Lab Exercise – ARP

Objective

To see how ARP (Address Resolution Protocol) works. ARP is an essential glue protocol that is used to join Ethernet and IP.

Requirements

Wireshark: This lab uses the Wireshark software tool to capture and examine a packet trace. A packet trace is a record of traffic at a location on the network, as if a snapshot was taken of all the bits that passed across a particular wire. The packet trace records a timestamp for each packet, along with the bits that make up the packet, from the lower-layer headers to the higher-layer contents. Wireshark runs on most operating systems, including Windows, Mac and Linux. It provides a graphical UI that shows the sequence of packets and the meaning of the bits when interpreted as protocol headers and data. It color-codes packets by their type, and has various ways to filter and analyze packets to let you investigate the behavior of network protocols. Wireshark is widely used to troubleshoot networks. You can download it from www.wireshark.org if it is not already installed on your computer.

arp: This lab uses the "`arp`" command-line utility to inspect and clear the cache used by the ARP protocol on your computer. `arp` is installed as part of the operating system on Windows, Linux, and Mac computers, but uses different arguments. It requires administrator privileges to clear the cache.

ifconfig / ipconfig: This lab uses the "`ipconfig`" (Windows) command-line utility to inspect the state of your computer's network interface. `ipconfig` is installed as part of the operating system on Windows computers.

route / netstat: This lab uses the "`route`" or "`netstat`" command-line utility to inspect the routes used by your computer. A key route is the default route (or route to prefix 0.0.0.0) that uses the default gateway to reach remote parts of the Internet. Both "`route`" and "`netstat`" are installed as part of the operating system across Windows and Mac/Linux, but there are many variations on the command-line parameters that must be used.

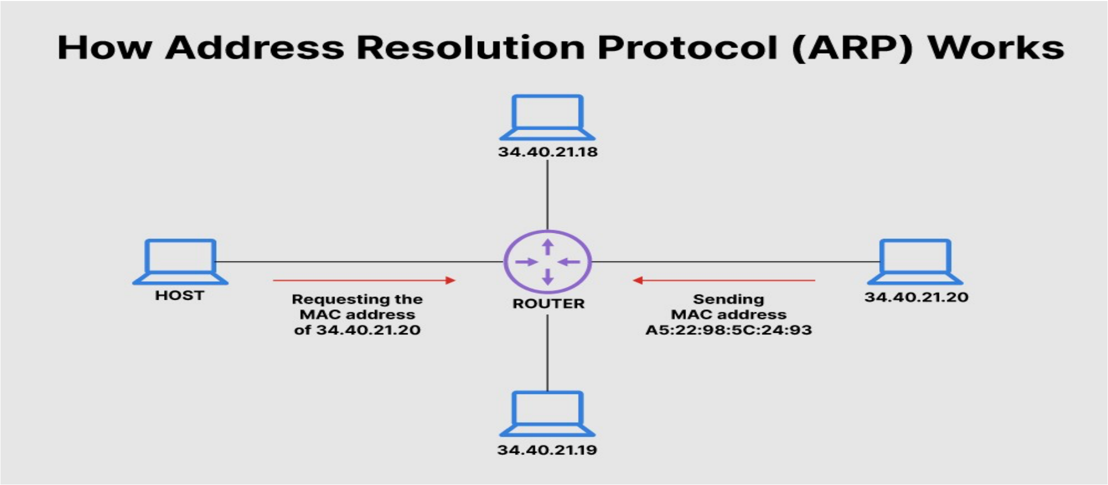
Browser: This lab uses a web browser to find or fetch pages as a workload. Any web browser will do.

Address Resolution Protocol (ARP) Meaning

Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN). This mapping procedure is important because the lengths of the IP and MAC addresses differ, and a translation is needed so that the systems can recognize one another. The most used IP today is IP version 4 (IPv4). An IP address is 32 bits long. However, MAC addresses are 48 bits long. ARP translates the 32-bit address to 48 and vice versa.

There is a networking model known as the Open Systems Interconnection (OSI) model. First developed in the late 1970s, the OSI model uses layers to give IT teams a visualization of what is going on with a particular networking system. This can be helpful in determining which layer affects which application, device, or software installed on the network, and further, which IT or engineering professional is responsible for managing that layer.

The MAC address is also known as the data link layer, which establishes and terminates a connection between two physically connected devices so that data transfer can take place. The IP address is also referred to as the network layer or the layer responsible for forwarding packets of data through different routers. ARP works between these layers.


How Address Resolution Protocol (ARP) Works
34.40.21.18
HOST
Requesting the MAC address of 34.40.21.20
ROUTER
Sending MAC address A5:22:98:5C:24:93
34.40.21.20
34.40.21.19

What Does ARP Do and How Does It Work?

When a new computer joins a local area network (LAN), it will receive a unique IP address to use for identification and communication. Packets of data arrive at a gateway, destined for a particular host machine. The gateway, or the piece of hardware on a network that allows data to flow from one network to another, asks the ARP program to find a MAC address that matches the IP address. The ARP cache keeps a list of each IP address and its matching MAC address. The ARP cache is dynamic, but users on a network can also configure a static ARP table containing IP addresses and MAC addresses.

ARP caches are kept on all operating systems in an IPv4 Ethernet network. Every time a device requests a MAC address to send data to another device connected to the LAN, the device verifies its ARP cache to see if the IP-to-MAC-address connection has already been completed. If it exists, then a new request is unnecessary. However, if the translation has not yet been carried out, then the request for network addresses is sent, and ARP is performed.

An ARP cache size is limited by design, and addresses tend to stay in the cache for only a few minutes. It is purged regularly to free up space. This design is also intended for privacy and security to prevent IP addresses from being stolen or spoofed by cyberattackers. While MAC addresses are fixed, IP addresses are constantly updated. In the purging process, unutilized addresses are deleted; so is any data related to unsuccessful attempts to communicate with computers not connected to the network or that are not even powered on.

What is address resolution protocol's relationship with DHCP and DNS? How do they differ?

ARP is the process of connecting a dynamic IP address to a physical machine's MAC address. As such, it is important to have a look at a few technologies related to IP. As mentioned previously, IP addresses, by design, are changed constantly for the simple reason that doing so gives users security and privacy. However changes on IP addresses should not be completely random. There should be rules that allocate an IP address from a defined range of numbers available in a specific network. This helps prevent issues, such as two computers receiving the same IP address. The rules are known as DHCP or Dynamic Host Configuration Protocol.

IP addresses as identities for computers are important because they are needed to perform an internet search. When users search for a domain name or Uniform Resource Locator (URL), they use an alphabetical name. Computers, on the other hand, use the numerical IP address to associate the domain name with a server. To connect the two, a Domain Name System (DNS) server is used to translate an IP address from a confusing string of numbers into a more readable, easily understandable domain name, and vice versa.

What is ARP in Networking Useful For?

ARP is necessary because the software address (IP address) of the host or computer connected to the network needs to be translated to a hardware address (MAC address). Without ARP, a host would not be able to figure out the hardware address of another host. The LAN keeps a table or directory that maps IP addresses to MAC addresses of the different devices, including both endpoints and routers on that network.

This table or directory is not maintained by users or even by IT administrators. Instead, the ARP protocol creates entries on the fly. If a user's device does not know the hardware address of the destination host, the device will send a message to every host on the network asking for this address. When the proper destination host learns of the request, it will reply back with its hardware address, which will then be stored in the ARP directory or table. If ARP is not supported, manual entries can be made to this directory.

ARP Spoofing/ARP Poisoning Attack

ARP spoofing is also known as ARP poison routing or ARP cache poisoning. This is a type of malicious attack in which a cybercriminal sends fake ARP messages to a target LAN with the intention of linking their MAC address with the IP address of a legitimate device or server within the network. The link allows for data from the victim's computer to be sent to the attacker's computer instead of the original destination. ARP spoofing attacks can prove dangerous, as sensitive information can be passed between computers without the victims' knowledge. ARP spoofing also enables other forms of cyberattacks, including the following:

Man-in-the-Middle (MTM) Attacks

A man-in-the-middle (MITM) attack is a type of eavesdropping in which the cyberattacker intercepts, relays, and alters messages between two parties—who have no idea that a third party is involved—to steal information. The attacker may try to control and manipulate the messages of one of the parties, or of both, to obtain sensitive information. Because these types of attacks use sophisticated software to mimic the style and tone of conversations—including those that are text- and voice-based—a MITM attack is difficult to intercept and thwart. A MITM attack occurs when malware is distributed and takes control of a victim's web browser. The browser itself is not important to the attacker, but the data that the victim shares very much is because it can include usernames, passwords, account numbers, and other sensitive information shared in chats and online discussions. Once they have control, the attacker creates a proxy between the victim and a legitimate site, usually with a fake lookalike site, to intercept any data between the victim and the legitimate site. Attackers do this with online banking and e-commerce sites to capture personal information and financial data.

Denial-of-Service Attacks

A denial-of-service (DoS) attack is one in which a cyberattacker attempts to overwhelm systems, servers, and networks with traffic to prevent users from accessing them. A larger-scale DoS attack is known as a distributed denial-of-service (DDoS) attack, where a much larger number of sources are used to flood a system with traffic. These types of attacks exploit known vulnerabilities in network protocols. When a large number of packets are transmitted to a vulnerable network, the service can easily become overwhelmed and then unavailable.

Session Hijacking

Session hijacking occurs when a cyberattacker steals a user's session ID, takes over that user's web session, and masquerades as that user. With the session ID in their possession, the attacker can perform any task or activity that user is authorized to do on that network. Authentication occurs when a user tries to gain access to a system or sign in to a restricted website or web service. The session ID is stored in a cookie in the browser, and an attacker engaged in session hijacking will intercept the authentication process and intrude in real time.

Lab - Network Setup

We want to observe the ARP protocol in action. ARP is used to find the Ethernet address that corresponds to a local IP address to which your computer wants to send a packet. A typical example of a local IP address is that of the local router or default gateway that connects your computer to the rest of the Internet. Your computer caches these translations in an ARP cache so that the ARP protocol need only be used occasionally to do the translation. The setup from the viewpoint of your computer is as shown in the example below.

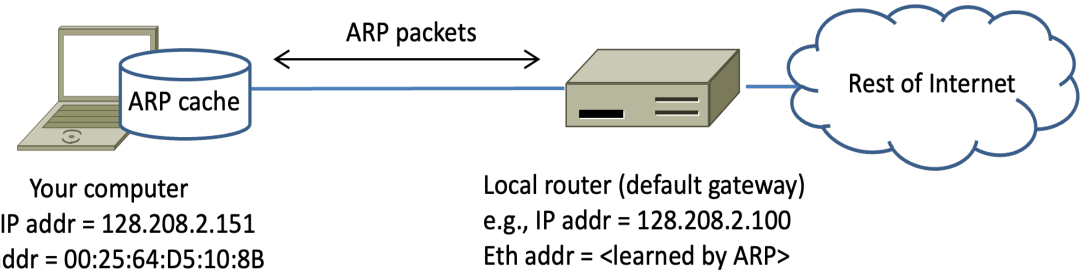

ARP packets
ARP cache
Rest of Internet
Your computer
e.g., IP addr = 128.208.2.151
Eth addr = 00:25:64:D5:10:8B
Local router (default gateway)
e.g., IP addr = 128.208.2.100
Eth addr = <learned by ARP>

Figure 1: Network setup under which we will study ARP in second part

How ARP Works

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it.

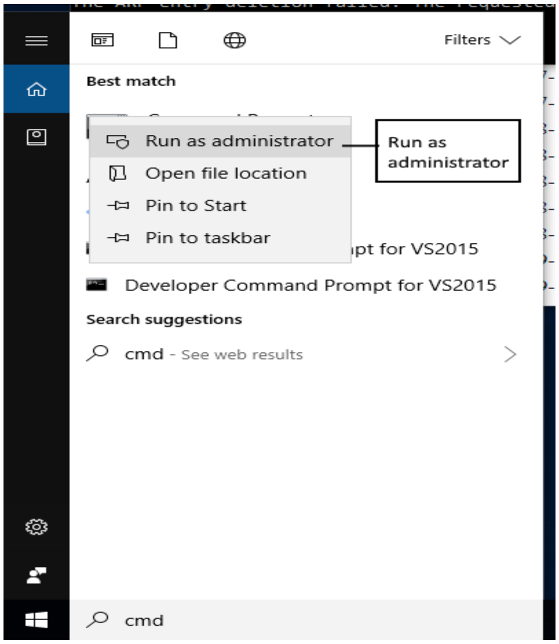
A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

There is a Reverse ARP (RARP) for host machines that don't know their IP address. RARP enables them to request their IP address from the gateway's ARP cache.

Step 1: Finding your IP address and Gateway address

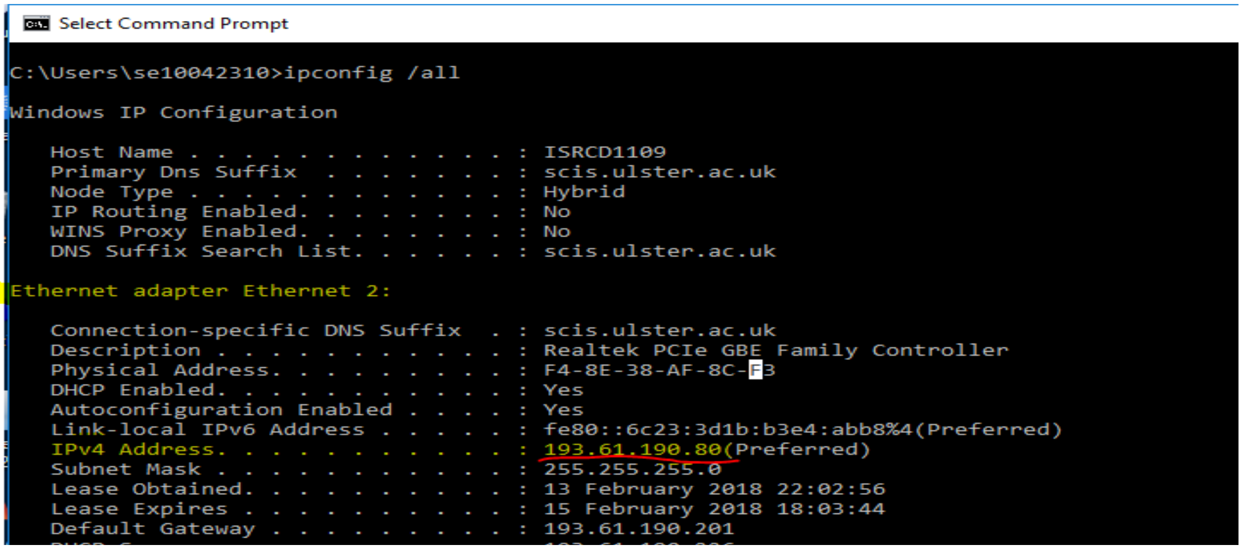
1. Open a command prompt. Please note that you cannot run as an administrator in the lab.

   Simply type *cmd*:



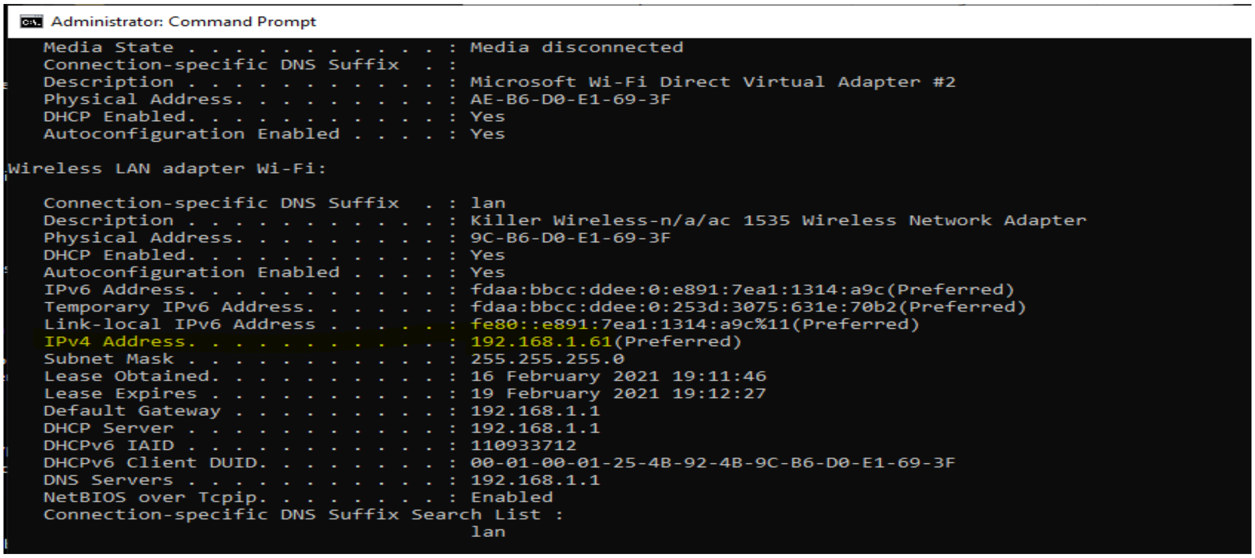
Run as administrator

2. *Find the **Ethernet** address of the main network interface OR the **wireless** address (see figure 3) of your computer with the* `ipconfig` *command*. You will want to know this address for later analysis. On Windows, bring up a command-line shell and type "`ipconfig /all`". Among the output will be a section for the main interface of the computer (likely an Ethernet interface) and its Ethernet address. Common names for the interface are "eth0" or "Ethernet adapter". An example is shown in figure 2, with added highlighting.



```
C:\Users\se10042310>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : ISRCD1109
   Primary Dns Suffix  . . . . . . . : scis.ulster.ac.uk
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : scis.ulster.ac.uk

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : scis.ulster.ac.uk
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : F4-8E-38-AF-8C-F3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6c23:3d1b:b3e4:abb8%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 193.61.190.80(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 13 February 2018 22:02:56
   Lease Expires . . . . . . . . . . : 15 February 2018 18:03:44
   Default Gateway . . . . . . . . . : 193.61.190.201
```

Figure 2: Finding the computer's Ethernet address with `ipconfig` (Windows)

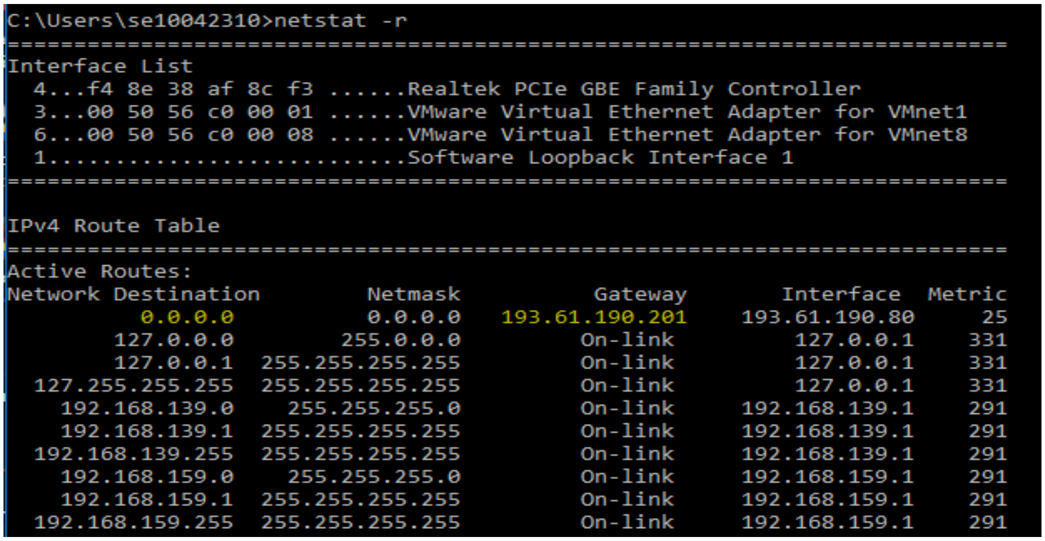


```
Administrator: Command Prompt
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : AE-B6-D0-E1-69-3F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Description . . . . . . . . . . . : Killer Wireless-n/a/ac 1535 Wireless Network Adapter
   Physical Address. . . . . . . . . : 9C-B6-D0-E1-69-3F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fdaa:bbcc:ddee:0:e891:7ea1:1314:a9c(Preferred)
   Temporary IPv6 Address. . . . . . : fdaa:bbcc:ddee:0:253d:3075:631e:70b2(Preferred)
   Link-local IPv6 Address . . . . . : fe80::e891:7ea1:1314:a9c%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.61(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 16 February 2021 19:11:46
   Lease Expires . . . . . . . . . . : 19 February 2021 19:12:27
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 110933712
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-4B-92-4B-9C-B6-D0-E1-69-3F
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       lan
```

Figure 3: Finding the computer's WiFi IP address with ipconfig (Windows)

3. *Find the IP address of the local router or default gateway that your computer uses to reach the rest of the Internet using the* `netstat` / `route` *command.* You should be able to use the `netstat` -r command on Windows.

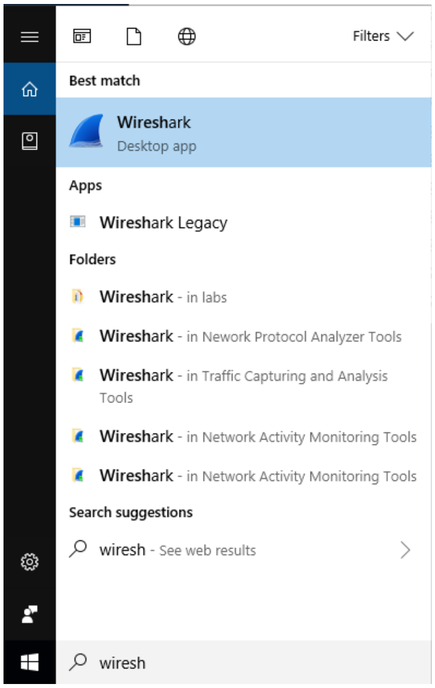
   Alternatively, you can use the route command ("`route print`" on Windows). In either case you are looking for the gateway IP address that corresponds to the destination of default or 0.0.0.0. An example is shown in figure 3 for `netstat`, with added highlighting.



```
C:\Users\se10042310>netstat -r
===========================================================================
Interface List
  4...f4 8e 38 af 8c f3 ......Realtek PCIe GBE Family Controller
  3...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  6...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    193.61.190.201    193.61.190.80     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.139.0    255.255.255.0         On-link     192.168.139.1    291
    192.168.139.1  255.255.255.255         On-link     192.168.139.1    291
  192.168.139.255  255.255.255.255         On-link     192.168.139.1    291
    192.168.159.0    255.255.255.0         On-link     192.168.159.1    291
    192.168.159.1  255.255.255.255         On-link     192.168.159.1    291
  192.168.159.255  255.255.255.255         On-link     192.168.159.1    291
```

Figure 4: Finding the default gateway IP address with `netstat` (Windows)

4. Now **run Wireshark** by typing "*wireshark*" in the bottom left search box in Windows



Filters

Best match

Wireshark
Desktop app

Apps

Wireshark Legacy

Folders

Wireshark - in labs

Wireshark - in Nework Protocol Analyzer Tools

Wireshark - in Traffic Capturing and Analysis Tools

Wireshark - in Network Activity Monitoring Tools

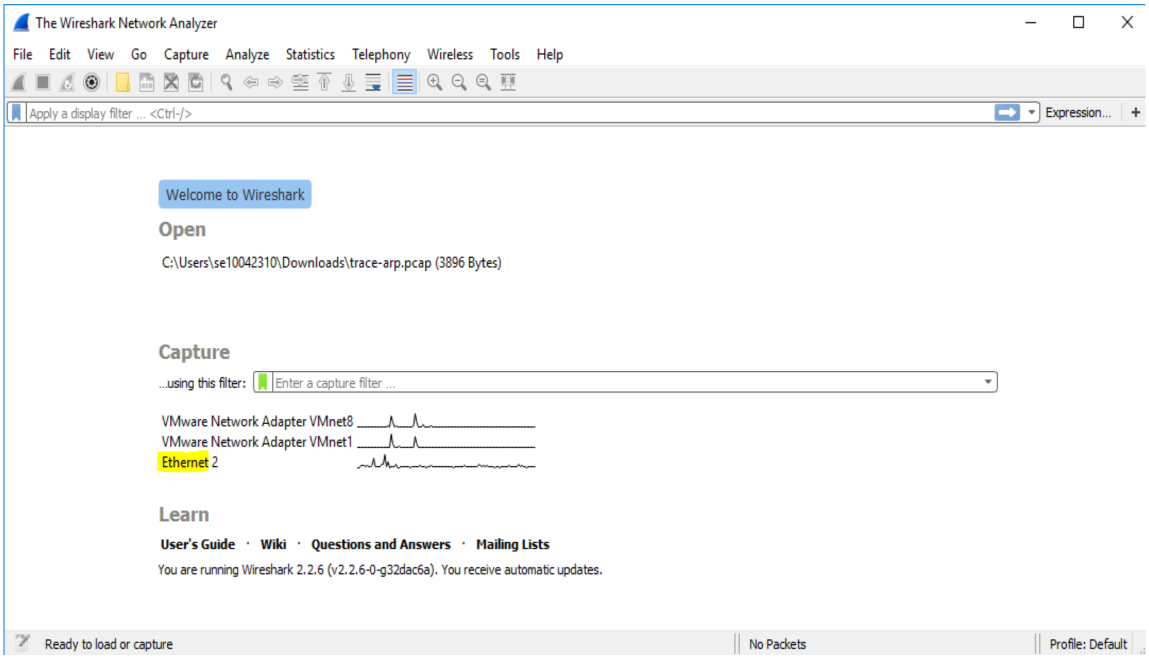
Wireshark - in Network Activity Monitoring Tools

Search suggestions

wiresh - See web results

wiresh

5. You should see the main Wireshark interface. **Click on the Ethernet interface** to start traffic analysis on that interface.



The Wireshark Network Analyzer

Welcome to Wireshark

Open

C:\Users\se10042310\Downloads\trace-arp.pcap (3896 Bytes)

Capture

...using this filter: Enter a capture filter ...

VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Ethernet 2

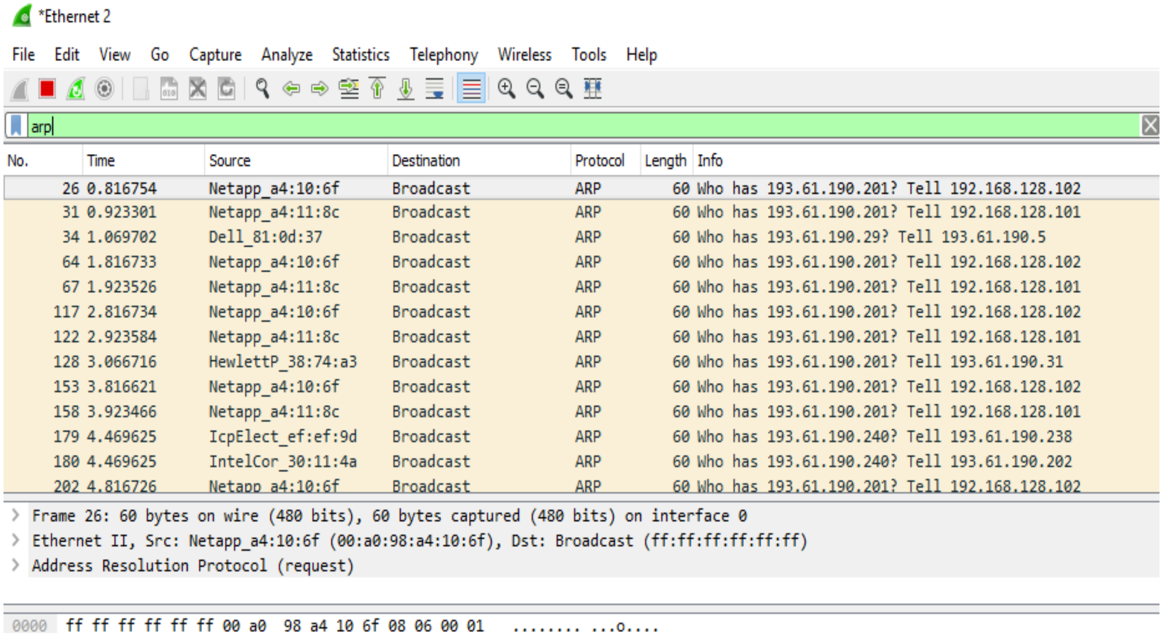
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.2.6 (v2.2.6-0-g32dac6a). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

6. *Add a filter of* "`arp`". Your capture window should be like the one pictured below.



No.	Time	Source	Destination	Protocol	Length	Info
26	0.816754	Netapp_a4:10:6f	Broadcast	ARP	60	Who has 193.61.190.201? Tell 192.168.128.102
31	0.923301	Netapp_a4:11:8c	Broadcast	ARP	60	Who has 193.61.190.201? Tell 192.168.128.101
34	1.069702	Dell_81:0d:37	Broadcast	ARP	60	Who has 193.61.190.29? Tell 193.61.190.5
64	1.816733	Netapp_a4:10:6f	Broadcast	ARP	60	Who has 193.61.190.201? Tell 192.168.128.102
67	1.923526	Netapp_a4:11:8c	Broadcast	ARP	60	Who has 193.61.190.201? Tell 192.168.128.101
117	2.816734	Netapp_a4:10:6f	Broadcast	ARP	60	Who has 193.61.190.201? Tell 192.168.128.102
122	2.923584	Netapp_a4:11:8c	Broadcast	ARP	60	Who has 193.61.190.201? Tell 192.168.128.101
128	3.066716	HewlettP_38:74:a3	Broadcast	ARP	60	Who has 193.61.190.201? Tell 193.61.190.31
153	3.816621	Netapp_a4:10:6f	Broadcast	ARP	60	Who has 193.61.190.201? Tell 192.168.128.102
158	3.923466	Netapp_a4:11:8c	Broadcast	ARP	60	Who has 193.61.190.201? Tell 192.168.128.101
179	4.469625	IcpElect_ef:ef:9d	Broadcast	ARP	60	Who has 193.61.190.240? Tell 193.61.190.238
180	4.469625	IntelCor_30:11:4a	Broadcast	ARP	60	Who has 193.61.190.240? Tell 193.61.190.202
202	4.816726	Netapp_a4:10:6f	Broadcast	ARP	60	Who has 193.61.190.201? Tell 192.168.128.102

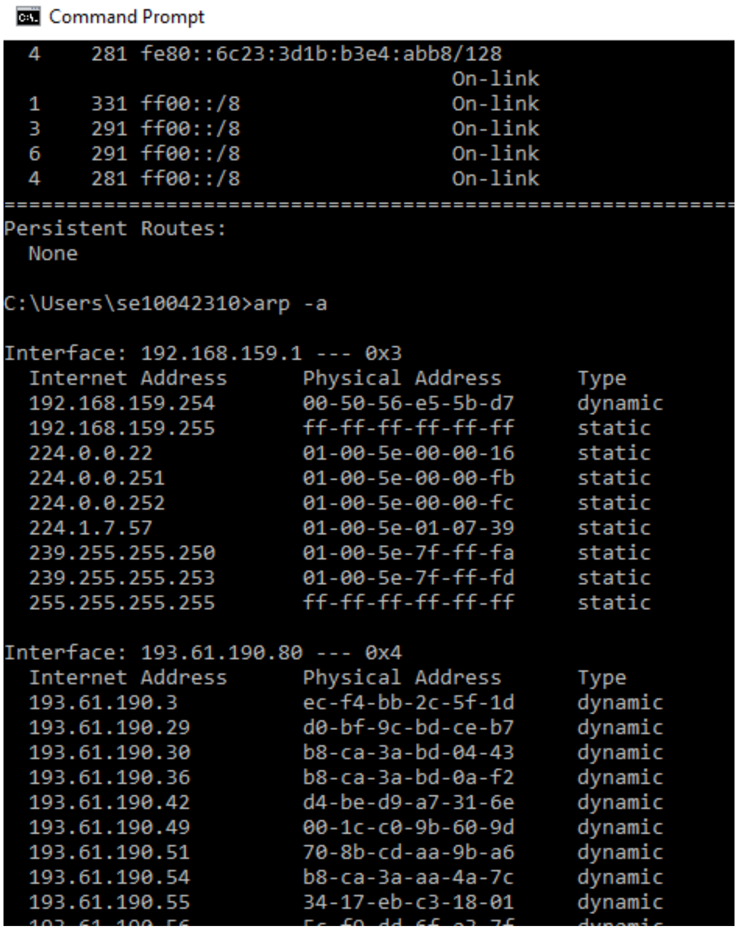
```
> Frame 26: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Netapp_a4:10:6f (00:a0:98:a4:10:6f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 a0  98 a4 10 6f 08 06 00 01   ........ ...o....
```

Figure 6: Setting up the capture options

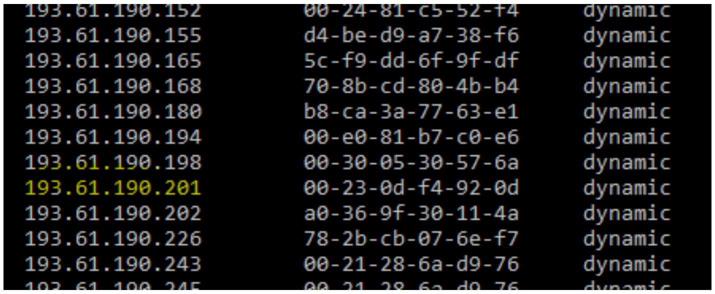
7. *When the capture is started, use the* "`arp`" *command to clear the default gateway from the ARP cache.* Using the command "`arp -a`" will show you the contents of the ARP cache as a check that you can run "`arp`".

   Go to command prompt and type **arp -a** as shown below.



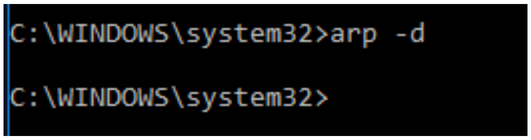
```
Command Prompt
  4    281 fe80::6c23:3d1b:b3e4:abb8/128
                                On-link
  1    331 ff00::/8             On-link
  3    291 ff00::/8             On-link
  6    291 ff00::/8             On-link
  4    281 ff00::/8             On-link
===========================================================
Persistent Routes:
  None

C:\Users\se10042310>arp -a

Interface: 192.168.159.1 --- 0x3
  Internet Address      Physical Address      Type
  192.168.159.254       00-50-56-e5-5b-d7     dynamic
  192.168.159.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.1.7.57            01-00-5e-01-07-39     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.253       01-00-5e-7f-ff-fd     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 193.61.190.80 --- 0x4
  Internet Address      Physical Address      Type
  193.61.190.3          ec-f4-bb-2c-5f-1d     dynamic
  193.61.190.29         d0-bf-9c-bd-ce-b7     dynamic
  193.61.190.30         b8-ca-3a-bd-04-43     dynamic
  193.61.190.36         b8-ca-3a-bd-0a-f2     dynamic
  193.61.190.42         d4-be-d9-a7-31-6e     dynamic
  193.61.190.49         00-1c-c0-9b-60-9d     dynamic
  193.61.190.51         70-8b-cd-aa-9b-a6     dynamic
  193.61.190.54         b8-ca-3a-aa-4a-7c     dynamic
  193.61.190.55         34-17-eb-c3-18-01     dynamic
```

You should see an entry for the IP address of the default gateway as shown in image below. In this case it is 193.61.190.201 which is the default gateway on my office PC.



```
  193.61.190.152        00-24-81-c5-52-f4     dynamic
  193.61.190.155        d4-be-d9-a7-38-f6     dynamic
  193.61.190.165        5c-f9-dd-6f-9f-df     dynamic
  193.61.190.168        70-8b-cd-80-4b-b4     dynamic
  193.61.190.180        b8-ca-3a-77-63-e1     dynamic
  193.61.190.194        00-e0-81-b7-c0-e6     dynamic
  193.61.190.198        00-30-05-30-57-6a     dynamic
  193.61.190.201        00-23-0d-f4-92-0d     dynamic
  193.61.190.202        a0-36-9f-30-11-4a     dynamic
  193.61.190.226        78-2b-cb-07-6e-f7     dynamic
  193.61.190.243        00-21-28-6a-d9-76     dynamic
```

8. To clear this entry, use the arp command with different arguments (“`arp -d`” on Windows) as follows. Type **arp -d** in the command prompt.

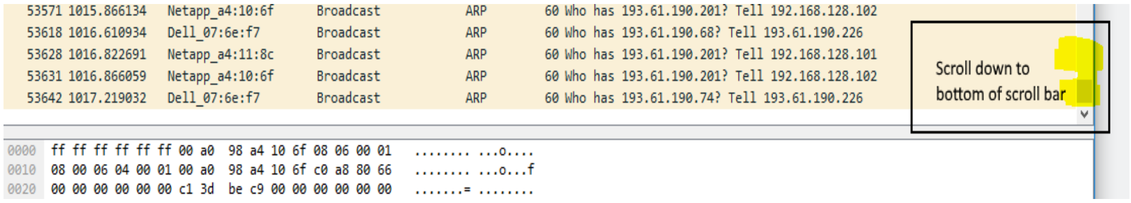


```
C:\WINDOWS\system32>arp -d

C:\WINDOWS\system32>
```

Note: This usage of `arp` *will need administrator privileges to run, so you have to run as a privileged user on Windows which is what you should have done in step 1. The command should run without error, but the ARP entry may not appear to be cleared if you check with "*`arp -a`*". This is because your computer will send ARP packets to repopulate this entry as soon as you need to send a packet to a remote IP address, and that can happen very quickly due to background activity on the computer.*

9. *Now that you have cleared your ARP cache,* ***fetch a remote page with your Web browser***. This will cause ARP to find the Ethernet address of the default gateway so that the packets can be sent.

10. You will see these packets flowing through your computer by scrolling down in the Wireshark window to the bottom as shown below.



```
53571 1015.866134   Netapp_a4:10:6f    Broadcast    ARP     60 Who has 193.61.190.201? Tell 192.168.128.102
53618 1016.610934   Dell_07:6e:f7      Broadcast    ARP     60 Who has 193.61.190.68? Tell 193.61.190.226
53628 1016.822691   Netapp_a4:11:8c    Broadcast    ARP     60 Who has 193.61.190.201? Tell 192.168.128.101
53631 1016.866059   Netapp_a4:10:6f    Broadcast    ARP     60 Who has 193.61.190.201? Tell 192.168.128.102
53642 1017.219032   Dell_07:6e:f7      Broadcast    ARP     60 Who has 193.61.190.74? Tell 193.61.190.226

0000  ff ff ff ff ff ff 00 a0  98 a4 10 6f 08 06 00 01   ........ ...o....
0010  08 00 06 04 00 01 00 a0  98 a4 10 6f c0 a8 80 66   ........ ...o...f
0020  00 00 00 00 00 00 c1 3d  be c9 00 00 00 00 00 00   .......= ........
```

Scroll down to bottom of scroll bar

11. These ARP packets will be captured by Wireshark. You might clear the ARP cache and fetch a document a couple of times. Hopefully there will also be other ARP packets sent by other computers on the local network that will be captured. These packets are likely to be present if there are other computers on your local network. In fact, if you have a busy computer and extensive local network then you may capture many ARP packets. The ARP traffic of other computers will be captured when the ARP packets are sent to the broadcast address, since in this case they are destined for all computers including the one on which you are running Wireshark. Because ARP activity happens slowly, you may need to wait up to 30 seconds to observe some of this background ARP traffic.

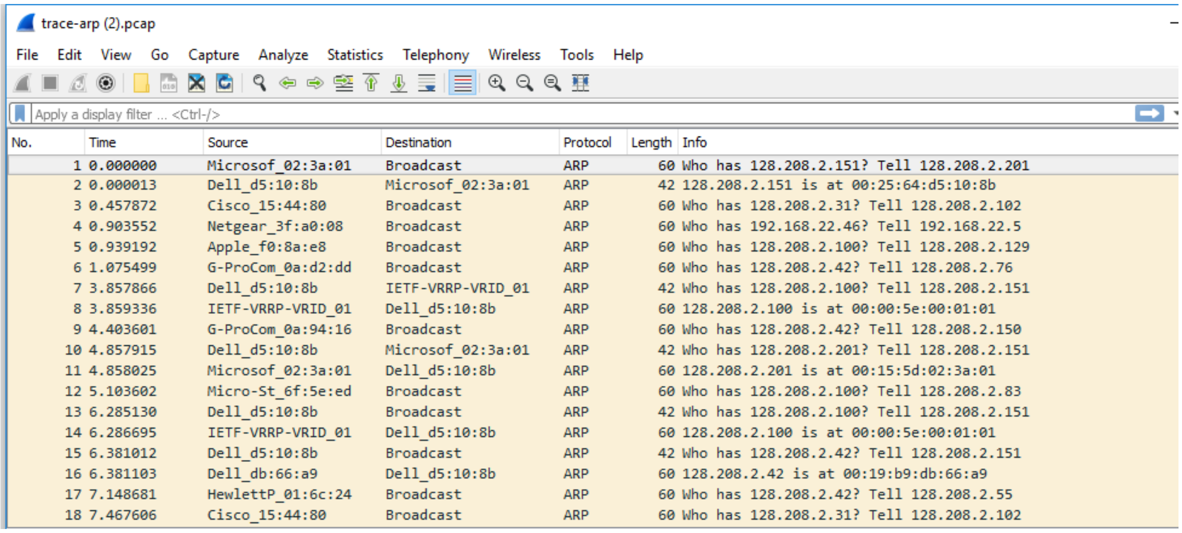
12. *Once you have captured some ARP traffic, stop the capture.* You will need the trace, plus the Ethernet address of your computer and the IP address of the default gateway for the next steps.

Step 2: Inspect the supplied ARP Trace

1. **Close** Wireshark.

2. Once Wireshark is closed, **open** the ARP trace here:
   https://kevincurran.org/com320/labs/wireshark/trace-arp.pcap

   You should see a screen as shown below.


trace-arp (2).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Microsof_02:3a:01	Broadcast	ARP	60	Who has 128.208.2.151? Tell 128.208.2.201
2	0.000013	Dell_d5:10:8b	Microsof_02:3a:01	ARP	42	128.208.2.151 is at 00:25:64:d5:10:8b
3	0.457872	Cisco_15:44:80	Broadcast	ARP	60	Who has 128.208.2.31? Tell 128.208.2.102
4	0.903552	Netgear_3f:a0:08	Broadcast	ARP	60	Who has 192.168.22.46? Tell 192.168.22.5
5	0.939192	Apple_f0:8a:e8	Broadcast	ARP	60	Who has 128.208.2.100? Tell 128.208.2.129
6	1.075499	G-ProCom_0a:d2:dd	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.76
7	3.857866	Dell_d5:10:8b	IETF-VRRP-VRID_01	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
8	3.859336	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
9	4.403601	G-ProCom_0a:94:16	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.150
10	4.857915	Dell_d5:10:8b	Microsof_02:3a:01	ARP	42	Who has 128.208.2.201? Tell 128.208.2.151
11	4.858025	Microsof_02:3a:01	Dell_d5:10:8b	ARP	60	128.208.2.201 is at 00:15:5d:02:3a:01
12	5.103602	Micro-St_6f:5e:ed	Broadcast	ARP	60	Who has 128.208.2.100? Tell 128.208.2.83
13	6.285130	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
14	6.286695	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
15	6.381012	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.42? Tell 128.208.2.151
16	6.381103	Dell_db:66:a9	Dell_d5:10:8b	ARP	60	128.208.2.42 is at 00:19:b9:db:66:a9
17	7.148681	HewlettP_01:6c:24	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.55
18	7.467606	Cisco_15:44:80	Broadcast	ARP	60	Who has 128.208.2.31? Tell 128.208.2.102

The setup from the viewpoint of your computer from this trace is shown in the example below.

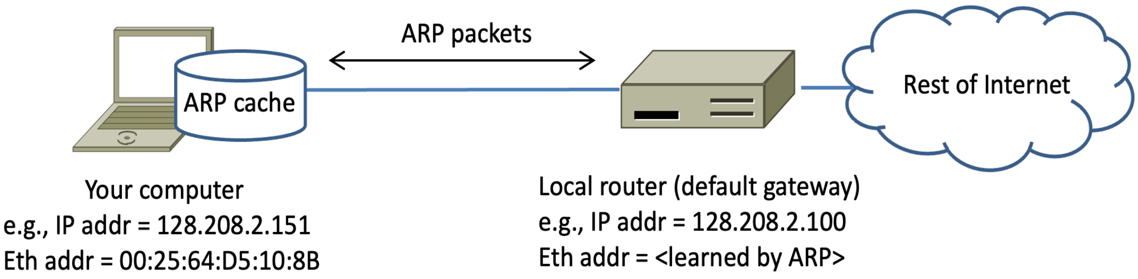

ARP packets
ARP cache
Rest of Internet
Your computer
e.g., IP addr = 128.208.2.151
Eth addr = 00:25:64:D5:10:8B
Local router (default gateway)
e.g., IP addr = 128.208.2.100
Eth addr = <learned by ARP>

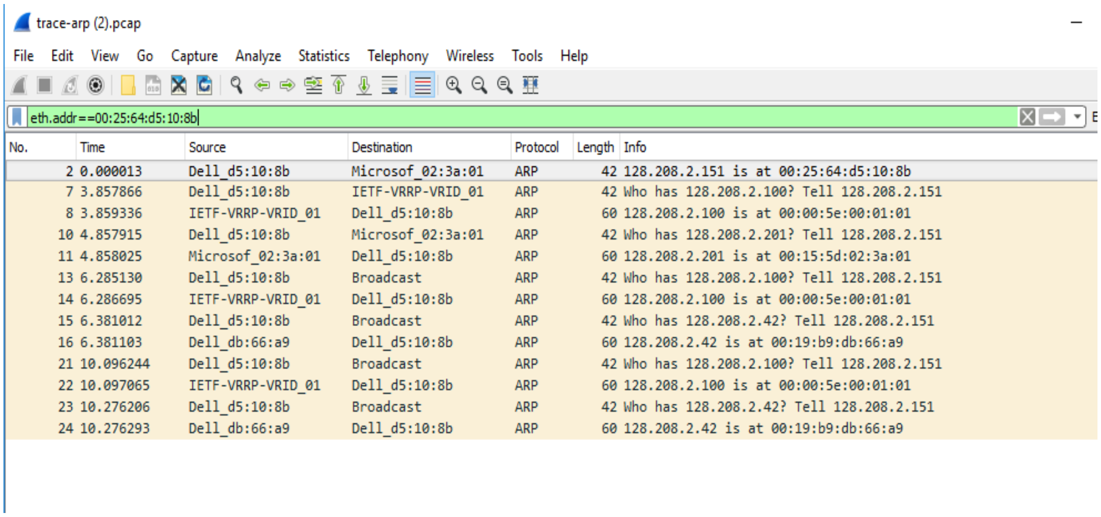
Figure 7: Network setup under which we will study ARP in this part

Note: **Ethernet address** of computer: 00:25:64:d5:10:8b and IP address of **gateway**: 128.208.2.100

3. Now we can look at an ARP exchange. Since there may be many ARP packets in your trace, we'll first narrow our view to only the ARP packets that are sent directly from or to your computer.

   Set a display filter for packets with the Ethernet address of your computer which is this case is ***00:25:64:d5:10:8b.***

   You can do this by entering an expression in the blank "Filter:" box near the top of the Wireshark window and clicking "Apply" or Enter. After applying this filter your capture should look something like the figure below, in which we have expanded the ARP protocol details.


trace-arp (2).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
eth.addr==00:25:64:d5:10:8b
```

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000013	Dell_d5:10:8b	Microsof_02:3a:01	ARP	42	128.208.2.151 is at 00:25:64:d5:10:8b
7	3.857866	Dell_d5:10:8b	IETF-VRRP-VRID_01	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
8	3.859336	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
10	4.857915	Dell_d5:10:8b	Microsof_02:3a:01	ARP	42	Who has 128.208.2.201? Tell 128.208.2.151
11	4.858025	Microsof_02:3a:01	Dell_d5:10:8b	ARP	60	128.208.2.201 is at 00:15:5d:02:3a:01
13	6.285130	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
14	6.286695	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
15	6.381012	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.42? Tell 128.208.2.151
16	6.381103	Dell_db:66:a9	Dell_d5:10:8b	ARP	60	128.208.2.42 is at 00:19:b9:db:66:a9
21	10.096244	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
22	10.097065	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
23	10.276206	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.42? Tell 128.208.2.151
24	10.276293	Dell_db:66:a9	Dell_d5:10:8b	ARP	60	128.208.2.42 is at 00:19:b9:db:66:a9

Figure 8: Capture of ARP packets, showing details of a request

Find and select an ARP request for the default gateway and examine its fields. There are two kinds of ARP packets, a request and a reply, and we will look at each one in turn. The Info line for the request will start with "Who has …". You want to look for one of these packets that asks for the MAC address of the default gateway, e.g., "Who has xx.xx.xx.xx …" where xx.xx.xx.xx is your default gateway. You can click on the + expander or icon for the Address Resolution Protocol block to view the fields:

- Hardware and Protocol type are set to constants that tell us the hardware is Ethernet and the protocol is IP. This matches the ARP translation from IP to Ethernet address.

- Hardware and Protocol size are set to 6 and 4, respectively. These are the sizes of Ethernet and IP addresses in bytes.

- The opcode field tells us that this is a request.

- Next come the four key fields, the sender MAC (Ethernet) and IP and the target MAC (Ethernet) and IP. These fields are filled in as much as possible. For a request, the sender knows their MAC and IP address and fills them in. The sender also knows the target IP address – it is the IP address for which an Ethernet address is wanted. But the sender does not know the target MAC address, so it does not fill it in.

Next, select an ARP reply and examine its fields. The reply will answer a request and have an Info line of the form “xx.xx.xx.xx is at yy:yy:yy:yy:yy:yy”:

- The Hardware and Protocol type and sizes are as set as before.
- The opcode field has a different value that tells us that this is a reply.
- Next come the four key fields, the sender MAC (Ethernet) and IP and the target MAC (Ethernet) and IP just as before. These fields are reversed from the corresponding request, since the old target is the new sender (and vice versa). The fields should now be all filled in since both computers have supplied their addresses.

Step 3: Details of ARP over Ethernet

ARP packets are carried in Ethernet frames, and the values of the Ethernet header fields are chosen to support ARP. For instance, you may wonder how an ARP request packet is delivered to the target computer so that it can reply and tell the requestor its MAC address. The answer is that the ARP request is (normally) broadcast at the Ethernet layer so that it is received by all computers on the local network including the target. Look specifically at the destination Ethernet address of a request: it is set to ff:ff:ff:ff:ff:ff, the broadcast address. So, the target receives the request and recognizes that it is the intended recipient of the message; other computers that receive the request know that it is not meant for them. Only the target responds with a reply. However, anyone who receives an ARP packet can learn a mapping from it: the sender MAC and sender IP pair. The ARP header for a request and a reply is 28 bytes for both the request and reply for IPv4.

(Please note that answers on next page to following 5 questions)

To look at further details of ARP, examine an ARP request and ARP reply to answer these questions:

1. *What opcode is used to indicate a request? What about a reply?*
2. *What value is carried on a request for the unknown target MAC address?*
3. *What Ethernet Type value which indicates that ARP is the higher layer protocol?*
4. *Is the ARP reply broadcast (like the ARP request) or not?*

Answers to Step 3: ARP request and reply

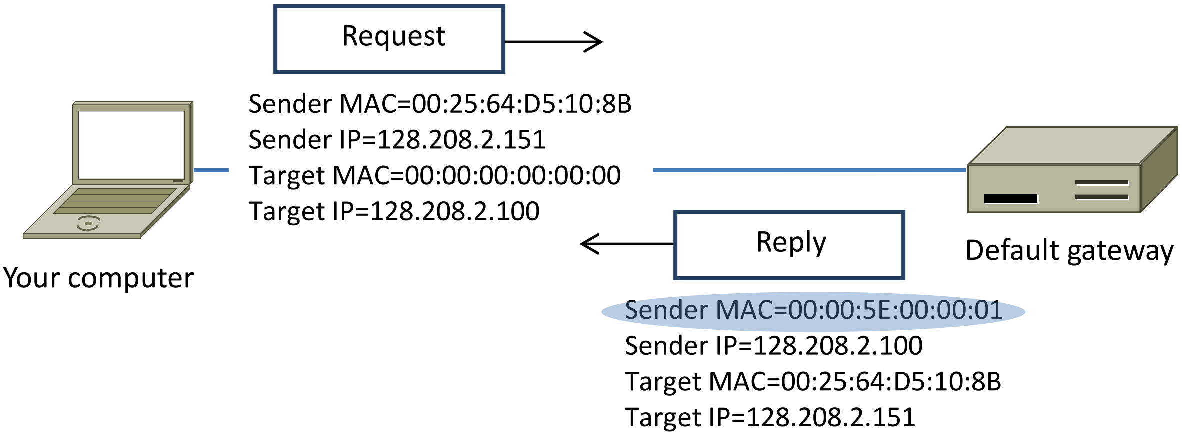


Figure 9: Details of the ARP request and reply to resolve the default gateway

There are several features to note:

- On the request, the target MAC is not known so it is usually filled in as 00:00:00:00:00:00.
- On the reply, the request target becomes the reply sender and vice versa.
- On the reply, the sender MAC returns the answer that is sought; it is highlighted.
- All of the fields that are shown are ARP header fields

Answers to the questions:

1. The request opcode is 1 and the reply opcode is 2.
2. The target MAC address of the request is normally all zeros, or 00:00:00:00:00:00.
3. The Ethernet Type value for ARP is 0x806.
4. The ARP reply is normally not broadcast. It is sent directly to the target using its Ethernet address.