IP Packet

Header Fields

The IP packet header

The IP packet header is a fixed-length, 20-byte header that is added to the beginning of each IP packet. It contains several fields that are used to identify the source and destination of the packet, as well as other important information about the packet.

1. Version: This 4-bit field indicates the version of the IP protocol being used. For IPv4 packets, this field is set to 4. For IPv6 packets, this field is set to 6.
2. Header Length: This 4-bit field indicates the length of the IP header in 32-bit words. The minimum value is 5, indicating a header length of 20 bytes. The maximum value is 15, indicating a header length of 60 bytes.
3. Type of Service: This 8-bit field is used to specify the quality of service (QoS) for the packet. It can be used to prioritize different types of traffic, such as voice or video traffic, over other types of traffic.
4. Total Length: This 16-bit field indicates the total length of the IP packet, including the header and data. The maximum value for this field is 65,535 bytes.
5. Identification: This 16-bit field is used to identify fragments of a larger packet. If a packet is too large to be sent in a single transmission, it may be divided into smaller packets called fragments. The Identification field allows the receiver to reassemble the fragments into the original packet.

The IP packet header

6. Flags: This 3-bit field is used to control fragmentation of the packet. The first bit is reserved and set to 0. The second bit is the Don't Fragment (DF) bit, which is set to 1 if the packet should not be fragmented. The third bit is the More Fragments (MF) bit, which is set to 1 for all fragments except the last one.

7. Fragment Offset: This 13-bit field indicates the position of the current fragment within the original packet. It is measured in units of 8 bytes.

8. Time to Live: This 8-bit field is used to limit the lifetime of the packet. It is decremented by one at each router hop and the packet is discarded if the Time to Live value reaches zero.

9. Protocol: This 8-bit field identifies the transport layer protocol that the packet is carrying, such as TCP or UDP.

10. Header Checksum: This 16-bit field is used to verify the integrity of the IP header. It is calculated based on the contents of the header and is checked by the receiver to ensure that the header has not been corrupted in transit.

11. Source Address: This 32-bit field contains the IP address of the sender of the packet.

12. Destination Address: This 32-bit field contains the IP address of the intended recipient of the packet.

DVRA

Distance Vector Routing Algorithm

What even….

Distance Vector Routing Algorithm (DVRA) is a type of routing algorithm used in computer networks to determine the best path for data packets to travel from one network node to another. In DVRA, each node maintains a table that contains the distance to all other nodes in the network.

Remember Centralized, Isolation and **Distributed**?

How...

1. Initialization: Each node in the network initializes its distance table. The distance table contains information about the distance to each node in the network, as well as the next-hop node to reach that destination.
2. Distance Calculation: Each node sends its distance table to its neighbors. The neighbors then use this information to update their own distance tables. They calculate the distance to each node in the network based on the distance information received from their neighbors.
3. Table Update: After calculating the distance to all nodes in the network, each node updates its distance table and sends it to its neighbors.
4. Convergence: This process continues until all the nodes in the network have the same distance table. This is called convergence, and it means that all nodes have the same information about the network and the best path to reach each node.
5. Routing: Once the distance table has converged, each node can use its table to determine the best path to reach any other node in the network.

TCP vs UDP

Transmission Control Protocol

v/s

User Datagram Protocol

Again, what even….

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are both transport layer protocols used in computer networking. While both protocols are used for communication between applications, they have several differences in terms of their features and usage.

Connection-oriented vs. Connectionless:

TCP is a connection-oriented protocol, which means that it establishes a connection between two endpoints before transmitting data. UDP, on the other hand, is a connectionless protocol, which means that it does not establish a connection before transmitting data.

Reliability

TCP is a reliable protocol, which means that it ensures that all data packets are delivered to the destination and in the correct order. UDP, on the other hand, is an unreliable protocol, which means that it does not ensure that all packets are delivered or that they are delivered in the correct order.

Flow Control

TCP provides flow control, which means that it regulates the amount of data that can be sent at a time and ensures that the receiving end can handle the data. UDP does not provide flow control, which means that the sending application can send data as quickly as it wants.

Congestion Control

TCP also provides congestion control, which means that it adjusts the transmission rate based on the network conditions. UDP does not provide congestion control and can lead to network congestion if the sending application sends data too quickly.

Usage

TCP is commonly used for applications that require reliable and ordered data transmission, such as file transfers, email, and web browsing. UDP is commonly used for applications that require fast and efficient transmission, such as video streaming, online gaming, and DNS.

IPv4 and IPv6

Configuration

IPv4

IPv4 addresses are assigned to devices on a network using two methods: static and dynamic IP address assignment.

1. Static IP Address Assignment: In this method, network administrators manually assign a fixed IP address to a device on the network. The static IP address remains the same until it is manually changed by the administrator. Static IP addresses are commonly used for devices that require a constant IP address, such as servers, routers, and printers.
2. Dynamic IP Address Assignment: In this method, IP addresses are automatically assigned to devices on the network using the Dynamic Host Configuration Protocol (DHCP). DHCP is a network protocol that assigns IP addresses, subnet masks, and other network parameters to devices on the network. When a device connects to the network, it sends a DHCP request, and the DHCP server responds with an available IP address. The IP address is typically assigned for a specific period of time, known as the lease time. When the lease time expires, the device must request a new IP address from the DHCP server.

IPv4

- Dynamic IP address assignment is commonly used for devices such as desktop computers, laptops, and mobile devices, which may connect and disconnect from the network frequently. It allows for efficient use of IP addresses and simplifies network administration, as the DHCP server can automatically assign and manage IP addresses for devices on the network.
- In both static and dynamic IP address assignment methods, IP addresses must be unique within the network to ensure that data is transmitted to the correct device. Network administrators must also configure other network parameters, such as subnet masks and default gateways, to ensure that devices on the network can communicate with each other and with devices on other networks.

IPv6

IPv6 addresses are assigned to devices on a network using two methods: stateless and stateful address assignment.

1. Stateless Address Assignment: In this method, devices on the network use their unique MAC address to generate their own IPv6 address. The process involves taking the MAC address and inserting additional characters to create a unique 128-bit IPv6 address. This method is known as EUI-64 (Extended Unique Identifier-64) format.
2. Stateful Address Assignment: In this method, IPv6 addresses are assigned by a DHCPv6 (Dynamic Host Configuration Protocol for IPv6) server. Similar to DHCP for IPv4, the DHCPv6 server provides IPv6 addresses, subnet masks, and other network parameters to devices on the network.

VLAN

Virtual Local Area Network

VLAN

A VLAN, or Virtual Local Area Network, is a logical grouping of devices on a network that share a common set of requirements or characteristics. A VLAN is created by configuring network switches to allow devices in a particular group to communicate with each other as if they were connected to the same physical network, even if they are physically located on different networks.

VLAN Memberships

VLAN membership refers to the process of assigning network devices to a particular VLAN. There are several methods for assigning VLAN membership, including:

1. Port-Based VLANs: In this method, network switches are configured to assign VLAN membership based on the physical switch port that a device is connected to. For example, all devices connected to port 1 may be assigned to VLAN 10, while devices connected to port 2 may be assigned to VLAN 20.
2. MAC-Based VLANs: In this method, network switches are configured to assign VLAN membership based on the MAC address of the device. This method is useful when a device needs to maintain VLAN membership regardless of the physical port it is connected to.
3. Protocol-Based VLANs: In this method, VLAN membership is assigned based on the type of network traffic being transmitted. For example, all VoIP traffic may be assigned to VLAN 10, while all video conferencing traffic may be assigned to VLAN 20.
4. Dynamic VLANs: In this method, VLAN membership is assigned dynamically based on various factors, such as user authentication, location, or other network policies.

Why VLANS?

- Improved Network Performance
- Increased Security
- Simplified Network Management
- Scalability
- Flexibility