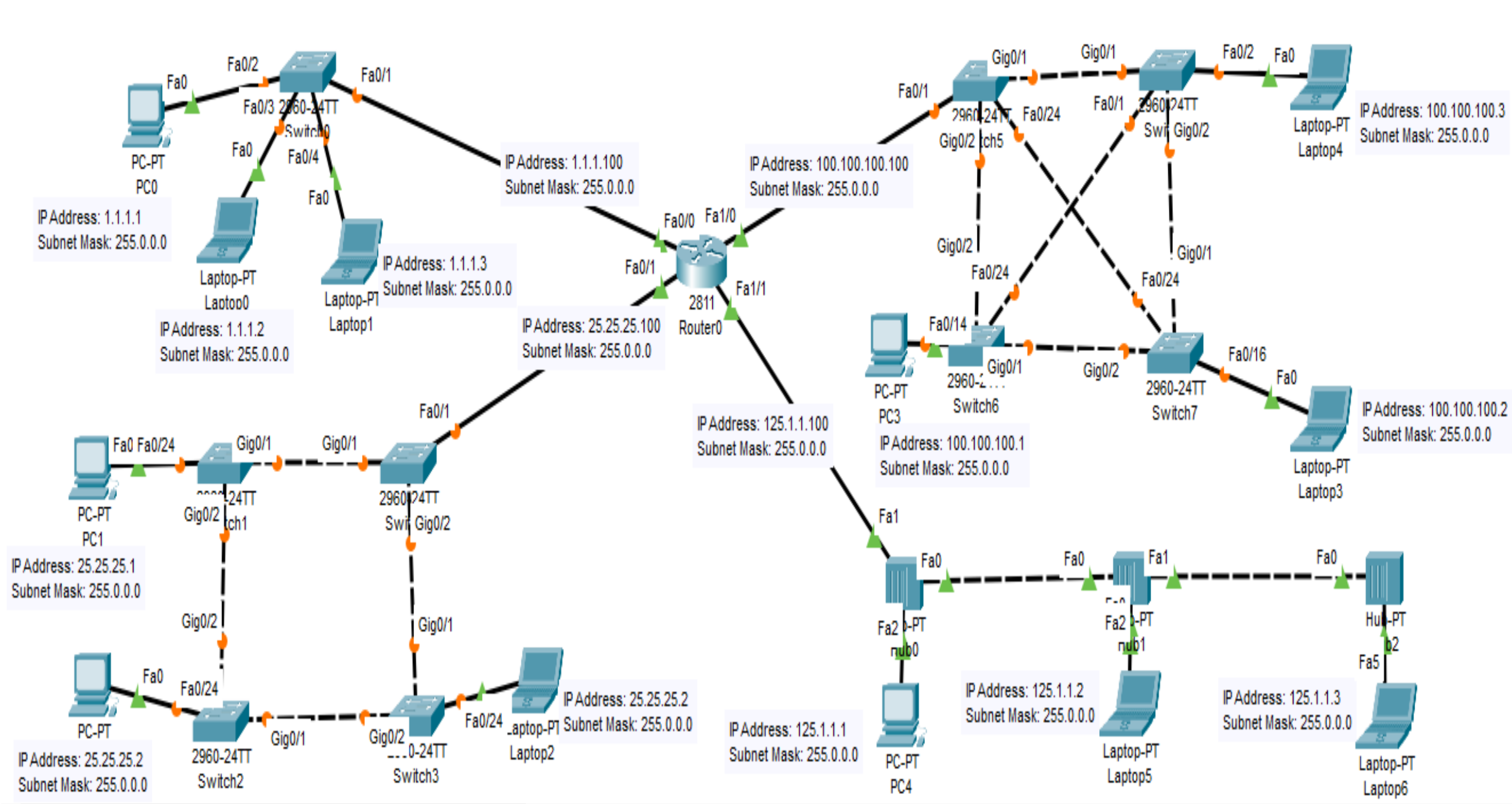
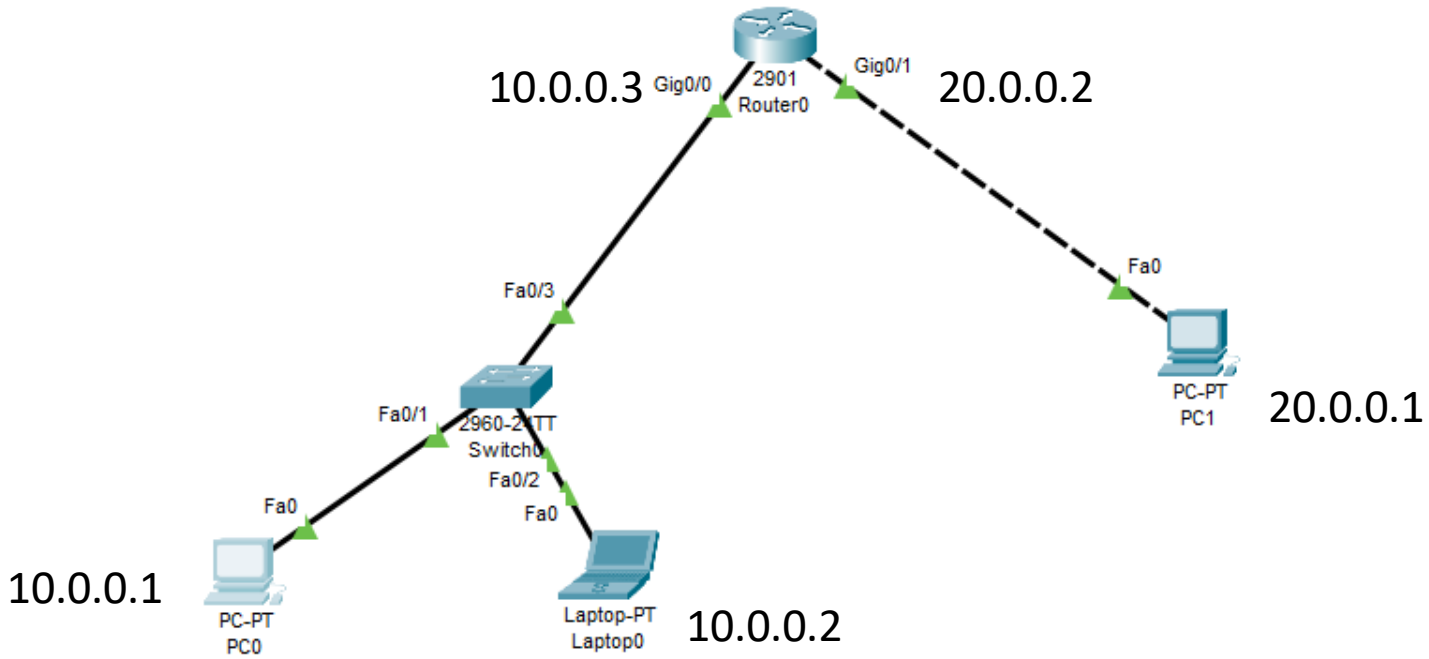
Commands


PC-PT
PC0
IP Address: 1.1.1.1
Subnet Mask: 255.0.0.0
Laptop-PT
Laptop0
IP Address: 1.1.1.2
Subnet Mask: 255.0.0.0
Laptop-PT
Laptop1
IP Address: 1.1.1.3
Subnet Mask: 255.0.0.0
IP Address: 1.1.1.100
Subnet Mask: 255.0.0.0
2811
Router0
IP Address: 25.25.25.100
Subnet Mask: 255.0.0.0
IP Address: 100.100.100.100
Subnet Mask: 255.0.0.0
IP Address: 125.1.1.100
Subnet Mask: 255.0.0.0
PC-PT
PC1
IP Address: 25.25.25.1
Subnet Mask: 255.0.0.0
PC-PT
PC2
IP Address: 25.25.25.2
Subnet Mask: 255.0.0.0
2960-24TT
Switch2
2960-24TT
Switch3
Laptop-PT
Laptop2
IP Address: 25.25.25.2
Subnet Mask: 255.0.0.0
PC-PT
PC3
IP Address: 100.100.100.1
Subnet Mask: 255.0.0.0
Switch6
2960-24TT
Switch7
Laptop-PT
Laptop3
IP Address: 100.100.100.2
Subnet Mask: 255.0.0.0
Laptop-PT
Laptop4
IP Address: 100.100.100.3
Subnet Mask: 255.0.0.0
PC-PT
PC4
IP Address: 125.1.1.1
Subnet Mask: 255.0.0.0
Laptop-PT
Laptop5
IP Address: 125.1.1.2
Subnet Mask: 255.0.0.0
Laptop-PT
Laptop6
IP Address: 125.1.1.3
Subnet Mask: 255.0.0.0

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 941, y: 395 Root 05:53:30



Time: 00:11:42 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)

Automatically Choose Connection Type

Type here to search 11°C Clear ENG IN 6:58 AM 11/21/2022

ping

- ping from PC0 to PC1

```
C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127

Ping statistics for 20.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

trace

- tracert command based on previous ping command
- On pc, there is tracert command and on router, there is trace command

```
C:\>tracert 20.0.0.1

Tracing route to 20.0.0.1 over a maximum of 30 hops:

  1    0 ms      1 ms      1 ms      10.0.0.3
  2    0 ms      0 ms      1 ms      20.0.0.1

Trace complete.
```

ipconfig

- ipconfig on PC0

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:70FF:FE6D:3A43
   IPv6 Address.....: ::
   IPv4 Address.....: 10.0.0.1
   Subnet Mask.....: 255.0.0.0
   Default Gateway.....: ::
                                 10.0.0.3

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

arp

- The **Address Resolution Protocol** (**ARP**) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.
- arp –a on PC0

```
C:\>arp
Cisco Packet Tracer PC ARP
Display ARP entries: arp -a
Clear ARP table: arp -d

C:\>arp -a
  Internet Address      Physical Address      Type
  10.0.0.2              0030.f2ab.da5e        dynamic
  10.0.0.3              00d0.bad9.6a01        dynamic
```

netstat

- Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols).

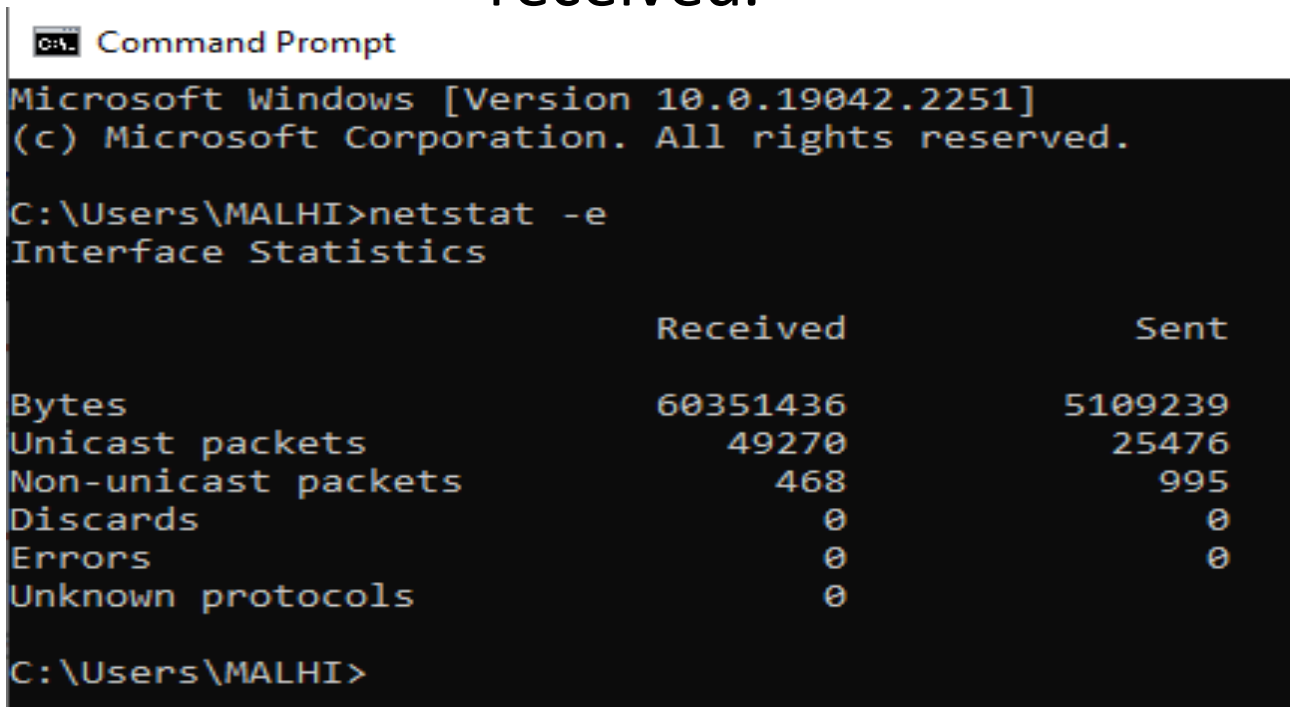
- **Syntax**
- **netstat** [**-a**] [**-e**] [**-n**] [**-o**] [**-p** *Protocol*] [**-r**] [**-s**] [*Interval*]

- Parameters

- **-a** : Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
-
- **-e** : Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with **-s**.
-
- **-n** : Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.

- **-o** : Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the **Processes** tab in Windows Task Manager. This parameter can be combined with **-a**, **-n**, and **-p**.
- **-p** ***Protocol*** : Shows connections for the protocol specified by *Protocol*. In this case, the *Protocol* can be **tcp**, **udp**, **tcpv6**, or **udpv6**. If this parameter is used with **-s** to display statistics by protocol, *Protocol* can be **tcp**, **udp**, **icmp**, **ip**, **tcpv6**, **udpv6**, **icmpv6**, or **ipv6**.
- **-s** : Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The **-p** parameter can be used to specify a set of protocols.
- **-r** : Displays the contents of the IP routing table. This is equivalent to the **route print** command.

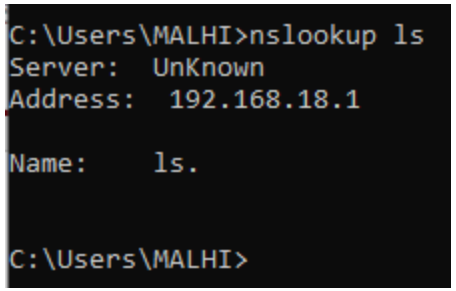
Parameter	Description
netstat –e	Displays Ethernet statistics, such as the number of bytes and packets sent and received.



nslookup

- Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works.

Parameter	Description
nslookup ls	Lists information for a DNS domain.



References

- https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat