Data Communications Laboratory

Switches, MAC addresses and ARP

Your Name: Jai Carey

Your Student ID: 45188416

Documentation Task 1.

State what features you can see on the switches (ports, power switches, etc) and what you know of their functions.

24 Fast Ethernet Ports

- To connect multiple devices in the same network via a LAN connection

2 Gigabit Ethernet Ports

- Alternative to fast ethernet ports (Can be used to connect to servers and other networking devices in the LAN)

Power Cable (Powers the device)
Console Port (Looks like RJ45)

- Used to connect a PC so that we can locally display and communicate with the switch and look at diagnostics and settings of the switch

There appears to be indicator lights on the top left of the back side.

Documentation Task 2.

What IP address has been assigned to each computer? What other IP address appear to be in use on this network?

What switch port is each computer connected to?

Since we have manually set the IP addresses of the computers, PC#1 is set to 192.168.1.61 and PC#2 is set to 192.168.1.62.

Since there are only these 2 PCs on the network and the switch is a Layer 2 device, the switch does not have an IP address, only a MAC address.

This means that there are no more IP addresses on the network.

PC#1 is connected FastEthernet0/1
PC#2 is connected FastEthernet0/2

Documentation Task 3.

Document what software you used to check whether your network was working and what the results were.

We performed a PDU message of type ping (ICMP) between the 2 PCs and traced the packets to identify if the message was successful and any issues in the network.

This resulted in a success and we know that the PCs are connected and can communicate with each other.

As we are using Cisco Packet Tracer, we can use their PDU tool, however in a real life scenario, we can use the CMD prompt to ping each of the known IP addresses.

Documentation Task 4.

Include in your documentation what you consider to be the useful information from *ipconfig /all* for your laptop’s Ethernet connection.

Physical Address (MAC): 0030.A3E4.4241

IPV4 Address: 192.168.1.61

Subnet Mask: 255.255.255.0

Documentation Task 5.

Let’s have a look at the ARP table held by the laptops. Get a command window running (if you do not already have one). In the window type arp –a and press Enter.

What devices have an entry in the ARP table? Record this in your documentation.

Could you see the physical address of the other laptop(s) and the switch in your network? If not ping the other computer(s) and try arp –a again. Try all the IP addresses you found in use in your network. Are entries for them now in the table? Add the results to your documentation if necessary. Do any IP addresses share the same MAC address?

Both PCs have each other in the ARP cache – this links their IP Address to their MAC Address.

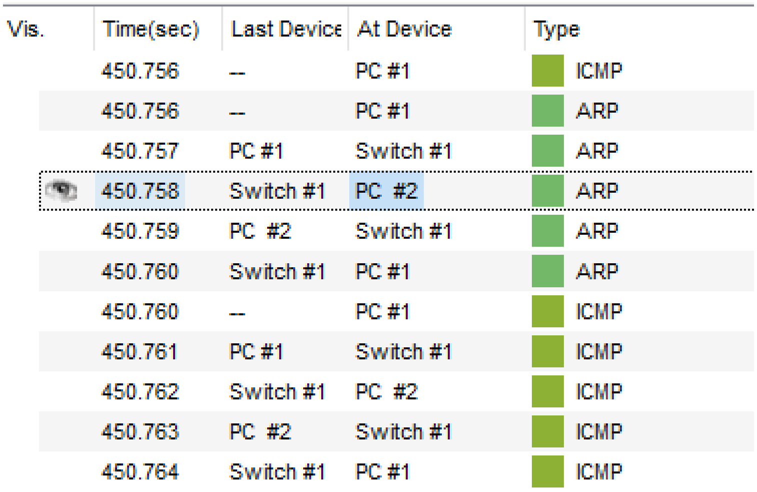
Yes, we can see the physical address of the other laptop. We cannot see the Switch in there because it has no IP address, so there is nothing to map in the ARP cache.

PC#1: 192.168.1.62 – 0060.3e76.50e2 – dynamic
PC#2: 192.168.1.61 – 0030.a3e4.4241 – dynamic

Documentation Task 6.

1. Does the arp table now contain an entry for each IP you pinged?
2. What are the hexadecimal values for the source and destination addresses in the first Ethernet frame in your capture containing an ARP request message?
3. Can you identify the arp messages corresponding to the all the entries in the arp table? List the two MAC addresses found in each pair of messages
4. Compare hexadecimal source and destination addresses to the information given in the source and destination fields of the main Wireshark packet summary window. Are they different? If so, what is the information telling you?
5. What else can you observe about the functioning of ARP from this capture?

1. The ARP cache of each PC now includes the other PC
2. 0030.A3E4.4241 >> FFFF.FFFF.FFFF (1st ARP Request Message)
3.



Vis.	Time(sec)	Last Device	At Device	Type
	450.756	--	PC #1	🟩 ICMP
	450.756	--	PC #1	🟩 ARP
	450.757	PC #1	Switch #1	🟩 ARP
👁	450.758	Switch #1	PC #2	🟩 ARP
	450.759	PC #2	Switch #1	🟩 ARP
	450.760	Switch #1	PC #1	🟩 ARP
	450.760	--	PC #1	🟩 ICMP
	450.761	PC #1	Switch #1	🟩 ICMP
	450.762	Switch #1	PC #2	🟩 ICMP
	450.763	PC #2	Switch #1	🟩 ICMP
	450.764	Switch #1	PC #1	🟩 ICMP

The 3rd ARP message is when the ARP request from PC#1 reaches PC#2, at which point, PC#2 will store PC#1s IP Address and MAC Address in its own ARP Cache.

The 5th ARP message is when the ARP reply fromr PC#2 reaches PC#1. PC#1 will then store the IP Address and MAC Address of PC#2 in its ARP Cache.

4. We are not using Wireshark.
5. It appears that the default value for an unknown MAC Address when initiating an ARP request is FFFF.FFFF.FFFF. It also appears that the MAC Address of each hop in a network is not recorded in the message at all and the MAC Address is only used to identify the EXACT device we are trying to communicate with.

Documentation Task 7.

Record the interesting and useful information from using the *show running-config* command

```
Building configuration
Current Config: 1103 bytes

No service timestamps
Not service password-encryption

Hostname Switch

Interface FastEthernet0/1
        Switchport mode trunk
All other Interfaces (23 more FastEthernet)


Interface Vlan1
        No IP Address
        Shutdown
```

Documentation Task 8.

Check that the entries in the switch's MAC table have the correct MAC addresses for your laptops and the correct port numbers (ie the ones you have plugged the cables into) and record your observations.

Note that the switch's MAC address table doesn't include IP numbers. Why do you think this is?

Yes, the MAC table includes the MAC addresses of the 2 PCs and the ports of the switch that they are mapped to.

The IP addresses are not included as a switch is a Layer 2 device and does not work with IP addresses at all.

Documentation Task 9.

Notice anything interesting in the Wireshark (PT – Simulation) capture on the machine that wasn’t involved in the ping?

How do you think the switch is filling its MAC table?

Based on the Request and Reply ARP messages (We didn’t use wireshark…)