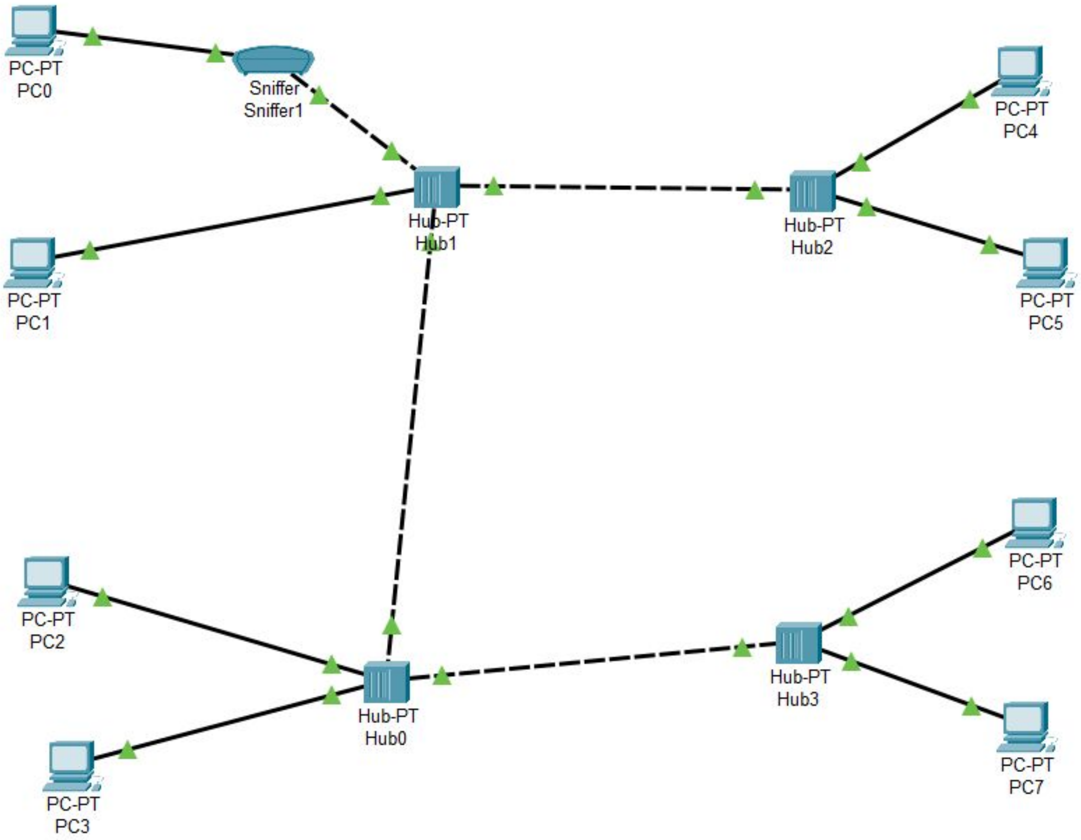
DEPARTMENT OF COMPUTER ENGINEERING
HACETTEPE UNIVERSITY
1977

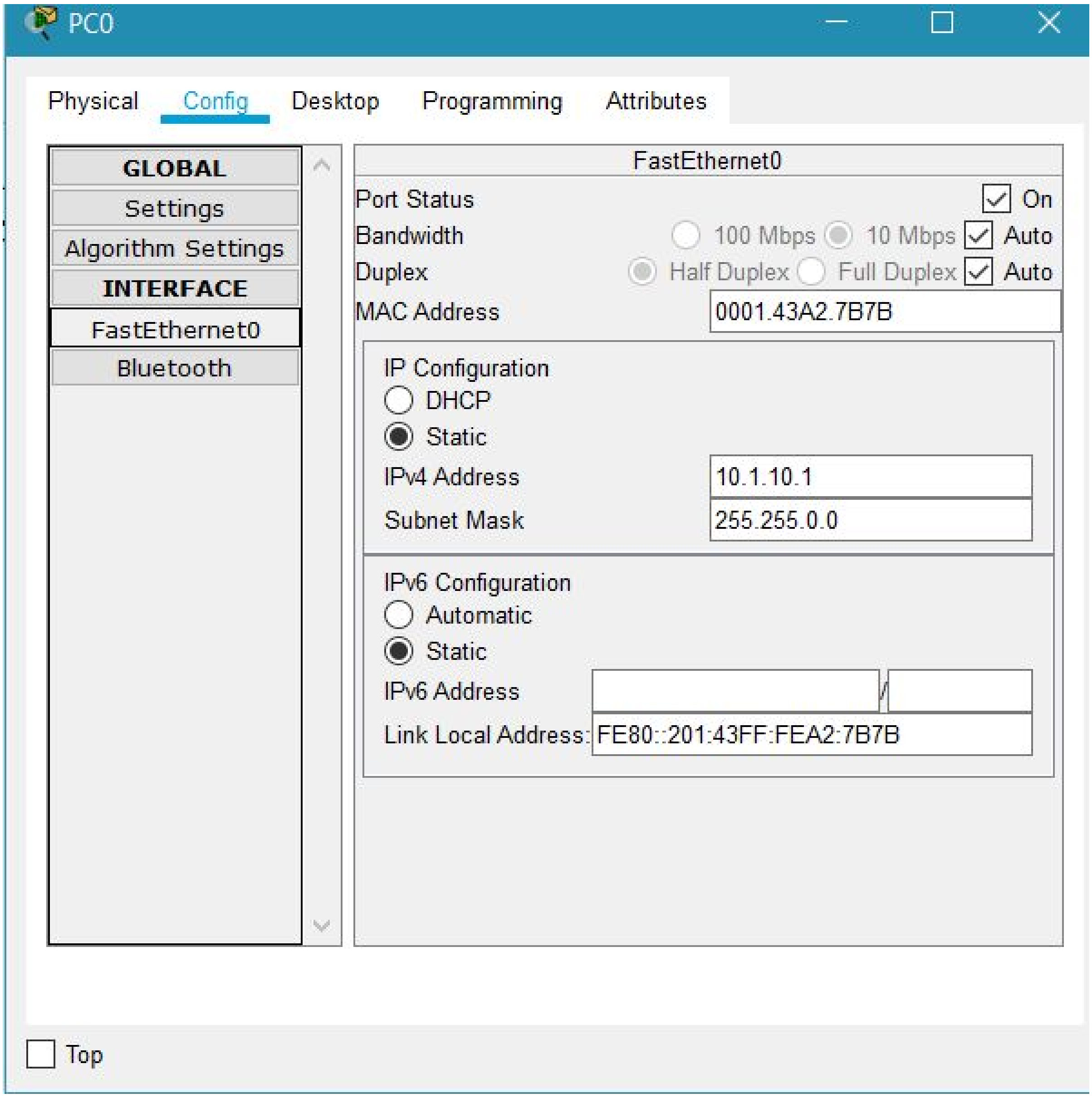
Gökhan Özeloğlu - 21627557
Burak Yılmaz - 21627868
BBM 453 Computer Networks Lab - LAN Lab Assignment
Group ID: 1



We put a sniffer to catch packets that we sent. We used copper straight-through wire to connect computers to hub devices. A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub.

We also used copper cross-over cable to connect hub devices. An Ethernet cross-over cable, also known as a crossed cable, connects two Ethernet network devices to each other. These cables were created to support temporary host-to-host networking in situations where an intermediate device, such as a network router, is not present.(Answered questions 1,2,4)

Green arrow means there is a connection between the devices.(Question answered 6)



FastEthernet0

Port Status ☑ On

Bandwidth ○ 100 Mbps ● 10 Mbps ☑ Auto

Duplex ● Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0001.43A2.7B7B

IP Configuration

○ DHCP

● Static

IPv4 Address 10.1.10.1

Subnet Mask 255.255.0.0

IPv6 Configuration

○ Automatic

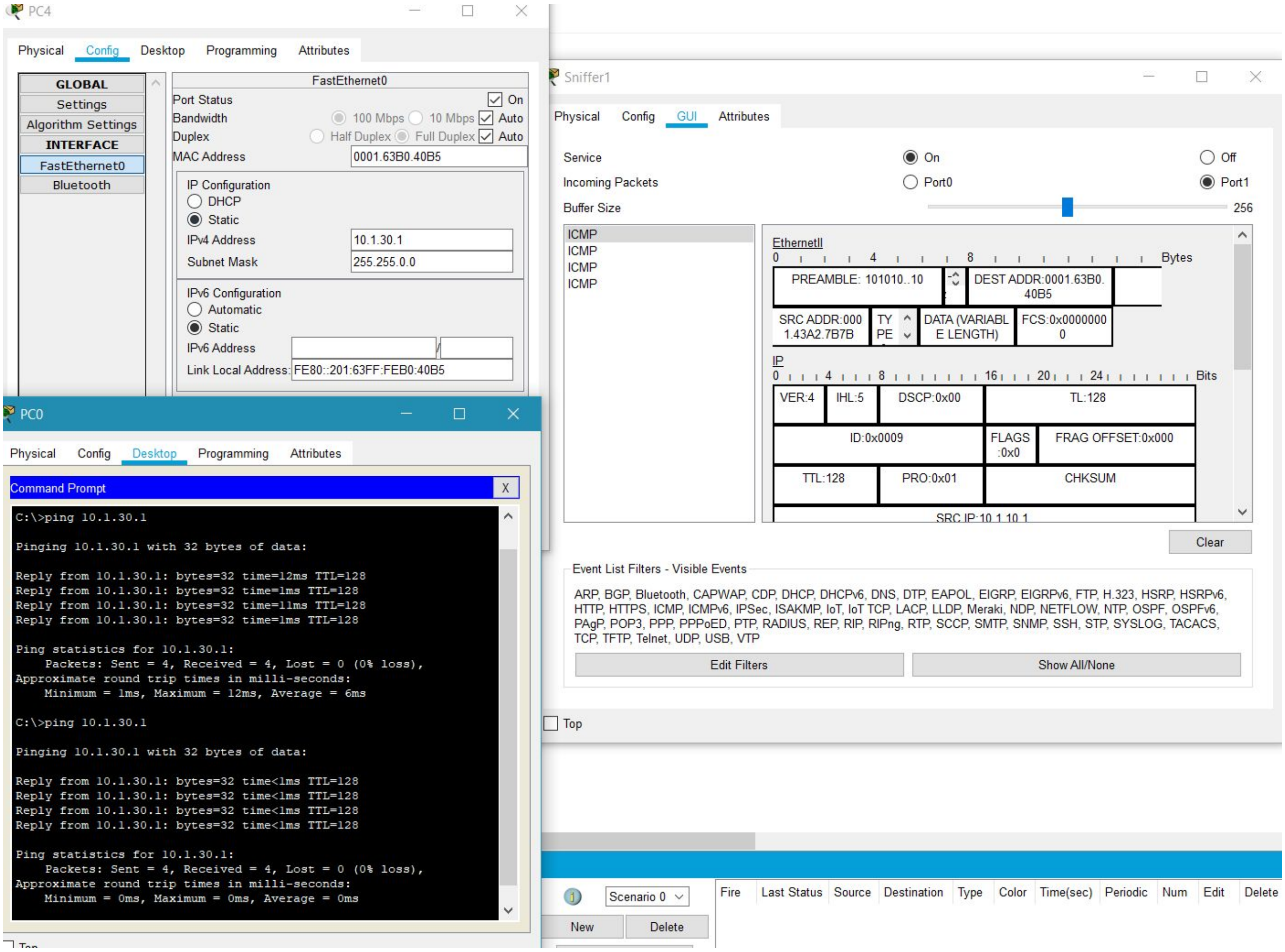
● Static

IPv6 Address /

Link Local Address: FE80::201:43FF:FEA2:7B7B

☐ Top

Our group number is 1 so that our IP is 10.1.xx.x.(Answered question 3)



FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0001.63B0.40B5

IP Configuration

○ DHCP

● Static

IPv4 Address 10.1.30.1

Subnet Mask 255.255.0.0

IPv6 Configuration

○ Automatic

● Static

IPv6 Address /

Link Local Address: FE80::201:63FF:FEB0:40B5

Service ● On ○ Off

Incoming Packets ○ Port0 ● Port1

Buffer Size 256

ICMP
ICMP
ICMP
ICMP

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | DEST ADDR:0001.63B0.40B5

SRC ADDR:0001.43A2.7B7B | TYPE | DATA (VARIABLE LENGTH) | FCS:0x00000000

IP

0 4 8 16 20 24 Bits

VER:4 | IHL:5 | DSCP:0x00 | TL:128

ID:0x0009 | FLAGS:0x0 | FRAG OFFSET:0x000

TTL:128 | PRO:0x01 | CHKSUM

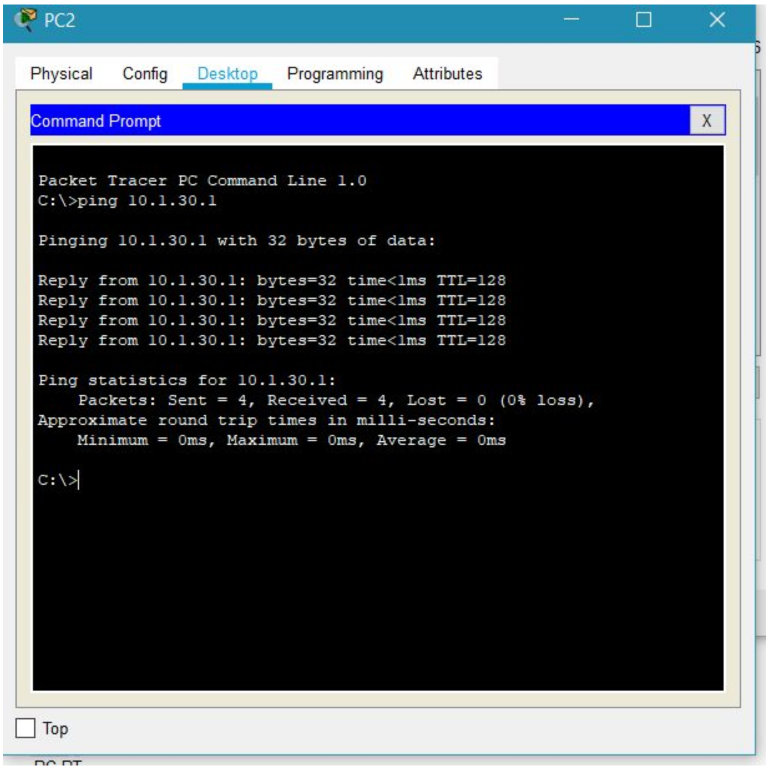
SRC IP:10.1.10.1

Event List Filters - Visible Events

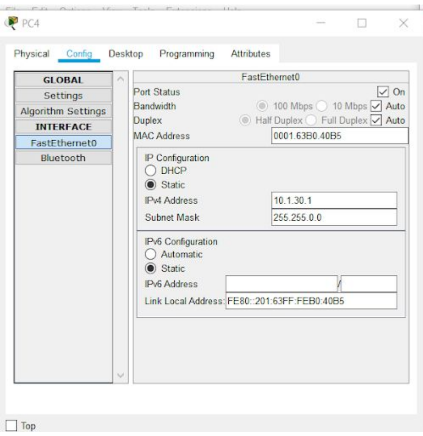
ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

```
C:\>ping 10.1.30.1

Pinging 10.1.30.1 with 32 bytes of data:

Reply from 10.1.30.1: bytes=32 time=12ms TTL=128
Reply from 10.1.30.1: bytes=32 time=1ms TTL=128
Reply from 10.1.30.1: bytes=32 time=11ms TTL=128
Reply from 10.1.30.1: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 6ms

C:\>ping 10.1.30.1

Pinging 10.1.30.1 with 32 bytes of data:

Reply from 10.1.30.1: bytes=32 time<1ms TTL=128
Reply from 10.1.30.1: bytes=32 time<1ms TTL=128
Reply from 10.1.30.1: bytes=32 time<1ms TTL=128
Reply from 10.1.30.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

We pinged PC(4) 10.1.30.1 IP Address from PC(0) 10.1.10.1 IP Address. We captured our packets from Sniffer1 which is expected in this case .We also see that the dest and source mac addresses on sniffer are compatible with the PC0 and PC4 that’s why we make sure that we ping the correct computer.(Questions answered 5,7,8)



```
Packet Tracer PC Command Line 1.0
C:\>ping 10.1.30.1

Pinging 10.1.30.1 with 32 bytes of data:

Reply from 10.1.30.1: bytes=32 time<1ms TTL=128
Reply from 10.1.30.1: bytes=32 time<1ms TTL=128
Reply from 10.1.30.1: bytes=32 time<1ms TTL=128
Reply from 10.1.30.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ● Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0001.63B0.40B5

IP Configuration

○ DHCP

● Static

IPv4 Address 10.1.30.1

Subnet Mask 255.255.0.0

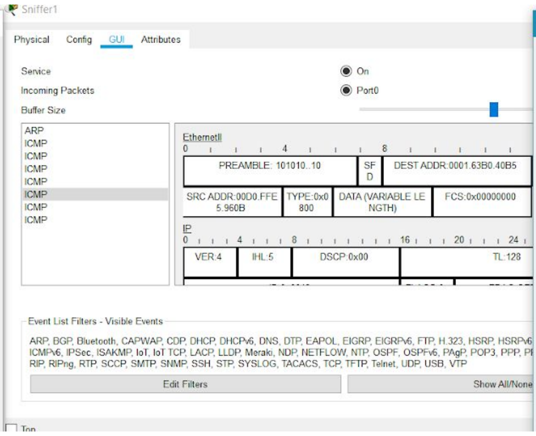
IPv6 Configuration

○ Automatic

● Static

IPv6 Address /

Link Local Address: FE80::201:63FF:FEB0:40B5



Service ● On

Incoming Packets ● Port0

Buffer Size

ARP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP

EthernetII

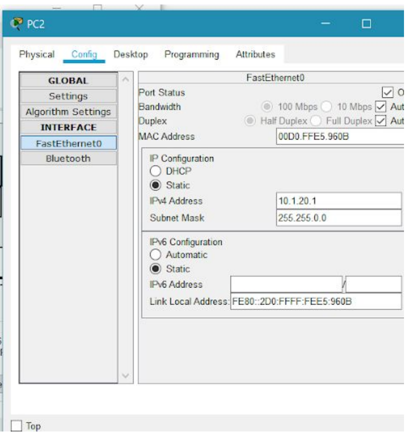
PREAMBLE: 101010..10	SFD	DEST ADDR:0001.63B0.40B5
SRC ADDR:00D0.FFE5.960B	TYPE:0x0800	DATA (VARIABLE LENGTH)	FCS:0x00000000

IP

VER:4	IHL:5	DSCP:0x00	TL:128

Event List Filters - Visible Events

ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6 ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PI RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP



FastEthernet0

Port Status ☑ O

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Aut

Duplex ● Half Duplex ○ Full Duplex ☑ Aut

MAC Address 00D0.FFE5.960B

IP Configuration

○ DHCP

● Static

IPv4 Address 10.1.20.1

Subnet Mask 255.255.0.0

IPv6 Configuration

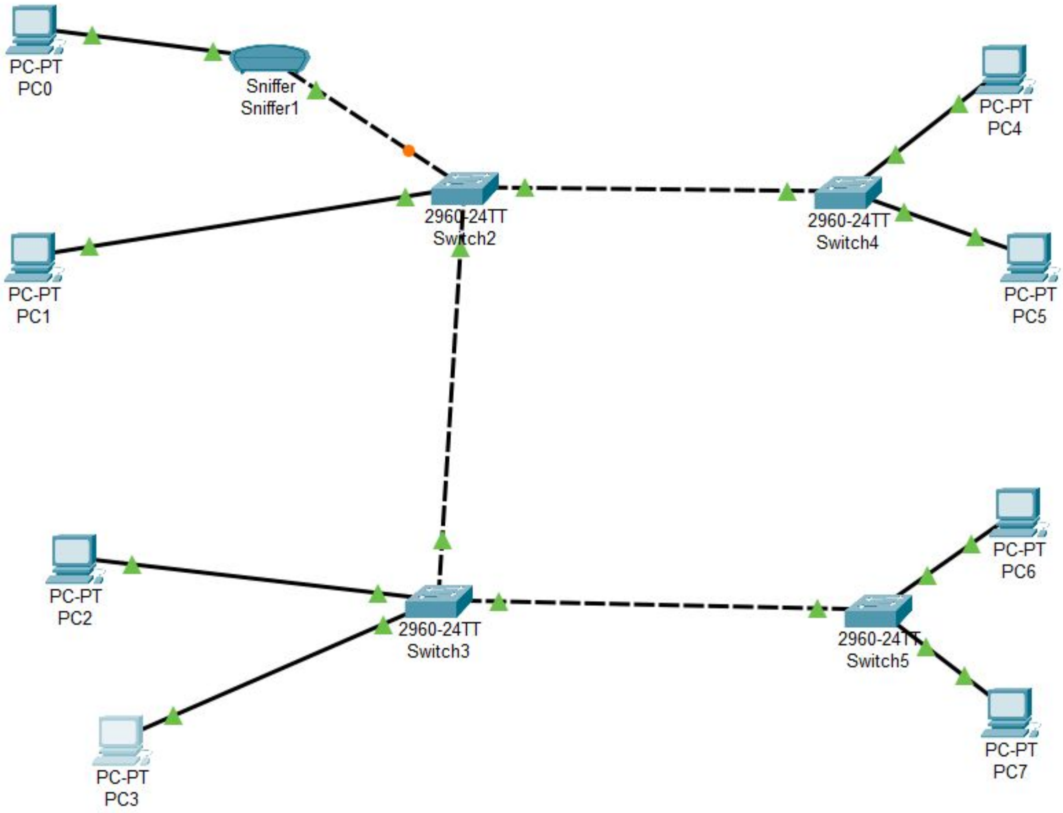
○ Automatic

● Static

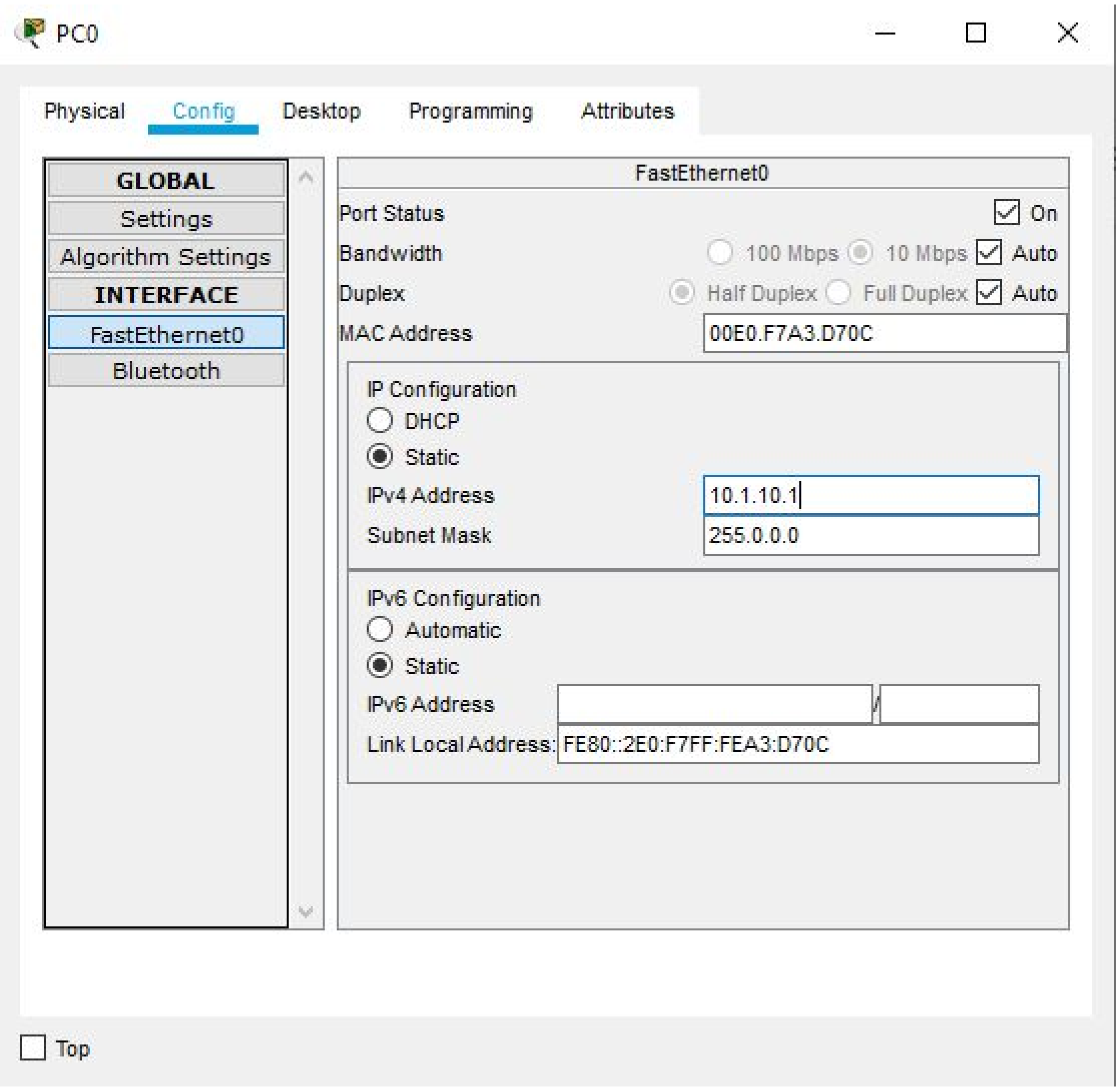
IPv6 Address /

Link Local Address: FE80::2D0:FFFF:FEE5:960B

We pinged PC(4) 10.1.30.1 IP Address from PC(2) 10.1.20.1 IP Address. We also captured our packets from Sniffer1 which is expected in this case . We did this experiment in addition to the previous one because even if there is no sniffer on the route we get the packets on sniffer because hubs distribute the packets to the whole network.



We put one sniffer to the network to catch packets that we sent.(Question answered 11,12)
Green arrow means there is a connection between the devices.(Question answered 14)



PC0

Physical | Config | Desktop | Programming | Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth

FastEthernet0

Port Status ☑ On

Bandwidth ○ 100 Mbps ● 10 Mbps ☑ Auto

Duplex ● Half Duplex ○ Full Duplex ☑ Auto

MAC Address 00E0.F7A3.D70C

IP Configuration
○ DHCP
● Static

IPv4 Address 10.1.10.1

Subnet Mask 255.0.0.0

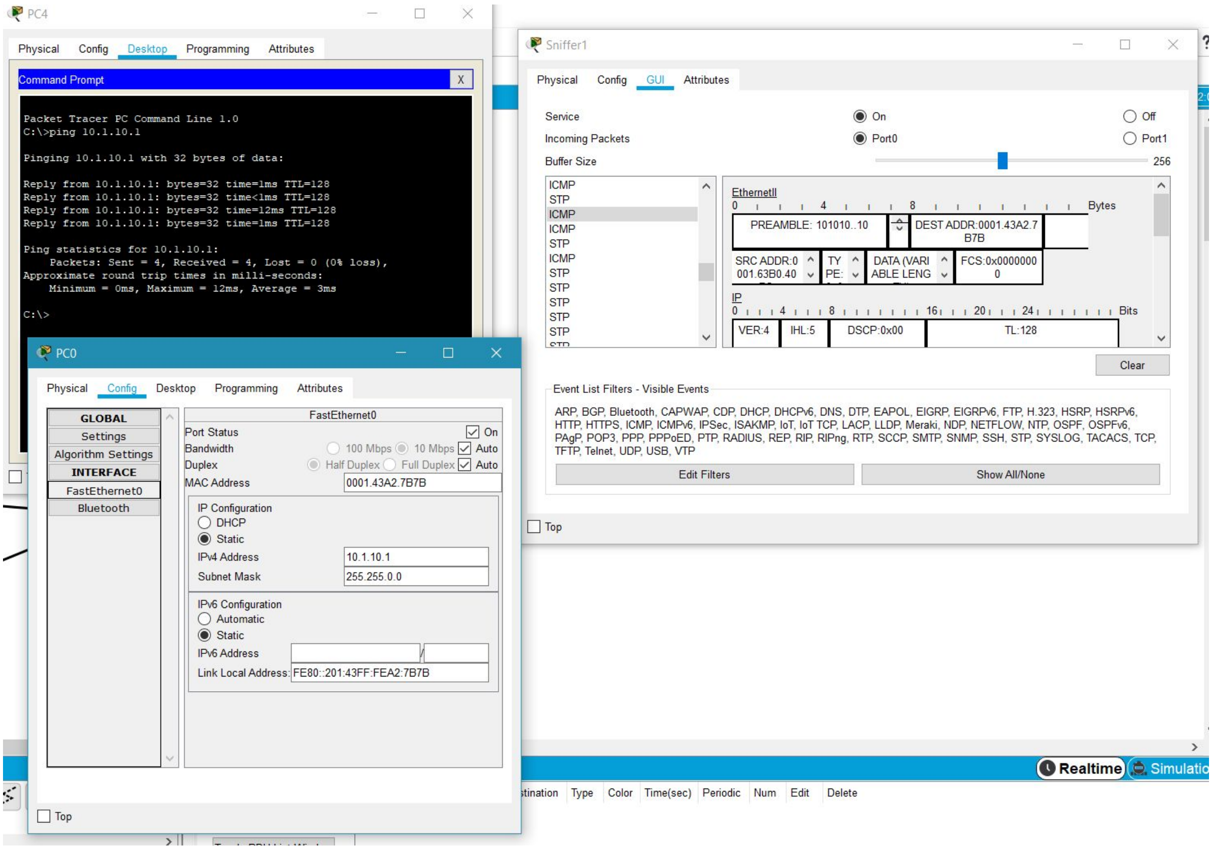
IPv6 Configuration
○ Automatic
● Static

IPv6 Address /

Link Local Address: FE80::2E0:F7FF:FEA3:D70C

□ Top

Our group number is 2. So, our IP address is 10.1.xx.x.



PC4

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.1.10.1

Pinging 10.1.10.1 with 32 bytes of data:

Reply from 10.1.10.1: bytes=32 time=1ms TTL=128
Reply from 10.1.10.1: bytes=32 time<1ms TTL=128
Reply from 10.1.10.1: bytes=32 time=12ms TTL=128
Reply from 10.1.10.1: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>
```

Sniffer1

Service ● On ○ Off

Incoming Packets ● Port0 ○ Port1

Buffer Size 256

ICMP
STP
ICMP
ICMP
STP
ICMP
STP
STP
STP
STP
STP

EthernetII

PREAMBLE: 101010..10 | DEST ADDR:0001.43A2.7B7B | SRC ADDR:0001.63B0.40 | TYPE: | DATA (VARIABLE LENG | FCS:0x00000000

IP

VER:4 | IHL:5 | DSCP:0x00 | TL:128

Event List Filters - Visible Events

ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

PC0

FastEthernet0

Port Status ☑ On

Bandwidth ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0001.43A2.7B7B

IP Configuration

○ DHCP

● Static

IPv4 Address 10.1.10.1

Subnet Mask 255.255.0.0

IPv6 Configuration

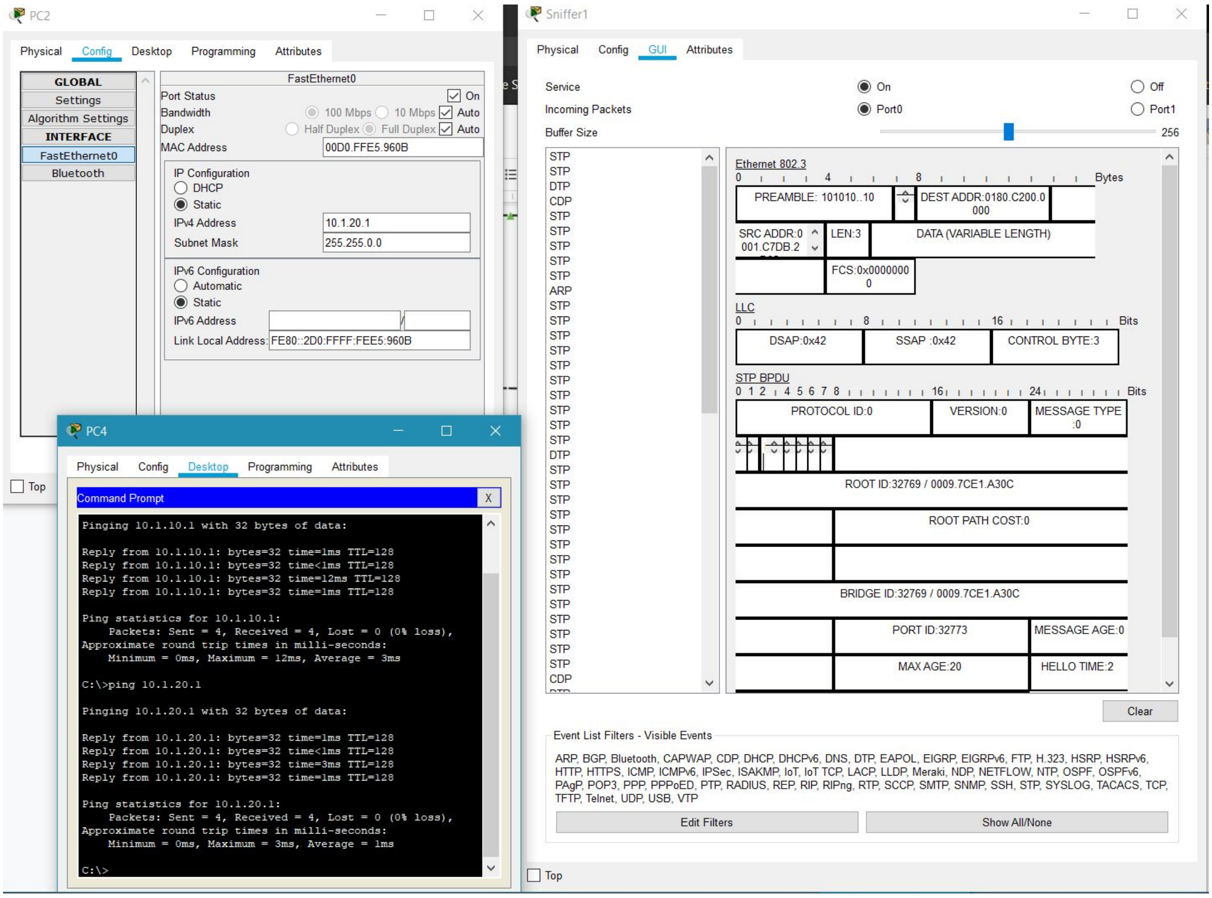
○ Automatic

● Static

IPv6 Address

Link Local Address: FE80::201:43FF:FEA2:7B7B

We pinged PC0(10.1.10.1) from PC4(10.1.30.1). We can see the captured packets on sniffer above which is expected in this case. We also compare the mac addresses on ICMP packages to make sure that pinged packets arrived on correct PC.(Question answered 13,15,16)



PC2

Physical | Config | Desktop | Programming | Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth

FastEthernet0

Port Status ☑ On
Bandwidth ○ 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ○ Full Duplex ☑ Auto
MAC Address 00D0.FFE5.960B

IP Configuration
○ DHCP
● Static
IPv4 Address 10.1.20.1
Subnet Mask 255.255.0.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address /
Link Local Address: FE80::2D0:FFFF:FE05:960B

□ Top

PC4

Physical | Config | Desktop | Programming | Attributes

Command Prompt X

```
Pinging 10.1.10.1 with 32 bytes of data:

Reply from 10.1.10.1: bytes=32 time=1ms TTL=128
Reply from 10.1.10.1: bytes=32 time<1ms TTL=128
Reply from 10.1.10.1: bytes=32 time=12ms TTL=128
Reply from 10.1.10.1: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>ping 10.1.20.1

Pinging 10.1.20.1 with 32 bytes of data:

Reply from 10.1.20.1: bytes=32 time=1ms TTL=128
Reply from 10.1.20.1: bytes=32 time<1ms TTL=128
Reply from 10.1.20.1: bytes=32 time=3ms TTL=128
Reply from 10.1.20.1: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>
```

Sniffer1

Physical | Config | GUI | Attributes

Service ● On ○ Off
Incoming Packets ● Port0 ○ Port1
Buffer Size 256

STP
STP
DTP
CDP
STP
STP
STP
STP
STP
ARP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
DTP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
CDP

Ethernet 802.3
0 4 8 Bytes
PREAMBLE: 101010..10 | DEST ADDR:0180.C200.0000
SRC ADDR:0001.C7DB.2 | LEN:3 | DATA (VARIABLE LENGTH)
FCS:0x00000000

LLC
0 8 16 Bits
DSAP:0x42 | SSAP :0x42 | CONTROL BYTE:3

STP BPDU
0 1 2 4 5 6 7 8 16 24 Bits
PROTOCOL ID:0 | VERSION:0 | MESSAGE TYPE :0
ROOT ID:32769 / 0009.7CE1.A30C
ROOT PATH COST:0
BRIDGE ID:32769 / 0009.7CE1.A30C
PORT ID:32773 | MESSAGE AGE:0
MAX AGE:20 | HELLO TIME:2

Clear

Event List Filters - Visible Events

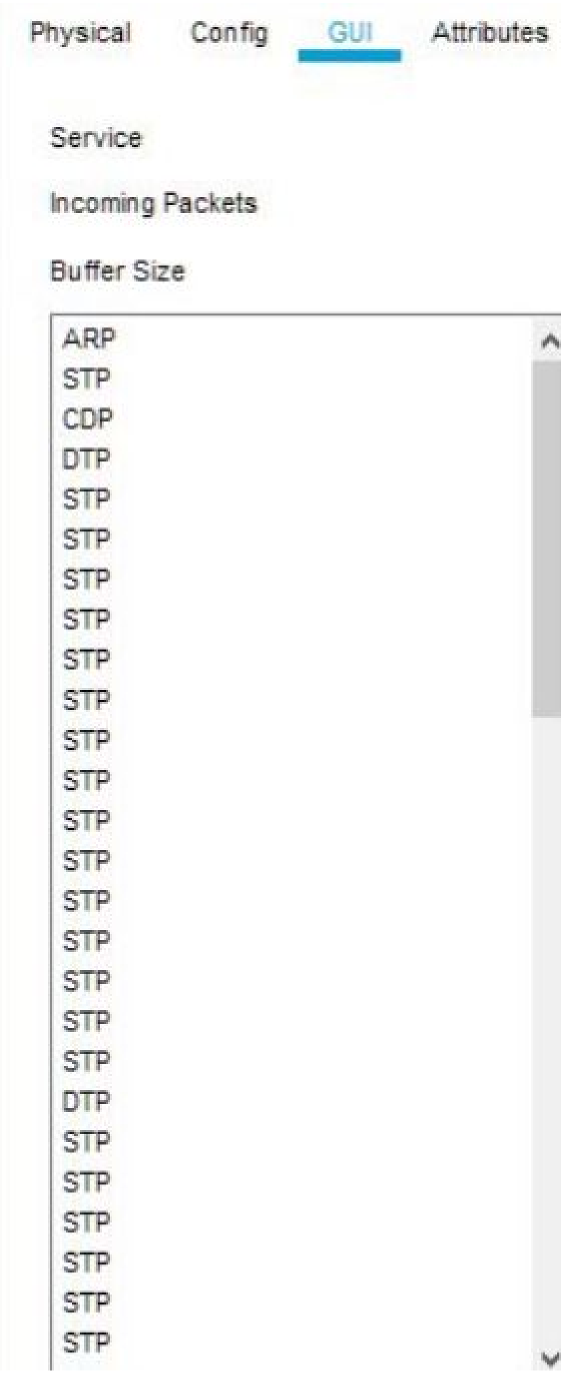
ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None

□ Top

We pinged PC2(10.1.20.1) from PC4(10.1.30.1). We can't see any captured ICMP packets on sniffer because unlike the hubs, switches only distribute the packets to the target host so in this case our target host is PC4 and there is no sniffer on the route.(Our sniffer only captures the packets on the route of PC0).(Question answered18)

Hubs operate on the physical layer, whereas Switches operate on the data link layer.Hubs distribute the packets which they capture to the whole network however switches do not do this. They only send the packets to the targeted client(not the whole network) in our case.(Question answered 19) .



Service

Incoming Packets

Buffer Size

```
ARP
STP
CDP
DTP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
DTP
STP
STP
STP
STP
STP
STP
```

ARP protocol(Address Resolution Protocol) : The first network-level protocol is the Address Resolution Protocol (ARP). ARP dynamically translates Internet addresses into the unique hardware addresses on local area networks.In our experiment, these devices use 48-bit physical addresses (mac address) while sending packages to each other. Physical addresses must be known to be able to exchange data over the network.In our case, the physical addresses of the devices must be known in order to send packets, that’s why we observed this protocol.

STP (Spanning Tree Protocol): It actively monitors all links of the network.It uses an algorithm to find redundant links, known as the STA (spanning-tree algorithm). The STA algorithm first creates a topology database then it finds and disables the redundant links.In this way, STP eliminates the risk of physical redundant links (for example loops) in networks. In our case we have a loop in our network which is constructed from switches.

CDP (Cisco Identification Protocol): CDP is a Cisco proprietary protocol that is used for collecting directly connected neighbor device information like hardware, software, device name details and many more. Each Cisco device stores the messages received from neighbor devices in a table that can be viewed. It is useful in a way that Network Engineers can gather information about neighboring network devices, determining the type of hardware or equipment, software version, active interfaces the device is using (whether physical or VLAN), how they are configured, and other useful information.

DTP (Dynamic Trunking Protocol): Dynamic Trunking Protocol is a Cisco proprietary trunking protocol, which is used to automatically negotiate trunks between Cisco switches. Dynamic Trunking Protocol can be used to negotiate and form trunk connection between Cisco switches dynamically.The main benefit of DTP is to increase traffic on a trunked link.