

A decorative graphic on the left side of the slide. It consists of a blue parallelogram and a light green parallelogram, both tilted at an angle. The blue shape is in the foreground, and the green shape is partially behind it. They are set against a dark blue background with faint, lighter blue diagonal stripes.

Introduction to Networks



Join the GUTS Discord
discord.gg/FfrfkFv

In the **#cdx2020-workshops** channel!

What is a network?

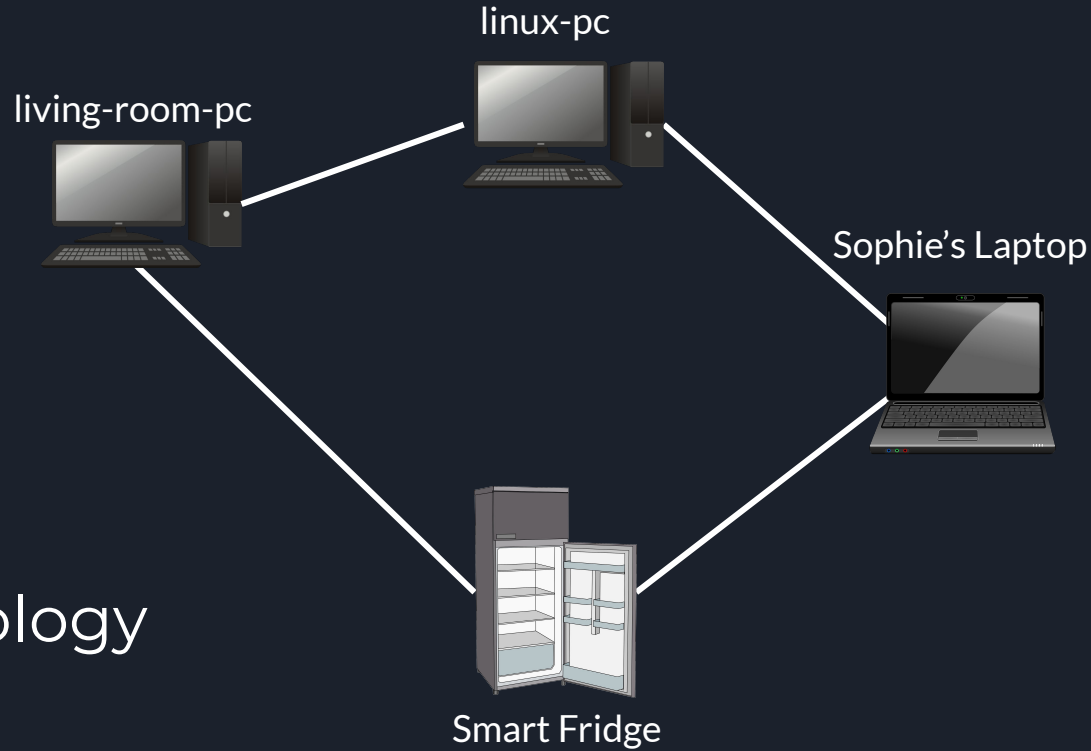
A network consists of two or more devices connected in a way that allows them to communicate

This can be done through:

- Ethernet cable
- Bluetooth
- WiFi
- etc...

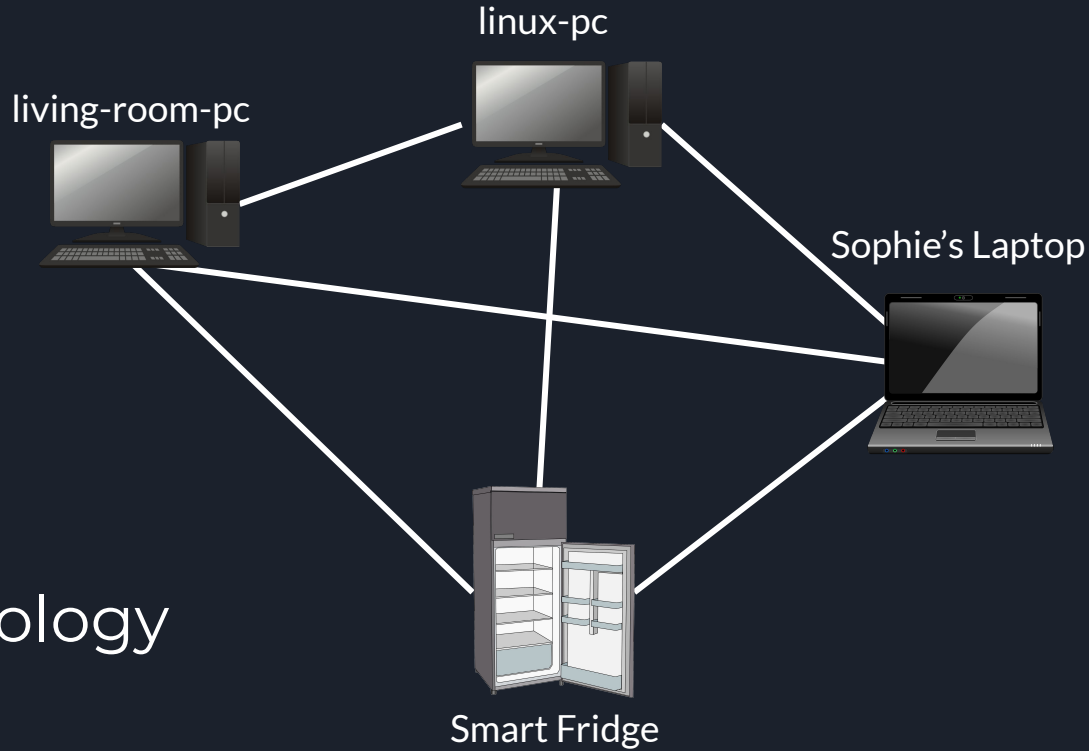


What is a network?



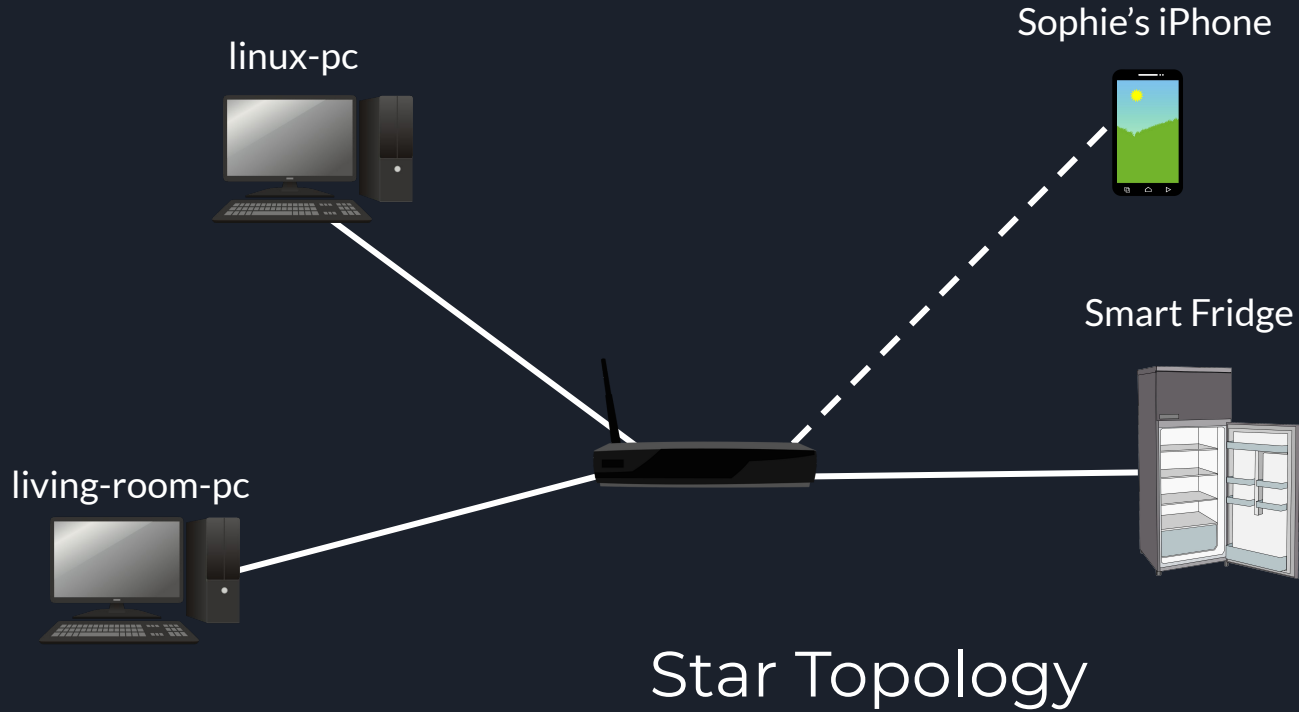
Ring Topology

What is a network?



Mesh Topology

What is a network?





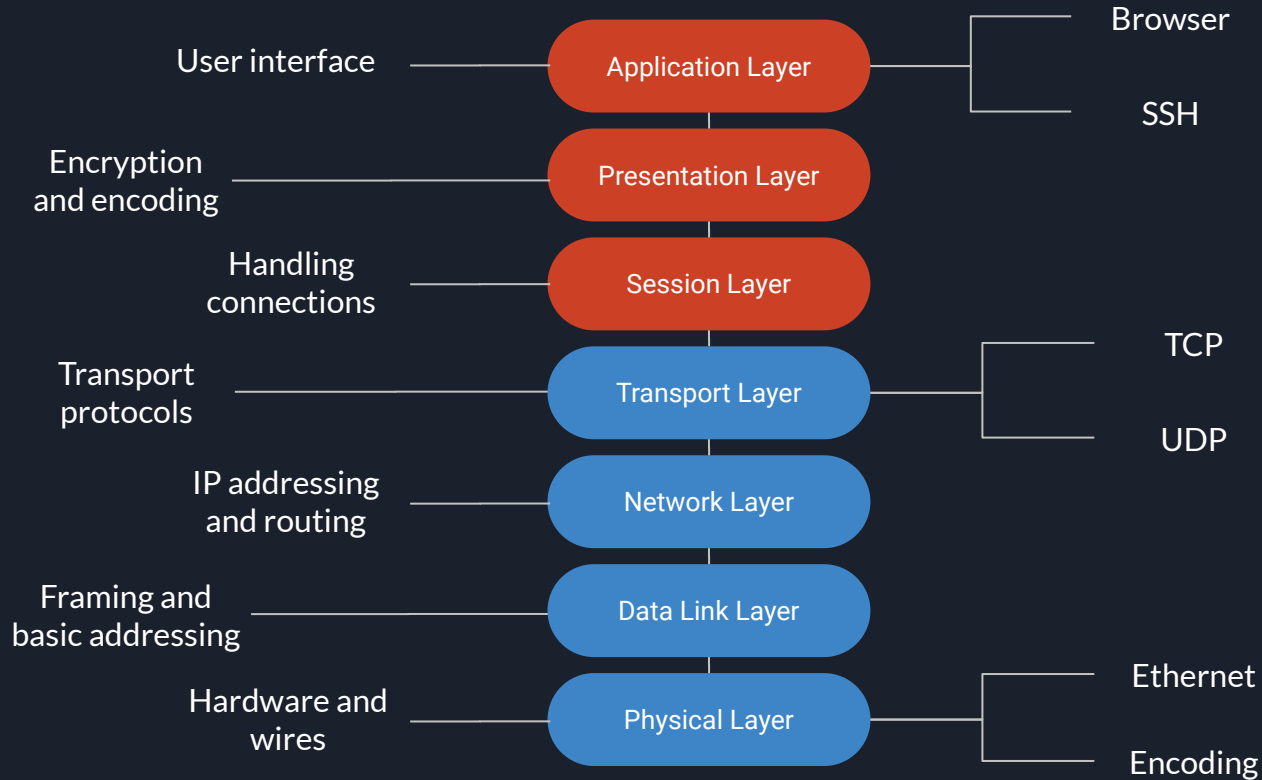
Describing a Network

How can we describe the different stages of a network?

The OSI (Open System Interconnections) model:

- Splits up the different stages of a network into 7 layers
- Each layer handles the data from the layer above and below
- Each layer has a specific function

The OSI Model





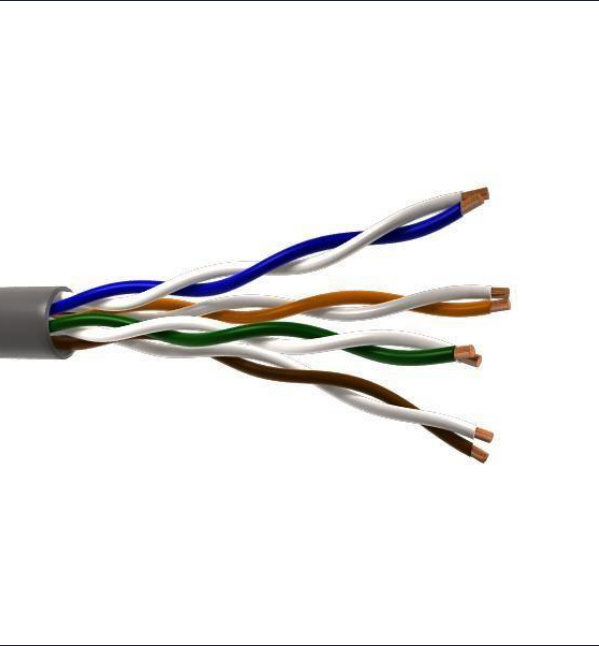
Layer 1 - Physical Layer

The Physical Layer is responsible for taking the raw electrical signals and converting them into bits so that the devices can read the data. The data is then sent onto the data link layer.

We'll be looking at two types of cables:

- Copper
- Fibre optic

Unshielded Twisted Pair (UTP)



- UTP consists of 4 sets of 2 cables twisted around each other
- Most commonly used in ethernet cables and phone lines
- Cables are twisted to reduce interference and noise

Advantages:

- Cheap and easy to make
- Cables are thin

Disadvantages:

- More interference over larger distances
- Slower speeds over larger distances

Fibre Optic Cable

- Fibre optic cables are made from thin glass tubes
- Light is sent along the glass tube using total internal reflection

Advantages:

- Very little noise
- High speeds over long distances
- Cheap to manufacture cables

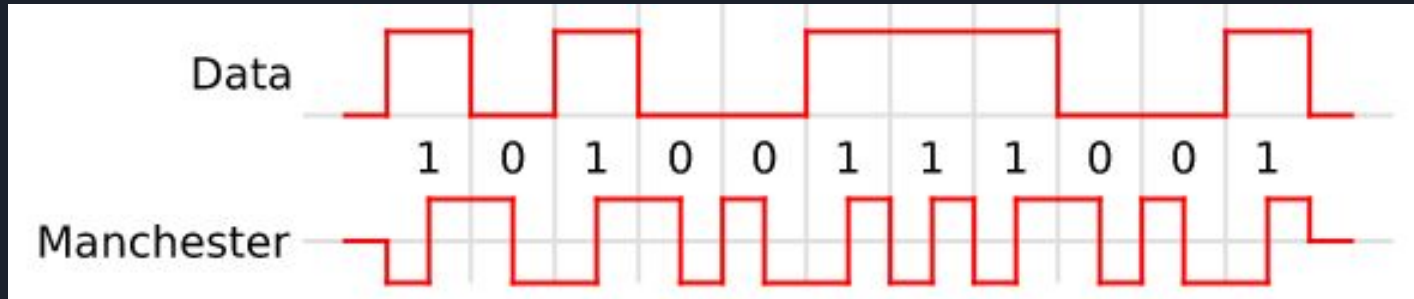
Disadvantages:

- Glass is fragile, can crack if bent
- Expensive laser to operate



Encoding

Raw electrical signals have to be converted into bits. There are several different ways to do this, but the most common is called Manchester Encoding:



High to Low = 0
Low to High = 1



Layer 2 - Data Link Layer

The data link layer is responsible for processing the raw bits from the physical layer, correcting any errors, and extracting information such as the source and destination device addresses.

We'll look at:

- MAC Addresses
- Framing
- Switches



What is a MAC Address?

Every device with the ability to connect to the internet will have a Network Interface Card (NIC). These cards are given a unique address when they are manufactured and we call this a MAC (Media Access Control) address.

MAC addresses are made up of 6 octets:

- AA:BB:CC:DD:EE:FF
- AA:BB:CC:11:22:33
- FF:DD:EE:CC:BB:AA

The first 3 octets are the same depending on the manufacturer

Framing and Error Correction

Ethernet Frame



The purpose of framing is to convert the raw bits from the physical layer into readable sections containing header information and data to pass on to the next layer.

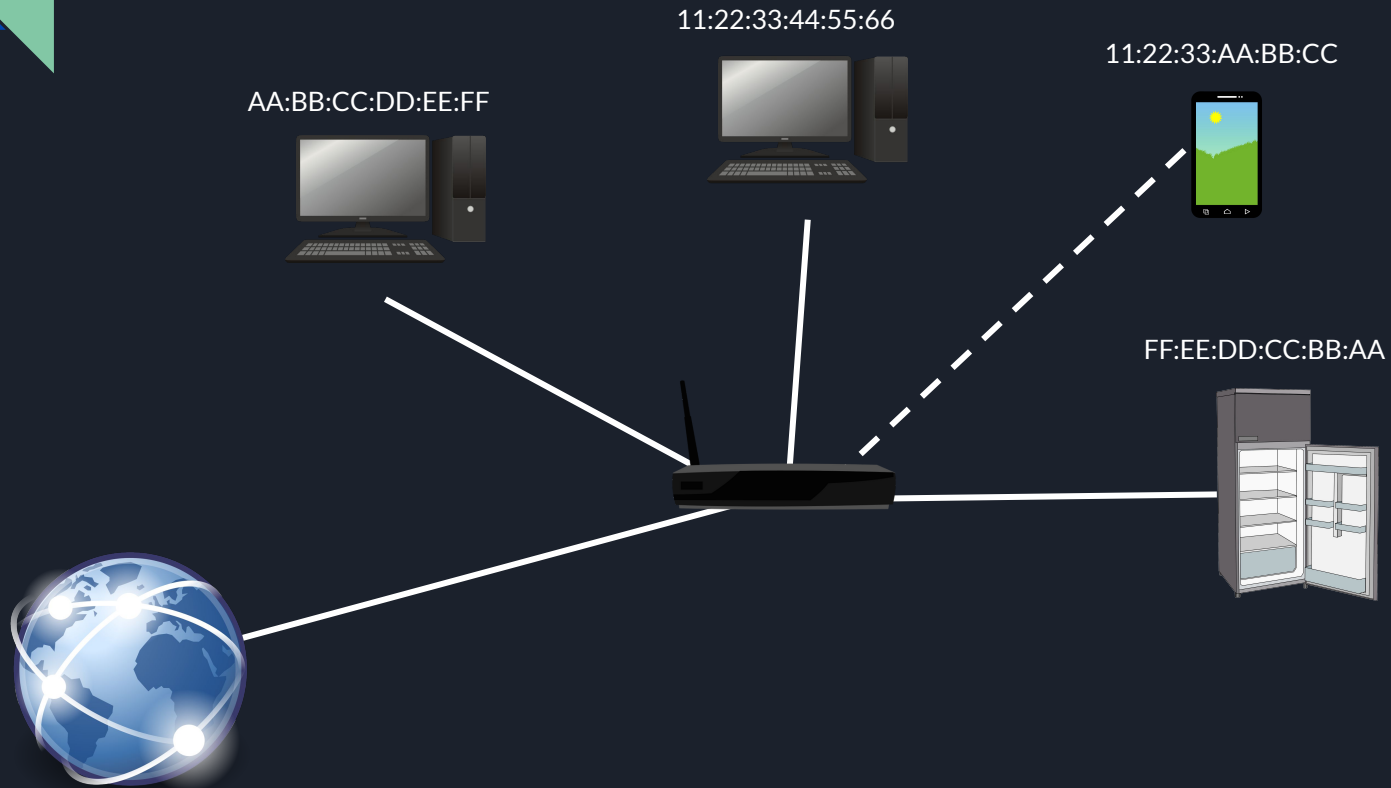
Raw bit streams can often be corrupted, so it's up to the data link layer to detect these errors and correct them by altering the 4 byte correction code at the end of the frame.

Switches

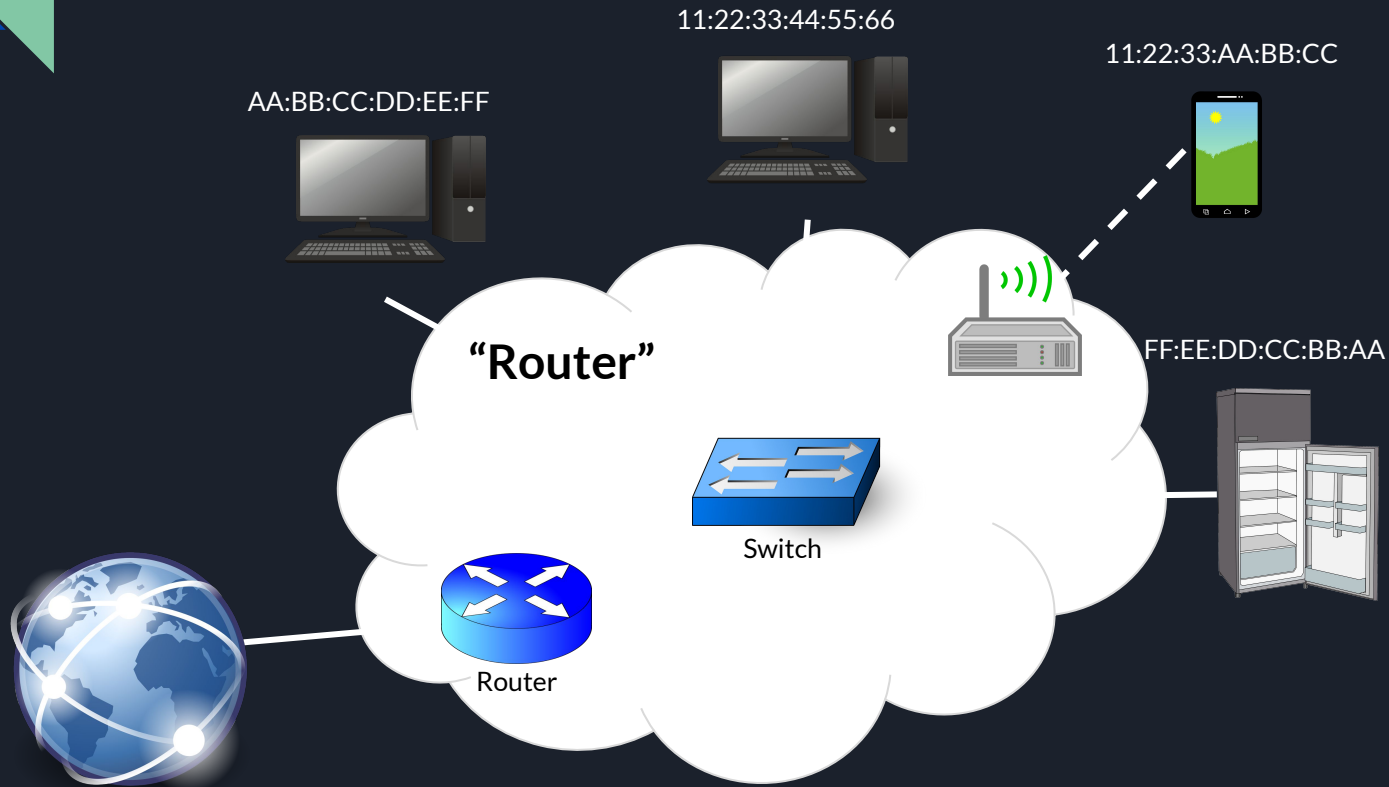
A switch is a layer 2 device that allows multiple devices to be connected via an ethernet cable. When a device sends a packet to the switch, the switch determines the destination MAC address and sends it to the appropriate device.



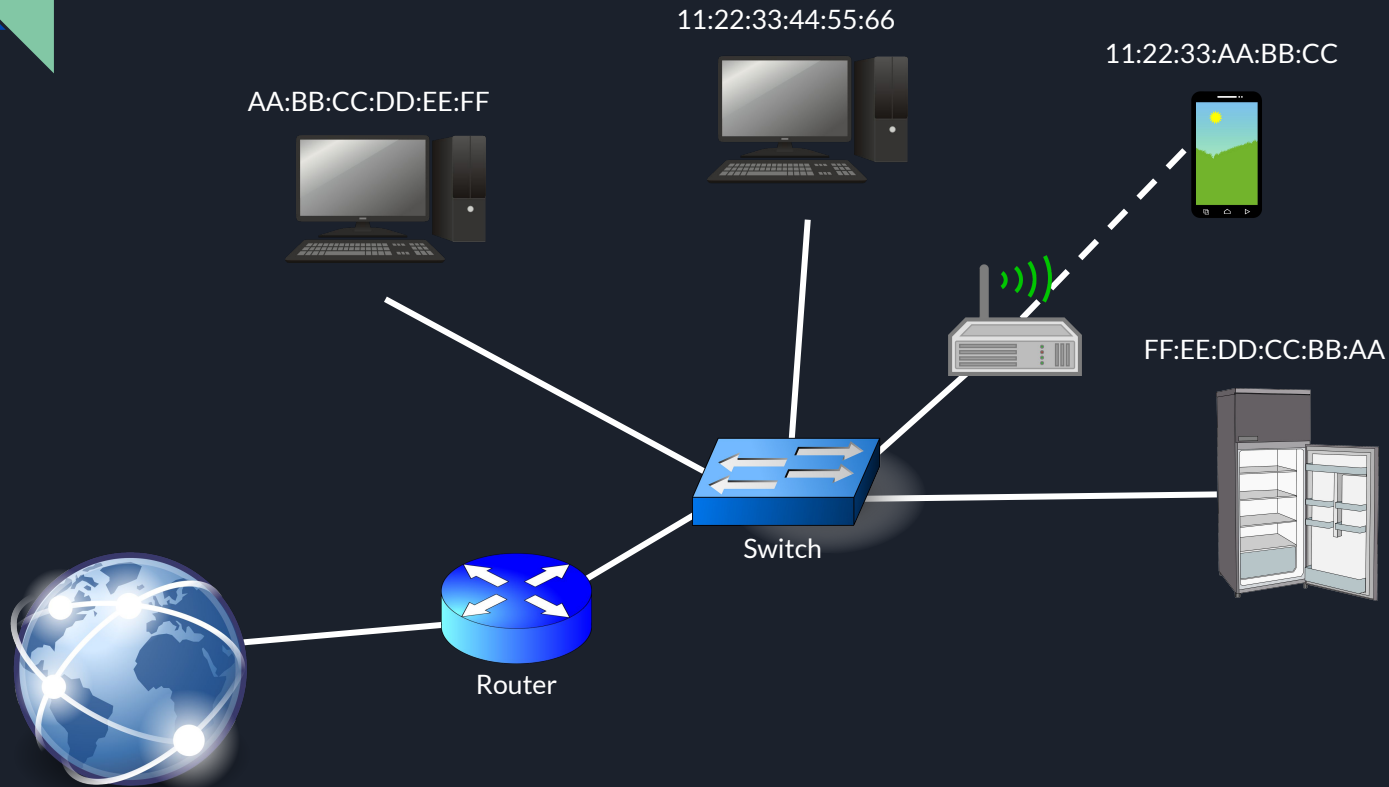
Back to the network...



Back to the network...



Back to the network...





Layer 3 - Network Layer

The network layer is responsible for extracting the useful information from frames and creating packets. It's up to the network layer to discover the best route for these packets. The main difference between the network layer and the data link layer is that packets can be sent across different networks.

We'll look at:

- IP addresses
- Packets
- IPv4 and IPv6



Internet Protocol Addressing

When a device connects to a network, it is given a unique address (this will be different on different networks) - this is called an IP address. A few examples could be:

- 192.168.0.1
- 10.0.0.1
- 130.209.241.197

Structure for IPv4 address [0-255].[0-255].[0-255].[0-255]



Source: Mr Robot



Public and Private IPs

There aren't enough IPv4 addresses to allocate to every device in the world, so to solve this we have private IP addresses. Private addresses can only be accessed from within the network and are unique for each network whereas public addresses can be accessed from anywhere with an internet connection.

Class	From	To
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255



Find your IP...

Find your private IP address:

- Windows: `ipconfig`
- Linux: `ifconfig` or `ip a`

Find your public IP address by searching “what is my IP” in pretty much any search engine

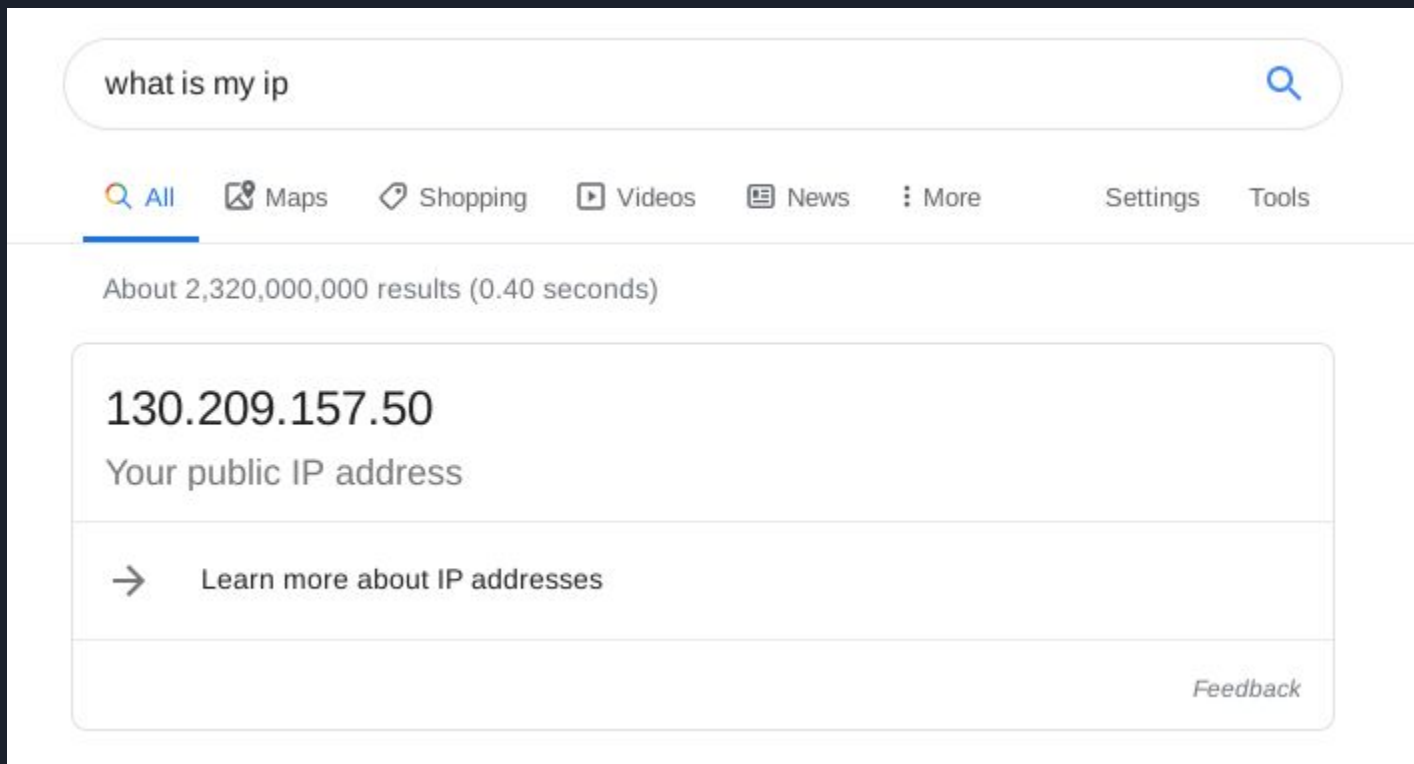


Private IP on Eduroam

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 7564 bytes 934599 (912.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7564 bytes 934599 (912.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.150.55 netmask 255.255.128.0 broadcast 172.30.255.255
    inet6 fe80::701e:107d:4b9e:3f16 prefixlen 64 scopeid 0x20<link>
    ether fe:56:fc:2c:dc:d9 txqueuelen 1000 (Ethernet)
    RX packets 710415 bytes 720217861 (686.8 MiB)
    RX errors 0 dropped 206 overruns 0 frame 0
    TX packets 336247 bytes 72431184 (69.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Public IP on Eduroam



A screenshot of a Google search interface. The search bar at the top contains the text "what is my ip" and a magnifying glass icon. Below the search bar is a horizontal menu with links: "All" (with a magnifying glass icon), "Maps" (with a location pin icon), "Shopping" (with a shopping bag icon), "Videos" (with a play button icon), "News" (with a newspaper icon), "More" (with a vertical ellipsis icon), "Settings", and "Tools". Below the menu, the text "About 2,320,000,000 results (0.40 seconds)" is displayed. The main content area shows the IP address "130.209.157.50" in a large font, followed by the text "Your public IP address". Below this is a link with a right-pointing arrow and the text "Learn more about IP addresses". At the bottom right of the content area is a link labeled "Feedback".

what is my ip

[All](#) [Maps](#) [Shopping](#) [Videos](#) [News](#) [More](#) [Settings](#) [Tools](#)

About 2,320,000,000 results (0.40 seconds)

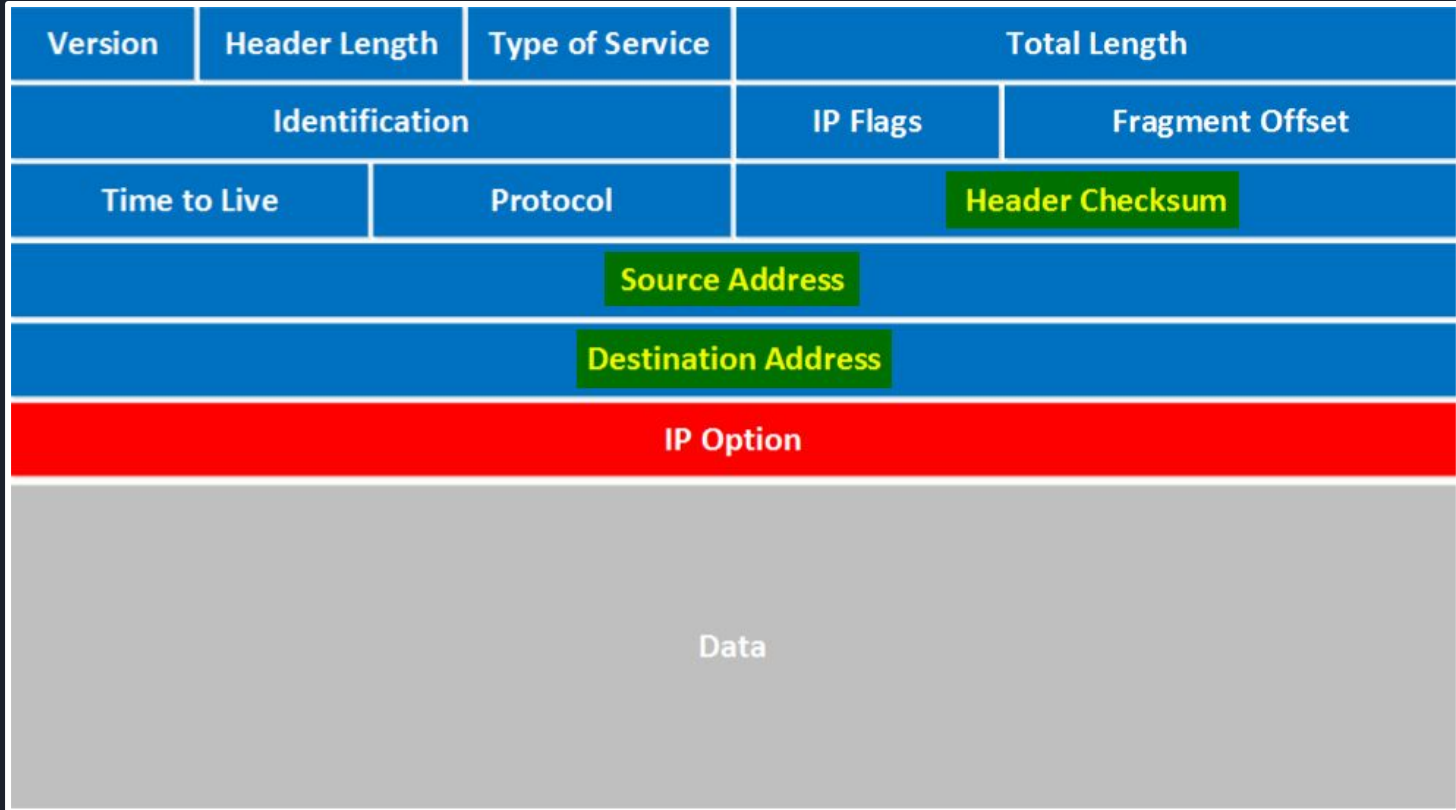
130.209.157.50
Your public IP address

→ [Learn more about IP addresses](#)

[Feedback](#)

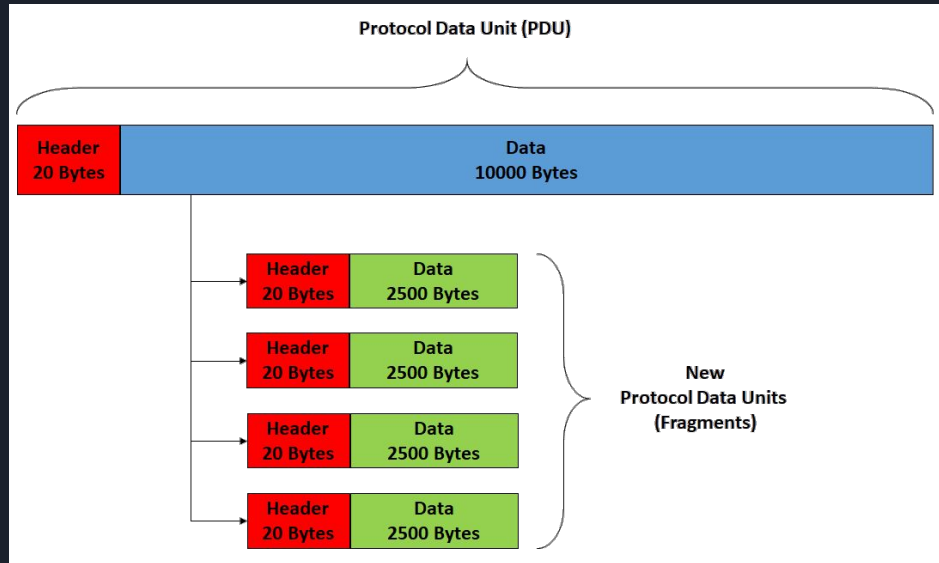


IPv4 Packet Structure



Fragmentation

The maximum size over ethernet is 1500 bytes, so any packets over this size will be separated into several smaller packets. This is called fragmentation.





Difference between IPv4 and IPv6

IPv4 addresses are 32-bit, meaning there are 2^{32} (around 4 billion) possible addresses available. This was fine back when the internet was first made, but now we've run out of possible IPv4 addresses. This is where IPv6 comes in...

IPv6 addresses are 128-bit, meaning there are 2^{128} (around 340 billion billion billion billion) possible addresses available. IPv6 was introduced in 2011 and has only recently become more widely used due to companies adding support for it.



IPv6 Address

8 groups of 4 hexadecimal digits:

2001:0DB8:0000:FE01:0000:0000:0000:AC10

Can be shortened by:

- Removing leading zeros
- Replacing 0000's with a single 0
- Remove multiple zeros with ::

2001:DB8:0:FE01::AC10



IPv6 Packet

Version	Traffic class	Flow label	
Payload length		Next header	Hop limit
Source address			
Destination address			



Transport Layer

The transport layer is responsible for making the network layer more reliable and much simpler to use. We'll be focusing on the two most widely used protocols that we probably use thousands of times a day without realising it:

- TCP
- UDP



But first... Ports

Before we move onto transport protocols, we need to understand what ports are first. Ports are just communication endpoints. They allow you to communicate with a certain process running on that device. For example, when you connect to a website, you're actually connecting to the IP at port 80 (e.g 192.168.0.1:80).

There are 65535 possible ports for TCP and UDP...



TCP

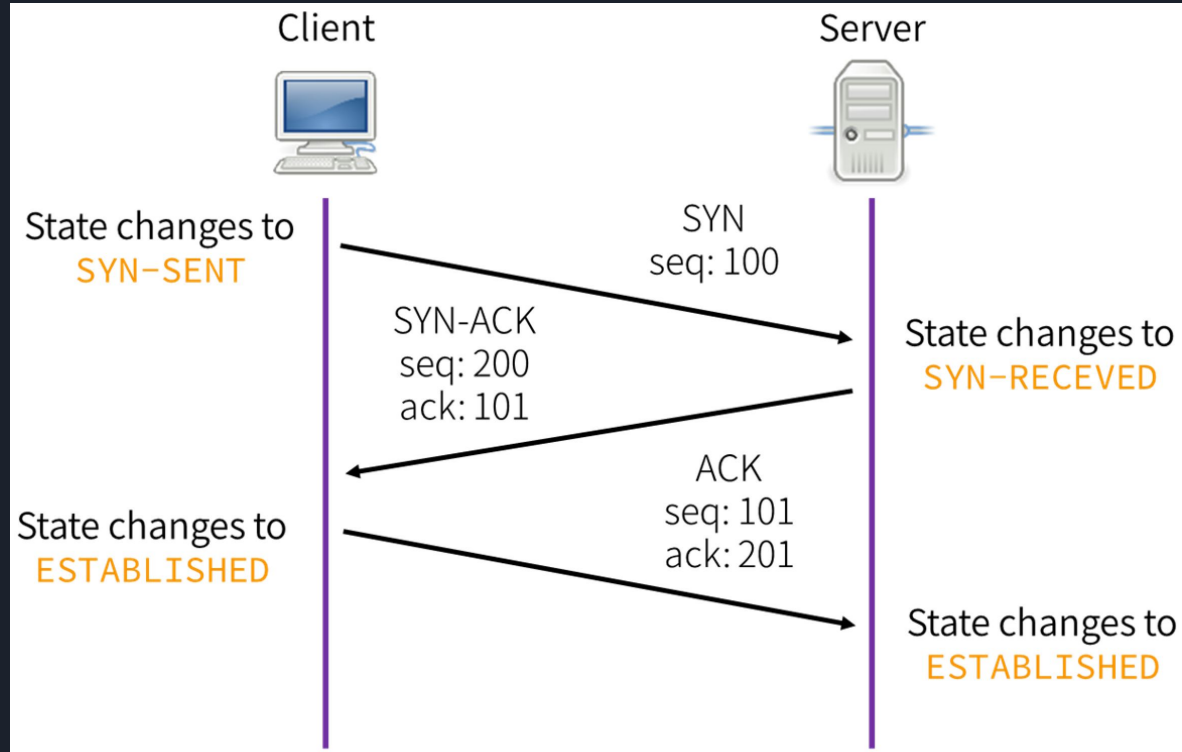
TCP (Transmission Control Protocol) is the most used protocol. This is because it is reliable and ensures that data reaches its target.

TCP ensures that:

- Data arrives at location
- Data arrives in the correct order

In order for TCP to ensure a reliable connection, it has to complete a 3-way handshake, which in turn makes it much slower...

3-way Handshake





UDP

UDP (User Datagram Protocol) does not check to ensure that the packets actually arrive at the other end and don't require a connection. This means it is much faster to send UDP packets. This is useful for services like:

- VoIP (voice over IP)
- Live streams and videos
- Streaming music

You are unlikely to notice if a few packets are dropped or in the wrong order when using these services, which makes UDP much more desirable.



Firewalls

The purpose of a firewall is to block incoming and outgoing packets in a network. You can set certain rules on firewalls to filter out connections from certain port ranges or from a certain program. Firewalls allow you to log everything on your network and can actually defeat a lot of malicious attacks.

For example, imagine you have spyware on your computer and it's constantly sending data to an IP. You could block all connections to and from that IP and any IP range that it uses, effectively making the malware useless (you would still have to remove it though).

You can also mitigate DDoS attacks. Imagine you had hundreds of IP addresses from a similar region spamming you with packets. You could block all IPs coming from that region (temporarily until you find a better way to mitigate the attack or they stop).



Network Tools

Command Line Tools:

- ping, arp, nslookup, dig, traceroute, netstat, nmap

Graphical Tools:

- Wireshark
- ZenMap

Web Tools:

- Whois
- Shodan



Nmap Port Scanning

Nmap is a popular tool for scanning for open ports on networks. It's a very powerful tool and allows you to determine the software and version running on the ports, and the operating system of the machine.

You can download it from the official site <https://nmap.org> or if you're using Kali Linux or other debian-based distro you can do `sudo apt-get install nmap`

If you want to use the GUI version you can download it here: <https://nmap.org/zenmap/>



Basic Port Scanning

We'll be using <http://scanme.nmap.org/> to practice nmap legally. There is a big debate on whether or not port scanning is illegal or not. To be safe, I would recommend only port scanning servers that you own or have permission to scan.

```
[murphy@laptop ~]$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-22 13:44 GMT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 945 filtered ports, 53 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 16.88 seconds
```




More on port scanning...

- sC flag runs default script
- sV flag determines the software version running on the ports
- O flag tries to figure out the OS running on the device
- p flag allows you to choose the port(s) to scan

More at `man nmap` or `nmap --help`



Whois

Whois gives you lots of information about the registrar of domains and servers. It's useful for finding out if an IP address is a VPN or not.

<http://whois.domaintools.com/>

Normal IP: <http://whois.domaintools.com/109.151.201.178>

VPN: <http://whois.domaintools.com/195.206.183.109>



Shodan

Shodan is a very powerful tool that allows you to collect information on servers all around the world. Shodan can be used to search for servers running certain operating systems or with certain ports open.

Here's an example report I made of the University of Glasgow servers:

<https://www.shodan.io/report/3UHCraVn>



Monitoring Network Traffic



Wireshark

```
sudo apt-get install wireshark
```

<https://www.wireshark.org/#download>

Remember to run it as administrator/root!



Attacks on Networks?

The issue with most public and home networks is that they trust every packet that is sent and usually have default firewall settings.

This opens up the network to a variety of attacks:

- Man in The Middle (MiTM)
- DNS Spoofing
- Deauthentication Attack

Address Resolution Protocol (ARP)



What does an ARP packet look like?

No.	Time	Source	Destination	Protocol	Length	Info
361	23.444245	ArrisGro_ef:cb:9f	GoodWayI_26:52:98	ARP	60	Who has 192.168.0.27? Tell 192.168.0.12
362	23.444252	GoodWayI_26:52:98	ArrisGro_ef:cb:9f	ARP	42	192.168.0.27 is at 00:50:b6:26:52:98
1146	29.076176	ArrisGro_37:ba:d0	GoodWayI_26:52:98	ARP	60	Who has 192.168.0.27? Tell 192.168.0.1
1147	29.076186	GoodWayI_26:52:98	ArrisGro_37:ba:d0	ARP	42	192.168.0.27 is at 00:50:b6:26:52:98

▼ Ethernet II, Src: ArrisGro_ef:cb:9f (10:56:11:ef:cb:9f), Dst: > Destination: GoodWayI_26:52:98 (00:50:b6:26:52:98)
> Source: ArrisGro_ef:cb:9f (10:56:11:ef:cb:9f)
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000

▼ Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: ArrisGro_ef:cb:9f (10:56:11:ef:cb:9f)
Sender IP address: 192.168.0.12
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.0.27

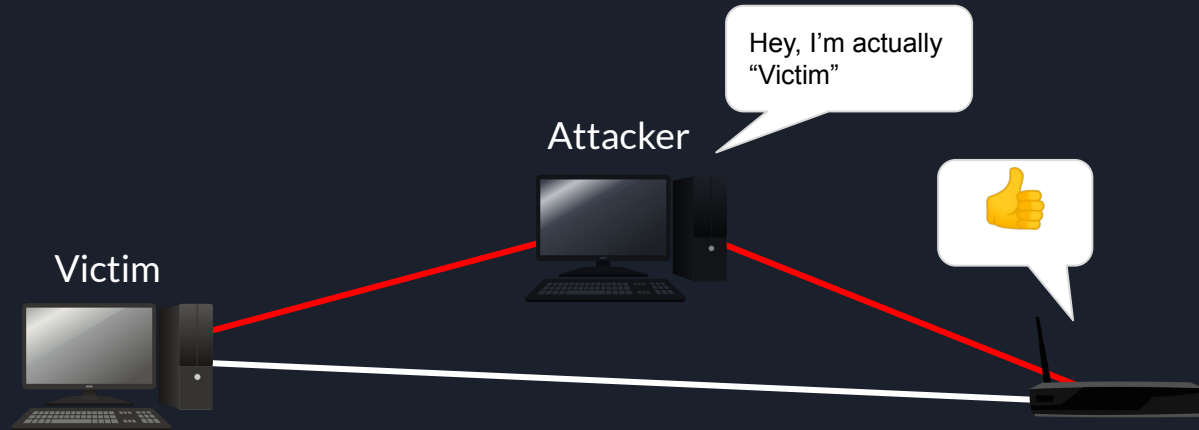
▼ Ethernet II, Src: GoodWayI_26:52:98 (00:50:b6:26:52:98), Dst: > Destination: ArrisGro_ef:cb:9f (10:56:11:ef:cb:9f)
> Source: GoodWayI_26:52:98 (00:50:b6:26:52:98)
Type: ARP (0x0806)

▼ Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: GoodWayI_26:52:98 (00:50:b6:26:52:98)
Sender IP address: 192.168.0.27
Target MAC address: ArrisGro_ef:cb:9f (10:56:11:ef:cb:9f)
Target IP address: 192.168.0.12

Man in The Middle Attack



Man in The Middle Attack





Example MiTM Code

Warning: PLEASE do not run this on eduroam or any other network you do not own

You can find my example code on my GitHub page:

https://github.com/fork-bombed/networks/blob/master/arp_spoof.py

This will only run the MiTM attack for less than a minute as it does not spoof replies for any other requests. Feel free to test it on your home network and see what data you can find in Wireshark.



Man in The Middle Attack

Now all the data between the victim and the router is going between the attacker. The attacker can now act as a “malicious firewall” and deny or even alter packets to and from the victim.

MiTM attacks used to be very dangerous as you could view people’s passwords and sensitive data sent over the network. But this is no longer this case. This is because of TLS (Transport Layer Security) which uses asymmetric encryption to encrypt HTTP packets (this is what the little HTTPS means in URLs).



DNS Spoofing

So you can't sniff passwords using MiTM attacks, so what's the point?

Well, remember we have full control of what goes in and out of their network - so we control what they see and what they don't. When the victim visits a website, they make a DNS request to retrieve the IP address of that website - so what if we intercepted the response and changed the IP?

The web browser would still show the domain name, but would be pointing to a different IP address - one where we could be running a phishing page to steal the user's credentials...



Flaws with DNS Spoofing

Remember TLS? Well it also helps to protect against DNS spoofing as well. When you alter the IP address in the DNS response, the browser will warn the user that the webpage is no longer secure since you are unable to provide the SSL certificate (since you don't have the private key, you are unable to complete the connection setup, so it will not show).

However, sometimes people aren't very observant and won't realise that there's not an SSL certificate on the page and still enter their details, so you can always rely on human error :)

Eventual treatment of all
HTTP pages in Chrome:



Not secure

example.com

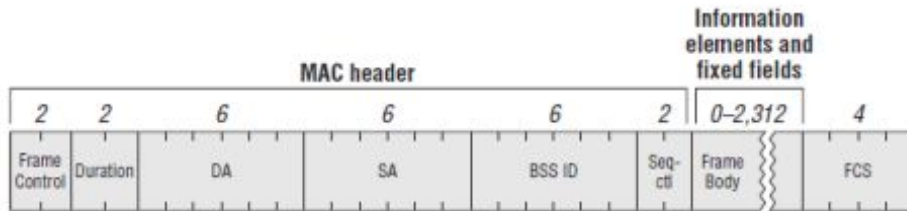


Deauthentication Attack

Deauthentication attacks allow you to temporarily kick anyone off a wireless network. They work by sending a spoofed management frame requesting that the victim's device is deauthenticated. This will cause them to disconnect from the network temporarily and reauthenticate. If you repeat this several times then the victim will not be able to access the internet. These attacks are very simple to execute and impossible to block.

These attacks are usually the beginning of some more advanced attacks such as capturing the 4-way handshake to crack WiFi passwords or setting up fake access points and tricking the reauthenticating devices into connecting.

Management Frames




We can spoof the source MAC address (SA) to our victim's address and set the subtype bits to 1100 for a deauthentication frame.

This is a super simple frame to craft and takes very little effort to make your own denial of service attack from it.

Source: <https://mrncciew.com/2014/09/29/cwap-802-11-mgmt-frame-types/>

TABLE 4.1 Management frame subtypes

Subtype bits	Subtype description
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response
1000	Beacon
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication
1101	Action
1110	Action no ack



Shout out to Nikos for the amazing notes
provided in NOSE2





What else do I do?

Running two more workshops before CDX:

- **OWASP** (Fri 7th Feb)
- **Pentesting** (Tue 11th Feb)

I run the *UofG Computing* Discord server (<https://discord.gg/ngvtDCc>)

President of *GUSEC* (Glasgow University Security Society)