [none</td>
<td>Takes the encryption type as argument. The two security modes supported are <strong>none</strong> and <strong>dtls</strong></td>
</tr>
<tr>
<td>[ipv4</td>
<td>ipv6] [ip-address</td>
</tr>
<tr>
<td>ip-mask/prefix]</td>
<td></td>
</tr>
<tr>
<td>list [ipv4-list name</td>
<td></td>
</tr>
<tr>
<td>ipv6-list-name]]</td>
<td></td>
</tr>
<tr>
<td>dtls [id-trustpoint</td>
<td></td>
</tr>
<tr>
<td>[identity-trustpoint label]]</td>
<td></td>
</tr>
<tr>
<td>[verification-trustpoint</td>
<td></td>
</tr>
<tr>
<td>[verification-trustpoint]</td>
<td></td>
</tr>
<tr>
<td>[ipv4</td>
<td>ipv6] [ip-address</td>
</tr>
<tr>
<td>ip-mask/prefix]]</td>
<td></td>
</tr>
<tr>
<td>list [ipv4-list name</td>
<td></td>
</tr>
<tr>
<td>ipv6-list-name]]</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-coap-proxy)# security none ipv4 1.1.0.0 255.255.0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> To delete all security configurations under coap proxy, use the <strong>no security</strong> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> max-endpoints {number}</td>
<td><em>(Optional)</em> Specifies the maximum number of endpoints that can be learnt on the switch. The default value is 10. The range is 1 to 500.</td>
</tr>
<tr>
<td>Example: Switch(config-coap-proxy)# max-endpoints 10</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> To delete all max-endpoints configured under coap proxy, use the <strong>no max-endpoints</strong> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> port-unsecure {port-num}</td>
<td><em>(Optional)</em> Configures a port other than the default 5683. The range is 1 to 65000.</td>
</tr>
<tr>
<td>Example: Switch(config-coap-proxy)# port-unsecure 5683</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> To delete all port configurations under coap proxy, use the <strong>no port-unsecure</strong> command.</td>
<td></td>
</tr>
</tbody>
</table>
### Step 7
**port-dtls** `{port-num}`

**Example:**
```
Switch(config-coap-proxy)#port-dtls 5864
```

(Optional) Configures a port other than the default 5684.

**Note** To delete all dtls port configurations under coap proxy, use the `no port-dtls` command.

### Step 8
**resource-directory** `[ipv4 | ipv6]` `{ip-address}`

**Example:**
```
Switch(config-coap-proxy)#resource-directory ipv4 192.168.1.1
```

Configures a unicast upstream resource directory server to which the switch can act as a COAP client.

With `resource-directory`, a maximum of 5 of ipv4 and 5 ipv6, ip addresses can be configured.

**Note** To delete all resource directory configurations under coap proxy, use the `no resource-directory` command.

### Step 9
**list** `[ipv4 | ipv6]` `{list-name}`

**Example:**
```
Switch(config-coap-proxy)#list ipv4 trial_list
```

(Optional) Restricts the IP address range where the lights and their resources can be learnt. Creates a named list of ip address/masks, to be used in the `security [none | dtls]` command options above.

With `list`, a maximum of 5 ip-lists can be configured, irrespective of ipv4 or ipv6. We can configure a max of 5 ip addresses per ip-list.

**Note** To delete any ip list on the COAP proxy server, use the `no list [ipv4 | ipv6]` `{list-name}` command.

### Step 10
**start**

**Example:**
```
Switch(config-coap-proxy)#start
```

Starts the COAP proxy on this switch.

### Step 11
**stop**

**Example:**
```
Switch(config-coap-proxy)#stop
```

Stops the COAP proxy on this switch.

### Step 12
**exit**

**Example:**
```
Switch(config-coap-proxy)#exit
```

Exits the COAP proxy sub mode.

### Step 13
**end**

**Example:**
```
Switch(config)#end
```

Returns to privileged EXEC mode.
Configuring COAP Endpoints

To configure the COAP Proxy to support multiple IPv4/IPv6 static-endpoints, perform the steps given below:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. coap endpoint [ ipv4 | ipv6 ] {ip-address}
4. exit
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>coap endpoint [ ipv4</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# coap endpoint ipv4 1.1.1.1</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# coap endpoint ipv6 2001::1</td>
</tr>
<tr>
<td></td>
<td>Configures the static endpoints on the switch.</td>
</tr>
<tr>
<td></td>
<td>• ipv4 - Configures the IPv4 Static endpoints.</td>
</tr>
<tr>
<td></td>
<td>• ipv6 - Configures the IPv6 Static endpoints.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To stop the coap proxy on any endpoint, use the no coap endpoint [ ipv4</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-coap-endpoint)# exit</td>
</tr>
<tr>
<td></td>
<td>Exits the COAP endpoint sub mode.</td>
</tr>
</tbody>
</table>
Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Example:

```
Switch(config)# end
```

---

### Monitoring COAP Proxy Server

To display the COAP protocol details, use the commands in the following table:

**Table 1: Commands to Display to COAP specific data**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show coap version</code></td>
<td>Shows the IOS COAP version and the RFC information.</td>
</tr>
<tr>
<td><code>show coap resources</code></td>
<td>Shows the resources of the switch and those learnt by it.</td>
</tr>
<tr>
<td><code>show coap endpoints</code></td>
<td>Shows the endpoints which are discovered and learnt.</td>
</tr>
<tr>
<td><code>show coap globals</code></td>
<td>Shows the timer values and end point values.</td>
</tr>
<tr>
<td><code>show coap stats</code></td>
<td>Shows the message counts for endpoints, requests and external queries.</td>
</tr>
<tr>
<td><code>show coap dtls-endpoints</code></td>
<td>Shows the dtls endpoint status.</td>
</tr>
</tbody>
</table>

**Table 2: Commands to Clear COAP Commands**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear coap database</code></td>
<td>Clears the COAP learnt on the switch, and the internal database of endpoint information.</td>
</tr>
</tbody>
</table>

To debug the COAP protocol, use the commands in the following table:

**Table 3: Commands to Debug COAP protocol**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug coap database</code></td>
<td>Debugs the COAP database output.</td>
</tr>
<tr>
<td><code>debug coap errors</code></td>
<td>Debugs the COAP errors output.</td>
</tr>
<tr>
<td><code>debug coap events</code></td>
<td>Debugs the COAP events output.</td>
</tr>
</tbody>
</table>
debug coap packets | Debugs the COAP packets output.
---|---
debug coap trace | Debugs the COAP traces output.
debug coap warnings | Debugs the COAP warnings output.
debug coap all | Debugs all the COAP output.

Note: If you wish to disable the debugs, prepend the command with a "no" keyword.

Examples: COAP Proxy Server

This example shows how you can configure the port number 5683 to support a maximum of 10 endpoints.

Switch# coap proxy security none ipv4 2.2.2.2 255.255.255.0 port 5683 max-endpoints 10

This example shows how to configure COAP proxy on ipv4 1.1.0.0 255.255.0.0 with no security settings.

Switch(config-coap-proxy)# security
  dtls  dtls
  none  no security

Switch(config-coap-proxy)#security none
  ipv4  IP address range on which to learn lights
  ipv6  IPV6 address range on which to learn lights
  list  IP address range on which to learn lights

Switch(config-coap-proxy)#security none ipv4
  A.B.C.D {/nn || A.B.C.D} IP address range on which to learn lights

Switch(config-coap-proxy)#security none ipv4 1.1.0.0 255.255.0.0

This example shows how to configure COAP proxy on ipv4 1.1.0.0 255.255.0.0 with dtls id trustpoint security settings.

Switch(config-coap-proxy)#security dtls
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4  IP address range on which to learn lights
  ipv6  IPV6 address range on which to learn lights
  list  IP address range on which to learn lights

Switch(config-coap-proxy)#security dtls id-trustpoint
  WORD  Identity TrustPoint Label

Switch(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT
  verification-trustpoint  Certificate Verification Label
<cr>

Switch(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT

Switch(config-coap-proxy)#security dtls
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4  IP address range on which to learn lights
ipv6 IPv6 address range on which to learn lights
list IP address range on which to learn lights

Switch(config-coap-proxy)# security dtls ipv4 1.1.0.0 255.255.0.0

---

For configuring ipv4 / ipv6 / list, the id-trustpoint and (optional) verification-trustpoint, should be pre-configured, else the system shows an error.

---

This example shows how to configure a Trustpoint. This is a pre-requisite for COAP security dtls with id trustpoint configurations.

```
ip domain-name myDomain
crypto key generate rsa general-keys exportable label MyLabel modulus 2048
```

Switch(config)#crypto pki trustpoint MY_TRUSTPOINT
Switch(config-trustpoint)#rsakeypair MyLabel 2048
Switch(config-trustpoint)#enrollment selfsigned
Switch(config-trustpoint)#exit

Switch(config)#crypto pki enroll MY_TRUSTPOINT
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

---

This example shows how to configure COAP proxy on ipv4 1.1.0.0 255.255.0.0 with dtls verification trustpoint (DTLS with certificates or verification trustpoints)

```
Switch(config-coap-proxy)#security dtls?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4 IP address range on which to learn lights
  ipv6 IPv6 address range on which to learn lights
  list IP address range on which to learn lights
```

Switch(config-coap-proxy)#security dtls id-trustpoint ?
  WORD Identity TrustPoint Label

Switch(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT?
  verification-trustpoint Certificate Verification Label
  <cr>

Switch(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT verification-trustpoint?
  WORD Identity TrustPoint Label

Switch(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT verification-trustpoint CA-TRUSTPOINT?
  <cr>

---

This example shows how to configure Verification Trustpoint. This is a pre-requisite for COAP security dtls with verification trustpoint configurations.

```
Switch(config)#crypto pki import CA-TRUSTPOINT pkcs12 flash:hostA.p12 password cisco123
% Importing pkcs12... Source filename [hostA.p12]?
Reading file from flash:hostA.p12
```
CRYPTO_PKI: Imported PKCS12 file successfully.

This example shows how to create a list named trial-list, to be used in the security [ none | dtls ] command options.

```
Switch(config-coap-proxy)#list ipv4 trial_list
Switch (config-coap-proxy-iplist)#1.1.0.0 255.255.255.0
Switch (config-coap-proxy-iplist)#2.2.0.0 255.255.255.0
Switch (config-coap-proxy-iplist)#3.3.0.0 255.255.255.0
Switch (config-coap-proxy-iplist)#exit
Switch (config-coap-proxy)#security none list trial_list
```

This example shows all the negation commands available in the coap-proxy sub mode.

```
Switch(config-coap-proxy)#no ?
ip-list Configure IP-List
max-endpoints maximum number of endpoints supported
port-unsecure Specify a port number to use
port-dtls Specify a dtls-port number to use
resource-discovery Resource Discovery Server
security CoAP Security features
```

This example shows how you can configure multiple IPv4/IPv6 static-endpoints on the coap proxy.

```
Switch (config)# coap endpoint ipv4 1.1.1.1
Switch (config)# coap endpoint ipv4 2.1.1.1
Switch (config)# coap endpoint ipv6 2001::1
```

This example shows how you can display the COAP protocol details.

```
Switch#show coap version
CoAP version 1.0.0
RFC 7252

Switch#show coap resources
Link format data =
</> </1.1.1.6/cisco/context> </1.1.1.6/cisco/actuator> </1.1.1.6/cisco/sensor> </1.1.1.6/cisco/lldp> </1.1.1.5/cisco/context> </1.1.1.5/cisco/actuator> </1.1.1.5/cisco/sensor> </1.1.1.5/cisco/lldp> </cisco/flood> </cisco/context> </cisco/showtech> </cisco/lldp>

Switch#show coap globals
Coap System Timer Values :
  Discovery : 120 sec
  Cache Exp : 5 sec
  Keep Alive : 120 sec
  Client DB : 60 sec
  Query Queue: 500 ms
  Ack delay : 500 ms
  Timeout : 5 sec
```
Max Endpoints : 10
Resource Disc Mode : POST

Switch# show coap stats
Coap Stats :
Endpoints : 2
Requests : 20
Ext Queries : 0

Switch# show coap endpoints
List of all endpoints :
Code : D - Discovered , N - New
# Status Age(s) LastWKC(s) IP
-------------------------------------------------------------------------------------
1 D 10 94 1.1.1.6
2 D 6 34 1.1.1.5

Endpoints - Total : 2 Discovered : 2 New : 0

Switch# show coap dtls-endpoints
# Index State String State Value Port IP
-----------------------------------------------
1 3 SSLOK 3 48969 20.1.1.30
2 2 SSLOK 3 53430 20.1.1.31
3 4 SSLOK 3 54133 20.1.1.32
4 7 SSLOK 3 48236 20.1.1.33

This example shows all options available to debug the COAP protocol.

Switch# debug coap ?
all Debug CoAP all
database Debug CoAP Database
ersors Debug CoAP errors
events Debug CoAP events
packet Debug CoAP packet
trace Debug CoAP Trace
warnings Debug CoAP warnings

Related Topics

Configuring COAP Proxy, on page 6
Autosmart Ports

• Finding Feature Information, page 15
• Information about Autosmart Ports, page 15
• Autosmart Port Macros, page 16
• Commands executed by CISCO_LIGHT_AUTO_SMARTPORT, page 16
• Enabling Autosmart Port, page 17
• Example: Enabling AutoSmart Ports, page 18

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about Autosmart Ports

Auto SmartPort macros dynamically configure ports based on the device type detected on the port. When the switch detects a new device on a port, it applies the appropriate Auto SmartPorts macro. When a link-down event occurs on the port, the switch removes the macro. For example, when you connect a Cisco IP phone to a port, Auto SmartPorts automatically applies the Cisco IP phone macro. The Cisco IP phone macro enables quality of service (QoS), security features, and a dedicated voice VLAN to ensure proper treatment of delay-sensitive voice traffic.

Auto SmartPorts uses event triggers to map devices to macros. The most common event triggers are based on Cisco Discovery Protocol (CDP) messages received from connected devices. The detection of a device (Cisco IP phone, Cisco wireless access point, Cisco switch, or Cisco router) invokes an event trigger for that device.
Link Layer Discovery Protocol (LLDP) is used to detect devices that do not support CDP. Other mechanisms used as event triggers include the 802.1X authentication result and MAC-address learned.

System built-in event triggers exist for various devices based mostly on CDP and LLDP messages and some MAC address. These triggers are enabled as long as Auto SmartPort is enabled.

You can configure user-defined trigger groups for profiles and devices. The name of the trigger group is used to associate a user-defined macro.

**Autosmart Port Macros**

The Auto SmartPort macros are groups of CLI commands. Detection of devices on a port triggers the application of the macro for the device. System built-in macros exist for various devices, and, by default, system built-in triggers are mapped to the corresponding built-in macros. You can change the mapping of built-in triggers or macros as needed.

A macro basically applies or removes a set of CLIs on an interface based on the link status. In a macro, the link status is checked. If the link is up, then a set of CLIs is applied; if the link is down, the set is removed (the no format of the CLIs are applied). The part of the macro that applies the set of CLIs is termed macro. The part that removes the CLIs (the no format of the CLIs) are termed antimacro.

When a device is connected to an Autosmart Port, if it gets classified as a lighting end point, it invokes the event trigger `CISCO_LIGHT_EVENT`, and the macro `CISCO_LIGHT_AUTO_SMARTPORT` is executed.

**Related Topics**

- Enabling Autosmart Port, on page 17
- Example: Enabling AutoSmart Ports, on page 18

**Commands executed by CISCO_LIGHT_AUTO_SMARTPORT**

When the macro is executed, it runs a series of commands on the switch.

The commands that are executed by running the macro `CISCO_LIGHT_AUTO_SMARTPORT` are:

- switchport mode access
- switchport port-security violation restrict
- switchport port-security mac-address sticky
- switchport port-security
- power inline port poe-ha
- storm-control broadcast level 50.00
- storm-control multicast level 50.00
- storm-control unicast level 50.00
- spanning-tree portfast
- spanning-tree bpduguard enable
Enabling Autosmart Port

By default, Auto SmartPort is disabled globally. To disable Auto SmartPorts macros on a specific port, use the `no macro auto global processing` interface command before enabling Auto SmartPort globally. To enable Auto SmartPort globally, use the `macro auto global processing` global configuration command. To enable Auto SmartPorts, perform this task:

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `device classifier`
4. `macro auto global processing`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables the device classifier. Use <code>no device classifier</code> command to disable the device classifier.</td>
</tr>
<tr>
<td><code>device classifier</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Switch(config)# device classifier</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables Auto SmartPorts on the switch globally. Use <code>no macro auto global processing</code> command to disable Auto SmartPort globally.</td>
</tr>
<tr>
<td><code>macro auto global processing</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Switch(config)# macro auto global processing</code></td>
<td></td>
</tr>
</tbody>
</table>
### Example: Enabling AutoSmart Ports

This example shows how you can enable AutoSmart Port.

- Switch> `enable`
- Switch# `configure terminal`
- Switch(config)# `device classifier`
- Switch(config)# `macro auto global processing`
- Switch(config)# `end`

**Related Topics**

- Enabling Autosmart Port, on page 17
- Autosmart Port Macros, on page 16

---

### Table

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Autosmart Port Macros, on page 16
- Example: Enabling AutoSmart Ports, on page 18
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about 2-event Classification

When a class 4 device gets detected, IOS allocates 30W without any CDP or LLDP negotiation. This means that even before the link comes up the class 4 power device gets 30W.

Also, on the hardware level the PSE does a 2-event classification which allows a class 4 PD to detect PSE capability of providing 30W from hardware, register itself and it can move up to PoE+ level without waiting for any CDP/LLDP packet exchange.

Once 2-event is enabled on a port, you need to manually shut/un-shut the port or connect the PD again to start the IEEE detection again. Power budget allocation for a class-4 device will be 30W if 2-event classification is enabled on the port, else it will be 15.4W.

Configuring 2-event Classification

To configure the switch for a 2-event Classification, perform the steps given below:
### SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. power inline port 2-event
5. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
<td>Specifies the physical port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>power inline port 2-event</td>
<td>Configures 2-event classification on the switch.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# power inline port 2-event</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

Example: Configuring 2-Event Classification, on page 21
Example: Configuring 2-Event Classification

This example shows how you can configure 2-event classification.

Switch> enable
Switch# configure terminal
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# power inline port 2-event
Switch(config-if)# end

Related Topics

Configuring 2-event Classification, on page 19
Example: Configuring 2-Event Classification
CHAPTER 4

Configuring Persistent POE

- Finding Feature Information, page 23
- Persistent POE, page 23
- Fast POE, page 24
- Supported Hardware for Persistent POE, page 24
- Configuring POE, page 26
- Example: Configuring Persistent POE, page 28

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Persistent POE

The Persistent POE provides uninterrupted power to connected PD device even when the PSE switch is booting.

Note

Power to the ports will be interrupted in case of MCU firmware upgrade and ports will be back up immediately after the upgrade.
Fast POE

**Fast PoE** - This feature remembers the last power drawn from a particular PSE port and switches on power the moment AC power is plugged in (within 15 to 20 seconds of switching on power) without waiting for IOS to boot up. When `poe-ha` is enabled on a particular port, the switch on a recovery after power failure, provides power to the connected endpoint devices within short duration before even the IOS forwarding starts up.

This feature can be configured by the same command as `poe-ha` which is already implemented. If the user replaces the power device connected to a port when the switch is powered off, then this new device will get the power which the previous device was drawing.

---

**Note**

Fast POE is supported on Catalyst 3850 only.

---

**Supported Hardware for Persistent POE**

Persistent POE is supported on the following Catalyst 3850 Switch Models:

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Cisco IOS Image</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-C3850-24T-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48T-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-24P-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48P-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48F-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-24U-S</td>
<td>IP Base</td>
<td>Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply</td>
</tr>
<tr>
<td>WS-C3850-48U-S</td>
<td>IP Base</td>
<td>Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply</td>
</tr>
<tr>
<td>WS-C3850-12S-S</td>
<td>IP Base</td>
<td>Stackable 12 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-24S-S</td>
<td>IP Base</td>
<td>Stackable 24 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>Switch Model</td>
<td>Cisco IOS Image</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WS-C3850-12XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply</td>
</tr>
<tr>
<td>WS-C3850-16XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply. 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-S switch.</td>
</tr>
<tr>
<td>WS-C3850-24XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-32XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply. 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-S switch.</td>
</tr>
<tr>
<td>WS-C3850-48XS-S</td>
<td>IP Base</td>
<td>Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WSC3850-48XS-FS</td>
<td>IP Base</td>
<td>Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WSC3850-24XU-S</td>
<td>IP Base</td>
<td>Stackable 24 100M/1G/2.5G/5G/10G UPOE ports, 1 network module slot, 1100-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24T-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48T-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-24P-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48P-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48F-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-3850-24U-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports,1 network module slot, 1100-W power supply</td>
</tr>
<tr>
<td>WS-3850-48U-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports,1 network module slot, 1100-W power supply</td>
</tr>
</tbody>
</table>
### Configuring POE

To configure Fast POE, perform the following steps:

**Note** You will need to configure the `poe-ha` command before connecting the PD, or you will need to manually shut/unshut the port after configuring `poe-ha`.

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Cisco IOS Image</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-C3850-12S-E</td>
<td>IP Services</td>
<td>Stackable, 2 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-24S-E</td>
<td>IP Services</td>
<td>Stackable, 24 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-12XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-16XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply. 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-E switch.</td>
</tr>
<tr>
<td>WS-C3850-24XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-32XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply. 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-E switch.</td>
</tr>
<tr>
<td>WS-C3850-48XS-E</td>
<td>IP Services</td>
<td>Stackable, SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WSC3850-48XS-F-E</td>
<td>IP Services</td>
<td>Stackable, SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24XU-E</td>
<td>IP Services</td>
<td>Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100-W power supply.</td>
</tr>
</tbody>
</table>
SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. power inline port poe-ha
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the physical port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> power inline port poe-ha</td>
<td>Configures POE High Availability.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# power inline port poe-ha</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

Example: Configuring Persistent POE, on page 28
Example: Configuring Persistent POE

This example shows how you can configure persistent POE on the switch.

```
Switch> enable
Switch# configure terminal
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# power inline port poe-ha
Switch(config-if)# end
```

Related Topics

Configuring POE, on page 26
Frequently Asked Questions

• Finding Feature Information, page 29
• Frequently Asked Questions, page 29

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Frequently Asked Questions

This section list some frequently asked questions about Network Powered Lighting.

• Question:
  What does "New Endpoint" in the "show coap stats" output mean? When does "New Endpoint" migrate to "Endpoint"?

  Answer:
  New endpoint means that an endpoint has been seen (Discovery packets received) but not yet registered by the CoAP proxy. The CoAP proxy will periodically look at the new endpoint and then send them a GET on “/well-known/core” to get more details, and once RSP is received, it is moved to “Endpoint”.

• Question:
  Why can I not do a "CoAP start" unless there is a security configuration?

  Answer:
  We need to ensure that all configurations related to CoAP are done and then it can be explicitly enabled. This avoids any intermittent unstable states across configurations.
• Question:
Why do we need to enforce drop into the "coap proxy" configuration mode "coap proxy<cr>"? When I have completed the configuration, I have to exit twice to get back to the switch prompt. I do not find this very user friendly.

Answer:
We would alternatively have to type "coap proxy" as prefix for each configuration that we do. It is a better option to get into a sub-mode, as all the configurations under the sub-mode relating to coap-proxy can be done.

• Question:
Why am I not able to unconfigure security or other parameters without first stopping the coap process?

Answer:
We need to ensure that all configurations related to CoAP are done and then it can be explicitly enabled. This also avoids and controls the complexity where the user might configure settings on the fly, when CoAP is enabled.

• Question:
When I stop coap, all configurations associated with the CoAP process are not removed automatically (or return to defaults). Why does the CoAP remember previous configuration? This seems very hard for users to start fresh.

Answer:
The system has been intentionally designed this way and this is expected behavior. Sometimes we just want to make minor changes, like change max-endpoints and re-start the proxy. It is a better option to hold all other configurations in place, else the user has to configure everything all over again.

• Question:
How can I see what the security configurations have been set?

Answer:
The command "show run" shows all the configurations.

• Question:
How can I tune the timer values?

Example:
wtsoo-3850#sho coap glo
Coap System Timer Values:
Discovery : 120 sec
Cache Exp : 5 sec
Keep Alive : 120 sec
Client DB : 5 sec
Query Queue : 500 ms
Ack delay : 500 ms
Timeout : 5 sec
Max Endpoints : 500
Resource Disc Mode : POST

Answer:
The timer values are fixed and are not tunable at the moment. The reason for this is to avoid inconsistency across systems.
What are the commands "list" and "endpoint" used for?

**Answer:**

The "list" command is to make it easier to configure multiple ip-addresses and give a name to it. Then you can assign the name instead of a single ip, to represent multiple ip’s. The "endpoint" command is used to configure a static end point, in cases where the endpoints do not advertise themselves.

**Question:**

How can I find the endpoint-to-port mapping by using the “show” command?

**Answer:**

We do not support that of now. However, other commands can be run to fetch this data. Currently, we can still get all the details mentioned using individual commands like "lldp neighbours", “ip dhcp”, "power inlines" and so on.