Experiment 16

Aim: TCP and UDP Communications (Packet Tracer 14.8.1)

Theory: This simulation activity explores the differences between TCP and UDP protocols, emphasizing their functionality in network communication. TCP, a connection-oriented protocol, ensures reliable data transmission through sequence and acknowledgment numbers, while UDP, a connectionless protocol, lacks these features, offering faster but less reliable communication. By generating various types of network traffic (HTTP, FTP, DNS, and email) and analysing packet data in Packet Tracer, students gain practical insights into multiplexing, port assignments, and protocol behaviours, laying a foundation for understanding networking principles.

Instructions:

Part 1: Generate Network Traffic in Simulation Mode and View Multiplexing

Step 1: Generate traffic to populate Address Resolution Protocol (ARP) tables.

Perform the following task to reduce the amount of network traffic viewed in the simulation.

a. Click **MultiServer** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **ping -n 1 192.168.1.255** command. You are pinging the broadcast address for the client LAN. The command option will send only one ping request rather than the usual four. This will take a few seconds as every device on the network responds to the ping request from MultiServer.

c. Close the **MultiServer** window.

Step 2: Generate web (HTTP) traffic.

a. Switch to Simulation mode.

b. Click **HTTP Client** and open the **Web Browser** from the desktop.

c. In the URL field, enter **192.168.1.254** and click **Go**. Envelopes (PDUs) will appear in the topology window.

d. Minimize, but do not close, the **HTTP Client** configuration window.

Step 3: Generate FTP traffic.

a. Click **FTP Client** and open the **Command Prompt** from the desktop

b. Enter the **ftp 192.168.1.254** command. PDUs will appear in the simulation window.

c. Minimize, but do not close, the **FTP Client** configuration window.

Step 4: Generate DNS traffic.

a. Click DNS Client and open the **Command Prompt**.

b. Enter the **nslookup multiserver.pt.ptu** command. A PDU will appear in the simulation window.

c. Minimize, but do not close, the **DNS Client** configuration window.

Step 5: Generate Email traffic.

a. Click **E-Mail Client** and open the **E Mail** tool from the Desktop.

b. Click **Compose** and enter the following information:

1) **To:** user@multiserver.pt.ptu

2) **Subject:** personalize the subject line

3) **E-Mail Body:** personalize the Email

c. Click **Send**.

d. Minimize, but do not close, the **E-Mail Client** configuration window.

Step 6: Verify that the traffic is generated and ready for simulation.

There should now be PDU entries in the simulation panel for each of the client computers.

Step 7: Examine multiplexing as the traffic crosses the network.

You will now use the **Capture/Forward button** in the Simulation Panel to observe the different protocols travelling on the network.

Note: The **Capture/Forward** button ' >| ' is a small arrow pointing to the right with a vertical bar next to it.

a. Click **Capture/Forward** once. All of the PDUs travel to the switch.

b. Click **Capture/Forward** six times and watch the PDUs from the different hosts as they travel on the network. Note that only one PDU can cross a wire in each direction at any given time.

What is this called?

A variety of PDUs appears in the event list in the Simulation Panel. What is the meaning of the different colors?

Part 2: Examine Functionality of the TCP and UDP Protocols

Step 1: Examine HTTP traffic as the clients communicate with the server.

a. Click **Reset Simulation**.

b. Filter the traffic that is currently displayed to only **HTTP** and **TCP** PDUs. To filter the traffic that is currently displayed:

1) Click **Edit Filters** and toggle the **Show All/None** button.

2) Select **HTTP** and **TCP**. Click the red "x" in the upper right-hand corner of the Edit Filters box to close it. Visible Events should now display only **HTTP** and **TCP** PDUs.

c. Open the browser on HTTP Client and enter **192.168.1.254** in the URL field. Click **Go** to connect to the server over HTTP. Minimize the HTTP Client window.

d. Click **Capture/Forward** until you see a PDU appear for HTTP. Note that the color of the envelope in the topology window matches the color code for the HTTP PDU in the Simulation Panel.

Why did it take so long for the HTTP PDU to appear?

e. Click the PDU envelope to show the PDU details. Click the **Outbound PDU Details** tab and scroll down to the second to the last section.

What is the section labeled?

Are these communications considered to be reliable?

Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values.

f. Look at the value in the Flags field, which is located next to the Window field. The values to the right of the "b" represent the TCP flags that are set for this stage of the data conversation. Each of the six places corresponds to a flag. The presence of a "1" in any place indicates that the flag is set. More than one flag can be set at a time. The values for the flags are shown below.

Flag Place	**6**	**5**	**4**	**3**	**2**	**1**
Value	URG	ACK	PSH	RST	SYN	FIN

Which TCP flags are set in this PDU?

g. Close the PDU and click **Capture/Forward** until a PDU with a checkmark returns to the **HTTP Client**.

h. Click the PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before?

i. Click the HTTP PDU which **HTTP Client** has prepared to send to **MultiServer**. This is the beginning of the HTTP communication. Click this second PDU envelope and select **Outbound PDU Details**.

What information is now listed in the TCP section? How are the port and sequence numbers different from the previous two PDUs?

j. Reset the simulation.

Step 2: Examine FTP traffic as the clients communicate with the server.

a. Open the command prompt on the FTP Client desktop. Initiate an FTP connection by entering **ftp 192.168.1.254**.

b. In the Simulation Panel, change **Edit Filters** to display only **FTP** and **TCP**.

c. Click **Capture/Forward**. Click the second PDU envelope to open it.

Click the **Outbound PDU Details** tab and scroll down to the TCP section.

Are these communications considered to be reliable?

d. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values.

What is the value in the flag field?

e. Close the PDU and click **Capture/Forward** until a PDU returns to the **FTP Client** with a checkmark.

f. Click the PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before?

g. Click the **Outbound PDU Details** tab.

How are the port and sequence numbers different from the previous results?

h. Close the PDU and click **Capture/Forward** until a second PDU returns to the **FTP Client**. The PDU is a different color.

i. Open the PDU and select **Inbound PDU Details**. Scroll down past the TCP section.

What is the message from the server?

j. Click Reset Simulation.

Step 3: Examine DNS traffic as the clients communicate with the server.

a. Repeat the steps in Part 1 to create DNS traffic.

b. In the Simulation Panel, change **Edit Filters** to display only **DNS** and **UDP**.

c. Click the PDU envelope to open it.

d. Look at the OSI Model details for the outbound PDU.

What is the Layer 4 protocol?

Are these communications considered to be reliable?

e. Open the Outbound PDU Details tab and find the UDP section of the PDU formats. Record the **SRC PORT** and **DEST PORT** values.

Why are there no sequence and acknowledgement numbers?

f. Close the **PDU** and click **Capture/Forward** until a PDU with a check mark returns to the **DNS Client**.

g. Click the PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before?

What is the last section of the **PDU** called? What is the IP address for the name **multiserver.pt.ptu**?

h. Click Reset Simulation.

Step 4: Examine email traffic as the clients communicate with the server.

a. Repeat the steps in Part 1 to send an email to **user@multiserver.pt.ptu**.

b. In the Simulation Panel, change **Edit Filters** to display only **POP3, SMTP** and **TCP**.

c. Click the first PDU envelope to open it.

d. Click the **Outbound PDU Details** tab and scroll down to the last section.

What transport layer protocol does email traffic use?

Are these communications considered to be reliable?

e. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. What is the flag field value?

f. Close the **PDU** and click **Capture/Forward** until a PDU returns to the **E-Mail Client** with a checkmark.

g. Click the TCP PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before?

h. Click the **Outbound PDU Details** tab.

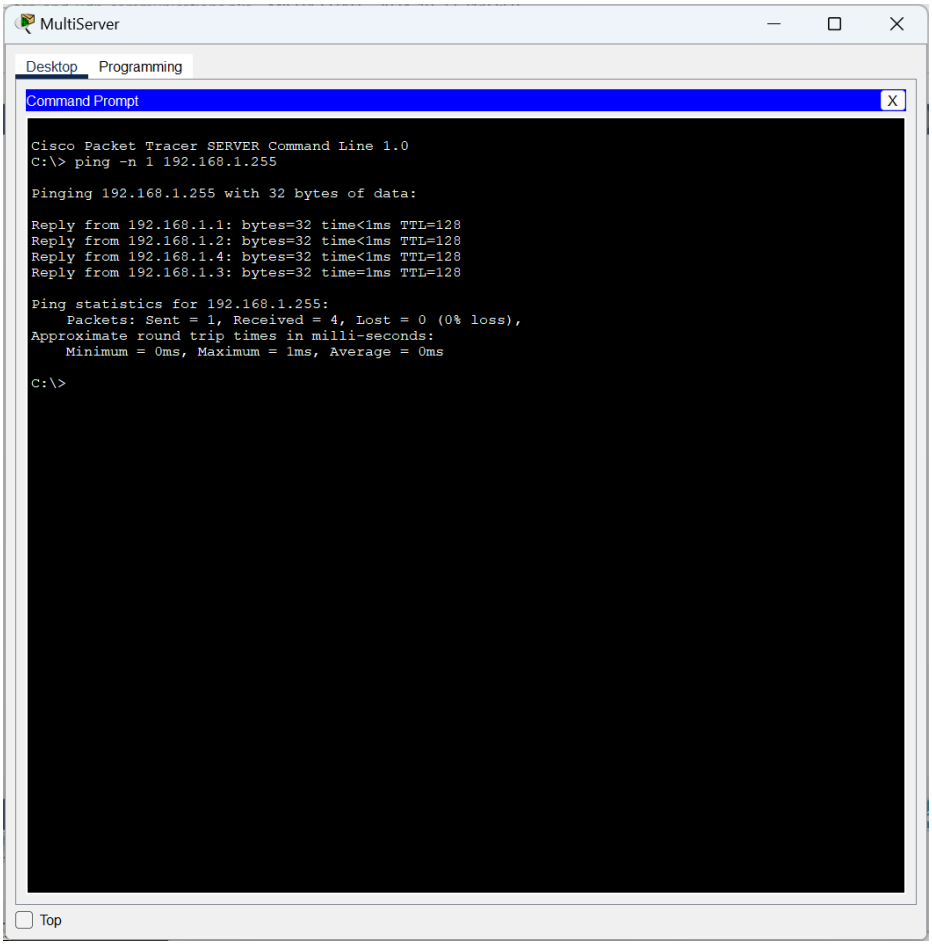
How are the port and sequence numbers different from the previous two results?

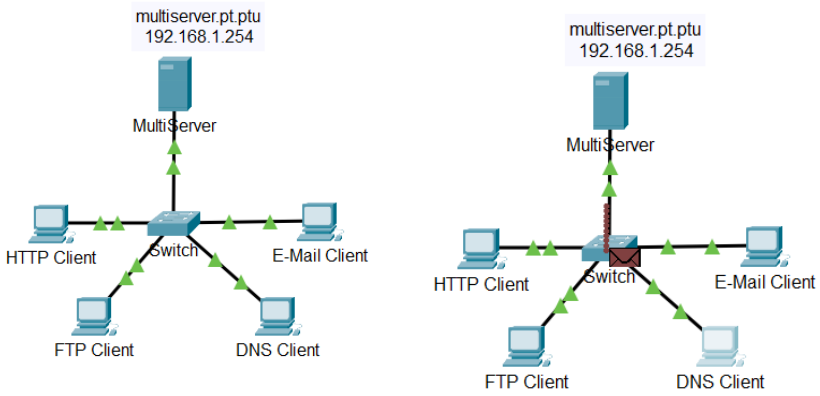
i. There is a second **PDU** of a different color that **E-Mail Client** has prepared to send to **MultiServer**. This is the beginning of the email communication. Click this second PDU envelope and select **Outbound PDU Details**.

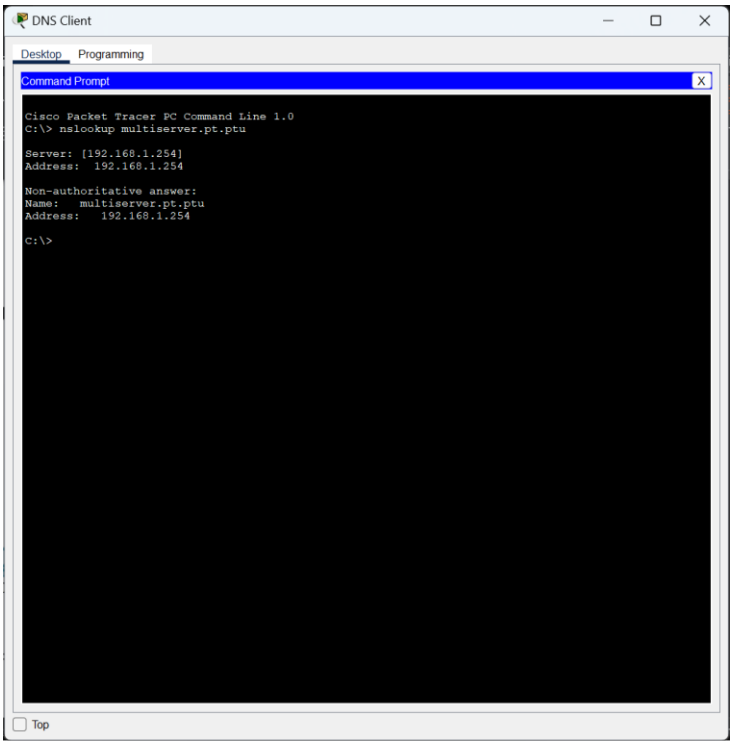
How are the port and sequence numbers different from the previous two **PDU**s?

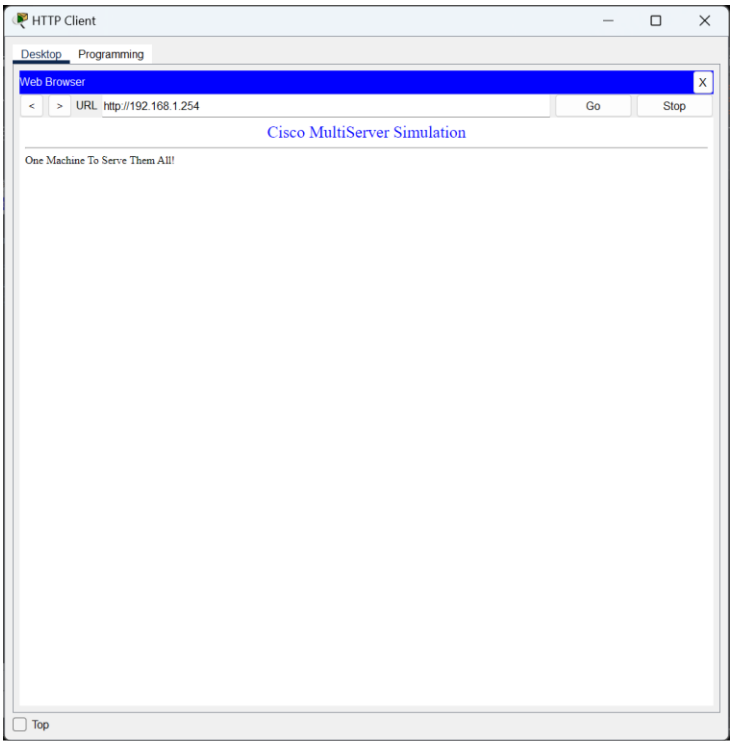
What email protocol is associated with TCP port 25? What protocol is associated with TCP port 110?

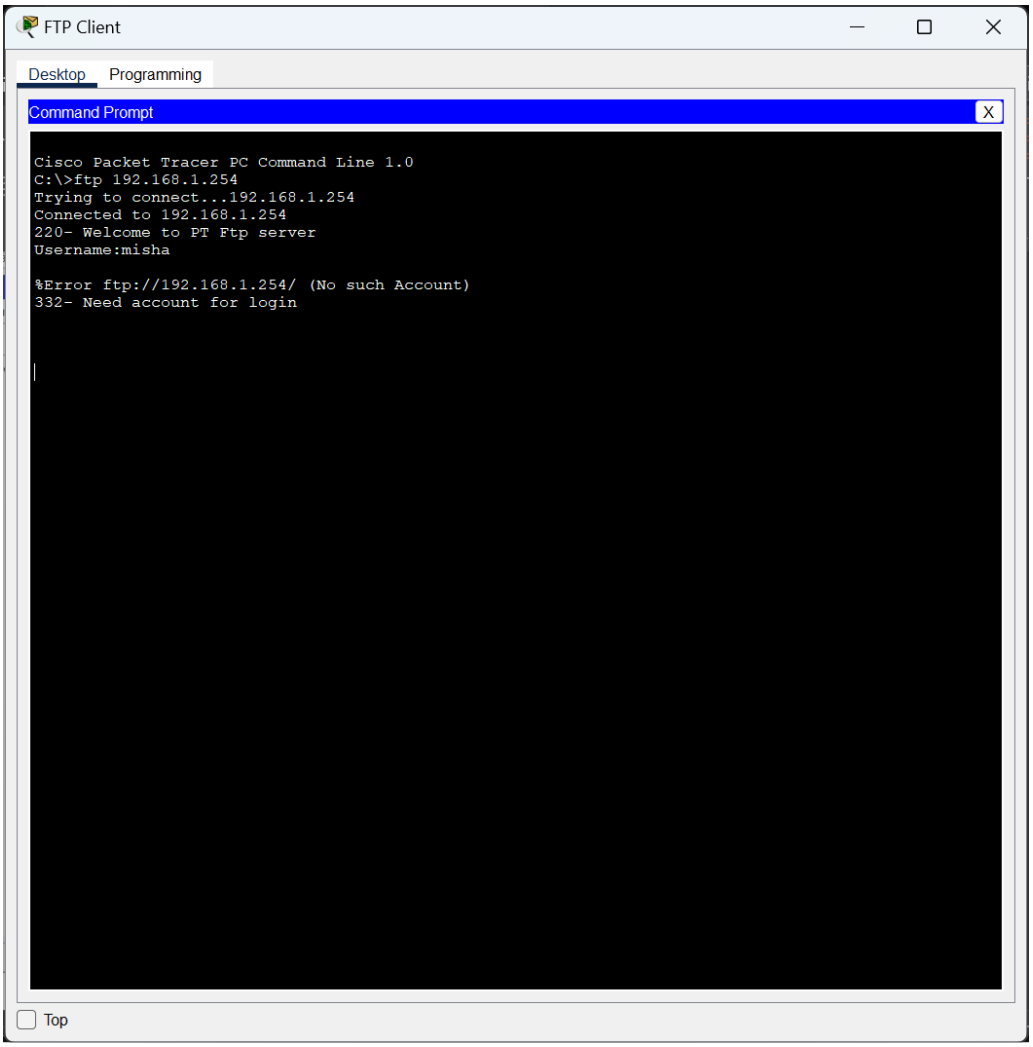
Commands/Results:




multiserver.pt.ptu
192.168.1.254
MultiServer
HTTP Client
Switch
E-Mail Client
FTP Client
DNS Client
multiserver.pt.ptu
192.168.1.254
MultiServer
HTTP Client
Switch
E-Mail Client
FTP Client
DNS Client


DNS Client
Desktop
Programming
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\> nslookup multiserver.pt.ptu
Server: [192.168.1.254]
Address: 192.168.1.254
Non-authoritative answer:
Name: multiserver.pt.ptu
Address: 192.168.1.254
C:\>
Top


HTTP Client
Desktop
Programming
Web Browser
URL http://192.168.1.254
Go
Stop
Cisco MultiServer Simulation
One Machine To Serve Them All!
Top


FTP Client
Desktop
Programming
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.254
Trying to connect...192.168.1.254
Connected to 192.168.1.254
220- Welcome to PT Ftp server
Username:misha
%Error ftp://192.168.1.254/ (No such Account)
332- Need account for login
Top

Experiment 17

Aim: Configure Secure Passwords and SSH (Packet Tracer 16.4.6)

Theory: This simulation activity explores the differences between TCP and UDP protocols, emphasizing their functionality in network communication. TCP, a connection-oriented protocol, ensures reliable data transmission through sequence and acknowledgment numbers, while UDP, a connectionless protocol, lacks these features, offering faster but less reliable communication. By generating various types of network traffic (HTTP, FTP, DNS, and email) and analysing packet data in Packet Tracer, students gain practical insights into multiplexing, port assignments, and protocol behaviours, laying a foundation for understanding networking principles.

Instructions:

Step 1: Configure Basic Security on the Router

a. Configure IP addressing on **PCA** according to the Addressing Table.

b. Console into RTA from the Terminal on PCA.

c. Configure the hostname as **RTA**.

d. Configure IP addressing on **RTA** and enable the interface.

e. Encrypt all plaintext passwords.

RTA(config)# **service password-encryption**

f. Set the minimum password length to 10.

RTA(config)# **security password min-length 10**

g. Set a strong secret password of your choosing. **Note**: Choose a password that you will remember, or you will need to reset the activity if you are locked out of the device.

h. Disable DNS lookup.

RTA(config)# **no ip domain-lookup**

i. Set the domain name to **CCNA.com** (case-sensitive for scoring in PT).

RTA(config)# **ip domain-name CCNA.com**

j. Create a user of your choosing with a strong encrypted password.

RTA(config)# **username *any_user* secret *any_password***

k. Generate 1024-bit RSA keys.

Note: In Packet Tracer, enter the crypto key generate rsa command and press Enter to continue.

RTA(config)# **crypto key generate rsa**
The name for the keys will be: **RTA.CCNA.com**
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: **1024**

l. Block anyone for three minutes who fails to log in after four attempts within a two-minute period.

RTA(config)# **login block-for 180 attempts 4 within 120**

m. Configure all VTY lines for SSH access and use the local user profiles for authentication.

RTA(config)# **line vty 0 4**
RTA(config-line)# **transport input ssh**
RTA(config-line)# **login local**

n. Set the EXEC mode timeout to 6 minutes on the VTY lines.

RTA(config-line)# **exec-timeout 6**

o. Save the configuration to NVRAM.

p. Access the command prompt on the desktop of **PCA** to establish an SSH connection to **RTA**.

C:\> **ssh /?**
Packet Tracer PC SSH
Usage: **SSH -l username target**
C:\>

Step 2: Configure Basic Security on the Switch

Configure switch **SW1** with corresponding security measures. Refer to the configuration steps on the router if you need additional assistance.

a. Click on **SW1** and select the **CLI** tab.

b. Configure the hostname as **SW1**.

c. Configure IP addressing on SW1 **VLAN1** and enable the interface.

d. Configure the default gateway address.

e. Disable all unused switch ports.

Note: On a switch it is a good security practice to disable unused ports. One method of doing this is to simply shut down each port with the '**shutdown**' command. This would require accessing each port individually. There is a shortcut method for making modifications to several ports at once by using the **interface range** command. On **SW1** all ports except FastEthernet0/1 and GigabitEthernet0/1 can be shutdown with the following command:

SW1(config)# **interface range F0/2-24, G0/2**
SW1(config-if-range)# **shutdown**
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
<Output omitted>
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

The command used the port range of 2-24 for the FastEthernet ports and then a single port range of GigabitEthernet0/2.

f. Encrypt all plaintext passwords.

g. Set a strong secret password of your choosing.

h. Disable DNS lookup.

i. Set the domain name to **CCNA.com** (case-sensitive for scoring in PT).

j. Create a user of your choosing with a strong encrypted password.

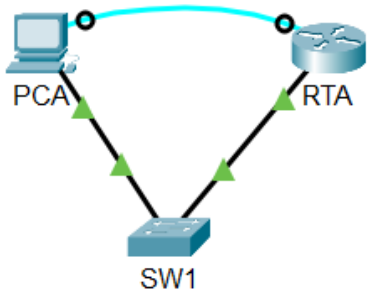
k. Generate 1024-bit RSA keys.

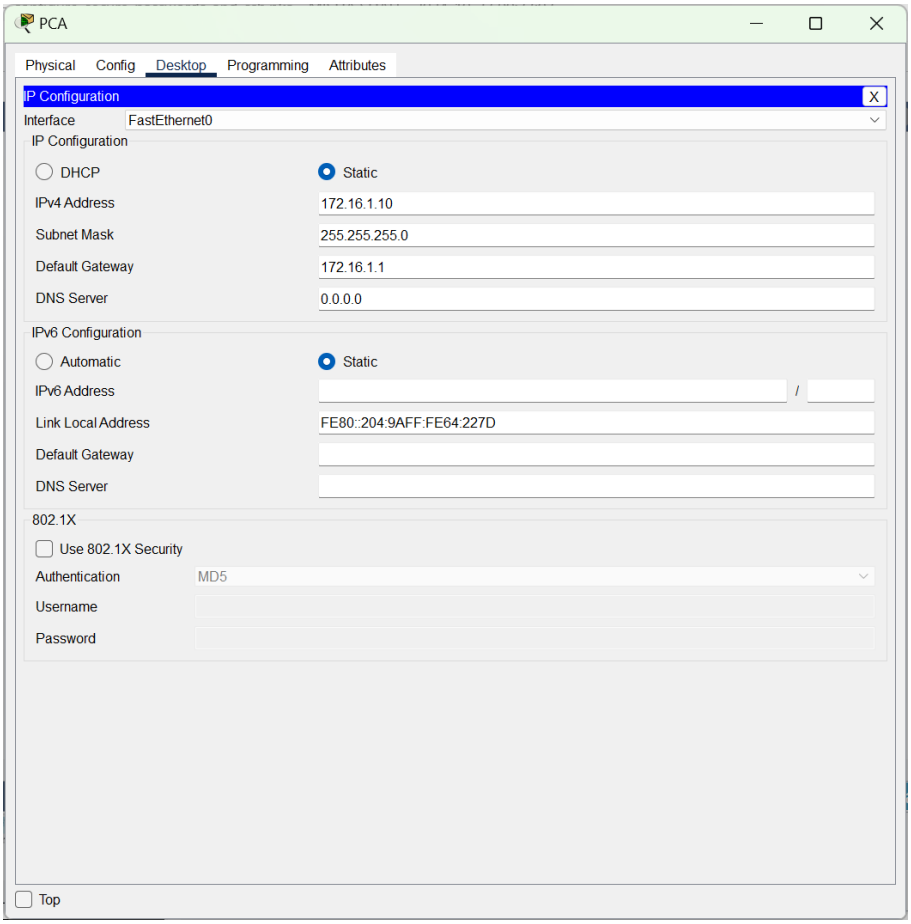
l. Configure all VTY lines for SSH access and use the local user profiles for authentication.

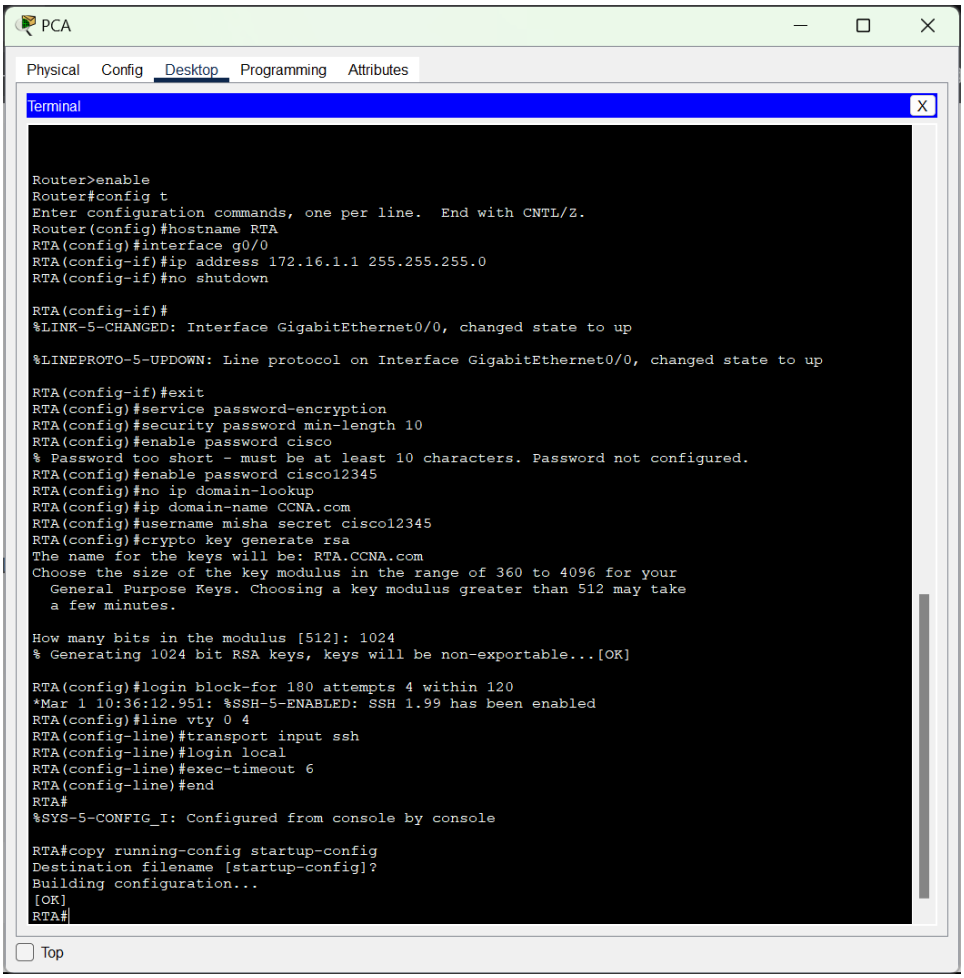
m. Set the EXEC mode timeout to 6 minutes on all VTY lines.

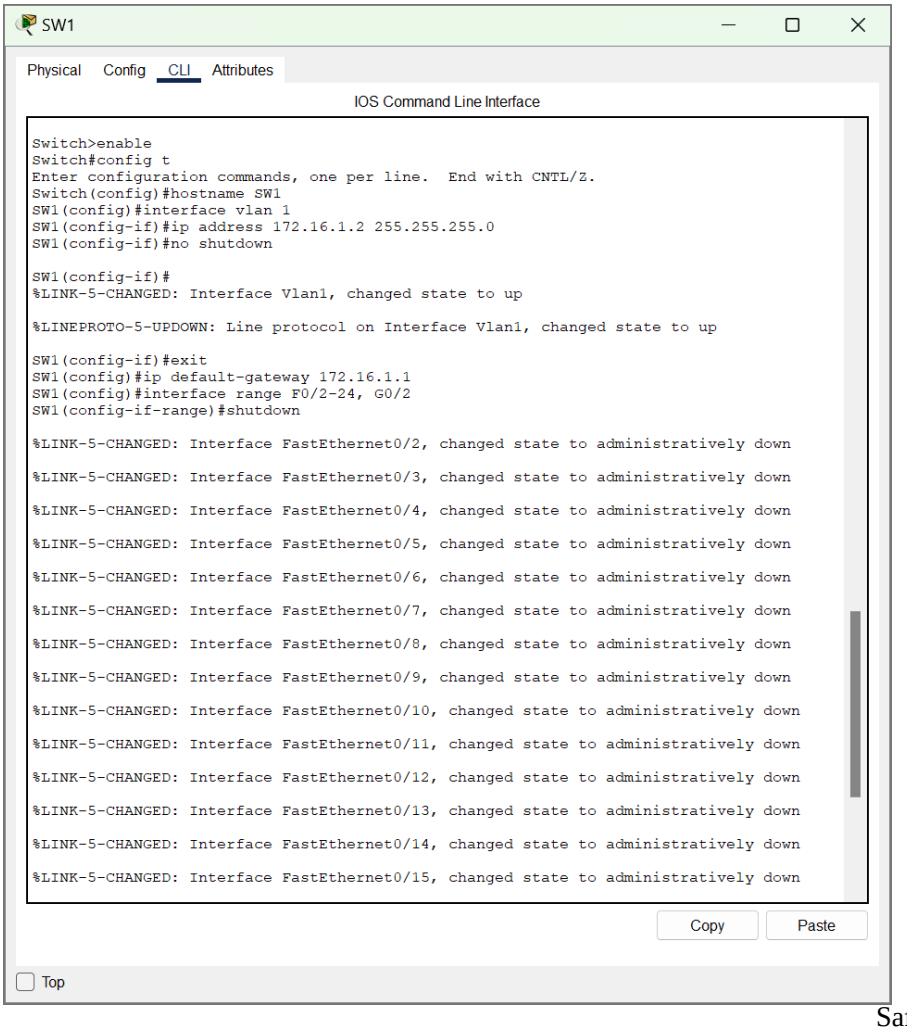
n. Save the configuration to NVRAM.

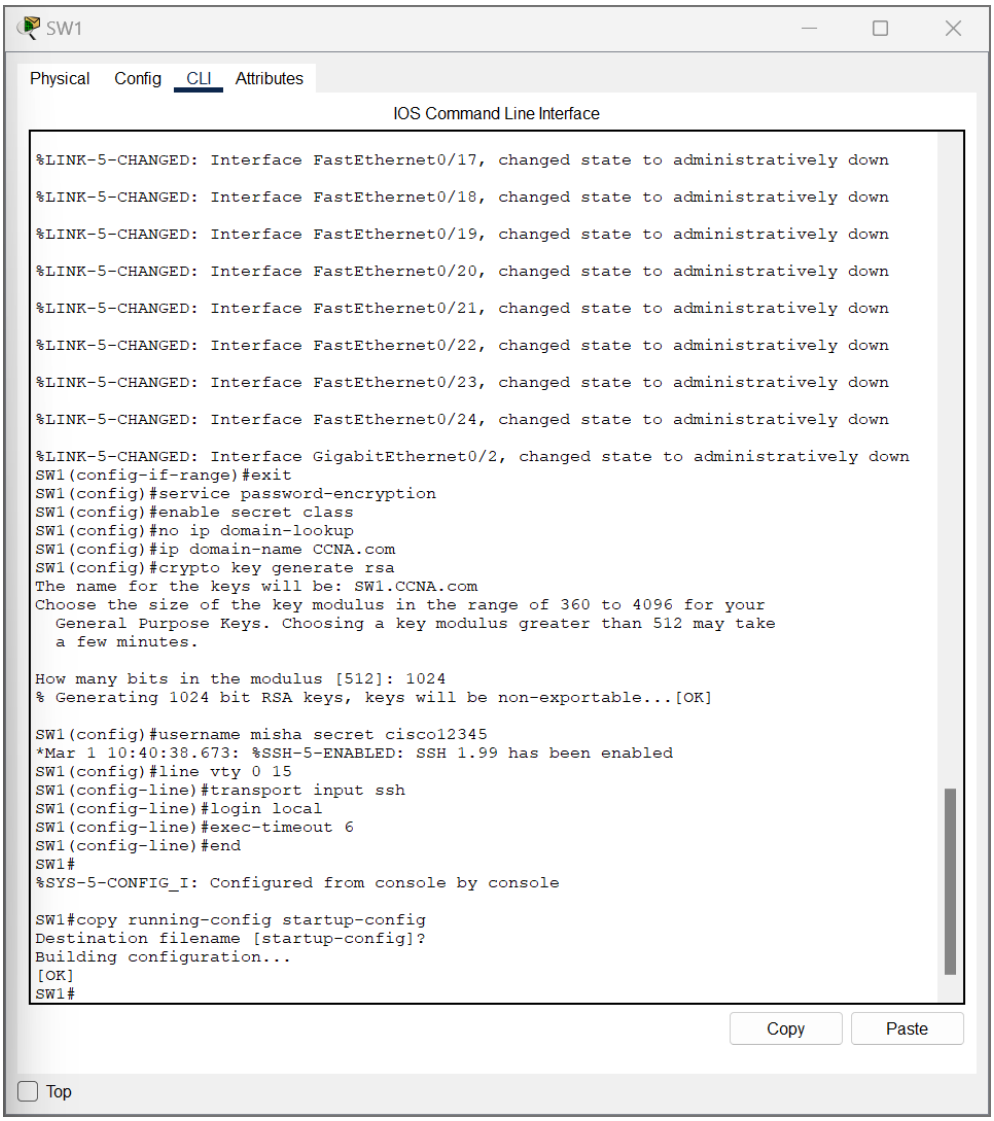
Commands/Results:






PCA
Physical
Config
Desktop
Programming
Attributes
Terminal
X
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RTA
RTA(config)#interface g0/0
RTA(config-if)#ip address 172.16.1.1 255.255.255.0
RTA(config-if)#no shutdown
RTA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
RTA(config-if)#exit
RTA(config)#service password-encryption
RTA(config)#security password min-length 10
RTA(config)#enable password cisco
% Password too short - must be at least 10 characters. Password not configured.
RTA(config)#enable password cisco12345
RTA(config)#no ip domain-lookup
RTA(config)#ip domain-name CCNA.com
RTA(config)#username misha secret cisco12345
RTA(config)#crypto key generate rsa
The name for the keys will be: RTA.CCNA.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
RTA(config)#login block-for 180 attempts 4 within 120
*Mar 1 10:36:12.951: %SSH-5-ENABLED: SSH 1.99 has been enabled
RTA(config)#line vty 0 4
RTA(config-line)#transport input ssh
RTA(config-line)#login local
RTA(config-line)#exec-timeout 6
RTA(config-line)#end
RTA#
%SYS-5-CONFIG_I: Configured from console by console
RTA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RTA#
Top


SW1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#interface vlan 1
SW1(config-if)#ip address 172.16.1.2 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SW1(config-if)#exit
SW1(config)#ip default-gateway 172.16.1.1
SW1(config)#interface range F0/2-24, G0/2
SW1(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
Copy
Paste
Top


SW1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
SW1(config-if-range)#exit
SW1(config)#service password-encryption
SW1(config)#enable secret class
SW1(config)#no ip domain-lookup
SW1(config)#ip domain-name CCNA.com
SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.CCNA.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
SW1(config)#username misha secret cisco12345
*Mar 1 10:40:38.673: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW1(config)#line vty 0 15
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#exec-timeout 6
SW1(config-line)#end
SW1#
%SYS-5-CONFIG_I: Configured from console by console
SW1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW1#
Copy
Paste
Top

Experiment 18

Aim: Interpret show Command Output (Packet Tracer 17.5.9)

Theory: This activity focuses on the analysis of router show commands, which are essential for network management and troubleshooting. By examining outputs from commands like show ip interface brief, show version, and show ip route, users can gather critical information about interface status, IOS versions, and routing paths. Understanding these commands enhances the ability to diagnose network issues, manage configurations, and ensure optimal performance. Mastery of these commands is fundamental for network engineers to maintain and troubleshoot network devices effectively.

Instructions:

Part 1: Analyze Show Command Output

a. To connect to ISPRouter, Click **ISP PC**, then the **Desktop** tab, followed by **Terminal**.

b. Enter privileged EXEC mode.

c. Use the following **show** commands to answer the Reflection Questions in Part 2.

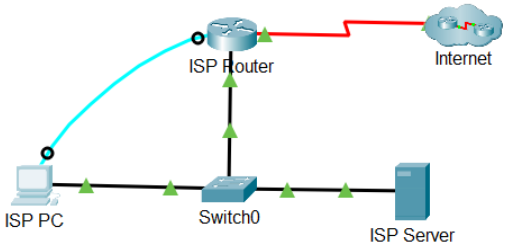
Note: If a command pauses with the -–More—prompt, make certain to hit the spacebar until the **ISPRouter#** prompt appears in order to obtain all of the command output.

show arp
show flash:
show ip route
show interfaces
show ip interface brief
show protocols
show users
show version

Part 2: Reflection Questions

1. Which commands can you use to determine the IP address and network prefix of interfaces?
2. Which command provides the IP address and interface assignment, but not the network prefix?
3. Which commands would you use to determine if an interface is up?
4. You need to determine the IOS version that is running on a router. Which command will give you this information?
5. Which commands provide information about the addresses of the router interfaces?
6. You are considering an IOS upgrade and need to determine if router flash can hold the new IOS. Which commands provide information about the amount of Flash memory available?
7. You need to adjust a router configuration, but you suspect that a colleague may also be working on the router from another location. Which command provides information about the lines being used for configuration or device monitoring?
8. You have been asked to check the performance of a device interface. Which command provides traffic statistics for router interfaces?
9. Customers are complaining that they cannot reach a server that they use for file storage. You suspect that the network may have become unreachable due to a recent upgrade. Which command provides information about the paths that are available for network traffic?
10. Which interfaces are currently active on the ISP Router?

Commands/Results:



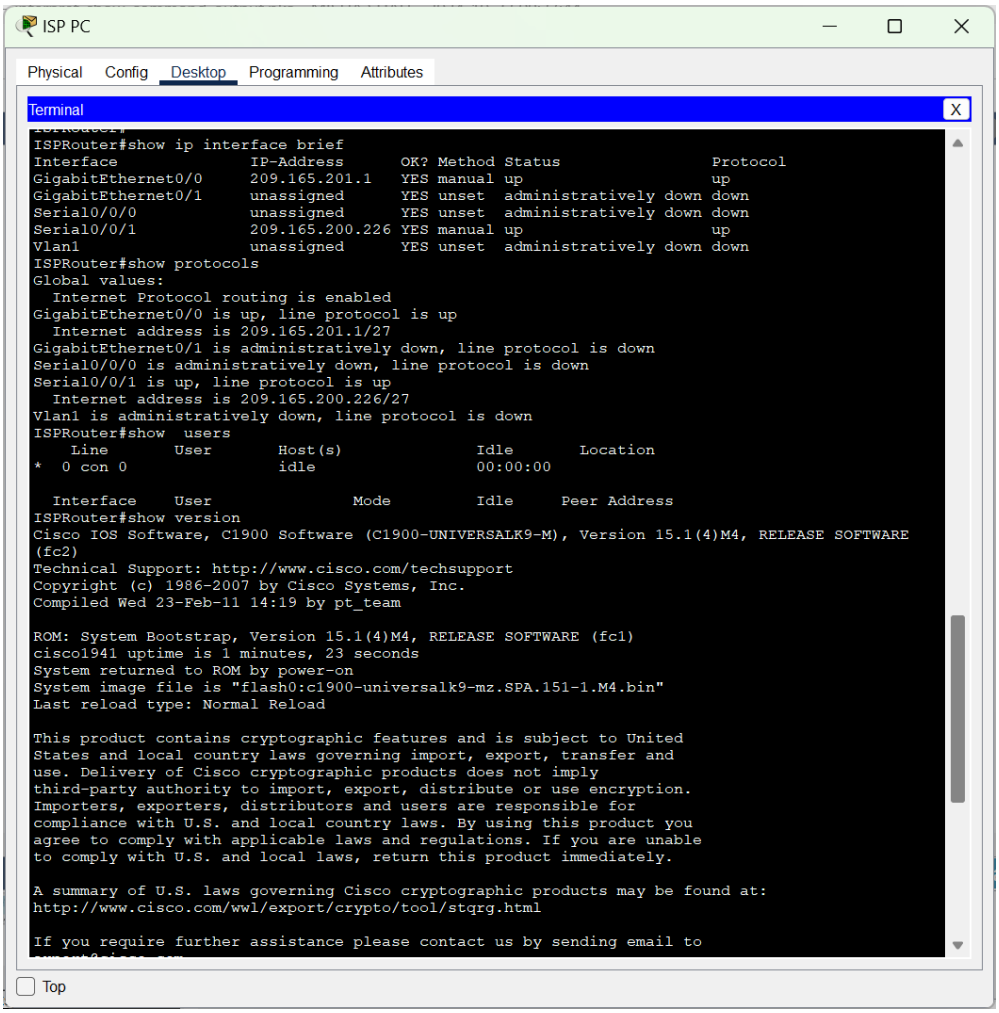
ISP PC

Physical Config Desktop Programming Attributes

Terminal

```
ISPRouter>enable
ISPRouter#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  209.165.201.1           -   0030.F275.CE01  ARPA   GigabitEthernet0/0
ISPRouter#show flash:

System flash directory:
File  Length   Name/status
  3   33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


ISPRouter#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Serial0/0/1
L       209.165.200.226/32 is directly connected, Serial0/0/1
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/27 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0

ISPRouter#show interfaces
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0030.f275.ce01 (bia 0030.f275.ce01)
  Internet address is 209.165.201.1/27
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
```

Top


ISP PC
Physical
Config
Desktop
Programming
Attributes
Terminal
X
ISPRouter#show ip interface brief
Interface   IP-Address   OK? Method Status   Protocol
GigabitEthernet0/0   209.165.201.1   YES manual up   up
GigabitEthernet0/1   unassigned   YES unset administratively down down
Serial0/0/0   unassigned   YES unset administratively down down
Serial0/0/1   209.165.200.226 YES manual up   up
Vlan1   unassigned   YES unset administratively down down
ISPRouter#show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 209.165.201.1/27
GigabitEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is administratively down, line protocol is down
Serial0/0/1 is up, line protocol is up
  Internet address is 209.165.200.226/27
Vlan1 is administratively down, line protocol is down
ISPRouter#show users
    Line   User   Host(s)   Idle   Location
* 0 con 0   idle   00:00:00

  Interface   User   Mode   Idle   Peer Address
ISPRouter#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 minutes, 23 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
Top