Brandon J. Danvers

HEART  STONY HILL

Fundamental concepts of computer networking

## Introduction

Computer networking is a crucial aspect of modern communication and enables the exchange of information and resources between computers and other devices. In this project, we will explore the basic concepts of computer networking, including the different types of networks, network topologies, network protocols, and the OSI model. We will also examine the challenges and security issues that arise in computer networking and explore the technologies and tools used to address them. By the end of this project, we will have a deeper understanding of the fundamentals of computer networking and its importance in today's digital world.

# What is a computer network?

A computer network is a system that connects two or more computing devices for transmitting and sharing information. Computing devices include everything from a mobile phone to a server. These devices are connected using physical wires such as fiber optics, but they can also be wireless.

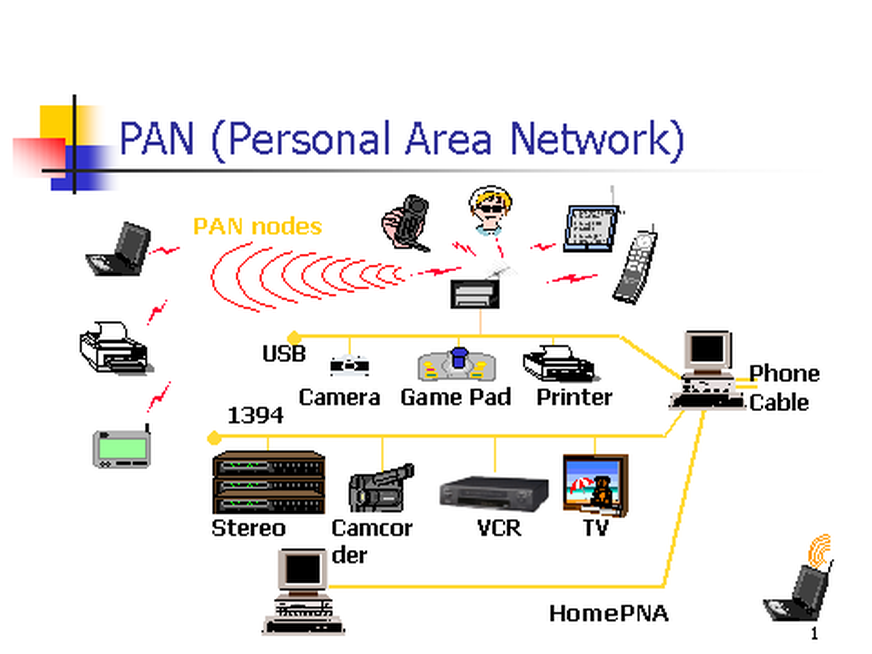
Computer networking is the branch of computer science that deals with the ideation, architecture, creation, maintenance, and security of computer networks. It is a combination of computer science, computer engineering, and telecommunication.

### Types of Computer Network

1. **Personal Area Network (PAN)**

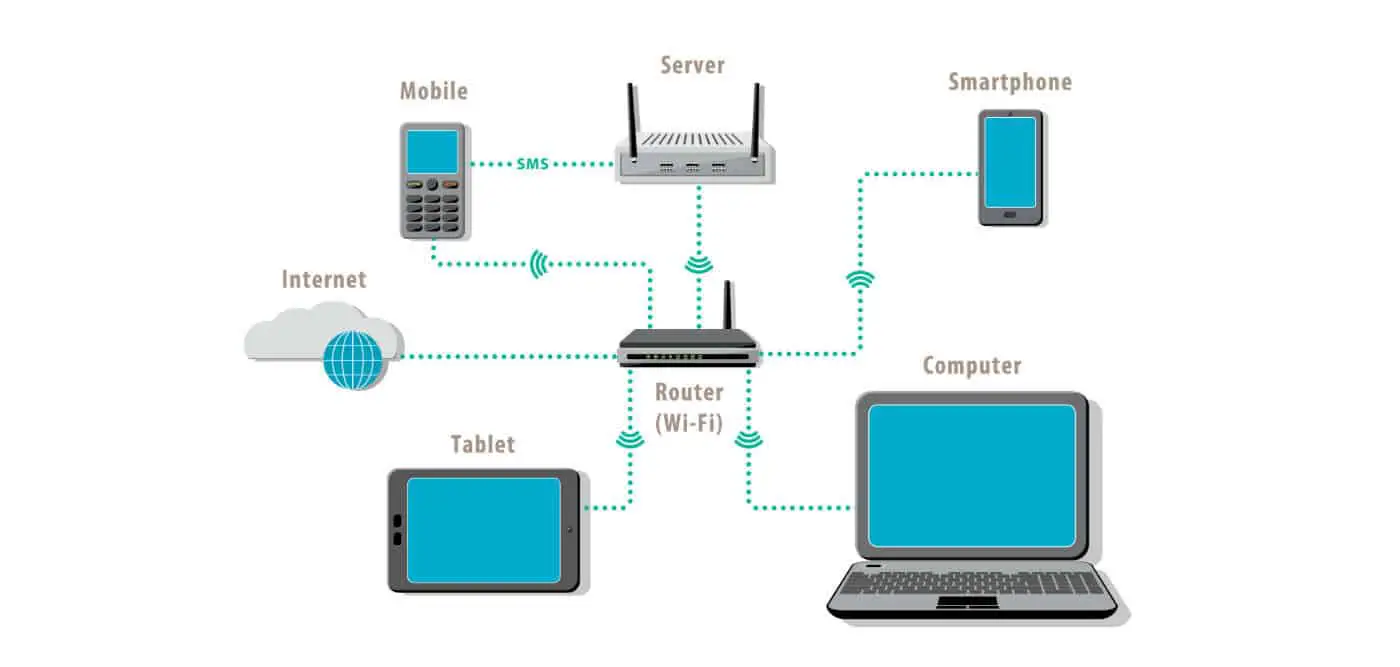
PAN is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centred only on an individual’s workspace. It has a network range of 1 to 100 meters from person to device providing communication with high transmission speed, helped by very easy maintenance and very low cost.

The PAN uses Bluetooth, IrDA, and Zigbee as technology.

Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.

2. **Local Area Network (LAN)**

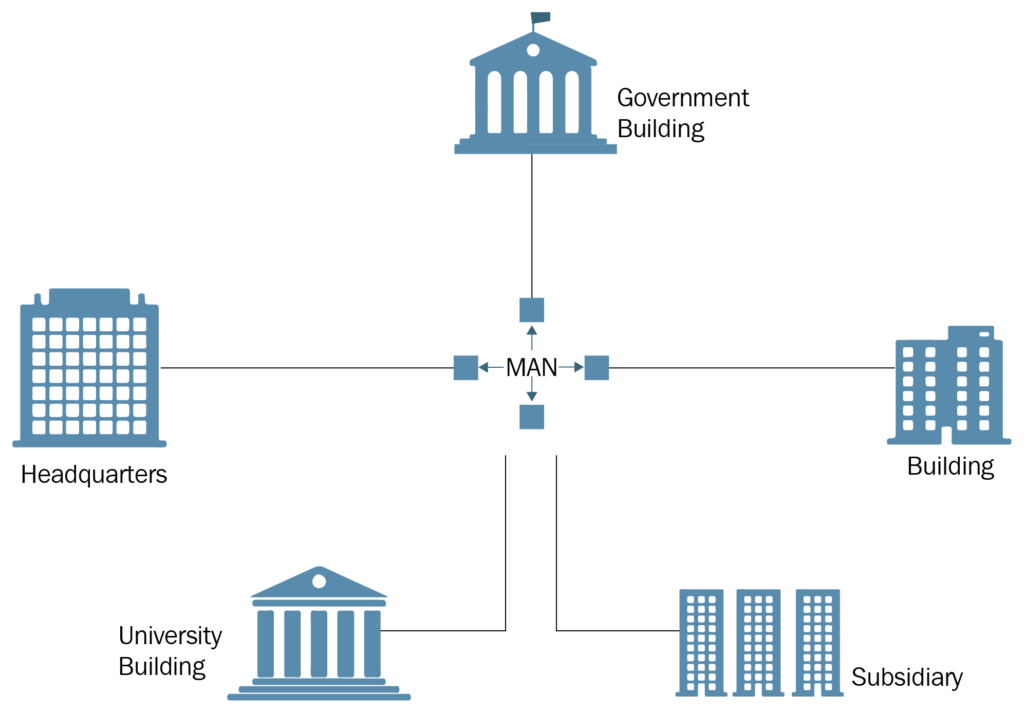
The most frequently used network, which connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-Fi. The range of a LAN is up to 2km & transmission speed is very high with easy maintenance and low cost.

Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.

4. **Metropolitan Area Network (MAN)**

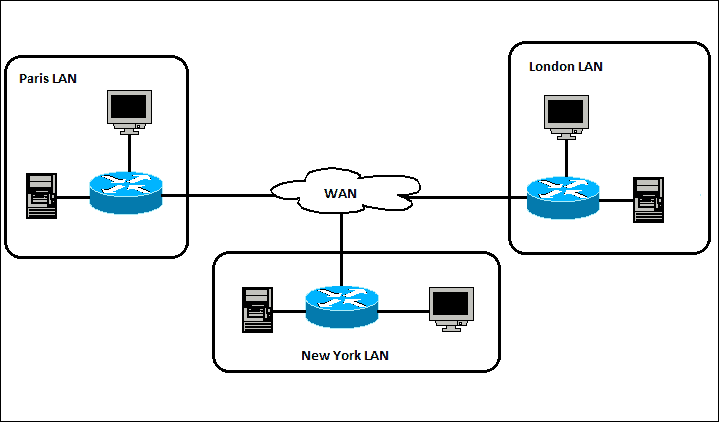
Larger than a LAN but smaller than a WAN. A type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area, using mainly FDDI, CDDI, and ATM as the technology with a range from 5km to 50km with an average transmission speed. It is difficult to maintain and it comes with a high cost.

Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.



5. **Wide Area Network (WAN)**

A type of computer network that connects computers over a large geographical distance through a shared communication path. WANs are not restrained to a single location, but extend over many locations. Another definition of a WAN is as a group of local area networks that communicate with each other with a range above 50km.



# What are network protocols?

An established set of rules that determine how data is transmitted between different devices in the same network. It allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.1 Network protocols can be equated to languages that two devices must understand for seamless communication of information in an easy, reliable and secure way.

# Types of Network Protocols

**Network Communication Protocols**

The efficiency of a network depends on the communication protocols used. In reality, without these protocols, computer networks would not be possible.

The formats and regulations that govern how data is exchanged via networks are formally described by these protocols.

This applies to both hardware and software, and is a requirement for communicating between your computing systems and in telecommunications.

In addition to handling syntax, synchronization, and semantic requirements that both analog and digital communications must meet to work, communication protocols also handle authentication and error detection.

* **HTTP**– known as *hypertext transfer protocol (HTTP)*, it is an application layer protocol that allows the browser and server to communicate.
* **TCP**– *Transmission Control Protocol (TCP)* It separates data into packets that can be shared over a network. These packets can then be sent by devices like switches and routers to the designated targets.
* **UDP**– *User Datagram Protocol (UDP)* works in a similar way to TCP, sending packets of data over the network. The key difference between the two is that TCP ensures a connection is made between the application and server, but UDP does not.

**Network Management Protocols**

To ensure steady communication and optimal performance throughout the network, network management protocols help specify the policies and processes needed to monitor, administer, and maintain your computer network. They also assist in communicating these demands across the network.

In general, network administrators can troubleshoot connections between hosts and clients using a management protocol. Management protocols give network administrators access to details on the status, availability, packet or data loss, and other aspects of the network connection's functionality.

All networked devices, including computers, switches, routers, and even servers, can be subject to the policies controlled by management protocols.

* **SNMP** - Network device management and monitoring are done using SNMP, or Simple Network Management Protocol. Administrators can monitor and edit endpoint data using this TCP-based protocol to change how devices behave throughout the network. In SNMP, agents are used to gather data and send it to a central SMNP manager, who then queries the agents and receives their responses.
* **ICMP** - The main function of ICMP, or Internet Control Message Protocol, is diagnostics. This protocol allows managed devices on the network to transmit error messages that contain details about problems with device connectivity via the network.

**Network Security Protocols**

Data in transit through network connections is kept safe and secure thanks to network security mechanisms. These protocols also specify how the network protects data from any unauthorized efforts to inspect or extract it. This protects your network data across all data kinds and network media by preventing access from unauthorized users, services, or devices.

Network security protocols typically use encryption and cryptography to protect data so that only specific formulas, algorithms, and logical keys can access it. Secure Socket Layer (SSL), Secure File Transfer Protocol (SFTP), and Secure Hypertext Transfer Protocol (HTTPS) are some of the most widely used protocols for network security.

* **SSL** - A network security technology called SSL, or safe Socket Layer, is primarily used to ensure safe internet connections and protect sensitive data. This protocol can support both server-to-server and server-to-server communication. To make data transfer over SSL unreadable, it is encrypted.
* **SSFP** - As its name suggests, the Secure File send Protocol (SFTP) is used to send files safely over a network. The client and server are authenticated, and data is encrypted.
* **HTTPS** - The secure variant of HTTP is HTTPS, or Secure Hypertext Transfer Protocol. To maintain security, data transferred between the browser and server are encrypted.

# What are network hardware components?

A group of physical or networked devices used for interaction and communication among hardware components operating on a computer network. These are specialized hardware elements that link to one another and allow a network to run smoothly and effectively.

**Hub**

A hub aids in dividing big network connections into numerous small network terminals and also as a point of dissemination. Computes have the priority to submit requests via cable to the Hub whenever they attempt to request a piece of data from the network (wired or wireless). All linked terminals will ascertain whether or not those requests are relevant to them after the hub transmits them over the network. All requests that are unrelated will be ignored.



**Modem**

"Modulator-Demodulator" is the definition of "modem." Moving data from one computer terminal to another computer terminal across a telephone network is the primary goal of utilizing a modem in a computer network.

There are several different kinds of modems.

* **Ethernet modem**: The computer system's NIC is where it is connected.
* **Wireless modem** - A wireless modem is a compact antenna-equipped device that connects to a computer terminal over a wireless network.



**Switches**

Switches are used in wired networks such as Ethernet. A switch is a small hardware component that receives data from other input ports and sends it to the proper output port, from which the destination terminal acquires data via the network.

Here are some examples of switches.

* Switches that are not managed - These switches are typically used in tiny areas, such as a home network.
* Managed switches are employed in medium-sized areas such as small and large companies. Smart switches and Enterprise controlled switches are the two categories.
* Ethernet switches - These switches are most commonly used to reduce network congestion and to connect to LAN points.
* PoE switches are short for "Power over Ethernet" switches.



**Gateway**

A gateway is a unique type of network hardware component that acts as a "Gate" between two networks.

Gateways, like firewalls, guard against undesired traffic since they are located at the network's edge, and all data enters and exits the network via Gateways.

Gateways operate on the OSI model's top tiers, which include the transport, session, presentation, and application layers.

However, communication between two identical network protocols is pointless.



# The Interplay between SSL Network Protocol and Network Hubs in Facilitating Network Communication

Network communication is critical in many fields, including business, academics, and personal connections, in today's interconnected society. The Secure Socket Layer (SSL) network protocol, which is now known as Transport Layer Security (TLS), emerged as a critical technology for assuring secure and encrypted communication over computer networks. Furthermore, network hubs are critical equipment for linking network devices within a local area network (LAN). This paper investigates how SSL and network hubs work together to improve network communication while protecting security and data integrity.

***Secure Socket Layer (SSL) Network Protocol***: 2.1 *Overview*:

SSL is a cryptographic protocol that allows a client and a server to communicate securely over an untrusted network. It operates at the network protocol stack's transport layer, assuring data transmission secrecy, integrity, and authentication.

2.2 *SSL Handshake*:

An SSL handshake protocol is done when a client begins an SSL connection with a server. A set of procedures are involved in the handshake to create a secure connection between the client and server:

1. *ClientHello*: The client sends a message to the server that includes the SSL/TLS versions and cipher suites that are supported.
2. *ServerHello*: The server answers with the SSL/TLS version and cipher suite it has chosen, as well as a digital certificate containing its public key.
3. *Client Authentication*: The client validates the server's digital certificate and obtains the server's public key.
4. *Key Exchange*: The client generates a random session key, encrypts it with the public key of the server, and transmits it back to the server.
5. *Session Key Generation*: The transferred session key is used by both the client and the server to generate symmetric encryption keys for subsequent secure data transmission.

2.3

*SSL Data Encryption*:

After the SSL handshake, the client and server begin secure data transmission. SSL encrypts data using symmetric encryption methods such as *Advanced Encryption Standard* (***AES***). The shared session key ensures that only the client and server can encrypt and decode information sent between them.

***Network Hubs***:

3.1 *Hub Functionality*:

A *network hub* is a central device that links many LAN network devices. Hubs operate at the network protocol stack's physical layer, forwarding network packets to all connected devices.

3.2 Hub Operation:

Network hubs segregate network segments and prevent devices linked to different hubs from communicating directly with one another. This isolation gives an extra degree of security by limiting the possibility of unauthorized access or eavesdropping. SSL encryption assures that even if an unauthorized device intercepts encrypted data transmitted through a hub, the information cannot be deciphered without the right decryption keys.

4.3 *Address Resolution*:

At the data link layer of a network, devices interact using ***MAC*** (*Media Access Control*) addresses. When a device transmits an *SSL*-encrypted packet, the hub receives it and forwards it to all other devices that are connected. The hub, however, cannot extract the destination ***MAC*** address from the encrypted data since the payload is encrypted. As a result, the packet is sent to all devices that are linked.

4.4 *SSL-Terminating Devices*:

***SSL***-terminating devices, such as load balancers or application delivery controllers, are frequently deployed between the network hub and the server to establish end-to-end SSL connections. These devices accept ***SSL***-encrypted communication, decrypt it with the proper private key, and then re-encrypt it before sending it to the server. This procedure enables the server to process the decrypted data while keeping the communication connection secure.

4.5 *Load Balancing*:

Load balancing can be accomplished by using network hubs in conjunction with ***SSL***-terminating devices to disperse incoming ***SSL*** connections over various servers. ***SSL*** handshake parameters, such as the requested URL or *server name indication* (***SNI***), can be analyzed by load balancers to select the proper server to handle the connection. Load balancing improves performance, scalability, and failure tolerance by evenly dividing ***SSL*** traffic among servers.

***Conclusion***:

The ***SSL*** network protocol and network hubs work together to provide safe and efficient network communication. ***SSL*** provides encryption, authentication, and data integrity protocols, allowing clients and servers to communicate securely. Network hubs, on the other hand, serve as mediators by forwarding network packets to linked LAN devices. While hubs do not directly interact with encrypted ***SSL*** data, they do help to segment and isolate networks, limiting unauthorized access. ***SSL***-terminating devices can be used to handle ***SSL*** encryption and decryption, allowing for easier load balancing while maintaining end-to-end security.

SSL and network hubs collaborate to build a strong network infrastructure that protects data privacy and ensures secure communication in a variety of circumstances. As technology advances, it is critical to be informed about new developments.

# Selecting the Optimal Computer Network for Small Businesses

***Introduction***:

Setting up a dependable and effective computer network is critical for the success of small businesses in today's digital age. Choosing the right network infrastructure takes careful consideration of a number of aspects, including size, budget, scalability, security, and usefulness. In this paper, we will look at the many types of computer networks and argue that a *local area network* (***LAN***) combined with a cloud-based solution is the greatest fit for small enterprises because of its cost-effectiveness, flexibility, security, and ability to support expansion.

1. *Local Area Network* ***(LAN***):

A *local area network* (***LAN***) is a network that links devices inside a specific geographical area, such as an office or a building. Because small organizations often have a limited workplace, a ***LAN*** is the best option. Here are some of the main reasons:

1. *Cost-effectiveness*: ***LAN***s demand less infrastructure investment than other network types. They connect PCs, printers, servers, and other devices using Ethernet cables or wireless connectivity. This ease of use results in decreased installation and maintenance expenses, which is especially advantageous for small firms on a tight budget.
2. *Fast and efficient communication*: A ***LAN*** allows enterprises to benefit from fast data transmission rates between devices. This improves overall productivity and efficiency by allowing for seamless collaboration, file sharing, and access to shared resources.
3. *Improved data security*: Small businesses deal with sensitive information and must safeguard it against illegal access. Security mechanisms such as firewalls, encryption protocols, and access controls can be implemented using ***LAN***s. The risk of external breaches is considerably decreased by keeping data within the local network.
4. ***Cloud-based Solutions***:

Small enterprises can use cloud-based solutions to supplement the capabilities of their LAN. Cloud computing provides various benefits, including:

1. *Scalability*: Cloud-based services allow you to scale resources up or down dependent on your company needs. As the organization expands, it may quickly increase its data storage, computer power, and software applications without making large upfront expenses. This scalability is especially beneficial for small organizations who want to adapt and grow quickly.
2. *Remote work and access*: Cloud-based solutions allow employees to access data and apps from any location with an internet connection. This freedom enables remote work, communication with external stakeholders, and better customer service. Furthermore, cloud services provide dependable backup and disaster recovery alternatives, ensuring business continuity even in the face of unexpected events.
3. *Cost-effectiveness*: Rather than investing in expensive hardware and maintaining an on-site server infrastructure, small businesses can use cloud-based services on a subscription or pay-as-you-go basis. This low-cost method avoids the need for large upfront capital investments and allows organizations to focus their resources on essential activities.

Conclusion:

Finally, when it comes to choosing a computer network for a small business, a mix of a LAN and cloud-based solutions is the best option. LANs provide a low-cost, secure, and efficient framework for internal communications and resource sharing in the workplace. Cloud-based services supplement this, providing scalability, flexibility, accessibility, and cost-efficiency while serving the specialized demands of small enterprises. Small firms can improve efficiency, protect sensitive data, adapt to changing demands, and position themselves for future development and success by deploying such a network architecture.

# OSI Model for Network Communication

The ***OSI*** (*Open Systems Interconnection*) model is a conceptual framework for standardizing communication system functionalities. It is used to facilitate network communication by splitting the process into seven discrete levels, each of which is accountable for a certain set of responsibilities. Let's go through each layer and show how information is conveyed through them.

1. *Physical Layer*: This layer is responsible for the transmission and reception of raw bit streams over a physical medium. It comprises requirements for cables, connectors, and *network interface cards* (***NICs***). At this layer, information is transmitted by converting digital data into electrical signals and modulating them to travel through a copper Ethernet cable.
2. *Data Link Layer*: The data link layer ensures reliable and error-free data flow between two directly connected devices. It frames the data received from the network layer and includes required control information, such as ***MAC*** (*Media Access Control*) addresses. The Ethernet protocol, which transmits data frames between switches in a *local area network* (***LAN***), is an example of this layer.
3. *Network Laye*r: The network layer is concerned with routing and logical addressing. It creates end-to-end communication routes across various networks. This layer handles IP addressing and routing protocols. The *Internet Protocol* (***IP***), which routes packets from the source device to the destination device over the internet, is an example of information transfer at this layer.
4. *Transport Layer*: Enables consistent data delivery between endpoints. It divides huge amounts of data into smaller parts, handles flow management, and provides error recovery procedures. The *Transmission Control Protocol* (***TCP***), for example, assures data packet delivery, establishes connections, and performs congestion control between applications.
5. *Session Layer*: Creates, manages, and terminates communication sessions between applications. It maintains session checkpoints, synchronization, and data exchanges in an orderly fashion. A secure session can be established between a web browser and a web server using protocols such as ***HTTPS***.
6. *Presentation Layer*: is in charge of data representation and ensures that data sent between programs is in a format that they can understand. It is responsible for duties such as data encryption, compression, and protocol conversion. Compression and decompression of picture or video files for network transmission is one example.
7. *Application layer*: nearest to end-user applications and provides services directly to the user. ***HTTP*** (for web browsing), ***SMTP*** (for email), and ***FTP*** (for file transfer) are among the protocols included. A web browser requesting a webpage through ***HTTP*** and receiving the response, which is subsequently rendered for the user, is an example.

Each layer of the OSI model performs certain functions that allow devices on a network to communicate with one another. The OSI model allows for standardized implementations and compatibility between diverse network devices and technologies by splitting the communication process into these layers.

As a network administrator, here are the steps I would take to troubleshoot a network outage and restore network connectivity:

1. *Verify the Issue*:

* Gather information about the reported network outage, such as the affected area, specific devices or services impacted, and any error messages received.
* Check if the issue is widespread or localized to a specific area or department.

1. *Communicate and Inform*:

* Notify the relevant stakeholders, such as users, IT team members, and management, about the network outage.
* Provide updates on the troubleshooting progress and estimated time for resolution.

1. *Check Physical Connections*:

* Inspect physical connections, such as cables, switches, routers, and modems, to ensure they are properly connected and there are no visible signs of damage.
* Re-seat any loose cables or connectors.

1. *Power Cycle Networking Equipment*:

* Power cycle the affected networking equipment, including switches, routers, and modems.
* Turn off the devices, unplug their power cables, wait for about 10-15 seconds, and then plug them back in and power them on.
* Allow sufficient time for the devices to boot up and establish connections.

1. *Test Local Connectivity*:

* Verify connectivity on a local level by checking if devices within the same network segment can communicate with each other.
* Ping other devices or run network diagnostic tools to check for connectivity and latency issues.

1. *Examine Network Configuration*:

* Review the network configuration settings on the affected devices to ensure they are correct and consistent with the network design.
* Check for any recent configuration changes or updates that might have caused the outage.

1. *Check Network Services*:

* Verify the availability and status of critical network services, such as DHCP, DNS, and gateway services.
* Ensure these services are functioning correctly and can be accessed by the affected devices.

1. *Monitor Network Traffic*:

* Use network monitoring tools to analyse network traffic patterns and identify any anomalies or excessive bandwidth consumption that could be causing the outage.
* Look for any network loops, broadcast storms, or denial-of-service (DoS) attacks that could impact network performance.

1. *Collaborate with Network Team*:

* Collaborate with other network administrators or IT team members to troubleshoot the issue collectively.
* Share information, observations, and findings to leverage collective knowledge and expertise.

1. *Contact Network Service Providers*:

* If the network outage persists and appears to be beyond the company's internal network, contact the relevant network service providers to report the issue.
* Provide them with the necessary information and work together to diagnose and resolve the problem.

1. *Document and Review*:

* Document the troubleshooting steps taken, findings, and the resolution for future reference.
* Conduct a post-mortem analysis to understand the root cause of the network outage and identify preventive measures to avoid similar issues in the future.

It is critical to preserve sensitive data and maintain the privacy and integrity of the wireless network by securing it against unauthorized access. Here is a detailed strategy that contains specific security procedures and protocols to assist in creating a more secure wireless network:

1. *Change the Default Settings*:

* Change the default administrator username and password of your wireless router.
* Modify the default ***SSID*** (*Service Set Identifier*) to a unique name that does not reveal the router's manufacturer or model.

1. *Use Strong Encryption*:

* Enable ***WPA3*** (*Wi-Fi Protected Access 3*) or ***WPA2*** with ***AES*** (*Advanced Encryption Standard*) encryption. Avoid using outdated and insecure encryption protocols like ***WEP*** (*Wired Equivalent Privacy*).

1. *Secure the Wi-Fi Network*:

* Disable *Wi-Fi Protected Setup* (***WPS***) as it can be susceptible to brute-force attacks.
* Enable *MAC* (***Media Access Control***) address filtering to allow only specific devices to connect to the network.

1. *Implement Robust Passwords*:

* Set a strong and unique password for your Wi-Fi network. Use a combination of upper and lowercase letters, numbers, and special characters.
* Change the Wi-Fi password periodically, ideally every few months.

1. *Enable Network Segmentation*:

* Configure a guest network for visitors or less trusted devices. Ensure it is isolated from your main network and has limited access privileges.

1. *Enable Firewall Protection*:

* Enable the built-in firewall on your wireless router to monitor and control incoming and outgoing network traffic.
* Regularly update the router's firmware to benefit from security patches and bug fixes.

1. *Disable Remote Management*:

* Disable remote administration of your router from external networks unless necessary. Restrict it to your local network if required.

1. *Enable Intrusion Detection/Prevention Systems* (***IDS/IPS***):

* Set up an IDS/IPS system to detect and prevent suspicious network activity or attacks. This can be done through dedicated hardware or software solutions.

1. *Maintain Updated Devices*:

* Keep your wireless router, access points, and connected devices updated with the latest firmware and security patches.
* Regularly check for firmware updates from the manufacturer's website or configure automatic updates if available.

1. *Educate Users*:

* Train network users about good security practices, such as avoiding connecting to unknown or unsecured networks and being cautious with sharing sensitive information over Wi-Fi.

1. *Regular Network Monitoring*:

* Monitor network logs and traffic patterns for any unusual activity or unauthorized access attempts.
* Utilize network monitoring tools to identify potential security threats and take appropriate actions.

1. *Use VPN (Virtual Private Network*):

* Encourage the use of VPNs, especially when connecting to the network remotely. VPNs encrypt data transmissions and provide an extra layer of security.

Remember that no security solution is perfect, but combining these procedures will considerably improve the security of the network. To remain ahead of developing threats and vulnerabilities, examine and update security policies on a regular basis.

### Bibliography

Mohanakrishnan R, (2022), *What Is a Computer Network? Definition, Objectives, Components, Types, and Best Practices*, <https://www.spiceworks.com/tech/networking/articles/what-is-a-computer-network/>

Expert C (2022), *Network Protocols & How They Can Benefit Your Business*, <https://www.cdw.com/content/cdw/en/articles/networking/types-of-network-protocols.html>

Kanade V (2022), *What Is Network Hardware? Definition, Architecture, Challenges, and Best Practices*, <https://www.spiceworks.com/tech/networking/articles/what-is-network-hardware/>

Cobb M (2021), *SSL (secure sockets layer)*, <https://www.techtarget.com/searchsecurity/definition/Secure-Sockets-Layer-SSL>

Ali M (2019), *LAN vs WAN: Which Network is Right for You?,* <https://www.fieldengineer.com/blogs/lan-wan-which-network-is-right-for-you>

Unknown author, (2017), *What is the Best Kind of Small Business Computer Network?*,https://www.mustardit.co.uk/it-blog/best-kind-small-business-computer-network

Shaw K, (2022), *The OSI model explained and how to easily remember its 7 layers*, <https://www.networkworld.com/article/3239677/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html>