Global Knowledge ™

Expert Reference Series of White Papers

Switching Essentials

Switching Essentials

Dheeraj (Raj) Tolani, CCSI, CCENT, CCNA, CCDA, CCNP, CCDP, CCIP, CCVP

Introduction

In every introductory class we teach we get students who are either puzzled about router essentials or switching essentials or both. This switching essentials white paper will give you the basics that will make learning about switching a little less painless when you sit in a course like *ICND1*, *ICND2*, *CCNA Boot Camp* or *BCMSN*.

Switching is an interesting topic. It could be an easy thing in your network, or it could be something that keeps you up nights. Switching can be simple, allowing us to connect our users from various systems (host systems and phones), or it can be a complicated system with various advanced topics.

In this white paper, we will address the basics of this Layer 2 technology and help you get your switch up and running. For our examples, we will use Cisco's 2950 switch.

In the past, some switches, such as the Cisco 1900 series, have given us the ability to configure the basics of switching using menus. I prefer to have more control over my switches, so I like the current switches that allow me to configure various components using the Cisco commands.

Same as a router, the switch allows us to configure some of the basic things using a set-up script. This set-up script is simply a yes/no interactive questionnaire that allows any novice to get the switch up and running. We will not be using the set-up script for our discussion.

When we say "no" to the set-up script, we're left in a basic mode (user EXEC mode, discussed in the previous router articles):

Switch>

At this mode, we don't have much power to do anything. In order to be able to configure anything, we need to be in privilege EXEC mode (a.k.a. enable mode). The command that takes us to the privilege exec mode is "enable":

Switch>enable
Switch#

You may remember from our previous articles about routers that the user EXEC mode is also known as privilege level 1, and the enable mode is known as privilege level 15. At privilege level 15, since we're allowed to do basically anything we wish, it's important to be careful of the commands we type. Sure don't want to accidentally type commands like "reload!"

We can determine the mode we're in by the prompts we see, or we can type the command "show privilege" to see what our privilege level is.

One of the basic things to configure is the switch hostname. The command to do that is "hostname" followed by the name that we wish to assign to the switch:

Switch#configure terminal
Switch(config)#hostname AccessSwitch
AccessSwitch(config)#

Note that changing a switch's name is a global task, so in order to pull that off, we needed to be in the global configuration mode. We used the "configure terminal" command to get there. Note, also, the change in the prompt. The prompt **[Switch(config)#]** tells us we're in global configuration mode, meaning whatever we configure here will have a global impact. So, we have changed the switch's name to AccessSwitch.

Unlike a router, which is a Layer 3 device and has many interfaces that we put IP addresses on, the switch is a Layer 2 device that doesn't really need any IP addresses. The only reason to assign an IP address on the switch would be to manage it remotely.

In fact, you could take a brand new 2950 switch out of the box, start plugging users into it, and the users would be able to communicate with each other and on the network (providing we haven't messed up the IP addresses on the PCs). Cisco's 2950 Catalyst switch assumes that all ports out of the box are part of one logical Layer 2 grouping called VLAN 1.

So, let's say we want to be able to manage this switch—meaning we want to be able to ping this switch from remote systems, telnet to and from it, ping from it, and possibly access it via http or any other GUI management method. The IP address we are about to assign will be used as a destination IP if we are connecting to the switch remotely. If we are pinging from the switch, then this IP address will be the source address.

In a switch, the IP address is assigned to a management VLAN. A VLAN is a logical interface, unlike a router, which is a physical interface. The default management VLAN is VLAN 1.

Let's configure this VLAN 1 with an IP address and ensure that remote systems can ping us:

AccessSwitch(config)#interface vlan 1
AccessSwitch(config-if)#ip address 10.1.1.100 255.255.255.0
AccessSwitch(config-if)#no shutdown
AccessSwitch(config-if)#exit
AccessSwitch(config)#ip default-gateway 10.1.1.1
AccessSwitch(config)#end
AccessSwitch#copy run start

What have we done here? First, we went to the software interface mode we wanted to configure, VLAN 1, and then we assigned the IP address on it while we were in the interface configuration mode (IP address 10.1.1.100 with a subnet mask of 255.255.255.0). Then, we brought up the interface using the "no shutdown" command. Next, the "exit" command takes us one step back to the global configuration mode where we assigned a default gateway of 10.1.1.1 for all remote communications from this switch's IP network (10.1.1.0 subnetwork).

Now we can ping all local systems, and we can go to our default gateway (Layer 3 device – router) for all remote communications, providing that remote router has a route for those destinations.

Wait… we rushed and gave other administrators in our organization the IP address of our switch. They are able to ping us, but unfortunately the telnet is not working. Hmm, I wonder why? That need to be fixed. Stay tuned.

Enabling Connectivity in our Switch

We configured an IP address on our management interface VLAN 1, and we assigned a default gateway on the switch, so people are now able to ping us. We are also able to ping our local and remote systems, proving to us that the router is routing and taking us to those remote networks (For demonstration purposes, our router IP is 10.1.1.1).

However, when people tried to telnet to our switch, they weren't able to. We have to allow telnet access so our other administrators can telnet to our device. We also want to ensure that we do all basic configurations so our switch is protected.

Let's configure the basic components. For explanation purposes, let's put a line number on the left side of the commands.

Line 1:	**AccessSwitch>enable**
Line 2:	**AccessSwitch#config t**
Line 3:	**AccessSwitch(config)#line vty 0 4**
Line 4:	**AccessSwitch(config-line)#login**
Line 5:	**AccessSwitch(config-line)#password cisco**
Line 6:	**AccessSwitch(config-line)#exit**
Line 7:	**AccessSwitch(config)#line console 0**
Line 8:	**AccessSwitch(config-line)#login**
Line 9:	**AccessSwitch(config-line)#password cisco**
Line 10:	**AccessSwitch(config-line)#exec-timeout 20 30**
Line 11:	**AccessSwitch(config-line)#logging sync**
Line 12:	**AccessSwitch(config-line)#end**
Line 13:	**AccessSwitch#copy run start**
Line 14:	**AccessSwitch#disable**
Line 15:	**AccessSwitch>**

In Line 1, using the "enable" command, we went to the privilege EXEC mode.

In Line 2, at the privilege EXEC mode, using the command "config t" (short for "configure terminal" since Cisco devices allow us to abbreviate to save time and typing), we went to the global configuration mode.

In Line 3, at the global configuration mode using the command "line vty 0 4", we specified that we wish to allow five simultaneous telnet connections to our AccessSwitch, 0 being the first connection and 4 being the fifth connection. So, 0-4 is a range.

In Line 4, we basically specified that we want people to be able to login.

In Line 5, we configured the password that will allow people to be able to login to this switch.

In Line 6, we used the "exit" command to go one step back. In this case, we went from line configuration mode to global configuration mode.

In Line 7, we used the "line console 0" command to go to the line configuration mode. For the console configuration, we were first there for VTY access—the five telnet connections we configured in Line 3.

Line 8 is the same as Line 4, but this time for connections on the console port.

Line 9 is the same as Line 5, but this time for connections on the console port.

Line 10 specifies that we want the connection to time out after 20 minutes and 30 seconds of no activity.

Line 11 specifies that all system alerts or status change messages will be thrown one line above the line where we're typing so our work will stay uninterrupted.

Line 12 uses the command "end," which takes us straight to the privilege EXEC mode. We could have used <ctrl+z> to accomplish this as well.

In Line 13, we saved the configuration from RAM to NVRAM so it will be loaded the next time we reload the box or if we lose power to the box.

In Line 14, we used the "disable" command to take us from privilege EXEC mode to user EXEC mode.

At Line 15, we are at the user EXEC mode.

The beauty of using Cisco's IOS is that the commands are very similar between routers and switches. Once you get some practice with routers, you can use the same skills on switches.

Now that we have a basic switch running and people are able not only to ping us but also to telnet to this switch, we should do some basic things to secure the switch and/or we should do some fun Layer 2 things.

VLAN Assignments

It's about time we do some fun things with our switch. We have just set up a basic IP address on it for management purposes, along with the default gateway so that it can be managed from remote locations.

Many other cool things can be set up on the switch that'll make our lives a little easier. We can even have people plugged into one switch and still be part of a different logical network. This logical breakdown of the networks is known as a Virtual Local Area Network (VLAN).

After you set up these VLANs, you'll need a Layer 3 device (router) so people from one VLAN can connect to another VLAN. That involves trunking to an external Layer 3 device using some protocols like dot1q. These topics are covered in the CCNA Boot Camp at Global Knowledge. In this article, we will get the VLANs created and talk about easy ways of doing some of these things.

When the switch is turned on, the default is that every port on that switch is part of the same logical group called VLAN1. All systems that will be plugged into this switch would therefore be part of the same grouping. The Layer 3 grouping is IP subnets. You would usually plan your VLANs and your IP subnets around the same time, and you'd typically have an IP subnet for every single VLAN. Every VLAN should be its own IP subnet.

Now that we are about to create logical grouping in this switch, we should be very comfortable with IP subnets. If you're not, you can check out my white paper "Solving the Mysteries of Subnetting" in the Knowledge Center at globalknowledge.com.

For example purposes, let's assume that our switch is a 24-port switch. We will create four VLANs and assign six ports in each VLAN. This is the same switch we have been using in our previous articles. Let's start with two VLANs and do the other two later.

The command to create the VLAN is done at the global configuration mode (refer to the previous articles if you are not sure about what the different modes are).

```
AccessSwitch>enable
AccessSwitch#conf t
AccessSwitch(config)#vlan 2
AccessSwitch(config-vlan)#name SecondFL
AccessSwitch(config-vlan)#exit
AccessSwitch(config)#vlan 3
AccessSwitch(config-vlan)#name ThirdFL
AccessSwitch(config-vlan)#end
AccessSwitch#
```

Now that we have created the VLANs, we can verify that they exist using the "Show vlan" command from the privilege EXEC mode. You can see from the configuration above that we also gave these VLANs a descriptive name (2nd Floor and 3rd Floor in our example). This optional descriptive name is just to make things easier later on if we have to troubleshoot any VLAN issues. If we had not given the names, then the system would have automatically assigned VLAN0002 and VLAN0003 as names for VLAN 2 and VLAN 3 respectively. These names don't describe the function of the VLANs. Typically you would use the names to describe the purpose of the VLAN in real life, like Marketing, or Production, or Research, or something that can identify the purpose of these VLANs.

At this point, these VLANs are not accomplishing anything, since we haven't assigned our ports to the VLANs. The ports still belong to the default VLAN 1. So, let's change our ports' memberships to VLAN 2 and VLAN 3.

For our example, let's assign port 7 to VLAN 2 and assign port 18 to VLAN 3. Here we go:

```
AccessSwitch#config t
AccessSwitch(config)#interface fa 0/ 7
AccessSwitch(config-if)#switchport access vlan 2
AccessSwitch(config-if)#exit
AccessSwitch(config)#interface fa 0/18
AccessSwitch(config-if)#switchport access vlan 3
```

Again, we can verify the membership by the "Show vlan" command.

All right. Mission accomplished. We have now created two VLANs (VLAN1 already exists so we really have three VLANs so far) and port 7 and port 18 have been specifically added to VLAN 2 and VLAN 3, respectively. We just have to repeat the above process for every other port whose VLAN assignment we want changed.

Don't you think it's tedious to create the VLANs and then assign every single port to their appropriate VLANs? Yep, me too. And there's an easier way. Current versions of the Cisco's Operating System provide an option to specify a range of ports so we can add multiple ports in a VLAN in one shot. Let's do that for the ports from fa 0/19 to fa 0/24 (remember fa in these commands just means FastEthernet):

```
AccessSwitch(config-if)#exit
AccessSwitch(config)#vlan 4
AccessSwitch(config-vlan)#exit
AccessSwitch(config)#interface range fa 0/19 – 24
AccessSwitch(config-if-range)#switchport access vlan 4
```

So, here we created the VLAN, VLAN4, and then assigned ports fa 0/19 to fa 0/24 in VLAN 4. This makes more sense than repeating the steps for every single port.

Now, some people argue that this two-step process—creating the VLANs then assigning the ports to the appropriate VLAN—is also too much. For those people (not for the exam), the correct answer would be to just go to the interface configuration mode and start assigning the ports to the VLANs. The Cisco switch is smart enough to know that the VLAN doesn't exist, and it will create the VLAN for you as well as assign the port(s) to the VLAN.

Let's see that in action. In this example, we'll pick the last port (fa 0/24) and assign it to VLAN 99, which doesn't exist. This will override the VLAN membership for port fa 0/24 from VLAN 4 to VLAN 99 (remember, in the previous steps we assigned port fa 0/24 to VLAN 4). The next few steps will reassign it to this new VLAN 99.

Again, remember that VLAN 99 doesn't exist. Here we go:

```
AccessSwitch(config-if-range)#exit
AccessSwitch(config)#interface fa 0/24
AccessSwitch(config-if)#switchport access vlan 99
% Access VLAN does not exist. Creating vlan 99
AccessSwitch(config-if)#end
AccessSwitch#
```

As you see in the commands above, the system throws an information message at you letting you know that the Access VLAN you are trying to assign to this port doesn't exist, and it will create it for you. Some ask why create a VLAN and then assign ports to it when the system is going to do that for you anyway? It is your choice.

At this point, we have VLANs created on our switch, an IP address on it for management, and passwords for telnet. This gets you ready to have some good ammunition for the ICND1, ICND2, CCNA Boot Camp or the BCMSN class. Keep in mind that these topics are going to be covered in much more interesting details in various other courses. I hope to see you in one of these classes at Global Knowledge.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge course:

Understanding Networking Fundamentals
ICND1 - Interconnecting Cisco Network Devices 1
ICND2 - Interconnecting Cisco Network Devices 2
CCNA® Boot Camp
BCMSN - Building Cisco Multilayer Switched Networks v3.0

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Dheeraj (Raj) Tolani has been working with Global Knowledge as a contract instructor teaching various networking courses including CCNA, CCNP, CCIP, CCVP tracks. He has been in the industry for over 17 years working with various technologies, including Cisco, Banyan Vines, Microsoft, and Novell. Dheeraj has worked as a consultant for various medical, financial, legal, government, and publishing companies. He runs a consulting company based out of New York City, which provides IP integration solutions. You can visit his Web site at www.rajtolani.com.