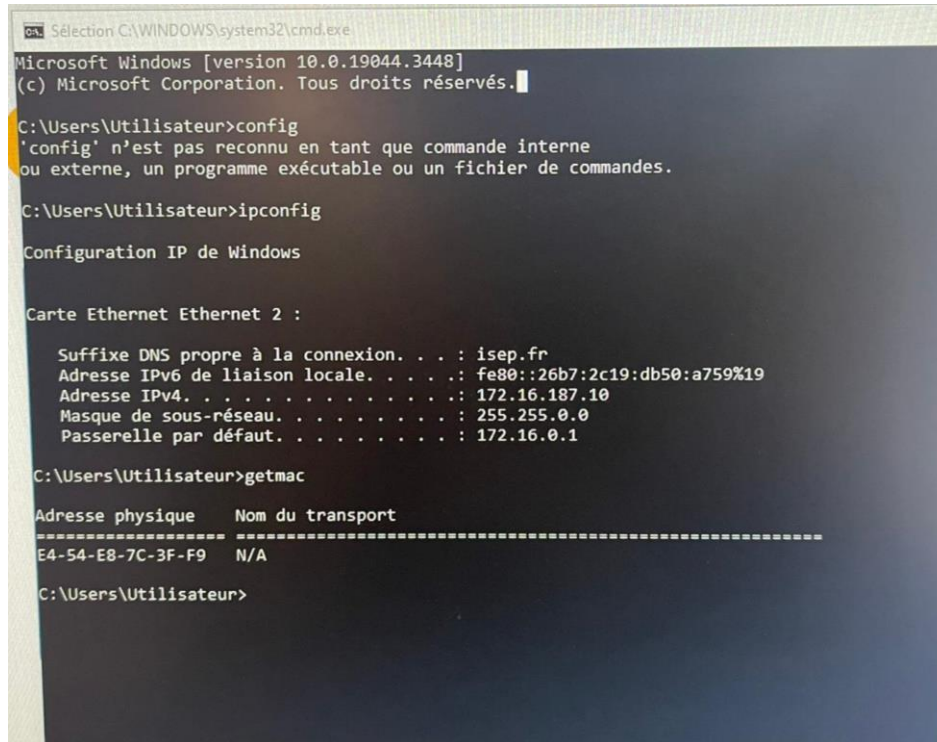


Lab – How to analyze Network Traffic with Wireshark

Part 1:

Step 1: a) b)



```
Sélection C:\WINDOWS\system32\cmd.exe
Microsoft Windows [version 10.0.19044.3448]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Utilisateur>config
'config' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\Utilisateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . . : isep.fr
    Adresse IPv6 de liaison locale. . . . : fe80::26b7:2c19:db50:a759%19
    Adresse IPv4. . . . . : 172.16.187.10
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 172.16.0.1

C:\Users\Utilisateur>getmac

Adresse physique    Nom du transport
-----
E4-54-E8-7C-3F-F9  N/A

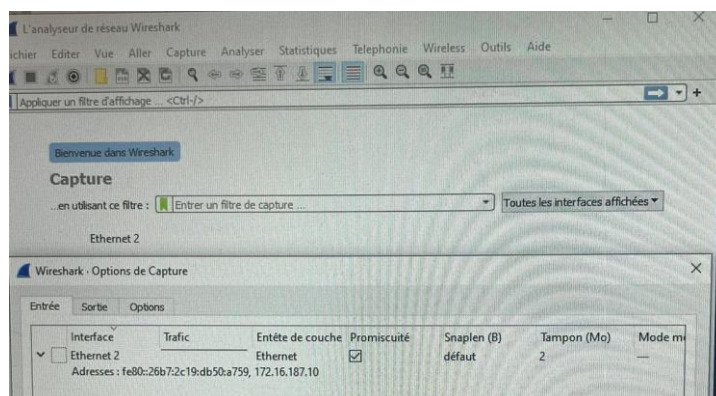
C:\Users\Utilisateur>
```

Step 1: c) The IP address is typically in IPv4 format (172.16.187.10), consisting of 32 bits. The MAC address is a 48-bit address typically represented in hexadecimal format (E4-54-E8-7C-3F-F9).

Step 1: d) The network mask is also known as the subnet mask. It is used to determine the network portion of an IP address. 255.255.0.0 (In binary form 11111111.11111111. 00000000.00000000) means that the first 16 bits (16 bits from the third octet) are allocated for the network (binary number 1). The remaining 16 bits are available for host addresses within that network (binary number 0).

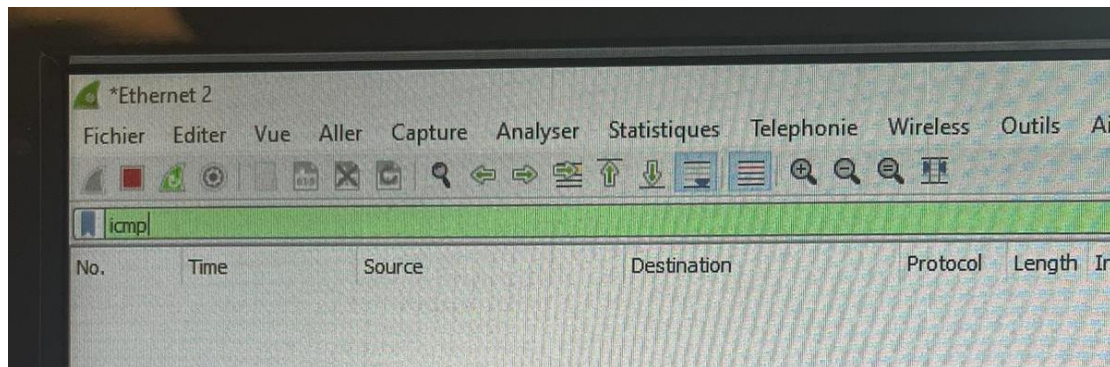
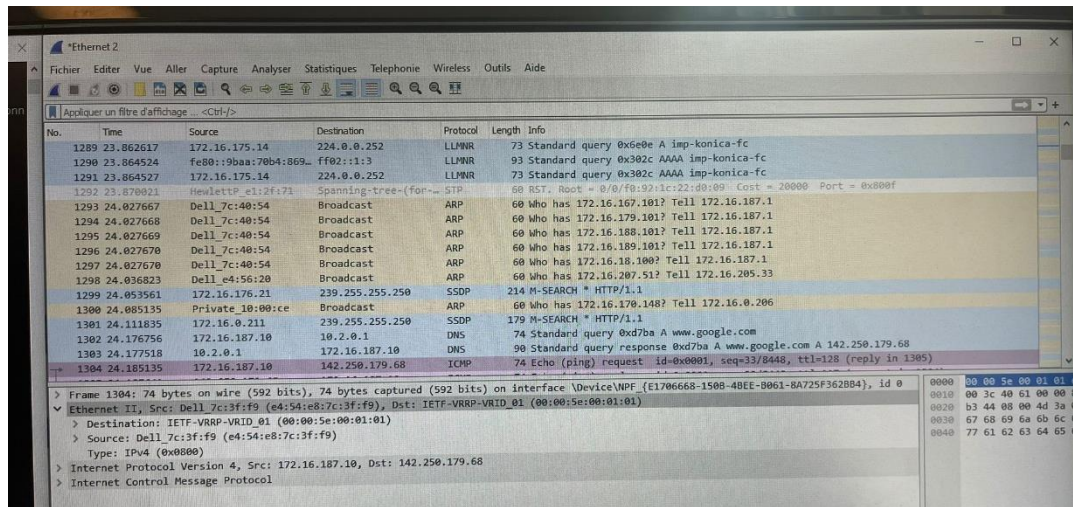
Step 1: e) For this WLAN, we can have the most 2^{16} hosts.

Step 2: a-d) IP is 172.16.187.10



Step 2: e-f) ping is used to test and diagnose network connections. It is often used

to check the status of communication between hosts.



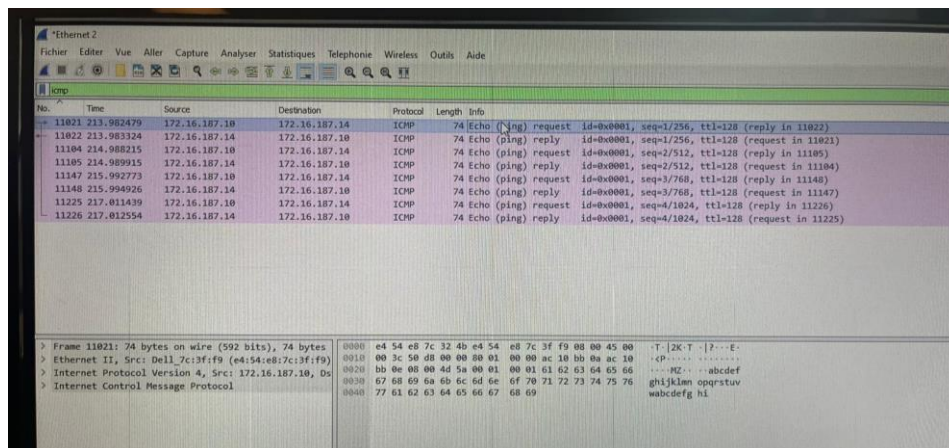
```
C:\Users\Utilisateur>ping 172.16.187.14

Envoi d'une requête 'Ping' 172.16.187.14 avec 32 octets de données :
Réponse de 172.16.187.14 : octets=32 temps<1ms TTL=128
Réponse de 172.16.187.14 : octets=32 temps=1 ms TTL=128
Réponse de 172.16.187.14 : octets=32 temps=2 ms TTL=128
Réponse de 172.16.187.14 : octets=32 temps=1 ms TTL=128

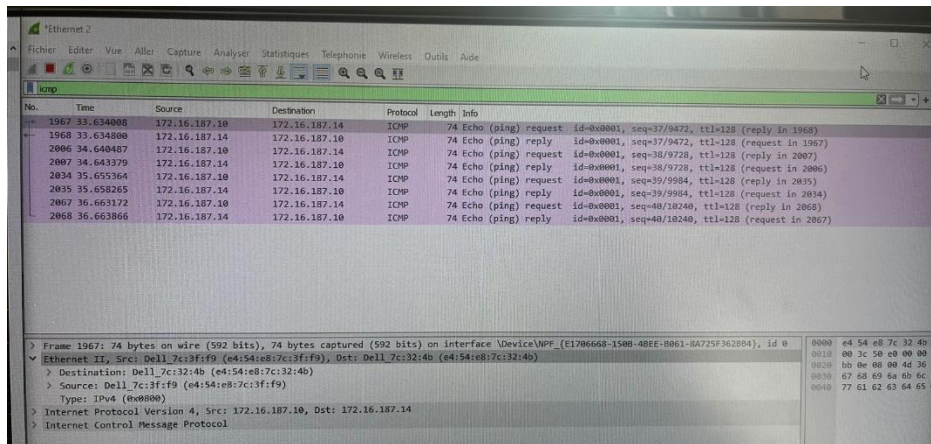
Statistiques Ping pour 172.16.187.14:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\Utilisateur>
```

Step 3: a)



Step 3: b)



1. The Source MAC address matches my PC's interface.
2. The Destination MAC address in Wireshark match my team member's MAC address.
3. The MAC address of the pinged machine is obtained by PC through the Address Resolution Protocol (ARP). When PC wants to communicate with another machine on the same local network, it uses ARP to discover the MAC address associated with the IP address of the target machine. ARP resolves the IP address to the corresponding MAC address, allowing PC to construct Ethernet frames for communication on the local network.

Part 2:

Step 1: a-b) The computer finds the IP addresses of website URLs by querying DNS (Domain Name System) servers. DNS servers provide the mapping between domain names and their corresponding IP addresses. When ping a website URL, computer checks its local cache, the hosts file, and then queries DNS servers to obtain the IP address associated with the domain name.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [version 10.0.19044.3448]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Utilisateur>ping www.yahoo.com

Envoi d'une requête 'ping' sur new-fp-shed.wg1.b.yahoo.com [87.248.100.215] avec 32 octets de données :
Réponse de 87.248.100.215 : octets=32 temps=20 ms TTL=52
Réponse de 87.248.100.215 : octets=32 temps=19 ms TTL=52
Réponse de 87.248.100.215 : octets=32 temps=20 ms TTL=51
Réponse de 87.248.100.215 : octets=32 temps=20 ms TTL=52

Statistiques Ping pour 87.248.100.215:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 19ms, Maximum = 20ms, Moyenne = 19ms

C:\Users\Utilisateur>
```

IP: 87.248.100.215

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Utilisateur>ping www.cisco.com

Envoi d'une requête 'ping' sur e2867.dsca.akamaiedge.net [23.206.65.124] avec 32 octets de données :
Réponse de 23.206.65.124 : octets=32 temps=2 ms TTL=244
Réponse de 23.206.65.124 : octets=32 temps=3 ms TTL=244
Réponse de 23.206.65.124 : octets=32 temps=2 ms TTL=244
Réponse de 23.206.65.124 : octets=32 temps=3 ms TTL=244

Statistiques Ping pour 23.206.65.124:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Users\Utilisateur>
```

IP:23.206.65.124

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Utilisateur>ping www.google.com

Envoi d'une requête 'ping' sur www.google.com [142.250.179.68] avec 32 octets de données :
Réponse de 142.250.179.68 : octets=32 temps=2 ms TTL=117
Réponse de 142.250.179.68 : octets=32 temps=2 ms TTL=117
Réponse de 142.250.179.68 : octets=32 temps=3 ms TTL=117
Réponse de 142.250.179.68 : octets=32 temps=3 ms TTL=117

Statistiques Ping pour 142.250.179.68:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Users\Utilisateur>
```

IP:142.250.179.68

Step 2: a-b)

The image shows a Wireshark packet capture of ICMP ping traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1743	25.171455	172.16.187.10	87.248.100.215	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 1744)
1744	25.191554	87.248.100.215	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=52 (request in 1743)
1708	26.187661	172.16.187.10	87.248.100.215	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 1781)
1781	26.206931	87.248.100.215	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=52 (request in 1780)
1835	27.202600	172.16.187.10	87.248.100.215	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 1836)
1836	27.222385	87.248.100.215	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=51 (request in 1835)
1900	28.216808	172.16.187.10	87.248.100.215	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 1901)
1901	28.236790	87.248.100.215	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=52 (request in 1900)

The packet details pane for the selected packet (Frame 1743) shows:

- Ethernet II, Src: Dell 7c:3f:f9 (e4:54:e8:7c:3f:f9), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
- Destination: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
- Source: Dell 7c:3f:f9 (e4:54:e8:7c:3f:f9)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.16.187.10, Dst: 87.248.100.215
- Internet Control Message Protocol

FOR www.yahoo.com
Destination IP: 87.248.100.215
MAC addresses: IETF-VRRP-VRID_01

No.	Time	Source	Destination	Protocol	Length	Info
2484	44.318155	172.16.187.10	23.206.65.124	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (reply in 2485)
2485	44.320727	23.206.65.124	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=244 (request in 2484)
2514	45.327762	172.16.187.10	23.206.65.124	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (reply in 2515)
2515	45.330799	23.206.65.124	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=244 (request in 2514)
2595	46.331487	172.16.187.10	23.206.65.124	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 2596)
2596	46.333939	23.206.65.124	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=244 (request in 2595)
2661	47.336680	172.16.187.10	23.206.65.124	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 2662)
2662	47.340329	23.206.65.124	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=244 (request in 2661)

Frame 2484: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{E1706668-1508-4BEE-B061-8A725F362B84}, id 0
 Ethernet II, Src: Dell 7c:3f:f9 (e4:54:e8:7c:3f:f9), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
 Destination: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
 Source: Dell 7c:3f:f9 (e4:54:e8:7c:3f:f9)
 Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 172.16.187.10, Dst: 23.206.65.124
 Internet Control Message Protocol

FOR www.cisco.com
 Destination IP: 23.206.65.124
 MAC addresses: IETF-VRRP-VRID_01

No.	Time	Source	Destination	Protocol	Length	Info
1304	24.185135	172.16.187.10	142.250.179.68	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 1305)
1305	24.187641	142.250.179.68	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=117 (request in 1304)
1359	25.196671	172.16.187.10	142.250.179.68	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 1360)
1360	25.199425	142.250.179.68	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=117 (request in 1359)
1401	26.202409	172.16.187.10	142.250.179.68	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 1402)
1402	26.206062	142.250.179.68	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=117 (request in 1401)
1487	27.218314	172.16.187.10	142.250.179.68	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 1488)
1488	27.221236	142.250.179.68	172.16.187.10	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=117 (request in 1487)

Frame 1304: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{E1706668-1508-4BEE-B061-8A725F362B84}, id 0
 Ethernet II, Src: Dell 7c:3f:f9 (e4:54:e8:7c:3f:f9), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
 Destination: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
 Source: Dell 7c:3f:f9 (e4:54:e8:7c:3f:f9)
 Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 172.16.187.10, Dst: 142.250.179.68
 Internet Control Message Protocol

FOR www.google.com
 Destination IP: 142.250.179.68
 MAC addresses: IETF-VRRP-VRID_01

1) MAC addresses formats are different: Web Ping uses a public IP address without requiring direct knowledge of the target server's MAC address.

2) What is the main difference between a local and a remote communication?

For Local Communication: the scope within the local network, the characteristics faster, lower latency, direct communication.

For Remote Communication: the scope across different networks, the characteristics may involve routers, higher latency, relies on external infrastructure.

Packet Tracer - Navigating the IOS

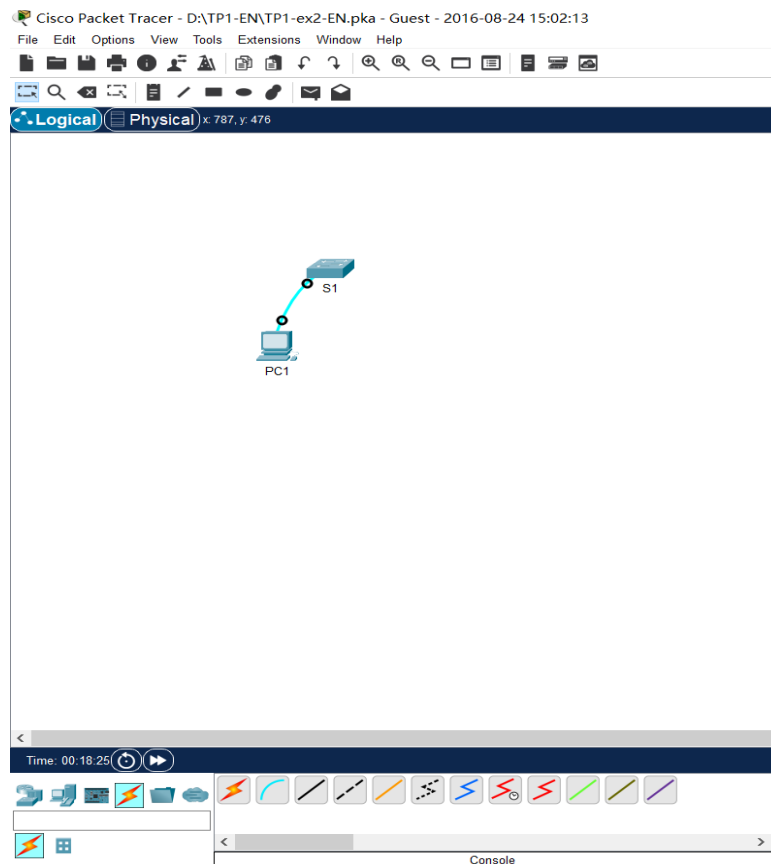
Packet Tracer - Basic Switch and End Device Configuration -

Physical Mode

Part 1:

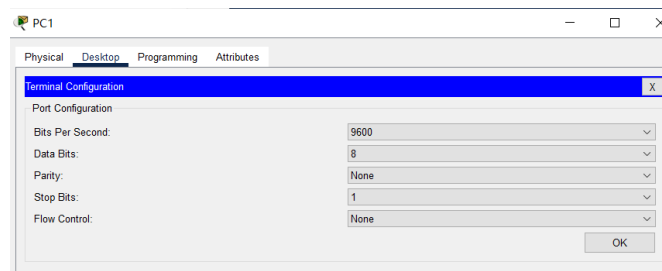
Step 1: Packet Tracer – Navigating the IOS

Connect PC1 to S1 using a console cable



Step 2: Establish a terminal session with S1.

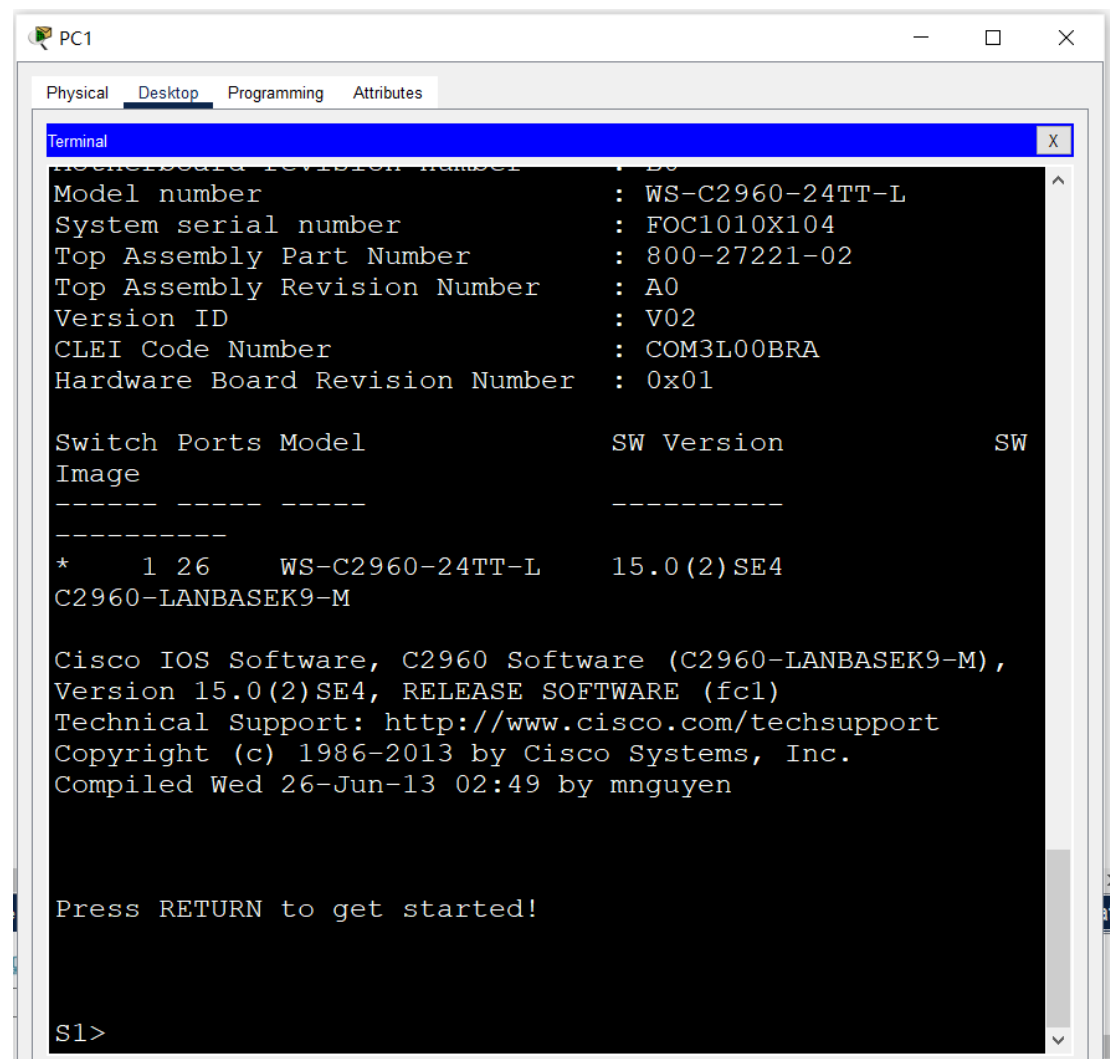
b.)



What is the setting for bits per second?

The setting for bits per second is 9600.

d.



What is the prompt displayed on the screen?

"S1>" is displayed on the screen.

Step 3: Explore the IOS Help

a.

```
S1>?
Exec commands:
  connect      Open a terminal connection
  disable      Turn off privileged commands
  disconnect    Disconnect an existing network connection
  enable        Turn on privileged commands
  exit          Exit from the EXEC
  logout        Exit from the EXEC
  ping          Send echo messages
  resume        Resume an active network connection
  show          Show running system information
  ssh           Open a secure shell client connection
  telnet        Open a telnet connection
  terminal      Set terminal line parameters
  traceroute    Trace route to destination
```

Which command begins with the letter 'C'?
The command of connect begins with the letter 'C'.

b.

```
S1>t?  
telnet  terminal  traceroute
```

Which commands are displayed?
'telnet', 'terminal', 'traceroute' are displayed.

c.

```
S1>te?  
telnet  terminal
```

Which commands are displayed?
'telnet' and 'terminal' are displayed.

Part2 : Explore EXEC Modes

Step 1 :

a.

```
S1>?  
Exec commands:  
  connect      Open a terminal connection  
  disable      Turn off privileged commands  
  disconnect    Disconnect an existing network connection  
  enable       Turn on privileged commands  
  exit         Exit from the EXEC  
  logout       Exit from the EXEC  
  ping        Send echo messages  
  resume      Resume an active network connection  
  show        Show running system information  
  ssh         Open a secure shell client connection  
  telnet      Open a telnet connection  
  terminal    Set terminal line parameters  
  traceroute  Trace route to destination
```

What information is displayed that describes the enable command?
Turn on privileged commands.

b.

```
S1>en  
S1>enable
```

What displays after pressing the Tab key?

The enable command has been completed.

```
S1>te
S1>te|
```

What would happen if you typed te<Tab> at the prompt?

The command will not be completed because the commands starting with 'te' include telnet and terminal, and the system does not know which command to complete it into.

c.

```
S1>enable
S1#|
```

Enter the enable command and press ENTER. How does the prompt change?

The symbol after S1 changes from > to #.

d.

```
S1#?
Exec commands:
  clear      Reset functions
  clock      Manage the system clock
  configure  Enter configuration mode
  connect    Open a terminal connection
  copy       Copy from one file to another
  debug      Debugging functions (see also 'undebug')
  delete     Delete a file
  dir        List files on a filesystem
  disable    Turn off privileged commands
  disconnect Disconnect an existing network connection
  enable     Turn on privileged commands
  erase      Erase a filesystem
  exit       Exit from the EXEC
  logout     Exit from the EXEC
  more       Display the contents of a file
  no         Disable debugging informations
  ping       Send echo messages
  reload     Halt and perform a cold restart
  resume     Resume an active network connection
  setup      Run the SETUP command facility
  show       Show running system information
--More--
```

```
S1#c?
clear  clock  configure  connect  copy
```

How many commands are displayed now that privileged EXEC mode is active?

5 commands. They are clear, clock, configure, connect and copy.

Step2:

a.

```
S1#c?  
clear  clock  configure  connect  copy  
S1#co?  
configure  connect  copy  
S1#co?  
configure  connect  copy  
S1#con?  
configure  connect  
S1#conf?  
configure  
S1#conf  
S1#configure  
Configuring from terminal, memory, or network  
[terminal]?
```

What is the message that is displayed?

Configuring form terminal, memory, or network.

b.

```
S1#configure  
Configuring from terminal, memory, or network  
[terminal]?  
Enter configuration commands, one per line.  End with  
CNTL/Z.  
S1(config)#|
```

How does the prompt change?

The prompt change from S1# to S1(config)#.

c.

```
S1(config)#exit  
S1#  
%SYS-5-CONFIG_I: Configured from console by console
```

Part 3 : Set Clock

a.

```
S1#show clock
*0:51:45.406 UTC Mon Mar 1 1993
S1#
```

What information is displayed? What is the year that is displayed?

'0:51:45.406 UTC Mon Mar 1 1993' is displayed. 1993 is the year that is displayed.

b.

```
S1#clock
% Incomplete command.
```

What information is being requested?

Incomplete command.

c.

```
S1#clock ?
set Set the time and date
```

What information is being requested?

Set the time and date.

d.

```
S1#clock set ?
hh:mm:ss Current Time
```

What information is being requested?

The specific hours, minutes and seconds of the clock.

```
S1#clock set
% Incomplete command.
```

What would have been displayed if only the clock set command had been entered, and no request for help was made by using the question mark?

Incomplete command.

e.

```
S1#clock set 15:00:00 ?
<1-31> Day of the month
MONTH Month of the year
```

f.


```
S1#clock set ?  
    hh:mm:ss  Current Time  
S1#clock set  
% Incomplete command.  
S1#clock set 15:00:00 ?  
    <1-31>   Day of the month  
    MONTH   Month of the year  
S1#clock set 15:00:00 31 01?  
% Unrecognized command  
S1#clock set 15:00:00 31 Jan?  
MONTH  
S1#clock set 15:00:00 31 Jan 2035 ?  
    <cr>  
S1#clock set 15:00:00 31 Jan 2035
```

g.

```
S1#show clock  
15:0:6.520 UTC Wed Jan 31 2035
```

Step 2 : Explore additional command messages.

a.

```
S1#cl  
S1#cl
```

What information was returned?

It returned 'cl'.

b.

```
S1#clock  
% Incomplete command.
```

What information was returned?

Incomplete command.

c.

```
S1#clock set 25:00:00  
                ^  
% Invalid input detected at '^' marker.
```

What information was returned?

Invalid input detected at '^' marker. Because 25 is not the correct expression for hours.

d.

```
S1#clock set 15:00:00 32
                        ^
% Invalid input detected at '^' marker.
```

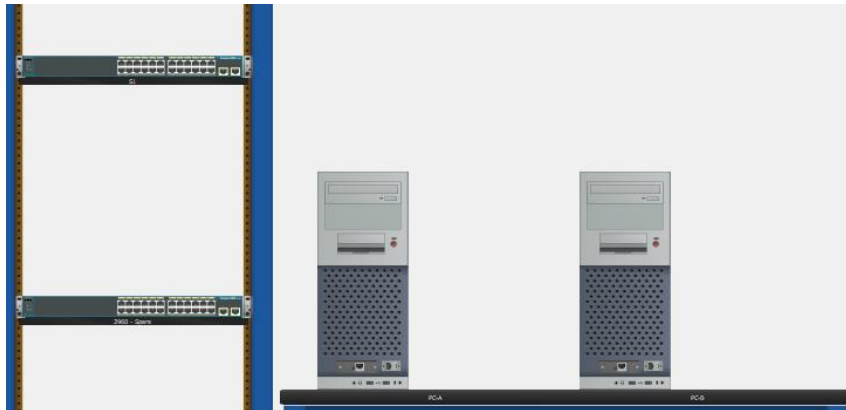
What information was returned?

Invalid input detected at '^' marker. Because 32 is not a correct date expression.

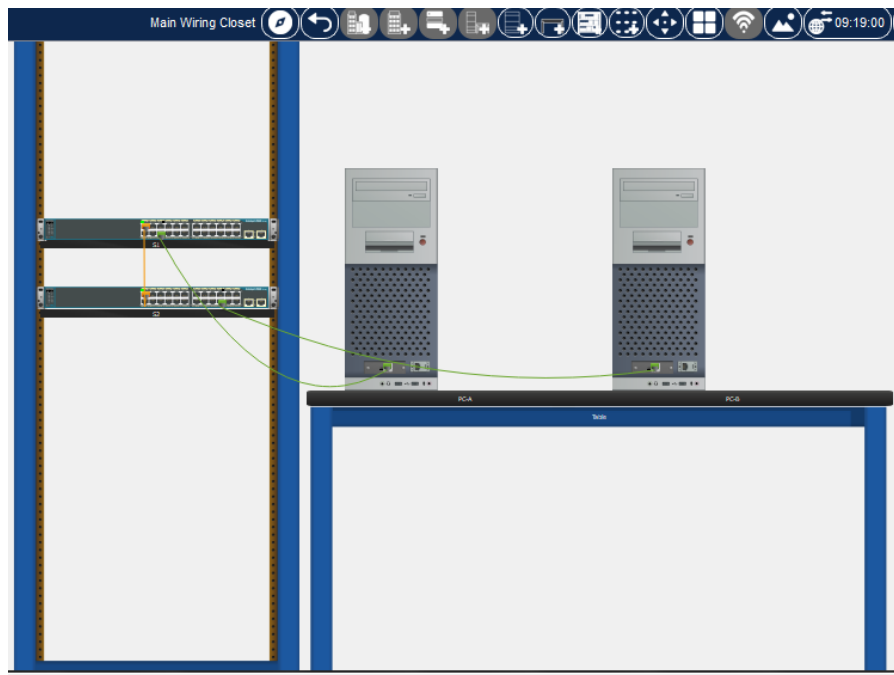
Lab - Basic Switch and End Device Configuration Physical Mode

Part 1: Set Up the Network Topology

(a) Click and drag switches to the Rack, click two PCs to the Table and Powered them.



(b) Connect the switches with PCs by cable to set up the network topology



Part 2 Configure PC Hosts

- (a) Configure static IP address information on the PCs according to the Addressing Table. Enter the IP address for PC-A (192.168.1.10) and the subnet mask (255.255.255.0), as listed in the IP addressing table.

```
Connection-specific DNS Suffix...:
Physical Address.....: 000A.F355.6C9E
Link-local IPv6 Address.....: FE80::20A:F3FF:FE55:6C9E
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                        0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-15-DB-75-3D-00-0A-F3-55-6C-9E
DNS Servers.....: ::
                        0.0.0.0
```

- (b) Repeat the previous steps to assign the IP address information for PC-

B

```
Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 0001.42D3.ABE6
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::

C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Part 3: Configure and Verify Basic Switch Settings

Connect the console cable between S1 and PC-A.

Connect the console cable between S2 and PC-B.



```
Physical Config Desktop Programming
Terminal
FastEthernet0/8      unassigned      YES manual down    down
FastEthernet0/9      unassigned      YES manual down    down
FastEthernet0/10     unassigned      YES manual down    down
FastEthernet0/11     unassigned      YES manual down    down
FastEthernet0/12     unassigned      YES manual down    down
FastEthernet0/13     unassigned      YES manual down    down
FastEthernet0/14     unassigned      YES manual down    down
FastEthernet0/15     unassigned      YES manual down    down
FastEthernet0/16     unassigned      YES manual down    down
FastEthernet0/17     unassigned      YES manual down    down
FastEthernet0/18     unassigned      YES manual down    down
FastEthernet0/19     unassigned      YES manual down    down
FastEthernet0/20     unassigned      YES manual down    down
FastEthernet0/21     unassigned      YES manual down    down
FastEthernet0/22     unassigned      YES manual down    down
FastEthernet0/23     unassigned      YES manual down    down
FastEthernet0/24     unassigned      YES manual down    down
GigabitEthernet0/1   unassigned      YES manual down    down
GigabitEthernet0/2   unassigned      YES manual down    down
Vlan1                192.168.1.1     YES manual up      up
S1#
```

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname s1
s1(config)#enable secret class
s1(config)#line console 0
s1(config-line)#password cisco
s1(config-line)#login
s1(config-line)#exit
s1(config)#
```

```
sl(config)#int vlan 1
sl(config-if)#ip address 192.168.1.1 255.255.255.0
sl(config-if)#no shutdown

sl(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

```
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
!
 banner motd ^CUnauthorized Access is Prohibited!^C
!
!
line con 0
 password cisco
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
end

sl# |
```



```

s1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 00E0.F780.A6A8
Motherboard assembly number    : 73-9832-06
Power supply part number       : 341-0097-02
Motherboard serial number      : FOC103248MJ
Power supply serial number     : DCA102133JA
Model revision number          : B0
Motherboard revision number    : C0
Model number                   : WS-C2960-24TT
System serial number           : FOC103321EY
Top Assembly Part Number       : 800-26671-02
Top Assembly Revision Number   : B0
Version ID                     : V02
CLEI Code Number               : COM3K00BRA
Hardware Board Revision Number : 0x01

Switch  Ports  Model          SW Version      SW Image
-----  -
* 1    26    WS-C2960-24TT  12.2            C2960-LANBASE-M

Configuration register is 0xF

```

Repeat the steps on the PC-b

```

s2#show ip int brife
^
% Invalid input detected at '^' marker.

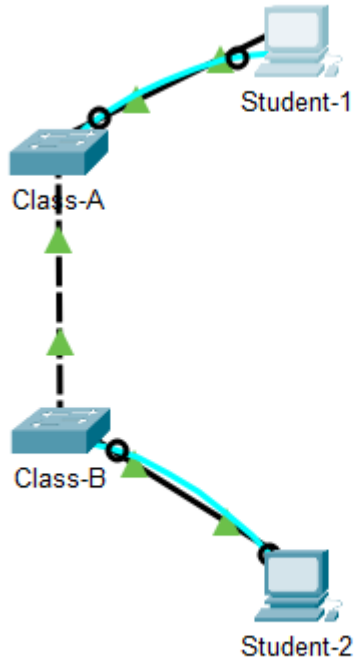
s2#show ip int brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/1 unassigned      YES manual up          up
FastEthernet0/2 unassigned      YES manual down        down
FastEthernet0/3 unassigned      YES manual down        down
FastEthernet0/4 unassigned      YES manual down        down
FastEthernet0/5 unassigned      YES manual down        down
FastEthernet0/6 unassigned      YES manual down        down
FastEthernet0/7 unassigned      YES manual down        down
FastEthernet0/8 unassigned      YES manual down        down
FastEthernet0/9 unassigned      YES manual down        down
FastEthernet0/10 unassigned      YES manual down        down
FastEthernet0/11 unassigned      YES manual down        down
FastEthernet0/12 unassigned      YES manual down        down
FastEthernet0/13 unassigned      YES manual down        down
FastEthernet0/14 unassigned      YES manual down        down
FastEthernet0/15 unassigned      YES manual down        down
FastEthernet0/16 unassigned      YES manual down        down
FastEthernet0/17 unassigned      YES manual down        down
FastEthernet0/18 unassigned      YES manual up          up
FastEthernet0/19 unassigned      YES manual down        down
FastEthernet0/20 unassigned      YES manual down        down
FastEthernet0/21 unassigned      YES manual down        down
FastEthernet0/22 unassigned      YES manual down        down
FastEthernet0/23 unassigned      YES manual down        down
FastEthernet0/24 unassigned      YES manual down        down
GigabitEthernet0/1 unassigned      YES manual down        down
GigabitEthernet0/2 unassigned      YES manual down        down
Vlan1          192.168.1.2     YES manual up            up
s2#

```

Packet Tracer - Skills Integration Challenge

Requirements

1.



2.

```
Switch>
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Class-A
Class-A(config)#interface vlan 1
Class-A(config-if)#ip address 128.107.20.10 255.255.255.0
Class-A(config-if)#no shutdown

Class-A(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
exit
Class-A(config)#exit
Class-A#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#interface vlan 1
S1(config-if)#ip address 128.107.20.15 255.255.255.0
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
exit
S1(config)#hostname Class-B
Class-B(config)#exit
Class-B#
%SYS-5-CONFIG_I: Configured from console by console

Class-B#
```