Dynamic Host Configuration Protocol

Serhii Zakharchenko

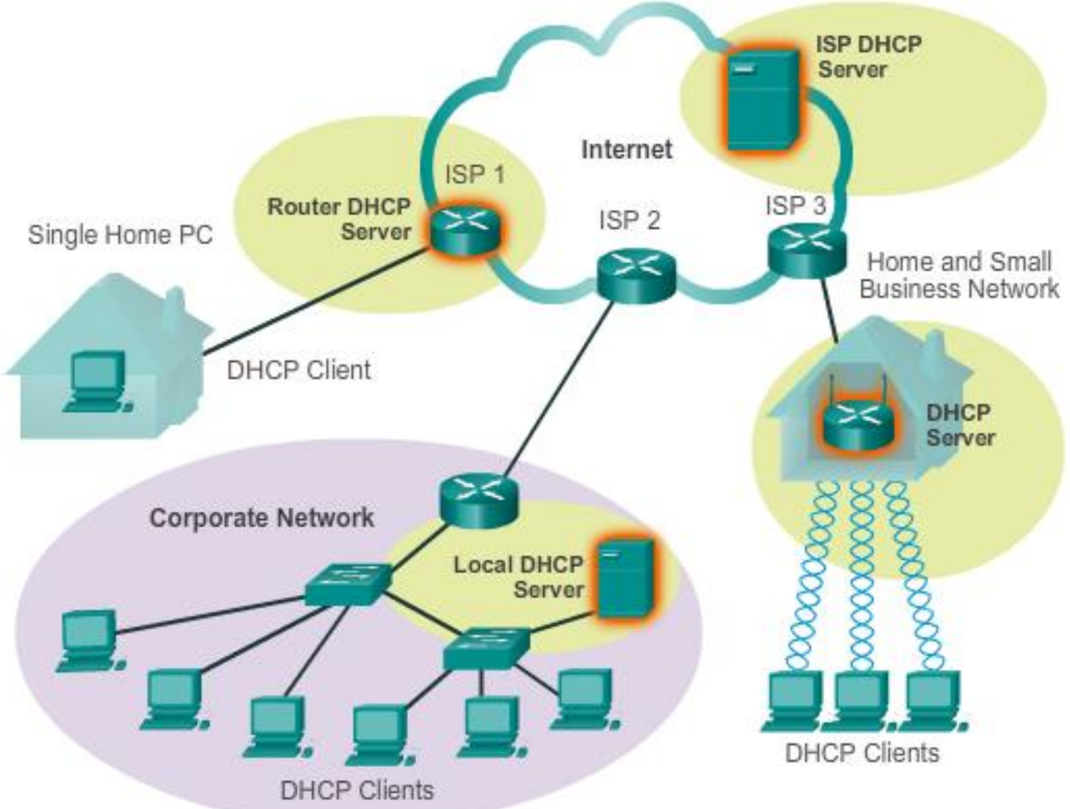
TRAINING CENTER

Agenda

- DHCP basics
- DHCP Security Problems
- DHCPv6 Overview

DHCP Introduction

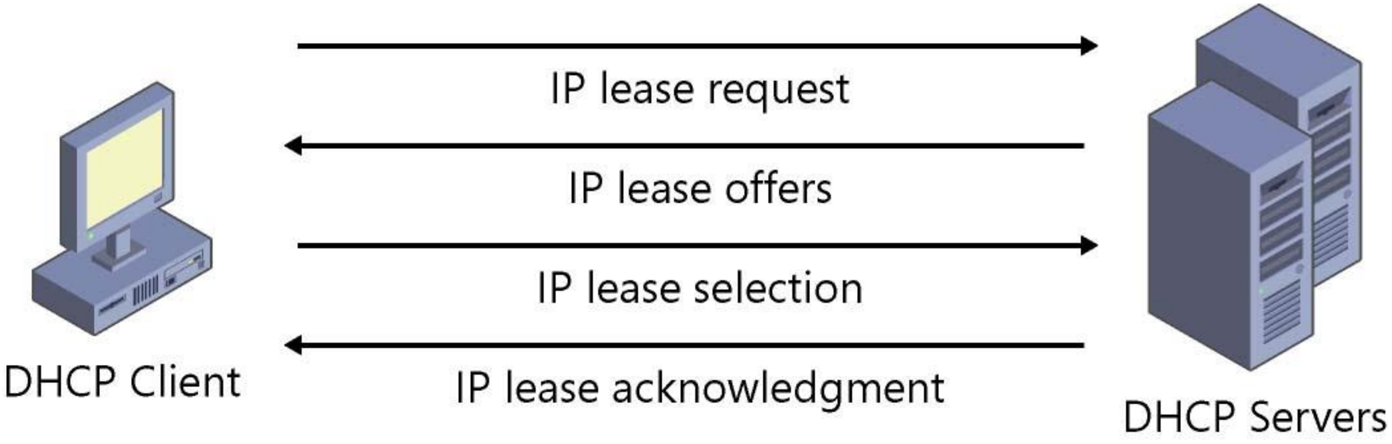
- DHCP service enables devices on a network to obtain IP addresses, subnet masks, gateway, and other IP networking parameters **dynamically** from a DHCP server.
- DHCP server is contacted, and address requested - chooses address from a configured range of addresses called a **pool** and "leases" it to the host for a **set period**
- DHCP used for general purpose hosts such as **end user devices**, and static addressing is used for network devices such as gateways, switches, servers and printers
- DHCP can pose a **security risk** because any device connected to the network can receive an address.



DHCP Operation

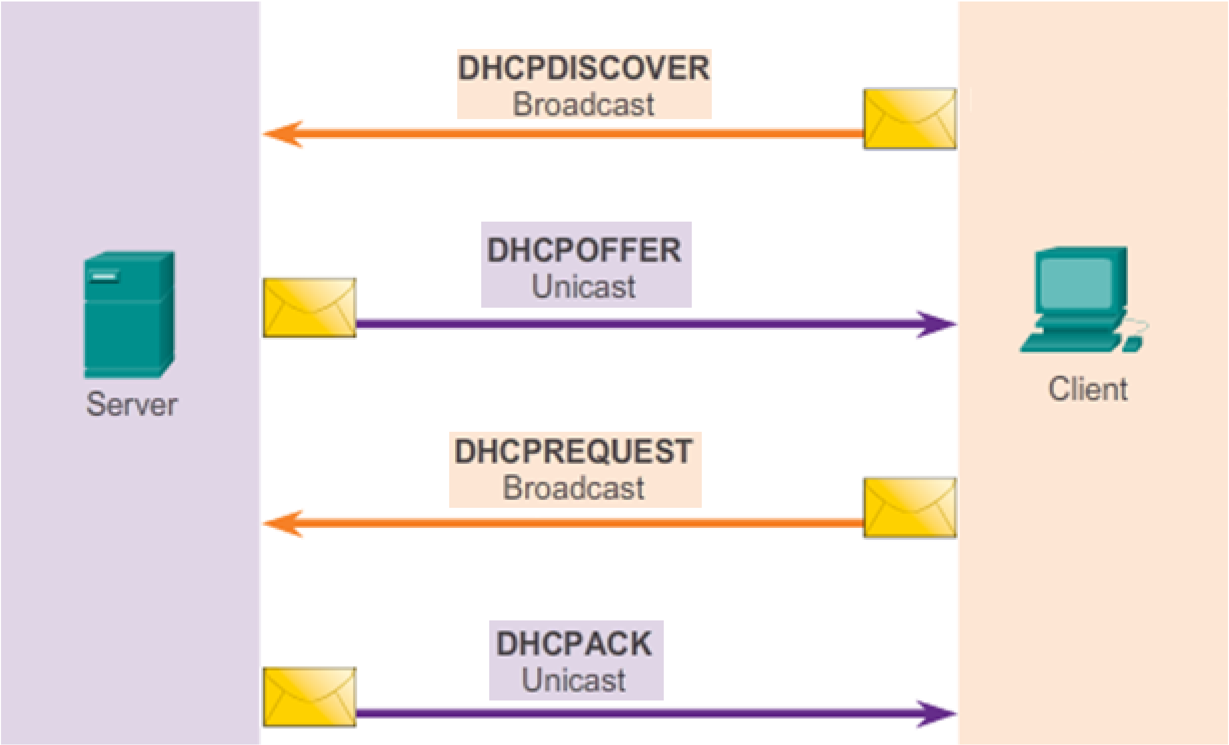
DHCP uses different address allocation methods

- **Manual Allocation** - The administrator assigns a pre-allocated IP address to the client, and DHCP communicates only the IP address to the device.
- **Automatic Allocation** - DHCP automatically assigns an IP address permanently to a device, selecting it from a pool of available addresses. No lease.
- **Dynamic Allocation** - DHCP dynamically assigns, or leases, an IP address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address. Most commonly used.

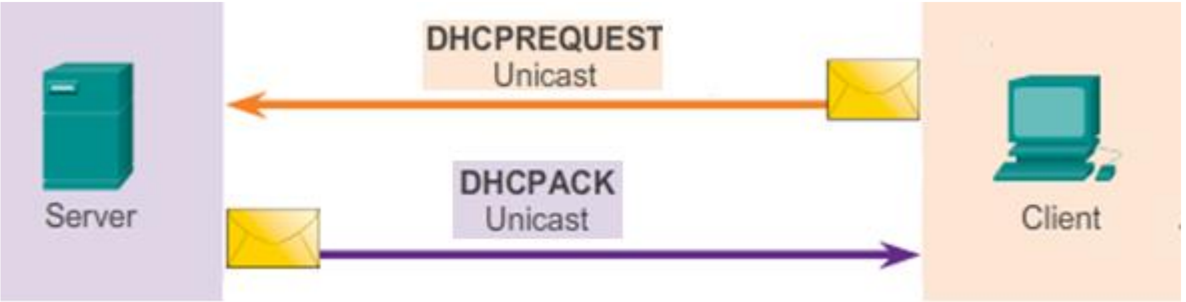


DHCPv4 Lease Origination and Renew

Lease Origination process



Lease Renewal process



DHCPNAK - sent by the server instead of the final acknowledgment

DHCPRELEASE - client sends this message to notify the server to release the occupied IP

DHCPINFORM - client has already received an IP and is asking the server for additional settings

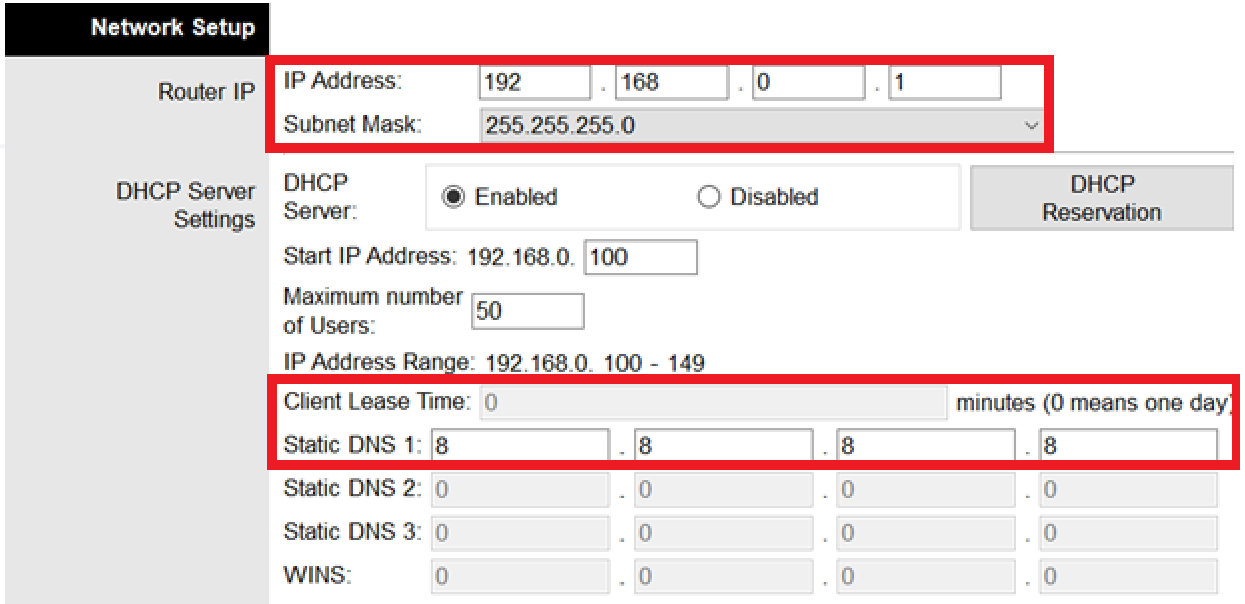
DHCP Configuration elements

DHCP server permits to configurate different elements:

- Addresses pool – may be described as a range from start to end IP-address, as a start IP-address and maximum number of users or as network IP-address, subnet mask and list of excluded addresses;
- Options 1 – Subnet mask
- Options 3 – Default Gateway
- Options 6 – DNS servers addresses
- Options 51 – Leased time

Full DHCP options list:

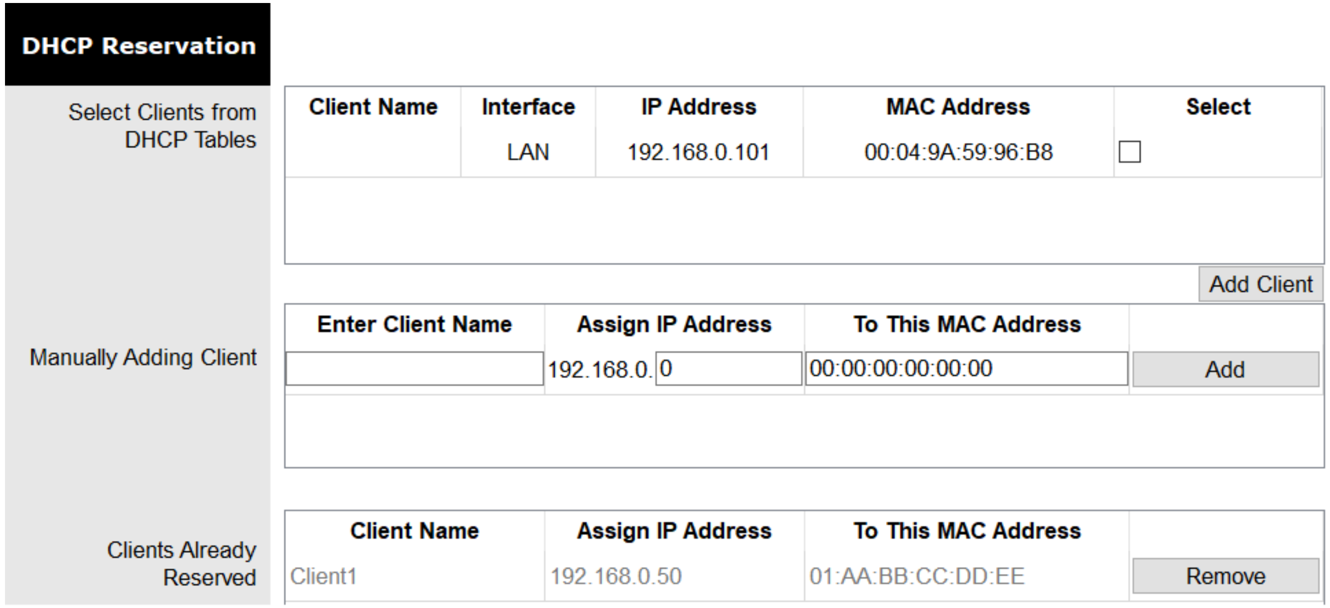
http://ecanet.ir/dhcp-option-list/



Network Setup

Router IP
IP Address: 192 . 168 . 0 . 1
Subnet Mask: 255.255.255.0

DHCP Server Settings
DHCP Server: ● Enabled ○ Disabled
DHCP Reservation
Start IP Address: 192.168.0. 100
Maximum number of Users: 50
IP Address Range: 192.168.0. 100 - 149
Client Lease Time: 0 minutes (0 means one day
Static DNS 1: 8 . 8 . 8 . 8
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0



DHCP Reservation

Select Clients from DHCP Tables

Client Name	Interface	IP Address	MAC Address	Select
	LAN	192.168.0.101	00:04:9A:59:96:B8	□

Add Client

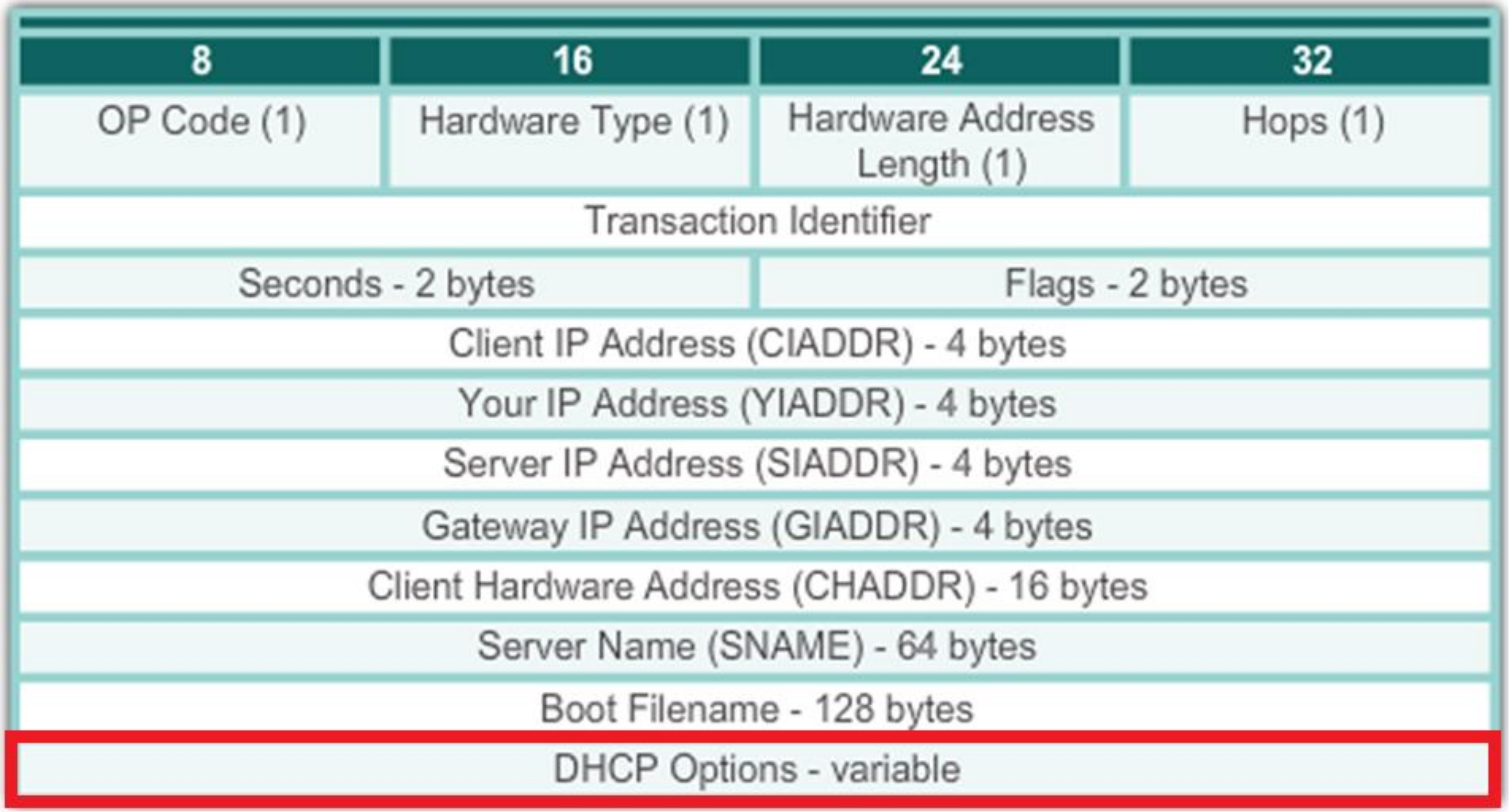
Manually Adding Client

Enter Client Name	Assign IP Address	To This MAC Address	
	192.168.0. 0	00:00:00:00:00:00	Add

Clients Already Reserved

Client Name	Assign IP Address	To This MAC Address	
Client1	192.168.0.50	01:AA:BB:CC:DD:EE	Remove

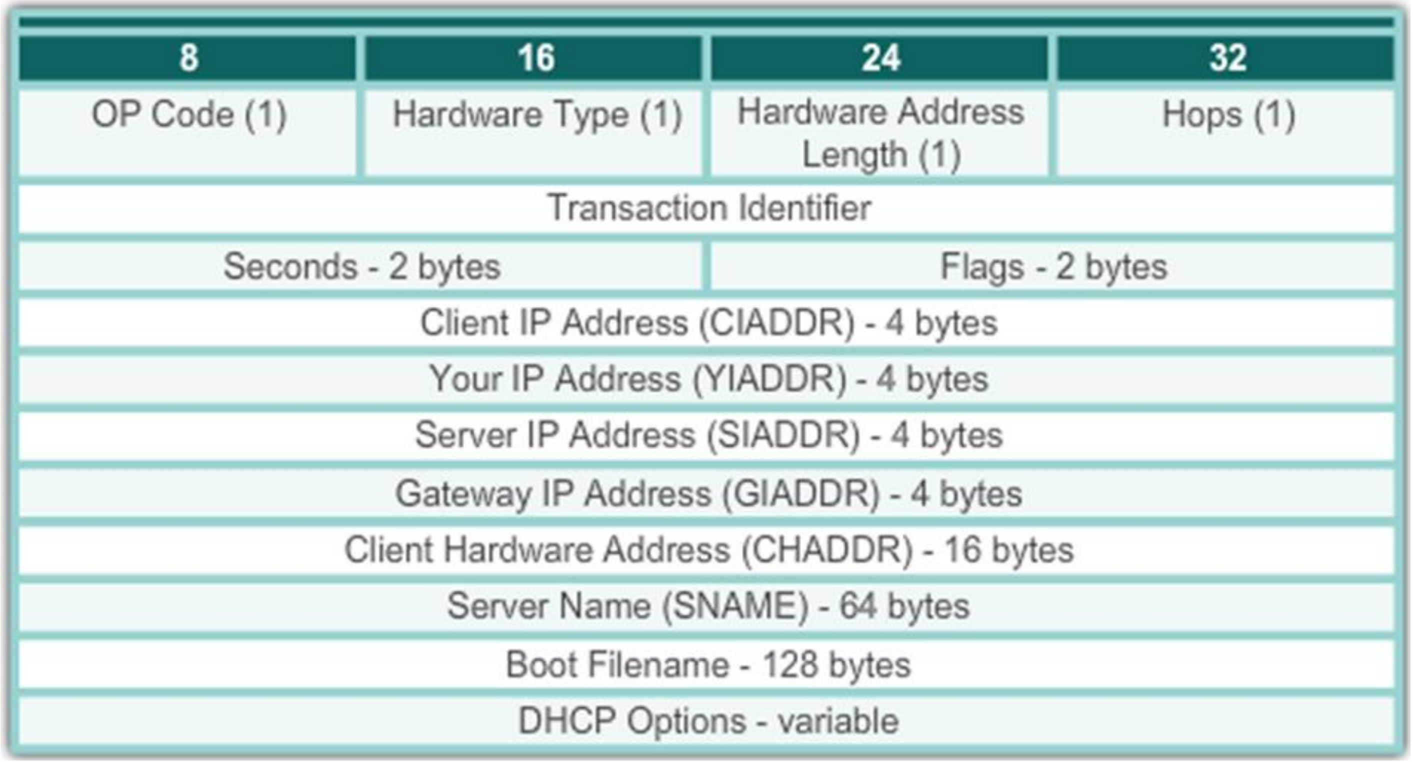
DHCPv4 Message Format



8	16	24	32
OP Code (1)	Hardware Type (1)	Hardware Address Length (1)	Hops (1)
Transaction Identifier			
Seconds - 2 bytes		Flags - 2 bytes	
Client IP Address (CIADDR) - 4 bytes			
Your IP Address (YIADDR) - 4 bytes			
Server IP Address (SIADDR) - 4 bytes			
Gateway IP Address (GIADDR) - 4 bytes			
Client Hardware Address (CHADDR) - 16 bytes			
Server Name (SNAME) - 64 bytes			
Boot Filename - 128 bytes			
DHCP Options - variable			

DHCPv4 Message Format

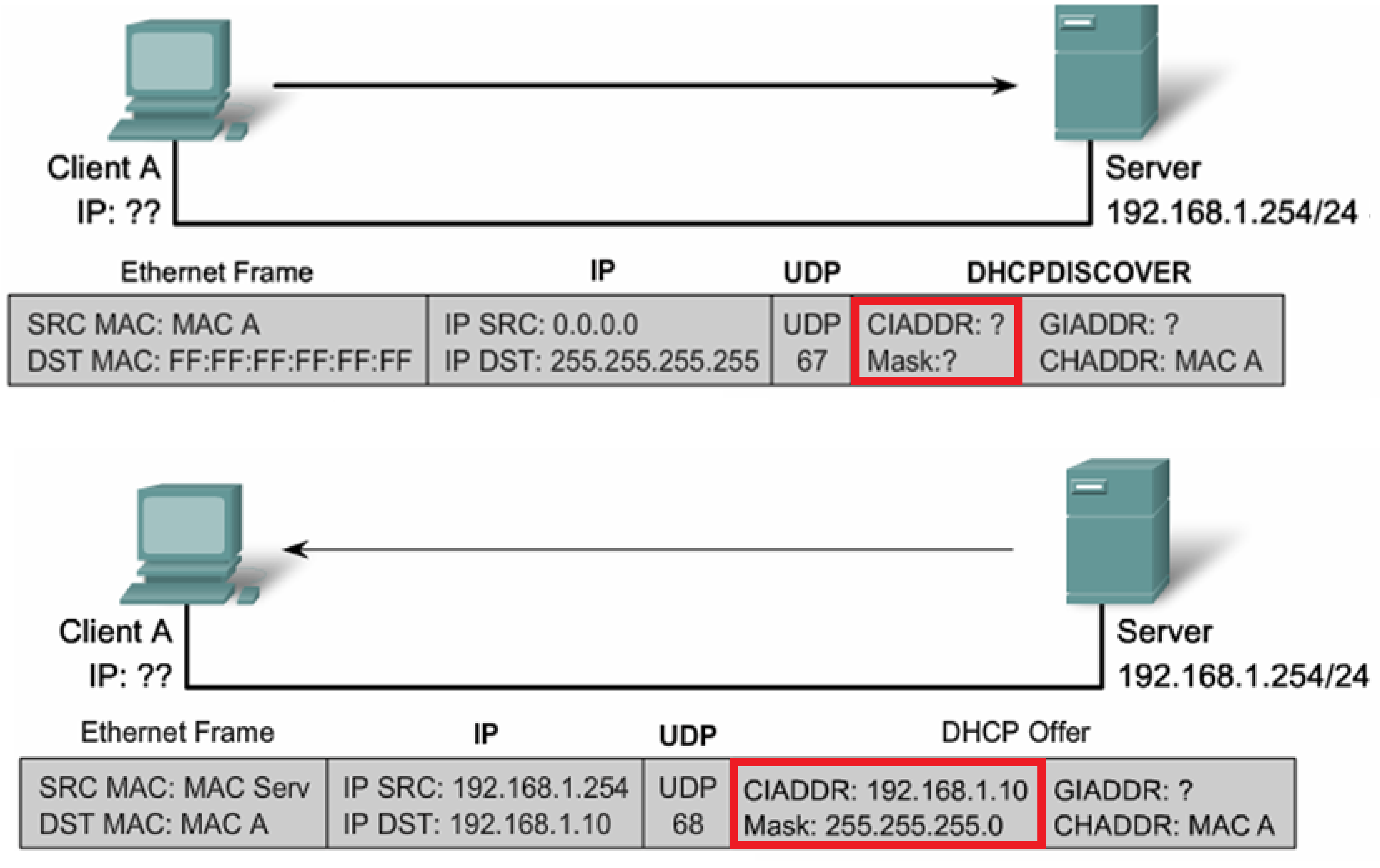
- **Hardware Address Length** - Specifies the length of the address.
- **Hops** - Controls the forwarding of messages. Set to 0 by a client before transmitting a request.
- **Flags** - Used by a client that does not know its IPv4 address when it sends a request. Only one of the 16 bits is used, which is the broadcast flag.
- **Server IP Address** - Used by the server to identify the address of the server that the client should use for the next step in the bootstrap process.



8	16	24	32
OP Code (1)	Hardware Type (1)	Hardware Address Length (1)	Hops (1)
Transaction Identifier			
Seconds - 2 bytes		Flags - 2 bytes	
Client IP Address (CIADDR) - 4 bytes			
Your IP Address (YIADDR) - 4 bytes			
Server IP Address (SIADDR) - 4 bytes			
Gateway IP Address (GIADDR) - 4 bytes			
Client Hardware Address (CHADDR) - 16 bytes			
Server Name (SNAME) - 64 bytes			
Boot Filename - 128 bytes			
DHCP Options - variable			

- **Gateway IP Address** - Routes DHCPv4 messages when DHCPv4 relay agents are involved. The gateway address facilitates communications of DHCPv4 requests and replies between the client and a server that are on different subnets or networks.

DHCP Discovery and Offer packets



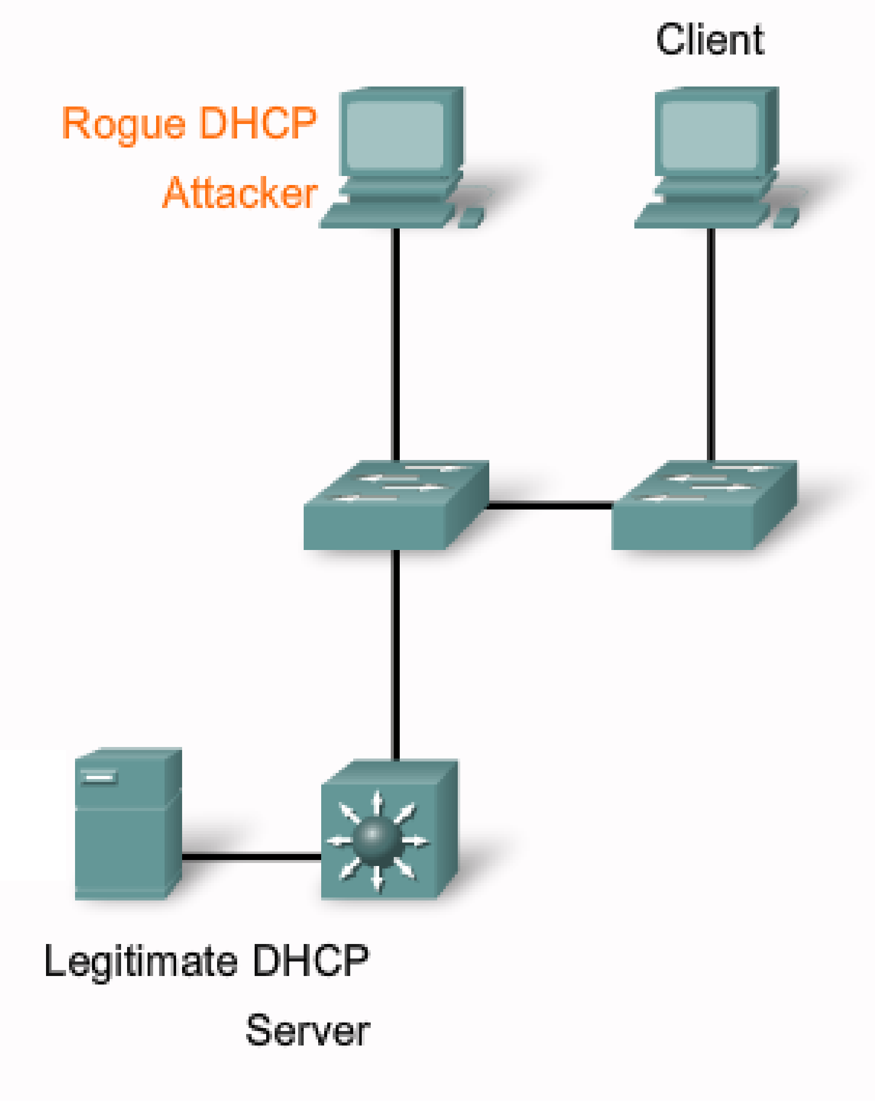
Ethernet Frame	IP	UDP	DHCPDISCOVER	
SRC MAC: MAC A DST MAC: FF:FF:FF:FF:FF:FF	IP SRC: 0.0.0.0 IP DST: 255.255.255.255	UDP 67	CIADDR: ? Mask:?	GIADDR: ? CHADDR: MAC A

Ethernet Frame	IP	UDP	DHCP Offer	
SRC MAC: MAC Serv DST MAC: MAC A	IP SRC: 192.168.1.254 IP DST: 192.168.1.10	UDP 68	CIADDR: 192.168.1.10 Mask: 255.255.255.0	GIADDR: ? CHADDR: MAC A

DHCP Spoofing Attack

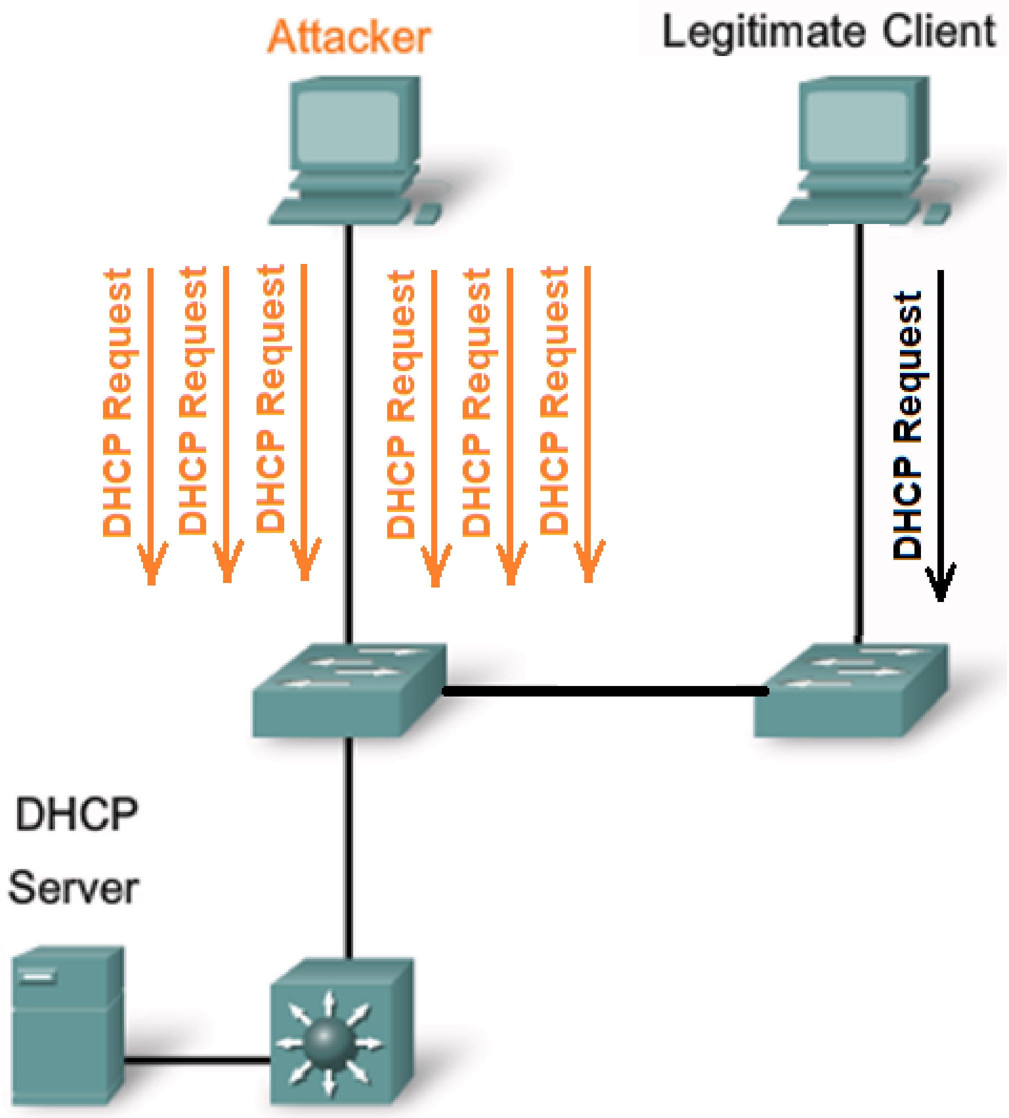
A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. A rogue server can provide a variety of misleading information:

- **Wrong default gateway** - Attacker provides an invalid gateway or the IP address of its host to create a man-in-the-middle attack. This may go entirely undetected as the intruder intercepts the data flow through the network.
- **Wrong DNS server** - Attacker provides an incorrect DNS server address pointing the user to a nefarious website.
- **Wrong IP address** - Attacker provides an invalid default gateway IP address and creates a DoS attack on the DHCP client.



DHCP Starvation Attack

- DHCP starvation attack is an attack that targets DHCP servers whereby forged DHCP requests are crafted by an attacker with the intent of exhausting all available IP addresses that can be allocated by the DHCP server.
- To hide the attack attacker uses MAC address spoofing
- Under this attack, legitimate network users can be denied service.



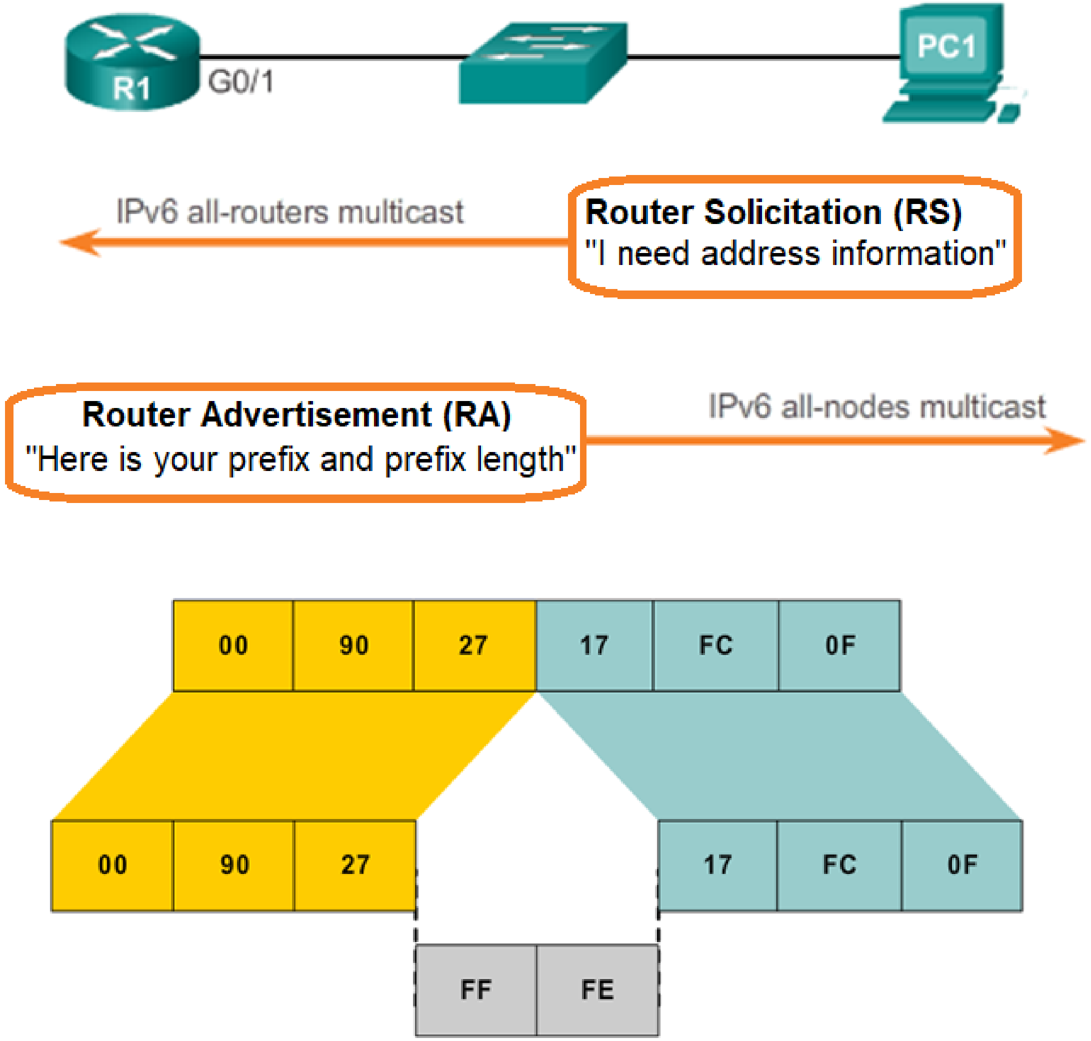
IPv6 dynamic global unicast addresses configuration

There are three methods in which IPv6 global unicast addresses can be assigned dynamically:

- **DHCPv6 Only** (Stateful DHCPv6)
- **Stateless Address Autoconfiguration** (SLAAC) - is a method in which a device can obtain an IPv6 global unicast address **without** the services of a DHCPv6 server.
- **SLAAC and DHCPv6** (Stateless DHCPv6) – is a combination of DHCPv6 and SLAAC, the IP-address is obtained via SLAAC, but other parameters via DHCPv6

Stateless Address Autoconfiguration

- The source of address information for the client is any router located on the same network as the client device.
- Router provides information about **network address** (prefix) and **prefix length**.
- Host ID (IID) creation ways:
  - **EUI-64** - Using the EUI-64 process, client will create an IID using its 48-bit MAC address.
  - **Randomly generated** - The 64-bit IID can be a random number generated by the client operating system.



IPv6 all-routers multicast

Router Solicitation (RS)
"I need address information"

Router Advertisement (RA)
"Here is your prefix and prefix length"

IPv6 all-nodes multicast

Summary

- DHCP service enables devices on a network to obtain IP addresses, subnet masks, gateway, and other IP networking parameters **dynamically** from a DHCP server.
- DHCP can pose a **security risk** via rogue DHCP servers or clients DoS attacks, then security measures need to be taken.
- Dynamic host configuration service is available **both** for **IPv4** and for **IPv6**