CA169: Week 8

ARP, DHCP, DNS AND ICMP

RECAP

- Last week we covered TCP & UDP
- Two of the main protocols for TCP/IP communication
- TCP – 3 way handshake
    - SYN
    - ACK
    - SYN/ACK
- UDP – Fire and forget

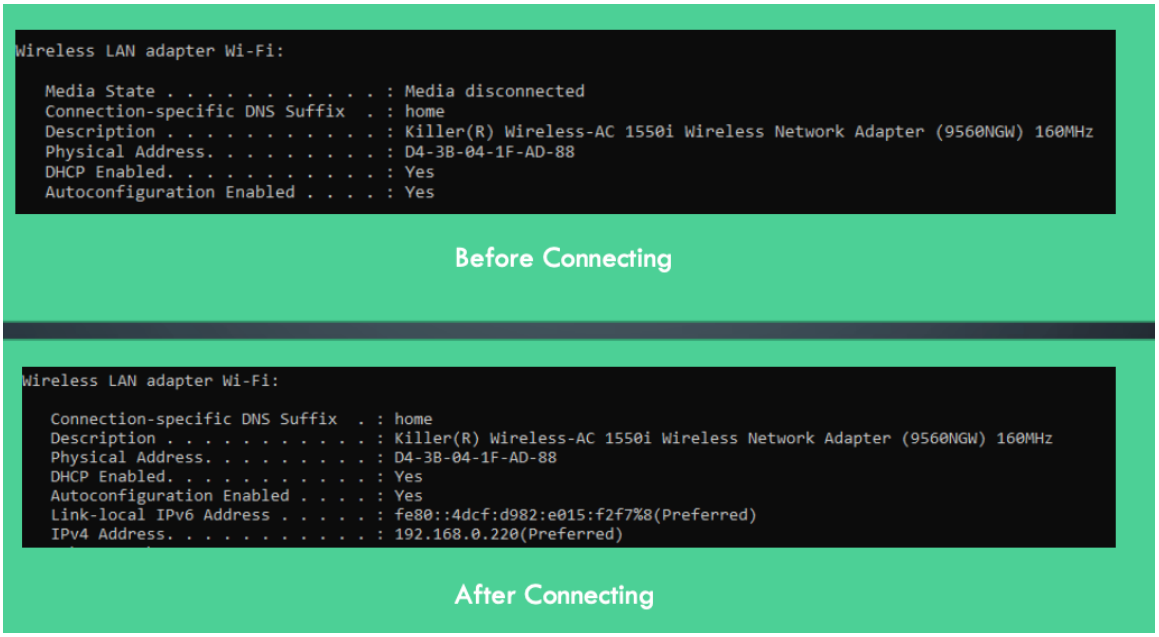
TODAY

- Helper protocols
- ICMP – general helper messages
- ARP – So your router knows who you are
- DNS – What is the ip address of www.google.com ?
- DHCP – How do I get an IP address on my network?

WHAT'S A DHCP?

- DYNAMIC HOST CONFIGURATION PROTOCOL
- On your home network you connect to your router
- Once you're connected you will see that you have an IP address

CONNECTING TO NETWORK BEFORE AND AFTER

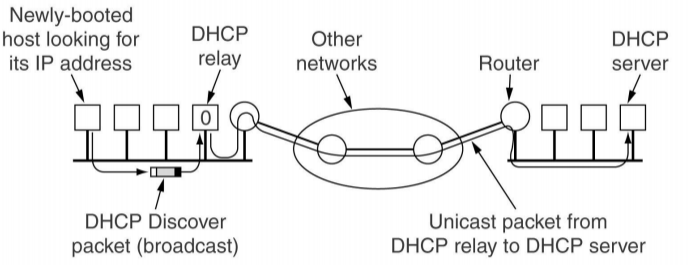


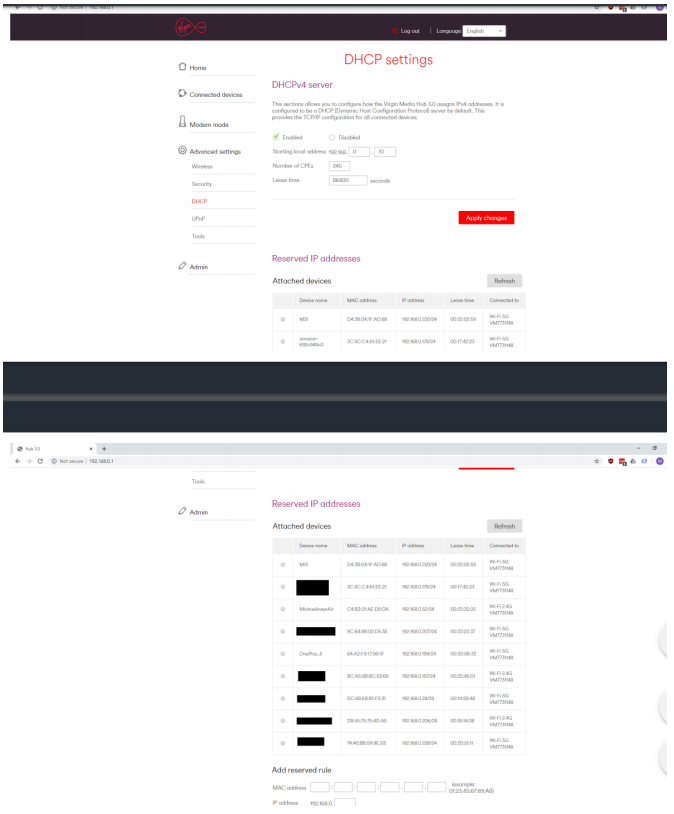
DHCP

- Allows manual IP assignment & auto assignment
- Replaces RARP & BOOTP
- Uses RARP server, not necessarily on same LAN
- DHCP relay agent exists on each LAN
- Normal operation – connection
- Workstation sends over MAC address
- Router adds IP + Mac to list of connected devices
- Machine is give IP

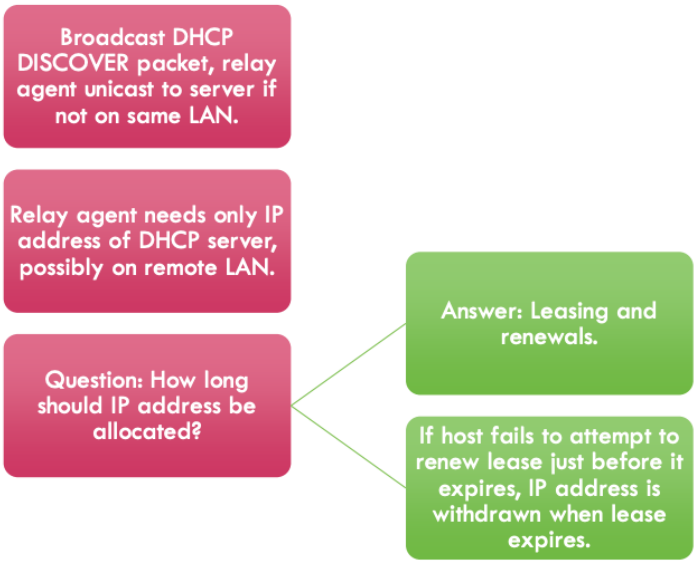
Connected Devices		
Name	**MAC**	**IP**
Printer	F6:AA:…	192.168.0.10
iPhone	AE:10:9F….	192.168.0.9
Workstation	64:5C:…..	192.168.0.11

- Allows manual IP assignment & auto assignment
- DHCP relay agent exists on each LAN





DHCP OPERATIONS



A NOTE ON LEASES

- DCHP gives out IP addresses
    - How many IPv4 addresses do we have?
- Routers are computers with small amounts of memory
    - 256 connected devices – what does this mean ?
- Am I always connected to my network ?

DHCP EXPERIMENT

- Note: do not do this if you are watching me live on stream!
- Open wireshark and start a capture
- Tell the router you are done with your IP address

```
ipconfig /release
```

- Now refresh your information

```
ipconfig /renew
```

- Refresh again

```
ipconfig /renew
```

- And release again

```
ipconfig /release
```

- Lets check wireshark! (dchp.cap on loop)
- Client lists info required
    - Address of local router
    - Subnet mask
    - Domain name
- Server responds with DHCP OFFER msg
    - Broadcast so that IPless station will read it
    - Contains IP address, local router, subnet mask, domain name & local domain name server
- Client indicated acceptance of address by echoing DHCP REQUEST with same information.

DHCP LEASES

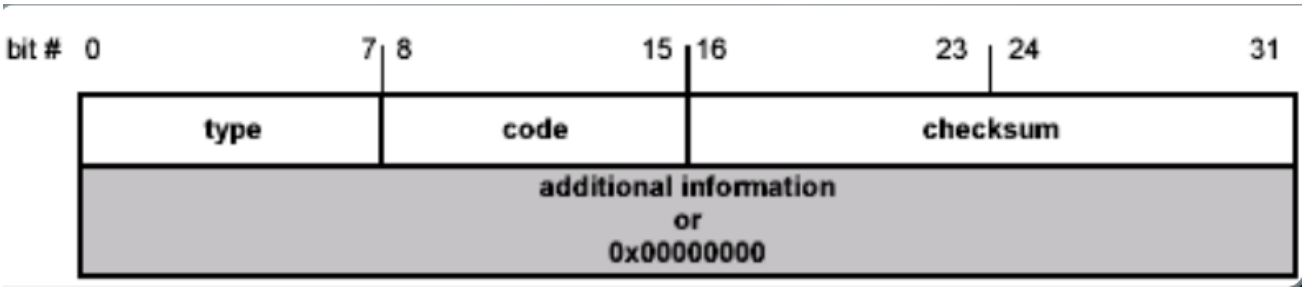
- IP addresses are leased only, not forever.
- Packets 14 & 15 show process of lease renewal.
- They happened because of our second ipconfig /renew command
- DHCP ACK includes duration of lease renewal (one day).
- If a lease expires, DHCP server is free to reallocate that IP address.
- The final ipconfig /release allows DHCP server to reallocate out IP address, thus recycling it.

ICMP

- INTERNET CONTROL MESSAGE PROTOCOL
- The IP (Internet Protocol) relies on several other protocols to perform necessary control and routing functions:
- Control functions (ICMP)
- Multicast signaling (IGMP)
- Setting up routing tables (RIP, OSPF, BGP, PIM, …)
- We will look at one of the simpler functions (e.g. PING)
- Helper protocol
- Supports:
- Error reporting
- Simple Queries
- All messages encapsulated as IP datagrams

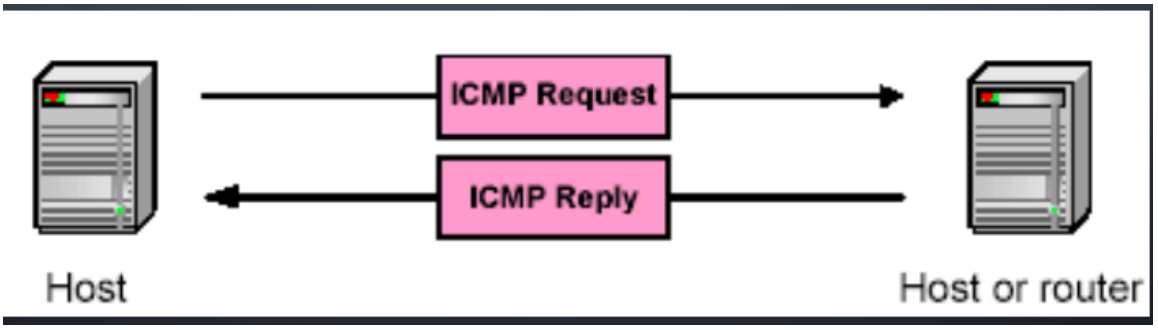
MESSAGE FORMAT

- 4 byte header:
- Type (1 byte): type of ICMP message
- Code (1 byte): subtype of ICMP message
- Checksum (2 bytes): similar to IP header checksum.
- Checksum is calculated over entire ICMP message
- If there is no additional data, there are 4 bytes set to zero.
- Each ICMP messages is at least 8 bytes lon



ICMP QUERY MESSAGE

- Simple request & response
- ICMP Request sent by host to a router or host
- ICMP Reply sent back to querying host



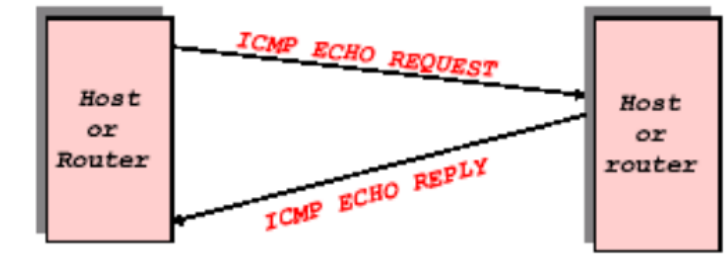
EXAMPLE ICMP QUERIES

- The ping command uses Echo Request/ Echo Reply

Type/Code:	Description
8/0 Echo	Request
0/0 Echo	Reply
13/0	Timestamp Request
14/0	Timestamp Reply
10/0	Router Solicitation
9/0	Router Advertisement

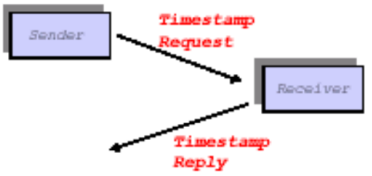
PING ECHO REQUEST AND REPLY

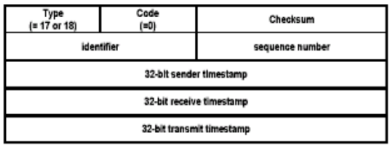
- Pings are handled directly by the kernel
- Each Ping is translated into an ICMP Echo Request
- The Pinged host responds with an ICMP Echo Reply
- The data portion of the request can be padded out to any size and is replicated in the reply
    - Useful for testing MTU and/or fragmentation
    - cf. “Ping of Death” DoS attack



ICMP TIMESTAMP

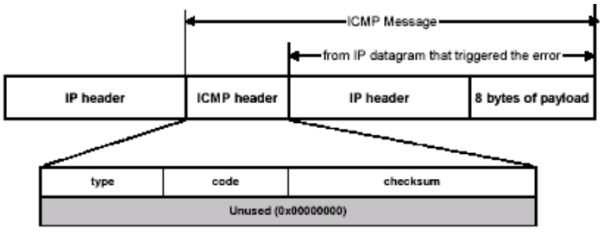
- A system (host or router) asks another system for the current time.
- Time is measured in milliseconds after midnight UTC (Universal Coordinated Time) of the current day
- Sender sends a request, receiver responds with reply

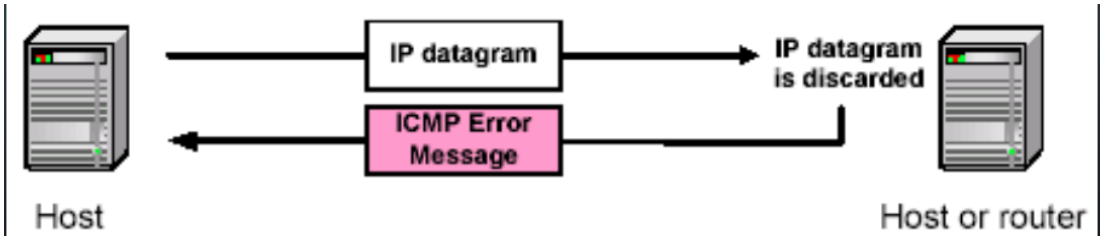




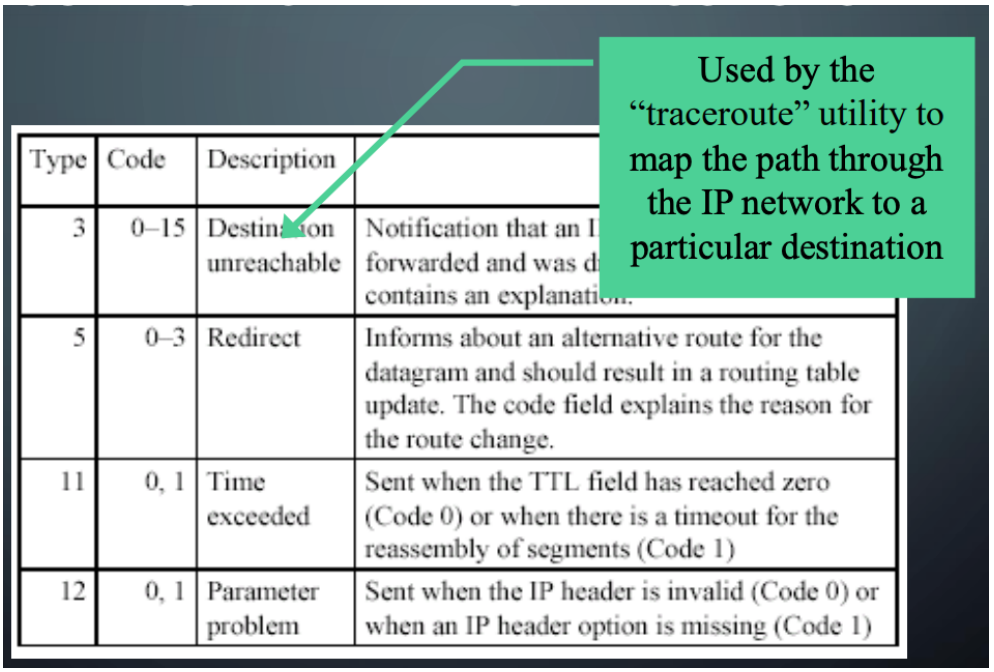
ICMP ERROR MESSAGE

- ICMP error messages report error conditions
- Typically sent when a datagram is discarded
- Error message is often passed from ICMP to the application program
- ICMP error messages include the complete IP header and the first 8 bytes of the payload (typically: UDP, TCP)





COMMON ICMP ERROR MESSAGES



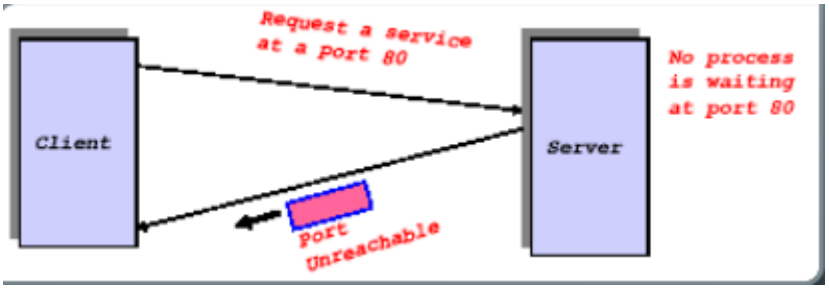
Type	Code	Description	
3	0–15	Destination unreachable	Notification that an I… forwarded and was d… contains an explanation.
5	0–3	Redirect	Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change.
11	0, 1	Time exceeded	Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1)
12	0, 1	Parameter problem	Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1)

DESTINATION UNREACHABLE

Code	Description	Reason for Sending
0	Network Unreachable	No routing table entry is available for the destination network.
1	Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests.
2	Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination.
3	Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application.
4	Fragmentation Needed and DF Bit Set	IP datagram must be fragmented, but the DF bit in the IP header is set.

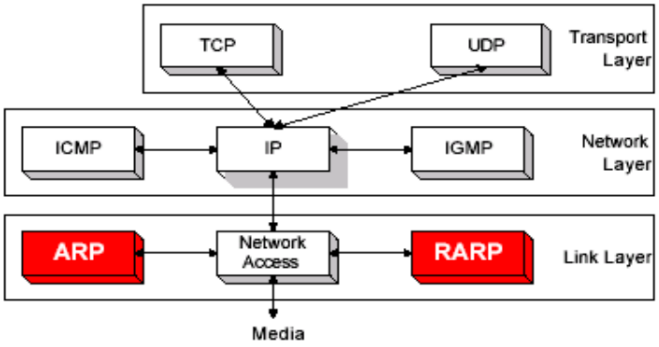
ICMP PORT UNREACHABLE

- From RFC 792: If, in the destination host, the IP module cannot deliver the datagram because the indicated protocol module or process port is not active, the destination host may send a destination unreachable message to the source host.



ARP

- ADDRESS RESOLUTION PROTOCOL
- The Internet is based on IP addresses
- Data link protocols (Ethernet, FDDI, ATM) may have different (MAC) addresses
- The ARP and RARP protocols perform the translation between IP addresses and MAC layer addresses
- ARP performs a lookup service that finds a MAC address for a given IP address.
- A system that needs a MAC address for a given IP address broadcasts a query which contains the IP address to all systems on the network.
- If a system receives the query and the IP address in the message matches its own IP address, it sends its MAC address to the sender of the query.



- IP and MAC addresses are the usual but not the only formats available to ARP

OPERATION OF ARP

- Each host maintains a table, the ARP cache, temporarily stores the results from previous address resolutions.
- ARP Request is broadcast to all systems on the network.
- In Ethernet, a frame is broadcast when the destination MAC address is set to broadcast address ff:ff:ff:ff:ff:ff.
- A broadcast frame is received and processed by all hosts.
- If a system receives the ARP request and the IP address in the message matches its own IP address, it issues an ARP Reply message to the sender of the query.

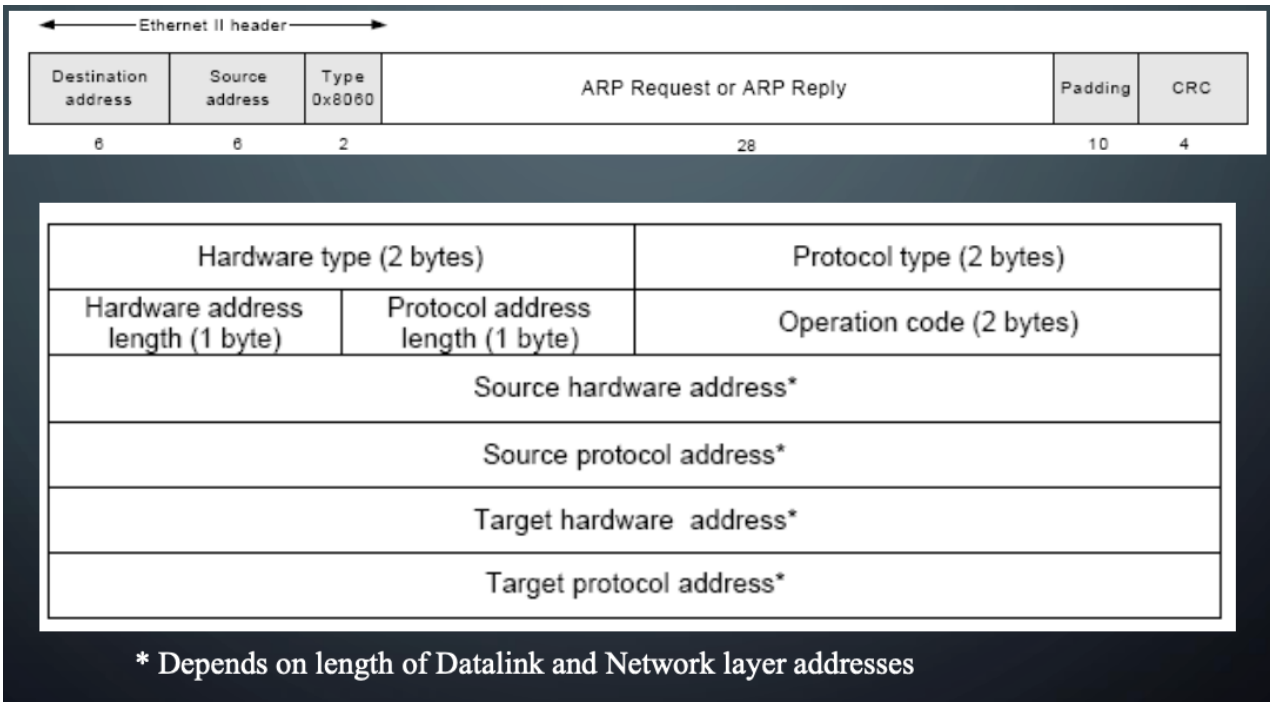
GRATUITOUS ARP

- Every host that sees an ARP Request verifies its ARP cache checking for the sender IP of the ARP Request.
- If such an entry exists, it updates the MAC address with the address in the ARP Request.
- Since ARP Requests are broadcast message, these updates are made by all systems each time an ARP Request is transmitted on the network.
- This feature is exploited in a concept that is called gratuitous ARP.

ARP VULNERABILITIES

- ARP may be used to redirect traffic intended for a certain IP address to another on the NW
- Broadcast ARP replies with invalid MAC addresses insert incorrect entries into ARP caches.
    - Poison ARP attack

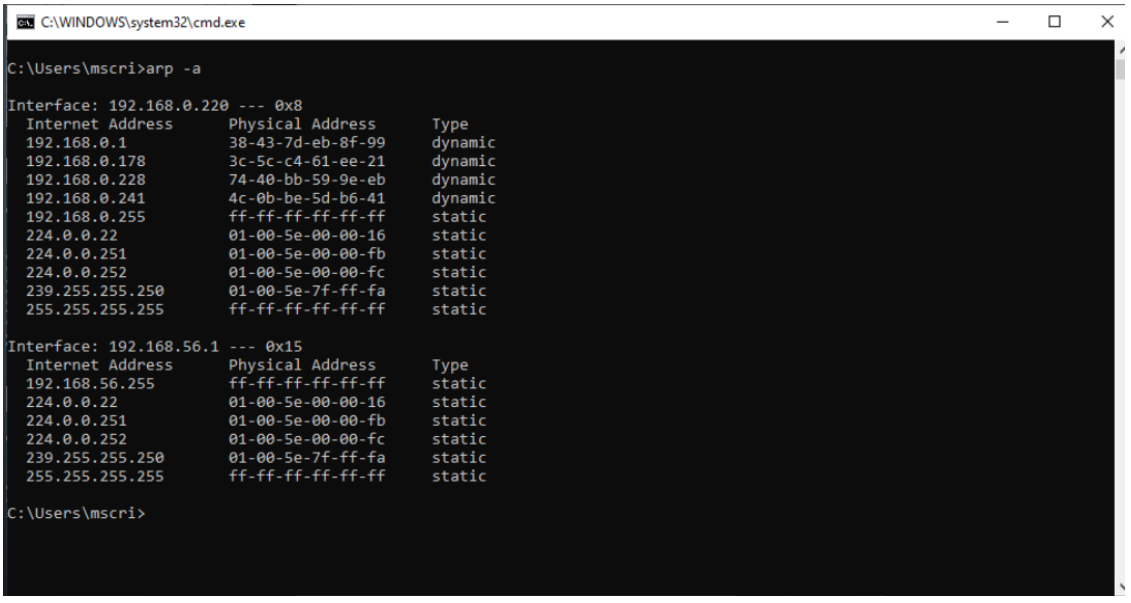
ARP PACKET FORMATS



NOTE: ARP PACKET FORMATS

- Ethernet carries ARP, with type set to 0x8060
- ARP message, in IP and Ethernet scenario is 28 bytes (48 bit MAC + 32 bit IP)
- Hardware type is datalink protocol
    - Ethernet = 0x0001, 802 = 0x0006
- Protocol type field is the network layer used
    - IP = 0x8000
- Operation code is 0x0001 for ARP requests and 0x0002 for ARP replies
- Hardware address length and Protocol address length specify length of addresses (MAC-6, IP-4).
- The next four fields contain the hardware address and the network address of the sender and the intended receiver of the ARP packet.
- The former is referred to as the source and the latter is referred to as the target.

An ARP, the Router, and My PC



arp Tool

- Issue `arp` command
- Tells you how to use it
- Issue `arp –a` it dumps its cache
  >arp –a I
  nterface 192.168.0.105 --- 0x10004

Internet Address	Physical Address	Type
192.168.0.1	00-06-25-8d-be-1d	dynamic
192.168.0.100	00:07:e9:53:87:d9	dynamic

MAKE DATA

- Issue `ping –n 1 192.168.0.1` from A
- Machine A sends a request message to B
- Check out arp.cap for results
- Note the source and destination addresses used in this trace.
- Now delete the arp cache with

```
arp –d 192.168.0.1
```

- Do second `ping –n 1 192.168.0.1`
- A issues arp request
- B replies , replenishing arp cache of A and allowing it to issue a ping request
- Finally issue third

```
ping –n 1 192.168.0.1
```

ARP EXERCISE

- Replicate the previous experiments
- Use `arp` and `ipconfig` to find out the IP and MAC addresses of the machines, clear the caches etc as done in the experiments. You will need 2 machines to do this.
- Something new:
- Check out the CRC calculations in the frames and account for any discrepancies.
- Use appropriate filters in Wireshark to limit captured traffic to that of interest for the experiment.
- Save your traces in Wireshark to a file.
-

PROXY ARP

- Proxy ARP is a configuration option for IP routers, where an IP router responds to ARP
- Request that arrive from one of its connected networks for a host that is on another of its connected networks.
- Without Proxy ARP enabled, an ARP Request for a host on a different network is unsuccessful, since routers do not forward ARP packets toanother network.

RARP

- Given an Ethernet address, what is the IP?
- RFC 903 – RARP sovves this problem – Broadcasts MAC gets back IP from RARP server.
- Broadcast address stays within 1 domain (router)
- Needs to get further or else have 1 RARP server in each MAC broadcast domain.
- Solution – use BOOTP

BOOTP

- RFCs 951, 1048, 1084
- Use UDP messages, broadcasts forwarded over routers!
- Also provides
    - info on IP of file server with disk image
    - IP address of default router
    - Subnet mask
- Problem: Manual config of IP – MAC, gives rise to errors.

WHY DNS

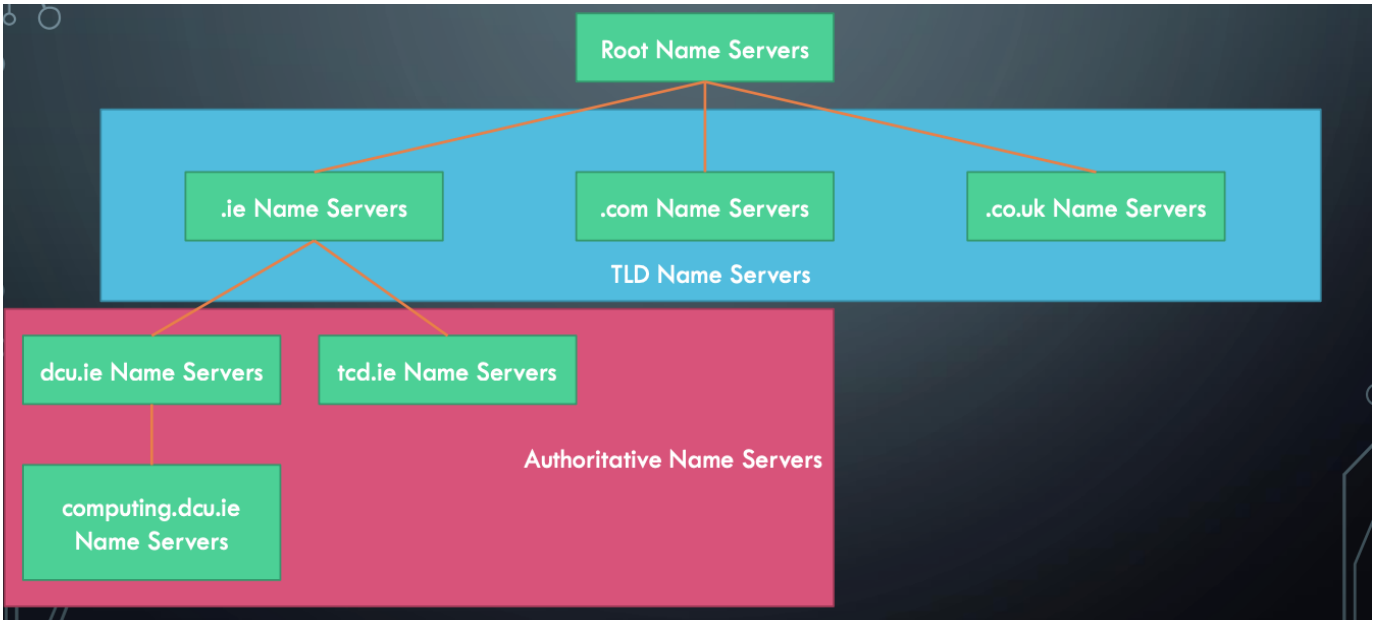
- DOMAIN NAME SYSTEM
- When you make a connection to a remote server you usually supply a domain name (e.g. www.google.com)
- The TCP/IP stack is used to send/receive data from remote computers
- The method for addressing in TCP/IP is an IP address
- How does www.google.com get resolved into an IP address
- Answer: DNS the Domain Name System

WHAT IS DNS

- A phone book mapping domain names to ip addresses
- When the number of domain names was small we used hosts.txt stored on your machine
- E.g. www.google.com 74.125.193.947
- Hosts.txt still exists!!
- C:\Windows\System32\Drivers\etc\hosts
- As the number of domain names grew, this solution became unworkable
- Essentially it's a server (DNS server) with a database of IP addresses
- When you send it a domain name, it returns an IP address
- This process is called a DNS lookup (or DNS resolve)

DNS STRUCTURE

- Think of how many times per second/minute people are visiting domains
    - Browsing
    - Email
    - Social Media
    - Phone apps
    - A single server would not be able to handle this load!
- The DNS system is structured to handle this
- The DNS database is distributed
    - There is no single DNS database
    - It is split into parts and distributed across the world
- The DNS database is structured
    - There are rules guiding what part of the database each server has
- The DNS database is replicated
    - Multiple copies of each database exist
- Root Name Servers
- Top Level Domain Name Servers
- Authoritative Servers
- Local Name Servers



DNS ROOT NAME SERVER

- Contacted first in order to find out the ip address for a domain
- Decides which TLD server to forward the request to
- There are many root name servers spread across the world
- Check: https://root-servers.org/

DNS - TLD NAME SERVERS

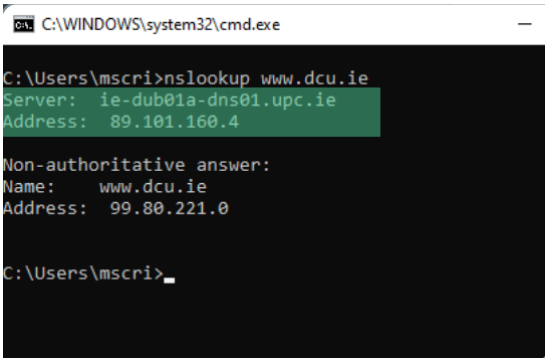
- Manages the DNS mappings for a top level domain
  - .com
  - .ie
  - .org
- ..ie name servers are managed by RIPE NCC
  - https://www.ripe.net/
    - RIPE also assigned us with our Class B address !

DNS - AUTHORITATIVE NAME SERVERS

- DNS mappings provided by an organisation
- E.g. HEANET manage the network infrastructure for third level universities in Ireland
- They contain the DNS mappings for DCU, TCD, UCD etc..
- Authoritative name servers can also be DCU itself
  - Mappings for “computing.dcu.ie”
- Computing.dcu.ie is also an authoritative name server
  - student.computing.dcu.ie

DNS – LOCAL NAME SERVERS

- There are also local name servers
- When you make a request from your home network you will use your network providers name server at first instance
- You can use nslookup to determine which name server is being used
- The local name server caches the addresses of common domains
  - E.g. www.google.com
-



DNS – ADDRESS RESOLUTION

- A user wants to visit student.computing.dcu.ie
- The local name server is first queried
- If it is not in the local name server, ask root server
- Root server returns the address of the TLD server
- The .ie server is then asked
- This returns the authoritative name server address
- We then ask the authoritative name server
- Finally we ask the last server
- Our address is returned
-