14. OSI Model

OSI stands for **Open Systems Interconnection** — a **reference model** used to describe how communication takes place between different computer systems.
It defines **standards and layers** for reliable data exchange between devices.

What is Network Security?

Network Security refers to the **technologies, policies, people, and procedures** that protect communication systems from **cyberattacks, unauthorized access, and data loss**.
In addition to protecting the network infrastructure itself, network security also protects the **traffic and assets** that move across or exist within the network.

It means protecting the network from **misuse, data theft, and unauthorized operations**.
It involves building a **secure infrastructure** of hardware, software, and users so that all can operate safely.
Network security works across several layers to **defend your network** from potential threats.

There are **three main types** of network security:

1. **Physical security** – Protecting the hardware itself.
2. **Technical security** – Protecting data and network systems.
3. **Administrative security** – Managing policies and access permissions.

How Does Network Security Work?

Digital transformation has made business operations faster, cheaper, and more productive — but it has also **increased cyber risks**.
From **Local Area Networks (LAN)** to **Wide Area Networks (WAN)** and **Internet of Things (IoT)** devices, every new connection creates a **potential vulnerability**.

The basics of network security include:

- Creating **strong passwords**
- **Logging out** completely from shared computers
- Controlling **access permissions**
- Using **encryption** to keep sensitive data safe
- Protecting **networks and software** from intrusions

Understanding Network Threats

To protect a network effectively, one must understand the **types of threats** that can harm it. Network threats can cause **data breaches**, **system crashes**, and other **serious consequences**.

Main ideas:

- A **network threat** targets computers or connected devices.
- It can **damage or disrupt** systems, applications, and services.
- Different threats have **different goals**.
- **Security policies** must identify weaknesses and protect against attacks.
- The **main goal** of most attacks is to **steal, modify, or block access** to valuable data.

Network Troubleshooting Basics

What is Network Troubleshooting?

Network troubleshooting is the process of **investigating, diagnosing, and fixing** network problems before they affect performance.
It helps administrators gain better visibility and **security insight** into all network components.
It can address **connection problems**, **security issues**, and **performance bottlenecks** to ensure smooth communication.

Why is Troubleshooting Important?

Even a **small failure** in one component can affect the entire network's performance and cause downtime.
Troubleshooting helps IT managers and network administrators understand issues **in real time** and improve **Quality of Service (QoS)**.
Early detection and repair reduce downtime and prevent **data loss**.
Monitoring tools also help manage network settings and track **key metrics** such as bandwidth and packet flow.

Examples of Troubleshooting Tools

Common tools include:

- ping, tracert, ipconfig, netstat, nslookup, pathping, route, and **PuTTY**.
  These tools help **diagnose and fix** network issues.

Typical problems include:

- **Video call delays**,
- **Slow application speeds**,
- **Interrupted VoIP calls**,
- **Unstable internet connection**, or
- **Incorrect IP settings**.

Main Steps of Network Troubleshooting

1. **Identify the problem and check physical connections**
   Gather all related information about the network and its devices.
   Check cables, routers, and hardware for issues such as **slow internet or connection drops**.
   Restart modems, routers, and computers to fix simple errors.

2. **Track and fix IP conflicts**
   Use the command **ipconfig** to check your computer's IP address.
   If it starts with **169.x.x.x**, the IP is invalid and needs to be reconfigured.

3. **Run a DNS check**
   Use **nslookup** to test if the DNS server is responding.
   If you get messages like "Request timed out" or "Server failed," then the DNS is the issue.

4. **Check for malware protection**
   Make sure your software and **firmware** are updated.
   Scan for malware that might slow down or block the connection.

5. **Check system logs**
   Analyze log files to discover system errors and performance problems.
   Logs give detailed information about every **program, device, or application**, helping identify the root cause.