Department of Information Technology

Chandigarh Engineering College
Landran, Mohali

Assignment no. - 1

Subject :- Routing & Switching

Subject Code :- BTEC905A-18

Name - Aditya Prabhakar

Roll no - 2102560

Course - B.tech / IT

Semester - 7th

Submitted to :-

Astha Gupta

Examine the role of network address translation. List out four translation method in detail.

Ans: Network Address Translation (NAT) - is a crucial networking technique used in router and firewalls to modify network address information while in transit. It primarily serves two purposes: Conserving IPv4 addresses and enhancing network security by acting as a barrier between the internal network and the external internet. NAT allows multiple devices in a local network to share a single public IP address. Here are four common methods of NAT in detail.

1) Static NAT (Network Address Translation):

- Description: Static NAT is one-to-one mapping method. It assigns a specific private IP address to a specific public IP address, ensuring a consistent mapping relationship.
- Use Case: Static NAT is typically used when a specific internal device (eg. a web server) needs to accessible from the internet with a fixed public IP address

- Advantages - Offers predictability and security, as the mapping is fixed and known in advance.

- Disadvantages - Inefficient in terms of address conservation, as it requires a public IP address for each internal device that need external access.

2) Dynamic NAT:

- Description - Dynamic NAT maps multiple internal IP addresses to a pool of public IP addresses. It assigns a public IP address dynamically from the pool when an internal device initiates an outgoing connection.

- Use case - Dynamic NAT is suitable for organization with a limited pool of public addresses where devices in the internal network need internet access but don't require fixed public IP's.

Advantages - Efficient use of public IP addresses as provides a degree of security as external host can not initiate connection to internal devices

Disadvantages :- Can lead to port exhaustion if the pool of public IP's is too small. It also lacks predictability for incoming connections.

3) PAT (Port Address Translation) or NAT overload :

> Description :- PAT is an extension of dynamic NAT that uses both IP addresses and port numbers to uniquely identify connections. It allows multiple internal devices to share a single public IP address by using different port numbers.

- Use Case :- PAT is commonly used by home and small office routers to enable multiple devices to access the internet using a single public IP address.

- Advantages :- Highly efficient in conserving public IP addresses and offers good security by masking ports along with IP addresses.

Disadvantages :- May have limitations in handling large no. of concurrent connections due to port exhaustion.

≥ NAT 64 C Network Address translation IPv6 to IPv4/6er

Description NAT64 is a specified form of NAT used to enable communication between IPv6-only and IPv4-only devices. It translate IPv6 addresses and packets into IPv4 addresses and packets.

Used Case : As the world transitions to IPv6, NAT 64 facilitates communication between IPv6 network legacy IPv4 network.

Advantages - Facilitates the co-existance IPv4 and IPv6 networks during the transition period.

Disadvantages - May introduced complexity and performance overhead, and certain application may not work seamlessly through NAT 64.

Q2:- Identify the need of using framing in computer networks. Categorize the different types of framing protocol with their format.

Ans:- Framing is a crucial process in computer networks that involves breaking up a stream of bits into manageable frames or packets for transmission and reception. Framing serves several essential needs in computer networks:

1) Frame Delimitation:- Framing defines the boundaries of individual frames within a continuous stream of data. This allows receiving devices to identify start & end of each frame, ensuring accurate data extraction.

2) Error detection:- By dividing data into frames, framing protocols can include error-checking mechanisms such as checksums or CRC codes in each frame.

3) Flow Control:- Framing helps in flow control by specifying the size of each frame. This allows the sender to regulate the rate of data transmission to match the receiver's capacity, preventing data overfl

- Multiplexing :- In many network scenarios multiple data streams need to be sent over a shared communication medium.

- Addressing :- Framing often includes addressing information, such as source & destination addresses to ensure that frames reach their intended recipients in multi-node network

Now, lets categorize different types of framing protocols along with their protocols or formats.

1) Character-Oriented Framing -

Format :- In character Oriented framing each frame begins & end with special characters (\$, & eg start & stop bits or control characters). This format is commonly used in asynchronous serial communication)

eg :- Asynchronous Transfer Mode (ATM)

1) Bit-Oriented framing.

Formal: Bit-Oriented framing does not rely on special characters but uses bit patterns to delineate frames. A common approach is to use a specific bit sequence (eg. flag or sync bits) to indicate start & end of frames.

Eg: HDLC (High level Data Link Control) and its variants, such as Synchronous Data link Control (SDLC) and frame relay.

2) Byte-Oriented Framing

Formal: Byte-oriented framing uses fixed-size fields to specify the frame length and address information. It often includes a frame header and frame trailer for error detection checking.

Eg: Ethernet frames, including IEEE 802.3 and Ethernet II, use byte-oriented framing. These frames typically consist of a preamble, destination & source MAC addresses, type or length

field, data payload, and Frame Checking sequence (FCS).

4) Frame Relay (Frame Switched) Framing :-

Format : Frame Relay framing is a form of frame switched framing. It uses addressable frames, and each frame has a data link connection identifier (DLCI) to identify the virtual circuit.

Eg :- Frame Relay is a packet switched WAN technology that uses DLCIs for frame identifications.

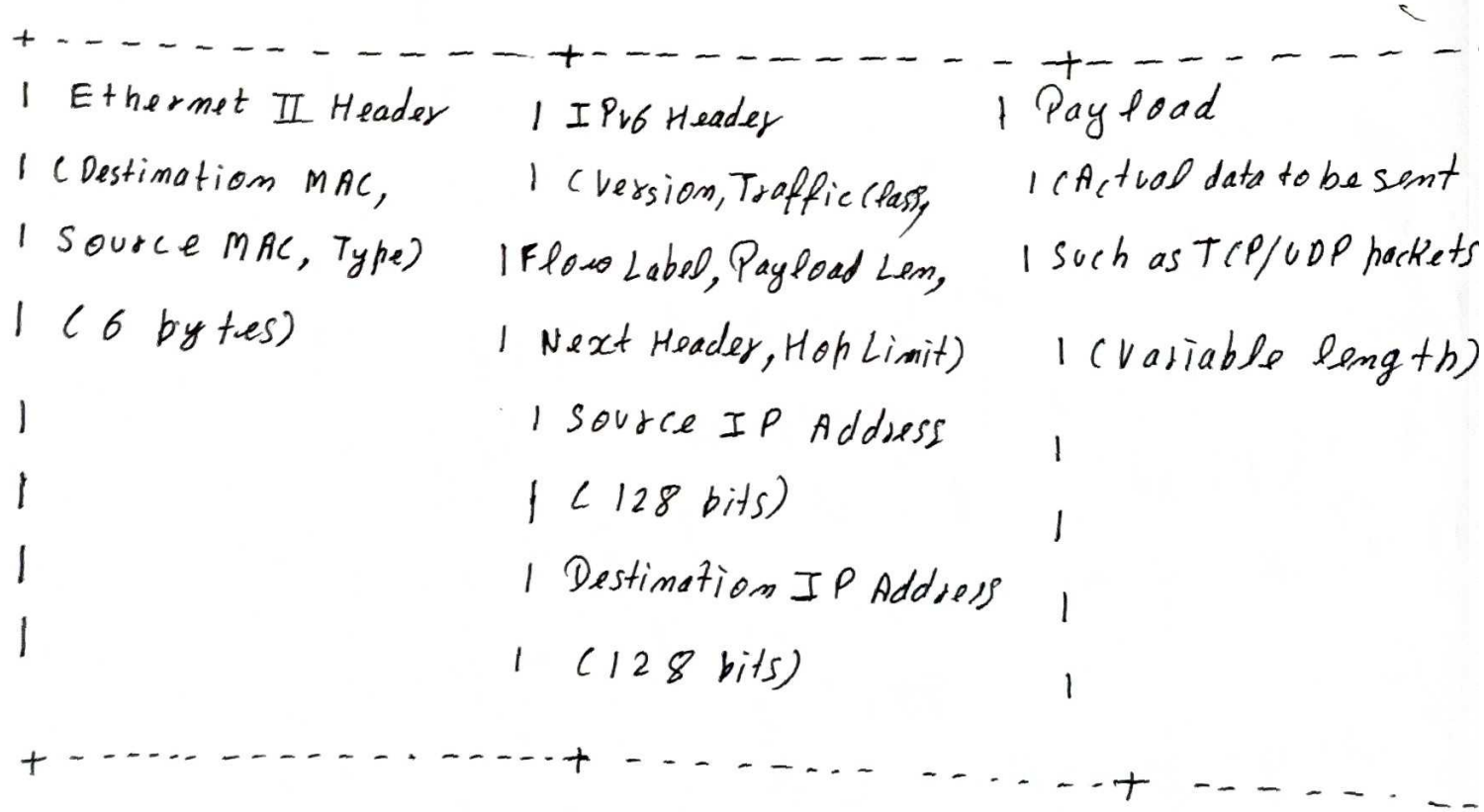
5) Asynchronous Transfer Mode (ATM) framing :-

Format :- ATM framing uses fixed size cells of 53-bytes, consisting of a 5 bytes header and a 48 byte payload. The payload can carry various types of data, including voice, video, and data.

Eg :- ATM networks used cell based framing and with fixed size ATM cell.

Q3:- Construct the IPV6 frame format. Compile minimum four advantages (1+1) of IPv6 over IPv4.

Ans:- The IPv6 (Internet Protocol version 6) frame format is designed to support the transmission of IPv6 packets over various network technologies. Unlike IPv4, IPv6 frame format is typically used within Data link layer protocols, such as Ethernet. Here is the basic structure of an IPv6 frame format.



Now let's discuss the four major advantages of IPv6 over IPv4.

1) Large Address Space (1st Advantage):

IPv6 provides a significantly large address space compared to IPv4. IPv4 uses 32-bit addresses allowing for approximately 4.3 billion unique addresses, which has been exhausted in many regions. In contrast IPv6 uses 128-bit addresses, offering approximately 340 undecillion (3.4×10^{38}) unique addresses. This abundance of addresses ensures that IPv6 can accommodate the growing number of devices and networks in the future.

2) Efficient Routing and Aggregation:

IPv6 simplifies routing by reducing the need for complex network address translation (NAT) and private address ranges which are common in IPv4. With its hierarchical addressing structure IPv6 allows for more efficient routing and aggregation of IP prefixes. This enhances the scalability and performance of the global internet.

Q4 :- Continue Link - 1 1 . . .

Enhanced Security :- . IPv6 includes built-in support for IPsec (Internet protocol security), which provides enhanced security features such as authentication and encryption at the network layer. While IPsec can be used with IPv4, it is not mandatory, leading to inconsistent implementation.

Simplified Network Configuration :-

IPv6 simplifies network configuration through features like stateless address auto configuration (SLAAC). With SLAAC, devices can automatically generate and configure their IPv6 addresses without relying on DHCP (Dynamic Host Configuration protocol). This simplifies network administration and reduce the need for manual IP address assignment.

These are some of the advantages of IPv6 over IPv4 address.

Q4 :- Compare Link state and distance vector routing protocol. Explain the steps involved in link state and distance vector routing protocol.

Ans:- Link state routing protocol and Distance vector routing protocol are two fundamental approaches routing in computer networks. Lets compare these two routing protocols and explain the steps involved in each :-

Distance Vector Routing	Link State Routing
1) Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth is required more due to flooding and sending of large link state packets
2) Based on local knowledge, since it updates table based on information from neighbors	Base on Global knowledge it have knowledge about entire network.
3) Make use of Bellman ford Algorithm.	Make use of Dijkastra's Algorithm.
4) Traffic is less	Traffic is more
5) Count of infinity problems.	No count of infinity problems.

	converges slowly i.e, good news spread fast and bad news spread slowly.	Converges faster.
7)	Persistent looping problem i.e loop will be formed.	No persistent loops, only transient loops
8)	Practical implementation is RIP and IGRP.	Practical implementation is OSPF and ISIS.

- Steps involved in link state Routing :-

:) Initialization :

. Routers starts with no information about the network.

:) They discover neighbouring routers and their link states.

- Link state Advertisement (LSA) Generation :

- Each router generates LSA's containing information about its local links and their states.

:) LSA include the router's unique identifier (Router ID).

Flooding:

- Router floods their LSA's throughout the network to inform all routers.
- Each router updates its link state database (LSDB) with received LSA's.

- Dijkastra's Algorithm:
  - Routers run Dijkastra's algorithm on the LSDB to compute the shortest path tree.
  - This tree represents the best path to each destination.

- Routing Table calculation:
  - Routers use the shortest path tree to calculate their routing tables.
  - The routing table specifies the next-hop router for each destination.

Steps involved in Distance Vector routing:

1. Initialization:
   - Routers starts with an empty routing table or an initial set of routers.
   - They exchange their routing tables with immediate neighbours.

- **Distance Vectors Updates**

- Routers periodically send their routing table to their neighbors.

> Each routing table entry includes the destination, the distance (metric) and the next-hop router.

- **Bellman-Ford Algorithm**:

Routers use the received routing tables to apply the Bellman-Ford Algorithm.

: They update their own routing tables based on the minimum cost-path to each destination.

- **Routing Table calculation**:

- Routers use the updated routing table to determine the best path for forwarding packets to each destination.

Q5 :- Outline different techniques & principles used in construction of a network.

Ans:- The construction of a network involves various techniques and principles to design, implement, and maintain a functional and efficient network infrastructure. Here is an outline of different techniques and ~~front~~ principle used in network construction.

1.) Network topology :-

- Choose an appropriate network topology (eg. star, ring, mesh, bus, Hybrid) that suits the organization's requirement and constraints.
- Consider factors like scalability, fault tolerance and cost of management when selecting a topology.

2) IP addressing and Subnetting :-

- Plan and allocate IP addresses and subnets systematically to ensure efficient address utilization & minimize IP conflicts
- Implement subnetting to divide large IP address range into smaller, manageable segments.

Routing & Switching - Design and configure routers and switches to enable efficient data forwarding and traffic routing within the network

Implement Dynamic routing protocols i.e (OSPF, BGP) and VLANs (Virtual LANs) for network segmentation & routing.

- Cabling & Physical Infrastructure :
- Select appropriate cabling types i.e (~~Ethernet~~ Ethernet, Fiber Optic) and design the physical layout of cables to ensure reliability & high speed data transmission.
- Considers factor's like cable length limitation & cable management for neat & ~~organization~~ organized installation.

- Network Security
- Implement security measures like firewalls, intrusion detection & prevention system, (IDS/IPS), and access controls to protect the network from unauthorized access & threats.

7) Quality of service

- Prioritize network traffic using QoS techniques to ensure that critical applications receives the necessary bandwidth and lowers for priority traffic doesn't consume excessive resources

- Implement traffic shaping queuing mechanisms to manage network congestion

8) Redundancy & High Availability :-

Incorporate redundancy at various levels (eg, hardware, links, data-centers) to ensure network availability in the event of failures

- Implement techniques like load balancing & failover mechanisms to distribute traffic and maintain uptime

8) Scalability & Capacity Planning :

- Plan for future growth and scalability by selecting network hardware & configurations that can accomodate increased traffic and devices.
- Monitor network performance and utilization to identify and address capacity bottlenecks proactively.

9) Network Monitoring & Management.

- Deploy network monitoring tools & systems to continuously monitor network performance, Identify issues and troubleshoot problems.

10) Documentation and Labeling:

- Maintain detailed documentation of network configuration, IP addresses, hardware inventory, and trouble shooting procedure.
- Label network devices & cables for easy identification and ~~trob~~ trouble shooting.

11) Disaster Recovery & Backup.

Establish disaster recovery plan & Backup strategies to recover data & network functionality in case of unforeseen events like hardware failures natural disasters, or cyber attacks.

12) Compliance and Regulations -

Ensure that the network infrastructure complies with relevant industry standards and regulations specially in sectors with specific compliance requirements (eg Healthcare, finance.)

12) User Training & Support :

Establish a helpdesk or support system for addressing user issues and enquiries.

14) Budget & Cost Management

- Optimized costs while maintaining network performance & security.

15) Lifecycle Management :

Develop a network lifecycle management strategy that includes planning, design, implementation, maintenance & eventual decommissioning of network components.

These are some of the basic principles to establish a good and secure network infrastructure.