Domain 4: Network Security

▼ Network Architecture

Concepts Covered:

- Networking
- Networking at a Glance
- Wi-Fi
- Identifying Threats
- Network Design
- Defense in Depth
- Zero Trust
- Network Access Control (NAC)
- Network Access Control (NAC) Deeper Dive
- Network Segmentation: Demilitarized Zone (DMZ)
- DMZ (Demilitarized Zone) Deeper Dive
- Segmentation for Embedded Systems and IoT
- Segmentation for Embedded Systems and IoT Deeper Dive
- Microsegmentation Characteristics
- Virtual Local Area Network (VLAN)
- Virtual Local Area Network (VLAN) Segmentation
- Virtual Private Network (VPN)

1. What is Networking?

- **Definition:** Networking is the process of connecting two or more computers or devices to share data, information, or resources.
- **Purpose:** Enables communication, resource sharing (e.g., printers, files), and collaboration between users and systems.
- **Components:** Involves hardware (routers, switches, firewalls), software (network operating systems), protocols (TCP/IP), and security (encryption, access controls).

Example: In an office, employees' computers are networked to share files and access a central printer.

2. Types of Networks

Local Area Network (LAN)

- **Definition:** A network covering a small geographic area, such as a single building or floor.
- **Use Case:** Connecting computers in an office, school, or home.
- **Example:** All computers in a school lab connected to share files and printers.

Wide Area Network (WAN)

- **Definition:** Connects networks over large distances, often between cities or countries.
- **Use Case:** Linking branch offices of a company in different cities.
- **Example:** The internet is the largest WAN.

3. Network Devices

Device	Function	Example Use
Hub	Connects multiple devices, broadcasts data to all ports. Not intelligent, can cause congestion.	Small home network
Switch	Connects devices, sends data only to intended recipient. More efficient than hubs.	Office switch connecting PCs and printers
Router	Directs data between networks, determines best path. Can be wired or wireless.	Home router connecting devices to the internet
Firewall	Filters network traffic based on rules, protects against unauthorized access.	Company firewall blocking suspicious traffic
Server	Provides resources/services to other computers (clients). Types: web, email, file, print, database.	File server storing shared documents
Endpoint	Devices at the ends of a network link (desktops, laptops, tablets, smartphones, servers).	Employee laptop accessing network resources

4. Networking Standards and Addresses

Ethernet (IEEE 802.3)

- **Definition:** Standard for wired network connections.
- **Function:** Ensures devices can communicate over the same cables.
- **Example:** Office computers connected via Ethernet cables.

MAC Address

- **Definition:** Unique hardware address assigned to each network device.
- **Format:** Example: 00-13-02-1F-58-F5.
- **Purpose:** Identifies devices at the data link layer.

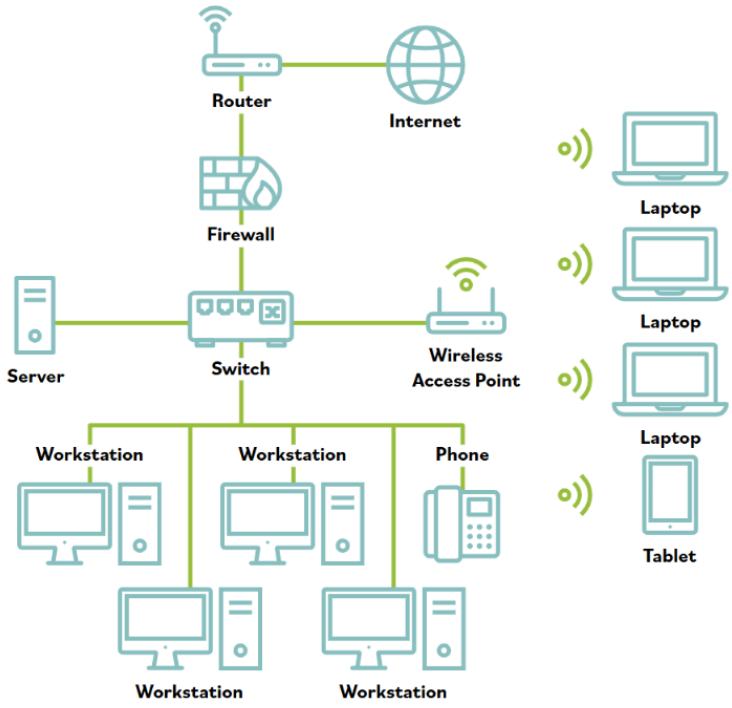
IP Address

- **Definition:** Logical address assigned to each device on a network.
- **Types:** IPv4 (e.g., 192.168.1.1), IPv6 (e.g., 2001:db8::ffff:0:1).
- **Purpose:** Identifies devices at the network layer, allows communication across networks.

5. Network Topologies

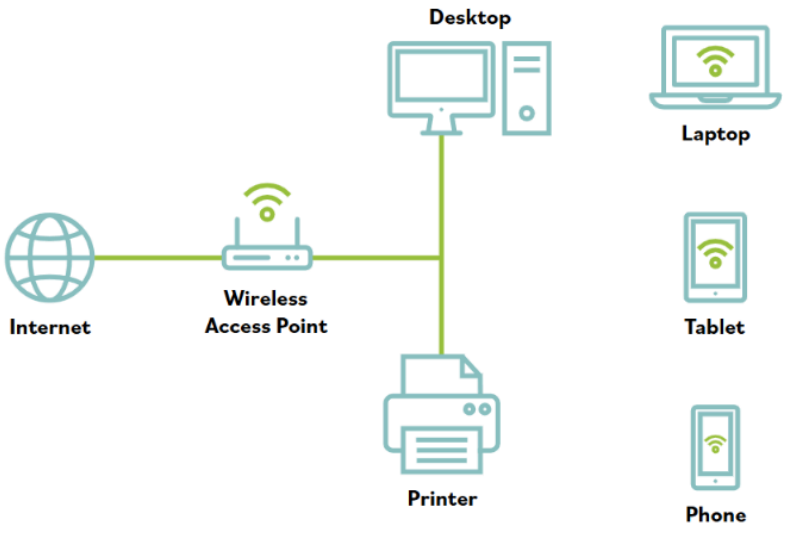
Small Business Network

- **Structure:** Devices connect to a switch, which connects to a firewall, then to the internet.
- **Security:** Firewall protects internal devices from external threats.



Home Network

- **Structure:** Router, firewall, and switch often combined in one device (wireless access point).
- **Simplicity:** Fewer devices, easier setup.



6. Wi-Fi (Wireless Networking)

- **Definition:** Wireless networking allows devices to connect without cables.
- **Advantages:** Easy deployment, mobility, cost-effective.
- **Range:** Suitable for homes and small offices; range extenders can increase coverage.
- **Security Risks:** Wireless signals can be intercepted from a distance, unlike wired networks which require physical access.

Example: Employees use laptops to connect to office Wi-Fi and move freely within the building.

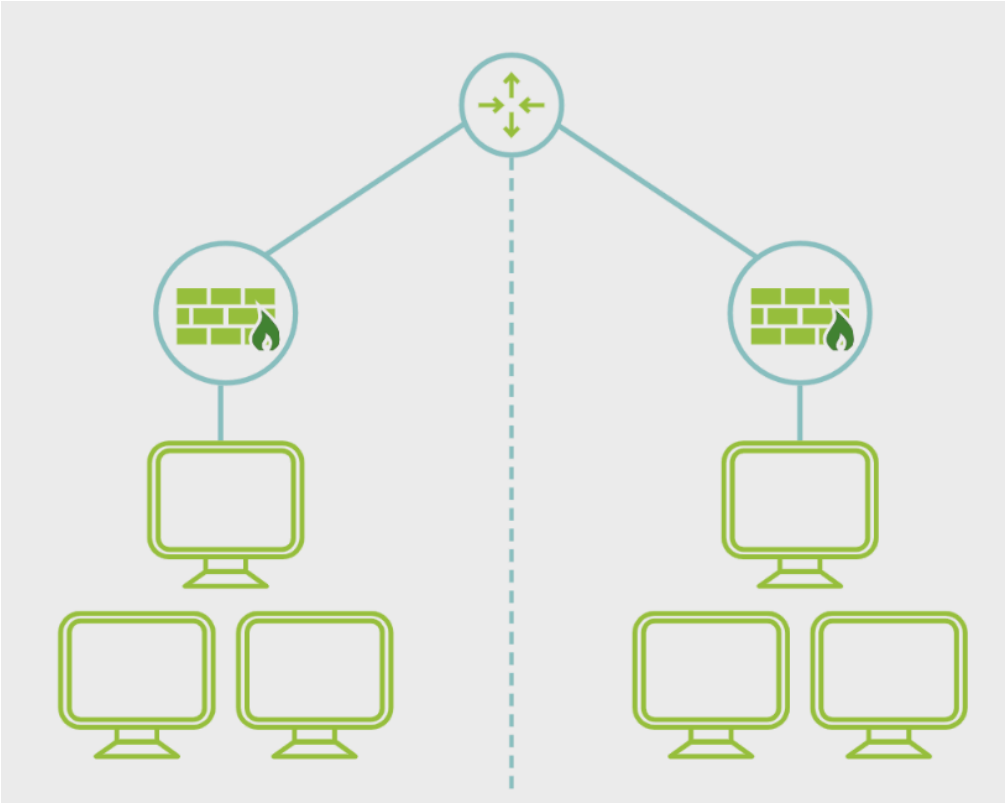
7. Identifying Threats

- **Intrusion Detection Systems (IDS):** Monitor network or host activity for suspicious behavior.
- **Example:** IDS detects "Advanced IP Scanner" software, which can be used for both legitimate network inventory and malicious reconnaissance.
- **Alert Analysis:** Details like process name, start time, and command line help determine if activity is legitimate or malicious.
- **Response:** Contact user to verify intent; legitimate tools can be misused by attackers.

8. Network Design Concepts

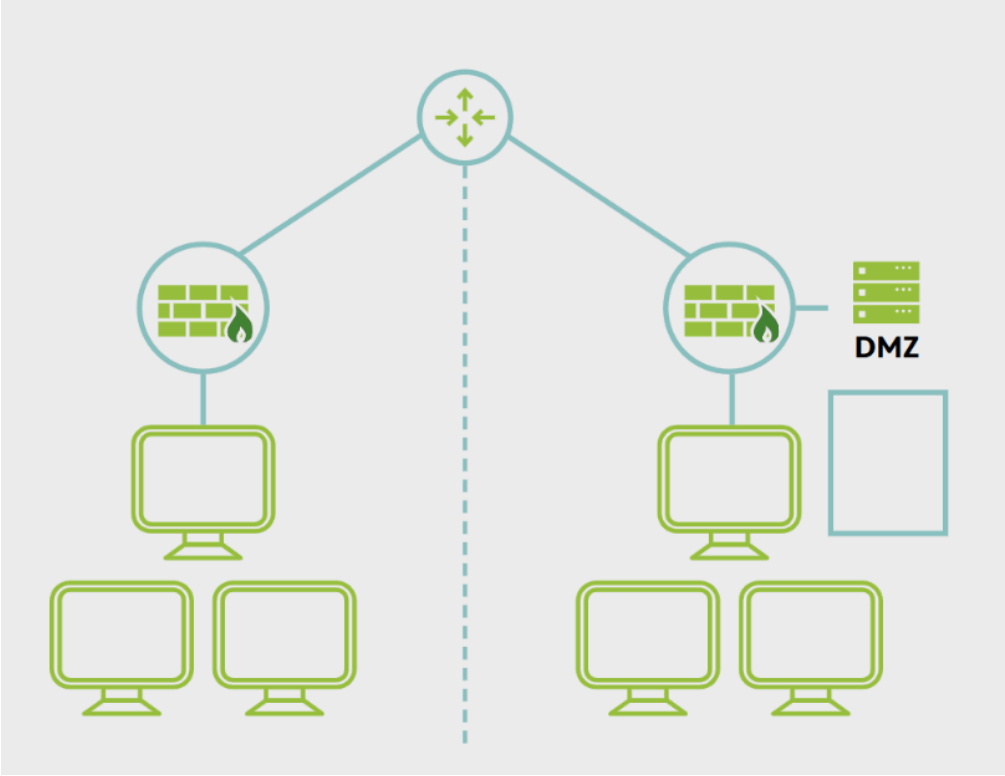
Network Segmentation

- **Definition:** Dividing a network into smaller parts to control traffic and enhance security.
- **Physical Segmentation:** Complete isolation from other networks.
- **Example:** Isolating sensitive research computers from the rest of the company network.



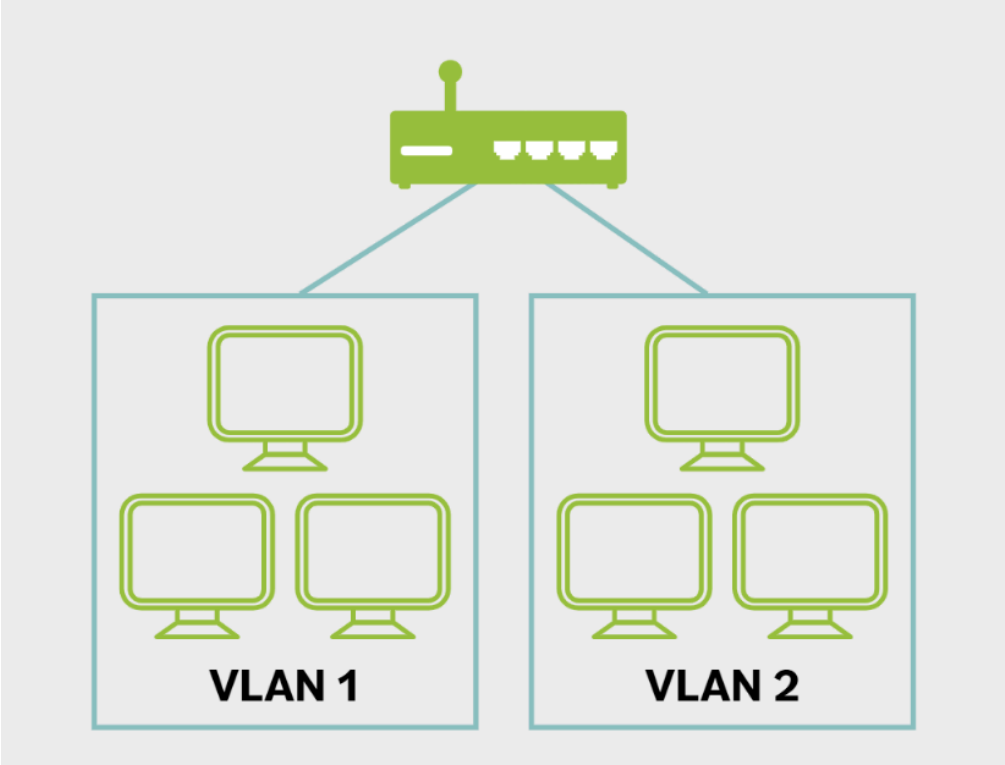
Demilitarized Zone (DMZ)

- **Definition:** A network area accessible to external users but isolated from the internal network.
- **Use:** Hosts public servers (web, email) while protecting internal resources.
- **Example:** A company's public website is in the DMZ, while internal databases are protected behind another firewall.



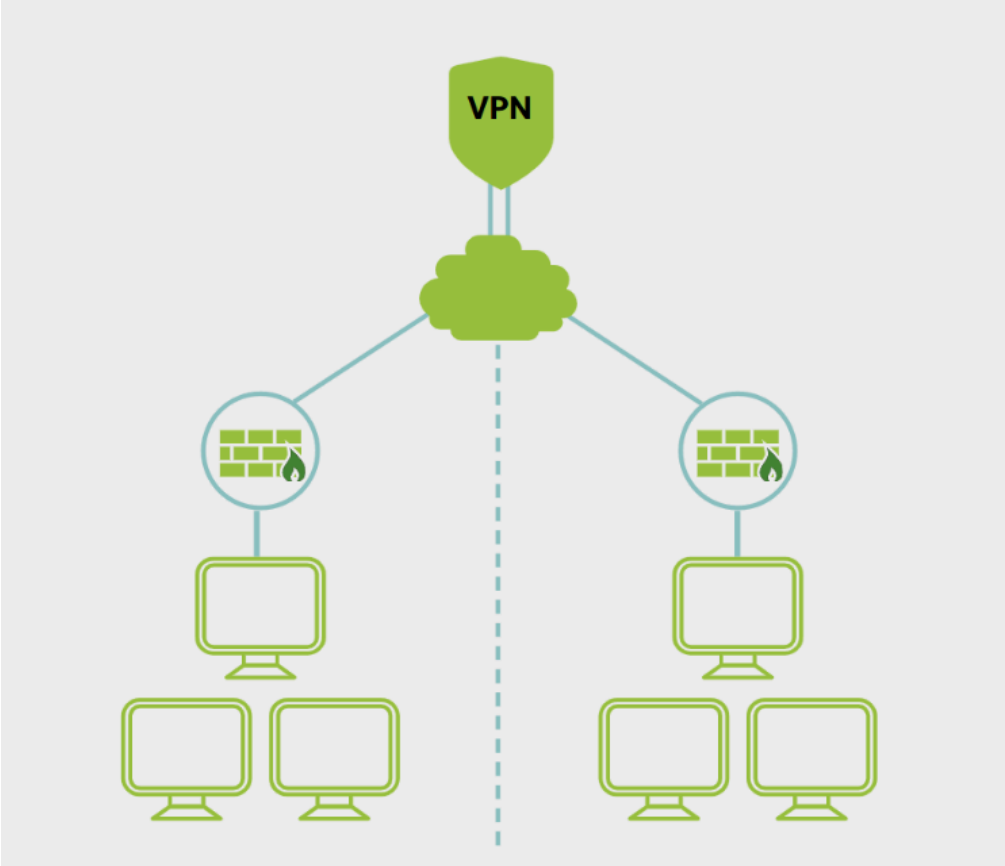
Virtual Local Area Network (VLAN)

- **Definition:** Logical segmentation of a network using switches, independent of physical layout.
- **Use:** Separate traffic for different departments or services.
- **Example:** HR and Finance computers are on separate VLANs, limiting access between them.



Virtual Private Network (VPN)

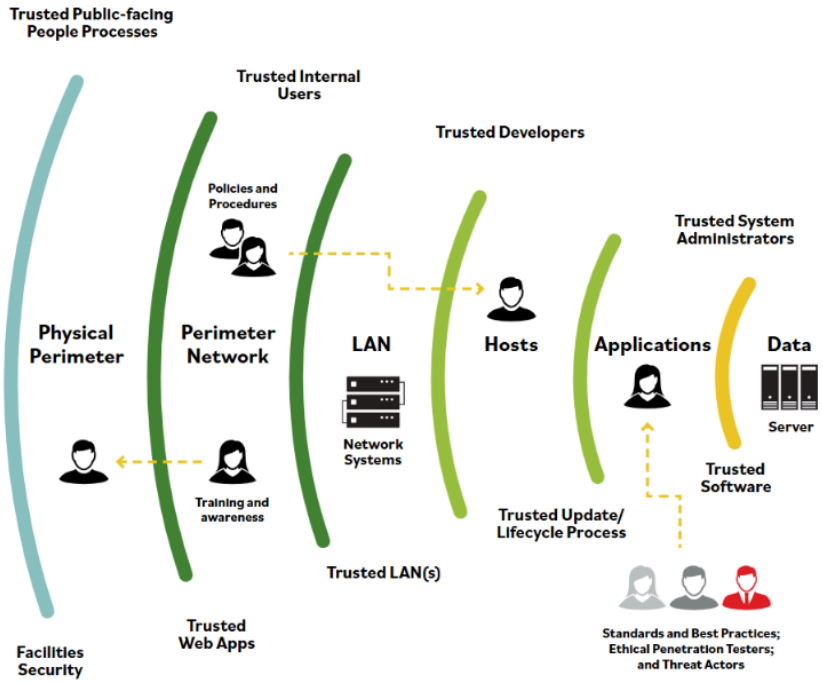
- **Definition:** Secure point-to-point connection over an untrusted network (like the internet).
- **Use:** Remote employees access company resources securely.
- **Example:** Employee connects to office network from home via VPN.



9. Defense in Depth

- **Concept:** Multiple layers of security controls (physical, technical, administrative) to protect assets.
- **Analogy:** Like a castle with walls, guards, and a moat protecting the crown jewels.
- **Layers:**
  - **Data:** Encryption, access management.
  - **Application:** Firewalls, monitoring.
  - **Host:** Antivirus, patch management.
  - **Internal Network:** IDS/IPS, internal firewalls.
  - **Perimeter:** Gateway firewalls, DMZs.
  - **Physical:** Locks, access control.
  - **Policies & Awareness:** Training, procedures.

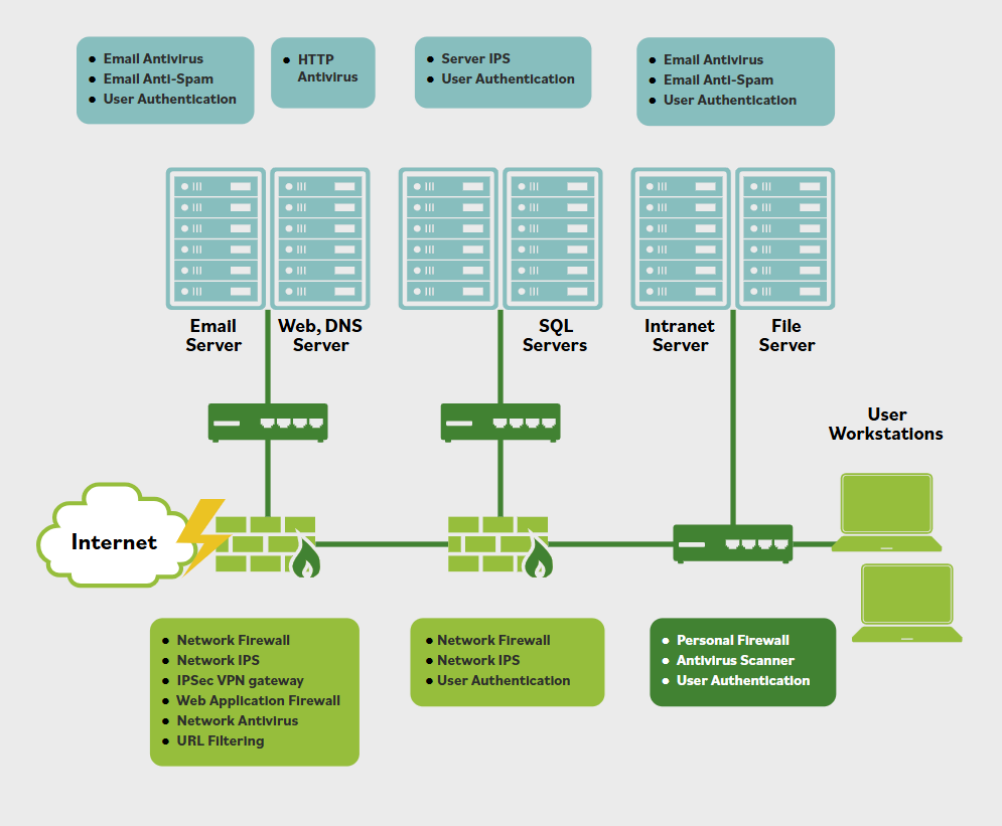
Example: Even if an attacker bypasses the firewall, they must overcome additional controls at each layer.



10. Zero Trust

- **Definition:** Security model that assumes no implicit trust; every access request is verified.
- **Features:** Microsegmentation, frequent reauthentication, focus on protecting assets directly.
- **Analogy:** At a concert, you show your ticket at multiple checkpoints, not just the entrance.
- **Implementation:** Firewalls and controls at every network segment, not just the perimeter.

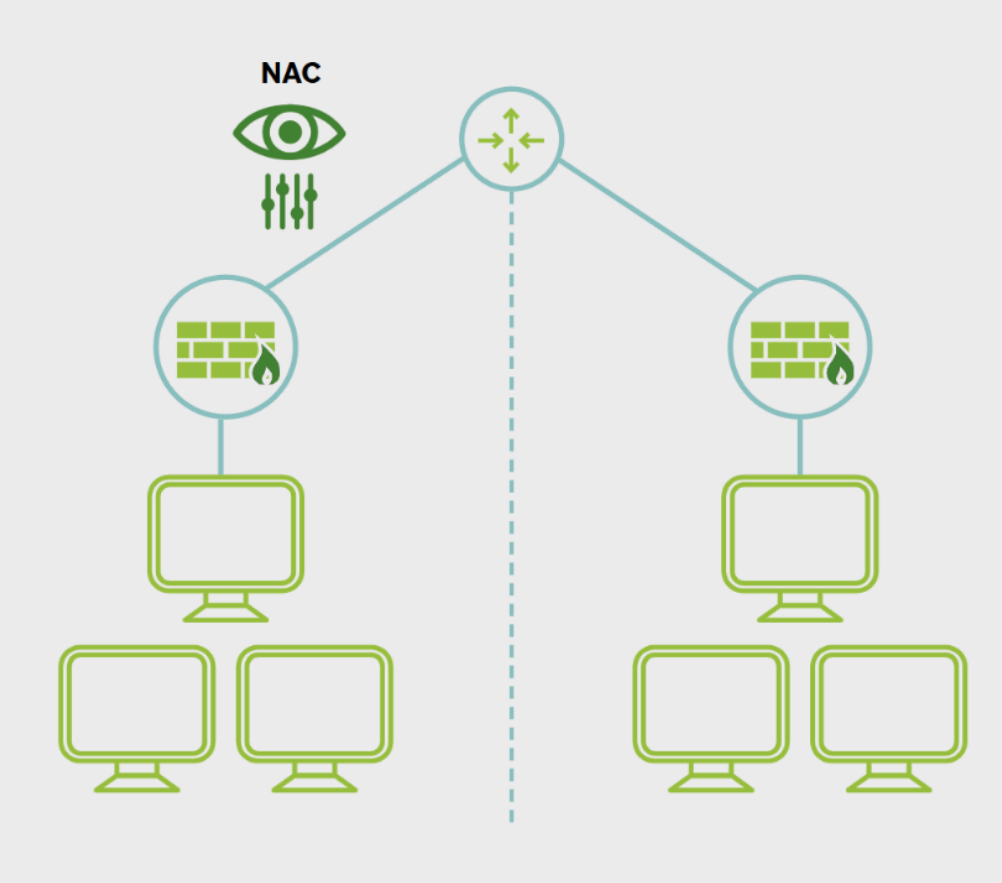
Example: Employee must authenticate to access each application or data set, even after logging into the network.



11. Network Access Control (NAC)

- **Purpose:** Controls which devices/users can access the network, enforcing security policies.
- **Scope:** Applies to internal users, guests, BYOD, and IoT devices.
- **Capabilities:** Identifies devices, isolates noncompliant ones, enforces onboarding and compliance.
- **Example Use Cases:**
  - Medical devices must meet security standards before connecting.
  - Guest devices are restricted to internet-only access.

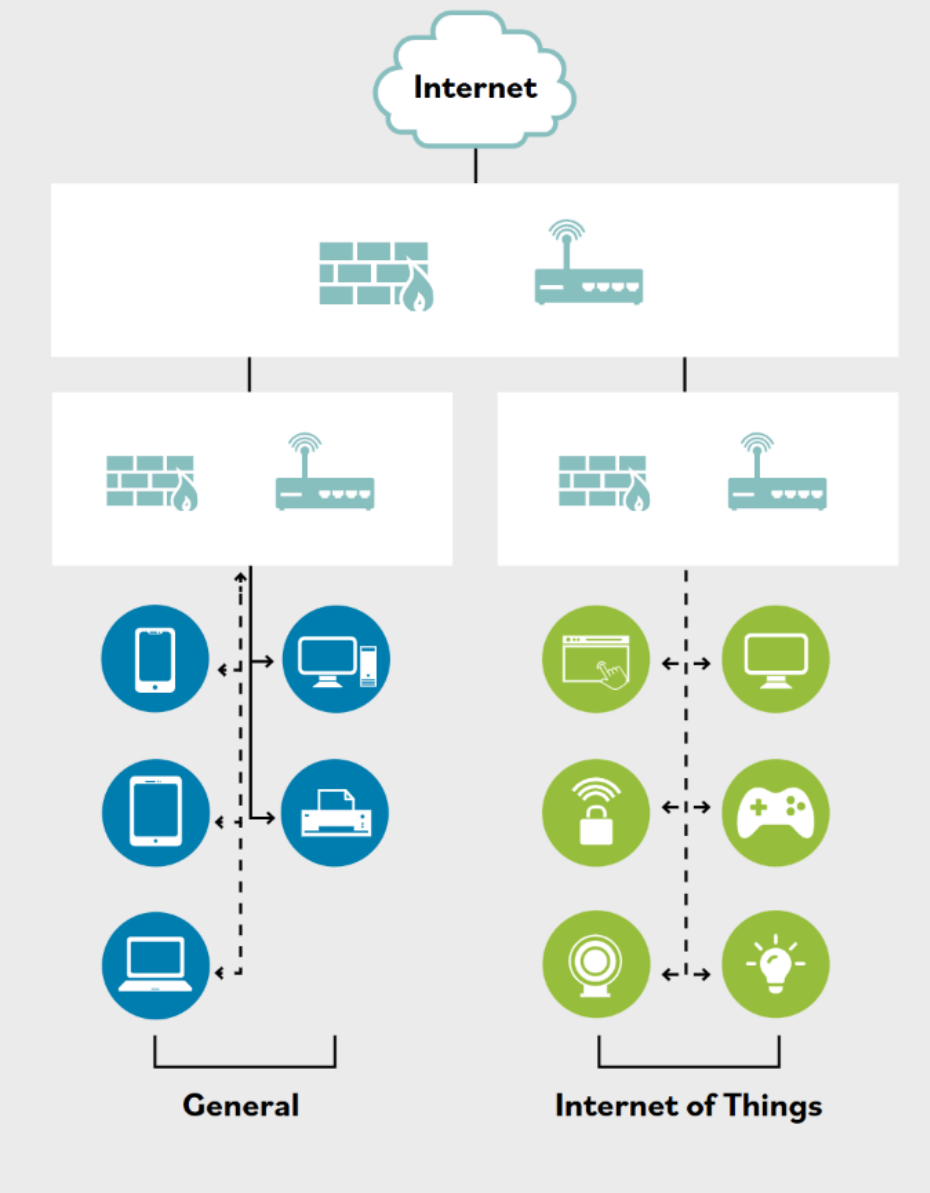
Example: Hotel Wi-Fi requires guests to accept terms and enter room details before granting access.



12. Network Segmentation for Embedded Systems and IoT

- **Embedded Systems:** Computers within larger devices (e.g., smart TVs, HVAC controls).
- **IoT Devices:** Network-enabled devices communicating over the internet (e.g., smart thermostats, cameras).
- **Risks:** Limited updates, multiple access routes, potential for remote exploitation.
- **Mitigation:** Segment these devices from critical business systems using VLANs, firewalls, or access controls.

Example: Smart lighting system is on a separate VLAN from company servers, preventing a breach from spreading.



13. Microsegmentation

- **Definition:** Highly granular network segmentation, often at the level of individual devices or users.
- **Benefits:** Enforces least privilege, limits lateral movement, ideal for cloud and shared environments.
- **Implementation:** Uses software-defined networking, security groups, or VPNs.
- **Example:** HR department's data is only accessible to HR staff, even within the same building.

14. VLANs in Practice

- **Purpose:** Limit broadcast traffic, segregate network segments, manage access.
- **Common Uses:**
  - Separate VoIP phones from computers.
  - Isolate data center traffic.

    - Restrict payroll access to authorized workstations.
- **Configuration:** Based on port, IP, MAC, or protocol.
- **Security Note:** VLANs improve organization but are not foolproof; attacks like VLAN hopping exist.

15. Virtual Private Network (VPN) in Practice

- **Definition:** Point-to-point connection, not always encrypted unless configured.
- **Use Cases:**
    - Remote employees access internal resources securely.
    - Secure site-to-site communication between offices.
- **Example:** A business partner connects to your network via VPN to collaborate on a project.

16. Additional Key Concepts

Intrusion Detection and Response

- **Host-based IDS (HIDS):** Monitors individual devices for suspicious activity.
- **Network-based IDS (NIDS):** Monitors network traffic for threats.
- **Alert Analysis:** Process details, user verification, and context are crucial for determining legitimacy.

Policy Enforcement and Onboarding

- **NAC Systems:** Enforce security policies, require device compliance before granting access.
- **Onboarding:** Devices must be identified and checked for compliance each time they connect.

Segmentation for Security

- **DMZs:** Used to host public-facing services while protecting internal networks.
- **Application Firewalls (WAF):** Filter and monitor HTTP traffic to and from web applications.

Embedded and IoT Device Security

- **Update Challenges:** Many devices lack regular updates, increasing vulnerability.
- **Segmentation:** Isolating these devices reduces risk to core business systems.

17. Summary Table: Key Networking Concepts

Concept	Definition/Function	Example/Use Case
LAN	Local network	Office computers
WAN	Wide area network	Internet
Switch	Directs traffic	Office network
Router	Connects networks	Home internet
Firewall	Filters traffic	Company security
VLAN	Logical segmentation	HR vs. Finance
VPN	Secure connection	Remote work
DMZ	Public-facing zone	Company website

Concept	Definition/Function	Example/Use Case
NAC	Access control	Guest Wi-Fi
Microsegmentation	Granular segmentation	Cloud security
IoT Segmentation	Isolate smart devices	Smart lighting

▼ Ports and Services Management

Concepts Covered:

- Transmission Control Protocol Internet Protocol (TCP/IP)
- Security of the Network
- Ports and Protocols (Applications/Services)
- Secure Ports
- SYN, SYN-ACK, ACK Handshake
- Intrusion Detection System (IDS)
- Preventing Threats

1. TCP/IP Overview

- **TCP/IP (Transmission Control Protocol/Internet Protocol)** is the most widely used networking protocol suite, developed in the early 1970s.
- It is a **protocol stack** (not a single protocol) consisting of many protocols, such as TCP, IP, UDP, ICMP, FTP, SMTP, DNS, etc.
- **Platform-independent and open standard:** Works on all major operating systems.
  - *Example:* Both Windows and Linux use TCP/IP for network communication.
- **Resource consumption and security:** While widely compatible, TCP/IP can use significant system resources and is vulnerable to attacks because it was designed for usability, not security.

TCP/IP Protocol Architecture Layers	
Application Layer	Defines the protocols for the transport layer.
Transport Layer	Permits data to move among devices.
Internet Layer	Creates/inserts packets.
Network Interface Layer	How data moves through the network.

2. TCP/IP Protocol Layers and Examples

Application Layer

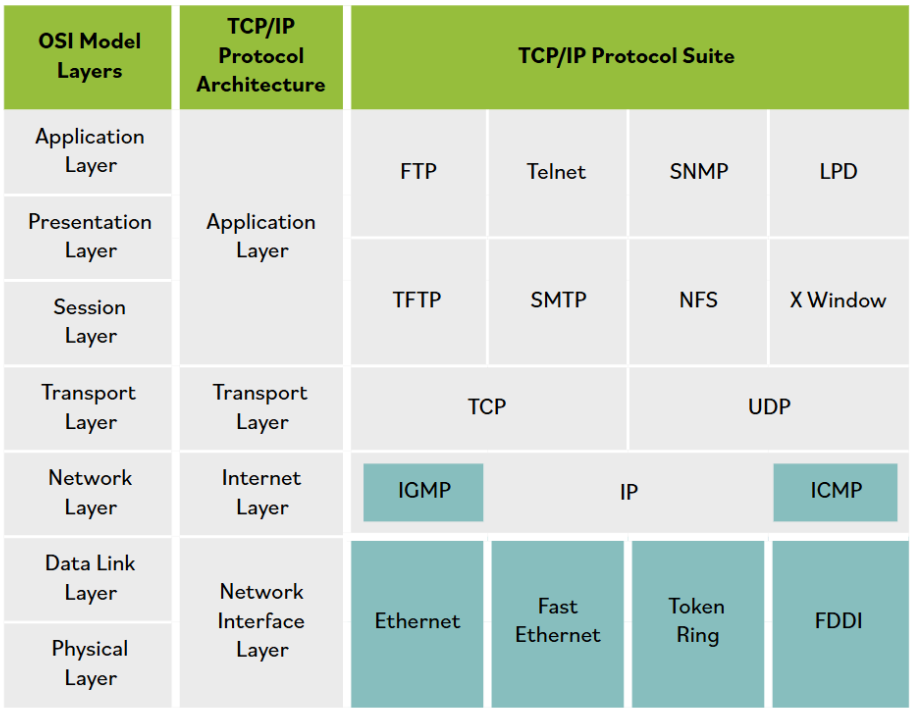
- **Protocols:** Telnet, FTP, SMTP, DNS.
  - *Example:* FTP (File Transfer Protocol) is used to transfer files between computers.

Transport Layer

- **TCP (Transmission Control Protocol):** Connection-oriented, reliable, full-duplex.
  - *Example:* Downloading a file via HTTP uses TCP to ensure all data arrives correctly.
- **UDP (User Datagram Protocol):** Connectionless, faster, but less reliable.
  - *Example:* Streaming a live video uses UDP for speed, accepting some data loss.

Internet Layer

- **ICMP (Internet Control Message Protocol):** Used for diagnostics and error reporting.
  - *Example:* The `ping` command uses ICMP to check if a remote server is reachable.



3. Network Security in TCP/IP

- **Vulnerabilities:** TCP/IP is susceptible to various attacks:
  - **DoS/DDoS attacks:** Overwhelm a system with traffic.
  - **Fragment and oversized packet attacks:** Exploit how data is split and reassembled.
  - **Spoofing and man-in-the-middle attacks:** Attackers impersonate or intercept communications.
- **Passive attacks:** Monitoring or "sniffing" network traffic to gather information.
  - *Example:* An attacker uses a packet sniffer to capture unencrypted passwords sent over the network.

4. Ports and Protocols

Physical Ports

- **Definition:** Hardware interfaces on devices (routers, switches, computers) for connecting cables.
  - *Example:* Ethernet port for a network cable.

Logical Ports

- **Definition:** Software-defined endpoints for network communication, identified by port numbers.
  - *Example:* Web servers use port 80 for HTTP and port 443 for HTTPS.

Port Ranges

Port Range	Description & Examples
Well-known (0-1023)	Core protocols (e.g., HTTP-80, HTTPS-443, DNS-53, SMTP-25)

Port Range	Description & Examples
Registered (1024-49151)	Vendor-specific or proprietary applications (e.g., RADIUS-1812, SQL Server-1433)
Dynamic/Private (49152-65535)	Temporary ports for client sessions

- **Multiple services per IP:** One IP can handle many services using different ports.
  - *Example:* A server can run a website (port 80), email (port 25), and FTP (port 21) simultaneously.

5. Insecure vs. Secure Protocols: Description and Risk

Insecure Protocol	Port	Description	Risk	Secure Alternative	Port	Example
FTP (File Transfer Protocol)	21	Used for transferring files between computers. Sends all data, including usernames and passwords, in plaintext.	Credentials and data can be easily intercepted by attackers using sniffing tools.	SFTP (SSH File Transfer Protocol)	22	Use SFTP to securely upload/download files to a server.
Telnet	23	Provides remote command-line access to systems. All communication is in plaintext.	Attackers can capture sensitive information (like passwords) and session data.	SSH (Secure Shell)	22	Use SSH for secure remote administration of servers.
SMTP (Simple Mail Transfer Protocol)	25	Standard protocol for sending emails. Default port transmits messages unencrypted.	Emails and credentials can be read or altered by attackers during transmission.	SMTP with TLS	587	Use SMTP with TLS (port 587) for secure email sending.
Time Protocol	37	Legacy protocol for time synchronization. Rarely used today.	Unauthenticated and can be spoofed, leading to incorrect time settings and potential log manipulation.	NTP (Network Time Protocol)	123	Use NTP for secure and accurate time sync across devices.
DNS (Domain Name Service)	53	Resolves domain names to IP addresses. Data is sent in plaintext.	Attackers can intercept or modify DNS queries (DNS spoofing or poisoning).	DNS over TLS (DoT)	853	Use DoT to encrypt DNS queries and prevent tampering.
HTTP (HyperText Transfer Protocol)	80	Foundation of web browsing. Transmits all data in plaintext.	Sensitive data (passwords, personal info) can be intercepted or modified in transit.	HTTPS (SSL/TLS)	443	Use HTTPS for secure web browsing and online transactions.

Insecure Protocol	Port	Description	Risk	Secure Alternative	Port	Example
IMAP (Internet Message Access Protocol)	143	Retrieves emails from a server. Default port sends data unencrypted.	Emails and login credentials are exposed to sniffing attacks.	IMAP with SSL/TLS	993	Use IMAP over SSL/TLS for secure email retrieval.
SNMP (Simple Network Management Protocol)	161/162	Manages and monitors network devices. Default versions send data in plaintext.	Network configuration and management info can be intercepted or altered.	SNMPv3 (with encryption)	161/162	Use SNMPv3 for secure device management and monitoring.
SMB (Server Message Block)	445	Used for sharing files and printers in Windows networks. Data is unencrypted.	Files and credentials can be stolen; protocol is often targeted by ransomware and worms.	NFS (Network File System, with encryption)	2049	Use NFS with encryption for secure file sharing (but still avoid across untrusted networks).
LDAP (Lightweight Directory Access Protocol)	389	Accesses and manages directory information (usernames, passwords, etc.). Data is unencrypted.	Directory data can be intercepted or manipulated, leading to unauthorized access.	LDAPS (LDAP over SSL/TLS)	636	Use LDAPS for secure directory services and authentication.

Key Points:

- **Plaintext protocols** are dangerous because attackers can easily capture and read the data.
- **Secure alternatives** use encryption (TLS/SSL or SSH) to protect data in transit.
- **Always prefer secure versions** (e.g., SFTP over FTP, SSH over Telnet, HTTPS over HTTP) to protect sensitive information.

6. TCP Three-Way Handshake (SYN, SYN-ACK, ACK)

- **Purpose:** Establishes a reliable TCP connection between client and server.
- **Steps:**
  1. **SYN:** Client requests connection (e.g., to web server on port 80/443).
  2. **SYN-ACK:** Server acknowledges and responds.
  3. **ACK:** Client confirms, connection established.
- *Example:* When you open a website, your browser and the server perform this handshake before data transfer begins.

7. Intrusion Detection System (IDS)

- **Definition:** Monitors and analyzes network or system activities for malicious actions or policy violations.
- **Role:** Part of a layered (defense-in-depth) security strategy; complements but does not replace firewalls.

Types of IDS

Type	Description	Example
HIDS	Host-based IDS: Monitors a single computer's logs and processes. Can detect file changes or malware on that host.	Detects if a specific server is compromised.
NIDS	Network-based IDS: Monitors network traffic for suspicious patterns. Can detect attacks across the network.	Detects a worm spreading through the network.

- **Response:** IDS can send alerts or alarms when suspicious activity is detected.
- **Limitation:** NIDS cannot see inside encrypted traffic; HIDS cannot detect attacks on other systems.

8. Security Information and Event Management (SIEM)

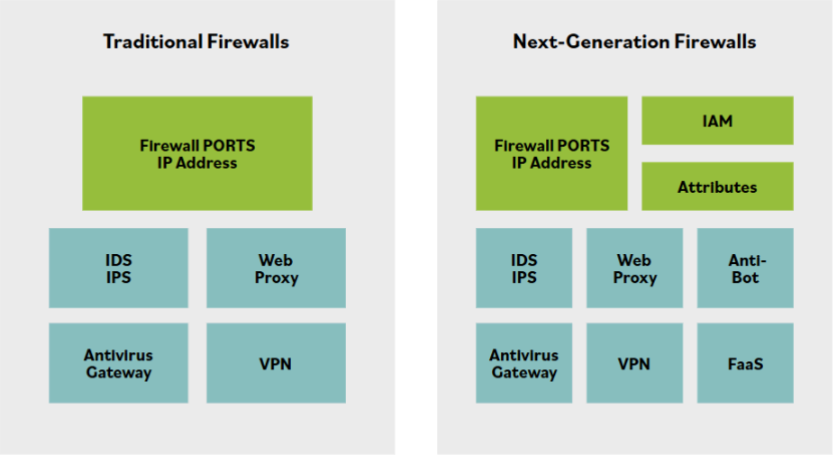
- **Definition:** Tools that collect and analyze security data from across an organization to identify threats and streamline security operations.
- **Function:** Aggregates logs from various sources (servers, firewalls, IDS) for centralized analysis.
  - *Example:* SIEM can correlate failed login attempts across multiple servers to detect a coordinated attack.

Summary:

- Use secure, encrypted protocols whenever possible.
- Understand the difference between physical and logical ports.
- IDS and SIEM are essential for modern network security monitoring and response.
- TCP/IP is foundational but must be secured with best practices and modern tools.

9. Preventing Threats & Security Controls

- **Keep systems and applications up to date:**
  - Apply vendor patches regularly to fix bugs and security flaws (patch management).
- **Remove or disable unneeded services and protocols:**
  - Only run necessary services to reduce attack surface.
  - *Example:* A web server running all services is vulnerable to attacks on any of those services.
- **Use intrusion detection and prevention systems (IDS/IPS):**
  - IDS monitors activity and sends alerts on suspicious behavior.
  - IPS is placed inline, actively blocking detected attacks.
  - Types include Network-based (NIDS/NIPS) and Host-based (HIDS/HIPS).
- **Use firewalls:**
  - Filter network traffic based on rules to enforce security policies.
  - Network-based firewalls protect entire networks; host-based firewalls protect individual systems.
  - Always place firewalls at internet gateways and consider internal network zoning.
  - Next-generation firewalls integrate proxy, IPS, and identity/access management, filtering traffic up to application layer (Layer 7).



- **Use up-to-date anti-malware and antivirus software:**
  - Essential for security best practices and compliance (e.g., PCI DSS).
  - Detect malware via signatures, pattern recognition, and machine learning.
  - Modern solutions cover viruses, rootkits, ransomware, spyware, and often include software firewalls and IDS/IPS.
- **Perform regular vulnerability and port scans:**
  - Identify missing patches, misconfigurations, new vulnerabilities, and ineffective policies.
  - Helps proactively remediate weaknesses before exploitation.

Summary:

- No single measure can prevent all threats; a layered security approach is essential.
- Combining patch management, service minimization, IDS/IPS, firewalls, anti-malware, and scanning provides robust defense.

▼ Secure Infrastructure Strategies

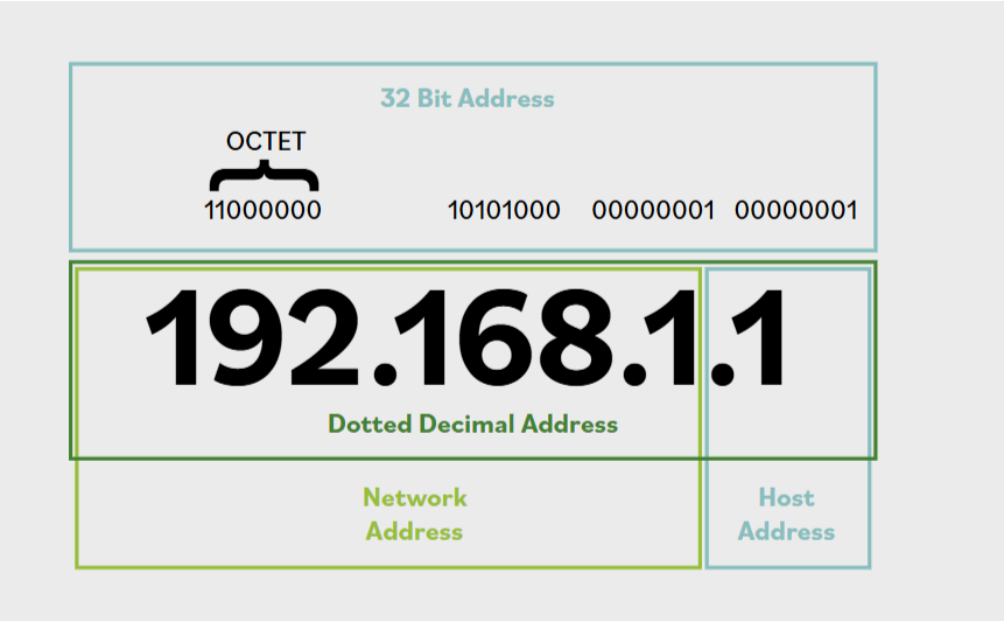
Concepts Covered:

- Internet Protocol (IPv4 and IPv6)
- Types of Threats
- Tools to Identify and Prevent Threats
- On-Premises Data Centers
- Deep Dive of On-Premises Data Centers
- Redundancy
- Example of Redundancy (Application of)

1. Internet Protocol (IP): IPv4 and IPv6

What is IP?

- **Internet Protocol (IP)** is a set of rules for addressing and routing data so it can travel across networks and arrive at the correct destination.



Versions of IP

- **IPv4 (Internet Protocol version 4):**
  - Uses a **32-bit address space** (about 4.3 billion addresses).
  - Example: `216.12.146.140`
  - Written as four octets (numbers 0–255) separated by dots.
    - **Octet Example:** In `192.168.1.10`, `192` is the first octet.
  - **Special Octet Values:**
    - `0` = network itself (not a device)
    - `255` = broadcast address (messages sent to all devices on the network)
  - **Address Structure:** Divided into **network** (assigned by organizations like ICANN) and **host** (identifies a device on the network).
  - **Subnetting:** To manage networks better, addresses are divided into subnets using a **subnet mask** (e.g., `255.255.255.0`).
  - **Address Shortage:** IPv4 addresses are limited; thus, **private address ranges** were created for internal use (not routable on the internet).
    - **Private Ranges:**
      - `10.0.0.0 – 10.255.255.254`
      - `172.16.0.0 – 172.31.255.254`
      - `192.168.0.0 – 192.168.255.254`
    - Example: Many homes use `192.168.1.x` for their Wi-Fi network.

- **Loopback Address:** `127.0.0.1` (used for self-diagnosis; pings the local machine).

- **IPv6 (Internet Protocol version 6):**
  - Uses a **128-bit address space** (virtually unlimited addresses).
  - Example: `2001:0db8:0000:0000:0000:ffff:0000:0001`
  - Written as eight groups of four hexadecimal digits, separated by colons.
    - Can be shortened: `2001:db8::ffff:0:1`
  - **Improvements over IPv4:**
    - **Larger address space:** No risk of running out of addresses.
    - **Security:** IPsec is mandatory, ensuring data integrity and confidentiality.
    - **Quality of Service (QoS):** Better management of network bandwidth.
  - **Special Addresses:**
    - `::1` = loopback (like `127.0.0.1` in IPv4)
    - `fc00::` to `fdff:ffff:...` = internal use (not routable)
    - `2001:db8::` = documentation/examples

2. Types of Cyber Threats

Common Threat Types

- **Spoofing:**
  - Pretending to be someone/something else to gain access.
  - Can spoof IPs, MAC addresses, usernames, etc.
  - Example: Sending an email that appears to come from your bank.
- **Phishing:**
  - Tricking users into visiting malicious websites via fake emails/links.
  - Example: An email that looks like it's from PayPal but leads to a fake site.
- **DoS/DDoS (Denial of Service/Distributed Denial of Service):**
  - Overloading a system to prevent legitimate use.
  - **DDoS** uses many computers to attack at once.
  - Example: Flooding a website with traffic so it crashes.
- **Virus:**
  - Malicious code that replicates itself and spreads, often requiring user action (e.g., opening an infected file).
  - Example: A Word document with a malicious macro.
- **Worm:**
  - Like a virus, but spreads automatically without user action.
  - Example: The "ILOVEYOU" worm spread via email attachments.
- **Trojan:**

- Malicious software disguised as something harmless.
- Example: A free game that secretly installs ransomware.

- **On-path Attack (Man-in-the-Middle):**
  - Attacker intercepts/modifies communication between two parties.
  - Example: Intercepting login credentials between a user and a website.
- **Side-channel Attack:**
  - Gathers information by observing device behavior (e.g., power usage, timing).
  - Example: Guessing encryption keys by measuring how long operations take.
- **Advanced Persistent Threat (APT):**
  - Long-term, sophisticated attacks by organized groups.
  - Example: Nation-state hackers targeting government agencies.
- **Insider Threat:**
  - Threat from trusted individuals (employees), intentional or accidental.
  - Example: An employee leaking confidential data.
- **Malware:**
  - Any software designed to harm, exploit, or otherwise compromise a system.
  - Example: Spyware, adware, ransomware.
- **Ransomware:**
  - Malware that encrypts files and demands payment to unlock them.
  - Example: WannaCry ransomware attack.

3. Tools to Identify and Prevent Threats

- **Anti-malware:** Detects and removes malicious software.
- **Firewalls:** Filters network traffic to block unauthorized access.
- **Intrusion Protection Systems (IPS):** Monitors and blocks suspicious activity.
- **SIEM (Security Information and Event Management):** Collects and analyzes log data for signs of threats.
- **Network Monitoring:** Observes network traffic for anomalies.
- **Endpoint Monitoring:** Watches activity on individual computers.

4. On-Premises Data Centers

What is an On-Premises Data Center?

- A data center owned and operated by the organization, located on its property.

Key Components and Considerations

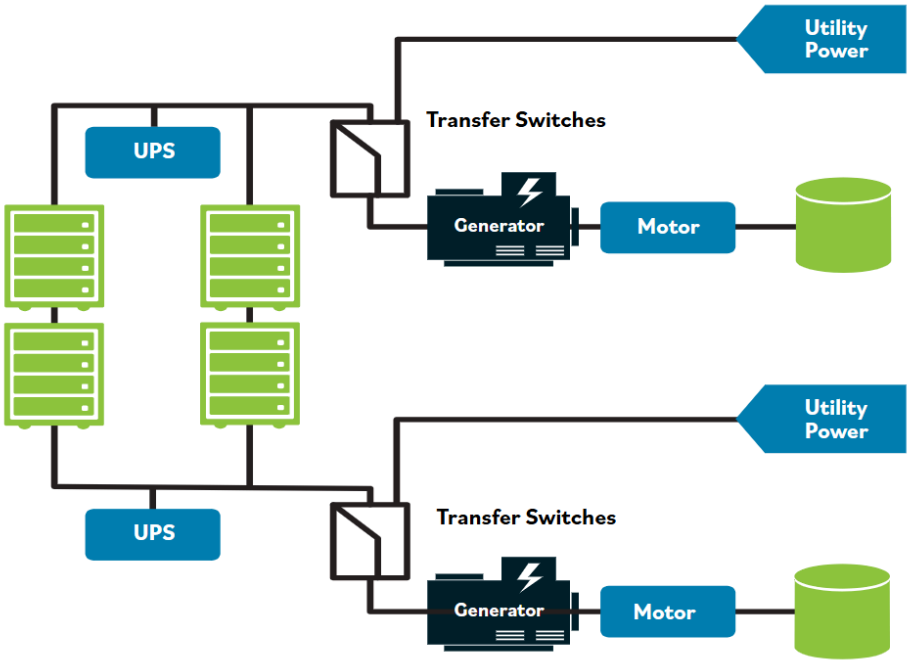
1. **Data Center/Closets:**
   - Physical security for wiring, servers, ISP equipment, switches.
   - Prevents intentional/unintentional damage.

2. **HVAC/Environmental Controls:**
    - Maintains proper temperature (18°–27°C/64°–81°F).
    - Uses sensors at various rack positions.
    - Controls dust, fumes, water/gas leaks, and sewer overflow.
    - Example: Cooling systems prevent server overheating and shutdowns.
3. **Power:**
    - Requires reliable, consistent power.
    - Uses backup generators and battery backups (UPS) for outages.
    - Example: Hospital data centers may have multiple power sources.
4. **Fire Suppression:**
    - Uses gas-based systems (less damaging to electronics) or dry-pipe water systems (water released only when fire detected).
    - Example: Sprinklers in a data center are carefully controlled to avoid water damage.

5. Redundancy

What is Redundancy?

- Having duplicate systems/components to ensure continued operation if one fails.



Applications of Redundancy

- **Power:** Two power supplies, multiple generators, different fuel types.
- **Data:** Multiple backups stored in different locations.

- **Network:** Multiple internet connections from different providers.
- **Example:** Hospitals may be connected to two separate power grids.

Summary Table

Concept	Explanation/Example
IPv4	32-bit, limited addresses, uses private ranges (e.g., 192.168.x.x)
IPv6	128-bit, virtually unlimited, improved security (IPsec), uses hexadecimal notation
Spoofing	Fake identity to gain access (e.g., fake email sender)
Phishing	Trick users into visiting malicious sites (e.g., fake bank emails)
DoS/DDoS	Overwhelm systems to block access (e.g., website crash)
Virus/Worm/Trojan	Malicious code—virus needs user, worm spreads itself, Trojan disguised as safe
On-path Attack	Intercepting communication (e.g., stealing login info)
Side-channel	Gaining info via device behavior (e.g., timing attacks)
APT	Long-term, sophisticated attacks (e.g., state-sponsored hacking)
Insider Threat	Threat from trusted individuals (e.g., employee leaks data)
Malware/Ransomware	Software to harm or extort (e.g., encrypts files for ransom)
Security Tools	Firewalls, anti-malware, IPS, SIEM, monitoring
Data Center Needs	Physical security, HVAC, power, fire suppression
Redundancy	Backup systems for power, data, network (e.g., multiple generators)

In summary:

IP addressing is critical for network communication, with IPv4 and IPv6 as main standards. Cyber threats are varied and require multiple layers of defense, both technical (firewalls, anti-malware) and physical (secure data centers with redundancy). Redundancy ensures that systems remain operational even if one component fails.

▼ Cloud Computing Infrastructure

Concepts Covered:

- Networking Models
- Open Systems Interconnection (OSI) Model
- Memorandum of Understanding (MOU) and Memorandum of Agreement (MOA)
- Cloud Computing
- Cloud Redundancy
- Cloud Characteristics
- Service Models
- Deployment Models
- Managed Service Provider (MSP)
- Service-Level Agreement (SLA)

Networking Models

Purpose and Importance

- **Networking models** provide frameworks and standards for connecting various hardware and software systems.
- **Goals:** Share information, coordinate activities, and accomplish joint/shared tasks.

Components of Networks

- Networks are built from the integration of:
  - **Communication devices** (e.g., routers, switches)
  - **Storage devices** (e.g., hard drives, cloud storage)
  - **Processing devices** (e.g., CPUs, servers)
  - **Security devices** (e.g., firewalls)
  - **Input/Output devices** (e.g., keyboards, monitors)
  - **Operating systems, software, services, data, and people**

Translating Security Needs

- **Premise:** All communication aims to exchange information and ideas to complete work.
- **Network and Security Goals:**
  - **Reliable, managed communications:** Ensure consistent and secure data exchange.
  - **Layered isolation:** Functions are separated into layers to enhance security and manageability.
  - **Packet-based communication:** Data is sent in packets for efficiency.
  - **Standardized routing and addressing:** Ensures data reaches the correct destination.
  - **Layer extensibility:** Higher layers can add more features.
  - **Vendor-agnostic, scalable, resilient:** Works across different manufacturers, can grow, and withstand failures.

Network Layers

Upper Layer (Host/Application Layer)

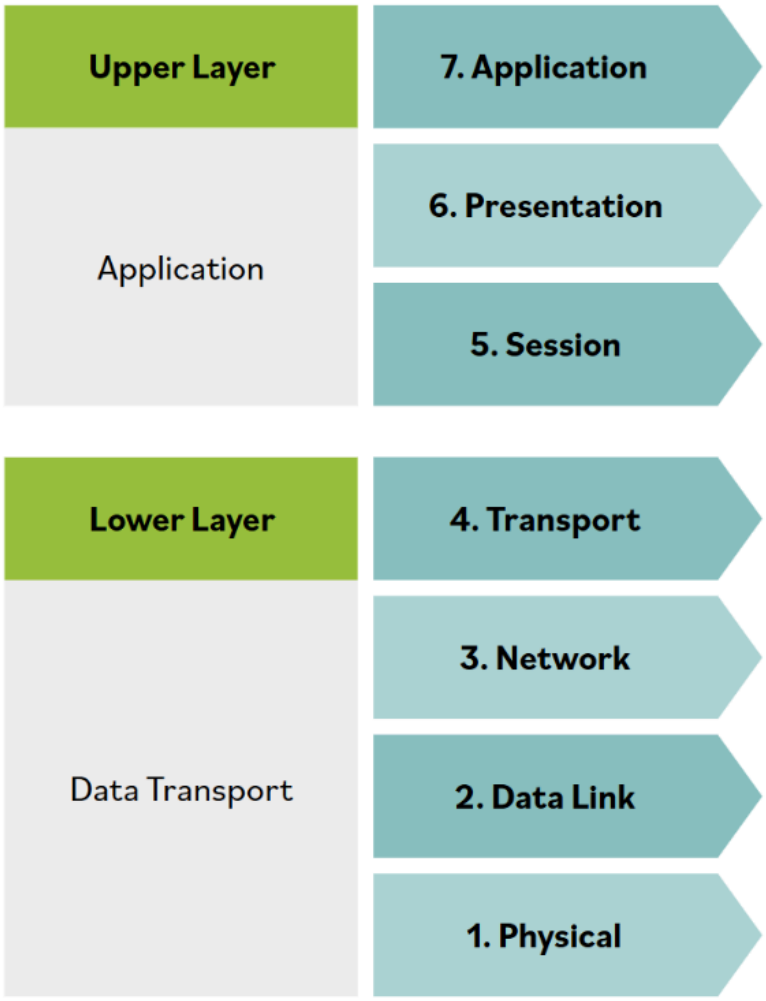
- **Responsibilities:**
  - Manages connection integrity and session control.
  - Handles session establishment, maintenance, and termination.
  - Transforms application data into a universal format.
  - Ensures remote partners are available.
- **Example:** Email applications use this layer to check if the recipient’s server is reachable.

Lower Layer (Media/Transport Layer)

- **Responsibilities:**
  - Receives bits from the physical medium and forms them into frames (structured data units).
  - Frames are like buckets holding water (bits); similar-sized buckets make transport predictable.

- Adds routing information to frames, creating packets.

- **Example:** Ethernet frames are used to transmit data over LAN cables.



Open Systems Interconnection (OSI) Model

Overview

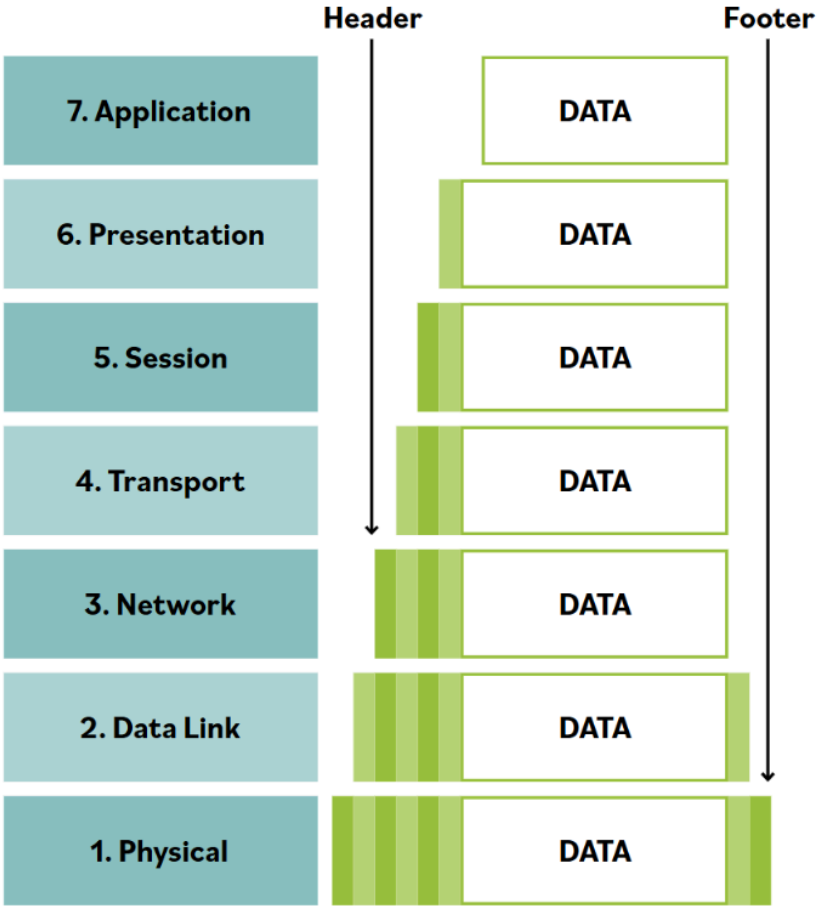
- **Purpose:** Standardize communication for interconnected computer systems.
- **Nature:** Theoretical model for ideal protocol operation.
- **Structure:** Divides networking tasks into seven layers, each with specific responsibilities.

The Seven OSI Layers

1. **Physical (Layer 1):** Transmits raw bits over a physical medium (e.g., cables, radio).
   - *Example:* Ethernet cables, Wi-Fi signals.
2. **Data Link (Layer 2):** Handles error detection/correction and frame formatting.

- *Example:* Switches, MAC addresses.

3. **Network (Layer 3):** Manages logical addressing and routing.
   - *Example:* Routers, IP addresses.
4. **Transport (Layer 4):** Provides reliable data transfer (e.g., error recovery, flow control).
   - *Example:* TCP, UDP protocols.
5. **Session (Layer 5):** Manages sessions (connections) between applications.
   - *Example:* NetBIOS, RPC.
6. **Presentation (Layer 6):** Translates, encrypts, or compresses data.
   - *Example:* JPEG, PNG file formats.
7. **Application (Layer 7):** Interfaces with end-user applications.
   - *Example:* Web browsers, email clients.



Layer Communication

- Each layer communicates with the one directly above and below it.
- *Example:* Layer 3 (Network) interacts with Layer 2 (Data Link) and Layer 4 (Transport).

Encapsulation and De-encapsulation

- **Encapsulation:** Each layer adds its own header (and sometimes footer) as data moves down the stack.
  - *Example:* Sending an email, the message is wrapped in headers for transport, network, and data link layers.
- **De-encapsulation:** As data moves up, each layer removes its header/footer to interpret the data.
  - *Example:* Receiving an email, the device strips off each layer's header/footer to reconstruct the message.

Memorandum of Understanding (MOU) and Memorandum of Agreement (MOA)

Purpose

- Agreements between organizations to share resources during emergencies for business continuity (BC) and disaster recovery (DR).
- Often done between competitors for industry-wide resilience.

Example

- **Hospital A and Hospital B:** If one faces a disaster, the other provides temporary facilities and resources.

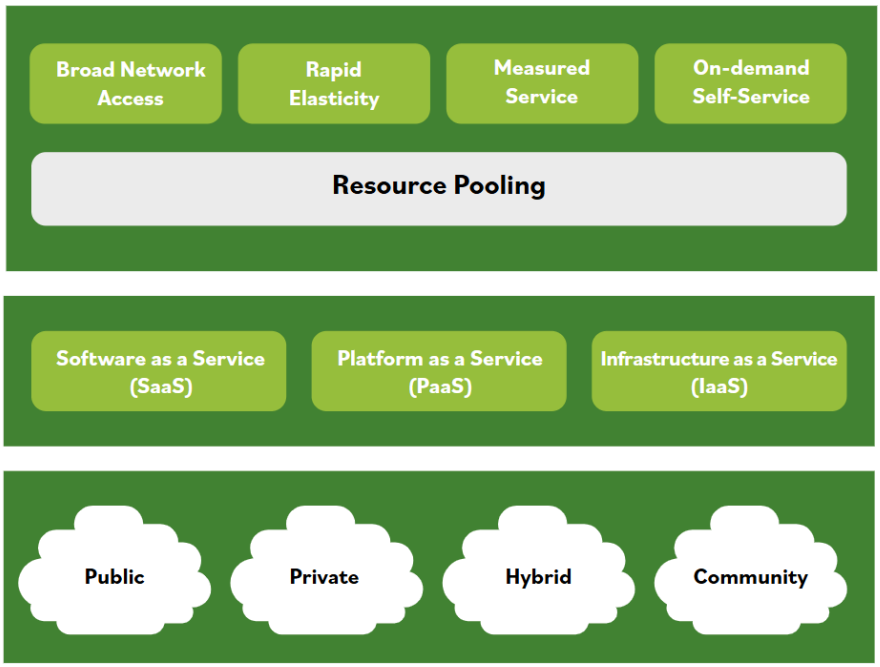
Types of Agreements

- **JOA (Joint Operating Agreement)**
- **MOU (Memorandum of Understanding)**
- **MOA (Memorandum of Agreement)**
- Sometimes required by regulations or industry guidelines.

Difference from SLA

- **MOU/MOA:** Focus on what can be done with systems/information.
- **SLA (Service-Level Agreement):** Specifies detailed, measurable service parameters (e.g., response times, uptime).

Cloud Computing



Definition

- **Cloud computing:** Internet-based access to shared computing resources (e.g., servers, storage, applications).
- **NIST Definition:** On-demand network access to a shared pool of configurable resources, quickly provisioned/released with minimal management.

Analogy

- Like electricity: Available on demand, pay for what you use, no need to manage the infrastructure yourself.

Benefits

- **Scalable and elastic:** Easily adjust resources as needed.
- **Cost-effective:** Pay-per-use, reduced ownership and maintenance costs.
- **Green IT:** Lower energy and cooling costs.
- **Quick deployment:** Rapidly launch new services without installing physical hardware.

Cloud Redundancy

- Cloud providers use multiple availability zones for high availability and disaster recovery.
- Organizations can pool resources and shift operations if one zone fails.

Cloud Service Models

Types

1. **Software as a Service (SaaS):**

- Provider hosts applications; users access via internet.
- *Example:* Google Workspace, Salesforce.

2. **Platform as a Service (PaaS):**
   - Provider offers a platform for app development/deployment.
   - *Example:* Microsoft Azure, Google App Engine.
3. **Infrastructure as a Service (IaaS):**
   - Provider offers virtualized computing resources.
   - *Example:* Amazon EC2, Microsoft Azure VMs.

Responsibility

- Varies by model: In SaaS, provider manages most; in IaaS, consumer manages more.

Cloud Deployment Models

Types

1. **Public Cloud:**
   - Open to anyone; resources shared among many users.
   - *Example:* Amazon AWS, Microsoft Azure public cloud.
2. **Private Cloud:**
   - Dedicated to one organization; can be on-premises or hosted.
   - *Example:* Company's internal cloud for sensitive data.
3. **Hybrid Cloud:**
   - Combination of public and private clouds.
   - *Example:* Sensitive data in private cloud, public cloud for less critical workloads.
   - **Benefits:** Control, flexibility, cost savings.
4. **Community Cloud:**
   - Shared by organizations with common interests.
   - *Example:* Cloud for universities in a region.

Managed Service Provider (MSP)

Definition

- An organization that manages IT assets/services for another company.
- **Common uses:** Outsourcing IT, network/security monitoring, help desk, payroll, incident response.

Examples

- **MDR (Managed Detection and Response):** Monitors security events.
- **Augmenting staff:** Temporary IT support for projects.

Service-Level Agreement (SLA)

Definition

- **SLA:** Contract between cloud provider and customer specifying service quality, availability, responsibilities, and remedies.
- **Purpose:** Set clear expectations and legal obligations.

Key Elements

- Infrastructure and security standards
- Disaster recovery processes
- Data location and ownership
- Audit rights and compliance
- Service availability and performance
- Data security, privacy, and access
- Data portability and exit strategy
- Problem resolution and change management

Summary Table

Concept	Definition/Role	Example/Key Point
Networking Models	Frameworks for interconnecting systems	OSI, TCP/IP models
OSI Model	7-layer model for standardizing network communication	Layer 3 = Network (routers, IP), Layer 2 = Data Link (switches)
Encapsulation	Wrapping data with headers/footers as it moves down layers	Sending an email
MOU/MOA	Agreements for shared resources in emergencies	Hospitals sharing facilities
SLA	Legal contract specifying service levels	Uptime guarantees, data ownership
Cloud Computing	On-demand, internet-based computing resources	AWS, Azure, Google Cloud
Service Models	SaaS, PaaS, IaaS (varying responsibility)	Gmail (SaaS), Azure (PaaS), AWS EC2 (IaaS)
Deployment Models	Public, Private, Hybrid, Community	Hybrid: Sensitive data private, rest public
MSP	Third-party IT management	Outsourced help desk, security monitoring