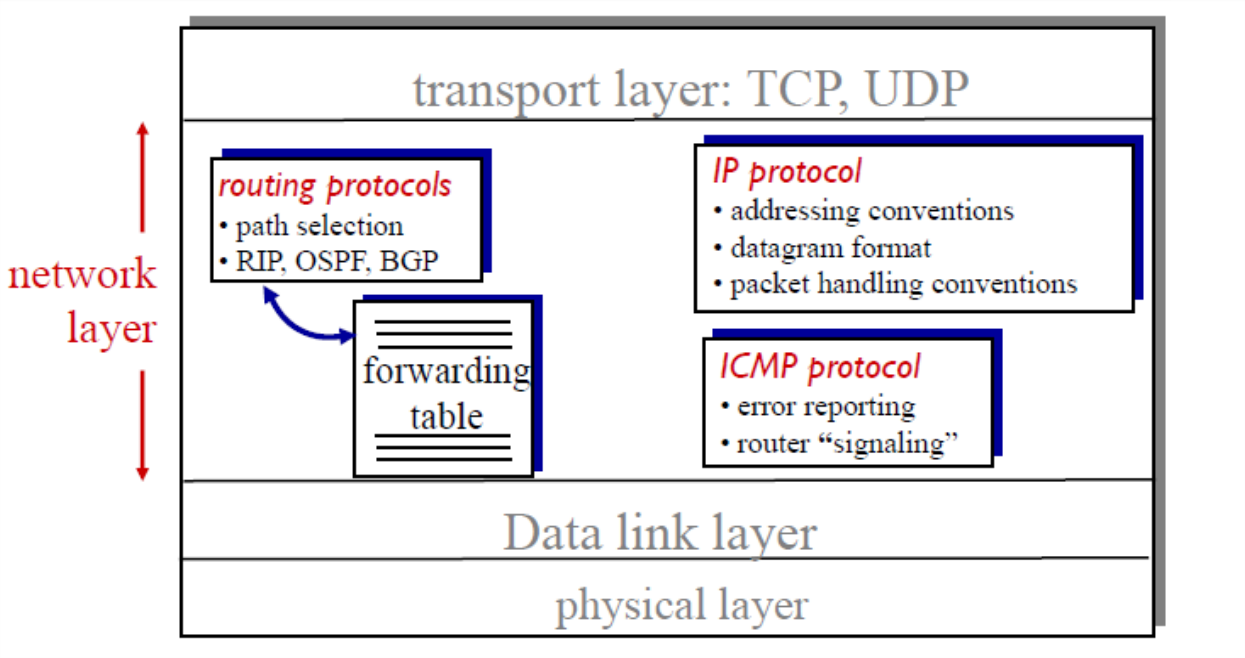
Network Layer - Part 2

IPv4, IPv6, IPSec, ICMP

The Internet network layer

Host, router network layer functions:



IP Addresses

The main features of IP address are:

- **IP**: (a logical address) Provides **connectionless**, best-effort (**unreliable)** delivery of datagrams through the network.
- IP addresses **are network layer addresses**.
- IP addresses are **32-bit** numbers.

IP Addresses: how to get one?

Q: How does a *host* get IP address?

The host can get IP address by using one of these two ways

1. **hard-coded** by system administrator in a file (Static addressing)
2. **Dynamic Host Configuration Protocol** (**DHCP**): dynamically get address from as server (plug-and-play)

DHCP: Dynamic Host Configuration Protocol

Goal: DHCP enables hosts dynamically obtain **IP addresses**, **subnet masks**, **gateways**, **DNS server information** from network server when it joins network.

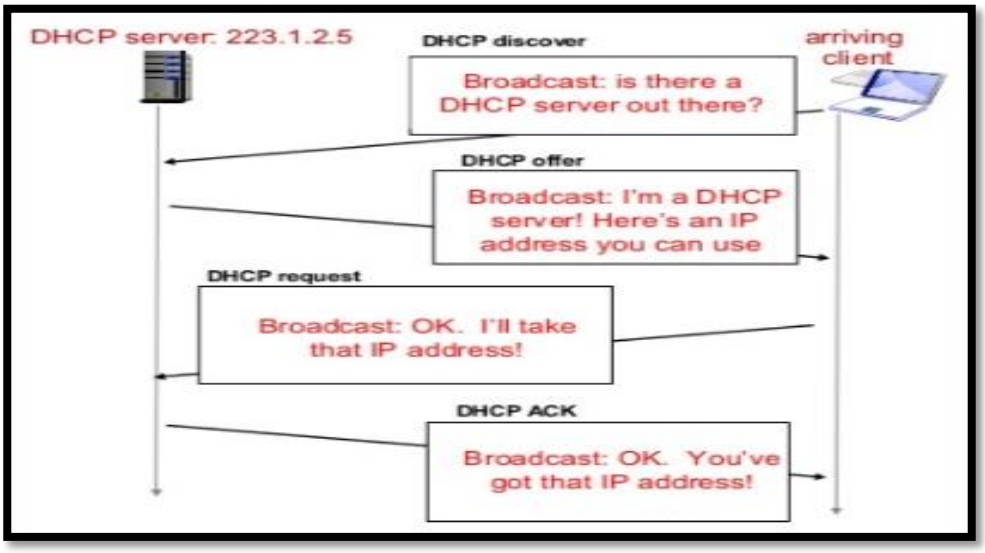
DHCP Working Steps (pool operation)

Step 1: When the client is connected to a network, a **DHCPDISCOVER** message is **broadcasted** from the client to the servers (**client asks for IP address**).

Step 2: When the DHCP server receives the **DHCPDISCOVER** request message then it replies with a **DHCPOFFER** message. This message contains all the network configuration settings required by the client.

Step 3: The client forms a **DHCPREQUEST** message in reply to **DHCPOFFER** message and sends it to the server indicating it wants to accept the network configuration sent in the DHCPOFFER message.

Step 4: Once the server receives DHCPREQUEST from the client, it sends the **DHCPACK** message indicating that now the client is **allowed to use the IP address assigned to it**.



DHCP: more than IP addresses

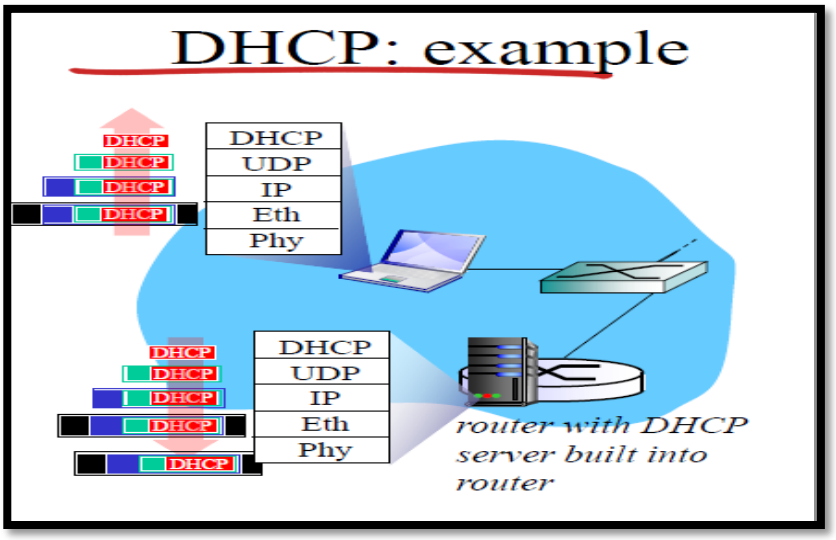
DHCP can return more information than just allocated IP address on subnet:

- Address of first-hop router for client.
- Name and IP address of DNS sever.
- Network mask. (Indicating network versus host portion of address).

DHCP: example

- DCP server formulates DHCP ACK containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server

- Encapsulation of DHCP server, frame forwarded to client, demuxing up to DHCP at client
- Client now knows its IP address, name and IP address of DNS server, IP address of its first-hop router



IPv6 Features

The ability to scale networks for future demands requires a **limitless supply of IP addresses** and **improved mobility**; IPv6 combines expanded addressing **with a more efficient and feature**-rich header to meet these demands.

- header format helps speed processing/forwarding
- header changes to facilitate QoS

The main benefits of IPv6 include the following:

- **Larger address space: IPv6 addresses are 128 bits, compared to IPv4's 32 bits**. This larger addressing space allows more support for addressing hierarchy levels, a much greater number of addressable nodes, and simpler auto configuration of addresses.
- **Globally unique IP addresses:** Every node can have a unique global IPv6 address, which eliminates the need for NAT.
- **Site multihoming: IPv6 allows hosts to have multiple IPv6 addresses** and allows networks to have multiple IPv6 prefixes. Consequently, sites can have connections to multiple ISPs without breaking the global routing table.
- **Header format efficiency:** A simplified header with a fixed header size makes processing more efficient.
- **Improved privacy and security:** IPsec is standard for IP network security, available for both IPv4 and IPv6.

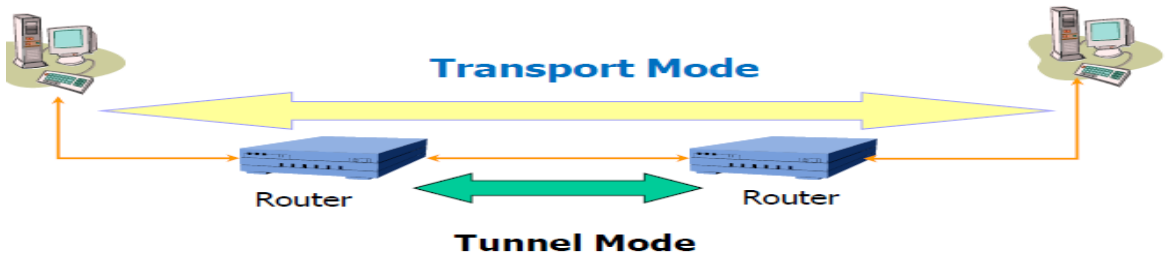
- ❖ **Flow labeling capability:** A new capability enables the labeling of packets belonging to particular traffic flows for which the sender requests special handling.

- ❖ **Increased mobility and multicast capabilities:** Mobile IPv6 allows an IPv6 node to change its location on an IPv6 network and still maintain its existing connections.

IP Security (IPSec)

- IP Security (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.
- IPSec **helps to create authenticated and confidential packets for the IP layer**.
- IPSec operates in one of two different modes: the transport mode or the tunnel mode.

Transport Mode	Tunnel Mode
IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer.	IPSec in the tunnel mode protects the original IP header.

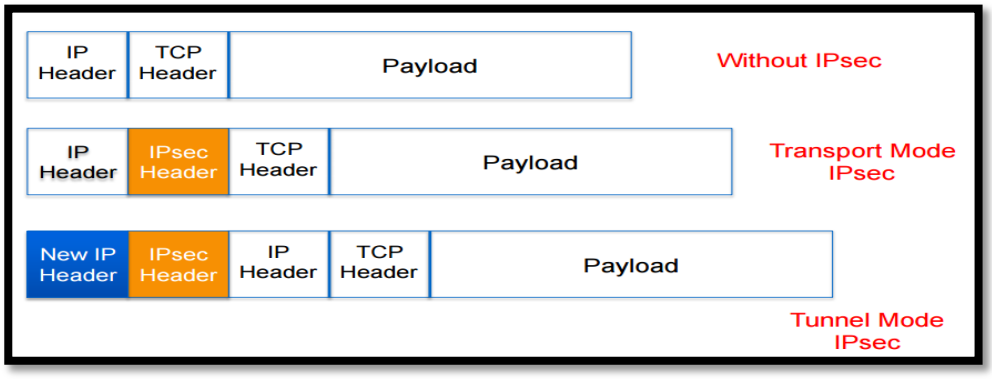


Transport Mode

- IPsec header is inserted into the IP packet
- No new packet is created
- Works well in networks where increasing a packet's size could cause an issue
- Frequently used for remote-access VPNs

Tunnel Mode

- Entire IP packet is encrypted and becomes the data component of a **new (and larger) IP packet**.
- Frequently used in an IPsec site-to-site VPN



Difference between IPV6 and IPV4

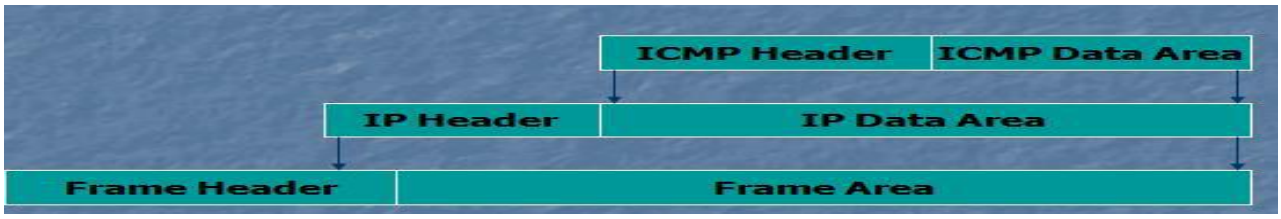
IPv4	IPv6
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals.
Checksum field is available in IPv4 header	No checksum field in IPv6 header.
Options fields are available in IPv4 header.	No option fields, but IPv6 Extension headers are available.
(ARP) is available to map IPv4 addresses toMAC addresses.	(ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).
Broadcast messages are available.	Broadcast messages are not available.
Manual configuration (Static) or DHCP (Dynamic configuration) is required to configureIPv4 addresses.	Auto-configuration of addresses is available.

Internet Control Message Protocol (ICMP)

ICMP is an error reporting protocol and is used by routers, hosts and network devices to generate error messages when there are problems delivering IP packets. It has the following features:

1. used by hosts & routers to **communicate network-level information**
2. **ICMP reports errors** (unreachable host, router, port, or a requested service is not available) **and sends control message**(echo request/reply (used by ping)
3. ICMP does not attempt to make IP a reliable protocol. It simply attempts to report errors and provide feedback on specific condition.

4. ICMP messages **carried on IP packet**.
5. ICMP messages are divided into **error-reporting messages** and **query messages**.



- ICMP message: type, code plus first 8 bytes of IP datagram causing error

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

Figure 1. ICMP message types

ICMP Applications

There are two simple and widely used applications which are based on ICMP:

1. **Ping:** The ping checks whether a host is alive & reachable or not. This is done by sending an **ICMP Echo Request packet** to the host, and waiting for an **ICMP Echo Reply** from the host.

2. **Trace route:** Trace route is a utility that records the route through the Internet between your computer and a specified destination computer. It also calculates and displays the amount of time each hop took.