Cisco 300 Series Switches

Small Business Solution Demonstration

For Small Business

Table of Contents

Cisco 300 Series Solution Overview

When you need advanced features and network management, but value is still a top priority, look to the Cisco 300 Series switches.

The Cisco 300 Series, part of the Cisco Small Business line of network solutions, is a portfolio of affordable managed switches that provide a reliable foundation for a small business network. With 8 to 48 ports of Fast Ethernet (including 2 or 4 Gigabit Ethernet uplinks) or 10 to 52 ports of Gigabit Ethernet connectivity, plus Power over Ethernet (PoE) options, these switches offer a comprehensive range of choices. The Cisco 300 Series Managed Switches deliver the advanced security, quality of service (QoS), energy-saving technology, and network features needed to support business-class data, voice, security, and wireless solutions. They are easy to configure and manage, include a limited lifetime warranty with next business day advance replacement (where available) and one year of technical phone support. The Cisco 300 Series Managed Switches provide the ideal combination of ease-of-use, affordability, performance, and capabilities in a solution designed specifically for small businesses.

Cisco 300 Series Demo Guide

This Demonstration Script is centered on the newly-released 300 Series Managed Switches – its advanced feature set, QoS capabilities and ease-of-use. The 300 Series makes it easy for Small Businesses to manage their network, build a new network, or expand an existing one, with or without a dedicated IT staff.

This document gives you the means to become more comfortable with the SG300 switch, and to help you demo it in sales and training events.

This script is accompanied by matching Videos on Demand to help you prepare for your demos, which can be found on the Cisco Support Community, along with SmartTips, Smart Designs, and other valuable information on Cisco's 300 Series switches. Go to: https://supportforums.cisco.com/community/netpro/small-business/switches?view=documents

There are 2 types of demonstrations in this document – Basic and Advanced.
The Basic demo gives instructions on how to demonstrate the Management interface, while keying in on feature highlights. The Advanced demo gives instructions on how to demonstrate a working solution in real time.

All through the demonstration, we focus on the following items:

- Intuitive Graphical User Interface (GUI)
- Ease of Configuration
- Cost savings for the Small Business:

    - Future proofing with IPv6
    - Power Optimizations (also known as Green Ethernet)
- Advanced Feature set compared to similar products (shown in Advanced Demo)

Demonstration Script Key

This demo provides a step-by-step guide to configuring various items in the switch.

STEP 1. Numbered instructions must be carried out in the order shown.

- Bulleted features in each script can be selected individually for alternate views or testing.

✎ Note Instructions worth noting!

Preparing for the Demo

Bill of Materials

The **Basic** demo requires the following devices:

- Cisco 300 Series Switch – SG300-10P or SG300-28MP
- Power Cord
- Ethernet Cable that is less than 50 meters (164 ft.) long
- 1 PC with the following software installed:
    - Latest version of Internet Explorer or Firefox
    - FindIT Small Business Toolbar – available at http://www.cisco.com/go/findit

The **Advanced** demo is more complex and gives a more realistic snapshot of a live network, with multiple devices communicating and packets going through the switch. This set of demonstrations would require additional equipment, as follows:

- Cisco 300 Series Switch – SG300-10P or SG300-28MP
- Power Cord
- Ethernet Cable
- Serial Cable
- 2 PCs:
    - Management PC with the following software installed:
        - Latest version of internet Explorer or Firefox
        - VLC Video Media Player version 0.8.6h (go to www.videolan.org/vlc/)
        - FindIT Small Business toolbar – available at http://www.cisco.com/go/findit
    - 1 other PC with VLC Video Media Player version 0.8.6h installed (included in package, or go to www.videolan.org/vlc/. Used for Multicast Demo
- A DVD of your favorite movie – used for Multicast Demo

✎ Note You can show the Advanced demos within the Basic form, by simply explaining the solution you are configuring and walking through the configuration process

Getting Ready: The Night Before your Demonstration

1. Make sure you are equipped with all the necessary items on the Bill of Materials, per the scenario you will demonstrate.
2. Ensure that the latest version of Internet Explorer is installed on your PC.
   - It is recommended to use Internet Explorer version 6.0 or later, and Firefox version 2.0 or later.
3. Familiarize yourself with how to change the IP address on your PC, so that it can communicate with the Switch. For more information and instructions on how to perform these functions on MACs and PCs, please refer to the accompanying Videos on Demand. or refer to your OS Help.
   - The switch is preconfigured to 192.168.1.254, so you would need to ensure that your PC's IP address is in the 192.168.1.0 subnet (for example: 192.168.1.25)
4. Reset the switch to its Factory Defaults, to show a clean, out-of-the-box configuration scenario.
   - To do this, insert a paper clip into the reset Button on the Front Panel of the Switch, and hold it for 10 seconds. Or, enter the switch management page, and navigate to **Administration > Reboot** and click on **Reboot to Factory Defaults**
5. Practice the demonstration scenarios a few times, so you get fluent with the demonstration actions and be comfortable with talking to the many benefits of the 300 series to your audience.

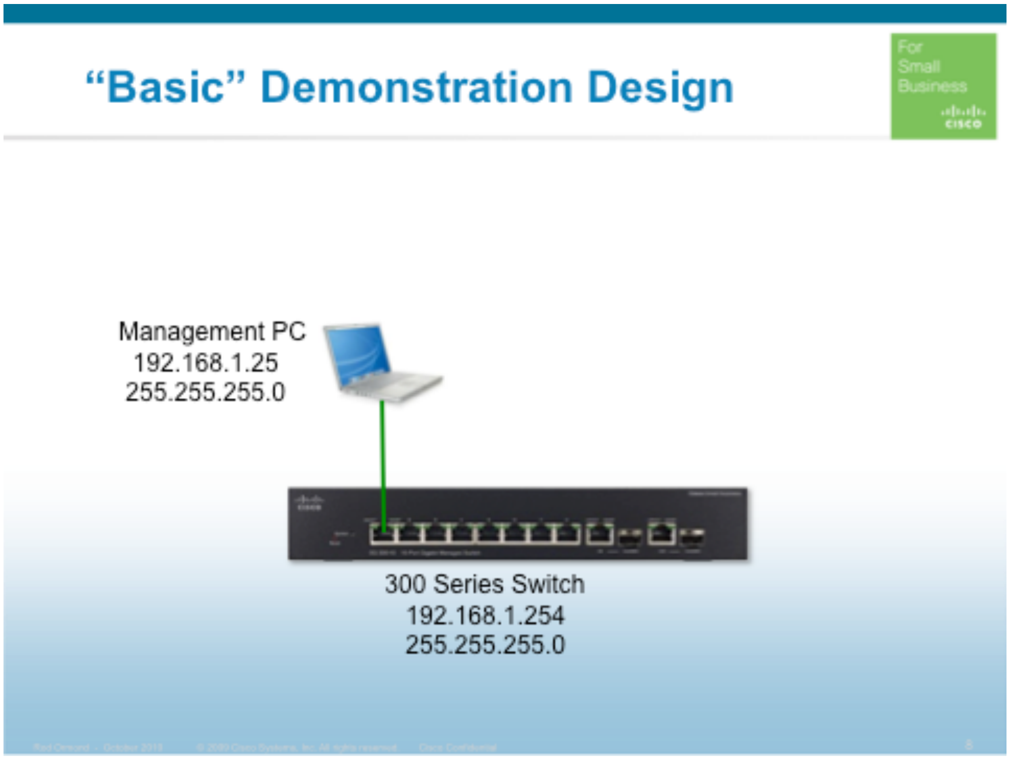
Device Setup

STEP 1. Plug the power cord to the Cisco 300 Series switch (power port is located at the back side of the switch).

STEP 2. Connect the Ethernet Cable from the Ethernet port of your management PC to Port 1 of the switch's Ethernet Port. The LEDs on the connected Port should become green to indicate that the Port is Operational.

- Port 1 is given as an example, but you can alternatively connect the cable to any other port on the switch.

Your network Topology should look something like this:



“Basic” Demonstration Design

Management PC
192.168.1.25
255.255.255.0

300 Series Switch
192.168.1.254
255.255.255.0

Basic Demo

This set of demonstrations is centered on the basic configuration of the 300 Series Switch. It is configured to out-of-the-box operation; however in many cases in real-world deployments, additional settings will be required.

It is important to highlight and showcase the intuitive management interface, its ease-of-use and aesthetics through your demonstration. This interface is common through not only the 300 Series switches, but also across many other SBTG products.

This section will cover the following scenarios:

- Gaining Access to the Switch
- Viewing System Information
- Defining an Identity
- Configuring the Management Interface, IPv4 and IPv6
- Configuring additional User Accounts
- Saving and Viewing the Switch Configuration
- Viewing Cost savings due to Power Optimizations
- Using the Robust and Efficient Help Options

Initial Setup: Gaining Access to the Switch

The Cisco 300 Series switch is accessible via the following options:

- Web-based configuration GUI
- FindIT – The Small Business Toolbar
- Menu based Console
- Remote Management using SNMP

Here we will demonstrate the first two options, as these are the easiest and most accessible.

Scenario 1: Web-based Configuration GUI

STEP 1. The switch is preconfigured for IP address 192.168.1.254. Ensure that your PC's IP address is in the 192.168.1.0 subnet (for example: 192.168.1.25).

STEP 2. Start a Web Browser.

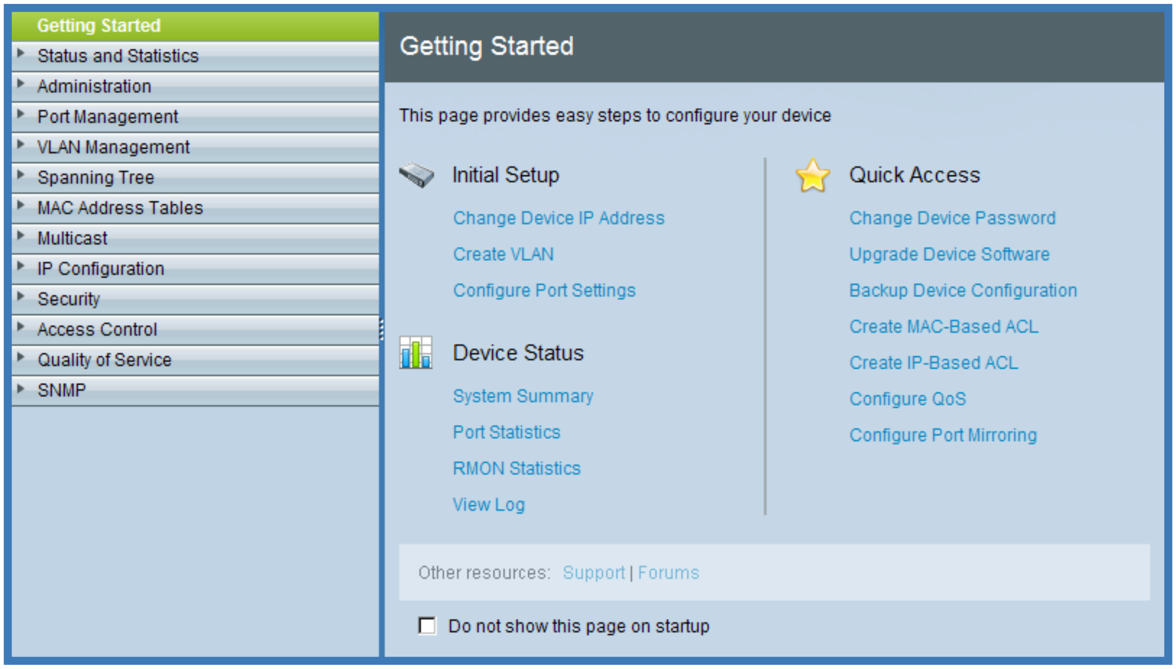
STEP 3. Enter the IP address of the switch (http://192.168.1.254) in the address bar.

STEP 4. When the login page appears, enter the user name and password; then click Login.
The default user name is **cisco**. The default password is **cisco**. Passwords are case sensitive.

Note For security reasons you will be prompted to change your password. This will be demonstrated in Scenario 1 of this document

STEP 5. Proceed to other Demo scenarios or utilize the Getting Started page to complete the Initial Setup. This page offers links to common tasks to get the switch configured and operational quickly.

STEP 6. You can also utilize the handy menu bar on the left hand side of the management web page to access various configuration options. This menu bar will appear on every screen for easy and quick navigation. We will access it throughout the Demo, so you become familiar with its possibilities.

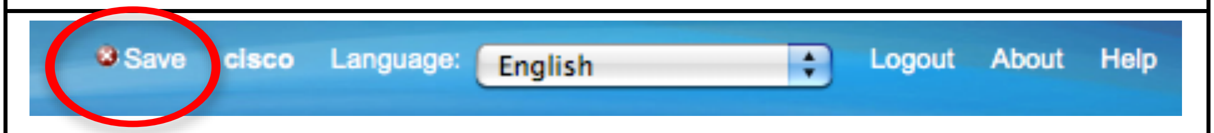


This page provides easy steps to configure your device

Note

During the device settings process, it's advisable to often Save your configuration, to protect your settings in case of a sudden shutdown due to power failure. You can do this on the upper right side of the screen as shown below.

The system will indicate that changes were made and that saving your configuration is required, by a red X sign next to the Save link.



Scenario 2: FindIT – The Small Business Toolbar

Cisco FindIT is a tool that allows you a safe and care-free management of your network.

It is free for download, and once installed on your PC, will automatically discover all supported Cisco Small Business devices in your network, list them in the Device Discovery sidebar and provide quick access to them. This tool saves you the time in organizing the Devices are organized by device type (router, switch, and so on).

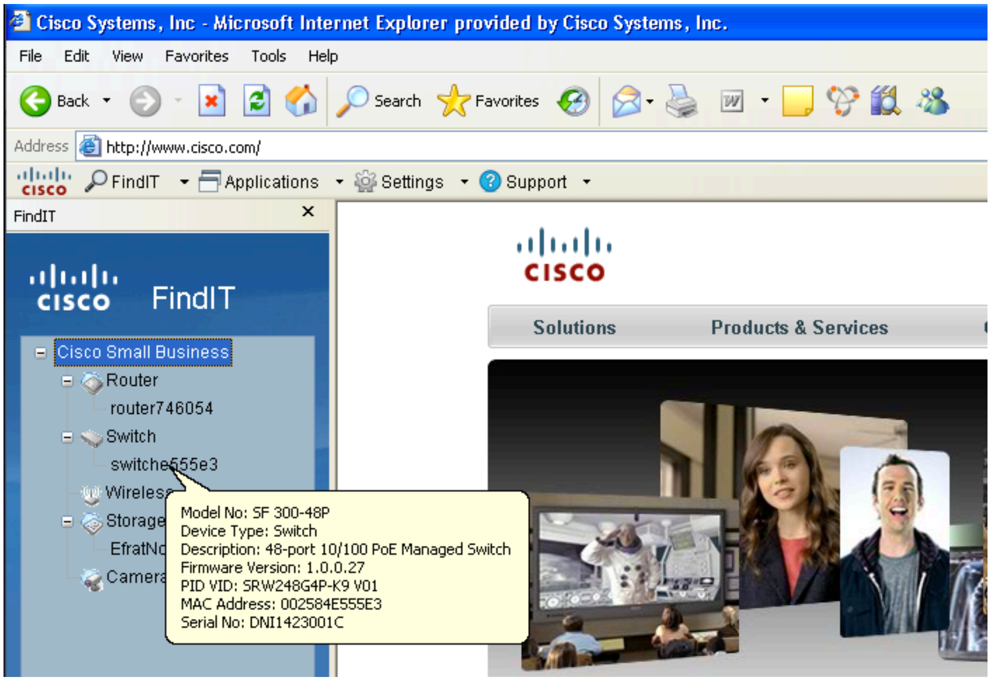
- To view device information, position your mouse over the device name.
- To launch a device manager, double-click the device name.

Note If you are running Internet Explorer on Windows Vista or Windows 7, you may have difficulties using programs like Cisco FindIT that use pop-up windows. Cisco FindIT uses a pop-up window to display its Help system. In addition, many of the Cisco device managers use pop-up windows for configuration settings.

You can install, find documentation, and obtain support for the Cisco FindIT Small Business Toolbar at the following location:

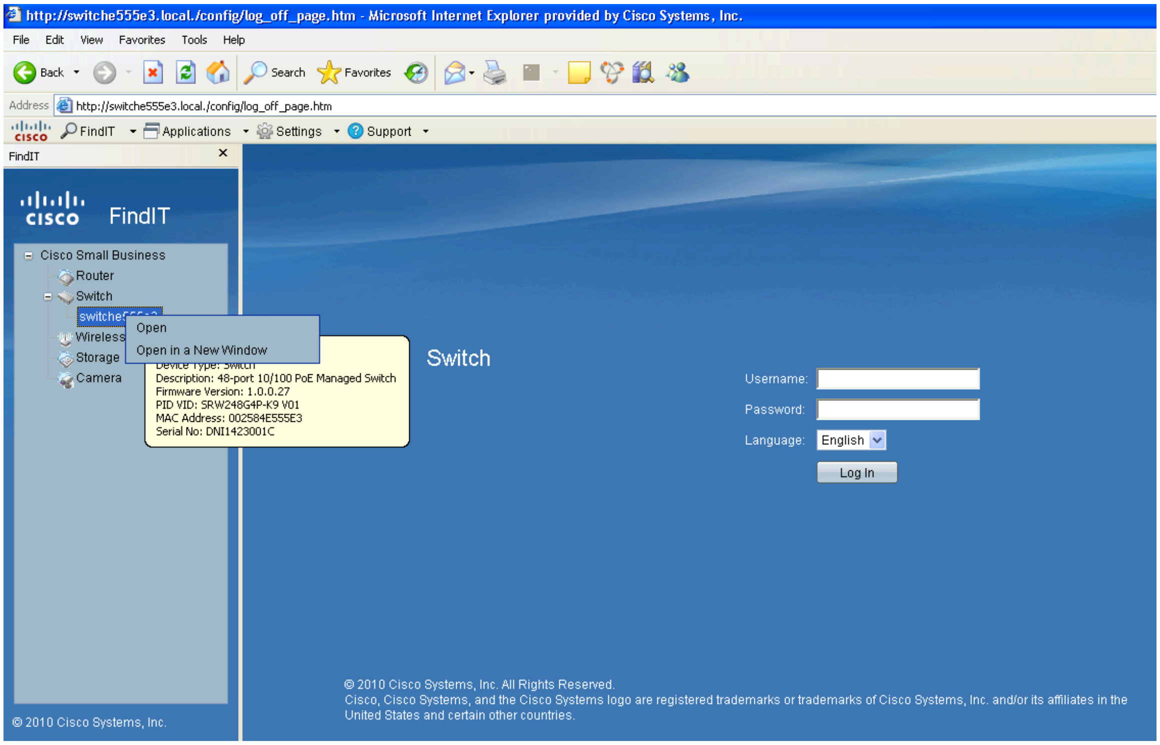
http://www.cisco.com/go/findit

STEP 1. From the FindIT Toolbar on the Internet Explorer window, the devices on your network will appear on the left-hand side of the window.
Hovering over the switch icon will provide a quick description to its configuration.



Model No: SF 300-48P
Device Type: Switch
Description: 48-port 10/100 PoE Managed Switch
Firmware Version: 1.0.0.27
PID VID: SRW248G4P-K9 V01
MAC Address: 002584E555E3
Serial No: DNI1423001C

Double click the link to the switch and the management Web GUI will appear. Proceed to configure it just as in the previous section



Device Type: Switch
Description: 48-port 10/100 PoE Managed Switch
Firmware Version: 1.0.0.27
PID VID: SRW248G4P-K9 V01
MAC Address: 002584E555E3
Serial No: DNI1423001C

Username:

Password:

Language: English

© 2010 Cisco Systems, Inc.

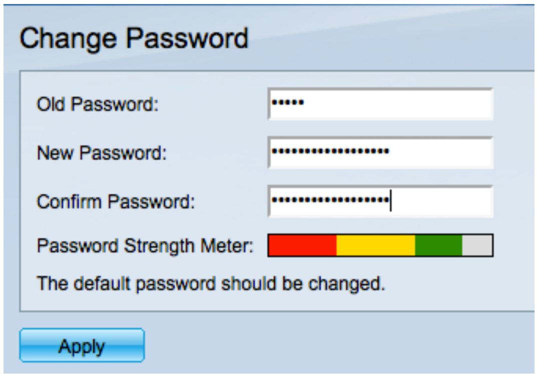
© 2010 Cisco Systems, Inc. All Rights Reserved.
Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Scenario 3: Changing the Default Password

Once you are logged into the system, it is advisable to change the default password to protect its access.

STEP 1. If this is your first time to log on, you will be prompted to change the default password. Alternatively, you can reach this tool from the **Getting Started** page, by clicking **Change Device Password.**

STEP 2. Apply your new password into the assigned spaces and save it for your records. Click **Apply** to save your settings.



Change Password

Old Password: •••••

New Password: ••••••••••••••••••

Confirm Password: ••••••••••••••••••

Password Strength Meter: 🟥🟨🟩

The default password should be changed.

Note The Password Strength Meter will measure the password strength, that is, how easy it is to hack it.
It is advised to enter a password that is not easy to hack, and contains many different characters, such as uppercase and lowercase letters, numbers and special characters.

Scenario 4: Viewing System Information

You can easily understand the state of the 300 Series switch, its key features, and view logs for troubleshooting purposes.

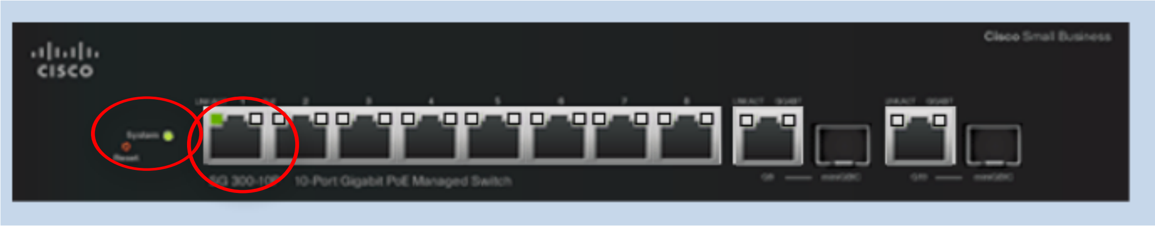
Viewing the Status of the Switch

STEP 1. On the menu bar, choose the **Status and Statistics** tab and select **System Summary**. This page shows key information about the switch and its ports.

STEP 2. Observe the picture of the switch, where you will see real-time status indication.

STEP 3. Notice the System LED on the left hand side of the picture. A green LED indicates that the system is operational and up and running

STEP 4. Observe Port 1 (where your PC is connected). Notice that there are 2 figures for LEDs on each port, just like on the switch itself.
The left LED indicates activity, and the right LED indicates PoE status
Notice that the left LED on that port is green, meaning that port is operational



Accessing Port Status

Viewing information about a specific port is very intuitive from the **Status and Statistics** page that you are already on.

STEP 1. In the **Status and Statistics** page, on the picture of the switch, double-click on the area of Port 1. This will automatically open up the status and configuration page for this port, where you can see connectivity status and edit various attributes of that port (such as Auto negotiation, flow control, MDI/MDIX).

STEP 2. Alternatively, you can reach this page from the **Port Management** menu, in the **Port Settings** page. Click on Port 1 radio button and click **Edit.**

Note The 300 Series GUI is intuitively designed to link between pages that are logically connected, and this is a common theme along the demonstration. In the example here, you can reach the port status page via different alternatives. However, you will find more examples as you run through the demonstration.

General Switch Information

General switch information is available on the **Status and Statistics** page.
Physical information can be viewed, as well as MAC address, Serial number, and also Firmware Version. This information is useful for maintenance purposes, For example, to assess whether an upgrade is on order.

Scenario 5: Defining an Identity

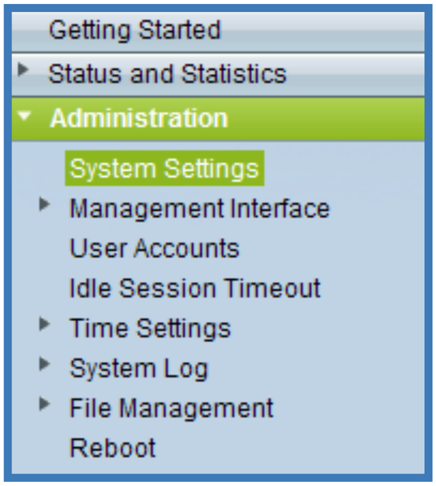
In order for your switch to be easily managed and discovered, you can give the switch an identity providing a location, contact, and name.

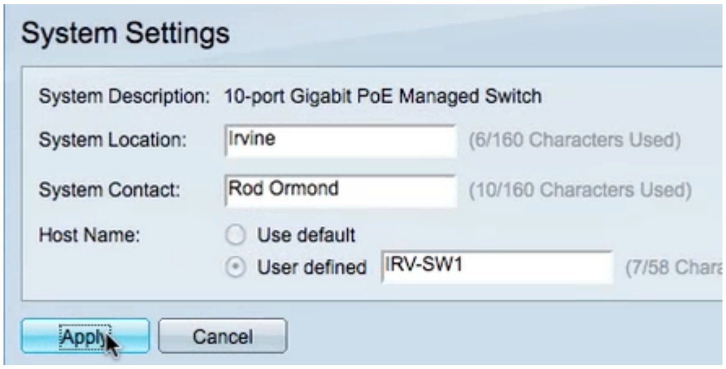
STEP 1. On the menu bar, choose the **Administration** tab and select **System Settings.**

STEP 2. Apply a **location** (for example: Irvine, CA) and **contact person** (for example: your name) for the switch. You can also change the **host name** to something that makes more sense to the network (for example: IRV-SW1, indicating 1st switch in Irvine).

STEP 3. Click **Apply** to save your changes.

STEP 4. You will be prompted with a Success notification at the top of the screen, once this action has taken effect.




System Settings

System Description: 10-port Gigabit PoE Managed Switch

System Location: Irvine (6/160 Characters Used)

System Contact: Rod Ormond (10/160 Characters Used)

Host Name: ○ Use default ● User defined IRV-SW1 (7/58 Chara

Scenario 6: Configuring IPv4 Settings

In order to easily manage the switch, it is important to configure its address such that it complies with the network. The switch can get a dynamic IP address from a DHCP server on the network, or be assigned a static IP address.

> Note The switch will default to get a dynamic IP address, however changing it to a static IP address will give the network administrator more manageability

Here we will show how to apply a static IP address to the switch

STEP 1. On the menu bar, from the **Administration** tab, choose the **Management Interface** tab and select **IPv4 Interface.**

STEP 2. Change the **IP Address Type** to **Static** by clicking on the Static radio button.

STEP 3. Apply an **IP address** and appropriate **network mask.**
In this demonstration we will remain with the default IP address 192.168.1.254, with a 24-bit subnet mask of 255.255.255.0.
No default gateway is required for this demo, so **Default Gateway** is **None.**

STEP 4. For demo purposes, we want to ensure connectivity between the switch and your PC, so do not apply these changes:
Click **Cancel** twice to disregard this configuration.
Or set the IP address to the default values as in Step 3 and Save.

Scenario 7: Configuring IPv6 Settings

IPv6 is the next generation Internet networking protocol and is intended to supersede the currently-used IPv4 protocol, which is limited in address space and flexibility it provides.

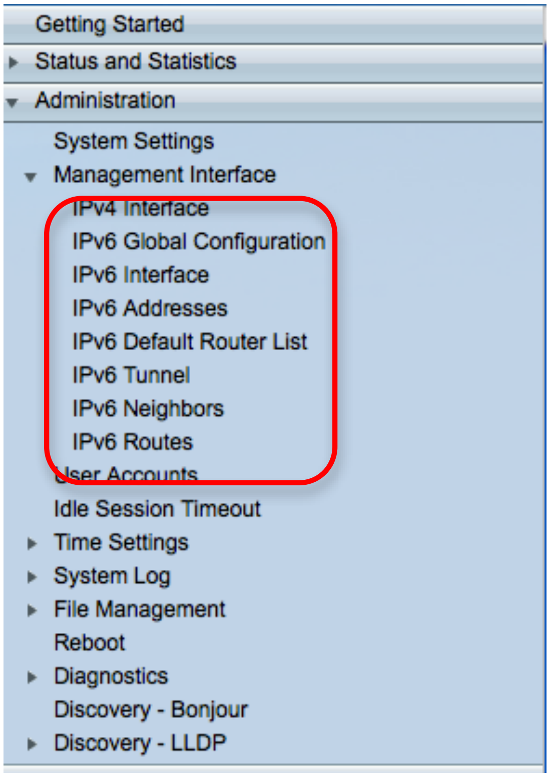
Internet Service Providers, PC manufacturers, and government agencies worldwide are adopting IPv6 so this standard will be the de-facto standard in the upcoming years.

The Cisco 300 Series switches already provide IPv6 capabilities, to provide scalability into future network configurations, therefore providing future protection, and decreases cost of ownership.

Note The 300 Series provides a Dual-stack mechanism, meaning it can translate between IPv4 and IPv6, depending on the network, and thereby allowing a healthy migration between the 2 standards.

The menu to configure IPv6 settings is available on the **Administration** tab, under **Management Interface**, in multiple IPv6 configuration setting menus, as seen here.

More information can be found on IPv6 configuration in the Cisco 300 Series datasheet.



Scenario 8: Configuring Additional User Accounts

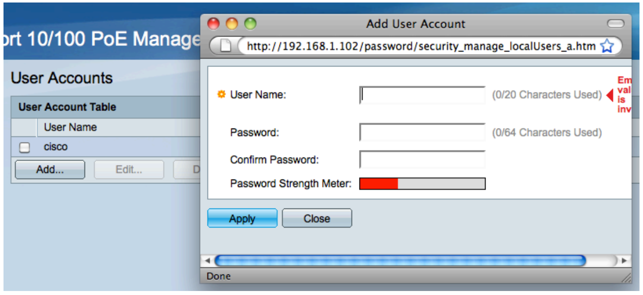
Adding new users to manage your system is valuable to offload IT personnel, and to enable other users to administrate the system, other than the default user. To do this, follow these steps:

STEP 1. From the **Getting Started** page, click the **Change Device Password.**
Alternatively, you can access the same page through the **Administration** tab, on the **User Accounts** link.

STEP 2. You will see the default username, which is **cisco**. Checking that username, and clicking **Edit** will enable you to modify the details of the default login. However it is not advisable to do so, in order to maintain a known default username and login.

STEP 3. Click on the **Add** button. This will open up another window in which you will be prompted to list the new user's details.

STEP 4. Enter a new username and a password which you will remember, and click **Apply.**



rt 10/100 PoE Manage

User Accounts

User Account Table

	User Name
□	cisco

Add User Account

http://192.168.1.102/password/security_manage_localUsers_a.htm

User Name: (0/20 Characters Used)

Password: (0/64 Characters Used)

Confirm Password:

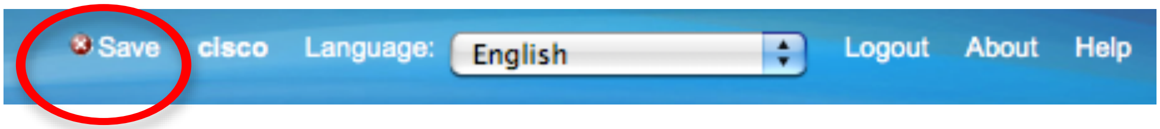
Password Strength Meter:

Scenario 9: Saving and Viewing your Configuration

During the device settings process, it's advisable to often save your configuration, to protect your settings in case of a power failure. Once you've applied changes to the switch, the system will indicate that changes were made, and that saving your configuration is required, by a red X sign next to the Save link.

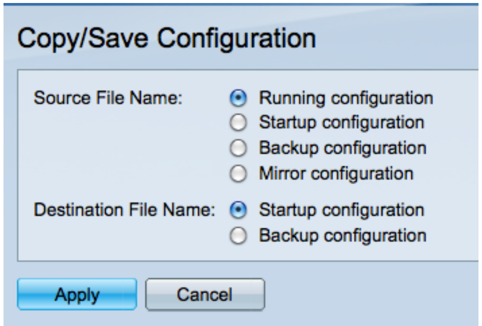
Saving your Settings to Internal Memory

You can save your work, by clicking on the easy **Save** link on the upper right side of the screen as shown below. This will direct you to the Copy/Save Configuration page, which you will utilize below in the demonstration.



STEP 1. On the menu bar, from the **File Management** tab, go into the **Copy/Save configuration.** This will show you different options for saving your configurations.

STEP 2. We would like to save the **Running configuration** into the **Startup configuration** so the switch would always start up with the changes we made.
Select **Running Configuration** from the Source File Name and **Startup configuration** from the Destination File Name and click **Apply**.
This will save your changes to the internal memory of the switch.



Copy/Save Configuration

Source File Name:
● Running configuration
○ Startup configuration
○ Backup configuration
○ Mirror configuration

Destination File Name:
● Startup configuration
○ Backup configuration

Saving your Settings to a Text Editable File

Additionally, you may save your configuration into an editable text file, on your PC.
This especially comes in handy when you need to apply common tasks to many switches on your network.

STEP 1. On the menu bar, from the **File Management** tab, go into the **Download/Backup Configuration/Log** page.

STEP 2. Select **HTTP** as Transfer method, Save Action as **Backup** and **Startup Configuration** as Source File Type.

STEP 3. Click **Apply.** This will trigger a popup to save the file to our PC's hard drive.

STEP 4. You can open the file you just saved from a simple text editor to see the changes that you made.

Green Ethernet

The Cisco 300 Series switches come with advanced capabilities to conserve energy. This is becoming more important as prices of energy rise, and electricity bills soar.

The 300 Series switches all have new advanced silicon, power supplies and fans that provide significant power and energy savings. In addition, the switch provides 2 more capabilities of further reducing power usage – powering down inactive ports, and adjusting the power usage based on the cable length (available only on Gigabit models).

Scenario 1: Energy Detect Mode

STEP 1. On the menu bar, from the **Port Management** tab, drop down the **Green Ethernet** tab and go to **Properties**.

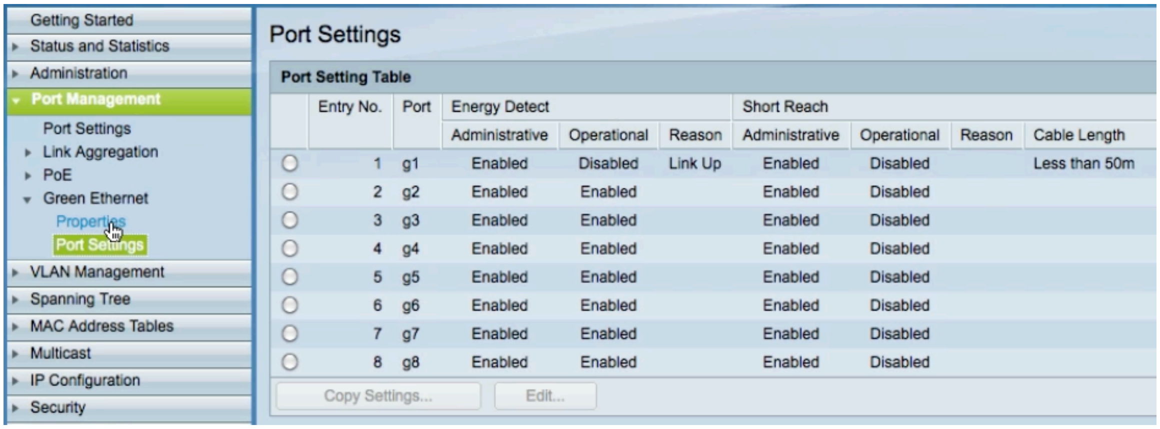
STEP 2. The switch defaults to reserving power, however you can disable it through the checkboxes in this menu.
Energy Detect Mode instructs the switch to significantly lower the power usage based on the energy detected on the ports. If a port is not connected, or the PC connected to it is shut down, that port will go into "sleep" mode and will wake up when it connected back again.
Energy Detect Mode is available both on Fast Ethernet and Gigabit models.
Short Reach instructs the switch to adjust the power usage based on the cable length that is used. Specifically, it will lower the power usage on connections that are using an Ethernet cable that is 50 meters (164 ft.) or less.
Short Reach mode is available only in Gigabit versions of the switch.

Note For this demo, notice that the Short Reach option is disabled at first. We will demo it in the next scenario, where we will enable this option, and will showcase the immediate savings this feature provides.

STEP 3. Here you can see the Power Savings of the Switch, in milliwatts, since its last boot time and the cumulative Energy saved in Watts/Hour.
Show that the switch has already saved 322 milliwatts, from the start.

STEP 4. In the **Port Settings** menu under **Port Management**, a list of the available ports will appear with its energy saving attributes. Here you can see where the power savings are coming from, and enable or disable the Energy Saving capabilities per port.

STEP 5. Notice that on port 1 (the port that your PC is connected to), the **Energy Detect** option is **disabled**, as the switch is detecting energy on that port, so it cannot shut it down.
The **Short Reach** option indicates that the cable connected to port 1 is less than 50m, but this option is disabled.



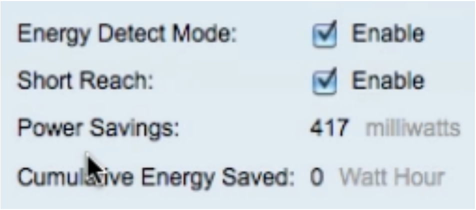
Port Settings

Port Setting Table

	Entry No.	Port	Energy Detect			Short Reach			
			Administrative	Operational	Reason	Administrative	Operational	Reason	Cable Length
○	1	g1	Enabled	Disabled	Link Up	Enabled	Disabled		Less than 50m
○	2	g2	Enabled	Enabled		Enabled	Disabled		
○	3	g3	Enabled	Enabled		Enabled	Disabled		
○	4	g4	Enabled	Enabled		Enabled	Disabled		
○	5	g5	Enabled	Enabled		Enabled	Disabled		
○	6	g6	Enabled	Enabled		Enabled	Disabled		
○	7	g7	Enabled	Enabled		Enabled	Disabled		
○	8	g8	Enabled	Enabled		Enabled	Disabled		

Scenario 2: Short Reach Mode

STEP 6. Go back to the Properties page to **Enable** the **Short Reach** option and click **Apply.** Notice that this automatically increases the power savings to **417 milliwatts** – a 95 milliwatt increase in savings, due to the short cable being used.



Energy Detect Mode: ☑ Enable

Short Reach: ☑ Enable

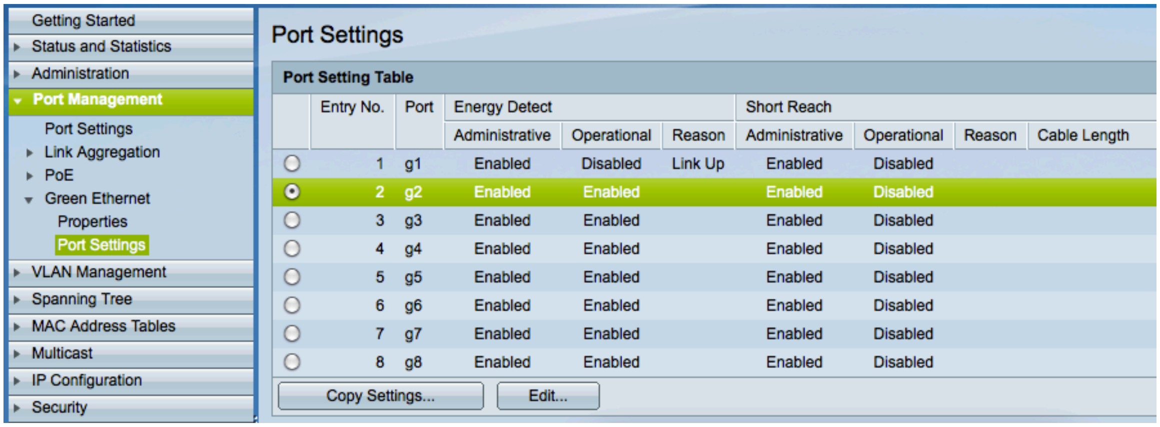
Power Savings: 417 milliwatts

Cumulative Energy Saved: 0 Watt Hour

STEP 7. Navigating back to the Port Settings page, you can see that the Short Reach option is enabled because the switch has detected a connection that is less than 50m long.

Scenario 3: Power Savings Configurations per Port

STEP 8. You can apply Energy Saving abilities per port. In the **Port Settings** menu under **Port Management**, a list of the available ports will appear with its energy saving attributes

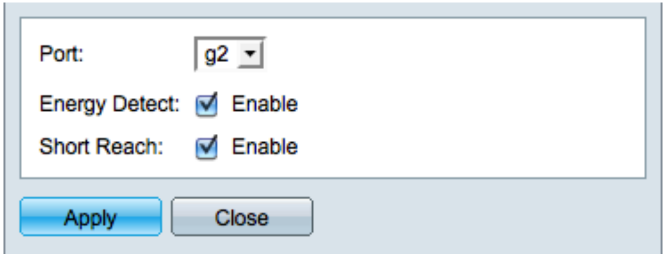


Port Settings

Port Setting Table

	Entry No.	Port	Energy Detect			Short Reach			
			Administrative	Operational	Reason	Administrative	Operational	Reason	Cable Length
○	1	g1	Enabled	Disabled	Link Up	Enabled	Disabled		
●	2	g2	Enabled	Enabled		Enabled	Disabled		
○	3	g3	Enabled	Enabled		Enabled	Disabled		
○	4	g4	Enabled	Enabled		Enabled	Disabled		
○	5	g5	Enabled	Enabled		Enabled	Disabled		
○	6	g6	Enabled	Enabled		Enabled	Disabled		
○	7	g7	Enabled	Enabled		Enabled	Disabled		
○	8	g8	Enabled	Enabled		Enabled	Disabled		

STEP 9. Check the desired port to configure, and click Edit at the bottom of the page. A pop-up block will appear where you will be able to set the Energy detection capabilities of that port



Port: g2

Energy Detect: ☑ Enable

Short Reach: ☑ Enable

Note When the Green Ethernet attributes of a port is changed, the link on that port will go down momentarily, until it initializes with the proper settings.

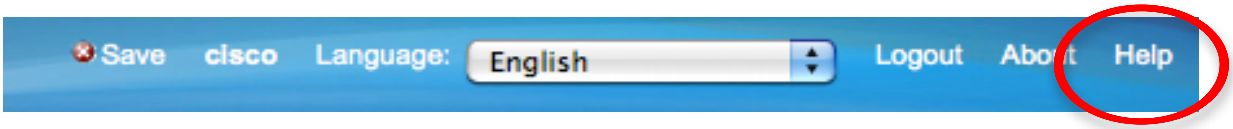
Using Help

A context-sensitive Help menu is available, to help network administrators with configuration information and general knowledge about the configuration options. This comes in handy when questions arise on on-site networking configuration options and possibilities.

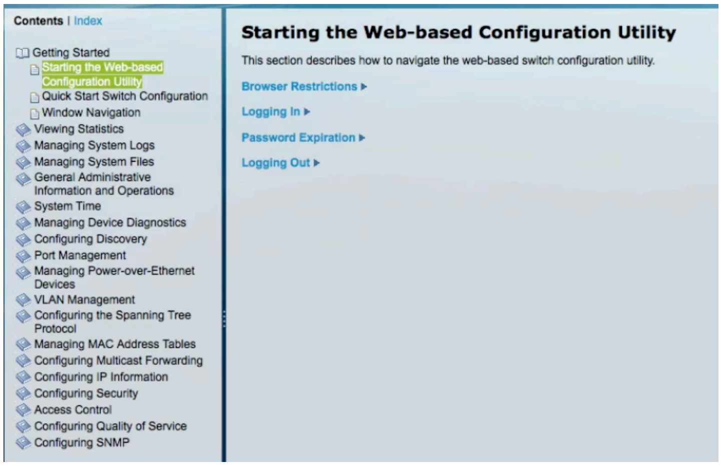
During this demonstration it is important to showcase and underscore the ease-of-use, intuitive and helpful management interface, and leadership compared to similar products.

Scenario 1: Accessing and Searching the Help pages

The Help Dictionary is accessible directly from the main configuration page and is always available, not dependant on the page you are navigating to.



Clicking on this link will open up the Help dictionary, presented as an on-line book. You can navigate through the chapters using the toolbar on the left hand side



Contents | Index

Getting Started
- Starting the Web-based Configuration Utility
- Quick Start Switch Configuration
- Window Navigation

Viewing Statistics
Managing System Logs
Managing System Files
General Administrative Information and Operations
System Time
Managing Device Diagnostics
Configuring Discovery
Port Management
Managing Power-over-Ethernet Devices
VLAN Management
Configuring the Spanning Tree Protocol
Managing MAC Address Tables
Configuring Multicast Forwarding
Configuring IP Information
Configuring Security
Access Control
Configuring Quality of Service
Configuring SNMP

Starting the Web-based Configuration Utility

This section describes how to navigate the web-based switch configuration utility.

Browser Restrictions ▸

Logging In ▸

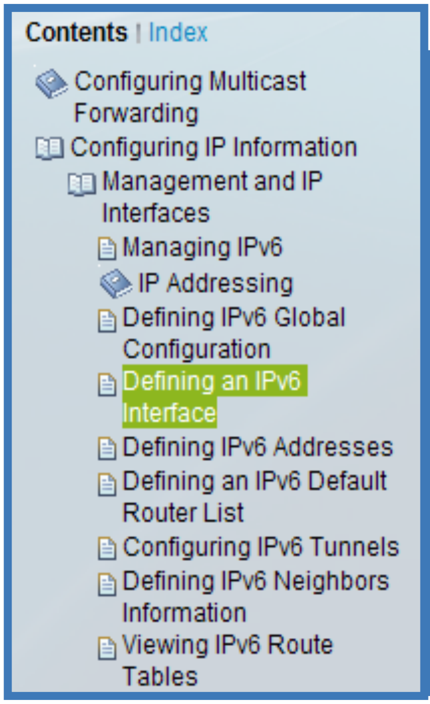
Password Expiration ▸

Logging Out ▸

You can also search through the dictionary from the search bar.

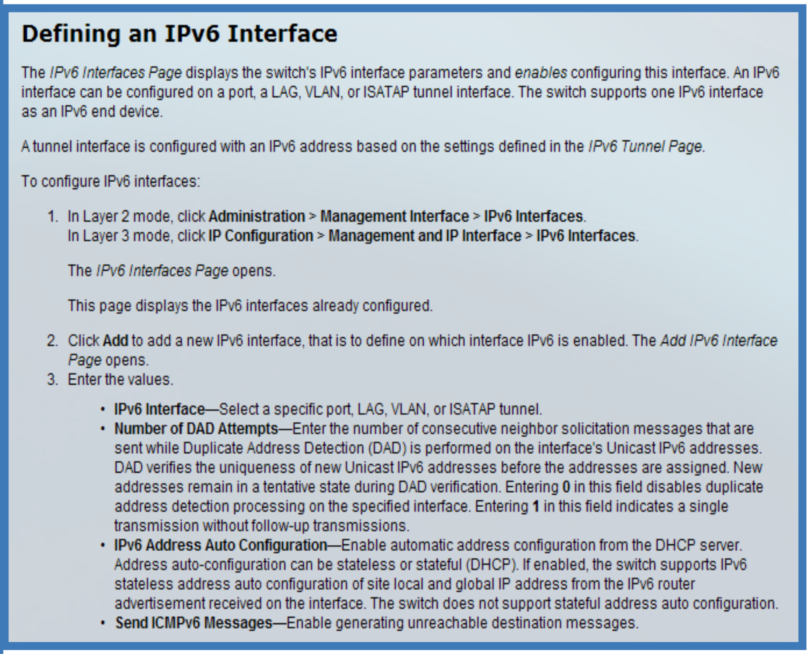
In this demonstration we will learn more about IPv6. You can access the relevant files in a couple of ways:

STEP 1. If you already know that this information is under the **Configuring IP Information** menu, in the **Management and IP Interfaces** page, we can simply go to that link and select one of the many pages available on this topic.



Contents | Index

- Configuring Multicast Forwarding
- Configuring IP Information
  - Management and IP Interfaces
    - Managing IPv6
    - IP Addressing
    - Defining IPv6 Global Configuration
    - Defining an IPv6 Interface
    - Defining IPv6 Addresses
    - Defining an IPv6 Default Router List
    - Configuring IPv6 Tunnels
    - Defining IPv6 Neighbors Information
    - Viewing IPv6 Route Tables



Defining an IPv6 Interface

The *IPv6 Interfaces Page* displays the switch's IPv6 interface parameters and *enables* configuring this interface. An IPv6 interface can be configured on a port, a LAG, VLAN, or ISATAP tunnel interface. The switch supports one IPv6 interface as an IPv6 end device.

A tunnel interface is configured with an IPv6 address based on the settings defined in the *IPv6 Tunnel Page*.

To configure IPv6 interfaces:

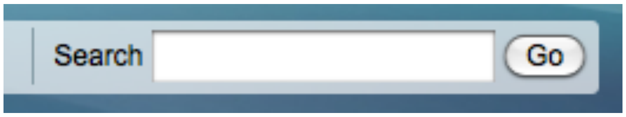
1. In Layer 2 mode, click **Administration** > **Management Interface** > **IPv6 Interfaces**.
   In Layer 3 mode, click **IP Configuration** > **Management and IP Interface** > **IPv6 Interfaces**.

   The *IPv6 Interfaces Page* opens.

   This page displays the IPv6 interfaces already configured.

2. Click **Add** to add a new IPv6 interface, that is to define on which interface IPv6 is enabled. The *Add IPv6 Interface Page* opens.
3. Enter the values.
   - **IPv6 Interface**—Select a specific port, LAG, VLAN, or ISATAP tunnel.
   - **Number of DAD Attempts**—Enter the number of consecutive neighbor solicitation messages that are sent while Duplicate Address Detection (DAD) is performed on the interface's Unicast IPv6 addresses. DAD verifies the uniqueness of new Unicast IPv6 addresses before the addresses are assigned. New addresses remain in a tentative state during DAD verification. Entering **0** in this field disables duplicate address detection processing on the specified interface. Entering **1** in this field indicates a single transmission without follow-up transmissions.
   - **IPv6 Address Auto Configuration**—Enable automatic address configuration from the DHCP server. Address auto-configuration can be stateless or stateful (DHCP). If enabled, the switch supports IPv6 stateless address auto configuration of site local and global IP address from the IPv6 router advertisement received on the interface. The switch does not support stateful address auto configuration.
   - **Send ICMPv6 Messages**—Enable generating unreachable destination messages.

STEP 2. If you are unsure of where this info is located, a Search tool is available on the Help page on its upper right hand side.



STEP 3. Typing in IPv6 will result in 36 different help topics, from which you can choose the most appropriate topic for your situation. Selecting **Defining an IP Interface** will lead us to the same exact page we navigated to manually, as in Step 1 of this demonstration.

Scenario 2: Context Sensitive Help – Accessing Help through Configuration

Another useful method of utilizing the Help menu is by accessing it during configurations. For example, if you are in the midst of configuring the IPv6 interface, and are in need of additional information on a line item or option, you can click the general Help link on the upper right hand side of the management page, and the relevant Help page will appear.

STEP 4. In the configuration bar on the left hand side go to the **Administration** menu, **Management Interface**, then go to **IPv6 Interface**.

STEP 5. Once you are in that page, click the Help link on the upper right hand side of the management page, and the relevant Help page will appear. This will be the same page that we navigated to manually on Step 1 of this demonstration.

Localization – Using different Languages to Manage the Switch

To ensure the globalization of the switch, the switch has been localized to 6 different languages. The management interface, on-box help, and product documentation come in English, French, German, Italian, Japanese and Spanish.
Any one of those languages can be downloaded to the switch, and will be available immediately for use on the management and configuration pages and on-box help.

The language dictionaries are available either on the product's CD or may be downloaded at www.cisco.com.

Note Make sure that you have already downloaded a language file onto your PC's hard drive, the night before your presentation.

To make this presentation even more successful, download 2 language dictionaries to your hard drive (for example: French and Italian), and show how you can easily alternate between the two.

Here we will showcase the downloading of a language dictionary, enabling it, and viewing the languages available on the switch.

During this demo, it is important to not only emphasize the ease of use and intuitive management interface, but also the Globalization, and the availability of language that, to some people, could be more intuitive.

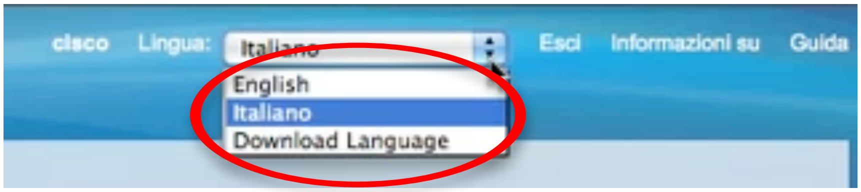
Scenario 1: Viewing the Languages that are locally available

STEP 1. Navigate to the **Status and Statistics menu**, then to the **System Summary** page.
Here you will see the languages that are currently available on the switch. Notice that the switch comes out-of-the-box with only English enabled.
Observe the languages listed under **Locale**, where you will see **en-US** (English).

STEP 2. If you have not already installed a second language, the second entry under **Locale** will not be populated.

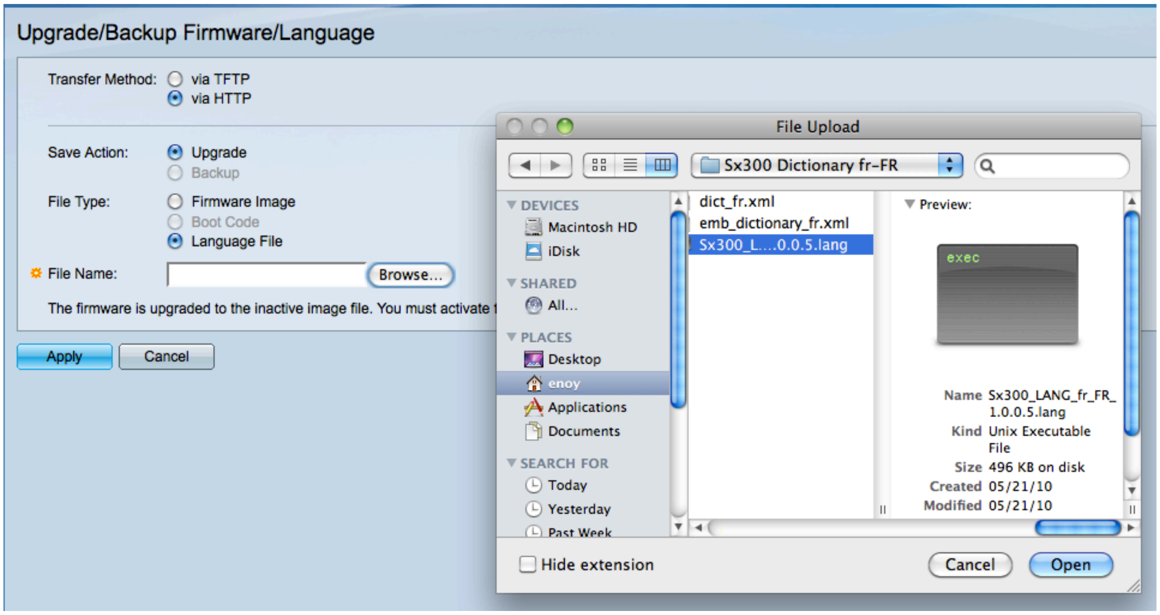
Scenario 2: Uploading a New Language onto the switch

STEP 1. The easiest method of downloading a new language is by utilizing the **Language** link at the top right hand side of the management page. If you drop down that menu, you will see the available languages already installed.
In this example, English is available as the default language and Italian as a second.



STEP 2. Select **Download Language** at the bottom of the menu. This will lead you to the **Upgrade/Backup Firmware/Language** page.
You can alternatively go into Navigate to **Administration** menu, then **File Management** page and select **Upgrade/Backup Firmware/Language.**

STEP 3. Select **via HTTP** as **Transfer Method**, and **Upgrade** as **Save Action**. Select **Language** as **File Type** as this is the file type you will be downloading. Click **Browse** to locate the Language file on your management PC's hard drive.
In this example, we will upgrade French as a second language.



Upgrade/Backup Firmware/Language

Transfer Method: ○ via TFTP ● via HTTP

Save Action: ● Upgrade ○ Backup

File Type: ○ Firmware Image ○ Boot Code ● Language File

File Name: Browse...

The firmware is upgraded to the inactive image file. You must activate t

Apply Cancel

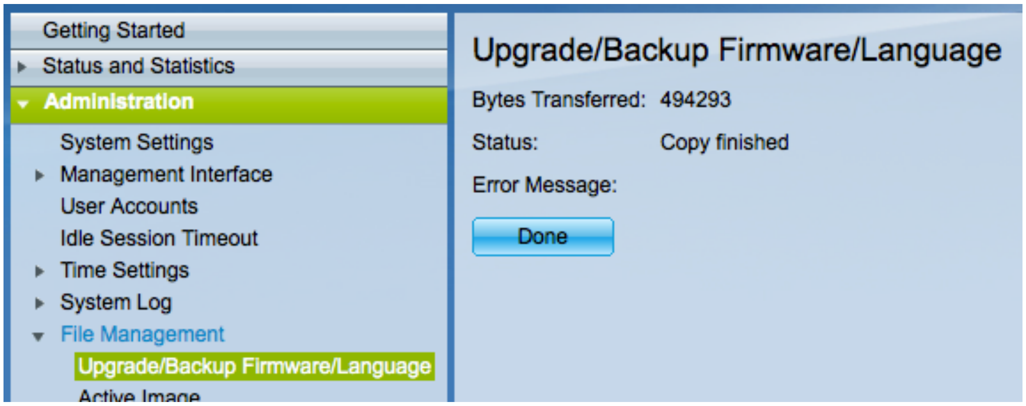
File Upload

Sx300 Dictionary fr-FR

dict_fr.xml
emb_dictionary_fr.xml
Sx300_L....0.0.5.lang

Name	Sx300_LANG_fr_FR_1.0.0.5.lang
Kind	Unix Executable File
Size	496 KB on disk
Created	05/21/10
Modified	05/21/10

STEP 4. Once the upload is complete, you will get a success indication message.



Upgrade/Backup Firmware/Language

Bytes Transferred: 494293

Status: Copy finished

Error Message:

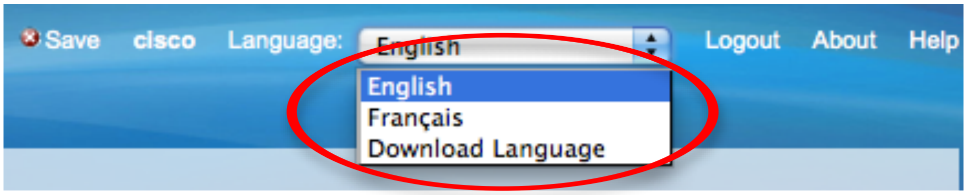
Done

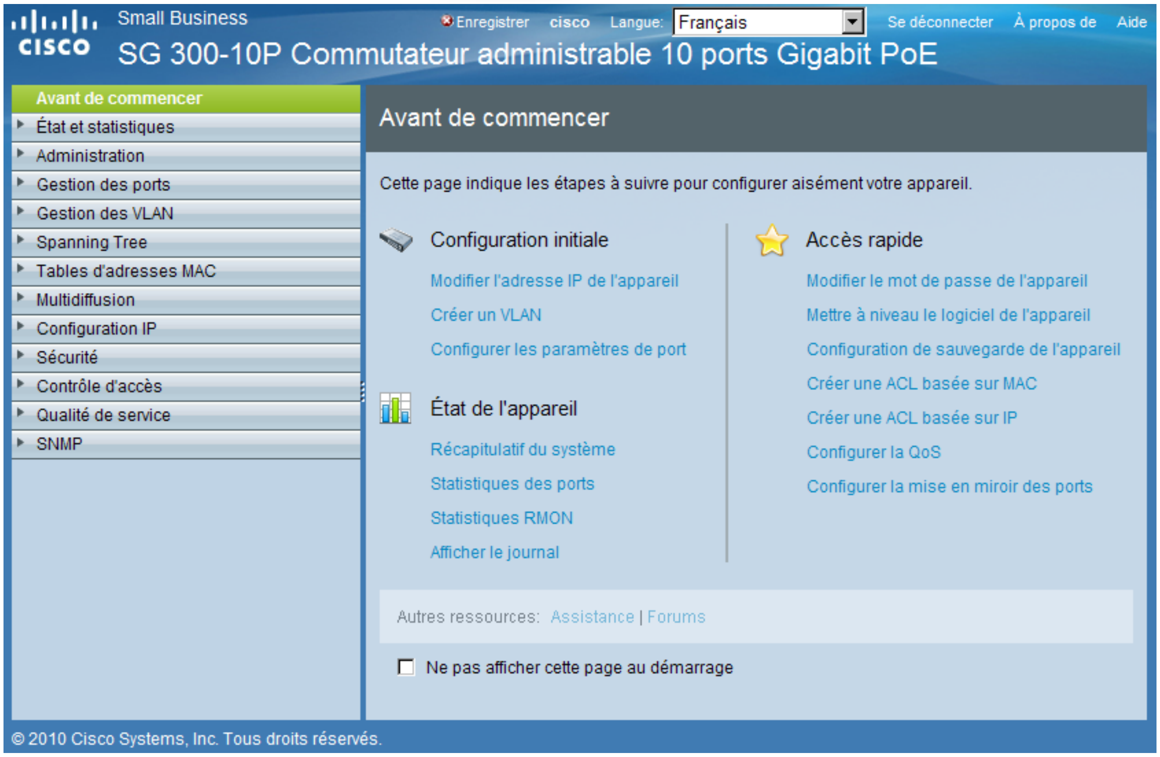
STEP 5. Once the download is complete, notice that the new languages you have downloaded is available on the switch

Scenario 3: Starting to Use the New Language

STEP 1. Once you have downloaded a new language onto the switch, it is easy to begin using it. From the Language drop down menu on the left hand side, select the language you want to use.

STEP 2. Upon selection, the language will be changed on the fly - all menu items and dictionary will be using your selected language, as seen in the screen shot below.





SG 300-10P Commutateur administrable 10 ports Gigabit PoE

- Avant de commencer
- État et statistiques
- Administration
- Gestion des ports
- Gestion des VLAN
- Spanning Tree
- Tables d'adresses MAC
- Multidiffusion
- Configuration IP
- Sécurité
- Contrôle d'accès
- Qualité de service
- SNMP

Avant de commencer

Cette page indique les étapes à suivre pour configurer aisément votre appareil.

Configuration initiale

- Modifier l'adresse IP de l'appareil
- Créer un VLAN
- Configurer les paramètres de port

État de l'appareil

- Récapitulatif du système
- Statistiques des ports
- Statistiques RMON
- Afficher le journal

Accès rapide

- Modifier le mot de passe de l'appareil
- Mettre à niveau le logiciel de l'appareil
- Configuration de sauvegarde de l'appareil
- Créer une ACL basée sur MAC
- Créer une ACL basée sur IP
- Configurer la QoS
- Configurer la mise en miroir des ports

Autres ressources: Assistance | Forums

☐ Ne pas afficher cette page au démarrage

© 2010 Cisco Systems, Inc. Tous droits réservés.

Advanced Demo

In this set of demonstrations we will showcase some of the advanced features that the 300 Series switches has to offer. This will require a slightly different setup than the Basic demo scenarios, which we have shown before, and additional equipment.

Note Please ensure that you have all the equipment necessary to complete your demonstration. Please refer to the Bill of Materials at the beginning of this document

Device Setup

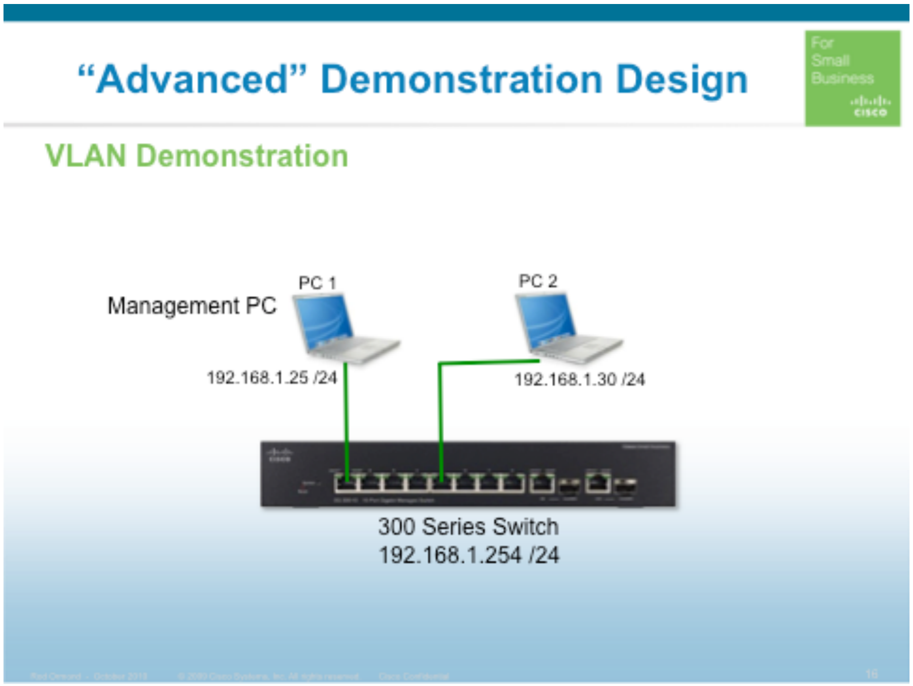
STEP 1. Leave your Management PC as you have it connected from the Basic demonstration, and keep the IP address as is (192.168.1.25 in this example).

STEP 2. Connect an Ethernet Cable from the Ethernet port of your other PC (PC2) to Port 5 of the switch's Ethernet Port. The LEDs on the connected Port should become green to note the Port is operational.

- Port 5 is given as an example, but you can alternatively connect the cable to any other port on the switch.

STEP 3. Configure PC2's IP address to 192.168.1.30, so it will be on the same subnet as the switch and your management PC.

Your network Topology should look like this:



"Advanced" Demonstration Design

VLAN Demonstration

Virtual LANs (VLANs)

To optimize network application performance and security, end-stations (users) that have common attributes or, for example, belong to the same group within the organization, can be grouped together to create one sub-network even if they are not physically on the same network. This segregation of subnets creates logical networks, which do not interfere one with the other, therefore increasing optimization of the network bandwidth and company productivity.

This grouping is called a Virtual LAN (VLAN), and is used widely within organizations' networks.

For example: you can group together your Sales and Marketing team into one VLAN and group the Accounting team into another, so traffic will flow seamlessly in-between these groups, and not interfere with one another.

The 300 Series switch fully manages the Virtual LANs – their administration through an easy configuration menu, and their traffic in a seamless manner without hindering on traffic performance, while providing wire-speed traffic. Moreover, since users/ports are grouped together, regardless of their physical location, this reduces the need for additional routers on the network, thereby providing significant savings. In addition, VLANs provide further security by reducing router hops and Broadcast traffic on the complete network.

This feature provides not only cost reduction, but also significantly increases the performance and safety of your network, and is easily managed and administered in the 300 Series switches.

In this demonstration, we will show how to easily Create a VLAN, Assign a port to the VLAN, Test the VLAN functionality and also how to use Layer 3 mode, the latter being an Advanced option.

Remember to showcase and focus on the key attributes of this feature and the benefits of the 300 Series switches:

- Ease of use
- Intuitive Management Interface
- Cost Savings
- Routing Functionality

In this demonstration, we will show how the Management PC and PC2 can communicate effectively when they are both on the same IP subnet, and using the same VLAN, which is the default management VLAN.
However when PC2 is configured to use a different VLAN, they cannot communicate between each other, although they are physically connected to the same switch.

This demo will take you through this process step-by-step.

Note If you do not have access to another PC, you can a camera instead of PC2, as stated in the BOM. The demo will work exactly the same.

Note This demonstration is equivalent to a real scenario, in where the Sales and Marketing group use VLAN 1 and the Accounting team uses VLAN 10. Random traffic will not flow between the two groups and will not interfere one with the other.

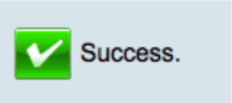
Scenario 1: Creating VLANs

STEP 1. On the menu bar, drop down the **VLAN Management** tab and select **Create VLAN**. Alternatively, you can reach this window by clicking the **Create VLAN** link in the **Getting Started** page.

Note VLAN 1 is created by default for data and management traffic. For stability reasons, please DO NOT delete this VLAN.

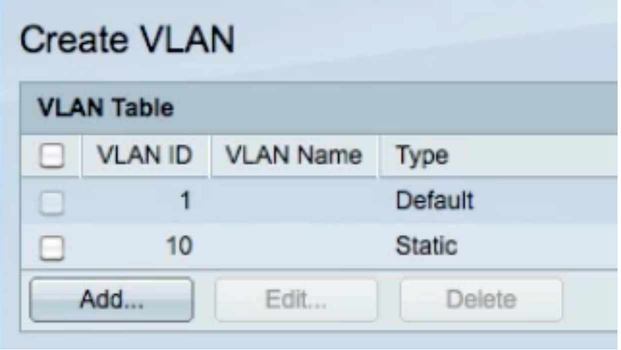
STEP 2. Click the **Add** button. A new window will appear to create a new VLAN. Type in 10 in the VLAN ID space and click **Apply.**

STEP 3. A Success icon will appear on the top to indicate your previous creation took effect



✓ Success.

STEP 4. Ensure that the VLAN you created is visible on the **Create VLAN** page.



Create VLAN

VLAN Table

□	VLAN ID	VLAN Name	Type
□	1		Default
□	10		Static

Scenario 2: Assign a VLAN to a port

STEP 5. In the **VLAN Management** tab, select **Interface Settings**
All the available interfaces of the switch will appear in a list.
Select e1 (or g1 in Gigabit switches) and click **Edit** at the bottom of the page. This will configure Port 1.

STEP 6. Set Interface 2 to **Access**, and click **Apply**
Repeat the same procedure for Port 5 (e5/g5).

Note Trunk is the default setting for the Interface VLAN Mode, and represents a case where multiple VLANs are passing through that port.

In case this interface will include more than one VLAN, its mode will have to be returned to Trunk. This will be the case when connecting Cisco Small Business IP Phones, such as SPA5xx or SPA3xx family, as these natively use a dedicated VLAN to differentiate and prioritize their traffic.

STEP 7. Test that there is connectivity between the 2 PCs, using a ping command:
On your management PC, open a command line prompt, and ping PC2's IP address as follows:
ping 192.168.1.30
Notice that ping queries are answered, and that connectivity is in place between the 2 devices.

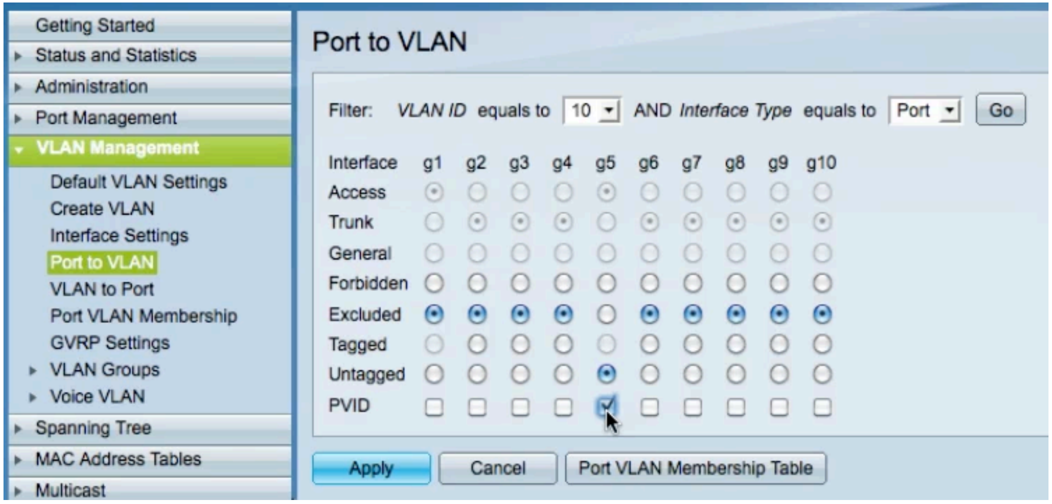
From PC2 you can use a ping command to PC1's IP address, to verify bi-directional connectivity.
ping 192.168.1.25
Notice that ping queries are answered, and that connectivity is in place between the 2 devices.

Scenario 3: Testing VLAN Functionality

STEP 8. In the **VLAN Management** tab, select **Port to VLAN**
All the available interfaces of the switch will appear in a list, including its mode and associated VLANs. Notice that e1 and e2 are set to Access.

STEP 9. Filter via VLAN ID 10 and click **Go.**

STEP 10. Check the PVID box on port 5, and click **Apply.**



Port to VLAN

Filter: *VLAN ID* equals to 10 AND *Interface Type* equals to Port Go

Interface	g1	g2	g3	g4	g5	g6	g7	g8	g9	g10
Access	●	○	○	○	●	○	○	○	○	○
Trunk	○	●	●	●	○	●	●	●	●	●
General	○	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○
Excluded	●	●	●	●	○	●	●	●	●	●
Tagged	○	○	○	○	○	○	○	○	○	○
Untagged	○	○	○	○	●	○	○	○	○	○
PVID	□	□	□	□	☑	□	□	□	□	□

STEP 11. Click on **Port VLAN Membership Table** at the bottom of that page. This will lead you to the **Port VLAN Membership** page on the **VLAN Management** menu.
Here we will see that Port 5 is now a member of VLAN 10,as you have just configured it.

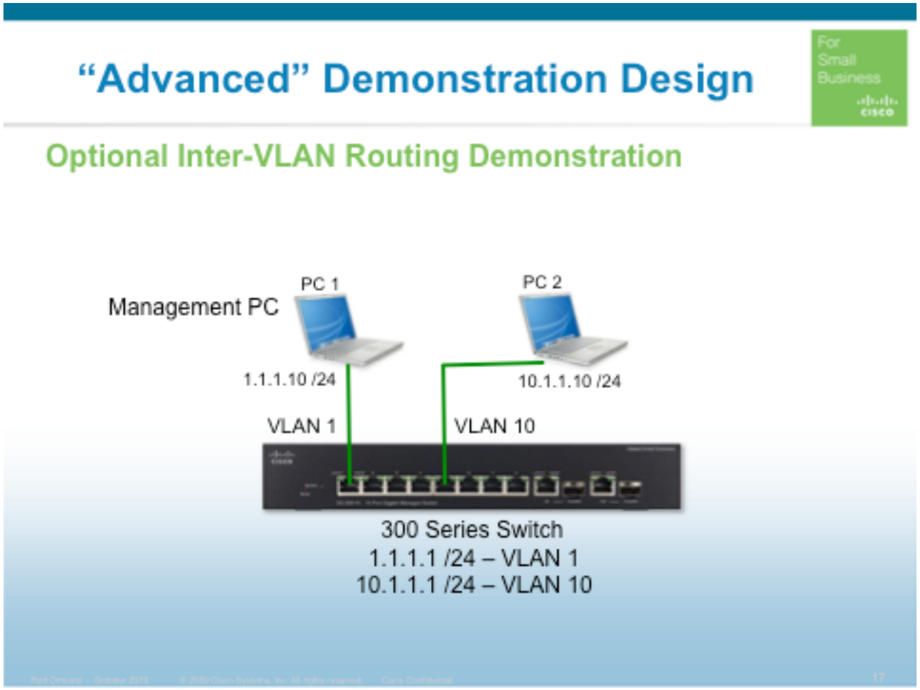
STEP 12. Now that the 2 ports are members of 2 different VLANs, let's test connectivity between the two devices.
Repeat Step 7 to test connectivity between the 2 PCs, through a ping test.
Notice that communication between the two devices have ceased, and packets cannot flow through between them, although they are physically on the same switch.

Scenario 4: Optional Inter-VLAN routing exercise utilizing layer 3 mode

This demonstration will focus on the switches' Routing capabilities.
This is a true differentiator for the 300 Series switches, as many competitive products do not share this functionality.
Moreover, the benefit for the end-user is huge as it saves the extra cost of purchasing additional routers, thereby saving cost for the typical business owner.

In this demonstration, we will show that 2 PCs that are physically connected to ports of the same switch can be assigned not only different Virtual LANs, but also different IP addresses, and behave as if they are on physically separate subnets. The switch routes between the 2 subnets, seamlessly, without disruptions.

We will assign IP addresses in different subnets to our Management PC (PC1) and to PC2, the following manner.
The network topology for this demo should look like this:



"Advanced" Demonstration Design

Optional Inter-VLAN Routing Demonstration

Activating Menu CLI

You will need to utilize the Menu CLI to enable the Layer 3 functionality of the switch.
To do so, follow the following steps:

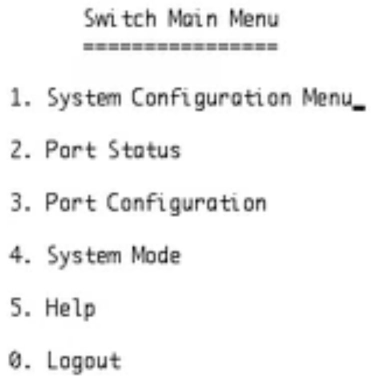
STEP 1. First, you will need to enable Layer 3 Functionality in the switch.
This can be done only through the configuration Menu in CLI.

STEP 2. To do this, connect the switch to your PC via the serial cable and open a Terminal application (HyperTerminal for Windows users)

STEP 3. Verify that the correct Terminal settings apply to your Terminal application, as following:

Data Rate: 115200
Date Bits: 8
Parity: None
Stop Bits: 1

Once the connection is established, enter the switch's Menu CLI screen.



```
          Switch Main Menu
          ================

     1. System Configuration Menu_

     2. Port Status

     3. Port Configuration

     4. System Mode

     5. Help

     0. Logout
```

STEP 4. Navigate using the down arrow button to **System Mode** and click **Enter.**

STEP 5. Navigate to **Edit** using the right arrow button. This will enable you to change the system settings, and will revert the prompt to the editable values.

STEP 6. Use the **space** button to change the configuration from **Layer 2** to **Layer 3.**

STEP 7. Hit the **Esc** button, then right arrow to **Save**, then type in **Y.**
The switch will immediately enter Layer 3 mode.

Note Changing the Routing mode of the switch as described above will reset the previously working settings of the switch, and all configurations done thus far will be eliminated.

You will also need to go back and recreate VLAN 10, and assign it to Port 5, as you've done in the previous demonstration.

Inter-VLAN Routing Demonstration using Layer 3 Mode

STEP 1. Launch a browser and connect to the management user interface of the switch, as we have done throughout the Basic demonstrations.

Note Since the previous configurations were reset, log in with the default username and password: **cisco** and **Cisco.**

You will be prompted again to change your password.

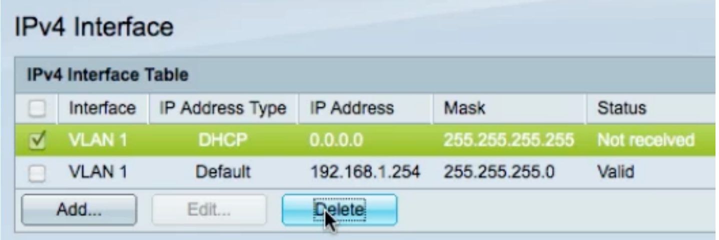
STEP 2. Create VLAN 10 and assign it to Port 5, as you did in the previous demonstration. Repeat Steps 1-11 of the previous demo.

Note Notice that the IPv4 Configuration page is slightly different, now that Layer 3 is enabled. It now lets you configure multiple IP Interfaces, whereas In the Basic demo, we could modify only one IP Address to the switch.

STEP 1. Create the IP interfaces for VLAN 1 and VLAN 10. We will assign the following:
1.1.1.1 to VLAN 1

10.1.1.1 to VLAN 10

STEP 2. Navigate to **IP Configuration** menu and go into **IPv4 Interface.**
Notice that the Interface that is saved for an address obtained by DHCP is present in the list. We will not need this interface, so it is advisable to delete it.
To do so, simply click that entry and choose **Delete.**

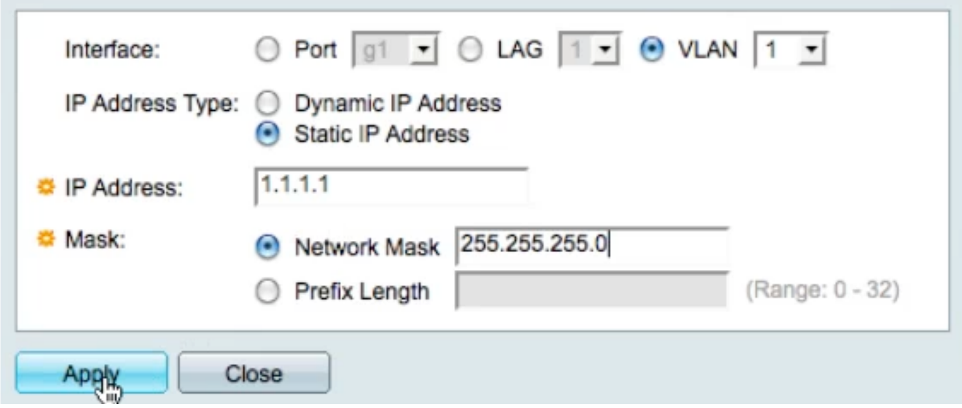


IPv4 Interface

IPv4 Interface Table

□	Interface	IP Address Type	IP Address	Mask	Status
☑	VLAN 1	DHCP	0.0.0.0	255.255.255.255	Not received
□	VLAN 1	Default	192.168.1.254	255.255.255.0	Valid

STEP 3. Add the interfaces discussed above, by clicking **Add** and applying the following information:
IP Address Type: Static IP Address
IP Address: 1.1.1.1
Mask: 255.255.255.0
VLAN: 1



Interface: ○ Port g1 ○ LAG 1 ● VLAN 1

IP Address Type: ○ Dynamic IP Address ● Static IP Address

IP Address: 1.1.1.1

Mask: ● Network Mask 255.255.255.0 ○ Prefix Length (Range: 0 - 32)

Note Connectivity to your PC will stop once the IP address has changed.

STEP 4. Change the static IP address of your Management PC to 1.1.1.10.
Configure the Default gateway to 1.1.1.1, which is now the address for VLAN 1 on the switch.

STEP 5. Ensure that communication has been restored to the switch. You can test this through a simple ping test from a command line window.

STEP 6. Access the switch's web management interface through the **new** IP address assigned. In your web browser, type in
http://1.1.1.1

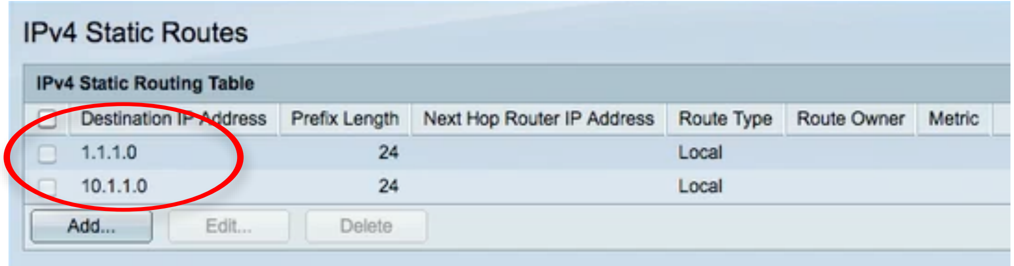
STEP 7. Go back to the **IPv4 Interface** page (in **IP Configuration** menu) and notice that the new interface for VLAN 1 has been changed to 1.1.1.1.

STEP 8. Create another IP Interface for VLAN 10. Follow steps 5-9 of this demo, using the following data:

IP Address Type: Static IP Address
IP Address: 10.1.1.1
Mask: 255.255.255.0
VLAN: 10

Change PC2's IP Address to 10.1.1.10

STEP 9. Navigate to **IP Configuration** menu, then to **IPv4 Static Routes**.
In this page you can see the new Static IP Addresses that were created.



IPv4 Static Routes

IPv4 Static Routing Table

☐	Destination IP Address	Prefix Length	Next Hop Router IP Address	Route Type	Route Owner	Metric
☐	1.1.1.0	24		Local		
☐	10.1.1.0	24		Local		

STEP 10. Now let's test connectivity between the 2 PCs, that are on different IP subnets.
From a command prompt on PC1 (1.1.1.10), ping the following address and verify that communication is successful:
Ping 1.1.1.1
→ this verifies communication with VLAN 1 IP address of the switch
Ping 10.1.1.1
→ this verifies communication with VLAN 10 IP address of the switch, basically showing the switch can route via Layer 3 IP communication
ping 10.1.1.10
→ this is PC2's IP address. This verifies successful communication between both PCs, and that routing is present.

You can conduct the same verifications from PC2, to ensure proper bi-directional communication.

This demo basically shows that 2 separate networks were created, without the use of a router, This type of scenario becomes especially useful when a business network is growing rapidly and a new user can't easily be assigned a physical port that is close to its network.

Moreover, in collaboration projects, where much traffic is generated within groups, VLANs provide an easy method of segregating traffic within a working group, thereby not interfering with other working groups within the company.

This also protects against security threats, such as sensitive information being broadcasted on the network. In this case, only qualified viewers will be able to see this information.

Multicast

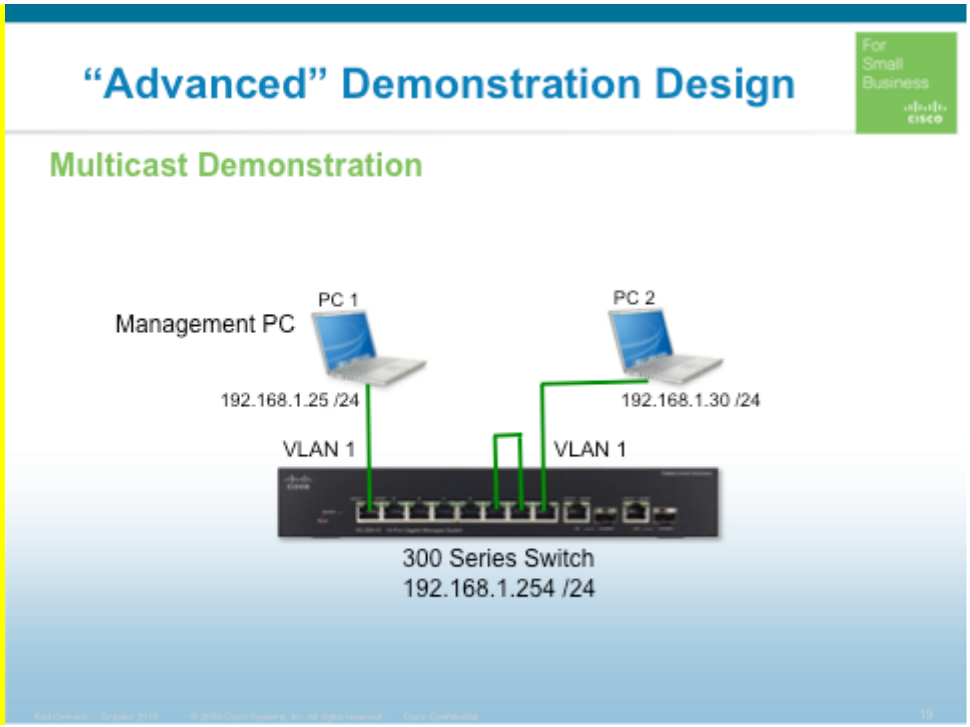
IP Multicast is a technique used for one-to-many communication in a network. The IGMP protocol, which implements Multicast is typically used for streaming media and IP-based television. While the latter is more applicable to residential networks, the former is commonly used in Small Businesses, for example: businesses that conduct learning courses for many participants, or communicate messages through video.

IGMP snooping is a powerful tool for energy and bandwidth conservation, as it requires the transmitter to send a packet only once, even if the media is delivered to many “listeners” (or “viewers”). Since the viewers are required to “register” for the streaming media service, packets are sent only to those registered ports. This powerful tool can be enabled in the switch, thereby realizing significant cost savings in bandwidth, CPU and energy consumption.

Scenario 1: Streaming a Video from a Source to Many Receivers

This demo shows how easy it is to setup IGMP in the 300 series switch, which reduce the energy, CPU and bandwidth consumption when streaming media. We will show how, without IGMP settings packets are being sent to all ports, while with IGMP settings packets are sent only to the “listeners” of that stream.

The setup will look like this:



“Advanced” Demonstration Design

Multicast Demonstration

STEP 1. Ensure that you have 2 PCs connected to your switch, as shown in the figure above, along with an Ethernet cable connected between two other ports on the switch. This will simulate 2 other active users on the network.
PC1 (Video Streaming Client) is connected to port1
PC2 (Video Streaming Server) is connected to port8
Ethernet Cable is connected between port6 and port7

STEP 2. Ensure that VLC software version 0.8.6h is installed on both PC1 and PC2
We will be using multicast address 225.5.5.5 and VLAN 1 as our multicast streaming address and VLAN

STEP 3. Check the status of the switch through the **Status and Statistics > System Summary** page. Notice that there is connectivity on ports 1, 6, 7 and 8.

STEP 4. Ensure that ports 1, 6, 7 an 8 are set for VLAN 1. Go to **VLAN Management > Port VLAN Membership** to view a list of ports and their corresponding VLANs

Setting up VLC Video Streaming Server

STEP 5. Insert a DVD movie into PC2's DVD drive and launch the **VLC application**.

STEP 6. In **File** menu, select **Wizard**. The **Streaming/Transcoding Wizard** appears. This will go through the setup of streaming a video from PC2 to the network.

STEP 7. Select **Stream to Network**, and click **Next**. The **Input** screen will appear. Select **Choose** under **Select a Stream**, and specify the source of the video you will be using. In this case it will be your local CD player. Go to **Disc** tab and select **DVD**, keep all other default settings as they are. Click **OK**, and then click **Next**.

STEP 8. Next we must tell the server how to stream the video.
As mentioned in Step 2, we will be using multicast address 225.5.5.5 for this demonstration.
Select **RTP Multicast** and enter **225.5.5.5** in the **Destination** window. Then click **Next.**

STEP 9. In the **Encapsulation format** screen, select the default **MPEG-TS** and click **Next**

STEP 10. Click **Finish** and exit VLC wizard

STEP 11. You should now hear your CD player start to spin, and you are now streaming to 225.5.5.5

Setting up VLC Video Streaming Client

STEP 12. We will now setup PC1 to receive the video stream.
Open the VLC application. Go to the **File** menu, then select **Open Network.**

STEP 13. In the **Network** tab, select the **UDP/RTP Multicast** radio button and in the **Address** field insert the multicast address that PC2 is streaming the video on – 225.5.5.5.

STEP 14. Click **Ok** and the stream will start to play

Scenario 2: IGMP Snooping

We will now show how multicast and IGMP snooping application on the 300 Series switch saves valuable resources.

The switch's default configuration is Multicast disabled. On the switch's front panel, show how this configuration sends traffic to all available ports, even the ones that are not viewing this video, thereby spending valuable resources. You can see this by showing how ports 6 and 7 (which are connected to each other and simulate 2 additional hosts) light up to show activity.

STEP 15. We will now enable Multicast to correct the default behavior.
In the **Multicast** menu, go to **Properties**.
Enable Multicast by checking the **Bridge Multicast Filtering Status** field.
Under **Forwarding Method for IPv4** select **IP Group Address**
Ensure that VLAN 1 is selected for Multicast VLAN ID
Click **Apply**

STEP 16. Next go to **IP Multicast Group Address**. Click **Add**.

STEP 17. Enter the following into the information pop-up window:
VLAN ID: 1
IP Multicast Group Address: 225.5.5.5
Click **Apply,** then **Close**

STEP 18. Now we will configure IGMP Snooping for the switch to monitor network traffic and to determine the relevant ports to which to send the multicast traffic, thus saving valuable resources.
Go to **IGMP Snooping.** Enable **IGMP Snooping Status** and click **Apply**

STEP 19. In the same window, select the radio button for VLAN 1 and click **Edit**.

STEP 20. In the window opened, enable the **IGMP Snooping Status** and leave the rest at rest at default. Click **Apply,** then **Close**

STEP 21. Go to **IGMP/MLD IP Multicast Group** menu and notice that our configured IP multicast address with VLAN 1 has been added as an entry.

STEP 22. Go back to look at the status LEDs in the front panel and notice that only ports that have registered for this video stream are lit up, and those that have not (i.e. the idle ports 6 and 7) are not getting any traffic sent to them. This basically saves the bandwidth on ports that are not requesting this video.

Security – Access Control Lists

This demonstration focuses on the security aspect of the 300 series switch. As the switch is an integral part of the Small Business network, it provides means for communications and running important applications. But keeping the network secure is an integral part of a Small Business day-to-day life. The 300 series switch includes a wide variety of security features that addresses these security concerns, such as Denial of Service (DoS), Physical Port Security, Management Authentication methods, Access Control and 802.1x, to name a few. This list of features further stresses the superiority of the 300 series switch over competitive products, while providing an enhanced feature-set at a competitive price.

This demonstration focuses on Access Control, a method of controlling the traffic that enters the switch, thereby acting as a filter to deny and/or allow traffic on certain ports to pass through.
We will go through the following steps, which will ultimately showcase how security is enabled:

1. Create an Access Control List (ACL)
2. Create an Access Control Entity (ACE), which is bound to an ACL
3. Bind the ACL to an interface
4. Show how the Access Control rules we've created come into action

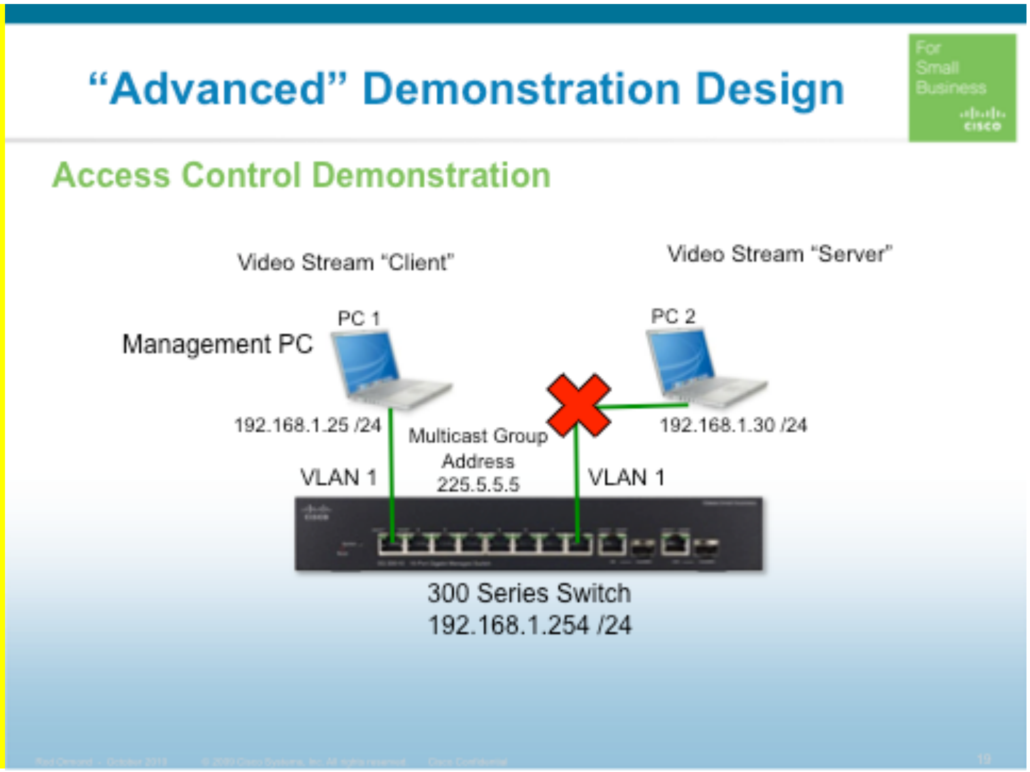
We will show how a video stream that is already passing from 1 port to another, will be denied to pass through, once Access Control is applied and bound to the streaming port (that which is connected to the streaming "server" – see setup below), therefore securing the local Small Business network.

Remember to showcase and focus on the key attributes of this feature and the benefits of the 300 Series switches:

- Ease of use
- Intuitive Management Interface
- Feature richness and market leadership

The setup is the same as in the previous demonstration – Multicast, as we will utilize the video streaming functionality that has already been set up. Note that the Ethernet cable that was plugged in to ports 6 and 7 will not be needed in this demonstration, and should be plugged out.

The setup should look like this:



“Advanced” Demonstration Design

Access Control Demonstration

STEP 1. As you have done in the previous demonstration – multicast, begin to stream video from the Video Streaming “Server”, connected to port 8, to the Video Streaming “Client” connected to port 1. Verify that you can see the video well on the receiving end.

Create an Access Control List (ACL)

STEP 2. Log into the switch’s management interface and navigate to **Access Control**. Show how you have the option to create ACLs and ACEs based on Layer-2 or Layer-3 address or protocol elements, including IPv6.

STEP 3. Go to **IPv4-Based ACL**, and click **Add**

STEP 4. Enter a name for this Access Control List in the **ACL List** window. Enter a name that is relevant to the operation you will be configuring, such as **“DenyAll”**. Note that many ACLs can be configured at any given time, therefore it's important to differentiate your ACL name so you will remember its functionality.

STEP 5. Click **Apply**, then **Close**

Create an Access Control Element (ACE)

STEP 6. Once the ACL has been created, you will return to the IPv4-Based ACL page, where you will find a shortcut to create an ACE for the ACL you've created - IPv4-Based ACE.
Show how intuitive the management interface is, such that it helps the user not forget important configuration items and guides the user through the process, by providing shortcuts and guidance.

STEP 7. Click on the **IPv4-Based ACE** button, or go to the **IPv4-Based ACE** link in the menu bar.

STEP 8. The IPv4-Based ACE page appears. Ensure that the ACL you are filtered on is **DenyAll.**
Notice that there are no ACEs configured.

STEP 9. Click **Add** to create a new traffic filter for the ACL we have just created

STEP 10. The ACE page appears. Notice that the ACL name is **DenyAll**.

STEP 11. We will assign to this ACE attributes that filter all incoming traffic into a given port.
Assign the following values to this page:
Priority: 1
Action: Deny
Protocol: Any
Source IP Address: Any
Destination IP Address: Any
Type of Service: Any
Click **Apply,** then **Close** to save your ACE

STEP 12. You will return to the IPv4-Based ACE page, where the ACE you've created will appear in the designated rows.

Bind the ACL to an interface

STEP 13. Now that we've created the elements in which we will control traffic, we will bind it to port 8, which is the video streaming server.
Go to **ACL Binding** and select port 8. Click **Edit**

STEP 14. Check the **Select IPv4-Based ACL** checkbox, and select the ACL you want to bind the port to. In our case there is only one option and that is **DenyAll**
We will apply these changes in the next section, when we will see Access Control List in action. Keep this window open.

Show the Access Control List in Action

STEP 15. Go back to watching the video you are streaming, on PC1 – the Video Streaming "Client".

STEP 16. Now revert to the switch's management interface and click **Apply** on the **ACL Binding** window. You will be returned to the **ACL Binding** page, where you can see that port 8 is bound to the ACL **DenyAll**

STEP 17. Show how the video has stopped on the receiving end, the moment the ACL was bound to port 8. This filter basically blocks anything from entering this port

STEP 18. Now let's un-bind the ACL from port 8 and see how the video continues to flow.
Click the port 8 checkbox and click **Clear.**

This will essentially allow all traffic that was blocked to flow through once more through the switch.
The movie that was stopped, upon creation of a ACL, will continue to stream once more once that ACL is un-bound from that port.

Quality of Service

Coming soon….