

CAMPUS NETWORK DESIGN

A PROJECT REPORT

Submitted by

SHAHBAZ SYED	[RA1811003010280]
ANOUSHKA HALDER	[RA1811003010283]
RAHUL DIT	[RA1811003010288]
ADYASHA PATTANAIK	[RA1811003010293]

Under the guidance of

Ms. S. POORNIMA

(Associate Professor, Department of Computer Science & Engineering)

in partial fulfilment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

of

FACULTY OF ENGINEERING AND TECHNOLOGY



S.R.M. Nagar, Kattankulathur, Kancheepuram District

DECEMBER 2020

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this project report titled “**CAMPUS NETWORK DESIGN**” is the bonafide work of “**SHAHBAZ SYED [RA1811003010280]**”, “**ANOUSHKA HALDER [RA1811003010283]**”, “**RAHUL DIT [RA1811003010288]**” and “**ADYASHA PATTANAIK [RA1811003010293]**” who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE

Ms. S. POORNIMA

GUIDE

Associate Professor,

Dept. of Computer Science & Engineering.

ABSTRACT

With the innovation and diffusion of new technology such as Universal computing, Enterprise mobility, E-commerce and Cloud computing, presence of Campus Network becomes more and more important. A university network has a number of uses, such as teaching, learning, research, management, e-library, result publishing and connection with the external users. The campus network system is a very large and complicated system. It is not only for modern teaching, integrated information management, but also to provide a variety of application services, so that information can be timely and accurate delivery. Thus, the construction of campus network is the inevitable choice of the development of information network.

This report introduces the goal of campus network design and the selection of network technology, network equipment selection and so on, and gives the concrete network topology diagram through the example of the campus network design and construction process. We have taken various topologies and designs into account and have reached a conclusion that is best suitable for our scenario. A hierarchical architecture of the campus network is configured with different types of security implementations for ensuring the quality of service. In this project, a tested and secure network design is proposed based on the practical requirements and this proposed network infrastructure is realizable with adaptable infrastructure.

TABLE OF CONTENTS

ABSTRACT	iii
1 OBJECTIVE	1
2 INTRODUCTION.....	2
3 PROJECT SCOPE	4
4 CAMPUS DIAGRAM	4
5 NETWORK REQUIREMENT ANALYSIS	5
6 NETWORK DIAGRAM WITH COMPONENTS	7
7 NETWORK AND SYSTEM INTEGRATION	8
7.1 CAMPUS NETWORK DESIGN MODELS	8
7.2 TOPOLOGY	11
8 IP NETWORK DESIGN GUIDELINES	15
8.1 IP SCHEME.....	17
8.2 IP ADDRESS MANAGEMENT.....	18
9 FEATURES AND SERVICES	20
9.1 WIRELESS ACCESS.....	20
9.2 SSH (SECURE SHELL).....	23
10 BILL OF MATERIAL	24
11 IMPLEMENTATION	29
11.1 IP CONFIGURATION	29
11.2 SETTING UP WIRELESS ACCESS POINTS	32
11.3 SSH IMPLEMENTAION.....	34
12 CONCLUSION	37
13 REFERENCE	38

1 OBJECTIVE

Development and inter-school, static, resource sharing, dynamic information release, distance learning and collaborative work stage, the development of school education and modernization, are all results of a strong and effective Campus Network. The network also provides an effective way for schools' managers and teachers to acquire resources and work together. Thus it is essential to build a secure and reliable campus network.

Our objectives are:

- i. To design a network with the most suitable topology for our needs.
- ii. The design should be reliable and cost effective.
- iii. Design an IP scheme that is simple and easy to manage.
- iv. The IP addressing scheme should improve the efficiency of the entire network through summarization and other techniques.
- v. Provide a secure wireless network for students and faculty to access the campus network and the Internet.
- vi. Provide security to protect the Internet connection and internal network from intruders.
- vii. Provide a network that can scale to support future expanded usage of multimedia applications.
- viii. To ensure a connection that provides high bandwidth that satisfies the need of everyone.
- ix. To provide a connection with least response time, possibly $1/10^{\text{th}}$ of a second for the interactive applications.
- x. Make sure that only authorized administrators can configure hardware remotely.

2 INTRODUCTION

A campus network is an autonomous network under the control of a university which is within a local geographical place. Present educational institutions pay more attention to IT to improve their students' learning experience. Architects of campus can achieve this if IT managers hold on to the fundamental principles addressed in this reference architecture, namely LAN or WAN connectivity design considerations, security, and centralized management. The network infrastructure design has become a critical part for some IT organizations in recent years. An important network design consideration for today's networks is creating the potential to support future expansion in a reliable, scalable and secure manner. This requires the designer to define the unique situation, particularly the current technology, application, and data architecture.

The physical network infrastructure is required for a contemporary university network. University Management and IT manager may know exactly what kind of network they want to set up, upcoming plans, and expected growths. Contingencies for future area, power, and other resource must be part of the physical plan of a university.

It is essential to build a network that can be scalable in the future. It starts with selecting a design and topology. Hardware is expensive. So the design that is built now may continue for the next few decades. Equipment should be used in line with international standards of systems and products to ensure that the system has a long vitality and scalability to meet future requirements of the system upgrade.

Reliability and high performance networks must be reliable, including network-level reliability such as routing, switching aggregation, link redundancy, and load balancing. The network must be of sufficient performance to meet the needs of the students and faculty. Thus it is recommended to use industry standard high performance equipment.

This generation of technological advancement have introduced us to wireless networks that is comparable to LANs in terms of responsiveness and speed. Compared with local area networks, wireless local area networks offer advantages at different places. One of the advantage of a wireless local area network is that if there is coverage of WLAN, users can move anywhere they want with their devices and transmit data at the same time. Other

advantages include easy installation, effective expansion, flexibility and cost savings.

Easy to manage, easy maintenance as the campus backbone network system is large, rich and complex application, the need for network management system has good manageability, network management system with monitoring, fault diagnosis, fault isolation, filtering settings and other functions to facilitate the management of the system and maintain. This makes sure that any fault in the system can be easily identified and fixed. These diagnostic systems need to be available only

This leads to the issue of security. New security threats keep emerging on a daily basis. We need to protect our system from various viruses and ransomwares, etc. To do this, we need to have a firewall and an encryption system for the entire network. While encryption system may slow down the network but it is necessary.

While we start building and designing this network for a small pool of people we need to think about the upgradability. Our systems need to be modular so that it can easily upgraded to newer technologies.

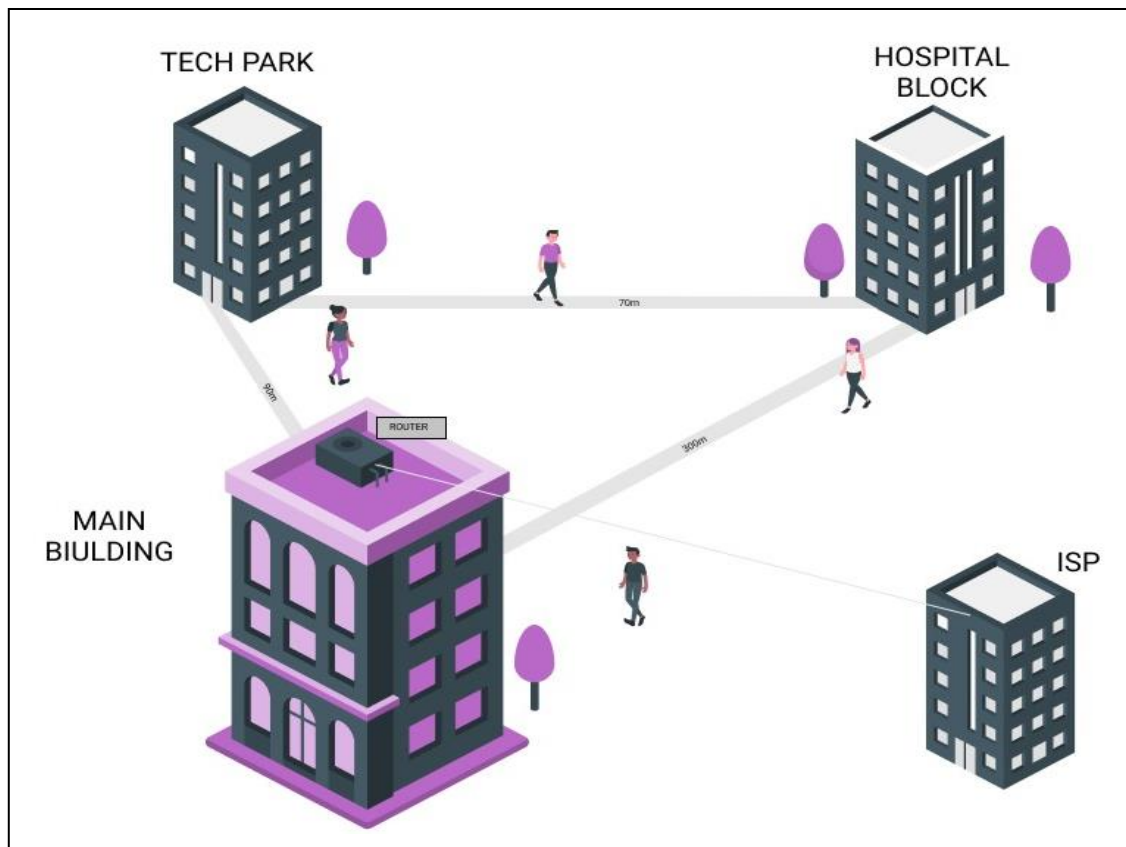
3 PROJECT SCOPE

The scope of our project is designing a network for a campus that consists of 3 buildings. The features are:

- A high speed cable internet connection is available in the main building.
- The main building consists of 20 users.
- The Tech Park building is 90 meters from the main building and has 20 users.
- The Hospital block is 300 meters from the main building and has 10 users.
- Internet needs to be shared from the main building to the other building with an appropriate topology design.
- Every building should have access to wireless connectivity from the lobby.
- The IP addressing plan needs to be centrally organized and manageable.
- Security has to be implemented to prevent attacks.
- A cost effective yet reliable and high speed connection needs to be built.

Thus we need to design a network that ensures a proper connection to the 50 users in 3 buildings.

4 CAMPUS DIAGRAM



5 NETWORK REQUIREMENT ANALYSIS

Some of the requirements to build our campus network are:

- The network should reliably deliver applications and provide reasonable response times from any host to any host.
- The network should be secure. It should protect the data that is transmitted over it and data stored on the devices that connect to it.
- The network should stay up all the time, even in the event of failed links, equipment failure, and overloaded conditions.
- The network should be easy to modify to adapt to network growth and general business changes.

To implement these the hardware and the quantity that's required are:

i. Routers

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node. A router which supports high speed internet connection, with the appropriate interface is required.

Routers form the core layer, also referred to as the network backbone. The core should be highly available and redundant. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly.

Features include:

- Scaling by using faster, and not more, equipment
- Providing reliability and fault tolerance
- Avoiding CPU-intensive packet manipulation caused by security, inspection, quality of service (QoS) classification, or other processes.
- Providing high-speed routing

ii. Switches

Switches are devices used on the network to transmit and receive data from one device to another or to many devices depending on the message intended. A switch provides the full bandwidth of the network to each port, thereby reducing collisions on the network. Switches also perform functions from the Data Link Layer (Layer 2 on the OSI [Open Systems Interconnection] Model).

Switches allow different nodes (a network connection point, typically a computer) of a network to communicate directly with one another in a smooth and efficient manner.

Switches form the distribution layer.

The distribution layer can provide

- Aggregation of LAN or WAN links.
- Policy-based security in the form of access control lists (ACLs) and filtering.
- Redundancy and load balancing.
- A boundary for route aggregation and summarization configured on interfaces toward the core layer.

iii. Wireless Access Point

It works in the access layer and provide connectivity to the end users.

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

The access layer serves a number of functions, including

- Layer 2 switching
- High availability
- Port security
- QoS classification and marking and trust boundaries
- Address Resolution Protocol (ARP) inspection
- Spanning tree

iv. Nodes

Any system or device connected to a network is also called a node. The end devices in the access layer connect to the switches or WLAN access point to connect to the internet.

v. Cables

Cables such as fiber optic and cat6 are the medium that connects these hardware devices. These connect the layers in between.

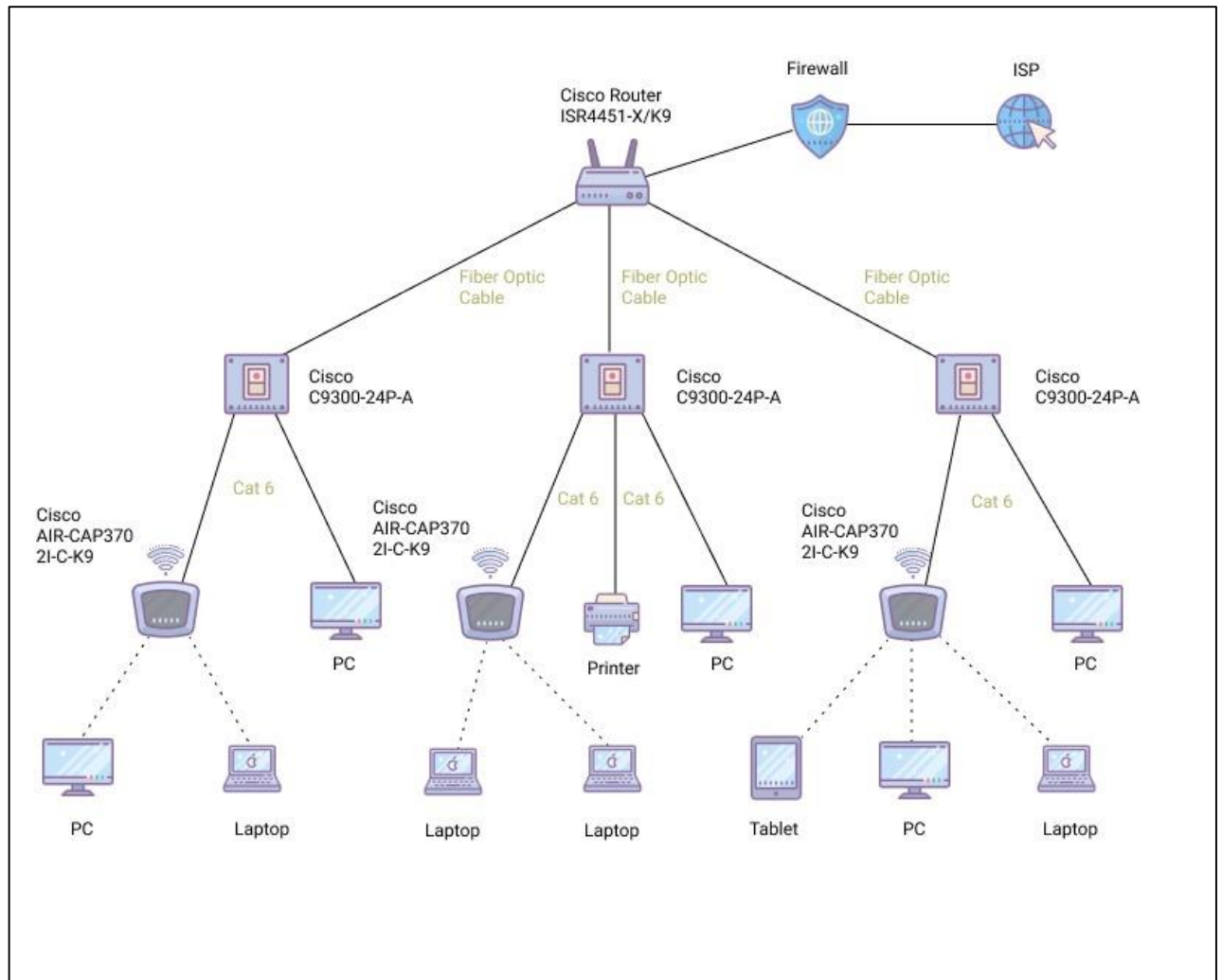
Fiber Optic

A fiber optic cable contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking. Compared to wired cables, fiber optic cables provide higher bandwidth and transmit data over longer distances.

Cat 6

Category 6 cable (Cat 6), is a standardized twisted pair cable for Ethernet and other network physical layers that is backward compatible with the Category 5/5e. The cable standard specifies performance of up to 250 MHz

6 NETWORK DIAGRAM WITH COMPONENTS



7 NETWORK AND SYSTEM INTEGRATION

7.1 CAMPUS NETWORK DESIGN MODELS

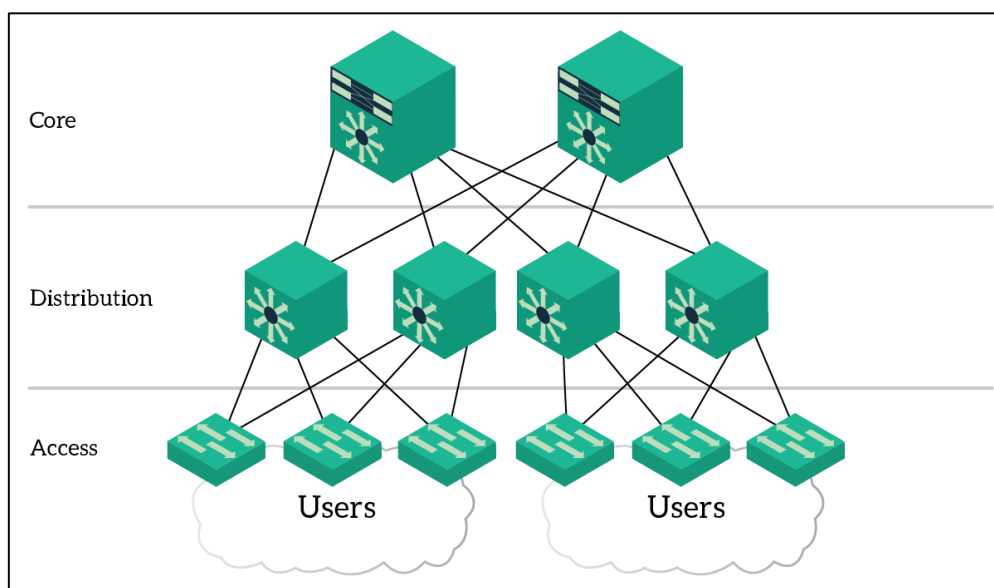
A campus network generally provides access to network communication services and resources to end users and devices that are spread over a single geographic location. It may be a single building or a group of buildings spread over an extended geographic area. Normally, the enterprise that owns the campus network usually owns the physical wires deployed in the campus.

Therefore, network designers typically tend to design the campus portion of the enterprise network to be optimized for the fastest functional architecture that runs on high speed physical infrastructure (1/10/40/100 Gbps). Moreover, enterprises can also have more than one campus block within the same geographic location, depending on the number of users within the location, business goals, and business nature. When possible, the design of modern converged enterprise campus networks should leverage the following common set of engineering and architectural principles:

- ❖ Hierarchy
- ❖ Modularity
- ❖ Resiliency

Hierarchical design models

The hierarchical network design model breaks the complex flat network into multiple smaller and more manageable networks. Each level or tier in the hierarchy is focused on a specific set of roles. This design approach offers network designers a high degree of flexibility to optimize and select the right network hardware, software, and features to perform specific roles for the different network layers.



A typical hierarchical enterprise campus network design includes the following three layers:

The Access Layer

The Access Layer is the one closer to the users. In fact, at this layer, we find the users themselves and the access-layer switches. The main purpose of this layer is to physically connect users to the network. In other words, there is just a cable between end-user PCs and access-layer switches.

At this layer, we apply network-access policies. These are the security policies we want to enforce in order to allow access to the network. For example, we can configure port-security or Network Access Control to ensure that only our company's PC can have access to the network. Furthermore, since we are talking about Layer 2, Spanning-Tree is running as a loop-prevention mechanism.

- ❖ **Device connectivity**—The access layer provides high-bandwidth device connectivity.
- ❖ **Resiliency and security services**—The access-layer design must ensure that the network is available for all users who need it, whenever they need it. As the connection point between the network and client devices, the access layer must help protect the network from human error and from malicious attacks.

Generally speaking, at this layer we generally use simple fixed form-factor Layer 2 switches. This is because if we want to support more users we aren't going to expand our access switches. Instead, we will simply add an access switch more.

The Distribution Layer

The Distribution layer bridges users to the core layer. It serves as a major spine for all users in an area, so it connects several access switches. In most deployment, Default Gateways for all the VLANs reside at the Distribution layer.

It is encouraged to reduce Layer 2 links in your network, having all Layer 3 links but the ones going directly to users. However, this is not yet possible as it requires some advanced access switches. As a result, the compromise implemented often-times is to have Layer 2 links between the Access and Distribution layer. This way, you can have default gateways residing at the distribution layer. Furthermore, here you can apply distribution policies. These policies include filtering traffic to allow some devices to reach only some of the other devices, or policy-routing (customizing routing, CCNP stuff).

- ❖ **Scalability**—At any site with more than two or three access-layer devices, it is impractical to interconnect all access switches. The distribution layer serves as an aggregation point for multiple access-layer switches.
- ❖ **Reduce complexity and increase resiliency**—The campus wired LAN has the option to use a simplified distribution layer, in which a distribution-layer node consists of a single logical entity that can be implemented using a pair of

physically separate switches operating as one device (StackWise Virtual) or using a physical stack of switches operating as one device.

At this layer, you have to use multilayer switches. Furthermore, their form factor should be at least stackable, so that you can expand the distribution layer in case you need more ports. In large deployments, you can find modular switches at this layer.

The Core Layer

In the Three-Tier Architecture, the Core Layer is the one coordinating everything. It has only one, simple purpose: connecting all the distribution layers together. In large enterprises, where you have several distribution switches, the core layer is also known as Backbone.

Cisco is very clear about the purpose of this layer. Its only role is to forward traffic, the fastest it can. Here you don't apply any policy, as you must try to reduce the load of the core so it can focus on routing. It is likely that your core switches talk with distribution switches using dynamic routing protocols, such as OSPF or EIGRP.

At this layer, we find the most advanced and expensive switches, the ones with the modular form factor. These are fully redundant devices supporting advanced Layer 3 switching features and dynamic routing protocols. However, remember that you need to keep your configuration as simple as possible on devices in this role.

Core Layer Technologies Technologies used at the core layer include the following:

- ❖ Routers or multilayer switches that combine routing and switching in the same device
- ❖ Redundancy and load balancing
- ❖ High-speed and aggregate links
- ❖ Routing protocols that scale well and converge quickly, such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) Protocol

This design model is typically used in campus networks, which are constructed of multiple functional distribution layer blocks. This design is most suitable to our need as:

- i. The main in the university controls and distributes the internet access. It has the core router. The core router then forwards the packet to the network that it is intended for.
- ii. The switches form the distribution layer. They forward the packets to the wired clients or the access points.
- iii. At the end, the clients which are the students and the faculty form the access layer who consume the media.

7.2 TOPOLOGY

Topology refers to the geometric arrangement of devices on a network. Local Area Networks (LANs) appear in one of three topologies: linear, ring, or star. Larger networks can be a combination of two or more of these. The configuration, or topology, of a network is key to determining its performance.

BUS Topology

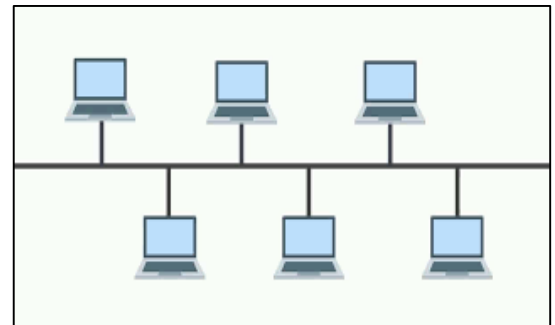
Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.

Features of Bus Topology

- ❖ It transmits data only in one direction.
- ❖ Every device is connected to a single cable

Advantages of Bus Topology

- ❖ It is cost effective.
- ❖ Cable required is least compared to other network topology.
- ❖ Used in small networks.
- ❖ It is easy to understand.
- ❖ Easy to expand joining two cables together.



Disadvantages of Bus Topology

- ❖ Cables fails then whole network fails.
- ❖ If network traffic is heavy or nodes are more the performance of the network decreases.
- ❖ Cable has a limited length.
- ❖ It is slower than the ring topology

Ring Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

Features of Ring Topology

- ❖ A number of repeaters are used for Ring topology with large number of nodes to prevent data loss.
- ❖ The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

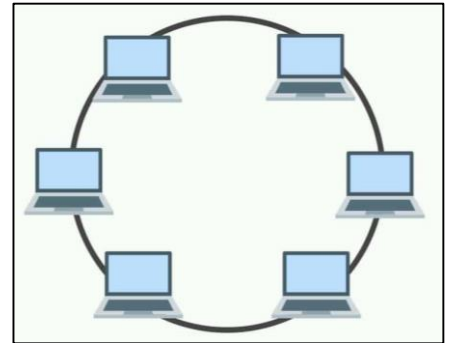
- ❖ In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
- ❖ Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

- ❖ Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- ❖ Cheap to install and expand

Disadvantages of Ring Topology

- ❖ Troubleshooting is difficult in ring topology.
- ❖ Adding or deleting the computers disturbs the network activity.
- ❖ Failure of one computer disturbs the whole network.



STAR Topology

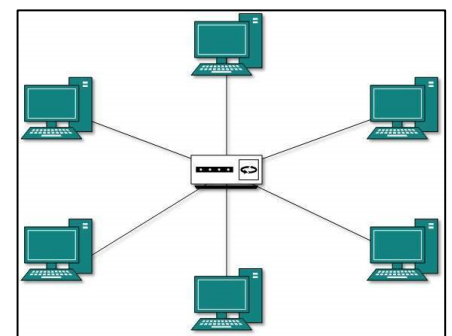
In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.

Features of Star Topology

- ❖ Every node has its own dedicated connection to the hub.
- ❖ Hub acts as a repeater for data flow.
- ❖ Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

- ❖ Fast performance with few nodes and low network traffic.
- ❖ Hub can be upgraded easily.
- ❖ Easy to troubleshoot.
- ❖ Easy to setup and modify.
- ❖ Only that node is affected which has failed, rest of the nodes can work smoothly.



Disadvantages of Star Topology

- ❖ Cost of installation is high.
- ❖ Expensive to use.
- ❖ If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- ❖ Performance is based on the hub that is it depends on its capacity

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has $n(n-1)/2$ physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

- ❖ **Routing**

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

- ❖ **Flooding**

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

Types of Mesh Topology

Partial Mesh Topology :

In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.

Full Mesh Topology :

Each and every nodes or devices are connected to each other.

Features of Mesh Topology

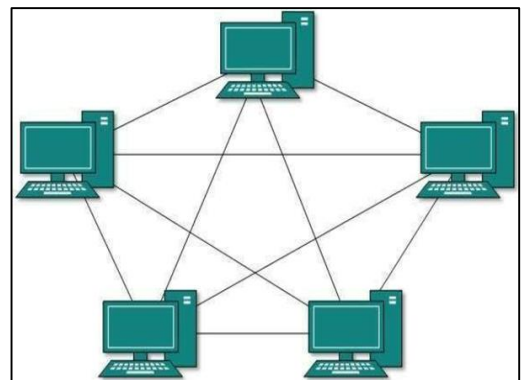
- ❖ Fully connected.
- ❖ Robust.
- ❖ Not flexible.

Advantages of Mesh Topology

- ❖ Each connection can carry its own data load.
- ❖ It is robust.
- ❖ Fault is diagnosed easily.
- ❖ Provides security and privacy.

Disadvantages of Mesh Topology

- ❖ Installation and configuration is difficult.
- ❖ Cabling cost is more.
- ❖ Bulk wiring is required.



TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Features of Tree Topology

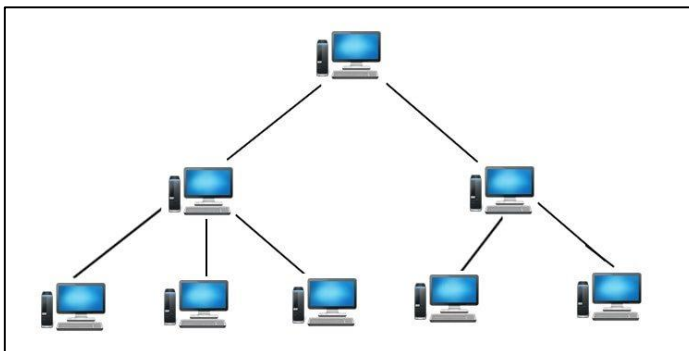
- ❖ Ideal if workstations are located in groups.
- ❖ Used in Wide Area Network.

Advantages of Tree Topology

- ❖ Extension of bus and star topologies.
- ❖ Expansion of nodes is possible and easy.
- ❖ Easily managed and maintained.
- ❖ Error detection is easily done.

Disadvantages of Tree Topology

- ❖ Heavily cabled.
- ❖ Costly.
- ❖ If more nodes are added maintenance is difficult.
- ❖ Central hub fails, network fails.



In our scenario, the tree topology and the hierarchical system design is the most suitable. Our model is a combination of tree and star topology as the 3 buildings with their own separate network is connected to the main router. This ensures the networks are separated and helps in central routing.

8 IP NETWORK DESIGN GUIDELINES

The IP network design depends on the type of network that is needed by the organization. It influences the network routing. The topology of the network also determines how the IP addresses are designed for the network.

An IP address uniquely identifies a device on an IP network. In case for IPv4, an IP address is 32 bits in length and is divided into two parts. The first part covers the network portion of the address and the second part covers the host portion of the address. The host portion can be further partitioned (optionally) into a subnet and host address. A subnet address allows a network address to be divided into smaller networks.

IP Address Classes IP addresses are split up into several different categories, including Class A, B, C, D (Multicast), and E (Reserved). Address classes are defined, in part, based on the number of bits that make up the network portion of the address, and in turn, on how many are left for the definition of individual host addresses.

- In Class A addresses, the first octet is the network portion.
- In Class B, the first two octets are the network portion.
- In Class C, the first 3 octets are the network portion.

Here for our purpose we use class C of IP addressing.

Subnetting

It allows us to create multiple logical networks that exist within a single Class A, B, or C network. If we do not subnet, we can only use one network from our Class A, B, or C network, which is simply unrealistic. Each data link on a network must have a unique network address, with every host on that link being a member of the same network. If we break a major network (Class A, B, or C) into smaller subnetworks, we can create a network of interconnected subnetworks. Each data link on this network would then have a unique network/subnetwork ID.

Here we have assigned a separate network to each of the buildings. As the number of users is less per network, we have gone with 255.255.255.0 as the default subnet for this scenario.

Summarization

Summarizing IP addresses ensures that there are no entries for child routes, which are routes that are created for any combination of the individual IP addresses contained within a summary address in the routing table. This summarization reduces the size of the routing table and allows the router to handle more routes.

As we have 3 different networks, the router whenever it reads the network bits can directly forward the packet to the interface that is connected to that network. It ensures a faster delivery of the packets.

For this case study we have 3 buildings with a certain amount of users in each. They are:

- Main building: 20 Users
- Tech Park: 20 Users
- Hospital building: 10 Users

In this case as we know the number of users in each space it is better to go for static IP address space. Each building can be assigned its own network. In each subnet the particular users can be assigned a particular IP address.

The advantages of static routing are:

- Static routing causes very little load on the CPU of the router, and produces no traffic to other routers.
- Static routing leaves the network administrator with full control over the routing behavior of the network.
- Very secure. No advertisements are sent, unlike with dynamic routing protocols.
- It is very predictable, as the route to the destination is always the same.
- It is useful to have a static address for a printer connected to the network.

8.1 IP SCHEME

The router in the main building is responsible for managing the network in the three main buildings. The IP scheme is as follows:

Main Building

The switch has access point connected to it. Client can connect wirelessly to the access point or directly connect via a wired link.

The network address is: 192.168.10.0
Subnet : 255.255.255.0
Range of hosts (20) : 192.168.10.1 – 192.168.10.20

Tech Park

A switch connects to the main router. The switch has access point connected to it. Clients can connect wirelessly to the access point or directly connect via a wired link.

The network address is: 192.168.11.0
Subnet : 255.255.255.0
Range of hosts (20) : 192.168.11.1 – 192.168.11.20

Hospital Building:

A switch connects to the main router. The switch has access point connected to it. Clients can connect wirelessly to the access point or directly connect via a wired link.

The network address is: 192.168.12.0
Subnet : 255.255.255.0
Range of hosts (10) : 192.168.12.1 – 192.168.12.10

8.2 IP ADDRESS MANAGEMENT

IP address management is the process of allocating and documenting IP addresses and subnets in a network. Recommended IP address management standards reduce the opportunity for:

- overlapping or duplicate subnets,
- non-summarization in the network,
- duplicate IP address device assignments,
- wasted IP address space,
- unnecessary complexity.

Address Space Planning

The administrators have to carefully assign the space to host devices. A certain amount of pre planning is required based on the number of users and the amount of growth the network will have in the future.

In this particular case we know the number of users per building. The hosts have each been assigned their own unique IP address. In each of those networks, the user space can grow to 256 users.

Hierarchical Addressing

Hierarchical addressing leads to efficient allocation of IP addresses. A hierarchical address plan allows us to take advantage of all possible addresses because we can easily group them together. This ensures that users in a particular building have the same network address. This also decreases the amount of routing table entries.

Benefits:

- Modular design and scalable solutions: Whether building a new network or adding a new service on top of an existing infrastructure, a modular design helps to deliver a long-term, scalable solution. IP addressing modularity allows the aggregation of routing information on a hierarchical basis.
- Route aggregation: Route aggregation is used to reduce routing overhead and improve routing stability and scalability.

Centralized IP Addressing

Address space planning and assignment can be best achieved using a centralized approach and maintaining a central IP inventory repository or database. The centralized approach provides a complete view of the entire IP address allocation of various sites within an organization. This helps in reducing IP address allocation errors and also reduces duplicate IP address assignment to end devices.

Recycling of IP addresses

For students who are graduating, their old IP addresses will become useless. These IP addresses need to be recycled and given to the new students. If this is not managed diligently then there will soon be a shortage of IP addresses in a given space.

9 FEATURES AND SERVICES

The features of the network are:

The main router is connected to the internet provided by the ISP. It acts as a firewall and allows only certain packets to go to and fro.

It is connected to 3 high end switch in each building via gigabit ports. Network has to be configured for each interface connecting to the switches.

The firewall ensures that only safe packets are sent to each of the network. Hence, subsequent filtering of packets are not required in the lower hierarchies.

- For example, packets sent from users of the open WLAN to TCP ports 80 (HTTP), 25 (SMTP), and 110 (POP), and UDP ports 53 (DNS) and 67 (DHCP) are permitted. All other traffic is denied.
- Intrusion Detection Systems can identify suspicious traffic patterns, e.g. – machines using Bittorrent – machines infected with certain viruses/worms – some network-based attacks
- SSL Certificates- Use certificates from well known certificate authorities.

9.1 WIRELESS ACCESS

Wireless access in the campus is deployed by connecting WLAN access point to the main switches in each building. The main challenge when it comes to wireless network is the coverage of the network throughout the building. A stable connection is required by the hosts so that there is no loss of work due to drop in connection.

Many students and faculty want secure access to the campus network using the wireless network to access the Internet. So it is important to have a strong security for the access points too.

Depending on the area that needs to be covered, we can add access points to a particular building. For example, one floor may have two access points at the opposite ends to ensure proper connectivity.

The benefits of wireless LAN are:

- Productivity gains through secure, location-independent network access—Measurable productivity improvements and communication.
- Additional network flexibility—Hard-to-wire locations connected wirelessly, without costly construction.
- Cost-effective deployment—Adoption of virtualized technologies within the overall wireless architecture.
- Easy to manage and operate—From a single pane of glass, centralized control of a distributed wireless environment.
- Support for wireless users—Bring-your-own-device (BYOD) design models.
- Efficient transmission of multicast traffic—Support for many group communication applications, such as video and push-to-talk.

Multicast Support

Video and voice applications continue to grow as smartphones, tablets, and PCs are added to wireless networks in all aspects of our daily life. In each of the wireless design models, the multicast support that users are accustomed to on a wired network is available wirelessly. Multicast is required in order to enable the efficient delivery of certain one-to-many applications, such as video and push-to-talk group communications.

Technology Standards

Over time with the advent of consumer devices operating in the 2.4-GHz industrial, scientific and medical band, the level of noise resulting in interference in this band has grown considerably. Likewise, many of the wireless devices available today are dual band and can operate in either the 2.4-GHz or 5-GHz band.

Both have its own set of advantages and disadvantages.

Range:

2.4Ghz provides signal the farthest when compared to 5Ghz. Hence it is more suitable for offices and campuses.

Bandwidth (speed):

Higher bandwidth means that files will download and upload faster, and high-bandwidth applications such as streaming video will perform much smoother and faster.

Higher frequencies allow faster transmission of data, also known as bandwidth. Therefore, the 5GHz with its higher bandwidth will provide much faster data connections than 2.4 GHz.

Interference:

5GHz is more suitable to cut through interference from other wireless devices as the channels used by 5GHz devices are usually less congested than 2.4GHz.

Through objects: 5GHz cannot pass through a lot of solid objects. 2.4GHz is more suitable in this regard.

Taking into account the above, **2.4GHz** is more suitable for our need. It gives a much bigger coverage and at the same time has better reception through walls.

802.11 Series

The first standard of the 802.11 series appeared in 1997 and it was created by the Institute of Electrical and Electronics Engineers. The IEEE 802 standards define two separate layers for the Data-Link layer of the OSI model. The one is Logical Link Control Layer and the other is media access control Layer.

The 802.11 only supports 2Mbps bandwidth and it can't meet the demands of the users anymore.

The 802.11b version was introduced in 1999. It supports 11Mbps bandwidth and it uses direct sequence spread spectrum technology.

The 802.11a version was created at the same time as 802.11b. It uses orthogonal frequency division multiplexing for data modulation. It supports voice, data and image transmission. It also supports 54 Mbps bandwidth

The 802.11g version appeared in 2002. It supports 54 Mbps bandwidth and 2.4 GHz frequency

The 802.11n version was the development of 802.11g. The rate was increased to 600Mbps. And, it supports 2.4GHz and 5GHz frequency. 802.11n can improve the quality of wireless transmission. It combines MIMO and OFDM technologies. MIMO means multiple in multiple out and it is commonly used in home routers for coordinated use of the multiple radio antennas in wireless network. The MIMO technology can increase the bandwidth and the range of the network

The 802.11ac version is popular one in the market. It appeared in 2012. It is a faster and scalable version than 802.11n. 802.11ac supports 1Gbps data rate and 5GHz frequency.

We have gone ahead with 802.11n 2.4GHz standard. It provides the highest bandwidth and range among others.

WLAN Security

Security has always been an important part of wired or wireless network. As time goes by, threats for all privacy information transferred from client devices through WLAN are growing. It's time to protect WLAN from being attacked.

There are authentication methods such as shared key, WEP, EAP, WPA/WPA2.

We have chosen WPA2-PSK as our encryption method.

WPA/WPA2-PSK

WPA stands for Wi-Fi Protected Access. WPA is also known as the draft IEEE 802.11i standard. It provides stronger encryption than WEP by using temporal key integrity protocol and advanced encryption standard technologies. WPA designed for home user is called WPA-PSK. It's the most simplified and powerful form of WPA. A person who uses WPA-PSK will configure a static key for security.

WPA2 is another version of WPA to security the network and WPA2-PSK a simple and safety choice for most of the home users. But WPA2 will decrease the performance of the network because encryption and decryption process are needed.

Advanced Encryption Standard (AES) was used for generation of the key. It uses a Pre-Shared Key (PSK) that is 8 or more characters in length, up to a maximum of 63 characters.

9.2 SSH (SECURE SHELL)

SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network. In addition to providing secure network services, SSH refers to the suite of utilities that implement the SSH protocol. Secure Shell provides strong password authentication and public key authentication, as well as encrypted data communications between two computers connecting over an open network, such as the internet.

The first version of SSH appeared in 1995 and was designed by Tatu Ylönen, who was, at the time, a researcher at Helsinki University of Technology and later went on to start SSH Communications Security, a cybersecurity vendor based in Finland.

SSH-2, the current version of Secure Shell protocols, was adopted as a Standards Track specification by the Internet Engineering Task Force (IETF) in 2006. SSH-2 is not compatible with SSH-1 and uses a Diffie-Hellman key exchange and a stronger integrity check that uses message authentication codes to improve security.

Functions that SSH enables include the following:

- secure remote access to SSH-enabled network systems or devices for users, as well as automated processes;
- secure and interactive file transfer sessions;
- automated and secured file transfers;
- secure issuance of commands on remote devices or systems; and
- secure management of network infrastructure components.

Secure Shell was created to replace insecure terminal emulation or login programs, such as Telnet, rlogin (remote login) and rsh (remote shell); SSH enables the same functions (logging in to and running terminal sessions on remote systems)

Quality of Service (QoS)

The primary role of QoS in rich-media campus networks is to manage packet loss, where high-bandwidth links with instantaneous congestion on the order of milliseconds can cause buffer overruns and a poor user experience. Another goal of campus QoS is to apply policies to at the edge to allow consistent treatment of traffic for a predictable user experience across the entire enterprise network.

QoS allows an organization to define different traffic types and to create more deterministic handling for realtime traffic. QoS is especially useful in congestion handling, where a full communications channel might prevent voice or video streams from being intelligible at the receiving side.

Congestion is common when links are oversubscribed by aggregating traffic from a number of devices, and also when traffic on a link to a device has come from upstream links with greater bandwidth. Rather than creating bandwidth, QoS takes bandwidth from one class and gives it to another class.

10 BILL OF MATERIAL

1. Cisco Router ISR4451-X/K9

Cisco 4451 Integrated Services Router, named as ISR4451-X, which supports 2 Enhanced service-module (SM-X) slots, delivers 1 Gbps to 2Gbps aggregate throughput. This router also supports two kinds of DDRM, data plane and control/services plane, which make administrator easy to manage the router.



Specification:

Product Code	Cisco ISR4451-X/K9
Aggregate Throughput	1 Gbps to 2Gbps
Total onboard WAN or LAN 10/100/1000 ports	4
RJ-45-based ports	4
SFP-based ports	4
Enhanced service-module (SM-X) slot	2
NIM (Network Interface Modules) slots	3
Onboard ISC slot	1
DDRM (data plane)	2 GB (default) / 2 GB (maximum)
DDRM (control/services plane)	4 GB (default) / 16 GB (maximum)
Flash Memory	8 GB (default) / 32 GB (maximum)
Power-supply options	Internal: AC, DC (roadmap) and PoE
Rack height	2 RU
Dimensions (H x W x D)	88.9 x 438.15 x 469.9 mm

Price: ₹ 5,19,836.99

Quantity : 1

2. Switch

Cisco C9300-24P-A

The Cisco Catalyst 9300 Series Switches are Cisco's lead stackable enterprise switching platform built for security, IoT, mobility, and cloud. At 480 Gbps, they are the industry's highest-density stacking bandwidth solution with the most flexible uplink architecture.



Specification:

Product Code	C9300-24P-A
Product Description	Catalyst 9300 24-port PoE+, Network Advantage
Total 10/100/1000 or Multigigabit copper ports	24 POE+
Default AC power supply	715W AC
Available PoE power	445W
Dimensions (H x W x D)	1.73 x 17.5 x 17.5 Inches
Weight	16.33 Pounds

Price: ₹182,851.19
Quantity: 3
Total Price: 3 x 182,851.19
=₹548553.57

3. Access Point

Cisco AIR-CAP3702I-C-K9

3700 Series utilizes a Purpose-built innovative chipset to provide a high density experience for enterprise network. 4 x 4 MIMO (multiple-input multiple-output) technology with three-spatial-stream offers a greater coverage for more reliability and capacity than competing access points.



Specifications:

Product Code	AIR-CAP3702I-C-K9
WiFi Standards	802.11a/b/g/n/ac
Ideal For	Midsize or large enterprises that require mission-critical traffic
Max Data Rate 5GHz	1.3 Gbps
MIMO Radio Design: Spatial Streams	4 x 4:3
Client count/ClientLink client count	200/128
Controller Available	Yes
Power	4 x 4:3 operation: 802.3at PoE+ Enhanced PoE, Universal PoE (UPOE) 3 x 3:3 operation: 802.3af PoE
Antenna	Internal Antenna
Regulatory Domain	C (C regulatory domain): - 2.412 to 2.472 GHz; 13 channels - 5.745 to 5.825 GHz; 5 channels
Dimensions (W x L x H)	22.1 x 22.1 x 5.4 cm (without mounting bracket)
Weight	1.13 Kg

Price: ₹64,066.89

Minimum quantity required: 3 * 2 = 6

Total Price: ₹3,84,401.34

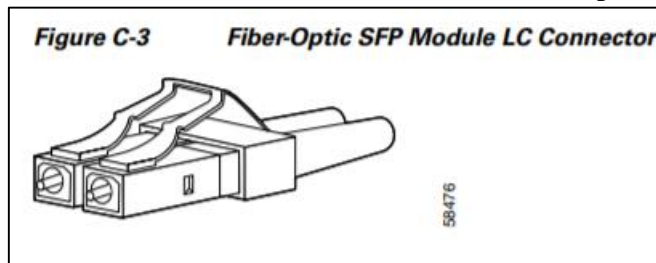
4. Cables:

a. Fiber optic cable

For connection between the main router to the switches in each building a fiber optic cable is best suited. The 100BASE-FX ports use MT-RJ connectors.



100m Fiber Optic Cable



Quantity =5

Price =5*7000= ₹35,000

b. CAT 6 cables

These cables would be used to connect the switch to the access points and other clients that use RJ45. It gives speed upto 10-Gigabit Ethernet.



100m Cat 6 cable price = ₹2300

Approximate Quantity required: 10

Total price = 10 * 2300 = ₹23,000

Approximate Total Bill:

This includes cost of only hardware network components.

Serial No.	Component	Quantity	Price
1	Cisco Router ISR4451-X/K9	1	5,19,836.99
2	Cisco C9300-24P-A	3	5,48,553.57
3	Cisco AIR-CAP3702I-C-K9	6	3,84,401.34
4	100m Fiber Optic Cable	5	35,000.00
5	100m Cat 6 cables	10	23,000.00
	Total		₹15,10,791.9

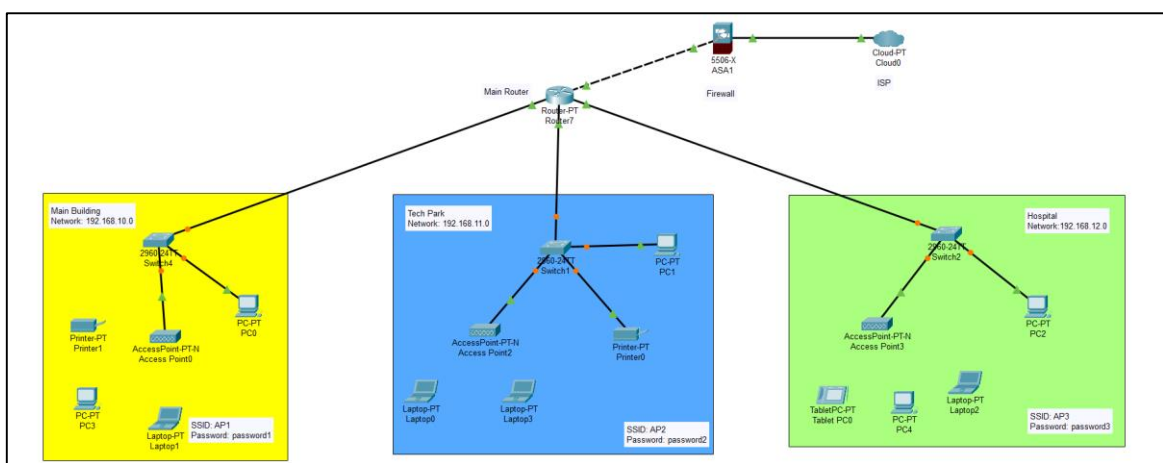
The total price will be: ₹15 lakh approximately

11 IMPLEMENTATION

We now know the design and topology that we want to implement. We can theoretically build and check our design in Cisco Packet Tracer.

As discussed earlier, we will implement a campus network that contains one core router in the main building, 3 switches in each building and the access points that helps the client in connecting to the network. We will then add services like securing the wireless access point and adding SSH encryption for remote configuration of the routers.

At first we add all the components to the Packet Tracer workspace. We connect all the components with copper straight through cable.



11.1 IP CONFIGURATION

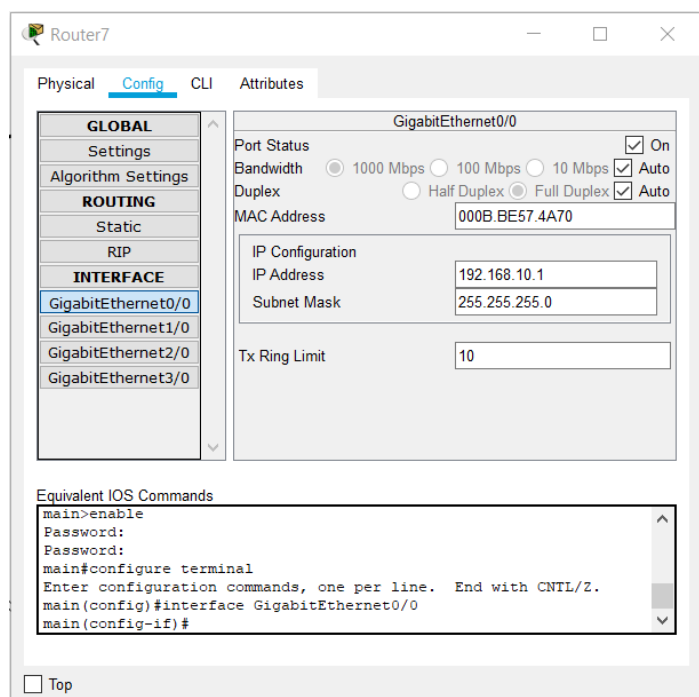
We implement static IP addressing. So we set up the network address for the interface in the main router and each of the clients in the 3 buildings.

Main Building

The network of main building is 192.168.10.0 and subnet is 255.255.255.0

The router configuration for interface GigabitEthernet0/0 is:

Here, the interface GigabitEthernet0/0 is the one that's connected to the switch of the main building.



The configuration of any one client is:

The screenshot shows a window titled "PC3" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying the "IP Configuration" dialog. The "Interface" dropdown is set to "Wireless0". Under "IP Configuration", the "Static" radio button is selected. The fields are filled with: IP Address: 192.168.10.3, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.10.1, and DNS Server: 0.0.0.0. Under "IPv6 Configuration", the "DHCP" radio button is selected, and the "Link Local Address" is set to FE80::2E0:8FFF:FE67:5E1C. A "Top" checkbox is at the bottom left.

The gateway is the IP of interface of main router.

Tech Park Building

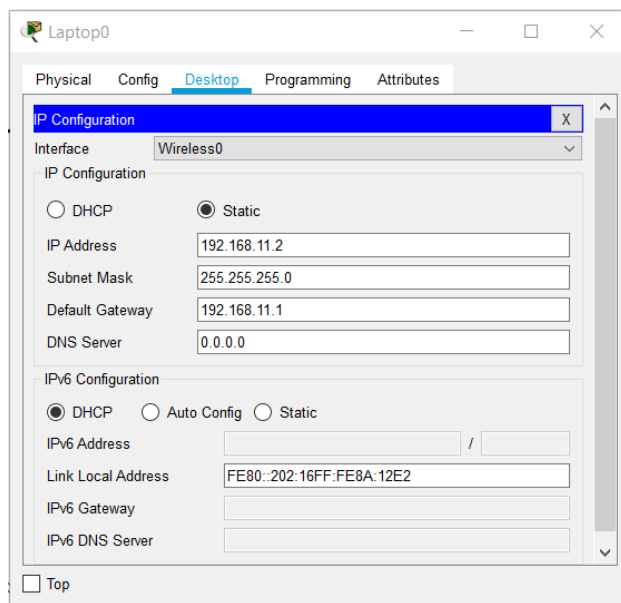
We configure the interface GigabitEthernet1/0 of the main router in similar way.

The screenshot shows a window titled "Router7" with tabs for Physical, Config, CLI, and Attributes. The "Config" tab is active, displaying the configuration for "GigabitEthernet1/0". The "Port Status" is "On". "Bandwidth" is set to "1000 Mbps" and "Duplex" is set to "Full Duplex", both with "Auto" selected. The "MAC Address" is 00D0.BA7E.2638. Under "IP Configuration", the "IP Address" is 192.168.11.1 and the "Subnet Mask" is 255.255.255.0. The "Tx Ring Limit" is set to 10. A sidebar on the left shows a tree view with "INTERFACE" expanded and "GigabitEthernet1/0" selected. At the bottom, a text area titled "Equivalent IOS Commands" contains the following commands:

```
main#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
main(config)#interface GigabitEthernet0/0
main(config-if)#
main(config-if)#exit
main(config)#interface GigabitEthernet1/0
main(config-if)#
```

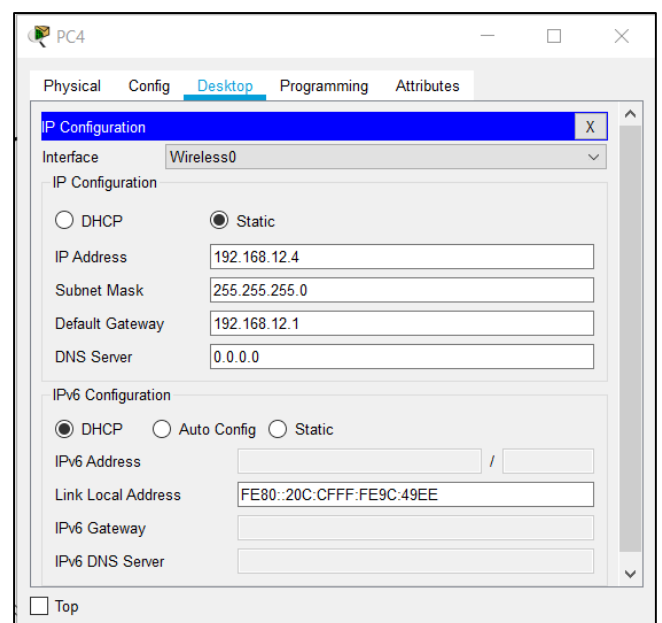
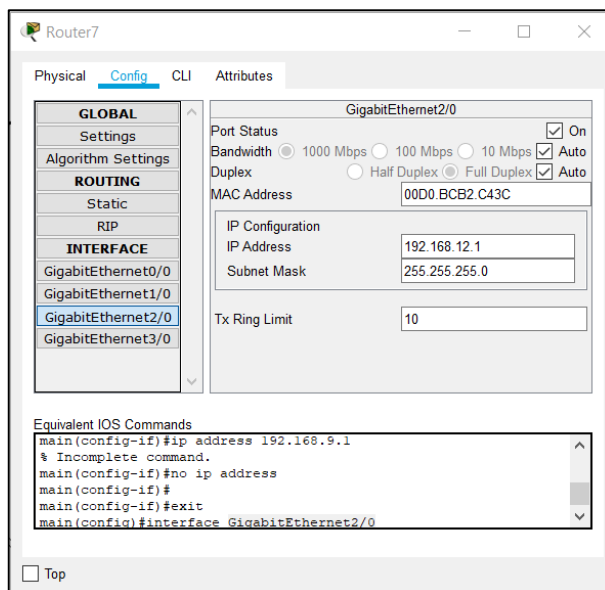
A "Top" checkbox is at the bottom left.

Client are then configured.



Hospital building

Router interface GigabitEthernet2/0 is configured.



Clients are similarly configured.

11.2 SETTING UP WIRELESS ACCESS POINTS

We set up APs in each of the networks with their own encrypted WPA2-PSK password.

The screenshot shows the configuration window for Access Point0, specifically the Port 1 configuration tab. The window has three tabs: Physical, Config (selected), and Attributes. On the left, there is a sidebar with 'GLOBAL' and 'INTERFACE' sections. Under 'INTERFACE', 'Port 1' is selected. The main area shows the configuration for Port 1. The 'Port Status' is checked and set to 'On'. The 'SSID' is 'AP1'. The '2.4 GHz Channel' is '6'. The 'Coverage Range (meters)' is '250.00'. Under 'Authentication', 'WPA2-PSK' is selected. The 'PSK Pass Phrase' is 'password1'. The 'Encryption Type' is 'AES'.

Main Building

SSID: AP1

Password: password1

Authentication: WPA2-PSK

Encryption: AES

Tech Park

SSID: AP2

Password: password2

Authentication: WPA2-PSK

Encryption: AES

The screenshot shows the configuration window for Access Point2, specifically the Port 1 configuration tab. The window has three tabs: Physical, Config (selected), and Attributes. On the left, there is a sidebar with 'GLOBAL' and 'INTERFACE' sections. Under 'INTERFACE', 'Port 1' is selected. The main area shows the configuration for Port 1. The 'Port Status' is checked and set to 'On'. The 'SSID' is 'AP2'. The '2.4 GHz Channel' is '6'. The 'Coverage Range (meters)' is '250.00'. Under 'Authentication', 'WPA2-PSK' is selected. The 'PSK Pass Phrase' is 'password2'. The 'Encryption Type' is 'AES'.

Hospital Building

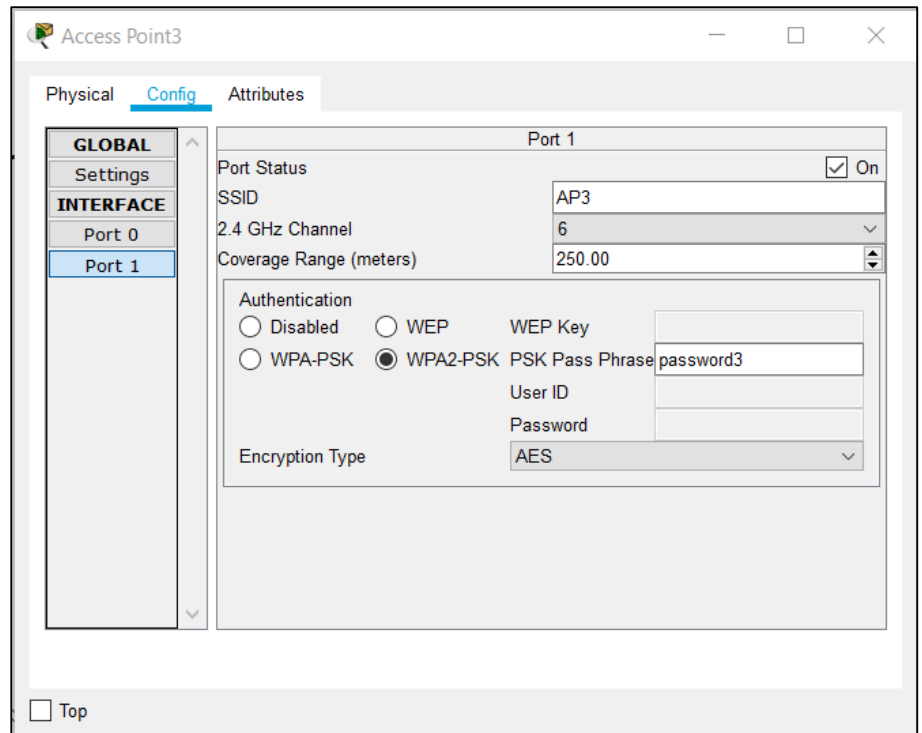
SSID: AP3

Password: password3

Authentication:

WPA2-PSK

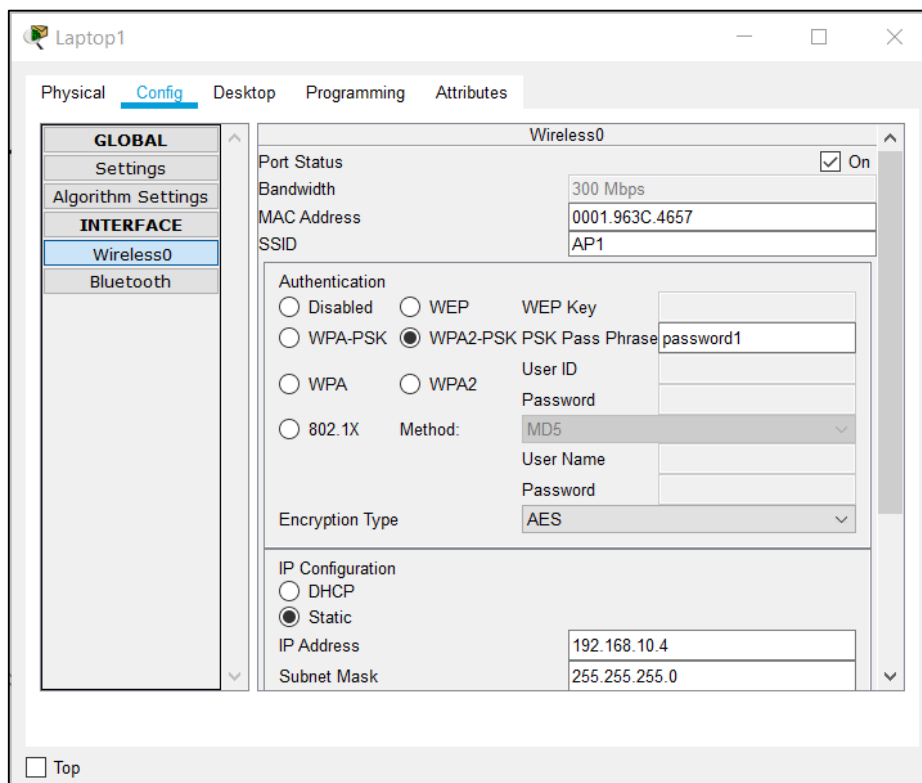
Encryption: AES



Each client's wireless setting is then setup. The appropriate SSID and password is entered.

For example,

Client connecting to the AP1 of main building with password: password1

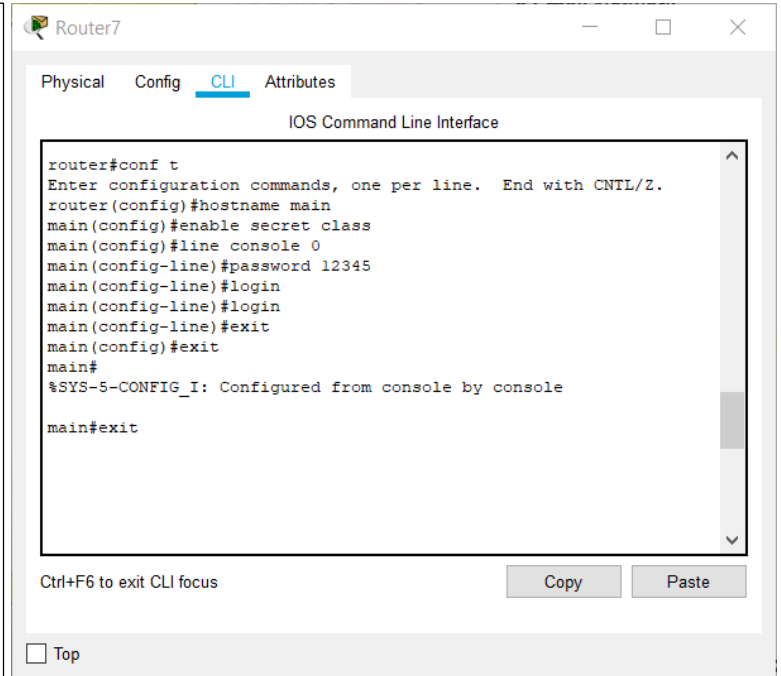


11.3 SSH IMPLEMENTATION

SSH secures the connection to router and ensures that only authorized personnel can remotely change the configuration of the router.

1. We first add password to the line of our router.

```
router#conf t
Enter configuration commands,
one per line. End with CNTL/Z.
router(config)#hostname main
main(config)#enable secret class
main(config)#line console 0
main(config-line)#password 12345
main(config-line)#login
main(config-line)#login
main(config-line)#exit
main(config)#exit
main#
```



2. We then create an IP domain and generate a RSA crypto key of 1024 bits.

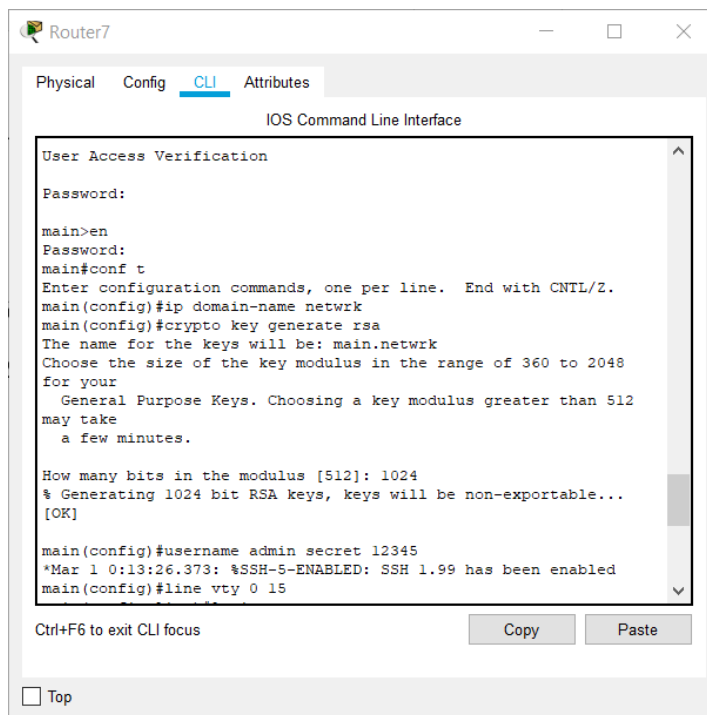
```
main#conf t
Enter configuration commands, one per line. End with CNTL/Z.
main(config)#ip domain-name network
main(config)#crypto key generate rsa
The name for the keys will be: main.network
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

main(config)#username admin secret 12345
*Mar 1 0:13:26.373: %SSH-5-ENABLED: SSH 1.99 has been enabled
main(config)#line vty 0 15

main(config-line)#login local
main(config-line)#transport input ssh
main(config-line)#exit
```

3. For line 0 to 15 we select transport as SSH



To check for SSH we try accessing the router from a client

```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.11.1
Trying 192.168.11.1 ...Open

[Connection to 192.168.11.1 closed by foreign
host]
C:\>ssh
Packet Tracer PC SSH

Usage: SSH -l username target

C:\>ssh -l admin 192.168.11.1

Password:

main>en
Password:
main#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
main(config)#
```

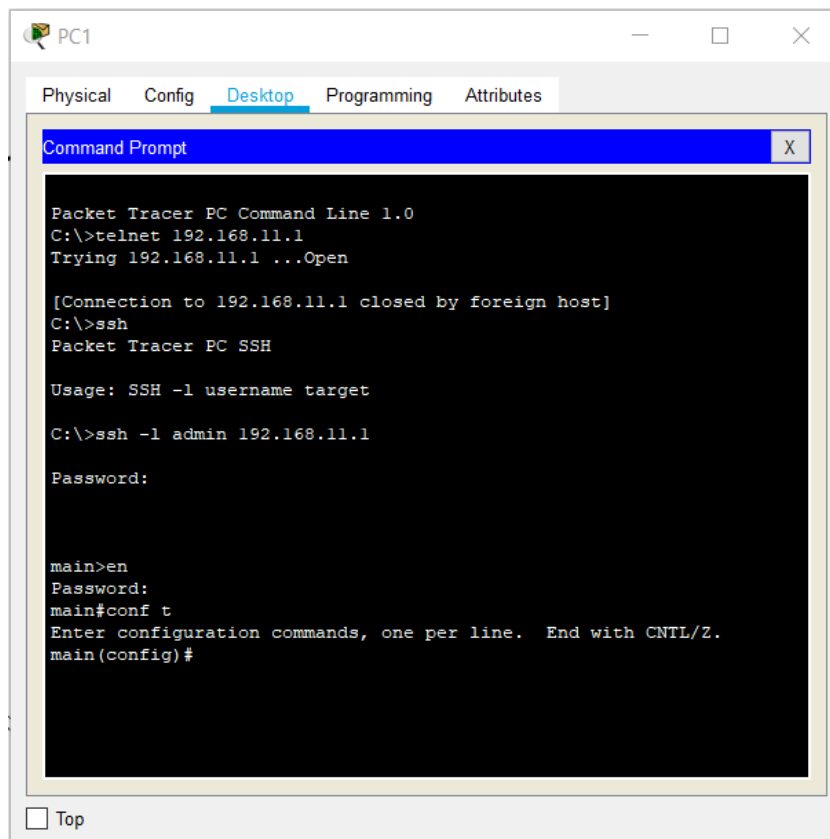
We first try Telnet.

It says that it has been closed by foreign host

Then we try SSH we username and the target IP address.

It asks for password.

After successful authentication, we can now configure the router.



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt X
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.11.1
Trying 192.168.11.1 ...Open

[Connection to 192.168.11.1 closed by foreign host]
C:\>ssh
Packet Tracer PC SSH

Usage: SSH -l username target

C:\>ssh -l admin 192.168.11.1

Password:

main>en
Password:
main#conf t
Enter configuration commands, one per line. End with CNTL/Z.
main(config)#
```

Router can now be configured remotely with SSH authentication.

SSH has hence been successfully configured.

12 CONCLUSION

In today's age having a reliable and effective network in campus is essential. With the advent of the Internet age, the impact of our education is unprecedented, and it also provides a rapid leap for education opportunities. The premise of network education is the construction of the network, and as the construction of the campus network is not only the construction of the network hard environment, but also must include the campus network maintenance and security, campus network resources and the effective application of the campus network. Only the full and effective application of the campus network in order to make the entire teaching model and the educational concept of a complete change in order to apply the new century to cultivate high-quality creative and complex talents needs for the campus network construction.

When designing a network, we have to keep in mind about the future upgradability. Keeping it cost effective is a challenge as reliability comes at the cost of expensive hardware. Security is another important factor that needs to be considered.

Wireless networks have become the future of connectivity. It brings a lot of convenience to people's lives. Even though we have seen that wired connections are more reliable, with the progress and continuous innovation of network technology, WLANs still play an important role in our daily life for many aspects.

Thus we see how even a simple network design can have several fundamental factor affecting it. All of those factors and features need to be considered and well planned prior to constructing the network. The internet plays a huge role in our lives today. It is upto us the network engineers to build and main connectivity that everyone can depend upon for their school, work or entertainment.

13 REFERENCE

- ❖ Campus LAN and Wireless LAN Solution Design Guide
<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html>
- ❖ Campus Wired Network Design Options
<https://www.router-switch.com/solution/campus-wired-network-design-options.html>
- ❖ Introducing Network Design Concepts
<https://students.mimuw.edu.pl/~zbyszek/sieci/CCNA4%20Sample.pdf>
- ❖ IPv4 Address Design
<https://flylib.com/books/en/3.293.1.30/1/>
- ❖ Cable and Connectors
https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3000/hardware/installation/guide/IE3000HIG/HIGCABLE.pdf
- ❖ Hardware Price
<https://www.router-switch.com/>
- ❖ Campus Wireless LAN Technology Design Guide - August 2014
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-CampusWirelessLANSDesignGuide-AUG14.pdf>
- ❖ SSH <https://www.ssh.com/ssh/protocol/>
- ❖ Wireless Network Standard
<https://www.technology.pitt.edu/help-desk/how-to-documents/wireless-network-standard>
- ❖ Pricilla Openheimer, “Top Down Network Design: a system analysis approach to design enterprise networks”, CISCO system inc, third Edition, 2011
- ❖ Wang Da. 'Network Engineering must read - network system design.' Beijing: Electronic Industry Press, 2006