Data Centre

Data Centre: Data centers are specialized facilities designed to house computer systems and associated components, such as telecommunications and storage systems. They are essential for various reasons:

1. **Centralized Control:** Data centers help companies manage all their IT resources in one place. This makes it easier to maintain and update systems.
2. **Adaptability:** They can easily grow to accommodate increasing demands. If a website becomes popular, a data center can quickly add more servers to handle the extra traffic.
3. **Reliability and Backup:** Data centers have backup systems to prevent downtime. If one server fails, another can take its place.
4. **Security:** They have strict security measures to protect sensitive data from hackers and other threats.
5. **Energy Efficiency:** Modern data centers use energy-efficient technologies to reduce their environmental impact.

Step-by-Step Load Balancing Process

1. **Client Request**:

An external client sends a request to a publicly accessible IP address associated with an application.

2. **Load Balancer Receives Request**:

The request first reaches the load balancer, which is configured to handle traffic for specific applications.

3. **Load Assessment**:

The load balancer checks the current load on each host (server) that handles the application. This assessment includes metrics like CPU load, memory usage, and active connections.

4. **Routing Decision**:
Using a predefined algorithm (e.g., round-robin, least connections, or IP hash), the load balancer determines the optimal host to handle the incoming request.

5. **Forwarding the Request**:
The load balancer forwards the request to the selected host, translating the public IP address to the host's internal IP address.

6. **Host Processes Request**:
The chosen host processes the request, which may involve additional calls to other hosts or services.

7. **Response Sent to Load Balancer**:
Once processing is complete, the host sends the response back to the load balancer.

8. **Response Relay**:
The load balancer receives the response and translates the internal IP address back to the client's public IP address, then forwards the response to the client.

9. **Security Layer**:
Throughout the process, the load balancer prevents clients from accessing hosts directly, enhancing security by masking the internal network structure.

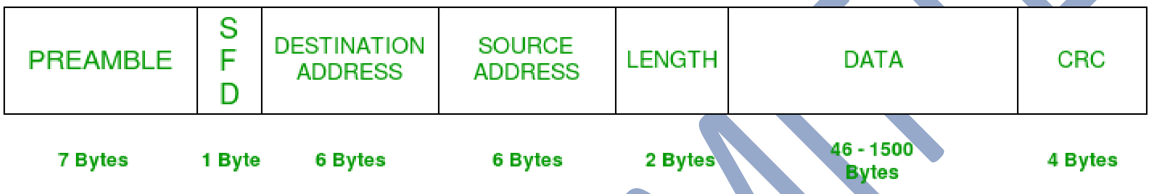
10. **Ongoing Load Monitoring**:
The load balancer continuously monitors the performance of each host and adjusts traffic distribution in real time based on current load conditions.

IEEE 802.3: This is the main set of standards governing Ethernet technology. It includes various specifications for different speeds and media types.

Common Types:

- **10BASE-T**: 10 Mbps over twisted pair cable.
- **100BASE-TX (Fast Ethernet)**: 100 Mbps, also over twisted pair.
- **1000BASE-T (Gigabit Ethernet)**: 1 Gbps over twisted pair.
- **10GBASE-T**: 10 Gbps over twisted pair.
- **100BASE-FX**: Fast Ethernet over fiber optics.
- **1000BASE-SX/LX**: Gigabit Ethernet over fiber optics.

Ethernet Frame Structure:



PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

IEEE 802.3 ETHERNET Frame Format

1. **PREAMBLE:** Ethernet frame starts with a 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allows sender and receiver to establish bit synchronization.

2. **Start of frame delimiter (SFD):** This is a 1-Byte field that is always set to 10101011. SFD indicates that upcoming bits are starting the frame, which is the destination address.

3. **Destination Address:** This is a 6-Byte field that contains the MAC address of the machine for which data is destined.

4. **Source Address:** This is a 6-Byte field that contains the MAC address of the source machine

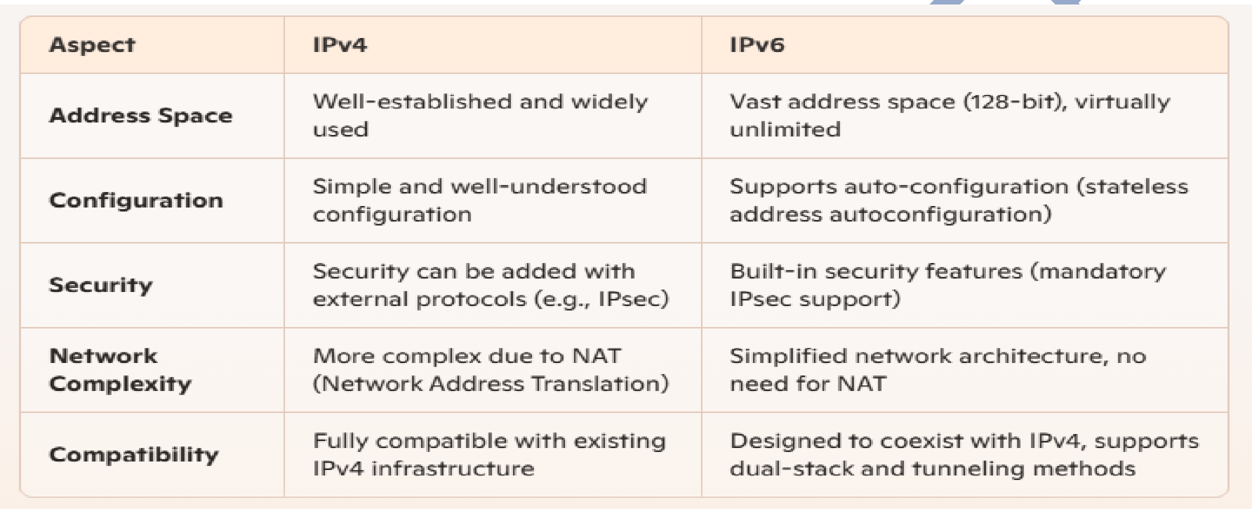
5. **Length:** Length is a 2-Byte field, which indicates the length of the entire Ethernet frame. This 16-bit field can hold a length value between 0 to 65535.

6. **Data:** This is the place where actual data is inserted, also known as **Payload** . Both IP header and data will be inserted here if Internet Protocol is used over Ethernet.

7. **CRC:** Cyclic Redundancy Check (CRC) is a powerful error detection method used in the Data Link Layer. CRC is highly effective in detecting various types of errors, including single-bit errors, burst errors, and many other error patterns. It's a crucial mechanism for ensuring reliable data transmission over networks.

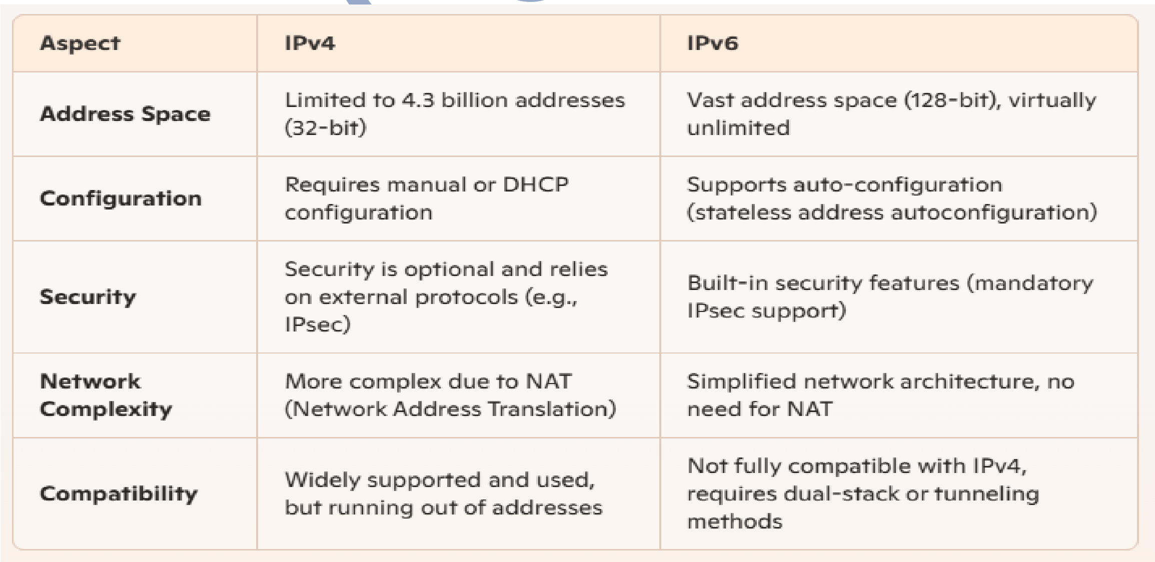
Network Layer

Advantages of IP4 and IP6



Aspect	IPv4	IPv6
Address Space	Well-established and widely used	Vast address space (128-bit), virtually unlimited
Configuration	Simple and well-understood configuration	Supports auto-configuration (stateless address autoconfiguration)
Security	Security can be added with external protocols (e.g., IPsec)	Built-in security features (mandatory IPsec support)
Network Complexity	More complex due to NAT (Network Address Translation)	Simplified network architecture, no need for NAT
Compatibility	Fully compatible with existing IPv4 infrastructure	Designed to coexist with IPv4, supports dual-stack and tunneling methods

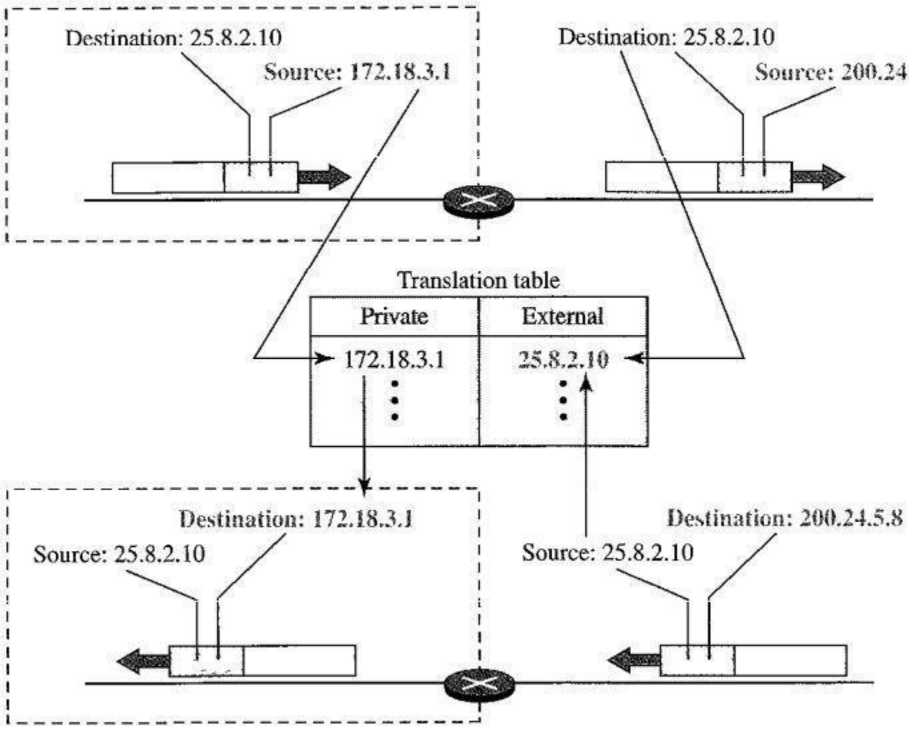
Limitations of IP4 and IP6



Aspect	IPv4	IPv6
Address Space	Limited to 4.3 billion addresses (32-bit)	Vast address space (128-bit), virtually unlimited
Configuration	Requires manual or DHCP configuration	Supports auto-configuration (stateless address autoconfiguration)
Security	Security is optional and relies on external protocols (e.g., IPsec)	Built-in security features (mandatory IPsec support)
Network Complexity	More complex due to NAT (Network Address Translation)	Simplified network architecture, no need for NAT
Compatibility	Widely supported and used, but running out of addresses	Not fully compatible with IPv4, requires dual-stack or tunneling methods

NAT- Network Address Translation

What is NAT: NAT stands for **Network Address Translation**. It’s a process used in computer networking that modifies **network address information** in the IP header of packets while they are in transit across a traffic routing device that is to translate Public IP to Private IP and vice versa. This is often used to allow multiple devices within a local network to share a single public IP address.



Where is it used?

NAT is commonly employed in home or office networks where several devices, like computers, smartphones, or tablets, need to access the internet using a single IP address provided by an internet service provider.

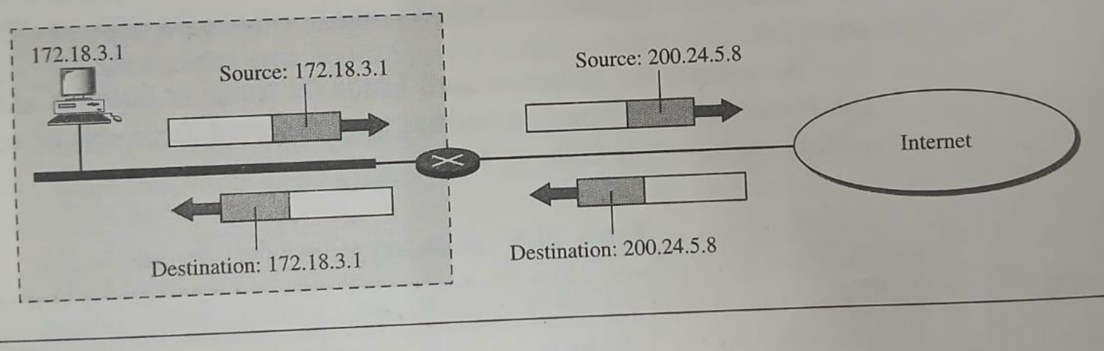
How does it Work??

Translation Process:

- **Outgoing Traffic**: When a device sends a request to the internet, the router captures the private IP address and the port number used by the device. It then replaces this information with its own public IP address and a unique port number, creating a mapping in its NAT table.

- **Incoming Traffic**: When the response returns from the internet, the router uses the mapping in its NAT table to translate the public IP and port back to the original private IP address and port, forwarding the data to the correct device

Figure 19.11 *Addresses in a NAT*



Why is a 5-column NAT table preferable over a 2-column table?

A **5-column NAT table** provides a more comprehensive view of network traffic and is better suited for complex scenarios, like handling multiple connections or differentiating between traffic types. Below are the comparisons:

Aspect	2-Column NAT Table	5-Column NAT Table
Structure	Source Private IP ↔ Translated Public IP	Source IP, Source Port, Destination IP, Destination Port, and Protocol
Details Stored	Only maps private and public IPs.	Tracks additional details like ports and protocols.
Port Translation	Limited to basic IP mapping.	Handles PAT (Port Address Translation), which allows multiple devices to share one public IP.
Use Case	Simple NAT scenarios.	Complex network environments, such as web servers and multi-user systems.

Network Congestion

Network Congestion: Network congestion occurs when the amount of data being transmitted exceeds the network's capacity, causing delays and packet loss. It typically arises from high traffic volume, inefficient routing, or insufficient bandwidth.

Key Effects of Network Congestion:

1. **Increased Latency:** Data takes longer to travel from source to destination.
2. **Packet Loss:** Some packets may be discarded, leading to retransmissions.
3. **Reduced Throughput:** The effective data transfer rate decreases, impacting performance.

Causes of Congestion:

- **High User Demand:** Many users trying to access the network simultaneously.
- **Insufficient Bandwidth:** The network cannot handle the amount of traffic.
- **Network Configuration Issues:** Poorly optimized settings can contribute to congestion.

Congestion Control Approaches:

End-to-End Congestion Control Procedure

1. **Connection Establishment**:
   - The sender and receiver establish a connection (e.g., using TCP's three-way handshake).
2. **Initial Transmission**:
   - The sender starts transmitting data using an initial congestion window size, which is often small.
3. **Monitoring Feedback**:
   - The sender monitors acknowledgments (ACKs) from the receiver. These ACKs inform the sender that packets have been successfully received.
   - If the sender does not receive an ACK for a packet within a certain timeframe (timeout), it assumes packet loss has occurred.

4. **Adjusting Transmission Rate**:
    - **Slow Start**: The sender exponentially increases the congestion window size for each ACK received until a threshold (slow start threshold) is reached.
    - **Congestion Avoidance**: Once the threshold is reached, the sender switches to linear growth of the congestion window to avoid further congestion.
    - **Fast Retransmit**: If the sender receives multiple duplicate ACKs (indicating a packet loss), it retransmits the lost packet immediately without waiting for a timeout.
    - **Fast Recovery**: After retransmitting, the sender reduces its congestion window and enters congestion avoidance mode to stabilize the transmission rate.
5. **Feedback Loop**:
    - The process continues, with the sender adjusting its transmission based on the feedback from the network (via ACKs or timeouts) to ensure it doesn't overwhelm the network.

Network-Assisted Congestion Control Procedure

1. **Packet Transmission**:

- Similar to end-to-end, the sender transmits packets to the receiver. However, network elements (routers and switches) monitor the state of the network.

2. **Network Monitoring**:

- Routers track metrics such as queue lengths and packet loss rates. Routers take action when congestion is detected (e.g., queues are filling up).

3. **Explicit Congestion Notification (ECN)**:

- Instead of dropping packets when congestion occurs, routers can mark packets with a congestion notification.

- This notification signals to the sender that the network is experiencing congestion.

4. **Feedback to Sender**:

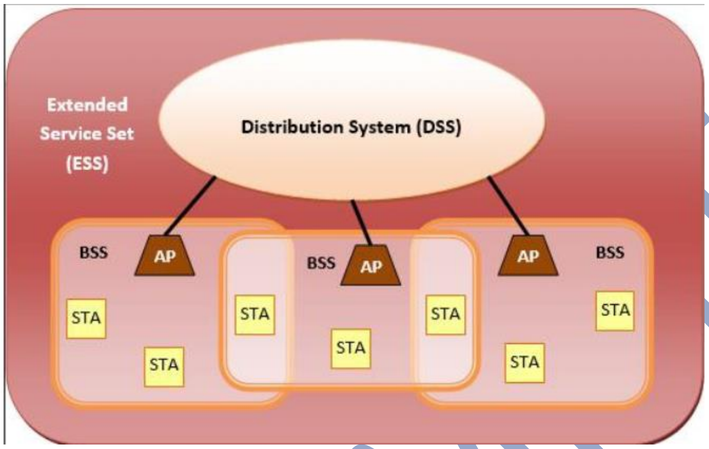
- When the sender receives a marked packet or feedback from the network, it adjusts its sending rate:

  Reduce Rate: The sender may decrease its congestion window or send fewer packets until congestion is alleviated

Wireless Network

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows



1. Stations (STA)

- **Wireless Access Point (WAP):** Also known as an access point (AP), it's like a central hub that connects devices to the network. Think of it as the main gateway to the internet.
- **Clients:** These are the devices that connect to the WAP, such as computers, laptops, smartphones, tablets, etc.

2. Basic Service Set (BSS)

- A BSS is a group of stations that communicate directly with each other.
- **Infrastructure BSS:** Devices communicate through a central access point. This is the most common type of wireless network, like your home Wi-Fi.
- **Independent BSS:** Devices communicate directly with each other in a peer-to-peer fashion, without a central access point. This is often used for temporary networks or in situations where an access point isn't available.

3. Extended Service Set (ESS)

- An ESS is a collection of multiple BSS connected together.
- This allows devices in different BSS to communicate with each other, creating a larger network.

4. Distribution System (DS)

- The DS is responsible for connecting the access points in an ESS.
- It ensures that data can be transmitted between devices in different BSS.

Cryptography

➢ Types and difference of Cryptography:

Cryptography can be broadly classified into several types based on the methods used to secure data. The two primary types are **Symmetric-key cryptography** and **Asymmetric-key cryptography**, along with other specialized techniques like **hashing** and **digital signatures**.

1. **Symmetric-Key Cryptography (Secret Key Cryptography)**

In symmetric-key cryptography, the **same key** is used for both encryption and decryption. This means that both the sender and the recipient must share the secret **key before communication can take plac**e. Symmetric-key cryptography is fast and efficient, making it ideal for encrypting large amounts of data.

- **Examples of Symmetric Algorithms**:
  - **AES (Advanced Encryption Standard)**
  - **DES (Data Encryption Standard)**
  - **RC4: Rivest Cipher 4**
  - **3DES (Triple DES): Triple Data Encryption Standard**

Advantages:

- Faster and more efficient, especially for encrypting large amounts of data.
- Suitable for bulk data encryption.

Disadvantages:

- Key distribution is a challenge, as the key must be securely shared between the parties involved.
- If someone steals the key, they can access the communication and break its security.

2. **Asymmetric-Key Cryptography (Public Key Cryptography)**

In **asymmetric cryptography**, there are two keys: a **public key** and a **private key**. The public key is used to encrypt the message, and the private key is used to decrypt it. The public key can be freely shared with anyone, while the private key must remain secret. This method allows secure communication between parties who have never shared a key in advance.

- **Examples of Asymmetric Algorithms**:
  - **RSA (Rivest-Shamir-Adleman)**
  - **ECC (Elliptic Curve Cryptography)**
  - **DSA (Digital Signature Algorithm)**

Advantages:

- Solves the problem of key distribution because only the public key is shared.
- Provides mechanisms for **digital signatures**, allowing for authentication and non-repudiation.

Disadvantages:

- Slower than symmetric-key encryption, which makes it less efficient for encrypting large volumes of data.
- Requires more computational resources.

Symmetric Key	**Asymmetric Key**
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other to decrypt.
The size of the ciphertext is the same or smaller than the original plaintext.	The size of the ciphertext is the same or larger than the original plaintext.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data needs to be transferred.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher

Symmetric Key	**Asymmetric Key**
In symmetric key encryption, resource utilization is low compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is lower as only one key is used for both encryption and decryption purposes.	Security is higher as two keys are used, one for encryption and the other for decryption.
Examples: 3DES, AES, DES and RC4	**Examples:** Diffie-Hellman, ECC, El Gamal, DSA and RSA