CS3103
Computer Networks Practice
github.com/securespider

01. Intro

Revision

DHCP Getting IP address, gateway and DNS server

- Uses DHCP Discover, Offer, Request, Acknowledge
- DHCP renew to
- DHCP release if no longer in use

ARP MAC address from IP address

- ARP Query, Reply (only within same network)

DNS Mechanism to get IP from URL

- DNS query, recursive DNS/resolvers, Authoritative DNS

HTTP Application layer TCP connection

- HTTP Request, Response

Subnet Interface with same subnet-ID

- Classful vs Classless
- Security, performance(reduce broadcasts and collisions)

Supernet Merging small networks into larger network w single prefix

NAT Network Address Translation: Changing private addresses to public addresses

02. ARP/DHCP

ARP

Proxy ARP Host or router responds to ARP request for host on other networks

Gratuitous ARP Sends ARP request for its own IP

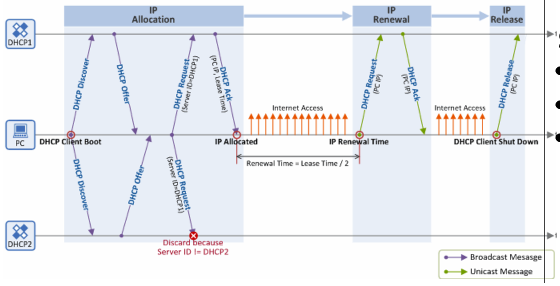
- Detect if there is other host sharing same IP address
- Utilised after IP assigned by DHCP

Vulnerability (ARP Poisoning)

- Forgery of requests and reply
- Stateless protocol: Replies can be sent without requests
- Must update ARP cache with new reply

DHCP

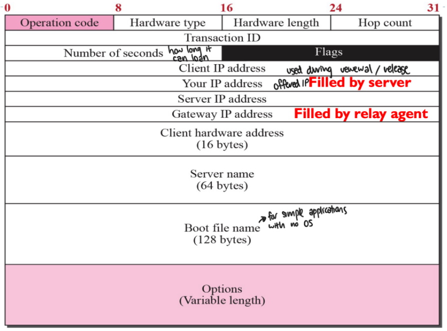
- Allocation of IP addresses from a pool
  - Static configuration for indefinite time (routers)
  - Automatic configuration
  - Dynamic configuration for specific duration (loans)
- Server waits on UDP 67 and Client communicates on UDP 68



Relay Agent

- Device that forwards requests to one of more DHCP server
  - DHCP server does not have to be in same subnet
- Places its IP address in router-address field
- Increments hop count by 1

Packet Format



Field OP 1 - request, 2 - reply

HTYPE and HLEN Network hardware type and length of address

- Ethernet is type 1 and length 6

Hops Initialised as 0 and increments whenever passing through another router

Xid Transaction ID to match response to request

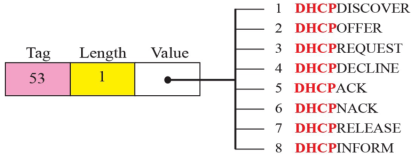
Seconds Type since client boot

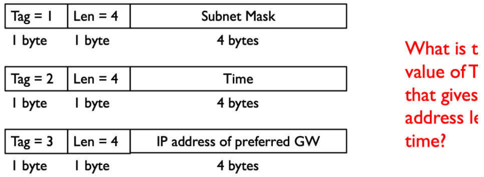
Flags Indicate broadcast(1) and other reserved use

- When client cannot accept unicast, MSB set to 1 (broadcast)

.. All known is field, the rest set to 0

Option Used mostly in reply for addi info to client




Tag = 1 | Len = 4 | Subnet Mask
1 byte | 1 byte | 4 bytes

Tag = 2 | Len = 4 | Time
1 byte | 1 byte | 4 bytes

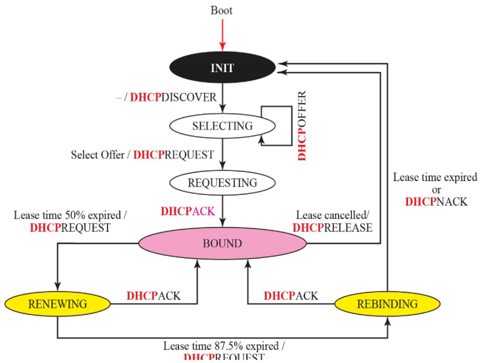
Tag = 3 | Len = 4 | IP address of preferred GW
1 byte | 1 byte | 4 bytes

What is t
value of T
that gives
address le
time?

Server

- Server stores a (key, value) pair for each client
- Key identifies client (IP-subnet and MAC address)
- Value is IP address assigned and lease time
  - Leased time represented in seconds in relation to client clock
  - Lease expiration = time client sent DHCPReq + Lease duration DHCPAck
  - 0xFFFFFFFF == infinite time

Process


Boot
INIT
– / DHCPDISCOVER
SELECTING
DHCPOFFER
Select Offer / DHCPREQUEST
REQUESTING
DHCPACK
BOUND
Lease time 50% expired / DHCPREQUEST
Lease cancelled/ DHCPRELEASE
Lease time expired or DHCPNACK
RENEWING
DHCPACK
DHCPACK
REBINDING
Lease time 87.5% expired / DHCPREQUEST

- Rebinding may have diff info vs Renew = same info