**Module 7.Managing a Cisco Internetwork**

Beginner Question

1. Explain Privileged Mode

Privileged mode allows users to view the system configuration, restart the system, and enter router configuration mode. Privileged mode also allows all the commands that are available in user mode. Privileged mode can be identified by the # prompt following the router name. From the user mode, a user can change to Privileged mode, by running the "enable" command. Also we can keep a enable password or enable secret to restrict access to Privileged mode. An enable secret password uses stronger encryption when it is stored in the configuration file and it is safer.

The Privileged mode can be identified as shown below

**Router#**

This is the second mode of the IOS. This mode can be accessed only from the *user exec* mode by executing the **enable** command. Since the **enable** command is used to access this mode, this mode is also known as the **enable mode**.

To close this mode or to return into the *user exec* mode, use the **exit** command or the **end** command.

As the name suggests, this mode includes privileged or powerful commands. This mode is usually used for the following purposes: -

* To view, save and erase device configuration
* To take the backup of the current device configuration
* To restore the configuration from backup
* To install a new IOS image file
* To debug or troubleshoot the device
* To restart or reload the device

Although this mode allows the user to manage device configuration and IOS image files, it does not allow the user to change the device configuration.

2. Find Boot SystemCommands

BCDBoot is a command-line tool used to configure the boot files on a PC or device to run the Windows operating system. You can use the tool in the following scenarios:

* **Add boot files to a PC after applying a new Windows image.** In a typical image-based Windows deployment, use BCDBoot to set up the firmware and system partition to boot to your image. To learn more, see [Capture and Apply Windows, System, and Recovery Partitions](https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/capture-and-apply-windows-system-and-recovery-partitions).
* **Set up the PC to boot to a virtual hard disk (VHD) file that includes a Windows image.** To learn more, see [Boot to VHD (Native Boot): Add a Virtual Hard Disk to the Boot Menu](https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/boot-to-vhd--native-boot--add-a-virtual-hard-disk-to-the-boot-menu).
* **Repair the system partition.** If the system partition has been corrupted, you can use BCDBoot to recreate the system partition files by using new copies of these files from the Windows partition.
* **Set up or repair the boot menu on a dual-boot PC.** If you've installed more than one copy of Windows on a PC, you can use BCDBoot to add or repair the boot menu.

Router1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#boot system flash:c3620-jk9o3s-mz.122-7a.bin

Router1(config)#boot system flash:c3620-jos56i-l.120-11.bin

Router1(config)#boot system slot0:c3620-ik9s-mz.122-13.bin

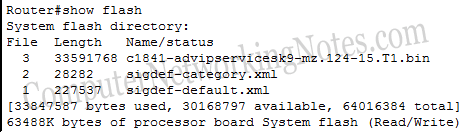
Router1(config)#boot system rom

Router1(config)#end

3.”sh flash” use and explain

Router#show flash

This command will display the content of flash memory, used space and available space. By default router stores IOS image file in flash. We can use this command to check the available space in Flash memory while updating / restoring IOS files.



4. Find traceroute Command

Traceroute is a command-line tool included with Windows and other operating systems. Along with the ping command, it’s an important tool for [understanding Internet connection problems](https://www.howtogeek.com/126265/how-to-troubleshoot-internet-connection-problems/), including packet loss and high latency.

If you’re having trouble connecting to a website, traceroute can tell you where the problem is. It can also help visualize the path traffic takes between your computer and a web server.

## How Traceroute Works

## When you connect to a website – say, howtogeek.com – the traffic has to go through several intermediaries before reaching the website. The traffic goes through your local router, your Internet service provider’s routers, onto larger networks, and so on.

## Traceroute shows us the path traffic takes to reach the website. It also displays the delays that occur at each stop. If you’re having issues reaching a website and that website is working properly, it’s possible there’s a problem somewhere on the path between your computer and the website’s servers. Traceroute would show you where that problem is.

## We’ve used traceroute to explain – and demonstrate — [who provides the Internet service for your Internet service provider](https://www.howtogeek.com/123599/who-provides-internet-service-for-my-internet-service-provider/).

In more technical terms, traceroute sends a sequence of packets using the ICMP protocol (the same protocol used for the ping command.) The first packet has a time-to-live (also known as TTL, or hop limit) of 1, the second packet has a TTL of 2, and so on. Each time a packet is passed to a new router, the TTL is decreased by 1. When it reaches 0, the packet is discarded and the router returns an error message. By sending packets in this manner, traceroute ensures that each router in the path will discard a packet and send a response.

Tracert Command Syntax:

**tracert [-d] [-h MaxHops] [-w TimeOut] [-4] [-6] target [/?]**

Intermediate Question

1. Find command of Current Configuration and Stored Configuration

Following basic commands are used for configuration :

1. Changing the hostname of a switch to GfgSwitch :

It is used to set the name of the device.

switch(config)#hostname GfgSwitch

GfgSwitch(config)#

2. To add a banner message :

It provides a short message to the user who wants to access the switch.

GfgSwitch(config)#banner motd &

Enter Text message. End with character '&'

$ This is GeeksforGeeks floor Switch #

3. To set IP address in Switch :

IP address is the address of device in network.

GfgSwitch(config)#interface vlan1

GfgSwitch(config-if)#ip address 172.16.10.1 255.255.255.0

GfgSwitch(config-if)#exit

GfgSwitch(config)#ip default-gateway 172.16.10.0

4. To set the current clock time :

This is set the current time stored in the switch.

GfgSwitch#clock set 3:03:14 June 25 2020

5. Apply password protection (enable password, secret password, console password and vty password) :

Enable password :

The enable password is used for securing privilege mode.

GfgSwitch(config)#enable password GFGGFG

Enable secret password :

This is also used for securing privilege mode but the difference is that it will be displayed as ciphertext(\*\*\*) on the configuration file.

GfgSwitch(config)#enable secret GFGGFG

Line console password :

When a person will take access through console port then this password will be asked.

GfgSwitch(config)#line console 0

GfgSwitch(config-line)#password GFG

GfgSwitch(config-line)#login

Line VTY password :

When a person want to access a router through VTY lines (telnet or ssh) then this password will be asked.

GfgSwitch(config)#line VTY 0 2

GfgSwitch(config-line)#password GFGGFG

GfgSwitch(config-line)#exit

6. Copy to startup-configuration file from running-configuration file :

GfgSwitch#copy running-config startup-config

7. To watch startup-configuration file and running-configuration file :

GfgSwitch#show startup-config

GfgSwitch#show running-config

8. Clear mac address table :

Switch stores MAC addresses in MAC address table

GfgSwitch#clear mac address-table

**Stored Configuration:**

Router#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

2. Find command of NVRAM,TFTP Server

**NVRAM**:

The nvram command has other uses as well for advanced users, from settings like [disabling the startup boot chime sound on a Mac](https://osxdaily.com/2012/11/04/disable-mac-boot-chime/) to [always booting into verbose mode in Mac OS X](https://osxdaily.com/2007/03/25/always-boot-mac-os-x-in-verbose-mode/) or even [enabling safe boot mode from the terminal](https://osxdaily.com/2014/09/04/enable-safe-mode-boot-command-line-mac/) for remote management or a headless/keyboardless Mac. For those interested in learning more about this powerful command, the man page for nvram is quite helpful, as is the basic –help flag to show other syntax options:

% nvram --help

nvram: (usage: no such option as --)

nvram [-x] [-p] [-f filename] [-d name] [-c] name[=value] ...

-x use XML format for printing or reading variables

(must appear before -p or -f)

-p print all firmware variables

-f set firmware variables from a text file

-d delete the named variable

-c delete all variables

name=value set named variable

name print variable

Note that arguments and options are executed in order.

**TFTP Server:**

To start the TFTP server from the command line, type the tftpd command.

tftpd [-l] [-p port] [-t timeout] [-r maxretries] [-c concurrency\_limit]

[-s maxsegsize] [-f file] [-a archive directory [-a ...]]

[-b IP address] [directory ...]

The following parameters are used for the tftpd command:

**-l**

Logs all incoming read and write requests and associated information to the system log. Logged information includes the IP address of the requestor, the file requested, and whether the request was successful.

**-p port**

Uses the specified port. The TFTP server usually receives requests on well-known port 69. You can specify the port in which requests are to be received.

**-t timeout**

Sets the packet timeout. The TFTP server usually waits 5 seconds before assuming a transmitted packet has been lost. You can specify a different timeout period in seconds.

**-r maxretries**

Sets the retry limit. The TFTP server usually limits the number of retransmissions it performs due to lost packet to 5. You can specify a different retry limit.

**-c concurrency\_limit**

Sets the concurrency limit. The TFTP server creates both threads and processes to handle incoming requests. You can specify the limit for the number of threads that may be concurrently processing requests under a single process. When the limit is exceeded, a new process is created to handle requests. The default is 200 threads.

**-s maxsegsize**

Sets the maximum block size that can be negotiated by the TFTP block size option. The default is 8192.

**-f file**

Specifies a cache file. You can specify a file containing information on files to be preloaded and cached for transmission. A cache file consists of one or more entries. For clarity, place each entry on a separate line. An entry has the form:

a | b <pathname>

where:

* a indicates that the specified file is cached in ASCII form. The file is preconverted to netascii format.
* b indicates that the specified file is cached in binary form, with no conversion.

The following examples show cache file entries:

a  /usr/local/textfile  
b  local/binaryfile

If a relative pathname to the file is specified, the TFTP server searches the specified directories for the file.

The cached version of a file is used only for requests requiring the specified format. For example, the binary cached version of a file is not used in satisfying a request for the file in netascii format. If a file is to be retrieved in both binary and ASCII formats, the user must specify that two copies of the file be cached with one in binary format, and the other in netascii format.

Caching is not dynamic. The cache files are read in when the TFTP server is started and are not updated, even if the file on disk is updated. To update or refresh the cache, the TFTP server must be recycled.

**-a archive directory**

Specifies an archive directory. The files in this directory and its subdirectories are treated as binary files for downloading. This option is useful on EBCDIC machines that act as file servers for ASCII clients. Multiple **-a** options can be specified; one directory per **-a** option. Directories must be specified as absolute path names. You can specify no more than 20 directories.

**-b IP address**

Uses the specified IP address. The TFTP server usually binds to INADDR\_ANY or the IPv6 unspecified address, in6addr\_any. You can specify the IP address on which requests are to be received. TFTP requests that come in on other IP addresses will not be accepted by this instance of TFTPD.

**directory**

Specifies an absolute path name for a directory. You may specify no more than 20 directories on the tftpd command line.

If the TFTP server is started without a list of directories, all mounted directories are considered active.

If a list of directories is specified, only those directories specified are active. That list is used as a search path for incoming requests specifying a relative path name for a file.

3. Explain LLDP protocol

The smooth-running operation of the various networking devices in a [LAN](http://www.orbit-computer-solutions.com/local-area-network-lan/) or switched network means that all [protocols](https://www.orbit-computer-solutions.com/home/routing-protocols/) and applications are enabled and that all devices and are configured correctly.  
However, the larger the network gets, the more difficult it will be for the network administrator to control, manage, and sort out configuration problems.

This is where the IEEE 802.1AB Link Layer Discovery Protocol (LLDP) steps in.

The [Link Layer Discovery Protocol](https://www.orbit-computer-solutions.com/link-layer-discovery-protocol-lldp/) (LLDP) is a protocol that can be used to support non-Cisco devices on your network.

LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network and learn about each other.

LLDP like CDP runs over the data-link layer of your network that includes non-Cisco devices or different network-layer protocols.

### How does LLDP work?

LLDP enabled network devices regularly exchange LLDP advertisements with their network neighbors and store this information in their internal database (MIB).  
A Network Management Software – NMS can use [SNMP](http://www.orbit-computer-solutions.com/understanding-simple-network-management-protocol-snmp/)to access this information to build an inventory of the network devices connected to the network and other applications.

## ow to configure LLDP

**Disabling and Enabling LLDP on an Interface**  
LLDP is disabled globally on all supported interfaces. You must enable LLDP globally to allow a device to send LLDP packets. However, no changes are required at the interface level.

You can configure an individual interface to selectively not to send and receive LLDP packets with the **no lldp transmit** and **no lldp receive** commands.

This example shows**how to globally enable LLDP.**

Switch# configure terminal  
Switch(config)# lldp run  
Switch(config)# end

This example shows how to globally **disable LLDP**.

Switch# configure terminal  
Switch(config)# no lldp run  
Switch(config)# end

Advance question

1. How to Erasing the Configuration in CLI

router> enable

router# write erase

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] <Press Enter key>

router# reload

Proceed with reload? [confirm] <Press Enter key>

-OR-

Would you like to enter the initial configuration dialog? [yes|no] no <Press Enter key>

–OR–

Do you want to save the configuration of the AP? [yes|no] no <Press Enter key>

2. How to find Gathering Neighbor Information, Gathering Port and Interface Information

An interface data structure stores information from a network to which it is connected. Using this information, an Open Shortest Path First (OSPF) router builds hello packets. These hello packets are exchanged between directly-connected neighbors to learn more about each other. You can use the **show ip ospf neighbor** command to observe the neighbor data structure. This command displays OSPF-related neighbor information.

**Port**: A port is an address on a single machine that can be tied to a specific piece of software. It is not a physical interface or location, but it allows your server to be able to communicate using more than one application.

## Interfaces:

Interfaces are networking communication points for your computer. Each interface is associated with a physical or virtual networking device.

Typically, your server will have one configurable network interface for each Ethernet or wireless internet card you have.

In addition, it will define a virtual network interface called the “loopback” or localhost interface. This is used as an interface to connect applications and processes on a single computer to other applications and processes. You can see this referenced as the “lo” interface in many tools.

Many times, administrators configure one interface to service traffic to the internet and another interface for a LAN or private network.

In DigitalOcean, in datacenters with private networking enabled, your VPS will have two networking interfaces (in addition to the local interface). The “eth0” interface will be configured to handle traffic from the internet, while the “eth1” interface will operate to communicate with the private network.