Higher Nationals - Summative Assignment Feedback Form

Student Name/ID	M.M.M AASHIK /E230667		
Unit Title	**Unit 02: Networking**		
Assignment Number	1	**Assessor**	
Submission Date	16/09/2024	**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	

Assessor Feedback:

LO1 Examine networking principles and their protocols

Pass, Merit & Distinction Descripts P1 P2 M1 ☐ ☐ ☐

LO2 Explain networking devices and operations.

Pass, Merit & Distinction Descripts P2 M2 D1 ☐ ☐ ☐

LO3 Design efficient networked systems.

Pass, Merit & Distinction Descripts P3 P4 M3 ☐ **D2** ☐ ☐ ☐

LO4 Implement diagnose and demonstrate prepared networked systems.

Pass, Merit & Distinction Descripts P5 ☐ **M4** ☐ **M5** ☐

D3 ☐

* Please note that grade decisions are provisional. They are only confirmed once internal and external moderation has taken place and grades decisions have been agreed at the assessment board.

Assessor Feedback:		
Grade:	**Assessor Signature:**	**Date:**
Resubmission Feedback: • Please note resubmission feedback is focussed only on the resubmitted work		
Grade:	**Assessor Signature:**	**Date:**
Internal Verifier's Comments:		
Signature & Date:		

• Please note that grade decisions are provisional. They are only confirmed once internal and external moderation has taken place and grades decisions have been agreed at the assessment board.

Important Points:

1. It is strictly prohibited to use textboxes to add texts in the assignments, except for the compulsory information. eg: Figures, tables of comparison etc. Adding text boxes in the body except for the before mentioned compulsory information will result in rejection of your work.
2. Avoid using page borders in your assignment body.

4. Ensure that you give yourself enough time to complete the assignment by the due date.
5. Excuses of any nature will not be accepted for failure to hand in the work on time.
6. You must take responsibility for managing your own time effectively.
7. If you are unable to hand in your assignment on time and have valid reasons such as illness, you may apply (in writing) for an extension.
8. Failure to achieve at least PASS criteria will result in a REFERRAL grade.
9. Non-submission of work without valid reasons will lead to an automatic RE FERRAL. You will then be asked to complete an alternative assignment.
10. If you use other people's work or ideas in your assignment, reference them properly using HARVARD referencing system to avoid plagiarism. You have to provide both in-text citation and a reference list.
11. If you are proven to be guilty of plagiarism or any academic misconduct, your grade could be reduced to A REFERRAL or at worst you could be expelled from the course
12. Use word processing application spell check and grammar check function to help editing your assignment.
13. Use **footer function in the word processor to insert Your Name, Subject, Assignment No, and Page Number on each pag**e. This is useful if individual sheets become detached for any reason.

STUDENT ASSESSMENT SUBMISSION AND DECLARATION

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

Student name: M.M.M AASHIK		Assessor name: MS. BEVAN
Issue date:	Submission date: **16.09.2024**	Submitted on: **30.10.2024**
Programme: Pearson BTEC HND in Computing		
Unit: **2 -Networking**		
LAN Design & Implementation for BlueScope Steel Corp.		

Plagiarism

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalized. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any

material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

Guidelines for incorporating AI-generated content into assignments:

The use of AI-generated tools to enhance intellectual development is permitted; nevertheless, submitted work must be original. It is not acceptable to pass off AI-generated work as your own.

Student Declaration

Student declaration
I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.
Student signature: Date:

UNIT 2 – NETWORKING

ASSIGNMENT BRIEF

Student Name/ID Number	M.M.M AASHIK/E230667
Unit Number and Title	**Unit 2 – Networking**
Academic Year	2024
Unit Tutor	
Assignment Title	**LAN Design & Implementation for BlueScope Steel Corp.**
Issue Date	
Submission Date	
Submission Format	

The submission should be in the form of an individual report written in a concise, formal style using single spacing (refer to the assignment guidelines for more details) and a formal presentation with 810 slide.

Individual Report

You are required to make use of headings, paragraphs, and subsections as appropriate, and all work must be supported with research and referenced using Harvard referencing system. Please provide intext citation and a list of references using Harvard referencing system. **The recommended word count is 3,000–3,500 words for the report excluding annexures, although you will not be penalised for exceeding the total word limit,** although you will not be penalized for exceeding the total word limit.

Presentation

A formal 10–15-minutes presentation (8-10 slides as a guide, with supporting speaker notes) to communicate an investigation to a non-technical audience discussing the key features and characteristics of a range of network types, topologies, hardware, and software that you have been used for the new network implementation and demonstrate your network blueprint and the packet tracer simulation.

Unit Learning Outcomes

LO1. Examine networking principles and their protocols.

LO2. Explain networking devices and operations.

LO3. Design efficient networked systems.

LO4. Implement diagnose and demonstrate prepared networked systems.

Transferable skills and competencies developed

- Computational thinking (including its relevance to everyday life)
- Demonstrate knowledge and understanding of essential facts, concepts, principles, and theories relating to computing and computer applications.
- Use such knowledge and understanding in the modelling and design of computer-based systems for the purposes of comprehension, communication, prediction, and the understanding of tradeoffs.
- Recognize and analyze criteria and specifications appropriate to specific problems, and plan strategies for their solutions.
- Critical evaluation and testing: analyze the extent to which a computer-based system meets the criteria defined for its current use and future development.
- Methods and tools: deploy appropriate theory, practices and tools for the design, implementation, and evaluation of computer-based systems.

Computing-related practical skills:

- The ability to specify, design and construct reliable, secure, and usable computer-based systems.
- The ability to evaluate systems in terms of quality attributes and possible trade-offs presented within the given problem.
- The ability to deploy effectively the tools used for the construction and documentation of computer applications, with particular emphasis on understanding the whole process involved in the effective deployment of computers to solve practical problems.
- The ability to critically evaluate and analyze complex problems, including those with incomplete information, and devise appropriate solutions, within the constraints of a budget.

Generic skills for employability

- Intellectual skills: critical thinking; making a case; numeracy and literacy.
- Self-management: self-awareness and reflection; goal setting and action planning.
- Independence and adaptability; acting on initiative; innovation and creativity.
- Interaction: reflection and communication.
- Contextual awareness, e.g. the ability to understand and meet the needs of individuals, business, and the community, and to understand how workplaces and organisations are governed.

Learner name:	**ION RECORD**
Qualification:	
Unit number & title:	
Description of activity undertaken (please be as specific as possible)	
Description of activity undertaken	
Assessment criteria (for which the activity provides evidence)	
Assessment criteria	
How the activity meets the requirements of the assessment criteria, including how and where the activity took place	
How the activity meets the requirements of the assessment criteria	

Witness name:		**Job role:**	
Witness signature:		**Date:**	
Learner name:			
Learner signature:		**Date:**	
Assessor name:		**Date:**	
Assessor signature:			
Assessor signature:		**Date:**	

WITNESS STATEMENT

Assignment Brief and Guidance:

BlueScope is an Australian based Sheet metal manufacturer based in Melbourne. The company manufactures sheet metal and other steel-based products, and CEO plan to expand the company operations in Darwin and management decided to open new branch office in Darwin with the data centre. The company is planning to expand their business operations with their latest branch at Darwin and wants it to be one of the most prominent tech-oriented offices in Darwin with the latest tech facilities such as IoT and smart devices such as auto lighting and physical security solutions smart gates and new ERP software.

You have been appointed as the junior network administrator of BlueScope and your task is to, design and restructure the existing network. Prepare a network architectural design and implement it with your suggestions and recommendations to meet the company requirements.

The floor plan of the head office in Melbourne is as follows:

Floor 1:

- Reception area (5 employees)
- Sales & Marketing Department (20 employees)
- Customer Services Area – with Wi-Fi facilities
- Factory area (30 employees)
- Warehouse and the distribution (25 employees)

Floor 2:

- Director suits (5 suits)
- Boardroom with Video conferencing facility and Wi-Fi.
- Administration Department (25 Employees)
- HR Department (6 employees)

Floor 3:

- Accounting & Finance Department (15 employees)
- IT Department (6 employees)
- The Server Room

The newly established floor plan of the Darwin is as follows:

Floor 1:

- Reception area (2 employees)
- Customer Services Area– with Wi-Fi facilities
- Factory area (35 employees)
- Warehouse and the distribution (20employees)

Floor 2:

- Administration Department (15 Employees)
- HR Department (7 employees)
- Accounting & Finance Department (18 employees)
- IT Department (6 employees)
- The Server Room

The following requirements are given by the Management.

- All the departments **must be separated** with **unique subnets.**
- **The conferencing room of the head office and Customer Services Areas** of each branch are to be **equipped with Wi-Fi connections**.
- **Connectivity between two branches** (Melbourne and Darwin) which would allow intra-branch connectivity between departments. (Use of VPN or Inter VLAN routing)
- **The necessary IP ranges** must be decided by the network designer and should be used for all the departments and subnetting calculations must

Be provided within the report **except the server room**.

- **The number of servers required for the Server room** needs to be decided by the Network designer and should be assigned with

  192.168.10.0/24 subnet. (Uses **static IPs**)

- **The Sales and Marketing** Team also needs to access Network resources **using WIFI** connectivity.

(Note: Clearly state your assumptions. You are allowed to design the network according to your assumptions, but main requirements should not be violated)

Activity 01

- Discuss the benefits and constraints of different network system types that can be implemented in the Darwin office. Furthermore discuss the type of networks recommended for the restructuring of Melbourne and Darwin offices.

- Discuss the different protocols utilized for the communication and the connectivity of the 2 offices which can be implemented in the Darwin branch and the main IEEE Ethernet standards that can be used in above LAN and WLAN design of BlueScope.

- Discuss the importance and impact of network topologies and assess the main network protocol suites that are used in network design using examples. Recommend suitable network topologies and network protocols for the above scenario and evaluate your answer with valid points.

Activity 02

- Discuss the operating principles of network devices (Ex: Router, Switch, Etc.) and server types that can be used for above scenario while exploring

Different servers that are available in today's market with their specifications and recommend server/servers for the above scenario and justify your selection with valid points.

- Discuss the inter-dependence of workstation hardware and networking software and provide examples for networking software that can be used in the above network design.

Activity 03

- Prepare a written network design plan to meet the above -mentioned user requirements including a blueprint drawn using a modelling tool (Ex: Microsoft Visio, EdrawMax) and test and evaluate the proposed design by analysing user feedback with the aim of optimizing your design and improving efficiency.

- (Support your answer by providing the VLAN and IP Subnetting scheme for the above scenario and the list of devices, network components and software used to design the network for above scenario and while justifying your selections.)

- Install and configure Network services, devices and applications (Ex: VLAN, Wi-Fi, DNS, Proxy, Web, Etc.) according to the proposed design to accomplish the user requirements and design a detailed Maintenance schedule for above Network.

***Note: - Screen shots of Configuration scripts should be presented in your document. Your packet tracer file must be submitted to the cloud drive and share the link in the appendix of document for the assessor verification purposes.**

Activity 04

- Implement a networked system based on your prepared design with valid evidence.

- Prepare 10-15 minutes presentation which includes the design (Network type, topologies, devices, and software you used for the implementation, and you need to justify with the valid reasons. The presentation should include your blueprint of the design and the packet tracer demonstration with testing interface pinging's and trace routes). **Add your presentation slides in the appendix of the report.**

- Develop test cases and conduct verification (Ex: Ping, extended ping, trace route, telnet, SSH, etc.) to test the above Network and analyse the test results against the expected results.

- Recommend potential future enhancements for the networked system with valid justifications and critically reflect on the implemented network, including the plan, design, configurations, tests, and the decisions made to enhance the system.

Recommended resources

Please note that the resources listed are examples for you to use as a starting point in your research – the list is not definitive.

Web links:

- https://blog.netwrix.com/ (2022) Network Devices Explained [online] Available at: https://blog.netwrix.com/2019/01/08/network-devices-explained/ [Accessed 1 August 2022] https://www.checkpoint.com/ (n.d.) what is a Firewall? [online] Available at: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/ [Accessed 1 August 2022]
- https://www.checkpoint.com/ (n.d.) what is an IoT Gateway? [online] Available at: https://www.checkpoint.com/cyber-hub/network-security/what-is-iot/what-is-an-iot gateway/ [Accessed 1 August 2022]
- https://www.cloudflare.com/en-gb/ (n.d.) A global network built for the cloud [online] Available at: https://www.cloudflare.com/en-gb/learning/network-layer/internet-protocol/ [Accessed 1 August 2022]
- https://www.comparitech.com/ (2020) Variable Length Subnet Mask (VLSM) Tutorial [online] Available at: https://www.comparitech.com/net-admin/variable-length-subnet-mask-vlsm tutorial/ [Accessed 1 August 2022]
- https://www.comptia.org/ (n.d.) What Is a Network Protocol, and How Does It Work? [online] Available at: https://www.comptia.org/content/guides/what-is-a-network-protocol [Accessed 1 August 2022]
- https://www.ibm.com/uk-en (2021) Networking [online] Available at: https://www.ibm.com/uken/cloud/learn/networking-a-complete-guide [Accessed 1 August 2022]
- https://www.ibm.com/uk-en (2022) TCP/IP protocols [online] Available at: https://www.ibm.com/docs/en/aix/7.2?topic=protocol-tcpip-protocols [Accessed 1 August 2022]
- https://www.lifewire.com/ (2022) what Is Bandwidth? Definition, Meaning, and Details [online] Available at: https://www.lifewire.com/what-is-bandwidth-2625809 [Accessed 1 August 2022]
- https://www.ncsc.gov.uk/ (2019) Secure design principles [online] Available at: https://www.ncsc.gov.uk/collection/cyber-security-design-principles [Accessed 1 August 2022]
- https://www.serverwatch.com/ (2021) Network Server [online] Available at: https://www.serverwatch.com/servers/network-server/ [Accessed 1 August 2022]
- https://www.techtarget.com/ (2022) IoT gateway [online] Available at: https://www.techtarget.com/iotagenda/definition/IoT-gateway [Accessed 1 August 2022]
- https://www.univention.com/ (2022) Brief Introduction: DHCP and DNS [online] Available at: https://www.univention.com/blog-en/brief-introduction/2019/03/brief-introduction-dhcp dns/ [Accessed 1 August 2022]

Virtual Network Simulators:

- https://www.adobe.com/ (n.d.) DNS/DHCP/EMAIL VIA PACKET TRACER [online] Available at: https://express.adobe.com/page/7ogipygZfOh0B/ [Accessed 1 August 2022]

- https://techgenix.com/ (2019) Tips and tools for simulating a complex network in a virtual lab [Online] Available at: https://techgenix.com/simulating-network-in-virtual-lab/ [Accessed 1 August 2022]
- https://www.eve-ng.net/ (2022) EVE - The Emulated Virtual Environment For Network, Security and DevOps Professionals [online] Available at: https://www.eve-ng.net/ [Accessed 1 August 2022]
- https://www.gns3.com/ (2022) The software that empowers network professionals [online] Available at: https://www.gns3.com/ [Accessed 1 August 2022] https://www.netacad.com/ (n.d.) Cisco Packet Tracer [online] Available at: https://www.netacad.com/courses/packet-tracer [Accessed 1 August 2022]

Journal articles.

- Agyemang, J., Kponyo, J. and Klogo, G., 2022. The State of Wireless Routers as Gateways for Internet of Things (IoT) Devices. [online] Pubs.sciepub.com. Available at: [Accessed 1 August 2022].
- Oje, A. (2021) Optimization and analysis of the packet switched network with focus on the 3G network. Journal of Physics: Conference Series, Volume 1734, International Conference on Recent Trends in Applied Research doi:10.1088/1742-6596/1734/1/012037 Available at: https://iopscience.iop.org/article/10.1088/1742-6596/1734/1/012037/meta [Accessed 1 August 2022].
- Tyagi, A. (2020) TCP/IP Protocol Suite. International Journal of Scientific Research in Computer Science Engineering and Information Technology doi:10.32628/CSEIT206420 Available at: https://www.researchgate.net/publication/346829282_TCPIP_Protocol_Suite [Accessed 1 August 2022].
- Van der Toorn et al. (2022) Addressing the challenges of modern DNS a comprehensive tutorial. Computer Science Review, Volume 45, 2022, 100469, https://doi.org/10.1016/j.cosrev.2022.100469
- Xu, G. (2021) Research on the Application of the IPv6 Network Protocol. Journal of Physics: Conference Series doi:10.1088/1742-6596/2031/1/012040 Available at: https://iopscience.iop.org/article/10.1088/1742-6596/2031/1/012040/pdf [Accessed 1 August 2022].
- ZHUKOVYTS'KYY, Igor & PAKHOMOVA, Victoria. (2018). Research of token ring network options in automation system of marshalling yard. Transport Problems. 13. 149-158. doi:10.20858/tp.2018.13.2.14.

Reading:

- Bonaventure, O. (2011) Computer Networking: Principles, Protocols and Practice, The Saylor Foundation, Available at: https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Examine networking principles and their protocols		
P1 Discuss the benefits and constraints of different network types and standards. **P2** Explain the impact of network topology, communication and bandwidth requirements.	**M1** Assess common networking principles and how protocols enable the effectiveness of networked systems.	**D1** Evaluate the topology protocol selected for a given scenario and how it demonstrates the efficient utilisation of a networking system.
LO2 Explain networking devices and operations		
P3 Discuss the operating principles of networking devices and server types. **P4** Discuss the interdependence of workstation hardware and relevant networking software.	**M2** Explore a range of server types and justify the selection of a server for a given scenario, regarding cost and performance optimisation.	
LO3 Design efficient networked systems		
P5 Design a networked system to meet a given specification. **P6** Design a maintenance schedule to support the networked system.	**M3** Analyse user feedback on your designs with the aim of optimising your design and improving efficiency.	**D2** Critically reflect on the implemented network, including the design and decisions made to enhance the system.
LO4 Implement and diagnose networked systems		
P7 Implement a networked system based on a prepared design.	**M4** Recommend potential enhancements for the networked systems.	
P8 Document and analyse test results against expected results.		

Acknowledgement

I needed the assistance and advice of several reputable people to complete my task successfully. I'd like to start by thanking ESOFT for providing me with a welcoming workspace where I could finish my task. I'm very happy that the report is finished. I want to express my gratitude to Mr. Bevan Sir for her helpful instructions for assignments throughout my first semester. Finally, I'd like to share my sincere appreciation to all of the family members and classmates who helped me a lot in finalizing this project within the limited time.

THANKYOU SO MUCH!!!

ACTIVITY 01

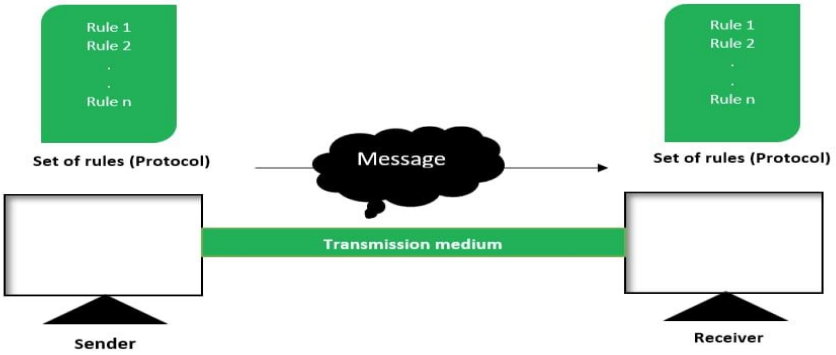
Introduction to Networking

A system network is a collection of networked devices, including servers, routers, switches, computers, and other hardware and software components, that can interact and share resources. Networks serve a range of services, including file sharing, Internet access, and data transfer. Ethernet, WI -FI, Bluetooth, and TCP/IP are some of the technologies and protocols used to build networks. To ensure performance, security, and dependability, networks must be carefully planned, configured, and managed. Network engineers and administrators are in charge of developing, configuring, managing, and protecting computer networks for businesses, organisations, and people.

(Staff, 2022)

Introduction about data communication

Data communication refers to the transfer of digital data between two or more devices or units. This data transfer can occur via wired and wireless connections as well as other communication mechanisms.



(Anon., 2023)

Data transmission is critical in today's culture because it enables information to be accessed and exchanged in real time, independent of physical location. The primary purpose of data communication is to ensure the efficient and accurate flow of information between various entities such as people, organisations, and systems. To interact properly with one another, devices or entities must use protocols and standards.

Computer Networking

A computer network is a system that allows two or more computing devices to communicate and share information. A cell phone and a server are both examples of computing devices. These devices are typically connected via physical lines such as fibre optics, although they can also be wireless. (Mohanakrishnan, 2024)

Advantage of Networking

- **Central data storage**

A central node (file server) allows you to store files and make them available to all users in your organization.

- **Anyone can connect to a computer network**.

The skills required to connect to a modern computer network are very basic. Registration is also easy, so even small children can use it with confidence.

- **Rapid problem solving**

By splitting a long process into several short processes, each of which is handled by a connected device, a specific problem can be solved more quickly.

- **Reliability**

Data backup is necessary to ensure reliability. If an equipment failure, crash, etc. occurs and the information on one PC is compromised or inaccessible, another copy of the same information can be used in the future on another workstation, so operations can continue.

- **Highly adaptable**.

The technology is known to be very adaptable, allowing users to learn all they need to know about key concepts such as programming without sacrificing usefulness.

❖ **Ensuring security through authentication**

Furthermore, the system is responsible for the security and protection of information. Only authorized system users can access specific data sets or applications, so no one else can compromise the security or protection of the information.

Disadvantage of network

❖ **Expensive**

Network execution may be costly in the event of an initial setup since wires and cable costs are significant, and occasionally equipment is also pricey.

❖ **Viruses and malware**

In a computer network, viruses can spread through the network to other computers.

❖ **Network management**

Network management is difficult because it requires experienced personnel to manage such a large network. People who take on this role must be trained.

❖ **Information loss**

When a computer network fails, data can be lost or become inaccessible for long periods of time.

❖ **The system can be hacked**

The threat of system hacking exists in the case of Wide Area Networks (WAN). Some security mechanisms should be included to prevent similar incidents.

Characteristics of Network

➢ **Security**

One of the most important characteristics of a computer network is security. Currently, most organizations rely on computers connected through a network. Therefore, if the computer network technology is not robust and secure, unauthorized access to the company's important data may occur. On the other hand, today's computer network technologies mainly provide the highest level of security and prevent unwanted access.

- **Reliability**

Computer networks are very reliable technologies, and users can use these technologies to quickly connect their devices. To ensure high reliability, computer networks contain many power sources. Whether a user needs to print, check messages, join a meeting, or access data from another computer, the network experience remains consistent.

- **Scalability**

The ability to grow as needs change while maintaining good performance is called scalability. The Internet is the best example of scalability. Many new users join and communicate with other devices over the Internet, and our network continues to function normally.

- **Data flow**

Users use computer networks to access and send data, such as files, documents, and other types of information. It is a vital component of computer networks as it allows data to be transferred from one device to another.

- **High performance**

The time taken for a command is used to evaluate performance. If the time taken to send data is short and the response is fast, the ability to transfer data and utilize more resources is a great advantage to the user. Using multiple processors improves performance.

- **Fault tolerance**

Computer networks also have good fault tolerance. Imagine two devices are connected to each other through both wired and wireless channels. If the sender device is sending information and the wireless medium is failing at the receiver device, it will determine the best alternative option and send the information to the receiver device (wired medium in this case). This means that you can continue working even if the network goes down or is interrupted. This is how fault tolerance works.

- **Quality of Service**

This means that users can prioritize and change data transfers while reducing transfer delays. Moreover, if this is done regularly, data loss can be avoided. Hence, another feature of computer networks is that they provide a high level of service to their users.

- **Compatibility with hardware and software components**

Another great benefit of computer networks is that multiple connected devices can access the same software. This means that the same program can be used on different devices. This will increase compatibility and allow this work to be completed. As a result, computer networks make the software easier to use and make better use of the physical components. (mayank_bohra, 2024)

Types of computer networks

WAN (Wide Area Network)

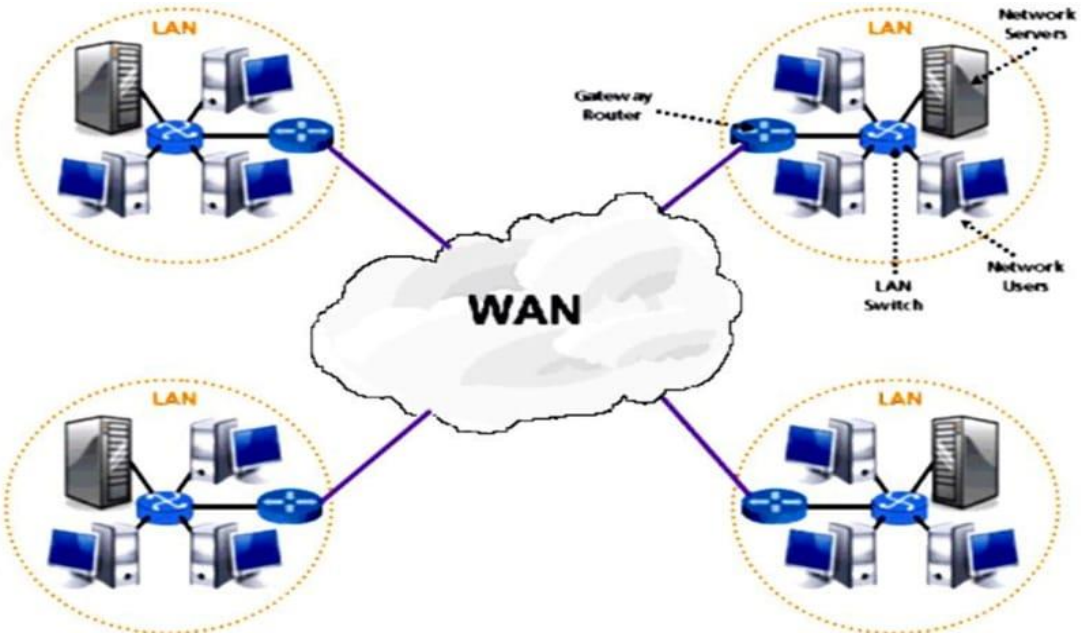
A wide area network (also known as a WAN) is a type of computer network that connects several smaller networks across a large geographic area. Wide area networks (WANs) can connect computers in multiple cities, countries, or even continents.

Advantages of WAN

WANs enable remote offices and users to connect to a central network and share resources like printers, servers, and databases. WANs can be configured to handle a wide range of communication protocols, making them extremely adaptable to changing business requirements. Businesses that need to grow their network infrastructure should employ WANs, which can handle a huge number of users and devices. WANs enable network administrators to control and monitor all connected resources and devices from a centralised location.

Disadvantages of WAN

Because WANs necessitate distinct technology and long-distance connections, they are frequently more expensive, and creating and maintaining one can be challenging and require specialised expertise and skills. Hacking, data theft, and unauthorised access are among security issues that can affect WANs. The performance of real-time applications such as video conferencing and online gaming can be impacted by the complexity of WAN connections and data transmission over vast distances.



(Hadjira, 2020)

LAN (Local Area Network)

A local area network (LAN) is a group of computers and peripherals connected to a specific geographic area, such as an office building or campus. The devices are connected to a server through a shared communication line or wireless connection. A LAN can serve as few as two or three users in a home office, or thousands of users in a corporate headquarters. Homeowners and IT administrators set up LANs to allow network nodes to communicate with each other and share resources such as printers and network storage. A LAN contains various network components such as cables, switches, routers, firewalls, load balancers, Wireless Access Points (WAPs) etc. A LAN can connect various network devices such as: gaming consoles, servers, desktop and laptop computers, printers, Internet of Things (IoT) devices.

Advantages of LAN

The advantage of a local network is that it is fast and cheap. If you want to build a network at a lower cost and with more flexibility, you should consider a local network. If you need to access data, you need to log into your computer and get all the data from the server. All the data on the connected computers is secured on a single server with authentication. LAN software programs are also shared and can be part of the programs that all the devices on the network can use. This is because it is expensive to buy licenses for all the devices on the network. It is more secure to have the information on the server. If you want to add or remove data from the server, you can do it quickly on your computer and the information is easily accessible on other devices. You can grant users access to this specific data. Devices connected through a LAN communicate directly at very high speeds, depending on the LAN model and

the Ethernet cables installed. The maximum speeds can be 10Mbps, 100Mbps, or 1000Mbps. LANs are a cost-effective and simple form of communication. The Internet is easy to connect to a network. The speed of data and information transfer is higher than others. LANs can be expanded at any time, and users can add or remove computers or devices from the network without affecting the entire network.

Disadvantages of LAN

The security of information and data can be violated by unauthorized or unauthorised users. Users can misuse our confidential data and information, which can occur due to technical errors or misconfiguration of Internet devices. A local area network is the design or installation of a building or apartment. It is not possible to set up a LAN network within a wide area network, as LANs have limited resources and are not very powerful. If the files on the server are corrupted or crash, it will cause problems in the operation of all computers connected to the network. Purchasing communication hardware devices such as hubs, switches, routers etc. is expensive. Large office LANs require experts to manage and solve organizational problems. Building a LAN is expensive as software needs to be installed on the LAN servers. This is considered to be one of the disadvantages of LAN as it takes time to copy files and information from one place to another with USB sticks and other external storage media. LANs cover a small area for networking. LANs require a lot of upgrade and maintenance efforts. Data and security breaches are discovered frequently. Cables and connectors are often easily damaged. Computers and devices often fall off the network easily. Troubleshooting network-related issues requires expert advice and support, which can sometimes be costly.

(Anon., 2023)

WLAN (Wireless Local Area Network)

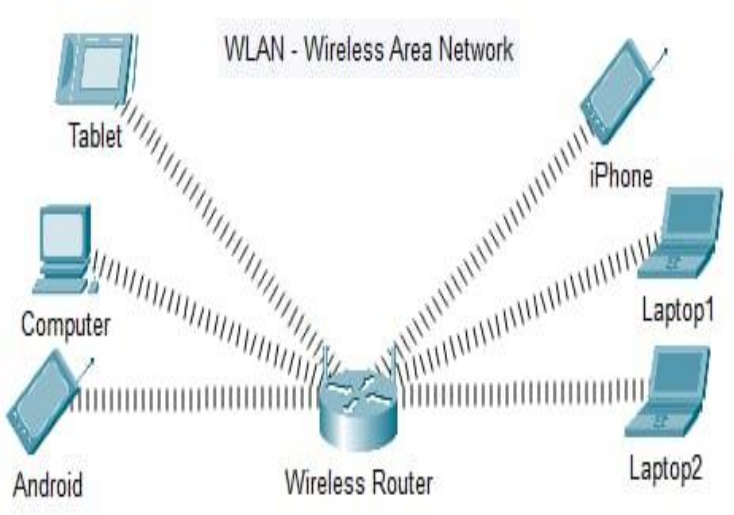
The term "WLAN" describes a specific kind of computer network that allows wireless connections and communications between devices over a constrained space, such as university, office, or house.

Advantages of WLAN

It is a reliable method of communication. It's reduces the number of physical cables, making it a versatile method of communication. WLAN also reduces the value of ownership. This makes it easier to add or remove workstations. It covers a small area at high speed. You can move your workspace and stay connected. Sunlight is not required for propagation. The direction of connectivity are often anywhere i.e. you'll connect devices in any direction unless it's within the range of access point. Easy installation and you would like don't need extra cables for installation. It's also useful during disasters such as earthquakes and fires. Wireless networks can connect people during any disaster.

Disadvantages of WLAN

WLAN requires a license. It's a limited area to hide. Government authorities can control the signal flow of WLANs and even limit it if necessary. This affects data transmission from connected devices to the Internet. As the number of connected devices increases, the data transfer speed decreases. It's uses frequencies and can interfere with other devices using those frequencies. In the case of rain or thunderstorms, communication can be interrupted. It has low security, so attackers can access the data transmitted. The signal can also be affected by the environment compared to using fibre optics. Radiation from WLAN is often harmful to the environment. WLAN is more expensive than cables and hubs because it has an access point. You can receive signals from the nearest signal through the access point. It's required to vary the network card and access point when standard changes. You still need LAN cables to act as the backbone of the WLAN. Because WLAN uses frequencies, data transfer speeds are slower than wired connections. There is a high probability of errors occurring. Communications are not secure, which means unauthorized users may gain access.



(Stungnet, 2023)

Virtual Private Network (VPN)

A VPN (Virtual Private Network) is a service that offers a safe and encrypted online connection. Internet users can use a VPN to better their online privacy and anonymity, as well as to avoid regional restrictions and censorship. A VPN essentially extends a private network onto a public network, allowing users to securely send and receive data over the Internet.

Advantages of VPN

A VPN should allow you too securely and remotely log into your corporate network and software at any time, from anywhere in the world, and on any device. Your team members should be able to enjoy the same benefits they get from being in the office, whether they're at home, in a co-working space, in a hotel, or on an airplane. VPNs are relatively easy to install and use, and it doesn't take long to train your organization's teams on how to use them. VPNs offer companies the benefits of improved security and regulatory compliance. This is especially true for remote and hybrid teams. It is equally useful for on-site teams. This way, customer data is securely transmitted over a VPN instead of over an open, insecure network. Regulatory compliance is especially important in industries that handle sensitive data, such as healthcare, insurance, and financial services. When your team works remotely, they access systems and files over the home internet or public networks, neither of which are as secure as a VPN or cloud-based SaaS network. There is a big risk that files and data will be intercepted by cybercriminals and hackers. Maintenance is also the responsibility of the provider, making it more cost-effective. A VPN or other SaaS-based software is managed by the provider, so it does not require hardware storage space on your internal servers.

Disadvantages of VPN

Slower connection speeds

One of the most common disadvantages of using a VPN is that it can slow down your Internet connection speed. Because VPNs route your traffic through remote servers and encrypt data transmissions, you may experience slower browsing speeds and longer latency, especially when connecting to servers far from your physical location.

Cost considerations

While many VPN providers offer free or low-cost subscriptions, premium VPN services with advanced features and faster servers often require a subscription fee. For budget-conscious users, the cost of maintaining a VPN subscription may outweigh the perceived benefits, especially if your need for enhanced privacy or geo-blocking features is minimal.

Complexity and technical challenges

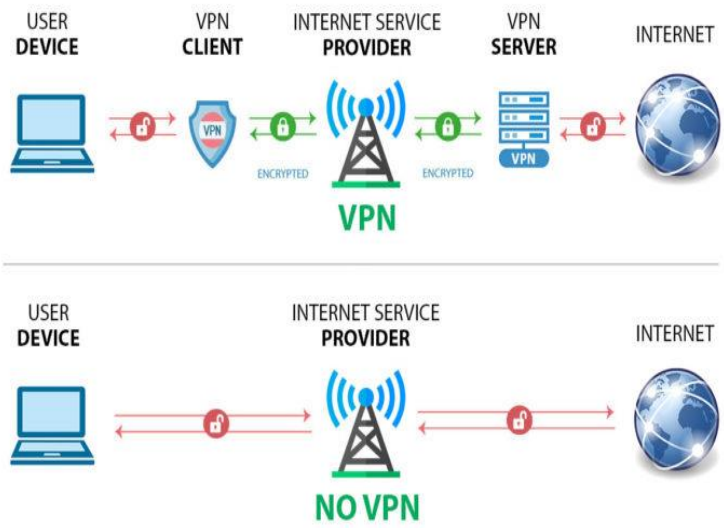
Setting up and configuring a VPN can be daunting for inexperienced users, especially when it comes to advanced features such as encryption protocols, server selection, and split tunnelling. Additionally, troubleshooting connection issues, DNS leaks, and compatibility issues with certain applications and devices may require technical expertise, which can be difficult for non-technical people.

Potential for abuse

Although VPNs offer legitimate privacy and security benefits, they can also be used for nefarious purposes, such as circumventing copyright laws, performing illegal activities, and evading law enforcement. As a result, some VPN providers may face scrutiny and legal challenges due to their users' actions, which could tarnish the reputation of the technology as a whole.

Trust a reliable provider

To ensure the security and privacy of your online activities, it is paramount to choose a reputable and trustworthy VPN provider. However, not all VPN services are created equal, and some may employ questionable practices, such as logging user data, selling user information to third parties, and violating encryption standards. Users should do thorough research and due diligence before trusting their data to a VPN provider.



(Mendenhall, 2022)

Software-Defined Networking (SDN)

Software-Defined Networking (SDN) is an approach to network management that enables dynamic, programmatically efficient network configuration and improves network performance and monitoring by separating the control plane (which determines where traffic should be sent) from the data plane (which actually moves packets to the selected destination).

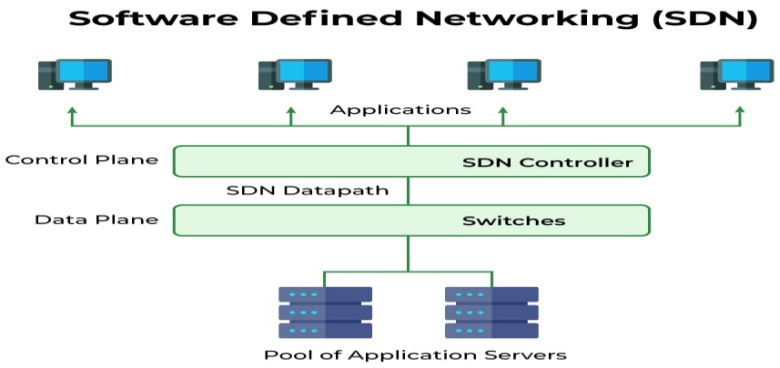
Advantages of SDN

The network is programmable, changes can be made more easily through the controller rather than through individual switches. Only one data layer is required for each switch, switch hardware is less expensive. Hardware is abstracted, applications can be written on the controller regardless of the switch vendor. Security is improved because the controller can monitor traffic and implement security policies. For example, if the controller detects suspicious activity in network traffic, it can redirect or drop packets. It enables centralized management of the network, simplifying network configuration and monitoring and enables dynamic and flexible network configuration, making it easy to scale the network up or down as needed. SDN automates many network management tasks, reducing the need for manual intervention and reducing the risk of human error. It's reduces costs by optimizing the use of network resources and reducing the need for proprietary hardware.

Disadvantages of SDN

SDN has been around for several years, but it is still a relatively new technology compared to traditional networking approaches. Some organizations may hesitate to adopt SDN due to concerns about its maturity and reliability, especially for mission-

critical applications and large-scale deployments. There is a perception that SDN is not robust enough to handle the complexities and high availability requirements of operational networks, which can lead to potential performance issues and downtime. SDN can improve network security in many ways, but it also introduces new security risks that must be carefully addressed. A centralized SDN controller becomes a single point of failure, and if compromised, an attacker may gain complete control over the entire network. Therefore, it is important to secure the communication channel between the controller and its network devices. In addition, the programmability of SDN may introduce new attack vectors, leading to disruptions and security breaches, as malicious code and applications can be introduced into the SDN ecosystem. Implementing SDN can be a complex and challenging process, especially in large heterogeneous networks with traditional infrastructure and multiple vendors. Integrating SDN with existing network components, protocols, and management systems can be difficult, requiring extensive planning, testing, and possibly hardware or software upgrades. Enterprises may also need to retrain or acquire new skills for network personnel to effectively manage and operate SDN environments, further increasing deployment complexity and costs. Although SDN theoretically promotes vendor-independent open standards, in practice, interoperability issues may arise between SDN solutions from different vendors. Although SDN theoretically promotes vendor-independent open standards, in practice, interoperability issues may arise between SDN solutions from different vendors. Some SDN controllers or network applications may not work smoothly with third-party hardware or software, which can result in vendor lock-in and compatibility issues. Moreover, as SDN evolves and new standards and protocols emerge, organizations may need to adapt or migrate their SDN infrastructure, which may result in disruption and additional costs. SDN promises to improve network performance and scalability, but there are concerns about whether SDN controllers can effectively handle large deployments and high-throughput environments. If not properly designed and implemented, a centralized control plane can become a bottleneck, resulting in poor performance and latency issues, especially in scenarios with high network traffic volumes and frequent policy changes. SDN adoption often requires significant upfront investments, including new hardware, software, training, and migration costs.



(de, 2024)

The Melbourne office and Darwin office of the BlueScope Company should use the following network types.

In Melbourne office the Local area network (LAN) is needed for the wired connection in each department. Wireless local area network (WLAN) Nis needed for the Wi-Fi in meeting rooms and customer service area .Virtual private network (VPN) and this is helpful for the secure intra branch communication with Darwin. In Darwin office Local area network (LAN) is also use for the wired connection in the surrounding of the office .Wi-Fi of the customer service area of the Darwin office is connected Melbourne office through the Virtual private network (VPN)Melbourne office and Darwin office of the BlueScope Company offices require secure and scalable network solutions in order to maintain secure of the information that company needed to maintain a devises such as IoT, smart devices, and business operations to support. Wi-Fi connectivity is essential for some departments (Sales & Marketing, Customer Service, and Boardroom) but must be segregated for security. VPN connectivity will be used for intra-branch communication to ensure secure and encrypted communication between Melbourne and Darwin.

Introduction of network models

In computing, a network model is a database model designed as a flexible way to represent objects and their relationships. Its special feature is that a graph, viewed as a graph where the object types are nodes and the relationship types are arcs, is not limited to a hierarchy or grid.

The network model was originally invented by Charles Bachman and developed in 1969 as a standard specification published by the consortium Conference on Data Systems Languages (CODASYL). This was followed by another publication in 1971, which became the basis for most applications. Further work continued into the early 1980s, culminating in the ISO specification, but had little effect on the products.

The Bachman effect is recognized in the term Bachman diagram, a schematic notation that represents the schema of a database expressed by a network model. In the Bachman diagram, labelled rectangles represent record types and arrows represent one-to-many relationship types between records (CODASYL artyps). (Mindmatrix, 2024)

Introduction to network topology

Network topology refers to the logical or physical structure of connections and devices in a computer network. It shows the connections and communications between the various devices and network components.

There are 2 network topology. These are

- Physical topology
- Logical topology

- Physical topology refers to the actual physical layout of the network and it describe how the network of the one devices are physically connected with one another network

- Logical topology refers to the abstract representation of the data flow of and is transmitted within a network and its help's to define the proper channel and maintain the network

Types of network topologies

- Network Topology

Network topology describes the logical or physical configuration of a computer network. There are numerous types of network topologies, such as the following:

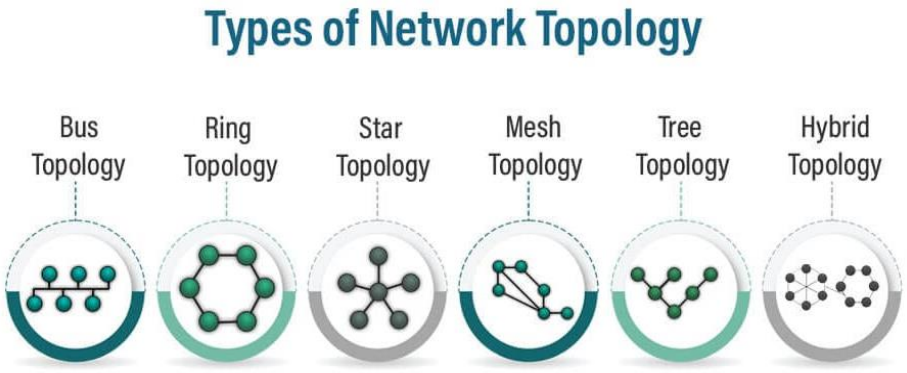
- Bus Topology - All devices are interconnected by a single cable in a bus topology.
- Star Topology - All devices are linked together via a star topology, or central hub or switch.
- Ring Topology - All devices are linked together in a circle using a topology called a ring.
- Mesh Topology - Each device in the network is connected to every other device, or in a mesh topology.
- Tree Topology - Multiple star networks are connected to a main bus in a tree topology, which combines the bus and star topologies.
- Hybrid Topology - A hybrid topology is a network topology in which two or more different topologies are combined to form a single network.

Every topology has unique advantages and disadvantages, and it is best suited for specific network sizes and application kinds. The topology choice is influenced by a number of factors, including traffic flow, network size, and the required amount of redundancy.

The importance of network topologies

The impact that network topologies have on cost-effectiveness, scalability, dependability, and performance makes them important. The network topology that is employed can have an impact on the reliability of the data transmission, ease of administration, and error-resistantness. Since each network topology has unique benefits and drawbacks, the optimal network architecture for a given application must be selected. Network topologies affect the network's security as well as its ability to handle increasing traffic volumes as it grows. Thus, choosing the right network design could ensure the highest level of affordability, scalability, and network performance.

There a lot of network topologies. There are,



(pedamkar, 2024)

1. **Star topology**

Star topology refers to the network design that can be connected directly with central nodes and it is called as hub. The star topology not connected to each other and do not communicate with each other but instead pass the messages to the central nodes and the topology will forward the messages either to all the connected network or the specific destination system .And the connection from clients to the hub is done through coaxial cable or RJ-45 cable.

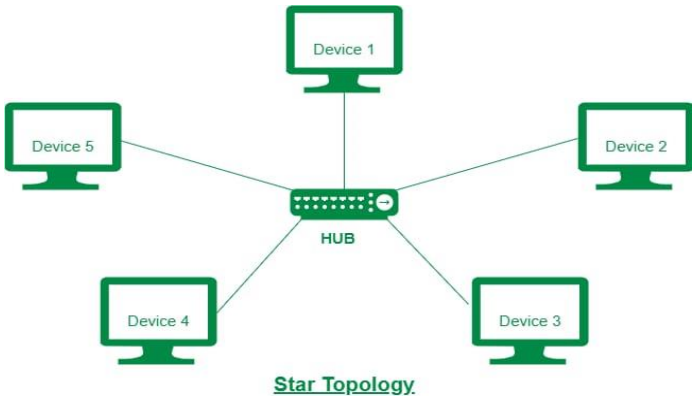
Advantages of star topology

If one cable or device breaks, others will continue to work. This works well because there are no data collisions. This is cheaper because each device only needs one I/O port and only one connection link to the hub. Easier to install in working environment. Errors

are often easy to find because connections are easily visible. There is no network interruption when devices are plugged in or unplugged. Each device only needs one connection to connect to the hub. If you have N devices connected in a star, you only need N cables to connect them. So queuing is easy.

Disadvantages of star topology

If a network switch fails, the connected nodes are disabled and cannot communicate. The cost of the interface device (network switch) is higher .If one bar breaks, all the bars break; without them, no device will work. Hubs are central system, so they require additional resources and regular maintenance. Requires additional hardware (hub or switch) which increases costs. Performance depends on a single hub.



(ashushrma378, 2022)

2. Mesh topology

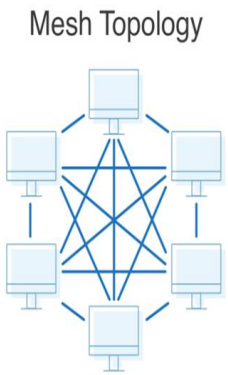
In computer networking, a mesh topology is a network architecture in which all devices are linked to all other devices, creating a "mesh" of connections. Because every device in the network has many paths to access every other device, this improves redundancy and fault tolerance. In a mesh design, every device acts as a data relay, transmitting data through a number of intermediary devices to the target device. This makes it possible for numerous data transmissions to take place at once, improving network performance and reducing congestion.

Advantages of Mesh Topology

By guaranteeing that data can still be sent over alternate paths in the event that a connection or node fails, a mesh architecture offers fault tolerance. Because nodes may be added to the network with ease and without affecting the performance of other nodes, a mesh architecture is incredibly scalable. Data can be transmitted across numerous pathways simultaneously in a mesh architecture, which results in a high bandwidth. Through the use of several channels for encrypted data transmission, a mesh topology enhances security.

Disadvantages Mesh Topology

A mesh topology, in which each node is connected to every other node, can be challenging to create and manage. Mesh topologies can be more expensive than other topologies and require more gear and cabling. Because it requires monitoring several pathways to ensure effective data transfer, a mesh topology can be challenging to maintain. A fully-connected mesh architecture is unfeasible due to the exponential growth in connections needed as the number of devices increases.



(Contributor, 2019)

3. Bus Topology

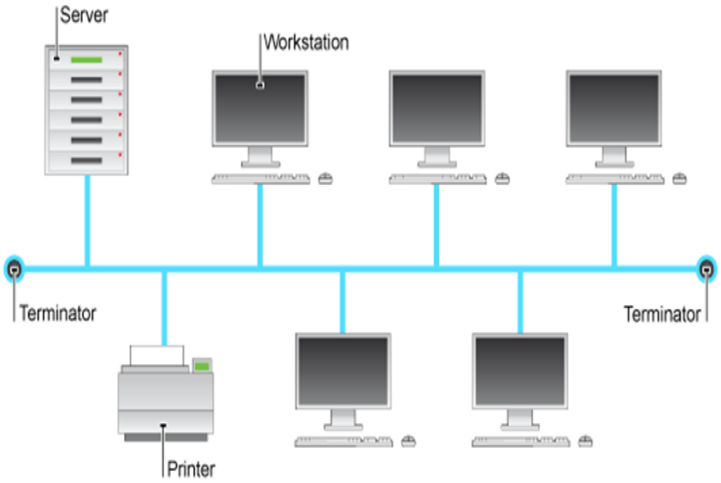
With a bus topology computer network, every device is connected to every other device by a single channel of communication called a "bus." Every device connected to the network gets all communications; only the ones meant for it are processed. Along the bus, data is transferred both ways. For small networks, bus topology is easy to use and reasonably priced, but if there is an issue with the bus itself, it may have performance issues and be difficult to resolve.

Advantages of Bus Topology

One of the easiest and most direct network topologies to set up is a bus topology. Bus topologies use minimal hardware and cabling, making them an affordable choice for small networks. It is easy to add additional devices to a bus architecture without causing any network disruptions. The fact that the remainder of the network is still functioning regularly makes it simple to locate and isolate the issue.

Disadvantages of Bus Topology

A bus topology can only handle a certain number of devices and has restricted scalability. If the cable breaks, the network as a whole breaks. Bus topologies are not appropriate for larger networks that need longer cable runs since the core wire's length is restricted. Because every device in a bus architecture is connected by a single cable, data access and network hacking by unauthorized users is facilitated.



(Khan, 2022)

4. Ring Topology

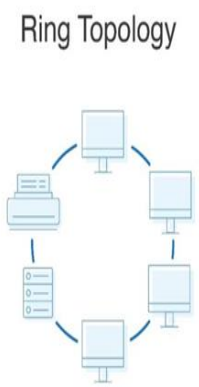
In computer networking, a ring topology is a set up where devices are physically connected to two additional devices, one on each side of the configuration, forming a circular chain. Data travels in a single direction from one device to the next around the ring until it arrives at its destination. High dependability is one of the many advantages of a ring topology, as there is only one device that can fail and no single point of failure in the network. It might also be easier to manage because all of the devices are set up in an easy-to-understand structure.

Advantages of Ring Topology

In a ring architecture, data is sent progressively from one node to another. Bus topology can lead to collisions, which are eliminated by ring topology. Ring topologies are easy to maintain because of their closed loop structure, which facilitates problem identification and troubleshooting. Fault tolerance is achieved by ring topologies, which permit data transmission in both directions.

Disadvantages of Ring Topology

A ring architecture because every data packet sent over the network needs to be processed by every node in the ring. The proper operation of each node in the network is necessary for ring topology, and if one node fails, restricting a ring topology's ability to scale. When ring concentrators and other additional gear are needed, ring topologies can be more expensive than bus topologies.



(Contributor, 2019)

5. Tree Topology

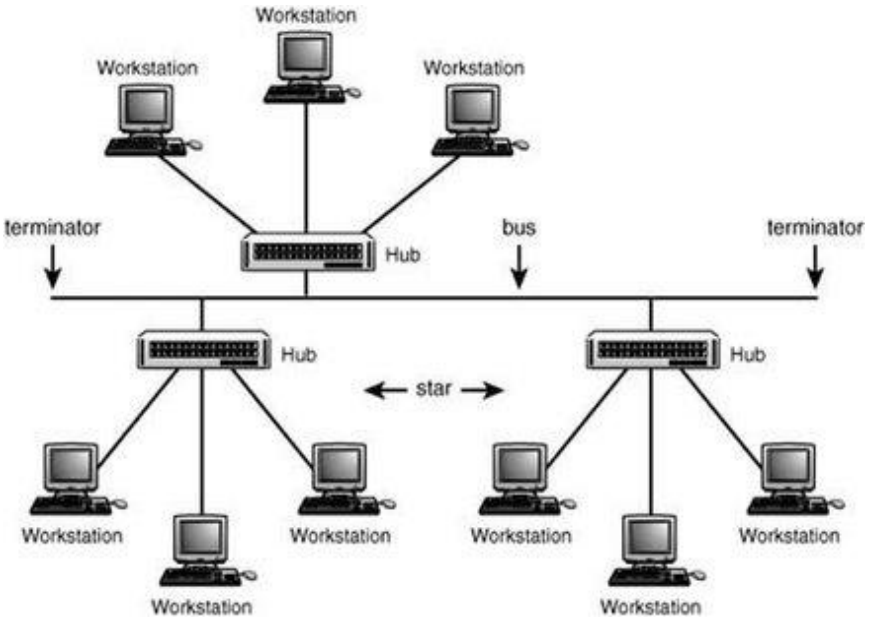
A computer network design known as a tree topology arranges numerous devices in a hierarchical tree-like structure, with a tree structure at the top and one or more layers of child nodes branching out below it. New child nodes can be connected to each other by existing child nodes to form a branching tree structure. Large networks, such those in businesses or universities, usually utilize this architecture because of its well-known scalability, flexibility, and ease of maintenance.

Advantages of Tree Topology

Large networks can benefit from tree topology due to its great scalability and simplicity of accommodating a large number of nodes. Nodes can be added or removed without impacting the network as a whole. The tree topology hierarchy is easy to handle and may be managed at each level individually. Given that it can be designed to provide fault tolerance and redundancy, tree topology is a trustworthy network design.

Disadvantages of Tree Topology

Tree topology can be expensive to set up and maintain, especially for larger networks. The hierarchical structure of tree topology can be difficult to design and implement. An analysis of a tree topology's performance can take into account factors like network traffic and the number of nodes connected to each level of the tree. The network as a whole may be at risk if the tree topology node fails, since it is a single point of failure.



(Anon., -)

Hybrid Topology

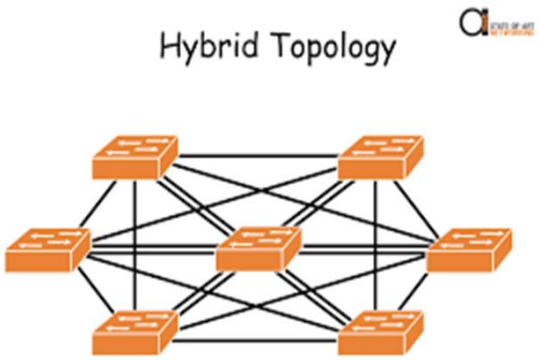
A hybrid topology is a kind of network architecture where a single network is created by combining two or more distinct topologies. In this kind of topology process, we merge two or more distinct topologies to produce a resultant topology that contains, rather than just one, the greatest aspects (and the worst aspects) of all of the component basic topologies. The topology mix is completed in compliance with the requirements of the organization. For example, in an office setting where one department uses a mesh topology and another a star topology, connecting these topologies will result in a hybrid topology that combines the best features of both mesh and star topologies.

Advantages of Hybrid Topology

The benefits of multiple topologies are combined into one topology using this topology. Changes are feasible in accordance with the requirements. It is extremely adaptable. Error identification and correction are easy. The speed of a topology rises when two topologies are merged.

Disadvantages of Hybrid Topology

It's an expensive network. The design of a hybrid network is very intricate. Large numbers of cables are required during the installation procedure of hybrid architectures because they are usually greater in scale. The installation procedure is challenging. Hubs, which join two distinct networks, can be highly costly.



(Anon., 2018)

Network topology needed for the Darwin office is star topology and mesh topology.

Introduction to Network protocols

Network protocols are a collection of rules that control communication between two or more devices through a network in a simple, trustworthy, and secure manner.. These protocols provide the structure, timing, order, and error handling for data communication between devices. Network protocols are formal standards and norms that specify communication between two or more devices via a network. They are made up of rules, methodologies, and configurations. Protocols must be followed by devices on both sides of a communication exchange in order for information to be sent and received efficiently.

A few instances of network protocols are HTTP, FTP, SMTP, DNS, and TCP/IP.

Numerous organizations and standards agencies have defined and published a number of network protocols over the years. Several of the most significant and well-liked network protocols are:

- File Transfer Protocol (FTP) - FTP enables file transfers between devices.
- Simple Mail Transfer Protocol (SMTP) - It is an application level protocol that is used to deliver email across the internet quickly and accurately.

- Hyper Text Communicate Protocol (HTTP) - A communication system called is used to transfer hypertext between devices. It outlines the means by which the web browser and web server can communicate.
- Internet Protocol (IP) - Is used to identify devices on a network.
- Transmission Control Protocol (TCP) - Data organization used to enable secure transfer between the server and the client
- Domain Name Service (DNS) - Using the (DNS), IP addresses can be converted into human-readable hostnames.

TCP/IP (Transmission control protocol / internet protocol)

End-to-end communication via the internet and other computer networks is made possible by the TCP/IP (Transmission Control Protocol/Internet Protocol) family of network protocols. It consists of two main protocols: Transmission Control Protocol (TCP), which provides stable, ordered, and error-checked data flow between applications, and Internet Protocol (IP), which handles the routing and addressing responsibilities necessary for network device connections. Two other protocols that are a part of TCP/IP are the Internet Control Message Protocol (ICMP) and the User Datagram Protocol (UDP). It is the foundation of the modern internet and the main method of communication for most networked devices.

1. **OSI Model (open system interconnection)**

A theoretical framework that explains the communication within a computer network is called the OSI (Open Systems Interconnection) model. Each of the seven tiers specifies a certain network communication function. They are:

i. **Physical Layer:** The physical layer defines the network's physical components, including its connections, cables, and communication methods.
ii. **Data Link Layer:** The data link layer allows data to be transmitted between two devices that are linked to the same physical network. It also handles the identification and correction of errors.
iii. **Network Layer:** At the network layer, data routing between various networks is carried out. It also provides logical addressing, such as IP addresses.
iv. **Transport Layer:** The transport layer provides safe end-to-end communication between two devices. It ensures that data is delivered in the correct order and manages congestion.
v. **Session Layer:** The session layer is in charge of starting, maintaining, and ending communication sessions between two devices.

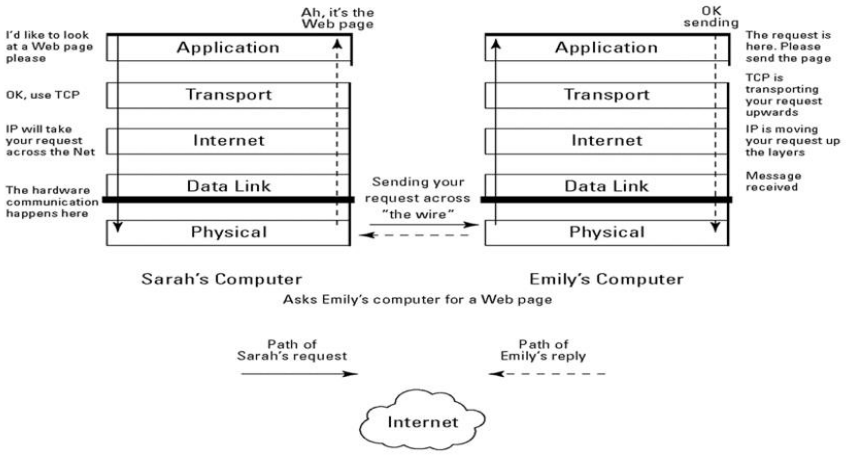
vi. **Presentation Layer:** The presentation layer determines how data is delivered between programs and how it is organized. It oversees tasks including data compression and encryption.

vii. **Application Layer:** The way user apps communicate with the network is defined by the application layer. It is made up of protocols such as HTTP, FTP, and SMTP.

The OSI model guarantees the coexistence of different network technologies and provides a specified framework for network communication. It also provides a consistent language for network engineers to use while analyzing and debugging network issues.

The advantages and disadvantages of the OSI (Open Systems Interconnection)

Advantages	Disadvantages
A common foundation for network communication is provided by the OSI model.	Protocol fitting is a laborious process.
Each layer in the modular OSI model handles a specific task related to network communication.	It is limited to use it as a model of reference.
The OSI model's layered architecture makes it easier to identify and troubleshoot network issues.	Doesn’t specify any particular protocol.
The OSI model provides a systematic way to communicate and comprehend network topics.	Certain services are repeated over many layers, including the transport and data connection layers, in the OSI network layer model.
The OSI model is scalable because of its modular design.	Due to the fact that each layer must wait for data from the one before it, layers cannot operate in tandem.



(Anon., 2015)

IP (Internet Protocol: As an addressing protocol, IP is purpose-built. Mostly TCP is used with it. As messages travel through a network of nodes to their final destination, the IP addresses in the packets help in their routing. Network connections are made using the most widely used protocol, TCP/IP.

There are four layers in all, and each one serves a particular purpose in communication.

i. **Network Interface Layer:** A device is connected to a physical network via the network interface layer, which also provides services for data transmission across the network. It is made up of Wi-Fi and Ethernet protocols.

ii. **Internet Layer:** The Internet Layer is used to route data packets logically between many networks. Internet Protocol (IP), a component of the Internet, is used to route data.

iii. **Transport Layer:** The transport layer provides safe end-to-end communication between two devices. It is composed of TCP and UDP protocols.

iv. **Application Layer:** The way user apps communicate with the network is defined by the application layer. It has several protocols that enable data exchange and network resource access, such as SMTP, HTTP, and FTP.

The TCP/IP paradigm is similar to the OSI model in that it has fewer levels but focuses on the practical features of network communication. It is now the accepted norm for network communication and is extensively utilized in the Internet and other networks.

The advantages and disadvantages TCP/IP model (transmission control / internet protocol)

Advantages	Disadvantages
Since CP/IP is compatible with a large variety of hardware and applications, it offers a flexible networking paradigm.	The tiers' functions are not appropriately divided by the TCP/IP paradigm.
Any size network can be fitted with TCP/IP due to its scalability.	Security was not considered during the creation of the core TCP/IP protocols.
TCP/IP is not governed by a single company or organization since it is based on open standards.	Because the TCP/IP paradigm lacks inherent QoS features, it could be more challenging to assign the highest priority to network traffic for real-time applications.
TCP/IP is easy to modify to meet the specific needs of a network and supports a variety of network protocols.	There are limitations to the administration and monitoring tools available in the TCP/IP paradigm.
Reduced overhead and delay were considered when designing TCP/IP.	While the TCP/IP paradigm is generally flexible, certain protocols within it are less flexible and may not be suitable for all applications or networks.
The internet is built on TCP/IP, which is also widely used by almost all modern networking hardware and software.	This can make setting up and maintaining a TCP/IP-based network more challenging.

HTTP (Hyper Text Transfer Protocols)

Information systems that are distributed, collaborative, and use hypermedia commonly use the application layer protocol HTTP. The web browser serves as the client in this client-server system of operation. HTTP is used to transfer data via the World Wide Web, including text, photos, and other multimedia files. In a request-and-response protocol, the client sends the server a request, which the server processes before sending the client a response.

DHCP (Dynamic Host Configuration Protocol)

Network administrators can automate IP address distribution in a network by using the DHCP communication protocol. Each device utilizing an IP network must have a distinct IP in order to connect to the internet. DHCP enables network administrators to centrally

distribute IP addresses and automatically deliver a new IP address whenever a device connects from a different location on the network. DHCP utilizes a client-server architecture.

DNS (Domain Name System protocol)

In order to translate or map host names to IP addresses, the DNS protocol is helpful. DNS operates using a client-server architecture and a distributed database over a set of name servers.

FTP (File Transfer Protocol)

The File Transfer Protocol, which is built on top of TCP, enables file sharing between hosts, both local and remote. FTP establishes control and data connections on two separate TCP networks to transmit files. Data connections are used to transport actual files, while control connections are used to transfer control information like passwords and commands for retrieving and storing files. For the duration of the file transmission, both of these connections are active simultaneously.

How Protocols Enable the Effectiveness of Network Systems

Network protocols are the crucial backbone to correctly and effectively transmit data across various devices and networks. TCP/IP gives a solid framework for the purpose of communication on the Internet, hence takes care of the reliable delivery of the data packets. HTTP is then employed for the smooth transmission of web pages, while SMTP enables the worldwide transmission of emails. Other protocols include FTP and HTTP that will surely be of great help for authoritative file access and transfer, while TCP and UDP are purposed for carrying out different data transmission needs. These provide different protocols for different network tasks, which allows modular and scalable development. Standards of these protocols realize the interoperability of devices and software into a cohesive and efficient network environment. Modern networking with its vivid applications and services would not be possible without these protocols.

Introduction about IEEE

The Institute of Electrical and Electronics Engineers (IEEE), a professional organization, advances technical innovation and excellence for the good of humanity. The IEEE, which was established in 1963, is the largest technical professional association in the world, with more than 400,000 members spread over more than 160 nations. Its goal is to assist engineering research and development across a range of disciplines and to foster technological excellence and advancement by fostering the creation and use of standards for technology. It also offers its members resources and opportunities for professional growth.

The work of IEEE is most recognized for helping to create standards that are widely utilized by business, the government, and academia to guarantee that technology is dependable, secure, and interoperable. To bring together researchers, engineers, and other professionals from around the world to share knowledge, exchange ideas, and work on projects, it also supports a large number of conferences, seminars, and other events.

Local area network (LAN) and wireless area network are covered by these specifications (WLAN). It is possible to divide the Ethernet IEEE 802.3 LAN into two categories:

- Interconnecting media: An essential component of the Ethernet network design is the medium through which signals are sent. Coaxial cable was one of the original forms of Ethernet connecting media.

- The number 802 has no significance: In the IEEE's project numbering structure, which established standards, it was only the next number.

The IEEE standards in computer networks and their purpose are listed below.

IEEE 802 -LAN/MAN Overview and architecture

IEEE 802.1 -LAN/MAN Bridging and management

IEEE 802.1s -Multiple spanning tree

IEEE 802.1 w -Rapid reconfiguration of spanning tree

IEEE 802.1x -Port-based network access control

IEEE 802.2 -Logical Link Control (LLC)

IEEE 802.3- CSMA/CD access method (Ethernet)

IEEE 802.3ae -10 Gigabit Ethernet

IEEE 802.4 -Token passing bus access method and Physical layer specifications

IEEE 802.5 -Token Ring access method and Physical layer specifications

IEEE 802.6 -Distributed Queue Dual Bus (DQDB) access method and Physical layer specifications (MAN)

IEEE 802.7 -Broadband LAN

IEEE 802.8 -Fiber Optic

IEEE 802.9 -Isochronous LANs (standard withdrawn)

IEEE 802.10- Interoperable LAN/MAN Security

IEEE 802.11 -Wireless LAN MAC and Physical layer specifications

IEEE 802.12- Demand-priority access method, physical layer and repeater specifications

IEEE 802.13- Not used

IEEE 802.14 -Cable modems (proposed standard was withdrawn)

IEEE 802.15 -Wireless Personal Area Network (WPAN)

IEEE 802.16 -Wireless Metropolitan Area Network (Wireless MAN)

IEEE 802.17 -Resilient Packet Ring (RPR) Access

IEEE 802

IEEE 802 is an Institute of Electrical and Electronics Engineers (IEEE) standard set that includes

The physical and data link levels of the Open Systems Interconnection (OSI) paradigm. It defines

Standards and protocols for wired local area networks (WLAN), metropolitan area networks

(MAN), and wireless networks; defines characteristics, operating procedures, protocols, and

Services for networks that carry variable sized packets; and specifies the development and

Handling of compatible devices and equipment.

IEEE 802.3

IEEE 802.3 is a working group of standard standards maintained by the Institute of Electrical and

Electronics Engineers (IEEE) for Ethernet, a form of packet-based physical communication in a

Local area network. It specifies a physical layer and a data link layer for a wired, fast Ethernet

Network connection's media access control, or MAC address. These physical connections are

Formed by copper or fiber cables between nodes or equipment like as routers, switches, and hubs.

In general, IEEE 802.3 standards define the physical medium and operation of Ethernet.

However, there are other variants of this standard in use today.

IEEE 802.6

DQDB (Distributed Queue Dual Bus), an IEEE 802.6 standard, is a MAN (Metropolitan Area

Network) protocol. It is a high-speed shared medium access control protocol that operates on a

Bus network. It features two unidirectional buses for control reasons, and the bus may transfer

Data, video, and audio through a network with bandwidth assigned according to time periods.

The paired bus has the advantage of being utilized to address failure configuration. It has a range

of up to 30 miles at 34-55 Mbps

IEEE 802.11

IEEE standard 802.11 describes Wireless Local Area Network (WLAN) or WiFi. It includes all

WLAN series items. It is designed for a range of about 100 meters. It does not offer the service

Throughout the coverage region, preventing continuous connectivity. In terms of usability, this

802.11 standard offers less scalability

ACTIVITY 02

The operating principles of network devices

Network Devices

Network devices are physical devices that enable computer network hardware to connect and communicate with one another. With the aid of network devices, you may move data quickly, reliably, and correctly over one or more networks. The hardware elements required to construct and run computer networks are known as networking devices. For these devices to operate successfully and efficiently, a set of operating guidelines must be followed. Some of the most widely used networking devices operate on the following principles:

- Switches
- Routers
- Firewalls
- Access Points
- Hubs
- Repeater
- Gateway

o Switches

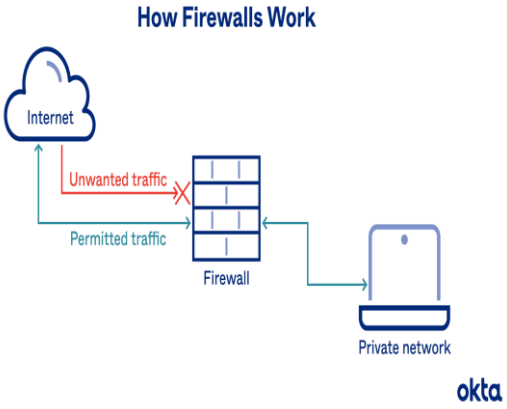
A switch is a multiport bridge with a buffer and a design that can improve efficiency (more ports equal less traffic) and performance. A device at the data link layer is a switch. As it can do error checking before forwarding data, the switch is particularly effective because it only forwards good packets to the intended port and does not transmit packets with problems. To put it another way, the switch separates the hosts' collision domain, while the broadcast domain stays the same

- **Routers**

  Similar to a switch, a router directs data packets according to their IP addresses. The router is primarily a Network Layer device. Routing decisions are made by routers, which typically connect LANs and WANs, using a routing table that is constantly being updated. The router splits the broadcast domains of the hosts linked through it. (geeksforgeeks, 2024)

- **Firewalls**

  Network traffic, including inbound and outbound, is managed by firewalls to provide network security. Data packets are inspected by firewalls before being allowed or blocked in accordance with preset criteria. The IP address, port number, or application type of the source and destination can be used by firewalls to filter traffic.



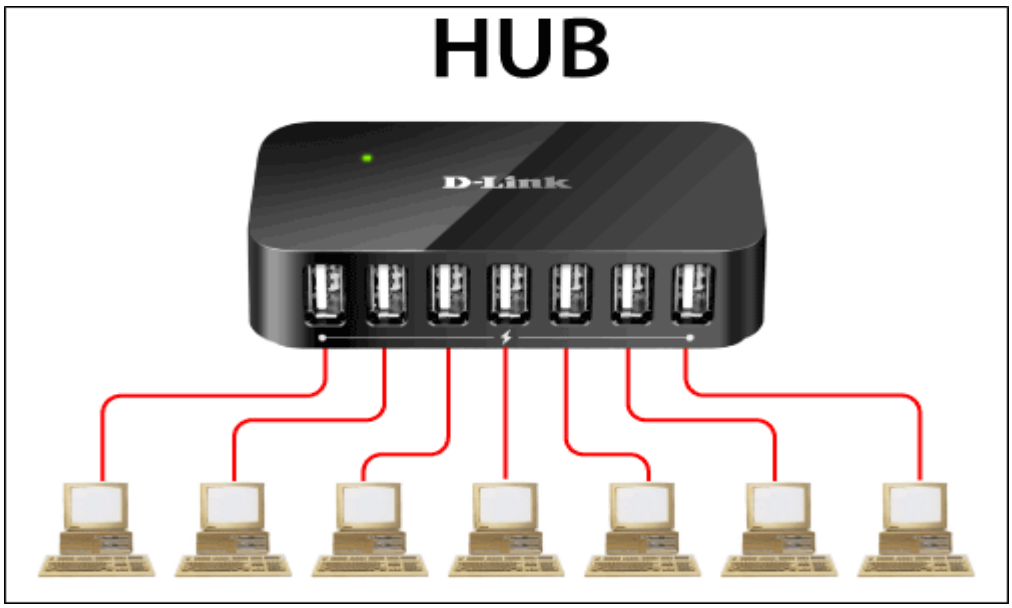
(Okta, n.d.)

- **Access Points**

  Access points are used to link wireless devices to wired networks. By sending out a wireless signal, access points enable wireless devices to connect to the network. Security protocols like WPA and WPA2 are used by access points to safeguard the wireless network and stop illegal access.

Hubs

In general, a hub is a multi-port repeater. A hub joins several wires that come from several branches, like the connector in a star topology that joins various stations. Data packets are delivered to all connected devices since hubs are unable to filter data. In other words, all hosts connected by Hub continue to share a single collision domain. Additionally, they lack the intelligence to choose the best route for data packets, which results in waste and inefficiency.

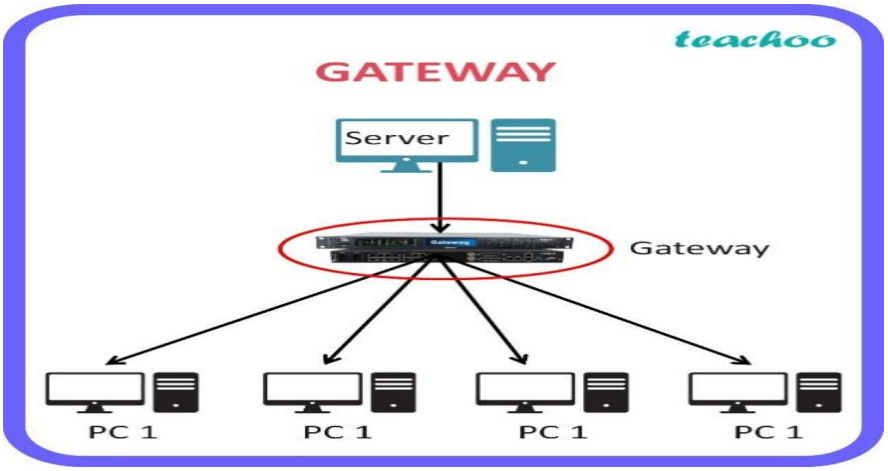


Repeater

A network device that amplifies or regenerates signals is called a repeater. It is a straightforward gadget that boosts signal strength to expand a network's range and functions at the physical layer of the OSI model. In order to overcome signal attenuation or loss in long-distance communication networks, repeaters are widely utilized.

Gateway

A gateway is a networking device that acts as an interface between two different networks or protocols so that they can communicate with each other. A gateway can be a software application or a hardware device that transforms data between two different networks or network segments. The main purpose of a gateway is to enable data transmission between networks that would not be possible otherwise.



Hardware and networking software for workstations

Workstations are computers used for individual or group work. A local area network contains devices called mainframe terminals. For a computer workstation to be connected to the network, a network interface card (NIC) needs to be installed. Input devices, processing units, output devices, and supplemental storage devices are all examples of hardware. The server is a physical and software device that maintains network resources, stores data, and carries out client actions.

Workstation hardware helps organizations interact with one another more effectively, but because it is often only compatible with a small number of networking operating systems, it is challenging for enterprises to migrate to a new one.

A workstation is a personal computer made for single use, while a server running a network operating system manages data, users, groups, security, applications, and other network-related tasks. (Morales, 2024)

Introduction for networking software

Any network needs networking software because it makes it easier for administrators to establish, maintain, and monitor networks. Conventional networks consist of specialized hardware like switches and routers that include networking software as part of the overall solution. By separating the software and hardware, Software-Defined Networking (SDN) makes it simpler to innovate and modify the network. The separation of functions from hardware is known as network functions virtualization (NFV).

Software applications are different from network software. Software applications allow users to carry out specific tasks, whilst the former lets administrators see how the network is really put together. In order to enable seamless access for end users to network resources, network software must be "invisible" to them.

Administrators can access and control data thanks to two crucial features: user management and file management. Administrators can set the location of data storage and user access with file management while adding or removing users from the network with user management. The internet is a worldwide interconnected system of servers and computers because network software enables many devices to connect to one another and to other networks. (sdxcentral, 2023)

Types of networking software

Patch management software

Patch management software is a great approach for IT staff to ensure fast update installation on each device in a network of many devices. It facilitates a smoother operation and makes it possible for each system to download and automatically run updates from a patch controlled by centralized software. Because of this, an organization's equipment and systems no longer require constant updating.

Network Storage software

There are many different ways that data needs to be saved, and network storage software makes it possible for enterprises to manage databases. This enables simple access and addresses security issues.

Asset management software

Asset management software is an effective solution that aids businesses in maintaining their networks at peak performance levels by boosting visibility of their network infrastructure and maintaining frequent tracking and monitoring of crucial indicators. It operates from a central hub or server room and is not tied to any hardware, which lowers costs and enhances user and client experience.

Data arching software

Software for data archiving is an excellent option for businesses that need to save data quickly and effectively. It makes data management easier, lowers expenses, and guarantees data security. It is crucial to make sure that the archived data won't need to be accessed very soon because archive software doesn't operate the same way as ordinary standard backups.

Security surveillance software

Network software needs security surveillance software to monitor and connect security solutions, even if data storage and linking devices are essential network software components. Big networks are perfect for large networks since they offer reliable live and recorded browser-based video. Better-targeted software creates a network

architecture that minimizes attack surfaces and hides components from harmful parties in order to protect weak units. By creating outbound-only connections with cloud service and provider providers, this is accomplished.

Network management software

Network management software is an excellent option for monitoring, managing, and troubleshooting any network performance issues. It is hosted by numerous market-leading companies and provides a range of alternatives to assist businesses in improving network performance.

Deployment and migration software

The key points of the terms "software," "network," "deployment," "movement," and "regular upgrades" are that organizations can manage networks more effectively with the help of migration software, which also offers an interface for simple monitoring of any deployment or data movement between hardware and databases. Additionally, it ensures that all data transfers between normal backups and archives must through compatibility tests, lowering the risk of data loss.

Printer and fax software

Whenever their businesses expand, working organizations require crucial equipment like fax machines and printers. Wi-Fi printing and other common solutions might not always be the ideal option, particularly for large businesses or educational institutions. Organizations may handle several activities, configure IP printers, and distribute updates using this software's user-friendly interface. Additionally, it can allow businesses to print, fax, and distribute papers and correspondence among many locations. (Mohanakrishnan, 2024)

Components of network software

- **Control layer**

The network operating system and network control software make up the system's "brain," which is part of the control layer, which is a crucial element of the architecture. It is in charge of translating requirements from the applications to the network components after obtaining them from the applications. The controller, which makes it possible for top and bottom layer communication through API interfaces, is also used to control infrastructure layer or data plane devices.

- **Infrastructure layer**

Once the infrastructure layer, sometimes referred to as the data plane, has received orders from the control layer, it is in charge of transferring or forwarding data packets. Using the controller's directives as a guide, it manages user traffic.

- **Application layer**

The network information, network status, and network requirements for resource availability and application are all transmitted via the application layer, sometimes referred to as the application plane. It comprises of one or more API drivers and the application logic. (Mohanakrishnan, 2024)

Advantages of network software

- Team members can share files, work together, and interact in real time thanks to network software, which improves communication and collaboration.
- Network software can increase productivity by automating repetitive operations, speeding business processes, and ensuring that all team members are using the same information. This reduces errors and increases efficiency.
- To protect data from unwanted access or breaches, network software provides additional safety functions including access controls, firewalls, and encryption.
- By lowering the requirement for physical hardware and infrastructure, network software can will provide in saving money. Also, it can reduce the need for travel with in meetings, which can save money for organizations.

Server types that used for above scenario while exploring different servers that are Available in today's market with their specifications.

Servers

A server is a computer system or gadget that joins a network and gives other computers or gadgets access to resources, services, or data. It is designed to manage several client demands while delivering services in a trustworthy and effective way. Large-scale data centers that provide cloud computing, storage, and virtualization can be found among servers, as can smaller systems that provide standard functions like file sharing and printing.

Usually, servers are built to run constantly and manage several client requests at once. They can handle more complicated and demanding applications because they have more memory, computing power, and storage than typical client PCs. They are usually kept in safe, climate-controlled spaces with backup power supply to guarantee their availability.

A server is a sophisticated machine that computes, stores and manages data, devices, and systems across a network. This complex computer system makes resources available to networking units in order for them to deliver specialized services such as displaying web pages and sending or receiving emails, among other things. The servers are always operational. Most servers are never shut off since they are typically utilized to supply services that are continually necessary. As a result, when servers fail, they can cause a slew of issues for network users and businesses. Servers are frequently configured to be fault tolerant in order to relieve these concerns.

Types of servers:

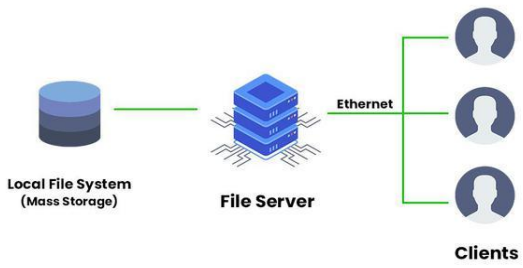
- File server
- Web server
- Email server
- Database server
- Application server
- Virtualization server
- Proxy Server
- DHCP Server
- DNS Server

In generally, because they offer the resources and services necessary for businesses to run successfully, servers are essential parts of contemporary computer networks.

- **Software server**

File server

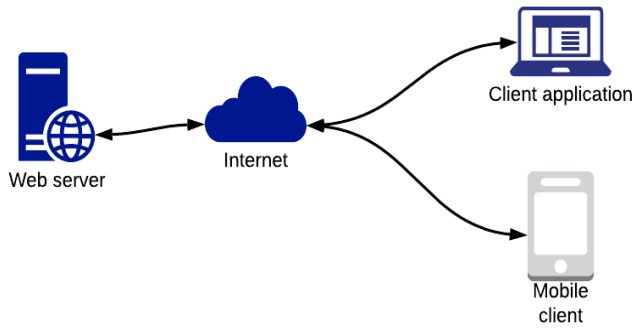
A dedicated server used for managing and storing network-shared data files is called a file server. It can be used to store financial data by the Accounting and Finance Department and administrative files and documents by the Administration Department. File sharing protocols including SMB, NFS, and FTP can be supported by the file server because of its fast CPU and big storage capacity.



Web server

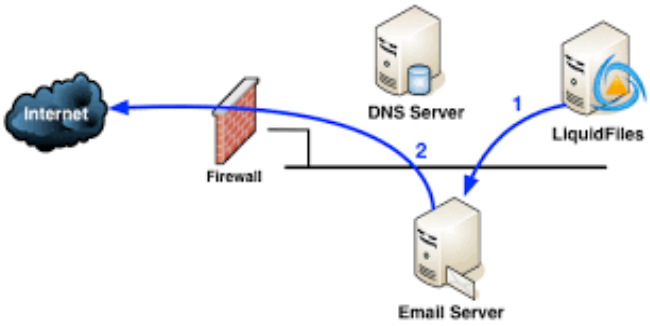
Public domain software is used to access the internet through an open-source web server. These servers establish a connection between user computer and any saved data from an internet website. Information for the internet is stored on web servers and is

retrieved using "HTTP" code before being transferred to your web browser. One of the most popular server types is this one.



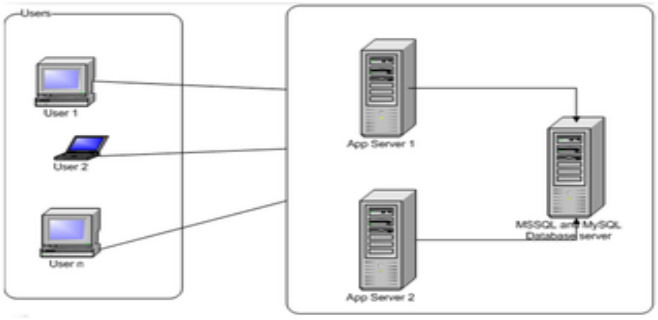
Email server

An email server is a specialized computer that controls email traffic and keeps email messages. It can be used by the Customer Service Department and HR Department to handle email correspondence with clients and staff. The email server should support email protocols like SMTP, POP3, and IMAP and have a fast processor and lots of storage space.



Database server

Large storage areas are served by database servers, which are used and accessed by businesses to run a number of different programs. Depending of the database structures, a database server can operate.

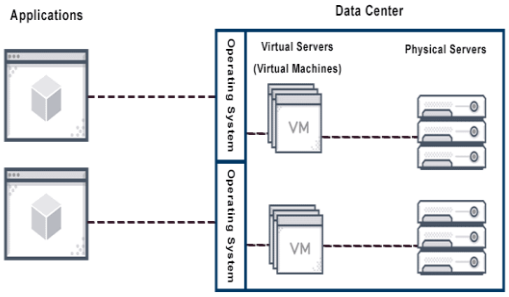


Application server

These servers use virtual server connections to link clients to software programs. Users can browse applications without having to download data on their hardware thanks to this. Application servers are perfect for organizations because they can efficiently host substantial volumes of application data to several users simultaneously.

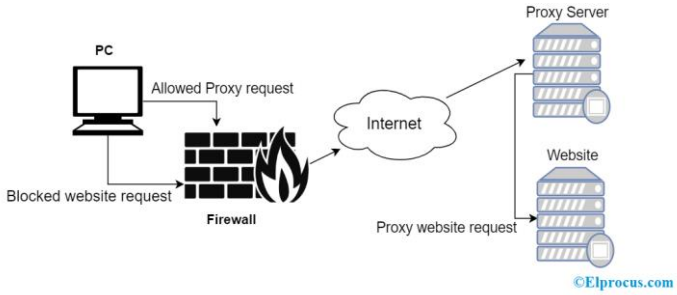
Virtual machine (VM)

Virtual machines only store and connect data in virtual space. IT teams use software called a hypervisor, commonly referred to as a virtual machine monitor (VMM), to build virtual machines. A hypervisor can run hundreds of virtual machines on a single piece of physical hardware. As they are the cheapest sort of server to run, this server virtualization technique is frequently utilized for data transfer and storage.



Proxy Server

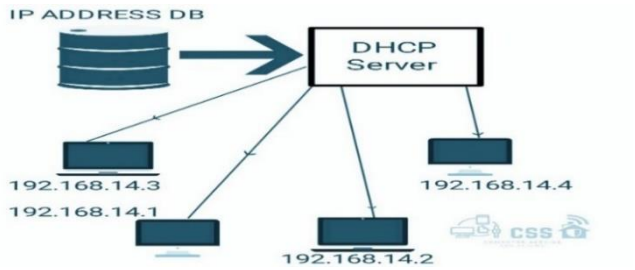
An intermediary between a client and the internet is a proxy server. A web page request made by a client is initially sent via the proxy server. The proxy server then assesses the request, sends it to the internet, and gives the client the response. Software used as proxy servers includes Squid, Nginx, and Apache HTTP Server instances. The exact proxy server software and specs needed by Alliance Health will depend on their business requirements, security requirements, and content filtering needs.



DHCP Server

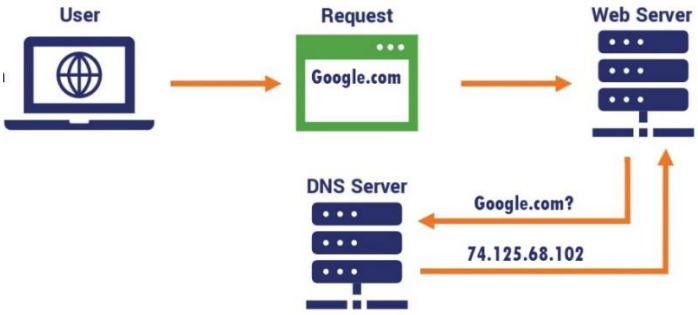
Devices on a network are automatically assigned IP addresses by a Dynamic Host Configuration Protocol (DHCP) server. By allocating IP addresses, subnet masks, default gateways, and other network configurations automatically, DHCP servers can facilitate the setup of new network devices. DHCP servers simplify modifications and network problem solving by centralizing control of IP address allocation and configuration parameters. DHCP servers can aid in IP address conservation by only allocating IP addresses to devices when necessary.

Software for DHCP servers includes Dnsmasq, ISC DHCP, and Microsoft DHCP Server. Alliance Health's network size, device kinds, and other needs will dictate the DHCP server software and specs.



DNS Server

The task of translating human-readable domain names, such as www.alliancehealth.com, into IP addresses, such as 192.168.0.1, which computers use to interact on the Internet, falls to a DNS server. DNS servers enable users to enter domain names instead of IP addresses, which might facilitate connections to network or internet services. Improve network performance by storing the IP addresses and domain names that are frequently accessed in a cache. This will lessen the need for repetitive lookups when enforcing security policies, like preventing access to particular domains, or when detecting and blocking malicious domain names. (Rehman, 2021)



Hardware server

A physical computer designed to supply resources or services to other computers or network devices is called a hardware server. In the context of Alliance Health, hardware servers can be utilized to offer services including file storage, web hosting, application hosting, database administration, and more. When choosing a hardware server, some crucial specifications to take into account are:

- The server's brain is its processor, and a faster processor enables the server to manage more requests and execute more programs simultaneously. The server needs memory, or RAM, in order to execute many services and applications. The better a server can manage high workloads, the more memory it possesses.
- Alliance Health's unique requirements will dictate the kind and quantity of storage needed. Large volumes of storage for files or databases, together with fast storage like solid-state drives (SSDs) for instantaneous data access, may be needed by servers.

- For servers to communicate with other network devices, they need reliable and fast networking capabilities. Advanced network protocol support and high-speed Ethernet interfaces can be necessary. In order to guarantee high availability and reduce downtime in the case of a hardware breakdown, hardware redundancy is essential for mission-critical applications and services.

The most well-known producers of hardware servers are Lenovo, Dell, HP, and IBM. Alliance Health's hardware server selection will be based on a number of criteria, including their budget and unique requirements.

There are 3 main types of Hardware Servers:

- Tower Server
- Rack Server
- Blade Server

- **Tower server**

Tower servers are independent servers designed to resemble towers or desktop PCs. They can be utilized for many different activities, including file sharing, print servicing, and application execution, and are designed with small to medium-sized organizations in mind. Tower servers are easier to set up and maintain than rack or blade servers, and they are also less expensive. Tower servers come in a range of shapes and sizes, from entry-level single-processor models to top-tier multi-processor models with lots of RAM and storage. For small enterprises without a separate data center or server room, they are ideal.

- **Think System ST250 V2 Tower Server**

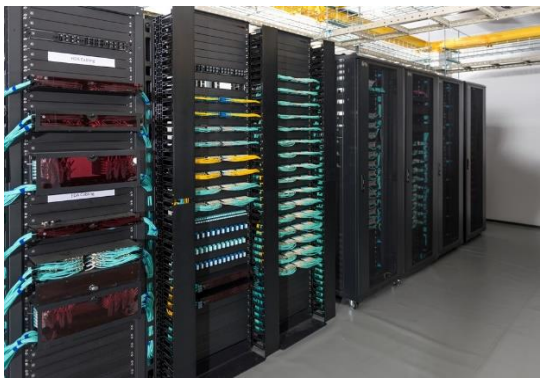
The best tower server in the market Think System ST250 V2 Tower Server is a powerful hardware server manufactured by Lenovo.

- **PowerEdge T350 Tower Server**

Another best tower server in the market Think System ST250 V2 is a high-performance tower server designed for small-to-medium-sized businesses.

- **Rack Server**

These servers are designed to be mounted in a cabinet or rack large enough to hold several servers. Large businesses or data centers that need great density and scalability often utilize rack servers. Database administration, virtualization, and web hosting are just a few of the various uses for them.

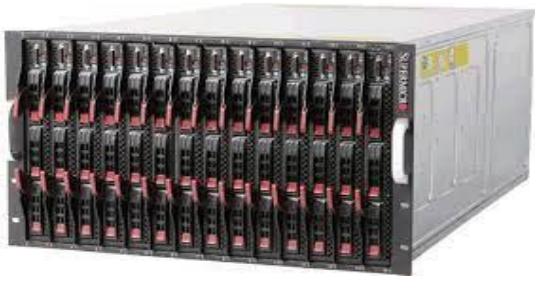


Dell EMC PowerEdge R940

The Dell EMC PowerEdge R940 is a powerful rack server designed for high-performance computing, data analytics, and other demanding workloads. Available in the today's market.

Blade Servers

Blade servers are modular servers that fit into a blade enclosure, which has the capacity to house several blade servers. They are usually utilized in large companies or data centers where scalability and high density are necessary. Because they are easy to maintain and can be hot-swapped, blade servers can be changed out without requiring a system shutdown.



Cisco UCS B200 M6

The Cisco UCS B200 M6 is a blade server that offers high performance and scalability for a wide range of applications. Available in the today's market.

Think System SN850 Blade Server

Another best blade server available market Think System SN850 is a high-end blade server from Lenovo that is designed for demanding workloads and virtualization environments. It offers a flexible, modular design that allows for easy customization and scalability

Introduction for network security

The goal of network security is to stop unauthorized users from accessing network resources, identify and mitigate cyber-attacks and security lapses, and guarantee that authorized users have secure access to the network resources they require. According to IBM's most recent Cost of a Data Breach research, 83% of businesses have had several breaches, with each one costing an average of $4.35 million. In order to defend against cyberattacks, network security maintains the integrity of network resources and traffic

Type's network security

VPNs (Virtual private networks)

Virtual private networks, or VPNs, enable remote workers to securely access corporate networks even when using unsafe public Wi-Fi connections by encrypting their data and hiding its IP address and location. Additionally, they encrypt user traffic to protect it from hackers.

NAC (Network access control)

The role-based access control (RBAC) regulations, which include confirming a user's identification and providing them access to network resources, are enforced by means of NAC solutions. By keeping unauthorized users away from resources, they are not permitted to access and RBAC helps in the prevention of data breaches.

Application security

Applications and application programming interfaces (APIs) are protected from network intruders using application security, which is the process security teams use. Due to the fact that many business apps are hosted in public clouds, which makes it easier for hackers to exploit their weaknesses, firms that utilize apps to manage sensitive data are vulnerable to cybercriminals. (IBM, n.d.)

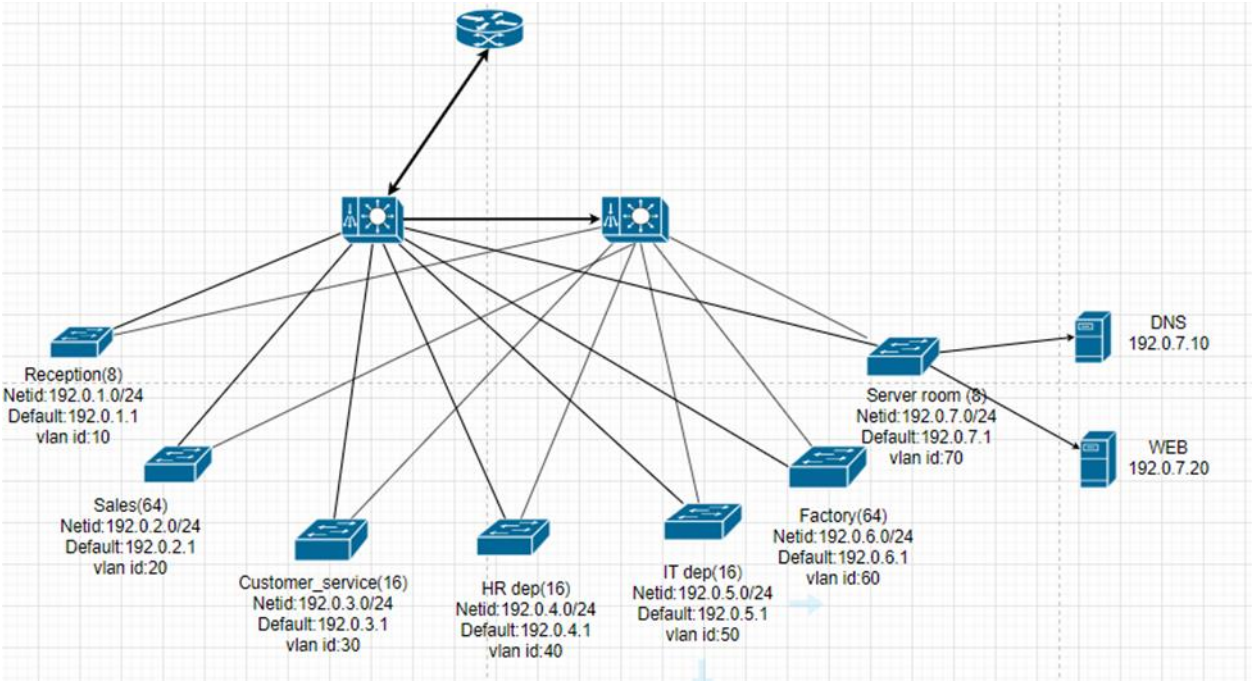
Firewalls

Firewalls are hardware or software that allow valid traffic to pass through while preventing unauthorized traffic from entering or exiting a network. They exist in many shapes and sizes, and they examine traffic via packet filtering. Next-generation firewalls (NGFWs) that are more advanced include threat intelligence feeds, application awareness and control, AI and machine learning, intrusion prevention, and these more security features. Some of these above-mentioned network securities can be used to develop the BlueScope company security.

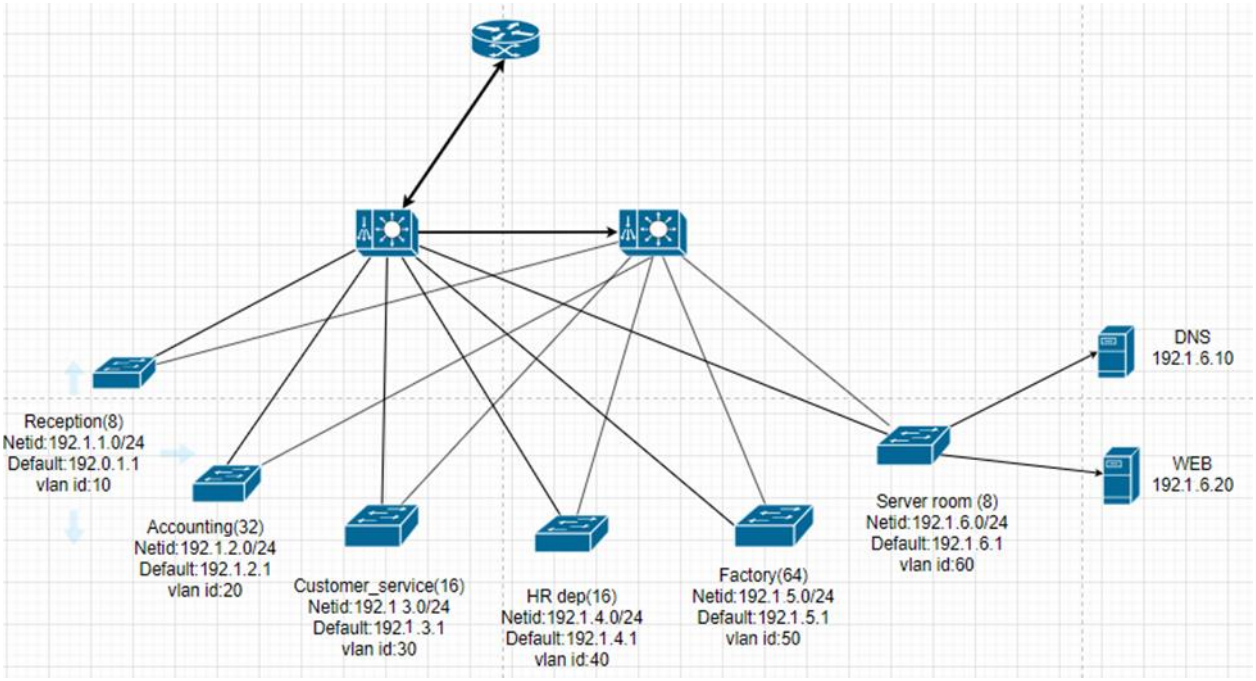
ACTIVITY 03

Network design plan to meet the above mentioned user requirements including a blueprint drawn using a modeling tool.

Branch A blueprint



Branch B blueprint



The list of devices, network components and software used to design the network for above scenario.

The hardware and software needed to set up computer networks in households and companies are referred to as computer network components. A wide range of software is used to plan, create, run, and keep an eye on computer networks. This is known as network software.

Hardware that uses in network

01. Switch 2960.

The 2960 switch is a pretty reliable device to be used for network design in Cisco Packet Tracer, considering the variety of features it has, along with performance. Support of QoS, VLANs, and sophisticated security protocols helps the 2960 enhance network performance and ensure data safety. Its flexibility is open for network growth, and this Layer 2 switching has made it very suitable for connecting devices within one network. Because of its prestige regarding reliability and manageability, the 2960 series is very suitable for small and medium-sized network installations.

02. Server.

The Cisco Packet Tracer network server is a prime hub for data storage and access. It acts like a storage facility for programs and files that can be shared by, and used with, other network devices with ease. The server, therefore, plays a major role in effective management and hosting of applications, with increased productivity and cooperation in the usage of resources within the network.

03. Printer

In other words, adding a printer to a Cisco Packet Tracer network will simulate a basic feature of practical networks. The printer device is part of any extra devices to enable one to boast about connectivity over the network and allow people an encounter with networked resources, such as document sharing and printing. This option raises the realism of the model by showing how, with networks, it would be possible to use and communicate in a corporate or home environment.

04. Router 1941

The Cisco 1941 router is one of the most reliable options for a small to medium-sized network because of its strong performance and adaptability. It provides a secure environment in a network with its built-in security. This is scalable architecture; hence, using modern technologies enables agility in response to shifting network demands.

Therefore, it may be used in many networking scenarios. The 1941 router presents a flexible and low-cost way to deploy the network, as performance, security, and adaptability are well balanced.

05. PCs

In a network simulation, the PC in Cisco Packet Tracer acts as a connecting device. It acts just like a replacement for the workplace, allowing users to access network assets and run applications on the computer-a realistic set of network topology activities. The PC is needed to test the settings of networks concerning their operability in a virtual environment, test the connections, and perform fixing of issues.

06. Copper Straight Through cable.

A Copper Straight Through cable that function at different network levels is coupled with cables, such as when a PC is being connected to a switch or a router. In it, the signal ongoing is preserved, and appropriate connecting devices are enabled by sending data from the transmit (TX) pin on one end to the receive (Rx) pin on the other. Such a cable design is very often used in situations where devices on both ends serve different purposes in data transfer, providing smooth interaction inside a network.

07. Copper cross-over cable.

Cisco Packet Tracer uses copper crossover to connect the same type of devices, like two PCs or routers, without the use of any intermediate device, such as a switch. It enables both ends devices to communicate in both directions, negotiating the transmit and receive cables at one end. Copper crossover cables allow the establishment of a point-to-point link, which directly interchanges data and communicates between similar devices; hence, the network can be effectively designed and tested in virtual environments.

Software's that use in the network.

01. Microsoft Visio.

A good drawing tool that makes it easier to create intricate network designs is Microsoft Visio. Its large form collection and user-friendly interface make it perfect for graphically depicting intricate network systems. Visio enables accurate documentation and efficient network plan communication by streamlining the design process with its configurable designs and smooth interface with other Microsoft Office programs.

02. Firewall software

The firewall software controls the incoming and outgoing network traffic by enacting the pre-defined set of security rules. It keeps the network protected from various external threats through the use of filtering in the traffic and prohibiting probably malicious connections, thus ensuring overall network security.

03. VPN software

The VPN software will create and manage a secure, encrypted connection between the Melbourne and Darwin branches. In this way, any data that is transmitted on the internet will not be accessed by unauthorized users, and secure communication can be granted between the two locations.

04. Cisco packet tracer

Depending on the specifications and network design plan, it may use the following hardware, software, and network components: Equipment: Cisco routers are routers Cisco wireless access points parts that make up a network Connectivity between buildings using fiber optic cable
Ethernet wiring for networking within buildings Networks are segmented using VLANs. IP addresses are assigned using DHCP servers. Resolution of domain names Cisco IOS DNS server software is used to setup switches and routers. Virtualization-based server administration and resource allocation software uses DHCP server software (like ISC DHCP) to manage IP addresses. To resolve domain names, DNS server software—like BIND—is utilized.

05. Network management software

It is used in monitoring and managing network health and performance. It therefore provides means through which configuration of network devices, analysis of patterns of traffic, and troubleshooting issues that may hamper the smooth running and efficiency of the network are done.

Configuration of VLAN and IP Subnetting

- **Head office Melbourne table**

Department	VLAN	IP address	Subnetting	Devices
Reception area (8)	VLAN 10	192.168.1.0/26	255.255.255.192	Computers, switch, phone.
Sales & Marketing Department (64)	VLAN 20	192.168.1.64/26	255.255.255.192	Computers, switch, phone, laptops, printer.
Customer Services Area (16)	VLAN 30	192.168.1.128/26	255.255.255.192	Computer, switch, phone, WIFI.
Factory Area (64)	VLAN 40	192.168.1.192/26	255.255.255.192	Computer, switch, phone, printer.
Warehouse and Distribution (32)	VALN 50	192.168.2.0/26	255.255.255.192	Computers, switch, phone, laptops, printer.
Accounting & Finance Department (32)	VLAN 60	192.168.2.64/26	255.255.255.192	Computer, switch, phone, printer.
Administration Department (32)	VLAN 70	192.168.2.128/26	255.255.255.192	Computers, switch, phone,

				laptops, printer.
HR Department (16)	VLAN 80	192.168.2.192/26	255.255.255.192	Computers, switch, phone, laptops, printer.
Boardroom and Video conferencing room (8)	VLAN 90	192.168.3.0/26	255.255.255.192	Computer, switch, camera, laptop.
IT Department (16)	VLAN 100	192.168.3.64/26	255.255.255.192	Computer, switch, printer
Director suits (8)	VLAN 110	192.168.3.128/26	255.255.255.192	Computer, switch, printer
The Server Room (8)	VLAN 120	192.168.3.192/26	255.255.255.192	Server, computer, switch.

- **Newly established Darwin table**

Department	VLAN	IP address	Subnetting	Devices
Reception area (8)	VLAN 10	192.168.4.0/26	255.255.255.192	Computers, switch, phone.
Customer Services Area (8)	VLAN 20	192.168.4.64/26	255.255.255.192	Computer, switch,

				phone, WIFI.
Factory Area (64)	VLAN 30	192.168.4.128/26	255.255.255.192	Computer, switch, phone, printer.
Ware house and the distribution (64)	VLAN 40	192.168.4.192/26	255.255.255.192	Computers, switch, phone, laptops, printer.
Administration Department (32)	VLAN 50	192.168.5.0/26	255.255.255.192	Computer, switch, phone, printer.
HR Department (16)	VLAN 60	192.168.5.64/26	255.255.255.192	Computers, switch, phone, laptops, printer.
Accounting & Finance Department (32)	VLAN 70	192.168.5.128/26	255.255.255.192	Computer, switch, phone, printer.
IT Department (16)	VLAN 80	192.168.5.192/26	255.255.255.192	Computer, switch, printer
The server Room (8)	VLAN 90	192.168.6.0/26	255.255.255.192	Server, computer, switch.

3.2.4. Ip address calculation

- **Melbourne IP Address**

Department	Network ID	Default Gateway	Subnet mask	Broadcast ID	IP range
Factory Area	192.168.1.128	192.168.1.129	255.255.255.192	192.168.1.191	192.168.1.129-192.168.1.190
Sales & Marketing Department	192.168.1.32	192.168.1.33	255.255.255.192	192.168.1.95	192.168.1.33-192.168.1.94
Ware house and the distribution	192.168.1.192	192.168.1.193	255.255.255.192	192.168.1.255	192.168.1.193-192.168.1.254
Accounting & Finance department	192.168.3.0	192.168.3.1	255.255.255.224	192.168.3.31	192.168.3.1-192.168.3.30
Administration Department	192.168.2.32	192.168.2.33	255.255.255.192	192.168.2.95	192.168.2.33-192.168.2.94
HR Department	192.168.2.96	192.168.2.97	255.255.255.240	192.168.2.111	192.168.2.97-192.168.2.110
IT Department	192.168.3.32	192.168.3.33	255.255.255.248	192.168.3.39	192.168.3.33-192.168.3.38
Customer Service Area	192.168.1.96	192.168.1.97	255.255.255.192	192.168.1.127	192.168.1.97-192.168.1.126
Reception Area	192.168.1.0	192.168.1.1	255.255.255.224	192.168.1.31	192.168.1.1-192.168.1.30

Boardroom and the conference	192.168.2.16	192.168.2.17	255.255.255.240	192.168.2.31	192.168.2.17-192.168.2.30
Director Suits	192.168.2.0	192.168.2.1	255.255.255.240	192.168.2.15	192.168.2.1-192.168.2.14
The Server Room	192.168.10.0	192.168.10.1	255.255.255.0	192.168.10.255	192.168.10.1-192.168.10.254

- **Darwin IP Address**

Department	**Network ID**	**Default Gateway**	**Subnet mask**	**Broadcast ID**	**IP range**
Reception Area	192.168.4.0	192.168.4.1	255.255.255.240	192.168.4.15	192.168.4.1-192.168.4.14
Customer service Area	192.168.4.16	192.168.4.17	255.255.255.240	192.168.4.31	192.168.4.17-192.168.4.30
Factory Area	192.168.4.32	192.168.4.33	255.255.255.192	192.168.4.95	192.168.4.33-192.168.4.94
Warehouse and the distribution	192.168.4.96	192.168.4.97	255.255.255.192	192.168.4.159	192.168.4.97-192.168.4.158
Administration Department	192.168.5.0	192.168.5.1	255.255.255.192	192.168.5.63	192.168.5.1-192.168.5.62
HR Department	192.168.5.64	192.168.5.65	255.255.255.240	192.168.5.79	192.168.5.65-192.168.5.78

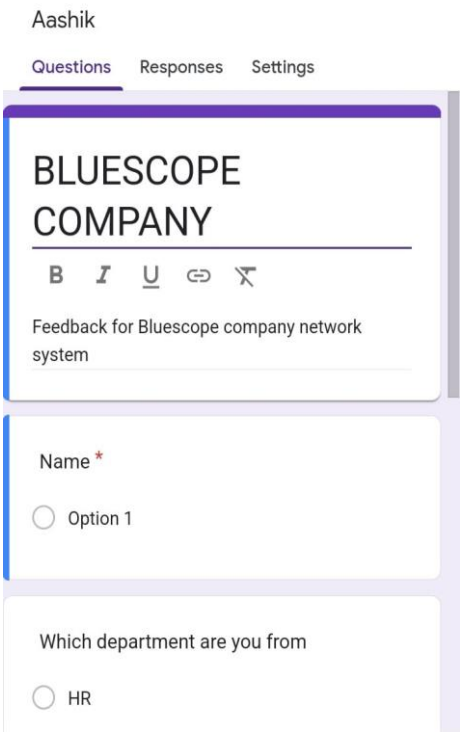
Accounting and finance Department	192.168.5.80	192.168.5.81	255.255.255.224	192.168.5.111	192.168.5.81-192.168.5.110
IT Department	192.168.5.112	192.168.5.113	255.255.255.248	192.168.5.119	192.168.5.113-192.168.5.118
Server Room	192.168.10.0	192.168.10.1	255.255.255.0	192.168.10.255	192.168.10.1-192.168.10.254

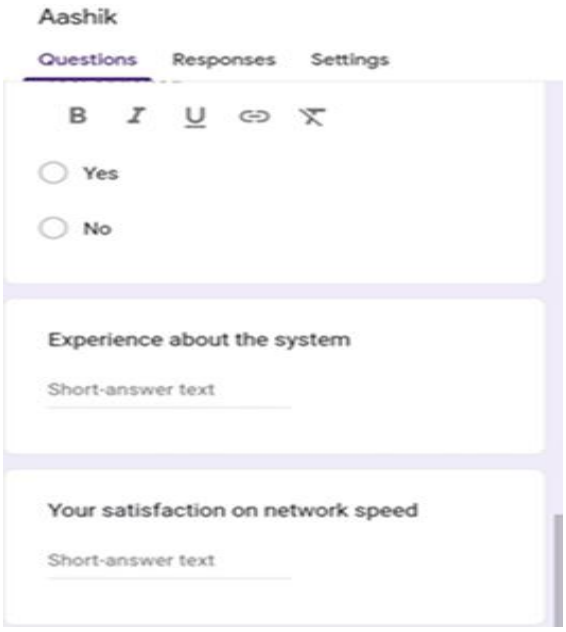
Network maintenance schedule for blue scopes company

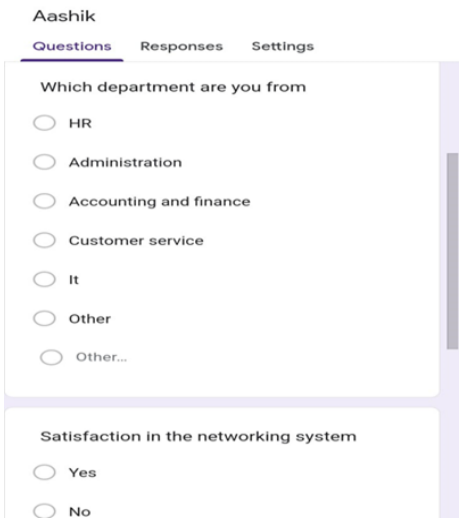
vice	Occurrence	Duration	Notice
Backup schedule			
Email server	Weekly	2 hours	When shutting down our server, we'll provide you 23 hours' notice.
Database server	Daily	2 hours	No additional notes
File server	Daily	3 hours	Will provide 23 hours' notice when taking down Administrative server.
Update testing			
Windows update	Weekly	2 hours	Will provide 34 hours' notice when longer down time is requiring.
Server update	Weekly	2 hours	No additional notes
Security update	Daily	40 minutes	No additional notes

Proposed design to meet the requirements and analyses user feedback by using a User feedback form.

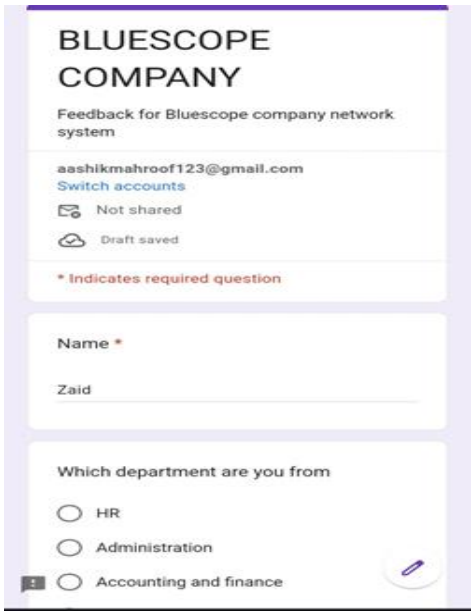
User Feedback form

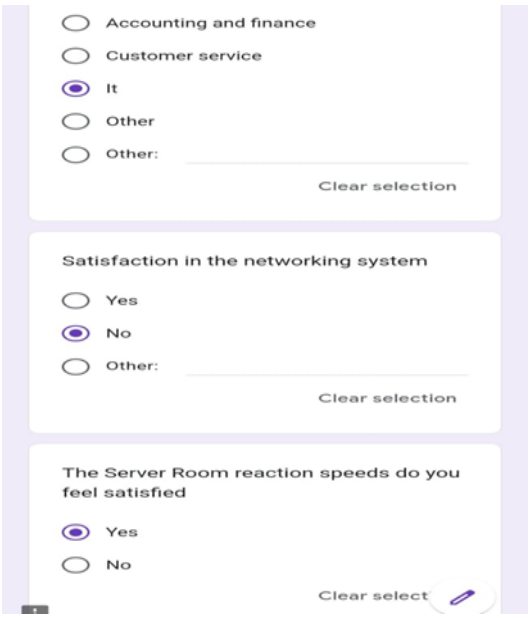


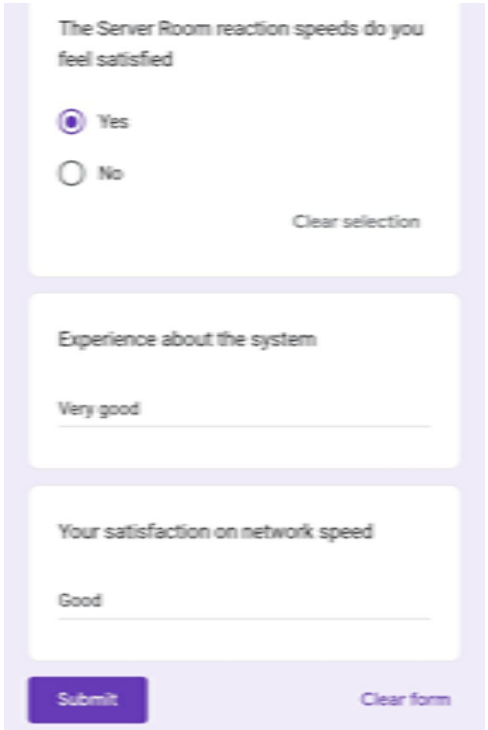




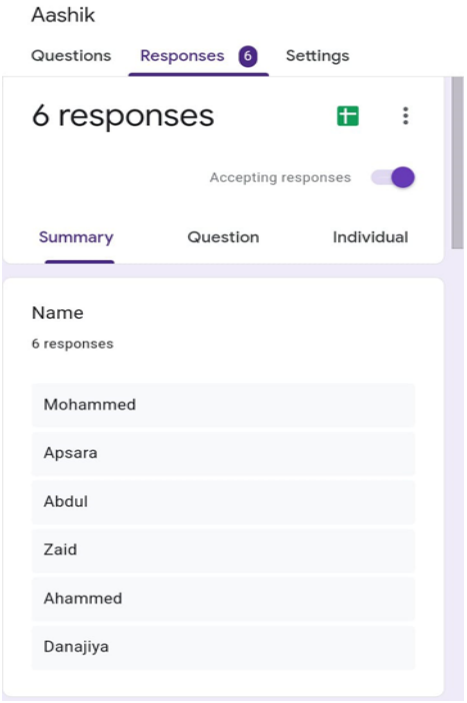
Feedback form 01

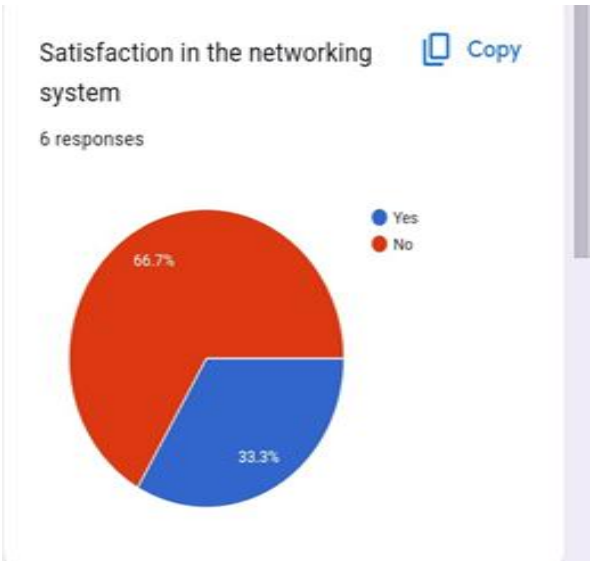


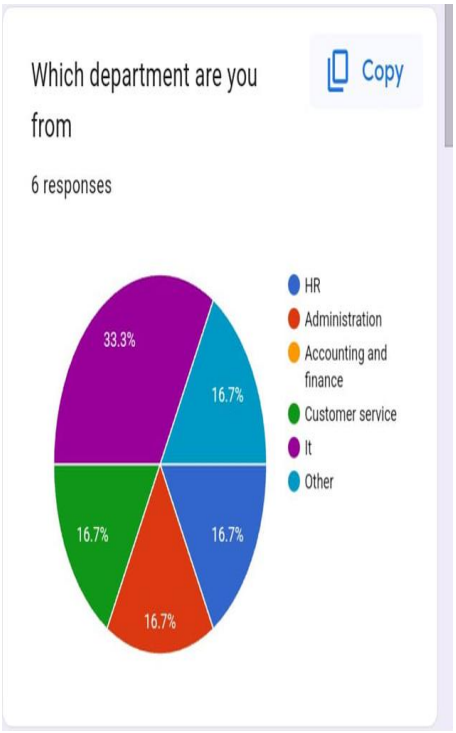


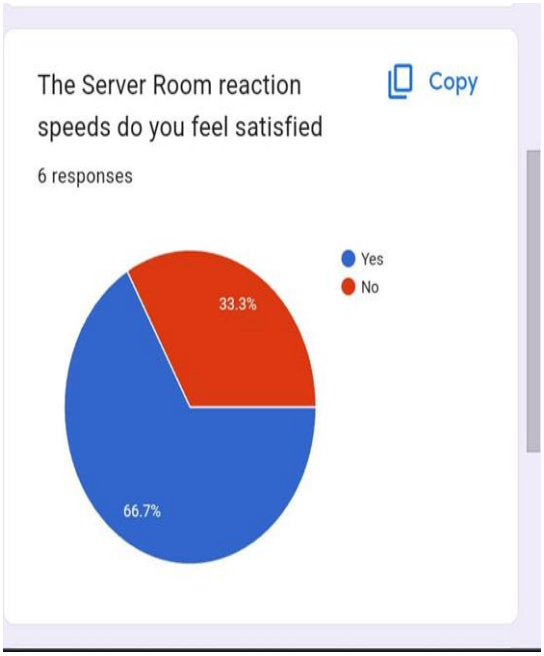


Feedback Analysis









Overall feedback form summary

The feedback form developed aims to gather user experience of BlueScope's Darwin branch network infrastructure to assess its effectiveness and recommend necessary changes. In form, it starts from simple user information such as name and department to associate answers with specific segments of the network. Of course, participants are expected to provide feedback on speed, connection, Wi-Fi signal coverage and the usefulness of the VPN connection.

The hardware and software section has currently created reviews on higher hardware components such as printers, laptops, server accessibility and firewall security. Users evaluate the performance of smart devices, such as automated lighting security systems and how they connect to the network. The information collected relates to the effectiveness of the operation of the selected ERP software, the network and the use of applications and other essential services by the representatives of a particular company.

Satisfaction is also generally evaluated and users report the problems encountered and improve or add information about the idea. The form also asks users to evaluate

network support and maintenance services, verify that the maintenance and support work is efficient and easy for the public. This feedback is very important to solve the problem of improving the network to meet the needs and expectations of users.

Choices and the selection from the network

Segmentation and Subnets: This segmentation of the network into separate subnets for each service was due to the need for effective traffic management and increased security. We separate network traffic by assigning a single IP range to different services, minimizing congestion and reducing the risk of unauthorized access. This also makes troubleshooting much easier and allows better performance management because problems in one subnet do not directly affect others. The design of the subnet scheme was intended to have sufficient address space and accommodate future growth, thus a balance between current and future scalability.

Hardware Selection

Routers, switches and access points should be chosen based on their performance and scalability. High-quality routers and managed switches are chosen to support inter-server traffic and provide easy VLAN maintenance. Access points were selected based on their ability to provide reliable Wi-Fi coverage in critical areas such as customer service and conference rooms. This hardware is implemented to ensure that the network can support a significant volume of traffic and provide a stable connection, which is extremely important for the operational efficiency of offices powered by BlueScope technology.

VPN Implementation

That is why setting up a VPN gateway of connectivity for the Melbourne and Darwin branches has a strategic nature: it allows for secure and reliable communication between the two locations. This addresses the need for data encryption across the internet due to sensitive information and privacy. The VPN solution supports full intra-branch connectivity and allows for secure data exchange, vital for operational integrity and collaboration across the branches.

ERP and Application Access

Implementing ERP software and integrating it with the network is crucial for optimizing business operations. Network design must meet ERP system requirements for bandwidth and reliability to effectively manage operations. Easy access to other applications is important for user productivity and operational efficiency.

Maintenance and Support

A structured maintenance and support plan is in place to ensure network reliability and performance. The basis of regular updating and monitoring allowed us to deal with any potential problems in advance. This will ensure security and efficiency so that the network does not waste too much downtime, thus improving user satisfaction. Network design focuses on performance, security and scalability. During network design, it was verified that the network met current operational requirements while being adaptable to future needs. Cumulatively, these decisions together support a robust and efficient network infrastructure to match BlueScope's vision of a technology-enabled office environment.

Activity 04

Creating vlans for the servers

4.1. Network Design

IOS Command Line Interface

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen


Press RETURN to get started!


Switch>
Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#name reception
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name sales
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name customer_service
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name hr
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name server_room
Switch(config-vlan)#
Switch(config-vlan)#exit
Switch(config)#
```

Share the vlans for the switches

```
Switch(config)#vtp domain a
Changing VTP domain name from NULL to a
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#
Switch(config)#
```

Enable vtps to switches

Switch 1

Reception

```
Switch>
Switch>enable
Switch#configure teminal
                 ^
% Invalid input detected at '^' marker.

Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain a
Changing VTP domain name from NULL to a
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#
Switch(config)#
```

Sales

```
Press RETURN to get started!


Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain a
Changing VTP domain name from NULL to a
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#
```

HR

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain a
Changing VTP domain name from NULL to a
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#
```

Server room

```
Switch>enable
Switch#congigure terminal
                 ^
% Invalid input detected at '^' marker.

Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain a
Changing VTP domain name from NULL to a
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#
```

Configuring interface to other switches fom server switch

Sales

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain a
Domain name already set to a.
Switch(config)#vtp mode client
Device mode already VTP CLIENT.
Switch(config)#
Switch(config)#interface range fa0/23-fa0/24
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#
```

HR

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain a
Domain name already set to a.
Switch(config)#vtp mode client
Device mode already VTP CLIENT.
Switch(config)#
Switch(config)#
Switch(config)#interface range fa023-fa0/24
                                 ^
% Invalid input detected at '^' marker.

Switch(config)#interface range fa0/23-fa0/24
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#
```

Configuration that has enable to vlan information

Default vlan

```
Switch>enable
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Gig0/1, Gig0/2
10   reception                         active
20   sales                             active
30   customer_service                  active
40   hr                                active
50   server_room                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/1-fa0/22
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Assigning vlan default to reception

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/1-fa0/22
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
10   reception                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22
20   sales                             active
30   customer_service                  active
40   hr                                active
50   server_room                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Assigning vlan default to sales

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
10   reception                         active
20   sales                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22
30   customer_service                  active
40   hr                                active
50   server_room                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Assigning vlan default to HR

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
10   reception                         active
20   sales                             active
30   customer_service                  active
40   hr                                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22
50   server_room                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Assigning vlan default to server_room

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/24, Gig0/1, Gig0/2
10   reception                         active
20   sales                             active
30   customer_service                  active
40   hr                                active
50   server_room                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Router configuration

```
Router#enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#interface gi0/0/0
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#ip dhcp pool reception
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default
% Incomplete command.
Router(dhcp-config)#default-router
% Incomplete command.
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns 192.168.10.10
Router(dhcp-config)#exit
Router(config)#
```

```
Router(config)#ip dhcp pool sales
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns 192.168.10.10
Router(dhcp-config)#exit
Router(config)#
```

```
Router(config)#ip dhcp pool customer_service
Router(dhcp-config)#network 192.168.3.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#dns 192.168.10.10
Router(dhcp-config)#
Router(dhcp-config)#exit
```

```
Router(config)#ip dhcp pool hr
Router(dhcp-config)#network 192.168.4.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.4.1
Router(dhcp-config)#dns 192.168.10.10
Router(dhcp-config)#
Router(dhcp-config)#exit
```

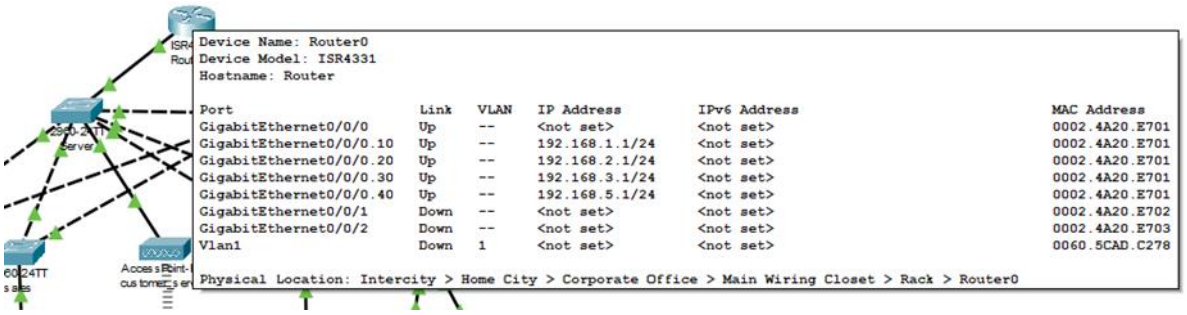
Assigning sub interface for the vlans

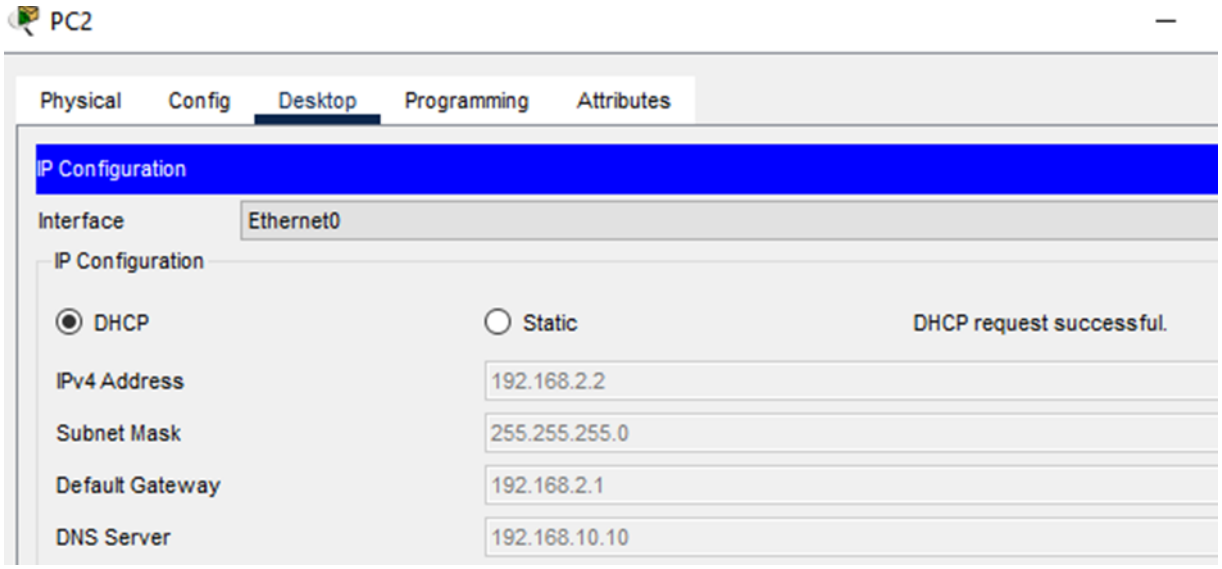
```
Router(config)#interface gi0/0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.20, changed state to
up

Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.2.1
% Incomplete command.
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#exit
```

```
Router(config)#interface gi0/0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.30, changed state to
up

Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#exit
```

```
Router(config)#
Router(config)#interface gi0/0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.10, changed state to
up

Router(config-subif)#encapsulationdot1q 10
                                          ^
% Invalid input detected at '^' marker.

Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#exit
Router(config)#
```

```
Router(config)#interface gi0/0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.40, changed state to
up

Router(config-subif)#encapsulation dot1q 40
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
```





PC1

Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

- DHCP
- Static

DHCP request successful.

IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	192.168.10.10

IPv6 Configuration

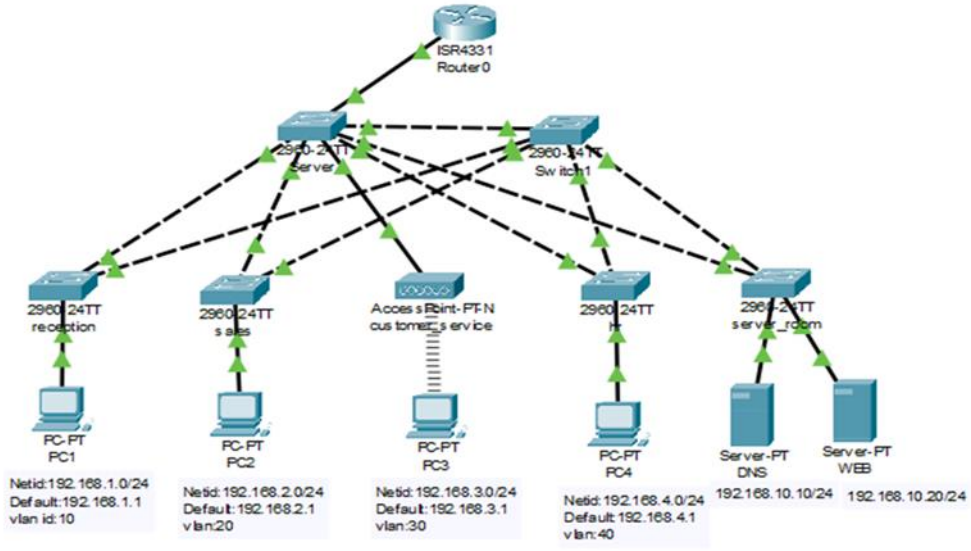
- Automatic
- Static

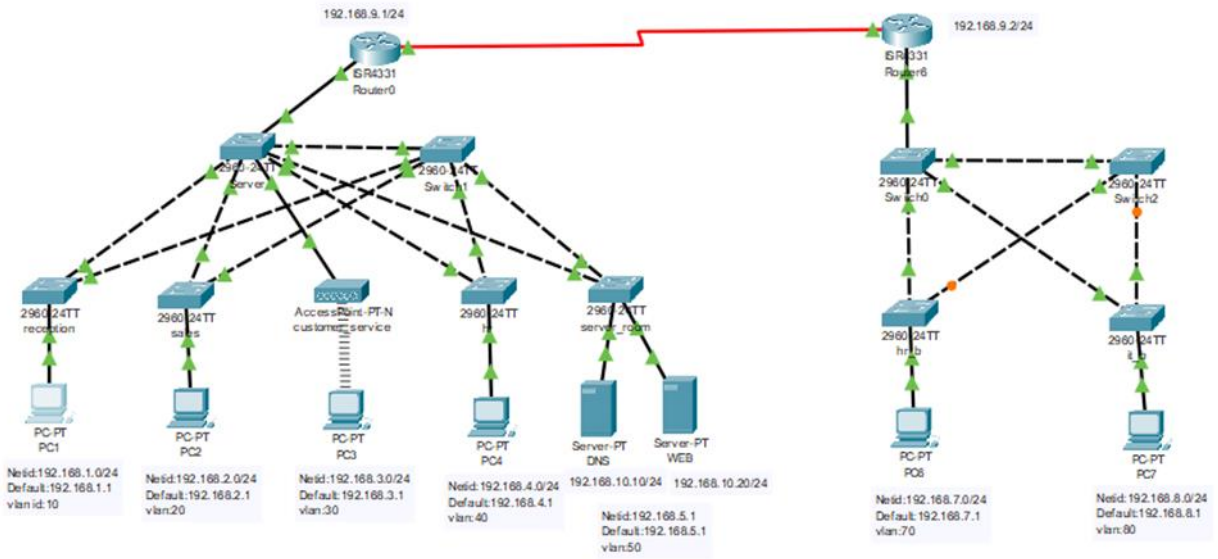
IPv6 Address	/
Link Local Address	FE80::201:C9FF:FE42:9B39
Default Gateway	
DNS Server	

802.1X

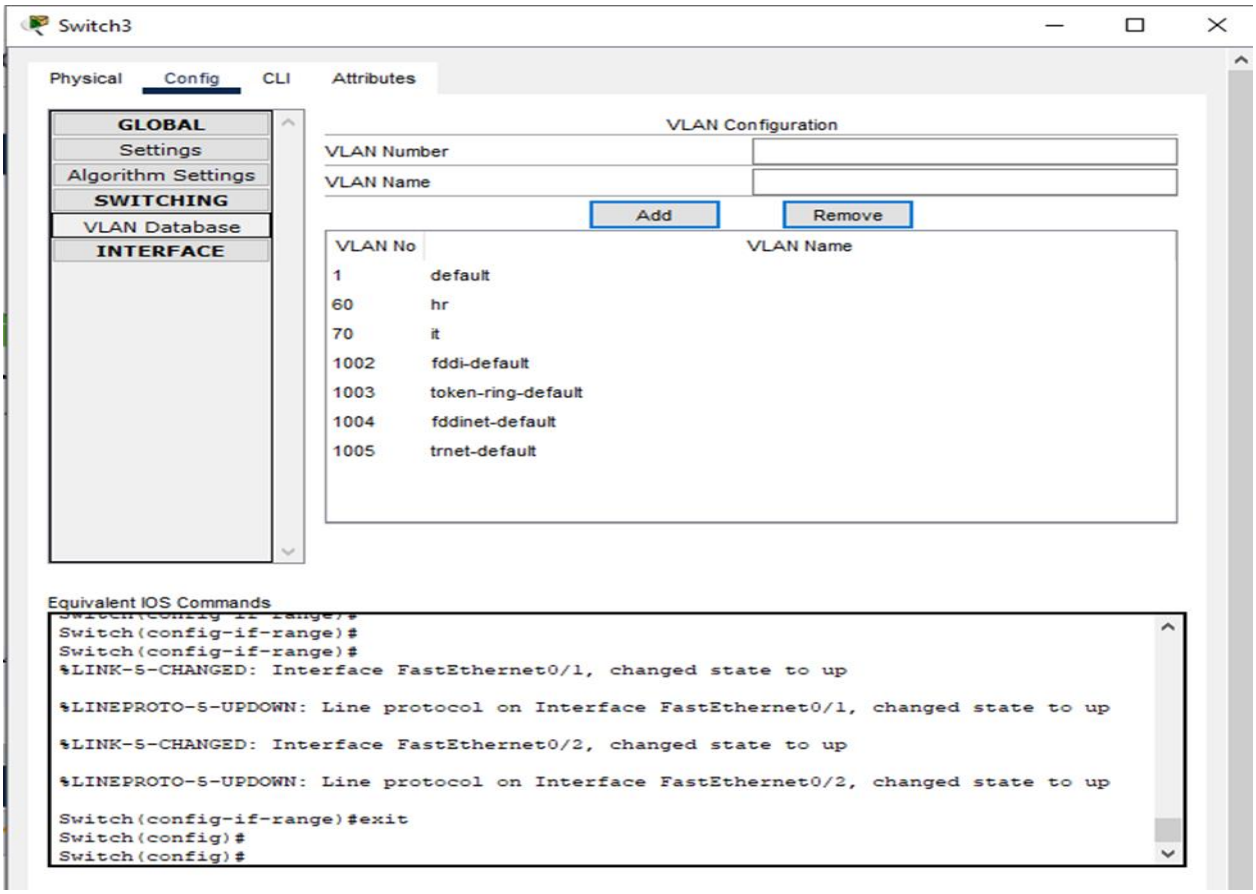
- Use 802.1X Security

Authentication	MD5
Username	
Password	

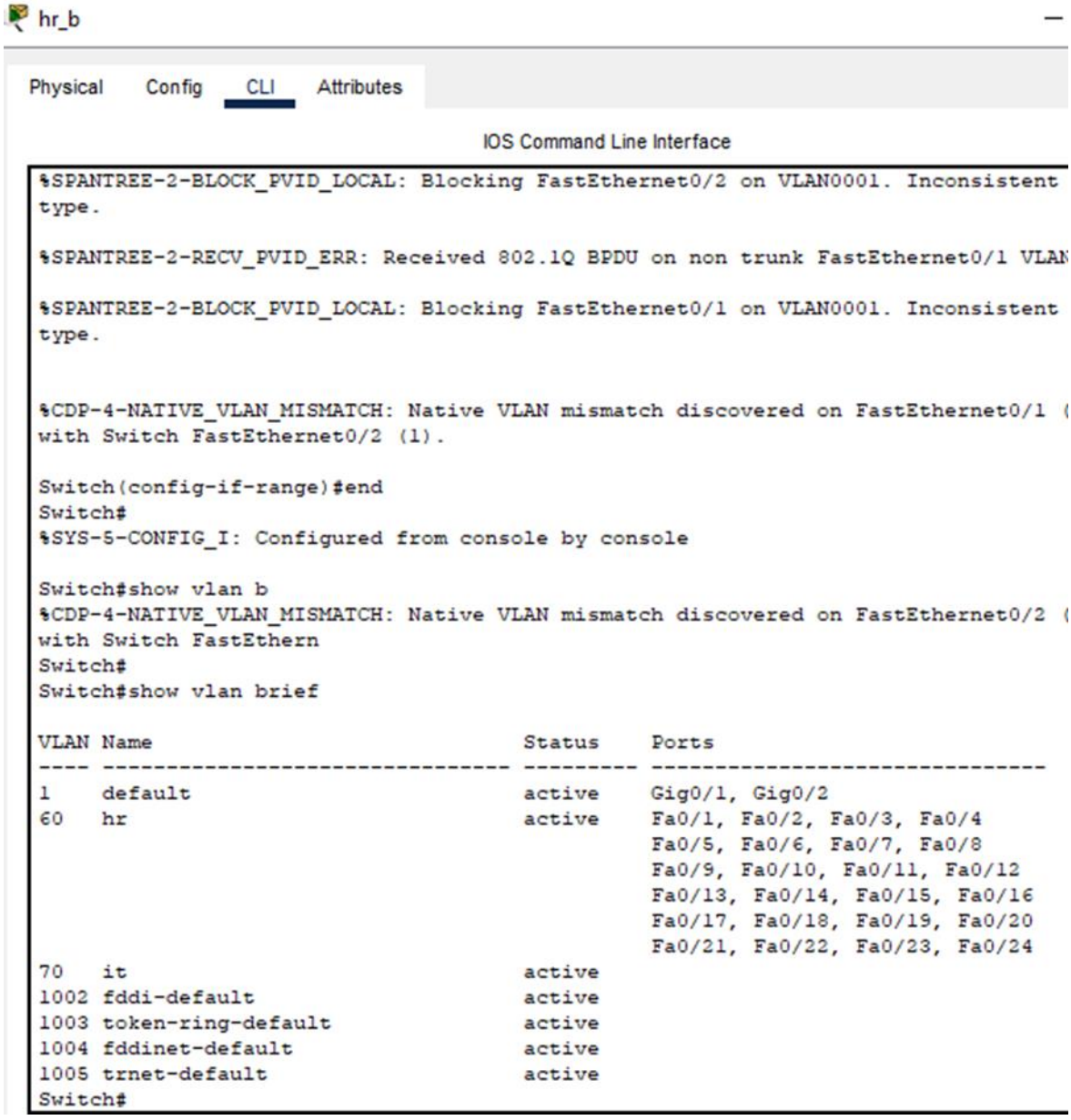



192.168.9.1/24
ISR4331
Router0
192.168.9.2/24
ISR4331
Router6
2960-24TT
reception
2960-24TT
sales
Access-Point-PT-N
customer_service
2960-24TT
server_room
2960-24TT
Switch0
2960-24TT
Switch2
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
Server-PT
DNS
Server-PT
WEB
PC-PT
PC8
PC-PT
PC7
Netid:192.168.1.0/24
Default:192.168.1.1
vlan id:10
Netid:192.168.2.0/24
Default:192.168.2.1
vlan:20
Netid:192.168.3.0/24
Default:192.168.3.1
vlan:30
Netid:192.168.4.0/24
Default:192.168.4.1
vlan:40
192.168.10.10/24
192.168.10.20/24
Netid:192.168.5.1
Default:192.168.5.1
vlan:50
Netid:192.168.7.0/24
Default:192.168.7.1
vlan:70
Netid:192.168.8.0/24
Default:192.168.8.1
vlan:80

Branch B


Switch3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
SWITCHING
VLAN Database
INTERFACE
VLAN Configuration
VLAN Number
VLAN Name
Add
Remove
VLAN No
VLAN Name
1 default
60 hr
70 it
1002 fddi-default
1003 token-ring-default
1004 fddinet-default
1005 trnet-default
Equivalent IOS Commands
Switch(config-if-range)#
Switch(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#

Assigning Branch B vlans to HR



```
Router(config)#
Router(config)#interface gi0/0/0.50
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.50, changed state to
up

Router(config-subif)#
Router(config-subif)#encapsulation dot1q 60
Router(config-subif)#ip address 192.168.7.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 70
Router(config-subif)#ip address 192.168.7.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#exit
Router(config)#
Router(config)#interface gi0/0/0.80
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.80, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.80, changed state to
up

Router(config-subif)#encapsulation dot1q 80
Router(config-subif)#ip address 192.168.8.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#exit
```

```
Router(config)#ip dhcp pool hr_b
Router(dhcp-config)#network 192.168.7.1 255.255.255.0
Router(dhcp-config)#default router 192.168.7.1
                              ^
% Invalid input detected at '^' marker.

Router(dhcp-config)#default-router 192.168.7.1
Router(dhcp-config)#dns 192.168.10.10
Router(dhcp-config)#
Router(dhcp-config)#exit
Router(config)#
Router(config)#ip dhcp pool it_b
Router(dhcp-config)#network 192.168.8.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.8.1
Router(dhcp-config)#dns 192.168.10.10
Router(dhcp-config)#exit
```

Serial port connection

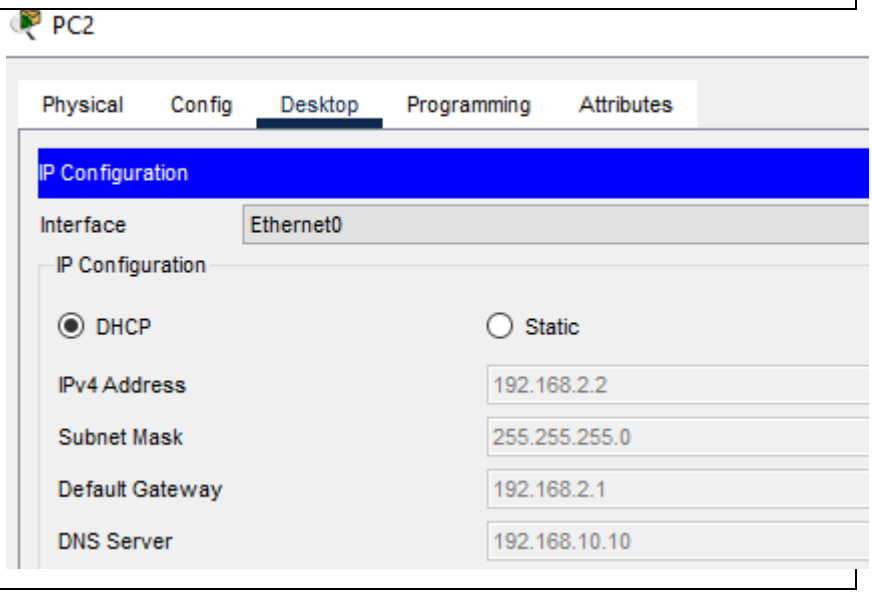
```
Router>
Router>enable
Router#comfigure terminal
                 ^
% Invalid input detected at '^' marker.

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#interface se0/1/0
Router(config-if)#ip address 192.168.9.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#
```

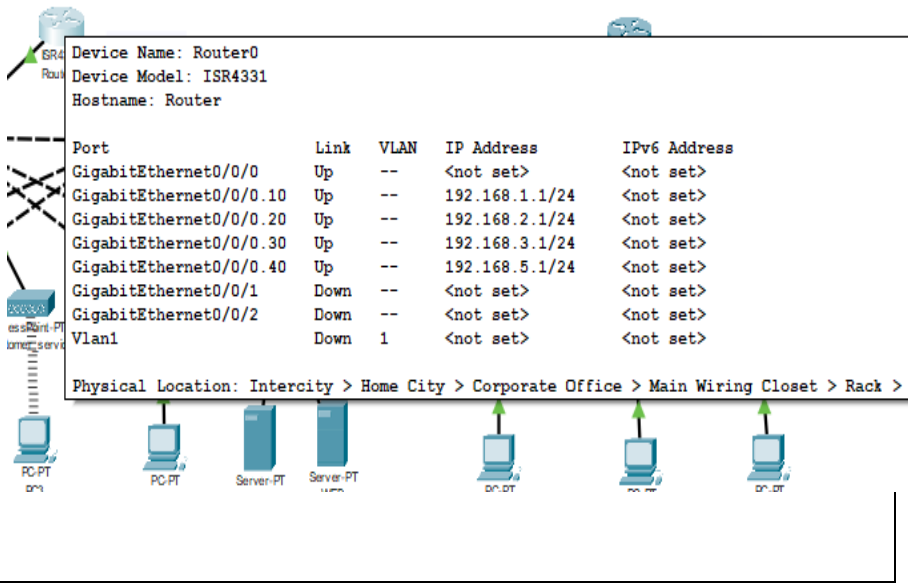
The message transfers

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=5ms TTL=128
Reply from 192.168.1.2: bytes=32 time=36ms TTL=128
Reply from 192.168.1.2: bytes=32 time=14ms TTL=128
Reply from 192.168.1.2: bytes=32 time=21ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 36ms, Average = 19ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=13ms TTL=128
Reply from 192.168.1.2: bytes=32 time=24ms TTL=128
Reply from 192.168.1.2: bytes=32 time=22ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 24ms, Average = 15ms

C:\>
```

Testing of network design

Test case 01

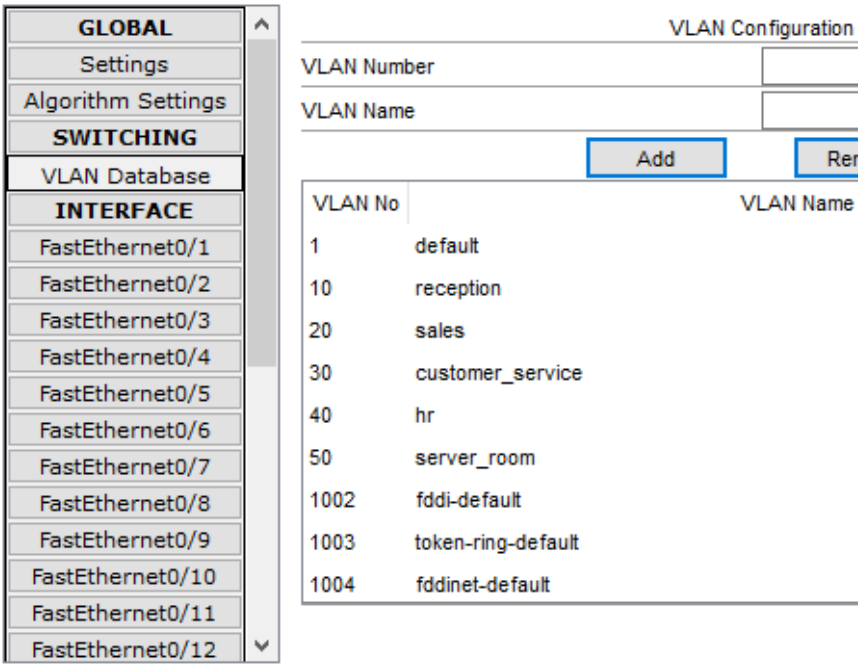
Test	Expected result	Actual result
dhcp test in IT department	Should display the Ip address related to dhcp form	

Test	Expected result	Actual result
IP address test in router	When mouse icon touches the router display tab and show the	

	default gate address	

Test	Expected result	Actual result
Show vlan brief	Type show vlan brief and display vlans in the branch	

```
Switch>enable
Switch#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------
1    default                             active    Fa0/1, Fa0/2,
                                                   Fa0/5, Fa0/6,
                                                   Fa0/9, Fa0/10
                                                   Fa0/13, Fa0/1
                                                   Fa0/17, Fa0/1
                                                   Fa0/21, Fa0/2
10   reception                           active
20   sales                               active
30   customer_service                    active
40   hr                                  active
50   server_room                         active
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
Switch#
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/1-fa0/22
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Show vlans	Getting whether the VTP vlan setting	

BlueScope's network design begins with a basic ping test to ensure that devices on subnets can communicate. Use extensive ping tests to check for packet loss under load. Next, run trace tests to confirm the correct routes between the Melbourne and Darwin offices. Next, try Telnet and SSH connections to ensure secure remote access to network devices. Test the VPN connection by establishing a connection between two offices, then check the communication speed and file transfer. For Wi-Fi, connect devices to customer service areas and test access to network resources. Also, perform a security check to prevent unauthorized connections. Finally, integrate IoT devices, ensuring they work smoothly without disrupting network traffic. These tests confirm that the network is working properly and securely supporting all necessary operations.

Future Enhancement Recommendations network design

Overall Network Analysis and Assessment

This update with Cisco Packet Tracer requires a detailed analysis of the current network infrastructure, including identifying points of congestion and vulnerabilities due to outdated hardware and software. Using tools like Cisco's DNA Center can help find

inefficiencies and areas needing attention, while comparing current performance metrics against benchmarks will evaluate the effectiveness of updates.

Upgrade and Expand Network Infrastructure

The content discusses the importance of upgrading network infrastructure with more sophisticated Cisco devices to meet the demands of modern network environments. It emphasizes replacing outdated routers, switches, and firewalls with the latest versions that offer higher data flow, better traffic management, and improved security features. The integration of Cisco's latest high-performance switches and routers is highlighted as a way to significantly increase network performance, supporting technologies like Multi-Gigabit Ethernet and advanced QoS features. Expanding the network with compatible devices also allows for increased flexibility and scalability to support heavier and more complex traffic and operations.

Simplify Management and Documentation of the Network

The objective is to simplify and make the network system more accessible to users to reduce errors and improve management efficiency. This involves documenting the network design, logically identifying devices, and using intuitive management tools for monitoring and configuration.

Enhance Security Protocols

Security is one of the main factors to consider when upgrading a network system. A more advanced network system with security controls should be implemented to prevent potential threats. To do this, you will use strong encryption protocols to secure data transmission, create an access control list to block unauthorized access, and conduct frequent security audits to detect and remedy vulnerabilities. Advanced security appliances, such as Cisco Adaptive Security Appliances, can be installed for comprehensive threat protection, including firewall protection, VPN service and intrusion prevention systems. To this end, you will secure the network by generally anticipating evolving cyber threats.

Implement a Proactive and Forward-Thinking Approach

It means that it has to embrace a proactive approach which should pre-estimate the different future developments in networking technology. It is continuous upgrading of the system with recent trends and emerging standards, such as adoption of Software Defined Networking and latest security protocols, that keeps the network at edge. Further refinement will also be developed from continuous improvement through on-the-job training sessions, consultations with domain experts, and feedback from consumers. By having an edge over technological advancements, the network will grow into a more dependable, safe, and competent sphere.