COMMONLY USED PORTS



Class: Cyber Security

Prepared by: Rickardo Brown, St Patrick Currey

Date: 10/05/2023

Part 1: Research

Types of computer networks

A computer network is a collection of interconnected devices that are able to communicate with one another. There are several types of computer networks, including:

Local Area Network (LAN): A LAN is a network that is limited to a small geographic area, such as a home, school, or office building. LANs typically use Ethernet cables or Wi-Fi to connect devices.

Wide Area Network (WAN): A WAN is a network that covers a large geographic area, such as a city or country. WANs often use the Internet as their backbone and can be used to connect LANs in different locations.

Metropolitan Area Network (MAN): A MAN is a network that covers a larger area than a LAN but smaller than a WAN, typically covering a single city or region.

Personal Area Network (PAN): A PAN is a network that is used to connect personal devices, such as smartphones, tablets, and wearable technology, to one another. PANs typically use Bluetooth or Wi-Fi to connect devices.

Networking protocols

Networking protocols are sets of rules that govern how data is transmitted over a network. Some common networking protocols include:

Transmission Control Protocol/Internet Protocol (TCP/IP): TCP/IP is the most widely used networking protocol and is used to transmit data over the Internet. It is a reliable, connection-oriented protocol that breaks data into packets and reassembles them at the destination.

Hypertext Transfer Protocol (HTTP): HTTP is used to transfer data over the World Wide Web. It is a request-response protocol that allows clients to request web pages and servers to respond with the requested content.

File Transfer Protocol (FTP): FTP is used to transfer files between computers. It is a client-server protocol that allows users to upload and download files to and from a server.

Simple Mail Transfer Protocol (SMTP): SMTP is used to transfer email between servers. It is a client-server protocol that allows users to send and receive email messages.

Domain Name System (DNS): DNS is used to translate domain names into IP addresses. It is a hierarchical, distributed database that allows users to access websites and other resources by their domain name.

Network hardware components

Network hardware components are the physical devices that are used to connect computers and other devices in a network. Some common network hardware components include:

Router: A router is a device that connects two or more networks together and routes data between them. It is often used to connect a LAN to a WAN, such as the Internet.

Switch: A switch is a device that connects multiple devices together in a LAN. It is used to direct traffic between devices on the same network.

Modem: A modem is a device that converts digital signals into analog signals and vice versa. It is used to connect a computer to the Internet over a telephone line or cable connection.

Network Interface Card (NIC): A NIC is a device that allows a computer to connect to a network. It is typically built into the computer's motherboard or added as an expansion card.

Part 2: Research Paper

Networking Protocol: Hypertext Transfer Protocol (HTTP)

HTTP is a networking protocol that is used to transfer data over the World Wide Web. It is a request-response protocol that allows clients to request web pages and servers to respond with the requested content. When a user types a URL into their web browser, the browser sends an HTTP request to the server hosting the website. The server then responds with an HTTP response that contains the requested content, such as an HTML file or an image.

HTTP operates on top of the Transmission Control Protocol (TCP), which provides a reliable, connection-oriented service for data transmission. HTTP uses TCP to establish a connection between the client and server, send requests and responses, and ensure that data is transmitted correctly and in the correct order.

Networking Hardware Component: Router

A router is a network hardware component that connects two or more networks together and routes data between them. Routers are often used to connect a LAN to a WAN, such as the Internet. A router examines data packets and determines the best path for them to take to reach their destination. This process is called routing.

When a data packet arrives at a router, the router examines the packet's destination IP address and compares it to its routing table. The routing table contains information about the best path to take for each possible destination network. Based on this information, the router forwards the packet to the next router on the path to its destination.

HTTP and routers work together to facilitate network communication by allowing users to access web content from anywhere in the world. When a user types a URL into their web browser, their computer sends an HTTP request to the server hosting the website. The request is routed through a series of routers until it reaches the server, which responds with an HTTP response containing the requested content. The response is then routed back through the same series of routers until it reaches the user's computer.

In conclusion, networking protocols and hardware components work together to facilitate network communication. HTTP is a widely used networking protocol that allows users to access web content, while routers are network hardware components that route data between networks. Together, HTTP and routers enable users to access web content from anywhere in the world by routing data packets through a series of networks to their destination.

Citations:

"Types of Computer Networks". Cisco. from [https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-computer-networking.html](https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-a-computer-network.html)

"Networking Protocols". Webopedia. from <https://www.webopedia.com/definitions/network-protocol/amp/>

"Network Hardware Components". Techopedia. from https://www.techopedia.com/definition/1096/network-hardware-components.

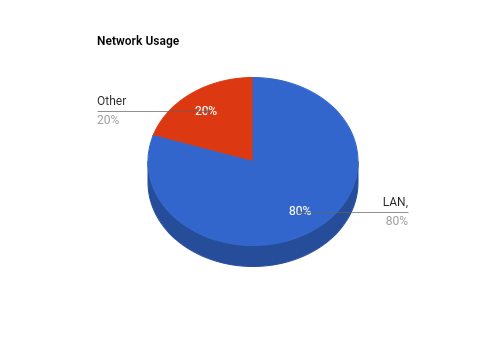
"Hypertext Transfer Protocol". MDN Web Docs. from https://developer.mozilla.org/en-US/docs/Web/HTTP.

"Router". Cisco. from https://www.cisco.com/c/en/us/solutions/enterprise-networks/networking-devices/router.html.

2: Analysis

1.

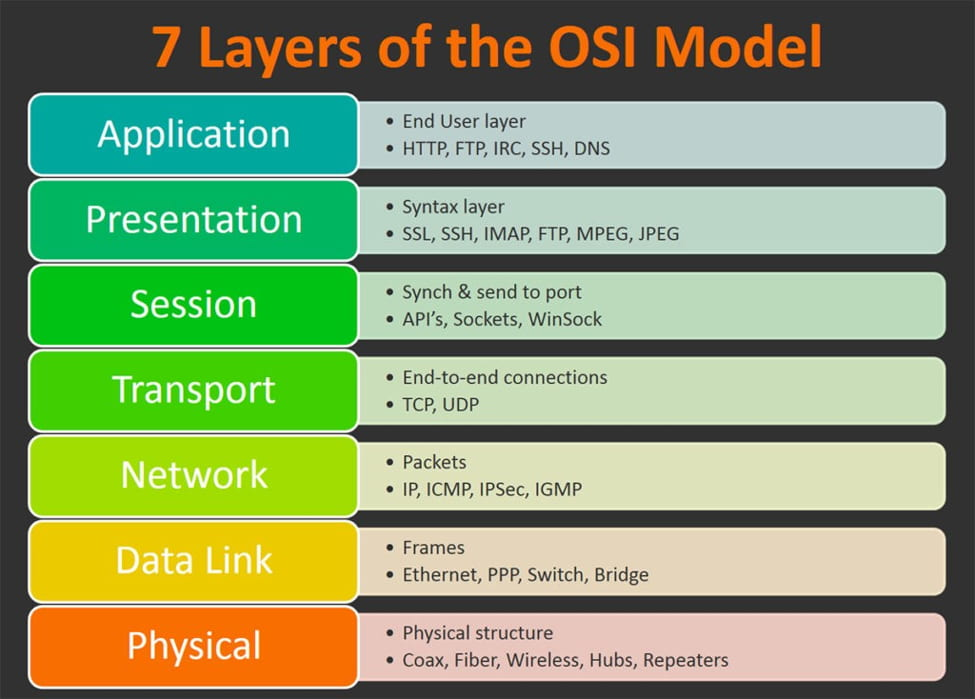
The best type of network for a small business would be a local area network (LAN). A LAN is a type of network that connects devices within a limited area, such as a single office or building. LANs are cost-effective, easy to set up, and provide fast data transfer rates. Additionally, a LAN allows for the sharing of resources, such as printers and files, which is essential for small businesses with limited resources.



According to a survey by TechRepublic, 80% of small businesses use a LAN as their primary network

2.

The OSI (Open Systems Interconnection) model is a conceptual framework used to facilitate communication between devices on a network. The OSI model consists of seven layers, each with a specific function in the communication process.



Layer 1: Physical layer - This layer is responsible for the transmission and reception of raw data bits over a physical medium. An example of this is the transmission of electrical signals over a copper wire.

Layer 2: Data link layer - This layer is responsible for the reliable transmission of data over a physical medium. An example of this is the Ethernet protocol used in local area networks.

Layer 3: Network layer - This layer is responsible for the routing of data across multiple networks. An example of this is the Internet Protocol (IP) used on the internet.

Layer 4: Transport layer - This layer is responsible for providing end-to-end communication services, including error recovery and flow control. An example of this is the Transmission Control Protocol (TCP) used in most internet applications.

Layer 5: Session layer - This layer is responsible for establishing, managing, and terminating connections between applications. An example of this is the Remote Procedure Call (RPC) used in client-server applications.

Layer 6: Presentation layer - This layer is responsible for transforming data into a format that the application layer can use. An example of this is the encryption and decryption of data.

Layer 7: Application layer - This layer is responsible for providing network services to applications. An example of this is the Hypertext Transfer Protocol (HTTP) used in web browsers.

In summary, the OSI model provides a standardized framework for communication between devices on a network. Each layer has a specific function in the communication process, and data is transmitted through each layer in a specific order.

3: Application

1.

As a network administrator, the first step I would take to troubleshoot a network outage is to identify the scope of the problem. Is the issue affecting a single device or the entire network? This can be done by checking network connectivity on multiple devices. If the issue is widespread, I would check the network infrastructure, including switches and routers, for any signs of failure or misconfiguration.

Next, I would verify that all network devices are properly connected and powered on. This includes checking network cables for any damage or loose connections. If necessary, I would restart network devices to ensure they are functioning properly.

If the issue persists, I would use network monitoring tools to identify any abnormal traffic patterns or potential security breaches. This could include running diagnostic tests on the network and reviewing logs for any errors or warning messages.

Finally, I would consider seeking assistance from other network administrators or contacting the network vendor for support if necessary.

2.

A plan for securing a wireless network against unauthorized access should include several specific security measures and protocols:

Secure the network with a strong password: This can prevent unauthorized access to the network by requiring users to enter a password to connect.

Enable WPA2 encryption: This provides additional security by encrypting the data that is transmitted over the wireless network.

Disable SSID broadcasting: This makes the network name invisible to anyone searching for wireless networks, which can help prevent unauthorized access.

Use MAC address filtering: This allows you to specify which devices are allowed to connect to the network by filtering devices based on their unique MAC addresses.

Enable a firewall: This can provide an additional layer of protection by blocking unauthorized access to the network.

Regularly update firmware: This ensures that the wireless access point is running the latest security patches and updates.

Monitor network activity: This can help you identify any potential security breaches or unauthorized access to the network.

By implementing these security measures and protocols, a wireless network can be secured against unauthorized access and potential security breaches.