Computer Network & Network Design (IAE - II)

> *CONTENT WARNING:*
> *READING THIS DOCUMENT MAY CAUSE SUDDEN BURSTS OF INTELLIGENCE.*
> *PROCEED WITH CAUTION.*

1. a) IPv4 vs IPv6

Aspect	IPv4	IPv6
Address Length	32 bits (4 bytes)	128 bits (16 bytes)
Address Format	Four octets, separated by dots (e.g., 192.168.1.1)	Eight groups of four hexadecimal digits, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
Address Space	Limited to around 4.3 billion unique addresses (2^32)	Vast address space (2^128) – 340 undecillion addresses
Header Complexity	More complex header structure with options (e.g., checksum, length, etc.)	Simplified header with fewer fields, making it more efficient for processing
Configuration	Requires manual configuration or DHCP	Supports auto-configuration (Stateless Address Autoconfiguration)
NAT (Network Address Translation)	Often used to deal with address shortage	Designed to avoid the need for NAT, as the address space is large enough
Security	Security is optional (IPsec not mandatory)	Security is built-in, and IPsec is mandatory
Broadcast	Supports broadcast communication	Does not support broadcast; uses multicast and anycast instead
Transition	Already widely deployed, but has limitations due to address exhaustion	Not widely deployed yet, but future-proof with a larger address space
Routing	Routing can be inefficient due to limited address space and subnetting	More efficient routing due to a larger address space and hierarchical addressing

1. b) Lossy Compression vs Lossless Compression

Aspect	Lossy Compression	Lossless Compression
Data Retention	Some data is lost during compression (irreversible)	No data is lost; original data can be perfectly restored
Quality	Reduces quality to achieve higher compression ratios (e.g., slight loss in image/audio quality)	Maintains full quality of the original data
Compression Ratio	Higher compression ratio, leading to smaller file sizes	Lower compression ratio compared to lossy methods
Use Cases	Common in multimedia (e.g., images, videos, audio, etc.)	Used for text files, documents, source code, software, etc.
Examples	JPEG (images), MP3 (audio), MPEG (video)	ZIP, PNG, FLAC, GIF, TIFF
Reversibility	Irreversible; once compressed, quality can't be fully restored	Reversible; the original data can be fully recovered
Speed	Faster compression and decompression times	Slower compression and decompression, but lossless
File Size	Typically smaller due to higher compression	Larger file sizes compared to lossy compression

2. What is NAT?

NAT (Network Address Translation) is a technique used in networking where private IP addresses (which are not globally routable) are translated into a public IP address when sending packets to the internet. This helps conserve public IP addresses and allows multiple devices on a local network to share a single public IP address.

Types of NAT:

1. **Static NAT**: A one-to-one mapping between a private IP and a public IP.
2. **Dynamic NAT**: A private IP is mapped to a pool of public IPs.
3. **PAT (Port Address Translation)**: A form of NAT where multiple devices are mapped to a single public IP address but with different port numbers.

Benefits:

- Saves IP address space.
- Provides security by hiding internal IP addresses from the external network.

Congestion Control

Congestion control refers to techniques used in networking to prevent network congestion, which occurs when too much data is sent over a network, causing delays and packet loss. It involves controlling the rate at which data is sent to avoid overwhelming the network.

Common Congestion Control Algorithms:

1. **TCP Congestion Control** (such as slow start, congestion avoidance, and fast retransmit).
2. **Active Queue Management** (e.g., RED - Random Early Detection).

Key Mechanisms:

- **Flow Control**: Manages how much data a sender can send before waiting for acknowledgment.
- **Congestion Window**: TCP uses this to control the amount of data in transit.

UDP Header Format

The **UDP (User Datagram Protocol)** header is simple and does not include features like flow control or error correction, unlike TCP. It consists of the following fields:

Field	Size	Description

Source Port	16 bits	The port number of the sender.
Destination Port	16 bits	The port number of the receiver.
Length	16 bits	The length of the UDP header and data in bytes.
Checksum	16 bits	Optional field used for error-checking the header and data.
Data	Variable	The payload or message data being sent.

UDP is a connectionless protocol, meaning it does not establish a connection before sending data.

Leaky Bucket

The **Leaky Bucket** algorithm is a traffic shaping mechanism used to control the rate at which data packets are transmitted over a network. It is used to smooth out bursty traffic into a steady flow.

- **Bucket**: The bucket represents a fixed capacity buffer.
- **Leaky**: The bucket leaks out data at a constant rate (steady rate).
- **Overflow**: If data is sent too quickly and the bucket overflows, packets are discarded or delayed.

The leaky bucket algorithm is useful in scenarios like rate-limiting or controlling the bandwidth used by a network connection.

UDP Applications

UDP is used in applications where speed is more important than reliability. It is used in scenarios where small amounts of data need to be transmitted quickly, and the application can handle any loss or corruption of data.

Common UDP Applications:

1. **DNS (Domain Name System)** - Resolves domain names into IP addresses.

2. **VoIP (Voice over IP)** - Allows for voice communication over the internet (e.g., Skype, WhatsApp).
3. **Streaming Media** - Live video/audio streaming (e.g., YouTube, Netflix).
4. **Online Gaming** - Fast-paced games requiring real-time transmission of data.

UDP is ideal for applications where low latency and real-time performance are more important than ensuring every packet is successfully received.

RPC (Remote Procedure Call)

RPC is a protocol that allows a program to execute a procedure (subroutine) on another machine within a shared network, as if it were a local procedure call. It abstracts the communication between the client and server, making remote interactions appear like local function calls.

- **Client-side Stub**: The client sends the request for the procedure to be executed.
- **Server-side Stub**: The server receives the request and executes the procedure.

RPC is widely used in client-server architectures and distributed systems.

RLE (Run-Length Encoding)

RLE (Run-Length Encoding) is a simple form of data compression where consecutive identical data elements (runs) are stored as a single data value and count. This is effective for compressing data with long runs of repeated characters or values.

Example:

- Input: `AAAABBBCCDAA`
- Output: `4A3B2C1D2A`

RLE is commonly used in image compression (e.g., TIFF format) and simple text encoding.

DNS (Domain Name System)

DNS (Domain Name System) is the system that translates human-readable domain names (e.g., www.example.com) into machine-readable IP addresses (e.g., 192.0.2.1). It acts as a "phonebook" for the internet.

DNS Structure:

1. **DNS Resolver**: Resolves the domain name by contacting DNS servers.
2. **DNS Server**: Stores records like A (address), MX (mail exchange), and CNAME (canonical name) records.

DNS Process:

1. A user types a URL into their browser.
2. The browser queries a DNS server to resolve the domain name to an IP address.
3. The DNS server returns the corresponding IP address, and the browser connects to the web server.

3. FTP (File Transfer Protocol)

FTP (File Transfer Protocol) is a standard network protocol used to transfer files between a client and a server over a TCP-based network. FTP can be used for both uploading files from a local system to a server or downloading files from a server to a local system.

Key Features:

- **Client-Server Model**: FTP works based on a client-server model, where the client initiates the connection and the server listens for requests.
- **Port Numbers**:
  - **Control Port**: FTP uses port 21 for control commands (commands to manage the connection).
  - **Data Port**: FTP uses port 20 for transferring data (files).
- **Modes**:
  - **Active Mode**: The server opens a random port to send data to the client.
  - **Passive Mode**: The client opens a random port to receive data from the server (used to navigate firewalls).
- **Authentication**: FTP often requires a username and password for access, though **Anonymous FTP** is available for publicly accessible files.

Command Examples:

- `GET` and `PUT`: Commands used to download and upload files.
- `LIST`: Lists files and directories on the server.

SNMP (Simple Network Management Protocol)

SNMP (Simple Network Management Protocol) is an Internet standard protocol used for monitoring and managing devices on a network, such as routers, switches, servers, and printers. SNMP allows network administrators to track the performance, uptime, and status of network devices.

Key Components:

1. **Managed Devices**: Devices on the network (routers, switches, etc.) that are being monitored.
2. **SNMP Agents**: Software running on the managed device that collects and stores data, and responds to SNMP queries.

3. **Network Management Systems (NMS)**: Software that collects data from SNMP agents, processes it, and provides a user interface for managing the devices.

Operations:

- **GET**: Request data from a managed device.
- **SET**: Modify a device's settings or configurations.
- **TRAP**: The agent sends unsolicited notifications (traps) to the NMS about an event or change in status (e.g., failure, error).
- **Walk**: Retrieve a series of related data points from the device (e.g., system statistics).

Versions:

1. **SNMPv1**: Original version, lacks strong security features.
2. **SNMPv2**: Improved performance, but still had security limitations.
3. **SNMPv3**: Includes robust security features (authentication and encryption).

HTTP (HyperText Transfer Protocol)

HTTP (HyperText Transfer Protocol) is the foundational protocol used for transmitting web pages and other resources over the internet. It defines the rules for communication between web browsers (clients) and web servers, allowing users to request web pages and receive them in return.

Key Features:

- **Request-Response Model**: HTTP follows a client-server communication model. The client (browser) sends an HTTP request to the server, and the server responds with the requested content.
- **Stateless**: HTTP is a stateless protocol, meaning each request is independent and has no knowledge of previous requests.
- **HTTP Methods**:

    - **GET**: Request to retrieve data from the server (e.g., web page).
    - **POST**: Send data to the server (e.g., form submission).
    - **PUT**: Update data on the server.
    - **DELETE**: Delete data from the server.
- **HTTP Status Codes**: Responses from the server, such as:
    - `200 OK`: The request was successful.
    - `404 Not Found`: The requested resource was not found.
    - `500 Internal Server Error`: A server-side error occurred.

HTTP Versions:

1. **HTTP/1.1**: The widely used version with improvements over HTTP/1.0.
2. **HTTP/2**: A more efficient version, allowing multiplexing, header compression, and prioritization.
3. **HTTP/3**: The latest version, which uses QUIC (Quick UDP Internet Connections) for faster, more secure connections.

OSPF (Open Shortest Path First)

OSPF (Open Shortest Path First) is a link-state routing protocol used within an Autonomous System (AS) to determine the best path for data to travel across the network. OSPF is widely used in large enterprise networks and is designed to be more scalable and efficient than other routing protocols like RIP (Routing Information Protocol).

Key Features:

- **Link-State Protocol**: OSPF routers exchange information about the state of their links (connections) with other routers in the network. Each router builds a map of the network and uses it to calculate the shortest path to all other routers using **Dijkstra's Algorithm**.

- **Cost Metric**: OSPF uses cost as the metric for determining the best path. The cost is typically based on bandwidth, with lower-cost paths being preferred.
- **Hierarchical Design**:
  - **Areas**: OSPF networks are divided into areas for better scalability. Each area has a backbone (Area 0) that connects all other areas.
  - **ABR (Area Border Router)**: Routers that connect different areas of the network.
- **LSA (Link-State Advertisements)**: Routers share information about the network topology using LSAs to keep the routing table up-to-date.
- **Fast Convergence**: OSPF reacts quickly to network changes (such as link failures), allowing for faster reconvergence compared to protocols like RIP.

OSPF Process:

1. **Neighbor Discovery**: OSPF routers discover and establish neighbor relationships.
2. **LSA Exchange**: Routers exchange link-state advertisements to update their routing tables.
3. **Shortest Path Calculation**: Routers calculate the best path to each destination based on the received LSAs.

Advantages:

- Efficient and scalable.
- Supports hierarchical network designs.
- Converges quickly when there are network changes.

4. a) IPv6 Header, TCP Headers, IPv4

IPv6 Header:
The IPv6 header is simplified compared to IPv4. It consists of the following fields:

Field	Size	Description
Version	4 bits	IPv6 version (always `6` for IPv6).
Traffic Class	8 bits	Used for differentiated services (Quality of Service).
Flow Label	20 bits	Used for labeling packets belonging to the same flow.
Payload Length	16 bits	Length of the data being carried by the packet.
Next Header	8 bits	Identifies the next protocol (e.g., TCP, UDP, ICMP).
Hop Limit	8 bits	Limits the number of hops the packet can make.
Source Address	128 bits	The 128-bit IPv6 address of the sender.
Destination Address	128 bits	The 128-bit IPv6 address of the receiver.

IPv4 Header:
IPv4 header is more complex and consists of the following fields:

Field	Size	Description
Version	4 bits	IPv4 version (always `4` for IPv4).
IHL (Header Length)	4 bits	Length of the header in 32-bit words.
Type of Service (TOS)	8 bits	Specifies the quality of service (QoS).
Total Length	16 bits	Total length of the IPv4 packet (header + data).
Identification	16 bits	Unique identifier for fragmentation.
Flags	3 bits	Flags indicating whether fragmentation is allowed.
Fragment Offset	13 bits	Position of fragmented data in the original packet.
TTL (Time to Live)	8 bits	Limits the lifespan of the packet.

Field	Size	Description
Protocol	8 bits	Specifies the higher-level protocol (TCP, UDP, etc.).
Header Checksum	16 bits	Ensures integrity of the header data.
Source Address	32 bits	Sender's IP address.
Destination Address	32 bits	Receiver's IP address.
Options	Variable	Optional fields (e.g., security, timestamp).
Padding	Variable	Ensures the header is a multiple of 32 bits.

TCP Header:
The TCP header is used for reliable communication and contains the following fields:

Field	Size	Description
Source Port	16 bits	Port number of the sending application.
Destination Port	16 bits	Port number of the receiving application.
Sequence Number	32 bits	Number used to track the sequence of the sent data.
Acknowledgment Number	32 bits	If ACK is set, this field contains the next expected sequence number.
Data Offset	4 bits	The length of the TCP header.
Reserved	3 bits	Reserved for future use.
Flags	9 bits	Contains control flags like SYN, ACK, FIN, etc.
Window Size	16 bits	Specifies the size of the sender's window for flow control.
Checksum	16 bits	Error-checking for the header and data.
Urgent Pointer	16 bits	Indicates if the data is urgent (when URG flag is set).
Options	Variable	Optional fields used for various features (e.g., MSS).
Data	Variable	Actual data being transmitted.

4. b) Distance & Link-State Routing

Distance-Vector Routing:

- **Concept**: Each router maintains a table (vector) with the shortest known distance to every other router in the network.
- **How It Works**: Routers share their routing tables with their neighbors, and each router updates its table based on the received information.
- **Algorithm**: Common distance-vector protocols include **RIP (Routing Information Protocol)**.
- **Drawback**: Slower convergence and prone to routing loops (e.g., count-to-infinity problem).

Link-State Routing:

- **Concept**: Routers maintain a map of the network topology (link-state database) and use it to compute the shortest path to each destination using an algorithm like **Dijkstra's**.
- **How It Works**: Each router periodically sends out updates to all routers in the network, containing information about its directly connected links.
- **Algorithm**: Common link-state protocols include **OSPF (Open Shortest Path First)**.
- **Advantages**: Faster convergence and better scalability compared to distance-vector routing.

4. c) Image Compression: GIF & JPEG

GIF (Graphics Interchange Format):

- **Compression Type**: Lossless compression.
- **Color Depth**: Supports up to 256 colors.

- **Use Cases**: Best for simple images, logos, animations, and graphics with flat colors.
- **File Size**: Often larger due to the color limitation and the use of lossless compression.
- **Animation**: Supports simple animations.

JPEG (Joint Photographic Experts Group):

- **Compression Type**: Lossy compression.
- **Color Depth**: Can support millions of colors, making it ideal for photographs.
- **Use Cases**: Best for photographs and complex images where slight quality loss is acceptable.
- **File Size**: Generally smaller than GIF due to lossy compression.
- **Animation**: Does not support animations.

4. d) TCP Congestion Control

TCP Congestion Control is used to avoid network congestion and ensure efficient transmission of data. It employs several algorithms to manage how data is sent and to adjust the rate based on network conditions.

Main Algorithms:

1. **Slow Start**: Initially, the congestion window size (cwnd) is small. The sender increases the window size exponentially until it reaches a threshold.
2. **Congestion Avoidance**: After slow start, TCP increases the cwnd linearly (additive increase) to avoid congestion.
3. **Fast Retransmit**: If a packet is lost, it is retransmitted immediately after receiving three duplicate ACKs.
4. **Fast Recovery**: After fast retransmit, TCP enters fast recovery to avoid reducing the congestion window drastically.

Key Terms:

- **Congestion Window (cwnd)**: The sender's buffer size, which limits the number of packets in transit.
- **Threshold (ssthresh)**: The point at which TCP switches from exponential growth (slow start) to linear growth (congestion avoidance).

4. e) TCP Timers

TCP Timers are used to manage various aspects of the TCP protocol, such as retransmissions and connection timeouts.

1. **Retransmission Timer**: Ensures that unacknowledged packets are retransmitted after a timeout period.
    - If no ACK is received for a segment, TCP will retransmit it after the timeout.
2. **Persist Timer**: Keeps the connection open if the window size is 0, preventing the sender from stopping and waiting for the receiver's buffer to become available.
3. **Keep-Alive Timer**: Used to check the status of a connection by sending probes to the peer when there is no data transfer for a certain period.
4. **Time-Wait Timer**: Ensures that the receiver has received all segments of a connection before closing.

4. f) Connectionless and Connection-Oriented Services

Connectionless Service:

- **Description**: A communication model where there is no setup of a dedicated path between the sender and receiver before data transfer. Each packet is treated independently.
- **Example Protocol**: **UDP (User Datagram Protocol)**.
- **Characteristics**:

- No handshaking between sender and receiver.
- No guaranteed delivery or ordering of packets.
- Faster but less reliable.

Connection-Oriented Service:

- **Description**: A communication model where a connection is established between the sender and receiver before data transfer. The connection ensures that data is delivered reliably and in order.
- **Example Protocol**: **TCP (Transmission Control Protocol)**.
- **Characteristics**:
  - Connection is established via a handshake (e.g., three-way handshake in TCP).
  - Ensures reliable delivery, ordering, and error checking.
  - Slower but more reliable.

NOTE: THIS IS NOT FINALIZED YET, SOME REFINEMENTS WILL BE MADE.