# Networking 2

@Emma

# Where are my packets going????

# How does my computer know where the router is?

Dynamic Host Configuration Protocol

Also how you got your IP address

# What is an IP address?

IP address is just a number

You can think of it as the phone number to your house

http://3520653040

# Stages of DHCP

Discover

- Prefers last IP

Offer

Reply

Accept

# What does DHCP give me?

1. Ip address
2. Subnet Mask
3. Router
4. Dns servers

# What is a subnet?

A subnet describes a range of addresses

# What is a subnet mask?

The subnet mask splits the ip address into the host  and network addresses.

# Clients must renew IP lease or else …


This is a DHCP server…

But it’s also a DHCP client?

# How do routers know where to send things

Send to the default route

Until it reaches a backbone

# How do backbone routers know where to go?

Border Gateway Protocol

That forms an autonomous system.

Facebook outage triggered by BGP configuration issue as services fail for 6 billion

# Why do we need routers

You would have to know everyone on lan

No redundancy

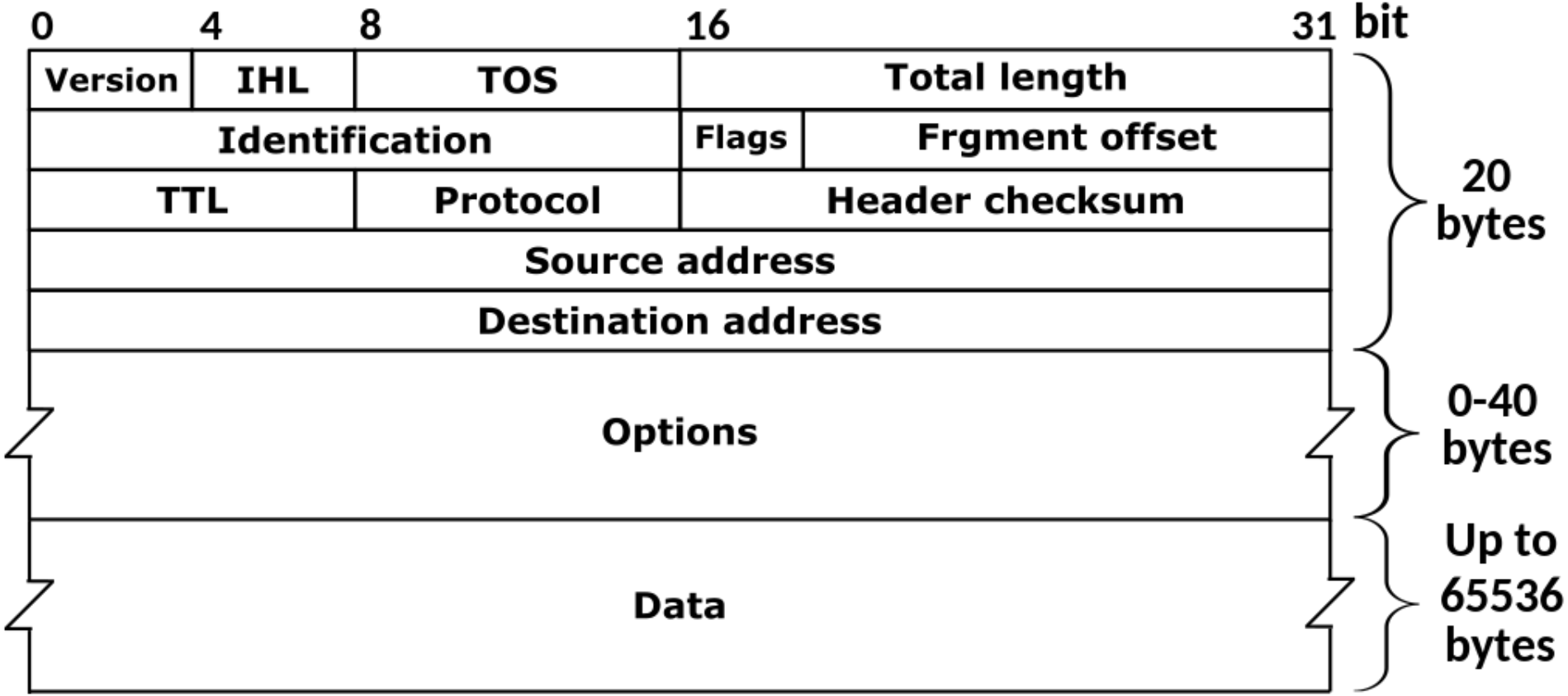

# What Security benefits do router have

Firewalls!

Can prevent bad stuff getting into our home network

# What is in my packets??

# What is an IP packet



# What happens when you PING?

Ping is part of Internet Control Message Protocol which sits on top of IP

# What's the problem with Graphs?

Cycles!

Which is why we need the ttl

# How do we know our packet was dropped?

ICMP

# How does trace route work

```
emma@penguin:~$ traceroute emmareuter.com
traceroute to emmareuter.com (143.204.154.78), 30 hops max, 60 byte packets
 1  100.115.92.193 (100.115.92.193)  0.272 ms  0.123 ms  0.042 ms
 2  100.115.92.25 (100.115.92.25)  2.208 ms  1.234 ms  1.091 ms
 3  192.168.86.1 (192.168.86.1)  3.065 ms  3.814 ms  3.739 ms
 4  072-182-096-001.res.spectrum.com (72.182.96.1)  17.160 ms  24.474 ms  25.523 ms
 5  tge0-0-4.ausbtx5201h.texas.rr.com (66.68.1.221)  33.453 ms  33.320 ms  33.056 ms
 6  agg25.ausutxla01r.texas.rr.com (24.175.43.223)  23.239 ms  19.619 ms  33.288 ms
 7  agg22.dllatxl301r.texas.rr.com (24.175.41.46)  39.268 ms  24.529 ms  39.175 ms
 8  bu-ether14.dllstx976iw-bcr00.tbone.rr.com (66.109.6.88)  40.449 ms bu-ether24.dllstx976iw-b
cr00.tbone.rr.com (66.109.6.52)  19.073 ms bu-ether14.dllstx976iw-bcr00.tbone.rr.com (66.109.6.
88)  27.296 ms
 9  66.109.5.121 (66.109.5.121)  27.113 ms 209-18-43-77.dfw10.tbone.rr.com (209.18.43.77)  26.8
61 ms  26.580 ms
10  99.83.71.240 (99.83.71.240)  25.326 ms  26.240 ms 99.83.71.242 (99.83.71.242)  27.081 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  server-143-204-154-78.dfw3.r.cloudfront.net (143.204.154.78)  26.194 ms  27.874 ms  27.446
ms
```

# Follow along

Tracert - windows

Traceroute - unix

# What options do?

More fragments says there are more fragments coming.

# What happens on top of IP

ICMP, TCP or UDP …

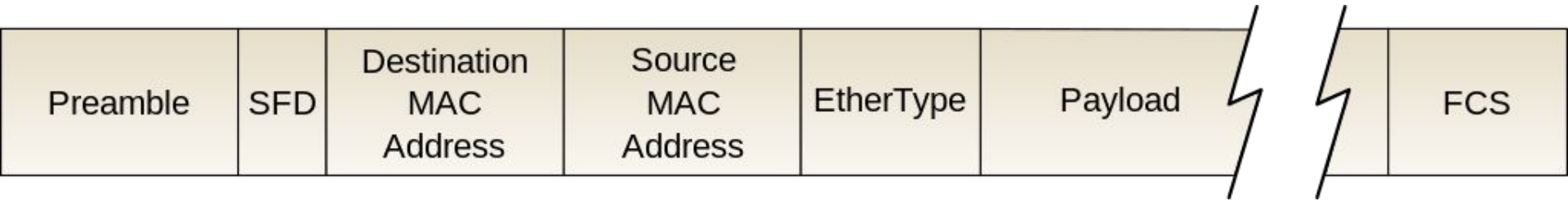
# What's the difference between TCP and UDP?

- Reliability
- Speed
-

# What happens over TCP?

HTTP, DNS, DHCP, FTP

# How does it get to the router though?



# How do we know what mac address

Through address resolution protocol!

# What does ARP do?

Maps from IP -> Mac address

Because IP addresses can change

Needed to actually get packets to computers

Never leaves the LAN

# Thanks

Feel free to ask questions!

# Hack the box

- https://app.hackthebox.com/invite
- Sign up
- https://app.hackthebox.com/starting-point
- Nmap -sC -sV <ip address>