

Cisco Configuration Professional for Catalyst (CCP-CATALYST)

Abstract

This document describes the benefits of Cisco® Configuration Professional for Catalyst and how it can be used to manage a stack or cluster of Cisco Catalyst® switches with a simple and intuitive GUI hosted on the switch itself.

In addition, this document covers how Cisco® Configuration Professional for Catalyst enables the onboarding and monitoring of Cisco Catalyst switches after they are unpacked from the box to exploit the power of Cisco Catalyst and Cisco IOS® Software while managing your network.

Contents

1. Introduction	5
2. List of supported browsers	5
3. List of supported switches	5
4. Where to download the Cisco Configuration Professional software	5
5. Installing new switches with Cisco Configuration Professional	6
5.1 Steps to perform on a switch factory-shipped with Cisco Configuration Professional	6
5.1.1 Before the installation procedure	6
5.2 Switch installation steps	6
5.2.1 Basic configuration	6
5.2.2 Interface configuration	7
5.2.3 Layer 3 configuration	7
5.2.4 Advanced configuration	8
5.2.5 Summary page	8
6. Installing Cisco Configuration Professional on existing switches	9
6.1 Steps to install CCP-C.tar	9
6.2 Steps to install Cisco IOS Software (.tar image)	10
7. Introduction to the user interface	10
7.1 Monitoring dashboard	10
8. Configuring switch system settings	12
8.1 Set clock	12
8.1.1 Set system clock during initial setup	12
8.1.2 Set system clock later with Cisco Configuration Professional	13
8.2 Basic switch configuration	14
9. Connect via Bluetooth	14
9.1 Steps to connect to the switch via Bluetooth	14
10. Connecting uplinks	16
10.1 Standalone uplink interface	16
10.2 Bundled uplink interfaces (LAG)	17
11. Managing endpoint devices	17
11.1 Monitoring endpoint devices (clients)	17
11.2 Configurations for endpoints	18
11.2.1 Monitoring PoE clients	18
11.2.2 Configuring data and voice VLANs for clients	18
11.2.3 Ports as trunks	19
11.2.4 Bundle multiple access ports as LAG (EtherChannel)	19
11.2.5 Speed up client connections (portfast)	20
12. Administrative workflows	20
12.1 Gain visibility into the traffic pattern passing through the switch or switch stack	20
12.2 Secure the network by protecting the switch against vulnerabilities	21
12.3 Conserve operational expenses through energy saver	24
12.4 Add a static route	25
12.5 Replace a faulty switch with a new switch	26
12.5.1 Upgrade Cisco IOS on the new switch to match the old switch	26
12.5.2 Replace the configuration on the new switch	26
12.6 Erase switch configuration	27
13. Tools	27
13.1 Validate reachability within the network	27

13.2 Know your switch health	27
13.3 Getting technical support	28
13.4 Choose your language settings.....	29
13.5 Using the CLI	30

1. Introduction

Cisco Configuration Professional for Catalyst is software that provides users an easy-to-use and intuitive graphical interface to configure, manage, and monitor a standalone, stack, or cluster of Cisco Catalyst switches. It is independent of the Cisco IOS Software version on the switch.

Note: This white paper is based on Cisco Configuration Professional release 01.04.00

2. List of supported browsers

- Mozilla Firefox 48 or later
- Microsoft Internet Explorer 11 or later
- Apple Safari 9 or later
- Google Chrome 52 or later

3. List of supported switches

- Cisco Catalyst 2960-X Series Switches
- Cisco Catalyst 2960-XR Series Switches
- Cisco Catalyst 2960-L Series Switches
- Cisco Catalyst 2960-Plus Series Switches
- Cisco Catalyst 2960-CX Series Switches
- Cisco Catalyst 3560-CX Series Switches
- Cisco Catalyst Digital Building Series Switches

4. Where to download the Cisco Configuration Professional software

The Cisco Configuration Professional for Catalyst software is available as an independent software (.tar file) downloadable from the <https://www.cisco.com/go/ccp-catalyst> website.

When customers deploy newer versions of Cisco IOS Software (15.2(5)E or later), Cisco Configuration Professional is bundled with the Cisco IOS image (.tar file).

On newer switches, such as the 2960-L and Digital Building Series, Cisco Configuration Professional is preloaded on the switch at manufacturing and can be used to onboard the switch to the network out of the box without a console connection. Table 1 lists the Cisco IOS Software versions for supported by the various Cisco Catalyst switch series.

Table 1. Supported Cisco IOS versions for different Cisco Catalyst switches

Switch series	Cisco IOS version
2960-X	15.2(5)E1
2960-XR	15.2(5)E1
2960-L	15.2(5c)E
2960-Plus	15.2(5)E1
2960-CX	15.2(5)E1
36560-CX	15.2(5)E1
Digital Building	15.2(5)EX

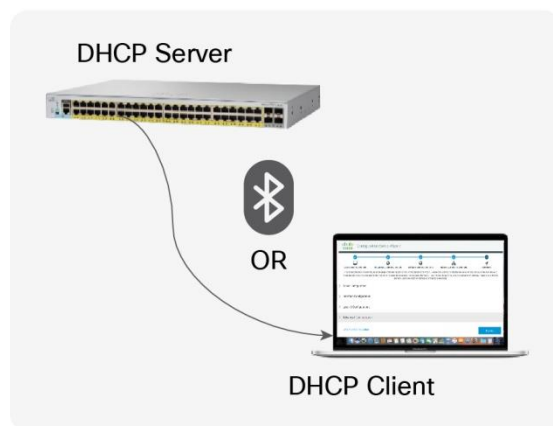
5. Installing new switches with Cisco Configuration Professional

For those switches that are factory-shipped with Cisco Configuration Professional, users can initiate switch installation (day-0 setup) with a PC or tablet browser.

There are two ways of connecting to the switch (Figure 1):

1. Using an Ethernet cable to connect a computer to any Ethernet port of the switch
2. Bluetooth pairing between a computer or tablet and a Bluetooth USB dongle attached to the switch

Figure 1. Connecting a new switch to a laptop, PC, or tablet



5.1 Steps to perform on a switch factory-shipped with Cisco Configuration Professional

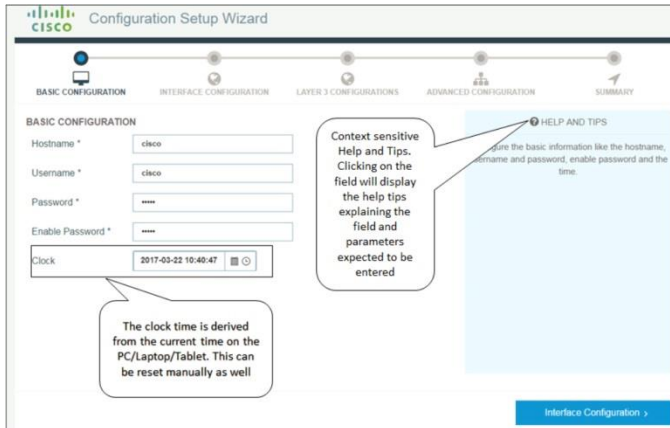
5.1.1 Before the installation procedure

1. Power up the switch and launch the switch to day0 mode following the [instructions](#).
2. Connect to the switch over any Ethernet port. Set the NIC to accept a DHCP IP address.
3. The switch acts as a DHCP server and assigns the connected PC an IP address from a predefined IP pool (10.0.0.0 /24).
4. The switch by default has an IP address of 10.0.0.1. The UI can be accessed on the browser with the IP address 10.0.0.1. Default username/password: cisco/cisco.

5.2 Switch installation steps

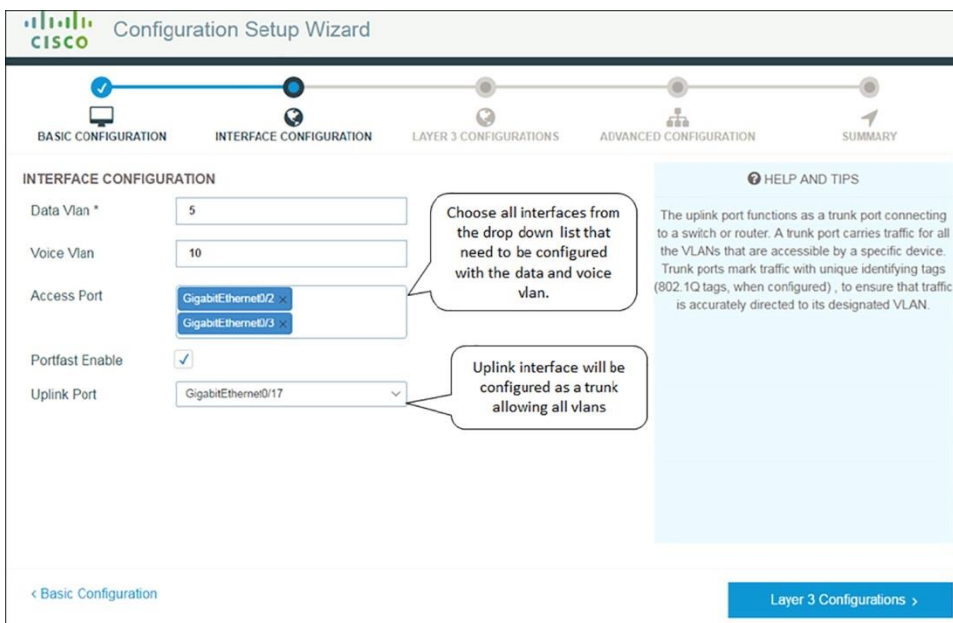
5.2.1 Basic configuration

This step allows users to configure the switch with parameters to identify a switch and minimum mandatory security parameters.



5.2.2 Interface configuration

This step allows users to configure the segmentation parameters and also define the interfaces that will be connected to end-user devices as well as the interface that will connect to the existing network.



5.2.3 Layer 3 configuration

This step allows users to configure the IP address of the switch interfaces that may be used to access the switch or that will serve as a gateway for end devices connected to the switch.

Configuration Setup Wizard

BASIC CONFIGURATION INTERFACE CONFIGURATION **LAYER 3 CONFIGURATIONS** ADVANCED CONFIGURATION SUMMARY

LAYER 3 CONFIGURATIONS

Default Gateway *

Default Route

If the license on the switch allows for routing the default route can be entered

IP Address Assignment

Interface	Existing IP	New IP	Subnet
Vlan1	10.6.0.1	<input type="text"/>	<input type="text"/>
Data Vlan 5	<input type="text"/>	5.5.5.5	255.255.255.0
Voice Vlan 10	<input type="text"/>	<input type="text"/>	<input type="text"/>

Data and voice vlan configured in Step 2 display

If the license on the switch allows for more than one SVI, ip addresses can be assigned to multiple vlans

HELP AND TIPS

Configure the IP Address, default gateway and default route if applicable in this screen. The interfaces configured in the previous step will be available for configuring them with an IP address.

< Interface Configuration Advanced Configuration >

5.2.4 Advanced configuration

This step allows users to enable protocols that will enable access to the switch for configuration once installed on the network.

Configuration Setup Wizard

BASIC CONFIGURATION INTERFACE CONFIGURATION LAYER 3 CONFIGURATIONS **ADVANCED CONFIGURATION** SUMMARY

ADVANCED CONFIGURATION

Enable VTP transparent mode

Enable Telnet

Enable SSH

Domain Name *

RSA Key *

The new switch will be configured by default in VTP mode transparent. Uncheck to change the VTP mode to server

HELP AND TIPS

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

< Layer 3 Configurations Summary >

5.2.5 Summary page

This page allows users to review the configuration options selected in the previous four steps.

The screenshot shows the Cisco Configuration Setup Wizard interface. At the top, there is a progress bar with five steps: BASIC CONFIGURATION, INTERFACE CONFIGURATION, LAYER 3 CONFIGURATIONS, ADVANCED CONFIGURATION, and SUMMARY. Below the progress bar, a summary of the configuration steps is provided. The main content area is divided into three sections: Basic Configuration, Interface Configuration, and Layer 3 Configurations. A callout box with a speech bubble points to the Basic Configuration section, containing the text: "Expand the options to review the configuration options".

Section	Field	Value
Basic Configuration	Hostname	CISCO
	Username	CISCO
	Password	CISCO
	Enable Password	CISCO
	Clock	10:40:47 22 March 2017
Interface Configuration	Data Vlan	5
	Voice Vlan	10
	Access Port	GigabitEthernet0/2 GigabitEthernet0/3
	Portfast Enable	Enable
	Uplink Port	GigabitEthernet0/17
Layer 3 Configurations	Default Gateway	5.5.5.1

Once the configuration is submitted, the IP address assigned to the switch changes to the IP address configured on the Layer 3 Configuration screen (section 3.2.3).

The user interface will be redirected to this new IP address.

6. Installing Cisco Configuration Professional on existing switches

This section describes how to use Cisco Configuration Professional on supported switches in existing deployments. This is for switches that were not factory-shipped with Cisco Configuration Professional or cannot be upgraded to the Cisco IOS Software version that is bundled with Cisco Configuration Professional.

Note: Cisco Configuration Professional for Catalyst is independent of the switch Cisco IOS Software.

There are two options for installing Cisco Configuration Professional:

1. Download only Cisco Configuration Professional and use the existing Cisco IOS Software (download only the CCP-C.tar).
2. Download a Cisco IOS bundle file that contains Cisco Configuration Professional and a newer version of Cisco IOS.

6.1 Steps to install CCP-C.tar

1. Browse to <https://www.cisco.com/go/ccp-catalyst> and download the CCP.tar image for the switch.
2. Download the CCP-CATALYST file to the switch flash.
3. Create a directory on the flash:
mkdir flash:CCP-CATALYST
4. Expand the .tar file in the flash:
archive tar /xtract flash:c2960l-cwml.tar flash:CCP-CATALYST

5. Configure the switch parameters.
6. Point the switch to the CCP-CATALYST files:


```
ip http path flash:CCP-CATALYST
```
7. Specify authentication parameters:
 - a. `ip http authentication enable`
 - b. `ip http authentication aaa/local`
8. Enable the switch to act as the HTTP server:
 - a. `ip http server`

Access Cisco Configuration Professional from the web browser by using the IP address configured on the switch.

The username and password will be as configured on the switch locally or using AAA.

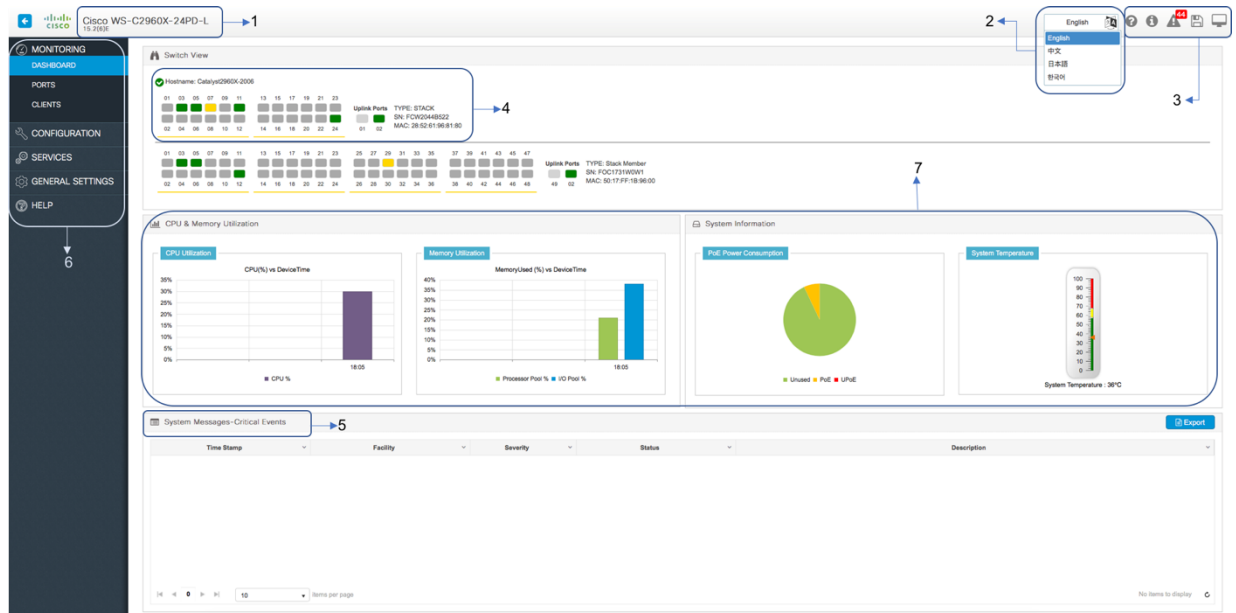
6.2 Steps to install Cisco IOS Software (.tar image)

The procedure is the same as the Cisco IOS upgrade procedure on a switch with a .tar image.

7. Introduction to the user interface

7.1 Monitoring dashboard






The dashboard provides a single-pane view of the switch. The user can monitor the connected and error ports, the health of the switch, Power over Ethernet (PoE) available, critical alerts on the switch, etc.



This is a single-pane view of the switch, and it provides the following details:

1. **Switch details:** Hardware type of the switch and the Cisco IOS Software version currently running on it.
2. **Language support:** The user interface can be converted to easily support other languages.
Current language support: English (default), Mandarin, Japanese, and Korean

3. **Icons:**

-  Opens a guide to explain the features being configured on the switch.
-  Displays the version of Cisco Configuration Professional running on the switch.
-  Displays the latest system logs from the switch.
-  Clicking this icon will save the current configuration of the switch to the startup configuration.
-  Clicking this icon brings up the Command-Line Interface (CLI).

4. **Switch view:** Dynamic display of switch ports and their status for each switch, along with display of its hostname, serial number, and MAC address. In the case of a stack, details about the role of each switch, such as primary or stack member details, are displayed.

5. **System messages:** Displays the critical switch logs. Only the Critical, Alerts, and Emergency logs are displayed here.

The logs are color-coded to show the level of the log.

The logs can be exported to an Excel spreadsheet for troubleshooting or attaching to a Cisco Technical Assistance Center (TAC) case.

6. **Navigation pane:** The pane is a tree design with two levels of branching.

The first level has Monitoring, Configuration, Services, General Settings, and Help.

- **Monitoring**

Dashboard: A single-page view of the switch health.

Ports: Displays all the port statistics. The error counters on the individual and bundled ports are displayed on this page.

Clients: Gives a snapshot view of the end devices connected to the switch and also provides details such as:

- Switch port to end device mapping
- Device type (router, switch, IP phone, Windows PC, etc.)
- VLAN of the end device
- MAC address of the end device
- IP address of the end device
- Power drawn by the end device
- Operating system of the end device

This list can be exported as a spreadsheet and saved for auditing purposes.

- **Configuration**

Switch: General and basic switch configurations can be done on this page (such as setting the hostname, switch IP address, Maximum Transmission Unit [MTU], etc.) Other switch-level settings such as physical stacking, virtual stacking parameters, spanning tree, VLAN Trunking Protocol, and Bluetooth can be configured here.

Ports: Port parameters such as VLAN association, DHCP Snooping, quality of service, and storm control parameters can be configured on this page.

Troubleshooting: Basic troubleshooting, such as connectivity of devices from the switch, can be performed by using ping or traceroute. Device health checks can be performed by running diagnostics. The user can also erase switch configurations or reload the switch stack or individual switch.

VLAN: Configuration related to VLAN, such as creation of Layer 2 VLAN and Switch Virtual Interface (SVI), as well as setting up IP DHCP Snooping on a list of VLANs in order to secure the network, can be done on this page.

- **Services**

NetFlow: Allows configuration of the switch to export details of the packets sent to the switch on different ports.

Static routing: Through this page, users can create new static routes or modify or delete existing routes on supported platforms.

Security: Users can set up comprehensive security on the switch through this pane by configuring port-based Authentication, Authorization, and Accounting (AAA) using either RADIUS, TACACS+, or Lightweight Directory Access Protocol (LDAP) along with support for multiple access policies such as IEEE 802.1X, MAC Authentication Bypass (MAB), and WebAuth.

ACL: Access control lists can be configured through this page, allowing the administrator to limit network traffic and restrict network access to certain users and devices.

Energy Saver: Using this service, user can harness the potential of Cisco EnergyWise® and Energy-Efficient Ethernet (EEE) to decrease energy consumed by the switch and endpoints connected to the switch by setting different power levels and using the Cisco EnergyWise Wake on LAN feature.

- **General Settings**

Management: HTTP and SNMP parameters can be configured on this page.

Software update: Provides administrators an option to upgrade the Cisco Configuration Professional version or the switch Cisco IOS version remotely through the local system.

System: Various time-related settings, such as setting the time zone and adding a Network Time Protocol (NTP) server can be done through this page. Administrators can also create Dynamic Host Configuration Protocol (DHCP) scopes and transfer a configuration file to or from the switch into a Trivial FTP (TFTP) server or local system.

User Administration: Allows administrators to control access to the switch by setting up new users and their privilege levels, modifying the password or privilege level of existing users, and deleting users altogether.

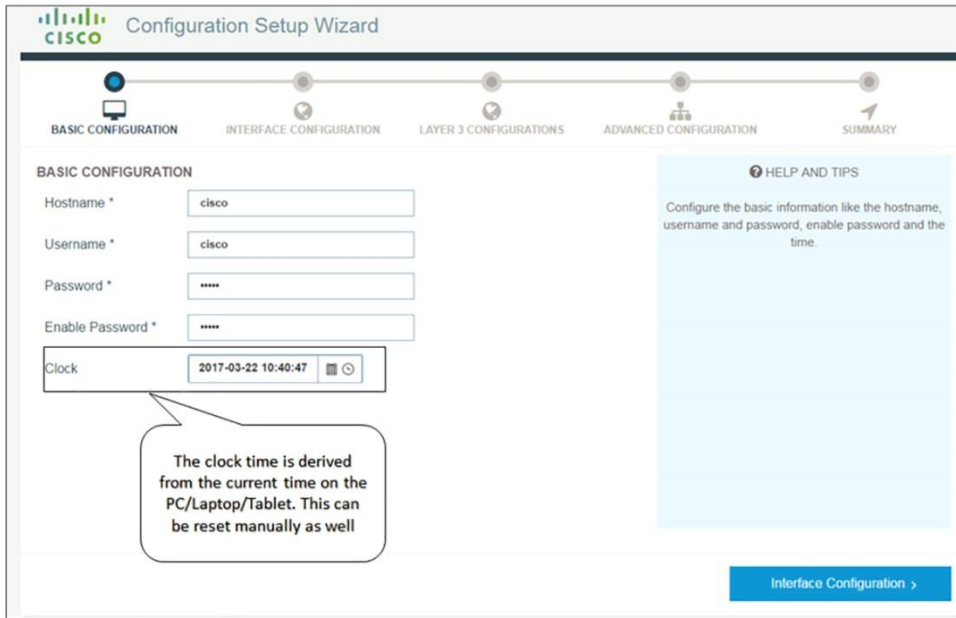
7. **Switch information:** Dashlets displaying critical real-time system information such as CPU and memory utilization, system temperature and power consumption. The dashboard is refreshed every 60 seconds with updated data.

8. Configuring switch system settings

8.1 Set clock

8.1.1 Set system clock during initial setup

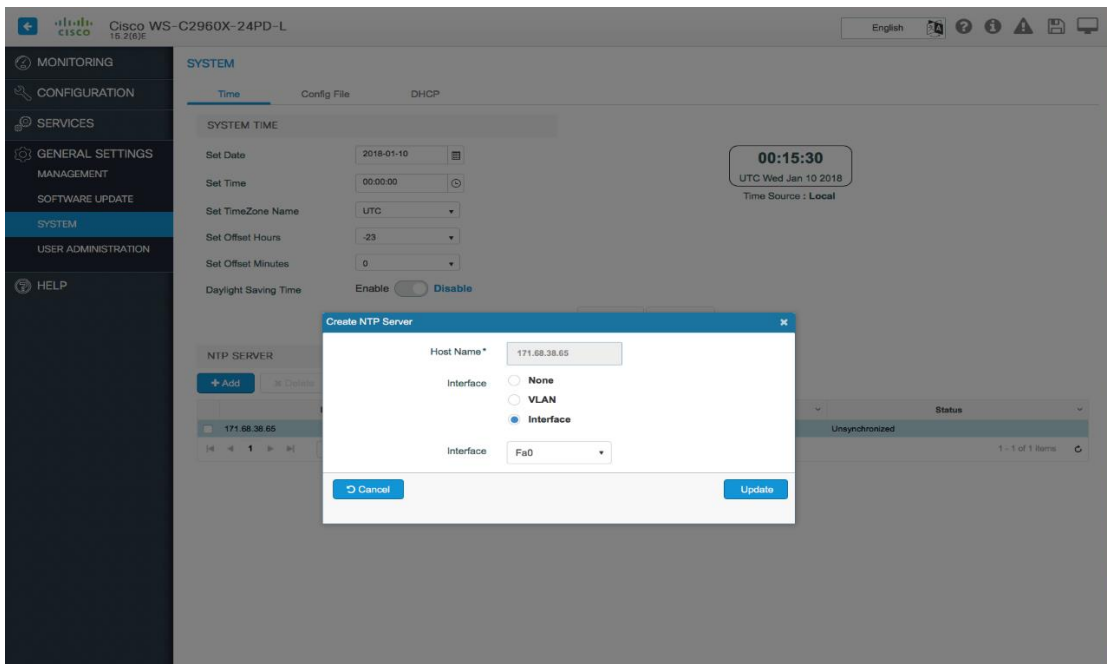
During the initial setup of switches shipped with Cisco Configuration Professional, the date and time is populated automatically from the clock on the user's laptop. They can also be set manually.



8.1.2 Set system clock later with Cisco Configuration Professional

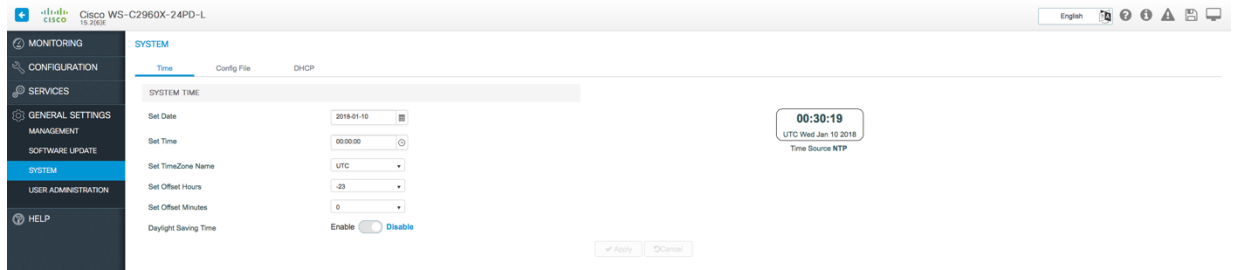
Configure clock to synchronize with NTP server

A user can synchronize the switch clock by configuring an NTP server under **General Settings > System > Time**. Once an NTP server is added, the user can check the synchronization status on the same page.



Configure clock manually

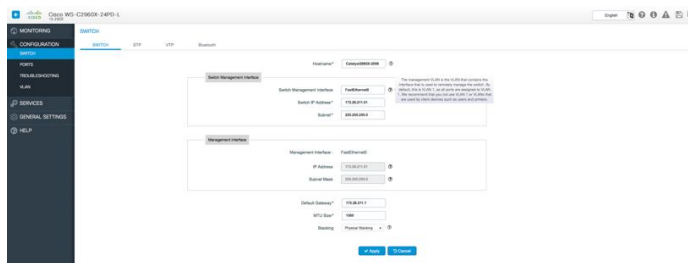
A user can also set the system time manually on the switch, along with advanced options such as setting the time zone and enabling daylight savings. These settings can be found under **General Settings > System > Time**.



8.2 Basic switch configuration

Basic attributes of the switch, such as the hostname, default gateway or route, system MTU, and switch management IP address can be configured on this page.

Note: Hovering over the “?” explains the fields in detail. The input ranges are also explained.

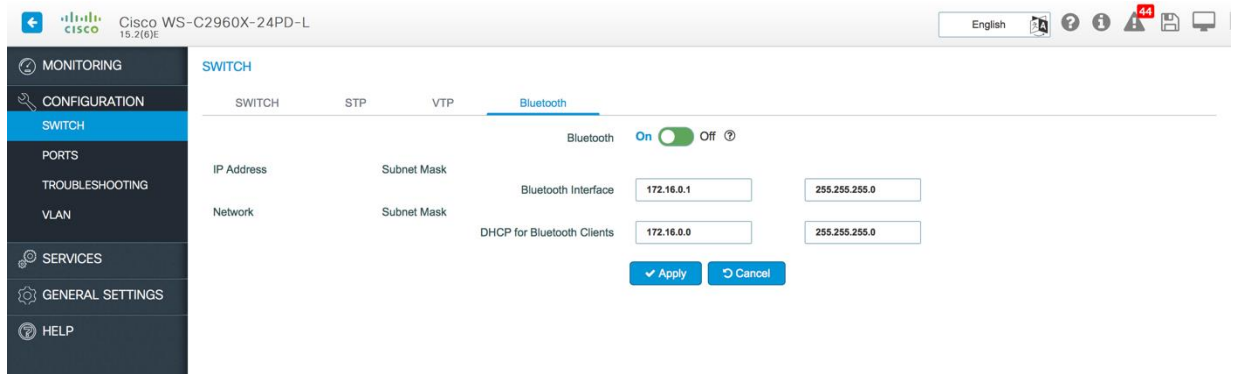


9. Connect via Bluetooth

9.1 Steps to connect to the switch via Bluetooth

Over-the-air access to the web UI and CLI through Telnet and SSH is available for switches that support an external Bluetooth dongle that plugs into the USB port, providing easy access to the switch. Cisco Configuration Professional provides an easy way to configure the switch for Bluetooth under **Configuration > Switch > Bluetooth**:

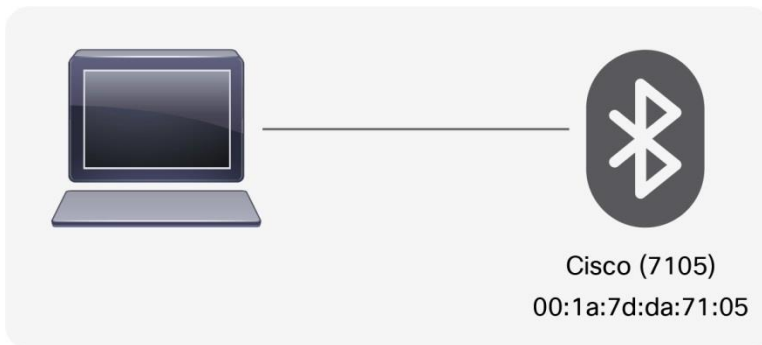
- Connect a Bluetooth dongle to the USB port on the switch (USB 2.0 with Bluetooth version 4.1).
- Once the dongle is connected, toggle Bluetooth to On.
- Assign an IP address to the Bluetooth interface.
- Create a DHCP pool for the Bluetooth PAN devices in the same subnet as the Bluetooth interface.



- Scan for Bluetooth devices from the laptop.

Note: The dongle name shows up with the last four characters of the MAC address.

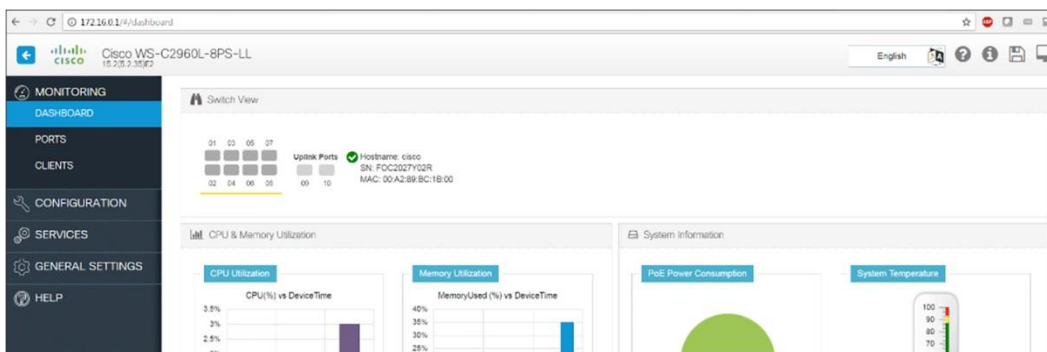
```
cisco#show bluetooth stats
BT Interface is Ready
BT Dongle Present: Yes
BT Stack Enabled: Yes
BT Stack Ready: Yes
Attached BT dongle mac: 00:1A:7D:DA:xx:xx
```



Once the device is connected via Bluetooth, you will see the following:

```
cisco#show ip interface brief Bluetooth0
Interface          IP-Address      OK? Method Status          Protocol
Bluetooth0        172.16.0.1     YES NVRAM  up
```

- You will now be able to access the user interface of the switch by typing the IP address of the Bluetooth interface in the browser.



10. Connecting uplinks

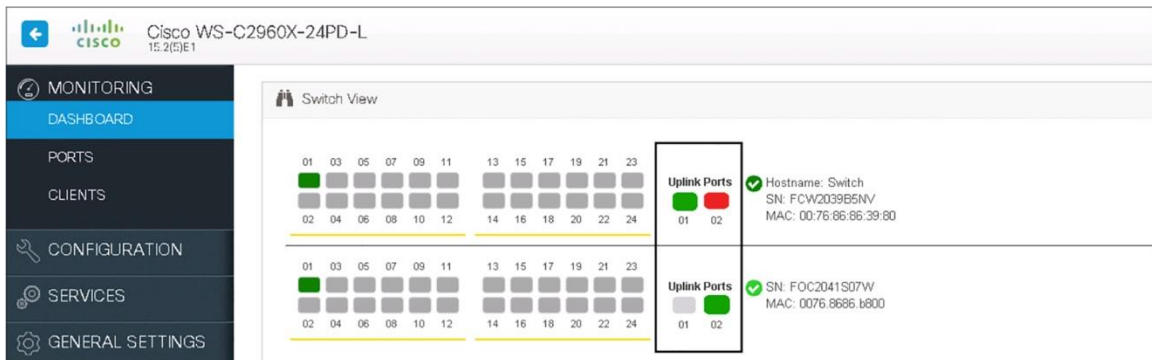
The switches connect to other network devices on ports marked “Uplink Ports.” These are highlighted in the figure below.

The color of a port indicates its status.

Gray: Port is “down.”

Green: Port is “up.”

Red: Port is in “error” condition.



The uplink can be a single port (standalone interface) or can be multiple ports bundled together (Link Aggregation Group [LAG] interface or EtherChannel).

An uplinks can be configured as a trunk interface (Layer 2 port) or can be assigned an IP address (Layer 3 port).

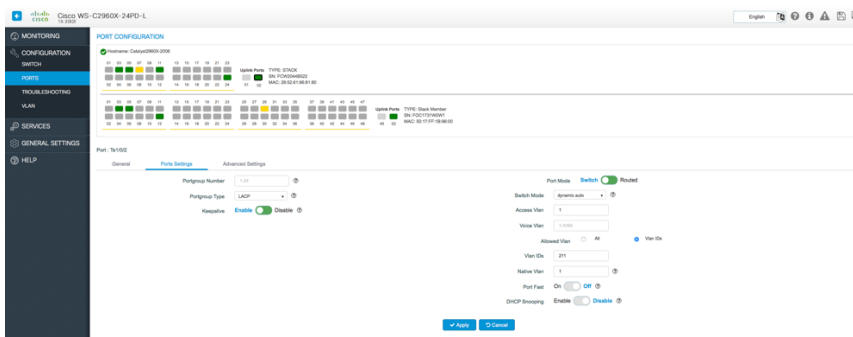
10.1 Standalone uplink interface

A single trunk port can be configured by selecting the appropriate port from the port view under **Configuration > Ports**, which allows configuration to be set all the way from adding a description to configuring Auto QoS. A user can also easily configure the port as a routed port by toggling the port mode.

On the same page, Cisco Configuration Professional allows users to configure multiple ports at once.

To configure multiple ports at once, select multiple ports in the switch view (to select multiple ports in Windows, Ctrl-click; on a Mac, Command-click).

Note: When multiple interfaces are selected, the old port configurations of the individual ports are erased.



10.2 Bundled uplink interfaces (LAG)

Multiple ports can be selected and bundled to act as one port.

After selecting the interfaces to bundle, select the protocol to bundle: Link Aggregation Control Protocol (LACP), Port Aggregation Protocol (PAgP), or ON.

Also enable or disable the keep-alive, based on whether the aggregation method needs to be active/passive or Desirable/Auto.

Portgroup Number 2

Portgroup Type LACP

Keepalive LACP

Port Mode Switched

Switch Mode dynamic auto

Access Vlan 1

Voice Vlan 1-4094

Allowed Vlan All

Vlan IDs 1-4094

Native Vlan 1

Port Fast On

DHCP Snooping Enable

Apply Cancel

Once the port channel is configured and the ports are bundled in the port channel, the port statistics of the port channel can be viewed on the Monitoring dashboard under **Monitoring > Ports**.

Switch/Port	Description	Status	PortType	VLANIP	Duplex	Power	Speed	TxBytes	RxBytes	PktsDrop	SwitchType
Gi1/0/1		not connected	Access	1	auto	0.0	auto	0	0	0	Master
Gi1/0/2		not connected	Access	1	auto	0.0	auto	0	0	0	Master
Gi1/0/3		connected	Access	1	a-full	0.0	a-1000	212561564	0	0	Master
Gi1/0/4		connected	Access	1	a-full	0.0	auto	0	0	0	Master
Gi1/0/5		connected	Access	1	a-full	0.0	a-1000	212557137	3844406	0	Master
Gi1/0/6		not connected	Access	1	auto	0.0	auto	0	0	0	Master
Gi1/0/7		connected	Access	9	a-full	12.8	a-1000	120587197	64375169	0	Master
Gi1/0/8		not connected	Access	1	auto	0.0	auto	0	0	0	Master
Gi1/0/9		not connected	Access	1	auto	0.0	auto	0	0	0	Master
Gi1/0/10		not connected	Access	1	auto	0.0	auto	0	0	0	Master

Port Te1/0/2

	Packets	Total	Sent	Received
Total	1448201	1336169	112035	112035
Broadcast	146928	146928	0	0
Multicast	1301709	1189241	112035	112035
CRC Errors	0	0	0	0
Runs	0	0	0	0
Errors	0	0	0	0

PORT CHANNEL SUMMARY

Group	Port-channel	Protocol	Ports	SwitchType
2	Po2	LACP	Te1/0/2,Te1/0/2	Master

Clear Counters

All counters related to the port selected. Also displayed are the details related to the port channel of selected interface.

11. Managing endpoint devices

11.1 Monitoring endpoint devices (clients)

Clients can be connected to the physical ports on the switch.

The type of end clients connected and their details, such as their MAC address, IP address, VLAN associated, and power drawn from the switch can be viewed on the Clients page under **Monitoring > Clients**. This list can also be exported to a spreadsheet for easy documentation.

MAC	Switch Port	Client Name	OS	Manufacturer	IP	VLAN	PoE Drawn	Images
DigibEthernet1024	Branch-24-SW1		Cisco IOS Software	cisco WS-C2960X-48PD-L	172.28.211.31	211	DW	
DigibEthernet7012	Catalyst2960X-2009		Cisco IOS Software	cisco WS-C2960X-24PD-L	172.28.211.90	1	DW	
DigibEthernet1011	Catalyst2960X-2009		Cisco IOS Software	cisco WS-C2960X-24PD-L	172.28.211.90	1	DW	
DigibEthernet1017	SEPACAS191C9A8B		ipsw713-4-25R2-2	Cisco IP Phone 9971	30.0.0.3	NA	12.80W	
DigibEthernet7009	SEPACAS191C9A8B		ipsw713-3-133	Cisco IP Phone 9971	30.1.1.102	NA	14.99W	
TeDigiEthernet1022	Catalyst2960X-2008		Cisco IOS Software	cisco WS-C2960X-24PD-L	30.0.0.1	1	DW	
TeDigiEthernet1023	Catalyst2960X-2008		Cisco IOS Software	cisco WS-C2960X-24PD-L	30.0.0.1	1	DW	
DigibEthernet1005	Catalyst2960X-2008		Cisco IOS Software	cisco WS-C2960X-24PD-L	30.0.0.1	1	DW	
DigibEthernet7005	Catalyst2960X-2008		Cisco IOS Software	cisco WS-C2960X-24PD-L	30.0.0.1	1	DW	
FastEthernet0	VLAN_211		Cisco IOS Software	cisco WS-C3750X-48	172.28.211.2	211	DW	

11.2 Configurations for endpoints

Different kinds of end clients can connect to the switch, such as IP phones, PCs, cameras, access points, VM servers, printers, point-of-sale devices, etc. Cisco Configuration Professional provides ways to easily monitor and manage clients connected.

11.2.1 Monitoring PoE clients

If the end client is drawing power from the switch to boot up, the port clearly indicates the amount of power being drawn. To see this, hover over the port in the switch view of the Monitoring dashboard under **Monitoring > Ports**.

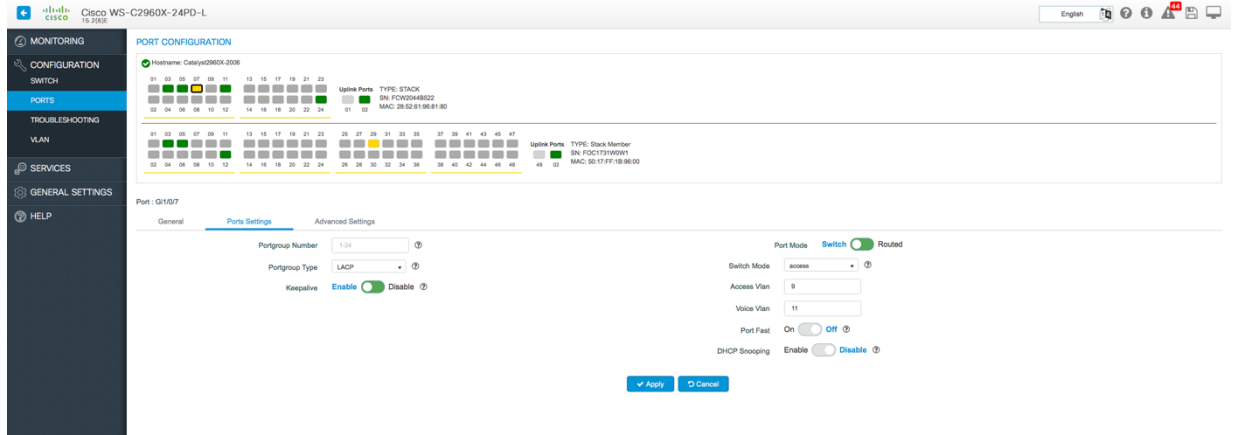
SwitchPort	Description	Status	Access
Gi1/0/1		not connected	Access
Gi1/0/2		not connected	Access
Gi1/0/3		connected	Access

11.2.2 Configuring data and voice VLANs for clients

When PCs and laptops are connected to the IP phone port, which in turn is connected to the switch port, it is best practice is to segregate the voice traffic from the IP phone and the data traffic from the PC. Configure the port to send phone traffic on a voice VLAN and traffic from PCs on the data VLAN.

Click on the port that needs to be configured in the switch view.

Note: Multiple ports can be selected to apply configurations at the same time (on a Windows PC, Ctrl-click; on a Mac, Command-click). Any preexisting configurations on the ports selected will be erased.



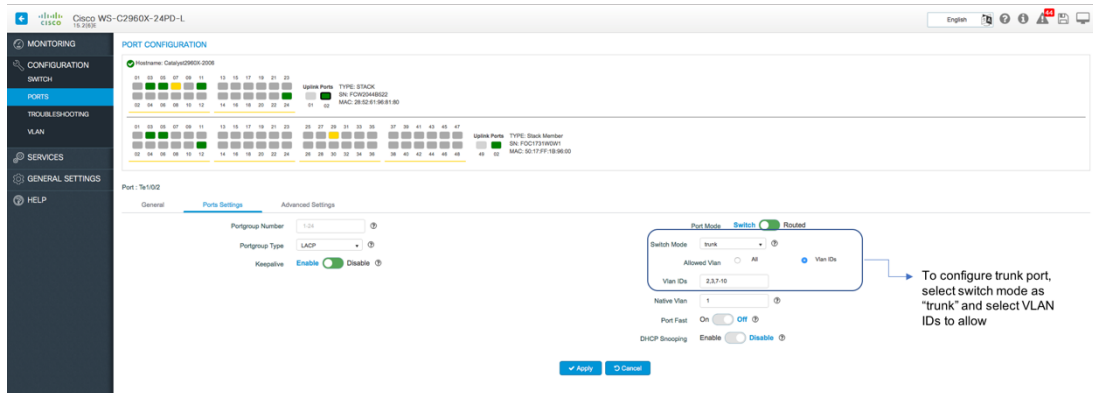
11.2.3 Ports as trunks

When connecting VM server ports or access points that carry WLAN traffic to the switch, the switch port will need to be configured as a trunk.

Click on the port that needs to be configured.

Filter the VLANs allowed on the trunk by selecting the VLAN IDs and listing the VLANs under the VLAN IDs, separated by commas (,) or hyphens (-).

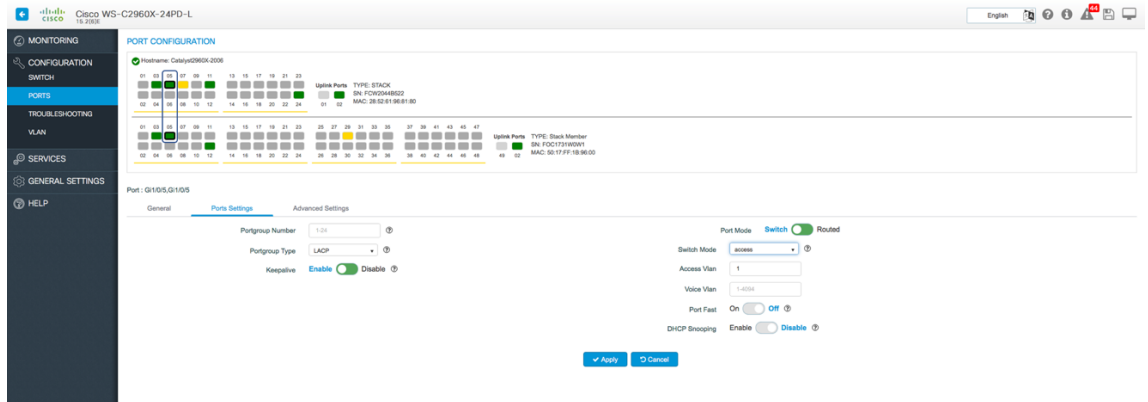
Note: Multiple ports can be selected to apply configurations at the same time (on a Windows PC, Ctrl-click, on a Mac, Command-click). The preexisting configurations on the ports selected will be rewritten to default configurations.



11.2.4 Bundle multiple access ports as LAG (EtherChannel)

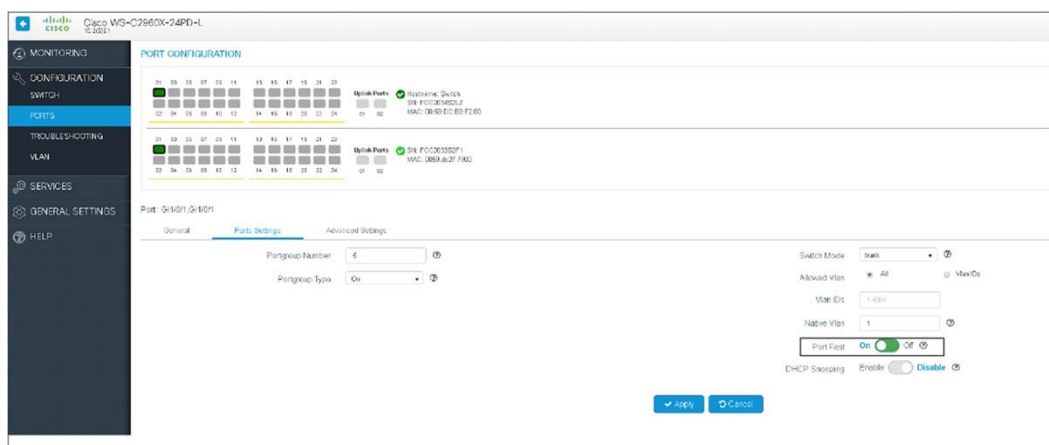
When connecting multiple ports of a switch to multiple ports on the end client, such as servers or hubs, to get better throughput multiple interfaces can be selected and configured in a bundle. (To select multiple interfaces on Windows, Ctrl-click; on a Mac, Command-click.)

Note: When multiple interfaces are selected, the original configurations on the interfaces are erased.



11.2.5 Speed up client connections (portfast)

Ports connecting to phones, lights, etc. sometimes need to be transitioned from listening to a forwarding state in groups of 5 instead of in groups of 60.



12. Administrative workflows

12.1 Gain visibility into the traffic pattern passing through the switch or switch stack

NetFlow can be configured on the switch to export details of the packets forwarded to and from the switch in order to gain visibility into the network.

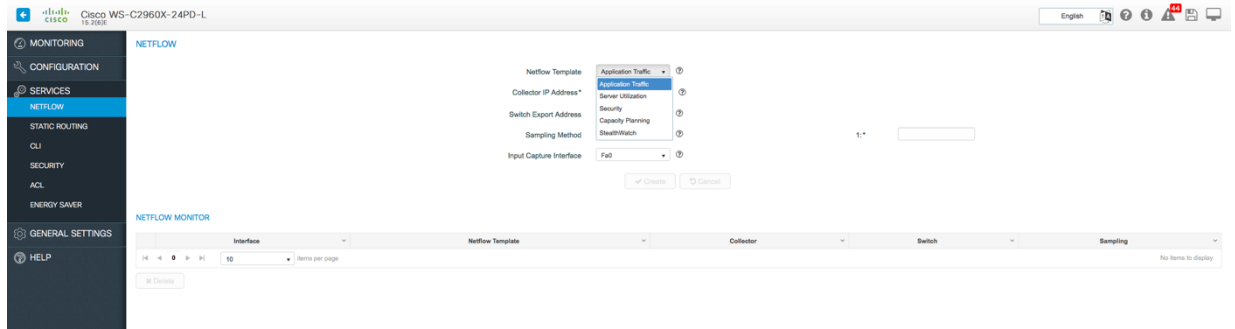
NetFlow can now be configured with Cisco Configuration Professional with just a few clicks under **Services > NetFlow**. Templates are used to configure NetFlow, thus eliminating the need to understand a complicated set of commands.

The 2960-X and 2960-XR Series support full NetFlow from Cisco IOS 15.2(5)b onward with minimal impact on performance. (Check the configuration guide for the switch model to confirm that it supports NetFlow.)

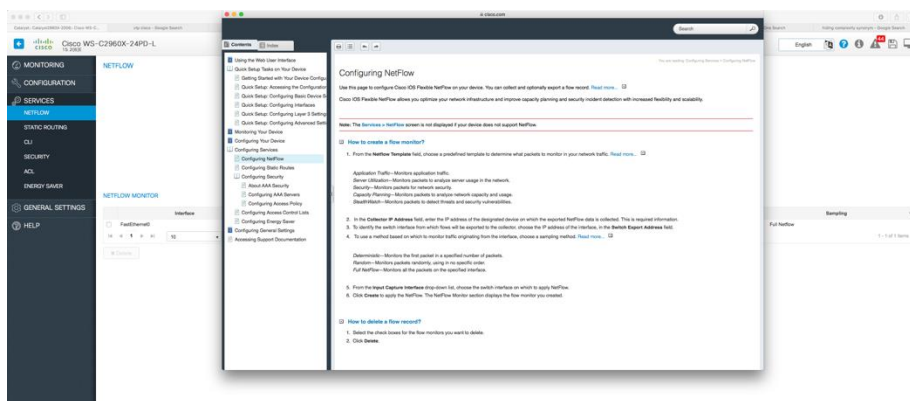
Choose the template and sampling method based on the reason for enabling NetFlow. Full, Random, and Deterministic sampling methods are supported.

Configure the IP address of the collector (using software such as Lancope or Cisco Stealthwatch® that displays the information collected and exported by the switch in a human-readable form).

Apply the configured parameters to the switch interface (VLAN, port etc.).



Note: Refer to the switch configuration guide to understand NetFlow in detail.



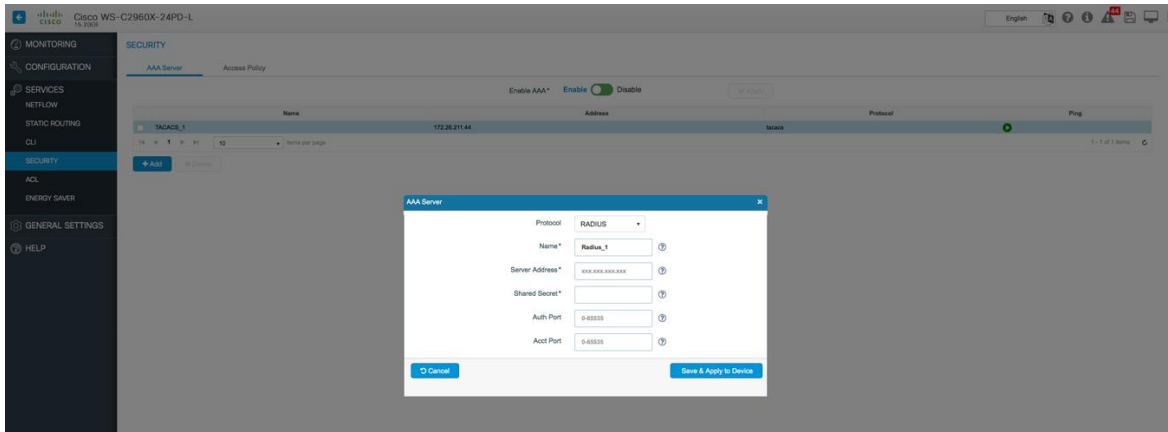
All the interfaces (VLAN and physical ports) configured with NetFlow can be viewed under the Flow monitor list.

NetFlow applied to the interface can be deleted with a single click.

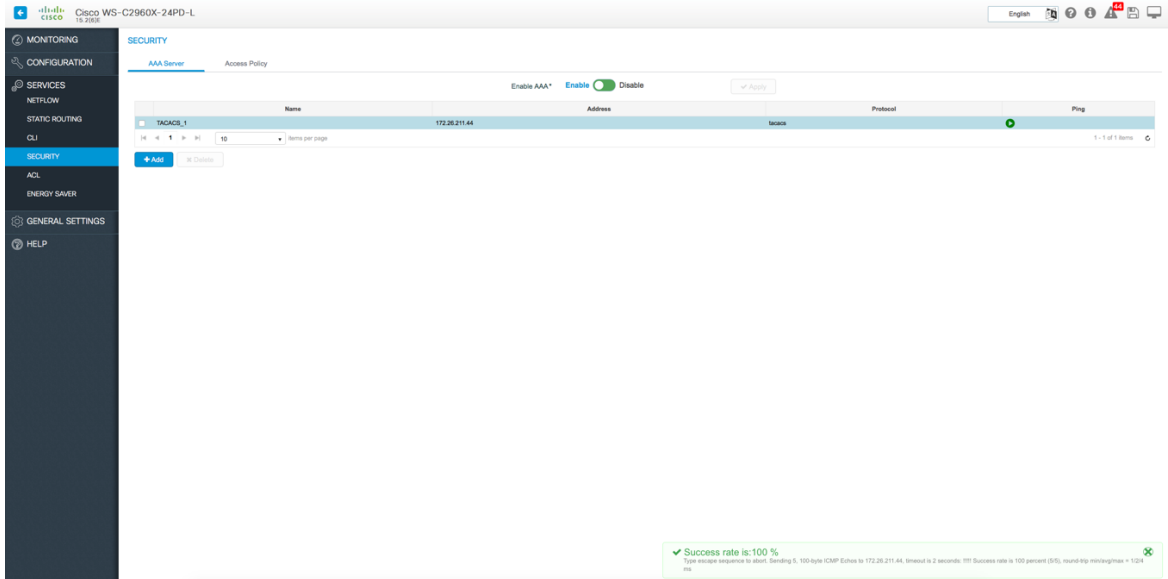
12.2 Secure the network by protecting the switch against vulnerabilities

Protecting the network at the access layer is not only essential for the integrity of the network but also saves crucial bandwidth by filtering rogue data closer to endpoints as packets travel toward the core. Cisco Configuration Professional enables administrators to secure the network against rogue clients, servers, and application traffic by providing options to configure AAA, ACL, and IP DHCP Snooping.

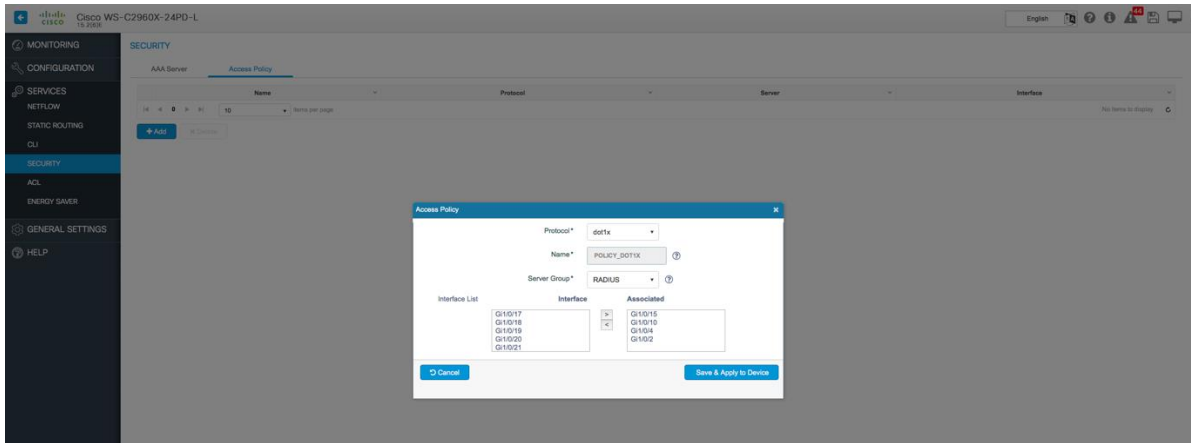
Administrators can control a client's access by configuring AAA services. Based on the deployment model and network requirement, a user has the flexibility to configure and manage RADIUS, TACACS+, and LDAP servers under **Services > Security > AAA Server**.



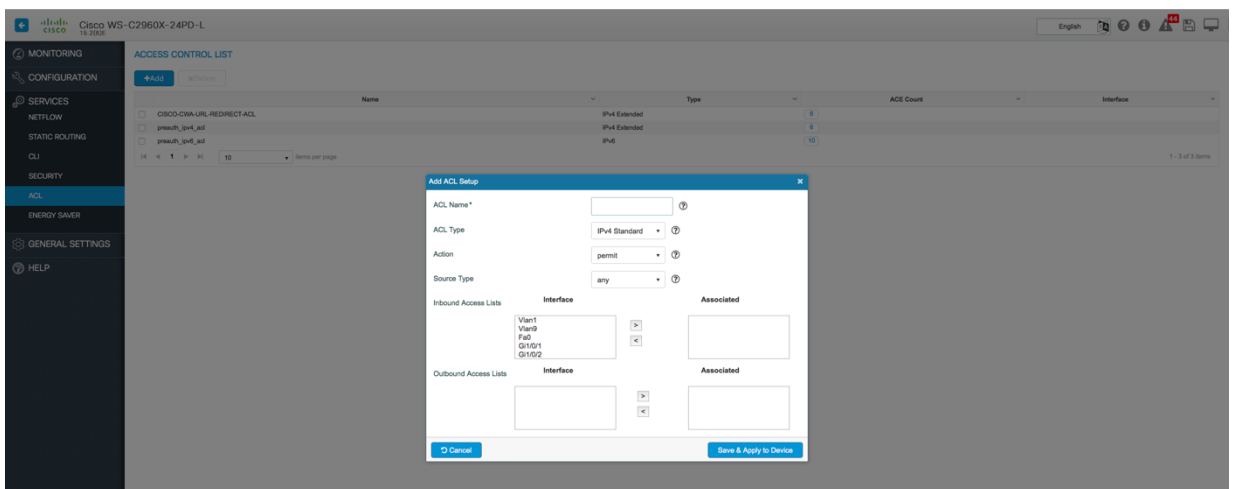
Once an AAA server is added, a user can modify server properties, verify its reachability, or delete the server altogether, thus allowing complete management and monitoring through the same window.



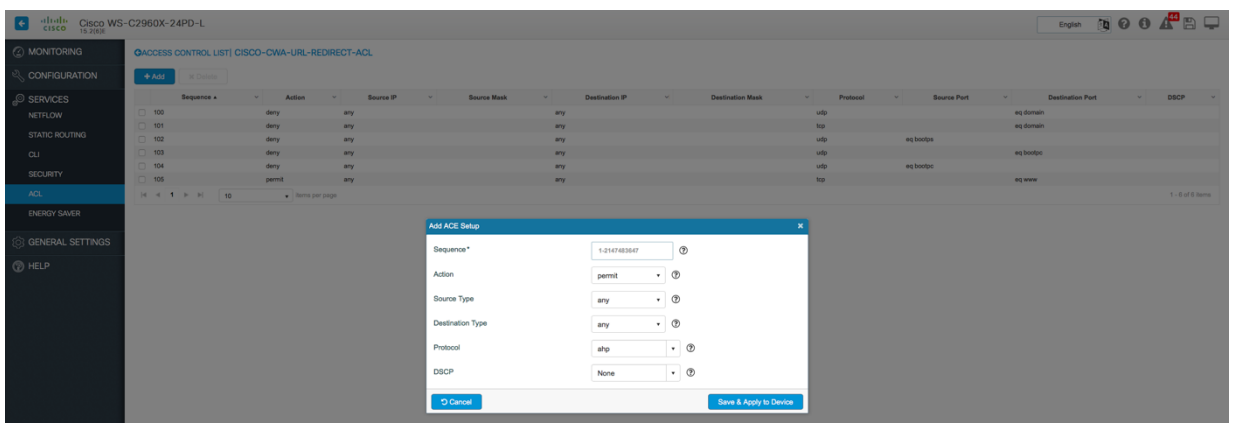
For 802.1X supplicants, IEEE 802.1X can be configured. For devices that do not support 802.1X the administrator also has the option to configure MAC Authentication Bypass and WebAuth through Cisco Configuration Professional under **Services > Security > Access Policies** and apply the settings to multiple interfaces at once.



While an administrator can secure the network against unwanted clients through AAA, there still is a possibility of rogue application traffic coming in through authorized clients. To protect the network against such traffic, the user can configure ACLs under **Services > ACL** and apply them to VLANs and ports.



Once an ACL list is created, the user has the option to create, modify, and delete multiple access control entries associated with the ACL.

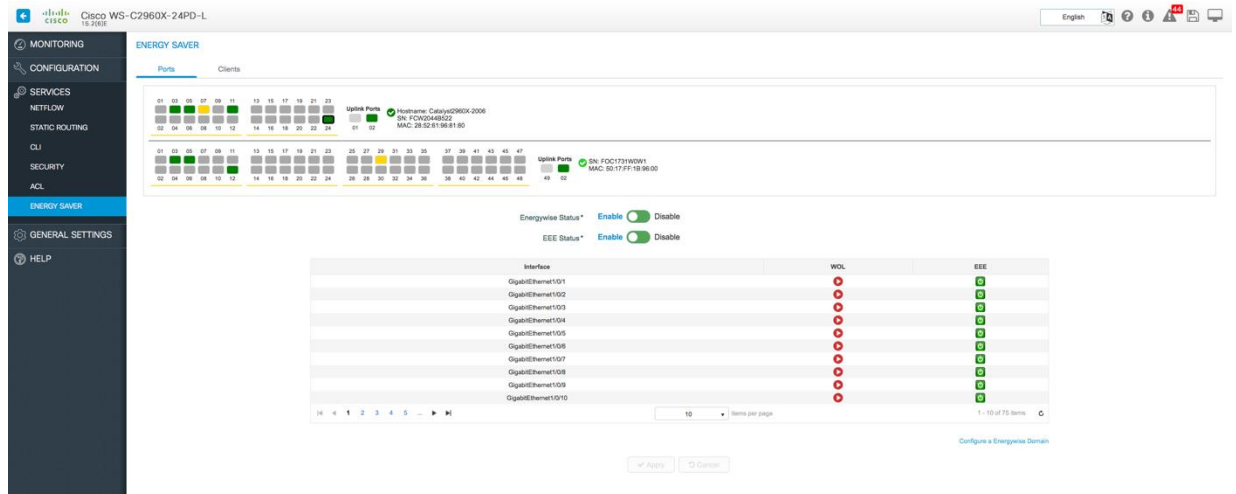


When using DHCP, the switch could be exposed to various potential exploits through untrusted servers. Cisco Configuration Professional allows you to secure your network against such vulnerabilities by providing options to set IP DHCP Snooping, either under **Configuration > VLAN > IP DHCP Snooping** or under **Configuration > Ports > Port Settings**.

Note: Enabling IP DHCP Snooping places all ports in untrusted mode by default, thus blocking various DHCP messages. Please read the configuration guide before enabling this feature.

12.3 Conserve operational expenses through energy saver

Cisco EnergyWise, along with EEE, can provide insight into power usage and help reduce energy costs significantly. Cisco Configuration Professional can be used to tap into those savings by providing an easy-to-use method to provision Cisco EnergyWise and EEE on your Cisco Catalyst switch under **Services > Energy Saver**.



A user can simply enable EnergyWise and EEE, and the switch will be configured with default values for the EnergyWise domain, which can be easily overridden by selecting **“Configure an EnergyWise Domain.”**

A user can also send a Wake on LAN (WoL) magic packet to a specific device on an EnergyWise network by clicking the Play button next to the interface.

Note: A red Play icon indicates that there are no clients connected to this interface and therefore WoL is not available.

Energy Efficient Ethernet can be enabled at all ports by toggling EEE Status to Enable.

ENERGY SAVER

Ports Clients

Energywise Status* Enable Disable

EEE Status* Enable Disable

Interface	WOL	EEE
GigabitEthernet1/0/31		
GigabitEthernet1/0/32		
GigabitEthernet1/0/33		
GigabitEthernet1/0/34		
GigabitEthernet1/0/35		
GigabitEthernet1/0/36		
GigabitEthernet1/0/37		
GigabitEthernet1/0/38		
GigabitEthernet1/0/39		
GigabitEthernet1/0/40		

10 items per page 31 - 40 of 48 items

✓ Successfully submitted the request to run WoL
EnergyWise query, timeout is 6 seconds: Success rate is (0/0) setting entities Queried: 0 Responded: 0 Time: 0.001 seconds

Granular control over power settings is provided per interface, thus giving users the flexibility to control behavior at either the switch or interface level. A green icon for EEE on each interface indicates that it is enabled; it can be turned off simply by clicking the icon, which will turn red once disabled.

ENERGY SAVER

Ports Clients

Energywise Status* Enable Disable

Clients	SwitchPort	Power Level
Branch-24-5911	GigabitEthernet1/0/24	Full
Catalyst2960L-2009	GigabitEthernet1/0/12	Full
Catalyst2960L-2009	GigabitEthernet1/0/11	Full
SEP1624161024488	GigabitEthernet1/0/7	Sleep
SEP160482133383	GigabitEthernet1/0/29	Hibernate
Catalyst2960X-2006	TenGigabitEthernet1/0/2	Full
Catalyst2960X-2006	TenGigabitEthernet1/0/2	Full
Catalyst2960X-2006	GigabitEthernet1/0/8	Full
Catalyst2960X-2006	GigabitEthernet1/0/5	Full
VLAN_211	FastEthernet0	Full

10 items per page 1 - 10 of 10 items

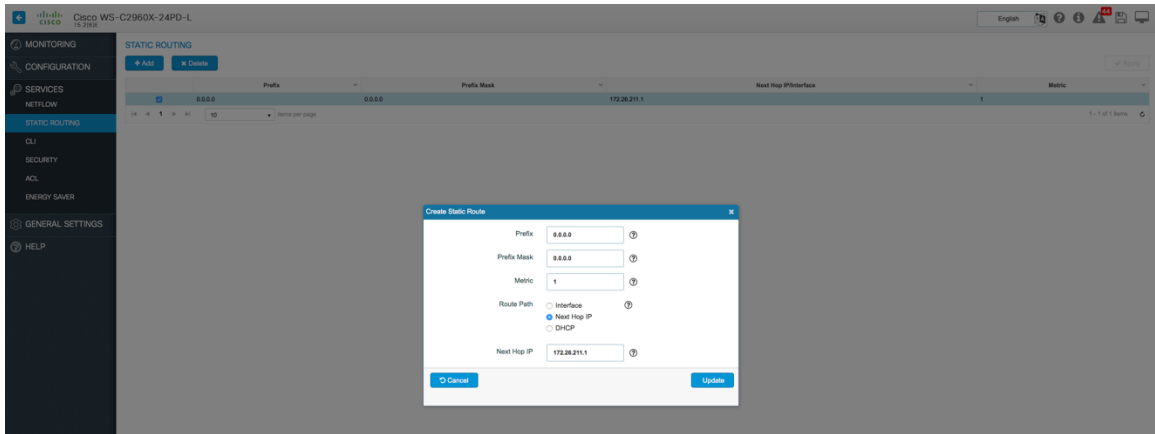
Apply to all

Under **Services > Energy Saver > Clients**, the user can use EnergyWise power levels to consistently manage power usage for the clients connected. Power levels supported are Full (10), Sleep (2), Hibernate (1), and Shut (0).

12.4 Add a static route

Static routes can be added on the switches from Cisco Configuration Professional (the license on the switch needs to support it).

Note: "IP routing" on the switch is enabled automatically when a static route is applied.



12.5 Replace a faulty switch with a new switch

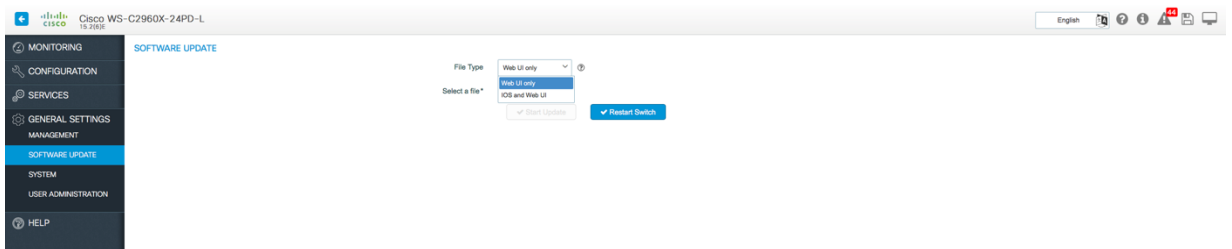
Before replacing any switch in the network, the new switch needs to be brought to the exact same state as the old switch in terms of Cisco IOS version, configuration, etc.

12.5.1 Upgrade Cisco IOS on the new switch to match the old switch

The Cisco IOS version on the new switch can be changed without the need for complex setup of TFTP/FTP file servers.

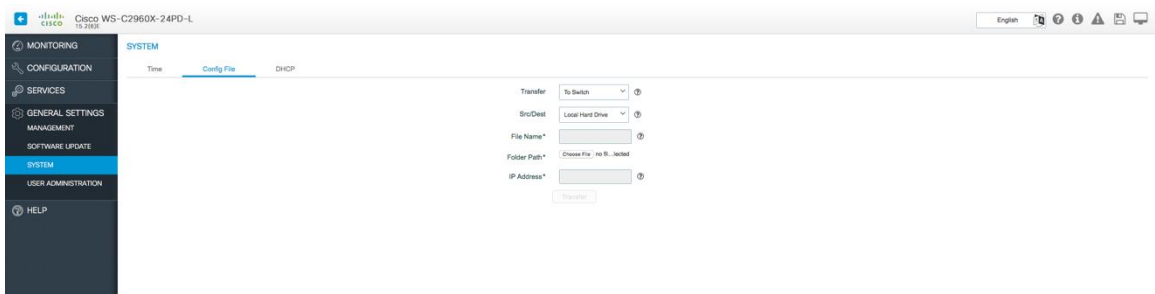
Download the Cisco IOS file (the same version that is running on the old switch) from Cisco.com to the local system.

Under **General Settings > Software Update** select IOS and Web UI from the drop-down. Point to the file to upgrade to on Cisco Configuration Professional and click Start Update.



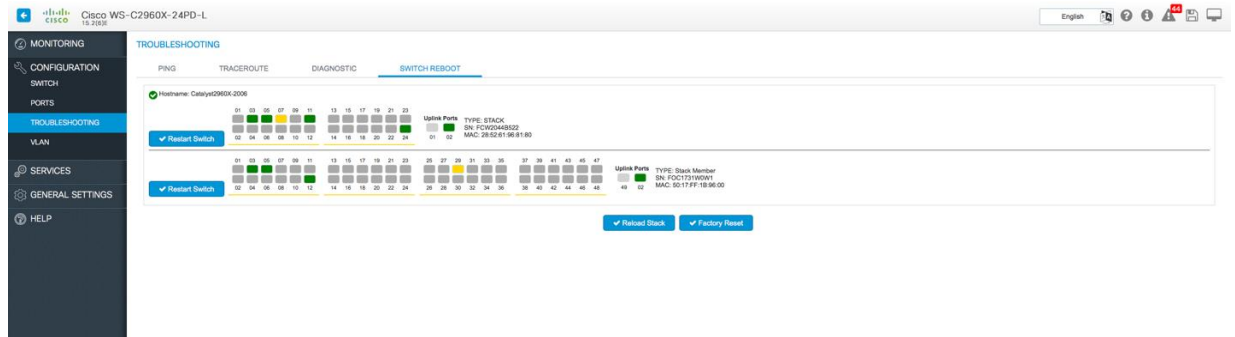
12.5.2 Replace the configuration on the new switch

Cisco Configuration Professional can be used to load a configuration onto the new switch with a single click under **General Settings > System > Config File**. The file can be located locally on the laptop or on a file server used for configuration backup.



12.6 Erase switch configuration

To remove all existing configurations on a switch before it is shipped to a different location or sent back to Cisco as a faulty switch, you can erase its configuration. This can be easily done from Cisco Configuration Professional by clicking the factory reset button under **Configuration > Troubleshooting > Switch Reboot**.

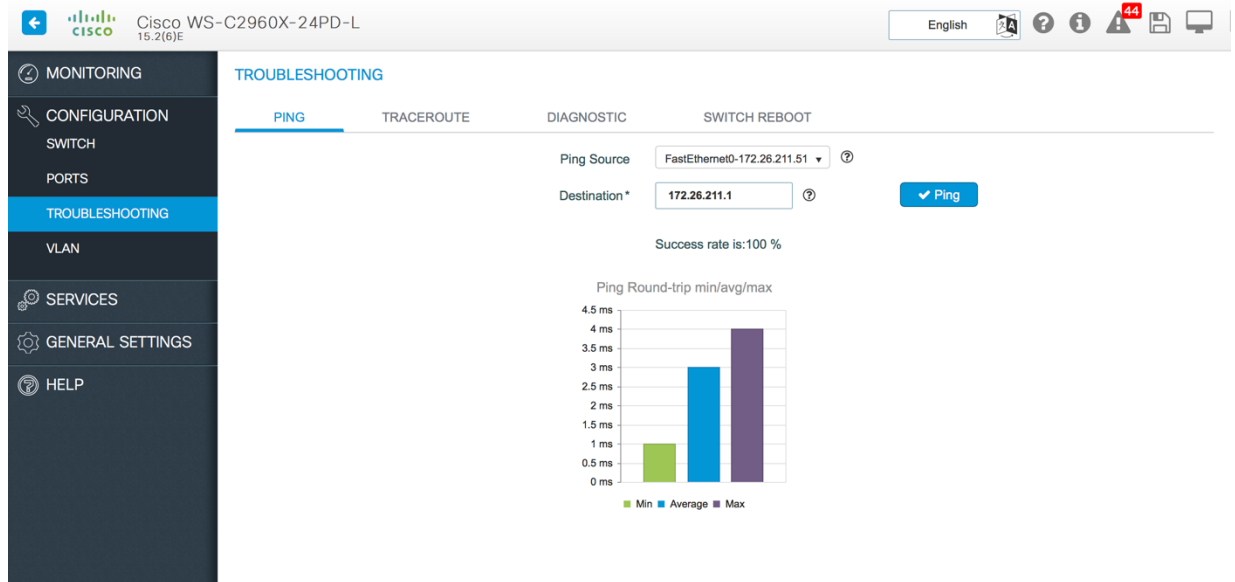


13. Tools

Cisco Configuration Professional for Catalyst provides many tools that an administrator would require on a regular basis to manage and troubleshoot various issues related to reliability of the switch and the reachability of the network under **Configuration > Troubleshooting**.

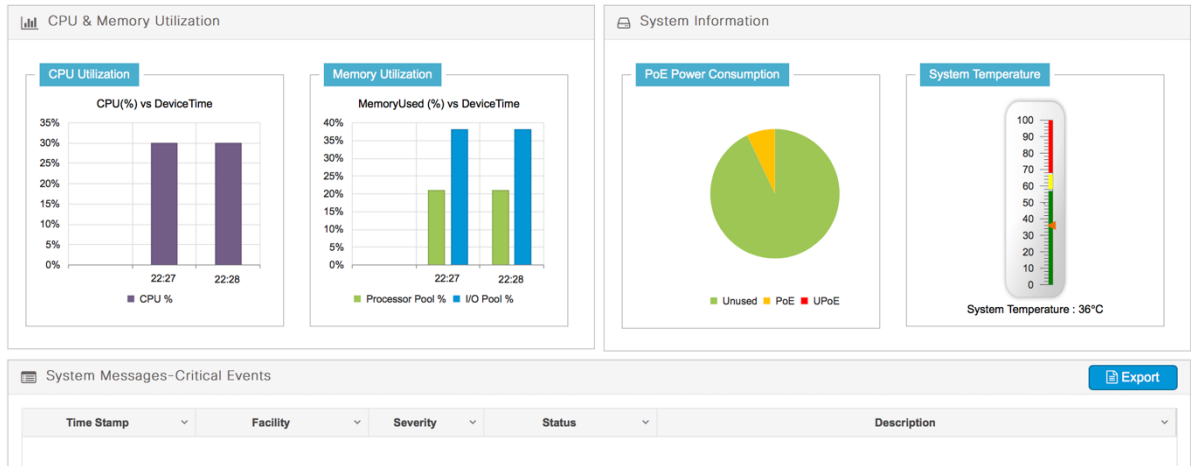
13.1 Validate reachability within the network

A user can easily validate reachability, along with the hops traversed to reach that particular destination, under Troubleshooting simply by adding the destination address and selecting a source address from all available options.



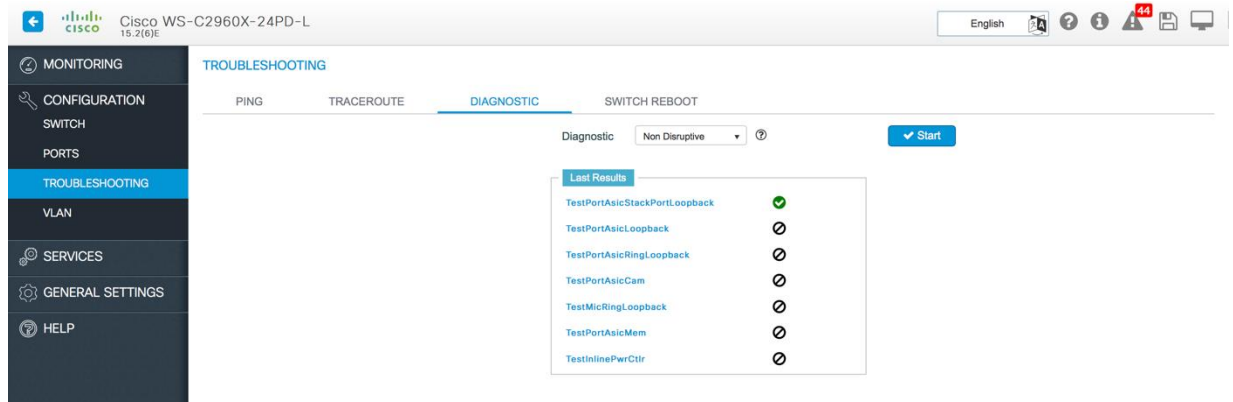
13.2 Know your switch health

The Monitoring dashboard on the switch gives a quick view of the health of the switch. The **CPU, memory, system temperature, and critical logs** of the switch are displayed on a single dashboard. The logs can be exported to attach to TAC cases or for documentation.



Diagnostics tests can be run from Cisco Configuration Professional, with options for both disruptive and nondisruptive tests, in order to gain insights into the reliability of the switch.

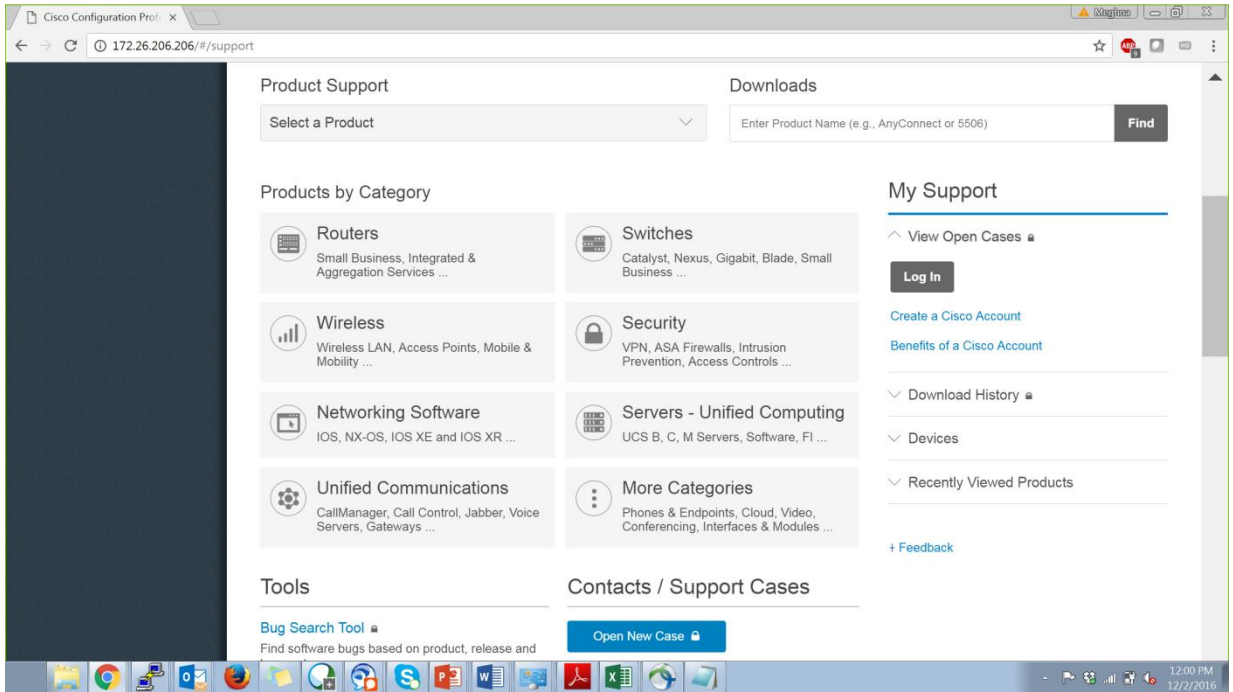
Note: Some of the diagnostic are intrusive; that is, the switch will be rebooted to run them. These tests will display a warning before running.



13.3 Getting technical support

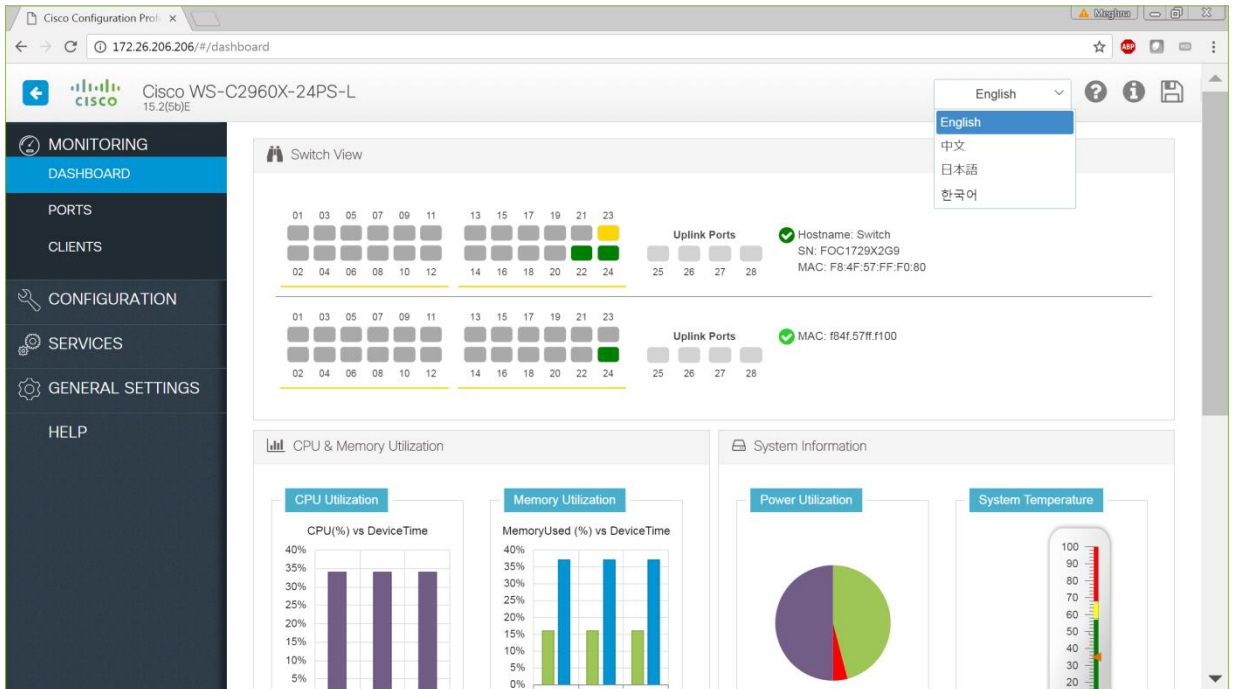
Cisco Configuration Professional gives easy access to support through quick links to the configuration guide and technical support. A user can access the guide to various features available through this software from any window simply by clicking the “?” icon in the top right corner of the window.

Also easily accessible is the complete configuration guide available at Cisco.com that details the exhaustive list of features available for the particular Cisco IOS version. This guide is available under **Help > Documentation**.



13.4 Choose your language settings

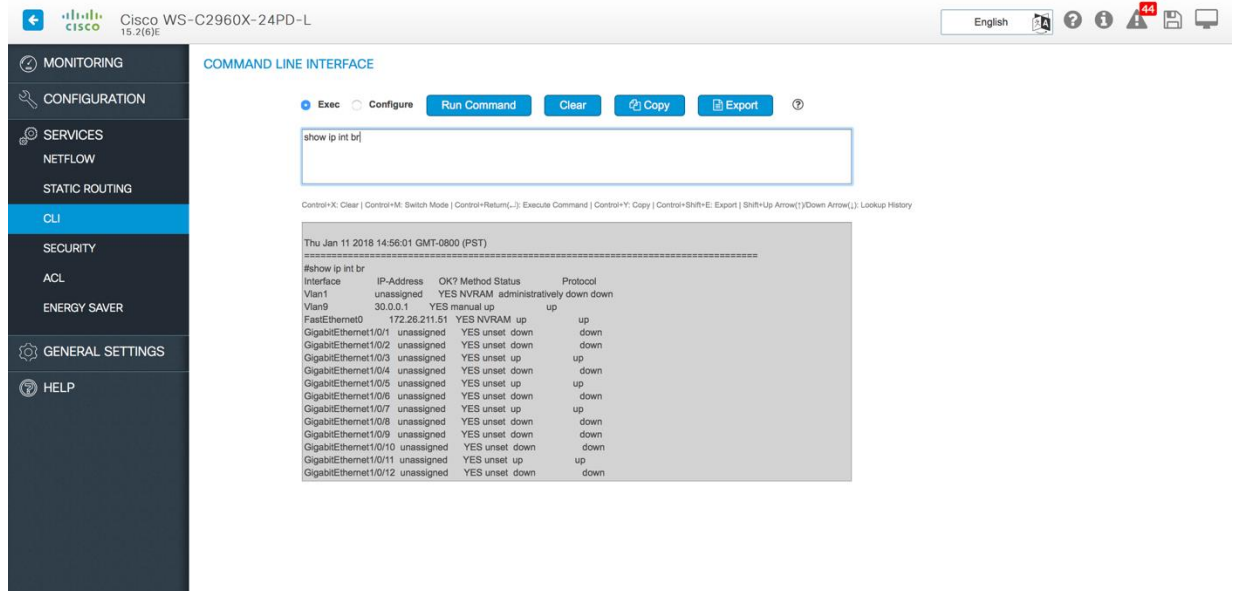
Cisco Configuration Professional supports multiple languages: English, Korean, Mandarin, and Japanese. The language can be easily changed from any window of the tool by selecting the desired language from the top right corner.



13.5 Using the CLI

The switch CLI can easily be launched from Cisco Configuration Professional instead of having to use Telnet/SSH or a console into the switch to run commands.

It can be done either by clicking the monitor icon in the top right corner of the screen from any window or under **Services > CLI**, wherein the user can easily copy or export the output of the command that is run.



The screenshot displays the Cisco Configuration Professional interface for a Cisco WS-C2960X-24PD-L switch. The left sidebar contains navigation menus for Monitoring, Configuration, Services, CLI, Security, and General Settings. The main window is titled 'COMMAND LINE INTERFACE' and features a command prompt area with the command 'show ip int br' entered. Below the command prompt, the output of the command is displayed in a terminal window, showing the status of various interfaces including Vlan1, Vlan9, and several GigabitEthernet ports.

```
Thu Jan 11 2018 14:56:01 GMT-0800 (PST)
#show ip int br
Interface      IP-Address      OK? Method Status  Protocol
Vlan1          unassigned     YES NVRAM  administratively down down
Vlan9          30.0.0.1       YES manual up       up
FastEthernet0  172.28.211.51  YES NVRAM up       up
GigabitEthernet1/0/1  unassigned     YES unset down   down
GigabitEthernet1/0/2  unassigned     YES unset down   down
GigabitEthernet1/0/3  unassigned     YES unset up     up
GigabitEthernet1/0/4  unassigned     YES unset down   down
GigabitEthernet1/0/5  unassigned     YES unset up     up
GigabitEthernet1/0/6  unassigned     YES unset down   down
GigabitEthernet1/0/7  unassigned     YES unset up     up
GigabitEthernet1/0/8  unassigned     YES unset down   down
GigabitEthernet1/0/9  unassigned     YES unset down   down
GigabitEthernet1/0/10 unassigned     YES unset down   down
GigabitEthernet1/0/11 unassigned     YES unset up     up
GigabitEthernet1/0/12 unassigned     YES unset down   down
```




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)