CCNA

Student Lab Manual

NETWORKERS HOME

IGNITE YOUR GENIUS

L – 165, 6th Sector, Gayathri Complex, HSR Layout
Next to Spatika HospitalBangalore – 560102
Karnataka – India

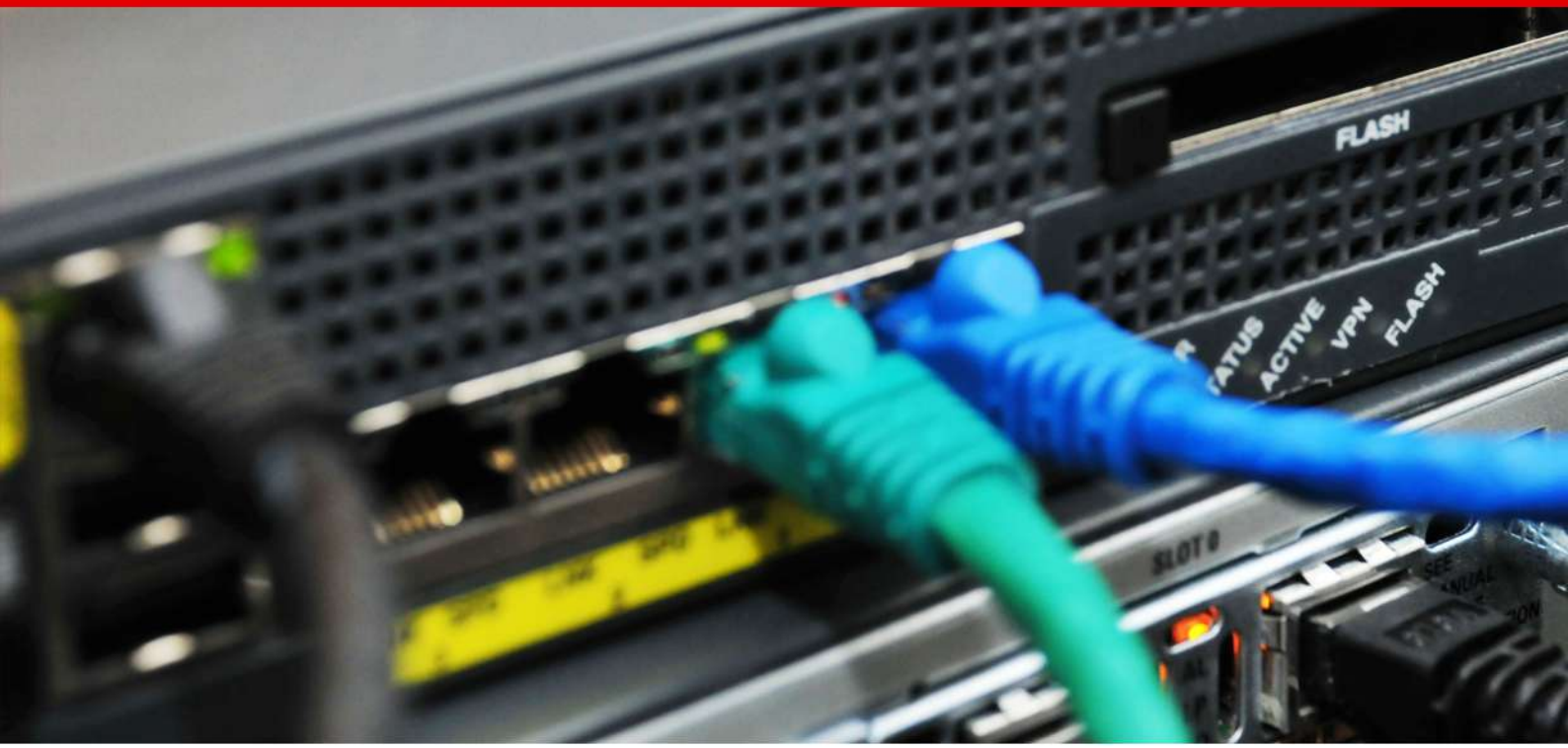
www.networkershome.com

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

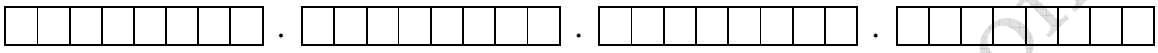
WORK BOOK : Module:1 - IP Addressing



Module 1 – IP Addressing

IP ADDRESSING RULES

- IP addresses must be unique in a network
- IP addresses only have meaning when read in conjunction with a subnet mask - ANDing
- 32 bits (0 or 1) divided into 4 octets



- IP address has two portions – network and host
- Each octet has a decimal value range of 0 to 255, except for the first octet, which is 1 to 255
- The network portion can not be all 0's nor all 1's
- The first octet can not be 127 (network), this is reserved for loopback and also to check if protocol stack is correctly configured. Errors can easily be resolved by reloading TCP/IP and rebooting.
- The host portion can not be all 0's – this defines the network address
- The host portion can not be all 1's – this defines a broadcast in that particular network
- The IP address 255.255.255.255 defines a general broadcast

USEFUL STATISTICS

Class	1st octet range decimal	1st octet structure binary	Total Number of networks	Maximum Number of hosts/network	Address Structure	Default Subnet Mask
A	1 – 127	0xxxxxxx	2^7-2 126	2^{24}-2 16,777,214	N.H.H.H	255.0.0.0
B	128 – 191	10xxxxxx	2^{14} 16,384	2^{16}-2 65,534	N.N.H.H	255.255.0.0
C	192 – 223	110xxxxx	2^{21} 2,097,152	2^8-2 254	N.N.N.H	255.255.255.0
D	224 – 239	1110xxxx	Reserved for multicasting			
E	240 - 255	1111xxxx	Reserved for experimental and future use			

- Note that x = 0 or 1, also N = Network portion and H = Host portion

Subnetting

Six steps of subnetting

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
254	**126**	**62**	**30**	**14**	**6**	**2**	**0**

1. Find the number of networks required.
2. Find the number of bits to borrow (Use the chart)
3. Find the Increment number on the chart.
4. Write the New mask (256 – Increment)
5. Write the new network numbers. Use the increment to write the numbers. First network will be the increment and the last network will be one increment less than the mask.
6. Write the range of valid hosts and the broadcast address for each network.

Subnetting Exercises

1. You have a Class C address of 192.168.5.0. You would like to break it into 7 Subnets. Write the new Subnet Mask, First, Last and Broadcast addresses for the new Subnetworks.

2. You have a Class B address of 150.5.0.0 You would like to break it into 15 Subnets. Write the new Subnet Mask, First, Last and Broadcast addresses for the First 5 Subnetworks.

3. You have a Class A address of 50.0.0.0. You would like to break it into 50 Subnets. Write the new Subnet Mask, First, Last and Broadcast addresses for the First 5 Subnetworks.

4. If you have sub-netted a network 172.16.0.0 with a mask of /20. Which of the following addresses are broadcast addresses? (Choose all that apply)

   A. 172.16.32.255
   B. 172.16.47.255
   C. 172.16.79.255
   D. 172.16.159.255

5. What would your subnet mask be if you want 5 networks with 20 hosts each?

   A.

6. You are required to break the 172.15.0.0 network into subnets having a capacity of 450 hosts with the maximum allowed subnets. What would your mask be?

   A.

7. Convert 1101 1001 into Decimal and Hex.

8. If your mask is 255.255.255.224, which of the following addresses are valid IP Addresses? (Choose all that apply)

   A. 192.165.4.37
   B. 195.5.2.63
   C. 172.6.5.32
   D. 11.5.1.94

9. If your mask on a Class C network is /29, how many subnets and host per subnet do you have?

   A.

10. What is the binary range of Class A, Class B and Class C addresses?
    A.
    B.
    C.

11. If you routers ID is 192.168.1.60/240, what is the range of valid addresses that you can configure for a PC connected to the same Interface?
A.

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK Module:2 - OSI Reference Model

OSI Reference Model

LAYERING BENEFITS & REASONS

- To divide the interrelated aspects of network operation into less complex operations.
- To define standard interfaces to achieve compatibility and multivendor integration.
- To achieve a modular approach to networking protocols so new applications and services can be deployed without redesigning other layers.
- To keep changes in one area from affecting other layers.
- To ease troubleshooting using data packets which will have specific information about each layer.

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

APPLICATION LAYER (Layer 7)

- Provides interface between OSI RM and end user applications
- Provides network services to user client/server-based applications
- Establishes and defines program-to-program communication
- Identifies availability of intended communication partner
- Examples include ftp, tftp, http, www browsers, DNS, SMTP, telnet

PRESENTATION LAYER (Layer 6)

- Defines data format for transmission
- Ensures arriving data from the network can be used by the application and information sent by the application can be transmitted on the network
- Performs encryption and decryption
- Example representations include ASCII, EBCDIC, JPEG, TIFF, PICT, MPEG, MIDI, HTML

SESSION LAYER (Layer 5)

- Defines how to start, control and end sessions
- RPCs operate at this layer
- Logon Validation happens at this layer.
- Named Pipes defined at this layer – Named Pipes use TCP to guarantee communications, example – NetLogon
- Session layer organizes communication through simplex, half-duplex or full-duplex
- Example protocols include SQL, RPC, NetBIOS, Named Pipes

TRANSPORT LAYER (Layer 4)

- Segments data to be passed down to the Network layer and reassembles data for the Session and upper layers
- Provides the choice of connection-oriented and guaranteed (TCP) or connectionless and non-guaranteed (UDP) delivery of data
- Provides end-to-end transport services
- Provides flow control to overcome congestion in the receiving host's buffers
- TCP uses port numbers to multiplex from the Transport layer through to the Application layer
- [multiplex = ability to send different data from a number of applications in the same transport connection]
- 3 flow control mechanisms:

Buffering

Each computer has enough buffer space to hold data before it is processed

Congestion Avoidance

Receiving computer notices its buffers are filling quickly and sends a stop message to the sending host to temporarily stop transmitting while it processes data already received. It then signals that it is ready for more data. Example protocols – Synchronous Data Link Control (SDLC), Link Access Procedure, Balanced (LAPB), ICMP Source Quench (slows down rate instead of stopping it)

Windowing

Defines maximum number of packets that can be sent before an acknowledgement is expected

- Connection-oriented protocols establish and terminate sessions, for example, the TCP 3-way handshake
- Ports are defined in RFC 1700.
- The first 1023 ports are reserved, or well-known ports used by the Operating System

- The remaining ports (1024 – 65,535) are available for use by client/server-based applications

20, 21	FTP		69	TFTP
23	Telnet		70	Gopher
25	SMTP		80	http
53	DNS		119	NNTP
67	DHCP Server		161	SNMP
68	DHCP Client		179	BGP

- Example protocols include TCP, UDP, SPX, IPX

NETWORK LAYER (Layer 3)

- Defines the network address
- Routers operate at this layer
- Segments from the Transport layer are placed into packets and passed down to the Data Link layer
- Network layer routes data from one node to another
- Determines the best path/route to destination device to use for routing data on the internetwork – this is done by the protocol using hop count (IP RIP) or tick (IPX RIP), where 1 tick = 1/18th of a second
- Network layer maintains routing table
- IP addressing consists of a network and host address specified with a Subnet Mask. (IP Address 131.107.2.1 Subnet Mask 255.255.0.0) where 131.107 is the Network and 2.1 is the Host address
- IPX addressing 2a.01c0.1234.5ac9 consists of network and host (MAC) address. The Right-most 12 Hex-digits represents the MAC Address or Host address and and remaining Hex-digits in the front represent the Network Address. The Network Address can be up to 8 Hexadecimal digits, defined by the Network Administrator. In this example, 2a is the network address and 01c0.1234.5ac9 is the MAC or host address.

DATA LINK LAYER (Layer 2)

- Provides error-free link between 2 devices – CRC used for error checking
- Packets from the Network layer are placed into frames

- Data Link layer handles physical transmission of data from one node to another
- Handles error notification
- IEEE subdivided this layer into 2 sublayers

Logical Link Control (LLC)

Uses Destination Service Access Points (DSAP) and Source Service Access Points (SSAP) to help lower protocols access Network layer protocols

Media Access Control (MAC)

Builds frames from bits
Performs CRC
Handles MAC addresses – first 6 digits of 12 hex define vendor ID, next 6 is the serial number for that vendor ID

- Protocols in the 2nd layer

LAN	Ethernet, Token Ring, FDDI, ArcNet
WAN	PPP, SLIP, Frame Relay, ISDN, ATM, X.25, SDLC, HDLC, CDP

- Media access methods
  Contention-based – Ethernet (CSMA/CD)
  Token-passing
  Polling
- WAN technologies
  - *Plain Old Telephone Service (POTS)*
  - *Integrated Services Digital Network (ISDN)*
    - Basic Rate Interface (BRI) - 2 B channels at 64 kbps each + 1 D channel at 16 kbps for signaling
    - Primary Rate Interface (PRI) - 23 B channels + 1 D channel (64 kbps)
  - **Dedicated leased line – T1**
    - Charged monthly, approximately $2 - $5 / mile / month
    - Fast speed : 1.544 Mbps
  - *Serial Line Internet Protocol (SLIP)*
    - Can only use IP
  - *Point to Point Protocol (PPP)*
    - Supports IP, IPX, NetBEUI, AppleTalk

- Internetworking devices used at the 2nd layer

- **Bridges**
- **Switches**

PHYSICAL LAYER (Layer 1)

- Defines connections – RJ-45, RJ-11, BNC, HSSI, RS-232
- Places frames, represented as bits, onto media as electric signals or pulses of light
- Hubs and repeaters operate at this layer

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK Module:3 - Router Basics

Router Basics

ROUTER CONFIGURATION SOURCES

- Routers can be configured from:
  - Console terminal
  - Auxiliary port – externally, via modems
  - Virtual terminals (Telnet) – after installation

INTERNAL CONFIGURATION COMPONENTS

- RAM
  - Contains dynamic / running configuration
- NVRAM
  - Contains backup of configuration (startup configuration)
- Flash
  - Contains copy of Cisco IOS
- ROM
  - Contains a subset of IOS
  - Contains bootable IOS image
- Interfaces
  - Network connections which packets enter/exit from routers, e.g. Ethernet, serial, BRI, Token Ring
- Console and auxiliary ports
  - Main command-line interface used for configuration

ROUTER STARTUP SEQUENCE – SUMMARY

1. Bootstrap program loaded from ROM
2. Bootstrap runs the POST
3. Bootstrap locates IOS in Flash
4. IOS is expanded and then loaded into RAM
5. Once IOS is loaded into RAM, it looks for startup-config in NVRAM
6. If found, the configuration is loaded into RAM

ROUTER MODES

- **User EXEC mode** (look, but don't change)
  - Automatically enter this mode when router is turned on
  - You can perform basic tasks, such as connect to remote devices, perform basic tests
  - Prompt : **Router>**

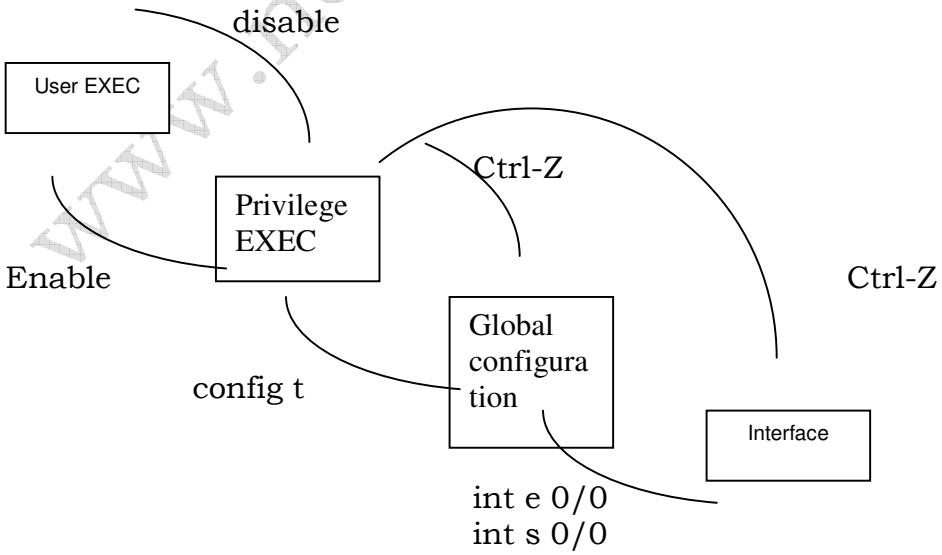
- **Privileged EXEC mode**
  High-level testing commands
  Set operating parameters
  Command to enter : Router>enable
  Prompt : **Router#**

- **Global configuration mode**
  Commands apply to features that affect the system as a whole
  Enter from privileged EXEC mode with command : Router#config t
  Prompt : **Router(config)#**

- **Interface mode**
  Configure interface, such as Ethernet, serial
  Enter from global configuration mode with command :
  Router(config)#int e 0/0
  Or Router(config)#int s 0/0
  Prompt : **Router(config-if)#**

- **Setup mode**
  Helps new user to create a configuration for the first time, via a series of questions
  Prompted at bootup or enter **setup** at router# prompt

- **Rommon mode**
  Provides router with a small subset of IOS and helps router boot if IOS not found in Flash
  Prompt : Rommon 1>



OVERVIEW OF USER INTERFACE COMMANDS

- **Editing commands**
  - Ctrl-A beginning of line
  - Ctrl-E end of line
  - Ctrl-F forward one character
  - Ctrl-B back one character
  - Esc-F forward one word
  - Esc-B back one word

- **Command History**
  - Enabled by default
  - 10 commands recorded in history buffer by default
  - Use history size command to change to a maximum of 256
  - Ctrl-P or Up arrow shows most recent
  - Show history command at privileged EXEC mode shows if enabled and history size
  - Tab keys completes entries of known keywords

SETTING ROUTER NAME

- Router(config)#**hostname** (*desired_name*)

WELCOME BANNER

- Displayed when router is accessed
- Displayed prior to prompting for a password
- Syntax : Router(config)#**banner motd** #*message*#

SAVING CONFIGURATION CHANGES

- To save running (active) configuration to startup configuration for availability at next bootup
  Router#copy running-config startup-config
- To delete startup configuration
  Router#erase startup-config
  Then reload

VIEWING / VERIFYING CONFIGURATION

- Router(config)#show run

ROUTER STATUS COMMANDS

- Show version [RAM]
  Shows IOS configuration
  Image file name and location
  How long router is up and active
- Show startup-config [NVRAM]
  Shows image size
  Shows backup configuration file
- Show running-config [RAM]
  Shows current, active configuration
- Show interfaces
  Shows statistics/parameters for all configured interfaces
- Show flash [Flash]
  Shows information on Flash memory device includes all IOS images

Router Passwords

- **LOGGING INTO THE ROUTER**

```
Router(config)#line con 0
              login
              password xxxxxxxxxxx
```

- **SETTING AN ENABLE MODE PASSWORD**

```
Router(config)#enable password xxxxxxxxxxxx
```

- **SETTING AN ENCRYPTED ENABLE MODE PASSWORD**

```
Router(config)#enable secret xxxxxxxxxxxxx
```

- **SETTING A TELNET SESSION PASSWORD**

```
Router(config)#line vty 0 4
              login
              password xxxxxxxxxxxxxxx
```

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK Module:4 - Router Basics Labs

Lab 1 – Connecting a Dump Terminal / PC to the router

- Connect the Console Adapter to either Com1 or Com2 on the back of your PC.
- Connect the Rollover cable from the back of the Console Adapter to the Console Port on the Router.
- Make sure the PC is up and running before turning the Router on.

Hyper Terminal Configurations

- Open Hyper Terminal under Accessories.
- Give the Connection a Name (Cisco).
- Specify that you are using either Com1 or Com2 (based on what port you connected the console adapter to)
- On the Port Properties dialog, Click on ***Restore Defaults*** and then Click on ***OK***.
- Press Enter couple of times.
- If the router is up, you should see the Router prompt.

Lab 2 - Stepping through different command modes and getting help

Stepping Through Different command modes

- **Router>** indicates that you are in User Exec Mode.
- On the **Router >** Type **enable** and Press **Enter.** Your prompt should look like **Router#.**
- The **Router#** indicates that you are in Privileged Exec Mode
- Type **Disable.** It will take you from Privileged Mode to User Mode. Your prompt should look like **Router>.**
- You can also type in **En** to go into Privileged Mode from User Mode. The reason being, there is no other command in User Exec that starts with the letters **En.**
- Similarly, you can type **Disa** instead of **Disable** at the Privilege Mode to go into User Exec Mode.
- If you want to exit out completely, type **logout.** Logout will log you out of the router. You should see the prompt asking you press **Enter** to get started. Press **Enter**.
- You can also type **Exit** to logout of the Router from either User or Privilege Mode.
- Press **Enter** to get started again.
- Type **?.** It displays all the commands that can be type in the current Mode (User Exec). It will give a short description about each command and stop after each page.
- Press the **Enter** Key. What happens? Write it down.
- Press the **Spacebar** Key. What happens? Write it down.
- Type **?.** If you want to exit out of help without seeing all the commands press **Ctrl-C or Esc.**

- Type **enable.** Type **?** followed by the **spacebar** key until you return back to the prompt.

- Did you see more commands when Typed **?** in Privileged Mode than in User Mode?

- Cisco Help is ***Context sensitive.*** It displays help based on where you typed ?.

- If you wanted to find out about all the commands that start with a specific letter, you can type that letter followed by **?**. It will only display commands that start with that letter. Type **S?**. What does it show you?

- To go to the Global Configuration mode, type **Configure Terminal** from the Privileged Mode. You can also type **Config t** to have the same effect. Your prompt should look like **Router(config)#**. This is the prompt for Global Configuration Mode.

- Type **Exit**. To go down one level you could use **Exit**.

- Type **Disable.** This should take you to User Exec Mode. Can we get to configuration mode from here?

- Type **Config t.** What happens?

- Type **En.** Your prompt should look like **Router#**.

- Type **Config t.** Your Prompt should like **Router(config)#**. Can we logout from here?

- Type **Logout.** What happens?

- To go to Configure a specific interface, you have to go into that interface. The command that will allow you to go into a specific interface is as follows :
  Interface Type Slot/Port

- Type **Int Ethernet 0/0**. You could also have typed **Int E 0/0.** This allows you to configure the Ethernet interface 0/0. The prompt should look like **Router(config-if)#**.

- If you wanted to configure the Serial interface, type **Interface Serial 0/0 or Int S 0/0.** Does your prompt change?

- The prompt for all your interfaces is the generic **Router(config-if)#.**

- To go back to Global Configuration, Type **exit.**
- Type **Int e 0/0** to go back into interface configuration mode.
- To go back directly back into Privileged Mode, you can either type **Ctrl-Z or end.**
- Where did "**END**" take you ?
- Type **Config t**
- Type **Int e 0/0**
- Ctrl-Z
- Where did "**CTRL-Z**" take you?

Stepping through Context-sensitive Help to set the Time for the Router

- In the Privileged Mode, Type **Cl?.**
- What command will allow you to set the Clock?
- Type **Clock ?.** What should you type next?
- Type **Clock set ?.** What should you type next? (Hr:Min:Secs)
- Type **Clock set 17:25:00** and Press **Enter**.
- What is response?
- Type **Clock set 17:25:00 1 ?.** What should you type next? (Day of the Month Month)
- Type **Clock set 17:25:00 1 may ?** What should you type next (Year)
- Type **Clock set 17:25:00 1 Dec 2000** and Press **Enter**

Terminal History

- What happened when we pressed up arrow ?

- Type **Show history.** It shows the last set of commands you have typed. By default, the router will keep track of the last 10 commands.

- Type **Terminal history size 100** to change the history size to 100.

- Type **Show Terminal** to see the change. (Towards the bottom of the output)

Editing Keys

- Press **CTRL – P.** It will show you the Previous Command.

- Press **CTRL-P.** It will show you the command you typed before the Previous command.

- Press **CTRL – N.** It will show you the Next Command.

- Where is the cursor at? Let us say that you want to change something at the beginning of the line. Rather than using the arrow keys to scroll to the beginning of the line, you can accomplish the same by pressing **CTRL – A**

- Press **CTRL-A.** The cursor should be at the beginning of the line.

- Press **CTRL – E.** CTRL-E takes the cursor to the end of the line.

Show Commands

- All show commands are typed in Privilege Exec Mode (#).

- Type **SH INT S 0/0**. What is the status of the line?

- What is the Encapsulation type on the Serial interface?

- Type **SH Ver**. What does this command display?

- What is the name of the file that was used to boot the Router?

- How many interfaces does your router have?

- Type **SH IP Int Brief**. What does this command display?

Disabling Domain-lookup and Synchronizing the console line

- In global configuration mode, Type **no ip domain-lookup**.
- This command prevents the router from doing a Name lookup if you mistype a command?

- In global configuration mode, Type **line console 0**.
- This command takes you into the Console Configuration mode.
- Type **Logging Synchronous.** This prevents console messages from getting inserted into your command as you are typing.
- Type **no exec-timeout**. This command prevents the session from getting timed out after 2 minutes of idle time.

Lab 3 – Setting the Hostname and Banner

Setting the Router Name

- Go to Global Configuration by typing **Config t**
- Type **Hostname xxxxx (Where xxxxx is your name)**
- What happened to your prompt ? (It should be **Yourname(config)#)**
- Exit

Setting the Banner for Logging in

- Go to Global Configuration by typing **Config t**
- Type **Banner Motd #Welcome to *Yourname's* Router#** (You can start and end the message with Delaminating character of your choice)
- Type **End**.
- Type **Logout**.
- Press **Enter.** Do you see the banner displayed?

Lab 4 – Saving the Running-Config File

- Go to Privilege Mode.
- Type **Show running-Config or Show Run.** Does it show the hostname and Banner you set in the previous lab?
- Show **startup-Config or Sh star.** Do you have any startup-configuration file? Why not?
- To save this configuration, Type **Copy running-config startup-config** or **Copy Run Start** or **Wr.**
- Press **Enter** to take the default [Starup-config] for Destination Filename.

Lab 5 – Creating Aliases

Creating Aliases for Frequently Used Commands

Router#**config t**

Router(config)#**alias exec shr sh run**
*(This command creates a shortcut **shr** for the **show run** command)*

Router(config)#**alias exec shs sh start**
*(This command creates a shortcut **shs** for the **show start** command)*

Router(config)#**alias exec ship sh ip int brief**
*(This command creates a shortcut **ship** for the **show ip int brief** command)*

Router(config)#**alias exec shv sh ver**
*(This command creates a shortcut **shv** for the **show version** command)*

Router(config)#**alias exec cc config t**
*(This command creates a shortcut **cc** for the **config t** command)*

Testing the Aliases

- Try the different aliases you have created by typing them one at a time.

Lab 6 – Setting a Line Console Password

Setting the Line Console Password

Router>**en**
Router#**config t**
Router(config)#**line console 0**
Router(config-line)#**login**
Router(config-line)#**password *newyork***
Router(config-line)#**end**

Testing the Line Console Password

- Type **Logout** to exit out of the router's console. You should see a message that says "**Press Return to get started".**
- Press **Enter**.
- Do you get a prompt for password to get into **User Exec mode**?
- Type ***newyork*** (The password that was set).
- Are you in **User Exec mode**?
- Type **en** to get into **Privilege Exec mode.** Did it prompt you for a password?

Lab 7 – Setting the Enable Password

Setting the Enable Password

Router>**en**
Router#**config t**
Router(config)#**enable password *LA***
Router(config)#**end**

Testing the Enable Password

- Type **Logout** to exit out of the router's console. You should see a message that says "**Press Return to get started".**
- Press **Enter**.
- Do you get a prompt for password to get into **User Exec mode**?
- Type ***newyork*** (The Console password that was set).
- Are you in **User Exec mode**?
- Type **en** to get into **Privilege Exec mode.**
- Did it prompt you for a password?
- Type ***LA***. (The enable password that was set).
- Are you in **Privilege Exec Mode?**

Lab 8 – Setting the Enable Secret Password

Checking the enable password

- Type **Sh run**.
- Do you see the enable password in the clear text?

Setting the Enable Secret Password

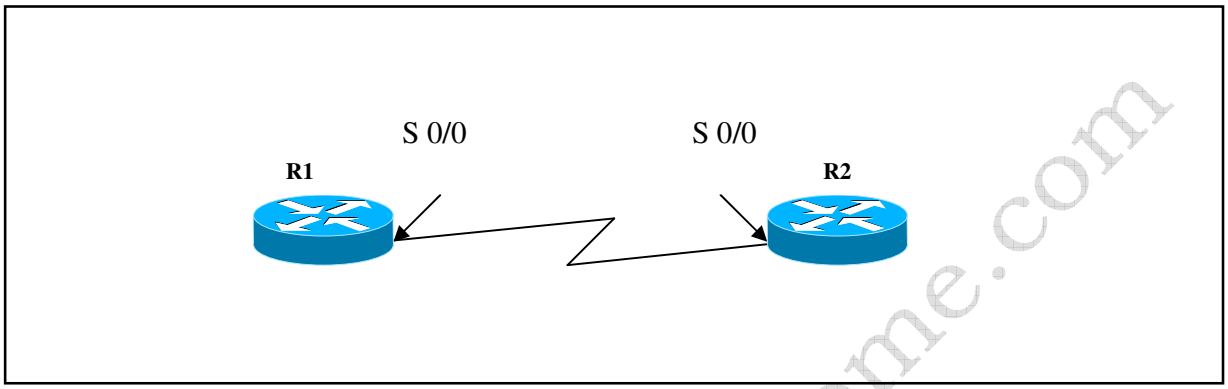
Router>**en**
Router#**config t**
Router(config)#**enable secret *trinet***
Router(config)#**end**

Testing the Enable Secret Password

- Type **Logout** to exit out of the router's console. You should see a message that says "**Press Return to get started".** Press **Enter**.
- Do you get a prompt for password to get into **User Exec mode**?
- Type ***newyork*** (The Console password that was set).
- Are you in **User Exec mode**?
- Type **en** to get into **Privilege Exec mode.** Did it prompt you for a password?
- Type ***LA***. (The enable password that was set).
- Did it work?
- Type ***netmet***
- Did it work?
- Type **Sh run**.
- Do you see both passwords?

- Which password works?

Lab 9 – Basic Serial Connection (HDLC)



Finding the Clock Source

- Type **Show Controller S 0/0.**
- Look for the word DCE or DTE in the top three lines.
- If it says DCE, you will provide the Clock (Speed for the link). It is normally specified by the Telephone Company based on your contract.

Configuring the Serial Interfaces with IP Addresses and bringing them up.

- Go into Global configuration mode by typing **Config t**.
- Enter into the Interface configuration mode for the Serial Interface by typing **Int S 0/0.**
- Set the IP Address of the Interface by typing **IP Address 10.0.0.X 255.0.0.0** where **X** is your number (1 or 2).
- If you were the clock source, you have to set the speed of the link. Type **Clock rate 128000** to set the speed of the line to 128 kbps.
- Bring the Interface up by typing **No shut**.

Verifying the connection

- Make sure both routers are configured before proceeding to the following section.

- In Privilege exec mode, type **SH IP INT BRIEF.**
- What is the status of your Serial line?
- Type **Ping 10.0.0.Y** where **Y** is your partner's IP address.
- Are you successful?
- Type **SH INT S 0/0**. What is the encapsulation type?
- Can you use this encapsulation with a non Cisco Router?
- Can you Authenticate the routers with this type of encapsulation?

Lab 10 – Basic Serial Connection (PPP)

(Builds on Lab 9)

Using PPP as the Authentication

- To change the encapsulation of the interface to PPP, type the following commands on both routers:

Router>**en**
Router#**config t**
Router(config)#**int S 0/0**
Router(config-line)#**encapsulation ppp**
Router(config-line)#**end**

- Type **SH INT S 0/0.**
- What is the encapsulation type?
- Ping your Partner's router.
- Are you successful?
- What are the advantages of using PPP over the Cisco Proprietary HDLC?

Lab 11 – Establishing a Telnet Session to your partner's router

(Builds on Lab 10)

Testing the Telnet Password

- Type **Telnet 11.0.0.X** (Where **X** is your partner's number)
- What message do you get?

Setting the Telnet Password

Router>**en**
Router#**config t**
Router(config)#**line vty 0 4**
Router(config-line)#**login**
Router(config-line)#**password *remote***

Testing the Telnet Password again

- Type **Telnet 11.0.0.X** (Where **X** is your partner's number)
- Did you get a password prompt?
- Type **remote**.
- Do you see your partner's Router prompt?
- Type **en**
- Type **netmet** for your partner's enable password.
- Type **Show run**. Do you see your partner's **Running-config**?

Switching between your Console and Remote Console

- Press **CTRL-SHIFT-6 and X.**
- Do you see your own router prompt?
- If you want to switch back to your partner's router, press **enter** twice

- Do you see your partner's Router prompt?

- To exit the remote session, type **quit**.

- On your own router , save your configuration by typing **copy run star.**

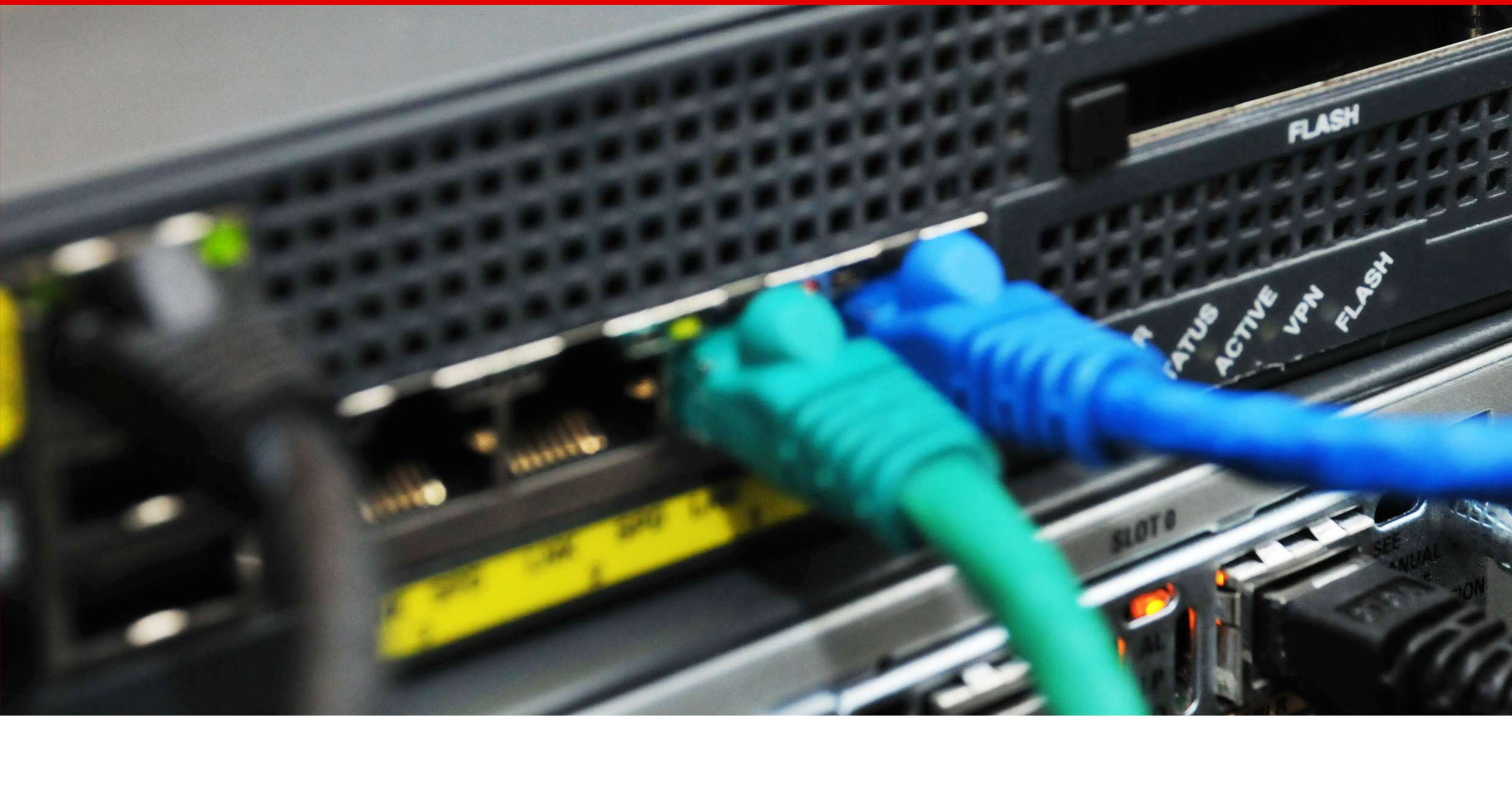
NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK

Module:5 - Advanced RoutingProtocols



Routing Protocols

Routing Tables

- Routers build routing tables initially based on their directly connected networks.
- If addition to directly connected networks, Routers can learn about destinations in one of three ways:
  - Static Routes: Manually added to the routing tables by the administrator.
  - Default Routes: Manually added to the routing table by the administrator to define a Default Gateway for the router. If the routing table does not have an entry for a destination network, send the packet to the Default Route.
  - Dynamically Learned through a Routing Protocol.
- Routing tables are used to send data along specific paths to reach a particular destination.
- Routers need to exchange routing tables so they can route data to networks that are not directly connected to them.
- Routers require a ***Routing Protocol*** in order to exchange routing tables with their neighboring routers and advertise networks.

Static Routes

Static Routes are User-defined, manually created routes. The administrator creates Static Routes in a Cisco Router using the ***IP Route*** Command

Syntax : **ip route** *destination-network subnet-mask Next-Hop-Router-IP-Address* {distance}

Example: ip route 11.0.0.0 255.0.0.0 10.0.0.2

Default Routes

Default Routes define a router as the default router for your router. When there is no entry for the destination network in a routing table, the router will forward the packet to its default router. Default routes help in reducing the size of your routing table.

Syntax : **ip route 0.0.0.0 0.0.0.0** ***next-hop-router***

Example: ip route 0.0.0.0 0.0.0.0 10.0.0.2

Routable and Routing Protocols

- A ***Routable Protocol*** is a network protocol that transports data across a network with a structure, which allows it to be routed to the specified destination network.
- A ***Routing Protocol*** is a method by which routers exchange information about the networks they can reach. Exchange of information allows routing tables to be built and exchanged. The process of updating routers is called ***convergence***.
- Routing Protocols determine the best path for the transport of data using some criteria, such as distance or metric. Examples include bandwidth, delay, hops and reliability.
- Routing Protocols are divided into two groups : Interior and Exterior
- Exterior Routing Protocols include:
  - Border Gateway Protocol(BGP)
  - Exterior Gateway Protocol(EGP)
- Interior Routing Protocols Include:
  - Routing Information Protocol(RIP)
  - Interior Gateway Routing Protocol(IGRP)
  - Open Shortest Path First(OSPF)
  - Enhanced Interior Gateway Routing Protocol(EIGRP)
- Two main Types of Interior Routing Protocols are ***Distance Vector*** and ***Link State***.

Distance Vector Routing Operation and Protocols

- The Routing updates includes the entire routing table.
- It uses a periodic update.
- Routing Update packets are sent as broadcast. Unicast packets can also be specified.
- Examples of Distance Vector Routing Protocols are RIP 1, RIP 2, IGRP

Link State Routing Protocols

- The Routing updates include only new changes to the routing table which saves bandwidth.
- Handles larger networks and is more scalable than Distance Vector Routing Protocols.
- Example OSPF, IS-IS

Administrative Distance

- Rating of the Trustworthiness of a routing information source.

- The Number is between 0 and 255

- The higher the value, the lower the trust. For example, 255 signifies no trust and therefore is ignored.
- Lowest administrative distance is always chosen as the routing protocol to use to transport data.
- Default administrative distances for common protocols are as follows :

Directly Connected = 0	**EIGRP** = 90	**OSPF** = 110
Static Routes = 1	**IGRP** = 100	**RIP** = 120

Distance Vector Routing Protocols

Common Characteristics of Distance Vector Routing Protocols.

Neighbors: As far as the routers are concerned the neighboring router is the one that shares a common data link. These routers have at least one interface on the same network.

Periodic Updates: The interval that the routers wait for before they advertise their routing table to neighboring routers.

RIP for IP – 30 Seconds
RIP for IPX – 60 Seconds
IGRP – 90 Seconds
RTMP – 10 Seconds

Broadcast Update: are used by routers to find other routers when they come online. They send their routing table to Broadcast address of 255.255.255.255, if the neighboring router talks the same routing protocol, it will respond and routers now know of each other.

Route Invalidation Timers: is the time that must pass before a Router considers a route to be invalid. If network 5.0 is connected to Router A and it goes down, Router A will notify its neighboring router, Router B of that fact. But what if Router A goes down.
This problem is handled by ***Route Invalidation Timer*** for each entry in the routing table. When Router B first hears about network 5.0 from Router A, it will set a route invalidation timer for that route. Since Router A was the one that gave him the news it expects Router A to keep updating that information on regular periodic updates, however if Router A fail to do so and misses **x** number of periodic updates, Router B will set that route in the routing table to unreachable.

Asynchronous Updates (Random Jitters or Time Jitters): Periodic Updates can collide and cause further delays in convergence. A Random Jitter will attempt to overcome this by introducing an offset value to the periodic update time, thus reducing the probability of updates colliding.

Routing Loops and Solutions

Routing Loops

Routing Loops can occur if the network's slow convergence on a new configuration causes inconsistent routing entries.

Solutions to Routing Loops

Counting to Infinity: Distance Vector Routing Protocols define a maximum value for Hops. The maximum Hop Count is 15 is commonly used.

Spilt Horizon: Spilt Horizon has two flavors, **Simple Split Horizon and Spilt Horizon with Poison Reverse**.
The logic behind **Simple Spilt Horizon** is that it is never useful to send information about a route back in the direction from which the information originally came. So if Router A learns about a Route through Router B, it will never send the same route back to Router A. This is known as suppressing routes.
Split Horizon With Poison Reverse does not work based on suppression, and it will include every route in its updates but it will tag them as unreachable. Lets say Router B receives a corrupted update believing that it can reach network 1.0 through Router C, Simple Split Horizon will not be able to avoid the loop, whereas Poison Reverse will definitely fix the problem. Router B will say 1.0 can be reached via Router C, but this time Router C will poison that route eliminating the routing loop.

Triggered Updates: Also known **as flash updates.** Changes to the network topology are sent instantaneously to neighboring routers.

Holddown Times: If the hop count to a given destination increases, the router sets a hold down timer for that route.By implementing this refinement we have reduced the likelihood of a bad or corrupted information getting into the routing table, but once again understand that nothing is free and in this case the trade off is convergence time.

Routing Information Protocol (RIP) Version 1

- Distance Vector
- Operating from Udp port 520
- Metric used by Rip is hop count
- Maximum hop count is 15, 16th hop is unreachable
- Periodic Update = 30sec
- Random Jitter (RIP_JITTER) = 15% (4.5 sec) so the Periodic Update can vary from 25.5 sec to 30 seconds.
- Invalidation timer = 180 sec (6 times the update timer)
- Holddown timer = 180 sec (6 times the update timer)
- Split horizon with Poisoned reverse with triggered update is used for stability of the operation.

RIP Version 2

RIP Version 2 Features and Concepts

- Route updates include subnet masks
- Authentication of Routing Updates
- Multicast address used for Routing Updates

IP Routing Configuration Tasks

Interface Configuration

1. Assign IP address and subnet mask
2. Set Clock Rate on Serial Interface at the DCE
3. Start the Interface

Example :

- Interface serial 0/0
- Ip address 110.0.0.1 255.0.0.0
- Clock rate 1000000
- No shutdown

Global Configuration

1. Select Routing Protocol
2. Specify the Interface Network Addresses

Example for RIP:

- Router Rip
- Network 10.0.0.0
- Network 11.0.0.0

Example for IGRP:

- Router IGRP 100
- Network 10.0.0.0
- Network 11.0.0.0

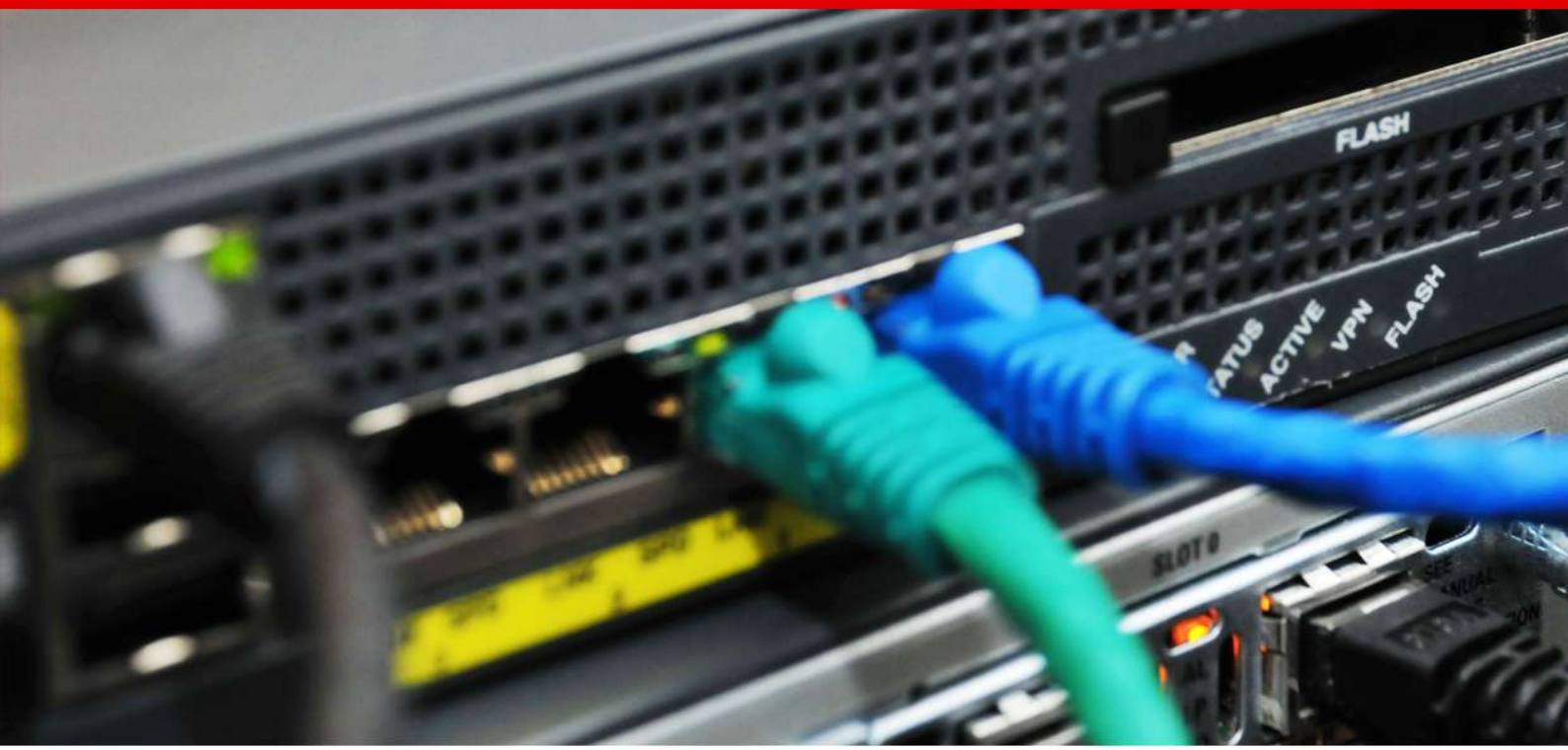
NETWORKERS HOME

IGNITE YOUR GENIUS

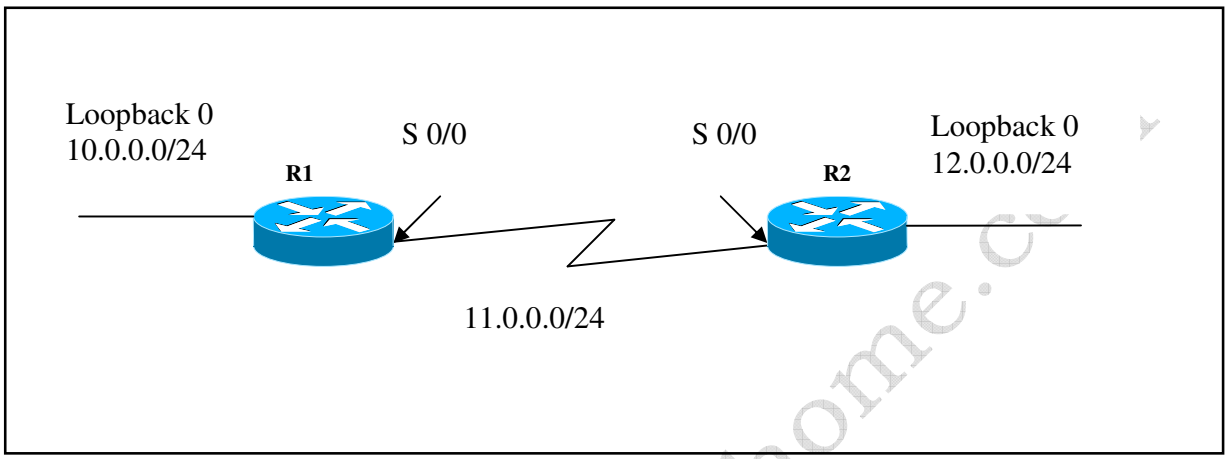
Cisco Certified Network Associate (CCNA)

WORK BOOK

Module:5 - Advanced RoutingProtocols Labs



Lab 1 – Basic Static Routes



Router 1

Would you like to enter initial configuration dialog (y/n)? **N**
Would you like to Terminate Autoinstall (y/n)? **Y (if Required)**
Router>**en**
Router#Config t
Router(config)#Hostname R1
R1(config)#interface Loopback 0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#interface S 0/0
R1(config-if)#**ip address 11.0.0.1 255.0.0.0**
R1(config-if)#**clock rate 128000** (if required)
R1(config-if)#**no shut**
R1(config-if)#**exit**
R1(config)#**ip route 12.0.0.0 255.0.0.0 11.0.0.2**

Router 2

Would you like to enter initial configuration dialog (y/n)? **N**
Would you like to Terminate Autoinstall (y/n)? **Y (if Required)**
Router>**en**

Router#Config t
Router(config)#Hostname R2
R2(config)#interface Loopback 0
R2(config-if)#ip address 12.0.0.1 255.0.0.0
R2(config-if)#interface S 0/0
R2(config-if)#**ip address 11.0.0.2 255.0.0.0**
R2(config-if)#**clock rate 128000** (if required)
R2(config-if)#**no shut**
R2(config-if)#**exit**
R2(config)#**ip route 10.0.0.0 255.0.0.0 11.0.0.1**

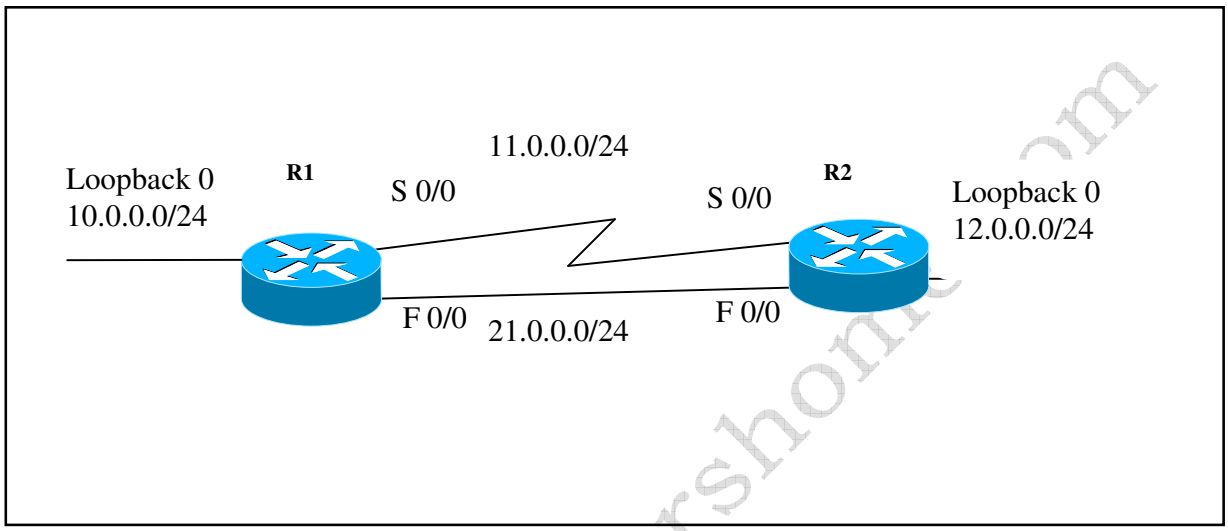
On Both Routers

Type **Show ip route**

- What networks do you see listed?

- Ping your partner's Loopback Interface address. Are you successful?

Lab 2 – Load Balancing Using Static Routes



Router 1

Would you like to enter initial configuration dialog (y/n)? **N**
Would you like to Terminate Autoinstall (y/n)? **Y (if Required)**
Router>**en**
Router#Config t
Router(config)#Hostname R1
R1(config)#interface Loopback 0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#interface S 0/0
R1(config-if)#**ip address 11.0.0.1 255.0.0.0**
R1(config-if)#**clock rate 128000** (if required)
R1(config-if)#**no shut**
R1(config-if)#interface F 0/0
R1(config-if)#ip address 21.0.0.1 255.0.0.0
R1(config-if)#**no shut**
R1(config-if)#**exit**
R1(config)#**ip route 12.0.0.0 255.0.0.0 11.0.0.2**
R1(config)#**ip route 12.0.0.0 255.0.0.0 21.0.0.2**

Router 2

Would you like to enter initial configuration dialog (y/n)? **N**
Would you like to Terminate Autoinstall (y/n)? **Y (if Required)**
Router>**en**
Router#Config t
Router(config)#Hostname R2
R2(config)#interface Loopback 0
R2(config-if)#ip address 12.0.0.1 255.0.0.0
R2(config-if)#interface S 0/0
R2(config-if)#**ip address 11.0.0.2 255.0.0.0**
R2(config-if)#**clock rate 128000** (if required)
R2(config-if)#**no shut**
R2(config-if)#interface F 0/0
R2(config-if)#ip address 21.0.0.2 255.0.0.0
R2(config-if)#**no shut**
R2(config-if)#**exit**
R2(config)#**ip route 10.0.0.0 255.0.0.0 11.0.0.1**
R2(config)#**ip route 10.0.0.0 255.0.0.0 21.0.0.1**

On R1

- Type **Show ip route 12.0.0.0**

- Do you see an Asterisks (*) against one of the routes?
  Note: The Asterisks represents the next path the router will take to get the packet to the destination

- Type **Ping 12.0.0.1.**

- Type **Show ip route 12.0.0.0**
  Note: The Asterisks is against the other route.

On R2

- Type **Show ip route 10.0.0.0**

- Do you see an Asterisks (*) against one of the routes?
  Note: The Asterisks represents the next path the router will take to get the packet to the destination

- Type **Ping 10.0.0.1.**

- Type **Show ip route 10.0.0.0**
  Note: The Asterisks is against the other route.

Lab 3 – Floating Static Routes

(Builds on Lab2)

On R1

R1(config)#**no ip route 12.0.0.0 255.0.0.0 11.0.0.2**
R1(config)#**ip route 12.0.0.0 255.0.0.0 11.0.0.2 20**

On R2

R2(config)#**no ip route 10.0.0.0 255.0.0.0 11.0.0.1**
R2(config)#**ip route 10.0.0.0 255.0.0.0 11.0.0.1 20**

On R1

- Type **Show ip route 12.0.0.0.**
- How many routes do you see for the 12.0.0.0 network?
- What happened to the route through 11.0.0.2?

On R2

- Type **Show ip route 10.0.0.0.**
- How many routes do you see for the 10.0.0.0 network?
- What happened to the route through 11.0.0.1?

On Both R1 and R2

Rx(config)#**int F 0/0**
Rx(config-if)#**shut**

- Type **Show ip route**
- Do you see the route through the 11.0.0.0 network appear in the routing table?
- Can you still get to your partner's loopback interface?

Lab 4 – Default Route

(Builds on Lab 3)

On R1 Create additional loopbacks

R1(config)#**int loopback 1**
R1(config-if)#**ip address 1.0.0.1 255.0.0.0**
R1(config-if)#**int loopback 2**
R1(config-if)#**ip address 2.0.0.1 255.0.0.0**
R1(config-if)#**int loopback 3**
R1(config-if)#**ip address 3.0.0.1 255.0.0.0**
R1(config-if)#**int loopback 4**
R1(config-if)#**ip address 4.0.0.1 255.0.0.0**

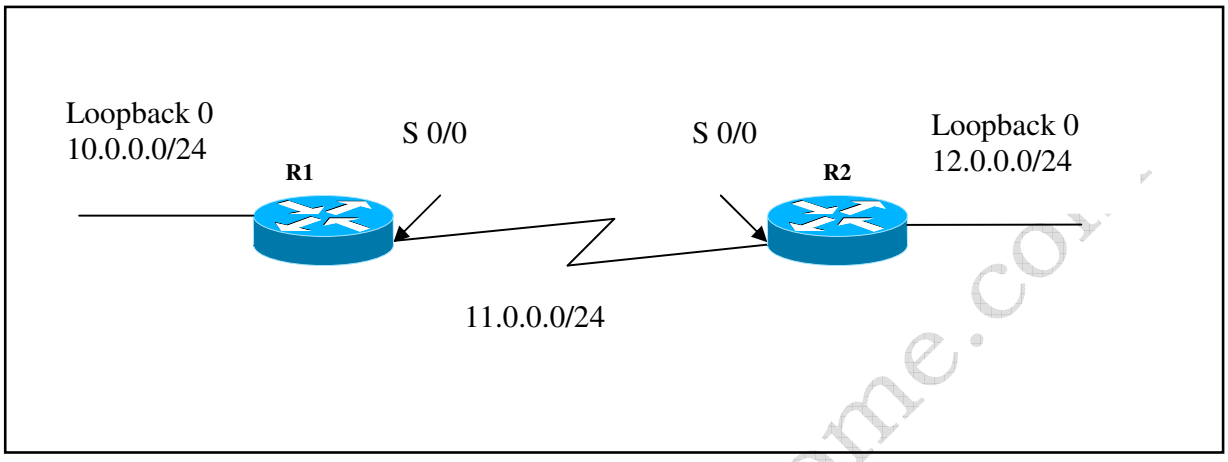
On R2 Create a Default route towards R1

R2(config)#**ip route 0.0.0.0 0.0.0.0 11.0.0.1**

On R2

- Type **Show ip route**
- Do you see routes for the new Loopback networks that were created on R1.
- Do you see a route with an Asterisk?
- What is the gateway of last resort?
- Ping 1.0.0.1 or 2.0.0.1 or 3.0.0.1 or 4.0.0.1.
- Are you successful?

Lab 5 – Basic RIP Configuration



Router 1

Router>**en**
Router#Config t
Router(config)#Hostname R1
R1(config)#interface Loopback 0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#interface S 0/0
R1(config-if)#**ip address 11.0.0.1 255.0.0.0**
R1(config-if)#**clock rate 128000** (if required)
R1(config-if)#**no shut**
R1(config-if)#**exit**
R1(config)#**router rip**
R2(config-router)#**network 10.0.0.0**
R2(config-router)#**network 11.0.0.0**

Router 2

Router>**en**
Router#Config t
Router(config)#Hostname R2
R2(config)#interface Loopback 0
R2(config-if)#ip address 12.0.0.1 255.0.0.0
R2(config-if)#interface S 0/0
R2(config-if)#**ip address 11.0.0.2 255.0.0.0**

R2(config-if)#**clock rate 128000** (if required)

R2(config-if)#**no shut**
R2(config-if)#**exit**
R2(config)#**router rip**
R2(config-router)#**network 11.0.0.0**
R2(config-router)#**network 12.0.0.0**

On Both Routers

Type **Show ip route**

- What networks do you see listed?
- Ping your partner's Loopback Interface address. Are you successful?

Lab 6– RIP Operation

(Builds on Lab 5)

On Both Routers

Rx#**debug ip rip (Where x is your Router number)**

```
RIP:    Sending V1 update to 255.255.255.255 via Serial 0/0 (11.0.0.1)
RIP:    Build update entries
            Network 10.0.0.0 metric 1
RIP:    Sending V1 update to 255.255.255.255 via Loopback 0 (10.0.0.1)
RIP:    Build update entries
            Network 12.0.0.0
            Network 11.0.0.0
RIP:    received V1 update from 11.0.0.2 on serial 0/0
            12.0.0.0 in 1 hop
```

Interesting Facts

- Does not include the directly connected network (11.0.0.0) in its update
- Does not include 12.0.0.0 network although it does exist in its routing table
- The destination address is a Broadcast
- It does not send periodic updates at constant intervals (Time Jitters)

On Router1

R1(config)#**int loopback 0**
R1(config-if)#**shut**

```
RIP:     build flash update entries
            network 10.0.0.0 metric 16
RIP:    received v1 update from 11.0.0.0 on Serial0/0
            2.0.0.0 in 16 hops (inaccessible)
RIP:    sending v1 update to 255.255.255.255 via Serial0/0 (11.0.0.1)
```

Interesting Facts

- When a route goes down, the router does not wait for Periodic Update. It sends a Triggered update with a Poisoned route with a metric of 16
- Notice R2 also sends an immediate Triggered Update back, indicating that you can't reach 10.0.0.0 cannot be reached through it.

On Router1

R1(config)#**int loopback 0**
R1(config-if)#**no shut**

Passive Interfaces

On Both Routers

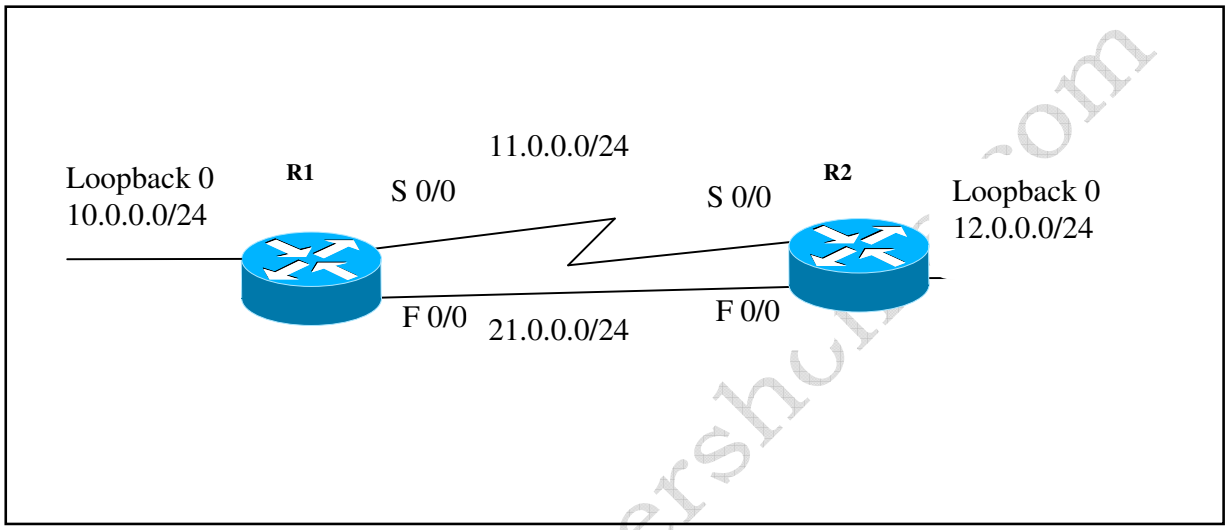
Rx(config)#**router rip**
Rx(config-router)#**passive interface Loopback 0**

Interesting Facts

- The router stops advertising from the Loopback interface. The command is useful for cutting down unnecessary broadcast over an interface that only has hosts on it and no router.

Lab 7– Load Balancing Using RIP

(Builds on Lab 6)



Router 1

Router>**en**
Router#Config t
R1(config)#interface F 0/0
R1(config-if)#**ip address 21.0.0.1 255.0.0.0**
R1(config-if)#**no shut**
R1(config-if)#**exit**
R1(config)#**Router rip**
R1(config-router)#**network 21.0.0.0**

Router 2

Router>**en**
Router#Config t
R2(config)#interface F 0/0
R2(config-if)#ip address 21.0.0.2 255.0.0.0
R2(config-if)#**no shut**
R2(config-if)#**exit**
R2(config)#**Router Rip**
R2(config-router)#**network 21.0.0.0**

On R1

- Type **Show ip route 12.0.0.0**

- Do you see an Asterisks (*) against one of the routes?
  Note: The Asterisks represents the next path the router will take to get the packet to the destination

- Type **Ping 12.0.0.1.**

- Type **Show ip route 12.0.0.0**
  Note: The Asterisks is against the other route.

On R2

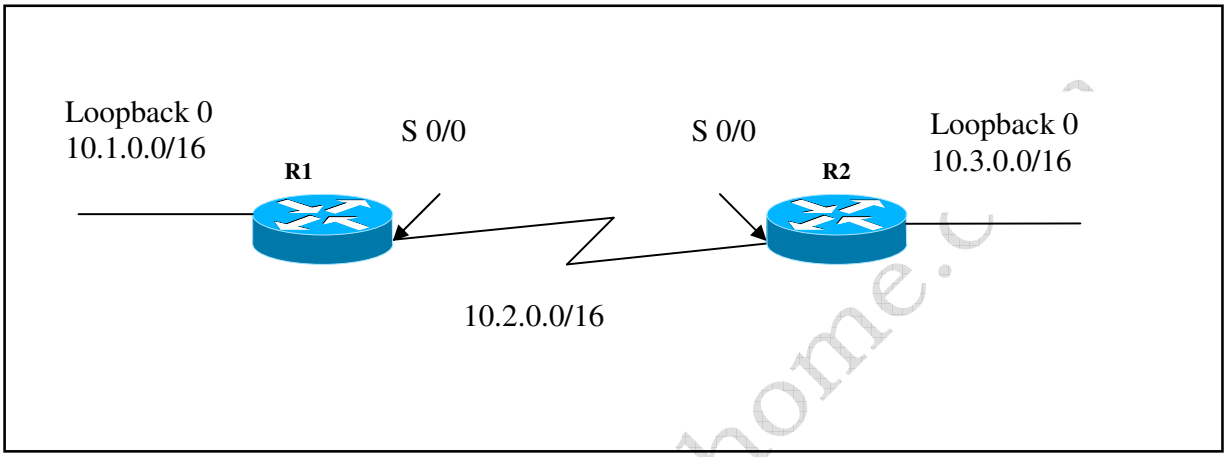
- Type **Show ip route 10.0.0.0**

- Do you see an Asterisks (*) against one of the routes?
  Note: The Asterisks represents the next path the router will take to get the packet to the destination

- Type **Ping 10.0.0.1.**

- Type **Show ip route 10.0.0.0**
  Note: The Asterisks is against the other route

Lab 9 - Basic RIP V2 Configuration



Router 1 Configuration

Router>**en**
Router#Config t
Router(config)#Hostname R1
R1(config)#interface Loopback 0
R1(config-if)#ip address 10.1.0.1 255.255.0.0
R1(config-if)#interface s 0/0
R1(config-if)#**ip address 10.2.0.1 255.255.0.0**
R1(config-if)#**clock rate 128000** (if required)
R1(config-if)#**no shut**
R1(config-if)#**router rip**
R1(config-router)#**version 2**
R1(config-router)#**network 10.0.0.0**

Router 2 Configuration

Router>**en**
Router#Config t
Router(config)#Hostname R2
R2(config)#interface S 0/0
R2(config-if)#ip address 10.2.0.2 255.255.0.0
R2(config-if)#**clock rate 128000** (if required)
R2(config-if)#**no shut**

R2(config-if)#interface Loopback 0
R2(config-if)#**ip address 10.3.0.1 255.255.0.0**
R2(config-if)#**router rip**
R2(config-router)#**version 2**
R2(config-router)#**network 10.0.0.0**

On Both Routers

- Go to Privileged Exec Mode (en)
- Type Sh IP route
- What routes do you see?

- Ping your partner's Loopback IP Address.
- Are you successful?

Lab 10 – RIP 2 Operations

(Builds on Lab 9)

On Both Routers

Rx#**debug ip rip (Where x is your Router number)**

```
RIP:    Sending V2 update to 224.0.0.9 via Serial 0/0 (11.0.0.1)
RIP:    Build update entries
            Network 10.0.0.0/8 metric 1, External Tag 0
RIP:    Sending V2 update to 224.0.0.9 via Loopback 0 (10.0.0.1)
RIP:    Build update entries
            Network 12.0.0.0/8 metric 2, External Tag 0
            Network 11.0.0.0/8 metric 1, External Tag 0
RIP:    received V2 update from 11.0.0.2 on serial 0/0
            12.0.0.0/8 in 2 hop metric 1, External Tag 0
```

Interesting Facts

- Update is a V2 Update
- Includes the Subnet Mask
- The destination address.

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK

Module:6 - Advanced RoutingProtocols

Enhanced IGRP (EIGRP)

- Cisco proprietary routing protocol.
- First released in 1994 with IOS version 9.21.
- Advance Distance Vector/Hybrid routing protocol that has the behavior of distance vector with several Link State features, such as dynamic neighbor discovery.

Features

- **Rapid Convergence**: EIGRP uses DUAL to achieve rapid convergence. It stores a backup route if one is available, so it can quickly re-converge incase a route goes down. If no backup route exists, EIGRP will send a query to its neighbor/s to discover an alternate path. These queries are propagated until an alternate route is found.
- **Reduced Bandwidth** Usage/Incremental Updates: In EIGRP updates are still sent to directly connected neighbors, much like distance vector protocols, but these updates are:
  - **Non-Periodic:** The updates are not sent at regular intervals, rather when a metric or a topology change occurs.
  - **Partial:** Updates will include the routes that are changed and not every route in the routing table.
  - **Bounded:** Updates are sent to affected routers only.

  Another issue regarding bandwidth usage is the fact that EIGRP by default will only consume 50% of the bandwidth of the link during convergence. This parameter can be adjusted to a higher or lower value eith the following command:
  Ip bandwidth-percent eigrp <AS number> <number that represents the percentage>
- **Classless Routing Protocol:** This means that advertised routes will include their subnet mask, this feature will eliminate the issue pertaining to discontiguous networks. VLSM and Manual Summarization is also supported on any router within the enterprise.

- **Security:** With IOS version 11.3 or better, EIGRP can authenticate using only MD5, the reason EIGRP does not support clear text is because, EIGRP can only be used within CISCO routers, and all Cisco routers support MD5 authentication. But the routes are not encrypted, so a sniffer can easily see the password/s.

- **Multiple Network Layer Protocol Support:** EIGRP can support IP, IPX, and AppleTalk, whereas the other routing protocols support only one routed protocol. EIGRP will also perform auto-redistribution with NLSP, IPXRIP, RTMP. EIGRP supports incremental SAP and RIP updates, 224 HOPS, and it uses bandwidth + delay which is far more better than just Ticks and Hops used by IPXRIP. For RTMP it supports event driven updates, but it must run in a clientless networks(WAN), and also a better metric calculation.

- **Use Of Multicast Instead Of Broadcast:** EIGRP uses multicast address of 224.0.0.10 instead of broadcast.

Open Shortest Path First (OSPF)

History

- OSPF Version 1 was specified in RFC 1131 in 1988. This protocol was finalized in 1989.
- OSPF Version 2 (Current version). The most recent specifications are specified in RFC 2328.

OSPF Features

- Scales better than Distance Vector Routing protocols. It virtually has no practical Hop Count Limit.
- Provides Load Balancing (Equal and Unequal).
- Introduces the concept of Area's to ease management and control traffic.
- Provides Authentication.
- Uses Multicast versus Broadcasts.
- Convergence is Faster than in Distance Vector Routing protocols. The reason for that is it floods the changes to all neighboring routers simultaneously rather than in a chain.
- Supports Variable Length Subnet Masking (VLSM), FLSM and Supernetting.
- Provides bit-based Route summarization.
- There are no periodic updates. Updates are only sent when there are changes.
- Router only send changes in updates and not the entire full tables.
- OSPF uses a Cost Value, instead of hop count. Cost is based on the speed of the link. Cost = 10^8/Bandwidth.
- Classless Routing Protocol.
- It relies on IP to deliver the Packets. Use port 89.

Areas

- Area is a logical grouping of OSPF routers.
- Areas divide an OSPF domain into sub-domains.
- Areas allow OSPF to be extremely scalable.
- Areas reduce the Memory, CPU utilization and amount of traffic in a network.
- Most of the traffic can be restricted to within the area.
- Routers within an area will have no detailed knowledge of the topology outside of their area.

- Reduced size of the Database reduces Memory requirements for the routers.

- Area's identified by a 32-bit Area ID. Can be denoted in Decimal format(0) or Dotted format (0.0.0.0)
- OSPF requires one area to be Area 0, known as the backbone area.
- Backbone area or Area 0, connects all the other area to each other.
- Three types of Traffic may be defined in relation to areas:
    - Intra-area traffic consists of packets that are passed between routers within a single area.
    - Inter-area traffic consists of packets that are passed between routers in different areas.
    - External traffic consists of packets that are passed between a router within the OSPF domain and a router within another Autonomous systems.

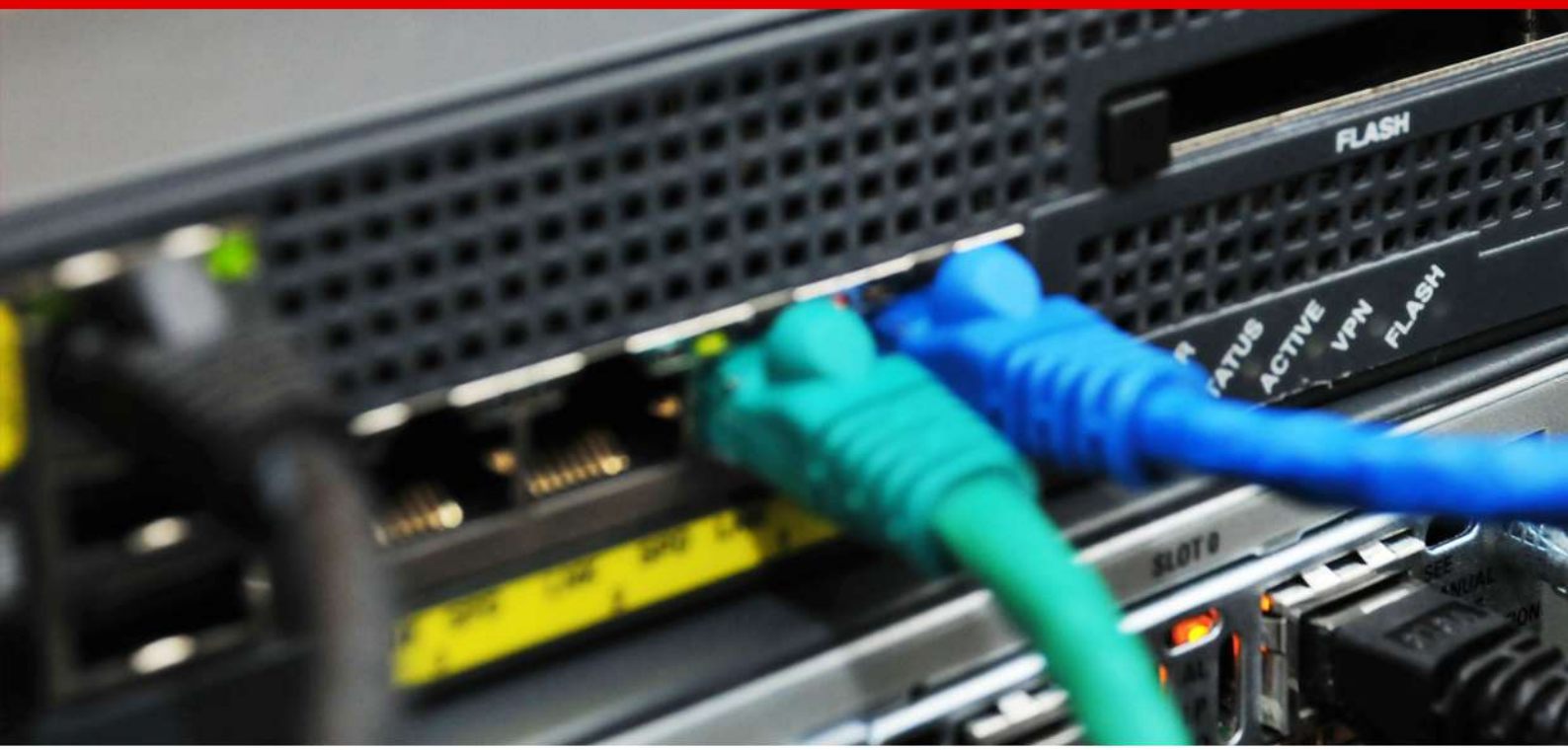
NETWORKERS HOME

IGNITE YOUR GENIUS

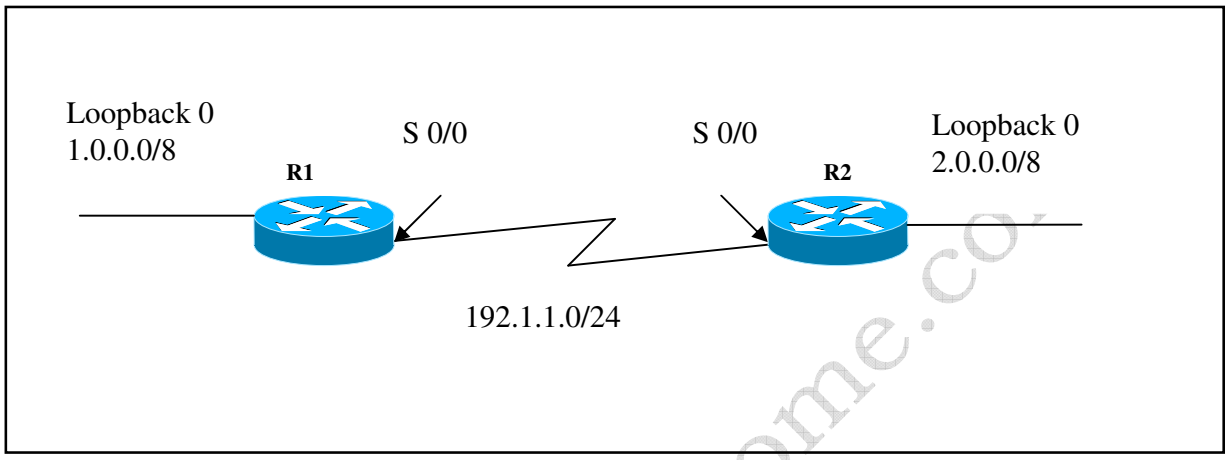
Cisco Certified Network Associate (CCNA)

WORK BOOK

Module:6 - Advanced Routing Protocols Labs



Lab 1 - Basic EIGRP Operation



R1 Configuration

Interface	IP Address	Subnet Mask
Loopback 0	1.1.1.1	255.0.0.0
S 0/0	192.1.1.1	255.255.255.0

R2 Configuration

Interface	IP Address	Subnet Mask
Loopback 0	2.2.2.2	255.0.0.0
S 0/0	192.1.1.2	255.255.255.0

On R1

router#**conf t**
router(config)#**hostname R1**
R1(config)#**Router eigrp 1**
R1 (config-router)#**net 1.0.0.0**
R1 (config-router)#**net 192.1.1.0**

On R2

Router#**conf t**
router(config)#**hostname R2**
R2(config)#**Router eigrp 1**

R2 (config-router)#**net 2.0.0.0**
R2 (config-router)#**net 192.1.1.0**

Test the Configuration

- Type **SH IP ROUTE**
- What routes do you see?
- Are the metrics advertised correct?
- Breakdown the Calculation for the Metric.

  Metric = Bandwidth $_{(min)}$ + Delay$_{(sum)}$

- Type **SH IP EIGRP NEIGHBOR**

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	192.1.1.2	Se0/0	10	00:06:21	12	200	0	2

- What is the Hello Time?
- Type **SH IP EIGRP TOPOLOGY.** This shows the Topology table.
- Type **SH IP EIGRP TOPOLOGY 2.0.0.0.**
- Notice the Vector and Composite Metric
- Type **SH IP EIGRP TRAFFIC**
- See how the Hello # are changing and updates are not.
- Bring the loopback interface down
- Note the Values in the output. See how the queries number increased
- Bring the loopback interface back up
- Note how the update # changes

Changing the Hello-interval and Hold-time timers

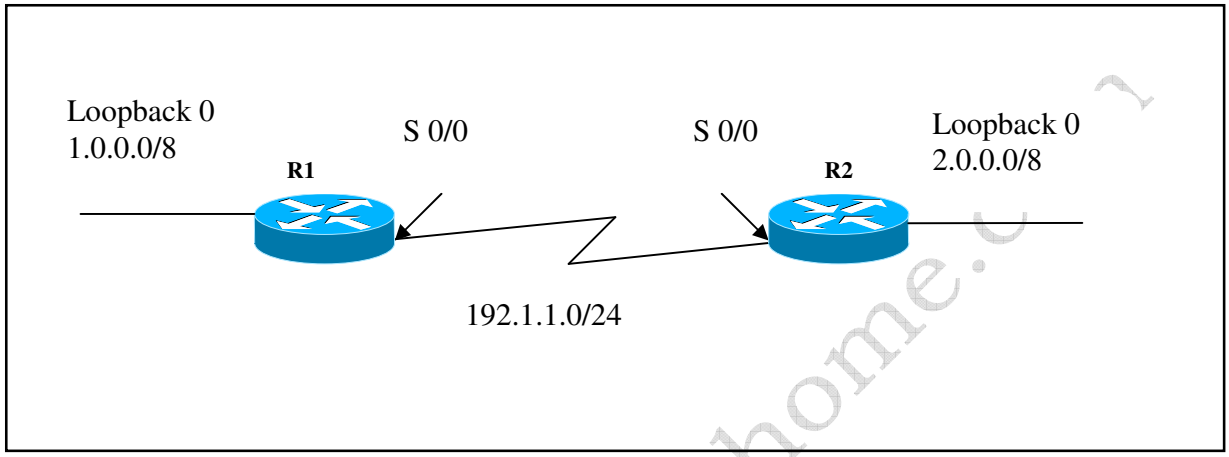
On Both Routers

R1(config)#**int S 0/0**
R1(config-if)#**ip hello-interval eigrp 1 20**
R1(config-if)#**ip hold-time eigrp 1 60**

- Type **SH IP EIGRP NEIGHBOR**

- What and whose time do you see?

Lab 2 – OSPF in a Point-to-Point Configuration



R1 Configuration

Interface	IP Address	Subnet Mask
Loopback 0	1.1.1.1	255.0.0.0
S 0/0	192.1.1.1	255.255.255.0

R2 Configuration

Interface	IP Address	Subnet Mask
Loopback 0	2.2.2.2	255.0.0.0
S 0/0	192.1.1.2	255.255.255.0

On R1

router#**conf t**
router(config)#**hostname R1**
R1(config)#**Router ospf 1**
R1 (config-router)#**net 1.0.0.0 0.255.255.255 area 0**
R1 (config-router)#**net 192.1.1.0 0.0.0.255 area 0**

On R2

Router#**conf t**
router(config)#**hostname R2**
R2(config)#**Router ospf 1**

R2 (config-router)#**net 2.0.0.0 0.255.255.255 area 0**

R2 (config-router)#**net 192.1.1.0 0.0.0.255 area 0**

Test the Configuration

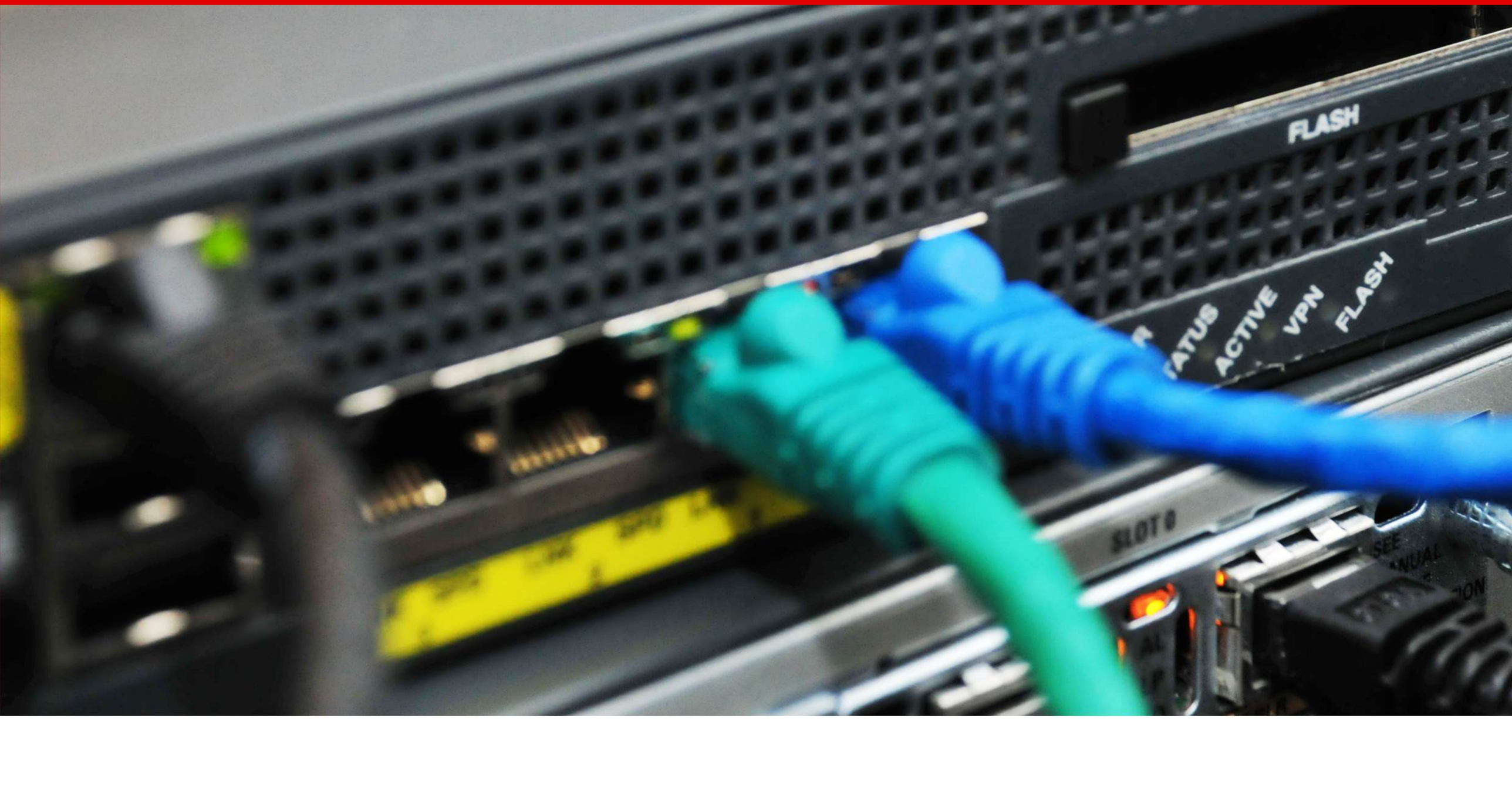
- Type **SH IP ROUTE**
- What routes do you see?
- Type **SH IP OSPF NEIGHBOR**
- Notice the State (Full/-). There is no DR or BDR in a Point-to-point network.
- Type **SH IP OSPF INT S 0/0**
- Notice the Network Type is POINT-TO-POINT and No DR or BDR information is displayed

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK Module:7 - Access Control Lists (ACL)



Access Lists

OVERVIEW

- Used to define the type of traffic that should be allowed or restricted from crossing a router (entering or exiting a router interface)
- Set of rules that help control flow of packets into or out of a router
- Statements that specify how the router will handle the traffic flow through specified interfaces

USES OF ACCESS LISTS

- Filter packet flow in/out of router interfaces
- Restrict/reduce contents of routing updates, e.g. from RIP, IGRP
- Identify packets that will initiate dial-on-demand connections (interesting packets)

TYPES OF ACCESS LISTS

- ***Standard Access Lists:*** Check source address of packets and permit or deny the packets based on network, subnet or host address.

- ***Extended Access Lists:*** Check both source and destination addresses for filtering. Packets can be filtered based on protocols within a suite (e.g. TCP/IP) and port numbers. Extended Access Lists add more granularity than Standard Access Lists.

Access Lists Operation and Application

- Operate in sequential, logical order, following a top-down order of tests
- If no conditions, or tests, are met, a final implicit deny will drop that particular packet
- Routers stop processing once the first instance of a condition is met in the written access list
- Only one access list per protocol per interface is permitted
- Access lists can be inbound or outbound, with reference to a router interface
- Location and sequential order can affect performance of router
- Written in global configuration mode (by the **access-list** command) and grouped, or linked in interface mode for the appropriate router interface (by the **access-group** command)

VERIFYING ACCESS LISTS

- **Show interface** or **show [ip|ipx] interface**
  Use to see if an interface is grouped to an access list
  Returns IP addresses and all configuration parameters
- **Show access-lists**
  Shows details of all access lists configured
- **Show [ip|ipx] access-list**
  Shows access lists for a specified protocol

ACCESS LISTS TYPES AND NUMBERS

Protocol	Type	Access List Number Range
IP	Standard	1-99
	Extended	100-199

WILDCARD MASK BITS

- 0 indicates that the corresponding bit should be checked
- 1 indicates that the corresponding bit should be ignored
- Examples
  00000111 indicates that only the last three bits in the corresponding octet should be ignored

  0.0.0.0 indicates any IP address – check all bits in all four octets

  255.255.255.255 indicates that all bits should be ignored – use the **any** statement

  Match any IP address 0.0.0.0 255.255.255.255 – any address, ignore all bits

  Match a specific IP address w.x.y.z 0.0.0.0 – check all bits so they match – use the **host** command, as follows: host w.x.y.z

CONFIGURING STANDARD IP ACCESS LISTS

- Creating the accessing list
  Router(config)#**access-list** [1-99] [permit|deny] *source_address wildcard_mask*

- Applying it to an interface

Router(config-if)#**ip access-group** [1-99] [in|out]

- Note the last statement in the access-group statement. In or out specifies incoming or outgoing traffic. By default, all access lists are applied to outgoing traffic, i.e. if the in or out statement is omitted, out will be applied.

EXAMPLES

Permitting only a specific network

To allow only traffic from 172.16.0.0 to pass through the router…

Access-list 1 permit 172.16.0.0 0.0.255.255
(implicit deny all – not necessary to write)

int e 0
ip access-group 1 out

Denying a specific host

To deny only the host 172.16.4.10 and permit everyone else to communicate with 172.16.3.0…

Configuring Extended IP Access Lists

OVERVIEW

- Extended IP Access Lists filter based on source and destination addresses, specific protocols and even ports defined by TCP or UDP
- Extended IP Access Lists offer more granularity than Standard Access Lists and can be used in a wider range of situations in providing access security to a network through a router

CONFIGURATION

- Creating the access list

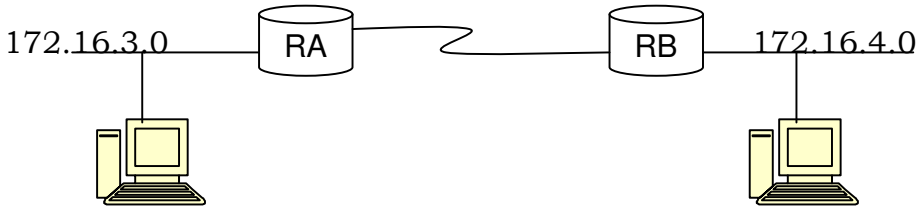
Router(config)#**access-list** [100-199] [permit|deny] [ip|tcp|icmp] *source_address source_mask destination_address destination_mask* [eq|neq|lt|gt] *port_number*

- Applying it to an interface

Router(config-if)#**ip access-group** [100-199] [in|out]

EXAMPLES

Blocking only FTP traffic from one network



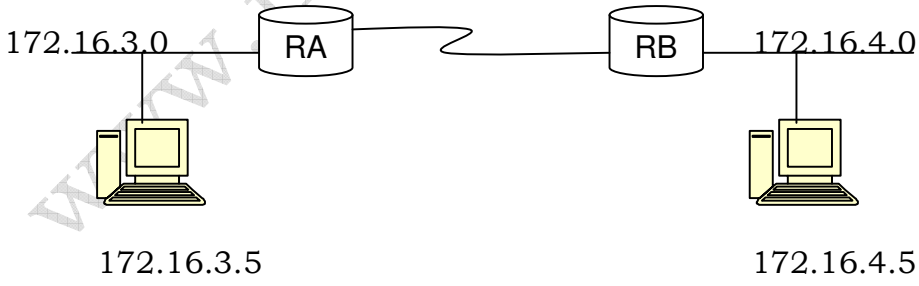
- The aim here is to block all FTP traffic from 172.16.3.0 entering 172.16.4.0 by creating an extended access list at RB

Access-list 101 deny tcp 172.16.3.0 0.0.0.255 172.16.4.0 0.0.0.255 eq 20
Access-list 101 deny tcp 172.16.3.0 0.0.0.255 172.16.4.0 0.0.0.255 eq 21
Access-list 101 permit ip any any
Int e 0/0
Ip access-group 101 out

Note the third line in the access list – it permits all other IP-based traffic

from anywhere going anywhere.

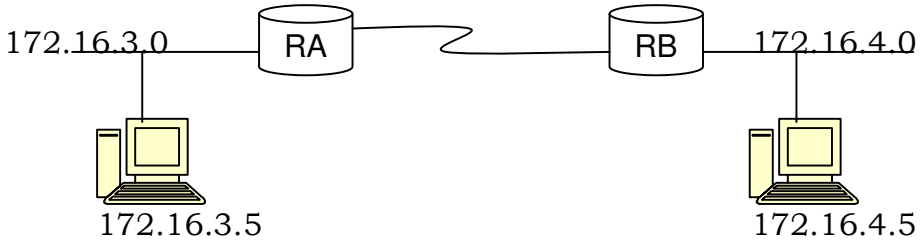
Denying all web-based (www) traffic entering a network



- The aim here is to block all networks from accessing the www service on the 172.16.4.0 network.

Access-list 101 deny tcp any any eq 80
Access-list 101 permit ip any any
Int e 0/0
Ip access-group 101 out

Denying a host from executing a ping statement to a network



- The aim here is to stop the host 172.16.3.5 from pinging other hosts on the 172.16.4.0 network.

Access-list 101 deny icmp host 172.16.3.5 any echo
Access-list 101 permit ip any any
Int e 0/0
Ip access-group 101 out

Verifying Access Lists

Show Access-lists displays the definition of all access lists that are created on the router.

Show IP access-lists displays the definition of IP access lists on this router.

Show IP interface displays the interface that are using a given access-list.

NETWORKERS HOME

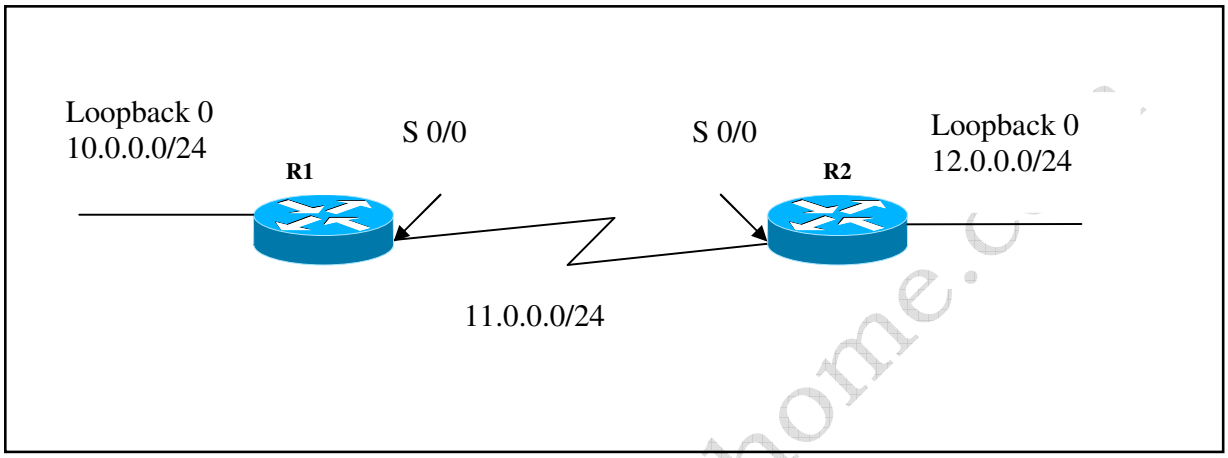
IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK

Module:7 - Access Control Lists (ACL)Labs

Lab 1 – Denying a Host Using Standard Access Lists



Router 1

Router>**en**
Router#Config t
Router(config)#Hostname R1
R1(config)#interface Loopback 0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#interface S 0/0
R1(config-if)#**ip address 11.0.0.1 255.0.0.0**
R1(config-if)#**clock rate 128000** (if required)
R1(config-if)#**no shut**
R1(config-if)#**exit**
R1(config)#**Router Rip**
R1(config-router)#**network 10.0.0.0**
R1(config-router)#**network 11.0.0.0**

Router 2

Router>**en**

Router#Config t
Router(config)#Hostname R2
R2(config)#interface Loopback 0
R2(config-if)#ip address 12.0.0.1 255.0.0.0
R2(config-if)#interface S 0/0
R2(config-if)#**ip address 11.0.0.2 255.0.0.0**
R2(config-if)#**clock rate 128000** (if required)
R2(config-if)#**no shut**
R2(config-if)#**exit**
R2(config)#**Router Rip**
R2(config-router)#**network 11.0.0.0**
R2(config-router)#**network 12.0.0.0**

On R1

Creating a Standard Access-list that blocks Host 12.0.0.1 from accessing R1

R1(config)#**Access-list 10 deny 12.0.0.1 0.0.0.0**
R1(config)#**Access-list 10 permit any**

Applying the access-list to the Serial Interface

R1(config)#**int S 0/0**
R1(config-if)#**ip access-group 10 in**

On R2

Testing the Standard Access list

- Ping your Partner's PC using Extended ping and using 12.0.0.1 as the source address by doing the following:
  - Type **Ping** and press enter
  - Press **Enter** on the Protocol prompt to accept **ip** as the protocol.
  - Specify 11.0.0.1 as the Target IP Address.
  - Take the default for the Count, Datagram and Timeout values.
  - Press **y** for extended commands
  - Type **12.0.0.1** for the Source Address
  - Take the defaults for the rest of the prompts.
- Are you successful?

- Why or why not?

Deleting the Access-List

R1(config)#**no access-list 10**
R1(config)#**int S 0/0**
R1(config-if)#**no ip access-group 10 in**

Lab 2 – Denying a Network Using Standard Access Lists

(Builds on Lab 1)

On R2

Creating a Standard Access-list that blocks Network 10.0.0.0 from accessing R2

R2(config)#**Access-list 10 deny 10.0.0.0 0.255.255.255**
R2(config)#**Access-list 10 permit any**

Applying the access-list to the Serial Interface

R2(config)#**int S 0/0**
R2(config-if)#**ip access-group 10 in**

On R1

Testing the Standard Access list

- Ping your Partner's PC using Extended ping and using 10.0.0.1 as the source address by doing the following:
    - Type **Ping** and press enter
    - Press **Enter** on the Protocol prompt to accept **ip** as the protocol.
    - Specify 11.0.0.2 as the Target IP Address.
    - Take the default for the Count, Datagram and Timeout values.
    - Press **y** for extended commands
    - Type **10.0.0.1** for the Source Address
    - Take the defaults for the rest of the prompts.
- Are you successful?
- Why or why not?

Deleting the Access-List

R2(config)#**no access-list 10**
R2(config)#**int S 0/0**
R2(config-if)#**no ip access-group 10 in**

Lab 3 – Denying an Entire Network from using Telnet

(Builds on Lab 2)

R1

Creating a Extended Access List that blocks anyone from Accessing the router via telnet to the Router

R1(config)#**Access-list 101 deny tcp any any eq 23**
R1(config)#**Access-list 101 permit ip any any**

Applying the access-list to the Serial Interface

R1(config)#**int S 0/0**
R1(config-if)#**ip access-group 101 in**

R2

Testing the Extended Access list

- Type **Telnet 11.0.0.1**.
- Are you successful?

Deleting the Access-List

R1(config)#**no access-list 101**
R1(config)#**int S 0/0**
R1(config-if)#**no ip access-group 101 in**

Lab 4 – Denying an Entire Network from Using HTTP

(Builds on Lab 3)

R1

Connecting the PC and configuring the Ethernet port on Router 1

- Connect the PC to the Router's Ethernet port using a Crossover cable.
- Configure the PC with the following configuration parameters:
    - IP Address : 20.0.0.2 255.0.0.0
    - Subnet Mask : 255.0.0.0
    - Default Gateway : 20.0.0.1
- On the Router, do the following:
    - R1#**Config t**
    - R1(config-t)#**int E 0/0**
    - R1(config-if)#**IP address 20.0.0.1 255.0.0.0**
    - R1(config-if)#**no shut**
    - R1(config-if)#**Router rip**
    - R1(config-router)#**network 20.0.0.0**

R2

Enabling HTTP on the Router

R2(config)#**IP http server**

PC 1

Testing the HTTP Server

- Open IE, on the PC and type **http://11.0.0.2.**
- Do you see the Router Web Page?

R2

Creating a Extended Access List that blocks anyone from using HTTP

R2(config)#**Access-list 150 deny tcp any any eq 80**
R2(config)#**Access-list 150 permit ip any any**

Applying the access-list to the Serial Interface

R2(config)#**int S 0/0**
R2(config-if)#**ip access-group 150 in**

Testing the Extended Access List

- Open IE, on the PC and type **http://11.0.0.2.**
- Do you see the Router Web Page?

Deleting the Access-List

R2(config)#**no access-list 150**
R2(config)#**int S 0/0**
R2(config-if)#**no ip access-group 150 in**

Lab 5 – Denying a Host from Pinging

(Builds on Lab 4)

R2

Creating an Extended Access List that blocks a Host from Pinging

R2(config)#**Access-list 101 deny icmp host 20.0.0.2 any echo**
R2(config)#**Access-list 101 permit ip any any**

Applying the access-list to the Serial Interface

R2(config)#**int S 0/0**
R2(config-if)#**ip access-group 101 in**

R1

Testing the Extended Access list

- On the PC, Type **Ping 11.0.0.2**.
- Are you successful?

R2

- On R2, Type **Ping 20.0.0.2**.
- Are you successful?
- Why or why not?

Deleting the Access-List

R2(config)#**no access-list 101**
R2(config)#**int S 0/0**
R2(config-if)#**no ip access-group 101 in**

Lab 6 – Denying a Network from Pinging

(Builds on Lab 5)

R1

Creating an Extended Access List that blocks a Network from getting Pinged

R1(config)#**Access-list 101 deny icmp any 20.0.0.0 0.255.255.255 echo**
R1(config)#**Access-list 101 permit ip any any**

Applying the access-list to the Serial Interface

R1(config)#**int S 0/0**
R1(config-if)#**ip access-group 101 in**

R2

- On R2, Type **Ping 20.0.0.2**.
- Are you successful?

R1

Testing the Extended Access list

- On the PC, Type **Ping 11.0.0.2**.
- Are you successful?
- Why or why not?

Deleting the Access-List

R1(config)#**no access-list 101**
R1(config)#**int S 0/0**
R1(config-if)#**no ip access-group 101 in**

Lab 7 – Named Access List

(Builds on Lab 6)

Creating a Named Standard Access-list on R1 that blocks Network 12.0.0.0 from coming into R1

R1(config)#**IP access-list standard DENY-12**
R1(config)#**deny 12.0.0.0 0.255.255.255**
R1(config)#**permit any**

Applying the access-list to the Serial Interface

R1(config)#**int S 0/0**
R1(config-if)#**ip access-group DENY-12 in**

On R2

Creating a Named Extended Access-list that blocks Network 10.0.0.0 from accessing the 12.0.0.0 Network

R2(config)#**IP access-list extended DENY-10-TO-12**
R2(config)#**deny 10.0.0.0 0.255.255.255 12.0.0.0 0.255.255.255**
R2(config)#**permit any**

Applying the access-list to the Serial Interface

R2(config)#**int S 0/0**
R2(config-if)#**ip access-group DENY-10-TO-12 in**

Testing the Named Access list

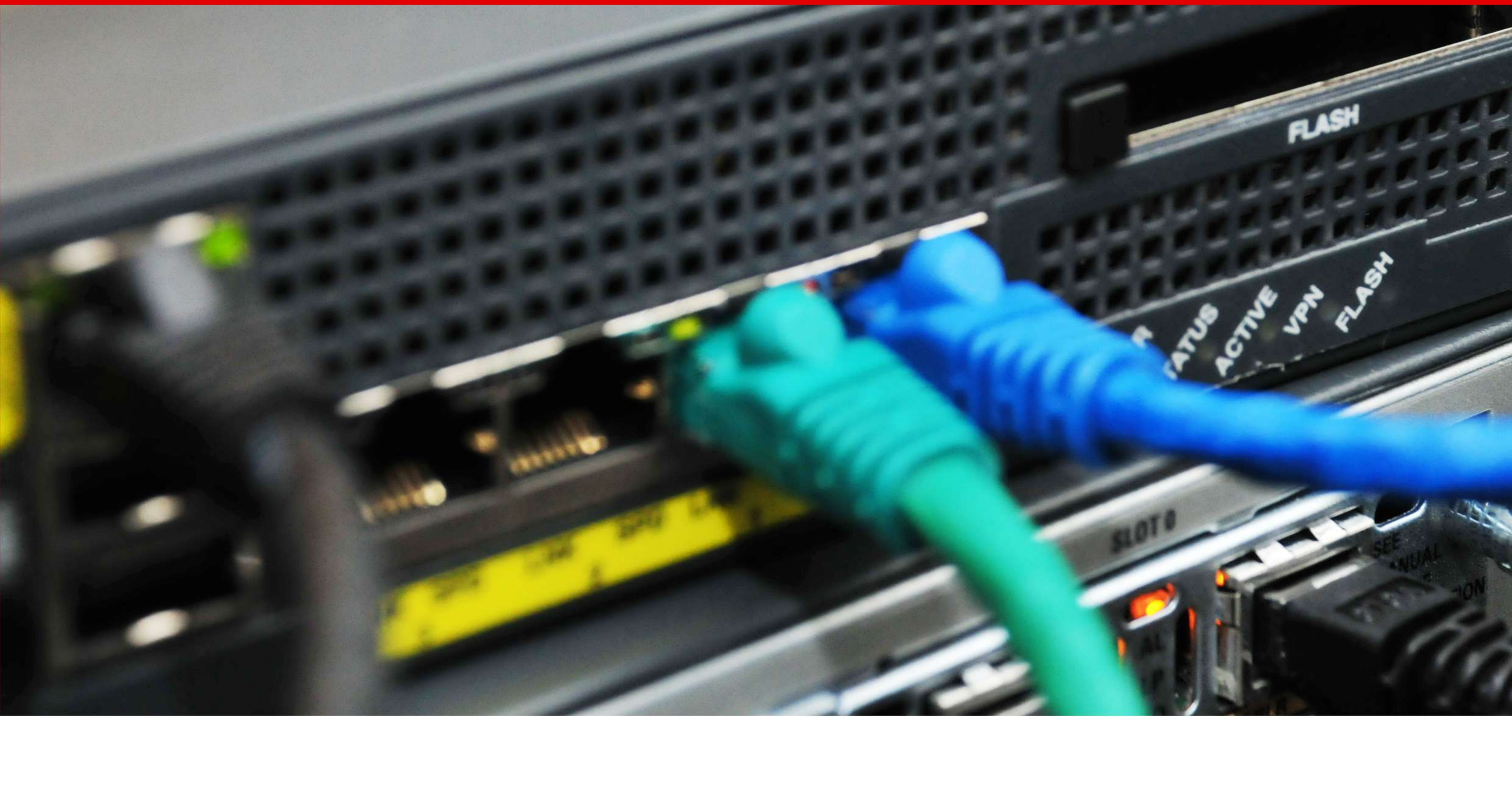
- Ping your Partner's Loopback.
- Are you successful?

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK Module:8 - Frame Relay



Frame Relay

OVERVIEW

- Frame Relay defines the interconnection process between the Customer Premises Equipment (CPE) device, such as a router, acting as a DTE and the service provider's local access switching equipment, acting as a DCE.
- Frame Relay is a Layer 2 packet-switched WAN protocol
- Frame Relay can be configured in a point-to-point or multipoint environment, through the use of subinterfaces.
- Frames are encapsulated in one of two formats:
  Cisco default, proprietary
  IETF use to connect to routers from different vendors (e.g. Lucent, Bay)

FRAME RELAY TERMINOLOGY

- **Local Access Rate (AR)**
  - Clock speed of connection to the Frame Relay cloud
  - Also known as local access loop, local loop

- **Data Link Connection Identifier (DLCI)**
  - Number that identifies the logical circuit between the CPE and FR switch (Layer 2)
  - DLCIs between each pair of routers are used to create a PVC
  - DLCIs only have local significance
  - DLCI numbers
    0-15 reserved for signaling
    16-991 available for use
    992-1007 reserved for layer 2 management
    1008-1023 in-channel signaling
  - Inverse ARP maps DLCI number (Layer 2) to IP address (Layer 3)

- **Local Management Interface (LMI)**
  - Protocol used for communication between Frame Relay switch and CPE
  - Signaling standard
  - LMI is responsible for managing the connection and maintaining status between the 2 devices
  - Keepalive packets verify that data is flowing between the 2 devices
  - LMI provides congestion notification

- 3 LMI standards
  Cisco (default)
  ANSI
  ITU Q.933a
- LMI sent every 10 seconds by default
- For IOS 10.3 and later, LMI type is auto-sensed (Frame Relay switch will send this to the router)
- To set the LMI type,

  Router(config)#**lmi-type** [cisco|ansi|itu]

❖ **Committed Information Rate (CIR)**
- Minimum guaranteed bandwidth for data transfer, within the Frame Relay cloud.

❖ **Oversubscription**
- When the sum of CIRs on all virtual circuits coming into a device exceed the access line speed. Once oversubscription occurs, packets are dropped.

❖ **Committed Burst (Bc)**
- Maximum number of bits the Frame Relay network agrees to transfer.

❖ **Excess Burst**
- Maximum number of uncommitted bits that the Frame Relay switch will attempt to transfer beyond the CIR
- Dependent on the service provider

❖ **Forward Explicit Congestion Notification (FECN)**
- When the Frame Relay switch recognizes congestion, it will set the DE bit to 1 in the Frame Relay packet bound for the destination. The destination router may drop the packet upon arrival.

❖ **Backward Explicit Congestion Notification (BECN)**
- When the router detects congestion, it sets the BECN bit to 1 and sends a packet to the source router, so the source router can reduce it's rate of transmission of packets

❖ **Discard Eligibility (DE)**
- When the router detects congestion, this bit is turned to 1 for oversubscribed traffic. Packets with a DE bit equal to 1 will be discarded first by receiving routers.

SUBINTERFACES

- Provide a method of separating one physical network connection into multiple logical connections, i.e. one local loop can support many PVCs
- A single physical interface (s 0/0) can simulate multiple logical interfaces (s 0/0.1, s 0/0.2, and so on), called subinterfaces.
- Subinterfaces can be configured to support 2 connection types:

Point-to-point

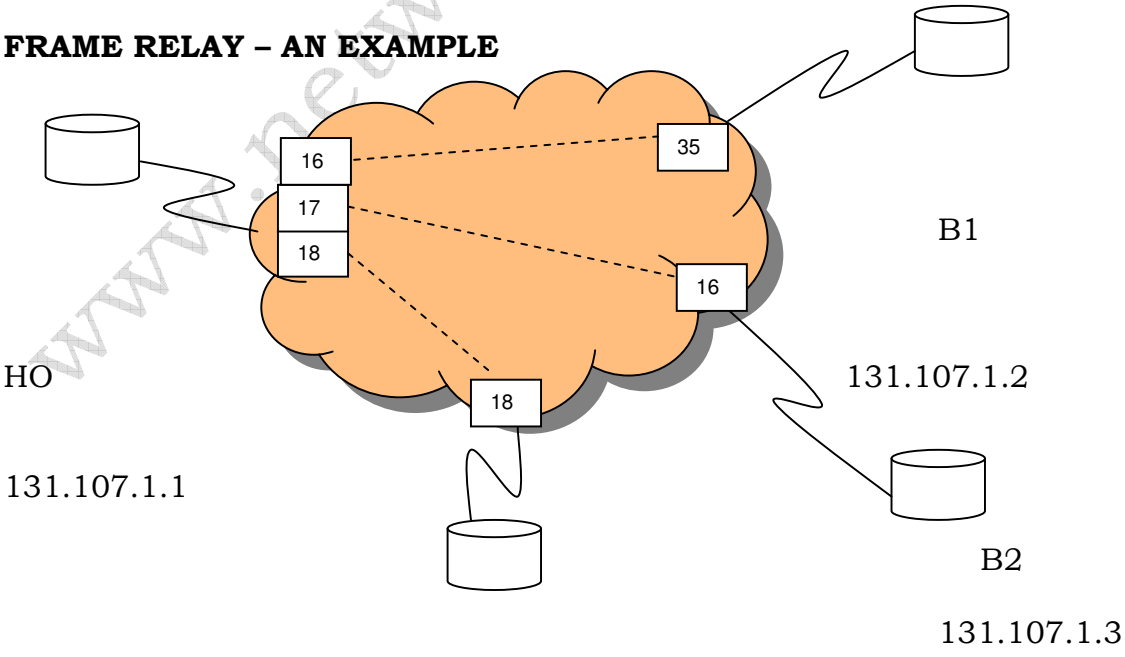
Does not forward broadcasts or routing updates
PVC connection is established from one subinterface to another
Interfaces are on the same subnet
Each subinterface has it's own local, unique DLCI number

Multipoint

Forwards broadcasts and routing updates
A single interface establishes multiple PVCs to multiple interfaces or subinterfaces on remote routers
All participating subinterfaces are on the same subnet, with unique local DLCIs

- Total number of subinterfaces = 1, …, 4294967293
- Subinterfaces can be added at any time, even during normal operation

FRAME RELAY – AN EXAMPLE



Once the DLCIs have been assigned by the service provider, mappings are created as follows (by Inverse ARP):

Router HO	
Local DLCI	*Destination Address*
16	131.107.1.2
17	131.107.1.3
18	131.107.1.4

Router B1	
Local DLCI	*Destination Address*
35	131.107.1.1

Router B2	
Local DLCI	*Destination Address*
16	131.107.1.1

Router B3	
Local DLCI	*Destination Address*
18	131.107.1.1

So, if router B1 wishes to forward a packet to router HO, it sends the packet through it's local DLCI 35, as all packets sent on that DLCI will get to 131.107.1.1 (router HO).

Now B1, B2 and B3 can each ping HO and vice versa, as there is a mapping of the path to get to the destination, butB1, B2 and B3 cannot ping each other.

For B1 to ping B2, for example, there must be a mapping from B1 to B2 via HO. This is done by the following command done at each respective router…

At router B1…

Frame-relay map ip 131.107.1.3 35

At router B2…

Frame-relay map ip 131.107.1.2 16

Similar mappings would need to be made for interconnecting B1 to B3 and B2 to B3.

Note	Mappings must be two-way for two-way communication, for example, ping.

This set up of routers is called a hub and spoke topology.

VERIFYING FRAME RELAY CONGIGURATION – USEFUL COMMANDS

- **Show frame-relay pvc**

  Shows DLCIs used and their status
  Shows LMI type
  Shows number of FECN and BECN bits received

- **Show ip route**

  Shows routing table

- **Show frame-relay map**

  Shows IP address to DLCI mapping
  Shows if link to remote site is up or down

- **Show frame-relay lmi**

  Shows lmi traffic status
  Shows if link to Frame Relay switch from CPE is up or down

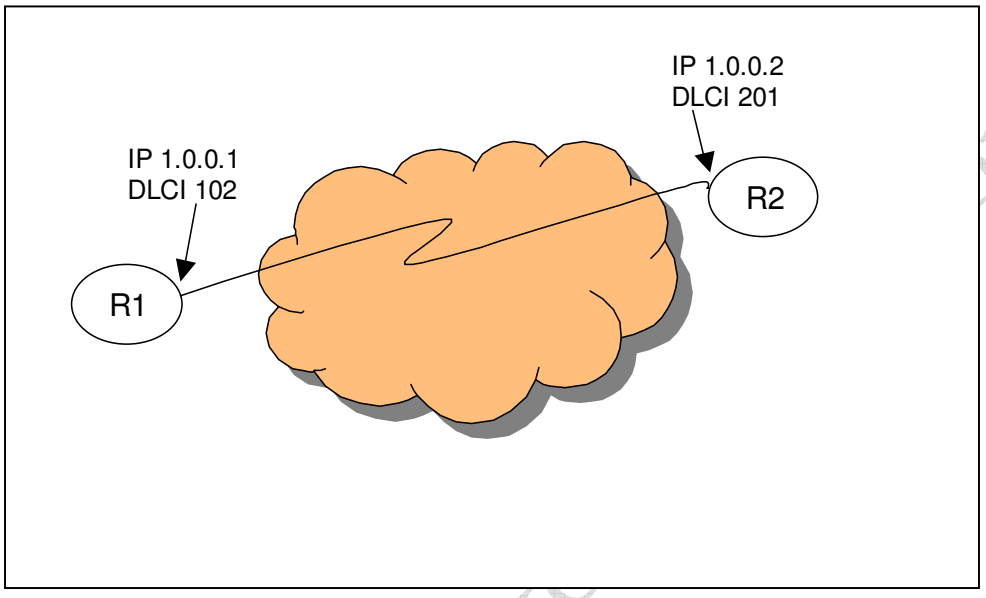
NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK Module:8 - Frame Relay Labs

Lab 1 – Point to Point Connection Using Frame-Relay



R1 Configuration

Router(config)#**hostname R1**
R1(config)#**int S 0/0**
R1(config-if)#**encap frame-relay**
R1(config-if)#**IP address 1.0.0.1 255.0.0.0**
R1(config-if)#**no shut**

R2 Configuration

Router(config)#**hostname R1**
R2(config)#**int S 0/0**
R2(config-if)#**encap frame-relay**
R2(config-if)#**IP address 1.0.0.1 255.0.0.0**
R2(config-if)#**no shut**

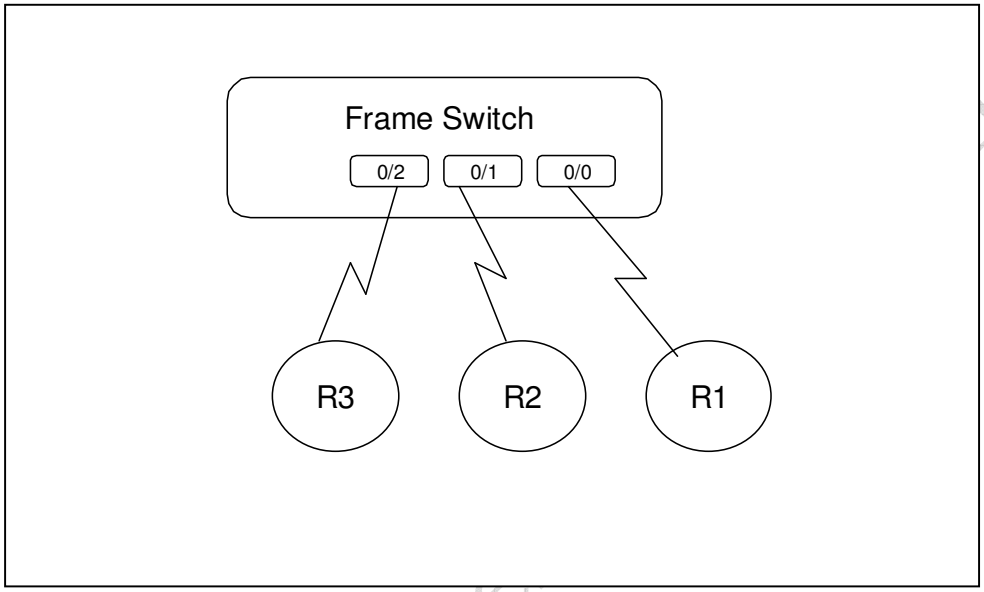
On Both Routers

- Type **SH Frame-relay lmi**.
- Notice the ***Number Status Enq. Sent*** and ***Number Status Msgs Rcvd*** numbers are the only ones that are changing.

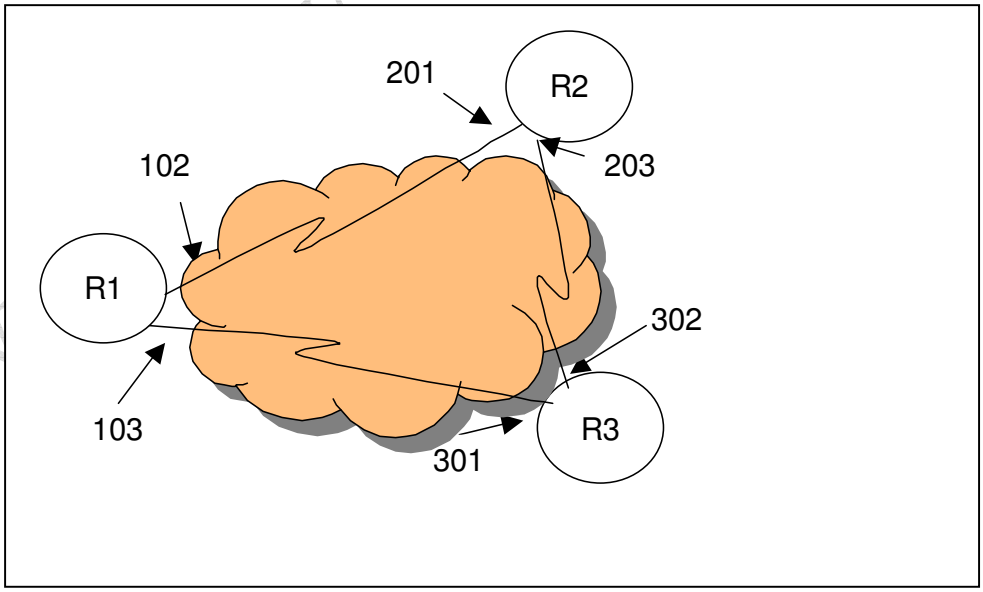
- The Lmi's are sent every 10 seconds. These are also known as Keepalives.
- Type **SH Frame-relay PVC.**
- Notice your Local DLCI number and it's status.
- Type **SH Frame-relay Map**.
- Notice it automatically maps your local DLCI number to the remote routers IP address.
- What is the this process called?
- Ping your partner's Router.
- Are you successful?

Lab 2 – Full Mesh Using Inverse ARP

Physical Layout



Logical Layout



On R1

R1#**conf t**
R1(config)#**int S 0/0**
R1(config-if)#**ip address 1.0.0.1 255.0.0.0**
R1(config-if)#**encapsulation frame-relay**
R1(config-if)#**no shut**

On R2

R2#**conf t**
R2(config)#**int S 0/0**
R2(config-if)#**ip address 1.0.0.2 255.0.0.0**
R2(config-if)#**encapsulation frame-relay**
R2(config-if)#**no shut**

On R3

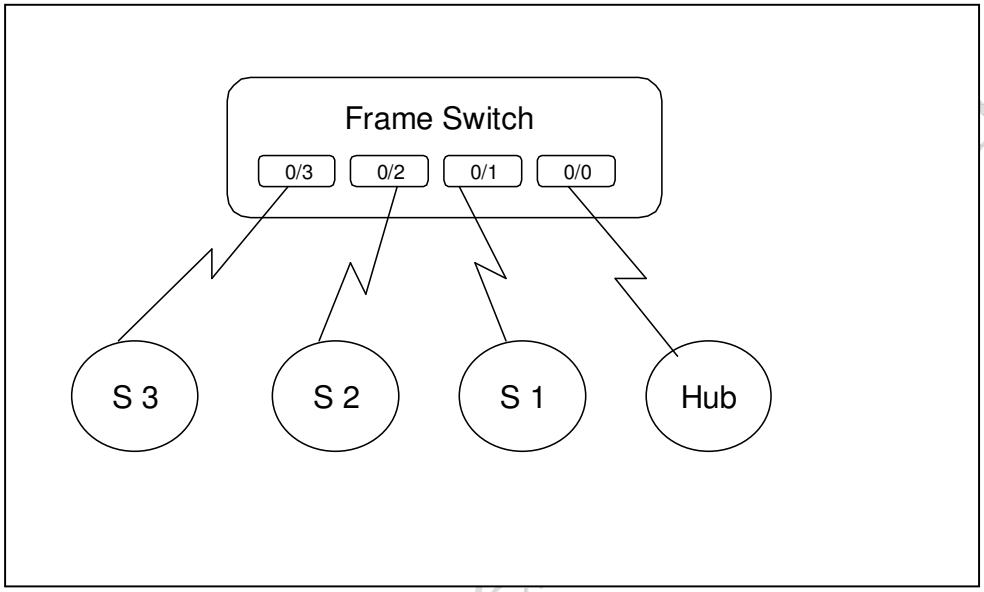
R3#**conf t**
R3(config)#**int S 0/0**
R3(config-if)#**ip address 1.0.0.3 255.0.0.0**
R3(config-if)#**encapsulation frame-relay**
R3(config-if)#**no shut**

On All Routers

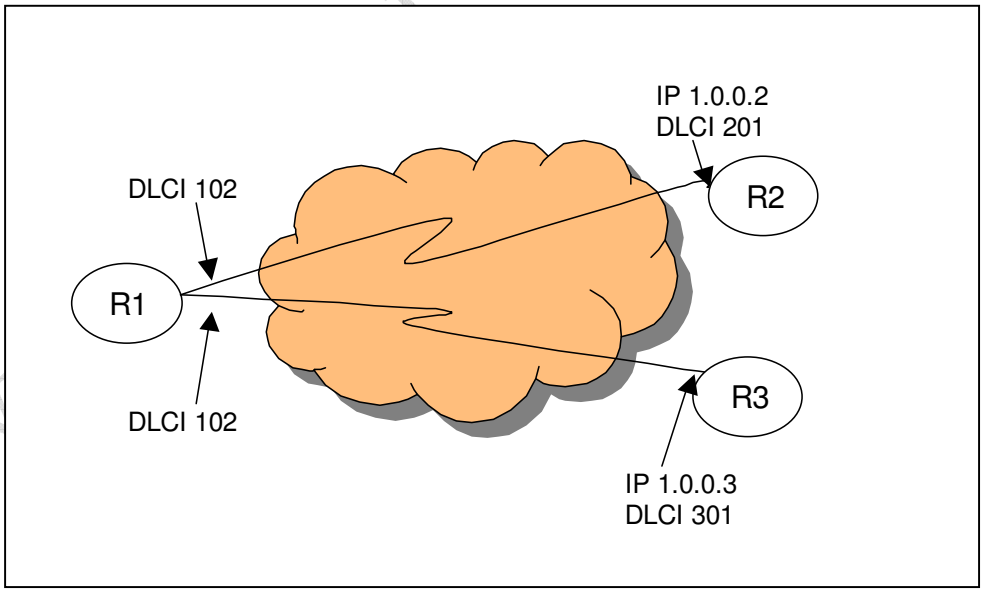
- Type **SH Frame-relay MAP**
- How many Frame-relay mappings do you see on all router?
- Can each router ping the other 2 routers?

Lab 3 – Hub-n-Spoke Using Inverse ARP

Physical Layout



Logical Layout



On Hub

hub#**conf t**
hub(config)#**int S 0/0**
hub(config-if)#**ip address 1.0.0.1 255.0.0.0**
hub(config-if)#**encapsulation frame-relay**
hub(config-if)#**no shut**

On S1

S1#**conf t**
S1(config)#**int S 0/0**
S1(config-if)#**ip address 1.0.0.2 255.0.0.0**
S1(config-if)#**encapsulation frame-relay**
S1(config-if)#**no shut**

On S2

S2#**conf t**
S2(config)#**int S 0/0**
S2(config-if)#**ip address 1.0.0.3 255.0.0.0**
S2(config-if)#**encapsulation frame-relay**
S2(config-if)#**no shut**

On All Routers

- Type **SH Frame-relay Map**.
- How many mappings do you have at the Hub?
- How many mappings do you have at the two spokes?
- Ping from one spoke to the other.
- Are you successful?

On the Spokes put in the Frame-relay map statements

On S1

S1(config)#**int S 0/0**
S1(config-if)#**frame-relay map ip 1.0.0.3 201**

On S2

S2(config)#**int S 0/0**

S2(config-if)#**frame-relay map ip 1.0.0.2 301**

On the Spoke Routers

- Ping from one spoke to the other.
- Are you successful?

Lab 4 – Hub-n-Spoke Using Sub-Interfaces

(Same Physical Layout and Switch Configuration as Lab)

Frame-Relay Configuration Using Subinterfaces

On Hub

hub#**conf t**
hub(config)#**int S 0/0**
hub(config-if)#**encapsulation frame-relay**
hub(config-if)#**no shut**
hub(config-if)#**exit**
hub(config)#**int S 0/0.1 point-to-point**
hub(config-subif)#**ip address 1.0.0.1 255.0.0.0**
hub(config-subif)#**frame-relay interface-dlci 102**
hub(config-fr-dlci)#**exit**
hub(config-Subif)#**exit**
hub(config)#**int S 0/0.2 point-to-point**
hub(config-subif)#**ip address 2.0.0.1 255.0.0.0**
hub(config-subif)#**frame-relay interface-dlci 103**
hub(config-fr-dlci)#**exit**
hub(config-Subif)#**exit**
hub(config)#**router rip**
hub(config-router)#**net 1.0.0.0**
hub(config-router)#**net 2.0.0.0**

On S1

S1#**conf t**
S1 (config)#**int S 0/0**
S1 (config-if)#**encapsulation frame-relay**
S1 (config-if)#**no shut**
S1 (config-if)#**exit**
S1 (config)#**int S 0/0.1 point-to-point**
S1 (config-subif)#**ip address 1.0.0.2 255.0.0.0**
S1 (config-subif)#**frame-relay interface-dlci 201**
S1 (config-fr-dlci)#**exit**
S1 (config-Subif)#**exit**
S1(config)#**router rip**
S1(config-router)#**net 1.0.0.0**

On S2

S2#**conf t**
S2(config)#**int S 0/0**
S2(config-if)#**encapsulation frame-relay**
S2(config-if)#**no shut**
S2(config-if)#**exit**
S2(config)#**int S 0/0.1 point-to-point**
S2(config-subif)#**ip address 2.0.0.2 255.0.0.0**
S2(config-subif)#**frame-relay interface-dlci 301**
S2(config-fr-dlci)#**exit**
S2(config-Subif)#**exit**
S2(config)#**router rip**
S2(config-router)#**net 2.0.0.0**

On the Spoke Routers

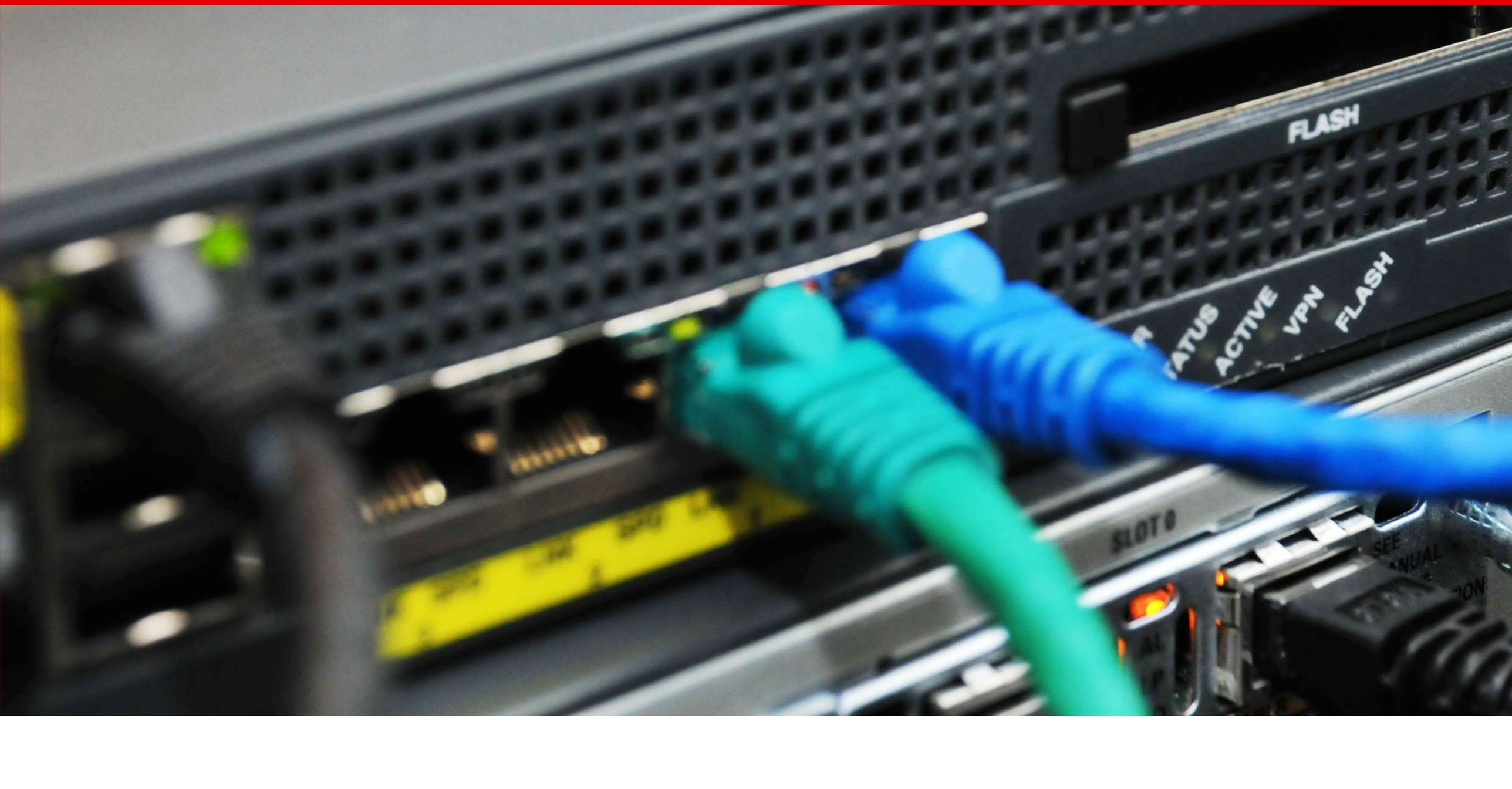
- Type **SH IP ROUTE**
- What routes do you see there?
- Can the Spokes ping Other Spoke Routers?

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK Module:9 - Cisco Discovery Protocol



Cisco Discovery Protocol (CDP)

OVERVIEW

- Provides details about directly connected Cisco devices, such as address, protocol used
- CDP starts automatically by default for IOS 10.3 and later
- CDP operates at Layer 2, so it is not necessary for the neighboring device to be in the same domain, or share a common network address for communication
- Advertisements about neighbors are multicast to the address 0100.0ccc.cccc
- Routes are learned through *hello* type updates

CDP PARAMETERS

- **CDP Timer**
  - How often updates are sent
  - Default = 60 seconds
  - To change default time
  - Router(config)#**cdp timer** *new_update_time*

- **CDP Holdtime**
  - The time the CDP packet sent should be kept by the receiving router before being discarded
  - Default = 180 seconds
  - To change default time
  - Router(config)#**cdp holdtime** *new_holdtime*

DISABLING AND ENABLING CDP

- To disable CDP
  - Router(config)#**no cdp enable**

- To disable CDP on an interface
  - Router(config-if)#**no cdp enable**

- To enable CDP
  - Router(config)#**cdp run**

SHOWING CDP NEIGHBOURS

- For each connected Cisco device, the following information can be displayed
  - Device ID router hostname/domain name
  - Local port type and # e.g. Ethernet 0/0
  - Holdtime
  - Device capability e.g. router, switch
  - Hardware platform e.g. 2600, 1900
  - IOS version
  - Neighbour's remote port type and number

- For a brief summary
  Router#**show cdp neighbors**

- For detailed information
  Router#**show cdp neighbors detail**

- To look at a single device
  Router#**show cdp entry** *router_name*

- To display information about your local router
  Router#**show cdp interface**

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK

Module:9 - Cisco Discovery Protocol (CDP) Labs

Lab 1 –3 – CDP Labs

********** ***Instructor Led*** **********

NETWORKERS HOME

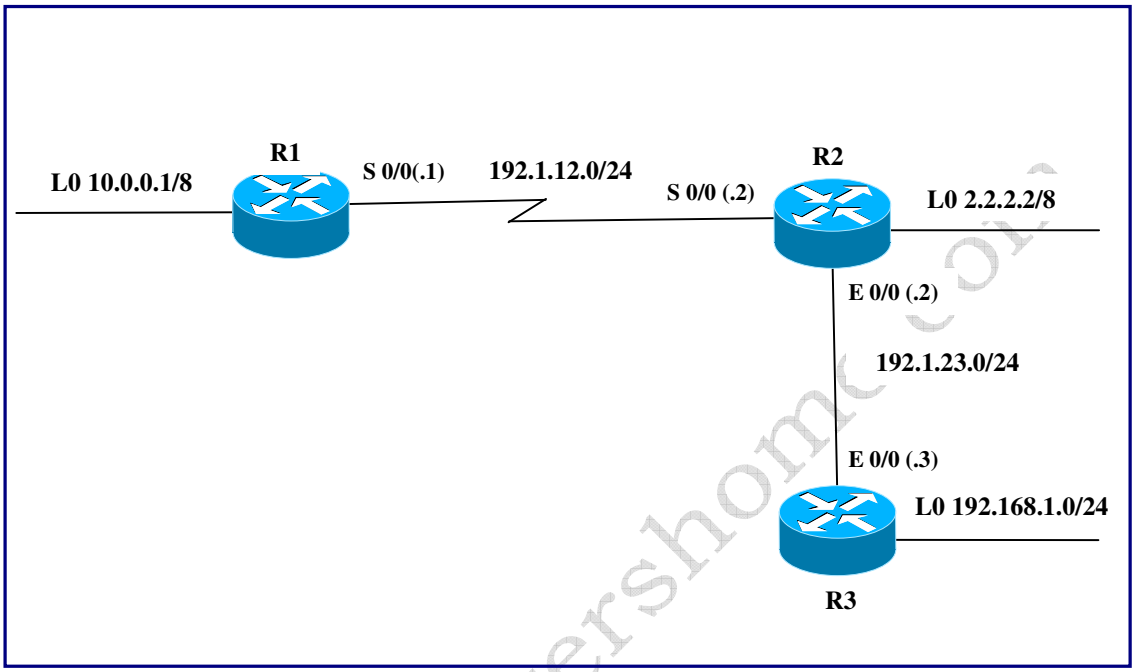
IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK

Module:10 - Network AddressTranslation (NAT) Labs

Lab -1 NAT



Objective: Configure NAT and PAT on R1 and R3 to route traffic from the private networks to the Internet (R2 – 2.2.2.2).

ISP (R2) assigns R1 a public range of 195.1.1.0/24 network. Configure R2 to route all packets destined for this network towards R1.

On R2

R2(config)#**ip route 195.1.1.0 255.255.255.0 192.1.12.1**

Translate the 10.0.0.0 Network behind R1 into a range of Class C addresses assigned to R1 by the ISP. Use the range 195.1.1.1 – 195.1.1.250 for the pool.

On R1

R1(config)#**access-list 121 permit ip 10.0.0.0 0.255.255.255 any**
R1(config)#**ip nat pool DP 195.1.1.1 195.1.1.254**
R1(config)#**ip nat inside source list 121 pool DP**
R1(config)#**interface Loopback0**

R1(config-if)#**ip nat inside**

R1(config-if)#**interface S0/0**
R1(config-if)# **ip nat outside**

R1 should use 195.1.1.251 for its Web Server so that people on the outside can access it. The internal web server is at 10.0.0.80. Configure a secondary address of 10.0.0.80 on the loopback address to test this configuration.

On R1

R1(config)#**ip nat inside source static 10.0.0.80 195.1.1.251**
R1(config)#**interface Loopback 0**
R1(config-if)#**ip address 10.0.0.80 255.0.0.0 secondary**

On R1

- Type **Show IP nat translations.** Do you see the static translation already present in the translation table.
- Ping 195.1.1.252 from R2. Are you successful?
- On R1, Ping **2.2.2.2** with the source of **10.0.0.1**.
- Are you successful?
- Type **Show IP nat translations.** Do you see the Dynamic translation done for the 10.0.0.1 as 195.1.1.1?

ISP (R2) assigns R3 a public range of 195.1.3.32/30 subnet. Configure R2 to route all packets destined for this network towards R3

On R2

R2(config)#**ip route 195.1.3.32 255.255.255.252 192.1.23.3**

Translate the 192.168.1.0 Network behind R3 using the 195.1.3.33 address (PAT). The entire should be able to go out simultaneously using this address.

On R3

R3(config)#**access-list 121 permit ip 192.168.1.0 0.0.0.255 any**
R3(config)#**ip nat pool DP 195.1.3.33 195.1.1.33**

R3(config)#**ip nat inside source list 121 pool DP overload**
R3(config)#**interface Loopback0**
R3(config-if)#**ip nat inside**
R3(config-if)#**interface E 0/0**
R3(config-if)# **ip nat outside**

There is a web server at 192.168.1.5 and a DNS server at 192.168.1.6. Translate these servers to 192.168.1.34 on the outside. Use Static PAT to accomplish this task.

On R3

R3(config)#**ip nat inside source static tcp 192.168.1.5 80 195.1.1.34 80**
R3(config)#**ip nat inside source static udp 192.168.1.6 80 195.1.1.34 53**
On R3

- Type **Show IP nat translations.** Do you see the static translation already present in the translation table.
- On R3, Ping **2.2.2.2** with the source of **192.168.1.1**.
- Are you successful?
- Type **Show IP nat translations.** Do you see the Dynamic translation done?

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK Module:11 - Switching

Switching

COLLISION DOMAINS

- A group of network nodes on an Ethernet network that share the network media that can experience collisions within a collision domain.
- Networks can be segmented into multiple collision domains for optimization of network functionality.

NETWORK SEGMENTATION USING BRIDGES

- Bridges operate at layer 2 and therefore use MAC addresses to decide whether to forward data
- Cisco routers can act as bridges.
- It increases the number of collision domains.
- Bridges build Layer 2 address table also called forwarding tables by *listening* to hosts communicate.
- It looks at the frames destination in its address table and sends the frame towards the destination host.
- Bridges maintain one logical network, network is only physically segmented

NETWORK SEGMENTATION USING ROUTERS

- Routers create separate collision domains by creating separate layer 3 networks.
- Layer 3 networks are referred to as Broadcast domains.
- In large networks, routers need to be able to carry the excessive load placed by a large number of hosts.

NETWORK SEGMENTATION USING SWITCHES

- A switch is essentially a bridge with multiple ports and intelligence
- Switches forward data based on MAC addresses as they operate at layer 2
- Switches will build forwarding tables the same way as bridges.
- Switches increase the number of collision domains
- Enables high speed data exchange
- LAN switches can operate in three different modes:
    - Cut-through
        - Frames forwarded as soon as the destination address is read and the forwarding table is consulted

        - Produces the lowest amount of latency
    - Fragment-free
        - Frames forwarded as soon as the first 64 bytes are received
    - Store and Forward
        - Frames forwarded once the entire frame is received
        - Ensures corrupt frames are not forwarded
        - Latency through the switch varies with frame length.
        - The switch receives the complete frame before beginning to forward it.
        - Highest latency

SWITCH FUNCTIONS

- **Address learning**
    - Initially MAC address table is empty – switch will flood networks to forward data
    - Hosts are added to the table as soon they start communicating
- **Frame filtering**
    - If the destination MAC address exists in the MAC address table, frame is not flooded, it is sent out only on the appropriate port
    - Broadcasts and multicasts are flooded to all ports, except the originating port
- **Loop avoidance**
    - Duplicate frames must be prevented from traveling over redundant paths that may exist for backup or transmission redundancy.
    - Broadcasts will continually flood around a loop structure – broadcast storm
    - Multiple copies of non-broadcast frames may be delivered to the same destination, causing errors
    - The same frame will be received on different ports of the same switch, causing instability in the MAC address table

LOOPING SOLUTION – SPANNING TREE PROTOCOL (STP)

- Algorithm developed by DEC, revised by IEEE (Specification 802.1d)
- STP is used to avoid switching loops.
- STP reconfigures as the network topology changes to avoid the creation of new loops
- STP enabled by default on all Cisco Catalyst switches

VIRTUAL LANs (VLANs)

- A VLAN is a broadcast domain, similar in concept to a domain

- Hosts in different VLANs cannot communicate with each other, unless their data is routed through a router
- VLANs can exist on a single switch, or they can span 2 or more switches. If two or more switches are used, they must be connected

  using the trunk port (fast Ethernet) and ISL (Inter Switch Link) encapsulation.
- ISL is Cisco proprietary for interconnecting multiple switches over the fast Ethernet (fa) ports.
- ISL operates at layer 2, it adds a new header section and a new FCS
- Fast Ethernet ports on routers have ISL capability.
- IEEE 802.1q is another encapsulation that can also be used to connect multiple switches with multiple VLAN's
- By default, all ports have membership of VLAN 1
- VLAN membership can be statically configured or dynamically, through a server or VMPS (VLAN Membership Policy Server)
- Up to 64 VLANs supported on 1900 switches

Frame Tagging

- Frame tagging assigns a unique user-assigned ID to each frame.
- A unique identifier is placed in the header of each frame as it is forwarded between switches.

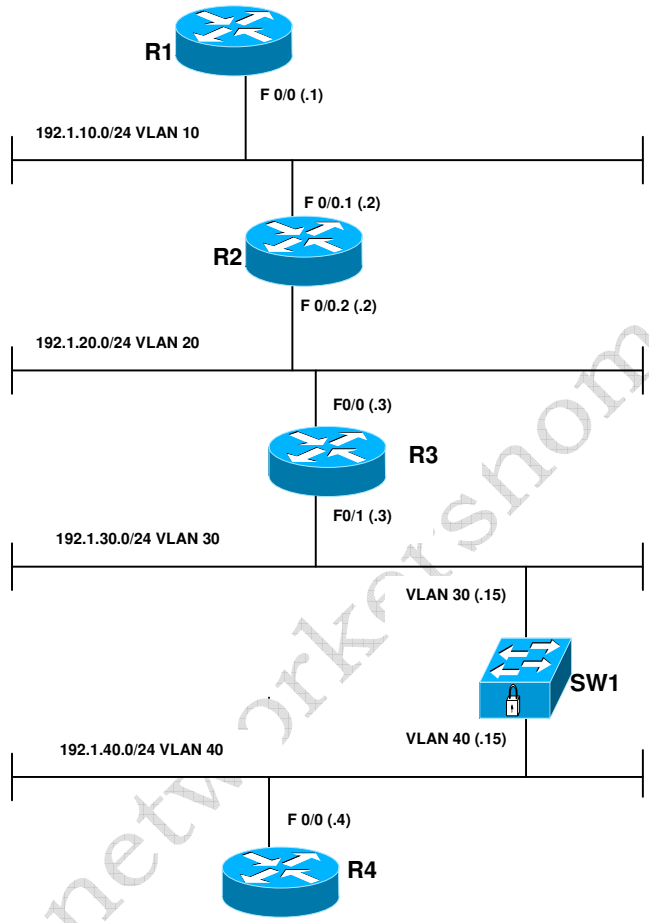
NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK Module:11 - Switching Labs

Lab 1-Creating and Routing with VLAN's



Configure Switch1 as the VTP Server and the other Switch(s) as VTP Clients. Use CISCO as the Domain name. Authenticate the relationship using CCNP as the password.

SW1

VTP domain CISCO
VTP mode server
VTP password CCNP

SW2

VTP domain CISCO
VTP mode client
VTP password CCNP

Configure the Trunk ports on the Switches using Dot1q as the encapsulation

On Both Switches

Interface range F0/XX – XX
Switchport trunk encapsulation dot1q
Switchport mode trunk

Create the VLANs based on the Diagram on the VTP Server (SW1)

SW1

VLAN 10
VLAN 20
VLAN 30
VLAN40

Assign the Switch Ports connected to Routers to the appropriate VLANs. Configure the ports that connect to a router that has Sub-interfaces as a Trunk using Dot1q as the encapsulation mechanism. Turn on IP Routing on SW1 to make it act as Layer 3 switch. Configure SW1 with SVI ports based on the Diagram

SW1

```
Interface F 0/1
 Switchport mode access
 Switchport access vlan 10
!
Interface F 0/2
 Switchport trunk encapsulation dot1q
 Switchport mode trunk
!
Interface F 0/3
 Switchport mode access
 Switchport access vlan 20
!
```

```
Interface F 0/4
 Switchport mode access
 Switchport access vlan 40
!
Ip routing
!
Interface VLAN 30
 Ip address 192.1.30.15 255.255.255.0
!
Interface VLAN 30
 Ip address 192.1.40.15 255.255.255.0
```

SW2

```
Interface F 0/3
 Switchport mode access
 Switchport access vlan 30
```

Configure the Routers with the IP Addresses based on the Diagram. Configure Loopback 0 on all routers and SW1. Use the format of X.X.X.X/8 for the IP address of the loopback. Use 15 for Switch1.

R1

```
Interface F 0/0
 Ip address 192.1.10.1 255.255.255.0
 No shut
!
Interface Loopback 0
 Ip address 1.1.1.1 255.0.0.0
```

R2

```
Interface F 0/0
 No shut
!
Interface F 0/0.1
 Encapsulation dot1q 10
 Ip address 192.1.10.2 255.255.255.0
!
Interface F 0/0.2
 Encapsulation dot1q 20
 Ip address 192.1.20.2 255.255.255.0
!
Interface Loopback 0
 Ip address 2.2.2.2 255.0.0.0
```

R3

```
Interface F 0/0
 Ip address 192.1.20.3 255.255.255.0
 No shut
!
Interface F 0/1
  Ip address 192.1.30.3 255.255.255.0
  No shut
!
Interface Loopback 0
 Ip address 3.3.3.3 255.0.0.0
```

R4

```
Interface F 0/0
 Ip address 192.1.40.4 255.255.255.0
 No shut
!
Interface Loopback 0
 Ip address 4.4.4.4 255.0.0.0
```

SW1

```
Interface Loopback 0
 Ip address 15.15.15.15 255.0.0.0
```

Configure RIP v2 on all the Routers and the Layer 3 Switch. Advertise the Loopback networks on the devices.

R1

```
Router Rip
 Version 2
 No auto-summary
 Network 1.0.0.0
 Network 192.1.10.0
```

R2

```
Router Rip
 Version 2
 No auto-summary
 Network 2.0.0.0
 Network 192.1.10.0
 Network 192.1.20.0
```

R3

```
Router Rip
 Version 2
 No auto-summary
 Network 3.0.0.0
 Network 192.1.20.0
 Network 192.1.30.0
```

R4

Router Rip
Version 2
No auto-summary
Network 4.0.0.0
Network 192.1.40.0

SW1

Router Rip
Version 2
No auto-summary
Network 15.0.0.0
Network 192.1.30.0
Network 192.1.40.0

Lab 2- Configuring Port Security

Task 1
Configure VLAN 50 on SW1. Configure Ports F 0/3 and F0/4 on SW2 in VLAN 50. Configure SW2 such that only R3 F 0/1 and R4 F 0/1 can connect to ports F 0/3 and F0/4 on SW2 respectively. If another port tries to connect to these ports, the ports should be error disabled.

SW1

VLAN 50

SW2

```
Interface F 0/3
 Switchport mode access
 Switchport access vlan 50
 Switchport port-security
 Switchport port-security mac xxxx.xxxx.xxxx
!
Interface F 0/4
 Switchport mode access
 Switchport access vlan 50
 Switchport port-security
 Switchport port-security mac xxxx.xxxx.xxxx
```

Task 2
Configure F 0/5 – F 0/8 in VLAN 50 on SW2. Enable Port Security for these ports such that only 1 MAC address can be connected to them. You would like to learn the MAC address dynamically.

SW2

```
Int range F 0/5 – F 0/8
Switchport mode access
Switchport access vlan 50
Switchport port-security
Switchport port-security mac-address sticky
```

Task 3
Configure F 0/15 also in VLAN 50 on SW2. Enable Port security for these ports such that 5 MAC addresses can be connected to this port. The first 2 MAC addresses that are allowed to connect are 0001.1010.AB12 and 0001.1010.AB13. The remaining 3 can be learned dynamically.

SW2

```
Int F 0/15
Switchport mode access
Switchport access vlan 50
Switchport port-security
Switchport port-security max 5
Switcport port-security mac-address 0001.1010.AB12
Switcport port-security mac-address 0001.1010.AB13
Switcport port-security mac-address sticky
```

Lab 3- Configuring Port Fast

Task 1

Configure the port range from F0/1 – 6 on SW1 in a way that, the link will come up as soon as someone plug in a network cable into some of these ports bypassing STP learning/listening states.

SW1

```
Interface range F0/1 - 6
Spanning-tree portfast
```

Output of command:

SW1

```
show spanning-tree interface F0/1 portfast

VLAN10 enabled
```

Explanation:

After a port on the switch has linked and joined the bridge group, STP runs on that port. A port that runs STP can be in one of five states:

- **blocking**
- **listening**
- **learning**
- **forwarding**
- **disabled**

STP dictates that the port starts out blocking, and then immediately moves through the listening and learning phases.

By default, the port spends approximately 15 seconds listening and 15 seconds learning.

During the listening state, the switch tries to determine where the port fits in
the spanning tree topology. The switch especially wants to know whether this port is part of a physical loop. If the port is part of a loop, the port can be chosen to go into blocking mode.

The **blocking state** means that the port does not send or receive user data in order to eliminate loops.
If the port is not part of a loop, the port proceeds to the learning state, in which the port learns which MAC addresses live off this port. This entire STP initialization process takes about 30 seconds.

If you connect a workstation or a server with a single NIC card or an IP phone to a switch port, the connection cannot create a physical loop. These connections are considered leaf nodes. There is no reason to make the workstation wait 30 seconds while the switch checks for loops if the workstation cannot cause a loop.

Cisco added the PortFast or fast-start feature. With this feature,
the STP for this port assumes that the port is not part of a loop and immediately moves to the forwarding state and does not go through the blocking, listening, or learning states. This command does not turn STP off. This command makes STP skip a few initial steps (unnecessary steps, in this circumstance) on the selected port.

NOTE: Never use the PortFast feature on switch ports that connect to other switches, hubs, or routers. These connections can cause physical loops, and spanning tree must go through the full initialization procedure in these situations. A spanning tree loop can bring your network down. If
you turn on PortFast for a port that is part of a physical loop, there can be a window of time when packets are continuously forwarded (and can even multiply) in such a way that the network cannot recover.

At the global level, you enable BPDU guard on Port Fast-enabled NNIs by using the **spanning-tree portfast bpduguard default** global configuration command. Spanning tree shuts down NNIs that are in a Port Fast-operational state if any BPDU is received on those NNIs.

In a valid configuration, Port Fast-enabled NNIs do not receive BPDUs. Receiving a BPDU on a Port Fastenabled NNI signals an invalid configuration, such as the connection of an unauthorized device,and the BPDU guard feature puts the interface in the error-disabled state.

At the interface level, you enable BPDU guard on any NNI by using the **spanning-tree bpduguard enable** interface configuration command without also enabling the Port Fast feature. When the NNI receives a BPDU, it is put in the error-disabled state.

Lab 4- Configuring BPDU Guard

Task 1

The IT departament just found out that someone in the lobby area just plugged in a switch into port F0/6 on SW1. Configure a command globally on SW1 that if someone connects a hub or a switch to any of the access ports, the port will be disabled. Also make sure that after 4 minutes the disabled port comes up automatically

SW1

Spanning-tree portfast bpduguard
!
Errdisable recovery cause bpduguard
Errdisable recovery interval 240

Output of command:

SW1

show errdisable recovery

ErrDisable Reason Timer Status
---------------- --------------
udld Disabled
bpduguard Enabled
rootguard Disabled
pagp-flap Disabled
dtp-flap Disabled
link-flap Disabled
Timer interval: 240 seconds
Interfaces that will be enabled at the next timeout:

show spanning-tree summary
Root bridge for: VLAN1, VLAN10, VLAN13, VLAN16, VLAN19, VLAN20, VLAN30

PortFast BPDU Guard is enabled
UplinkFast is disabled
BackboneFast is disabled
…

Explanation:

Port Fast-enabled ports do not receive **BPDUs**. Receiving a BPDU on a Port Fast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state.

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port
from participating in the spanning tree.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking ports. Configure Port Fast only on ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled port moves directly to the spanning-tree
forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can also configure bpduguard under an interface using the command **"spanning-tree bpduguard".**

NETWORKERS HOME

IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK Module:12 - Router Maintenance

Router Maintenance Commands

Command	Description
Copy startup-config tftp	Backs up the Startup-config file to a TFTP server
Copy tftp startup-config	Restoring the Startup-config file from a TFTP server
Show Flash	Displays the contents of Flash including the IOS Operating System File.
Copy flash tftp	Backs up the IOS File to a TFTP Server
Copy tftp flash	Upgrades or restores the IOS From a TFTP Server
Tftpdnld	A Rommon mode command used to recover the IOS when it is lost. Requires the setting of the following parameters. (Case-sensitive) IP_ADDRESS=XX.XX.XX.XX IP_SUBNET_MASK=XXX.XXX.XXX.XXX DEFAULT_GATEWAY=XX.XX.XX.XX TFTP_SERVER=XX.XX.XX.XX TFTP_FILENAME=IOS Filename

NETWORKERS HOME

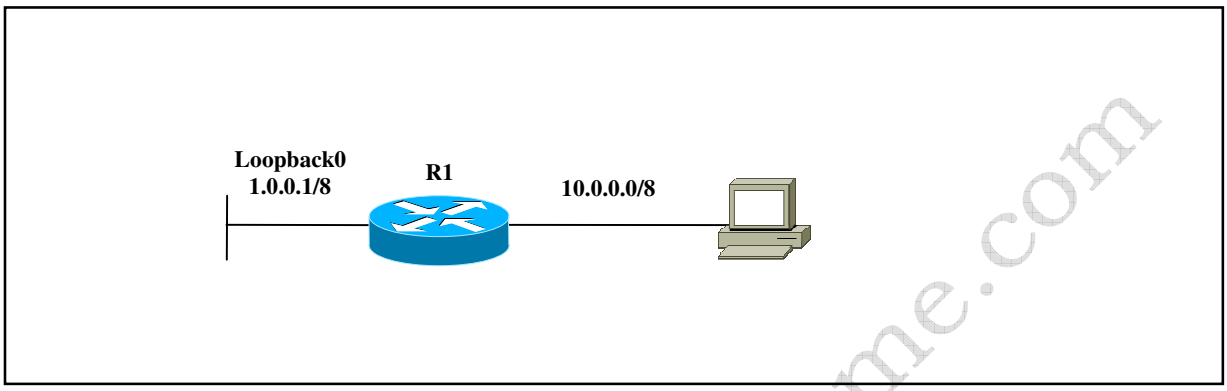
IGNITE YOUR GENIUS

Cisco Certified Network Associate (CCNA)

WORK BOOK

Module:12 - Router Maintenance Labs

Lab 1 – Backing up Startup-config to a TFTP Server



Configuring the Router and the PC

Router 1

Router>**en**
Router#**Config t**
Router(config)#**Hostname R1**
R1(config)#**interface Loopback 0**
R1(config-if)#**ip address 1.0.0.1 255.0.0.0**
R1(config-if)#**interface E 0/0**
R1(config-if)#**ip address 10.0.0.1 255.0.0.0**
R1(config-if)#**no shut**
R1(config-if)#**line console 0**
R1(config-line)#**login**
R1(config-line)#**logging synch**
R1(config-line)#**no ip domain-lookup**
R1(config-line)#**end**
R1#**wr**

PC

IP Address : **10.0.0.2**
Subnet Mask : **255.0.0.0**
Default Gateway : **10.0.0.1**

Backing up Startup-config to Tftp-Server

- Double-click the **Cisco TFTP Server** Icon on your Desktop.
- What is the IP address of the TFTP Server?
- What is the default directory for the TFTP Server?
- Switch to Hyper terminal.
- In Privilege Exec, Ping the IP address of the TFTP Server (**Ping 10.0.0.2)**
- Are you successful?
- Type **copy startup-config tftp**
- Specify the IP address of the TFTP server as the Remote Server.
- Specify **Startup-config** as the destination filename for the file.

Verifying the creation of the file

- Open Windows Explorer and browse to the Default TFTP Server folder.
- Do you see the Startup-config file?
- Open it with notepad.

Lab 2 – Restoring the Startup-config from a TFTP Server

- In Privilege Exec, type **erase startup-config** to delete the startup-config file.

Restoring Startup-config from the Tftp-Server

- In Privilege Exec, Ping the IP address of the TFTP Server (**Ping 10.0.0.2)**

- Type **copy tftp startup-config** and follow the prompts to restore the file.

Verifying the restoration of the Startup-config file

- In Privilege Exec, type **sh start** and check the configuration.

Lab 3 – Backup IOS Using Cisco TFTP Server

Finding the name of the IOS File

- In Privilege Exec, type **Sh Flash**.
- What is the name of the IOS File? _____

Backing up your IOS to a TFTP Server

- Double-click the **Cisco TFTP Server** icon on the Desktop, if not already open.
- In Privilege Exec, type **Copy flash tftp** and follow the prompts using the filename of your IOS.
- Switch to the **Cisco TFTP Server** program and notice the file being copied.
- Once the copying is done, verify the creation of the file in the default folder for the Cisco TFTP Server

Lab 4 – Upgrading the IOS from a TFTP Server

Upgrading IOS from the Tftp-Server

- In Privilege Exec, Ping the IP address of the TFTP Server (**Ping 10.0.0.2)**
- Type **copy tftp flash** and follow the prompts to restore the file.
- Why does it ask you to erase flash before proceeding? _____

Lab 5 – Recovering IOS from a TFTP Server

Simulating a lost or corrupted IOS

- In Privilege Exec, type **erase flash** to delete the flash and simulate a corruption of the IOS.
- Type **reload** to restart the router.

Setting up the TFTP parameters in Rommon Mode

- When the router reloads, what mode does it go into and why?
- As the router did not load the Startup-config, it does not have any IP configuration to connect to the TFTP Server.
- To set IP configuration parameters, use the following commands: (The commands are case-sensitive)
    - **IP ADDRESS=10.0.0.1**
    - **IP_SUBNET_MASK=255.0.0.0**
    - **DEFAULT_GATEWAY=10.0.0.1**
    - **TFTP_SERVER=10.0.0.2**
    - **TFTP_FILE=(IOS Filename)**

Recovering the IOS

- Type **tftpdnld.**
- Verify the parameters and type **y** to start the download.
- Once the download is done, reload the router.
- Can you get in?
- Is your old configuration file still valid?
- Why was the configuration file still intact?