CSCI 5160-001 Intro to Enterprise Networks

Lab 0 USING PC#06

Introduction to Lab tools and LAN Cabling

Fall 2022

[redacted]

OBJECTIVES

1. **Learn the basics of LAN cabling.**
2. **Learn how to connect a Personal Computer to a Cisco Router/Switch for configuration.**
3. **Learn basic configuration commands used on Cisco Equipment, including user levels.**
4. **Learn how to secure a router/switch.**
5. **Learn how to connect to a router remotely via Telnet.**
6. **Learn the use of Wire shark packet sniffer.**
7. **Learn how to use a commserver for connectivity.**
8. **Learn how to Telnet to commserver.**
9. **Learn how to use Extended Ping in CISCO and Windows**
10. **Learn to calculate Path MTU and GIANT Packets**
11. **Learn how Proxy ARP works.**
12. **Learn to back up a Router/Switch IOS.**
13. **Learn password recovery on a router and a switch.**

1. **Learn the basics of LAN cabling:**

   Determine the type of cable needed to connect the following devices:

   - PC to a Router
     - Straight Through Cable
   - PC to a PC
     - Crossover Cable
   - Router to Router
     - Crossover Cable
   - Router to Switch
     - Straight Through Cable
   - Switch to Switch
     - Crossover Cable
   - Hub to Switch
     - Crossover Cable
   - PC to Hub
     - Straight Through Cable
   - PC to Switch
     - Straight Through Cable

2. **Learn how to connect a Personal Computer to a Cisco Router/Switch for**

   - Connect the roll-over cable from the PC to the console of the router/switch.
   - Start HyperTerminal on the PC and use the default settings (You can also use putty client).
   - A console session will begin after successfully completing the previous steps.

```
User Access Verification

Username: adimin
Password:
% Login invalid

Username:
Username:
Username:
Username: admin
Password:
commserver#
commserver#
commserver#
commserver#show run
Building configuration...


Current configuration : 2436 bytes
!
! Last configuration change at 20:15:47 UTC Fri Jan 17 2025
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname commserver
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
memory-size iomem 5
!
dot11 syslog
ip source-route
!
!
```

3. Learn the different user levels and navigate between them:

Introduction to the Cisco IOS (Inter Operating System)

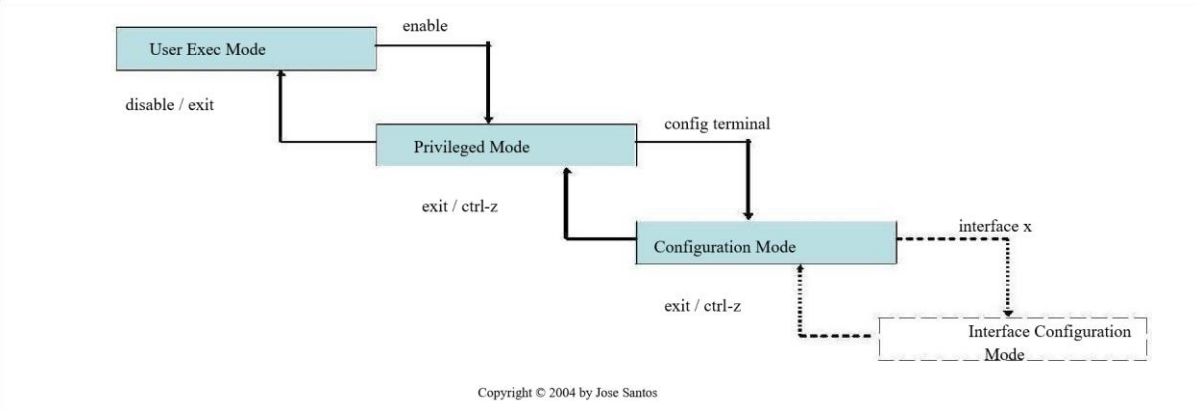
As a security feature, the Cisco IOS software separates the EXEC sessions into two access levels. These levels are user EXEC mode and privileged EXEC mode. The privileged EXEC mode is also known as “enable” mode. The following are the features of the user EXEC mode and privileged EXEC mode:

- The **user EXEC** mode allows only a limited number of basic monitoring commands. This is often referred to as a view only mode. The user EXEC level does not allow any commands that might change the configuration of the router. The user EXEC mode can be identified by the > prompt.

- The **privileged EXEC** mode provides access to all router commands. This mode can be configured to require a password. For added protection, it can also be configured to require a

user ID. This allows only authorized users to access the router. Configuration and management commands require that the network administrator be at the privileged EXEC level. Global configuration mode and all other more specific configuration modes can only be reached from the privileged EXEC mode. The privileged EXEC mode can be identified by the # prompt.

- To access the privileged EXEC level from the user EXEC level, enter the **enable** command at the > prompt. If a password is configured, the router will then ask for that password




```
*Jan 17 22:12:50.091: %SYS-5-CONFIG_I: Configured from console by console
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int ga
R1(config)#int gi
R1(config)#int gigabitEthernet 0/1
R1(config-if)#
```

4. Learn how to secure a router/switch

The cisco IOS has to be secured to prevent unauthorized access at different levels. The first level of password is required to enter the privileged mode from the user exec mode.

The two commands that can be used to set a password for privileged EXEC mode are:

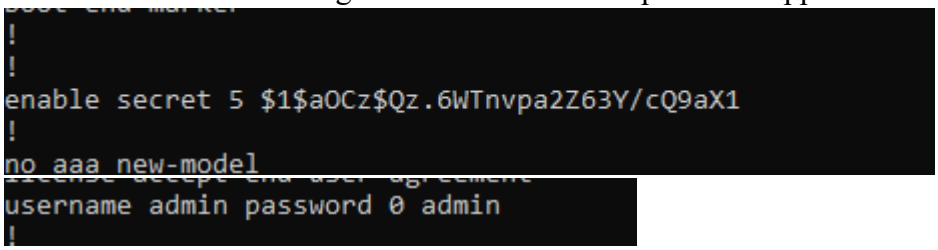
- **enable password**
- **enable secret**

If both commands are used, the **enable secret** command takes precedence.

The other password is used for the method of logging into the router. Different lines are used for logging in i.e line vty is requred for telnet. Set the password for these lines and also enable login. Hence, whenever a user tries to access the router via any line he must be prompted for a password.

- Setup different passwords for enable and console levels

Disconnect & reconnect again. Remember which password applies to which level.



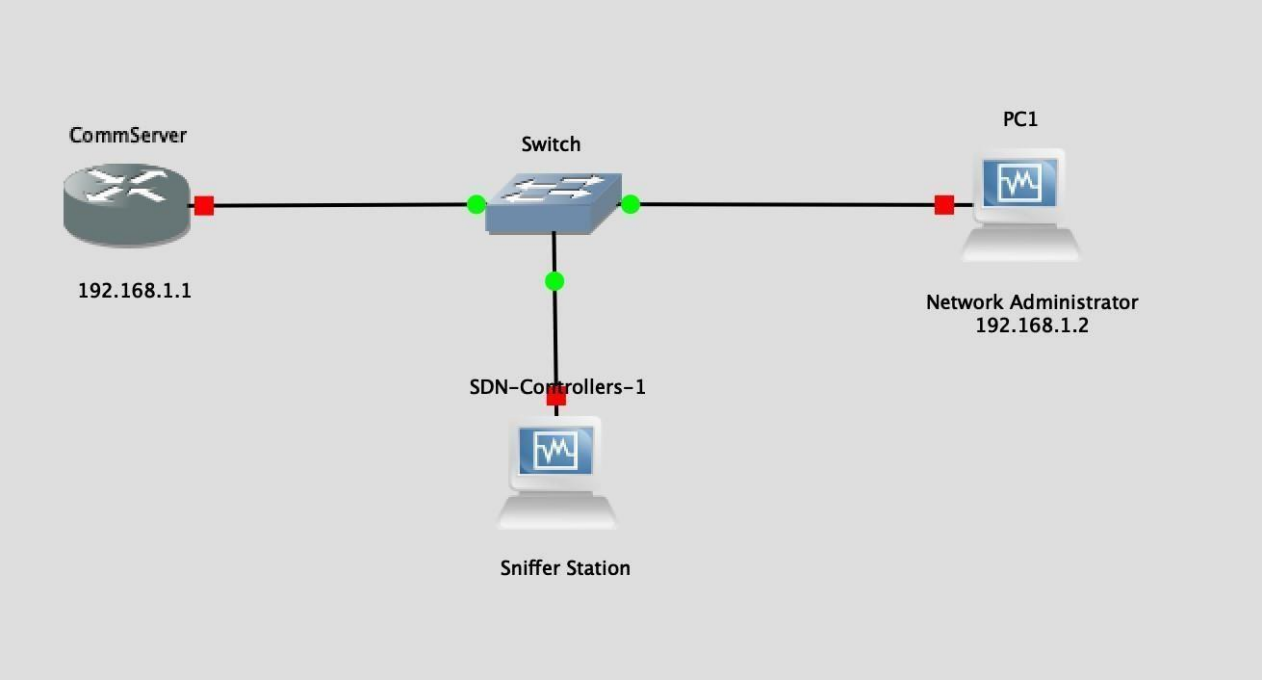
5. Learn how to connect to a router remotely via Telnet

Telnet is used for remote access to a router by a PC. The Ethernet port of the PC must be connected to the network to telnet into any router. A router must have a vty password and login to authenticate the user. The IP address of the router is used to telnet into it.

```
User Access Verification

Username: admin
Password:
commserver#
```

- Use one of the Ethernet interfaces available at the router to build the following network



a) Telnet

i. Configure Telnet password on your router Commands:

line vty 0 15
transport input telnet
login local
username jose password lab123 exit

ii. Access Cisco IOS from your Computer via the network

b) Telnet using encryption: SSH

i. Use the same diagram

ii. Type the following commands ip domain-name jose.com crypto key generate rsa

800 ip ssh version 2 line vty 0 15
transport input ssh login local
username jose password lab123
exit

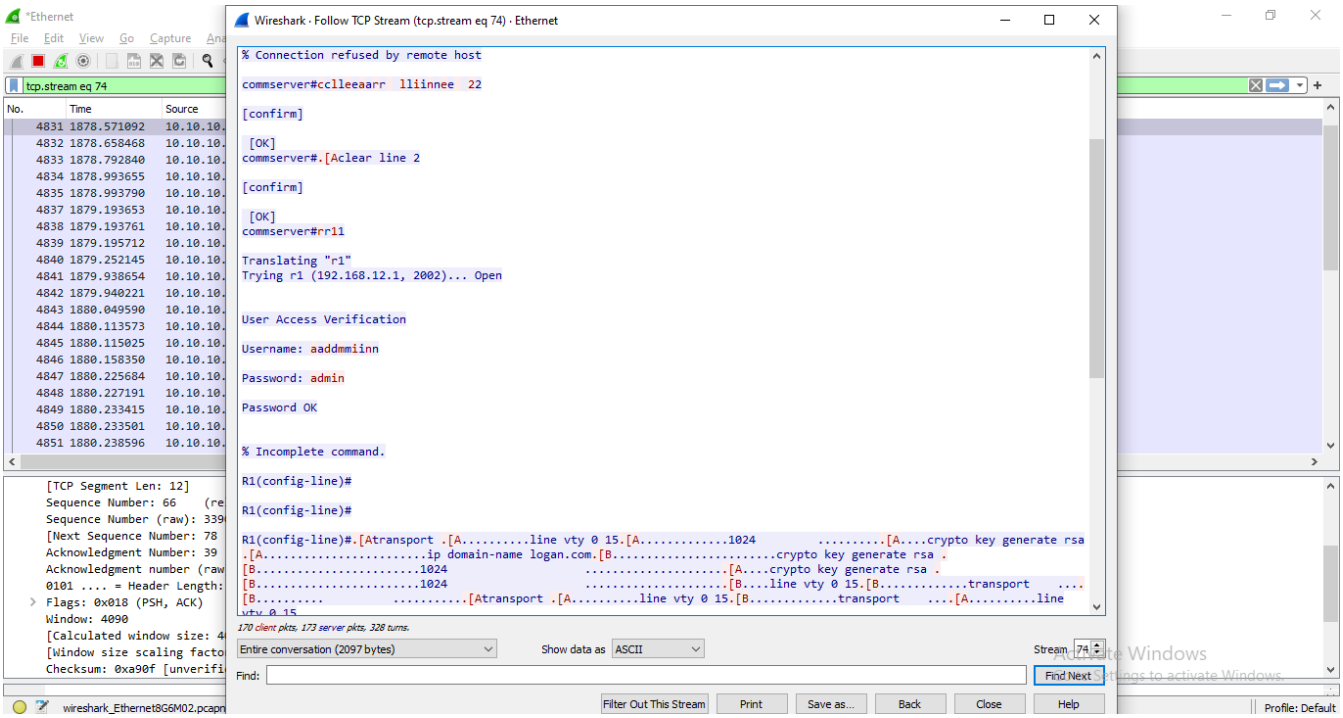
iii. Go to the computer and open a SSH client and access Cisco IOS

Check whether telnet is working or not. If not, report the problem and how to fix it.

6. Learn the use of Wireshark packet sniffer:

Wireshark is a packet sniffing tool which can be downloaded from the internet for free. The basic purpose of Wireshark is to capture all the packets passing through an interface and then display them.

Use Wireshark on PC2 to obtain the Telnet Password of the Network Administrator (when he/she tries to login). ** Dissect appropriate frames/packets used by telnet, highlight password info and include in your report.



7. Learn how to use a commserver for connectivity

A commserver is used when multiple console sessions are required. It can be used to work efficiently with multiple routers/switches which are not configured for remote access.

1. Complete the connections from the commserver to the 3 Cisco 3600 routers telnet
2. Telnet into the 3 routers

interface Loopback1

ip address 172.21.1.1 255.255.255.0

!--- This address is used in the IP host commands.

! --- Work with loopback interfaces, which are virtual and always available.

!--- Also you can use any of your interface ip if needed. Any of your own ip also works

ip host R1 2002 172.21.1.1

!--- The host R3 is connected to port 14 of the comm server.

!--- Ensure that the IP address is that of an interface on the comm server.

line 2 17

(Check which lines are used using the "show line" command)

transport input all

exit

no ip domain-lookup

!---to avoid dns lookup when you try to login by local host name R1

8. Learn How to Telnet to Commserver

1. First you need to connect a crossover cable from your PC to interface fast Ethernet of commserver.

2. Now assign IP address on fast Ethernet interface of commserver and assign same subnet IP address on PC.

3. You can assign IP address on your PC in Local Area Connection settings. You can assign IP address and mask.

4. Now open multiple telnet sessions using Putty. How many sessions can you open? Explain Why?

You can open as many connections as you set in line vty 0 4. Here we can 5 connetions, with 0 being inclusive.

5. How many line VTY's session can be configured in commserver.
16 sessions

6. Refer configuration below to configure Telnet session:

(config)# line vty 0 4 password
LAB login local
transport
input telnet
exit

9. Extended Ping with options in Windows and Cisco.

When a normal **ping** command is sent from a router, the source address of the **ping** is the IP address of the interface that the packet uses to exit the router. If an extended **ping** command is used, the source IP address can be changed to any IP address on the router. The extended **ping** is used to perform a more advanced check of host reachability and network connectivity. The extended **ping** command works only at the privileged EXEC command line. The normal ping works both in the user EXEC mode and the privileged EXEC mode. In order to use this feature, enter **ping** at the command line and press **Enter.**

This is an example with extended commands and sweep details:
Router>**enable** Router
#**ping**

Protocol [ip]:
!--- The protocol name.

Target IP address: 192.168.40.1 *!--- The address to ping.*

Repeat count [5]: 10
!--- The number of ping packets that are sent to the destination address.

Datagram size [100]:
!--- The size of the ping packet in size. The default is 100 bytes.

Timeout in seconds [2]:
!--- The timeout interval. The ping is declared successful only if the !--- ECHO REPLY packet is received before this interval.

Extended commands [n]: y

!--- You choose yes if you want extended command options
!--- (Loose Source Routing, Strict Source Routing, Record route and Timestamp).

Source address or interface: 172.16.23.2
!--- Ping packets are sourced from this address and must be the IP address !--- or full interface name (for example, Serial0/1 or 172.16.23.2).

Type of service [0]:
!--- Specifies Type of Service (ToS).

Set DF bit in IP header? [no]:
!--- Specifies whether or not the Don't Fragment (DF) bit is to be !--- set on the ping packet.

Validate reply data? [no]:
!--- Specifies whether or not to validate reply data.

Data pattern [0xABCD]:
! --- Specifies the data pattern in the ping payload. Some physical links
!--- might exhibit data pattern dependent problems. For example, serial links !
--- with misconfigured line coding. Some useful data patterns to test !--- include all 1s (0Xffff), all 0s (0x0000) and alternating !--- ones and zeros (0Xaaaa).

Loose, Strict, Record, Timestamp, Verbose[none]: *!--- IP header options.*

Sweep range of sizes [n]: y
!--- Choose yes if you want to vary the sizes on echo packets that are sent.

Sweep min size [36]:
Sweep max size [18024]: Sweep interval [1]:

A. Now use ping command with options in windows command prompt and attach your results in report.

```
R1#
R1#ping
Protocol [ip]:
Target IP address: 10.10.10.2
Repeat count [5]: 10
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.10.10.200
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.200
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/4 ms
R1#
```

10. Learn to calculate Path MTU and GIANT Packets

MTU means a **maximum transmission unit** (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet. The Internet's Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission. To check MTU refer following steps:

- Download mtupath.exe and save it in C drive
- Open cmd and change directory to c (cd c :\)
- Check path MTU (between your PC and Google.com)

```
C:\Users\rahul>cd c:\

c:\>mtupath google.com

MTU path scan to google.com (216.58.217.46), ttl=64, limit=48
# 16 processing - best MSS 1472 (estimated MTU 1500) [pPPPPpPppPppppppp]
# 01 nearest minimum MTU on local interface

        #1 MSS IN RANGE     1 <==  1471 ==>  1472
        #2 MSS EXCEEDED  1473 <== 14911 ==> 16384
```

```
c:\>mtupath google.com

MTU path scan to google.com (142.250.72.46), ttl=64, limit=48
# 16 processing - best MSS 1472 (estimated MTU 1500) [pPPPPpPppPpppppp]
# 01 nearest minimum MTU on local interface

        #1 MSS IN RANGE     1 <==  1471 ==>  1472
        #2 MSS EXCEEDED  1473 <== 14911 ==> 16384
```

- Ping google.com with packet option: size in range & set do not fragment flag in packet

```
C:\Users\rahul>ping -f -l 1472 google.com

Pinging google.com [216.58.217.46] with 1472 bytes of data:
Reply from 216.58.217.46: bytes=64 (sent 1472) time=31ms TTL=54
Reply from 216.58.217.46: bytes=64 (sent 1472) time=20ms TTL=54
Reply from 216.58.217.46: bytes=64 (sent 1472) time=21ms TTL=54
Reply from 216.58.217.46: bytes=64 (sent 1472) time=20ms TTL=54

Ping statistics for 216.58.217.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 31ms, Average = 23ms
```

- Ping google.com with packet option: size exceeded (Giant packet) & set do not fragment flag in packet

```
C:\Users\rahul>ping -f -l 1473 google.com

Pinging google.com [216.58.217.46] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 216.58.217.46:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
Pinging google.com [142.250.72.46] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 142.250.72.46:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

c:\>
```

- Explain what are runt and giant packet types and how to troubleshoot those packets?
    - Runt packets are frames the go below the minimum size of 64 bytes. A giant packet are Ethernet frames larger than 1518 bytes.
    - To troubleshoot these packets, generally we should check for any collisions/loops in the network. Also, if the NIC is properly working, maybe reset/reinstall the drivers. Make sure

the device is configured properly. Replace NICs or switches if the hardware itself is the root cause. Also make sure the MTU settings are similar between devices.

12. Learn to backup a Router/Switch IOS

1. The routers IOS is located in the Flash. This IOS can be saved on the TFTP server using the command *copy flash tftp.*
2. The name of the IOS can be found with command show flash command.

3. ***copy flash tftp*** command is used to copy IOS from Flash to TFTP server. It takes following three parameters.

    a. **Source filename** Name of IOS file that need to be copied.

    b. **Address or name of remote host** IP address of TFTP Server. (To use name we need to configure DNS service on router.)

    c. **Destination filename** Name of file used at destination to store the source file.

4. Now after taking backup now we can delete current IOS by using following command **Router#delete:[IOS File Name].**

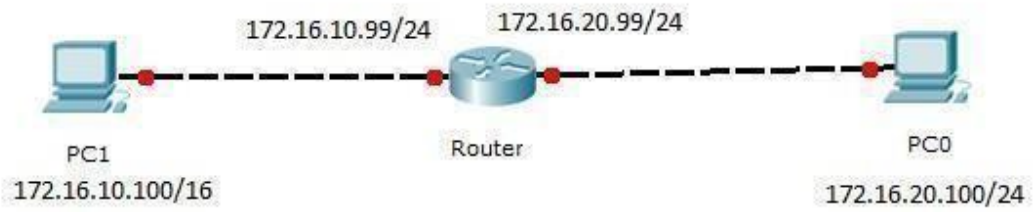
5. Use Reload command to reload the router. During the boor process router will copy and decompress the IOS file in RAM.

11. Learn how Proxy ARP works.

The Cisco IOS software uses proxy ARP (as defined in RFC 1027) to help hosts with no knowledge of routing determine the media addresses of hosts on other networks or subnets. For example, if the router receives an ARP request for a host that is not on the same interface as the ARP request sender, and if the router has all of its routes to that host through other interfaces, then it generates a proxy ARP reply packet giving its own local data-link address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host. Proxy ARP is enabled by default.

To enable proxy ARP if it has been disabled, use the following command in interface configuration mode (as needed) for your network:

Command	Purpose
Router(config -if)# **ip proxy-arp**	Enables proxy ARP on the interface.



- PC1 has a /16 subnet mask. PC1 believes that it is directly connected to all of the network 172.16.0.0. When PC1 needs to communicate to PC0, it believes PC0 is directly connected, so it sends ARP request to PC0.
- The ARP broadcast reaches the router port, but does not reach PC0. The broadcast does not reach PC0 because routers, by default, do not forward broadcasts.
- Since Router knows target address (172.16.20.100) is on another subnet and can reach PC0, it replies with its own MAC address to PC1.
- This is Proxy ARP reply that router sends to PC1. The ARP replies are always unicast to the original requester. From now on, PC1 forwards all the packets that it wants to reach 172.16.20.100 to the MAC address of the router. Since, the router knows how to reach PC0, the router forwards packet to PC0.
- On Cisco interfaces Proxy ARP is enabled by default. Proxy ARP can be disabled with the command **no ip proxy-arp**
- Ping from PC1 to PC2. Configure the **no ip proxy-arp** command on the router interface. Now Ping from PC1 to PC2. Explain the result?

PC1 arp table:

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.10.10.1               -   001a.2ff0.f521  ARPA   GigabitEthernet0/1
Internet  172.16.10.99             4   0023.0470.9c90  ARPA   GigabitEthernet0/0
Internet  172.16.10.100            -   001a.2ff0.f520  ARPA   GigabitEthernet0/0
Internet  172.16.20.99             0   0023.0470.9c90  ARPA   GigabitEthernet0/0
Internet  172.16.20.100            1   0023.0470.9c90  ARPA   GigabitEthernet0/0
R2#
```

When I issue the command, no ip proxy-arp, there is no longer a ping connection with PC1 and PC2. It seems that the proxy-arp allows connectivity between directly connected connections.

Refer following URL for details:

http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfipadr.html#wp1001233.