

KLE Society's  
KLE Technological University



## **COMPUTER NETWORKS - 2**

Site Visit Report

# **SURVEY ON SDM DENTAL COLLEGE CAMPUS NETWORK**

### **TEAM - A23**

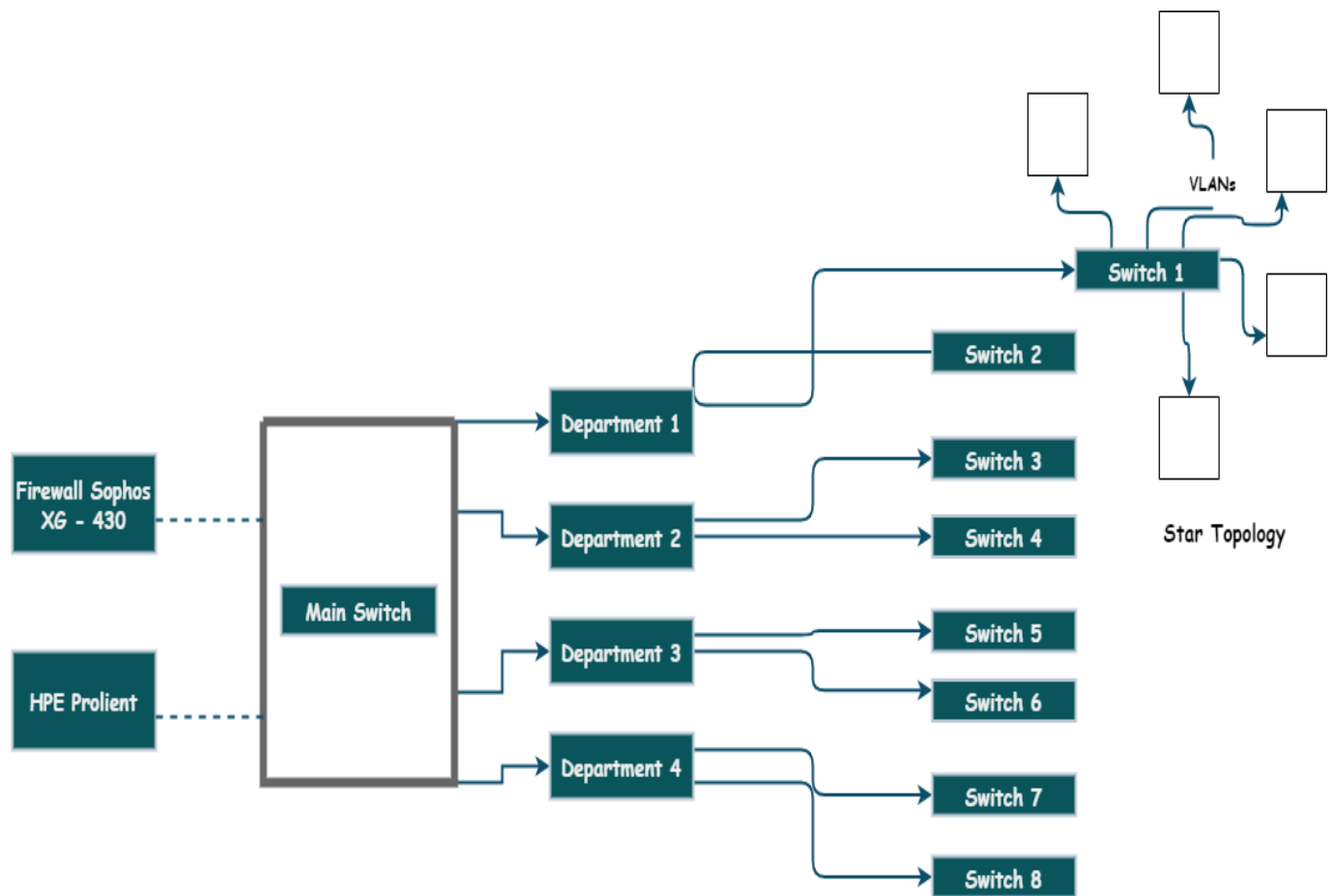
<b>Shreeya Goggi</b>	<b>01fe19bcs045</b>
<b>Rashmi Kiragi</b>	<b>01fe19bcs057</b>
<b>Renuka Talwar</b>	<b>01fe19bcs068</b>
<b>Aishwarya C</b>	<b>01fe19bcs070</b>
<b>Sahana Bhasme</b>	<b>01fe19bcs072</b>

### **COURSE TEACHER**

**Dr. Vijayalaxmi**

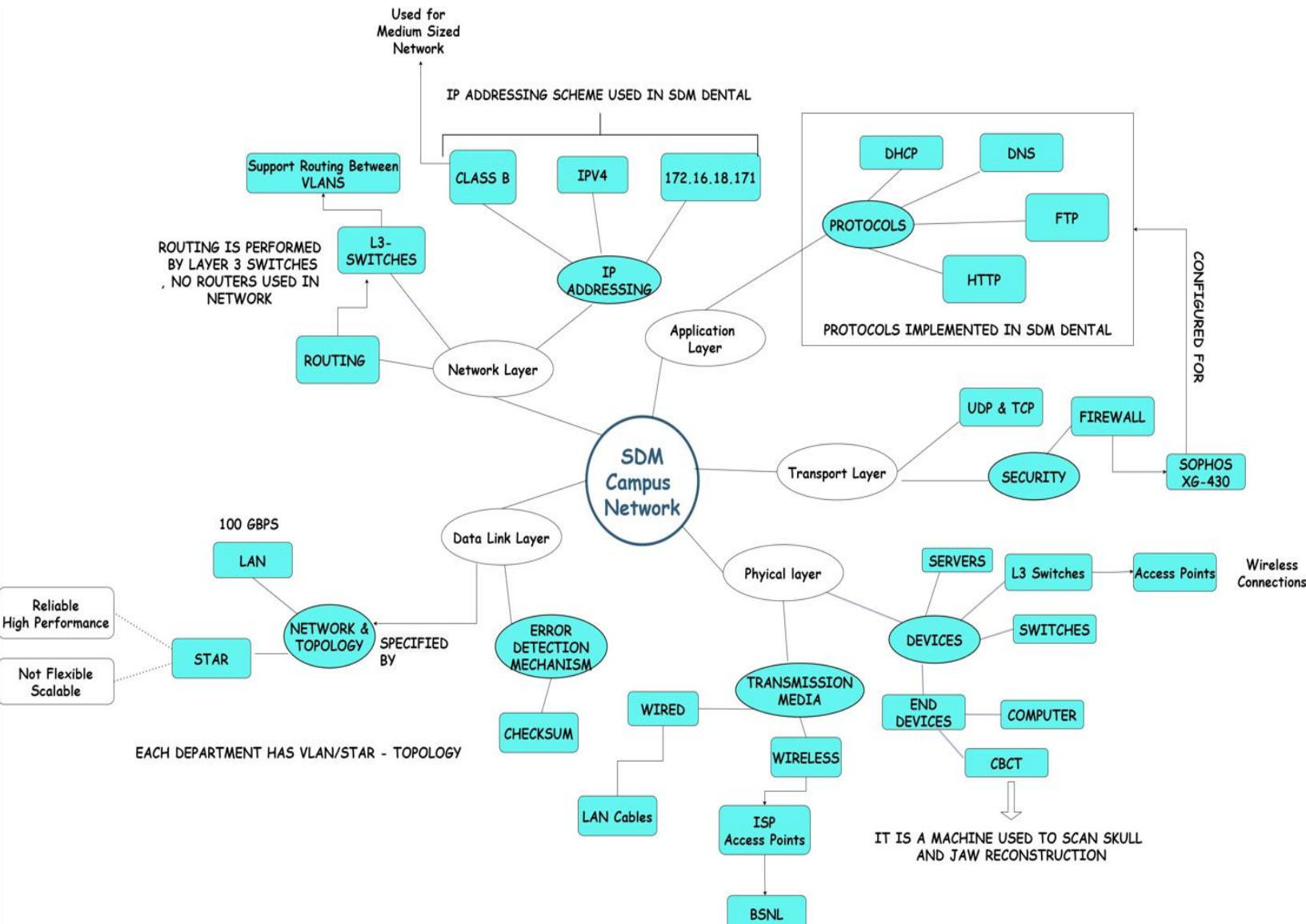
**SCHOOL OF COMPUTER SCIENCE & ENGINEERING  
HUBLI-580 031 (India)  
Academic year 2021-22**

# NETWORK ARCHITECTURE



The SDM Dental college network topology has four departments each department consisting two wings. They have used SOPHOS XG – 430 firewall for securing against cyber-attacks. There is a HPE ProLiant rack server for 3D printing. The Firewall and rack servers are connected to main switch, to which different departments are connected. Each department has one core switch to which different end devices are connected. It follows the star topology. And the SDM Dental is itself a subnet hence it has no subnetworks within it.

# MINDMAP



## **GAPS IDENTIFIED**

- The current topology used is STAR Topology which requires additional equipment and if a switch or a hub fails all devices connected to that network will have no network.
- There is no private wireless network. They are dependent on ISP to access Wi-Fi facilities which is not cost effective.
- In case of any network failure they are dependent on ISP to identify network faults and restoration.
- There is no Wi-Fi facility at the hostel. Students have to come to the campus to access Wi-Fi facilities in allotted time.
- Do not have any fault detection software.
- Since main servers are located in Ujire and sub servers are in SDM Dental the network is managed from Ujire, in case of any network failure they are dependent on Ujire for network restoration.
- The Application level protocols are configured in Firewall which can result in a single point of failure.

## PROPOSED SOLUTION

- Preferring Hybrid topology over Star topology.

Disadvantages of star topology:

- It is expensive to install as this type of network uses the most cable (network cable is expensive)
- Extra hardware is required (hubs or switches) which adds to cost.
- If a hub or switch fails, all the devices connected to it will have no network connection.

Advantages of hybrid topology:

- It is extremely flexible. It is very reliable. It is easily scalable as Hybrid networks are built in a fashion which enables for easy integration of new hardware components. Error detecting and troubleshooting is easy.

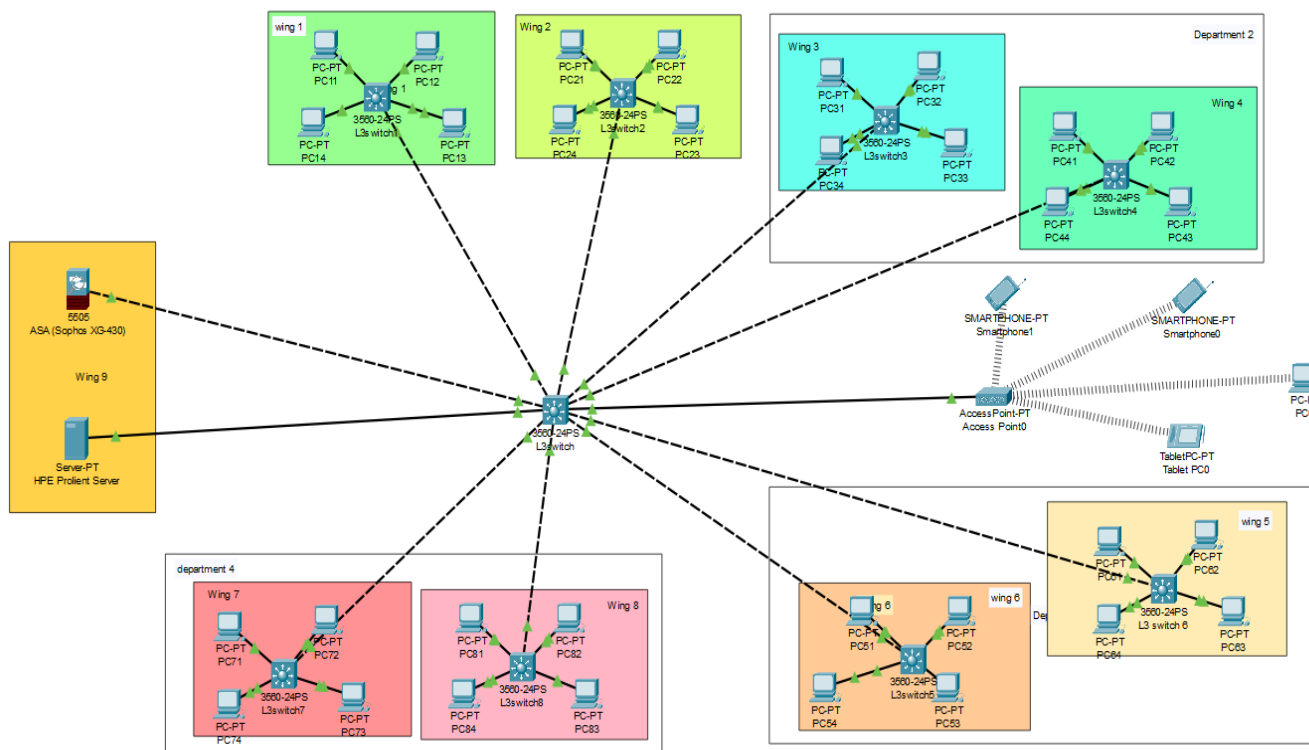
- To design a private wireless campus network, instead of depending completely on ISP hotspots.

Advantages:

- Easy to manage in case of network faults/failure, need not be dependent on outsiders
- Service can be provided in less time.
- Can be extended to hostels.

- To maintain separate servers for http and ftp service.
- Instead of Using access points Wifi routers can be used which provide better bandwidth, speed and both wireless and wired devices can be connected.

# DETAILS OF ARCHITECTURE SIMULATED IN CISCO PACKET TRACER

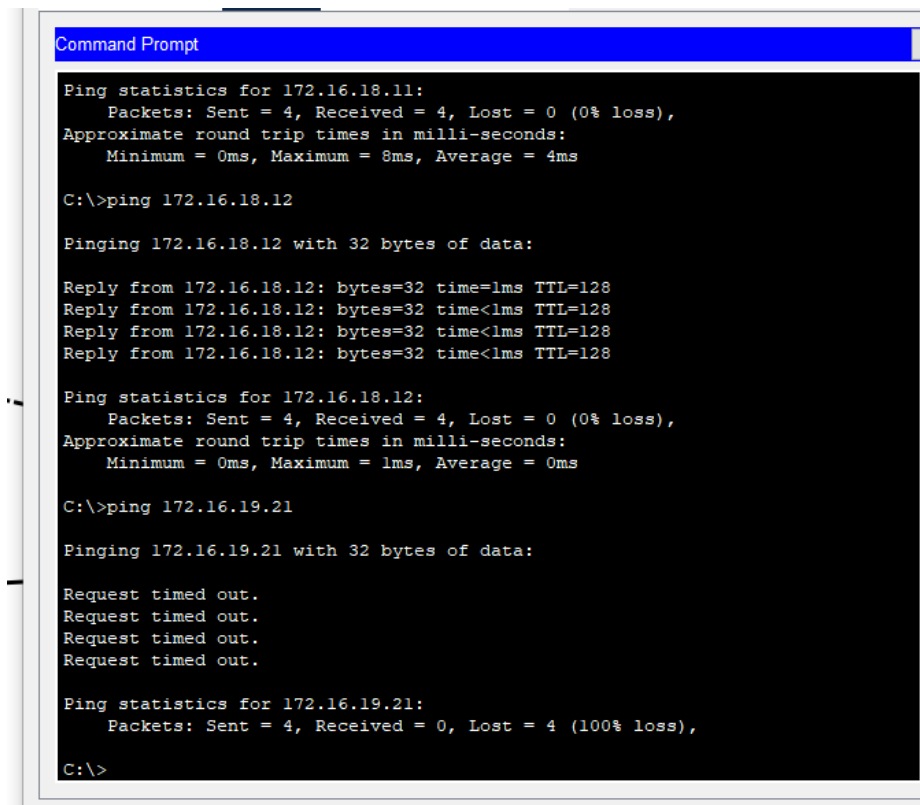


## IP SCHEME AND CALCULATIONS.

- They have used class B IP addressing.
- Class B IP address range 128-191.
- The first 16 bits represent network id and remaining 16 bits represent hostid.
- The first 16 bits are all 1s, hence the subnet mask is 255.255.0.0
- Class B has  $2^{16}$  hosts i.e., 65,534 devices can be in network which is suitable for smaller organizations.

## SIMULATION OUTPUT AND RESULTS OF EXISTING NETWORK

### INTRA VLAN



```
Command Prompt

Ping statistics for 172.16.18.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 4ms

C:\>ping 172.16.18.12

Pinging 172.16.18.12 with 32 bytes of data:

Reply from 172.16.18.12: bytes=32 time=1ms TTL=128
Reply from 172.16.18.12: bytes=32 time<1ms TTL=128
Reply from 172.16.18.12: bytes=32 time<1ms TTL=128
Reply from 172.16.18.12: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.18.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 172.16.19.21

Pinging 172.16.19.21 with 32 bytes of data:

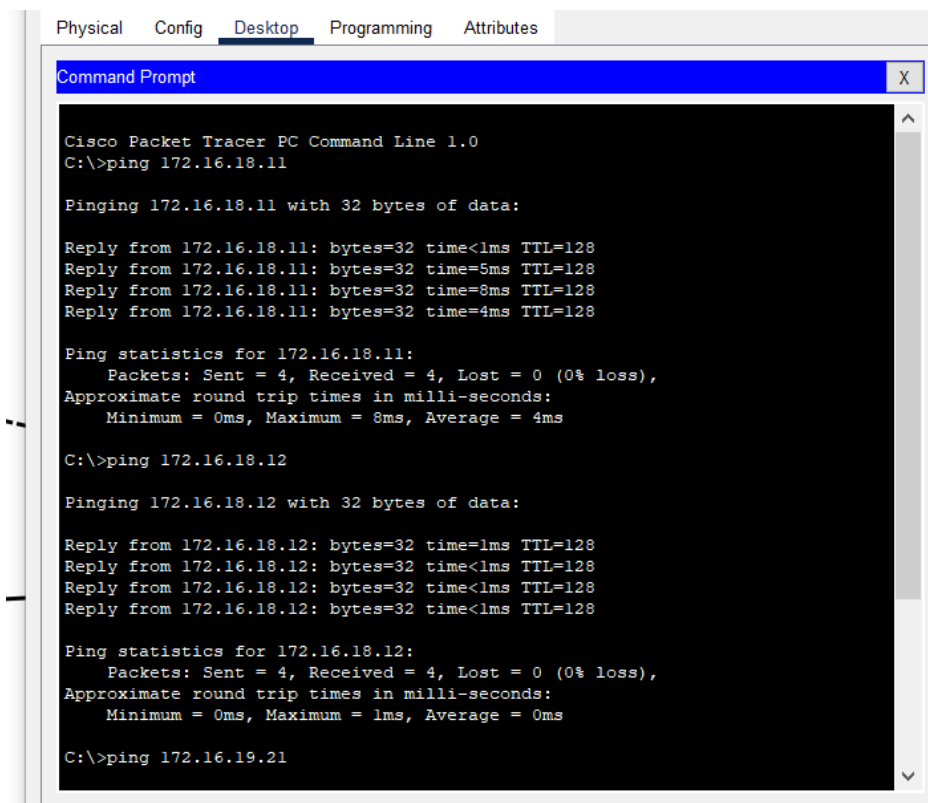
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.19.21:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

## PING BETWEEN DEVICES.



The screenshot shows the Cisco Packet Tracer PC Command Line 1.0 interface. The 'Desktop' tab is selected. The command prompt displays the results of three ping commands. The first ping is to 172.16.18.11, showing four successful replies with times of 1ms, 5ms, 8ms, and 4ms, and statistics of 4 sent, 4 received, 0 lost, and an average round trip time of 4ms. The second ping is to 172.16.18.12, showing four successful replies with times of 1ms, 1ms, 1ms, and 1ms, and statistics of 4 sent, 4 received, 0 lost, and an average round trip time of 0ms. The third ping is to 172.16.19.21, which is partially visible at the bottom of the screen.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.18.11

Pinging 172.16.18.11 with 32 bytes of data:

Reply from 172.16.18.11: bytes=32 time<1ms TTL=128
Reply from 172.16.18.11: bytes=32 time=5ms TTL=128
Reply from 172.16.18.11: bytes=32 time=8ms TTL=128
Reply from 172.16.18.11: bytes=32 time=4ms TTL=128

Ping statistics for 172.16.18.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 4ms

C:\>ping 172.16.18.12

Pinging 172.16.18.12 with 32 bytes of data:

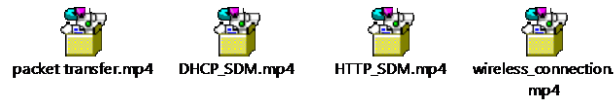
Reply from 172.16.18.12: bytes=32 time=1ms TTL=128
Reply from 172.16.18.12: bytes=32 time<1ms TTL=128
Reply from 172.16.18.12: bytes=32 time<1ms TTL=128
Reply from 172.16.18.12: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.18.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

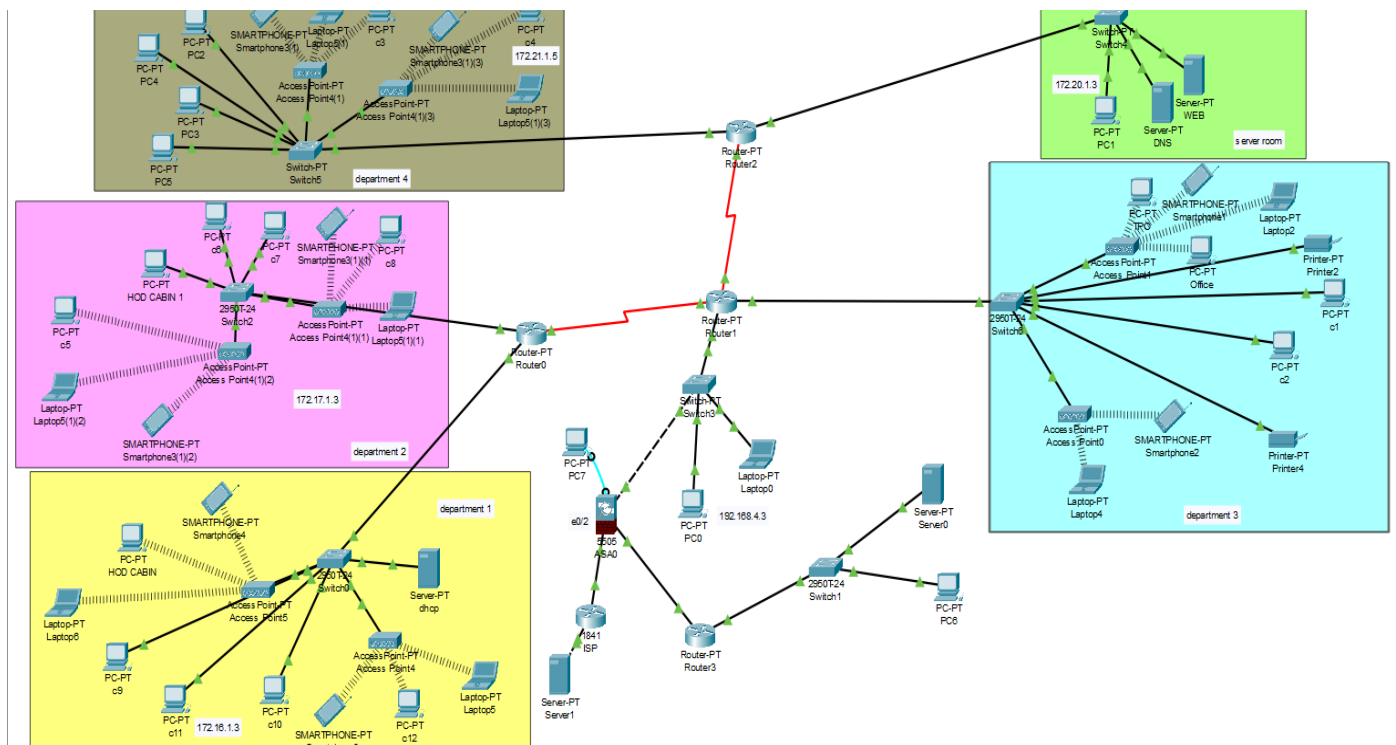
C:\>ping 172.16.19.21
```



# SIMULATION CLIPS



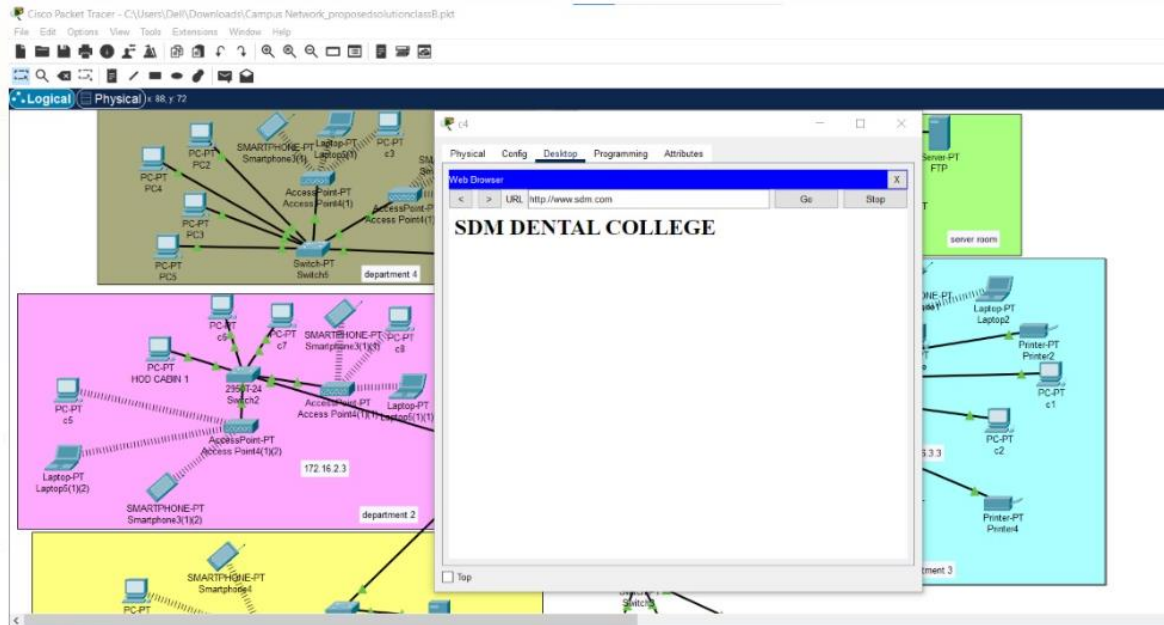
## Proposed Solution



In the proposed solution we have replaced L3 switches with routers which are serially connected to each other. We have removed the wings. Each department has one switch to which end devices are connected thus achieved hybrid topology. HTTP and DHCP are configured in different servers hence there is no single point failure.

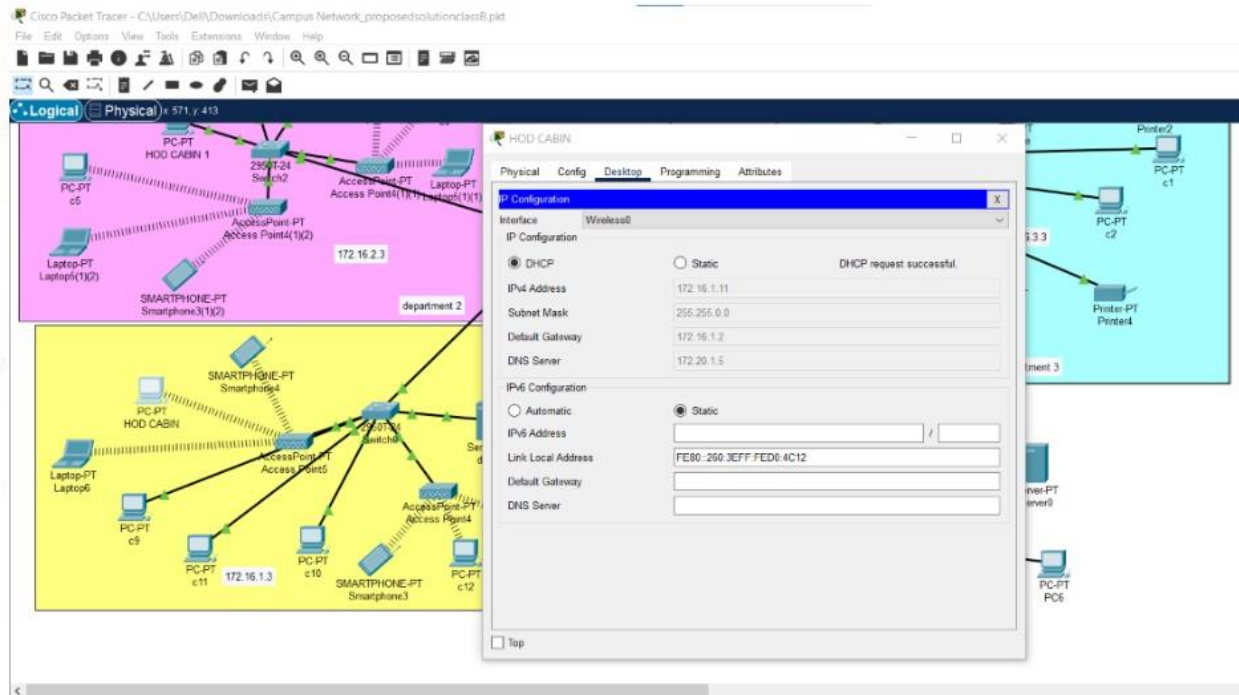
## SIMULATION OUTPUT AND RESULTS OF PROPOSED NETEWORK

HTTP.



Separate HTTP is enabled. The domain name along with IP address is configured in DNS.

DHCP.



Separate DHCP server is configured which assigns IP address dynamically to all the devices in the network.

## PERFORMANCE OF THE PROPOSED ARCHITECTURE.

- The proposed architecture has class B IP schema.
- Routers used to connect to other networks.
- Sophos firewall has set such that it blocks outside cyber-attacks.
- Configured separate servers for HTTP, DHCP, DNS.

# **COMPARISON BETWEEN EXISTING ARCHITECTURE AND PROPOSED ARCHITECTURE.**

- The existing architecture has L3 switches which is replaced by router as router can take a routing decision much faster than a switch. It provides only port security. It provides security measures to protect the network from security threats.
- Lack of WAN functionality is another major disadvantage with layer 3 switches. This means we can't do away with routers completely and we will need both routers and layer 3 switches for routing traffic within and outside the organization.
- In the existing architecture the SOPHOS firewall maintains all the Application layer protocols like HTTP, DNS, DHCP, SMTP, FTP which leads to single point failure. So, in the proposed architecture we have used separate servers for different applications.
- The advantages of a private network technology are:
  1. Better control
  2. Increased security
  3. No monthly fees
  4. More customizable
  5. Proven technology
  6. Network availability
- The disadvantages of a public network technology are:
  1. Coverage limitations
  2. Longevity
  3. Low customization
  4. Lower security
  5. Shared bandwidth
  6. Service fees
  7. No control or maintenance

# LEARNINGS FROM THE SURVEY

- Understanding the working of network in real time.
- Correlating the theoretical problems to real time applications.
- Understanding how to design a private network.
- Understanding how firewall works.
- Understanding the working of various network devices.
- Understanding the difference between L3 switch and router.
- Understanding the IP schema.

# LIMITATIONS

- Unable to configure FTP and HTTP using firewall due to the limitation of cisco packet tracer.
- Unable to develop a network fault detection application which could not be deployed using cisco packet tracer.

# CONCLUSIONS

In this survey, the various concepts are being discussed which were used in SDM Dental college the network architecture, the topology used and its advantages and disadvantages and what steps that can be taken to improve their network. The proposed methodology was to use a hybrid topology which is better topology and no dependency as compared to the star topology and instead of ISP Wi-Fi routers can be used, to connect both wireless and wired devices and also they provide high bandwidth and speed. They have configured application protocols like DHCP, Http in the SOPHOS firewall which can result in single point of failure. Through the survey, it can be concluded that using ISP every time for Wi-Fi access and fault tolerance.

# REFERENCES

- [1] [sophos-xg-series-hardware-br.pdf](#)