NETWORKING

Networking is the practice of connecting computers, devices, and systems to share data, resources, and services. It forms the backbone of modern communication, enabling everything from the Internet to localized device interactions.

Types of Networks

- LAN (Local Area Network): A small network in a limited area like an office or home.
- WAN (Wide Area Network): Connects multiple LANs over large distances (e.g., the Internet).
- WLAN (Wireless LAN): A LAN that uses Wi-Fi for connectivity.
- MAN (Metropolitan Area Network): Spans a city or campus.
- PAN (Personal Area Network): For personal devices like Bluetooth headphones.
- VPN (Virtual Private Network): Extends private networks over public infrastructure securely.

Network Components

- **Hardware**: Includes routers, switches, hubs, access points, and cables.
- **Software**: Network operating systems, firewalls, and management tools.
- **Protocols**: Rules and conventions for data exchange, such as TCP/IP, HTTP, and FTP.

Networking Hardware:

- **Routers**: Direct traffic between networks.
- **Switches**: Connect devices within a single network.
- **Access Points**: Enable wireless connectivity.
- **Cables**: Physical mediums like Ethernet for wired connections.

Networking Protocols

- **Transmission Control Protocol/Internet Protocol (TCP/IP)**: Foundation of Internet communication.
- **HyperText Transfer Protocol (HTTP/HTTPS)**: For web browsing.
- **Simple Mail Transfer Protocol (SMTP)**: For email.
- **File Transfer Protocol (FTP)**: For file transfers.
- **Domain Name System (DNS)**: Resolves domain names into IP addresses.

How Networks Work

- **Data Packets**: Information is split into packets, transmitted, and reassembled at the destination.
- **IP Addressing**: Devices use unique IP addresses for identification and routing.
- **DNS**: Translates human-readable domain names into machine-readable IP addresses.
- **Routing**: Directs data from source to destination across networks.
- **Switching**: Connects devices within a network by forwarding packets to the correct device.

Network Security

- Protecting networks from unauthorized access, attacks, and data breaches.
- Techniques include firewalls, encryption, VPNs, and intrusion detection systems.
- **Firewalls**: Monitor and control incoming/outgoing traffic.
- **Encryption**: Secures data during transmission.
- **VPNs**: Protect data over public networks.
- **Authentication**: Verifies user and device identities.

- **Cyber Threats**: Includes malware, phishing, DDoS attacks, and ransomware.

Who is a Network Engineer; A **Network Engineer** is an IT professional responsible for designing, implementing, managing, and troubleshooting computer networks to ensure efficient and secure data communication within an organization. They play a vital role in maintaining network infrastructure, enabling seamless connectivity for users, systems, and applications.

Roles and Responsibilities of a Network Engineer

1. **Network Design and Planning**:
    - Develop network architectures based on organizational needs.
    - Plan for scalability, reliability, and security in network designs.
2. **Installation and Configuration**:
    - Set up network devices like routers, switches, firewalls, and access points.
    - Configure network settings, protocols, and security measures.
3. **Monitoring and Maintenance**:
    - Use monitoring tools to track network performance.
    - Perform regular maintenance, updates, and upgrades to hardware and software.
4. **Troubleshooting and Problem Resolution**:
    - Diagnose and fix network-related issues such as connectivity problems, latency, or security breaches.
    - Conduct root cause analysis for recurring issues.
5. **Security**:
    - Implement firewalls, VPNs, and intrusion detection/prevention systems.

    - Protect the network against cyber threats by configuring access controls and monitoring systems.
6. **Documentation**:
    - Maintain detailed records of network configurations, layouts, and changes.
    - Create and update network diagrams and procedures for troubleshooting.
7. **Collaboration**:
    - Work closely with IT teams, developers, and external vendors.
    - Assist other departments in understanding and using network resources effectively.

Installing, Configuring, and Supporting Network Equipment:

- Installing, configuring, and supporting network equipment is a critical responsibility in IT and networking roles, ensuring smooth operation and connectivity within an organization. Here's an overview of the process:
- ---
- **1. Planning and Preparation**
- **Assess Requirements**: Understand the network needs, including bandwidth, security, and scalability.
- **Equipment Selection**: Choose suitable hardware like routers, switches, firewalls, and access points, considering future scalability.
- **Network Design**: Create a network topology diagram to visualize connections and ensure proper placement of equipment.
- **Obtain Necessary Tools**: Gather cabling, patch panels, power supplies, and configuration tools.
- ---
- **2. Installing Network Equipment**
- **Physical Setup**:
- Mount equipment in racks or appropriate locations.
- Connect devices using Ethernet cables, fiber optics, or other media.
- Ensure proper ventilation and power supply.

- **Cable Management**: Organize and label cables to simplify troubleshooting and maintenance.

- **3. Configuring Network Devices**
- **Access Device Interfaces**: Use console ports, web interfaces, or management software.
- **Initial Configuration**:
- Set device hostname and passwords.
- Assign IP addresses and subnets.
- **Routing and Switching**:
- Configure VLANs, routing protocols (e.g., OSPF, BGP), and Layer 2/3 settings.
- **Security**:
- Enable firewalls, access control lists (ACLs), and intrusion detection/prevention systems.
- Configure secure management protocols (e.g., SSH, HTTPS).
- **Wireless Setup (if applicable)**:
- Set SSIDs, encryption (e.g., WPA3), and access policies.

- **4. Testing and Validation**
- **Connectivity Tests**: Use tools like ping, traceroute, and network analyzers.
- **Performance Validation**: Measure latency, throughput, and packet loss using tools like iPerf.
- **Redundancy**: Test failover configurations for high availability.

- **5. Supporting and Monitoring**
- **Monitoring**:
- Use Network Monitoring Systems (NMS) like Nagios, SolarWinds, or PRTG.
- Set up SNMP traps and Syslog for real-time alerts.
- **Maintenance**:
- Perform regular firmware updates and backups.

- Replace aging hardware proactively.
- **Troubleshooting**:
- Identify and resolve issues using diagnostic tools and logs.
- Engage in root cause analysis for recurring problems.
- ---
- **6. Documentation**
- Maintain accurate records of configurations, IP address allocations, and network diagrams. These documents are essential for troubleshooting and future upgrades.

TCP /IP Addressing / DOD Model
(Transmission Control Protocol/Internet Protocol)
(Department of Defense)
Process/Application

Assignment:
Timing difference between IP address and MAC address:

- **48-bits MAC address:** Identifies a device to other devices.
- **32-bits IP address:** Identifies the device globally.
- A network packet needs both addresses to get to its destination.

1. **MAC Address (Media Access Control):**
    - **48-bit Address**: True for most modern MAC addresses (e.g., Ethernet). Some newer standards use 64 bits.
    - **Device-to-Device Identification**: Correct. The MAC address is a unique hardware identifier assigned to a device's network interface card (NIC) and is used within the local network.
2. **IP Address (Internet Protocol):**
    - **32-bit Address**: This is true for IPv4, which uses 32-bit addresses. However, IPv6 uses 128-bit addresses.
    - **Global Identification**: Correct. IP addresses are used to identify devices globally on the internet or across different networks.

3. **Both Addresses in Networking:**
    - Correct. Network packets use **both addresses** for routing. The IP address identifies the destination network and device, while the MAC address is used for communication within the local network (e.g., Ethernet frames).

Notes:

- The MAC address operates at **Layer 2 (Data Link Layer)** of the OSI model, while the IP address operates at **Layer 3 (Network Layer)**.
- MAC addresses are fixed to hardware, while IP addresses can change (e.g., dynamically assigned by DHCP).

The following are some good basic networking resources to get you started.

TCP/IP Protocols

Note: Links without description are official RFCs from the Internet Engineering Task Force (IETF).

* [Address Resolution Protocol (ARP)](https://datatracker.ietf.org/doc/rfc826/)
* [Border Gateway Protocol (BGP)](https://datatracker.ietf.org/doc/rfc4271/)
* [Domain Name System (DNS)](https://datatracker.ietf.org/doc/rfc1035/)
* [Dynamic Host Configuration Protocol (DHCP)](https://datatracker.ietf.org/doc/rfc2131/)
* [File Transfer Protocol (FTP)](https://datatracker.ietf.org/doc/rfc959/)
* [Hypertext Transfer Protocol (HTTP/1.1)](https://datatracker.ietf.org/doc/rfc2616/)
* [Hypertext Transfer Protocol Version 2 (HTTP/2)](https://datatracker.ietf.org/doc/rfc7540/)
* [Internet Protocol Version 4 (IPv4)](https://tools.ietf.org/html/rfc791/)
* [Internet Protocol Version 6 (IPv6)](https://datatracker.ietf.org/doc/rfc2460/)
* [Network Address Translator (NAT)](https://datatracker.ietf.org/doc/rfc1631/)

* [Simple Mail Transfer Protocol (SMTP)](https://datatracker.ietf.org/doc/rfc5321/)

* [Simple Network Management Protocol (SNMP)](https://datatracker.ietf.org/doc/rfc1157/)

* [Secure Shell (SSH)](https://datatracker.ietf.org/doc/rfc4251/)

* [Transmission Control Protocol (TCP)](https://datatracker.ietf.org/doc/rfc793/)

* [Telnet](https://datatracker.ietf.org/doc/rfc854/)

* [User Datagram Protocol (UDP)](https://datatracker.ietf.org/doc/rfc768/)

Courses and YouTube Videos

* [Cisco Networking Academy Courses](https://www.netacad.com/courses/networking) - A various networking courses (Essentials, CCNA, CCNP, etc.).

* [Network Chuck OSI Model](https://www.youtube.com/watch?v=oIRkXulqJA4)

* [Network Chuck Subnetting Playlist](https://www.youtube.com/watch?v=5WfiTHiU4x8&list=PLIhvC56v63IKrRHh3gvZZBAGvsvOhwrRF)

Tutorials

* [Networking](https://www.youtube.com/watch?v=rL8RSFQG8do&list=PLF360ED1082F6F2A5) - A series of YouTube tutorials about networking by Eli the Computer Guy.

* [Wireshark Tutorial for Beginners](https://www.youtube.com/watch?v=flDzURAm8wQ&list=PL6gx4Cwl9DGBI2ZFuyZOl5Q7sptR7PwYN) - TheNewBoston Wireshark Tutorial for Beginners.

* [MikroTik WinBox Manual](https://wiki.mikrotik.com/wiki/Manual:Winbox) - The official manual for MikroTik's WinBox software.

Books

* [Cisco Press](https://www.ciscopress.com/) - Cisco authorized book publisher where you can get all books and official guides for Cisco certifications.

* [Practical Packet Analysis (3rd Edition)](https://nostarch.com/packetanalysis3) - An amazing book about analyzing network packets using Wireshark.

* [Attacking Network Protocols](https://nostarch.com/networkprotocols) - A Hacker's Guide to Capture, Analysis, and Exploitation

by James Forshaw.

* [Automate Your Network: Introducing the Modern Approach to Enterprise Network Management](https://www.amazon.com/Automate-Your-Network-Introducing-Enterprise/dp/1799237885) - Probably one of the best books for network automation by John W. Capobianco.

Software and Tools

Online tools

* [Online nslookup](https://www.nslookup.io) - An online DNS client to view and debug DNS configuration.

* [Online whois](https://whois.domaintools.com/) - An online whois record tool for getting information about domains.

* [OUI Lookup Tool](https://www.wireshark.org/tools/oui-lookup.html) - An online OUI lookup for searching vendors of MAC addresses.

* [MXToolbox](https://mxtoolbox.com/) - A large number of various tools (DNS lookup, MX lookup, Whois, SPF lookup, and more).

Packet capture and analysis

CHECKOUT THE Hacking Scenarios: https://hackingscenarios.com

* [Wireshark](https://www.wireshark.org/) - The most popular free and open source network protocol analyzer.

* [Tshark](https://tshark.dev/) - A CLI version of Wireshark.

* [tcpdump](http://www.tcpdump.org/) - A powerful open source command-line packet analyzer.

* [NetworkMiner](https://www.netresec.com/?page=NetworkMiner) - A network forensic tool for PCAP file analysis.

* [Malware-Traffic-Analysis.net](https://malware-traffic-analysis.net/) - A large collection of malicious PCAP files that can be used to practice packet capture skills.

* [Publicly Available PCAP files](https://www.netresec.com/?page=PcapFiles) - A list of publicly available PCAP files for additional training.

Network simulators and emulators

* [GNS3](https://gns3.com/) - A powerful free and open source network simulator.

* [Cisco Packet Tracer](https://www.netacad.com/courses/packet-tracer) - Cross-platform network visual simulation tool designed by Cisco Systems.

* [EVE-NG](https://www.eve-ng.net/) - A powerful network simulator. Both Community and Professional editions are available.

* [Cisco Modeling Labs](https://www.cisco.com/c/en/us/products/cloud-systems-management/modeling-labs/index.html) - An online platform that helps network engineers simulate the behavior of Cisco routers, switches, and access points. It is intended for customers from enterprise backgrounds.

* [Cisco Virtual Internet Routing Lab (VIRL)](https://learningnetwork.cisco.com/s/virl) - It is a Cisco IOS-based comprehensive network simulation environment. It is intended for all individuals and trainees.

Firewalls and switches

* [pfSense](https://www.pfsense.org/) - An open source firewall/router computer software distribution based on FreeBSD.

* [OPNsense](https://opnsense.org/) - OPNsense is an open source, easy-to-use, and easy-to-build FreeBSD based firewall and routing platform.

* [Open vSwitch](https://www.openvswitch.org/) - Open vSwitch is a production quality, multilayer virtual switch licensed under the open source Apache 2.0 license.

Remote access and sharing tools

* [Remmina](https://remmina.org/) - An open source remote access tool. It supports RDP, SSH, VNC, and other protocols for remote access.

* [PuTTY](https://www.putty.org/) - One of the most popular SSH and Telnet clients for Windows.

* [FileZilla](https://filezilla-project.org/) - An open source tool for file transfer. Support FTP, FTPS and SFTP protocols.

* [WinSCP](https://winscp.net/eng/index.php) - A popular SFTP client and FTP client for Windows.

* [SecureCRT](https://www.vandyke.com/products/securecrt/) - A commercial SSH and Telnet client and terminal emulator by VanDyke Software.

* [WinBox](https://mikrotik.com/download) - Official MikroTik GUI software for administration of MikroTik RouterOS.

Other tools

* [Nmap](https://nmap.org/) - A free and open source software for network discovery and security auditing.

* [Zenmap](https://nmap.org/zenmap/) - The official Nmap Security Scanner GUI.

* [Draw.io](https://github.com/jgraph/drawio-desktop) - An open source software for creating network diagrams and topologies.

Certifications

* [Cisco certifications](https://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html)

IP Addressing / Private

IP Addressing / Private
Network (N) | Host (H)

BIT = 1 and 0 binary
Byte = 8 bit
1 Octet = 8 bits

Class

- A: Large network | Range: 1–126 | Private IP ranges: [N . H . H . H]
- B: Medium ✓ | Range: 128–191 | Private IP ranges: [N . N . H . H]
- C: Small network | Range: 192–223 | Private IP ranges: [N . N . N . H]
- D: 224–239 | Multicast, Broadcast
- E: 240–254 | Research

Assignment:
IANA meaning and functions

Subnet Mask

- A subnet mask identifies the class of the network address, the host bits, and the network bits.
- The subnet mask for class A is 255.0.0.0.
- The subnet mask for class B is 255.255.0.0.
- The subnet mask for class C is 255.255.255.0.

IIIIIIIII																															

Loopback Address

- The loopback address is 127.0.0.1.
- It is reserved for testing network faults