Chapter 2
Switch Management

The 1900 switch is a low-end model in the Cisco Catalyst switch family. You can buy two different models in the Catalyst 1900 switch family: the 1912 and the 1924. The 1912 switches have 12 10BaseT ports and the 1924 switches have 24 10BaseT ports. Each has two 100Mbps uplinks—either twisted-pair or fiber. Since the 1900 switch can now run a version of the Cisco IOS, you can use it to thoroughly understand switching through all Cisco switching products. Not all Cisco switches run a version of the IOS, but they will eventually.

In this chapter, you will learn how to start up and configure a Cisco Cat-alyst 1900 switch using the Command-Line Interface (CLI). I will begin by explaining how to connect a console cable, and then I will discuss what hap-pens when a 1900 switch is powered up. After you learn how to connect a console cable to the switch and get the switch working, I will teach you the basic configuration commands that you can use on the 1900 switch. After you learn the basic commands, I will show you how to configure Virtual LANs(VLANs) on the switch as well as ISL routing and Virtual Trunk Protocol (VTP).

The basic commands covered in this chapter include the following:

- Setting the passwords
- Setting the hostname
- Configuring the IP address and subnet mask
- Identifying the interfaces
- Setting a description on the interface
- Defining the port duplex of a port
- Verifying the configuration
- Managing the MAC address table
- Setting permanent and static MAC addresses
- Configuring port security
- Describing the show version command
- Changing the LAN switch type
- Configuring VLANs
- Adding VLAN memberships to switch ports
- Creating a VTP domain
- Configuring trunking
- Configuring pruning

Features of the 1900 Switch

The Catalyst 1900 switch can now use a CLI to configure the Cisco Internetworking Operating System (IOS) on the switch. Before the CLI was available, the 1900 switch could only be configured through a menu system. The CLI makes configuring the switch really close to how you would con-figure a router. The Cisco Catalyst 5000 series, which is one of Cisco’s higher-end models, is still *set-based*, which means you use the set command to configure the router. This book only covers the Catalyst 1900 switch con-figuration commands.

There are two types of operating systems that run on Cisco switches:

IOS-based In this system, you can configure the switch from a CLI that is similar to Cisco routers. Catalyst 1900, 2820, and 2900 switches can be used with an IOS-based CLI, although they can be set with a menu system as well.

Set-based This system uses older, set-based CLI configuration commands. The Cisco switches that use the set-based CLI are the 2926, 1948G, 4000, 5000, and 6000 series.

It's time to be introduced to the 1900 series of Catalyst switches. Why the 1900? Because that is what Cisco uses on the CCNA exam, of course, and also because it allows you to run a CLI with IOS-based commands on a less expensive switch than the 5000 series. The 1900 switches are great for home offices or other small offices where you can get 10Mbps switched ports with 100Mbps uplinks at a decent price.

The Three Configuration Options

The Catalyst switch uses a CLI, which is more like the router configuration. However, you can configure the switch with a Web-based method using the Visual Switch Manager (VSM). To configure the switch through the VSM, you just have to type in the IP address of the switch at a Web browser. You will learn how to add an IP address to the switch later in this chapter. The 1900 switches also have the original menu system that allows you to configure the switch through a series of menu-based options. To configure the switch with Telnet or VSM, an IP address must be configured on the switch.

Connecting to the Console Port

The 1900 switch has a console port on the back of the switch, just like the 2500 routers. It is an RJ-45 port, and it uses a rolled cable to connect to a terminal. At this point, you need to start a terminal emulation program like Hyper-Term in Windows. The settings for this program are as follows:

Data Bits - 8
Parity - None
Stop Bits 1
Speed 9600Bps
Flow Control - None

1900 Switch Start-up

Before you power on the switch for the first time, check to make sure you have completed the following:

You have plugged in all the network cables securely.
You have connected a terminal to the console port.
You have configured your terminal software correctly.

Once you have checked everything in this list, plug the power cable into the switch and watch the light sequence. Then check the output on the con-sole. Figure 2.1 shows the 1900 switch and the Light Emitting Diode (LED) locations.

A green system light appears if the switch is operational. It will be amber if a system malfunction has occurred. The RPS is a redundant power supply light that is on if an RPS is detected in the switch. The only button on the 1900 switch is the mode button. By pressing the mode button, you can see three different status lights on the switch:

- **STAT** This light shows the status of the ports. If it is green, this indicates a device is plugged into the switch. Green is active, and a green blinking light is activity on the port. If the port is amber, there has been a link fault.
- **UTL** This light indicates the bandwidth of the switch. When you press the mode button on a 1912 switch, and the LEDs for ports 1 through 4 come on, this means the bandwidth utilization of the switch is somewhere between 0.1 and1.5Mbps. If lights 5 through 8 come on, this indicates that the utilization is between 1.5 and 20Mbps, and lights 9 through 12 indicate bandwidth between 20 and 120Mbps.
- **FDUP** This light will show you which ports are configured at full duplex.

When the 1900 switch is first powered on, it runs through a power-on self test (POST). At the start, all port LEDs are green. These LEDs turn off after the POST completes. If a port is determined failed by the POST, both the Sys-tem LED and the port LED turn amber. If no failures occur during the POST, all LEDs blink and turn off.

After the POST runs and you have a console cable connected to the switch, the following menu shows up. By pressing K, you can use the Command-Line Interface, and when you press M, you will be allowed to configure the switch through a menu system. Pressing I allows you to configure the IP configuration of the switch; however, this can also be accomplished through the menu or CLI at any time. Once the IP configuration is set, the selection no longer appears.

The switch output below is the output on the console screen after the switch is powered up.

```
        1 user(s) now active on Management Console.
        User Interface Menu
        [M] Menus
        [K] Command Line
        [I] IP Configuration
Enter Selection:k
CLI session with the switch is open. To end the CLI session, enter [Exit].
```

Connecting to an Ethernet Port

The Catalyst 1900 series of switches have fixed port types. They are not modular like the 5000 series switches. The 1900 switches use only 10BaseT ports for workstations and 100BaseT or FX for uplinks. Each switch has either 12 (model 1912) or 24 (model 1924) 10BaseT switch ports, each having one or two Fast Ethernet uplinks. The 100BaseX ports are referred to as ports A and B. To connect the ports to another switch as an uplink, you must use a crossover cable. It would be nice if they had a button for this function, but they don’t. When connecting devices like workstations, servers, printers, and routers to the switch, you must use a straight-through cable. Connecting between switches uses a crossover cable.

When a device is connected to a port, the port-status LED light comes on and stays on. If the light does not come on, the other end might be off, or there might be a cable problem. Also, if a light goes on and off, there is a possible auto-speed and duplex problem. I'll show you how to check that in the next section. If you do not have a device connected to the switch, the port light will come on when booted, and then it will turn off.

Cisco 1900 IOS Configuration Commands

In this section, I will show you how to configure the basics on the 1900 Catalyst switch. I will show you how to Set the passwords Set the hostname Configure the IP address and subnet mask Identify the interfaces, Set a description on the interfaces, Define the duplex of a port Verify the configuration, Manage the MAC address table, Set permanent and static MAC address, Configure port security, Use the show version command, Change the LAN switch type.

Setting the Passwords

The first thing that you should configure on a switch is the passwords. You don't want unauthorized users connecting to the switch. You can set both the user mode and privileged mode passwords, just like a router. However, it is mostly done with different commands than for a router. The login (user mode) password can be used to verify authorization of the switch, including accessing any line and the console. The enable password is used to allow access to the switch so the configuration can be viewed or changed. This is the same as any Cisco router. The passwords cannot be less than four characters or more than eight. They are not case sensitive. Even though the 1900 switch uses a CLI running an IOS, the commands for the user mode and enable mode passwords are different than for a router. You use the command enable password, which is the same, but you choose different access levels, which are optional on a Cisco router but not on the 1900 switch.

Setting the User Mode and Enable Mode Passwords

You use the same command to set the user mode password and enable mode password on the 1900 switch. However, you do use different level commands to control the type of access each password provides.

To configure the user mode and enable mode password, press K at the router console output. Enter enable mode by using the enable command. And then enter global configuration mode by using the config t command.

The following output shows an example of how to get into enable mode and then into global configuration mode.

```
1 user(s) now active on Management Console.
  User Interface Menu
          [M] Menus
          [K] Command Line
          [I] IP Configuration
  Enter Selection:k
CLI session with the switch is open.
To end the CLI session, enter [Exit].
>enable
#config t
Enter configuration commands, one per line. End with CNTL/Z
```

(config)#

Once you are in global configuration mode, you can set the user mode and enable mode passwords by using the enable password command. The following output shows the configuration of both the user mode and enable mode passwords.

```
(config)#enable password ?
level Set exec level password
(config)#enable password level ?
  <1-15>             Level number
```

To enter the user mode password, use level number 1.
To enter the enable mode password, use level mode 15.

Remember the password must be at least four characters, but not longer than eight characters. The switch output below shows the user mode password being set and denied because it is more than eight characters.

```
  (config)#enable password level 1 todd lammle
   Error: Invalid password length.
Password must be between 4 and 8 characters
```

The following output is an example of how to set both the user mode and enable mode passwords on the 1900 switch.

```
(config)#enable password level 1 todd
(config)#enable password level 15 todd1
(config)#exit
#exit

CLI session with the switch is now closed. Press any key to continue.
```

At this point, you can press Enter and test your passwords. You will be prompted for a user mode password after you press K and then an enable mode password after you type **enable**. After I exited configuration mode and then the privileged mode, the following console screen appeared. Notice that when I pressed K this time, the switch prompted me for a user mode password.

```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.1993-1998
All rights reserved.

  Enterprise Edition Software

  Ethernet Address:                         00-30-80-CC-7D00

  PCA Number:                               73-3122-04

  PCA Serial Number:                        FAB033725XG

  Model Number:                             WS-C1912-A
  System Serial Number:                                  FAB0339T01M
  Power Supply S/N:                                      PHI031801CF
  PCB Serial Number:                          FAB033725XG, 73-3122-04
  -----------------------------------------------
1 user(s) now active on Management Console. User Interface Menu
        [M] Menus
        [K] Command Line Enter Selection: K Enter
        password: ****
CLI session with the switch is open. To end the CLI session, enter [Exit].
>en
Enter password:****
#
```

After I entered user mode, I typed **en**, which is a shortcut for the enable command, and was prompted for the enable password.

Setting the Enable Secret Password

The **enable secret** password is a more secure password and supersedes the enable password if set. You set this password the same way you set the enable secret password on a router. If you have an enable secret set, you don't even need to bother setting the enable mode password.

```
(config)#enable secret todd2
```

You can make the **enable password** and **enable secret** commands the same on the 1900 switch, but on a router you are not allowed to do this. You can use the command show running-config (show run for short) to see the current configuration on the switch.

```
#sh run
Building configuration...
Current configuration:
Enable secret 5 $1$FMFQ$wFVYVLYn2aXscfB3J95.w.
enable password level 1 "TODD"
Enable password level 15 "TODD1"
```

Notice the enable mode passwords are not encrypted by default, but the enable secret is. This is the same password configuration technique that you will find on a router. One more thing to notice is that even though I typed the passwords as lowercase, the running-config shows the passwords as uppercase. It doesn't matter how you type them or how they appear in the configuration because the passwords are not case sensitive.

Setting the Hostname

The hostname on a switch, as well as on a router, is only locally significant. This means that it doesn't have any function on the network or name resolution whatsoever. However, it is helpful to set a hostname on a switch so that you can identify the switch when connecting to it. A good rule of thumb is to name the switch after the location it is serving. The 1900 switch command to set the hostname is exactly like any router: you use the hostname command.

Remember, it is one word. The switch out-put below shows the console screen. Press K to go into user mode, enter the password, use the enable command, and enter the enable secret password. From global configuration mode, type the command hostname **hostname**.

```
1 user(s) now active on Management Console.

User Interface Menu
        [M] Menus
        [K] Command Line
        [I] IP Configuration
        Enter Selection: K
        Enter password: ****
CLI session with the switch is open. To end the CLI session, enter [Exit].
>en
Enter password:***
#config t
Enter configuration commands, one per line.
CNTL/Z
(config)#hostname Todd1900EN
Todd1900EN(config)#
```

Notice that as soon as I pressed Enter, the hostname of the switch appeared. Remember that from global configuration mode, which you enter by using the config t command, the running-config is changed. Any changes you make in this mode take effect immediately.

Setting IP Information

You do not have to set any IP configuration on the switch to make it work. You can just plug in devices and they should start working, just like they would on a hub. There are two reasons why you would set the IP address informa-tion on the switch: so you can manage the switch via Telnet or other man-agement software, or if you wanted to configure the switch with different VLANs and other network functions. The Catalyst 1900 switch has some default settings already configured on the switch from the factory. The default settings on the switch are as follows:

IP address and default gateway: 0.0.0.0
CDP: Enabled
Switching Mode: Fragment Free
100BaseT ports: Auto-negotiate duplex mode
10BaseT ports: Half duplex
Spanning Tree: Enabled
Console password: Not set

By default, no IP address or default-gateway information is set. You would set both the IP address and the default gateway on a layer-2 switch, just like any host. By typing the command **show ip (or sh ip)**, you can see the default IP configuration of the switch.

```
Todd1900EN#sh ip
IP Address: 0.0.0.0
Subnet  Mask:  0.0.0.0  Default  Gateway:  0.0.0.0
Management VLAN: 1 Domain name:
Name  server  1:  0.0.0.0  Name  server  2:  0.0.0.0
```

```
HTTP server : Enabled HTTP port : 80
RIP : Enabled
```

Notice in the above switch output that no IP address, default gateway, or other IP parameters are configured. To set the IP configuration on a 1900 switch, use the command **ip address**

The default gateway should also be set using the **ip default-gateway** command.
The switch output below shows an example of how to set the IP address and default gateway on a 1900 switch.

```
Todd1900EN#config t
Enter configuration commands, one per line.
End with CNTL/Z
Todd1900EN(config)#ip address 172.16.10.16 255.255.255.0
Todd1900EN(config)#ip default-gateway 172.16.10.1
Todd1900EN(config)#
```

Once you have your IP information set, use the show ip command to verify your changes.

```
Todd1900EN#sh ip
IP   Address:   172.16.10.16   Subnet   Mask:   255.255.255.0
Default Gateway: 172.16.10.1 Management VLAN: 1
Domain name:
Name server 1: 0.0.0.0 Name server 2: 0.0.0.0
HTTP server: Enabled HTTP port : 80
RIP: Enabled
Todd1900EN#
```

To change the IP address and default gateway on the switch, you can either type in new addresses or remove the IP information with the no ip address and no ip default-gateway commands.

Configuring Switch Interfaces

It is important to understand how to access switch ports. The 1900 switch uses the type slot/port command. For example, Ethernet 0/3 is 10BaseT port 3. Another example would be Fast Ethernet 0/26. This is the first of the two Fast Ethernet ports available on the 1900 switch.
The 1900 switch type slot/port command can be used with either the interface command or the show command. The interface command Allows you to set interface-specific configurations. The 1900 switch has only one slot: zero (0)The help screens, for configuring interfaces, are only moderately helpful. The help screens will show you that the ports are 1–25 for Ethernet, and ports 26 and 27 are available for Fast Ethernet only. Since this is a 1912, it really only has ports 1–12. However, there is a port 25 on the back of the switch. This is an Attachment Unit Interface (AUI) adapter for connecting switches together, or even for connecting the 1900 switch to a coax Ethernet network.

Configuring the 10BaseT Interfaces

To configure an interface on a 1900 switch, go to global configuration mode and use the interface command. The following help screens describe the type slot/port configuration method. From global configuration, use the interface command and the type, either Ethernet or Fast Ethernet inter-face. I am going to demonstrate the Ethernet interface configuration first.

```
Todd1900EN#config t
Enter configuration commands, one per line.
End with CNTL/Z

Todd1900EN(config)#int ethernet ?
 <0-0> IEEE 802.3
```

The previous output asks for the slot. Since the 1900 switch is not modular, there is only one slot. The next output gives us a slash (/) to separate the slot/ port configuration.

```
Todd1900EN(config)#int ethernet 0?
/
Todd1900EN(config)#int ethernet 0/?
<1-25> IEEE 802.3
```

After the 0/ configuration command, the above output shows the amount of ports you can configure. However, if you only have a 1912 switch, you really only have ports 1–12, 25 on the back of the switch, and 26 and 27 as the 100Mbps uplinks. The FastEthernet ports did not show up on the above out-put because we chose the Ethernet interface as our type and the ports are FastEthernet.

The output below shows the completed command.

```
Todd1900EN(config)#int ethernet 0/1
Todd1900EN(config-if)#
```

Once you are in interface configuration, the prompt changes to (config-if). After you are at the interface prompt, you can use the help commands to see the available commands.

```
Todd1900EN(config-if)#?
```

Interface configuration commands:

cdp	Cdp interface subcommands
description	Interface specific description
duplex	Configure duplex operation
exit	Exit from interface configuration mode
help	Description of the interactive help system
no	Negate a command or set its default
port	Perform switch port configuration
shutdown	Shutdown the selected interface
span tree	Spanning tree sub system
Vlan-membership	Vlan-membership configuration

You can switch between interface configurations by using the **int e0/#** command at any time from global configuration mode.

Configuring Interface Descriptions

You can administratively set a name for each interface on the 1900 switch. Like the hostname, the descriptions are only locally significant. For the 1900 series switch, use the description command. **You cannot use spaces with the description command**, but you can use underscores if you need to.

Setting Descriptions

To set the descriptions, you need to be in interface configuration mode. From interface configuration mode, use the description command to describe each interface. You can make the descriptions more than one word, but you can't use spaces. You'll have to use the underscore as shown below:

```
Todd1900EN#config t
Enter configuration commands, one per line. End with CNTL/Z
Todd1900EN(config)#int e0/1
Todd1900EN(config-if)#description Finance_VLAN
Todd1900EN(config-if)#int f0/26
Todd1900EN(config-if)#description trunk_to_Building_4
Todd1900EN(config-if)#
```

Fast Ethernet Interface Configuration

To configure the two Fast Ethernet ports, the command is still type slot/ port, but the type is Fast Ethernet instead of Ethernet. An example would be interface FastEthernet 0\#.

The switch output below shows the configuration of a FastEthernet port on the 1900 switch. Notice that the command is interface FastEthernet, but the slot is still 0. The only ports available are 26 and 27.

```
Todd1900EN(config)#int FastEthernet ?
 <0-0> FastEthernet IEEE 802.3

Todd1900EN(config)#int FastEthernet 0/?
<26-27> FastEthernet IEEE 802.3

Todd1900EN(config)#int FastEthernet 0/26
Todd1900EN(config-if)#int fast 0/27
Todd1900EN(config-if)# [control+Z]
```

In the configuration example above, I set the description on both a 10Mbps port and a 100Mbps port.

Viewing Descriptions

Once you have configured the descriptions you want on each interface, you can then view the descriptions with either the **show interface** command or the **show running-config** command.

```
Todd1900EN#sh int e0/1
Ethernet 0/1 is Suspended-no-linkbeat
```

```
          Hardware    is Built-in 10Base-T
          Address is 0030.80CC.7D01
          MTU
          1500          bytes, BW      10000 Kbits
          802.1d STP State:            Forwarding           Forward Transitions:  1
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description: Finance_VLAN
Duplex setting: Half duplex
Back pressure: Disabled

Todd 1900EN#sh run
Building configuration...
Current configuration: hostname "Todd1900EN"!
ip    address    172.16.10.16    255.255.255.0    ip    default-gateway
172.16.10.1!
interface Ethernet 0/1
description "Finance_VLAN"!
[output cut]
```

Notice in the above switch output that the sh int e0/1 command and the show run command both show the description command set on an interface.

Configuring the Port Duplex

The 1900 switch has only 12 or 24 10BaseT ports and comes with one or two FastEthernet ports. You can only set the duplex on the 1900 switch, as the ports are all fixed speeds. Use the **duplex** command in interface configuration.

In the switch output below, notice the options available on the Fast-Ethernet ports.

```
Todd1900EN(config)#int f0/26
Todd1900EN(config-if)#duplex ?

  Auto                       Enable auto duplex configuration
  Full                       Force full duplex operation
  full-flow-control          Force    full    duplex    with flow control
  Half                       Force    half    duplex    operation


Todd1900EN(config-if)#duplex full
```

Table B.1 shows the different duplex options available on the 1900 switches. The 1900 FastEthernet ports default to *auto duplex*, which means they will try to auto detect the duplex the other end is running. This may or may not work. It is a good rule of thumb to set the duplex to half on a Fast-Ethernet port.

TABLE .1 Duplex Options

Parameter	**Definition**
Auto	Set the port into auto-negotiation mode. Default for all 100BaseTX ports.
Full	Forces the 10 or 100Mbps ports into full-duplex mode.
Full-flow-control	Works only with 100BaseTX ports, uses flow control so buffers won’t overflow.
Half	Default for 10BaseT ports, forces the ports to work only in half-duplex mode.

Once you have the duplex set, you can use the show interface command to view the duplex configuration.

```
Todd1900EN(config-if)#duplex full
Todd1900EN#sh int f0/26

Fast Ethernet 0/26 is Suspended-no-linkbeat

  Hardware      is Built-in 100Base-TX
  Address is 0030.80CC.7D1A
  MTU 1500      bytes, BW        100000 Kbits
  802.1d STP State:              Blocking             Forward Transitions:  0

Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description: trunk_to_Building_4
Duplex setting: Full duplex
Back pressure: Disabled
```

In the output above, the duplex setting shows full duplex.

Verifying IP Connectivity

It is important to test the switch IP configuration. You can use the Ping pro-gram, and you can telnet into the 1900 switch. However, you cannot telnet from the 1900 switch or use trace route.

In the following example, I pinged a host on the network from the 1900 CLI. Notice the output on a successful ping: exclamation point (!). If you receive periods (.) instead of exclamation points, that signifies a timeout.

```
Todd1900EN#ping 172.16.10.10
Sending 5, 100-byte ICMP Echos to 172.16.10.10, time out is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max 0/2/10/ ms
```

```
Todd1900EN#telnet 172.16.10.10
^
% Invalid input detected at '^' marker.
```

In the Telnet example above, notice the error when I tried to telnet from the 1900 switch. The command is not available on the 1900 switch. However, remember that you can telnet into a switch at any time, as long as IP is configured correctly.

Erasing the Switch Configuration

The switch configuration is stored in NVRAM, just as any router. You can-not view the startup-config, or contents of NVRAM. You can only view the running-config. When you make a change to the switches' running-config, the switches automatically copy the configuration on the switch to NVRAM. This is a big difference from a router where you have to type copy running-config startup-config. That option is not available on the 1900 switch.

You can delete the configuration in NVRAM on the 1900 switch if you want to start over on the switches' configuration. To delete the contents of NVRAM on a 1900 switch, use the **delete nvram** command.

Notice in the switch output below that there are two options: nvram and vtp. I want to delete the contents of NVRAM to the factory default settings.

```
Todd1900EN#delete    ?
  Nvram     NVRAM   configuration
  Vtp       Reset   VTP configuration to defaults
  Todd1900EN#delete    nvram
```

```
Command resets the switch with factory defaults. All system parameters will revert to their
default factory settings. All static and dynamic addresses will be removed.

Reset system with factory defaults, [Y]es or [N]o?Yes
```

Notice the message received from the switch when the command delete nvram is used. Once you say yes, the configuration is gone.

Managing the MAC Address Table

Do you remember how bridges and switches filter a network? They use MAC (hardware) addresses burned into a host's network interface card (NIC) to make forwarding decisions.

The switches create a MAC table that includes dynamic, permanent, and static addresses. This filter table is created by hosts sending a frame and by the switch learning the source MAC address and from which segment and port it was received.

The switch keeps adding new MAC addresses that are sent on the net-work into the MAC filter table. As hosts are added or removed, the switch dynamically updates the MAC filter table. If a device is removed, or if it is not connected to the switch for a period of time, the switch will age out the entry.

You can see the switch's filter table by using the command show mac-address-table. The following output shows the information received when using the **show mac-address-table** command.

```
Todd1900EN#sh mac-address-table
Number of permanent addresses : 0
Number of restricted static addresses : 0
Number of dynamic addresses : 4

   Address             Dest Interface        Type        Source
                                                         Interface List
    00A0.246E.0FA8     Ethernet 0/2          Dynamic     All
    0000.8147.4E11     Ethernet 0/5          Dynamic     All
    0000.8610.C16F     Ethernet 0/1          Dynamic     All
    00A0.2448.60A5     Ethernet 0/4          Dynamic     All
```

The addresses in the table above are from the four hosts connected to my 1900 switch. They are all dynamic entries, which means the switch looked at the source address of a frame as it entered the switch interface, and it placed that address in the filter table. Notice that I have hosts in interfaces 1, 2, 4, and 5.

The Catalyst 1900 switch can store up to 1024 MAC addresses in the fil-ter table. If the MAC filter table gets full, the switch will flood all new addresses until one of the existing entries gets aged out.

You can also clear the MAC filter table by using the **clear mac-address-table** command. You can clear dynamic, permanent, and restricted static addresses.The switch output below shows the different options available when using the clear mac-address-table command.

```
#clear mac-address-table ?
dynamic               Clear 802.1d          dynamic address
permanent             Clear       802.1d    permanent addresses
restricted            Clear       802.1d    restricted static address
<cr>
```

Setting Permanent and Static MAC Addresses

Administrators can specifically assign permanent addresses to a switch port. These addresses are never aged out. You can do this to provide security to a port, which means that unless you specifically configure a hardware address to a switch port, it won't work. Administrators can also create static entries in the switch; these entries actually create a path for a source hardware address. This can be really restrictive, and you need to be careful when set-ting static entries because you can basically shut your switch down if you do not plan the configuration carefully.

Setting Permanent MAC Address Entries

You can configure a permanent MAC address to a switch port by using the global configuration command **mac-address-table permanent** [mac-address] [interface].

In the example below, the options are as follows:

Aging-time This can be used to change the age a MAC address is allowed to stay in the filter table before being cleared.

Permanent This sets a permanent address to an interface. If the user changes the host NIC card, then the host will not work until you change the permanent entry address.

Restricted This is used with the **static** command to set a path for source hardware addresses. Very restrictive for where a host can send a frame.

To configure a permanent hardware address to an interface, use the command mac-address-table permanent from global configuration mode, as shown below:

```
Todd1900EN#config t
Enter configuration commands, one per line. End with CNTL/Z
 Todd1900EN(config)#mac-address-table ?


  Aging-time                 Aging time of dynamic addresses

  Permanent                  Configure a permanent address

  Restricted                 Configure a restricted static address
```

After you choose the mac-address-table permanent command, add the hardware address and the interface it is associated with. This will restrict the interface to only accept frames from this source hardware address.

```
 Todd1900EN(config)#mac-address-table permanent ?
  48 bit hardware address
  Todd1900EN(config)#mac-address-table permanent 00A0.2448.60A5 e0/4
```

Once you have configured the entry, you can verify this entry by using the show mac-address-table command.

```
Todd1900EN#sh mac-address-table
Number of permanent addresses : 1
Number of restricted static addresses : 0
Number of dynamic addresses : 3

  Address                          Dest Interface    Type        Source
  Interface List
  00A0.2448.60A5                   Ethernet 0/4      Permanent   All
  00A0.246E.0FA8                   Ethernet 0/2      Dynamic     All
  0000.8147.4E11                   Ethernet 0/5      Dynamic     All
  0000.8610.C16F                   Ethernet 0/1      Dynamic     All
  Todd1900EN#
```

In the switch output above, notice that interface 4 now has a permanent entry with hardware address 00A0.2448.60A5. No other device can connect into interface 4 without updating the permanent entry in the MAC filter table.

Setting Static MAC Address Entries

You can take this security thing one step further. You can now tell a source interface that it is only allowed to send frames out of a defined interface. You do this with the restricted static command. Seems that it could cause some real havoc at work; you may only want to use this command on your friends if it is a slow day at work. That'll liven things up a bit.

The command **mac-address-table restricted static** is looking for two options: The first one is the hardware address of the destination inter-face. The second option will be the source interface that is allowed to communicate with this destination interface.

After entering the command mac-address-table restricted static from global configuration mode, enter the hardware address of the destination device:

```
Todd1900EN(config)#mac-address-table restricted static ?
48 bit hardware address
Todd1900EN(config)#mac-address-table restricted static 00A0.246E.0FA8 ?
Ethernet                        IEEE 802.3
Fast Ethernet                   Fast Ethernet IEEE 802.3
```

Once you add the hardware address of the destination device, add the interface address this destination hardware address is associated with.

```
  Todd1900EN(config)#mac-address-table restricted static 00A0.246E.0FA8 e0/2 ?
 Ethernet                       IEEE 802.3
 Fast Ethernet                  Fast Ethernet IEEE 802.3
<cr>
```

Now that you have entered the destination information, enter the source interface that is allowed to communicate with the destination address.

```
Todd1900EN(config)#mac-address-table        restricted        static
00A0.246E.0FA8  e0/2  e0/5
```

Once you have finished your command string, you can see the three dif-ferent types of entries we now have in the MAC filter table by using the show mac-address-table command (use sh mac for a shortcut).

```
Todd1900EN#sh mac
Number of permanent addresses :            1
                                       addresses          :
                                       1[dynamic/permanen
Number   of restricted static          t/restricted
Number   of dynamic addresses          :   2

Address          Dest Interface                Type             Source Interface List

-----------------------------------------------------------

00A0.2448.60A5         Ethernet 0/4            Permanent             All
00A0.246E.0FA8         Ethernet 0/2            Static                Et0/5
```

```
0000.8147.4E11          Ethernet 05             Dynamic           All
0000.8610.C16F          Ethernet 0/1            Dynamic           All
Todd1900EN#
```

The command I just entered has restricted interface 0/5 to only send frames to interface 0/2 using the destination hardware address 00A0.246E.0FA8. Remember that you can clear the entries with the **clear mac-address-table** [dynamic/permanent/restricted] [int dest] [int source] command.

Configuring Port Security

Port security is a way of stopping users from plugging a hub into their jack in their office or cubicle and adding a bunch of hosts without your knowl-edge. By default, 132 hardware addresses can be allowed on a single switch interface. To change this, use the interface command **port secure max-mac-count**.The following switch output shows the command port secure max-mac-count being set on interface 0/2 to allow only one entry.

```
 Todd1900EN#config t
 Enter configuration commands, one per line.
 End with CNTL/Z
 Todd1900EN(config)#int e0/2
 Todd1900EN(config-if)#port secure ?
max-mac-count Maximum number of addresses allowed on the port
<cr>

Todd1900EN(config-if)#port secure max-mac-count ?
<1-132> Maximum mac address count for this secure port

Todd1900EN(config-if)#port secure max-mac-count 1
```

The secured port or ports you create can use either static or sticky-learned hardware addresses. If the hardware addresses on a secured port are not stat-ically assigned, the port sticky-learns the source address of incoming frames and automatically assigns them as permanent addresses. *Sticky-learns* is a term Cisco uses for a port dynamically finding a source hardware address and creating a permanent entry in the MAC filter table.
<cr>

Using show version command

You can use the show version command to view basic information about the switch. This includes how long the switch has been running, the IOS ver-sion, and the base MAC address of the switch. This MAC address is important because if you lose your password, there is no password recovery on the 1900 switch. You need to send Cisco this MAC address, and they'll send you a password that will allow you to get into your switch. The switch output below shows you the configuration of the system hard-ware, the software version, and the names and sources of the configuration and boot files.

```
Todd1900EN#sh ver
Cisco Catalyst 1900/2820 Enterprise Edition Software Version V9.00.00
Copyright (c) Cisco Systems, Inc.                                   1993-1999
Todd1900EN uptime is 0day(s) 03hour(s) 37minute(s) 15second(s)
```

```
cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory
Hardware board revision is 5
Upgrade Status: No upgrade currently in progress.
Config File Status: No configuration upload/download is in progress
15 Fixed Ethernet/IEEE 802.3 interface(s) Base Ethernet Address: 00-
B0-64-75-6A-C0
Todd1900EN#
```

Notice that the output shows 15 fixed Ethernet 802.3 interfaces, which will tell you this is a 1912 switch. The 1912 has 12 10BaseT ports, 1 AUI port, and 2 FastEthernet ports: 15 ports in all. The 1924 has 24 10BaseT, 1 AUI, and 2 FastEthernet ports: 27 ports in all.

Changing the LAN Switch Type

You can see the LAN switch version running on a 1900 switch by using the **show port system** command. You can change it from global configuration mode with the **switching-mode** command. You can only use **store-and-forward** or **Fragment Free**.

The command show port system will show you the default LAN switch type of Fragment Free. The command switching-mode from global configuration mode allows you to change the LAN switch type to store-and-forward.

```
1900EN#sh port system
Switching mode: Fragment Free
Use of store and forward for multicast: Disabled Network port: None
  Half duplex backpressure (10 Mbps ports): Disabled
  Enhanced Congestion Control (10 Mbps ports): Disabled
  Default port LED display mode: Port Status

  1900EN(config)#switching-mode ?
  fragment-free Fragment Free mode
  store-and-forward Store-and-Forward mode
```

If you change the LAN switch type, you change it for all ports on the switch.

Configuring VLANs

Configuring VLANs is the easy part of the job. It is trying to under-stand which users you want in each VLAN that is time consuming. Once you have decided the number of VLANs you want to create and the users that will be members of each VLAN, you can create your VLAN. You can create up to 64 VLANs on a 1900 switch. A separate spanning-tree instance can be configured per VLAN. To configure VLANs on the 1900 series switch, choose K from the initial user interface menu to get into IOS configuration. Even though you can create VLANs with the Menu system available with the 1900 switch, I will only show you how to configure VLANs with the 1900 switch CLI. This is because it is the Cisco IOS and also because the CCNA exam objectives only cover the CLI method of configuration on the 1900 switch.

The following switch output is the console display when connecting to a 1900 switch. Press K to enter the CLI mode, and enter global configuration mode using the enable command and then config t.

```
1 user(s) now active on Management Console.
```

```
User Interface Menu
[M] Menus
[K] Command Line
[I]     IPConfiguration
Enter Selection:K
CLI session with the switch is open.
To end the CLI session, enter [Exit].
```

To configure VLANs on an IOS-based switch, use the vlan [vlan#] name [vlan name] command. I am going to demonstrate how to configure VLANs on the switch by creating three VLANs for three different departments.

```
>en
#config t
Enter configuration commands, one per line.
End with CNTL/Z

(config)#hostname 1900EN
1900EN(config)#vlan 2 name sales
1900EN(config)#vlan 3 name marketing
1900EN(config)#vlan 4 name mis
1900EN(config)#exit
```

After you create the VLANs that you want, you can use the show vlan command to see the configured VLANs. However, notice that by default all ports on the switch are in VLAN 1. To change the VLAN associated with a port, you need to go to each interface and tell it what VLAN to be a part of..Once the VLANs are created, verify your configuration with the show vlan command (sh vlan for short).

```
1900EN#sh vlan

   VLAN Name        Status        Ports
   ------------------------------------
   1  Default       Enabled       1-12, AUI, A, B
   2  Sales         Enabled
   3  Marketing     Enabled
   4  Mis           Enabled




    1002    fddi-default               Suspended
    1003    token-ring-default         Suspended
    1004    fddinet-default            Suspended
    1005    trnet-default              Suspended

 ------------------------------------

 [output cut]
```

Now that we can see the three VLANs created, we can assign switch ports to a single VLAN.

Each port can only be part of one VLAN. Trunking, which I will cover in a minute, makes a port available to more than one VLAN at a time.

Assigning Switch Ports to VLANs

You can configure each port to be in a VLAN by using the **vlan-membership** command. You can only configure VLANs one port at a time. There is no command to assign more than one port to a VLAN at a time with the 1900 switch.

Remember that you can configure either static memberships or dynamic memberships on a port. This book and the CCNA exam objectives only cover the static VLAN memberships.

In the following example, I configure interface 2 to VLAN 2, interface 4 to VLAN 3, and interface 5 to VLAN 4.

```
1900EN#config t
Enter configuration commands, one per line.
End with CNTL/Z
 1900EN(config)#int e0/2
1900EN(config-if)#vlan-membership ?

  dynamic    Set    VLAN    membership    type    as    Dynamic
  Static     Set    VLAN    membership    type    as    Static


1900EN(configif)#vlan-membership static ?
<1-1005> ISL VLAN index
  1900EN(config-if)#vlan-membership static 2
   1900EN(config-if)#exit
   1900EN(config)#int e0/4
  1900EN (config-if)#vlan-membership static 3
  1900EN(config-if)#exit
  1900EN(config) #int e0/5
  1900EN(config-if)#vlan-membership static 4
```

```
  1900EN(config-if)#exit
  1900EN(config)#exit
```

Now, type **show vlan** again to see the ports assigned to each VLAN.

```
 1900EN#sh vlan

          VLAN Name            Status      Ports
          ------------------------------------
          1    Default         Enabled     1, 3, 6-12, AUI, A, B
          2    Sales           Enabled     2
          3    marketing       Enabled     4
```

```
4      Mis              Enabled    5
1002   fddi-default     Suspended
       token-ring-
1003   defau            Suspended
1004   fddinet-default  Suspended
1005   trnet-default    Suspended

------------------------------------

[ouput cut]
```

You could also just type **show vlan #** to gather information about only one VLAN at a time.

```
1900EN#sh vlan 2

VLAN Name    Status        Ports

--------------------------------

2    sales         Enabled     2

--------------------------------

VLAN Type        SAID MTU                    Parent    RingNo    BridgeNo    Stp
              Trans1 Trans2

------------------------------------------------------------

2 Ethernet 100002 1500    0        1        1          Unkn 0        0

1900EN#
```

Another command you can use to see the ports assigned to a VLAN is show vlan-membership. Notice that this command shows each port on the switch, which VLAN the port is a member of, and the membership type (static or dynamic).

```
1900A#sh vlan-membership
Port    VLAN    Membership
1       1       Static
2       2       Static
3       1       Static
4       4       Static
5       5       Static
6       1       Static
7       1       Static
8       1       Static
9       1       Static
10      1       Static
11      1       Static
12      1       Static
AUI     1       Static

A       1       Static
B       1       Static
```

Configuring Trunk Ports

The 1900 switch only runs the Dynamic Inter-Switch Link (DISL) encapsulation method. To configure trunking on a Fast Ethernet port, use the inter-face command **trunk** [parameter].The following switch output shows the trunk configuration on interface 26 to trunk on.

```
1900EN#config t
Enter configuration commands one per line.  End with CNTL/Z
1900EN (config)#int f0/26
1900EN (config-if)#trunk ?

Auto   Set DISL state to AUTO
Desirable   Set DISL state to DESIRABLE
no negotiate   Set DISL state to NONEGOTIATE
Off   Set DISL state to OFF
On   Set DISL state to ON

1900EN(config-if)#trunk on
```

The following list describes the different options available when setting a trunk interface.

- **Auto** The interface will become trunked only if the connected device is set to on or desirable.

- **Desirable** If a connected device is either on, desirable, or auto, it will negotiate to become a trunk port.

- **Nonegotiate** The interface becomes a permanent ISL trunk port and will not negotiate with any attached device.

- **Off** The interface is disabled from running trunking and tries to convert any attached.

- **On** The interface becomes a permanent ISL trunk port. It can negotiate with a connected device to convert the link to trunk mode.

Which VLANs are now on the trunked port? All of them by default. You cannot configure the trunked port to only allow certain VLANs by default. In the next section, I will show you how to clear VLANs from a trunked port.

Clearing VLANs from Trunk Links

As previously discussed, all VLANs are configured on a trunked link unless cleared by an administrator. Use the **clear trunk** command if you don't want a trunked link to carry VLAN information for two reasons: because you want to stop broadcasts on a certain VLAN from traversing the trunk link, or because you want to stop topology-change information from being sent across a link where a VLAN is not supported.

To delete VLANs from a trunk port on a 1900, use the interface command **no trunk-vlan**. In the following example, I clear VLAN 5 from being communicated across the trunked link.

```
1900EN(config-if)#no trunk-vlan ?
<1-1005> ISL VLAN index
1900EN(config-if)#no trunk-vlan 5
1900EN(config-if)#
```

Unfortunately, there is no command to clear more than one VLAN at a time on the 1900. You would not typically clear more than a few VLANs anyway because, functionally, it makes no difference if they are turned on. If you had security, broadcast, or routing update issues, then you would need to consider it.

Verifying Trunk Links

To verify your trunk ports, use the **show trunk** command. If you have more than one port trunking and want to see statistics on only one trunk port, you can use the **show trunk** [port_number] command.

For the 1900 switch, the FastEthernet port 0/26 is identified by trunk A, and port 0/27 is identified by trunk B. Below, I demonstrate how to view the trunk port on interface 26:

```
 1900EN#sh trunk ?
 A  Trunk A
 B  Trunk B
1900EN#sh trunk a
DISL state: Auto, Trunking: On, Encapsulation type: ISL
```

Notice in this output that DISL is auto, trunking is on, and ISL is the VLAN-encapsulation type on trunk links. To see which VLANs are allowed on a trunked link, use the **show trunk [A or B] allowed-vlans** command. The following example shows the VLANs allowed on the trunked interface 26.

```
1900EN#sh trunk ?
A       Trunk A
B       Trunk B
1900EN#sh trunk a ?
allowed-vlans           Display allowed vlans
joined-vlans            Display joined vlans
joining-vlans           Display joining vlans
                        Display pruning eligible
prune-eligible          vlans
<cr>
```

```
1900EN#sh trunk a allowed-vlans
1-4,    6-1004
1900EN#
```

We cleared VLAN 5 in the preceding section, and the output now states that VLAN 5 is not being included on the trunked link.

Configuring ISL Routing

To support ISL routing on one FastEthernet interface, the router's interface is divided into logical interfaces, one for each VLAN. These are called *sub-interfaces*. Since we have four VLANs, we need four subinterfaces. Each one of the VLANs is a separate subnet, so here is the addressing I want to use:

VLAN 1	default	172.16.10.0/24
VLAN 2	sales	172.16.20.0/24
VLAN 3	marketing	172.16.30.0/24
VLAN 4	mis	172.16.40.0/24

Each of the hosts in their VLAN must use the same subnet addressing. To configure the router-on-a-stick for inter-VLAN routing, you need to complete three steps:

- Enable ISL trunking on the switch port the router connects to
- Enable ISL encapsulation on the router's sub interface.
- Assign an IP address to the sub interface and other logically addressing if applicable (IPX, for example).

To create a sub interface from global configuration mode, choose the Fast Ethernet interface, a period, and then a number. You will now be in the (config-subif) prompt for the interface. To configure ISL routing on a sub interface, use the **encapsulation isl [vlan-number]** command. You can then assign an IP address, IPX address, AppleTalk address, etc., to the sub interface. This is a unique subnet and all the hosts on that VLAN should be in that same subnet. It is not required but is highly recommended. Here is how to configure the 2621 router to support ISL routing with our four VLANs. First, I'll configure a sub interface with the same number as the VLAN I want to route. This is locally significant only, which means it doesn't matter at all what the sub interface numbers are on the network. Notice that you need to set the encapsulation next, or you will receive an error when trying to set the sub interface's IP address. VLAN 1 is in the 172.16.10.0 network. I need to assign a sub interface a valid host address from within that subnet.

```
2621#config t
2621(config) int f0/0.1
2621(config-subif)# encapsulation isl 1
2621(config-subif)# ip address 172.16.10.1 255.255.255.0
2621(config-subif)# int f0/0.2
2621(config-subif)# encapsulation isl 2
```

```
2621(config-subif)# ip address 172.16.20.1 255.255.255.0
2621(config-subif)# int f0/0.3
2621(config-subif)# encapsulation isl 3
2621(config-subif)# ip address 172.16.30.1 255.255.255.0
2621(config-subif)# int f0/0.4
2621(config-subif)# encapsulation isl 4
2621(config-subif)# ip address 172.16.40.1 255.255.255.0
2621(config-subif)#exit
2621(config)#int f0/0
2621(config-if) no shutdown
```

After setting the encapsulation and IP address for VLAN 1, I did the same configurations for VLANs 2, 3, and 4. Notice, however, that each sub interface is in a separate subnet.

Configuring VTP

A Catalyst 1900 switch is configured by default to be a VTP server, as are all switches. To configure VTP, first configure the domain name you want to use, as discussed in the next section. Once you configure the VTP information on a switch, you need to verify the configuration.

Configuring the Domain

When you create the VTP domain, you have the option to set the domain name, password, operating mode, and pruning capabilities of the switch (we discuss pruning in a minute). Use the vtp global configuration mode command to set this information. In the following example, I set the switch to a vtp server, the vtp domain to Lammle, and the vtp password to todd.

```
Todd1900EN(config)#vtp ?
Client: VTP client
domain:  Set VTP domain name
password:  Set VTP password
pruning:  VTP pruning
server:  VTP server
transparent:  VTP transparent
trap: VTP trap
```

```
Todd1900EN(config)#vtp server
Todd1900EN(config)#vtp domain   lammle
Todd1900EN(config)#vtp password todd
```

After you configure the VTP information, you can verify it with the **show vtp** command.

```
Todd1900EN#sh vtp
VTP version: 1
Configuration revision:                0
Maximum VLANs supported locally: 1005
Number of existing VLANs:                5
VTP domain name                      :   lammle
```

```
    VTP password                          :   Todd
   VTP operating mode           :   Server
   VTP pruning mode             :   Disabled
   VTP traps generation         :   Enabled

Configuration last modified by: 0.0.0.0 at 00-00-0000 00:00:00
Todd1900EN#
```

The preceding switch output shows the VTP domain, the VTP password, and the switch's mode.

Adding to a VTP Domain

You need to be careful when adding a new switch into an existing domain. If a switch is inserted into the domain and has incorrect VLAN information, the result could be a VTP database propagated throughout the internetworking with false information. Cisco recommends that you delete the VTP database before adding a switch to a VTP domain.

In this appendix, I showed you how to delete the NVRAM on the 1900 switch. However, this does not delete the VTP configuration on the switch, because VTP information has its own NVRAM. To delete the VTP informa-tion configured on a 1900 switch, you must use the delete vtp command. The following switch output shows how to delete the VTP NVRAM database.

```
Todd1900EN#delete ?
 Nvram  NVRAM configuration
 vtp       Reset VTP configuration to defaults

Todd1900EN#delete vtp

      This command resets the switch with VTP parameters set to factory defaults. All other
      parameters will be unchanged.
      Reset  system with VTP parameters set to actory defaults,

      [Y]es  or [N]o?  Yes
```

Once you type in the command, you will be prompted to set the VTP infor-mation back to the factory default configuration.

```
                    VTP operating mode            :  Server
                    VTP pruning mode              :  Disabled
                    VTP traps generation          :  Enabled
```

VTP Pruning

The following example shows how to turn on pruning in a 1900 switch. There is not a lot to it. Remember that if you turn VTP pruning on in a VTP server, you turn it on for the whole domain as well.

```
Todd1900EN(config)#vtp ?
```

```
 Client              VTP          Client
 Domain              Set          VTP domain name
 password            Set          VTP password
pruning                 VTP          Pruning
server                  VTP          server
transparent  VTP                     Transparent
trap                      VTP        trap
Todd1900EN(config)#vtp pruning ?
disable                   Disable    VTP pruning
enable                    Enable VTP pruning
```

```
Todd1900EN(config)#vtp pruning enable
Todd1900EN(config)#
```

Notice that you turn VTP pruning on for the whole switch. This will not send VTP broadcasts down a trunked link if no VLANs configured on this switch are present down the link.

Restoring or Upgrading the Catalyst 1900 IOS

You can upgrade or restore the IOS on Cisco Catalyst 1900 switches, although there is no command to back up the IOS image from the Catalyst 1900 switch to a TFTP host.

The command to upgrade or restore the IOS to a 1900 switch is

copy tftp://tftp_host_address/IOS_filename opcode

where:

copy tftp tells the switch to copy an IOS from a TFTP host.

//tftp_host_address is the address of the TFTP host.

IOS_filename is the IOS file stored in your TFTP default directory (for example, cat1900EN_9_00.bin is my enterprise edition).

opcode is the command that tells the router to download the file to flash memory.

Here is an example of the command being used:

```
1900B#copy tftp://192.168.0.120/cat1900EN_9_00.bin opcode
TFTP operation succeeded
1900B#
```

Backing up and Restoring the Catalyst 1900 Configuration

The configuration file for a Cisco Catalyst 1900 switch is just called nvram on the 1900 switch. The command to copy the file to a TFTP host is

copy nvram tftp://tftp_host_address/config_name

Before you make a backup, it’s a good idea to ping the TFTP host from the console of the device to make sure you have good LAN connectivity:

```
1900B#ping192.168.0.120 Sending 5, 100-byte ICMP Echos to 192.168.0.120, time out is 2 seconds:!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max 0/2/10/ ms
```

After checking the connectivity, you can issue the **copy nvram tftp**: command to make a backup copy of the configuration, as in the following example.

```
1900B#copy nvram tftp://192.168.0.120/1900en
Configuration upload is successfully completed
```

And here’s an example of the output from the console of a TFTP host.

```
Wed June 01 14:16:10 2000: Receiving '1900en' file from 192.168.0.120 in ASCII mode
##
Wed Mar 01 14:16:11 2000: Successful.
```

Notice the TFTP host copied two UDP packets, which are represented by pound signs (#) in ASCII mode.

You can restore a configuration back to a Catalyst 1900 switch from a TFTP host by using the following command:

copy tftp://tftp_host_address/config_name nvram

You need to know the filename as well as the IP address of the TFTP host to run this command, as in this example:

```
1900B#copy tftp://192.168.0.120/1900en nvram
TFTP successfully downloaded configuration file
```

The command at the end of the string tells the TFTP host where to copy the file to—in this case, nvram.To delete the startup-config file, or what is just called nvram, on the 1900 switch, use the delete nvram command, as follows:

```
1900B#delete nvram
This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.
Reset system with factory defaults, [Y]es or [N]o?
```

The above command does not affect the switch too much unless you have VLANs set. The switch will work fine without a configuration. However, adding an IP address for management is recommended.

CDP with the 1900 Switch

CDP works with all Cisco devices, including the Catalyst 1900 switch. The output on the 1900 switch looks like this:

```
switch#sh cdp
Global CDP information: CDP version: 2
Sending CDP packets every 60 seconds
sending a hold time value of 180 seconds
#
```

Notice that both the router and the switch have a CDP timer of 60 seconds and a hold time of 180 seconds. This means that CDP information received from neighbour routers will be kept for 180 seconds. If the router or switch does not hear from the neighbour again before the hold time expires, the information will be discarded.

You can change the timers on both devices with the **cdp timer** and **cdp hold time** commands from global configuration mode:

```
switch#config t
Enter configuration commands, one per line.
End with CNTL/Z switch(config)#cdp ?

advertise-v2                                    CDP      sends      version-2
advertisements
Hold time Specify the hold time (in sec) to be sent in packets
Timer Specify the rate at which CDP packets are sent (in sec)
```

At this point, you can change the timer and hold time on the 1900 switch, as follows:

```
switch(config)#cdp timer 90
switch(config)#cdp hold time 240
```

Summary

This appendix introduced you to the Catalyst 1900 switch. You also learned how to do the following:
Set the passwords. Three passwords were discussed: two enable pass-words and the enable secret password.
Set the hostname and configure a name for the switch. Configure the IP address and subnet mask.
Identify the interfaces with either a show interface or configuration command.
Set a description on the interfaces by using the description command.
Define the port duplex of a port, with full or half duplex.
Verify the configuration with the show running config command.
Manage the MAC address table with the show mac address-table command.
Set permanent and static MAC addresses with the mac-address-table command.
Configure port security with the port secure command.

Key Terms

Be sure you’re familiar with the following terms before taking the exam.
Auto duplex
Dynamic entries
Port security set-based

Assignments

1 Marks Questions

1) IOS stands for ____
2) Using ___ port Switch can be connected to a terminal for configuring
3) Name the three modes of a Switch to read its status.
4) To connect through an Uplink port ___ cable needs to be used

5) CLI is a ________
6) User Mode Password is known as ______
7) Give the command to verify the Switch Running Configuration
8) Give the command to verify the ip on CISCO Switch
9) Give the command to see the specifications of a given Switch interface.
10) What is the default duplex setting for 10BaseT interface?
11) What is the default duplex setting for 100BaseT interface?
12) Sitich Configurations are stored in ______
13) Give the command to reset a switch configuration
14) How will you get the mac address table in Switch?
15) What is the term “Sticky Learns” in switches?
16) What are the operatin modes for a switch?
17) Give the command to know different vlans and its memberships on a Switch
18) How to remove a given vlan from tunked port?
19) Trunked link carry all vlans by default. True/False?
20) VTP stands for ____
21) CDP stands for ____

7 Marks Questions

1) What are the three options available for configuring a CISCO Switch?
2) Give the different STATUS indications for a switch port.
3) What is the significance of UTL and FDUP status in CISCO switches?
4) Give the different CLI modes and its significance with CISCO Switches
5) What are the different levels of passwords & its significances in a CISCO Switches?
6) Give the procedure to assign passwords to a CISCO Switch
7) Give the procedure to assign ip address & default gateway on a CISCO Switch
8) Give the procedure to assign hostname & discription for an interface on a CISCO Switch
9) What are the different Duplex settings for a switch interface? Explain
10) Explain the procedure to configure the duplex value for different possible values in Switch.
11) What is the significance of Permanent mac address in mac address table? How to set this add?
12) What is the significance of Static mac address in mac address table? How to set this add?
13) What is the significance of port secure cammand? Explain
14) Give the procedure to create 4 vlans and assign port membership to each on a Switch
15) Demonstrate an ISL routing on a single router interface to implement inter VLAN routing
16) Demonstrate backing up and restoring the Switch Configuration files with example.
17) What is CDP? Illustrate how to configure CDP on the CISCO Switches.
18) Demonstrate how do you upgrade the Switch IOS with proper steps.

10 Mark Questions

1) What is ISL Routing? What is its advantage? Demonstrate an ISL routing on a switched network
having 4 VLANs defined.
2) What is MAC address table? What are the different types of entries in this table? Give its significance.
3) Give the different methods of security implementation on Switched Networks.