Computer Networks
Assignment-1

Name: Dolton Fernandes
Roll No: 2018111007

Design LAN for the locality you are staying right now - Apartment/Township/Colony/Village/Campus/etc.

You need to address the following aspect:
1) Topological design
2) Choice of cables at various levels
3) Choice of networking devices - types/category of the device, port speed, Hub/Switch
4) IP Addressing schema

Give description of your locality (layout, number of houses, distances involved, etc), state your assumptions and use cases. A detailed design is expected, discussing the specifics of each aspect/component required for implementing the LAN. Discuss options available/considered by you, give reasons for choices made and for rejecting an available option.

LAN Design for my locality:

- **Name:** Ajanta Blue Bells, Aurangabad
- **Type:** Row houses + 3 separate buildings with apartments
- **Number of row houses:** 83
- **Number of apartments:** 100
- **Row Houses Layout:** The rows houses are spread into 6 groups

Group	ID	Location	Layout	Total
1	R1	Top Left	2 rows with 8 each	2*8=16
2	R2	Top Centre	2 rows with 8 each	2*8=16

3	R3	Top Right	1 row with 5	1*5=5
4	R4	Centre Left	2 rows with 7 each	2*7=14
5	R5	Bottom Left	2 rows with 8 each	2*8=16
6	R6	Bottom Centre	2 rows with 8 each	2*8=16
Total =				83

- **Apartments Layout:** The apartments are divided into 3 buildings with 7 storeys each.

Location	ID	Layout	Total
Top	A1	7 storeys with 5 apartments on each floor	7*5=35
Centre	A2	7 storeys with 4 apartments each on floors 1-5 and 5 apartments each on floors 6-7	5*4+2*5=30
Bottom	A3	7 storeys with 5 apartments on each floor	7*5=35
Total =			100

The objective is to design a network for my residential area and provide an IP addressing schema. Choose a topology to suit the residential area, find suitable cables, networking devices and provide an IP addressing schema.

LAN (Local Area Network) is typically used for a residential area whose maximum length spans for a maximum of 1km.

Network Design Necessities:

1. **Increase network availability**: Increasing network availability is a technical goal usually achieved through the implementation of network redundancy features.
2. **Security / Privacy:** The data and information shared using this network should be highly secure.
3. **Scalability:** Over time, the network requirements for an organization will change. So our design should be robust to this.

4. **Network performance**: Improving performance through the implementation of a new network or the upgrade of an existing network is another common example of a technical goal.
5. **Troubleshooting:** When a problem occurs in the network fixing it should be easy, thus the design should be simple and understandable.
6. **Cheap:** For a fixed goal, try to minimize the cost incurred.

Different Topology designs:

1) **Bus Topology:** Alternatively referred to as line topology, bus topology is a network setup where each computer and network device is connected to a single cable or backbone.

Advantages of bus topology:

1) It works well when you have a small network.

2) It's the easiest network topology for connecting computers or peripherals in a linear fashion.
3) It requires less cable length than a star topology.

Disadvantages of bus topology:

1) It can be difficult to identify the problems if the whole network goes down.
2) It can be hard to troubleshoot individual device issues.
3) Bus topology is not great for large networks.
4) Terminators are required for both ends of the main cable.
5) Additional devices slow the network down.
6) If a main cable is damaged, the network fails or splits into two.

2) **Star Topology:** Alternatively referred to as a star network, star topology is one of the most common network setups. In this configuration, every node connects to a central network device, like a hub, switch, or computer. The central network device acts as a server and the peripheral devices act as clients.

Advantages of star topology:

1) Centralized management of the network, through the use of the central computer, hub, or switch.
2) Easy to add another computer to the network.
3) If one computer on the network fails, the rest of the network continues to function normally.

Disadvantages of star topology:

1) May have a higher cost to implement, especially when using a switch or router as the central network device.
2) The central network device determines the performance and number of nodes the network can handle.
3) If the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network.

3) **Mesh Topology:** In a network setup such as ours, scalability and cost take preference over robustness and traffic control. So such a highly expensive and not easily scalable network is not recommended for a residential area like ours.

4) **Ring Topology**: In the layout of our residential area we can see that the design is quite complicated and designing a ring topology will be a tough job. Also an error in a single node can affect all the other nodes and thus is not recommended in such a setup.

The network we'll be using - Hybrid (Star + Bus): As the name suggests, this network topology is a combination of star topology and bus topology also known as tree topology. The main network cable still goes to all the row house groups and the 3 apartment buildings, but now it only connects to a switch for each group/building and not to each individual row house/apartment. This switch then connects the row houses/apartments in that particular group/building.

Advantages:

1) It provides high scalability, as leaf nodes can add more nodes in the hierarchical chain.
2) Other nodes in a network are not affected, if one of their nodes get damaged
3) It provides easy maintenance and fault identification.
4) Supported by several hardware and software vendors.
5) Point-to-point wiring for individual segments.

Disadvantages:

1) Large cabling is required as compared to star and bus topology.
2) On the failure of a hub, the entire network fails.
3) Tree network is very difficult to configure than other network topologies.

Switched Ethernet is one of the most preferred LAN technologies because each node has its own dedicated point-to-point circuit. It's better than a Hub based ethernet in many ways like privacy, efficiency etc.

Switched Ethernet vs Hub-based ethernet?:

1) Easy to setup and modify.
2) Stores information about packet occurrence/transfer time and hence makes it easier to debug.
3) Though the initial cost of a switch is higher than a hub the maintenance cost will be low and will have a long life.
4) Increases network performance drastically because there is a dedicated point-to-point circuit for every node.
5) It helps to reduce the number of broadcast domains.
6) Supports VLANs that can help in Logical segmentation of ports.
7) Switches can make use of CAM tables for Port to MAC mapping.
8) Scalable and can include newer applications.
9) The data sent to a specific node only reaches that node thus ensuring privacy of data.

High Level Architecture Choices:

1) 3-tier architecture:

Network Requirements:

a) ***Small network***: Provides services for up to 200 devices.
b) ***Medium-size network***: Provides services for 200 to 1,000 devices.
c) ***Large network***: Provides services for 1,000+ devices.

Divide into 3 areas. Core, Distribution and Access.

a) Core:

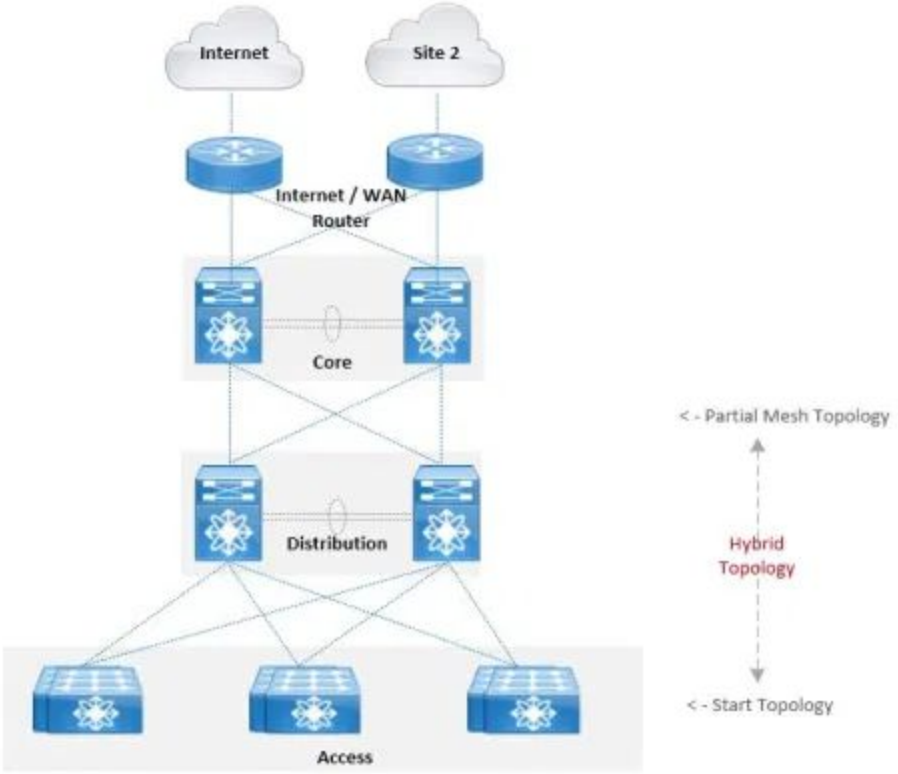
- In charge of fast routing, To get traffic as quickly as possible from one distribution switch to another distribution switch.
- Gateway to the Internet or other sites.
- The core layer also provides scalability and fast convergence.

b) Distribution:

- A multilayer sw capable doing routing. High capacity, High port speed and density.
- A layer that aggregates the server access layer, using switches to segment workgroups and isolate network problems in a data center environment.

c) Access:

- We can use L2 switch because we are not based on routing but in mac address forwarding.
- A layer that is used to grant user access to network devices.

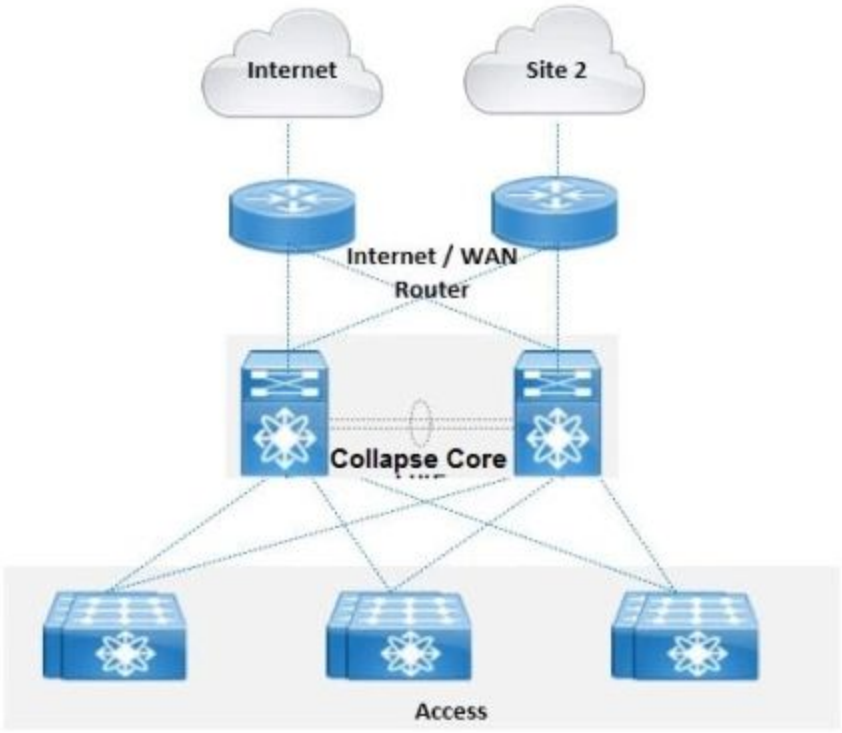


2) 2-tier architecture:

The *three-tier hierarchical design* maximizes performance, network availability, and the ability to scale the network design.

However, many small enterprise networks do not grow significantly larger over time. Therefore, a ***two-tier hierarchical design*** where the core and distribution layers are collapsed into one layer is often more practical. A

"***collapsed core***" is when the distribution layer and core layer functions are implemented by a single device. The primary motivation for the collapsed core design is reducing network cost, while maintaining most of the benefits of the three-tier hierarchical model.



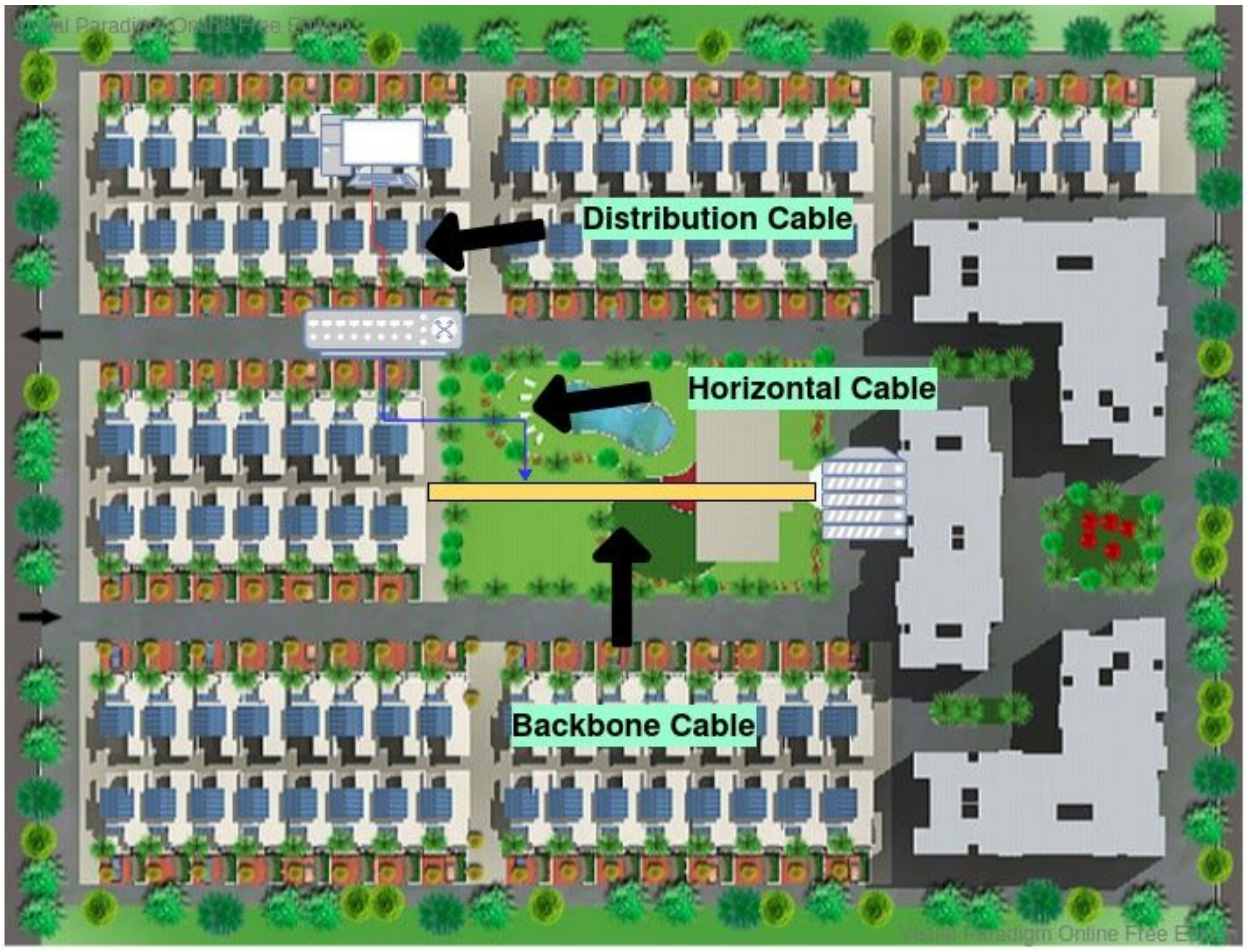
∴ We can use the 2-tier architecture in the centre building where all use a single network connection such as a Wi-fi or a common ethernet. For the row houses too we can use the 2-tier architecture as there are not many access switches and can be handled by a single distribution switch.

Cables:

Ideally we should have:

1) Consistency: Standard systems for phone, Ethernet, and ISDN cabling so that troubleshooting and cabling updates are not complicated.
2) Easy to debug: The system should be simple and traceable so that in case of an error the point of failure can be easily found and fixed.
3) Easy to modify: The tenants should be able to move around their devices at home such as printers, PCs etc.
4) Long life: Future proof or scalable, easy to add new nodes to the network.

Mainly we have 3 types of cables:



Backbone, Horizontal and Distribution as shown in the above diagram.
The Backbone cable connects the main server to the various switches of different groups/buildings.
The Horizontal cable connects the group/building switches to the switches of individual row houses/apartments.
The Distribution cable connects the row house/apartment switch to the various LAN ports in different rooms in the row houses/apartments.

The Backbone Cable is about 1km long, but only an optical cable can handle those lengths without a repeater; although it is more costly than a twisted pair, it is needed for the given length and to sustain service quality. Since the backbone cable is responsible for carrying the whole network to all nodes, it must be secure

and free of congestion and traffic. Optical fiber is chosen because it has a transmitting capacity 26,000 times greater than twisted pairs

Optical Fibers:.

1) **SMF: Single Mode Fiber:**The single mode fibers are used for transmission when the distance is very high. These cables are very expensive as they use lasers as their source.
2) **MMF: Multi Mode Fiber:** The multi mode fibers are used for lesser distances, they are cheaper and use LEDs as the source.

Backbone Cable: Since the necessary distance is just around 1 km, a Step multimode optical fiber capable of delivering up to 1Gbps over that distance can be used without much attenuation or bandwidth loss. As compared to single mode optical fiber, this is a more cost-effective approach.

Horizontal Cable: The horizontal cables linking the segment switches to the row house/apartment switches only need to be 50-100 meters long, resulting in 1000BaseT Unshielded Cat 5e twisted pair cables with a bandwidth of up to 100MHz. This is suitable for this application, since it connects to a switch that connects to a maximum of 12 homes.

Distribution cables: The transmission cables connect different rooms and ethernet ports to the villa switch and will only be a few meters long (2-8 meters). We can use a 100BaseT Unshielded Cat 5 twisted pair cable, which will accommodate up to 100 Mbps and has a maximum bandwidth of 100MHz and is cost effective.

Device Selection:

1) **Wireless Access Point:** APs are wireless network devices that act as a portal for devices to connect to a LAN. An AP is useful for extending the wireless coverage of an existing network and increasing the number of potential users. High-speed Ethernet cables run from a router to an access point, which transforms the wired signal of the router into the wireless signal of the access point. An AP is a sub-device within a LAN that provides

another location for devices to connect from, which enables more devices on the network without slowing down connectivity. A router can sometimes act as an access point, but not all access points can be routers. Each home has a WAP to connect all the devices at home like mobile phones, tablets, laptops, PCs, TVs etc to the internet. On an average there are at least 6-8 devices in a home given today's situation where everyone has a mobile phone. Thus to connect them wirelessly and give a good connection, it is good to have a strong WAP such as the D-Link DAP_2230 which has good long range coverage. It allows upto 12 users to connect at a time and provides a Multi-SSID network to divide the network for different users. It also provides maximum bandwidth of 2Gbps.

2) **Access Switches:** Access switches are placed in each group/building, each group/building contains at max of 16 houses and each needs 2 ports one for the WAP and one for direct ethernet connection, thus each access switch need to have at least 32 access ports, so we need something like the Cisco Catalyst 4232 - Switch.

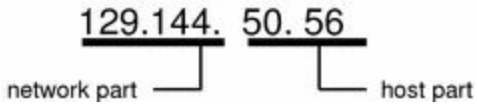
It has 32 ports with 10/100/1000BaseT configurations. It has access control to ensure network security, has a cable diagnostic function to troubleshoot wiring problems and has an optical uplink port.

3) **Distribution Switches:** Distribution switches are crucial since they handle a vast number of other access switches, which in turn handle thousands of nodes; thus, even though the switch is costly, it is best to select an expensive distribution switch that is efficient. As a result, we went with the Cisco catalyst 9300 series, which has a 480 gbps bandwidth, dual optical speeds, and leading PoE capabilities. It is energy efficient and provides PnP (Plug and Play) features, making it quick to manage and scale. Since there

are eight access switches in all, only one distribution switch is required to connect them.

4) **Router:** Finally we need a router to connect our LAN to WAN, that is by connecting the distribution switch to the WAN (internet). For this we can use the Cisco ISR 4331 2GE 2NIM 1SM. It provides DDos mitigation for the security and PoP and works on both AC and DC supplies and provides bandwidth of upto 25 Gbps.

IP Addressing Schema: Each network running TCP/IP must have a unique network number, and every machine on it must have a unique IP address. It is important to understand how IP addresses are constructed before you register your network and obtain its network number. The IP address is a 32-bit number that uniquely identifies a network interface on a machine. An IP address is typically written in decimal digits, formatted as four 8-bit fields separated by periods. Each 8-bit field represents a byte of the IP address. This form of representing the bytes of an IP address is often referred to as the **dotted-decimal format**. The bytes of the IP address are further classified into two parts: the network part and the host part. The following figure shows the component parts of a typical IP address, 129.144.50.56.



Let's assume that all devices use IPv4 addressing. We agree that by eliminating the address size restriction, we will be able to reduce the amount of wasted host addresses. This approach is also known as classless addressing, and it is preferable to classful addressing in how it allows one to define the amount of bits necessary for the address, while classful addresses have a fixed size. We have two types of addressing in IPv4:

a) **Dynamic:** It means "constantly changing." The prefix dyna means power; however, dynamic IP addresses aren't more powerful, but they can change (or be changed).
b) **Static:** It means staying the same. Static. Stand. Stable. Yes, static IP addresses don't change.

Most IP addresses assigned today by Internet Service Providers are dynamic IP addresses. It's more cost effective for the ISP and you. Static addressing is cheaper to maintain than dynamic addressing, but static addressing is less secure and only suitable for office environments. Residential areas like my area are more suited to dynamic addressing.

The 10.0.0.0 network is being subnetted and used for the internal network. The assumption is that the PAT is set up for internet access. In this network, subnetting is done mainly to reduce traffic due to broadcast messages. Additionally, any internet-related restrictions also can be affected with this subnetting. We also use VLAN. The purpose of VLANs (Done using IP addresses and port switches in certain cases) in addition to subnetting is to divide the LAN logically to implement various policies related to security, privacy and internet access.

Assuming 6-8 devices per house on average, we can say there will be at max 8 * 183 = 1464 devices. We can use the 11 bit addressing schema (2^{11} = 2048). Thus we can have 32 - 11 = 21 bit addressing for the network. Since all users in a residential area have fair access to the network, no classes in the addressing schema are required. So, assuming that 10.1.0.0/21 is our first IP address, we will have an

address over the next 2048 addresses and dynamically delegate those addresses to residents as they boot their devices and connect to the network.

References:

1) https://www.2000trainers.com/ccda-study-guide/network-design-technical-goals/
2) https://www.computerhope.com/jargon/b/bustopol.htm
3) https://www.computerhope.com/jargon/s/startopo.htm
4) https://computernetworktopology.com/tree-topology/
5) https://www.guru99.com/hub-vs-switch.html
6) https://layer3life.wordpress.com/2017/04/19/3-tier-architecture/
7) https://www.fiberplusinc.com/systems-offered/advantages-wireless-access-points/
8) https://docs.oracle.com/cd/E19504-01/802-5753/6i9g71m2o/index.html
9) https://whatismyipaddress.com/dynamic-static