★ What is the Internet ?

The Internet is a global network of interconnected computers and networks.
Uses TCP/IP protocols and packet switching.
Runs on any communications substrate.

★ What is a Communication Network?

A communications network is a network of links and nodes arranged so that messages may be passed from one part of the network to another.

★ What is the Client – Server Architecture ?

Client server architecture is a computing model in which the server hosts,delivers, and manages most of the resources and services requested by the client.

Every computer or process in a network can act as a server or client in a client-server architecture.

A server is the one who provides requested services.
Clients are the ones who request services.

Client server architecture - example

- Mail servers
- File servers (Google Docs)
- Web servers

The three components are client server architecture,

- workstations

  Workstations are also called client computers.

- Servers

  Servers are defined as fast processing devices that act as centralized repositories of network files, programs, databases, and policies.

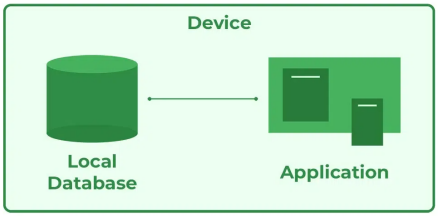
- networking devices

  Networking devices are a medium that connects workstations and servers in client server architecture.

Types of client server architecture

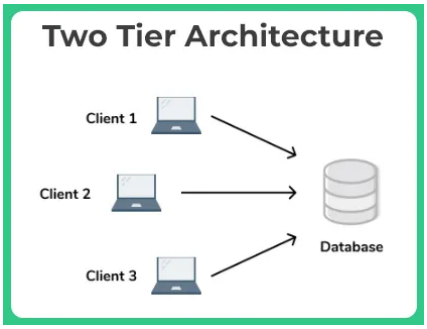
- 1-tier architecture

  1-tier architecture consists of several layers, such as presentation layer, business layer, and data layer, that are combined with the help of a unique software package.



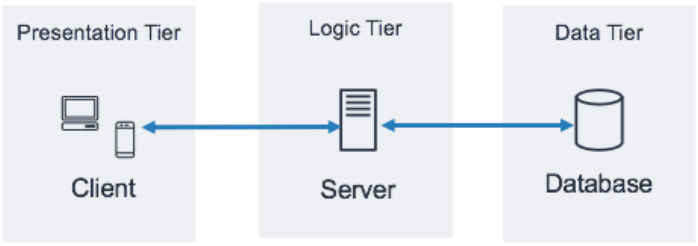
• 2-tier architecture

Front-end (client) communicates with Back-end (server). Simple but limited for large applications.



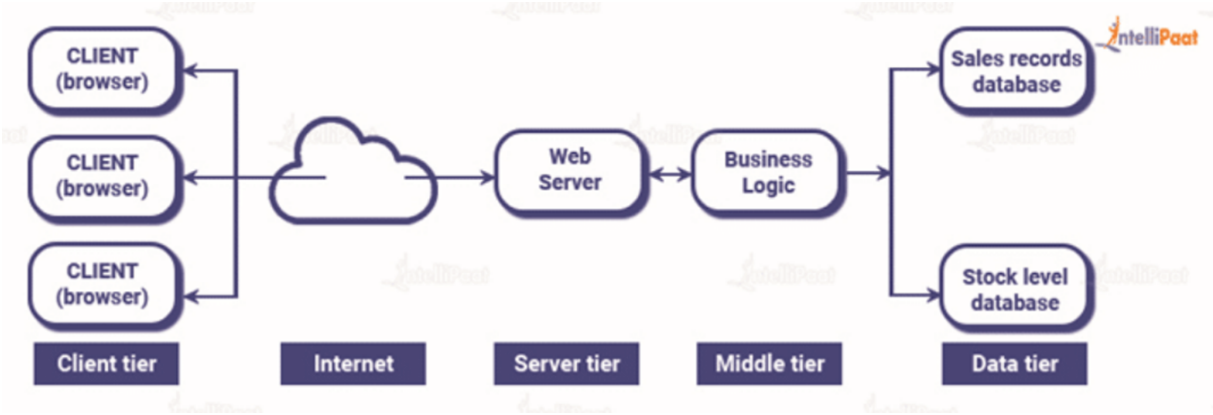
• 3-tier architecture

presentation layer - for user interaction (Front-end)
application layer - for processing and logic. (Middle layer)
database layer - for data storage. (Back-end)



• N-tier architecture (N-tier architecture is multilayered client-server)

This architecture has a provision for locating each function as an isolated layer that includes presentation, application processing, and management of data functionalities.



This short note making resources are,google search engine,chat gpt and lecture slides

WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

★ Difference between peer-to-peer network and client server architecture

Client server architecture	Peer-to-peer architecture
It has specific clients and servers.	There is no differentiation between clients and servers.
It has centralized data management.	It has its own data and applications.
The purpose is to share information.	Its main goal is to maintain connection among peers.
Data is provided only in response to a request.	In this network, peers have the authority to request as well as provide a service.
It is suitable for small as well as large networks.	It is suitable for less users, less than 10 devices.

★ Advantages and disadvantages of client-server architecture

Advantages of Client-Server Architecture:

1. Scalability: Easy to handle many clients as it grows.
2. Centralized Management: Easy to control and update everything from one place.
3. Resource Sharing: Efficient use of resources by centralizing them.
4. Enhanced Security: Better protection of sensitive data on the server.
5. Cost-Effectiveness: Saves money by using shared resources.

Disadvantages of Client-Server Architecture:

1. Single Point of Failure: If the server goes down, everyone loses access.
2. Network Dependency: Needs a stable and fast network connection.
3. High Initial Setup Cost: Setting up the server can be expensive.
4. Increased Complexity: Managing a server adds complexity.
5. Performance Bottlenecks: Server limitations can slow down clients.
6. Limited Offline Access: Some functions may not work without the server.

★ What is the Internet ?

The Internet is a global network of interconnected computers and networks.

The internet is a public network accessible to anyone.

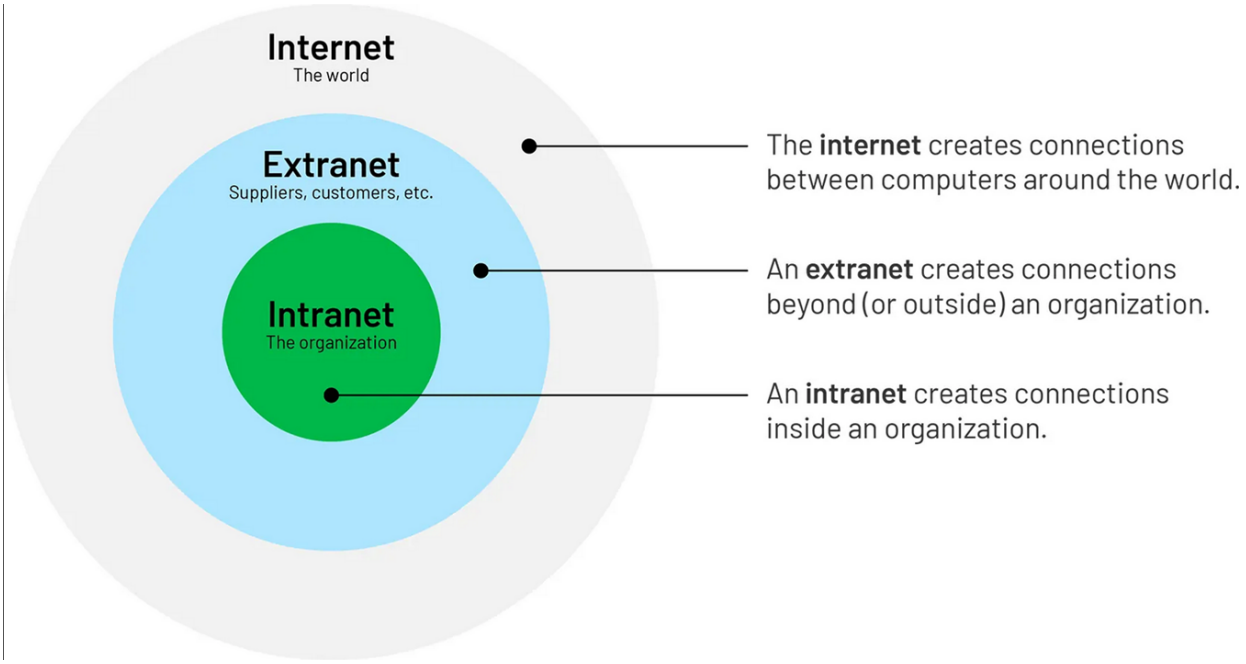
★ What is the Intranet ?

intranets are private networks accessible only to authorized users within an organization.

★ What is the extranet ?

Extranets are private networks that allow external parties to access certain parts of an organization's intranet.

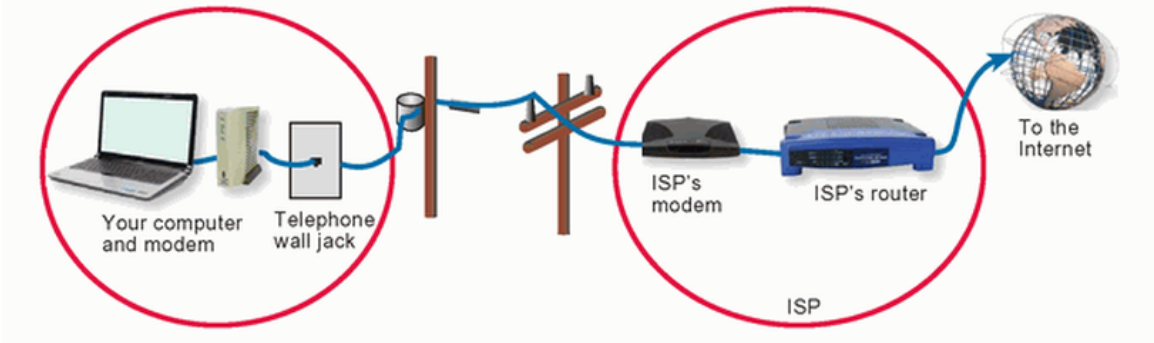
This short note making resources are,google search engine,chat gpt and lecture slides



★ Types of Internet connection

- **Dial-UP**

Connection through modem and a public switched telephone network(PSTN).
Encoding & Decoding of analog signals is done by modem.



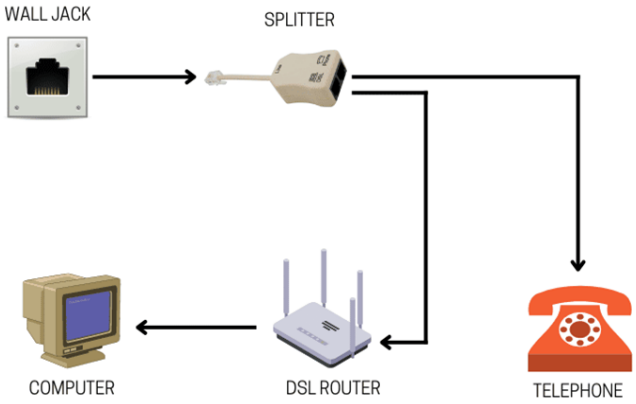
Advantages
- Low Cost
- Availability

Disadvantages
- Low Speed
- Requires phone line
- Route busy

• **Digital Subscriber Line(DSL)**

High-speed data service that works over copper telephone lines.

DSL is considered a "symmetrical" technology (same download and upload speeds)



Advantages

Downloads are faster than uploads
DSL simultaneously keeps your Internet connection and phone lines open
DSL uses the existing wiring infrastructure of your telephone line

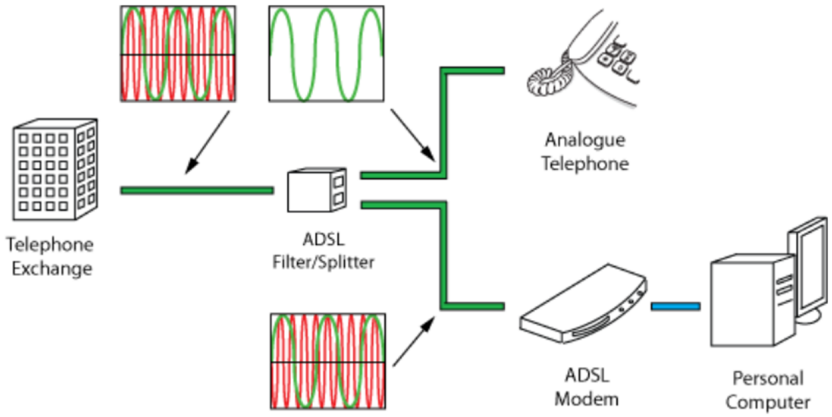
Disadvantages

Large amount of uploading is not possible
DSL is limited to a certain perimeter
Compared to dial up ,it is expensive

• **ADSL**

Technology used for delivering high-speed internet access over traditional copper telephone lines

specific type of DSL technology that is designed to provide faster download speeds than upload speeds.



This short note making resources are,google search engine,chat gpt and lecture slides

WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

Advantages

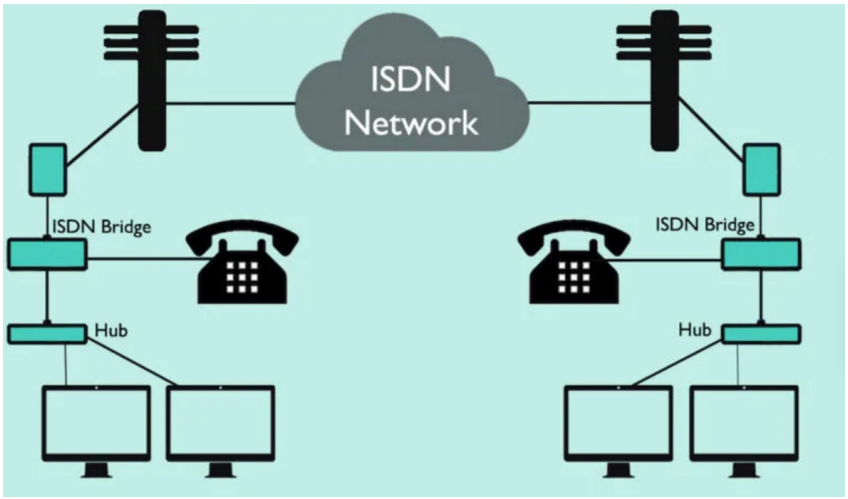
Very fast download speeds
Transfers data digitally
ADSL connections are always on – no connection time.

Disadvantages

Not available to everyone, need ADSL coverage in your area.
Hardware costs are higher

- **ISDN (Integrated Services Digital Network)**

It put together speech and information on the same line



Advantages

Multiple digital channels
Speedy
Can be used for other activities Eg. Video conferencing

Disadvantages

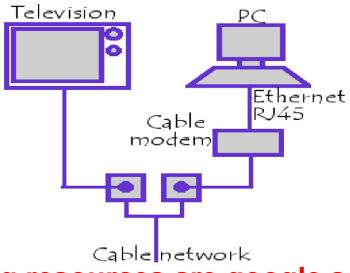
It is very costly than other typical telephone system

- **Cable Modem**

Cable modems provide Internet access using the same cables that transmit cable television

uses a special cable, known as a coaxial cable, and a modem.

Cable modem connections are faster than dial-up and DSL connections.



Advantages

- High connection speed
- Convenient
- Does not affect your phone line
- Easy setup with self installation kit

Disadvantages

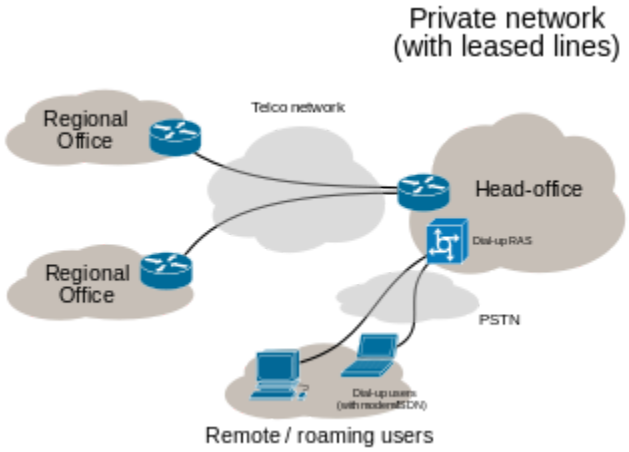
- Higher price than dialup and DSL connection
- Higher security risk than dialup or DSL
- Not available to all cable TV networks
- speed can be affected by the number of users on the same network.

• Leased Line

A leased line is a high-speed internet connection between two locations.

The service involves renting a dedicated cable from the telecom to connect two offices or branches together, enabling users to transfer large volumes of data and giving a consistent connection to the internet.

only pay a monthly bill based on usage



Advantages

- Dedicated connection between customer premises and provider local exchange

- Bandwidth is dedicated to a customer
- Symmetric speed
- High performance
- High reliability
- Greater speed
- Public IP are generally provided

Disadvantages

- Higher cost

- **Fiber optic**

  fastest type of internet connection available today.

  It uses fiber-optic cables to transmit data, and it can provide speeds of up to 1 Gbps or more.

  Advantages
  - High speed
  - Reliability
  - Security
  - Distance
  - scalability

  Disadvantages
  - Cost
  - Accessibility
  - Maintenance
  - Fragility
  - Compatibility

- **Satellite**

  Satellite internet is a wireless connection that uses a satellite dish to communicate with a satellite in orbit.

  Equipment required-mini dish satellite receiver and satellite modem

  Advantages
  - High speed internet access
  - Does not tie up with local phone service or cable TV subscription
  - Connection speed is not affected by phone or cable wiring

  Disadvantages
  - More expensive than DSL and cable
  - Large setup fee. Expensive equipment upfront. Has to be setup by trained technician.

- **Wireless**

  Use of radio waves to transmit data wirelessly between devices that are connected to a local area network (LAN).

  The speed and range of a WiFi network depend on several factors

  - type of WiFi standard being used (such as 802.11ac or 802.11ax)
  - the distance between devices,
  - any obstacles or interference in the environment.

Advantages

- Convenience
- Mobility
- Cost-effective
- Flexibility

Disadvantages

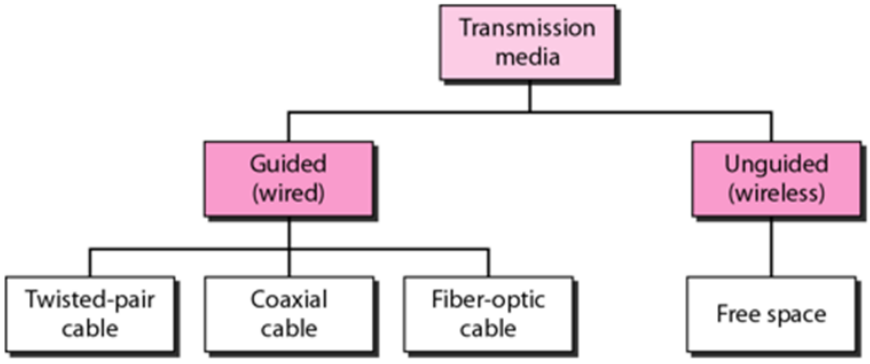
- Security concerns
- Interference
- Limited range
- Health concern

• Mobile /cellular

Mobile internet uses cellular networks to provide internet access on mobile devices such as smartphones and tablets.

Mobile internet speeds can vary depending on the network coverage and the number of users on the network.

★ Transmission Media



1. Guided (wired)

Twisted pair cable
Coaxial cable
Fiber optic cable

2. Unguided (wireless)

Radio wave
Microwave
infrared

★ Guided (wired) Transmission Media

1. Twisted Pair Cables

Consists of one or more pairs of insulated strands of copper wire twisted around one another

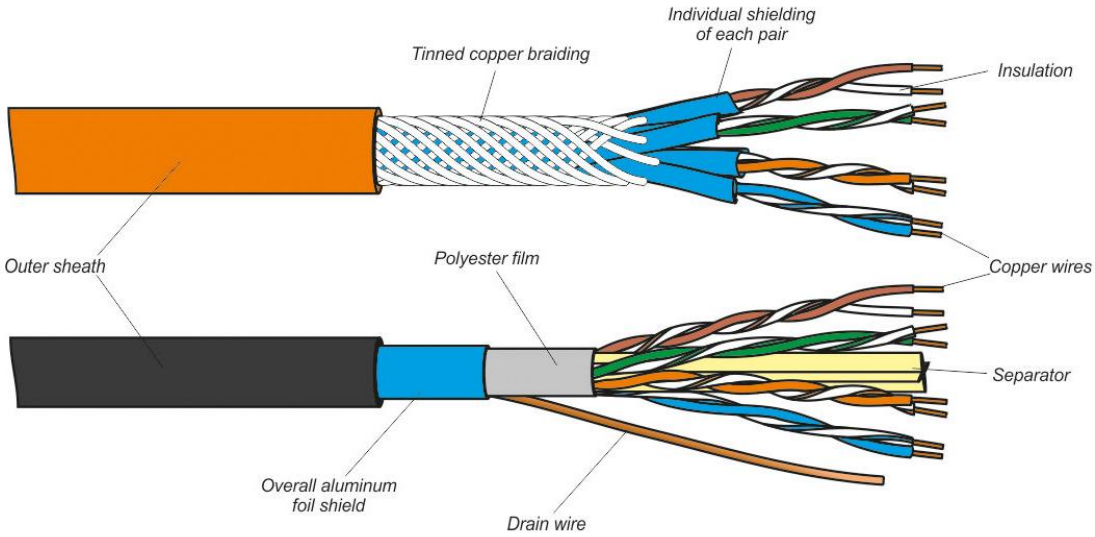
Two types.

- Shielded Twisted Pair Cables (STP)

  Characteristics of STP,
  - Speed 10-100 Mbps.
  - Moderately expensive .
  - Maximum cable length is 100 m.
  - Similar in construction of the UTP.

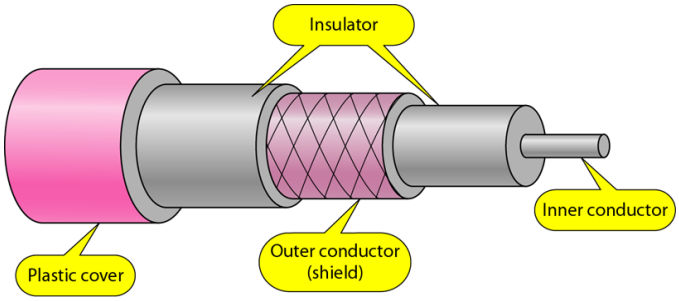
- Unshielded Twisted Pair Cables (UTP)

  Characteristics of UTP,
  - Speed 10,100,1000 Mbps.
  - Least expensive.
  - Maximum cable length is 100 m.
  - Media connector size is small.
  - Easy to install



2. Coaxial cable

has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield.



Characteristics of Co–axial Cables,

- Speed 10-100 Mbps.
- Inexpensive.
- Maximum cable length is 500 m.
- Can be run longer distances than shielded twisted pair(STP), unshielded
- twisted pair(UTP) without the need for repeaters.
- Media & connector size is Medium

3. Fiber Optic Cables

It's a network cable that contains strands of glass fiber inside an insulated casing. It consists of a center glass core surrounded by several layers of protective materials.

They are designed to carry data for long distances and at very high bandwidth (gigabit speed)

Fiber-optic Cable Advantages

- Good medium for high-bandwidth
- high-speed
- long-distance data transmissions.
- Immune to interference
- Highly secure; eliminates possibility of electronic eavesdropping

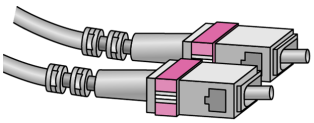
Disadvantages of Fiber Optic Cables

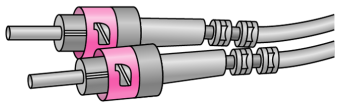
- Expensive as compared to other media
- Harder to install and modify
- Physical Damage

Fiber-optic Cable Characteristics

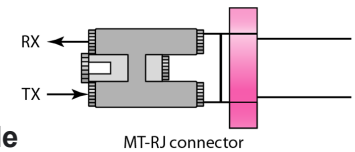
- bandwidth 100 Mbps - 1 Gbps
- Maximum cable length is 2 km.
- cost is very expensive

Fiber-optic Media Connectors


SC connector


ST connector

- ST (straight tip)
- SC (straight connection)
- MIC (medium interface connector)
- SMA (subminiature type A)



MT-RJ connector

★ Primary Techniques for Sending Signals across a Cable

- Baseband transmission
- Broadband transmission

★ Cable Selection Criteria

- Bandwidth
- Budget
- Capacity
- Scope
- Placement

★ Unguided (wireless) Transmission Media

- Radio waves
  used for cellular networks, Wi-Fi, Bluetooth, and other wireless communication technologies.

- Microwave
  cellular networks, Wi-Fi networks, and satellite communications.

- Infrared
  used for remote controls and some short-range communication

★ Wireless Propagation Methods

1. Ground propagation
2. Sky propagation
3. Line of sight propagation

★ Advantages of Wireless Communication

- Mobility
- Flexibility
- Cost-effectiveness
- Easy installation and setup

★ What is Proxy Server ?

A proxy server is an intermediary server that acts as a gateway between a client computer and another server.

★ Why Proxy Server ?

- Storing local copies of web pages for quick access.
- Proxy servers can be used to filter content, blocking access to certain websites or types of content.
- using a proxy server, the client's IP address is hidden from the target server,
- Speeding up web communication by caching and compressing data.
- Proxy servers can be used to filter out malicious traffic, providing an extra layer of security.

★ Access Control

The process by which resources or services are granted or denied on a computer system or network

★ Access Control Terminology

1. Identification
   A user accessing a computer system would present credentials or identification, such as a username

2. Authentication
   Checking the user's credentials to be sure that they are authentic and not fabricated, usually using a password

3. Authorization
   Granting permission to take the action .A computer user is granted access.

4. Custodian
   The person who reviews security settings.Also called Administrator

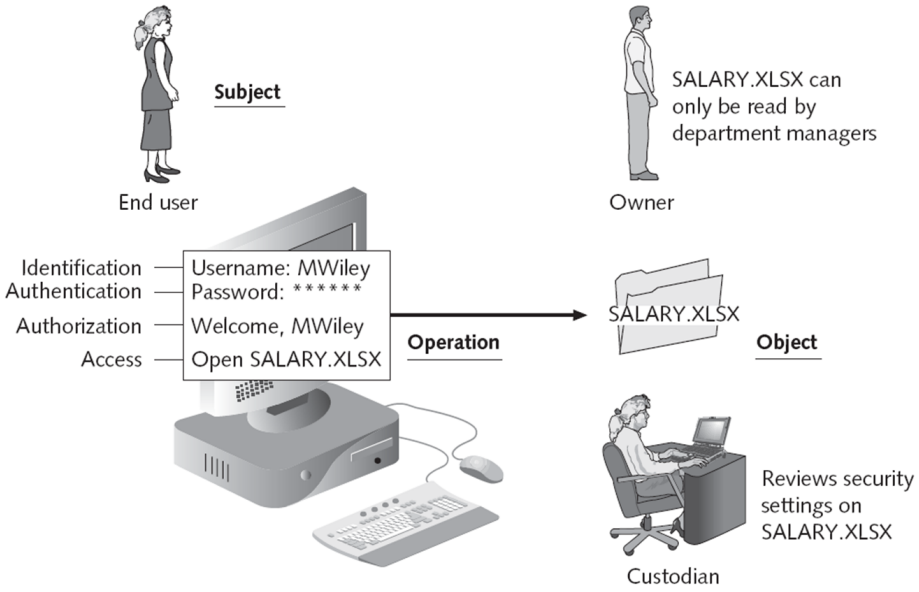


Figure 7-1 Access control process and terminology

★ Access Control Models

1. Mandatory Access Control (MAC)
   Most restrictive model—used by the military
   The end user cannot implement, modify, or transfer any controls

2. Discretionary Access Control (DAC)
   The least restrictive--used by Windows computers in small networks

In the DAC model, a subject can also change the permissions for other subjects over objects

User Account Control (UAC)

Asks the user for permission when installing software

Principle of least privilege
- Users run with limited privileges by default
- Applications run in standard user accounts
- Standard users can perform common tasks

3. Role-Based Access Control
   Sometimes called Non-Discretionary Access Control.
   Used in Windows corporate domains

4. Rule-Based Access Control
   Controls access with rules defined by a custodian.
   Example: Windows Live Family Safety

★ **The methods to implement access control are divided into two broad categories**

1. Physical access control

Physical access control primarily protects computer equipment.

Designed to prevent unauthorized users from gaining physical access to equipment in order to use, steal, or vandalize it.

Physical access control includes computer security, door security, mantraps, video surveillance, and physical access logs

- Video Surveillance
  Closed circuit television (CCTV)
  Using video cameras to transmit a signal to a specific and limited set of receivers

- Physical Access Log
  Can also identify if unauthorized personnel have accessed a secure area

  Physical access logs originally were paper documents

  Today, door access systems and physical tokens can generate electronic log documents

2. Logical access control

- Access control lists (ACLs)
  A set of permissions attached to an object.
  Specifies which subjects are allowed to access the object
  And what operations they can perform on it

- Group policies
  - A Microsoft Windows feature that provides centralized management and configuration of computers and remote users

  - Group Policy is used in corporate domains to restrict user actions that may pose a security risk

- Account restrictions
  - Time of day restrictions
    - Limit when a user can log on to a system
    - These restrictions can be set through a Group Policy
    - Can also be set on individual systems
  - Account expiration
    - The process of setting a user's account to expire
    - Orphaned accounts are user accounts that remain active after an employee has left an organization
    - Can be controlled using account expiration

- Passwords

  - A secret combination of letters and numbers that only the user knows.
  - A password should never be written down.
  - Must also be of a sufficient length and complexity so that an attacker cannot easily guess it (password paradox)

★ Introduction to Backup & Restore

The purpose of backup is to protect data from loss.

.

The purpose of restore is to recover data that is temporarily unavailable due to some unexpected event.

★ Enterprise Level Backup Apps

- Paragon Backup & Recovery includes customer support
- Backup4All Professional
- GRBackPro7

★ What is Cloud Computing?

Cloud computing is a use of internet-based services to access and manage computer resources.

Example - Dropbox, Slack, Evernote and Google Cloud

★ Cloud Service Models

1. Software as a Service (SaaS)

SaaS is a model of software deployment where an application is hosted as a service provided to customers across the Internet.

SaaS is a cloud model where software is hosted online, accessible via subscriptions.

Examples: Google Workspace, Salesforce.

2. Platform as a Service (PaaS)

Platform as a service (PaaS) is a cloud computing model where a third-party provider delivers hardware and software tools to users over the internet

Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com

3. Infrastructure as a Service (IaaS)

Infrastructure as a service (IaaS) is a type of cloud computing service that offers essential compute, storage, and networking resources on demand, on a pay-as-you-go basis.

Examples: Amazon Outposts, Azure Stack, and Google Anthos

★ Virtual Machines

VM technology allows multiple virtual machines to run on a single physical machine.

Advantages of virtual machines:

- Run operating systems where the physical hardware is unavailable,
- Easier to create new machines, backup machines, etc.,
- Software testing using “clean” installs of operating systems and software,
- Emulate more machines than are physically available,

★ Advantages of Cloud Computing

- Lower computer costs
- Reduced software costs
- Instant software updates
- Unlimited storage capacity
- Increased data reliability
- Device independence
- Universal document access

★ Disadvantages of Cloud Computing

- Requires a constant Internet connection
- Does not work well with low-speed connections
- Features might be limited
- Can be slow
- Stored data can be lost
- Stored data might not be secure

★ What is IoT ? (Internet of Things)

IoT is a network of connected physical objects that exchange data over the internet, enabling remote monitoring and control for various applications.

★ Top 10 Strategic IoT Technologies and Trends - GARTNER

Trend No. 1: Artificial Intelligence (AI)
Trend No. 2: Social, Legal and Ethical IoT
Trend No. 3: Infonomics and Data Broking
Trend No. 4: The Shift from Intelligent Edge to Intelligent Mesh
Trend No. 5: IoT Governance
Trend No. 6: Sensor Innovation
Trend No 7: Trusted Hardware and Operating System
Trend No 8: Novel IoT User Experiences
Trend No 9: Silicon Chip Innovation
Trend No 10: New Wireless Networking Technologies for IoT

★ Benefits of IoT

- Save time and money
- Enhance employee productivity
- Improve the customer experience
- Monitor their overall business processes
- Integrate and adapt business models
- Make better business decisions
- Generate more revenue

★ consumer iot products & Services

- Helmet Concussion Sensor
- Medical Alert Watch
- Smart Fitness Clothing and Smart Running Shoes
- One-Button Product Purchases
- Garden Sensors
- Smart Televisions

★ Network speed

Network speed, also known as data transfer rate, refers to the speed at which data is transferred between two devices on a network.

★ Network bandwidth

Bandwidth refers to the maximum amount of data that can be transmitted over a network connection in a given period of time.

★ Throughput

Throughput refers to the actual amount of data that is successfully transmitted over a network connection in a given period of time.

★ Malware

Includes different types of programs designed to be harmful or malicious

- Spam
  - Spamming is sending mass unsolicited emails Messages are called spam

- Adware and spyware
  - Adware
    - Pop-ups or banner ads
    - Generate income
    - Use CPU cycles and Internet bandwidth
    - Reduce PC performance

  - Spyware
    - Malware
    - Secretly gathers personal information
    - Usually installed by accident
    - Browser hijacker

- Viruses
  - Virus - A program that replicates itself and infects computers

    - Needs a host file
    - May use an email program to infect other computers
    - The attack is called the payload
    - Check to see if message is a hoax

- Worms
  - Self-replicating
  - Do not need a host to travel
  - Travel over networks to infect other machines
  - Conficker worm

- Botnet
  - Network of computer zombies or bots controlled by a master
  - Fake security notifications
  - Denial-of-service attacks (DoS)
  - Cripples a server or network by sending out excessive traffic

- Trojan horses
  - Appears to be legitimate program
  - Actually malicious
  - Might install adware, toolbar, keylogger, or open a backdoor

- Ransomware
  - Malware that prevents you from using your computer until you pay a fine or fee

• Rootkits

Set of programs
Allows someone to gain control over system
Hides the fact that the computer has been compromised
Nearly impossible to detect
Masks behavior of other malware

★ OSI Model

The Open System Interconnection Reference Model (OSI Reference Model or OSI Model) is an abstract description for layered communications and computer network protocol design.

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption
		5. Session	Interhost communication
	Segments	4. Transport	End-to-end connections and reliability, Flow control
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

Layer1: Physical Layer

The Physical Layer defines the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a physical medium.

This includes the layout of pin, voltages, cable specification, hubs, repeaters, network adapters, host bus adapters, and more

The same applies to local-area networks, such as Ethernet, token ring ,

Layer 2: Data Link Layer

The Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer.

- Media Access Control (MAC)
  Mac is lower sub-layer, and it defines the way about the media access transfer, such as CSMA/CD/CA(Carrier Sense Multiple Access/Collision Detection/Collision Avoidance)

- Logical Link Control (LLC)
  LLC provides data transmission method in different network. It will re-package date and add a new header.

Layer 3: Network Layer

The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer.

The Network Layer performs
- network routing functions,
- perform fragmentation and reassembly,
- report delivery errors.

Routers operate at this layer—sending data throughout the extended network and making the Internet possible.

Layer 4: Transport Layer

The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers.

The Transport Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control.

Layer 5: Session Layer

The Session Layer controls the dialogues (connections) between computers.

It establishes, manages and terminates the connections between the local and remote application.

It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures.

Layer 6: Presentation Layer

The Presentation Layer establishes a context between Application Layer entities, in which the higher-layer entities can use different syntax and semantics, as long as the presentation service understands both and the mapping between them.

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa.

This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems.
It is sometimes called the syntax layer.

Layer 7: Application Layer

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application.

Application layer functions typically include:
identifying communication partners,
determining resource availability,
synchronizing communication.

Some examples of application layer implementations include
Hypertext Transfer Protocol (HTTP)
File Transfer Protocol (FTP)
Simple Mail Transfer Protocol (SMTP)

★ **TCP / IP Protocol**

<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>Application Layer</td><td rowspan="3">Application Layer
TELNET, FTP, SMTP, POP3, SNMP, NNTP, DNS,NIS, NFS, HTTP, ...</td></tr>
<tr><td>Presentation Layer</td></tr>
<tr><td>Session Layer</td></tr>
<tr><td>Transport Layer</td><td>Transport Layer
TCP , UDP , ...</td></tr>
<tr><td>Network Layer</td><td>Internet Layer
IP , ICMP, ARP, RARP, ...</td></tr>
<tr><td>Data Link Layer</td><td rowspan="2">Link Layer
FDDI, Ethernet, ISDN, X.25,...</td></tr>
<tr><td>Physical Layer</td></tr>
</table>

★ Network Protocols

Network protocols are a set of rules outlining how connected devices communicate across a network to exchange information easily and safely.

1. TCP / IP

The Internet (and most other computer networks) are connected through TCP/IP networks

TCP/IP is actually a combination of two protocols:

- **IP, Internet Protocol,** is used to move packets (chunks) of data from one place to another

  Example: 192.168.1.1

- **TCP, Transmission Control Protocol,** ensures that all necessary packets are present, and puts them together in the correct order

  Example, FTP, HTTP, SMTP, TELNET

  TCP (Transmission Control Protocol)
  - Datagrams
  - Connection Oriented
  - End to End error checking
  - Source Port, Destination Port
  - Sockets, Well Known Ports

2. UDP (user datagram protocol)

- Connectionless
- One Way
- Fast, Simple
- No guarantee of delivery

  Example: NFS, DNS, DHCP, NTP, TALK

3. ICMP (Internet control message protocol)

- Error Messages
- Intended for the TCP/IP software itself
- PING (host unreachable messages)
- Simple Headers

4. Application Protocols

- **SMTP: Simple Mail Transport Protocol**

  The protocol is very simple
  SMTP is a push protocol, information is pushed to a remote site
  Uses port 25

- **HTTP: HyperText Transport Protocol**

  Client –server communication protocols
  Hypertext Transfer Protocols
  HTTP is a pull protocol, the user pulls information from a remote site.
  Protocol consists of GET and POST commands to transfer data.

- **HTTPS: HyperText Transport SSL (Secure)**

  Client –server communication protocols
  Secure communication over a computer network

  HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer.

  The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

- **SNMP: Simple Network Management Protocol**

  Simple Network Management Protocol (SNMP) is an internet standard protocol used to monitor and manage network devices connected over an IP.

- **FTP: File Transfer Protocol**

  File Transfer Protocol,
  User authentication
  Anonymous

  used to transfer computer files between a client and server on a computer network.

  built on a client-server model architecture and uses separate control and data connections between the client and the server.

  GET/PUT/DEL/CWD

- **Telnet: Interactive login**

  User command and an underlying TCP/IP protocol for accessing remote computers.

  Through Telnet, an administrator or another user can access someone else's computer remotely.

- **SSH: Secure Shell telnet**

  A cryptographic network protocol for operating network services securely over an unsecured network.

The best known example application is for remote login to computer systems by users.

- **DNS: Domain Name Service**

  A Domain Name System (DNS) turns domain names into IP addresses, which allow browsers to get to websites and other internet resources.

★ Email clients

• Email clients are web-based or desktop apps that allow you to manage email accounts from different email service providers.

• Outlook, for example, also has a desktop version that allows you to connect @outlook accounts and email accounts provided by other hosting platforms.

• Easily customize your email client.
• Emails can be backed up to the computer

★ Email server

An email server, also called a mail server, is essentially a computer system that sends and receives emails.

★ Email Gateway

All emails pass through this Email Gateway and are checked for potential security threats. An Email Gateway, hence, acts as a firewall for emails.

★ Why Use Desktop Email Clients?

• Easily Manage Multiple Emails (with Different Domains)
• Access Your Email Offline
• Security Features and Encryption
• Seamlessly Integrate With Desktop Apps

★ Webmail

A webmail is a web-based email service that allows you to use email features using your website browser.

For example, Gmail's webmail allows you to manage Gmail accounts only.

★ POP3 (Post Office Protocol 3)

• Most recent version of a standard protocol for receiving email.
• Mail access client
• Uses port 110
• Messages are downloaded to the client but can be stored on the server.
• Does not easily allow multiple clients

★ **IMAP (Internet Mail Access Protocol)**

- Improved POP3
- Automatically assigns folders
- Leaves mail on server
- Only transfers as much as needed per message (headers, subject only on list)

★ **DHCP (Dynamic Host Configuration Protocol)**

DHCP is a way of assigning temporary IP addresses as needed

★ **ARP (Address Resolution Protocol)**

- Protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. Or

- procedure for mapping a dynamic IP address to a permanent physical machine address in a local area network (LAN).

★ **RARP (Reverse Address Resolution Protocol)**

used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its Link Layer or hardware address, such as a MAC address.

★ **Remote Login**

Remote Login is the ability to access the data stored on a computer from a remote location.