Network Protocol

Network Layer Part: 3

ISLAMIC UNIVERSITY COLLEGE
Computer Technical Engineering Department

Computer Networks Protocols

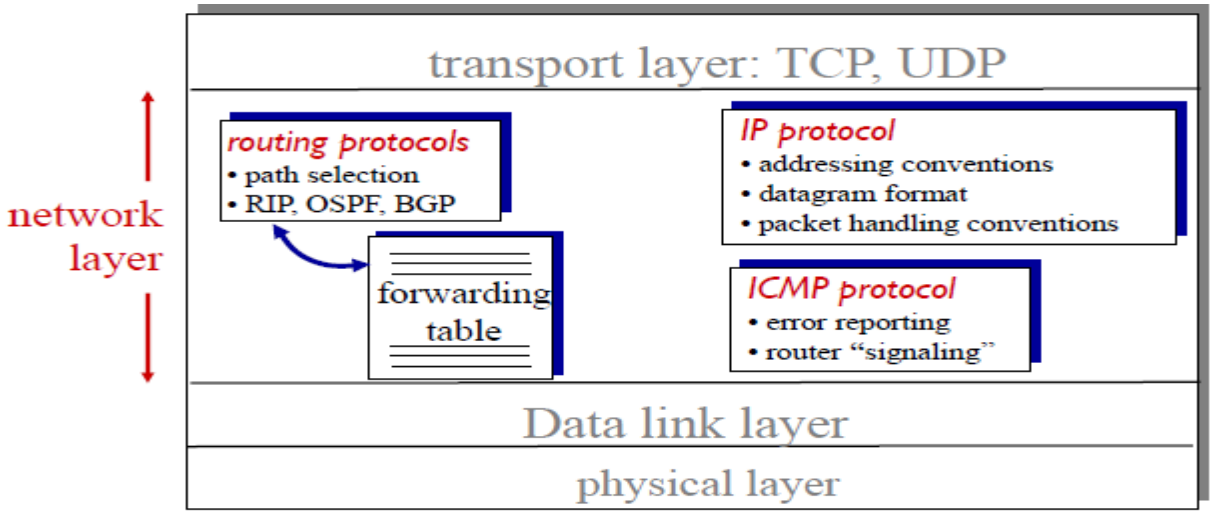
Lecture No.5:Network Layer Part 3

Prepared By: Dr. ENG. Mustafa S. Al-Bayati

IPv4, IPv6, IPSec, ICMP

The Internet network layer

host, router network layer functions:



IP Addresses

- **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?

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

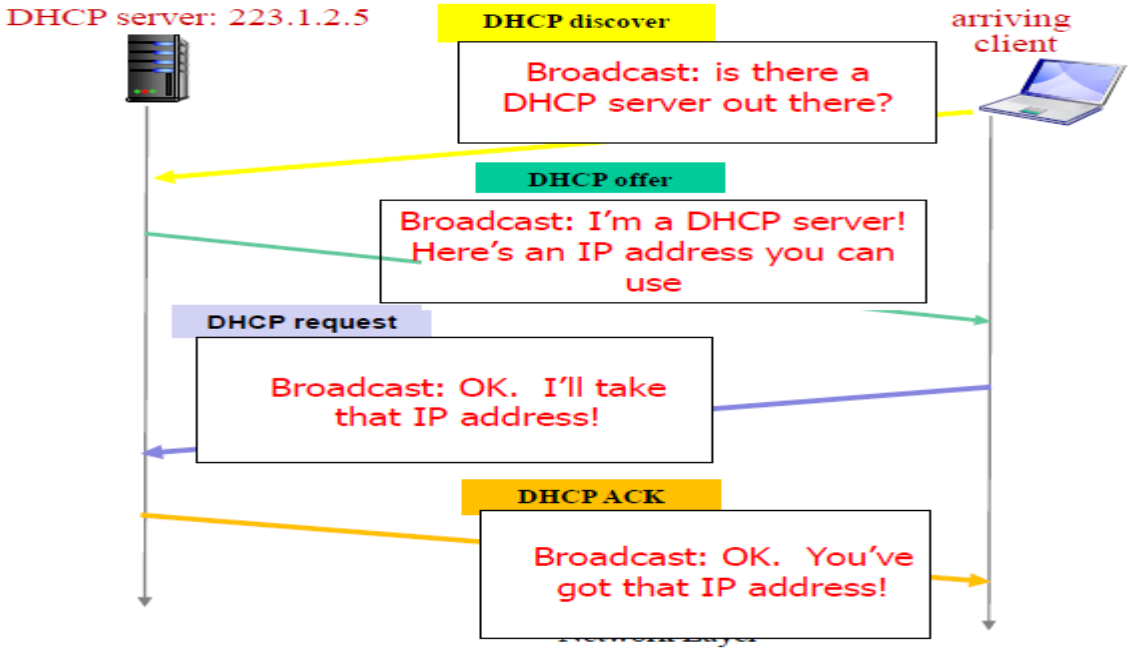
DHCP: Dynamic Host Configuration Protocol

Goal: allow host to *dynamically* obtain its IP address from network server when it joins network

DHCP overview*: (pool operation)*

1. host broadcasts "**DHCP discover" msg**
2. DHCP server responds with "**DHCP offer" msg**
3. host requests IP address: "**DHCP request" msg**
4. DHCP server sends address: "**DHCP ack" msg**

DHCP client-server scenario



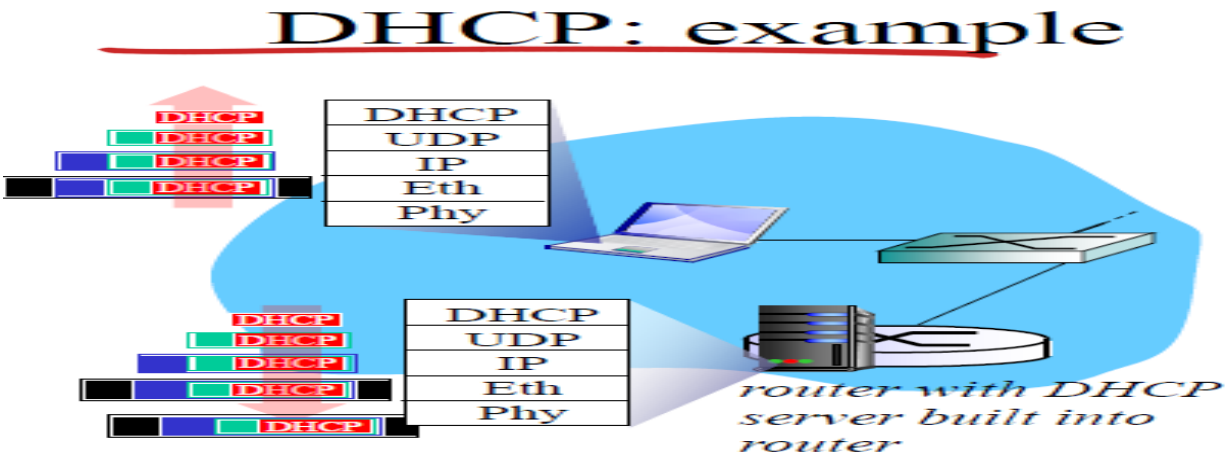
DHCP: more than IP addresses

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

- **address** of first-hop router for client
- **name and IP address** of DNS sever
- **network mask**

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**, 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**:

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.

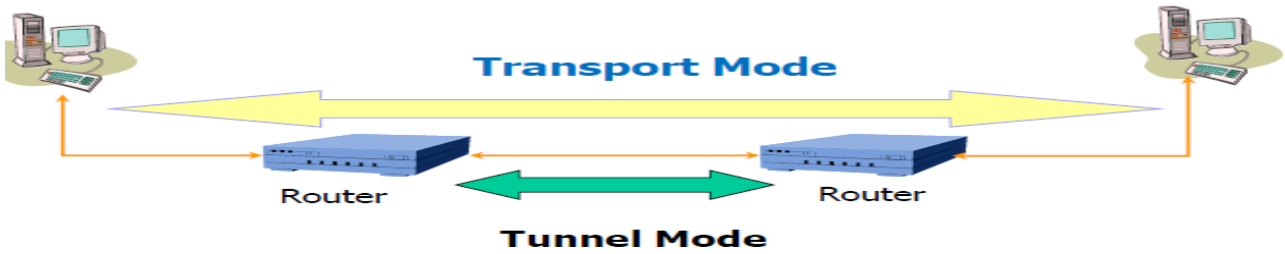
■**Increased mobility and multicast capabilities**:

Mobile IPv6 allows an IPv6 node to change its location on an IPv6 network and still maintain its existing connections.

IPSecurity (IPSec)

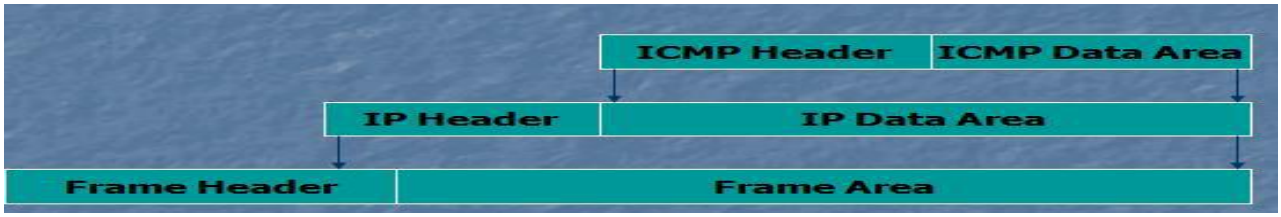
- IPSecurity (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.
- IPSec **helps to create authenticated and confidential packets for the IP layer** .
- IPSec operates in one of two different modes: the transport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



Internet Control Message Protocol (ICMP)

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



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

ICMP Applications

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

 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.

 Trace route.

Trace route is a used 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.