CCNA Command Guide

Routing and Switching Command Guide With Examples

ADAM VARDY

CCNA Command Guide

Routing and Switching Command Guide with Examples

Introduction

The CCNA Certification is a good foundation for other networking certifications should you may want to pursue in the future. Cisco Routers and Switches take up a huge chunk of the exam. The CCNA will test how much you know of Cisco hardware and software.

CCNA Command Guide: *Routing and Switching Command Guide with Examples* is designed to help you pass the CCNA Certification exam. The book is filled with the following:

- ***Illustrations***: The book is filled with diagrams and pictures that will help you understand the concepts and functions of Cisco Routers and Switches.
- ***Command Guides***: Each chapter includes several command guides that will help you improve your Routing and Switching Management skills.
- ***Outlined Concepts***: This book contains a good outline of topics, technical terms and information. This should help you understand and remember terms that are sure to come out in the certification exam.

While the main goal of this book is to help you pass the CCNA examination, most of the information found in this book has practical applications that you will find useful when performing your job as an IT professional.

This book is divided into two parts:

- ***Part One: Routing with Cisco Routers***
- ***Part Two: Switching with Cisco Switches***

At this point, you should understand that the concept of Routing and Switching is very similar except from the network layer they operate on. Most of the commands are the same but the command protocols are different. Much of this will be discussed in detail in the latter portions of each part.

Unlike other books that you can download from the internet, this book is very easy to use because of the special formatting it uses. Important concepts are in **boldface**, *italics* or ***both***. Since this is book is a command guide, the sample command lines that you can use to configure Cisco Routers and Switches are highlighted by using a `special font`.

Table of Contents

Introduction

Table of Contents

Part 1. Routing with CISCO Routers

Chapter 1. Layer 3 Routers

- Layer 3 (Network Layer)
- Functions of Layer 3 Router
- Types of Protocol
- Router Functions

Chapter 2. Router Management

- Cisco Routers
- Using the Cisco Routers
  - Local Connection
  - Configuring a CISCO Router
  - Cisco IOS Setup Mode Commands
  - Password Configuration
  - VTY Password
  - Setting-Up a Router Banners
  - Auxiliary Password
  - Privileged Password
  - Password Encryption
  - Recovering A Lost Password

Chapter 3. Network Routing

- Types of Network Routes
- Routing Protocols
- Routed Protocols
- Routing Methods

Chapter 4. Enhanced Interior Gateway Routing Protocol (EIGRP)

- Characteristics of EIGRP
- Components of EIGRP

Routing Tables
EIGRP Packet Types
Convergence
Diffusing Update Algorithm (DUAL)
Classful vs. Classless Routing
Configuring EIGRP
Managing EIGRP Operation
Other EIGRP-related Terms
Chapter 5. Open Shortest Path First (OSPF) Protocol
Characteristics of OSPF
Convergence
Cost Metric
OSPF Hierarchy
Selecting a Designated Router (DR)
Router ID (RID)
Configuring the OSPF
OSPF Protocol Configuration
Pertinent Commands
Part 2. Switching with CISCO Switches
Chapter 6. Layer 2 Switches
Hubs
Bridges
Switches
Hubs vs. Bridges vs. Switches
Switch Functions
Glossary of Terms (Switching)
Chapter 7. Switch Management
Handling Methods for Cisco Switches
Console Port
Auxiliary Ports
Chapter 8. Network Traffic Management
Switching Modes
Chapter 9. Spanning Tree Protocol (STP)

Problems caused by Transmission Loops:
Spanning Tree Protocol
Assigning STP Port Types
Root Ports
Designated Ports
Choosing Designated Ports based on STP Path Cost
Choosing Designated Ports based on Bridge ID
STP Convergence
Bridge Protocol Data Units (BPDUs)
STP Port States
Exclusive Cisco STP Options
Chapter 10. Virtual Local Area Network (VLAN)
Benefits of VLANs
Creating VLANs
Kinds of VLAN
VLAN Trunking
EtherChannel
Configuring EtherChannel
Types of Switch Ports
Chapter 11. Voice over IP (VoIP)
Quality of Service (QOS)
Cisco IP Phone
Cisco Discovery Protocol (CDP)
Enabling QoS in the Upstream Switch
Chapter 12. Troubleshooting Switches
Gathering Information
Troubleshooting Switch Connectivity
Conclusion

Part 1

Routing with CISCO Routers

Chapter 1. Layer 3 Routers

The network layer in both TCP/IP and Open Systems Interconnection network models is called *Layer 3*. Network layer protocols and devices are in charge of transferring data that are stored in packets from one host to another. This method of data transfer is called *routing*. These hosts can be adjacent to each other but they can also be several miles apart.

The difference between *Layer 2* (discussed in Part 3, Chapter 14) and Layer 3 is that the former routes data packets between devices that belong to the same LAN while the latter routes data frames between devices that belong to different LAN. This is where Layer 2 got is name, data link layer.

Layer 3 (Network Layer)

Logical addresses or more popularly known as IP addresses are assigned by Network Layer to all the devices connected to the network. These addresses are used to identify hosts (source and destination) and the specific network where data packets are being routed. Take note that IP addresses or logical addresses are assigned to network protocols and not to physical devices (modem, network card). For physical devices, physical addresses are assigned.

The functions of network layer include:

1. Acceptance of data pieces transported from transitions layer within the transfer host.
2. Assembling of data pieces into data packets. In each data packet, the network layer writes IP addresses of source and destination hosts for tracking.
3. Directing the data packets to the specific data link layer. The data link layer (Layer 2) will then send the data packets through the LAN connection.

Once the data packets have been sent to Layer 2, it will then perform the following functions:

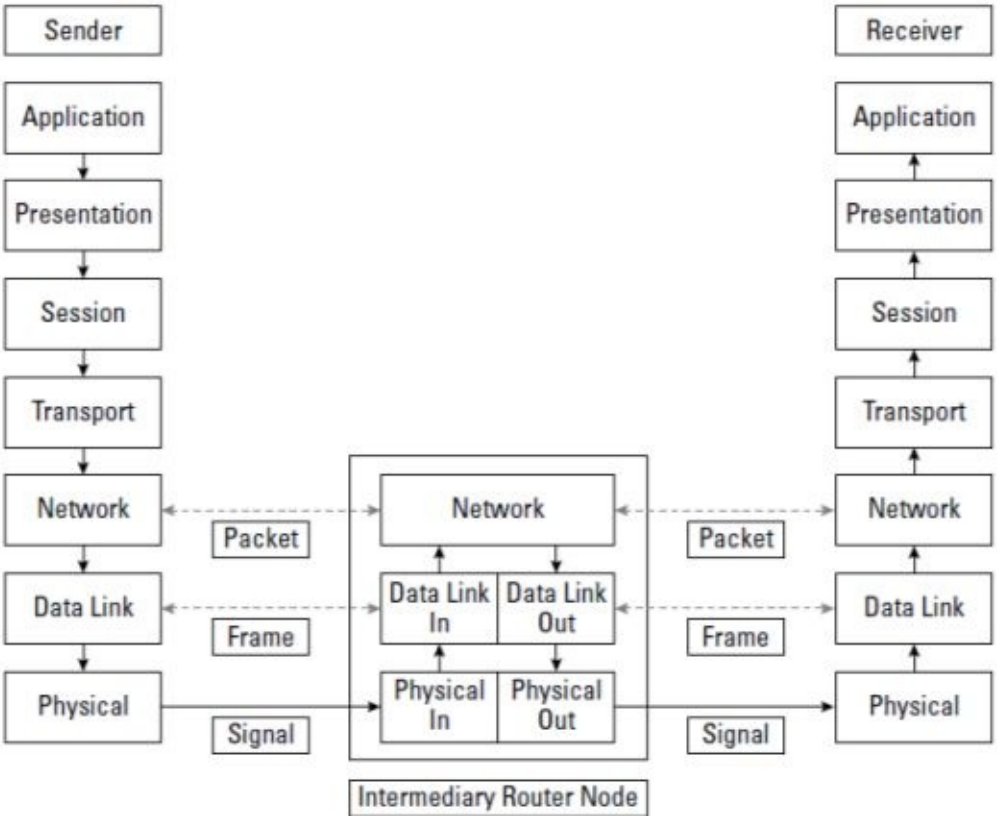
1. Acceptance of data packets from the network layer.
2. Assembling of the data pieces, stored in data packets, in a *data frame*. Layer 2 writes the physical MAC addresses of the source and destination hosts of the device in each assembled data frame.
3. Directing the data frame to the physical device displaying the correct physical MAC address. The device then decodes the data frame to readable optical or electrical signal.

Functions of Layer 3 Router

The Layer 2 switch is designed to oversee the creation of a single impact domain per port and the forwarding of data frames on exit transfer ports that managed to get to the frame's destination.

Using the snail mail analogy, Layer 2 switch acts as the mailman who delivers the mail to specific addresses inscribed in the envelope. Routers act as the local post office that organizes the letters by street before it hands the mail to the mailman.

Routers are usually slower than their Layer 2 counterpart is. This is because routers have to first check for data packets within the network layer whereas Layer 2 only checks datalink frames to check for the physical address of each data packet.



Network Layers (comp4net.com)

The above figure shows how data packets are sent, processed and read by an intermediary device. In this case, the intermediary device is a router. The flow of the data packets from source to destination hosts (sender to receiver) in the figure describes how data is being processed by two different LANs. The router inspects the data packets first in the network layer before it sends it to the data-link frame layer in the form of data frames. These data frames are then sent to specific physical devices.

While the main function of the router is to transfer data packets through the source and destination hosts of each network, it is also responsible for:

1. Inspection of the IP written in each passing data packet.

2. Extraction of the logical IP address of the destination host.
3. Inspection of the extracted IP address to decode the network where the data packet must be sent.
4. Sending of the data packet to the correct destination network. (This is if the router recognizes the destination network.)

If the router is unable to recognize the destination network, it will just transfer the data packet to its own exit gateway for outbound transfer.

Types of Protocol

At the network layer, there are two types of recognized protocols: *routing protocols* and *routed protocols*.

1. ***Routing Protocols*:** These protocols are used to transfer route update packets from one host to another. Information about new routes and new networks are stored within the route update packets. These packets are sent by routers to each other whenever a new route is opened or a new network is established.

   Among the more prominent routing protocols are Routing Information Protocol (RIP; Chapter 11), Enhanced Interior Gateway Routing Protocol (EIGRP; Chapter 12), and Open Shortest Path First (OSPF) Protocol (Chapter 13).

   These routing protocols employ varying systematic metrics to determine which routes and networks are better compared to others.

2. ***Routed Protocols*:** These protocols are used to transfer data packets as well as to identify hosts from networks in the global environment. Routed protocols assign a unique logical address for each host in the network.

   Good examples of routed protocols are AppleTalk, SNA, IPX and IPv6.

Router Functions

The four basic functions performed by a Layer 3 router are:

1. Maintaining routing protocols;
2. Establishing routing tables by means of routing protocols;
3. Keeping tab of routing tables; and
4. Routing data packets.

Keep in mind that logical IP address follows a hierarchy. They have numbers that correspond to the name of the network and numbers that correspond to the host device.

Consider the IP address of the network is 192.168.45.0 for example. Hosts within the network must have an IP address that begins with 192.168.45. Consequently, hosts within the network described by an IP address 192.168.62.0 should have hosts whose IP address begins with 192.168.62. In the two examples, the first three numbers are used to identify the network while the last number is used to identify the host.

Routing Protocols

Before two networks are able to send data packets to and from each other, the routers need to set up a consistent routing protocol. The different stages of setting up a consistent routing protocol are:

1. Setting up the routing protocol for each router;
2. Accessing the interface of each router; and
3. Customizing the options for routing protocols.

Unless the router is programmed to negotiate routing protocols with each other, you have to execute each stage to manage routing protocols.

Routing Tables

While routing protocols contain specific instructions on how the router should exchange information in forms of data packets within networks, routing tables manage the changes within the network, the paths for each network and the metrics for each path. Aside from that, routing tables also keep track of the following:

1. List of networks remembered and forgotten by each router
2. Data stored within the router interface
3. Metrics related to each path.

Chapter 2. Router Management

The Cisco Internetwork Operating System (Cisco IOS) is responsible for managing Cisco routers. Managing Cisco routers and managing Cisco switches is similar. For both routers and switches, only the output differs — the IOS commands are very similar. In fact, the graphical user interface used for managing both Cisco routers and switches is the same except for some differences. For instance, Cisco Router and Security Device Manager (SDM) is obviously only available for Cisco Routers (and not for Cisco Switches.)

Cisco Routers

The three classifications of Cisco Routers are as follows:

Cisco Router	***Best Suited for***
Entry-level Router	Access Layer and Distribution Layer
Midrange Router	Access Layer and Distribution Layer
Top-of-the-line Router	Core Layer and Distribution Layer

Top-of-the-line Cisco routers are designed to perform the following the routers in their respective networks:

- WAN gateway connectivity
- Inter-VLAN routing
- Open Shortest Path Fist (OSPF) backup designated router (BDR)
- OPSF designated router (DR)

Using the Cisco Routers

Like almost all router brands, Cisco does not allow user interaction, at least not directly. Managing the controls of a Cisco router can be done by connecting it to a computer host either remotely or locally. Once the router is connected to the computer host, users can now open the user interface in the computer host to engage with the Cisco Router.

Local Connection

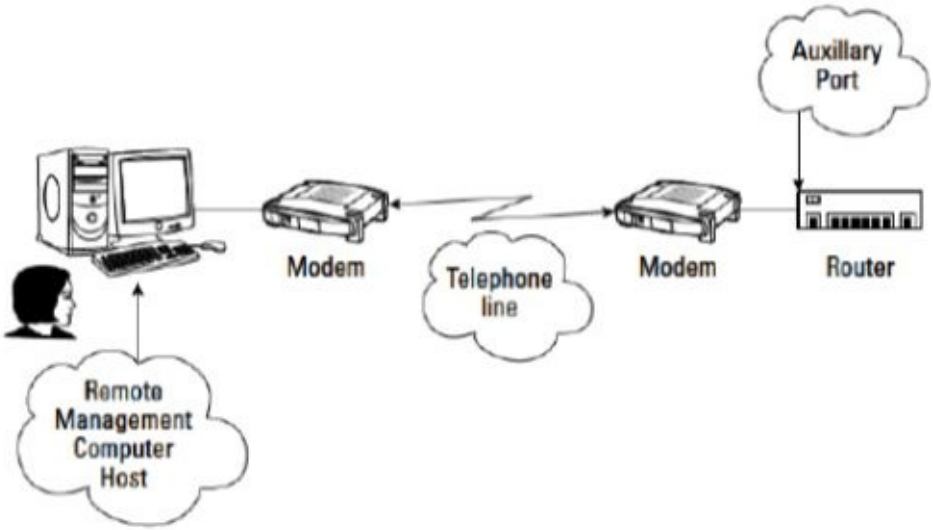
A typical cisco router has several ports that where line plugs can be inserted to connect to the host computer or other similar network-enabled devices.

Other ports, typically bearing different colors from the rest, serve other functions other than ensuring connectivity to network layers. These ports are:

Auxiliary Port

This port is used to connect a router to the main computer frame by means of a rollover cable. The modem connected to the auxiliary port of the router is connected via a telephone line to a similar modem that is connected to the main computer frame.

In theory, auxiliary ports are really designed with remote connections. The only difference is that setting up remote connections with the aid of auxiliary port requires a modem to be locally connected to the router via the auxiliary port.



Auxiliary ports (cisco.com)

Console Port

Similar to Auxiliary Ports, Console ports are designed to connect main computer frame to router through a rollover cable. This port is used to link the router to the console locally.

The Cisco Operating System has a *console facility* that aids user

interaction through prompts, status updates, error warnings, and diagnostic messages. The console facility can be accessed by connecting the router through its console port to the computer host using rollover cables.

After connecting the computer to the router using a physical connection, the *terminal emulation program* must be accessed in the computer to open the terminal setting in the router. Examples of terminal emulation programs are:

- HyperTerminal
- SecureCRT
- TeraTerm

Remote Connection

Using a remote management computer host, CISCO's terminal window and router console can be accessed remotely. Remote access to CISCO routers can be set up using:

- *Console Terminal Server* can be used to determine the IP address of the console. In fact, Console Terminal Servers can be programmed to assign router console facility to specific TCP/IP port serial as well as specific IP addresses in the network. Using any of the terminal emulation programs, `IP:port` can be connected to the Console Terminal Server.
- *Telnet Applications* can also be used to access the router's network IP address. The router is already assigned with a specific network IP address, which assists the network to detect the router.
- *Auxiliary Ports*, as explained in the previous section, can be used to connect the router to the remote management computer host.

Configuring a CISCO Router

If you don't understand how to configure a CISCO router, it is unlikely that you'll pass the CCNA certification exam. Aside from just getting the CISCO router hooked up, this section will also teach you how to deal with startup and running structure controls.

CISCO routers always come with the following items:

- AC power cord
- Rollover Cable
- Mounting Brackets

- Router and Security Device Manager CD
- Router Documentation CD

Freshly unboxed Cisco routers are not yet configured with any setting. The lack of a startup configuration requires you to create one. When no startup configuration settings are stored within the NVRAM, Cisco Routes return to setup mode in preparation for initial router configuration. This happens when the:

- device is being used for the first time; or when
- initial router configuration has been wiped off.

The two ways to build the initial configuration of a new Cisco Router are:

- Connecting to Cisco IOS setup mode commands
- Accessing the Initial Configuration Dialog Box

Cisco IOS Setup Mode Commands

1. Naming the Router

In the Cisco IOS command, you can specify a name for the router using a *hostname*. To name the router, just run the following code:

```
Router>en
Router #config t
Router(config) #hostname SampleName
RT01(config)#exit
RT01 #disable
RT01>
```

2. Setting up the management IP address configuration

The Cisco IOS commands `ip default-gateway` and `ip address`, you can now establish the IP gateway and IP address of the router. This lets you use HTTP or Telnet to establish a connection to the router from distant locations.

To customize the current default gateway and management IP address on the router, you can implement the following commands:

```
Router>en
Router #config t
```

```
Router(config) #int fe0/0
RT01(config) #ip default0gateway 192.168.72.2
RT01(config) #exit
RT01(config-if) #ip address 192.168.72.30
  255.255.255.255.0
RT01(config-if) #no shutdown
RT01(config-if) #exit
RT01 #disable
RT01>
```

The first two lines:

```
Router>en
Router #config t
```

can be used interchangeably with:

```
Router>enable
Router #configure terminal
```

These two lines enable the *privileged global configuration mode* in the Cisco IOS. This configuration mode allows you to implement commands that can tweak the settings of the global router or simply the settings of the entire router.

This line:

```
Router(config) #int fe0/0
```

can be used interchangeably with:

```
Router(config) #interface fastethernet0/0
```

This command allows you to choose which command interface to work on.

In the example provided in the previous page, this line:

```
RT1(config-if) #ip address 192.168.72.30
  255.255.255.255.0
```

sets both the IP address (`192.168.72.30`) and the subnet mask (`255.255.255.255.0`).

- To start a command interface, you first select it before implementing:
  `RT1(config-if) #no shutdown`
- To exit a command interface, you select it again before implementing:
  `RT1(config-if) #no shutdown`

The IOS prompt shows you what configuration mode you are in while keying in the IOS commands. Here are the different configuration modes:

Global Configuration Mode `(config)`

This mode allows you to change the settings by implementing commands codes for the whole router (global router).

Interface Configuration Mode `(config-if)`

After choosing the interface to work with, this mode is activated. This mode allows you to change the settings of the router interface.

Interface Range Configuration Mode `(config-if-range)`

By implementing the interface range command code, you can select the interface range to work with. This mode allows you to implement system codes to change the setting of all interfaces within the selected range.

Password Configuration

Router credentials can be changed by configuring Cisco IOS commands by entering credential values to `password` and `login` variables. Cisco routers don't have a pre-programmed password.

Cisco features routers that supply information to the network and the devices on it based on the kind of access enabled by a specific password. Cisco routers allow four kinds of access:

Console Password	This password grants access to the Router console via the Console Terminal Server or the console port.
Auxiliary Password	This password grants access to the Router console via the auxiliary port in the router.
VTY Lines Password	This password grants access to Telnet and Security Shell (SSH) to the Virtual Type Terminal (VTY). The VTY is called such because it does not require any physical connection from the terminal to the router. This remote connection uses the IP address of the router to connect the computer host directly to the network.
Privileged Password	This password grants access for select users who have a security clearance that allows them to configure the operation of the management computer host. These users are able to implement special IOS command.

By default, both the auxiliary port and console port are enabled regardless if a password is a configured for each of them. This poses a security vulnerability to the router network thus Cisco recommends that, at the very least, a console password must be configured.

Also by default, the VTY lines are disabled. Enabling VTY require the configuration of VTY password. To set the password for the Cisco router, the Cisco IOS interface can be instructed to prepare the router for authentication. In the IOS interface, implement the following commands to set the console password:

```
router001 > en
router001 #configure t
router001 (config)#line cons 0)
router001 (config-line) #password x1dmv4
```

```
router001 (config-line) #login
router001 (config-line) #exit
router001 (config) #exit
router001 #disable
router001 >
```

These lines can be used interchangeably:

```
router001 > en
router001 > enable
```

The same goes for this line:

```
router001 #config t
router001 #configure terminal
```

These two lines enable the *privileged global configuration mode* in the Cisco IOS. This configuration mode allows you to implement commands that can tweak the settings of the global router or simply the settings of the entire router. Also:

`line console 0`	This IOS command chooses the console line. All Cisco devices (routers or routers) only have one kind of console line: `console 0`
`Password x1dmv4`	This IOS command sets the password to `x1dmv4` on the access line of the console.

VTY Password

The following commands can be implemented in the Cisco IOS interface:

```
router001 > en
router001 #config t
router001 (config) #line vty 0 ?
  14 last line number
router001 (config-line) #line vty 0-12
```

```
router001 (config-line) #password newx1dmv4
router001 (config-line) #login
router001 (config-line) #exit
router001 (config) #exit
router001 #disable
router001 >
```

To have a good understanding of how each block of line is used:

`#line vty 0 ?`	This command poses a query that determines the number of VTY lines free.
`0-12 last line number`	This is the response of the Cisco IOS saying that lines 0 to 12 (or 13 lines) available for the router. This means there are exactly 13 Telnet sessions that can be simultaneously opened for this router.
`#line vty 0-15`	This command selects all the 0-12 VTY access lines available. Older versions of Cisco routers only use four VTY lines but newer implementations have at least 1,180 VTY lines. This is why the previous commands had to pose first an inquiry on how many VTY lines are available.
`#password newx1dmv4`	This IOS command sets the password to `x1dmv4` on the VTY lines chosen in the previous command line.

Cisco devices have several VTY access lines because of two major reasons:

1. **Several VTY access lines allow multiple users to manage the router:** Large router networks grants access to more than one router manager. By

using SSH or Telnet, router managers can access the router through remote connection.

2. **A VTY access line allows a user to connect to a different device also connected to the router.** In this case, two VTY lines are required. One that connects the computer unit to the router and another that connects the router to the other device.

Setting-Up a Router Banners

Router banners are brief messages that the router display to a terminal connected to it. This is common with routers that are being accessed by multiple computer terminals. It can even display which router a user is using including the configuration limits and connection guidelines.

Companies and organizations can also configure a security warning in the banner message to ward off potential unauthorized access to the router. This gives a company to exercise legal action should an illegal access be detected by the system.

The four different types of banners that Cisco routers can display are:

1. ***EXEC process creation banner:*** This type of banner is configured in the screen during the creation of EXEC processes.
2. ***Message of the Day (MOTD) banner:*** This banner displays a message every time a user establishes a connection with the router. Regardless if the connection is remote or local, the router will display this message when there is an attempt to log into the router network. The MOTD banner is usually used to ward off users attempting an illegal connection to the router.
3. ***Incoming terminal connection banner:*** This banner is often displayed after the MOTD banner. This banner is used to give additional information for users who are connecting using VTY or reverse TTY computer terminals.
4. ***Login banner:*** This banner is displayed to give information to the users about the router. This may also contain additional guidelines on how the connection should be used.

The following command can be implemented to setup an MOTD banner on every router connection:

```
router001 > en
router001 #config t
router001 (config) #banner motd /

Enter TEXT message. End with character '-'.

$This router is owned by example.com. Should the system
detect any unauthorized access to the router network,
the security system will trace the user login to display
security credentials from access point. If you are not
from example.com, nor a client nor a business partner,
please disconnect immediately.
-
router001 (config)#
```

The command `#banner motd /` opens the text editor interface. The delimiting character set in this command is "/", which means that the IOS interface will process the text input only until it detects a "/."

The delimiting character can be any character that could not be found on the text of the MOTD banner.

Resetting a Cisco Router

Whenever the router detects that there is no initial configuration activated in the NVRAM, it automatically implements Express Setup mode. This happens when the router has just been brought out of its box or if the initial configuration has been deleted from the NVRAM.

Relieving the Cisco router of its current configuration is usually a last-resort troubleshooting attempt to fix connection problems. After the router is reset, the following information will also lose their configured value:

- IP address
- Telnet password
- Host name
- Console password
- Subnet mask

- Default gateway

To reset the settings of the router and delete any configuration stored in the NVRAM:

1. Press the Mode button and held it for a few seconds. Hold the Mode button until the LED indicators in the router begin blinking.
2. Wait for the LED indicators to stop blinking before you stop holding the Mode button. After all the LED has stopped blinking, the router should reboot by itself.
3. Release the Mode button

The Cisco bootstrap program allows router managers to tweak the booting procedure of any Cisco router connected to the computer host. The boot command does the following:

- Manage the loaded Cisco IOS image file
- Enable the Ctrl + Break system key while the router is booting
- Select which initial configuration should be used
- Enable manual booting
- Format the size of the NVRAM.

The following command block instructs the IOS interface to show the available options for the boot command:

```
router001 >
router001 >en
Password: x1dmv4
router001 #config t
router001 (config) #
router001 (config) #boot ?
    system
    System Image

    manual
    Manual Boot

    boothlpr
    boots the Helper System Image
```

```
    private-config-file
    Private Configuration File

    Buffersize
    Determines the size for filesystem-simulated NVRAM

    helper-config-file
    Helper Configuration File

    config-file
    Configuration File

    Helper
    Helper Image

    enable-break
    Enables the Break process while booting

router001 (config) #exit
router001 #disable
router001 >
```

Technet24.ir

The following are the global configuration settings that can be executed using the boot command:

`booth1pr`	While this is not usually touched upon in the CCNA test, this command accesses the image file that helps the boot system.
`buffersize`	This allows the user to determine the memory size of the NVRAM. Should the user desire to add extra Cisco IOS images to the flash memory, the size of the NVRA must be increased.
`config-file`	This allows the user to determine the particular configuration file that should be using as the router boots up. This is used whenever the user needs to check on other alternatives to the initial configuration file.
`enable-break`	If this option is enabled, the user can disrupt the booting process by pressing Ctrl + Break shortcut keys.
`helper`	These options are also not included in the coverage of the CCNA test.
`helper-config-file`	
`manual`	This option allows the user to boot the router manually without impairing the system nor any configuration setting in place.
`private-config-file`	This option allows the user to determine the private configuration file that could be loaded while the router is booting up. Private configuration files are designed to safeguard highly-secured configuration information like encryption keys for SSH.

`system`	This option allows the user to load a specific image file in the IOS interface for checking.

Technet24.ir

The following command block is used to configure the router to access a particular IOS image file that is stored within the flash memory:

```
router001 >
router001 > en
Password: x1dmv4
router001 #conf t
router001 (config) #
router001 (config) #boot system flash:/c1440-
    example.com-mz.120-32.EY
router001 (config) #exit
router001 #disable
router001 >
```

The above code allows access to the image file bearing an address of :

```
flash:/c1440-example.com-mz.120-32.EY
```

In order to verify the options encoded on the said image file, the IOS command show boot can be used as in the example below:

```
router001 >
router001 > en
Password: x1dmv4
router001 #conf t
router001 show boot
BOOT path-list      : flash:/c1440-example.com-
mz.120-
                                          32.EY
Config file         : flash:/configuration.txt
Private-Config file : flash:/private-configuration.txt
HELPER path-list    :
Auto upgrade        : yes
Auto upgrade path   : yes
Enable Break        : no
Manual Boot         : no
```

```
NVRAM/Config file
    buffer size: 62642
router001 #disable
router001 >
```

The show boot command displays the current settings of the boot resources of the router.

Cisco Router File Systems

The three main directories that are used by the Cisco router are:

`Nvram`	This is where `private-config` and `startup-config` is stored.
`System`	This directory that is found in the RAM is where the `running-config` file is stored.
`Flash`	This directory refers to the flash memory. This where the Cisco IOS system image, which the bootstrap program loads, during the system boot process.

Auxiliary Password

Most Cisco routers have auxiliary ports. These ports can be protected by integrating a password specifically for auxiliary ports. To setup a password for auxiliary ports, the following command lines can be implemented in the system:

```
router001 > en
router001 #config t
router001 (config) #line aux 0
router001 (config-line) #password aux1dan4
router001 (config-line) #login
router001 (config-line) #exit
router001 (config) #exit
router001 #disable
router001 >
```

These two lines can be used interchangeably:

```
router001 > en
router001 > enable
```

The same goes for this line:

```
router001 #config t
router001 #conf ter
router001 #configure terminal
```

These two lines enable the *privileged global configuration mode* in the Cisco IOS. This configuration mode allows you to implement commands that can tweak the settings of the global router or simply the settings of the entire router. Also:

`line aux 0`	This IOS command chooses the auxiliary line. All Cisco devices (routers or routers) only have one kind of auxiliary line: `aux 0`
`password aux1dmv4`	This IOS command sets the password to `aux1dmv4` on the access line of the console.

Privileged Password

There are IOS commands that should only be configured by specific users as these commands are crucial to the overall functionality of the router. The two commands used to setup a privileged password are:

`enable password privx1dan14`	This command sets the string `privx1dan14` as the privileged password. In other words, before a user can access the functions that are restricted for privileged users, they must key in `privx1dan14` in the IOS interface.
`enable secret cryptx1dan14`	This command sets `cryptx1dan14` as the privileged password. Compared to the command line above, this password is encrypted. Also unlike the above command line, this command is supported only by newer IOS interfaces that are compatible with the newer implementations of Cisco routers.

Before you set the privileged password, you must first enable this option by keying in the following commands:

`enable password`	This enables password protection for administrative privileges. The password is stored in an unencrypted format.
`enable secret`	The same as the above command line except from the fact that the password is stored in an encrypted format.

Privileged passwords are stored in a server called *Terminal Access Controller Access Control Sytem (TACACS)*. This server is often used by larger networks composed of multiple routers that allow the administrators to configure the privileged password only once for all routers in the network as opposed to setting up the passwords on each of the routers.

```
router001 > en
router001 # config t)
router001 (config) #enable secret cryptx1dan14
router001 (config) #exit
router001 #disable
router001 >
```

Password Encryption

Passwords are saved in plain text format by default in the startup configuration file in NVRAM and running configuration in the RAM. By implementing the `show start-up config` command and the `show running-config` command, the passwords will be displayed in simple text. This poses a security risk especially if the routers hold confidential data resources in the system. This is why it is advised that passwords must be encrypted in the system.

Other passwords like theconsole password, auxiliary password, and VTY password are not encrypted regardless if the command `enable secret` is used to configure any of the three passwords. To encrypt these passwords, the `service password-encryption` command must be used. Consider the command block below:

```
router001 > en
router001 #config t
router001 (config) #service password-encryption
router001 (config) #exit
```

```
router001 #disable
router001 >
```

Recovering A Lost Password

Password can only be recovered if the `password-recovery` feature is enabled in the system before the password is lost. This can be done while the router undergoes the boot process. To recover the lost password, the following steps must be followed:

1. Using any of the methods enumerated in one of the previous sections in this chapter, interrupt the regular boot process.
2. Access the flash file system manually.
3. Prevent the Cisco IOS interface from accessing the startup configuration file by hiding it.
4. Start the router manually until the IOS has finished loading in the RAM.
5. Reactivate the startup configuration file.
6. Transfer the configuration file to RAM from NVRAM.
7. Change the password.
8. Store the running configuration.
9. Reset the boot process to its original settings.
10. Restart the router.

Chapter 3. Network Routing

The main role of routers is to transmit data packets from one network to another. Aside from this, the routers are responsible for the following:

- Transmit packages based on routing tables and routing protocols
- Maintain routing protocols
- Organize routing information into routing tables
- Manage routing tables

Data transmission paths that extend through different networks are called a

network route. Each route joins two end nodes, each representing a network device that is capable of being assigned with IP address. Examples of which are smart phones, tablets, gaming consoles, camera interface, and computer hosts.

It is possible to have more than one route in between nodes. This is because the router employs a special algorithm that computes for the best route available before a data packet is sent from one point (source) to another (destination). The algorithm takes into consideration route metrics, which include the cost of the resources, and the time it takes to send the data packets.

Within the data transmission path, there should at least be two routers positioned anywhere in between the source and destination nodes. For example, when sending a message via a chat module installed in your computer, the computer sends packets of data containing the message you intend to send to a computer user elsewhere. These data packets pass through the home router. The home router then transmits these data packets to the Internet Service provider (ISP) via the outbound gateway. The Internet Service Provider's outbound gateway then transmits the packets through cables and cables of integrated network chain until it reaches the network/ server of the recipient user. Data packets will be received by the router of the receiving host computer at lightning speed. Notice that, depending on the location of the recipient, data packets traveled through at least four routers:

- Home router of the sender
- Outbound Gateway (ISP) of the sender
- Inbound Gateway (ISP) of the recipient
- Home router of the recipient

Technet24.ir

Types of Network Routes

There are three types of network routes namely:

1. ***Static routes***

   Perfect for smaller networks, such as home networks, static routes are routes that are manually configured on the router. Aside from home networks, LAN connections can also be managed by static routes because these connections seldom change. If for any reason the connection changed, the router must be manually configured to indicate the new transmission paths.

   Static routes are useful to home and LAN connections because of the following:

a. **Efficient Routing:** Routing protocols are disabled whenever static routes are configured. Since routing protocols use bandwidth, static routes save bandwidth consumption. On the flipside, routing protocols are enabled whenever dynamic routing procedures are used. Routing protocols use bandwidth because update packets are being sent between two routers.

b. **Security:** Configuring static routes allows the user to manage the transmission paths used when sending data packets. This is useful for routers that have been transmitting highly-critical and highly-confidential information. Regularly updating static routes provide an extra layer of information security and foil any attempts to hack into the network system and phish for data. Also:

- Firewalls can be introduced to static routes to filter routing data within the network border.

- Regardless of the route, Virtual Private Networking (VPN) safeguards the data sending mechanism regardless of the route where the data travels.

  In other words, security risks can be managed by building a firewall or by using VPN.

However, while static routes have many upsides, they also have a few downsides like:

Technet24.ir

a. **Management Overhead:** Maintenance can be tricky because every time the data transmission paths change, the router configuration must be updated.

b. **Scalability:** Static routes are impractical when managing larger networks. Wide-scale networks are composed of thousands of routes to reach other areas of the network. A good example of these networks is commercial internet connections provided by the Internet Service Provider. Houses are connected to a single network managed by a server. Even so, it is impractical (and almost impossible) to configure all the routes to be static. Also, should any of the routes change, all the static routes in the network must also be changed. This is the reason why static networks are perfect only for small-scale networks.

c. **Accuracy:** If the network routes change and no configurations were made on the static network, the router will not have an accurate understanding of the network. As a result, data transmissions are either delayed or lost completely.

Static routes can be configured by using the Cisco interface by entering the following command:

```
ip route dest-ip subnet {next-hop_ip | interface}
```

2. Default routes

Whenever data packets are sent to a new destination network, packets follow a different kind of static routes. New destination networks are not likely to have an entry in the routing tables so a new route is assigned to them. This route is called default routes. It is not uncommon for a router to receive a data packet addressed to a new network that it has no information of; in this case, the router transmits the data packet through the default route.

Network managers always make sure that a default route is configured in the router in case data packets addressed to newer unrecognized networks is

received by the default outbound gateway. Default routes transmit data packets via the default gateway configured in the network.

Configuring default routes

Configuring default routes is similar to configuring a regular route using the global configuration mode. By using Cisco IOS interface, default routes can be configured manually by following the examples provided below:

Assuming that both the subnet mask and the IP address of the destination network are `255.255.255.255`, run the code below to configure the default route:

```
RT10-1> en
RT10-1 #config t
RT10-1 (config) #ip route 255.255.255.255
 255.255.255.255 serial 0/0
RT10-1 (config) #exit
RT10-1 #disable
RT10-1>
```

3. *Dynamic routes*

These routes change on a regular basis. The dynamics of dynamic routes are being managed by routing protocols. They are responsible for updating router configuration whenever changes such as the following happen:

- Link-state landscape
- Available bandwidth
- Updates in network traffic
- Updates in network topology

Using dynamic routes have the following advantages:

a. **Low maintenance:** Unlike static routes that require constantly updating the routing configuration whenever the network landscape changes, dynamic routes require no such laborious task. Dynamic routing immediately recognizes changes in data transmission paths. In response, router settings are immediately configured to complement changes in the network. This task is managed by routing protocols who exchange information with other routers on a regular basis.

b. **Accuracy:** Dynamic routes use routing protocols to gather information about other routers. This exchange of information between routers is done by sending back and forth update packets so the routing protocols can immediately configure router settings.

c. **Scalability:** Unlike static routes that are best-suited for smaller networks, dynamic networks are perfect for larger networks. Routing protocols manage hundreds or possibly thousands of routes in large-scale networks. This seems to be a logistical nightmare for static routes. For dynamic routes however, this is just another day in the office. Routing protocols minimize miscommunication among routers by constantly communicating with routes within their network

Dynamic routes only have one known disadvantage: network overheads. Since routing protocols facilitate a constant exchange of information with other routers, dynamic routes consume more bandwidth causing network overheads.

Routing Protocols

The main function of routing protocols is to exchange routes, network and metric information in forms of data packets to determine the best route available. This information is used to build a *routing table* that contains all the pertinent information about routes and the corresponding metrics associated to it.

There are several routing protocols but you only need to know three of them:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP); and
- Open Shortest Path First (OSPF)

Routed Protocols

The source and destination address of each data packet is assigned by *routed protocol*. The address tagged in the data packet is a unique combination of numbers that correspond to the address of the source and destination node. The most commonly-used routed protocols are:

- Novell Netware Internetwork Packet Exchange (IPX)
- AppleTalk
- Internet Protocol ver. 4 (IPv4)
- Internet Protocol ver. 6 (IPv6)

Depending on the results of the evaluations made by the routing protocol, the routers choose a destination for a data packet based on *decision criteria*. Routing tables build an inventory list of all the networks, paths, routes and metrics associated with all the nodes it has touched bases with before. Decisions made by the routing protocols are based on the information stored in the routing table.

Routing protocols base their decisions on two aspects:

1. ***Administrative/Virtual distance:*** This aspect measures the reliability of the information integrated in the data packets about the destination node. Routers gather information about the network routes through the following:

- *Direct connection to the network:* Routers do not use intermediaries to gather information about the routes. Updates in the form of data packet are sent to different routers for information-gathering purpose.

- *Indirect connection to the network (via other routers):* Pieces of information about other network not within range are gathered from what information other routers have gathered.
- *Static Route connection to the network:* The router is not directly in touch with a network but it is informed of its existence by the static route.

Routers compute for the reliability of the information based on the source. It follows a hierarchy that favors routers nearest it. Cisco measures

administrative distance by assigning distance values:

Source of Information	***Administrative Distance Values***
Direct Connection	0
Static route	1
Internal EIGRP	90
OSPF	110
RIP (ver. 1 and ver. 2)	120
External EIGRP	170

Routers prefer information with lower administrative distance values.

2. ***Routing Protocol Metrics:*** This computes the costs associated with each route. Examples of weighted costs are as follows: link state, available bandwidth and traffic.

The various routing protocol differs on how they calculate the efficiency of each of the router hence it is understandable that each of the routing protocols may have different preferred routes compared to the rest. When routing protocols disagree with each other, routers select the best route by computing for administrative distances instead.

Here are some of the metrics used in route selection:

a. **Bandwidth:** This refers to the capacity of information that can be held by a route to reach the destination. Bandwidth is measured in terms of *bits per second (bps)*. Routes with higher bandwidth are preferred by most routing protocols because data packets tend to reach the destination point faster with a larger bandwidth. This metric is given more weight by *EIGRP*.

b. **Hop Count**: This refers to the number of routers between the source node and the destination node. Router protocols tend to pick routes with less hop counts to minimize delay. RIP is notorious for using this metric on determining which route to pick.

c. **Cost:** This refers to the value computed based on the bandwidth of a network route. The figure is measure by 10^8 / bandwidth. OSPF uses this route more heavily than it does other routing protocol metric.

d. **Maximum Transmission Unit (MTU):** This refers to the size of each data packet. MTU is measured in terms of bytes. The bigger the size, the bigger the amount of data that can be transferred at any given time. EIGRP uses MTU heavily, preferring higher MTU values.

e. **Load**: This refers to the bandwidth presently consumed by the data traffic at any given route. It is computed by getting the difference between the available unused bandwidth and the total bandwidth of the route. EIGRP picks network routes with lower load.

f. **Reliability:** This refers to the how much time is available in a specific route. EIGRP selects route with higher reliability values.

g. **Delay:** This refers to the average amount of time a data packet takes to reach the destination host. This is compute based on the following metric:

- *Propagation delay*: This refers to the time taken by the signal to spread throughout all the transmission paths.

- *Transmission delay*: This refers to the time taken by data packets in between hops.

- *Queuing delay*: This refers to the time a packet spends in queue before it is released to an outbound port.

- *Processing delay*: This refers to the time spend by the router to inspect the encoded destination address.

Technet24.ir

Routing Methods

Routers use the different standards through which routing protocols compute for the most viable route. Before they even measure the efficiency of each route, routing protocols initiate a progressive trade of information between routers to build a reliable routing table. This exchange of information is done through many different methods. These are:

1. **Distance Vector Routing:** Routers, who are using protocols that measure distance between nodes, complete their routing table by the information taken from their own direct connection and from neighboring routers.

   This is a routing procedure where routers trust the information sent to them by neighbor routers. The information sent by neighbor routers is also sent to a different neighbor router who might not have direct connection with the original router that sent the information. *Rumor routing* is another name for distance routing.

   Distance vector routing employs the following special mechanisms to avoid incurring routing loops:

- *Triggered update:* This feature lets different routers share updates with each other once a router becomes functional or when something has changed within the network.

- *Poison reverse:* This feature sends a message to all neighbor routers that a specific network is down and therefore must not be used as a route for a data packet.

- *Split horizon:* This feature hinders the promotion of the route back to its original promoter.

- *Hold-down timer:* This feature hinders the acceptance of new updates on specific routes for a preset period if the route is deemed unavailable. This prevents the re-advertisement of routes that are not functional as this may

eventually lead to routing loops.

- *Route poisoning:* Similar to *poison reverse*, this feature sets the number of hops to the maximum number of hops plus 1. This automatically gives neighboring routers information that such route is no longer reachable.

- *Maximum hop count:* This feature makes sure that the data packet does not follow a route that requires more hops than the predetermined maximum hop count.

Routing Protocol	**Maximum Hop Count**
RIP	15
OSPF	255 *(subject to user configuration)*
EIGRP	Unlimited

Routing loops eventually lead to a route failing. This often takes time before all the concerned routers are informed.

The two protocols that use distance vector routing procedures are RIP and IGRP (not to be confused with EIGRP).

2. **Link-State Routing:** Routing protocols that follow link-state routing procedures build routing tables using information exclusively from the updates gathered from neighbor routers. Instead of just pooling the information found in the neighbor's routing table, link-state protocol gets a good view of the network topology and routes within and beyond neighboring routers.

Link-state protocols are characterized by the following:

- Compared to distance vector protocol that sends and receives route updates on a regular basis, link-state protocol only sends and receives update when change has been detected in any of the immediate routes.

- Aside from routing tables, link-state protocol also manages topology and neighbor tables.

- Updates send by neighbor routers only contain information about routes the changed.

- Routers under link-state protocols exchange “hello” packets to get a good understanding of neighbor routers.

Link-state routing is prominently configured in the *Open Shortest Path First* (OSPF).

3. ***Hybrid Routing***

Protocols that employ hybrid routing combines the properties of both link-state and distance vectors including:

- Similar with *distance vector protocols*, hybrid routing protocols use administrative distance metric to determine route quality.

- Similar with *link-state protocols,* hybrid routing protocols use MTU, load, reliability, delay and available bandwidth to determine route quality.

Cisco-proprietary *Enhance IGRP (EIGRP)* uses hybrid routing procedures.

Convergence: This refers to the first exchange of information made by the routers to each other as they attempt to connect to the network.

Technet24.ir

Chapter 4. Enhanced Interior Gateway Routing Protocol (EIGRP)

Unique to Cisco routers, Enhanced Interior Gateway Routing Protocol (EIGRP) has plenty of upsides compared to that of the Interior Gateway Routing Protocol (IGRP) and its successor Routing Information Protocol (RIP). Both IGRP and EIGRP are known to be a distance vector protocol. The only difference is that the latter of the two has a better set of distance vector and response algorithm. This algorithm is responsible for determining the best data path towards a particular destination. Also, it employs an advanced loop mitigation system compared to that of both IGRP and RIP making it perfect for link-state protocols.

Aside from the ones mentioned above, Cisco designed EIGRP to supersede IGRP's limitations. Compared to IGRP and RIP, EIGRP:

- Supports both VLSM and CIDR
- Congregates quickly
- Has a Hop count limitation is 255 with the default set at 100
- Utilizes the Diffuse Update Algorithm (DUAL) to check the value of the routes
- Maintains routes including those that are already-managed by different routing protocols
- Is attuned with the present IGRP implementation
- Can route Novell Netware Internetwork Packet Exchange (IPX), Apple Talk, Internet Protocol (IP) and other routed protocols.

Characteristics of EIGRP

EIGRP is widely-acknowledged as more of a *distance vector protocol*, but by definition, it is also a *hybrid routing protocol* because it has advanced features usually found only in link-state protocols. Here are the characteristics of the EIGRP:

1. EIGRP evaluates the efficiency of the routes by using these metrics:

   Default Metrics: Delay and Bandwidth

   Optional Metrics*:* MTU, load, Reliability

   Diffusing Update Algorithm: Route efficiency.

2. As with the rest of link-state routing protocols, OSPF and EIGRP direct the updates about routes only if it detects deviations within the network.
3. EIGRP is only exclusive to Cisco routers.
4. EIGRP performs its functions using two main directorial distance figures:

- 170 – routes from other protocols
- 90 – routes from EIGRP

Components of EIGRP

This router protocol comprises four components:

1. ***Protocol-dependent Modules:*** These are independent modules utilized by specific protocols when sending and receiving data packets within the OSI network layer.
2. ***Reliable Transport Protocol (RTP):*** This protocol guarantees a dependable delivery system that transports the EIGRP unicast or multicast data packets to routers nearby.
3. ***Neighbor Discovery/ Recovery:*** EIGRP employs a smart system that determines the existence of the nearest routers within the local network.
4. ***Dual finite-state machine:*** In order to estimate and determine routes that are free from loops, EIGRP uses a routing algorithm that recognizes a metric that selects routes based on the feasibility of each routing successors.

Routing Tables

EIGRP collects data about nearby routers and the landscape of the network and then stores it to a sequence of tables called routing tables. The three kinds of routing tables used by the EIGRP are:

1. ***Neighbor Table:*** This stores information using the local network or computer systems directly connected to each other. The information is then organized in a table that contains addressing and interface figures. Each Cisco routers uses its own EIGRP; hence:

- Each router is given a clear map of all the neighbor routers within the same network.
- Each router is given an inventory of details of each peer router.

2. ***Topology Table:*** This summarizes all network destinations that are routable through EIGRP and estimations using a metric that detects whether a destination is in an active or passive status. Each Cisco router also runs OPSF to manage a separate link-state table; hence:

- Each router has a clear map of network topology not just of its own network but the networks in surrounding network areas of neighbor routers.
- Each router gets a deeper understanding of the network topology by using link-state and neighbor table. It gets a clear picture of how the topology within the router's and its neighboring router's surrounding network vicinity work.

The topology table manages the following in each of the network destinations:

- *Successor Route:* This is the most efficient route to the destination point as determined by DUAL.
- *Feasible Successor Route:* This is the second best route to the destination point, also determined by DUAL.

3. ***Routing Table:*** This is a collection of all destination routes mapped down using the information obtained from all the entries in the topology table. If both the link-state and neighbor tables count the number of available routes, the routing table describes each route.

EIGRP Packet Types

1. ***ACKs/ Hello:*** (Unicast) This packet is used when initiating initial discovery or recovery process of neighboring router locations. ACKs are packets containing unicast addressed with a specific non-zero numbers exchanged as an acknowledgement receipts between routers.
2. ***Updates:*** (Unicast) These packets have routing procedures accepted by nearby devices to help create and manage a routing table for the overall network topology.
3. ***Queries:*** (Multicast) These packets that contain coded queries are sent when a destination point is activated.
4. ***Replies:*** (Unicast) These packets are sent as a response to the queries sent from the origin point.
5. ***Requests:*** (Unicast, Multicast) These packets are used to obtain pertinent information from nearby network devices.

Convergence

As mentioned earlier EIGRP has faster convergence than that of both IGRP and RIP because routers in the same local network merely exchange ACK packets instead of the usually distance vector protocols. With EIGRP, routers become more familiar with each other while undergoing the convergence procedure by exchanging network parameters to each of their neighbor tables.

- Routers are only considered as “nearby” or “neighboring” routers if the following conditions are satisfied:
- Routers have successfully transmitted and received ACK/ Hello packets with each other.
- They have the same independent system that has the same interface with similar routing designs.
- Each of their ACK/ Hello timer is set to the correct value especially for the following metrics:

    a. Network frequency at which each routers exchange ACK/ Hello packets with each other

    b. Farthest distance before the routers consider a router out of coverage network

Diffusing Update Algorithm (DUAL)

DUAL is a Cisco-proprietary algorithm that assesses each of the routes managed by the EIGRP. This algorithm is responsible for improving the performance of the EIGRP compare to IGRP by circumventing looping routes.

- DUAL calculates the *successor route* and the *feasible successor route* for the destination networks.
- DUAL allows EIGRP to use routes across different networks using varying subnets by means of *variable length subnet masking* (VLSM)
- DUAL provides other *feasible successor routes* should the best route be unavailable.

Technet24.ir

Classful vs. Classless Routing

The two types of routing protocol supported by EIGRP are classful and classless routing. If used in their default settings, both the IGRP, RIP (version 1) and EIGRP are all *classful routing protocols*. By implementing a *no auto-summary command* in the Cisco IOS interface, the router can be configured to support classless routing. The differences between the two routing protocols are as follows:

Classful Routing Protocol	***Classless Routing Protocol***
When sending route updates, this protocol does not transmit subnet data.	When sending route updates, this protocol transmits subnet data.
Based on the class of IP address, this protocol provides a summary of routes within the boundaries of the network.	This does not provide a summary of routes within the network unless manually commanded to using the router interface.

Discontiguous Networks are networks that have a number of subnets that contain varying classes of IP address. They are required when implementing classless routing protocol.

Configuring EIGRP

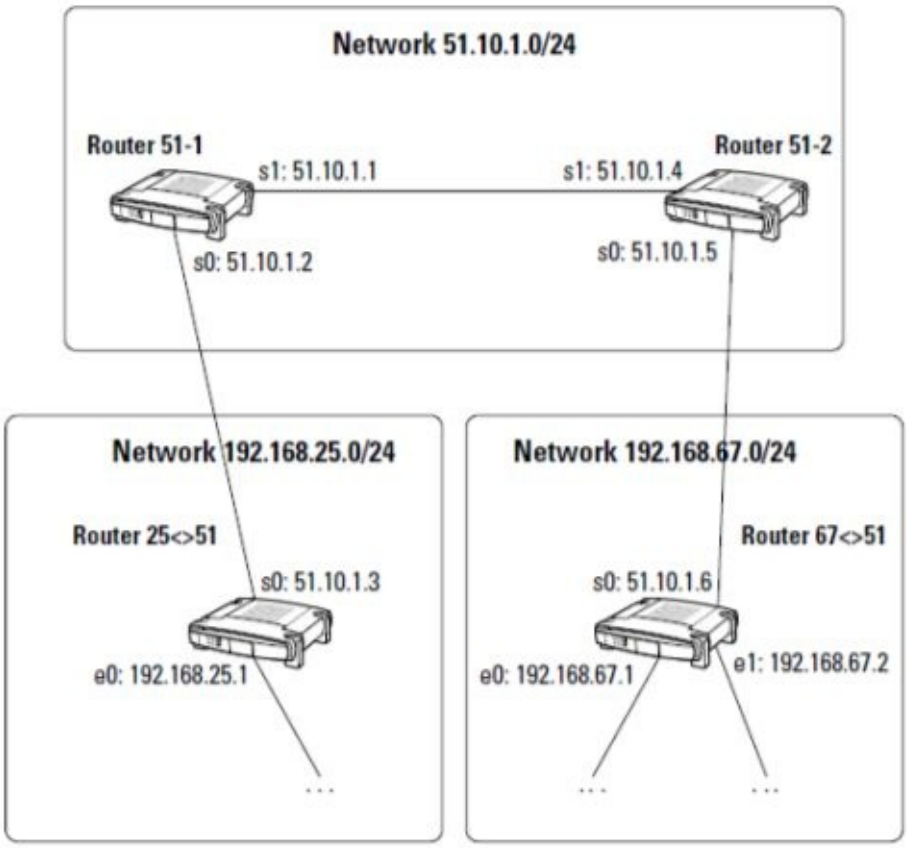
Similar to how RIP is configured in a Cisco router, EIGRP is configured by following these steps:

1. ***Run the EIGRP on each Cisco router***

   In the IOS interface, run the following code in global configuration mode:

   ```
   router eigrp as_id
   ```

   The `as_id` is the routing domain identification otherwise known as the autonomous system (AS) number. The AS number must be the same for all routers that will be sharing EIGRP routing information. This number should be within the range of 1 to 65535.



Routing Configuration of the EIGRP (cisco.com)

2. ***Enable EIGRP***

   As in the previous step, using the IOS interface run the following code to enable the EIGRP:

   ```
   Network int_IP
   ```

   The int_IP in the command is simply the IP address that will identify which interface will support the OSPF in the network.

Run the following codes when configuring the EIGRP:

For Router 51 -1

```
R51-1 > en
R51-1 #config t
R51-1(config)#router eigrp 1
R51-1(config-router) #network 192.168.25.2
R51-1(config-router) #network 51.10.0.2
R51-1(config-router) #no auto-summary
R51-1(config-router) #exit
R51-1(config) #exit
R51-1 #disable
R51-1 >
```

For Router 251:

```
R2551 > en
R2551 #config t
R2551(config)#router eigrp 1
R2551(config-router) #network 192.168.25.2
R2551(config-router) #network 51.10.0.2
R2551(config-router) #no auto-summary
R2551(config-router) #exit
R2551(config) #exit
R2551 #disable
R2551 >
```

Managing EIGRP Operation

Using the IOS Interface for Cisco routers, the elements of EIGRP can be monitored and verified to ensure that the routers are available to determine the best routes.

To take a good look at the routing tables, the following code can be run in the IOS interface:

```
show ip route
```

This command will then display the following information:

- Subnets available
- Information on the Network Internet Protocol
- Routes that are recognized and saved in the routing table

For each route, the interface displays the following data:

- Destination network that can be reached by the route as determined by the IP address
- If the router and the destination network of a route is directly linked to each other.
- The gateway's IP address if the router is not directly linked to the desired destination network of a route.

Other EIGRP-related Terms

Here are other EIGRP terms that you need to commit to memory in preparation for the CCNA Certification Exams:

1. ***Passive Destination Networks:*** These are converged networks where both the best (successor) and second best (feasible successor) routes are converged in the networks. All routers are aware of these routes without having to share *updates* with each other.

2. ***Active Destination Networks:*** These networks have not been converged yet. Routers are still on the process of exchanging routing information witch each other.

3. ***Smooth Round-Trip Timer (SRTT):*** The amount of time spent by a data packet to reach the neighboring router and then back to the origin router. This determines the amount of time routers typically wait for responses from nearby routers.

4. ***Retransmission Timeout (RTO):*** The value displayed here is the amount of time the router spends before it resends a data packet without notice of receipt from the neighboring router.

5. ***Queue Count (Q Cnt):*** The value displayed here represents how many data packets are lined up for sending. Some causes of high Q Cnt values are: (a) too much information sent to neighboring routers, (b) neighboring router is outdated hence not fast enough to receive data, and (c) error in the link between the origin and the destination routers.

Technet24.ir

Chapter 5. Open Shortest Path First (OSPF) Protocol

Just like EIGRP, Open Shortest Path First (OSPF) is a link-state routing protocol. Unlike EIGRP however, OSPF is not just supported by Cisco but also by other router manufacturers. When dealing with a wide-scale network environment, the OSPF uses a protocol called *IGP* short for *interior gateway protocol*. IGP creates and manages routes only within a *singular routing domain*.

Already mentioned in the previous chapter, a singular routing domain is simply *autonomous system (AS)*. The AS is simply routers and network addresses grouped together that are within the same routing network system. It can be inferred then that any network that has OSPF integrated in all the connected routers is operating under the AS.

Another example of an autonomous system is the *Intermediate System-to-Intermediate System (IS-IS)* routing protocol. This routing protocol is used for large networks like that of an internet service provider. The *Border Gateway Protocol (BGP)* is another good example of an autonomous system. The BGP is meant to link other autonomous system and large networks managed by internet service providers.

OSPF Routing Tables

Similar to the EIGRP, OSPF manages a *neighbor table* and a *routing table*. The only difference is that EIGRP has a *topology table* whereas the OSPF has a *link-state table*.

> ***Link-State Table:*** This table manages the connections between the router and neighboring router by measuring the stability of each of these connections. Simply, it observes the quality of routes to neighboring routers.

Characteristics of OSPF

1. As in EIGRP, route updates are only transmitted when OSPF has detected any change in the routes.
2. When the OSPF does detect changes, the router automatically transmits a *link-state advertisement (LSA)* in one of the routes whose properties are stored in the *routing table*. Only information about the changes in one of the routes is contained in the LSA.

- LSA packets leave almost no network footprint or trace.
- LSA traffic is kept at a minimum because OSPF keeps an inventory of routes.
- LSA traffic is organized in such a way that LSA packets reach the destination router immediately.

3. Routers shares CKA/ Hello messages with each other as they establish the values in each of their *neighbor tables* while undergoing the convergence process.
4. Unlike EIGRP, which is a Cisco-proprietary protocol, OSPF is supported by other router manufacturers.
5. OSPF converges fast compared to other protocols (except EIGRP).
6. OSPF works efficiently because it divides the system (routing domain) into different sectors of control.
7. Limitless amount of network hops are supported by the OSPF.
8. Variable-length subnet masking (VLSM) is supported by the OSPF.
9. OSPF organizes and reads routers in a hierarchical format.

Technet24.ir

Convergence

During the convergence process, the routers exchange pleasantries by sharing network parameters before storing received data to each of their *neighbor table*. There is no need to discuss in great detail how routers recognize each other as neighbors since *convergence* in OSPF is exactly the same with *convergence* in EIGRP.

Cost Metric

To measure the value of the connections established by each route, the OSPF employs a cost metric.

Route cost is a metric that determines the value of each connection by its bandwidth. By dividing the default 100Mbps or roughly, a million bits per second) bandwidth with the measured bandwidth of the connection.

For example, if the router measured the actual bandwidth as:

10 Gbps (10,000,000,000 bps)	100,000,000 bps / 10,000,000,000 bps	0.01
1 Gbps (1,000,000,000 bps)	100,000,000 bps / 1,000,000,000 bps	0.1
100 Mbps (100,000,000 bps)	100,000,000 bps / 100,000,000 bps	1
10 Mbps (10,000,000 bps)	100,000,000 bps / 10,000,000 bps	10
1 Mbps (10,000,000 bps)	100,000,000 bps / 1,000,000 bps	100

The faster the bandwidth of the connection, the lower the route cost. OSPF is designed to compute for least cost and use it for sending packets.

In the above example, the default reference bandwidth is pegged at 100 Mbps but using the Cisco IOS interface, you can change this reference value by using this code:

```
auto-cost reference bandwidth
```

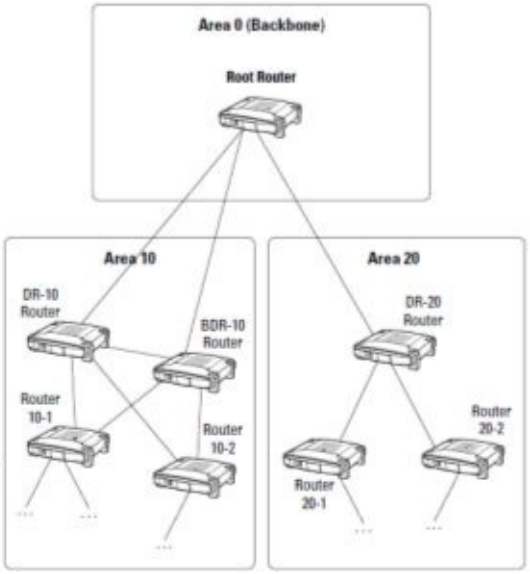
This is handy when using high-powered machines that transmit data packets in high-speeds. Instead of using 100 Mbps as reference, you can set it to 10 Gbps by

Technet24.ir

implementing the following command codes:

```
RT51-2> en
RT51-2 #config t
RT51-2(config) #auto-cost reference-bandwidth
10000000000
RT51-2(config) #exit
RT51-2 #disable
```

RT51-2>



OSPF Hierarchy

The OSPF employs a special routing algorithm that determines the shortest path between the origin point (router) and the destination point (neighbor router). This special algorithm is called the Djikstra routing algorithm.

The Djikstra algorithm in a router sees the origin router as a root router. The algorithm assigns areas where there is at a single *designated router (DR)*. Ideally however, a *backup designated router (BDR)* is also assigned.

Photo: OSPF Credit: routerprotocol.net

Refer to the figure on the left. Since DR-10 Router is nearer vis-à-vis other routers, it is designated as the designated router for Area 10. The same can be said for DR-20 router, which is the designated router for Area 20. In other words, if the root router intends to send a data packet to Router 10-1, it will first assess if the shorter route (DR-10) is available. If it is, then it sends the data packet through DR-10 en route to DR 10-1.

Technet24.ir

Selecting a Designated Router (DR)

The computations made by the *OSPF priority algorithm* determine the designated router. The algorithm produces a value within the range of 0 ANS 225 is integrated to the IOS interface by running:

```
ipospf priority value
```

The default value of the OSPF is 1. The router assigned with the highest OSPF priority value becomes the designated router. In the remote instance that two routers are assigned with the same OPSF priority value, the tie will be broken by using the *router ID (RID)*.

Using the following methods, users can choose which router should be assigned as a designated router by:

- *OSPF Priority:* Set the highest priority value for both the interface and the router.
- *Lookback Interfaces:* In each router, the user can create an effective lookback interface and set the highest IP address to one of the routers intended to be designated router.

Router ID (RID)

This is the IP address generated to serve as an identifier of the router. It is set by employing the following methods:

- Using the command router-id in the Cisco IOS interface
- Manually by:
- Assigning a high IP address to the router's loopback interface
- Assigning a high IP address in the router's active interface

Configuring the OSPF

The steps to configure the OSPF on any Cisco Routers are very similar to how both EIGRP and RIP can be configured. It is accomplished by:

1. ***Starting up the OSPF***

   In the global configuration mode, this command can be run in the Cisco IOS interface:

   ```
   router ospf pro_id
   ```

   The variable `pro_id` is assigned a number within the range of 1 and 65536. This number serves as an identifier of the protocol's routing process that exchanges information with other routers through the OSPF.

2. ***Enable OSPF on the interface***

   Using the Cisco IOS interface, OSPF is enabled by implementing this command code:

   ```
   network idt_IP IP_mask area area_idt
   ```

`idt_IP`	This assigns the IP address that will serve as the main identifier of the system interface where OSPF will be enabled.
`IP_mask`	This portion determines which of the IP addresses listed on the neighboring tables belong to the network.
`area area_idt`	This defines the extent by with the OSPF can operate.

The *IP mask* or *wildcard mask* are in essence simply *bit masks*. A bit mask is a combination of numbers 1 or 0 and is hence, following the binary system. In the OSPF, *bit masks* have the following significance:

`1`	Any number can be assigned to the matching bit in the IP address.
`0`	Exact number should be the same as that of the matching bit in the IP address.

Consider the IP address in its entirety. It is divided into four numbers or into 4 bytes with each byte containing 8 bits. The wildcards can be set as any number within the range of 0.0.0.0 and 255.255.255.255. These decimal numbers have the following significance:

255	Any number can be assigned to the matching bit in the IP address. When converted to the binary system, 255 is equivalent to a series of eight 0s.
0	Exact number should be the same as that of the matching bit in the IP address. When converted to the binary system, 255 is equivalent to a series of eight 1s.

If let's say the command code implemented in the Cisco IOS interface begins with the following IP address combination: 192.167.25.0 0.0.0.0 then only routers with IP address 192.167.25.0 are exposed. If, however, the IP address combination is 192.167.25.0 – 0.0.0.255 then all the routers that begin with 192.167.25 as an IP address will be exposed.

Here is the corresponding IP address for each of the Cisco router:

Router 10-1	172.10.78.0
Router 10-2	172.10.77.0
Router DR-10	172.10.75.0
Router BDR-10	172.10.76.0

Consider the following command configuration for *Router 10-1*:

```
R10-1 >en
R10-1 #config t
R10-1 (config) #router ospf 1
R10-1 (config-router) #network 172.10.78.0 0.0.0.255
    area 20
R10-1 (config-router) #network 172.10.78.0 0.0.15.255
    area 10
R10-1 (config-router) #exit
R10-1 (config) #exit
R10-1 #disable
R10-1 >
```

The above command configuration of router 10-1 affects the interface for both area 20 and area 10 by:

Technet24.ir

Area 20	Router 10-1 exposes to all routers within area 20 any routers assigned with the IP space 172.10.78 within the network with the same IP address 172.10.78
Area 10	Router 10-1 exposes to all routers within area 10 any routers whose IP begins with 172.10.7 only. Simply, the IP address can be 172.10.75 to 172.10.78.

OSPF Protocol Configuration

To display the current settings of the IP routing protocols, the following command can be keyed in to the IOS interface:

```
show ip protocols
```

The interface will display the following information:

- OSPF process identification
- Whether or not inbound update response filter is fixed
- Whether or not outbound update response filter is fixed
- Router Identification (RID)
- Current virtual distance between routers
- Sources of LSA sockets
- Number of active areas reached by the implemented command
- Reference bandwidth (for determining the route costs)
- List of OSPF and IP network areas listed for routing OSPF.

Technet24.ir

Pertinent Commands

When reviewing for the CCNA certification, you will find the following commands (not already mentioned in the previous section of this chapter) handy:

`show ip ospf interface`	This is used to inspect the current IP configuration of the OSPF protocol. • If the command is implemented in a specific interface, the interface will only display information pertaining to the said interface. • If this is not the case, then the command will display a comprehensive list of information pertaining to each interface powered by OSPF.
`ip ospf neighbor`	This displays information about OSPF information of neighbor routers.
`show ip ospf database`	This inspects the data held by the routing tables of the OSPF protocol. The command not only displays information about routers within the same network, it also displays the status of each connection from the root router.
`debug ip ospf`	This command code is use to troubleshoot any noticeable routing malfunctions.
`no debug ip ospf`	This command disables the debugging capabilities of OSPF.

Technet24.ir

Part 2
Switching with CISCO Switches

Technet24.ir

Chapter 6. Layer 2 Switches

If *Layer 3* is the *network layer*, were routers transmit data packets to other routers, *Layer 2* is the *data link layer* in networks that follow the TCP/IP or Open Systems Interconnection (OSI) model.

Layer 2 is responsible for sending data to physical devices. Each device is assigned with its own physical address recognized by the network to route data packets from one device to another. Otherwise called as Media Access Control (MAC) addresses, the physical addresses act as a unique identifier to specific network devices.

The features of the data link layer are as follows:

1. Communicates with the network layer to liaise the receipt of data packets from the source host
2. Assembles the received packets inside a *data frame* with the MAC address (local routing information).
3. Transmits the packaged *data frame* to the physical layer, which will then break down the code to specific optical and electrical signal.

The physical layer (comprised mainly by the physical device) transmits the codes inside the data frame through wired connection or wireless sending.

Within the receiving module, Layer 2 initiates the following:

1. Opens the data frame
2. Acquires the data packet from the data frame
3. Transmits the data packet to the network layer

For data link procedures, the TCP/IP (Ethernet) protocol is used at the data link layer. According to the standards prescribed by the IEEE802.X, the Ethernet manages the TCP/IP operations in Layer 2.

The main role of the data link layer is to manage the transmission of data frames locally between two physical devices bound together by the Local Access Network (LAN).

For a better understanding about how Layer 2 switches work, consider the following:

- Earlier LAN implementations used a coaxial cable to connect computers together.
- The bandwidth is spread and shared within the different devices connected to

the LAN.

- Due to the shared bandwidth, all data packets are shared to all devices connected to the LAN instead.

For example, there are four computer users — Matt, Mark, Joe, and Lucas — connected to a network. If a data packet is sent to Matt, the other users see the packet too. Not only does this undermine privacy of the content of said packet, Mark, Joe and Lucas need to delete the data packet because it is not addressed to them. Every time at least one of them receives a data packet, the rest would have to delete the packet on a regular basis. Not only is this bothersome; it is also inefficient.

Hubs

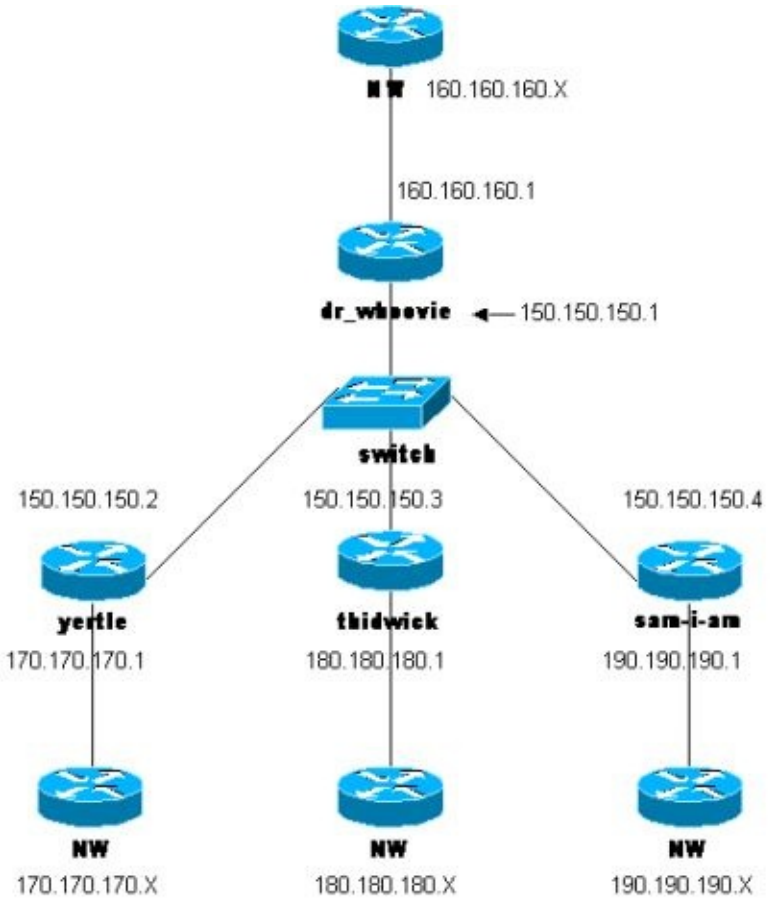
Having realized this problem, *hubs* were later introduced to integrate computer devices together using a single cable per device. Instead of coaxial cables, computer hubs use twisted-pair cables. RJ-45 connectors are used at end of cables to simplify connection.

RJ45 (rj-group.com)

When data frames are sent to a hub, they are transmitted to all host computers connected to the hub with the exception of the source device. Simply, the mechanism of the hub sends the data to all inbound ports except from where the data frame originated.

Since the data frames are being sent to different inbound ports while at the same time share the same bandwidth, there is a high possibility for data frames to collide. To completely devoid the network hub of data frame collisions, the Ethernet employs a special mechanism called Carrier Sense Multiple Access Collision Detect (CSMA/CD).

The CSMA/CF uses an algorithm that manages the transmission of data packets to the rest of the connected devices so that none of the transmitted packets will collide. This, however, consumes almost half of the bandwidth that could have been used for faster data transmission.



Hub (cisco.com)

The only way to circumvent the problem is to make the collision domain as little as possible. This is where Layer 2 bridges and switches come in.

Technet24.ir

Bridges

Bridges and hubs are both an interrelated computer devices connected in a LAN by means of a wired connection between each device. The only difference between bridges and hubs is that the former was able to keep the collision domain at a minimum.

Bridges and switches both create a single collision domain for every port. This causes data frames to be sent only through exit ports towards the frame destination.

Switches

Switches are a network device that creates a single collision domain for each port. This device transmits data frames via exit ports to reach the destination port of the computer host where the frames are intended to reach. Other characteristics of switches are as follows:

- *Switches are faster than routers*. Since switches operate at the data link layer (Layer 2), they don't have to check the packet header at the network layer (Layer 3). Switches only require information about the MAC address of both the source and destination of each data frame.
- *Switches are faster than bridges*. This is because switches use Application-specific Integrated Circuits (ASICs) hardware while bridges use software to fulfill their functions.

Using a switched network has several advantages:

- Switches provide a more efficient means to connect different hosts. This shortens the travel time from source host to destinations host.
- Switches prevent data frame collision by making sure that each of the hosts has its own collision domain.
- Switches check the MAC address configured in a data frame before sending it through the outbound part connected to the inbound port of the destination host. This makes sure that data frame is flooded to all the computer devices connected to the switched network.

Technet24.ir

Hubs vs. Bridges vs. Switches

	Features					
	Technology	**Duplex**	**Speed**	**VLAN Support**	**Collision Domain**	**Broadcast Domain**
Hubs	Port multiplexing	Half	Turtle	No	Whole hub	Whole Hub
Bridges	Software Switching	Half	Deer	No	1 per port	Whole Bridge
Switches	ASIC Switching	Full/ Half	Cheetah	Yes	1 per VLAN	1 per VLAN

Switch Functions

The three (3) functions that Cisco Switches must accomplish are:

1. *List down the MAC addresses of each of the computer devices connected to the switched network*. This is accomplished by Layer 2 switches through the following:

a. The switch examines every data frame received by the switched network. It takes note of the number of the entry port and the MAC address inscribed in the data frame. These pieces of information are then stored in the MAC address table.

b. The switch gradually forms a comprehensive MAC address table that will be used as reference for future data frame transmissions.

2. *Manage the data frames from each of the outbound ports (source host) or source switches to the inbound port (destination host) or destination switches*. Layer 2 switches decide where to send the data frames by determining which inbound port to send the data frame. This is of course dependent on the MAC address information that came with the received data frame. Switches then access the MAC address table to do the following:

a. The switch examines the data frame upon entering the network's inbound port. It checks the MAC address of the source and destination host carried by the data frame.

b. Using the information gathered from the data frame, it then looks at all the entries in the MAC address table.

- If the information from the data frame checks out with any of the entries in the MAC address table, the switch cascades the data frame to the inbound port of the destination host bearing the same MAC address inscribed in the data frame.
- If the information does not check out, it cascades the data frame to all outbound port of the network with the exception of the port where the data frame came in.

3. *Make sure that no loops are created within the switched network*. Data-link frames do not cease to exist until the frames find their corresponding destination host. In other words, if a frame is sent but coded with an unknown MAC address, the frame can spring from one port to another, non-stop within the network. This is not good because bandwidth consumption is also non-stop. In order to avoid this, a protocol called *Spanning Tree Protocol (STP)* is used in the system.

Glossary of Terms (Switching)

1. ***Address Learning:*** This phase is when the Layer 2 switch gathers the MAC address of the receiving port of each computer host. The switch forms a MAC address table consisting of the list of all the port numbers and their corresponding MAC address.

2. ***Forwarding:*** This phase is when the Layer 2 switch decides to transmit the data frame to an inbound port of one of the computer host within the switched network provided that the MAC address of the computer host match the MAC address contained in the data frame.

3. ***Filtering:*** This phase is when the Layer 2 switch decides to discard the data frame and all of its contents without sending it to any of the outbound ports.

4. ***Flooding:*** This phase is when the Layer 2 switch decides to transmit the data frame to all outbound ports except from the port where the data frame came in.

5. ***Loop Avoidance:*** By using the Spanning Tree Protocol, redundant transmission loops are discarded.

6. ***MAC Address Table Thrashing:*** These are different ports bearing the same MAC Address. When this happens, the switch doesn't know which inbound port the data frame should be sent.

7. ***Broadcast Storm:*** This happens when the data frame contains the MAC address of an unknown port. The data frame is then sent across interconnected switches wasting the bandwidth and thus, crashing the MAC address table.

8. ***Unicast Transmission:*** This involves a device transmitting a data frame to a singular destination device.

9. ***Multicast Transmission:*** This involves a device transmitting a data frame to multiple destination devices.

10. ***Broadcast Transmission:*** This involves a device transmitting a data frame to all devices within the local network.

Chapter 7. Switch Management

Since most GUI tools and IOS commands are the same for both Cisco routers and Cisco switches, handling Cisco switches is very much alike handling Cisco routers. One of the only noticeable differences between handling said Cisco devices is some tools exclusive for routers and some tools exclusive for switches. For example, Cisco Device Manager is only available for managing Cisco switches.

Handling Methods for Cisco Switches

Since the *data-link layer* is divided to three sublayers: *core layer*, *access layer* and the *distribution layer*, it will always come in handy to remember which switches are a perfect fit for which layer.

Cisco Switch	***Best Suited for***
Entry-level Switch	Access Layer and Distribution Layer
Midrange Switch	Access Layer and Distribution Layer
Top-of-the-line Switch	Core Layer and Distribution Layer

Notice that if we go back to the chapter that talks about Router Management *(Part 2, Chapter 9)*, you'll notice that the hierarchy of switches is the same as the hierarchy of routers.

Highly-specific functions are handled by *top-of-the-line switches*. These functions include:

- LAN gateway connectivity
- Inter-VLAN routing
- VLAN Trunking Protocol (VTP) domain control
- VLAM Membership Policy Server (VMPS)
- STP root bridge role

Since the above functions are crucial in the network, these functions must be managed by a very efficient switch device.

Connecting to a Cisco Switch

Similar to Cisco Routers, Cisco does not have a specialized hardware that allows direct user contact. Cisco switches can be leveraged to a computer panel where the Cisco Switch interface is setup. This way, Cisco switches can be maintained by either connecting remotely or connecting locally from a computer host to the switch.

Local Connection:

Cisco switches are typically built with multiple ports used to link network devices or computer hosts. Two of these ports are colored differently than the rest. These two ports are console and auxiliary ports. Both of these ports serve a different purpose other than ensuring a stable network connection.

Console Port

Using a rollover cable, this port is used to link the switch and the computer host together. The console port is used when establishing a local connection to the switch device. Having a *Console facility* is common to all Cisco devices controlled by Ciscio IOS. This facility acts as an interface that displays user prompts, diagnostic messages, error messages and status messages.

The management computer requires terminal emulation software installed before the computer and the switch can communicate with each other. Terminal emulation is supported by the following applications:

- HyperTerminal
- SecureCRT
- TeraTerm

Cisco switches need the following serial parameters setup in the Cisco Switch's connection profile:

- Data bits: 8
- Stop bits: 1
- Flow control: none
- Parity: none
- Baud rate: 9600

The above parameters control serial communications between switches by using communication ports like COM1, COM2, and COM3.

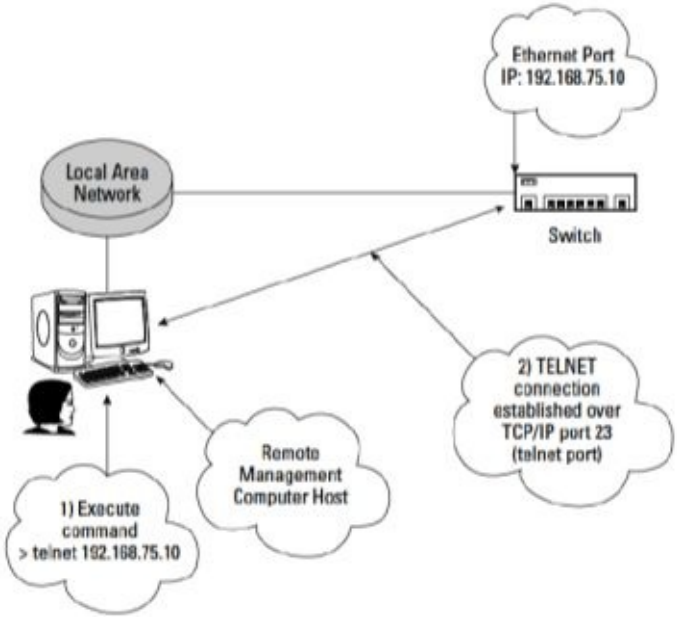
Auxiliary Ports

These are ports whose main role is to connect the switch to the management host through the rollover cable like that of the console port. The only difference is that this port is used to establish a local connection between the modem and the computer. The next step is to tweak the settings of the modem so that it can receive calls coming from the host computer through the telephone cable.

Establishing a Remote Connection

The common network environment often involves more than one switches. More often than not, these switches are located in different areas. A network set-up like this requires remote connection to the switches. The remote management host allows a working connection between a computer and the switch console. This remote connection is established via any of the following:

- Modem connection via the switch's auxiliary port
- Using a secured Telnet software that connections the switch's network IP address.
- Using a Console Terminal Server that connects the switch's console IP address



Console Terminal Server (cisco.com)

Switch Startup Procedure

Regardless of configured setting, the Cisco switch always performs the same process when turned on:

1. **The Cisco switch executes the *Power-on Self-Test (POST)*.** Stored in the Cisco Switch's ROM, the POST is a microprogram that determines whether the switch is in mint condition and can thus perform basic functions required of the switch's hardware.
2. **The switch then executes the boot loader software (also otherwise**

known as the *bootstrap program*). The boot loader is another microprogram stored in the switch's ROM that is designed to transition the switch to regular operation mode by accessing the IOS interface in the flash memory. If the IOS interface is not in the flash memory, the boot loader will attempt to load the interface from the

- ROM
- TFTP Server

3. **The Cisco Switch interface starts into the RAM.** The bootstrap program starts to power up the RX-boot image from the ROM. The RX-boot image is necessary to jumpstart the boot process.
4. **Begin the startup configuration.** After the switch interface gathered enough information from the RAM, the IOS then prepares the device to begin the configuration process in the NVRAM. Once the configuration process started in RAM, the configuration process is now called the *running configuration*. This configuration process adapts to the network settings while the Cisco switch is running.

The IOS configuration interface allows the user to change the following settings in the switches:

- IP address
- Telnet password
- Host name
- Console password
- Subnet mask
- Default gateway

Cisco Switch Configuration

All Cisco switch packages contain the following items:

- Switch Device
- AC power cable
- Rollover Cable
- Getting Started compact disc
- Mounting brackets

There is no default configuration integrated in the new Cisco switch. It is however designed to connect to the computer host via local connection even without a default configuration.

Startup configurations are only required when the switch is connected to a different switch or to a network gateway to establish remote connection with other network.

Cisco switches turns into setup mode when it does not detect any configuration stored in the NVRAM. The switch runs Setup mode during any of these two occasions:

- The switch is powered on for the first time after taking it out from the box.
- The initial configuration is erased from the NVRAM. The two ways to delete the configuration is by pressing the Mode button for ten seconds to initiate the reset process in the switch or by simply deleting the configuration from the IOS interface.

A new configuration setup can be created through any of the following methods:

- Cisco IOS interface commands
- Initial Configuration dialog
- Switch to Auto-install setting
- Express Setup Web form

Express Setup Mode

Only found in Cisco switches, the *Express Setup* utility lets users to configure the switch. It will require the supplication of the following settings:

- IP address
- Telnet password
- Host name
- Console password
- Subnet mask
- Default gateway

To setup the Express Setup mode manually through the switch, press the Mode button and hold it for 3 to 5 seconds or until all the LED indicators turned green. Using the IOS interface, locate the IP address of the switch.

If the switch does not have a startup configuration, setup mode can be avoided through any of the following methods:

- Abort the setup mode by using the shortcut key for paste: Ctrl + C
- If the setup dialog box inquires if you desire to change the setting of the switch, click “No”.

- If the setup dialog box inquires if you want to save the configuration, click "No".

Naming the Switch

The switch can be named using the Cisco IOS command: `hostname`. The names of the switches must be changed to avoid confusion when manually configuring only a select of the switches in operation. This helps identify which switches are which.

The following commands can be implemented in the IOS interface:

```
Switch > en
Switch #config t
Switch(config) #hostname switch001
switch001(config) #exit
switch001 #disable
switch001>
```

Setting the Main IP Address for the Switch

Similar to how the main IP address is set in a router, the Cisco IOS commands `ip default-gateway` and `ip address` are used to build the IP gateway and IP address of the switch. This method establishes a remote connection to the switch using both *HTTP* and *Telnet*. To adjust the current settings of the management IP and default gateway of the switch, the following command code can be implemented:

```
switch001 > en
switch001 #config t
switch001 (config) #int vlan2
switch001 (config-if) #ip address 192.168.71.22
255.255.255.255.0
switch001 (config-if) #no shutdown
switch001 (config) #ip default0gateway 192.168.71.12
switch001 (config) #exit
switch001 (config-if) #exit
switch001 #disable
switch001 >
```

Password Configuration

Switch credentials can be changed by configuring Cisco IOS commands by entering credential values to `password` and `login` variables. The concept of password configuration is similar for both Cisco routers and switches. For instance, Cisco switches can also set three kinds of password:

- Console Password
- Auxiliary Password
- VTY Lines Password
- Privileged Password

Check their definitions on *page 14 (Router Management)*.

Even if there is no password configured for both console and auxiliary ports, they are enabled by default. As in Cisco routers, the lack of password configured for the two ports is a threat to the security of the Cisco switches and all bits of information that pass through it.

The following command is also used to configure the Switch password:

```
switch001 > en
switch001 #configure t
switch001 (config)#line cons 0)
switch001 (config-line) #password y1csco
switch001 (config-line) #login
switch001 (config-line) #exit
switch001 (config) #exit
switch001 #disable
switch001 >
```

Simply, the above command block sets the password of the Cisco switch to `y1csco`. This section will not discuss in detail each portion of the code block as they are already discussed in Router Management (*page 15*)

Setting-Up Switch Banners

Switch banners are a short text display that is projected in the computer screen whenever the host has just logged into the Switch network. Setting-up banners in Cisco switches are similar with setting-up banners in Cisco routers. The four different types of banners that Cisco can likewise display are:

- EXEC process creation banner
- Message of the Day (MOTD) banner

- Incoming terminal connection banner
- Login banner

The description is the same as it is in Cisco routers. (See page 16)

The following command can be implemented to setup an MOTD banner on every router connections:

```
switch001 > en
switch001 #config t
switch001 (config) #banner motd /

Enter TEXT message. End with character '&'.

$This switch is owned and managed by enterprise.info. If
you are not connected to said company, please log off
the network
&

sitch001 (config)#
```

As in Cisco routers, Cisco switches considers the text between the "$" and the "&".

Resetting Cisco Switches

Again, similar to Cisco Routers, switches activate setup mode if its processor does not detect an initial configuration. This happens when the settings of the switch is reset. To delete the current configuration, perform the following functions:

1. Press and hold the Mode button in the switch for a few seconds. Release only when all the LED stops blinking.
2. By the time the LED stops blinking, the router is ready to reboot its system.

If you need to access a specific configuration (IOS image) file that is stored in the flash memory (instead of the device's NVRAM), implement the following command lines:

```
switch001 > en
Password: y1csco
switch001 #config ter
switch001 (config) #
switch001 (config) #boot system flash:/c1440-
```

```
    enterprise.info-mz.121-32.ES
switch001 (config) #exit
switch001 #disable
switch001 >
```

The above commands let you access the image file stored in this address:

```
flash:/c1440-enterprise.info-mz.121-32.ES
```

Auxiliary Password

Cisco switchers and routers alike have auxiliary ports. To configure a password for auxiliary ports, the following command lines can be implemented in the system:

```
switch001 > en
switch001 #config t
switch001 (config) #line aux 1
switch001 (config-line) #password auxycsco1
switch001 (config-line) #login
switch001 (config-line) #exit
switch001 (config) #exit
switch001 #disable
switch001 >
```

Privileged Password

Passwords can only be set so that only specific users can access specific functions disposed of by a Cisco switch.

```
switch001 > en
switch001 # config t)
switch001 (config) #enable secret cryptycssco1
switch001 (config) #exit
switch001 #disable
switch001 >
```

Recovering Lost Password

As in Cisco routers, Cisco's `password-recovery` feature should have been enabled before the password can be retrieved. If the feature is enabled, the following steps can be used:

Technet24.ir

1. When the switch begins to reboot, attempt to interfere with the system through any of the means enumerated in the previous sections.
2. Using the Cisco IOS Interface, access the file manually.
3. Hide the default configuration file to prevent the switch processors from accessing it.
4. Manually reboot the switch.
5. Unhide the default configuration file.
6. Relocate the configuration file from NVRAM to the flash memory.
7. Change the password.
8. Save the current configuration file.
9. Restart the switch.

Chapter 8. Network Traffic Management

Cisco Switches manages the traffic within the local-area network. The host devices tasked to send a data packet communicates first with the switch and the router before they transmit frame to a target computer device connected to a remote network. Most of the time, data transmission involves devices that are not connected on the same local network. Even before the data packet is sent to the destination network, it should first be transmitted to the LAN gateway. The LAN gateway then chooses then transmits the data packet to the wide-area network (WAN) until the packet reaches the destination local network.

Sending data packets in the same LAN: The MAC address of the destination host device is configured as the destination MAC address of the data packet.

Sending data packets to a different network: The MAC address of the LAN gateway is configured as the destination MAC address of the data frame. The LAN gateway routes the data packet to the WAN.

Switching Modes

Upon receipt of data frames, the switch decides what must be done to the data packets inside the frame. The three things that most Cisco switches do to the frame they receive are:

- Transmit the frame to the destination port
- Transmit the frame to all the ports (with that exception of the port the frame used to get in)
- Discards or filters the frame

The three switching modes supported by Layer 2 switches are:

1. ***Store-and-forward:*** This switching mode performs these steps:
   1. 1.1. The entire data frame is stored inside the switch's temporary memory.
   2. 1.2. The switch implements the frame check sequence (FMS) to make sure that the contents of the frame is valid.
   3. 1.3. The switch checks the MAC address of the source and destination of the data frame.
   4. 1.4. The switch remembers the MAC address of the source of the data frame in the same row as the incoming port. This information is then stored in the MAC address table.
   5. 1.5. In determining the destination MAC address, the switch then checks the MAC address table:

- If the MAC address table contains the destination MAC address, the switch transmits the data frame only on the outbound port described in the MAC address table.
- If the MAC address table does not contain the destination MAC address, the switch sends the data frame on all outbound ports with the exception of where the data frame went in.

2. ***Cut-Through:*** This switching mode is several times faster than the previous mode. The switch does not save the whole frame within its buffer memory. This mode manages the data frame immediately upon receipt of the first six bytes of the data packet:
   - 2.1. The switch immediately checks the first 6 bytes of the destination MAC address.
   - 2.2. The switch then compares the 6 bytes to the data entry listed in the MAC address table to compose a list of possible matches.

2.3. Once it finds a compatible match among the entries listed in the MAC address table, the switch automatically sends the data frame to the appropriate outbound even before the data frame has finished loading up in the inbound port of the switch.

This switching method does not compute for the FCS before it proceeds to transmit the data frame. The only downside of this switching method is that the switch does not filter the data frame to determine whether the frame is valid or not. This might cause traffic congestion in the network.

3. ***Fragment-Free:*** This switching mode is like a hybrid of the two previous switching modes. It combines the best features of both switching modes. This mode knows that valid frames have a size of at least 64 bytes. Fragment-free mode checks bit size and deems all data frames that have at least 64 bytes as a valid frame. In this mode, the switch does the following:

3.1. Upon receipt of the frame, this device saves the initial 64 bytes of the data frame in the switch's temporary memory module.

3.2. The switch inspects the MAC address of both the source and the destination of the MAC address inscribed in the received frame.

3.3. The switch then records the MAC address of the source and the corresponding inbound port where the data frame came in to the MAC address table.

3.4. The switch counterchecks the MAC address of the destination to the entries in the MAC address table.

- If the MAC address table contains the destination MAC address, the switch transmits the data frame only on the outbound port described in the MAC address table.
- If the MAC address table does not contain the destination MAC address, the switch sends the data frame on all outbound ports with the exception of where the data frame went in.

This switching mode transmit the frame as soon as it has received the first 64 bytes of the data frame has been received. Just like cut-through, fragment free switching mode does not compute for the FCS. Just like store-and-forward switching mode, fragment free mode prevents the switch from transmitting invalid data frames.

- Store-and-forward is slower because it calculates for the FCS but it is reliable because it calculates the FCS.
- Cut-through is faster because it does not need to hold the whole data frame and calculate the FCS but it is less reliable because forwards all frame regardless if they are valid or not.

Technet24.ir

- Fragment-free is not as fast as cut-through switching mode but it is faster than store-and-forward because fragment-free switching mode only checks the first 64 bytes. It also does not calculate the FCS.
- Invalid fames are typically smaller than the usual 64 bytes.
- Fragment-free switching modes only consider the first 64 bytes, making it faster and more efficient than store-and-forward.

Chapter 9. Spanning Tree Protocol (STP)

Switches are often interconnected with each other through self-repeating links that help ensure the integrity of inter-switch connections. The only downside of these self-repeating links is that they often lead to dangerous transmission loops that trashes the table containing MAC addresses and causes broadcast errors. Due to this, switches must find a way to avoid transmission loops. This is where *Spanning Tree Protocol (STP)* comes into play.

Self-repeating links that connects data-link switches together causes data frames to be sent repeatedly through the Layer 2 switches. Similar to data frames in Layer 3 networks, data-link frames does not die on its own when they are configured with a MAC address of an inexistent switch. Without switching protocols in place, frames like these just tend to bounce forever from one switch to another. This leads to bandwidth wastage.

Technet24.ir

Problems caused by Transmission Loops:

Transmission loops in the data-link layer often lead to the following:

1. ***Thrashing of the MAC Address Table:*** The integrity of the information reported and organized in the MAC address table is compromised whenever transmission loops occur. This is caused by different ports bundled together with similar MAC address. This causes confusion because the switch is unable to determine which exit port to access.

2. ***Broadcast Errors:*** Otherwise known as *broadcast storms,* broadcast errors happen when frames bounce non-stop to interconnected switch.

Spanning Tree Protocol

Spanning Tree Protocol closely monitors the network and organizes every established connection, especially self-repeating links. After compiling pertinent information about the switching network, STP disables self-repeating links, establishing optimized connections in-between switches.

- Under normal situations, optimized connections are enabled.
- If any of the optimized connections fail, STP picks randomly one of the less-preferred self-repeating links and enables it.

STP performs the above steps by assigning a *root bridge* or a switch that will take the role of the decision maker for the network. The root bridge also communicates with *nonroot bridges* or other switches connected to the LAN.

- ***Root bridge:*** This switch discriminates which routes should be used and which routes shouldn't be used.
- ***Nonroot bridge:*** This switch assists the root bridge in determining which routes between the root and nonroot bridges are preferred and which routes are not preferred.

The Spanning Tree Protocol implements three main operations to maintain a stable LAN connection:

1. ***Picking the STP Root Bridge:*** The root bridge is selected by determining which among the switch connected in the LAN has the lowest *bridge ID*.
2. ***Allocating roles for STP port types:*** Port types define the behavior or the roles played by the ports found in all the switches connected in the LAN. STP allocates specific roles for each of the ports in the switch for smooth connectivity.
3. ***Attaining STP convergence:*** The proper assignment of port types often leads to STP convergence. Once the ports are all properly set-up, the STP achieves a steady and loop-free network connectivity.

Assigning STP Port Types

STP organizes ports based on the roles assigned to the ports during the initial configuration of the STP. Role assignments are based on the Ethernet bandwidth cost computed by the distance from the root switch to any of the immediate nonroot switches.

As mentioned in the previous chapter, switches use self-repeating links that adds to the bandwidth limit of a particular path. These links provide additional options, if in case a single connection fails. These links are lumped together to a cluster called connection path. Each of these paths is associated with a bandwidth cost, computed by the STP before it chooses which path it will use to transmit data frames. The list of cost is as follows:

Bandwidth	***STP Cost Factor***
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

As you may have noticed, faster bandwidths are assigned with smaller STP cost factor when STP computes for path cost. This is because STP prefers faster bandwidths. A 10 Gbps path is obviously faster than a 1 Gbps, STP hence deems it efficient for data frames to travel at 10 Gbps than 1 Gbps because it saves time by 1/10 of a second.

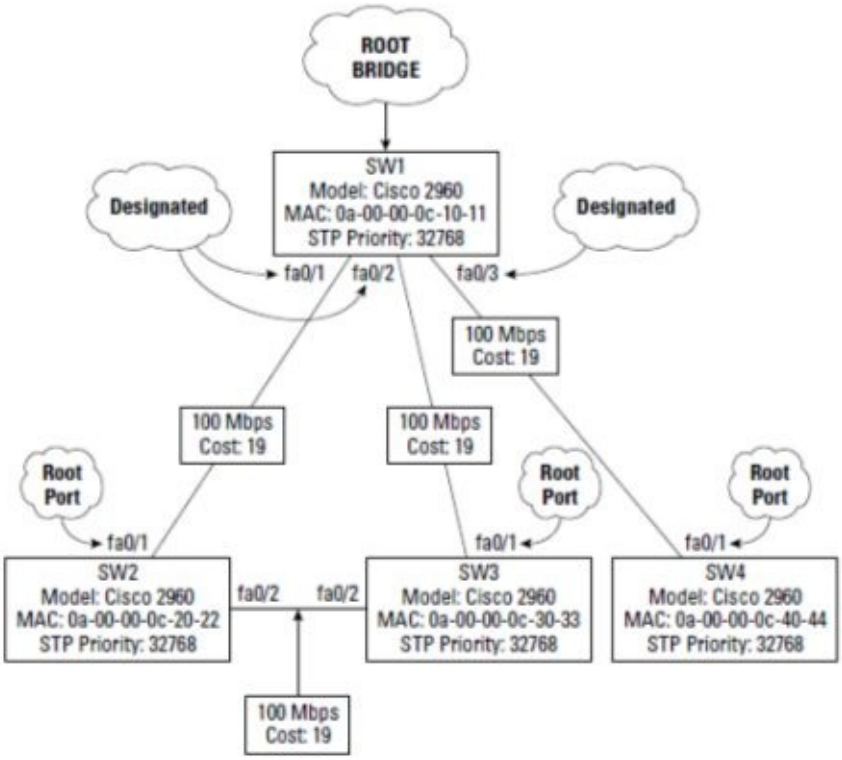
Spanning Root Protocol then reassigns 1 Gbps path as simply a *root port* or a secondary connection to the preferred path. Consequently, it also reassigns 100 MBps and 10 Mbps paths as a *designated port* and a *blocking port* respectively.

Root Ports

Once the STP has computed for and assigned a *root bridge* or the main path, the switch will use when sending data frames within the data-link layer, the STP will then select the second least cost as the *root port*. This port provides connection between the switch and the STP-designated root bridge. The characteristics required of a root port are:

- A port that incurs the least STP cost en route to the root bridge
- A port that connects the root bridge and the nonroot switch directly.

Switches use the STP to communicate among each other while at the same time calculating the cost in between each path near the root bridge. The other switch adds the cost measured by their neighbor to come up with the total cost of the path options between the nonroot switches and the root bridge.



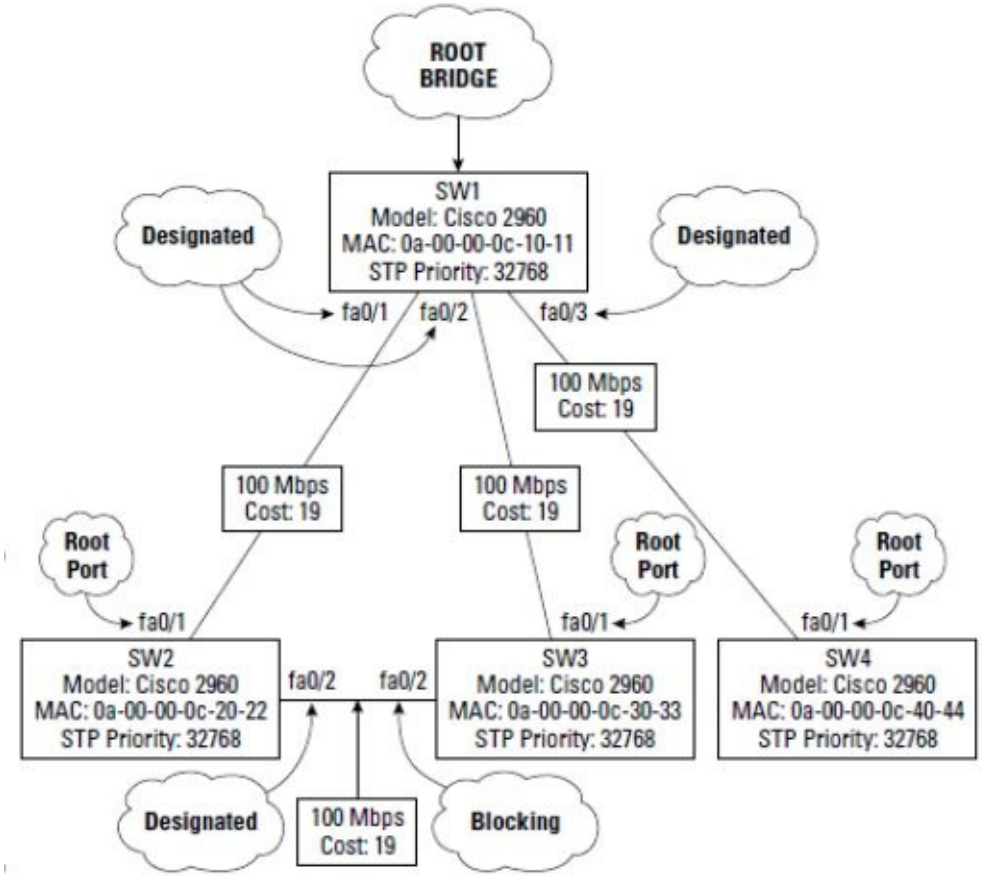
Root Ports (cisco.com)

Technet24.ir

Designated Ports

After the STP has assigned the root port for the switch, the other ports will be assigned to either act as a designated port or a blocking port.

- ***STP Designated Port:*** This port transmits received data-link frames in and out of the LAN.
- ***STP Blocking Port:*** This port does not transmit any of the data-link frames.



Designated and Blocking Ports (cisco.com)

Choosing Designated Ports based on STP Path Cost

The Spanning Route Protocol computes for the path cost between root bridges and nonroot switches. In the above diagram, when SW1 is tasked to send a data frame to SW2, it is presented with two choices: direct (fa0/1) and indirect path (fa0/2). Consider that the direct path only costs 19 to connect to SW2 whereas the indirect path costs 19 to get from SW1 to SW3, and then another 19 to get from SW3 to SW2. The total cost for the direct path is just 19 in contrast to the total cost of the indirect path as 38 (or a sum of 19 and 19). In this case, SW1 will choose the direct path towards SW2.

Take note that taking the direct path automatically means lest computed STP path cost. If let's say the path cost to get from SW1 to SW3 is just 2 and the cost from SW3 to SW2 is just 10 for a total of 12, then the indirect path now costs less compared to the direct path which costs 19.

Technet24.ir

Choosing Designated Ports based on Bridge ID

If the STP path cost is the same across all ports, the path with lowest Bridge ID assumes the role of the designated port or the root port.

STP Convergence

Once all the ports have been assigned with a specific role (forwarding or blocking) in the switch networks, the LAN is rid of loops. By building a catalogue of ports and their roles, the STP is able to stabilize the network despite the existence of looping links. A stabilized network is often referred to as the *converged network*.

Technet24.ir

Bridge Protocol Data Units (BPDUs)

BPDUs are unique data frames sent by switches to each other every 2 seconds. The information stored in the BPDU includes parameters that aid switches to choose a root bridge and decide which port will be assigned as either *designated* or *blocking*. These parameters include port IDs, bridge IDs and STP path costs.

Forward Delay	Hello Time	Maximum Age	Message Age	Port Identification	Bridge Identification	[illegible]

BPDU (stpcomputer.com)

STP Port States

STP manages the ports of switches by letting them assume any of these states:

Blocking ***Duration:*** 20 seconds *Max Age Timer*	Blocking ports are ports that are not allowed to forward data-link frames in the network. This port merely *listens* to the LAN. Blocking ports can receive and process BPDUs but it can transmit processed BPDU. Ports that are set to blocking state prevent the existence of transmission loops while STP converges the switch. A designated port can temporarily assume blocking state when the STP detects a network topology state notification (TCN) BPDU sent by neighboring routers. This prevents the creation of self-repeating links that can harm the network. The STP converges
Disabled ***Duration:*** For as long as the switch-administrator wills it to be disabled.	These ports have been manually disabled by the switch manager. These ports have no participation, direct or indirect, in the network activities. They are not part of the stabilizing process that STP performs to converge the network; thus, these ports unable to transmit or receive data frames.
Forwarding ***Duration:*** *Forever as long as the port is enabled.*	When a port dispenses forwarding function, it has become either a root port or a designated port. It can't be a blocking port for the reason that a port in a forwarding state should be able to transmit information. All ports currently in the forwarding state should be able to transmit or receive data frames.
Listening	Ports often undergo the listening

Technet24.ir

Duration: 15 seconds *Forward Delay Timer (Phase 1)*	phase in preparation for transmitting frames to other ports. This listening phase is named such because it listens to the BPDUs. Not every piece of information a listening port gets from listening to the network go to the MAC address table. The *forward delay timer* is made up of both the listening time (phase 1) and the learning time (phase 1). This also refers to the amount of time the port takes before it forwards a data frame to a different port.
Learning ***Duration:*** 15 seconds *Forward Delay Timer (Phase 2)*	The information gathered from the listening state is then recorded to the MAC address table. This phase is called the learning phase. These ports gather all pertinent information to help the switch dispense its functions effectively and efficiently. A port in the learning phase is not yet ready to forward data to other ports.

Exclusive Cisco STP Options

For some people, 50 seconds is still too long before the STP is able to converge the switch networks. Cisco, however, offers a solution for this concern. The following configuration can only be applied to Cisco routers to diminish dramatically the delay time before STP convergence:

1. ***PortFast:***

   This configuration option can be applied on ports whose participation is not a requirement of the STP. These ports are not part of the interconnection of hubs, bridges or switches. For instance, the singular link from the switch to the host device is unlikely to cause a switching loop; therefore, this link is not required to take part in the converging process by the STP.

   PortFast options turn off the STP protocol for the said link so that the link becomes active even before the STP convergence process is complete.

   To set the hypothetical interface fa0/1 interface using PostFast configuration, the following commands can be implemented:

```
switch001 > en
switch001 > config t
switch001 (config) >int fa0/1
switch001 (config-if-range) >spanning-tree portfast
```

2. ***BPDUGuard***

   This configuration option is used alongside the PortFast option when running the switches on the access layer. When the access layer is enabled, the PostFast option can cause potential harm to the network if it suddenly enabled links that interconnect switches together. Remember that the role of PostFast configuration is to disable STP on ports that are unlikely to create switching loops. Should a link be turned off accidentally, the exact opposite will be achieved: more loops will be created instead of avoided.

   The BPDU guard prevents this by turning the port into an error-disabled phase. The guard will then evaluate if PostFast option was correct to disable the STP of a particular link. If BPDU feels that PostFast erred in disposing of its functions, the concerned ports will generate an error message to alert the switch administrator of the mistake.

   To set the hypothetical interface fa0/1 interface using the BPDUGuard configuration, the following commands can be implemented:

```
switch001 > en
```

```
switch001 > config t
switch001 (config) >int fa0/1
switch001 (config-if-range) >spanning-tree bpduguard
    enable
```

3. ***BPDUFilter***

This option bars BPDU frames from getting through a port that has been determined by PostFast to be incapable of making transmission loops. If the BPDUFilter is disabled, the port will still receive BPDU frames incurring extra delay time. BPDU frames can only be used when STP is enabled hence it is not practical to still supply BPDU frames to ports where STP is already disabled.

To set the hypothetical interface fa0/1 interface with the BPDUFilter configuration, the following commands can be implemented:

```
switch001 > en
switch001 > config t
switch001 (config) >int fa0/1
switch001 (config-if-range) >spanning-tree
    bpdugfilter enable
```

4. ***UplinkFast***

This option decreases the time it takes for the STP convergence to finish by assigning a temporary backup root port within the switch. This allows the switch to switch ports immediately just in case the main root port fails.

To use UpLinkFast configuration, the following commands can be implemented:

```
switch001 > en
switch001 > config t
switch001 (config) >spanning-tree uplinkfast
```

5. ***BackboneFast***

This Cisco option lets the switch to automatically spot errors on links that are not directly connected to the switch. This error-detection configuration speeds up STP convergence.

To use Backbone Fast, the following commands can be implemented:

```
switch001 > en
```

```
switch001 > config t
switch001 (config) >spanning-tree backbonefast
```

Note that in both UpLinkFast and BackboneFast, the option is configured not on the particular link but on a specific switch. The above commands configured both configurations to `switch001`.

Technet24.ir

Chapter 10. Virtual Local Area Network (VLAN)

A Virtual Local Area Network (VLAN) is a collection of host devices and network resources depending on either the MAC addresses of the hosts or the role assigned by the ports in the system. A single VLAN can include more than one switch for as long as they belong to the same network.

Benefits of VLANs

The many upsides of creating a VLAN include:

1. ***Upgrade security***: Computer hosts or users can be assigned to manage each VLAN for close monitoring.
2. ***Upgrade network flexibility and management capability***: VLAN membership can be managed from a singular location even if the switches are located elsewhere if they are connected to the same network. *Inter-VLAN* and *VLAN Trunking Protocol (VTP)* allows switch managers to manage network resources with minimal effort.
3. ***Upgrade Network Efficiency and Usage*:** VLAN allows network managers to set which network resources are available to specific VLAN. This allows the network to conserve network resources.
4. ***Set a limit on the broadcast domain size*:** Probably the most important use of VLAN is to minimize the size of the broadcast domain. Subdividing the LAN into smaller logical VLAN will only require frames to be broadcasted on specific VLANs instead of the whole LAN.

Creating VLANs

To create a VLAN for a Cisco switch, the IOS command vlan must be used. The command should also assign a number to the VLAN. This number must be between 2 and 4094. Usually the VLAN is created based on the function it serves. Consider the block of code below:

```
Switch001 > en
Switch001 >config t
Switch001 (config) >vlan 2
Switch001 (config-vlan) >name Finance
Switch001 (config-vlan)>exit
Switch001 (config)>
```

The above code creates a VLAN called “Finance.”

Technet24.ir

Kinds of VLAN

- ***Static VLAN:*** Using the Cisco IOS command `switchport access vlan`, a specific port will be assigned to a specific VLAN. This creates a static VLAN. Otherwise called as the port-based VLAN, static VLANs are based on the ports, which the computer hosts latch on to establish a connection with the switch. This is perfect for small-scale networks. This kind of VLAN may need consistent manual port intervention, making it hard for wide-scale networks to adopt a static VLAN membership.
- ***Dynamic VLAN:*** The VLAN Membership Policy Server (VMPS) is enabled whenever dynamic VLAN is used. The VMPS maintains the MAC addresses of all linked devices and lists them down in a table. Each MAC addresses can then be assigned to a specific VLAN. Regardless of how your devices are connected in the network, the device will always be allocated to the right VLAN.

VLAN Trunking

This process lets the switches transmit VLAN data through various interswitch connections connected via a trunk ports. Trunk ports enable VLAN to extend its reach to more than just one switch.

Technet24.ir

EtherChannel

When using RTP, switch managers are always advised to enable EtherChannel for repeating interswitch connections. This process clusters redundant ports into one virtual trunk. Since this includes grouping several ports together, this process is also called *port trunking*. This process is called *link aggregation*.

As much as eight ports can be grouped together through the EtherChannel. The benefits of EtherChannel are:

1. ***Manage faults:*** EtherChannel is built to have a *fault tolerance* mechanism infused to it. Should a link or port start to show signs of failing, EtherChannel will resend data traffic to other operational ports.

2. ***Distribute load:*** Etherchannel is built with a load-balancing algorithms that distributes network traffic through other ports instead of concentrating on a single por.

3. ***Raise Bandwidth:*** When Etherchannel bundled up eight redundant ports together to a single virtual port, the bandwidth is increased by as much as the total bandwidth of each of the eight bundled up ports.

When Cisco developed the EtherChannel, at least two protocols are put in place and these are:

- ***Link Aggregation Control Protocol (LACP):*** This protocol uses IEEE 8023.3ad to control the EtherChannel. LACP is not exclusive to just Cisco switches. In fact, other brands can use LACP for their switches.

- ***Port Aggregation Protocol (PAgP):*** Unlike LACP, PAgP is Cisco-owned. This protocol can only manage EtherChannel within Cisco switches.

Configuring EtherChannel

The steps below can set the ports to fulfill the function of both VLAN port trunk and EtherChannel port trunk:

1. ***Establish an EtherChannel port trunk:***
   1. 1.1. Create the port trunk by implementing the Cisco IOS command: `interface port-channel`.
   2. 1.2. Choose which physical interface to assign the EtherChannel trunk the previous step created. For this step, implement this Cisco IOS command: `interface range`.
   3. 1.3. Assign the chosen interface to the EtherChannel trunk by `implementing channel-group`.
2. ***Set the VLAN trunk to the logical port trunk:***
   1. 2.1. Select the EtherChannel port and then implement the Chisco IOS command: `interface port-channel`.
   2. 2.2. Set the selected EtherChannel port as the trunk port by implementing the Cisco IOS command: `switchport mode trunk`.

Types of Switch Ports

The two types of Switch ports can be either access ports or trunk ports. These types can be manually assigned to a switch port by using the IOS command: switchport mode. Aside from this Cisco command, Dynamic Trunking Protocol (DTP) can be used to manage switch ports including assigning its type and thus, its function in the network.

1. ***Access Ports*:** Switch ports are, by default, set to function as access ports. If the port is directly linked to another switch, DTP converts the switch port to a trunk port.

2. ***Trunk Ports:*** Switch ports must be manually configured before they assume the responsibilities of being a trunk ports. If the port is connected to a host device or end device like IP telephone or computer host, DTP converts the switch port to an access port.

Technet24.ir

Chapter 11. Voice over IP (VoIP)

Voice over IP protocols convert voice input, from the handset microphone connected to an IP phone, to digital signals. These protocols break down the converted digital signals into smaller bits wrapped inside data packets or IP packets. These IP packets are then transmitted over the network until they reach the destination IP telephony gateway. Once the IP packets arrive, the IP telephone immediately begins extracting the digital signals and converts them to analog sounds.

Quality of Service (QOS)

The QOS is a special configuration for VoIP to improve the quality of audio input and output. This involves full optimization of the conversion process so that the digital signal derived from the audio recording is properly converted, wrapped and sent to the destination without hitch.

The lack of QoS configuration in most VoIP leads to IP packets lagging behind other data frames sent through the network. This delay leads to the sound being delayed, broken or cut off completely.

VoIP implements QoS at two OSI levels:

- Layer 2 (Data Link Layer): Class of service (CoS)
- Layer 3 (Network Layer): IP priority

By default, the VoIP values in both layers are 0 (least priority). With QoS configured, VoIP gets a priority value of 5 (high priority).

Cisco IP Phone

The Cisco IP phone is a device specifically configured for VoIP. This device is connected to one of the switch access ports. The IP phone also acts as a Layer 2 switch. It has three ports:

- ***Internal Connection:*** This is a port found inside the IP phone. This port establishes a connection with the processor of the IP phone.
- ***PC (10/100 PC):*** Often used to connect the phone to the computer host, this port is the single most important port found in a typical Cisco IP Phone.
- ***Uplink (10/100 SW):*** This port is created specifically for establishing a stable connection between the switch access port (network) and the upstream

Cisco Discovery Protocol (CDP)

Obviously a Cisco-proprietary protocol, the CDP is created to find all the devices directly connected to the port. This protocol is enabled in Cisco switches and Cisco IP phones by default. CDP lets the upstream switch to locate the Cisco IP phone and convey the needed interaction numbers that are best for VoIP.

The switch can interact with the IP phone through the CDP to configure the PC port to either:

- ***Trusting PC port:*** This port *trusts* the CoS and IP priority values configured on all of the inbound IP packets.
- ***Nontrusting PC port:*** This port does not trust the CoS and IP priority values configured on all of the inbound IP packets. It will then keep the values for both IP priority and CoS at 3 (intermediate priority).

Technet24.ir

Enabling QoS in the Upstream Switch

To configure the upstream switch to support VoIP, QoS must first be turned on in the switch's IOS interface. Enabling the QoS requires the Cisco IOS command mls. Consider the command block below:

```
switch001 >en
switch001 >config t
switch001 >mls qos
```

The next step is to adjust the settings of the access ports to *trust* the CoS and IP priority values of inbound IP packets sent by the Cisco IP phone. To do this, implement the command block below:

```
switch001 >en
switch001 >config t
switch001 (config) >interface
switch001 (config-if) >switchport priority extend trust
switch001 (config-if) >mls qos trust cos
```

The above commands set the access port to a *trusting PC port* and on the last line it configured the switch to also trust CoS values.

Technet24.ir

Chapter 12. Troubleshooting Switches

In a typical problem-solving scenario, the first step is to gather pertinent information about the switch. Before proceeding to fix the problem, it always helps to have an idea of what the possible problems are. The IOS interface is always a good place to start when trying to find out what could have possibly gone wrong.

Gathering Information

1. **IOS Version**

   Even before you type in troubleshooting commands, it is important to know the version of Cisco IOS you are working on. The four ways to find out what the IOS version is are as follows:

- GUI display
- Cisco IOS command: `show version`
- IOS image file
- Output Message of the Boot Process

2. **Memory Contents and Switch Configuration**

   Another thing that must be determined before troubleshooting the switch is to know the configuration of the switch including which memory the switch is stored. The different ways to inspect switch configuration and memory contents are:

- Cisco IOS File System (IFS) commands to check on the configuration of the flash content, RAM and NVRAM.
- Cisco IOS commands:

`show tech-support`	This command checks every possible technical metrics used by the switch.
`show startup-config`	This command checks the initial configuration stored in the NVRAM
`show running-config`	This command checks the present configuration stored in the RAM
`Show flash`	This command inspects the contents of the flash memory.

3. **System Messages and Cisco Switch Logs**

   Aside from the intrinsic properties of switches, log files and system messages provide the most useful troubleshooting information. Most of the errors and causes of errors are listed in the log files. The information

Technet24.ir

from log files often offers a descriptive analysis of what could have probably gone wrong based on a self-check the device has undertaken.

The two ways to check these log files are through the following:

- Cisco Network Assistant (CAN)
- Cisco IOS command: `show logging`

The *logging levels* are as follows:

Syslog Type	***Description***	***Severity***	***Level***
`LOG_EMERG`	The switch is no longer usable.	0	Emergencies
`LOG_ALERT`	The switch needs to be checked immediately.	1	Alerts
`LOG_CRITICAL`	The switch has a “serious condition”.	2	Critical
`LOG_ERROR`	The switch has an “error-filled condition”.	3	Errors
`LOG_WARNING`	The switch has a “warning condition”.	4	Warnings
`LOG_NOTICE`	The switch has a “significant condition”.	5	Notifications
`LOG_INFO`	Information message	6	Informational
`LOG_DEBUG`	Debugging message	7	Debugging

Take note that `0` in severity means that the switch is not functional (zero functionality) and `7` means that the switch is fully functional.

Aside from the above information, the system can also provide the following information:

`Log buffer`	This shows the extent of the internal log buffer
`Trap logging`	This shows the logging information with respect to the Syslog servers.
`File logging`	This shows the properties of every file in the memory.
`Count and timestamp logging`	This shows the number of log messages recorded by the switch processors and the time log messages are created.
`Exception logging`	This shows the extent of the exception configured in the internal log buffer.
`Buffer logging`	This shows the internal configuration of the logging buffer.
`Monitor logging`	This shows the logging configuration of the VTL (SSH and TelNet).
`Console logging`	This shows the logging configuration of the console.
`Syslog logging`	This shows the logging configuration for the entire Cisco switch.

Technet24.ir

Troubleshooting Switch Connectivity

To repair the connectivity of the switch to the network, perform the following steps:

1. Check the patch panels and cables.

- Make sure that they are not damaged.
- Make sure that the contact pins are latched tightly to the switch ports.
- Make sure that the correct cable is used in the connection
- Make sure that the link does not surpass the extent of the distance supported by Ethernet connection.

2. Check the port integrity of the switch.

Check the status of the ports by implementing the following Cisco IOS commands:

- `show logging`
- `show vlan`
- `show interfaces trunk`
- `show interfaces switch ports`
- `show interfaces status`
- `show interfaces status err-disabled`

3. Use the Cisco IOS commands: traceroute and ping.

- The *Ping* tool is a command that sends empty IP packets to a specific IP address to measure the connection between the two ports.

1. Start the CNA.
2. Using level_15_acess, logon to the switch
3. Click the *Troubleshooting* tab.
4. Click *Ping and Trace*.
5. Within the Ping and Trace dialogue box, choose *Ping* tool.
6. Insert the IP address of the *Destination*.
7. Click *Start*.

In the IOS interface, implement the following command:

```
switch001 >ping 192.168.72.00
```

- The *Trace route* tool is a command that treads the IP route between the source and destination nodes within the TCP/IP network.

1. Start the CNA.
2. Using level_15_acess, logon to the switch
3. Click the *Troubleshooting* tab.
4. Click *Ping and Trace*.
5. Within the Ping and Trace dialogue box, choose *Layer 3 trace* tool.
6. Insert the IP address of the *Destination*.
7. Click *Start*.

Technet24.ir

Conclusion

Thank you again for purchasing this book.

I hope this book was able to give you comprehensive information on CCNA routing and switching. Using this book as a guide, you could become a network engineer with a solid foundational knowledge of the mechanisms of Cisco networks.

Finally, if you enjoyed this book, then I'd like to ask you for a favor. Would you be kind enough to leave a review for this book on Amazon? It'd be greatly appreciated!