21BDS0340

Abhinav Dinesh Srivatsa

Information Security and Audit Lab

Task – I

Question 1

Aim: Create a LAN using a hub with 3 nodes.

Tools and Concepts Required:

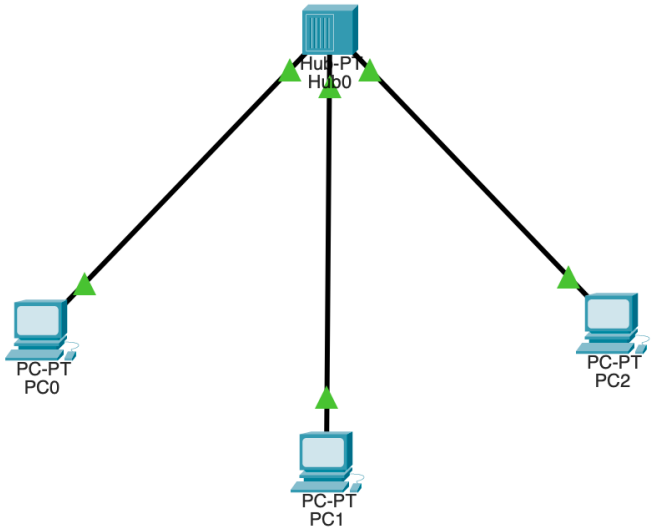
- Cisco Packet Tracer
- Hub
- Personal Computers
- Wiring
- Sniffer

Procedure:

- Create a LAN with a hub
- Understand the packet flow with the ping command
- Introduce a sniffer into the network
- Understand the working of a sniffer

Output:

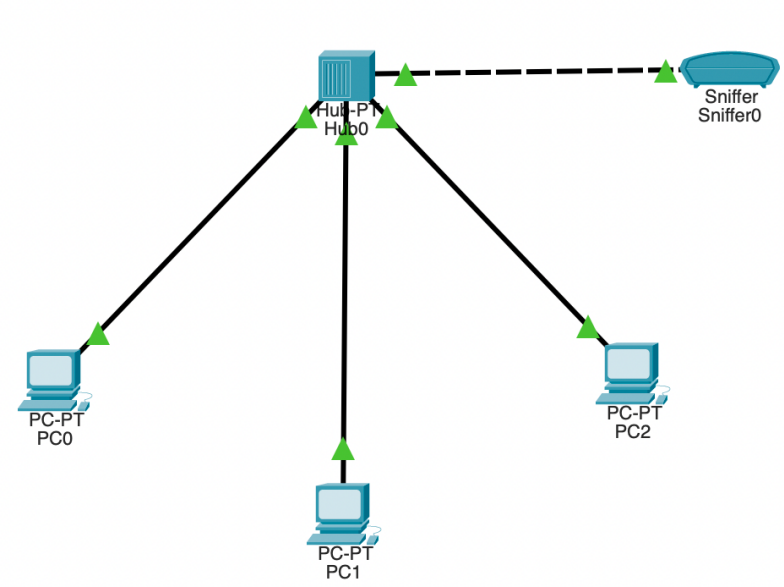
LAN with hub:



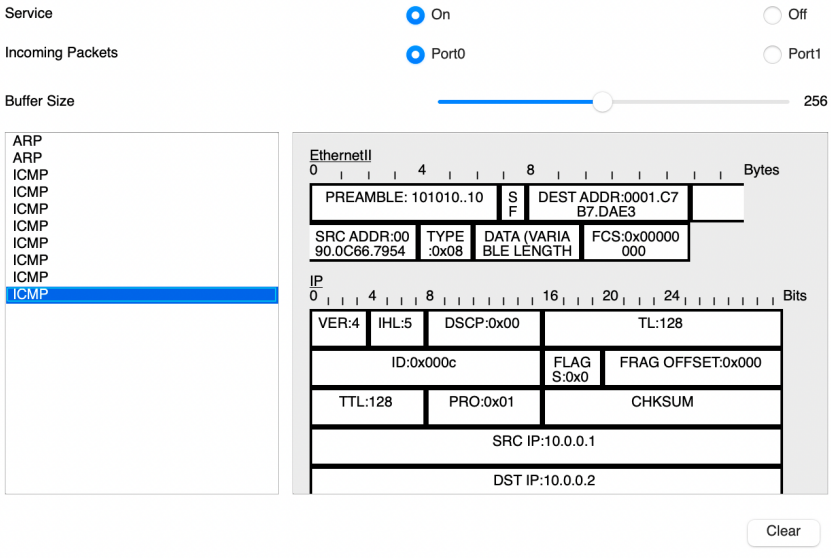
Understand the packet flow with the ping command:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time=1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Introduce a sniffer into the network:



Understand the working of a sniffer:



Security Analysis:

Vulnerabilities	Threats	Attack
Outdated software	Physical access with insider access	Malware infection to hardware by insider access
Weak passwords	Unauthorised access by gaining a password	Denial of service by blocking hub access
Lack of encryption	Data theft by insider attacks	Phishing by insider attack
Direct offline hub access		

Prevention:

- Keeping the nodes and hub in a sperate room for nobody to access directly.
- Encrypt and mandate strong password usage

Result:

This network is extremely secure, but all the nodes can only connect to each other and none of them to the internet. This type of connection is very good for local file storages and broadcasting.

Question 2

Aim: Create a LAN using a switch with 3 nodes.

Tools and Concepts Required:

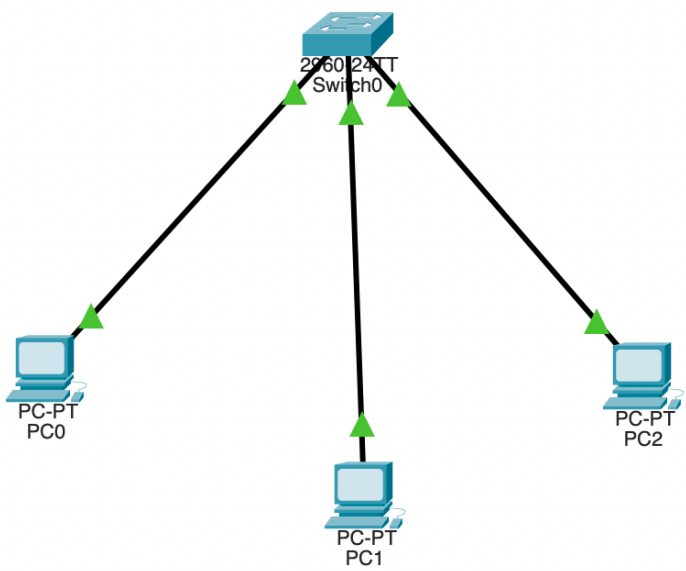
- Cisco Packet Tracer
- Switch
- Personal Computers
- Wiring
- Sniffer

Procedure:

- Create a LAN with a switch
- Understand the packet flow with the ping command
- Introduce a sniffer into the network
- Understand the working of a sniffer

Output:

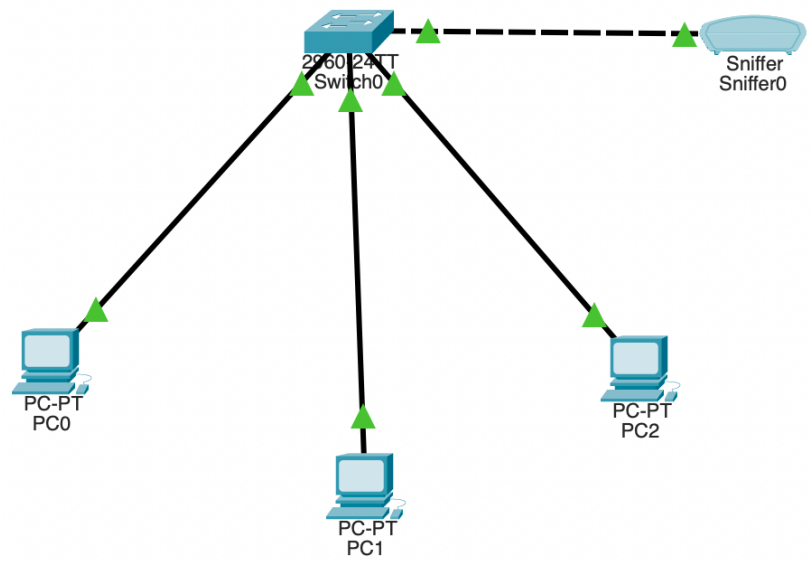
LAN with switch:



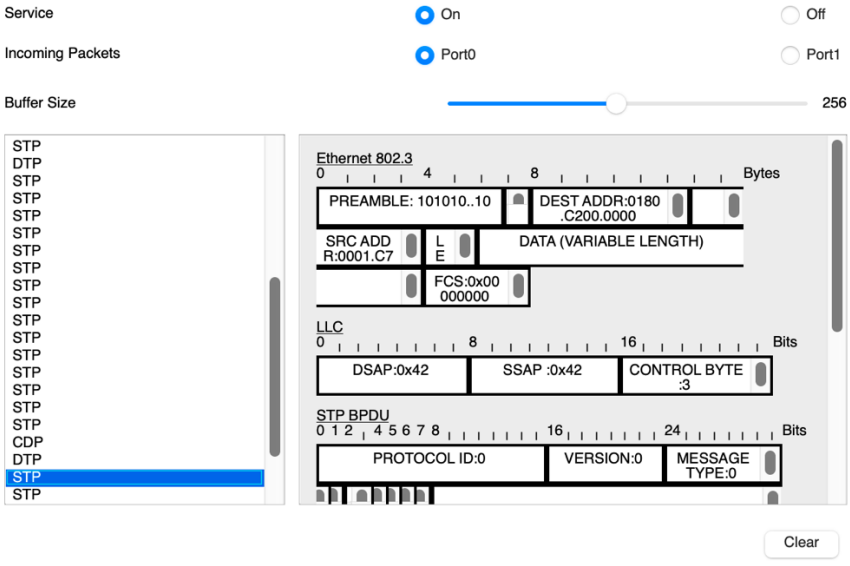
Understand the packet flow with the ping command:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Introduce a sniffer into the network:



Understand the working of a sniffer:



Security Analysis:

The setup will have the exact same security analysis as with the first question (hub instead of switch)

Vulnerabilities	Threats	Attack
Outdated software	Physical access with insider access	Malware infection to hardware by insider access
Weak passwords	Unauthorised access by gaining a password	Denial of service by blocking hub access
Lack of encryption	Data theft by insider attacks	Phishing by insider attack
Direct offline hub access		

Prevention:

- Keeping the nodes and hub in a sperate room for nobody to access directly.
- Encrypt and mandate strong password usage

Result:

This network is extremely secure, but all the nodes can only connect to each other and none of them to the internet. This type of connection is very good for local file storages or for fast computer communication.