Unit 19 Computer networking

11/9/22

Coleg gwent

Rhys Llewellyn Holley

Introduction

The evolution of networks over the years has led to the need for a range of different network models. These models are designed to meet different requirements and to enable users to access the network in various ways. This evaluation will explore the three main network models (peer-to-peer, client/server and thin client) and assess their suitability for different application scenarios. It will consider ease of use, set-up, performance, and suitability for different applications, as well as current trends in networking such as BYOD, IOT and cloud computing. This evaluation will provide examples of how these different network models are suitable for different networking applications, highlighting both their benefits and drawbacks.

Peer to peer

Peer-to-peer (P2P) networking is a type of network topology in which each node, or computer, acts as both a client and a server, allowing users to share resources with each other directly. It is a decentralized system that allows users to access files, programs, and data stored on other computers within the network. Although P2P networks have many advantages, there are also some potential drawbacks that should be considered.

Advantages of Peer to Peer Networking

1. Low cost: One of the main advantages of P2P networks is that they are relatively inexpensive to set up and maintain. Since all computers in the network act as both clients and servers, there is no need for a dedicated server to manage the network. This means that the overall cost of setting up and maintaining a P2P network is much lower than a traditional client-server network.

2. Increased flexibility: P2P networks are highly flexible since all nodes in the network can access and share resources with each other. This means that users can access and share files and programs from any other computer in the network without the need for a centralized server.

3. Improved scalability: P2P networks are highly scalable since new nodes can be added to the network without any changes to the existing nodes. This means that the network can easily accommodate additional users and resources as needed.

Disadvantages of Peer-to-Peer Networking

1. Security risks: One of the main drawbacks of P2P networks is that they are more vulnerable to security risks. Since all nodes in the network can access and share resources with each other, malicious users can easily gain access to sensitive data and files stored on other computers.

2. Low reliability: Another potential drawback of P2P networks is that they are less reliable than traditional client-server networks. The lack of a centralized server means that the network is more susceptible to downtime if one of the nodes fails or is disconnected from the network.

3. Resource management: Managing resources in a P2P network can be difficult since there is no central server to manage the resources. This means that users must manually manage resources to ensure that all nodes in the network have adequate access to resources.

Conclusion

In conclusion, P2P networks have both advantages and disadvantages that should be considered when determining the best network topology for a particular application. While P2P networks can be beneficial in certain scenarios, the potential security risks and lack of reliability should be carefully weighed before implementing a P2P network.

Client/server

Client server networking is widely used in many organizations today as it provides an efficient and reliable way to share resources. In this setup, clients (computers) request services from a server (a computer or device that provides services). This type of networking has many advantages, but also some disadvantages.

Advantages

1. Secure: Client server networks are more secure than other networks, as the server computer is responsible for keeping the data safe and secure.

2. Reliable: Client server networks are more reliable than other networks as the server can provide consistent and reliable performance.

3. Centralized control: Client server networks provide centralized control over the network as all users connect to the same server. This makes it easier to manage user accounts, security policies, and other system settings.

4. Flexibility: Client server networks are more flexible than other networks as they can be easily expanded to accommodate more users and resources.

5. Scalability: Client server networks can be easily scaled up or down to accommodate changes in the number of users and resources.

Disadvantages

1. Cost: Client server networks require a server computer, which can be expensive to purchase and maintain.

2. Complexity: Client server networks can be more complex to set up and maintain than other networks.

3. Dependency: Client server networks are dependent on the server computer and if the server fails, the network will be affected.

4. Single point of failure: Client server networks can be vulnerable to security breaches as the server computer is a single point of failure.

5. Limited control: Client server networks can limit control over the network as all users must connect to the same server.

Conclusion

In conclusion, client server networking has many advantages as well as some disadvantages. It is important to weigh the pros and cons before deciding if this type of networking is the right choice for an organization. With the right setup and configuration, client server networking can provide an efficient and reliable way to share resources

Thin client

Thin client networking is a technology used to decrease the amount of hardware and software needed for a network. This type of technology is especially useful for businesses that have multiple users working on the same network. Instead of each user having their own separate computer, they can access a shared computer or “thin client” through the network. This article will discuss the advantages and disadvantages of thin client networking.

Advantages

1. Lower maintenance costs: Because thin clients have fewer components, they require less maintenance than traditional computers. This means fewer repair costs and less time spent troubleshooting.

2. Increased security: Since all data is stored on the server, it is more secure than on a traditional computer. Data is also more easily backed up and can be accessed from any location with an internet connection.

3. Easier to manage: Because all of the software is stored on the server, it is much easier to manage than multiple separate computers. Updates can be applied to the entire network at once, rather than having to update each individual computer.

4. Increased reliability: Since all of the hardware is in one place, it is more reliable than multiple separate computers. This means that if one component fails, it can be easily replaced without having to worry about the entire network going down.

Disadvantages

1. Network congestion: If too many users are on the network, it can cause slowdowns or lag. This can be especially problematic if the network is not powerful enough to handle the load.

2. Limited hardware compatibility: Thin clients cannot run all types of hardware. This means that some specialized hardware or software will not be compatible with the thin client.

3. Increased initial costs: Since the server and thin clients will need to be purchased, this can be a more expensive option than purchasing multiple separate computers.

4. Increased power consumption: Since the server will be running 24/7, it will require more power than multiple separate computers.

Conclusion

In conclusion, thin client networking can be an advantageous option for businesses that need to provide multiple users with the same resources. It can result in lower maintenance costs, increased security, and easier management. However, it may come with some disadvantages such as limited hardware compatibility, increased initial costs, and increased power consumption.

BYOD

Bring Your Own Device (BYOD) refers to the practice of allowing employees to use personal devices for work purposes. BYOD has become increasingly popular in recent years as businesses benefit from improved employee productivity, cost savings, and higher morale. Despite these benefits, BYOD also presents security challenges, as company data and networks must be protected from malicious actors.

Benefits of BYOD

BYOD offers businesses the ability to save costs by avoiding the purchase and maintenance of workplace technology. Employees can use their own devices, which are often more up-to-date than workplace devices, thus avoiding the need to purchase new equipment. Employees also tend to be more productive when using their own devices, as they are familiar with the technology and can work more efficiently. An additional benefit of BYOD is that it can improve employee morale. Employing BYOD gives employees the freedom to use their own devices and allows them to work from anywhere. This flexibility can create a happier and more productive workforce.

Risks of BYOD

The greatest risk of BYOD is the potential for security breaches due to malicious actors. As employees connect their personal devices to the company network, they may unknowingly introduce malware or viruses. Additionally, personal devices may not have the same security protocols in place as workplace devices, leaving the network vulnerable to attack. Another risk of BYOD is the potential for data leakage. Personal devices are typically not subject to the same oversight and monitoring as workplace devices, making it easier for employees to share or leak company data.

Organizations considering BYOD should take steps to ensure the security of their networks. This includes implementing encryption technologies and authentication protocols to protect data from intrusion. Additionally, organizations should provide employees with clear guidelines on acceptable use of devices, including what data can and cannot be stored on personal devices.

Conclusion

BYOD can offer businesses many benefits, such as cost savings and improved employee productivity. However, it also presents security challenges that must be addressed. Organizations should carefully consider the potential risks and benefits of BYOD before deploying a BYOD network. By taking the necessary steps to protect the network and data, businesses can take advantage of the many benefits of BYOD while keeping their networks secure.

Topology

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network and may be depicted physically or logically. Network topologies may be physical or logical. Physical topology is the placement of the various components of a network, including device location and cable installation, while logical topology illustrates how data flows within a network, regardless of its physical design. Network topology is an important factor in network design. It is used to determine the most efficient way of connecting various devices and nodes on a network. It also provides an understanding of how data is transmitted between nodes. The most common types of network topology are mesh, star, bus, ring, and tree. A mesh topology connects each node to every other node on the network, creating a redundant system that allows for greater data redundancy and reliability. In a star topology, all nodes are connected to a central hub or switch, creating a point-to-point connection. A bus topology links each node to a single, continuously running cable, allowing for quick and easy signal transmission. A ring topology works by connecting each node to two other nodes on the network, forming a closed loop. Finally, a tree topology is similar to a bus topology, however each node is connected to multiple other nodes. Network topology plays an important role in ensuring the reliability and performance of a network. It is essential that the topology of a network is designed appropriately to ensure maximum efficiency and reliability.

WAN

Network Wide Area Networks (WANs) are networks that span large geographic areas, connecting multiple sites and networks across the globe. They are used to connect LANs and other types of networks, such as the Internet, to enable users to communicate and share information with each other.

WANs are typically made up of routers, hubs, switches, and other networking equipment that allow the different sites to communicate with each other over long distances. WANs are typically used by large organizations, such as corporations or universities, which have multiple locations. By connecting all of the locations together, users can access resources from any of the sites, regardless of their location.

WANs are also used by ISPs to provide internet access to their customers. One of the key advantages of WANs is that they are very reliable and secure. They use sophisticated security protocols to protect data as it travels between sites, preventing unauthorized access or manipulation. They also use redundant connections and failover systems to ensure that data is delivered quickly and reliably. In addition,

WANs can be configured to provide Quality of Service (QoS), which allows certain types of traffic, such as voice or video, to be given priority over other types of traffic. This ensures that critical applications and services are always available, even during periods of high network traffic. Overall, WANs are an invaluable tool for businesses and organizations that need to connect multiple sites across large distances. By providing reliable and secure connections, as well as QoS capabilities, WANs enable organizations to maximize their productivity and efficiency.

Lan's

Network LANs (Local Area Networks) are computer networks that are limited to a certain geographical area, such as a single building or office. These networks are used to connect computers and other networked devices to share resources, such as printers and files, and to communicate with each other.

Network LANs are typically built using networking hardware such as switches, routers, and Wi-Fi access points. Switches and routers are used to segment the network into different subnets and control the flow of data between them. Access points are used to provide wireless access to the network.

Network LANs can be configured in different ways, depending on the needs of the organization. For example, they can be configured as a hub and spoke topology, where there is a central switch or router that all other devices connect to, or as a mesh topology, where each device is connected to multiple other devices.

Network LANs also come in different types, such as Ethernet and Wi-Fi. Ethernet networks are typically used for wired connections, while Wi-Fi networks are used for wireless connections. Network LANs can also be configured to use different protocols, such as TCP/IP, TCP/IP is the most common protocol used on modern networks, and it is used to communicate between networked devices.

Network LANs provide numerous benefits to organizations, including increased security, improved performance, scalability, and cost savings. They also enable organizations to more easily share resources and communicate with each other.

In conclusion, network LANs are an essential part of modern networking, and they provide numerous benefits to organizations. They are a cost-effective and efficient way to connect computers and other networked devices, and provide improved security, performance, scalability, and cost savings. conclusion, a LAN can be a great way to share resources and access the Internet within a small geographic area. However, it is important to consider the cost and security implications before deciding to set up a LAN.

Functions of network components

Network Interface Card (NIC)

Characteristics: Physical hardware component installed in computers and devices.

Function: Enables devices to connect to a network by providing a physical interface for transmitting and receiving data.

Switch

Characteristics: Central network device with multiple ports.

Function: Directs data packets to their intended destination within a local area network (LAN) based on MAC addresses.

Router

Characteristics: Device that connects multiple networks and forwards data packets between them.

Function: Routes data packets between different networks based on IP addresses, enabling communication between devices on different subnets or across wide area networks (WANs).

Modem

Characteristics: Device that modulates and demodulates analog/digital signals for transmitting data over different types of communication channels.

Function: Converts digital data from a computer into a format suitable for transmission over telephone lines (DSL modem), cable lines (cable modem), or other communication mediums.

Firewall

Characteristics: Security device or software that monitors and controls incoming and outgoing network traffic.

Function: Protects networks from unauthorized access and potential threats by filtering and blocking suspicious or malicious traffic.

Access Point (AP)

Characteristics: Wireless device that allows devices to connect to a wireless network.

Function: Acts as a central hub for wireless communication, providing wireless connectivity to devices within its range.

Network Cables

Characteristics: Physical cables used to establish wired connections between network devices.

Function: Transmit data signals between devices, such as Ethernet cables (e.g., Cat 5e, Cat 6) for LAN connections.

Network Protocols and Standards

Characteristics: Set of rules and guidelines for data communication and network operations.

Function: Define how devices communicate, establish data transfer methods, and ensure interoperability between different network components and technologies.

Conclusion

In conclusion, there is no one-size-fits-all approach to network models and topologies. Depending on the networking requirements of a business, one of the three models – peer-to-peer, client/server, or thin client – may be more suitable than the others. The emergence of new technologies such as BYOD, IOT, and cloud computing have also increased the need for businesses to consider how different types of network models can be used to best meet their networking requirements. With careful analysis of the business's networking requirements and the potential benefits and drawbacks of each model, the best network model for any given application can be chosen.