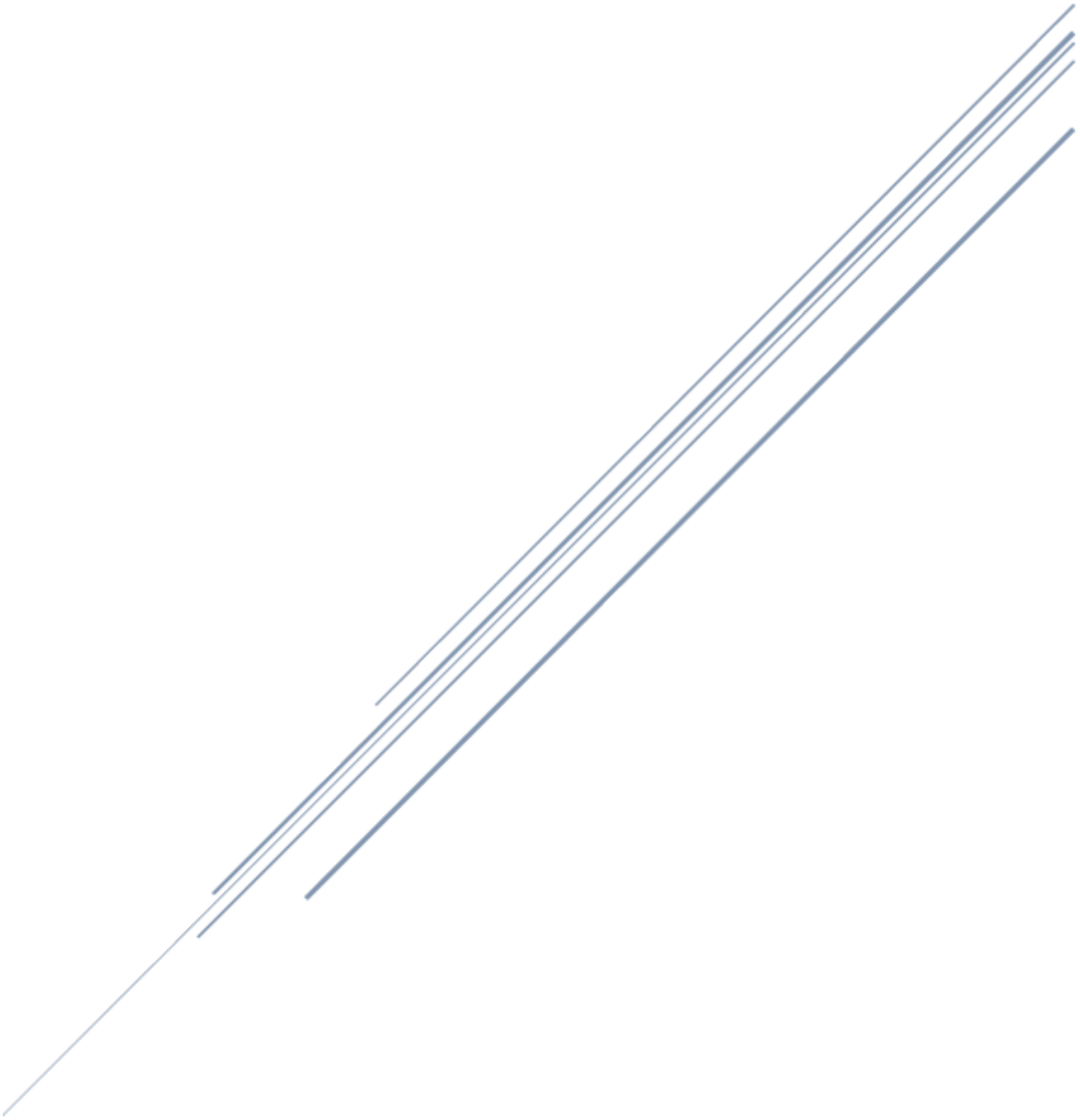
Fundamental concepts of computer networking



Konnel Bennett
Cybersecurity

Types of computer networks

LAN (Local Area Network)

A LAN is a computer network that connects devices within a small geographical area, such as an office building, a school, or a home. A LAN typically uses Ethernet cables, Wi-Fi, or a combination of both to connect devices and share resources such as printers, files, and internet access. LANs are typically owned and managed by a single organization, and are designed for high-speed communication and file sharing among devices in close proximity.

WAN (Wide Area Network)

A WAN is a computer network that spans a large geographic area, such as a city, country, or even multiple countries. WANs are typically used by organizations that need to connect multiple remote locations, such as branch offices or data centers. WANs use a variety of technologies to connect devices, including leased lines, satellite links, and the internet. WANs are slower than LANs, but can cover much larger distances.

MAN (Metropolitan Area Network)

A MAN is a computer network that covers a geographic area larger than a LAN but smaller than a WAN, typically a single city or metropolitan area. MANs are used by organizations that need to connect multiple locations within a city, such as local government agencies or universities. MANs use a combination of technologies such as fiber optic cables and wireless connections to connect devices and share resources.

PAN (Personal Area Network)

A PAN is a computer network that connects devices within a very small area, typically a few meters. PANs are used to connect personal devices such as smartphones, laptops, and wearable technology to each other and to the internet. Bluetooth and Wi-Fi are common

technologies used to create PANs. PANs are used for activities such as file sharing, printing, and internet access.

Networking protocols

TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP is a set of protocols that are used to connect devices to the internet and to each other. The TCP protocol is responsible for breaking data into packets, while the IP protocol is responsible for routing those packets across the internet. TCP/IP is the foundation of the internet and is used by all devices that connect to it.

HTTP (Hypertext Transfer Protocol)

HTTP is a protocol that is used to transfer data between web servers and web browsers. HTTP is used to send requests from a web browser to a web server, and to receive responses from the server. HTTP is a stateless protocol, which means that each request and response is independent of any previous request or response.

FTP (File Transfer Protocol)

FTP is a protocol that is used to transfer files between devices over a network. FTP allows users to upload and download files between a client and a server. FTP is often used by web developers to upload files to web servers, and by businesses to transfer large files such as software updates or customer data.

SMTP (Simple Mail Transfer Protocol)

SMTP is a protocol that is used to send email messages between devices. SMTP is responsible for transferring the message from the sender's email server to the

recipient's email server. SMTP is a simple text-based protocol that allows email clients and servers to communicate with each other.

Networking protocols

DNS (Domain Name System)

DNS is a protocol that is used to translate human-readable domain names (such as www.konnel.com) into IP addresses that can be understood by computers. DNS servers maintain a database of domain names and their corresponding IP addresses, and are responsible for directing internet traffic to the correct server. Without DNS, users would need to remember the IP addresses of every website they wanted to visit.

Network hardware components

Routers

A router is a networking device that connects multiple devices on a network and forwards data between them. Routers are used to connect devices to the internet, and to create local area networks (LANs) and wide area networks (WANs). Routers use routing tables to determine the most efficient path for data to travel between devices on a network. Routers also provide security features such as firewalls to protect networks from unauthorized access.

Switches

A switch is a networking device that connects multiple devices on a network and allows them to communicate with each other. Switches are used to create LANs, and are used to manage network traffic. Switches can determine the destination of data packets and forward them to the appropriate device, which reduces network congestion and improves network performance.

Modems

A modem is a networking device that allows devices to connect to the internet over a telephone or cable line. Modems convert analog signals from a telephone

or cable line into digital signals that can be understood by computers, and vice versa. Modems are used by internet service providers (ISPs) to provide internet access to customers.

Network hardware components

NICs (Network Interface Cards)

A NIC is a hardware component that allows a device to connect to a network. A NIC can be installed in a device such as a computer or printer, and allows it to communicate with other devices on the network. NICs can be wired or wireless, and provide a unique identifier (MAC address) for the device on the network. NICs are essential for connecting devices to a network, and are often built into modern devices such as smartphones and tablets.

Routers and TCP/IP (Transmission Control Protocol/Internet Protocol)

When a device wants to send data to another device on a different network, it sends the data to the default gateway, which is the IP address of the router that connects the device to the internet. The router then uses the TCP/IP protocol to break the data into packets and forwards them to the appropriate destination using the routing table. TCP/IP is the networking protocol that is used to break data into packets and route them across the internet, while routers are the networking hardware devices that are responsible for forwarding those packets between different networks. Together, TCP/IP and routers enable devices on different networks to communicate with each other.

Part 2: Analysis

What if?

What if we were to consider a hypothetical scenario in which a small business needs to set up a computer network. What type of network would be best suited for their needs? Justify your answer.

Passing Grade Internet Cafe, a LAN would be the most suitable network type as it is a small business operating within a limited geographical area. A LAN would allow the cafe's computers to share resources such as printers, files, and an internet connection. This would enable the cafe to provide internet access to its customers, share files between employees, and centrally manage its network resources.

Furthermore, a LAN is relatively easy and cost-effective to set up and maintain compared to other network types such as wide area networks (WANs) or metropolitan area networks (MANs). LANs require only basic network hardware components such as routers, switches, and NICs, which are readily available and affordable. Additionally, LANs are secure as they are not exposed to the internet, reducing the risk of cyberattacks.

In the case of which Passing Grade Internet Café, a LAN would be the most suitable network type for Passing Grade Internet Cafe's needs as it would enable the cafe to share resources, provide internet access to customers, and centrally manage its network resources in a cost-effective and secure manner.

OSI model

The OSI (Open Systems Interconnection) model is a conceptual framework that describes how data is transmitted between devices on a network. It is a seven-layer model that specifies how communication should occur between devices on a network, with each layer performing a specific function in the transmission process.

The seven layers of the OSI model are:

- Physical Layer: This layer deals with the physical aspects of network communication, such as transmitting bits over a physical medium. Examples of devices at this layer include network cables, hubs, and repeaters.
- Data Link Layer: This layer deals with the logical transmission of data between devices, including error detection and correction. Examples of devices at this layer include switches, bridges, and NICs.
- Network Layer: This layer deals with the routing of data packets between devices on different networks. Examples of devices at this layer include routers and Layer 3 switches.
- Transport Layer: This layer deals with the reliable transmission of data between devices, including error recovery and flow control. Examples of protocols at this layer include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
- Session Layer: This layer manages the communication sessions between devices, including establishing, maintaining, and ending sessions. Examples of protocols at this layer include NetBIOS and RPC (Remote Procedure Call).
- Presentation Layer: This layer deals with the presentation of data to the application layer, including data encoding, compression, and encryption. Examples of protocols at this layer include JPEG and MPEG.
- Application Layer: This layer deals with the interaction between applications and the network, including providing services such as email, file sharing, and web browsing. Examples of protocols at this layer include HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol).

OSI model

To facilitate communication between devices on a network, the OSI model specifies how data is transmitted through each layer. For example, when a user sends an email using a web-based email client, the email is transmitted as follows:

- The email data is divided into bits and transmitted over the physical layer using network cables.
- The data link layer adds header and trailer information to the data to create a data frame that includes error detection and correction.
- The network layer adds routing information to the data frame to ensure it is transmitted to the correct destination.
- The transport layer adds a port number to the data frame to ensure it is delivered to the correct application.
- The session layer establishes and maintains a connection between the email client and server.
- The presentation layer encodes the email data in a format that can be read by the email application.
- The application layer uses the SMTP protocol to send the email data to the email server, which then forwards it to the recipient's email client.

In summary, the OSI model facilitates communication between devices on a network by defining how data is transmitted through each layer. Each layer performs a specific function in the transmission process, which enables devices to communicate with each other in a structured and standardized way.

Part 3: Application

What if?

Imagine you are a network administrator for a company and you have just received a report of a network outage. What steps would you take to troubleshoot the issue and restore network
connectivity?

Passing Grade Solutions is a company that specializes in providing cutting-edge technology solutions for businesses of all sizes. We pride ourselves on delivering innovative solutions that help businesses streamline their operations, improve their efficiency, and ultimately achieve their goals.

Recently, we received a report of a network outage affecting our organization. As the network administrator, my primary responsibility is to troubleshoot and resolve this issue as quickly as possible to minimize any disruption to our operations.

Network outages can be caused by a wide range of factors, including hardware failures, software glitches, configuration errors, and even cyber-attacks. Identifying the root cause of the outage is critical in restoring network connectivity and preventing future outages.

As the network administrator, I will follow a rigorous troubleshooting process to identify the source of the outage and take appropriate actions to restore network connectivity. This may include checking physical connections, verifying network device configurations, and restarting network devices.

Ultimately, my goal is to minimize downtime and ensure that Passing Grade Solutions' network infrastructure is running smoothly and efficiently to support our business operations.

What if?

As a network administrator for Passing Grade Solutions, these are the steps I would take to troubleshoot and restore network connectivity:

1. **Verify the outage:** The first step is to confirm that there is indeed a network outage. This can be done by checking with users to see if they are experiencing any issues, checking network monitoring tools, and examining server logs for any error messages.
2. **Identify the affected systems:** Once the outage has been confirmed, the next step is to identify the affected systems. This can be done by reviewing network topology diagrams, examining switch configurations, and using network monitoring tools to determine which devices are not responding.
3. **Isolate the problem:** Once the affected systems have been identified, the next step is to isolate the problem to a specific device or network segment. This can be done by disabling and enabling network devices one at a time to see if the problem clears up.
4. **Check network cabling and physical connections:** Sometimes network connectivity issues can be caused by faulty cabling or loose connections. I would

physically inspect network cables and connections to ensure they are secure and properly connected.

5. **Check device configurations:** Network connectivity issues can also be caused by misconfigured network devices. I would check the configuration of affected devices to ensure they are properly configured.
6. **Restart network devices:** If the issue is not resolved by any of the above steps, I would try restarting affected network devices. This can often clear up network connectivity issues.
7. **Monitor network:** Once connectivity has been restored, I would continue to monitor the network to ensure that there are no further issues.

What if?

After troubleshooting, we found that the issues are with the faulty routers, it caused the outage at company. Routers are an essential component of any network infrastructure, as they are responsible for directing traffic between different network segments and ensuring that data is transmitted efficiently and securely.

This caused a range of issues, including:

1. **Network downtime**

   A router outage can result in a complete loss of network connectivity, causing disruptions in business operations and communication.

2. **Slow network performance**

If the routers are not able to handle the volume of traffic on the network, it can lead to slow network performance, causing delays and frustration for users.

3. **Security vulnerabilities**

   Routers are responsible for enforcing network security policies and protecting against cyber-attacks. If the routers are not functioning correctly, it can leave the network vulnerable to security breaches and data theft.

4. **Difficulty in troubleshooting**

   Routers are a critical component of network infrastructure, and troubleshooting router issues can be complex and time-consuming. This can result in prolonged network downtime and increased costs for the company.

We addressed the problem and had all the routers changed and reprogrammed and Passing Grade Solutions network has been restored.

What if?

Develop a plan for securing a wireless network against unauthorized access. Your plan should include specific security measures and protocols.

These are the comprehensive plan we have developed for securing a wireless network against unauthorized access.

- Secure Network with Encryption The first step to securing a wireless network is to ensure that the network is encrypted. The most used encryption protocol for wireless networks is WPA2 or WPA3. Encryption prevents unauthorized access to the network by making the data transmitted over the network unreadable to anyone who does not have the encryption key.

- Change Default Credentials Most wireless routers come with default usernames and passwords, which are easily accessible to hackers. Therefore, the second step in securing a wireless network is to change the default credentials to a strong password that is difficult to guess. It is essential to change the username and password regularly and to ensure that the password is a combination of uppercase and lowercase letters, numbers, and special characters.

- Enable Firewall A firewall is a security system that monitors and controls incoming and outgoing traffic on a network. A firewall can prevent unauthorized access to the network by blocking suspicious traffic. It is recommended to enable a firewall on the wireless router to prevent unauthorized access to the network.

What if?

- MAC Address Filtering MAC address filtering is another effective way to secure a wireless network. A MAC address is a unique identifier assigned to each device that connects to a network. By enabling MAC address filtering, only devices with specific MAC addresses can connect to the network. To enable MAC address filtering, the network administrator must create a

whitelist of MAC addresses for the devices that are authorized to connect to the network.

- Keep Network Firmware Up-to-Date The firmware is the software that runs on the wireless router. It is essential to keep the firmware up-to-date to ensure that the router has the latest security patches and features. Most wireless routers have an automatic update feature that can be enabled to ensure that the firmware is updated regularly.

- Implement Two-Factor Authentication Two-factor authentication (2FA) is a security mechanism that requires users to provide two forms of authentication to gain access to a network. In addition to the username and password, a 2FA system may require a second form of authentication, such as a fingerprint scan or a one-time password sent to the user's mobile phone. Implementing a 2FA system can significantly reduce the risk of unauthorized access to the wireless network.

What if?

- Network Segmentation Network segmentation is the process of dividing a network into smaller segments to reduce the risk of a security breach. By dividing the network into smaller segments, it is easier to isolate and contain security breaches, preventing unauthorized access to sensitive areas of the network. For example, a company may choose to segment its wireless network into separate segments for guests and employees.

- Educate Employees on Network Security Finally, it is essential to educate employees on network security best practices. Employees must be trained on how to create strong passwords, how to recognize and report suspicious activity, and how to avoid clicking on links or downloading attachments from unknown sources. Providing regular training and reminders to employees can significantly reduce the risk of a security breach.

By implementing these measures, organizations can significantly reduce the risk of unauthorized access to their wireless networks and ensure that sensitive information is protected.