Computer Network Security

What is a computer network?

This refers to interconnected computing devices that can exchange data and share resources with each other. Networked devices use a system of rules, that helps to transmit information over physical or wireless technologies called Communications Protocol.

What is a computer network made of?

The foundation of computer networking is made with the use of nodes and links. A network node may be classified as data communication equipment (DCE) and these would include a modem, hub or a switch. On the other hand, it could also be classified as data terminal transmission (DTE) such as two (2) or more computers and printers. A link refers to the transmission media connecting two nodes. Links can be physical, for example, cable wires or optical fibers or free space used by wireless networks.

DCE is is used to perform signal exchange, coding and line clocking tasks as part of intermediate equipment.

DTE is equipment that acts as sources or destinations in digital communication and is capable of converting information to signals and also reconverting received signals.

Why is computer networking important in cyber security?

Modern network solutions comes with in-built security features such as encryption and access control. To make it more secure solutions like antivirus software, fire walls and anti malware can be integrated to make the network even more secured. Having a good network security will play a crucial role in preventing cyber criminals from gaining access to valuable data and sensitive information. The risks of having poor cyber security in a company could include:

Operational risks - If hit with an attack and the network cannot withstand it, business operations will slow or worst case, come to a halt.

Financial risks - which would stem from the operational risk, business slowing down or stopping could result in loss of revenue and/or suffer from an attack that could potentially steal any intellectual property the company may have.

The different types of networks.

* Local area network (LAN) - an interconnected system limited in size and geography. Typically connecting computers and devices within a single office or building. This type of network is used by small companies or as a test network for small- scale prototyping. This is wired connectivity.
* Wireless local area network(WLAN) - as its name states it’s a LAN network with the difference being that its connectvity is with the use of wireless technology.
* Wide are networks(WAN) - A wide are network is on enterprise network spanning buildings, cities and countries. Compared to LAN that is fast within a close proximity, WAN is set up and used for long-distance communication that is secure and dependable.
* Metropolitan area network (MAN) - This integrates multiple LAN’s within a metro city into a bigger network. Made up of optical fibers and cables as its media, it supports a distributed application environment. Information and resources can be shared across MAN by users and can configured with having limited user access.
* Additionally, another form of MAN is Campus area network (CAN), which is widely used in a vast university campus. It allows departments with their own LAN’s being able to connected through it, thus enabling resource sharing between students.

Types of Network Topology

Bus Topology

In a bus topology, each device on the network is connected to a common main cable, creating a single communication path for all nodes. One point transmits data along a single route to another point. We cannot transmit data in both ways. Linear Bus Topology is the term used for this topology when it has exactly two endpoints and is primarily utilized for small networks.

Advantages of Bus Topology

* Bus topology is easy to set up and does not require a lot of cables.
* It is suitable for small networks with a low number of devices.
* It is cost-effective as it requires less cabling and hardware.
* Failure of a single device does not affect the rest of the network.

Disadvantages of Bus Topology

* A cable break in the backbone cable can cause the entire network to fail.
* As the number of devices increases, the network performance can slow down.
* It is challenging to identify and troubleshoot problems in the network.
* It has limited scalability, as adding new devices to the network is challenging

Ring Topology

The devices in a ring topology, such as computers, printers, or servers, are interconnected in a circular or ring-like pattern, which forms a closed loop. Two other devices link each device in the Ring topology., positioned on either side. The last device in the chain connects to the first device, completing the circuit. Each device in a ring topology is linked to two other devices, one on either side, forming a continuous ring or loop. In a ring topology, data is transmitted in one direction around the circle, with each device on the network reading and passing on the data until it reaches its destination.

Advantages of Ring Topology

* Reliability: A ring topology provides redundancy, meaning that transmitting data through the other devices in the loop is possible if one device fails. This makes the network more reliable than different topologies where a single point of failure can bring down the entire network.
* Balanced Network Traffic: In a ring topology, each device has an equal opportunity to transmit data, which helps to balance network traffic. This reduces the risk of congestion and ensures that all devices receive equal bandwidth.
* Efficient Use of Network Resources: In a ring topology, data travels in one direction around the loop, meaning there is no need for collision detection or retransmission of data. Making it a more efficient use of network resources and can result in higher performance.
* Scalability: A ring topology can easily scale up or down by removing or adding devices from the loop. This makes it a flexible option for networks that need to grow or shrink over time.
* Security: A ring topology provides security because data can only travel in one direction around the loop. Thus, it makes it more challenging for hackers to intercept data or inject malicious code into the network.

Disadvantages of Ring Topology

* Despite its advantages, a ring topology also has some disadvantages, including:
* Failure of a Single Device: While a ring topology is reliable, the failure of a single device can disrupt the entire network. This can occur when a device fails to transmit data or the cable connecting two devices breaks.
* Limited Number of Devices: A ring topology is limited in its support number. Each device must connect to the loop, which can determine the network’s size.
* Difficult to Troubleshoot: When a failure occurs in a ring topology, it can be challenging to locate the source of the problem. Data travels in a circular loop, making it hard to pinpoint where the failure occurred.
* Slow Performance: While a ring topology efficiently uses network resources, connecting many devices to the loop can also result in slow performance in the Ring topology. Data must travel through each device in the circle before reaching its destination.
* Cost: Implementing a ring topology can be higher than other topologies, especially if the network needs to cover a large area. Each device in the Ring topology must connect to the loop with a dedicated cable, which can cause slow performance.

Star Topology

In a star topology network, all devices directly link to a central switch or hub, serving as the central connection point. In this topology, Devices transmit data through the central hub, which then distributes the data to all devices connected. Hubs can either be active or passive, with active hubs containing repeaters and passive hubs being classified as non-intelligent nodes. Each node is connected directly to a central node, which serves as a repeater during data transmission.

Advantages of Star Topology

There are several advantages to using a star topology in a network:

* Easy to install and manage: All devices are connected to a central hub in a star topology, making it easy to add or remove devices without disrupting the network and quickly identifying and isolating network problems.
* High reliability: Each device in a star topology connects to the central hub with a separate cable, which means that if one cable or device fails, it will not impact the rest of the network.
* High performance: In a star topology, the data flow is centralized through the hub, reducing collisions and congestion on the network. This results in increased network performance and fast data transmission.
* Easy to troubleshoot: Since each device connects to the central hub, it is easy to identify and isolate network problems, which makes it easy to troubleshoot and fix network issues.
* Flexible: Adding new devices to the network can quickly expand a star topology, Making it a flexible topology that can grow and adapt to changing network requirements.

Disadvantages of Star Topology

There are a few disadvantages to using a star topology in a network:

* The central point of failure: The hub or switch is the central point of communication in a star topology. If the hub or switch fails, the entire network can be affected.
* Cost: A star topology requires more cabling and equipment than other network topologies, such as a bus topology. This can make it more expensive to install and maintain.
* Limited scalability: As the number of devices in the network grows, the number of cables required to connect all devices to the hub or switch can become unwieldy. This can limit the scalability of the network.
* Dependency on hub or switch: A star topology relies heavily on the hub or switch. The entire network can be affected if the hub or switch is not functioning correctly.
* Complex cabling: While a star topology is easy to manage, setting up and configuring the cabling for an extensive network can be problematic. Proper planning and installation of cabling is crucial for ensuring network efficiency and effectiveness.

Mesh Topology

Network channels connect each node to all the other nodes in a mesh topology. [Mesh topology](https://www.educba.com/what-is-mesh-topology/) is a point-to-point connection, which means that there are multiple paths that data can take between any two devices, providing redundancy and fault tolerance in case of a network failure.

The mesh topology supports two data transmission techniques: routing and flooding. In the routing technique, the nodes are equipped with a routing logic, such as selecting the shortest distance path to the destination node or avoiding routes with broken connections. On the other hand, the flooding technique involves broadcasting the data to all network nodes, eliminating the need for routing logic. While this technique enhances the network’s robustness, it may also generate unwanted network traffic and result in a heavy load on the network.

Types of mesh Topology

* Full Mesh Topology: In a full mesh topology, each device directly connects to all other devices, resulting in multiple redundant paths for data transmission between any two devices. This setup offers the highest degree of fault tolerance and redundancy, ensuring that data can still travelling between devices even if one or more connections fail. However, a full mesh topology can be expensive and difficult to manage, especially in more extensive networks.
* Partial Mesh Topology: In the partial mesh topology, only some devices directly connect to every other network device. Thus, it balances redundancy and cost-effectiveness, as people don’t need to connect all devices to every other device directly. In a partial mesh topology, people connect each device to at least two different devices, which means there are still multiple paths for data to travel between any two devices on the network. However, a partial mesh topology may have lower redundancy than a full mesh topology.

Advantages of Mesh Topology

Mesh topology has several advantages that make it a popular choice in networking applications, including:

* Fault Tolerance: Mesh topology provides redundancy and multiple paths for data to travel between devices, which means that if one link fails, data can be rerouted through another, ensuring that the network remains operational even in a network failure.
* Scalability: Mesh topology is scalable and can easily accommodate new devices without disrupting the existing network. New devices can be added to the network without affecting its performance, making it a popular choice for large networks.
* Flexibility: Mesh topology provides network design and topology flexibility. People can design the network to suit the application’s specific needs, with devices connected in a full mesh or partial mesh configuration.
* Reliability: Mesh topology provides a reliable way to manage networks, even in network failures. With multiple paths to travel between devices, data can be rerouted in case of network failures, ensuring the network remains operational.
* Security: Mesh topology provides a high level of security, as data can be transmitted over multiple paths between devices, making it difficult for attackers to intercept or disrupt the network.

Disadvantages of Mesh Topology

Mesh topology also has some disadvantages that should be considered while deciding whether to use it in a network, including:

* Cost: Implementing a mesh topology, especially in large networks, can be expensive. Users must connect every device in the network to multiple other devices., which can require a significant amount of cabling, hardware, and infrastructure.
* Complexity: Mesh topology can be complex to implement and manage, especially in more extensive networks. Users should use routing protocols and algorithms to drive traffic flow between devices. Failure detection and recovery mechanisms must be in place to ensure the network remains operational despite node failures.
* Latency: In a mesh topology, data may need to travel through multiple nodes to reach its destination, increasing latency and affecting network performance. It can be problematic in applications with critical low latency, such as real-time communication or online gaming.
* Network Overhead: The routing protocols used in mesh topology can generate significant network overhead, as devices must communicate with each other to manage traffic flow and detect node failures. However, it can affect network performance, especially in more extensive networks.
* Power Consumption: In wireless mesh networks, devices must transmit and receive data over the air, which can consume significant amounts of power. It can be a problem in applications with limited battery life, such as IoT sensors.

Tree Topology

A tree topology refers to a specific type of network topology where a central node, also known as the root node, is connected to one or more nodes, which in turn are connected to additional nodes, forming a hierarchical structure resembling a tree.

In a tree topology, nodes connected directly to the root node are called “level 1” nodes, while nodes connected to level 1 nodes are called “level 2” nodes, and so on. This hierarchical structure can expand to multiple levels, creating a large and complex network.

Advantages of Tree Topology

Some advantages of using a tree topology in a network include the following:

* Scalability: Tree topologies can be easily scaled to include additional nodes and branches as the network grows without affecting the network’s performance.
* Hierarchical structure: The hierarchical structure of a tree topology makes it easier to manage and organize large networks, as nodes can be grouped and managed by level.
* Efficient data transmission: In a tree topology, data only needs to travel up or down the hierarchy to reach its destination, making data transmission more efficient and faster.
* Centralized control: The root node in a tree topology provides centralized control over the network, making it easier to manage and monitor network traffic and security.
* Redundancy: Redundancy can be built into a tree topology by using multiple root nodes or backup systems, ensuring that the network remains operational even if one node fails.
* Flexibility: Designers create tree topologies to fulfill specific network requirements, such as accommodating various devices and protocols.
* Cost-effective: Tree topologies are cost-effective, as they require less cabling and hardware than other topologies, such as mesh or star topologies.

Disadvantages of Tree Topology

Some disadvantages of using a tree topology in a network include:

* Single point of failure: The root node in a tree topology represents a single point of failure. The entire network can become unavailable if the root node fails or is disconnected.
* Cost: While tree topologies can be cost-effective, they may require more cabling and hardware than other topologies, such as a bus or ring topology.
* Complexity: As the network grows, the complexity of the tree topology can increase, making it more challenging to manage and troubleshoot.
* A limited number of nodes: The number of branches created limits the number of nodes in a tree topology. In return, this can restrict the network’s scalability.
* Performance issues: In some cases, data transmission in a tree topology may be slower than in other topologies, such as a mesh topology, especially if there is a lot of network traffic.
* Maintenance: Maintaining and troubleshooting a tree topology can be more challenging than other topologies, especially if there are issues with the root node or the network branches.

Hybrid Topology

[Hybrid topology](https://www.educba.com/what-is-a-hybrid-topology/) refers to combining two or more different network topologies. It combines the advantages of each topology to create a more robust and flexible network infrastructure.

Advantages of Hybrid Topology

* Scalability: Hybrid topology allows for adding new network segments, making it easier to scale up or down as per the organization’s needs.
* Flexibility: Since a hybrid topology combines different topologies, it offers greater flexibility in network design, as the user can customize different segments to meet specific requirements.
* Robustness: Hybrid topology offers better redundancy and fault tolerance than other topologies. If one segment fails, the network can continue functioning through another segment.
* Cost-effective: Hybrid topology can be cost-effective because organizations can use existing infrastructure and add new technology only where necessary.
* Improved Performance: Hybrid topology can be designed to provide faster data transfer speeds, improved performance, and lower latency by using the most suitable topology for each network segment.

Disadvantages of Hybrid Topology

* Complexity: Hybrid topology can be more complex than other topologies. It requires knowledge and expertise to design and maintain, leading to higher costs and a greater chance of errors or issues arising.
* Maintenance: Hybrid topology requires regular maintenance to ensure all network segments function correctly. Implementing such a solution can become time-consuming and costly if an organization lacks in-house IT expertise.
* Security: Hybrid topology can be more vulnerable to security threats than other topologies, combining different segments with different security protocols and configurations, creating potential weaknesses that hackers can exploit.
* Compatibility: The different segments in a hybrid topology may use various technologies and protocols, making it challenging to ensure their compatibility. It can result in communication issues and performance problems.
* Cost: While hybrid topology can be cost-effective in some cases, it can also be more expensive than other topologies, particularly if the organization needs to invest in new infrastructure or technology to support the hybrid network.

The functions of common networking devices

Routers

* Routers are networking devices that connect multiple networks together, such as connecting a local network to the Internet. They use IP addresses to route data packets between networks, and they can be used to control traffic and filter unwanted traffic.

Switches

* Switches are networking devices that connect devices within a local network, such as connecting computers, printers, and servers. They use MAC addresses to direct traffic to the correct destination device, and they can also be used to control traffic and segment networks.

Hubs

* Hubs are older networking devices that operate at the physical layer of the network. They receive incoming data packets and broadcast them to all devices connected to the hub. They do not have the ability to control traffic or filter unwanted traffic.

Firewalls

* Firewalls are networking devices that protect a network from unauthorized access and malicious traffic. They can be hardware or software-based, and they monitor incoming and outgoing traffic to prevent unauthorized access and protect against network attacks.

Network Security Audit for X Telecommunications

I conducted a security audit by doing a basic scan network, using the Nassus tool. I determined that there were three vulnerabilities that could put the company’s network at risk of a breech or an attack. These area unpatched software and systems, insecure network protocol and insufficient access controls. These vulnerabilities are common and can be addressed by adhering to the measures that I have formulated for this company.

Measures to address these vulnerabilities

Using secure network protocols

* Protocols such as hyper text transfer protocol secure (HTTPS), secure shell (SSH) and secure socket layer transport layer security (SSL/TLS). These protocols provide secure data transferring and it would be best to use them for the company. More importantly given the nature of the company, SSL/TLS is highly recommended as this involves securing data between server/client. For example, credit card numbers, passwords etc.

Implement strong access controls

* Limiting user access on a need-to-know basis, where whoever trying to access a certain data would be granted permission. The use of multi factor authentication would also be crucial.

Ensuring all software is up to date

* This would include updating the software of the operating systems, applications and other security software. Ensuring regular patching is done with the latest security patches.

Educating employees

* Letting employees be educated on basic network security and what they can do help prevent attacks and how to identify potential threats earlier.

My plan to maintain and monitor the network security

Regular checkups should be conducted to ensure that the network security plan is being followed and to identify any new security risks that may have emerged. This will help ensure that the network remains secure and that any vulnerabilities are identified and addressed in a timely manner.

Update software and firmware.

* All software and firmware should be kept up to date with the latest security patches and updates. This includes firewalls, anti-virus software, and operating systems.

Conduct regular security audits.

* Regular security audits should be conducted to identify vulnerabilities in the network. Audits can be conducted within or by an external security firm on contract.

Back up data regularly

* Regular backups should be performed to ensure that data can be recovered in the event of a security breach or data loss.

Monitor network traffic

* Network traffic should be monitored continuously to detect any suspicious activity. This can be done by implementing intrusion detection and prevention systems and monitoring network logs

With this plan, X Telecommunications (XTC) will be a step closer in more secure and less vulnerable to any threats that may arise.

References

[www.techopedia.com](http://www.techopedia.com)

aws.amazon.com https://aws.amazon.com/what-is/computer-networking/

techtarget.com

educba.com

www.cbtnuggets.com

www.nternetsociety.org

[www.atonetworks.com](http://www.atonetworks.com)

blog.netwrix.com