Architecture, Operating Systems & Networking Report CA3

TU259

<Yuanshuo Du>

<D22125495>

School of Computer Science
TU Dublin – City Campus

<20230423>

Table of Contents

Content

Declaration

I hereby declare that the work described in this report is, except where otherwise stated, entirely my own work and has not been submitted as an exercise for a degree at this or any other university.

Signed:

_______Yuanshuo Du__________________

<Student Name>

<2023/04/23>

1. Chapter 1 - Introduction

1.1. Introduction to the project and its objectives

The project objective is to design and implement a local area network (LAN) for an e-commerce company. The project's primary goal is to provide a reliable and high-performance network infrastructure that can support the training center's requirements. To achieve this goal, we will need to research and choose the appropriate network components and create a subnet plan to improve network performance. A DHCP server will also be necessary to manage network devices. Finally, we will document all our research and solutions in a project report.

Additional features can be added to the project if desired to improve its functionality and efficiency.

1.2. Overview of the company and the building and the network requirement

The scenario is that an e-commerce company has decided to create a graduate training center in Dublin to offer programming training to new employees. The building purchased by the company will include two computer labs with 10 desktop PC's each and 20 additional wall jacks, one conference room with 50 seat capacity, and one open plan office area for permanent staff with 30 desks.

The network plan requirement should include a network diagram, appropriate components for the LAN, a subnet plan to increase network performance, and a DHCP server to manage network devices. Additionally, WiFi should be provided in all room locations, and any additional features can be introduced if desired. The objective of the project is to provide a network plan and design that will meet the requirements of the new business project.

1.3. Summary of brief

The first chapter, the introduction, will discuss the project's background and objectives, as well as provide an overview of the project. The second chapter, background research, will primarily investigate the usage, benefits, and advantages of various network equipment, comparing the roles of different network devices in the network.

Chapter three will focus on the selection of network equipment components in this project, including switches, routers, cables, and access points. It will conduct in-depth research and provide specific model recommendations, as well as the reasoning behind the choices.

Chapter four will cover network design, including network diagrams and layouts, along with descriptions of the diagrams. Additionally, it will address security considerations. Chapter five will discuss subnet planning design. To begin, the relevant terminology related to subnets will be studied, followed by a step-by-step subnet design plan.

Chapter eight emphasizes additional features, including redundancy, VLANs, Quality of Service (QoS), Network Access Control (NAC), Power over Ethernet (PoE), and more. The final chapter will provide a summary of the project and implementation recommendations.

2. *Background Research*

2.1. The LAN concept and its significance in the project

A local area network (LAN) is a network of computers and devices that share a common communication line or wireless connection to a server in a specific geographic area. LANs can vary in size, from a single user home network to an enterprise network with thousands of users and devices in an office or school. These computers in a LAN connect to each other through TCP/IP Ethernet or Wi-Fi(Andrew Froehlich, 2023).

The significance of LAN lies in its ability to enable communication between devices in a small area, such as a building or group of buildings, which allows users to share resources like printers, files, and applications. Compared to wide area networks (WANs), which cover larger geographic areas, LANs are faster because they cover a smaller area(comptia.org, 2023).

A LAN offers several advantages, including the ability to share resources like printers, files, and applications, faster data transfer rates, increased security, reduced cost of hardware and software, and easier communication between devices. These benefits are particularly relevant to an e-commerce company in Dublin as it requires connectivity between all devices in its building. By using a LAN, the company can ensure that all employees have access to necessary resources and information to complete their work efficiently, especially in the context of programming training.

The LAN will allow for the two computer labs, conference room, and open plan office area to be connected to each other and to the internet, enabling the transfer of data, sharing of resources, and communication between the devices. Additionally, the use of a LAN will allow for the implementation of a DHCP server, which will help manage the network devices, making it easier to configure and maintain the network.

Furthermore, the LAN will provide a foundation for the implementation of other network features and services such as security measures, centralized management, and data backup and recovery.

2.2. Creating a LAN

There are various phases involved in setting up a Local Area Network (LAN). The first step is to identify the purpose and scope of the LAN(Kim Staples, 2017). This includes determining the LAN's intended function, the number of users/devices it will support, and the physical space it will occupy. This information will aid in the selection of the best network topology and hardware components.

The proper network topology can be chosen once the purpose and scope have been identified. There are several topologies to choose from, including star, ring, bus, and mesh topologies. The topology chosen should be based on the network's requirements and budget.

Following the selection of the network topology, the appropriate hardware components, such as routers, switches, hubs, and network interface cards (NICs), might be chosen(Yaffet Meshesha, 2022). These components will aid in the development of the infrastructure required to support the LAN.

The following stage is to configure the LAN infrastructure, which includes installing network hardware, cabling, and other infrastructure components required to support the LAN. To guarantee that the infrastructure is properly set up, this step demands careful planning and attention to detail.

Once the infrastructure is in place, network settings for each device on the LAN, such as IP addresses, subnet masks, and gateway addresses, must be established. These settings aid in recognising and talking with each network device.

File and printer sharing, which allows users to access and share files and printers across the network, must also be configured(Mitch Harris, 2023). This phase entails establishing each device's settings to allow for file and printer sharing.

After configuring the LAN, it is critical to test it to ensure that it is operationally sound(Mitch Harris, 2023). Checking network connectivity, file and printer sharing, and security settings are all part of this process. Any difficulties that develop during testing should be fixed before deploying the LAN.

Finally, to maintain optimal performance and security, regular maintenance and troubleshooting are required. Updating software and firmware, monitoring network traffic, and generating routine backups are all part of routine maintenance. Troubleshooting entails locating and resolving any problems that develop, such as connectivity or performance concerns.

2.3. Switches

A switch is a crucial networking hardware device that connects computers and servers to each other within a network(Cisco, 2023c). Acting as a traffic cop at a busy intersection, the switch directs data packets to their intended destination while preventing traffic from interfering with each other. Connected devices can send data packets to the switch directly, or indirectly through a network element like a hub or router. Regardless of how they arrive, the switch can transfer data packets between connected devices directly, or forward them to a router if the destination is further away. With multiple ports, computers can be plugged into the switch and easily connect to the network(tutorialspoint.com, 2023).

When compared to network hubs, switches provide a significant improvement in traffic congestion and security. Hubs allow multiple devices to connect to a single port on a router, but all connected devices receive all data packets, creating unnecessary traffic and security risks.(Cisco, 2023c) Switches solve this problem by keeping track of the MAC addresses of connected devices and sending packets only to their intended destinations, reducing congestion and improving security.

Furthermore, switches differ from routers in that they connect devices within a LAN using MAC addresses, while routers connect LANs to other networks or the internet using IP addresses(Cisco, 2023c). While switches have evolved to perform more functions beyond just connecting devices, they remain a core component of network infrastructure. Modern switches act as both switches and routers, with built-in security capabilities that previously required dedicated firewalls. They can supply devices with power, incorporate machine learning, and act as network sensors, collecting data to help network engineers make informed decisions. With even more advancements expected, switches will continue to increase efficiency in data transmission across IT networks.

A core switch is different with normal switch is that core switch is a high-capacity switch generally located within the backbone or physical core of a network. It serves as the gateway to a wide area network (WAN) or the Internet. It is designed to handle high-bandwidth and mission-critical data transmission between different networks.

2.4. Routers

According to Cisco, Routers are networking devices that receive and send data on computer networks(Cisco, 2023b). Unlike network hubs or switches, routers connect networks together and can combine the functions of these components to improve Internet access or create business networks. They use IP addresses to route data packets between different networks, such as connecting a LAN to the internet(javatpoint, 2023). This allows devices on different networks to communicate with each other. Routers can also perform other functions, such as providing security through firewalls, managing network traffic to ensure optimal performance, and supporting virtual private networks (VPNs) to allow remote access to a private network. Routers are an essential component of modern networks and are used in homes, businesses, and data centers.

Routers act as "traffic cops" for business networks, act as intermediaries between various computer networks(Cisco, 2023a). They are responsible for directing data packets between networks and ensuring that the information is delivered to the correct destination. Routers are also capable of translating different types of network protocols and media formats, making it possible for devices using different technologies to communicate with each other.

Routers play a critical role in ensuring that a business network operates smoothly. They are responsible for connecting devices like computers, printers, and servers to the network, allowing them to communicate and share resources. Routers also analyze the data sent over the network and determine the most efficient path for it to take, ensuring that it arrives at its destination quickly and reliably.

In addition to their networking functions, routers also provide important security features that protect business networks from external threats. By controlling access to the network and monitoring traffic, routers can prevent unauthorized access to sensitive data and prevent cyber attacks. Furthermore, routers can prioritize traffic on the network, ensuring that critical applications and devices receive the necessary resources to function properly.

In terms of type of routers, routers can be classified into different types based on their functions and features. Wired and wireless routers are commonly used in homes and small offices. Wired routers use cables to share data and create wired LANs, while wireless routers use antennas to create wireless LANs(Cisco, 2023a). Edge routers are placed at the edge of networks and distribute data packets between one or more networks. Core routers, on the other hand, distribute data packets within networks and serve as the backbone of a network(Cisco, 2023a). Virtual routers are software-based and allow computers and servers to act as routers(Cisco, 2023a). They offer flexibility and scalability and can help set up remote offices on a network more quickly.

2.5. Cabling

Cabling involves a group of wires made of copper or glass that connects computers and other network components, allowing them to communicate and create a computer network(NetworkEncyclopedia, 2023). These network cables transfer data between different network components such as routers, switches, and storage area networks. Essentially, network cabling is the medium that facilitates the transfer of information between devices on a computer network(Dr. Roy Winkelman, 2013).

Network cables are a crucial component of any computer network, as they allow for the transfer of data and information between network devices. There are various types of network cables available, each suited to different network topologies, protocols, and sizes(tevelec.com, 2023). The three most common types of network cables are coaxial cable, twisted pair cable, and fiber-optic cable.

Coaxial cables are typically used for cable television systems and for connecting computers on a local area network (LAN). These cables consist of a copper wire wrapped in insulation, which is then covered by a second layer of insulation and a metal shield. The metal shield helps to reduce interference and noise from other devices, ensuring that data can be transferred without interruption(Networkhunt.com, 2023).

Twisted pair cables, on the other hand, are used for telephone systems and for connecting computers on a LAN. These cables consist of two insulated copper wires twisted together, which helps to reduce electromagnetic interference from other devices. Twisted pair cables come in two types: shielded and unshielded. Shielded cables have an additional layer of insulation that provides extra protection from interference.

Fiber-optic cabling is used for high-speed data transmission over long distances(Networkhunt.com, 2023). These cables use tiny strands of glass or plastic to transmit data using light pulses. Fiber-optic cables offer several advantages over other types of cabling, including faster data transfer speeds, greater bandwidth, and immunity to electromagnetic interference. However, they are also more expensive and fragile than other types of cabling.

2.6. Network Speed

Network speed is the measure of the data rate that a network connection or interface can support. It reflects the total capability of the connection, and the higher the capacity, the better the network performance is likely to be(Bradley Mitchell, 2020).

The type of cable used in a network can have a significant impact on its speed and performance. Different types of cables have different capabilities in terms of bandwidth, data transfer rates, and distance limitations(Kevin Parrish, 2023).

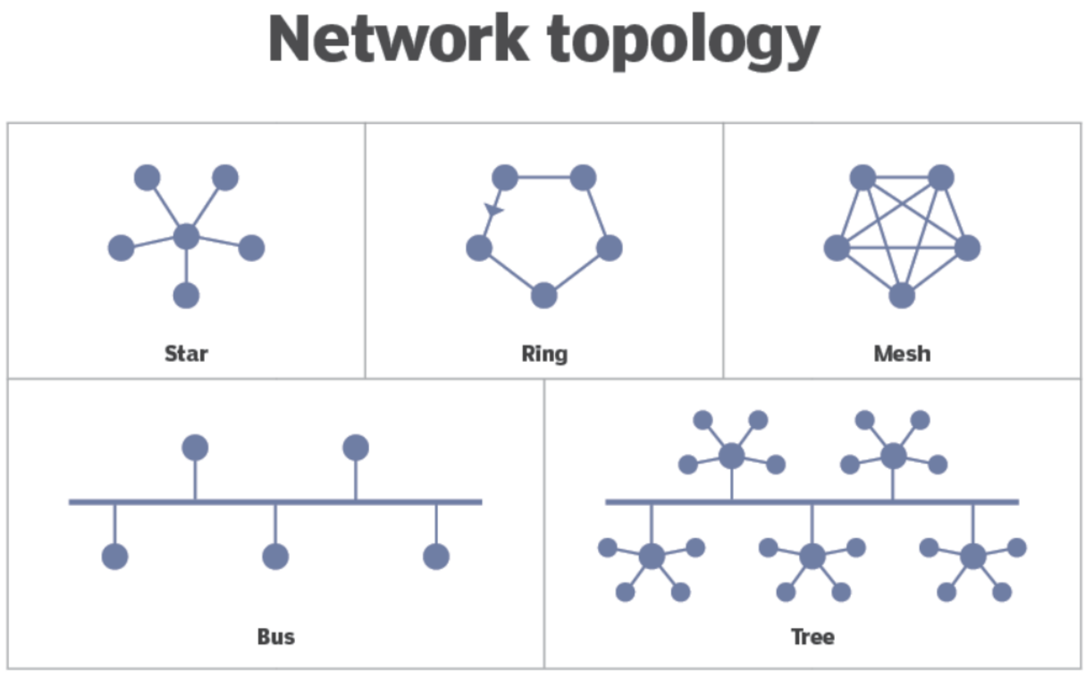
Coaxial cables, for example, have a relatively limited bandwidth and data transfer rate compared to twisted pair or fiber-optic cables. This means that data transfer speeds may be slower over longer distances or when transferring large amounts of data.

Twisted pair cables can provide higher bandwidth and data transfer rates than coaxial cables, and are more commonly used in LANs(Brian Nadel, 2020). However, their performance can be affected by electromagnetic interference (EMI) and radio frequency interference (RFI), which can reduce the quality of the signal and cause data errors.

Fiber-optic cables have the highest bandwidth and data transfer rates of all cable types, and are ideal for long-distance data transmission(BBC, 2023b). They are also immune to EMI and RFI, and provide high levels of security because they do not radiate electromagnetic signals. However, they are more expensive than other cable types and require specialized equipment for installation and maintenance.

2.7. Topologies

Network topology refers to the physical and logical arrangement of a network that describes how different nodes, switches, and routers are interconnected and how data flows. There are two types of network topologies: physical and logical. Physical topology represents the actual connections, wires, and cables in a network, while logical topology shows how data moves within a network, irrespective of physical connections(Cisco, 2023d).



(Network topology from techtarget.com(Andrew Froehlich, 2023))

A network topology is important for enhancing user experience and optimizing performance to fulfill business needs(Alexander S. Gillis, 2023b). Software programs with pre-built templates and symbols for network elements can be used to diagram network topologies, which can help identify bottlenecks and troubleshoot problems. When designing network topologies, considerations such as the network's purpose, performance needs, scalability, and redundancy requirements must be taken into account. Physical topologies are not as agile as logical topologies, which can be easily reconfigured to meet changing requirements by defining and enforcing fields in packet headers. However, physical topologies require more security measures as they rely on physical connections(Cisco, 2023d).

2.8. IP addressing

An IP address is a number that is used to identify a device on an IP network(Julio Jiminez, 2023). The address is made up of 32 binary bits that can be divided into a network piece and a host portion using a subnet mask(Julio Jiminez, 2023). The 32 binary bits are divided into four octets (one octet equals eight bits).

When a device connects to a network, it is assigned a unique IP address. This address is made up of four groups of up to three numbers, each having a maximum value of 255, separated by dots(BBC, 2023a).

In terms of main functions of an IP address. First, it is used to identify a specific machine, much like having a unique name. Second, it is used to provide the machine's location, similar to having a physical residential or commercial address(Samatha Bhargav, 2021). An IP address has two purposes: it identifies the host, or more specifically its network interface, and it specifies the host's position in the network, and hence the ability to construct a path to that host(ASTRA, 2022).

2.9. DHCP

DHCP is an abbreviation for Dynamic Host Configuration Protocol. It is a network management protocol that assigns an IP address to any device or node on a network so that it can communicate using IP(Alexander S. Gillis, 2023a). Instead than forcing network managers to manually assign IP addresses to all network devices, DHCP automates and centrally controls these configurations(Jason Gerend, 2021). DHCP is a protocol that allows for the quick, automatic, and central management of IP address distribution inside a network. It is also used to specify the device's subnet mask, default gateway, and DNS server information(Tim Fisher, 2020).

When a client computer or device connects to a network, it requires an IP address to communicate with other devices on the same network and the internet. DHCP is a network protocol that facilitates the assignment of IP addresses and other network configuration information to devices on a network(Netmanias, 2013).

When a client device starts up, it broadcasts a DHCP Discover message over the Ethernet network to discover available DHCP servers on the same subnet. This message has a destination MAC address of FF:FF:FF:FF:FF:FF, allowing it to communicate with all DHCP servers on the same subnet(Netmanias, 2013).

When the DHCP server receives the request, it provides an IP configuration from its preconfigured pool of available IP addresses to the client device. The IP configuration comprises the IP address, subnet mask, default gateway, and DNS server. This procedure is comprised of four steps: Discover, Offer, Request, and Acknowledgement(ComputerNetworkingNotes, 2020).

In the Discover phase, the client transmits a broadcast message in order to locate DHCP servers on the network. The DHCP server responds with an offer of an IP configuration in the Offer phase. In the Request phase, the client requests the DHCP server's proposed IP configuration. In the Acknowledgement phase, the DHCP server confirms the request and provides the client with the IP configuration(ComputerNetworkingNotes, 2020).

DHCP makes it simpler for administrators to administer large networks by streamlining the process of assigning IP addresses and other network configuration information to devices on a network. It also enables automatic IP configuration of devices, which reduces the likelihood of IP address conflicts and errors.

2.10. Wired Networks

Wired networks are networks that rely on physical cables to connect devices, making them ideal for office settings or stationary devices. These networks use cables to establish a connection between devices, like computers, and the Internet or other networks. Ethernet is a common technology used for wired networks as it provides a secure, fast, and stable connection between devices and the Internet.

A wired network has a number of advantages over wireless networks. The first thing, wired networks often enable quicker data transmission rates due to the larger capacity and dependability of the actual cables employed. This is especially significant for organizations and individuals that want big volumes of data to be moved swiftly and efficiently.

Second, wired networks are less likely to suffer from interference than wireless networks. Wireless networks rely on radio waves to carry data, which might be disturbed by physical impediments, other wireless signals, or even weather conditions. Wired networks, on the other hand, are not influenced by these elements, making them more dependable and constant in terms of data transport.

Finally, wired networks are typically more secure than wireless networks(Dr. Roy Winkelman, 2013). Because wired networks employ physical cables to link devices, it is far more difficult for unauthorized users to intercept data being carried across the network. This is especially crucial for corporations and other organizations that deal with sensitive information such as financial data, personal information, or trade secrets.

2.11. WiFi Networks

Wi-Fi is a wireless technology that allows devices to connect to the Internet and to one another. It enables simple communication and data transmission across a wide range of devices, including computers, mobile phones, and printers, without the use of physical cables. This technology is often used to construct a wireless network in households and businesses.

A Wi-Fi network is generally comprised of a wireless router linked to an Internet modem. The router serves as a central hub, broadcasting the Internet signal to all Wi-Fi enabled devices in its area. Devices may connect to the network by inputting the necessary security credentials, such as a password, and once joined, they can exchange files, stream media, and connect to the Internet.

The primary benefit of Wi-Fi is its ease and flexibility. It removes the need for cables and enables devices to be relocated and utilized in various locations across the network's service area. Wi-Fi technology has become commonplace in modern life, with applications in homes, companies, and public locations such as cafés and airports.

In addition to flexibility, there are a number of advantages of WIFI, it can be fast and easy to set up, as long as your computer has a wireless adapter. You can usually connect automatically to nearby networks with just a few clicks. Additionally, wireless networks can be more cost-effective than wired networks, as there is no need to purchase and install cables. Finally, wireless networks are expandable and adding new devices is as easy as turning on the device, provided the maximum number of devices on the network has not been exceeded.

2.12. Patch Panels

A patch panel is a device or unit that has a number of jacks, generally of the same or similar type, for connecting and routing circuits in a convenient and flexible manner for monitoring, linking, and testing circuits(wikipedia, 2022). Patch panels are widely used in computer networking, recording studios, and radio and television broadcasting. Each of these ports has a cable that connects to a different location. Patch panels can be extremely tiny, with only a few ports, or rather huge, with hundreds of ports(racksolutions.com, 2019).

Patch panels are utilized in various IT environments such as data centers, telephone company central offices, and communications closets to connect different devices. They play a crucial role in bundling connections from each port of the panel to different devices in the facility, which in turn helps to connect a LAN to a WAN or the Internet. Additionally, patch panels are commonly used in facilities with multiple telephone lines to consolidate them into one mainline for all phones. Understanding the function of patch panels can help determine whether they are necessary for a facility and how to set them up.

2.13. Drop Cables

A drop cable is a type of cable used in computer networks to connect a device's network interface card (NIC) to a transceiver or a wall plate. The purpose of the drop cable is to provide a temporary connection between the device and the network, allowing it to be easily disconnected and reconnected whenever necessary. In the case of thicknet Ethernet networks, the drop cable connects the NIC to a transceiver attached to the thicknet cable. In standard Ethernet networks, the drop cable connects the NIC to a wall plate, which is usually located in a fixed position on the wall. Drop cables are essential for maintaining the flexibility and mobility of devices on a network, as they allow computers to be moved around a room or office without having to reconfigure the entire network(networkencyclopedia.com, 2023).

2.14. Wall Jacks

A wall jack is a tiny box that accommodates Ethernet cables in computer networking and is essential for connecting devices to the network(dummies.com, 2016). To connect a computer to the network, plug one end of a patch cable, also known as a station cable, into the wall jack and the other end into the network interface on the computer. In the wiring closet, you connect the wall jack to the network switch, which routes network traffic to the right destination. Wall jacks, also known as keystone jacks, are critical components of large local area networks that make use of patch panels and wall plates. Keystone jacks are female connectors that snap into modular wall plates and patch panels to connect various cables to the larger network(CABLE MATTERS, 2022).

3. Chapter 3 - Components Selection

3.1. Research and analysis of suitable components for the project

3.1.1. Switches and selected justification

As we know in the research part, in computer networking, switches are essential for creating and managing networks. Unlike hubs, switches offer more advanced features such as the ability to filter and forward data packets based on their destination MAC addresses, which leads to better network performance and reduced congestion. Here I will choose some specific recommended models of switch

Core switch

Core switches are used in the backbone of the network to handle high traffic volumes and to connect other switches and routers. They are designed for maximum availability and performance, with features such as redundant power supplies and advanced network management capabilities.

Trend	Feature	Legacy fixed access switches			Benefits
		Catalyst 2960-X Series	Catalyst 2960-XR Series	Catalyst 9200 Series	
Scale and performance	Bandwidth per stack	80 Gbps	80 Gbps	Up to 160 Gbps	Twice the density at nearly the same price
	Uplinks	4x 1G SFP 2x 10G SFP+ 2x 10/100/1000BASE-T	4x 1G SFP 2x 10G SFP+	4x 1G SFP 4x 10G SFP+	

For the Core switch, I recommend the Cisco Catalyst 9200 Series as it is specifically designed for core switches. Compared to the 2960-X Series, the 9200 Series has more advantages.

The Catalyst 9200 Series offers more bandwidth capacity than the 2960-X Series and the 3560-CX Series, with up to 160 Gbps against 80 Gbps. Furthermore, the 9200 Series includes four 10G SFP+ uplinks, compared to the other two series' two 10G SFP+ uplinks.

In terms of port density, the 9200 Series has double the density for approximately the same price as the 2960-X Series, which might be a significant benefit in bigger networks with a high number of ports. The 3560-CX Series, on the other hand, has a more compact form factor and may be a better choice for deployments in limited locations where space is at a premium.

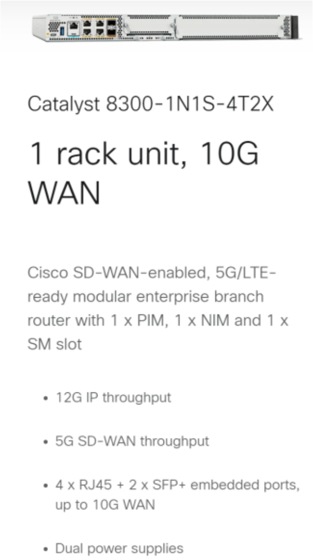
The Catalyst 9200 Series switch also offers other advanced features and capabilities, including role-based access control, encryption, a single common network operating system, programmable interfaces, rich contextual insights, and automation and assurance. These features provide a secure, reliable, and easy-to-manage network infrastructure that is ideal for modern network environments, such as smart buildings. The switch is flexible, scalable, and offers the necessary bandwidth for high-performance networking.

Server switch

Server switches are specialized switches designed for connecting servers to the network. They are typically optimized for low latency and high bandwidth, with features such as quality of service (QoS) prioritization and support for virtual LANs (VLANs).

As the server switch, the company can choose Cisco Nexus 9300 Series switches. Because of their industry-leading performance, scalability, and flexibility, the Nexus 9300 Series switches are a popular choice for data centers and server rooms. These switches, which enable multi-speed ports ranging from 1G to 400G, can meet the varied data requirements of modern data centers. Furthermore, to defend the network from security threats, the Nexus 9300 Series switches provide sophisticated security capabilities such as streaming telemetry, advanced analytics, and line-rate encryption (MACsec). They also enable unified ports, which can help to minimize operating expenses by supporting several protocols including 10/25G Ethernet, 8/16/32G Fibre Channel, RDMA over convergent Ethernet (RoCE), and IP storage. Finally, the Nexus 9300 Series switches provide intelligent buffers and zero packet loss, which can speed up application completion by up to 50%.

3.1.2. Routers and selected justification



Catalyst 8300-1N1S-4T2X

1 rack unit, 10G WAN

Cisco SD-WAN-enabled, 5G/LTE-ready modular enterprise branch router with 1 x PIM, 1 x NIM and 1 x SM slot

- 12G IP throughput
- 5G SD-WAN throughput
- 4 x RJ45 + 2 x SFP+ embedded ports, up to 10G WAN
- Dual power supplies

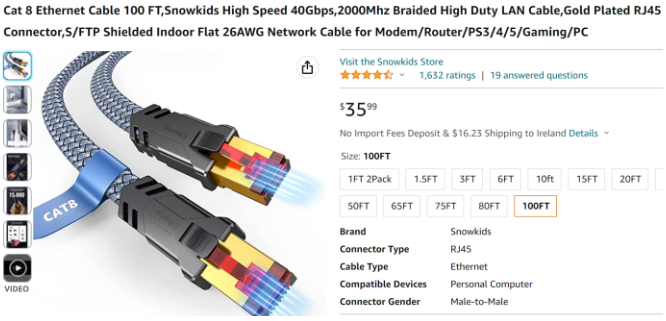
The Cisco Catalyst 8300-1N1S-4T2X router is suitable for the e-commerce company's new training center due to its SD-WAN capabilities, advanced connectivity, and multicloud access. The router is designed for enterprise branch networks and features a modular architecture with 5G/LTE-ready capabilities, allowing the business to transform its branch with cutting-edge wireless network standards. The router is also SD-WAN-enabled, allowing the organization to transition to a Secure Access Service Edge (SASE) with on-premises and cloud-delivered security. In addition, the router's visual administration interface with Cisco vManage will facilitate the simplification of network operations and the acceleration of network deployment. With 1 rack unit and up to 10G WAN, the Catalyst 8300-1N1S-4T2X router is a potent and compact option for the new training facility, enabling high-speed connectivity for the computer laboratories, conference room, and office area.

3.1.3. Cable and selected justification

The network cable, an essential accessory in the network, is also an accessory that is easily overlooked by everyone.

If the network cable is not chosen well, it will affect the speed of all the devices connected to the network cable. For example, if the router is a gigabit one and the broadband in the company is 500Mbps, it turns out that a 100Mbps cable is used. Then the final internet speed is only 100Mbps and the cable becomes the bottleneck in the whole network.

One might choose the Cat 8 Ethernet Cable 100 FT by Snowkids for its high speed of 40Gbps and bandwidth of 2000Mhz, which allows for efficient and reliable data transfer even over long distances. Additionally, the cable is shielded with S/FTP technology to reduce electromagnetic interference and crosstalk, resulting in a stable and clear signal. The gold-plated RJ45 connectors provide corrosion resistance and better connectivity. The flat design of the cable also makes it easier to install and less prone to tangling. Of course, the longer the network cable, the more expensive it is. Here only is an example of 100ft:



Cat 8 Ethernet Cable 100 FT,Snowkids High Speed 40Gbps,2000Mhz Braided High Duty LAN Cable,Gold Plated RJ45 Connector,S/FTP Shielded Indoor Flat 26AWG Network Cable for Modem/Router/PS3/4/5/Gaming/PC

Visit the Snowkids Store

★★★★☆ 1,632 ratings | 19 answered questions

$35.99

No Import Fees Deposit & $16.23 Shipping to Ireland Details

Size: 100FT

1FT 2Pack | 1.5FT | 3FT | 6FT | 10ft | 15FT | 20FT

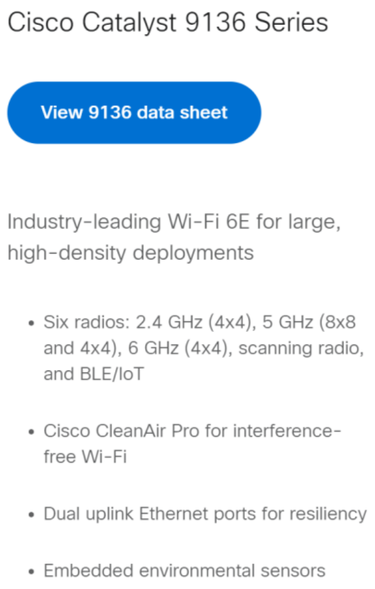
50FT | 65FT | 75FT | 80FT | 100FT

Brand	Snowkids
Connector Type	RJ45
Cable Type	Ethernet
Compatible Devices	Personal Computer
Connector Gender	Male-to-Male

3.1.4. Access points and selected justification

In the research section, we have already introduced the function of WiFi network, and its important equipment is Access point. Now I choose Cisco Catalyst 9136 Series as AP equipment. Because The Cisco Catalyst 9136 Series is a strong choice for those looking to take charge of their network. It offers a supersized spectrum for a better experience, providing faster and more efficient networking even during high traffic times. Additionally, the integrated AI network and device analytics, along with insights, make troubleshooting simpler, ensuring that your network stays running smoothly. With the ability to create your network on-premises, in the cloud, or both, the Cisco Catalyst 9136 Series offers flexibility to meet your needs. It also features WPA3 and no legacy security gaps, ensuring that your data remains safe. One of the standout advantages of the Cisco Catalyst 9136 Series is its industry-leading Wi-Fi 6E for large, high-density deployments. It features six radios, including 2.4 GHz (4x4), 5 GHz (8x8 and 4x4), 6 GHz (4x4), scanning radio, and BLE/IoT.

It also has Cisco CleanAir Pro for interference-free Wi-Fi, dual uplink Ethernet ports for resiliency, and embedded environmental sensors. Overall, the Cisco Catalyst 9136 Series offers a comprehensive and advanced solution for those looking to improve their network.



Cisco Catalyst 9136 Series

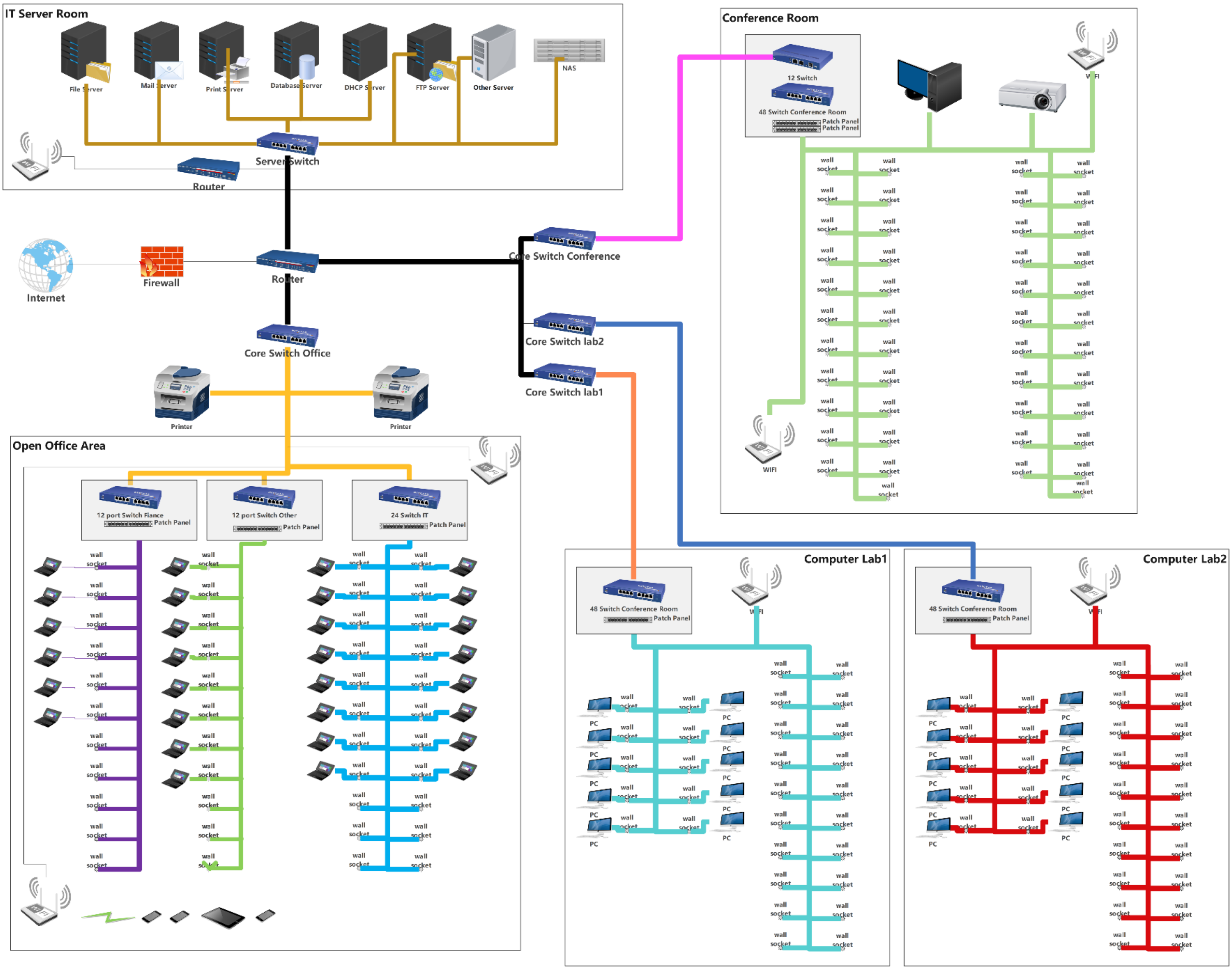
Industry-leading Wi-Fi 6E for large, high-density deployments

- Six radios: 2.4 GHz (4x4), 5 GHz (8x8 and 4x4), 6 GHz (4x4), scanning radio, and BLE/IoT
- Cisco CleanAir Pro for interference-free Wi-Fi
- Dual uplink Ethernet ports for resiliency
- Embedded environmental sensors

4. Chapter 4 - Network Design

4.1. Network Diagram

The network diagram will include a router, switches, access points, and various devices such as PCs and servers. The diagram will show the connection between these devices and the subnets they belong to:



4.2. Description of the diagram and layout:

link to the Internet and Firewall: The network is started out with a link to the internet that is guarded by a firewall. The firewall acts as the first line of protection against potential dangers from the outside world and helps to restrict access to the network by unauthorized users. This is accomplished by monitoring all network traffic, both incoming and outgoing, and blocking any communication that does not comply with the predetermined security regulations.

Core Router and Switches: Once the network traffic has been allowed via the firewall, it is connected to a core router, which in turn is connected to four core switches and a server switch. All of the switches are connected to the core router, which acts as a central point of connection and enables the switches to interact with one another. The core switches are high-performance switches that have been intended to give a high level of durability while also delivering a high level of performance. In big networks, they are often used to link the many different network devices to one another.

Switches in the Office One of the core switches is connected to three of the office switches and is used to manage the open office space. The wall jacks that are situated beneath the office desks are the means by which the office switches link each individual office workstation to the network. When the number of wall jacks is over-provisioned, it enables future expansion and guarantees that there will be sufficient network ports accessible for additional devices as the business expands.

Switch for the Conference Room The second core switch is connected to a switch that has 12 and 48 interfaces. This switch is utilized for the conference room. Up to fifty different electronic devices, such as a personal computer and a projector, can connect to the internet through this.

Computer Lab Switches: The third and fourth core switches are connected to 48-interface switches and are utilized for Computer Labs 1 and 2. These offer network access to ten desktop PCs in each laboratory, in addition to twenty wall plugs in each laboratory for connecting other equipment.

Server Switch: There is also a server switch that links to the IT server room, which houses a variety of servers including file servers, FTP servers, email servers, DHCP servers, database servers, print servers, and a NAS. In addition, there is a NAS that is connected to the server room. These servers are provided with network access via the server switch, which enables them to communicate with other devices that are connected to the network.

Access Points for WiFi: Lastly, every single room in the building is equipped with its own WiFi access point, which is connected to the switches by means of network cables. This enables electronic devices such as computers, cellphones, and tablets to connect to a wireless network.

4.3. Security Concerns

To guard against possible attacks, the network has numerous security problems that must be addressed. The first point of concern is the firewall settings, which must be properly configured to prevent unwanted network access. This can be accomplished by establishing rules to prohibit incoming communication that is not required for business operations, or by allowing intrusion detection and prevention systems to detect and block malicious traffic.

Network segmentation is another important security strategy that includes separating the network into smaller subnetworks, each with its own security rules and access restrictions.

This reduces the severity of any security breaches by making it more difficult for attackers to migrate laterally around the network. Regular updates and patching of network devices and software, including security updates for operating systems, firmware upgrades for network devices, and software patches for applications and services, are also necessary to address known vulnerabilities.

To limit access to authorized users, access controls such as strong passwords and multi-factor authentication should be introduced. This can be accomplished by assigning unique passwords to individual user accounts, mandating multi-factor authentication for critical systems or data, and enforcing password regulations such as complexity requirements and expiration dates. Physical security measures, such as securing server rooms and limiting access to network equipment, should also be considered to prevent unauthorized access or tampering with network devices. Regular security audits and assessments can also assist in identifying possible vulnerabilities and ensuring that security safeguards are functioning properly.

5. Chapter 5 - Subnet Plan

5.1. Subnet and its significance and related research

Subnetting is a technique used to divide a single IP network address into multiple smaller subnets. This technology allows a larger classful IP address to be further subdivided into several subnets, enabling an enterprise that uses a large classful address to allocate different subnets to different branch offices in different locations. Externally, the entire enterprise is a network address, but internally, different branch offices have different subnet addresses, so there is no need to apply for a separate network address for each site.

When we subnet a network, we basically divide it into smaller networks. For example, when a group of IP addresses is assigned to a company, the company may "divide" the network into smaller networks, one for each department. This way, the technical department and the management department can both have their own small networks. By dividing subnets, we can divide the network into smaller networks as needed, which also helps to reduce traffic and hide the complexity of the network.

Subnetting usually involves taking out a certain number of bits from the host identifier part of the IP address to be used as the subnets of the network, and the remaining host identifier part becomes the host identifier part of the corresponding subnet.

The number of bits to be allocated to the subnets depends mainly on the actual number of subnets to be divided.

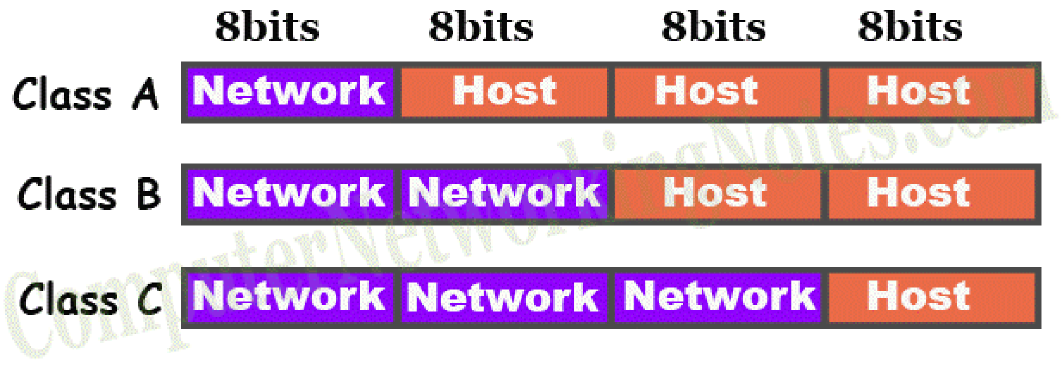
The IP address is then divided into three parts: network-subnet-host. Like traditional classful addresses, the boundary between the network part (network number + subnet) and the host part of the address is defined by the subnet mask.

Subnetting turns the address into a three-level structure: when there is no subnetting, the IP address has a two-level structure, where the network number field of the address is the "Internet part" of the IP address, and the host number field is the "local part" of the IP address. After subnetting, the IP address becomes a three-level structure. Subnetting only subdivides the local part of the IP address without changing the Internet part of the IP address.

5.1.1. Five classes according to the IP addressing

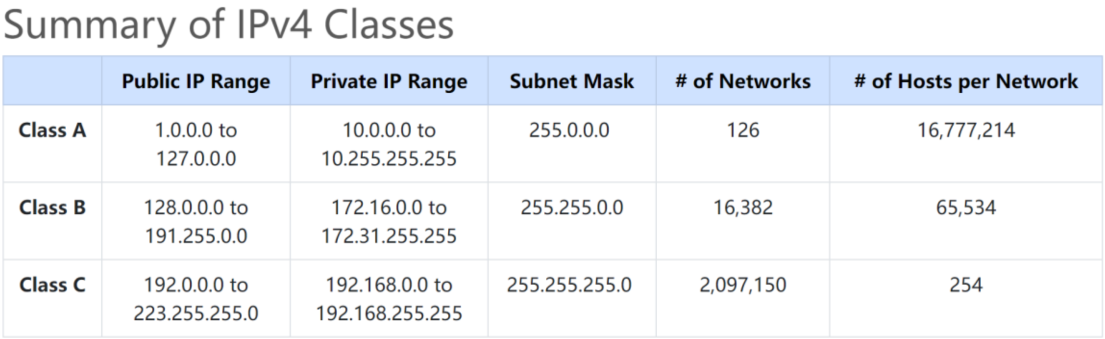
IP addresses are classified into five groups: A, B, C, D, and E. Each class has a separate acceptable address range and default subnet mask. The classifications are determined by the first octet of the IP address(meridianoutpost.com, 2023).

Class A: The first octet ranges from 1 to 126 (inclusive). Class A networks are used for extremely large networks including millions of hosts. The subnet mask is set to 255.0.0.0 by default.
Class B: The first octet ranges from 128 to 191 (inclusive). For medium-sized networks, Class B networks are employed. The subnet mask is set to 255.255.0.0 by default.
Class C: The first octet ranges from 192 to 223 (inclusive). Small networks are served by Class C networks. The subnet mask is set to 255.255.255.0 by default.
Class D: The first octet ranges from 224 to 239 (inclusive). Class D addresses are designated for multicasting, which is a means of simultaneously transmitting a message to a group of hosts. Individual hosts or networks are not identified by these addresses.
Class E: The first octet ranges from 240 to 255 (inclusive). Class E addresses are only used for testing and are not utilized on the public Internet.



	8bits	8bits	8bits	8bits
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host

(how bits are defined for network addresses and host addresses in each IP class)(computernetworkingnotes.com, 2022)



Summary of IPv4 Classes

	Public IP Range	Private IP Range	Subnet Mask	# of Networks	# of Hosts per Network
Class A	1.0.0.0 to 127.0.0.0	10.0.0.0 to 10.255.255.255	255.0.0.0	126	16,777,214
Class B	128.0.0.0 to 191.255.0.0	172.16.0.0 to 172.31.255.255	255.255.0.0	16,382	65,534
Class C	192.0.0.0 to 223.255.255.0	192.168.0.0 to 192.168.255.255	255.255.255.0	2,097,150	254

(Hosts per Network)(meridianoutpost.com, 2023)

5.1.2. Subnet mask

A subnet mask is a 32-bit number used to identify the network part (or prefix) of an IPv4 address. It helps define the boundaries of a network and separates an IP address into two parts: network bits and host bits. The network bits identify the network address, while the host bits identify individual hosts or devices within that network(freecodecamp.org, 2021).

Subnet masks are important in networking because they allow for the division of a larger network into smaller subnetworks, or subnets. By breaking up a network into subnets, it becomes easier to manage and more efficient in terms of data transmission.

When subnetting, the subnet mask is used to determine which bits in the IP address represent the network portion and which bits represent the host portion. This allows network administrators to allocate IP addresses more effectively and create subnets of varying sizes depending on the needs of the network.

5.1.3. Broadcast addresses

In IPv4 addressing, each IP address is divided into two parts: the network address and the host address. The subnet mask is used to separate these two parts. It does this by setting the bits that belong to the network address to all 1s and the bits that belong to the host address to all 0s(avinetworks.com, 2023).

The network address is used to identify a network and is reserved for this purpose. It cannot be assigned to any device as a unique identifier, as it is already used to identify the entire network. Instead, each device on the network is assigned a unique host address within that network.

The broadcast address, on the other hand, is used to send data packets to all devices on a network. When a device wants to send a packet to all other devices on the same network, it sends the packet to the broadcast address, which is always assigned to the highest possible address within the network range. This ensures that all devices on the network receive the packet(Terry Slattery, 2023).

The reason why we reserve the network and broadcast addresses is to prevent conflicts with unique device addresses. By reserving these addresses for special purposes, we ensure that no device can be assigned these addresses as a unique identifier, which could cause conflicts and disrupt network communication(Terry Slattery, 2023).

5.1.4. CIDR notation

In comparison to the previous way of utilizing subnet masks, CIDR notation is a more current method of describing IP addresses and network prefixes. The amount of bits utilized for the network prefix and the host component of an IP address is specified by the subnet mask. In contrast, CIDR notation defines the number of bits utilized for the network prefix directly in the IP address.

To express a network with a prefix length of 24 bits, for example, instead of using the subnet mask 255.255.255.0, CIDR notation would use the IP address followed by a slash and the number of bits in the network prefix: 192.168.1.0/24.

Because it may indicate network prefixes of any length, rather than simply the standard classes A, B, and C, CIDR notation enables for more efficient use of IP addresses. This means that networks may be scaled to meet their individual requirements rather than being constrained by preset block sizes. It also facilitates network prefix aggregation, which can reduce the size of routing tables and enhance overall network performance.

CIDR notation provides a more flexible and efficient means of assigning IP addresses and describing network prefixes, and it has become the industry standard for network addressing in modern networking.

5.2. Proposal for a subnet plan for the LAN

5.2.1. Subnet design step

Step 1: Identify the class
The IP address 178.16.0.0 falls under Class B.

Step 2: Identify the network and node
The network part of the address is the first two octets, i.e. 178.16, while the third and the forth octet will be used for the host or node.

Step 3: Apply the default subnet mask
The default subnet mask for Class B is 255.255.0.0.

Step 4: Convert the subnet mask to binary
255.255.0.0 in binary is 11111111.11111111.00000000.00000000

Step 5: Determine the custom subnet mask

We need to allocate subnets for the different areas with a minimum number of addresses required. We also need to reserve some addresses for future expansion and new employees. Here's the breakdown:

Computer lab 1: 10 desktop PCs and 20 wall jacks = 30 hosts

Computer lab 2: 10 desktop PCs and 20 wall jacks = 30 hosts

Conference room: 50 seat capacity + 1 PC+ 1 Projector= 52 hosts

IT Server room: 8 servers = 8 hosts

Open office area: 30 tables reserve 18 addresses in total for future expansion and new employees = 44 hosts (IT department: 16 employees reserve 6 addresses, Finance department: 6 employees reserve 5 addresses, Other departments: 8 employees reserve 3 addresses)
Open office area including the IT department, finance department, and other department.

Building WiFi: 100 wireless access points = 100 hosts

To calculate the custom subnet mask, we need to determine the total number of hosts required in the network, which is the sum of hosts in each location.

Total hosts = 30 (Computer lab 1) + 30 (Computer lab 2) + 52 (Conference room) + 8 (IT Server room) + 44 (Open office area) + 100 (Building WiFi) = 264 hosts

Next, we need to find the smallest power of 2 that is greater than or equal to the total number of hosts, which is 2^8 = 256. This means we need 8 bits for the host portion of the address.

Since we are using Class B network address 178.16.0.0, the default subnet mask is 255.255.0.0, which has 16 bits for the network portion of the address.

To calculate the custom subnet mask, we need to borrow bits from the host portion to create additional subnets. In this case, we need 8 bits for the host portion, so we can borrow 3 bits to create additional subnets.

The subnet mask will be 255.255.255.224 in decimal, which is equivalent to 11111111.11111111.11111111.11100000 in binary.

This means we can create up to 8 subnets, each with 32 addresses (30 usable hosts + network and broadcast addresses). We can assign each location to a different subnet to improve network security and manageability.

Create the subnet and allocate the addresses
We need to borrow additional bits from the host component of the IP address to establish subnets. Using the following formula, we can compute the amount of bits required:

2^n total number of hosts plus 2, where n is the amount of bits borrowed.

To allow 264 hosts + 2 (one for the network address and one for the broadcast address), we need to borrow 9 bits in this scenario.

Because we're borrowing 9 bits, the subnet mask for our custom subnet will be 255.255.255.128, giving us a binary subnet mask of 11111111.11111111.11111111.10000000.

We may establish the following subnets using this subnet mask:

Computer Lab1: Subnet 1: 178.16.0.0/25 (30 hosts),
Computer Lab2: Subnet 2: 178.16.0.128/25 (30 hosts)
Conference room: Subnet 3: 178.16.1.0/26 (52 hosts) Subnet 3
IT Server Room: Subnet 4: 178.16.1.64/29 (8 hosts) Subnet 4
Open office area: Subnet5: (178.16.1.72/26 (44 hosts)
Building WIFI: Subnet 6: 178.16.2.0/25 (100 hosts)

This will give us a total of six subnets, each with its own range of IP addresses, allowing us to operate the network more effectively and award addresses to departments or locations as needed.

The addresses ranges are below:
Computer Lab1: 178.16.0.0 - 178.16.0.127
Computer Lab2: 178.16.0.128 - 178.16.0.255
Conference room: 178.16.1.0 - 178.16.1.63
IT Server Room: 178.16.1.64 - 178.16.1.74
Open office area: 178.16.1.75 - 178.16.1.127
Building WIFI: 178.16.2.0 - 178.16.2.127

Security and manageability Concerns
Assign each location to a different subnet to improve network security and manageability. Subnetting can bring numerous benefits to a network, including improved security, manageability, and performance. By assigning each location to a different subnet, network

administrators can create isolated network segments that prevent unauthorized access to sensitive data and limit the spread of malware or viruses in case of a breach. Additionally, separating different locations into different subnets can make it easier to manage and troubleshoot the network, allowing quick isolation and identification of network issues without affecting the rest of the network. Furthermore, segmenting the network into smaller subnets can reduce the amount of broadcast traffic and optimize the routing of network traffic, leading to improved network performance.

6. Chapter 8 - Additional Features

In addition to the essential principles of the network design, various additional features have been introduced to improve network performance, security, and administration. These extra capabilities include redundancy, VLANs, Quality of Service (QoS), network monitoring, a guest network, network segmentation, Network Access Control (NAC), Power over Ethernet (PoE), cloud-based administration, and VPN connectivity.

Redundancy is a vital characteristic that has been incorporated into the network architecture to provide high availability and minimize downtime. The network includes redundant core switches, power supply, and network cables to guarantee that the network can continue to function even if a component fails.

VLANs have been developed to separate network traffic and improve security. This allows distinct sets of devices to be segregated into their own virtual networks, enhancing network control and monitoring.

QoS algorithms have been introduced to prioritize network traffic and guarantee that vital applications receive adequate bandwidth and low latency. This capability is especially critical for applications like as VoIP and video conferencing, which demand low latency and continuous communication.

Network monitoring tools have been included to proactively discover and troubleshoot network faults. This comprises traffic analysis, device monitoring, and security event tracking, which aids in the rapid identification and resolution of network problems.

A separate guest network has been set up to enable internet access to guests while keeping them apart from the main network. This function protects the primary network from unwanted access or infection from remote devices.

Network segmentation has been implemented to separate distinct types of traffic, such as voice and data traffic, and prevent interference between them. This network performance enhancement enables high-quality voice conversations and continuous data transfer.

NAC techniques have been deployed to limit network access and guarantee that only authorized devices and users have access. This helps to prevent illegal access and increase network security.

PoE technology has been used to power network devices such as access points and IP phones over network cables, eliminating the need for external power sources. This simplifies installation and lowers expenses.

Cloud-based management tools have been introduced to centrally monitor and configure network devices, simplifying network administration and minimizing the requirement for on-site management.

Finally, VPN connectivity has been introduced to enable distant network access while assuring safe and encrypted communication between remote users and the network. This is especially crucial for remote employees or those accessing the network from a separate location.

Overall, the extra features added into the network architecture assure a high-performance, secure, and easily-managed network.

7. Chapter 9 - Conclusion

7.1. Summary of the proposed network plan and design

The planned network plan for the e-commerce company's graduate training center in Dublin includes a secure internet connection protected by a firewall. The core router and switches are linked to the firewall and are in charge of network traffic management. One core switch manages the open office space, one manages the conference room, and two manage the computer laboratories. There is also a server switch that links to the IT server room, which houses a variety of servers.

A subnet plan with specified IP address ranges for each region of the network has been designed to increase network performance. The IP address range for the computer labs is 178.16.0.0 - 178.16.0.255, while the conference room is 178.16.1.0 - 178.16.1.63, the IT server room is 178.16.1.64 - 178.16.1.74, the open office area is 178.16.1.75 - 178.16.1.127, and the building WiFi is 178.16.2.0 - 178.16.2.127. This guarantees that each network segment has its own unique IP address range, reducing network congestion and increasing network efficiency.

A DHCP server has also been added in the network design to manage network devices and automatically assign IP addresses. This will simplify network administration and minimize network managers' workload.

Finally, WiFi access points have been put in every building rooms to enable electronic devices to connect to a wireless network. Staff and guests will benefit from the added convenience and flexibility.

Overall, the suggested network layout and design for the e-commerce company's graduate training center in Dublin is thorough and will match the business project's objectives.

7.2. Final recommendations for the successful implementation of the project

The successful implementation of the proposed network plan and design for the e-commerce company's graduate training center in Dublin requires careful consideration and planning. To ensure the network is designed and implemented correctly, it is highly recommended to hire a professional network engineer who has experience in designing and implementing complex networks. Additionally, regular maintenance and updates are crucial to keep the network functioning optimally, and security should be a top priority to prevent any potential security breaches.

Providing employee training will ensure that the network is used efficiently and securely. The network plan has been designed with scalability in mind to allow for future expansion as the business grows. This can include over-provisioning network ports, leaving room for additional switches, and considering future upgrades to network infrastructure.

8. References

Alexander S. Gillis. (2023a). *What is DHCP (Dynamic Host Configuration Protocol)?* Techtarget.Com. https://www.techtarget.com/searchnetworking/definition/DHCP

Alexander S. Gillis. (2023b). *What Is Network Topology? - Definition from SearchNetworking*. Techtarget.Com. https://www.techtarget.com/searchnetworking/definition/network-topology

Andrew Froehlich. (2023). *What is a LAN? - Definition from WhatIs.com*. Techtarget.Com. https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN

ASTRA. (2022, July 7). *The Beginner's Guide to IP Addressing – What, Why and How*. Wpastra.Com. https://wpastra.com/guides-and-tutorials/what-is-ip-address/

avinetworks.com. (2023). *What is Subnet Mask? Definition & FAQs | Avi Networks*. Avinetworks.Com. https://avinetworks.com/glossary/subnet-mask/

BBC. (2023a). *Addressing and protocols - Network topologies, protocols and layers - OCR - GCSE Computer Science Revision - OCR - BBC Bitesize*. BBC. https://www.bbc.co.uk/bitesize/guides/zr3yb82/revision/5

BBC. (2023b). *Factors that affect the performance of networks - Wired and wireless networks - OCR - GCSE Computer Science Revision - OCR - BBC Bitesize*. BBC. https://www.bbc.co.uk/bitesize/guides/zvspfcw/revision/8

Bradley Mitchell. (2020, April 7). *Introduction to Computer Network Speed*. Lifewire. https://www.lifewire.com/computer-network-speed-818118

Brian Nadel. (2020, May 13). *Ethernet cables: Everything you need to know | Tom's Guide*. Tomsguide.Com. https://www.tomsguide.com/reference/ethernet-cables-explained

CABLE MATTERS. (2022, March 4). *What Is a Keystone Jack?* CABLE MATTERS. https://www.cablematters.com/Blog/Networking/what-is-a-keystone-jack

Cisco. (2023a). *What are the Different Types of Routers - Cisco*. Cisco. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/types-of-routers.html#~overview

Cisco. (2023b). *What is a Router? - Definition and Uses - Cisco*. Cisco. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html

Cisco. (2023c). *What Is Network Switching? - Cisco*. Cisco. https://www.cisco.com/c/en/us/products/switches/what-is-network-switching.html

Cisco. (2023d). *What Is Network Topology? - Cisco*. Cisco. https://www.cisco.com/c/en/us/solutions/automation/network-topology.html

comptia.org. (2023). *LAN Definition | What Is Local Area Network | Computer Networks | CompTIA*. Comptia.Org. https://www.comptia.org/content/guides/what-is-a-local-area-network

ComputerNetworkingNotes. (2020, October 16). *How DHCP works Explained with Examples*. ComputerNetworkingNotes. https://www.computernetworkingnotes.com/ccna-study-guide/how-dhcp-works-explained-with-examples.html

computernetworkingnotes.com. (2022, April 9). *IP Address Classes Explained with Examples*. Computernetworkingnotes.Com. https://www.computernetworkingnotes.com/networking-tutorials/ip-address-classes-explained-with-examples.html

Dr. Roy Winkelman. (2013). *Chapter 4: Cabling*. University of South Florida. https://fcit.usf.edu/network/chap4/chap4.htm

dummies.com. (2016, March 26). *Network Building: Wall Jacks and Patch Panels - dummies*. Dummies.Com. https://www.dummies.com/article/technology/information-technology/networking/general-networking/network-building-wall-jacks-and-patch-panels-185245/

freecodecamp.org. (2021, April 20). *Subnet Mask Definition*. Freecodecamp.Org. https://www.freecodecamp.org/news/subnet-mask-definition/

Jason Gerend. (2021, July 29). *Dynamic Host Configuration Protocol (DHCP) | Microsoft Learn*. Microsoft. https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

javatpoint. (2023). *What is a Router in Computer Network? - javatpoint*. Javatpoint. https://www.javatpoint.com/router

Julio Jiminez. (2023, February 13). *Configure IP Addresses and Unique Subnets for New Users - Cisco*. Cisco. https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

Kevin Parrish. (2023, January 11). *Are Ethernet Cables Slowing Your Connection? | HighSpeedInternet.com*. Highspeedinternet.Com. https://www.highspeedinternet.com/resources/are-ethernet-cables-slowing-your-connection

Kim Staples. (2017, December 11). *How to set up a local area network (LAN)*. Broadbandchoices.Co.Uk. https://www.broadbandchoices.co.uk/broadband/guides/how-to-set-up-a-local-area-network

meridianoutpost.com. (2023). *5 Classes of IPv4 Addresses [Class A, B, C, D and E]*. Meridianoutpost.Com. https://www.meridianoutpost.com/resources/articles/IP-classes.php

Mitch Harris. (2023, March 25). *3 Ways to Configure Your PC to a Local Area Network - wikiHow*. Wikihow.Com. https://www.wikihow.com/Configure-Your-PC-to-a-Local-Area-Network

Netmanias. (2013, October 23). *Understanding the Basic Operations of DHCP | NETMANIAS*. Netmanias.Com. https://www.netmanias.com/en/post/techdocs/5998/dhcp-network-protocol/understanding-the-basic-operations-of-dhcp

NetworkEncyclopedia. (2023). *Cabling (networking) - Network Encyclopedia*. NetworkEncyclopedia. https://networkencyclopedia.com/cabling/

networkencyclopedia.com. (2023). *Drop Cable - Network Encyclopedia*. Networkencyclopedia.Com. https://networkencyclopedia.com/drop-cable/?utm_content=cmp-true

Networkhunt.com. (2023). *Different Types of Network Cable and Specifications - Networkhunt.com*. Networkhunt.Com. https://networkhunt.com/different-types-of-network-cable-and-specifications/

racksolutions.com. (2019, September 6). *What is a Patch Panel and Why You Need It?* Racksolutions.Com. https://www.racksolutions.com/news/blog/patch-panel/

Samatha Bhargav. (2021, May 2). *What is an IP Address, The Purpose and its Benefits*. Technotification.Com. https://www.technotification.com/2019/05/what-is-an-ip-address.html

Terry Slattery. (2023). *How to calculate a subnet mask from hosts and subnets | TechTarget*. Techtarget.Com. https://www.techtarget.com/searchnetworking/tip/IP-addressing-and-subnetting-Calculate-a-subnet-mask-using-the-hosts-formula

tevelec.com. (2023). *What Are the 4 Types of Network Cables? - Tevelec*. Tevelec.Com. https://www.tevelec.com/what-are-the-4-types-of-network-cables/

Tim Fisher. (2020, December 13). *What Is DHCP? (Dynamic Host Configuration Protocol)*. Lifewire.Com. https://www.lifewire.com/what-is-dhcp-2625848

tutorialspoint.com. (2023). *What are Switches in Computer Network*. Tutorialspoint.Com. https://www.tutorialspoint.com/what-are-switches-in-computer-network

wikipedia. (2022, November 19). *Patch panel - Wikipedia*. En.Wikipedia.Org. https://en.wikipedia.org/wiki/Patch_panel

Yaffet Meshesha. (2022, July 11). *How to Create a Local Area Network (LAN) (with Pictures) - wikiHow*. Wikihow.Com. https://www.wikihow.com/Create-a-Local-Area-Network-(LAN)