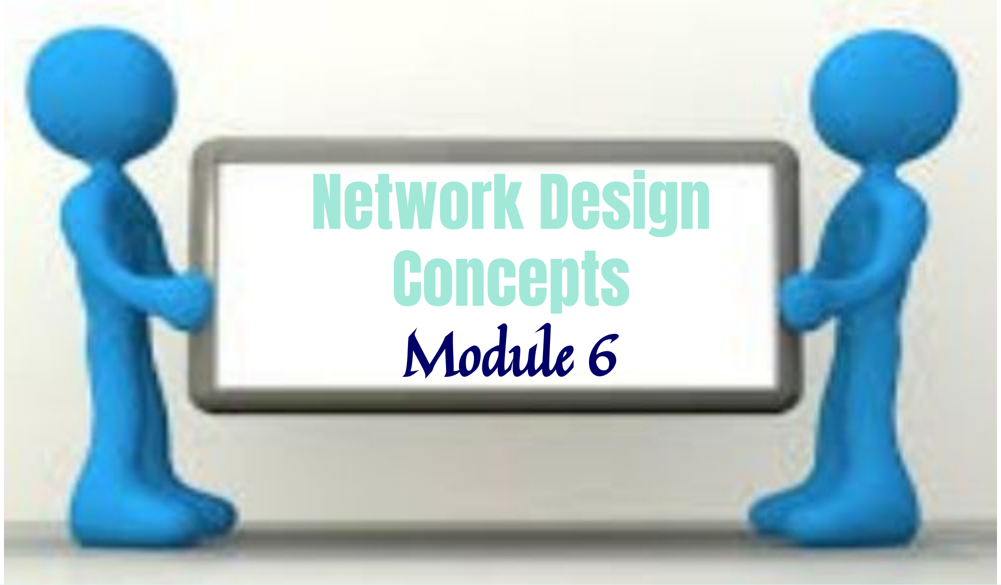


Network Design Concepts

Module 6

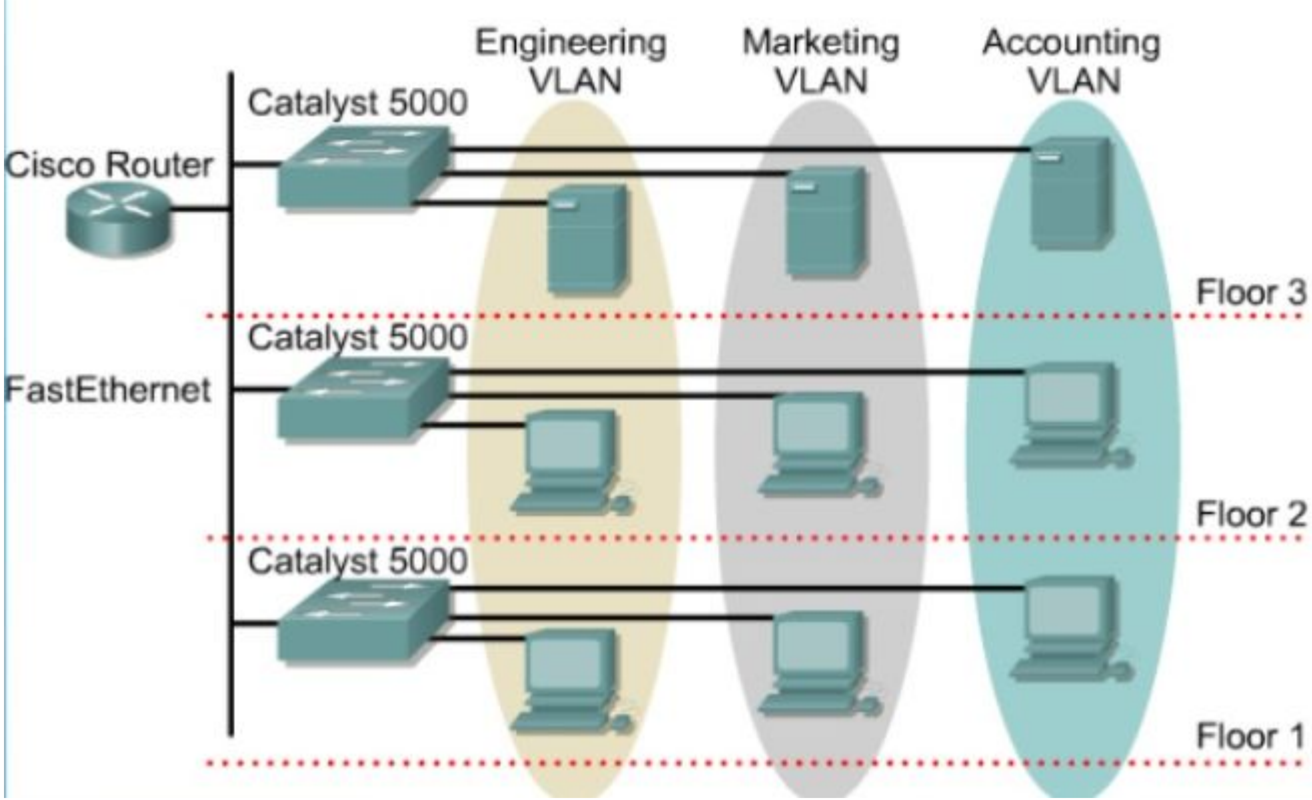
Network Design

- **Planning** of the **implementation** of a computer network infrastructure.
- Represented as a network diagram that serves as the blueprint for implementing the network physically
- Typically, network design includes the following:
  - Logical map of the network to be designed
  - Cabling structure
  - Quantity, type and location of network devices (router, switches, servers)
  - IP addressing structure
  - Network security architecture and overall network security processes

VLAN (Virtual LAN)

- A VLAN is a group of network services **not restricted** to a **physical segment** or LAN switch.
- Configuration or reconfiguration of VLANs is done through **software**.
- VLANs increase overall network performance by **logically grouping** users and resources together.
- VLANs are powerful tools for network administrators.
- A group of users needing high security can be put into a VLAN so that no users outside of the VLAN can communicate with them

Eg:


Engineering VLAN
Marketing VLAN
Accounting VLAN
Catalyst 5000
Cisco Router
Floor 3
Catalyst 5000
FastEthernet
Floor 2
Catalyst 5000
Floor 1

Why VLAN?

Virtual is Better than Real

- Location-independent
    - Marketing LAN can be all over the building
- Users can move but not change LAN
- Traffic between LANs is routed
    - Better to keep all traffic on one LAN
    - Reduce latency and traffic on a network
- Better security

VLAN Types

Static VLANs:

- The switch port that you assign a VLAN association to always maintains that association until an administrator manually changes that port assignment.

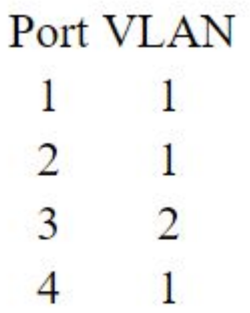
Dynamic VLANs:

- Are created through network management software.
- CiscoWorks 2000 or CiscoWorks for Switched Internetworks is used to create Dynamic VLANs.
- Allow for membership based on the MAC address of the device connected to the switch port.

Types of VLAN's

1) Layer 1 VLAN: Membership by Port

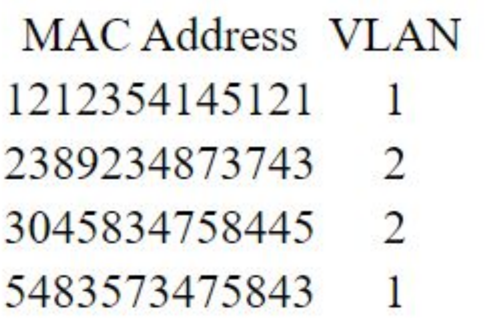
- Membership in a VLAN can be defined based on the ports that belong to the VLAN.
- Eg: In a bridge



Port	VLAN
1	1
2	1
3	2
4	1

- The main disadvantage of this method is that it does not allow for user mobility. If a user moves to a different location away from the assigned bridge, the network manager must reconfigure the VLAN.

2) Layer 2 VLAN: Membership by MAC Address



MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

- Here, membership in a VLAN is based on the MAC add
- The switch tracks the MAC addresses which belong to each VLAN
- Since MAC addresses form a part of the workstation's network interface card, when a workstation is moved, no reconfiguration is needed to allow the workstation to remain in the same VLAN. This is unlike Layer 1 VLAN's where membership tables must be reconfigured.
- The main problem with this method is that VLAN membership must be assigned initially. In networks with thousands of users, this is no easy task

3)Layer 2 VLAN: Membership by Protocol Type

4)Layer 3 VLAN: Membership by IP Subnet Address

How does VLAN work?

- When a LAN bridge receives data from a workstation, it tags the data with a VLAN identifier indicating the VLAN from which the data came. This is called **explicit tagging**.
- It is also possible to determine to which VLAN the data received belongs using **implicit tagging**. In implicit tagging the data is not tagged, but the VLAN from which the data came is determined based on other information like the port on which the data arrived.
- To be able to do the tagging of data using any of the methods, the bridge would have to keep an updated database containing a mapping between VLAN's and whichever field is used for tagging, called a **filtering database.**

- Bridges would have to be able to maintain this database and also to make sure that all the bridges on the LAN have the same information in each of their databases.
- The bridge determines where the data is to go next based on normal LAN operations.
- Once the bridge determines where the data is to go, it now needs to determine whether the VLAN identifier should be added to the data and sent.
- If the data is to go to a device that knows about VLAN implementation (VLAN-aware), the VLAN identifier is added to the data. If it is to go to a device that has no knowledge of VLAN implementation (VLAN-unaware), the bridge sends the data without the VLAN identifier.

Disadvantages

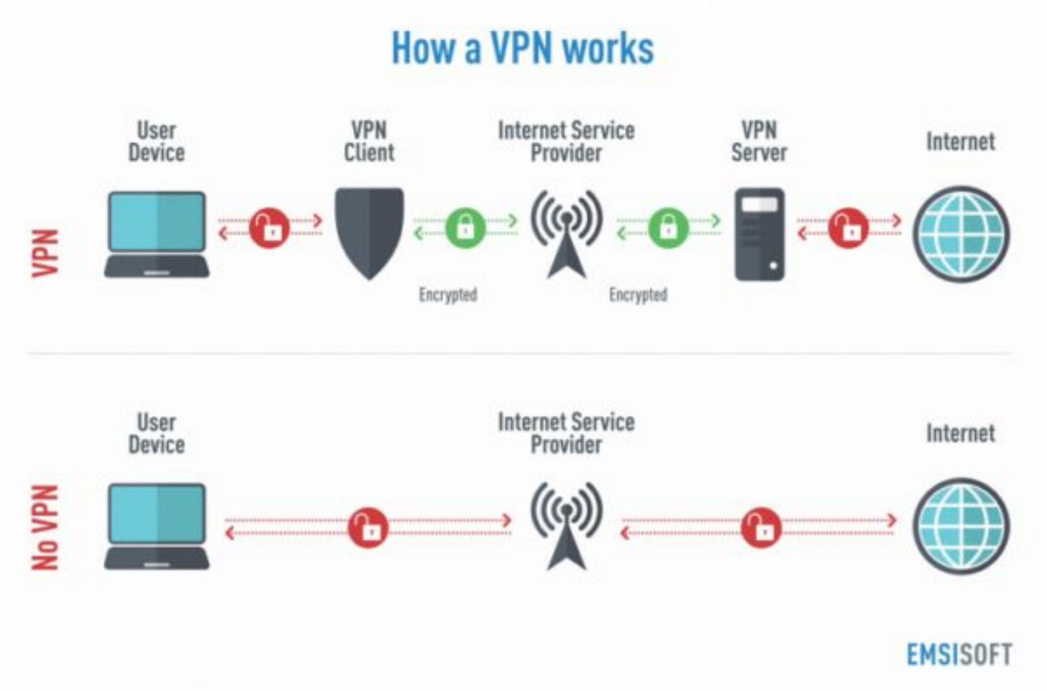
- High risk of virus issues because one infected system may spread a virus through the whole logical network
- Equipment limitations in very large networks because additional routers might be needed to control the workload
- More effective at controlling latency than a WAN, but less efficient than a LAN

VPN (Virtual Private Network)

- VPN, or Virtual Private Network, allows you to create a secure connection to another network over the Internet.
- VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi, and more.
- VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable.

How does VPN work?

- Encrypted VPN connection



Types of Virtual Private Network (VPN)

- **Remote Access VPN:**
  - Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely.
  - The connection between the user and the private network occurs through the Internet and the connection is secure and private.
  - Remote Access VPN is useful for home users and business users both.

- **Site to Site VPN:**
  - A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies.
  - Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.
- **Intranet based VPN:** When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
- **Extranet based VPN:** When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

Advantages

- Protect your online identity
- Secure online connections
- Prevent bandwidth throttling
- Bypass geo-blocking
- Bypass firewall

Disadvantages

- Sometimes slow internet speed
- Quality VPN is costly
- VPN blocker technology exists
- Not built for all devices

Difference between VLAN and VPN

- A VLAN helps group workstations that are **not within the same locations** in the same broadcast domain and VPN is related to **remote access** to a company’s network.
- VLAN is a **subcategory of VPN** and VPN is a means to create a secure network for secure data transmission.
- A VLAN is basically a means to logically **segregate networks without physically segregating** them with multiple switches. A VPN is used to connect two points in a **secure and encrypted tunnel**.

- A VPN keeps the data from prying eyes while it is in transit and no one in the network can capture the packets and read the data. The VLAN does not involve any **encryption technique,** but it is only used to divide your logical network into different sections for administration and security purposes.
- The VLAN is usually used when it is necessary for a person to connect with someone who can not be connected from outside the VLAN. It requires a special permission before access. VPN is used to communicate securely in an unsecured environment

Design Rules and Considerations

- The network should **stay up all the time**, even in the event of failed links, equipment failure, and overloaded conditions.
- 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 be **easy** to modify to **adapt** to network growth and general business changes.
- Because failures occasionally occur, **troubleshooting** should be easy. Finding and fixing a problem should not be too time-consuming

Fundamental Design Goals

- **Scalability**:
  - Scalable network designs can grow to include new user groups and remote sites and can support new applications without impacting the level of service delivered to existing users.
- **Availability**:
  - A network designed for availability is one that delivers consistent, reliable performance, 24 hours a day, 7 days a week. In addition, the failure of a single link or piece of equipment should not significantly impact network performance.

- **Security**:
    - Planning the location of security devices, filters, and firewall features is critical to safeguarding network resources.
- **Manageability**:
    - Easy to manage and support the network. A network that is too complex or difficult to maintain cannot function effectively and efficiently.
- **Performance**:
    - Adequate Response time, latency, throughput measures

Fundamental Design Factors

- What kind of topology?
  - Cable - type, length of cable, time to setup, cost, maintenance
- Cost - Maintenance + Overhead Cost
- Scalability
- Topology and Transmission Meida
- Create a Network Topology - Visual simulation
- Router
  - Various capability - Firewall, VPN, IP phone
- Switches
  - Managed and Unmanaged Switches

- Planning IP Address
    - private/ public addressing
    - No of hosts required: Addressing plan
- Routing Protocol
    - Commonly used OSPF and EIGRP
        - EIGRP-
            - Hybrid protocol with DV and LS
            - Suitable for all kind of networks except dial up
        - OSPF
            - Based on LS
            - Suitable for all kind of networks including dial up

Problems

1. Given 2 address and mask

   Device A: 172.16.17.30/20

   Device B: 172.16.28.15/20

   Mask : 255.255.240.0

   Determine if these devices are on the same subnet or different subnets?

Solution

Determining subnet for device A:

172.16.17.30	10101100.00010000.00010001.00011110
255.255.240.0	11111111.11111111.11110000.00000000
Subnet =	10101100.00010000.00010000.00000000 = 172.16.16.0

Looking at the address bits that have a corresponding mask bit set to one, and setting other address bits to zero (this is equivalent to performing a logical 'AND' between the may address), shows you to which subnet this address belongs. In this case, device A belongs tol 172.16.16.0.

Determining the subnet for device B:

72.16.28.15 10101100.00010000.00011100.00001111

255.255.240.0 11111111.11111111.11110000.00000000

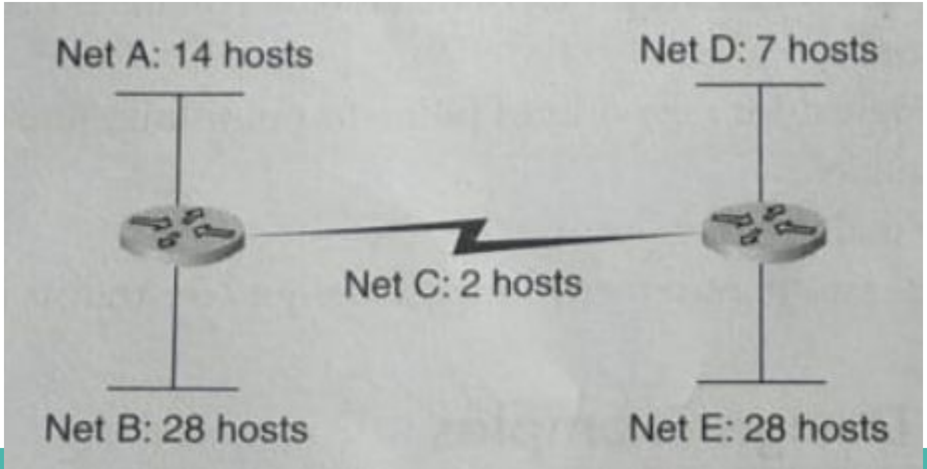
Subnet = 10101100.00010000.00010000.00000000 = 172.16.16.0

device B belongs tol 172.16.16.0.

Device A and device B have addresses that are part of the same subnet

2.

Given the Class C network of 204.15.5.0/24, subnet the network in order to create the network shown in Fig with the host requirements shown. Looking at the network shown in Fig. 9,3, you can see that you are required to create five subnets. The largest subnet must support 28 host addresses. Is this possible with a Class C network? If so, how?



Solution

To create the five needed subnets, you would need to use three bits from the Class C host bits.

Leaves you with 5 bits for the host address, no of hosts that can be accommodates are 2^5= 32 (30 usable). This meets the requirement. Therefore, you have determined that it is possible to create this network with a Class C network.

An example of how you might assign the subnetworks is provided as follows:
Net A: 204.15.5.0/27 host address range 1 to 30
Net B: 204.15.5.32/27 host address range 33 to 62
Net C: 204.15.5.64/27 host address range 65 to 94 t
Net D: 204.15.5.96/27 host address range 97 to 126
Net E. 204.15.5.128/27 most address range 129 to 158

3.

An ISP is granted a block of CIDR addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:

a. The first group has 64 customers; each needs 256 addresses.

b. The second group has 128 customers; each needs 128 addresses.

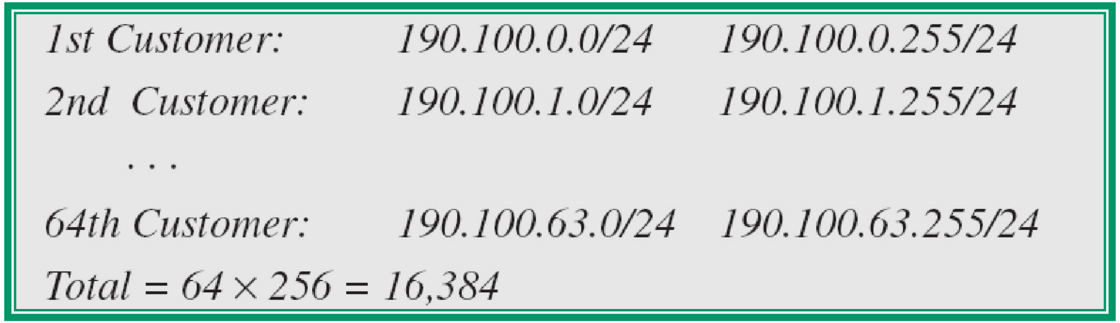
c. The third group has 128 customers; each needs 64 addresses.

Design the subblocks and find out how many addresses are still available after these allocations.

Solution

- *Group 1*

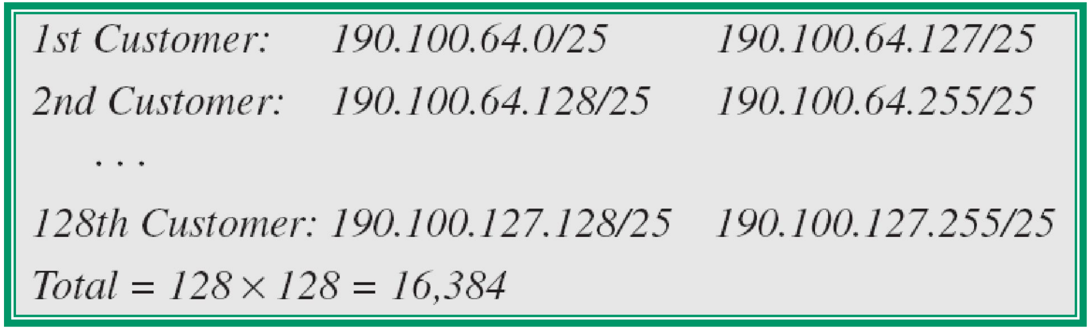
For this group, each customer needs 256 addresses. This means that 8 (log2 256) bits are needed to define each host. The prefix length is then 32 − 8 = 24. The addresses are



1st Customer:	190.100.0.0/24	190.100.0.255/24
2nd Customer:	190.100.1.0/24	190.100.1.255/24
. . .		
64th Customer:	190.100.63.0/24	190.100.63.255/24
Total = 64 × 256 = 16,384		

- *Group 2*

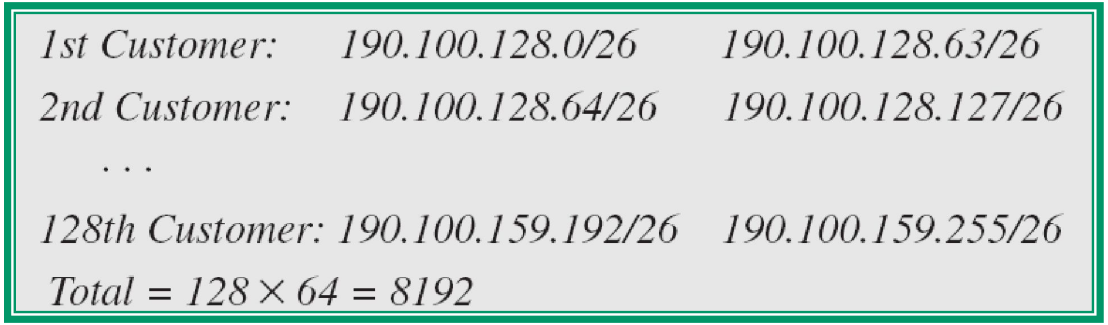
For this group, each customer needs 128 addresses. This means that 7 (log2 128) bits are needed to define each host. The prefix length is then 32 − 7 = 25. The addresses are



1st Customer:	*190.100.64.0/25*	*190.100.64.127/25*
2nd Customer:	*190.100.64.128/25*	*190.100.64.255/25*
. . .		
128th Customer:	*190.100.127.128/25*	*190.100.127.255/25*
Total = 128 × 128 = 16,384		

- *Group 3*

For this group, each customer needs 64 addresses. This means that 6 ($\log_2 64$) bits are needed to each host. The prefix length is then 32 − 6 = 26. The addresses are



1st Customer:	190.100.128.0/26	190.100.128.63/26
2nd Customer:	190.100.128.64/26	190.100.128.127/26
. . .		
128th Customer:	190.100.159.192/26	190.100.159.255/26
Total = 128 × 64 = 8192		

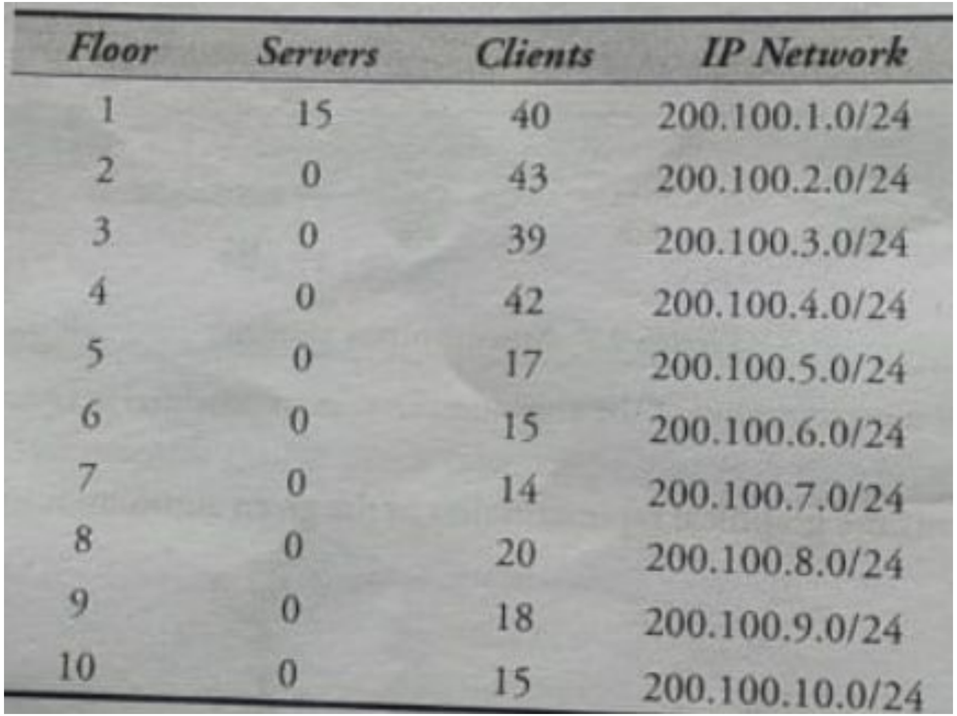
- *Number of granted addresses to the ISP: 65,536*
- *Number of allocated addresses by the ISP: 40,960*
- *Number of available addresses: 24,576*

Case Study

Mr. XYZ, IT Manager at the National Hospital, is responsible for running the network. Mr. XYZ has to suggest a network plan that fits the needs of the patient. The hospital is on the rise and management has provided funding for the growth of the network. Health professionals would like to be able to access communication systems using laptops in all patient rooms. Doctors and nurses will be able to view medical history, X-rays, medicines and the latest health information. Mr. XYZ bought new computers and installed them in a data centre. The wireless LAN (WLAN) has more than 30 laptops and an additional 15 are expected in 6 months. The computers should have a high degree of capacity. (contd)

Patient rooms are situated on the 6th and 10th floors of the hospital complex. Doctors should be able to manage and access the network from every level. A radio frequency analysis suggests that a single access point situated in each communication wardrobe can penetrate all rooms at each floor. The new network has 10 segments that enter a central router that also covers the Internet. Routing information protocol version 1 (RIPv1) runs the router. The back-end modern servers are housed in the same section as the ones used on the first level. Mr. XYZ points out that consumers worried about bad connectivity to the site. (contd)

The latest IP addresses is listed in Table



Floor	Servers	Clients	IP Network
1	15	40	200.100.1.0/24
2	0	43	200.100.2.0/24
3	0	39	200.100.3.0/24
4	0	42	200.100.4.0/24
5	0	17	200.100.5.0/24
6	0	15	200.100.6.0/24
7	0	14	200.100.7.0/24
8	0	20	200.100.8.0/24
9	0	18	200.100.9.0/24
10	0	15	200.100.10.0/24

Proposal

Mr. XYZ would like a proposal to update the network with simple switches and to allow quicker connections to the servers. The plan would also protect secure WLAN connectivity on floors 6 to 10. Include an IP address scheme that reduces the number of ClassC networks used by the hospital. Mr. XYZ aims to reduce the number of networks authorized by the ISP.

The following questions refer to this case study:

1. What are National Hospital's business requirements?

Answer The hospital needs to provide access to patient records, prescriptions, and information from patient rooms.

2. Are there any business-cost constraints?

Answer No cost restrictions were discussed.

3. What are the network's technical requirements?

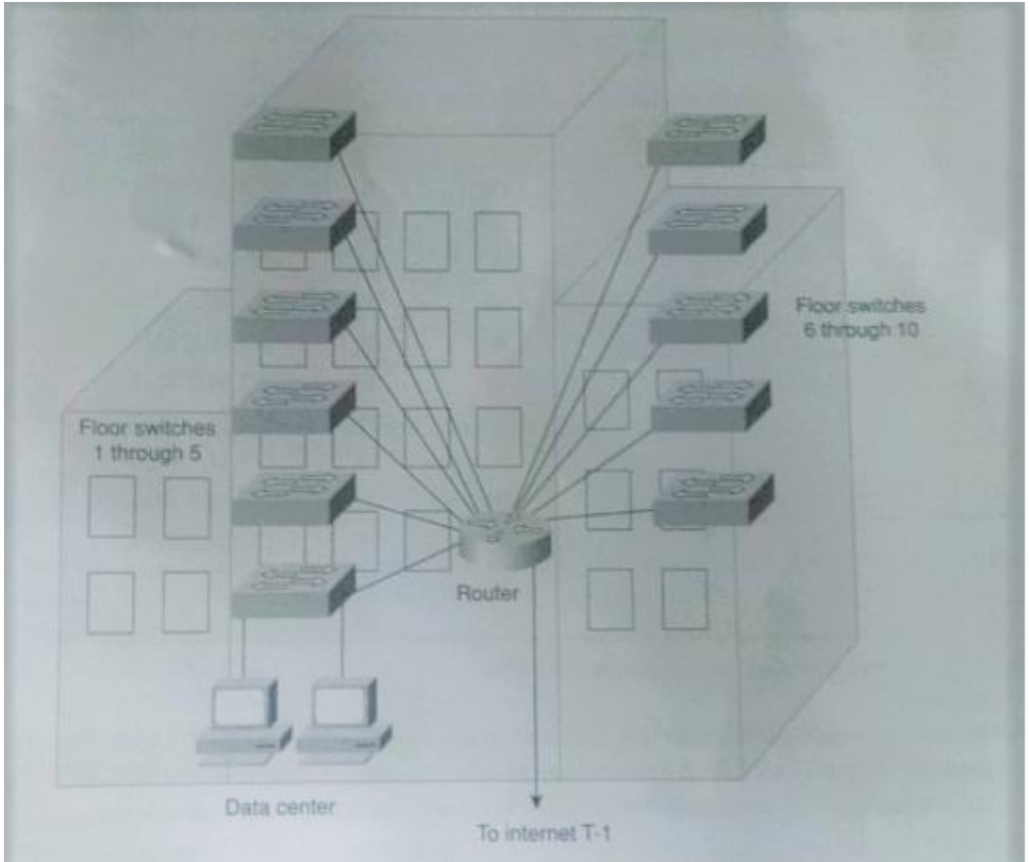
Answer The technical requirements are as follows: WLAN access from rooms on floors 6 through 10 redundant access to servers in the data centre. Fast switching between LAN segments.

4. What are the network's technical constraints?

Answer The technical constraint is as follows: Servers must be located in the first-floor data-centre rooms.

5. Prepare a logical diagram of the current network.

Answer Logical diagram for National Hospital current network is shown i



6. Does the hospital use IP addresses effectively?

Answer The hospital does not use IP addresses effectively. It uses Class C networks on each floor. Each floor wastes more than 200 IP addresses, because each Class C network provides up to 254 IP addresses.

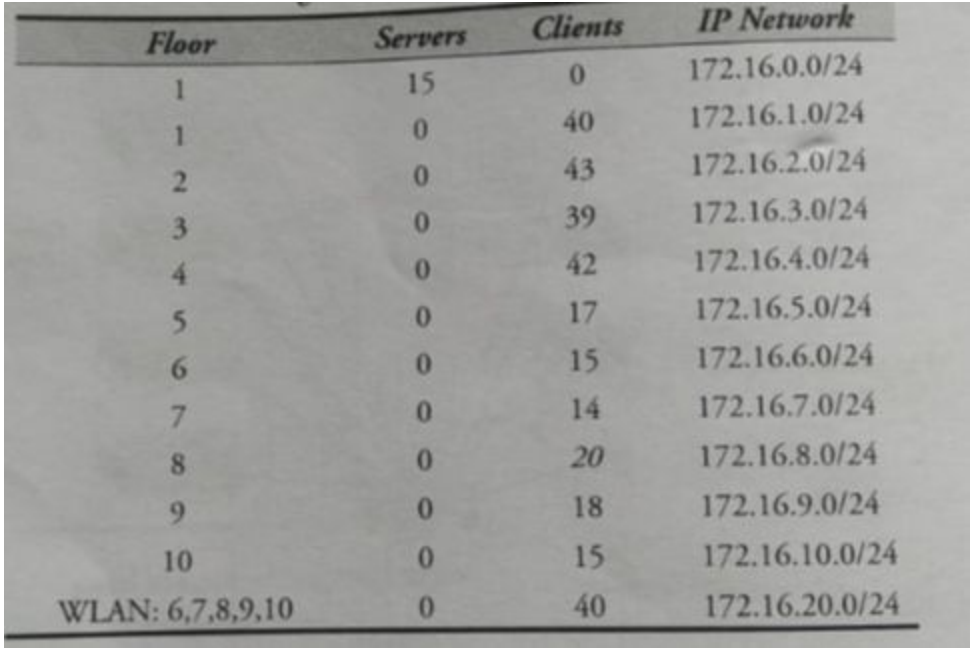
7. What would you recommend to improve the switching speed between floors?

Answer Recommend using a high-speed Layer 3 switch for the building LANs. They can use the router for Internet and WAN access.

8. Based on the number of servers and clients provided, what IP addressing scheme would you propose? Answer The primary recommendation is to use private addresses for the network. Using private addresses has been a best-practice policy for private internal networks.

With private addresses, the hospital could release eight of the Class C networks to the ISP, retaining two for ISP connectivity. With private addresses, the hospital can choose to use 172.16.0.0/16 for private addressing. Table (nxt slide) lists the addressing scheme using sufficient private address space for each network

IP Addressing Scheme Using Private Addresses



Floor	*Servers*	*Clients*	*IP Network*
1	15	0	172.16.0.0/24
1	0	40	172.16.1.0/24
2	0	43	172.16.2.0/24
3	0	39	172.16.3.0/24
4	0	42	172.16.4.0/24
5	0	17	172.16.5.0/24
6	0	15	172.16.6.0/24
7	0	14	172.16.7.0/24
8	0	*20*	172.16.8.0/24
9	0	18	172.16.9.0/24
10	0	15	172.16.10.0/24
WLAN: 6,7,8,9,10	0	40	172.16.20.0/24

9. What routing protocols would you recommend?

Recommend routing protocols that support variable-length subnet masks (VLSM). The nests tall. Recommend RIPv2 or enhanced interior gateway routing protocol (EIGRP). Do not recommend (OSPF) because of its configuration complexity.

10. Draw the proposed network solution

(Nxt Slide)

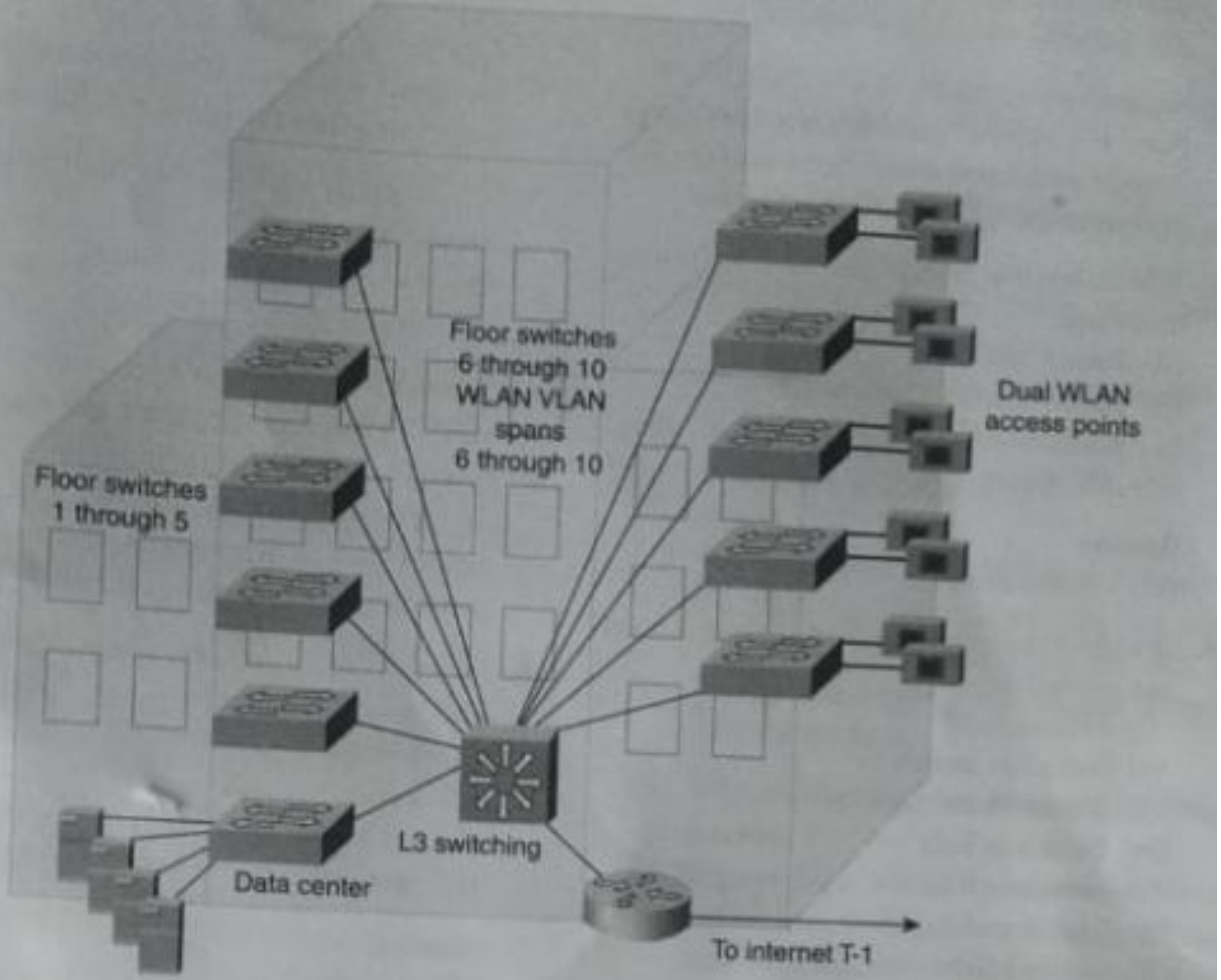


Figure 9.18: Network