NETWORK ARCHITECTURE

UNIT - IV

NETWORK ARCHITECTURE

- **ARCHITECTURE AND DESIGN** (/#/)
- **COMPONENT ARCHITECTURES / REFERENCE ARCHITECTURE** (/#/)
- **ARCHITECTURE MODELS**(/#/)
- SYSTEM AND NETWORK ARCHITECTURE
- ADDRESSING AND ROUTING ARCHITECTURE / FUNDAMENTALS
- ADDRESSING MECHANISMS
- ADDRESSING STRATEGIES / ROUTING STRATEGIES
- NETWORK MANAGEMENT ARCHITECTURE / MECHANISMS
- PERFORMANCE ARCHITECTURE / MECHANISMS
- SECURITY AND PRIVACY ARCHITECTURE / MECHANISMS

ARCHITECTURE & DESIGN

- Good network design is a process by which an extremely complex and nonlinear system is conceptualized.

- Network architecture and design development must be done in a systematic and reproducible manner.

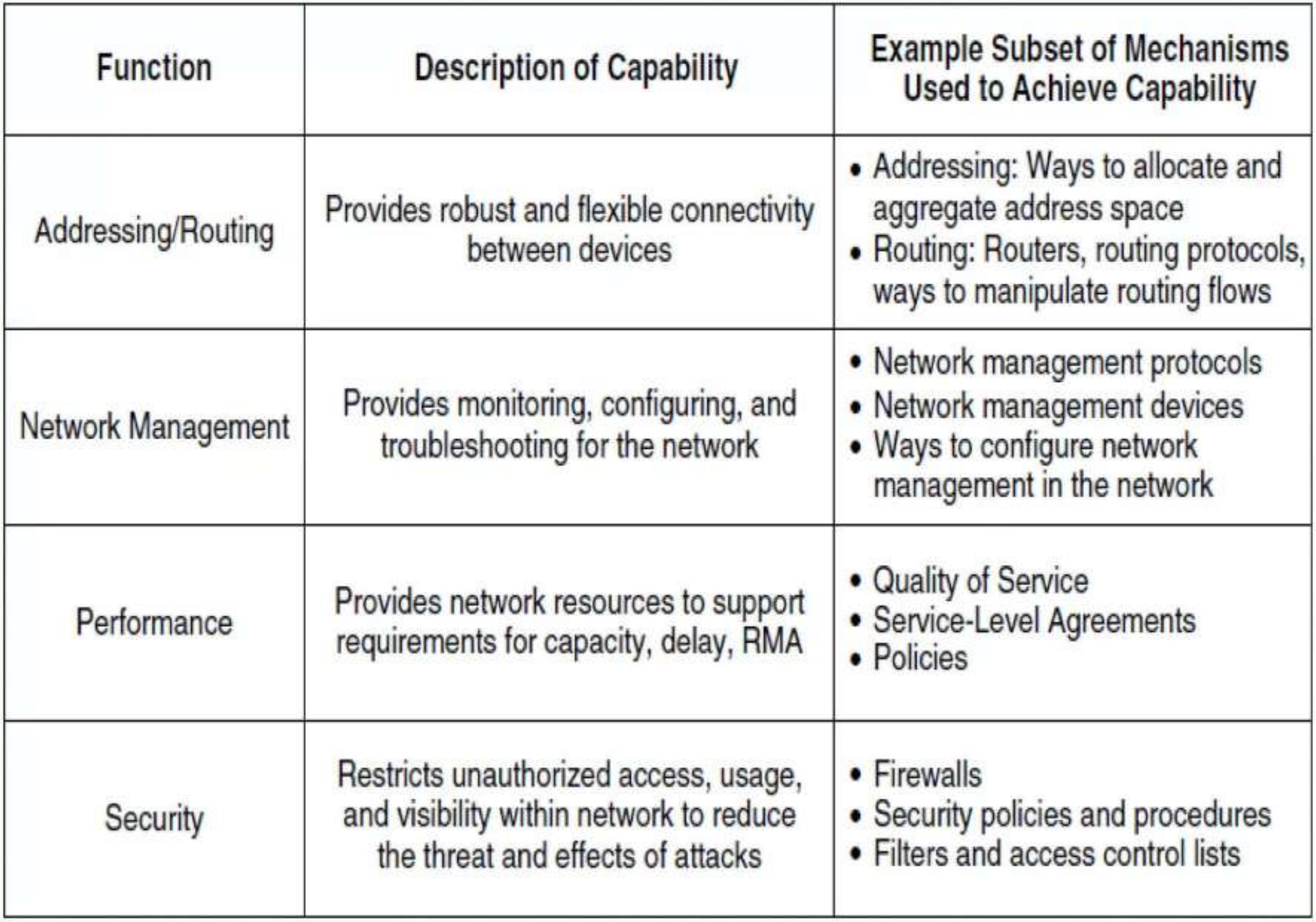
COMPONENT ARCHITECTURES

- Component architecture is a description of how and where each function of a network is applied within that network.

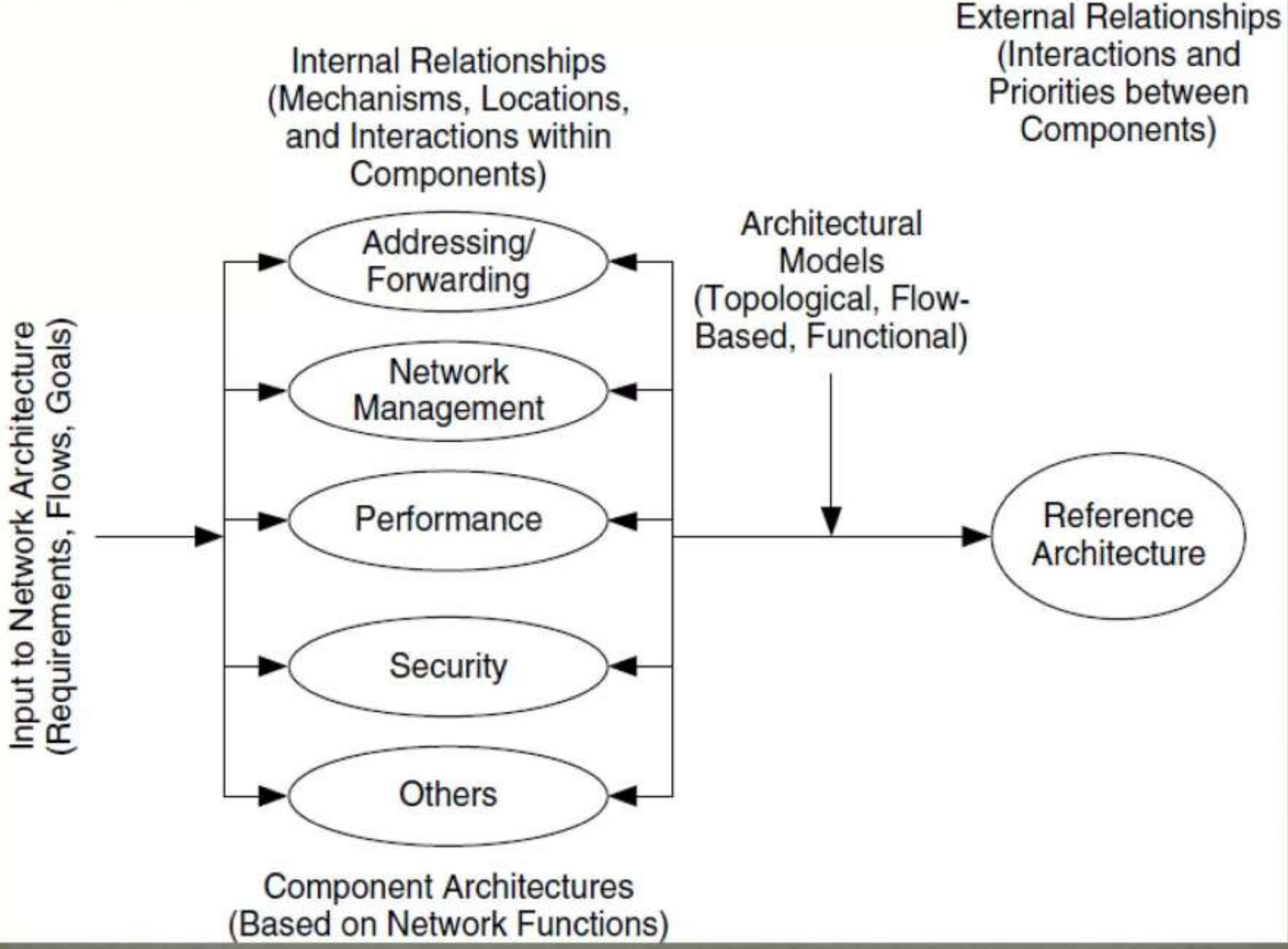
- It consists of a set of mechanisms (HARDWARE AND SOFTWARE) by which that function is applied to the network.

COMPONENT ARCHITECTURES

- It explores four functions / Architectures
  - ADDRESSING/ROUTING(Forwarding) architecture.
  - NETWORK MANAGEMENT architecture.
  - PERFORMANCE architecture.
  - SECURITY architecture.



Function	Description of Capability	Example Subset of Mechanisms Used to Achieve Capability
Addressing/Routing	Provides robust and flexible connectivity between devices	• Addressing: Ways to allocate and aggregate address space • Routing: Routers, routing protocols, ways to manipulate routing flows
Network Management	Provides monitoring, configuring, and troubleshooting for the network	• Network management protocols • Network management devices • Ways to configure network management in the network
Performance	Provides network resources to support requirements for capacity, delay, RMA	• Quality of Service • Service-Level Agreements • Policies
Security	Restricts unauthorized access, usage, and visibility within network to reduce the threat and effects of attacks	• Firewalls • Security policies and procedures • Filters and access control lists



External Relationships (Interactions and Priorities between Components)

Internal Relationships (Mechanisms, Locations, and Interactions within Components)

Input to Network Architecture (Requirements, Flows, Goals)

Addressing/ Forwarding

Network Management

Performance

Security

Others

Architectural Models (Topological, Flow-Based, Functional)

Reference Architecture

Component Architectures (Based on Network Functions)

COMPONENT ARCHITECTURES

- To determine how performance will work for a network.
- To determine how each mechanism works, and how they work together to provide performance for the network.

- This picture bellow shows how
- QoS – Quality of Service,
- SLA-Service Level Agreements and policies are applied.

Quality of service (QoS):

- It is the overall performance of a telephony or computer network,
- particularly the performance seen/measured by the users of the network.

Service Level Agreement

- A *SERVICE LEVEL AGREEMENT* is an important document that is used to define the level of a service between a service provider and their customer/service requester.
- It is a contract between a network service provider and a customer /service requester
- Aspects/Features of the service level agreement
  - scope, quality, responsibilities - are agreed between the service provider and the service user/ service requester.

COMPONENT ARCHITECTURES

- Developing COMPONENT ARCHITECTURE requires input, sets of user(), application, and device requirements, estimated traffic flows, and architectural goals defined for each individual network.

- This input forms a common foundation for all network functions.

COMPONENT ARCHITECTURES

- To facilitate determining where each mechanism may be applied, the network is divided into regions.

- Commonly used regions include:
  - access (edge),
  - Distribution(service available for use by a consumer or business user.),
  - core (backbone / fundamental/sets), and
  - External interfaces(MATLAB) & DMZs

DMZs

- Demilitarized Zone (sometimes referred to as a PERIMETER NETWORK)
- It is a physical or logical sub-network that contains an organization's external-facing services .
- The characteristics of each region help to identify where mechanisms are applied.
- When mechanisms have been chosen and applied to the network and we want to know about the internal(mechanisms , locations) relationships between these mechanisms.

MATLAB (matrix laboratory)

- MATLAB (matrix laboratory).
- MATLAB allows matrix manipulations.
- It is a multi-paradigm Numerical Computing Environment .
- (4GL) Fourth-Generation programming language.

REFERENCE ARCHITECTURE

- A reference architecture is a description of the complete network architecture.
- It contains all functions of the component architectures (i.e., functions).
- Each component

COMPONENT ARCHITECTURES

ADDRESSING AND ROUTING

ADDRESSING

- a 32-bit number that uniquely identifies a host(system).
- Simply called IP **address**
- IP **addresses** are normally expressed in dotted-decimal format, with four numbers separated by periods,
- Ex: such as 192.168.123.132.

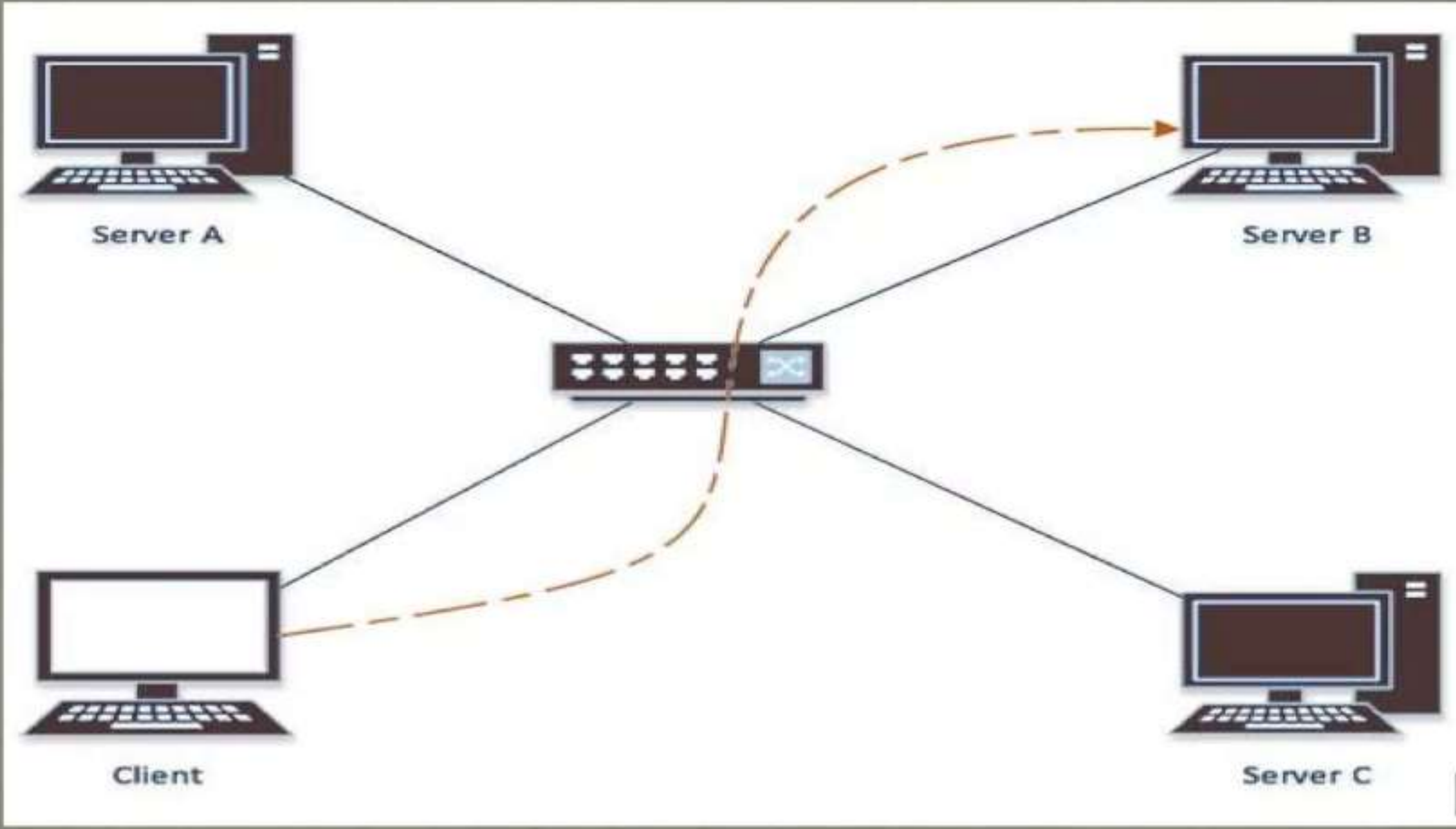
ROUTING

- Routing is the process of selecting best paths in a network.
- the process of moving a packet of data from source to destination.
- Routing is usually performed by a dedicated device called a router.

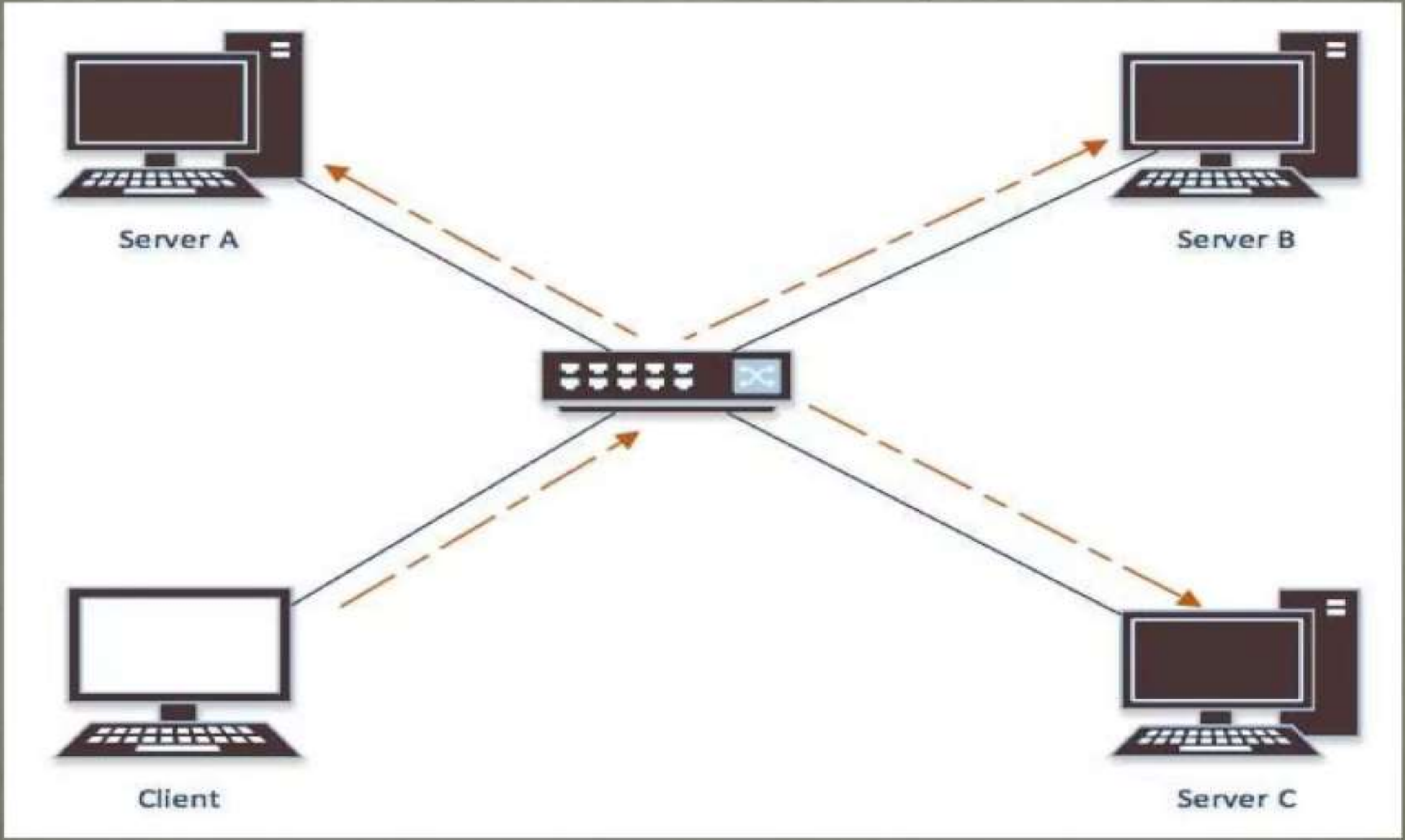
- **Routing schemes differ in their delivery semantics:**

- UNICAST - delivers a message to a single specific node(**FM/WTalkie**).
- BROADCAST - delivers a message to all nodes in the network(**TV**).
- MULTICAST - delivers a message to a group of nodes that have expressed interest in receiving the message(**email/teleconf/videoconf**).
- ANYCAST - delivers a message to anyone out of a group of nodes, typically the one nearest to the source(**network addressing and routing methodology**).
- GEOCAST - delivers a message to a geographic area(**ad-hoc networks**)

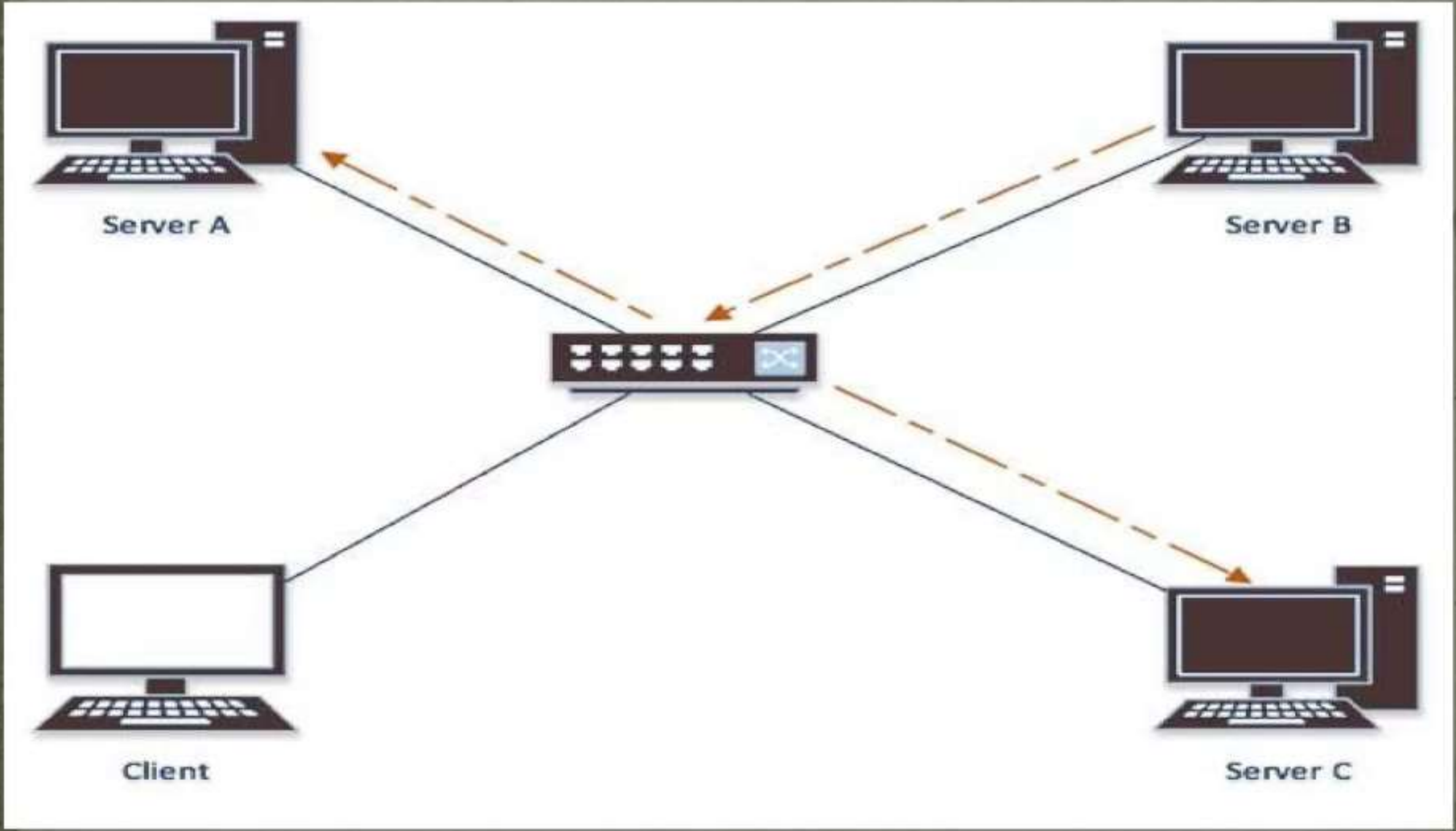
UNICAST ADDRESSING MODE:



BROAD CAST ADDRESSING MODE



MULTI CAST ADDRESSING



ADDRESSING & ROUTING

- Addressing is applying identifiers (addresses) to devices at various protocol layers (e.g., data-link layers and network layer)
- Ex: class A, B, C, D

- While routing is learning about the connectivity within and between networks and applying this connectivity information to forward IP packets toward their destinations.

THE ADDRESSING/ROUTING DESCRIBES:

- how user and management traffic flows are forwarded through the network.
- How hierarchy(level), separation, and grouping of users and devices are supported.
- There are several addressing and routing mechanisms that could be considered.

ADDRESSING MECHANISMS

- Sub-netting & Super-netting,
- Variable-length Sub-netting,
- Dynamic Addressing,
- Private Addressing,
- Virtual Lans (Vlans),
- Ipv6, And
- Network Address Translation (Nat).

SUB-NETTING

- **SUB-NETWORKING:**

Dividing a network into two or more networks is called **sub-netting**.

- **Subnet** is a logical.
- visible subdivision of an IP Network.

SUPER-NETTING

- **SUPER NETWORK.**
- **also called Classless Inter-Domain Routing (CIDR).**
- **It is a way to aggregate(**form or group**) multiple Internet addresses of the same class.**
- Example:
  - 192.168.98.0
  - 192.168.99.0
  - 192.168.100.0
  - 192.168.101.0
  - 192.168.102.0
  - 192.168.105.0

DYNAMIC ADDRESSING (DIP)

- DYNAMIC IP ADDRESSING:
  - It assigns a different IP address each time the ISP customer logs on to their computer.
  - Ex: 192.168.105.0
- STATIC IP ADDRESSING:
  - It is for one customer on one IP address.
- Ex: FTP, Interanet.

- **PRIVATE - ADDRESSES:**
  - Each IP node requires an IP address that is globally unique to the IP internetwork.
- **PUBLIC - ADDRESSES:**
  - When the public addresses are assigned, routes are programmed into the routers of the Internet so that traffic to the assigned public addresses can reach their locations.

- VIRTUAL LAN OR VLAN:
- which are mutually isolated so that packets can only pass between them via one or more routers.
- such a domain is referred to as a virtual local area network, virtual LAN or VLAN.

- Internet Protocol version 6 (IPv6) :
- It is the latest version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.
- Internet Protocol version 4 (**IPv4**):
- It is the fourth version in the development of the Internet Protocol (IP) Internet, and routes most traffic on the Internet.

IP Versions:

- ip v1 - 3 not formally assigned.
- ipv4 - 32 bit IP address. (Decimal)
- Example: 192.168.105.0
- Ipv5 - streamed protocaol(ST). connection oriented internet level protocol
- IPv6 - 128 bit IP address(Hexa Decimal.)
- Example:
- 2607:fodo:1002:0051:0000:0000:0000:0004

network address translation (NAT) :

- provides a method of modifying network address information in Internet Protocol (IP).
- The purpose of remapping one IP address space into another one IP address space.

ROUTING MECHANISMS

- Switching And Routing,
- Classless Inter-Domain Routing (CIDR):
- Multicasts,
- Mobile IP,
- Route Filtering/Peering/Routing/policies
- Confederations(IGP, EGP)

HUB/SWITCHING / ROUTING

- HUB
  - A common CONNECTION POINT for devices in a network.
  - to connect segments of a LAN.
  - A HUB contains multiple ports.
  - Ex: anything that comes in one port is sent out to the others.

plugable

HUB/SWITCHING / ROUTING

- SWITCH:
- A switch does essentially what a hub does, but more efficiently.
- It is a device that filters and forwards packets between LAN segments.
- Types:
  - Circuit Switching
  - Packet Switching
  - Message Switching

LINKSYS

ROUTER:

- A device that forwards data packets along networks.
- A smartest and most complicated of the bunch.
- A router is connected to at least two networks, Or two LANs
- Especially use for MANs/WANs.
- Routers integrate the functions of switch, DHCP Server(Dynamic Host Configuration Protocol) & Firewall.
- ADV : Increases the bandwidth.

LINKSYS
LINKSYS

CLASSLESS INTER-DOMAIN ROUTING (CIDR):

- Super Networiking.
- It is a method for allocating IP addresses and routing Internet Protocol packets.
- Example:
  - 192.168.98.0
  - 192.168.99.0
  - 192.168.100.0
  - 192.168.101.0
  - 192.168.102.0
  - 192.168.105.0

MOBILE IP

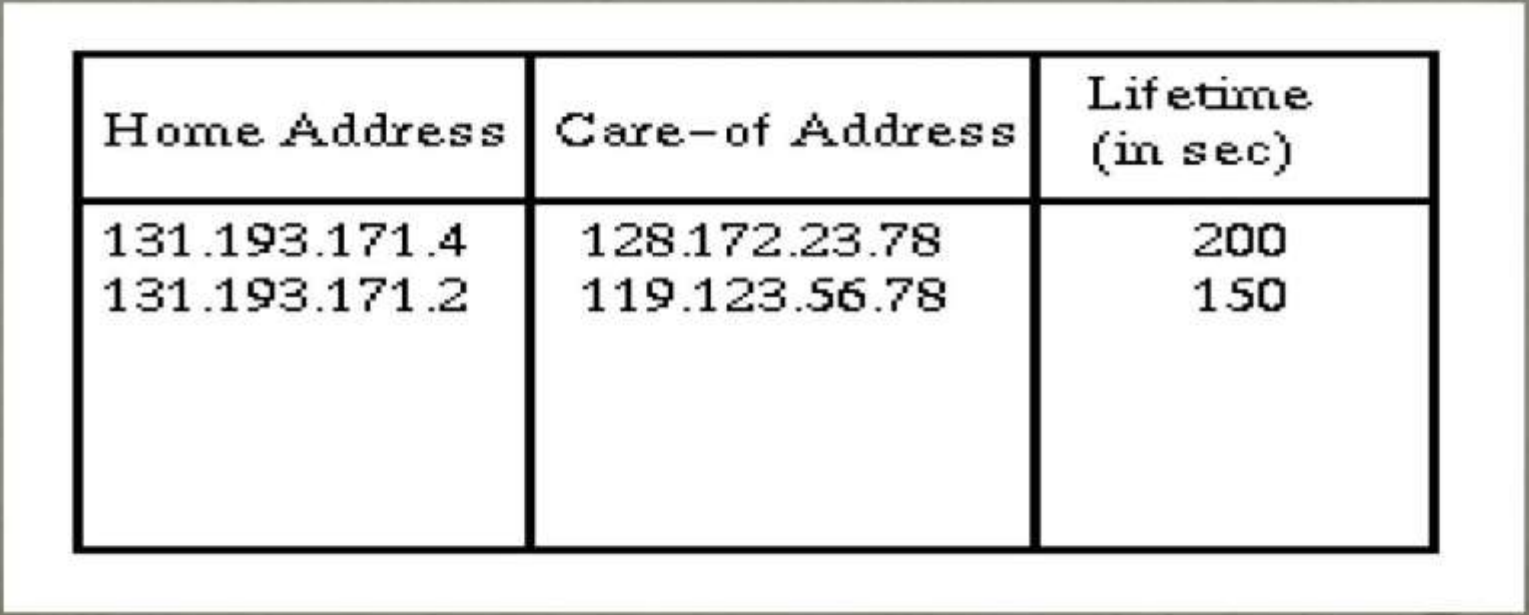
- Mobile IP stands for **Mobile Internet Protocol**.
- A **wireless connection** to the Internet.
- Designed to support (GENERIC device)host mobility.
- Stay connected regardless of location without changing IP address.
- Provide **confident access** to the Internet anytime, anywhere.

MOBILE IP

- Mobile Node : A node/device that changes its point of attachment to the Internet
- Home Agent : A router in the home network that communicates with the mobile node
- Foreign Agent: A router in a foreign network that delivers information between mobile node and its home agent
- Care-of-Address: Mobile Node’s current IP address
- Correspondent Node: Node/device that is communicating with the mobile node (i.e. web server)

MOBILE IP

- Each mobile node has two IP addresses
- - Permanent home address
- - Care-of Address(temporary IP address)
- Home Agent maintains a mobility binding table



Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

FILTERING/PEERING/POLICY

- **ROUTE - FILTERING:**
  - Designed to exchange routing and reachability information between autonomous systems in the local route database.
  - (**INPUT FILTERING -|- OUTPUT FILTERING**).
- **ROUTE - PEERING:**
- it is a voluntary interconnection.
- the purpose is **Exchanging Traffic between** the users of each network.
- **A POLICY:**
  - It is a **principle to guide decisions making** and achieve **quality** outcomes.

Confederations(IGP, EGP)

- **IGP** confederation :
- An **I**nterior **G**ateway **P**rotocol (IGP):
- Interior Gateway **P**rotocol (IGP) is a dynamic class routing protocol used by **A**utonomous **S**ystem.
- It is a type of protocol used for **exchanging routing information** between gateways (commonly **routers)** within an Autonomous System
- (for example, a system of corporate local area networks).
- It can be used to route network-level protocols like IP.

BGP confederation :

- BGP: Border Gateway Protocol
- It is a protocol that is used between routers to convey this information.
- It is a standardized Exterior Gateway Protocol.
- It is a method to use Border Gateway Protocol (BGP) to subdivide a single autonomous system (AS) into multiple internal sub-Autonomous System.
- Designed to exchange routing information between **Gateway Hosts** on the Internet.

NETWORK MANAGEMENT

- Network management is providing functions to
  - **control,**
  - **plan,**
  - **allocate,**
  - **deploy,**
  - **coordinate, and**
  - **monitor** network resources.
- Network management **mechanisms** include:
- Monitoring: Obtaining values for **end-to-end**, **per link**, and **per-element network** management characteristics.
- Instrumentation: Determining the **set of tools** and **utilities needed to monitor** and probe the network for management data.

NETWORK MANAGEMENT

- Configuration: Setting **parameters** in a network device for **operation and control** of that element.

- FCAPS components:
- The set of **fault, configuration, accounting, performance, and security** management components.
- **It is the ISO Telecommunications Management Network model .**
- **Framework for network management.**
-
- In-band and out-of-band management: Whether management data flow along the **same path or have a separate path**.

NETWORK MANAGEMENT

- Centralized and distributed management:
  - Whether the management system is in a single hardware platform or is distributed across the network among **multiple platforms**.(platform/language)
- Scaling(measure) network management traffic:
  - Determining **how much network capacity** should be reserved for network management.
- Checks and balances:
  - Using multiple mechanisms to verify that **variables are represented correctly**.

NETWORK MANAGEMENT

- Managing network management data:
  - Offloading old data, keeping track of storage availability for data, updating data types.
- MIB selection:
  - Determining which **management information bases**, and how much of each management information base, to use.
    - **(MIB) is a database used for managing the entities in a communications network.**
    - **Associated with the Simple Network Management Protocol (SNMP).**
- Integration into OSS:
  - How the management system will communicate with higher-level **operations support system.**

PERFORMANCE

- Performance consists of the set of **mechanisms** used to
- **configure,**
- **operate,**
- **manage,**
- **provision, and**
- **account** for resources in the networks.
- To allocate performance to **users, applications, and devices**.

PERFORMANCE

- This includes **capacity planning** and **traffic engineering**, as well as a variety of service mechanisms.
- **how network resources will be allocated to user** and **management traffic flows**.
- This consists of **prioritizing, scheduling, and conditioning traffic flows**
- mechanisms to **correlate(**mutual relationship or connection BW**) user, application, and devices and quality of service, policies, and service-level agreements** (SLAs).

QUALITY OF SERVICE

- It is the overall performance of a **computer network,** particularly the performance seen by the **users of the network**.
- QoS, is determining, **setting, and acting upon priority** levels for traffic flows.

SERVICE-LEVEL AGREEMENTS

- (SLAs) are informal or **formal contracts between a Service - provider and Service – Requester.**
- Policies are sets (formal or informal) of high-level statements about how network Resources / Services /Access Permissions are to be allocated among users.

SECURITY

- Security is a requirement to guarantee the confidentiality,
- integrity,
- availability of user,
- application, device, and network information and physical resources.
- it describes how system resources are to be protected from theft, damage, Denial Of Service (DOS(Hacker)/ACCESS Denied: attack is an attempt to make a machine or network resource unavailable) / unauthorized access.

SECURITY

- This consists of the **mechanisms used to apply security**, which may include such:

- ENCRYPTION,
- FIREWALLS,
- ROUTING FILTERS, AND
- NETWORK ADDRESS TRANSLATION (NAT) AND
- BIO-METRIC VERIFICATION(human characteristics
- Such as **EYE RETINAS, FINGERPRINT, VOICE BASED, PATTERNs Etc..**)

SECURITY

- Physical security and awareness:
  - The protection of devices from **physical access**
  - damage, and theft parts of the network from outside access)
  - getting users educated and involved with the day-to-day aspects of security in their network.
  - Helping them to understand the potential risks of violating security policies and procedures.

SECURITY

- The security mechanisms that were considered are:
- Security threat analysis:
  - The process to determine which components of the system need to be protected and the types of security risks (threats) they should be protected.
- Security policies and procedures:
  - Formal statements on rules & regulations for system/network.
  - Information access, in order to minimize exposure to security threats.

SECURITY

- Protocol and application security:
  - Securing management and network protocols(SNMP) and applications from unauthorized access and misuse.
- Encryption:
  - Making data unreadable if they are intercepted, by applying cipher algorithms together with a secret key(CRYTOGRAPHY).
- Network perimeter security:
  - Protecting the external interfaces between your network and external networks.

SECURITY

- Remote access security:
  - Securing network access based on traditional dial-in, point-to-point sessions, and virtual private network connections.
  - Ex: TEEM WEAVER.
  - REMOTE ADMINISTRATION TOOL (RAT).

ARCHITECTURAL MODELS

- THREE TYPES OF ARCHITECTURAL MODELS :
- topological models(LAN/MAN/WAN)
  - which are based on a geographical or topological arrangement.
- flow-based models(Peer to peer, Client-server, Hierarchical client-server, and Distributed computing)
  - which take particular advantage of traffic flows from the flow specification.
- functional models(service-provider, • intranet/extranet, • single-/multi-tiered performance, and • end-to-end models.)
  - which focus on one or more functions or features planned for in the network.

THANK YOU