

Ministry of Higher Education and Scientific Researches
Al-Mansour University College
Department of Computer Technology Engineering
Fourth Class



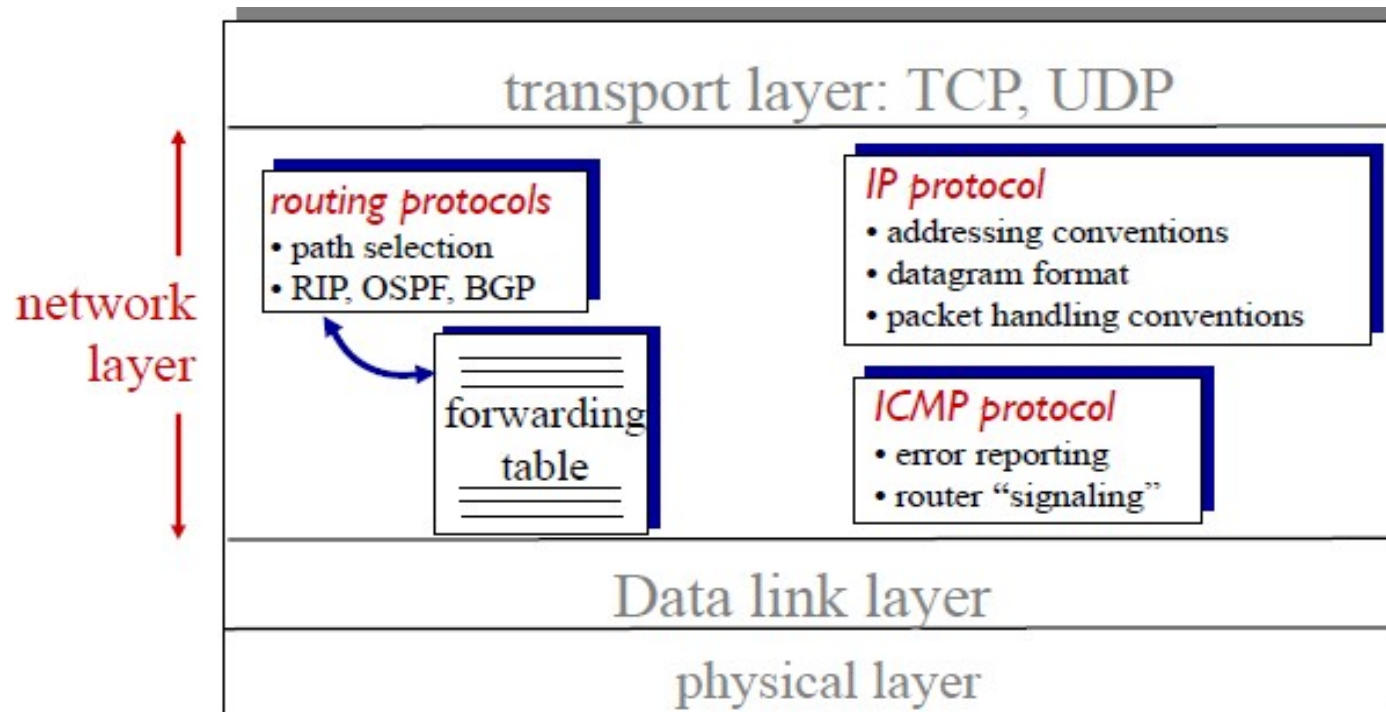
Computer Networks Protocols

Lecture Five: Network Layer IPv4, IPv6, IPSec, ICMP

Dr. Mahmoud Shuker Mahmoud

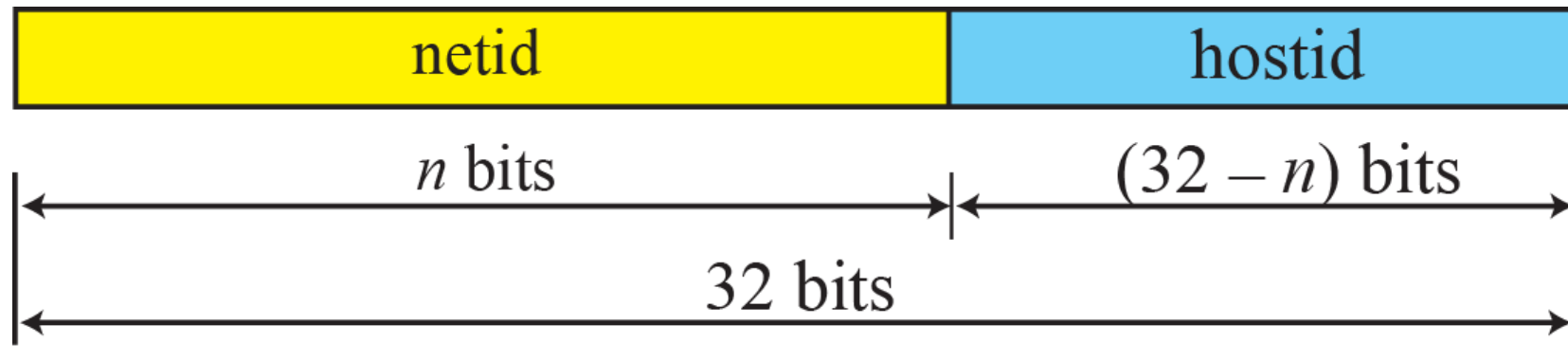
The Internet network layer

host, router network layer functions:



IPv4 Addressing

- **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.



Class A: $n = 8$

Class B: $n = 16$

Class C: $n = 24$

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

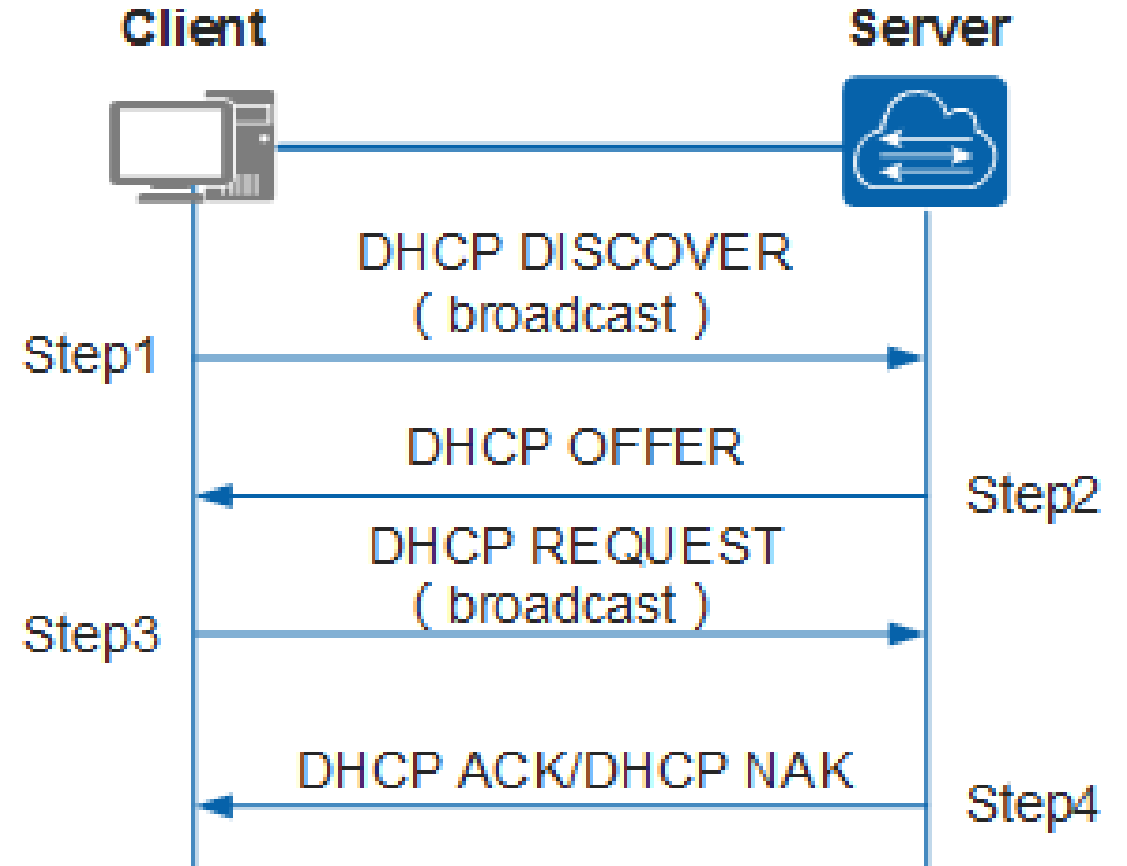
1. Hard-coded manually by system admin in a file
2. **DHCP**: Dynamic Host Configuration Protocol: dynamically get address from as server (plug-and-play)

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)

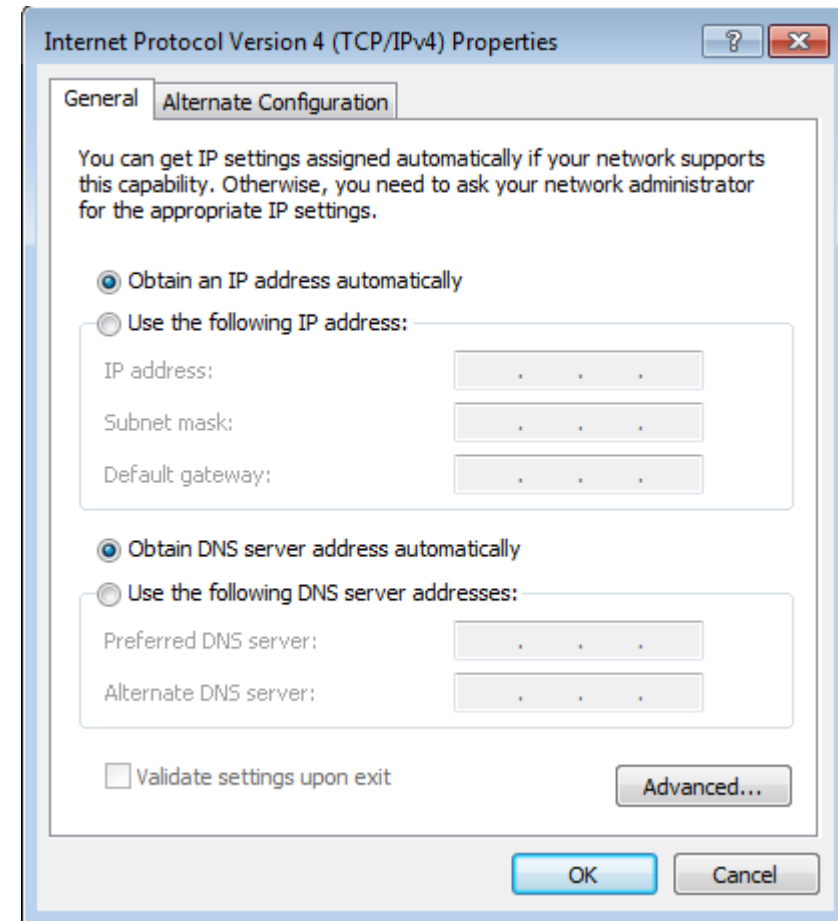
1. host broadcasts “**DHCP discover**” msg
2. DHCP server responds with “**DHCP offer**” msg
3. host requests IP address: “**DHCP request**” msg
4. DHCP server sends address: “**DHCP ack**” msg



DHCP: more than IP addresses

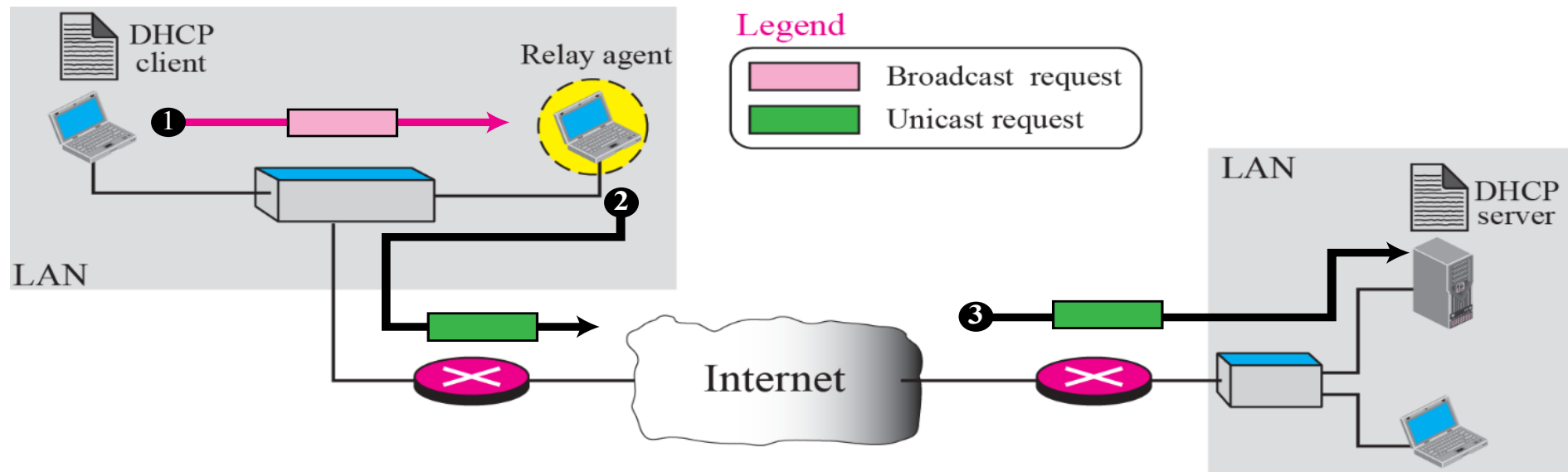
DHCP can return more than just an allocated IP address on the subnet:

- ✓ **Address of the first-hop router for client**
- ✓ **name and IP address of DNS server**
- ✓ **network mask**



There is one problem in this method that must be solved. The DHCP request is broadcast because the client does not know the IP address of the server. A broadcast IP datagram cannot pass through any router.

To solve the problem, there is a need for an intermediary. One of the hosts (or a router) can be used as a relay. The host in this case is called a **relay agent**.

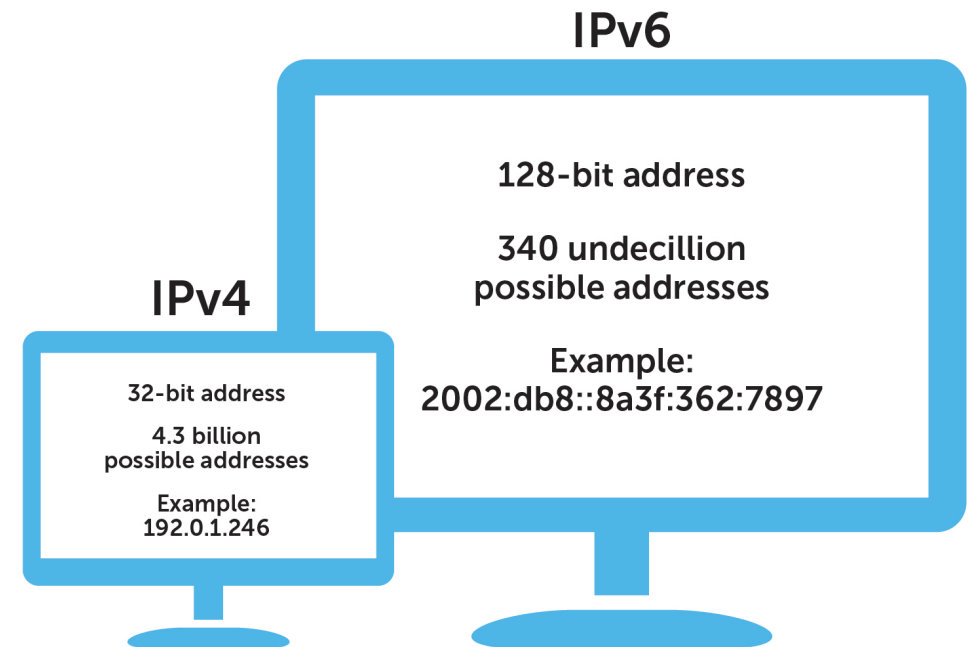


IPv6 Addressing

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.
- **Multicast instead of broadcast:** With IPv6 the multicast communication substitutes the needs of broadcasting by using **all node multicast**
- **Stateless and stateful address configuration:** IPv6 support besides the stateful addresses (DHCP) **a stateless addresses autoconfiguration feature (SLAAC)**

The rules used to compress the IPv6 Representation

- **Rule 1 (Leading Zero Compression):** Eliminate the starting zero(s) from any hextex (zeros to the left).
- **Rule 2 (Successive Zeros Compression):** Eliminate group of successive zeros by one double-colon (::) but you can perform this only once in your IPv6 address.

Example: Given the following IPv6 address (2001:1265:0000:0000:0AE4:0000:005B:06B0) used the rules to re-represent it in a compressed format.

Solution

Original IP

2001:1265:0000:0000:0AE4:0000:005B:06B0

After using **Rule 1** the IP can be compressed into:

2001:1265:0:0:AE4:0:5B:6B0

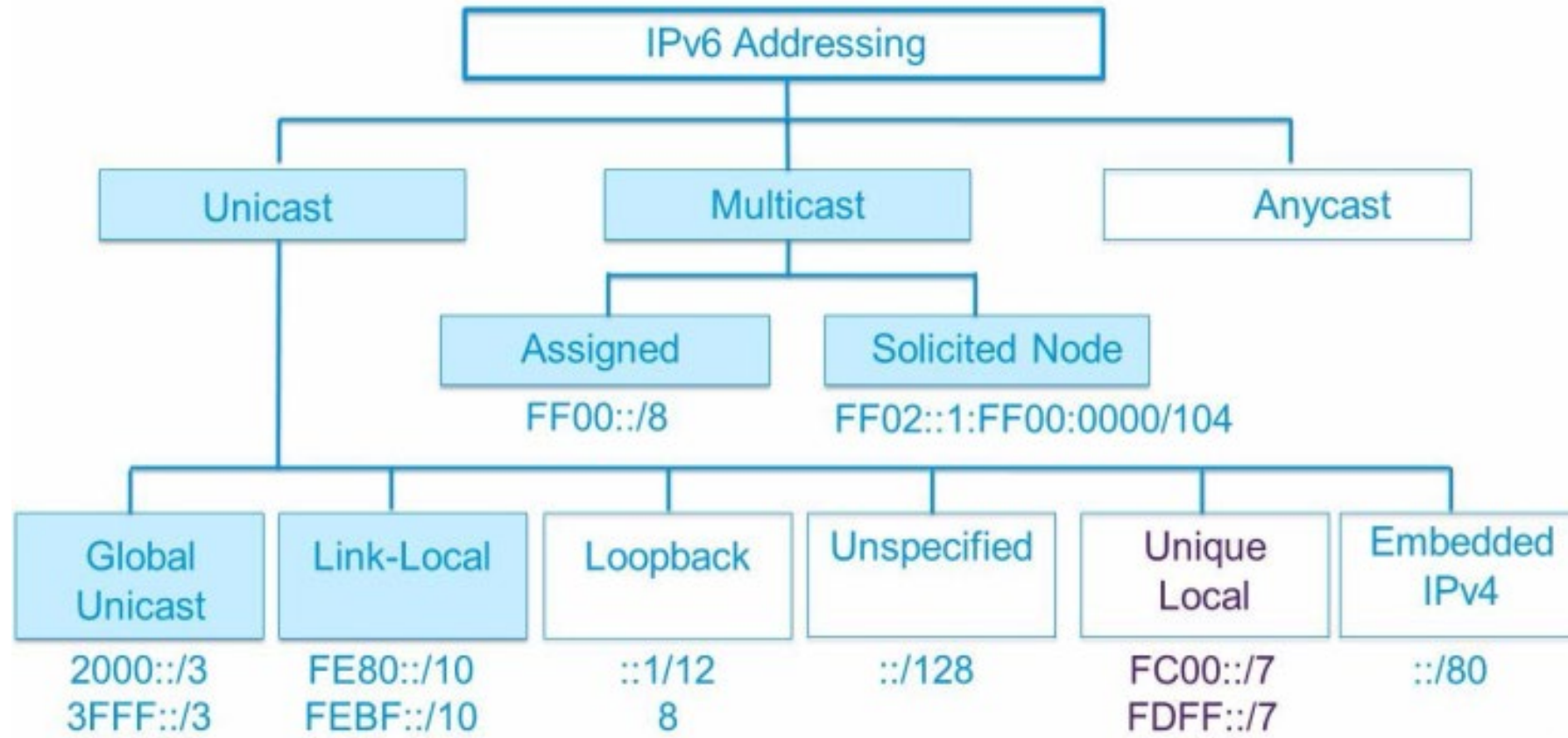
After using **Rule 2** the IP can be reduced into:

2001:1265::AE4:0:5B:6B0

Comparison between IPv4 and IPv6 Addresses

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

IPv6 Three Address Types



Three Levels of Hierarchy

An address in this block is divided into three parts:

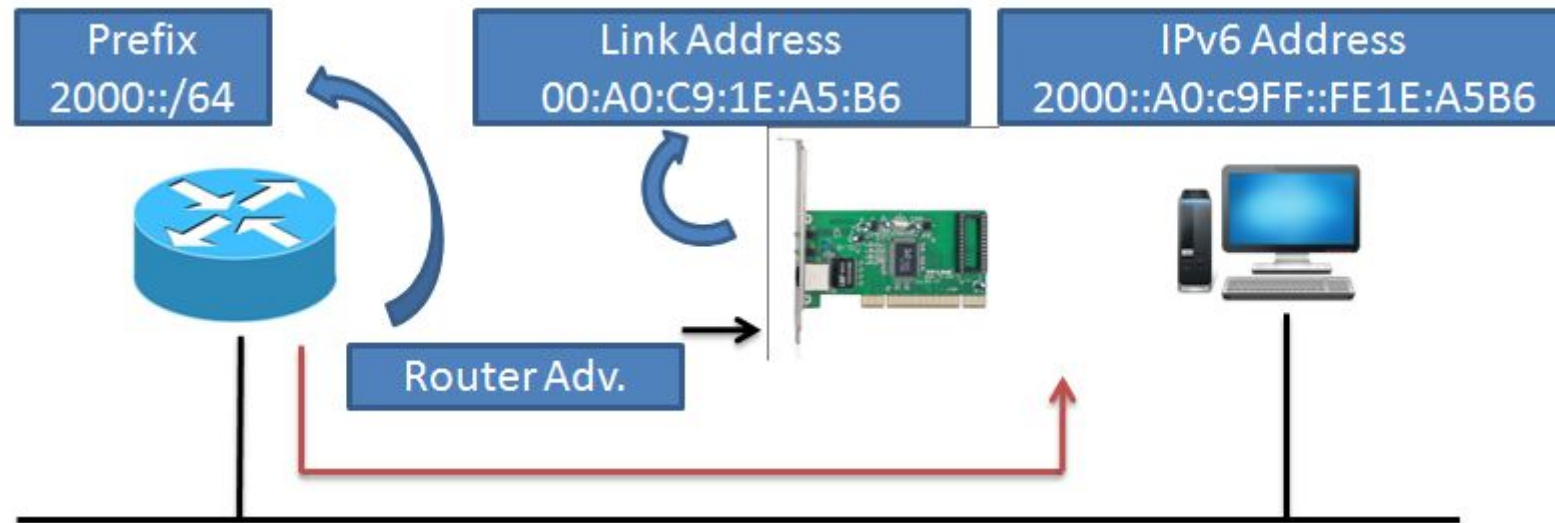
- Global routing prefix
- Subnet identifier
- Interface identifier

as shown in Figure below:



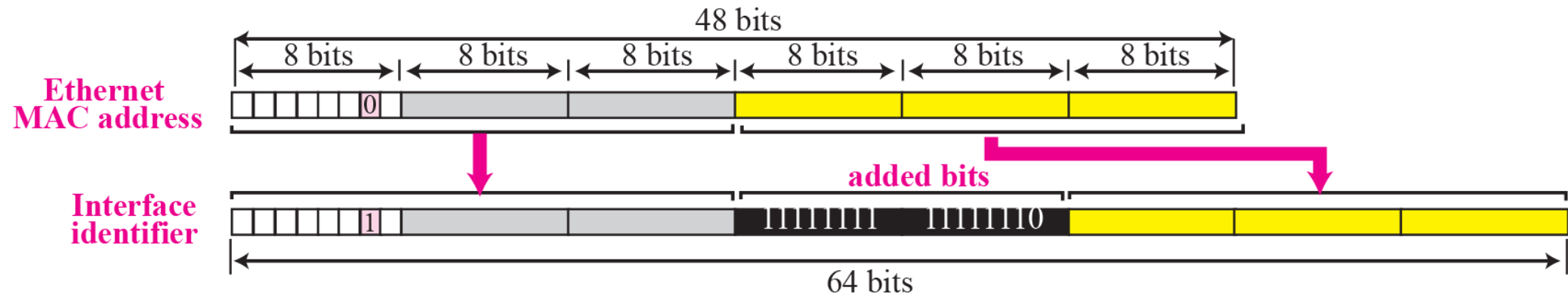
IPv6 Autoconfiguration

One of the interesting features of IPv6 addressing is the autoconfiguration of hosts. As we discussed in IPv4, the host and routers can be configured manually by the network manager. However, the Dynamic Host Configuration Protocol, DHCP, can be used to allocate an IPv4 address to a host that joins the network. In IPv6, DHCP protocol can still be used to allocate an IPv6 address to a host, but a host can also configure itself.



Interface Identifier

- The last 64 bits define the interface identifier.
- The interface identifier is similar to hostid in IPv4 addressing.
- The IPv6 addressing allows this opportunity. A physical address whose length is less than 64 bits can be embedded as the whole or part of the interface identifier, eliminating the mapping process. Mapping the 48-bit physical address defined by Ethernet to 64-bit extended unique identifier (EUI-64).



Example: Find the interface identifier if the Ethernet physical address is (F5-A9-23-14-7A-D2)₁₆ using the format we defined for Ethernet addresses.

Solution

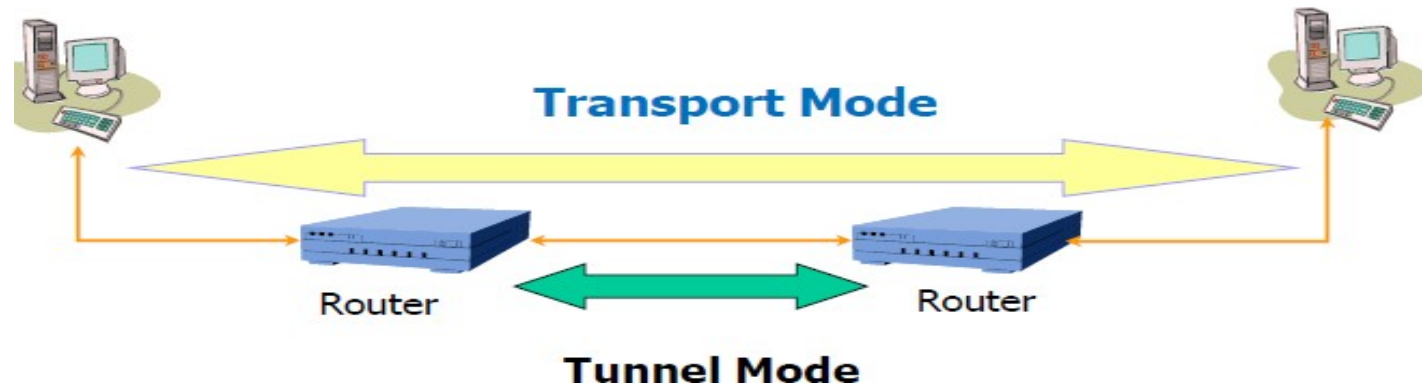
We only need to change the seventh bit of the first octet from 0 to 1, insert two octets (**FFFE**)₁₆ and change the format to colon hex notation.

The result is **F7A9:23FF:FE14:7AD2** in colon hex.

IP Security (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.
IP Header not Encrypted	IP Header Enceypted
Used for end-to-end communications (client and server)	Most commonly used between routers or ASA firewall (gateways)



IPsec Packet format transport mode vs. tunnel mod

Internet Control Message Protocol (ICMP)

ICMP has been designed to compensate for two *deficiencies* in IP protocol (Best effort delivery)

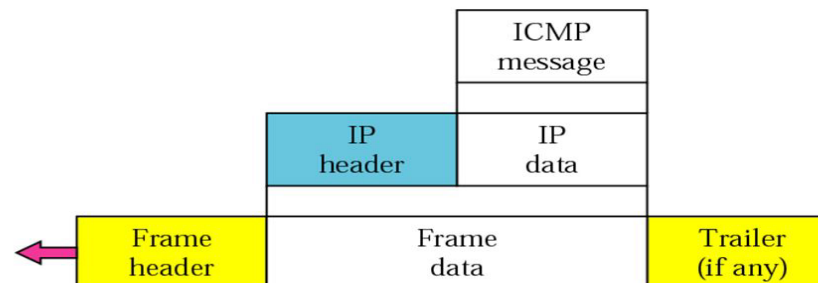
- 1- Lack of error control.
- 2- Lack of assistance mechanism.

ICMP messages are:

1- Error reporting messages: report a problem that a router or a host (destination) may encounter during its processing of the IP packet

2- Query messages: help the host (source) or the network manager get specific information from a router or another host.

- ✓ ICMP used by hosts & routers to communicate network-level information
- ✓ ICMP reports errors (unreachable host, router, port, or 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 the specific condition.
- ✓ ICMP messages are carried on IP packets.



ICMP Applications

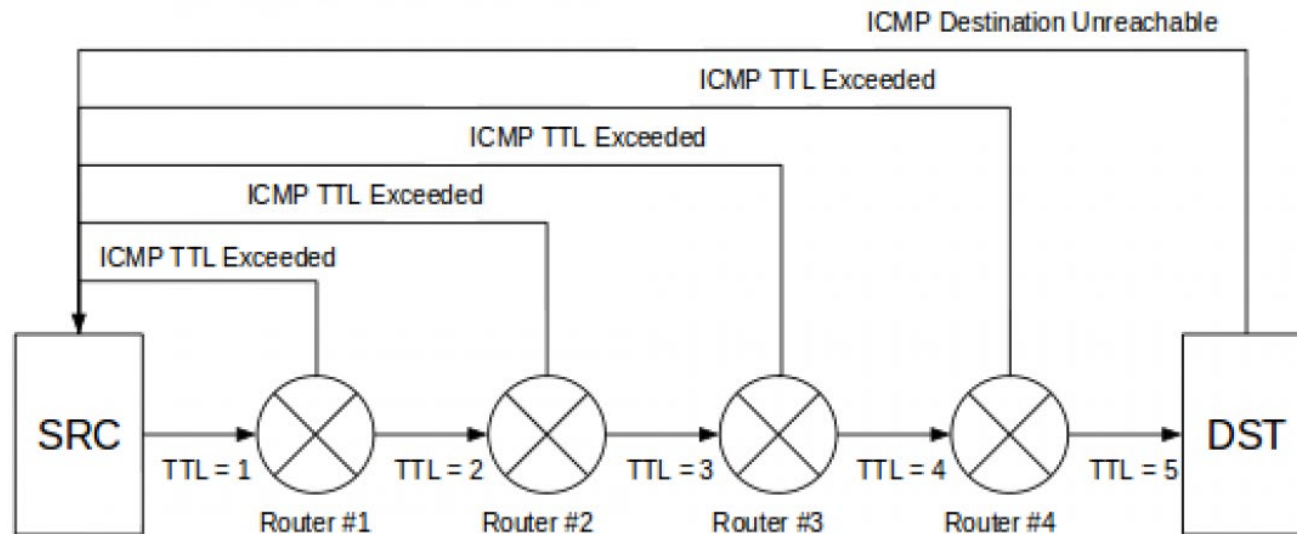
There are two simple and widely used applications that are based on ICMP:

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.

Traceroute.

Traceroute is used to 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.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\admin>ping baidu.cn

Pinging baidu.cn [220.181.111.85] with 32 bytes of data:
Reply from 220.181.111.85: bytes=32 time=267ms TTL=52
Reply from 220.181.111.85: bytes=32 time=267ms TTL=52
Reply from 220.181.111.85: bytes=32 time=267ms TTL=52
Reply from 220.181.111.85: bytes=32 time=267ms TTL=52

Ping statistics for 220.181.111.85:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 267ms, Maximum = 267ms, Average = 267ms

C:\Users\admin>tracert baidu.cn

Tracing route to baidu.cn [220.181.111.85]
over a maximum of 30 hops:
  0  *          <1 ms    *
  1  *          <1 ms    *
  2  *          *        *
  3  *          *        *
  4  *          *        *
  5  135 ms    135 ms    135 ms
  6  *          *        *
  7  153 ms    151 ms    151 ms
  8  152 ms    151 ms    151 ms
  9  366 ms    366 ms    365 ms
 10  327 ms    330 ms    333 ms
 11  269 ms    267 ms    268 ms
 12  *          *        380 ms
 13  *          *        *
 14  408 ms    407 ms    411 ms
 15  *          *        *
 16  292 ms    292 ms    292 ms    220.181.111.85

Trace complete.
C:\Users\admin>
```