**PROSIT 1 – ALEX’S QUEST**

**KEYWORDS** A

1. Innovative software development - Software development refers to a set of computer science activities dedicated to the process of creating, designing, deploying and supporting software.
2. Information system architect - a professional specialised in designing and managing the information systems of an organisation. They define the technological architecture and ensure the coherence, security and sustainability of IT systems.
3. Data management expert – a professional who designs strategies for enterprise databases, data warehouse systems, and multidimensional networks.
4. Cyber security specialist - a professional who is responsible for protecting computer systems, networks, and data from unauthorized access, theft, or damage.
5. Information system - an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products.
6. Information system architecture - a formal definition of the business processes and rules, systems structure, technical framework, and product technologies for a business or organizational information system.
7. Servers - a central computer that controls and provides information to other computers in a network
8. Databases - an organized collection of data or a type of data store based on the use of a database management system (DBMS)
9. Communication networks - connecting different systems and devices to share data and information. This setup includes hardware like computers, routers, switches, and modems, as well as software protocols that manage how data flows between these devices.
10. IS Architecture Diagram – diagrams which provide a visual illustration of a system's various components and show how they communicate and interact with each other. These diagrams document a system's structure and architecture.
11. Robust and Scalable architecture - Robust architecture is designed to meet needs; its structures are sufficient and resilient. A scalable architecture is an architecture that can scale up to meet increased workloads.
12. ADs – Active Directory (AD) enables administrators to manage permissions and access to network resources, stores data as objects, and categorizes directory objects by name and attributes.
13. Switches - connects network devices (printers, computers, and wireless devices/access points, and enables users to exchange data packets.
14. Endpoints - physical devices that connect to and exchange information with a computer network.
15. Application servers – connects the user interface to critical information contained in backend databases.
16. Firewalls - a network security device that separates a trusted internal network from an external network deemed untrustworthy, such as the internet. It regulates incoming and outgoing network traffic based on preset security rules.
17. Web servers - a computer system capable of delivering web content to end users over the internet via a web browser
18. DMZs - demilitarized zone is a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic.
19. Routers - a device that connects two or more packet-switched networks or subnetworks. It manages traffic between these networks by forwarding data packets to their intended IP addresses, and allows multiple devices to use the same Internet connection.

**CONTEXT** A

TechNova's outdated system struggles with performance, security, and scalability. Alex must design a modern, robust architecture to support the company's growth.

**PROBLEM STATEMENT** A

How can TechNova modernize its information system architecture to support its rapid growth and ensure optimal performance, security, and data management?

**CONSTRAINTS** A

* Scalable, Secure, Robust.
* Already existing IS.

**DELIVERABLE** A

Drawing up an IS architecture diagram

**GENERALIZATION** A

INFORMATION SYSTEMS ARCHITECTURE

**SOLUTION APPROACH** A

* Scalable, Secure, Robust.
* Already existing IS.

**ACTION PLAN** A

1. Study the IS Components
   1. Networks (Types- LAN, WAN, MAN, VLAN, VPN PROXY)
      1. Routers, switches, firewalls, endpoints, DMZS.
   2. Servers
      1. Application servers, web servers, FTP servers, mail servers, proxy servers Ads.
   3. Databases
      1. Types of Databases
2. Propose the IS diagram.

[**NETWORKS**](https://www.geeksforgeeks.org/network-and-communication/)

* A network is a set of devices connected by communication links.
* A network must meet the following network criteria:
  + Performance – It is measured by transit time and response time also depends on users, medium, hardware, and software.
  + Reliability – reliability is measured by the frequency of failure.
  + Security – Security protects data from unauthorized access.
* The security of a computer network is challenged every day by:
  + Equipment malfunctions
  + System failures
  + Computer hackers
  + Virus attacks
* It is categorized into three types: LAN, MAN, WAN. Into which categories of network falls is determined by its size, its ownership, the distance it covers, and its physical architecture.
  + Local Area Network
    - Privately owned that links the devices in a single office, building, or campus. Its s
    - Size is limited to a few kilometres.
    - Designed to allow resources to be shared between personal computers or workstations.
    - Uses only one type of transmission medium.
    - Most common LAN topologies are bus, ring, and star.
  + Metropolitan Area Network
    - Maybe wholly owned and operated by a private company or it may be service provided by a public company.
    - Designed to extend over an entire city.
    - A company can use MAN to connect the LANs in all its offices throughout a city.
  + Wide Area Network
    - Provides long-distance transmission of data over a country, a continent, or even the worldwide.
    - Connects all the company’s computers and devices, allowing them to share information and resources internally.

[**VLAN**](https://www.geeksforgeeks.org/virtual-lan-vlan/)

* Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer of OSI Model).
* VLAN ranges:
  + VLAN 0, 4095: These are reserved VLAN which cannot be seen or used.
  + VLAN 1: It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can’t be deleted or edit but can be used.
  + VLAN 2-1001: This is a normal VLAN range. We can create, edit and delete these VLAN.
  + VLAN 1002-1005: These are CISCO defaults for fddi and token rings. These VLAN can’t be deleted.
  + VLAN 1006-4094: This is the extended range of VLAN.

*Note:-*

* *FDDI stands for Fiber Distributed Data Interface. It is a set of ANSI and ISO guidelines for information transmission on fiber-optic lines in Local Area Network (LAN) that can expand in run upto 200 km (124 miles). The FDDI convention is based on the token ring protocol.*



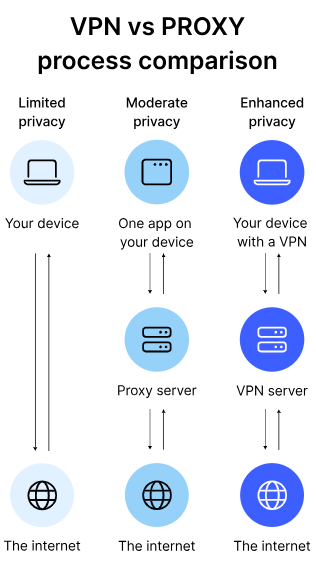
* *Token Ring protocol is a communication protocol used in Local Area Network (LAN). In a token ring protocol, the topology of the network is used to define the order in which stations send. The stations are connected to one another in a single ring. It uses a special three-byte frame called a “token” that travels around a ring. It makes use of Token Passing controlled access mechanism. Frames are also transmitted in the direction of the token. This way they will circulate around the ring and reach the station which is the destination.*

**VPN**

* A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet.
* It is a way to extend a private network using a public network such as the Internet.
* It makes use of tunnelling protocols to establish a secure connection.

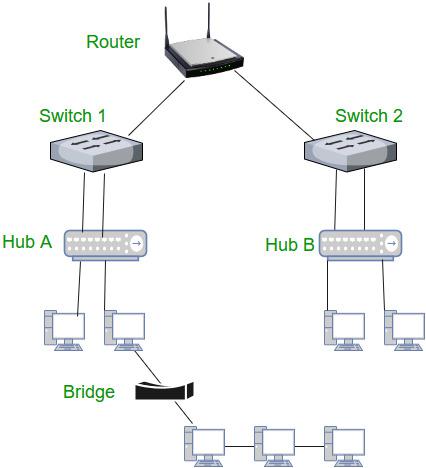
*Note:-*

*Tunnelling protocol - In computer networks, a tunnelling protocol is a communication protocol which allows for the movement of data from one network to another.*



[**ROUTERS**](https://www.geeksforgeeks.org/introduction-of-a-router/)

* A Router is a networking device that forwards data packets between computer networks.
* One or more packet-switched networks or subnetworks can be connected using a router.
* By sending data packets to their intended IP addresses, it manages traffic between different networks and permits several devices to share an Internet connection.



Functions of Router:

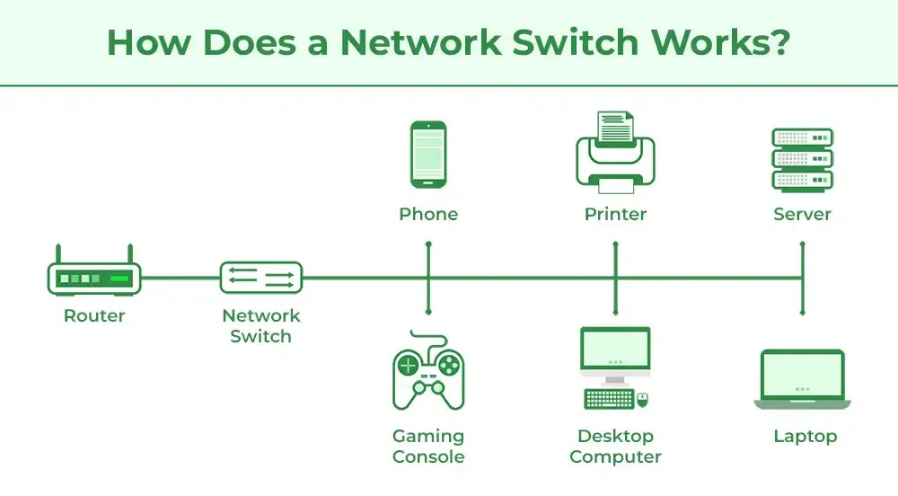
* Forwarding: The router receives the packets from its input ports, checks its header, performs some basic functions like checking checksum, and then looks up to the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.
* Routing: Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, It maintains a routing table that is made using different algorithms by the router only.
* Network Address Translation (NAT): Routers use NAT to translate between different IP address ranges. This allows devices on a private network to access the internet using a single public IP address.
* Security: Routers can be configured with firewalls and other security features to protect the network from unauthorized access, malware, and other threats.
* Quality of Service (QoS): Routers can prioritize network traffic based on the type of data being transmitted. This ensures that critical applications and services receive adequate bandwidth and are not affected by lower-priority traffic.
* Virtual Private Network (VPN) connectivity: Routers can be configured to allow remote users to connect securely to the network using a VPN.
* Bandwidth management: Routers can be used to manage network bandwidth by controlling the amount of data that is allowed to flow through the network. This can prevent network congestion and ensure that critical applications and services receive adequate bandwidth.
* Monitoring and diagnostics: Routers can be configured to monitor network traffic and provide diagnostics information in the event of network failures or other issues. This allows network administrators to quickly identify and resolve problems.

*Q. Difference between modem and router:*

*A modem is a device that links your home network to your internet service provider. A router is a device that enables all of your wired and wireless devices to access the internet simultaneously and to communicate with one another.*

**SWITCHES**

* The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments.
* It is responsible for filtering and forwarding the packets between LAN segments based on MAC address.
* Switches have many ports, and when data arrives at any port, the destination address is examined first and some checks are also done and then it is processed to the devices.
* Different types of communication are supported here like unicast, multicast, and broadcast communication.

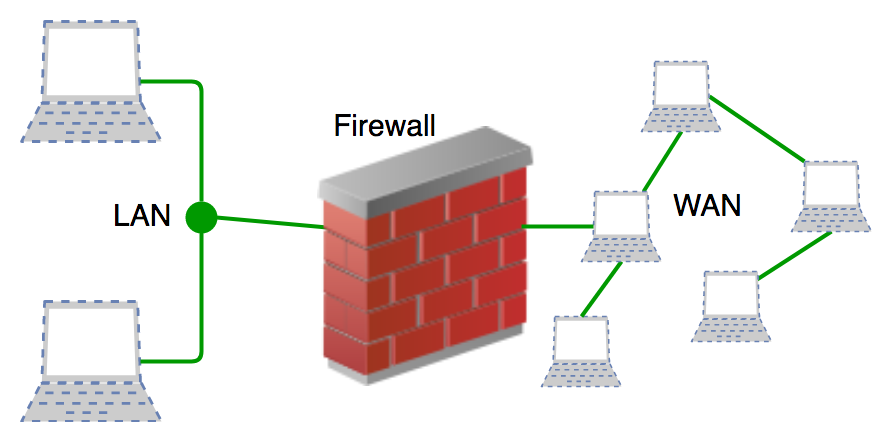


Features of Switches:

* It operates in the Data Link Layer in the OSI Model.
* It performs error checking before forwarding data.
* It transfers the data only to the device that has been addressed.
* It operates in full duplex mode.
* It allocates each LAN segment to a limited bandwidth.
* It uses Unicast (one-to-one), multicast (one-to-many), and broadcast (one-to-all) transmission modes.
* Packet-switching techniques are used to transfer data packets from source to destination.
* Switches have a more significant number of ports.

**FIREWALLS**

* A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic.
  + Accept: allow the traffic
  + Reject: block the traffic but reply with an “unreachable error”
  + Drop: block the traffic with no reply



* A firewall is a type of network security device that filters incoming and outgoing network traffic with security policies that have previously been set up inside an organization.
* A firewall is essentially the wall that separates a private internal network from the open Internet at its very basic level.

Functions of Firewall

* Every piece of data that enters or leaves a computer network must go via the firewall.
* If the data packets are safely routed via the firewall, all of the important data remains intact.
* A firewall logs each data packet that passes through it, enabling the user to keep track of all network activities.
* Since the data is stored safely inside the data packets, it cannot be altered.
* Every attempt for access to our operating system is examined by our firewall, which also blocks traffic from unidentified or undesired sources.

[**ENDPOINTS**](https://www.geeksforgeeks.org/endpoints-in-wireshark/)

* An “Endpoint” in simple terms is the logical endpoint that communicates back and forth with a network to which it is connected.
* It refers to a unit at the end of a communication channel.
* These are designed to perform specific or limited functions. In a network, it is the logical endpoint of separate protocol traffic of a specific protocol layer.

[**DMZ**](https://www.geeksforgeeks.org/what-is-demiltarized-zone/)

* Demilitarized Zones (DMZ) are used in cybersecurity.
* DMZs separate internal networks from the internet and are often found on corporate networks.
* A DMZ is typically created on a company’s internal network to isolate the company from external threats.
* While the name might sound negative, a DMZ can be a helpful tool for network security.
* The DMZ is a network barrier between the trusted and untrusted networks in a company’s private and public networks.
* The DMZ acts as a protection layer through which outside users cannot access the company’s data.
* DMZ receives requests from outside users or public networks to access the information and website of a company.
* For such type of request, DMZ arranges sessions on the public network. It cannot initiate a session on the private network.
* If anyone tries to perform malicious activity on DMZ, the web pages are corrupted, but other information remains safe.
* The goal of DMZ is to provide access to the untrusted network by ensuring the security of the private network.
* DMZ is not mandatory, but a better approach is to use it with a firewall.