Pearson

Higher Nationals in

Computing

Unit 2: Networking

Acknowledgement

The internship opportunity I had with BCAS campus was a great chance for learning and professional development. Therefore, I consider myself as a very lucky individual as I was provided with an opportunity to be a part of it. I am also grateful for having chance to meet so many wonderful people and professionals who led me through this internship period.

I express my deepest thanks to the assessor Mr. Mohamed Ishraque, who works as an IT professional and take lectures on computer programming related subjects and others supportive subjects. He helped me taking part in useful decision & giving necessary advices and guidance and arrange all facilities for this assignment. I choose this moment to acknowledge his contribution gratefully. I acknowledge that this assignment was done with help of internet resources.

Sincerely,
S. SHALOMSHAN
Date:30.12.2022

Introduction

Networking refers to the practice of connecting computers and other devices together in order to facilitate communication and the exchange of information. Networks can be as small as two devices connected together, or as large as the global internet, which connects billions of devices around the world.

There are many different types of networks, including local area networks (LANs), wide area networks (WANs), and wireless networks. Networks can be used for a variety of purposes, such as sharing resources like printers and files, or enabling communication through email and instant messaging.

Networks rely on a variety of hardware and software components to function, including routers, switches, and networking protocols. Network administrators are responsible for designing, implementing, and maintaining networks, and must have a strong understanding of how networks work and how to troubleshoot problems that may arise.

Contents

Part 1

Networking Principles Options

- Client-server architecture: In this model, one or more clients request services or resources from a central server. The server processes the request and sends a response back to the client. This architecture is commonly used for web applications, where the client is a web browser and the server is a web server hosting the application.
- Peer-to-peer (P2P) architecture: In this model, each device in the network acts as both a client and a server. Devices can communicate directly with each other without the need for a central server. P2P networks are often decentralized and can be more resilient to failures, but they can also be more susceptible to security threats.
- Cloud computing: In this model, a network of servers hosted by a third-party provider offers resources and services over the internet. Users can access these resources and services on demand, paying only for what they use. This can be a cost-effective solution for businesses, as it allows them to scale their computing resources up or down as needed without having to invest in physical infrastructure.
- Network protocols: Network protocols define the rules for how devices on a network should communicate with each other. Some common protocols include TCP/IP, HTTP, and FTP.
- Network security: It is important to secure a network against unauthorized access and attacks. This can be achieved through the use of firewalls, encryption, authentication, and other security measures.
- Network monitoring: Network monitoring involves tracking the performance of a network and identifying any issues or bottlenecks that may arise. This can be done through the use of network monitoring tools and techniques such as packet sniffing, traffic analysis, and network performance metrics.

There are many other networking principles and options that could be discussed, but these are some of the key ones to consider when building a system.

The Advantages & Disadvantages of Various Solutions to Achieve the Goal.

There are many solutions to achieve networking goals, each with its own advantages and disadvantages. Here are a few examples:

1. LAN (Local Area Network): Advantages: High data transfer speeds, low cost, easy to set up. Disadvantages: Limited geographic range, security risks if not properly configured.
2. WAN (Wide Area Network): Advantages: Allows connectivity over large geographic areas, can be used to connect multiple LANs. Disadvantages: Typically more expensive than LANs, can be slower than LANs due to the distance data has to travel.
3. VPN (Virtual Private Network): Advantages: Allows remote users to securely connect to a private network, can be used to bypass internet censorship. Disadvantages: Can be slower than a direct connection, may require specialized software or hardware.
4. Cloud computing: Advantages: Allows for access to scalable computing resources, pay-as-you-go pricing model. Disadvantages: Dependent on Internet connectivity, may be more expensive for heavy users.
5. Wireless networking: Advantages: Convenient, allows mobility. Disadvantages: May be prone to interference, can be less secure than wired networking.

This is just a small sample of the many solutions that are available for networking. It's important to carefully consider the specific needs and constraints of a given situation when choosing a networking solution.

How Each Solution Will Affect The Topology, Bandwidth, Protocols, Availability, Security, Cost & Communication

Network solutions can affect a variety of factors in a network, including topology, bandwidth, protocols, availability, security, cost, and communication.

1. Topology: The topology of a network refers to the way in which devices on the network are connected to each other. Different network solutions can use different topologies, such as a bus, star, or mesh.
2. Bandwidth: The bandwidth of a network refers to the amount of data that can be transmitted over the network at any given time. Network solutions that use high-speed technologies, such as fiber optic cables, can provide more bandwidth than solutions that use slower technologies, such as copper cables.
3. Protocols: Protocols are the rules and standards that govern how devices on a network communicate with each other. Different network solutions may use different protocols, depending on the needs of the network and the devices that are connected to it.
4. Availability: Network availability refers to the amount of time that a network is up and running. Network solutions that use redundant components and have built-in failover mechanisms can be more highly available than those that do not.
5. Security: Network security refers to the measures that are taken to protect a network from unauthorized access or attacks. Network solutions that use encryption, firewalls, and other security measures can provide a higher level of security than those that do not.
6. Cost: The cost of a network solution can vary widely, depending on the technologies and components that are used. Solutions that use more expensive technologies may have a higher upfront cost, but may also offer long-term benefits, such as increased performance or reliability.
7. Communication: The effectiveness of communication on a network can be influenced by the network solution that is used. Solutions that use high-speed technologies or have a larger bandwidth may be able to support more concurrent communication than those that do not.

The Roles & Function of Each Devices (eg router, server), Technology (eg: cloud) & Protocols Involved in.

A router is a networking device that forwards data packets between computer networks. It connects devices such as computers, smartphones, and tablets to the internet by sending and receiving data through a local area network (LAN) or a wide area network (WAN), such as the internet.

A server is a computer that provides resources, data, or services to other devices on a network. There are many different types of servers, including web servers, file servers, and application servers.

Cloud computing is a model for delivering IT services over the internet. Instead of running applications or storing data on a local computer or server, users can access them through the internet on a remote server. This allows users to access their data and applications from any device with an internet connection.

There are many different protocols involved in networking, including TCP/IP, HTTP, and FTP. TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of communication protocols that is used to connect devices on the internet. HTTP (Hypertext Transfer Protocol) is a protocol used to transfer data over the internet, including web pages and other files. FTP (File Transfer Protocol) is a standard network protocol used to transfer files between computers on a network.

Part 3

Test the Backup Solution & Internet Filtering, & Document

To test the backup solution, you should perform a trial run of the backup process to ensure that it is working correctly and that all of the necessary data is being backed up. This can be done by manually initiating a backup, or by setting the backup to run at a predetermined time and then verifying that the backup has been successful.

To test internet filtering, you can try accessing websites that are known to be blocked by the filter and verify that they are indeed blocked. You can also try accessing websites that are allowed by the filter and verify that they are not blocked.

To document the authentication and authorization settings, you should record the process for how users are granted access to the system, including any passwords, security questions, or other measures that are used. You should also record the process for how users are granted different levels of access to different resources within the system.

To document the internet filtering and bandwidth control settings, you should record the specific websites or types of content that are blocked or restricted, as well as any limits that have been set on bandwidth usage.

An efficient backup strategy should be based on the specific needs and requirements of the organization. Factors to consider when developing a backup strategy may include the amount of data to be backed up, the frequency with which backups should be performed, the types of data that are most important to protect, and the resources (such as time, money, and storage space) that are available for the backup process. Some common techniques for developing an efficient backup strategy include using incremental backups, storing backups offsite, and using automated tools to manage the backup process.

Authentication, Authorization settings

Authentication is the process of verifying that someone or something is who or what they claim to be. This is usually done by requesting some form of credentials, such as a username and password.

Authorization is the process of granting or denying access to a certain resource, based on the authenticated user's permissions. For example, an authenticated user might be authorized to access certain files on a server, but not others.

It is common for organizations to have different authentication and authorization systems in place for different resources. For example, a company might use one system for authenticating employees to their work computers, and a different system for authenticating users to the company's website.

Internet Filtering & Bandwidth Control

Internet filtering is the process of blocking or restricting access to certain websites or types of content on the internet. This can be done for a variety of reasons, such as to protect children from inappropriate content, to prevent employees from accessing non-work related websites, or to comply with government censorship requirements. There are several ways to implement internet filtering, including using software tools on individual computers or devices, configuring network-level controls, or using a combination of both.

Bandwidth control refers to the process of managing the amount of data that is transmitted over a network connection. It is often used to ensure that certain types of traffic are given priority over others, or to limit the amount of bandwidth that is available to individual users or devices. This can be helpful in situations where the available bandwidth is limited, or where certain types of traffic are more important or time-sensitive than others. There are a variety of tools and techniques that can be used to implement bandwidth control, including hardware devices, software applications, and network configuration settings.

Efficient Backup Strategy.

There are several ways to implement a network-efficient backup strategy, depending on your needs and resources. Here are a few options you might consider:

1. Incremental backups: Rather than backing up all of your data every time, incremental backups only copy the data that has changed since the last backup. This can save network bandwidth and storage space, especially if you have a large volume of data that doesn't change often.
2. Compression: Compressing the data you are backing up can also help save network bandwidth and storage space. Many backup software tools offer built-in compression options.
3. Bandwidth throttling: If you need to limit the impact of backups on your network, you can use bandwidth throttling to limit the amount of data that is transferred during backup operations. This can help you ensure that backups don't interfere with other network traffic.
4. Cloud-based backups: If you have a lot of data to back up, or if you need to back up data from multiple locations, you might consider using a cloud-based backup service. These services can be more network-efficient because they use optimized protocols and servers that are designed for large-scale data transfer.
5. Deduplication: Deduplication is a process that removes duplicate copies of data, so that only one copy is stored. This can save a significant amount of storage space, especially if you have multiple copies of the same data. Some backup software tools offer deduplication as an option.
6. Scheduling: Carefully scheduling your backups can also help you optimize your network usage. For example, you might schedule backups to run during off-peak hours, when network traffic is lighter.

Part 4

Explain How You Will Maintain the Network in a Healthy State

To maintain the network in a healthy state, it is important to implement a thorough device/network monitoring plan, a support plan, and an update/upgrade plan.

Device/Network Monitoring:

- Regularly check the status of all devices on the network, including routers, switches, servers, and workstations.
- Monitor network traffic to identify any bottlenecks or unusual activity.
- Use network monitoring tools to alert administrators to any issues or failures.
- Monitor device performance and capacity to ensure that the network has sufficient resources to meet the needs of users.

Support Plan:

- Establish a support plan to ensure that any issues with devices or the network can be quickly addressed.
- Have a plan in place for how to troubleshoot and resolve issues, including a list of common problems and their solutions.
- Establish a process for escalating issues to higher levels of support as needed.
- Consider implementing a network monitoring service that can provide round-the-clock monitoring and support.

Update/Upgrade Plan:

- Regularly check for updates and upgrades to devices and software on the network.
- Test updates and upgrades in a staging environment before implementing them in production.
- Have a process in place for rolling out updates and upgrades to ensure minimal disruption to users.
- Keep an inventory of all devices and software on the network, including version numbers and expiration dates, to ensure that everything is up-to-date.
- By implementing these measures, it will be possible to maintain the network in a healthy state and ensure that it continues to function optimally.

Conclusion

In conclusion, networking is a vital aspect of modern computing and communication. It allows devices to connect and communicate with each other, enabling the exchange of information and the sharing of resources. There are many different types of networks, ranging from small local area networks to the global internet, and a variety of hardware and software components are used to support their functioning. Network administrators play a crucial role in designing, implementing, and maintaining networks, and must have a strong understanding of how networks work and how to troubleshoot problems that may arise. As the use of networks continues to expand and evolve, the field of networking will continue to be an important and dynamic area of study and practice.

References

https://www.studocu.com/row/document/esoft-metro-campus/higher-national-diploma/networking-assignment/11737715

https://www.studocu.com/row/document/esoft-metro-campus/software-project-proposal/esoft-metro-cumpus-network-assignment/20976435

https://studylib.net/doc/25646121/networking-assignment---01

https://sites.google.com/site/tvcccis101ch0283/home/assignment-1

https://www.coursehero.com/file/17948444/Network-Assignment/

https://www.locusassignments.com/solution/unit-44-local-area-networking-technologies-sample-assignment