VLAN Best Practices and Security Tips for Cisco Business Routers

Objective

The objective of this article is to explain the concepts and steps for performing best practices and security tips when configuring VLANs on Cisco Business equipment.

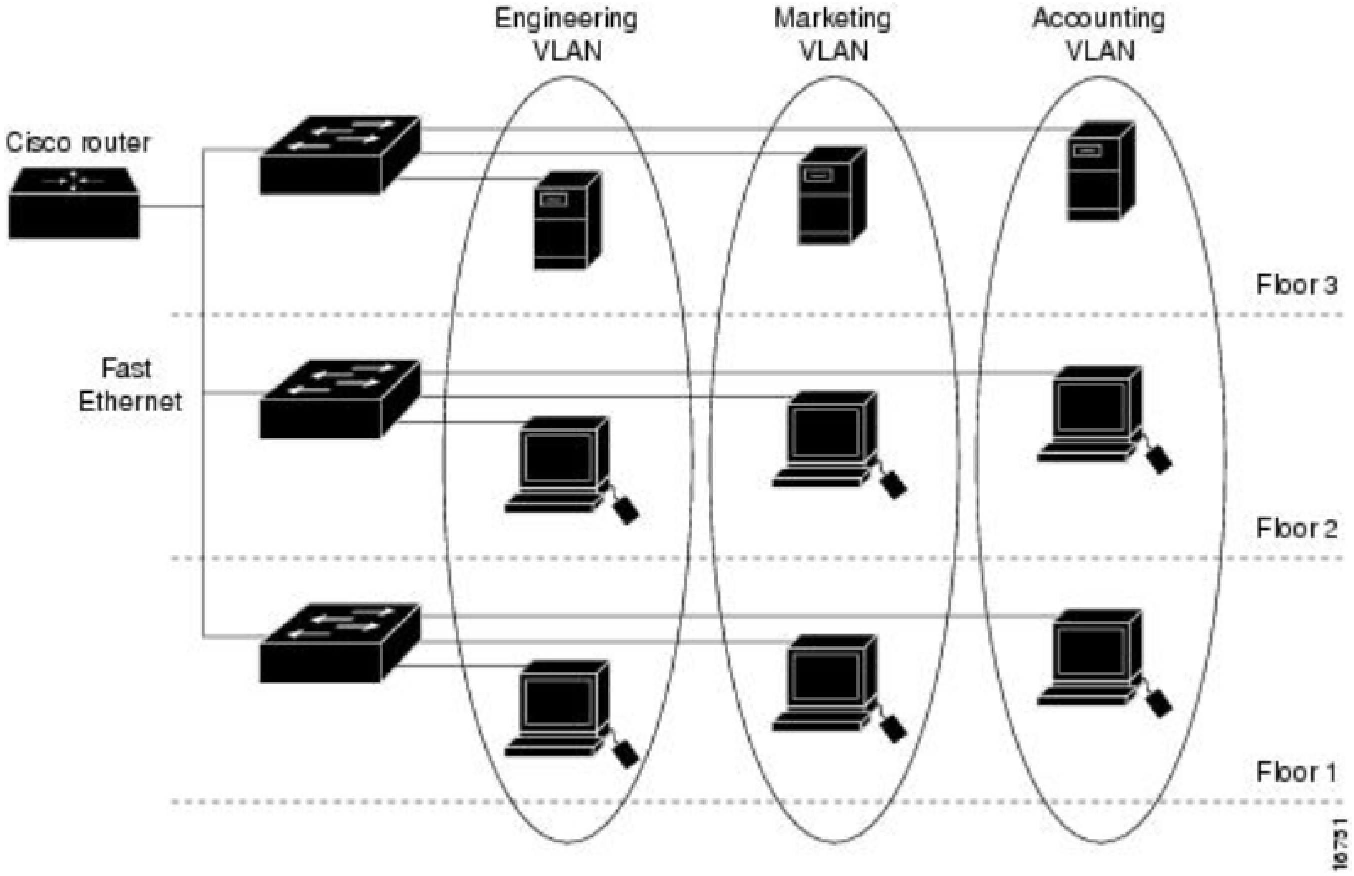
Table of Contents

Introduction

Want to make your business network more efficient while keeping it secure? One of the ways to do this is to correctly set up Virtual Local Area Networks (VLANs).

A VLAN is a logical group of workstations, servers, and network devices that appear to be on the same Local Area Network (LAN) despite their geographical distribution. In a nutshell, hardware on the same VLANs enable traffic between equipment to be separate and more secure.

For example, you might have an Engineering, Marketing, and Accounting department. Each department has workers on different floors of the building, but they still need to access and communicate information within their own department. It is essential for sharing documents and web services.



VLANs need to be set up with best practices in order to keep your network secure. Make the following smart choices when setting up VLANs. You won't regret it!

Applicable Devices

- RV042
- RV110W
- RV130
- RV132
- RV134W
- RV160W
- RV215W
- RV260
- RV260P
- RV260W
- RV320
- RV325
- RV340
- RV340W
- RV345
- RV345P

You might be interested to know that the RV160 or RV260 series routers can carry up to 16 VLANs, while the RV34x series routers can carry up to 32 VLANs. The RV320 supports up to 7 VLANs. If you would like to know how many VLANs your router can carry, check the Data Sheet for your specific model on the Cisco Website. Select **Support** and enter your model number or simply do a search for the Data Sheet and model number.

Some Quick Vocabulary for the Newbies

Access Port: An access port carries traffic for only one VLAN. Access ports are often referred to as an untagged port, since there is only one VLAN on that port and traffic can be passed without tags.

Trunk Port: A port on a switch that carries traffic for more than one VLAN. Trunk ports are often referred to as tagged ports since there is more than one VLAN on that port and traffic for all but one VLAN need to be tagged.

Native VLAN: The one VLAN in a trunk port that doesn't receive a tag. Any traffic that doesn't have a tag will be sent to the native VLAN. That is why both sides of a trunk need to make sure they have the same native VLAN or traffic will not go to the correct place.

Best Practice #1 - VLAN Port Assignment

Port Assignment Basics

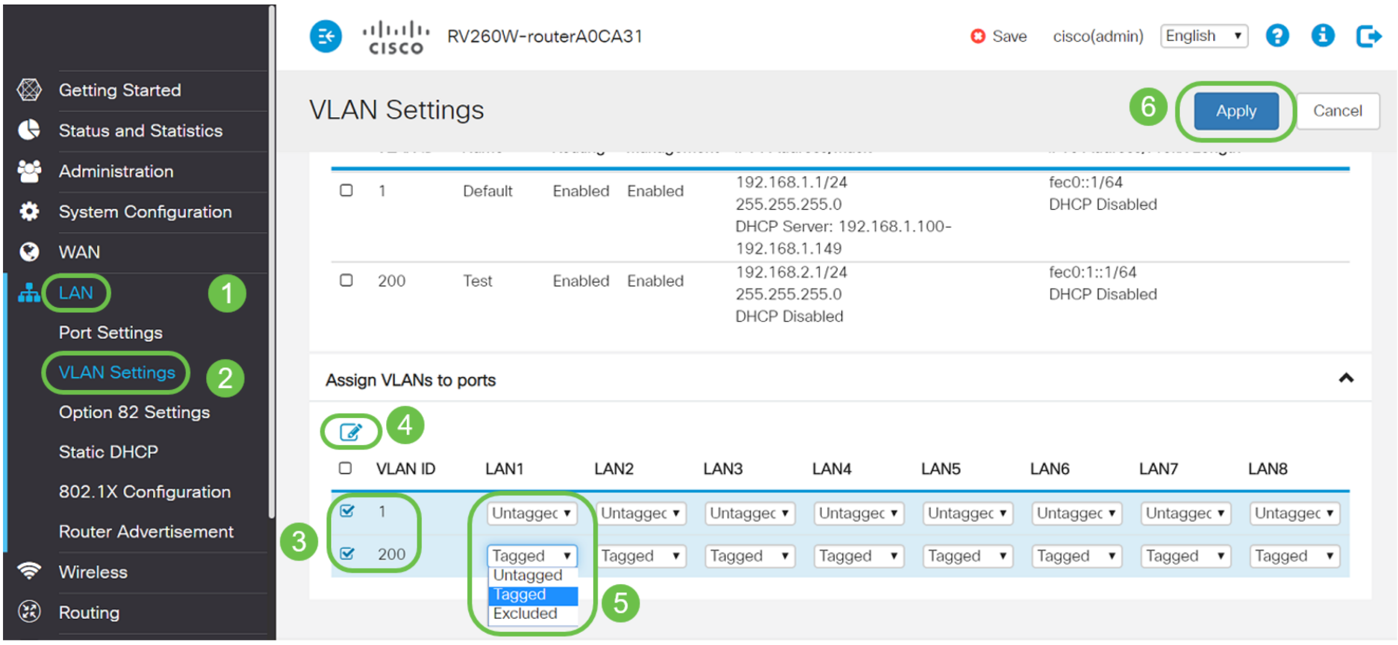
- Each LAN port can be set to be an access port or a trunk port.
- VLANs that you don't want on the trunk should be excluded.
- A VLAN can be placed in more than one port.

Configuring Access Ports

- One VLAN assigned on a LAN port
- The VLAN that is assigned this port should be labeled *Untagged*
- All other VLANs should be labeled *Excluded* for that port

To set these correctly, navigate to **LAN > VLAN Settings**. Select the *VLAN IDs* and **click** on *edit* icon. Select the drop-down menu for any of the LAN interfaces for VLANs listed to edit the VLAN tagging. Click **Apply**.

Check out this example of each VLAN assigned its own LAN port:



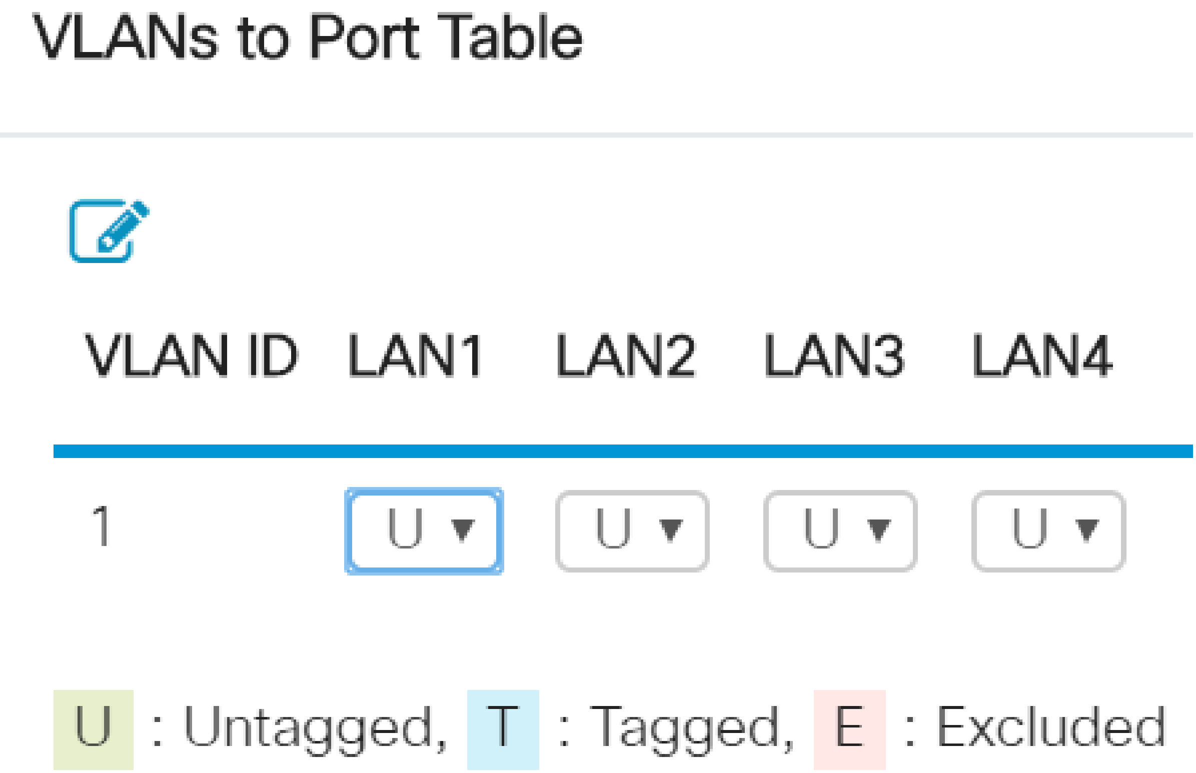
VLAN Settings

□	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149	fec0::1/64 DHCP Disabled
□	200	Test	Enabled	Enabled	192.168.2.1/24 255.255.255.0 DHCP Disabled	fec0:1::1/64 DHCP Disabled

Assign VLANs to ports

□	VLAN ID	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6	LAN7	LAN8
☑	1	Untaggec	Untaggec	Untaggec	Untaggec	Untaggec	Untaggec	Untaggec	Untaggec
☑	200	Tagged Untagged Tagged Excluded	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged

This Graphical User interface (GUI) image was taken from an RV260W router. Your options may appear slightly different. For example, on the RV34x series, the labels *Untagged*, *Excluded*, and *Tagged* are abbreviated to just the first letter. The process is still the same.



VLANs to Port Table

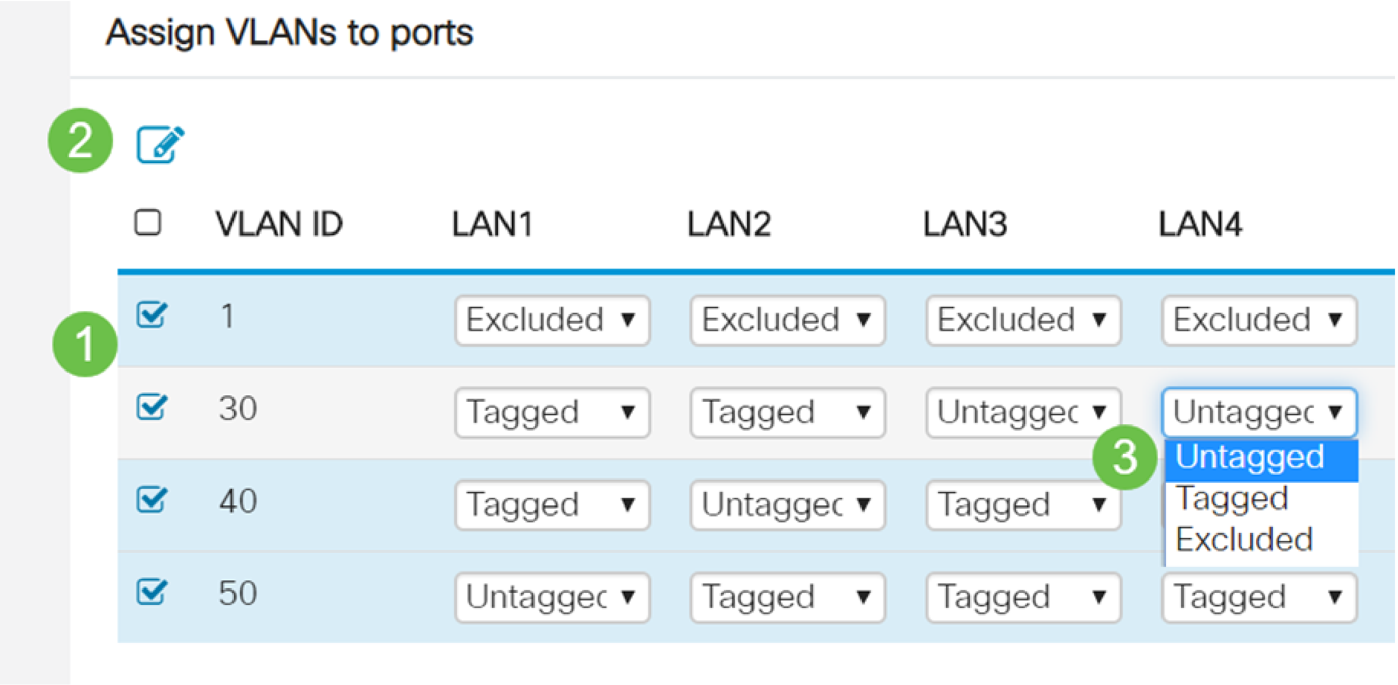
VLAN ID	LAN1	LAN2	LAN3	LAN4
1	U ▾	U ▾	U ▾	U ▾

U : Untagged, T : Tagged, E : Excluded

Configuring Trunk Ports

- Two or more VLANs share one LAN port
- One of the VLANs can be labeled *Untagged*.
- The rest of the VLANs that are part of the trunk port should be labeled *Tagged*.
- The VLANs that are not part of the trunk port should be labeled *Excluded* for that port.

Take a look at this example of various VLANs that are all on trunk ports. To set these correctly, select the *VLAN IDs* that need to be edited. **Click** on the *edit* icon. Change them based on your needs, following the above recommendations. By the way, did you notice that VLAN 1 is excluded from every LAN port? This will be explained in the section, Best Practice for Default VLAN 1.



Assign VLANs to ports

☐	VLAN ID	LAN1	LAN2	LAN3	LAN4
☑	1	Excluded ▼	Excluded ▼	Excluded ▼	Excluded ▼
☑	30	Tagged ▼	Tagged ▼	Untaggec ▼	Untaggec ▼
☑	40	Tagged ▼	Untaggec ▼	Tagged ▼	Untagged Tagged Excluded
☑	50	Untaggec ▼	Tagged ▼	Tagged ▼	Tagged ▼

Frequently Asked Questions

Why is a VLAN left untagged when it is the only VLAN on that port?

Since there is just one VLAN assigned on an access port, outgoing traffic from the port is sent without any VLAN tag on the frames. When the frame reaches the switch port (incoming traffic), the switch will add the VLAN tag.

Why are VLANs tagged when they are part of a trunk?

This is done so that traffic that passes doesn't get sent to the wrong VLAN on that port. The VLANs are sharing that port. Similar to apartment numbers added to an address to make sure the mail goes to the correct apartment within that shared building.

Why is traffic left untagged when it is part of the native VLAN?

A Native VLAN is a way of carrying untagged traffic across one or more switches. The switch assigns any untagged frame that arrives on a tagged port to the native VLAN. If a frame on the native VLAN leaves a trunk (tagged) port, the switch strips the VLAN tag out.

Why are VLANs excluded when they are not on that port?

This keeps the traffic on that trunk only for the VLANs the user specifically wants. It is considered a best practice.

Best Practice #2 - Default VLAN 1 and Unused Ports

All ports need to be assigned to one or more than one VLAN, including the native VLAN. Cisco Business routers come with VLAN 1 assigned to all ports by default.

A management VLAN is the VLAN that is used to remotely manage, control, and monitor the devices in you network using Telnet, SSH, SNMP, syslog, or Cisco’s FindIT. By default, this is also VLAN 1. A good security practice is to separate management and user data traffic. Therefore, it is recommended that when you configure VLANs, you use VLAN 1 for management purposes only.

To communicate remotely with a Cisco switch for management purposes, the switch must have an IP address configured on the management VLAN. Users in other VLANs would not be able to establish remote access sessions to the switch unless they were routed into the management VLAN, providing an additional layer of security. Also, the switch should be configured to accept only encrypted SSH sessions for remote management. To read some discussions on this topic, click on the following links on the Cisco Community website:

- Management VLAN Discussion #1
- Management VLAN Discussion #2

Frequently Asked Questions

Why is default VLAN 1 not recommended to virtually segment your network?

The main reason is that hostile actors know VLAN 1 is the default and often used. They can use it to gain access to other VLANs via "VLAN hopping". As the name implies, the hostile actor may send spoofed traffic posing as VLAN 1 which enables access to trunk ports and thereby other VLANs.

Can I leave an unused port assigned to default VLAN 1?

To keep your network secure, you really shouldn't. It is recommended to configure all those ports to be associated with VLANs other than default VLAN 1.

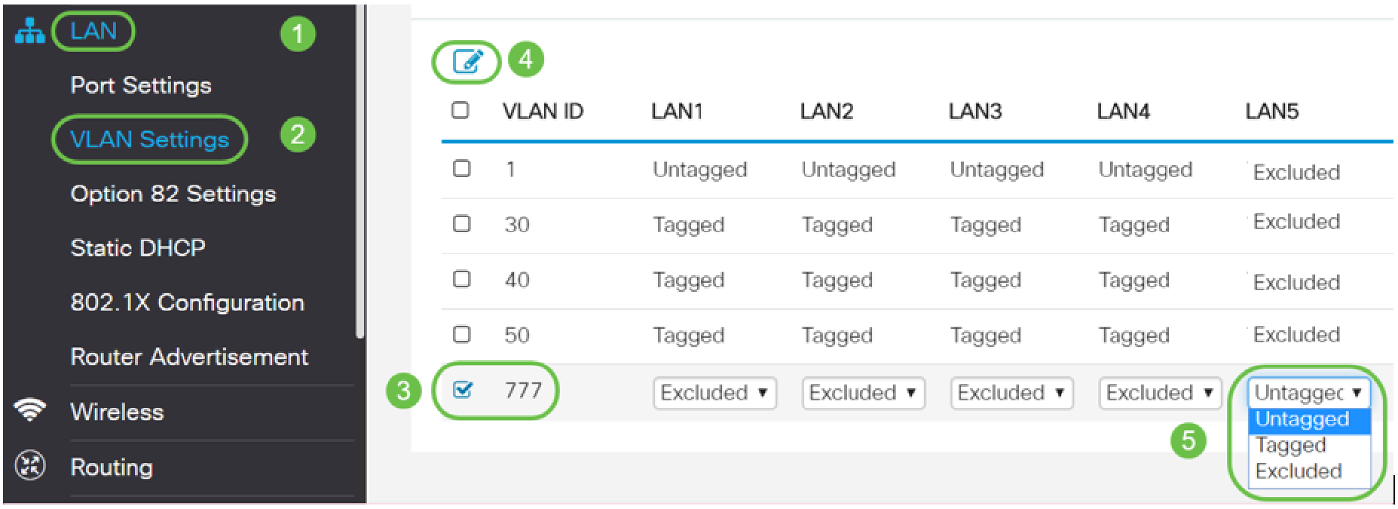
I don't want to assign any of my production VLANs to an unused port. What can I do?

It is recommended that you create a "dead-end" VLAN following the instructions in the next section of this article.

Best Practice #3 - Create a "Dead End" VLAN for Unused Ports

Step 1. Navigate to **LAN > VLAN Settings**.

Choose any random number for the VLAN. Be sure that this VLAN does not have DHCP, Inter-VLAN routing, or device management enabled. This keeps the other VLANs more secure. Put any unused LAN port on this VLAN. In the example below, *VLAN 777* was created and assigned to *LAN5*. This should be done with all unused LAN ports.



☐	VLAN ID	LAN1	LAN2	LAN3	LAN4	LAN5
☐	1	Untagged	Untagged	Untagged	Untagged	Excluded
☐	30	Tagged	Tagged	Tagged	Tagged	Excluded
☐	40	Tagged	Tagged	Tagged	Tagged	Excluded
☐	50	Tagged	Tagged	Tagged	Tagged	Excluded
☑	777	Excluded ▾	Excluded ▾	Excluded ▾	Excluded ▾	Untagged ▾

Notice that the other VLANs are excluded from this LAN port.

Step 2. **Click** on the *Apply* button to save the configuration changes you have made.

Best Practice #4 - IP Phones on a VLAN

Voice traffic has stringent Quality of Service (QoS) requirements. If your company has computers and IP phones on the same VLAN, each tries to use the available bandwidth without considering the other device. To avoid this conflict, it is good practice to use separate VLANs for IP telephony voice traffic and data traffic. To learn more about this configuration, check out the following articles and videos:

- Cisco Tech Talk: Voice VLAN Setup and Configuration Using Cisco Small Business Products (video)
- Configuring Auto Voice VLAN with QoS on the SG500 Series Switch
- Voice VLAN Configuration on the 200/300 Series Managed Switches
- Cisco Tech Talk: Configuring Auto-Voice VLAN on SG350 and SG550 Series Switches (video)

Best Practice #5 - Inter-VLAN Routing

VLANs are set up so that traffic can be separate, but sometimes you need VLANs to be able to route between each other. This is inter-VLAN routing and is typically not recommended. If this is a need for your company, set it up as securely as possible. When using inter-VLAN routing, make sure to restrict traffic using Access Control Lists (ACLs), to servers that contain confidential information.

ACLs perform packet filtering to control the movement of packets through a network. Packet filtering provides security by limiting the access of traffic into a network, restricting user and device access to a network, and preventing traffic from leaving a network. IP access lists reduce the chance of spoofing and denial-of-service attacks, and allow dynamic, temporary user-access through a firewall.

- Inter-VLAN Routing on an RV34x Router with Targeted ACL Restrictions
- Cisco Tech Talk: Configuring Inter-VLAN Routing on SG250 Series Switches (video)
- Cisco Tech Talk: Inter-VLAN Configuration on RV180 and RV180W (video)
- RV34x Inter-VLAN Access Limitation (CSCvo92300 bug fix)

Conclusion

There you have it, now you know some best practices for setting up secure VLANs. Keep these tips in mind when you configure VLANs for your network. Listed below are some articles that have step by step instructions. These will keep you moving toward a productive, efficient network that is just right for your business.

- Configuring VLAN Settings on the RV160 and RV260
- Configure Virtual Local Area Network (VLAN) Settings on an RV34x Series Router
- Configure VLAN Membership on RV320 and RV325 VPN Routers
- Configure Virtual Local Area Network (VLAN) Membership on an RV Series Router
- Configure VLAN Interface IPv4 Address on an Sx350 or SG350X Switch through the CLI