

ARP and DHCP Protocols

CO1507 Introduction To Networking

Jonathan Edwards 2023

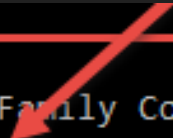
What is ARP

- **Address Resolution Protocol** (ARP) operates at **Data Link** layer of the **OSI model**
- ARP is essential for communication between hosts within an ethernet local area network
- ARP requires the use of **broadcasts** in order to operate

Logical V Physical Addressing

- Hosts on an Ethernet local area network are identified by their **IP address** (at layer 3 of the OSI model)
- IP addresses are an example of **logical addressing**
- **IP addresses** are assigned by users (or by software created by the users)
- Even if a server assigned those addresses this is essentially still configured by users
- Network Interfaces however are identified by their **MAC address** or **Physical Address**
- A **MAC address** is a **48 bit** address assigned at the factory by the manufacturer
- Written in **HEX**

```
Connection-specific DNS Suffix  . :  
Description . . . . . : Realtek PCIe GBE Family Controller  
Physical Address. . . . . : 40-8D-5C-23-63-BA  
IPsec Enabled . . . . . : No
```

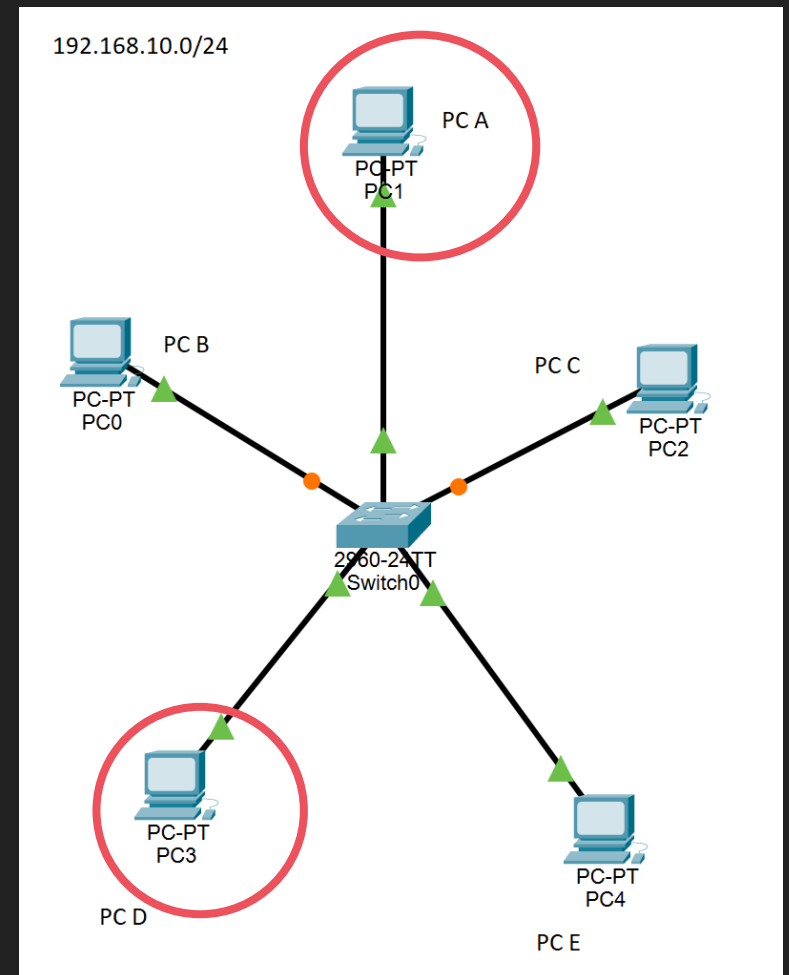


MAC address

- A MAC address is 48 bits long
- This is split into 6 octets (8 bits)
- Each octet is expressed in Hex (00 -> FF, is the same as 0 -> 255)
- Remember all data is binary to the computer
- The **first 3 octets** represent the **Organisationally Unique Identifier** (OUI)
- This means it is specific to the company who manufactured it
- The **last 3 octets** represent the **Network Interface Controller** (NIC)
- This means the individual piece of hardware

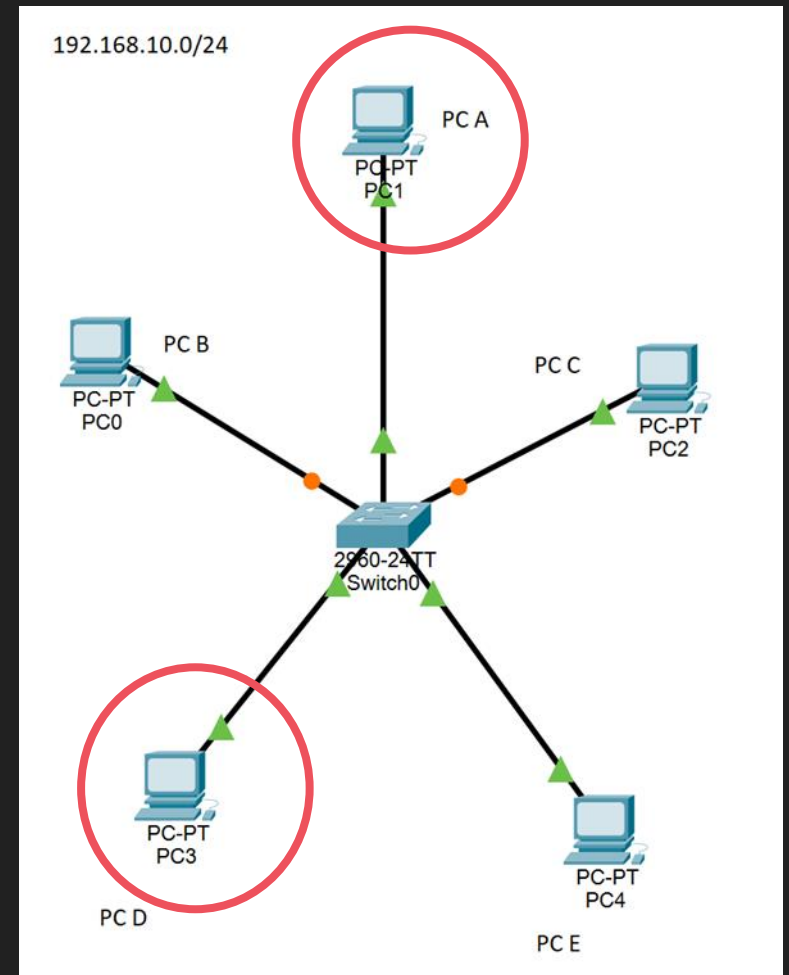
Why is ARP Needed?

- In this case **PC A** wishes to communicate with **PC D**
- **PC A** has an IP address of **192.168.10.2**
- **PC D** has an IP address of **192.168.10.5**
- The user of PC A types in "ping 192.168.10.5" at the command prompt
- How does **PC A** know...
 - Which network host that refers to?
 - Whether that IP address exists at all on any host within the LAN?
 - Whether the host with that IP address is turned on, or properly configured?
 - Answer: it doesn't!



Why is ARP Needed?

- For PC A s to communicate with PC D on the same LAN, it needs not only the **destination IP address** but also the **destination MAC (physical) address**
- Normally the host initiating communication knows (or *thinks* it knows) the **destination IP address** but NOT the **destination MAC address**
- So what do we do?
- We need **ARP**
- The function of **ARP** is to enable a host to obtain the **MAC address** corresponding to a known IP address.



How Does ARP Work?

- The ARP request is essentially like saying
'Which one of you has this IP address? please tell me your MAC address'
- PC A **broadcasts** to **all hosts** on the network sending out an ARP request frame as seen below:

ARP Request	Destination IP address	Source IP address	Destination MAC address [broadcast]	Source MAC address
	192.168.10.5	192.168.10.2	FF-FF-FF-FF-FF-FF	6a-21-23-3d-27-11

How Does ARP Work?

- The host with the IP address **192.168.20.3** will reply with its own MAC address using and **ARP reply** frame
- Notice how the **FF-FF-FF-FF-FF-FF** is replaced with **5c-45-21-e2-a7-23**

(Note: the **destination** addresses have now become **source** address, and vice versa)

ARP Response	Destination IP address 192.168.10.2	Source IP address 192.168.10.5	Destination MAC address 6a-21-23-3d-27-11	Source MAC address 5c-45-21-e2-a7-23
-----------------	--	-----------------------------------	---	---

How Does ARP Work?

○ REQUEST:

ARP Request	Destination IP address	Source IP address	Destination MAC address [broadcast]	Source MAC address
	192.168.10.5	192.168.10.2	FF-FF-FF-FF-FF-FF	6a-21-23-3d-27-11

○ RESPONSE:

ARP Response	Destination IP address	Source IP address	Destination MAC address	Source MAC address
	192.168.10.2	192.168.10.5	6a-21-23-3d-27-11	5c-45-21-e2-a7-23

How Does ARP Work

- **ARP** sends an **ARP request** frame to **all PCs** on the same LAN using a broadcast
- But it does not know the destination MAC address, in place of the destination MAC address, it uses a **broadcast** MAC address of **FF-FF-FF-FF-FF-FF** (48 1s in binary)
- The ARP request is sent to all PCs on the network because it uses the LAN's broadcast IP address
- A **broadcast address** is one where the entire **host id** address space is 1's in binary
- In this case it means an address ending **.255**

Broadcast Address

- 192.168.10.255

- 255.255.255.0

IP 11000000 10101000 00001010 11111111

Subnet mask 11111111 11111111 11111111 00000000

- All the host address space is 1' in binary (255 in this case)
- This is a **broadcast address**
- Every LAN will have one, whenever all the host bits are 1
- Just as every LAN has a network address, where all the host part bits are 0

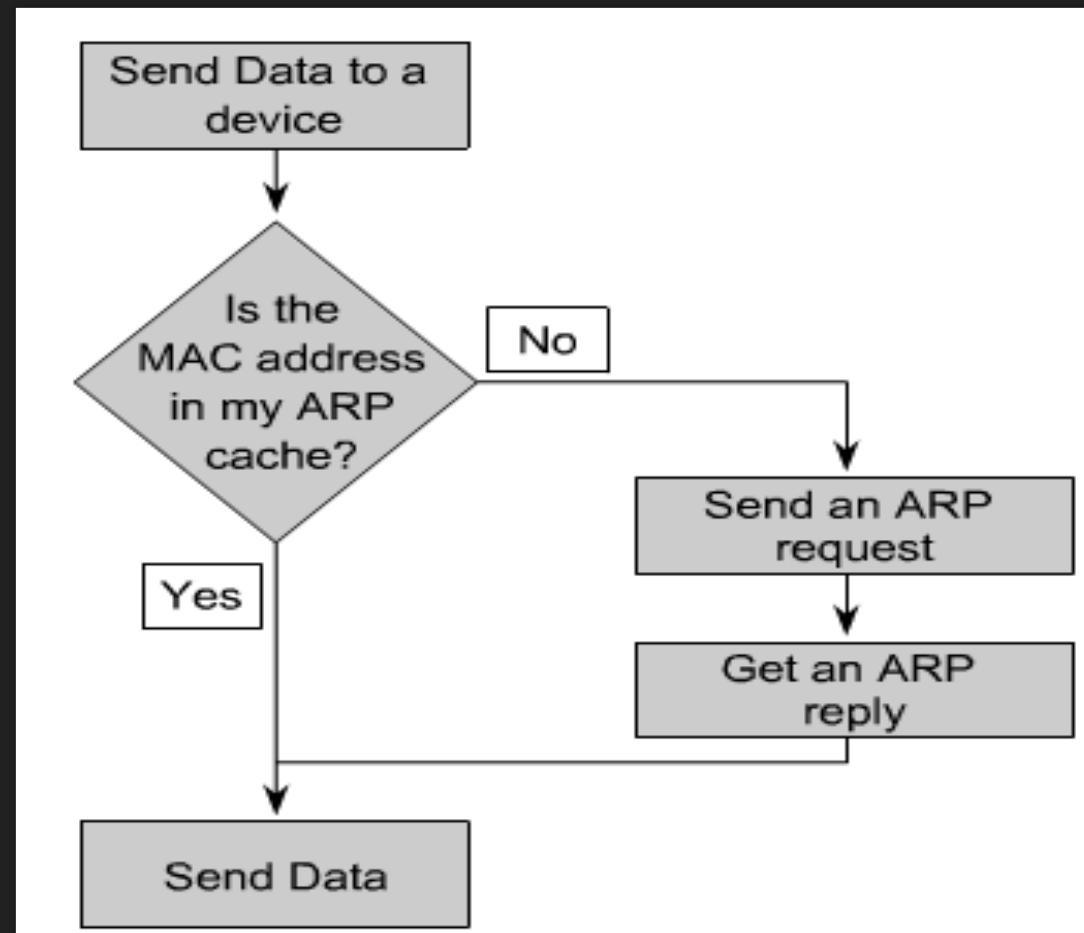
How Does ARP Work?

- Once PC A receives the destination MAC address, it inserts it in the frame for communication with PC B.
- The destination IP address and corresponding MAC address will then be stored by PC A in the **ARP table** as shown below

IP address	MAC address
192.168.10.5	6A-21-23-3D-27-11

- The **ARP table** from PC A now has an entry relating to **PC D**
- Every PC has its own **ARP table** to store data in.
- From here on, every time PC A needs to communicate with PC D, it checks to see if the entry is in the ARP table
- If it is, it uses it, if its not it uses ARP

ARP Flow Chart



ARP (A Windows Example)

- To see the contents of the **ARP table** in Windows use the command **arp -a** at the command prompt:

```
C:\Documents and Settings\local-admin>arp -a

Interface: 172.20.1.21 --- 0x2
    Internet Address      Physical Address      Type
    172.20.1.19           00-01-03-d5-20-17    dynamic

C:\Documents and Settings\local-admin>arp -d

C:\Documents and Settings\local-admin>arp -a
No ARP Entries Found
```

- To delete the contents of the ARP table, use the command, **arp -d**
- Use the **arp -a** command again to confirm that the contents have been deleted

ARP Tables

- The main reason for having the **ARP table** is to avoid sending broadcast messages every time any host communicates with another
- Broadcasts are necessary but slow down the performance of a network
- Every time you have broadcasts, the network becomes busy, host can't access it
- If we have too many broadcasts, the network becomes congested
- Therefore, broadcasts need to be kept to a minimum
- Excessive broadcast traffic would bring the performance of the network down

ARP Tables

- ARP entries don't last for ever if not refreshed, they have an aging process
- They are deleted after 2 minutes
- This ensures that hosts don't continue to rely on stale records
 - e.g. what is a host in the ARP table is shutdown, or has it's IP address changed, or is removed from the LAN altogether?

DHCP

- With a large network it may not be practical or desirable to use static addressing where a human technician assigns all addresses
- A lot of time would be consumed configuring PCs doing the same setup over and over again
- This is not easily scalable and is not dynamic
- What if a host is removed or turned off? what becomes of its IP address? can it be re-used elsewhere?

DHCP

- What about networks where hosts regularly join and then leave again within a relatively short time frame e.g. a Wi-Fi network in a public place?
- **Dynamic Host Configuration Protocol** (DHCP) is the solution
- **DHCP** can automatically allocate IP Addresses, Subnet Masks, Default Gateways etc. to hosts on a dynamic and scalable large scale network.
- A **DHCP** server is one running software dedicated to this one task
- DHCP is considered an **Application Layer** protocol

DHCP Server

- A **DHCP** server waits and listens for **DHCPDiscover** broadcasts from host clients
- The server then sends out a **DHCOffer** to the clients
- The host client may then accept the offer of an IP address
- A full **DHCPack** is then sent containing the IP, Subnet Mask, Default Gateway, and any other addresses depending on what is needed

DHCP server

- A **DHCP** server selects IP addresses from a 'pool' of available addresses
- These addresses will typically all belong to the same network address with the same subnet mask
- When a **DHCP** client host is turned off or removed from the network the IP address is released back into the pool and can be re-allocated elsewhere
- **DHCP** server pairs **IP addresses** with **MAC addresses** and records an **expiry** date/time for **leased** addresses
- DHCP uses the UDP transport layer protocol, and uses logical port 67 and 68

Configuring a DHCP server

- When configuring a DHCP server one must pay careful consideration to..
 - Choosing an appropriate pool of addresses
 - How many addresses will be required?
 - Which network address and subnet mask is appropriate?
 - E.g. if we need 300 addresses 192.168.10.0 and 255.255.255.0 is no use as it will only support 254 hosts
 - Do the hosts need to be configured with a default gateway or any additional information?

Packet Tracer DHCP Server

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.160.10.1

DNS Server: 0.0.0.0

Start IP Address: 192 168 10 2

Subnet Mask: 255 255 255 0

Maximum Number of Users: 128

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	512	0.0.0.0	0.0.0.0

☐ Top

A 3D rendering of a large yellow question mark standing on a field of smaller, dark grey question marks. The yellow question mark is the central focus, standing upright and casting a shadow. It is surrounded by a dense field of smaller, dark grey question marks that recede into the background, creating a sense of depth. The lighting is dramatic, with strong highlights and shadows.

Any Questions?