IEO Final Presentation

Made By Shanessa Kostaman | Tobias Agyasta Haloman

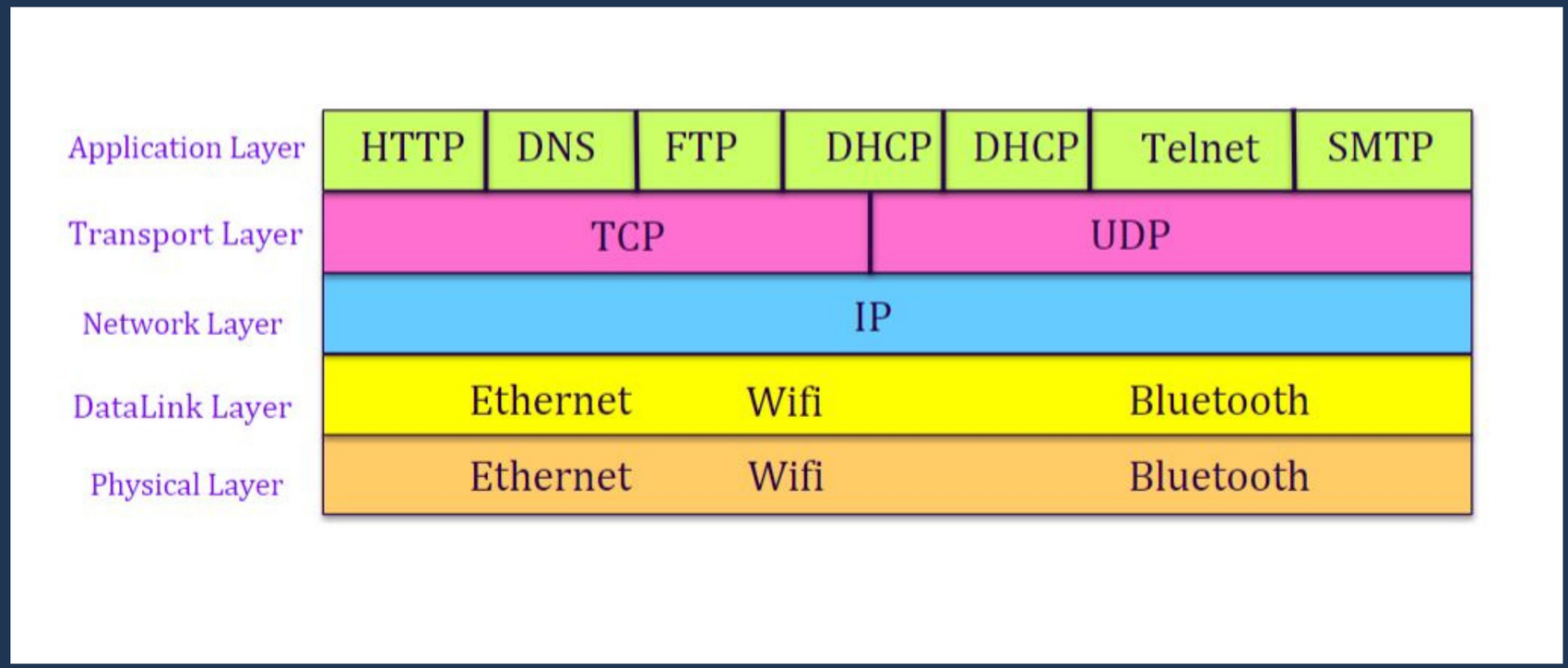
STUDENT NUMBER 4082419 | 4252861

TODAY'S DISCUSSION

TOPICS TO COVER

WEEK 7

NETWORK BASICS



WEEK 7

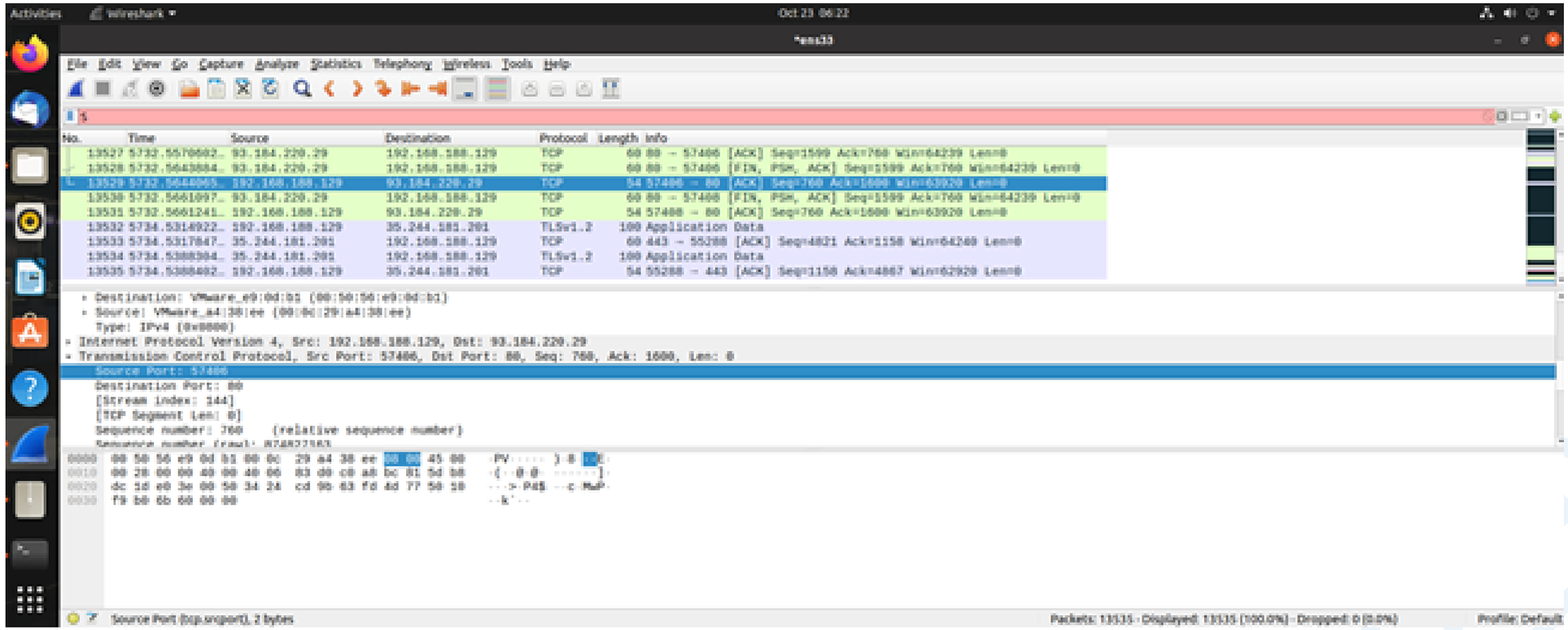
NETWORK BASICS

WHAT IS WIRESHARK?

Wireshark is a network packet analyzer.

WEEK 7

NETWORK BASICS



WEEK 7

NETWORK BASICS

IP ADDRESS

Source	Destination	Protocol	Length	Info
217.105.38.147	85.214.212.192	HTTP	632	GET /w2.html HTTP/1.1

This number is an exclusive number on all information technology devices (printers, routers, modems, etc) use which identifies and allows them the ability to communicate with each other on a computer network.

WEEK 7

NETWORK BASICS

MAC ADDRESS

```
Destination: JuniperN_03:a2:00 (30:7c:5e:03:a2:00)
Source: Dell_f2:1e:4e (f4:8e:38:f2:1e:4e)
```

MAC (Media Access Control) address is the hardware address of the Network Interface Card (NIC) of your computer.

WEEK 7

NETWORK BASICS

PORTS

```
Source Port: 63140
Destination Port: 80
```

network port is a 16-bit number that identifies one side of a connection between two computers.

WEEK 7

NETWORK BASICS

HOST

```
Hypertext Transfer Protocol
> GET /w2.html HTTP/1.1\r\n
  Host: courses.codemax.net\r\n
```

network host is a computer or other device connected to a computer network.

WEEK 8

IP ADDRESS

IFCONFIG AND IP

IFCONFIG (InterFace Configurator) and IP are sets of commands for Linux that allows for networking configuration through the command line. It is used to display and manage the IP address assigned to the machine it is running in.

WEEK 8

IP ADDRESS

WHAT IS PING?

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network.

WEEK 8

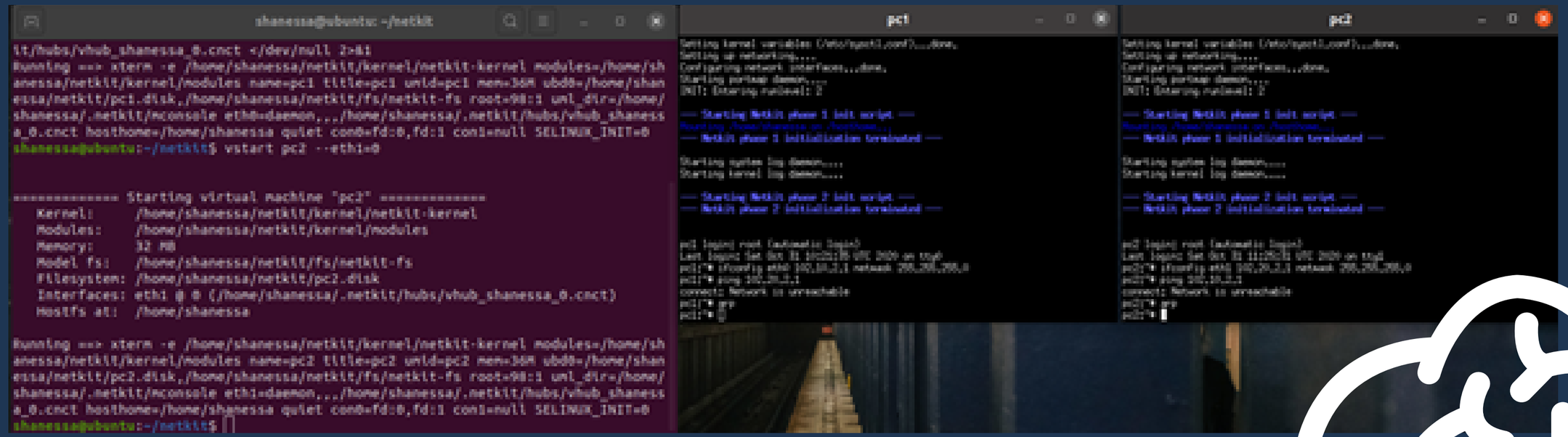
IP ADDRESS

WHAT IS ARP?

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite.

WEEK 8

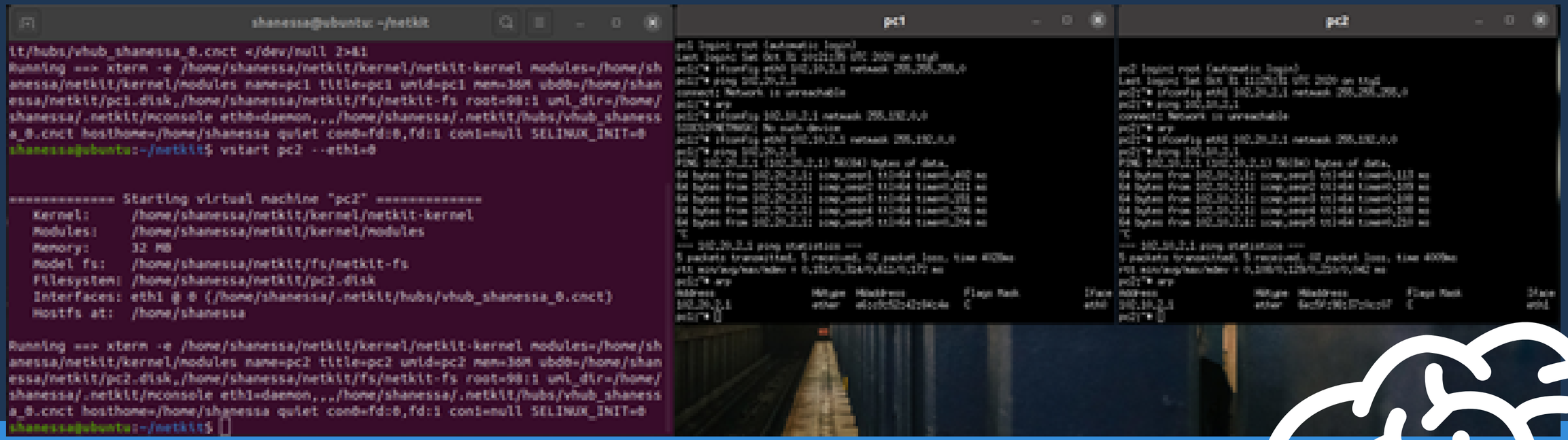
IP ADDRESS



WEEK 8

IP ADDRESS

CHANGED NETMASK



WEEK 8

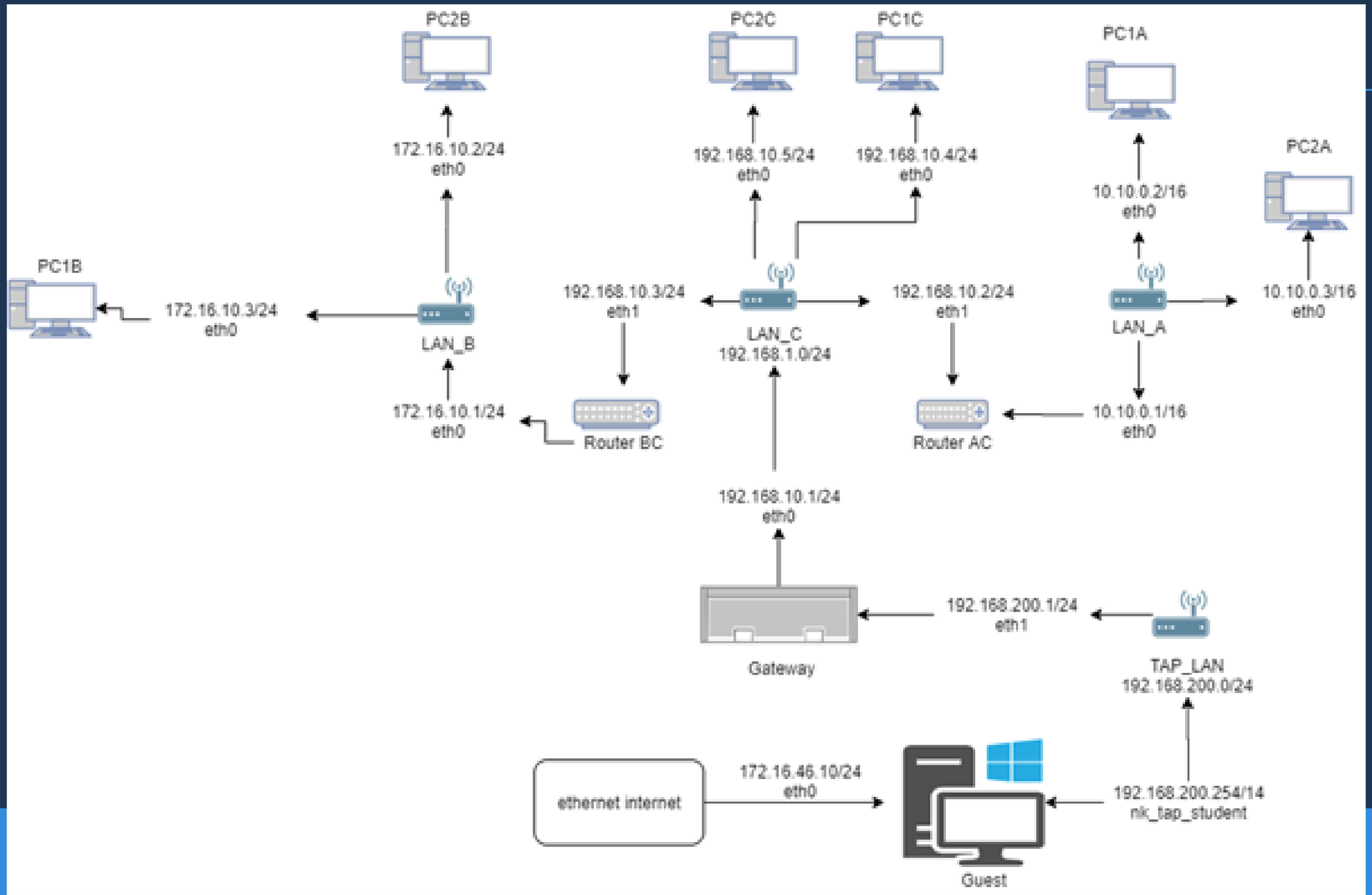
IP ADDRESS

WE'VE MADE OUR OWN NETWORK

1. PC1A, PC2A and RouterAC are connected to LANA
2. PC1B, PC2B and RouterBC are connected to LANB
3. PC1C, PC2C, RouterBC, RouterAC and Gateway are connected to LANC

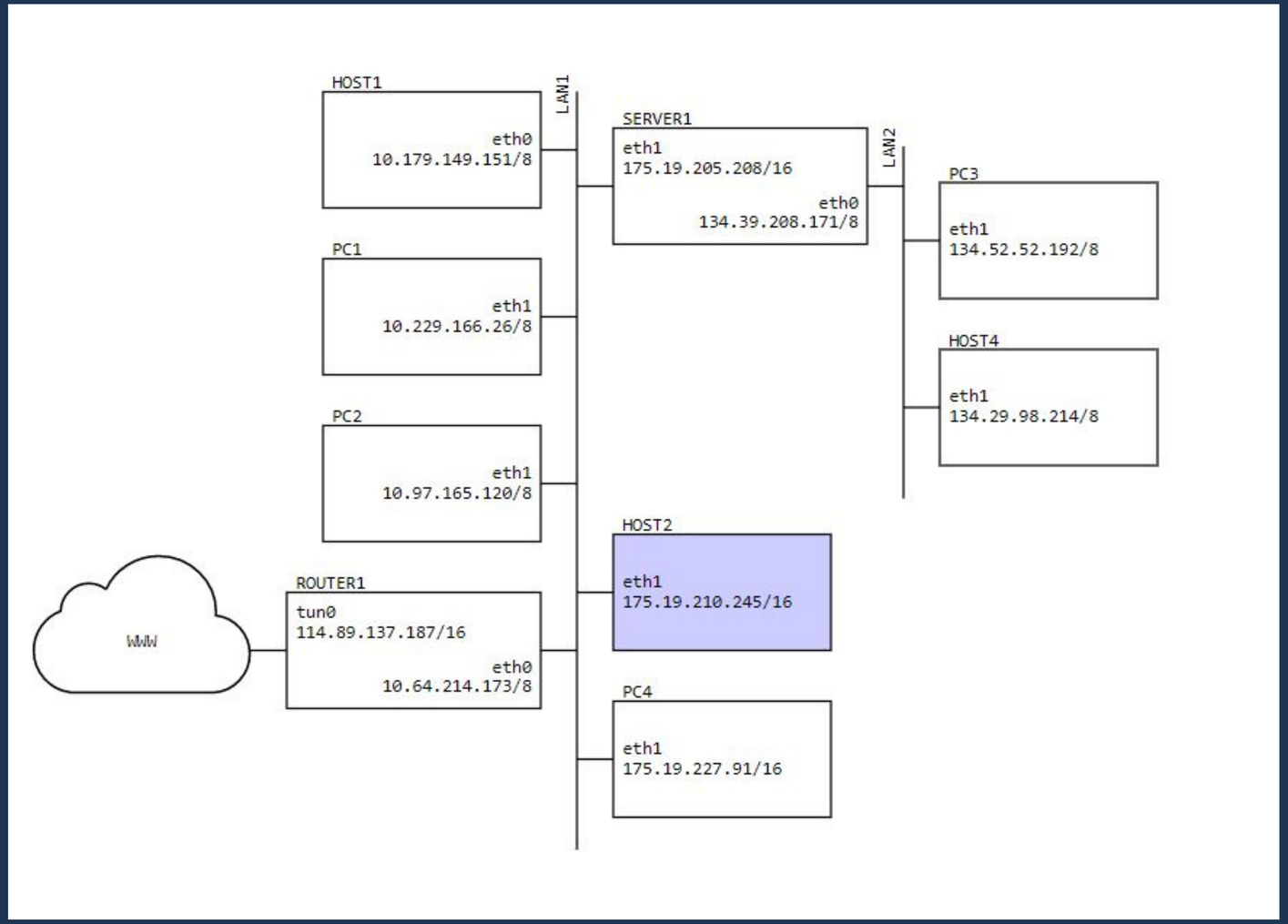
WEEK 8

IP ADDRESS



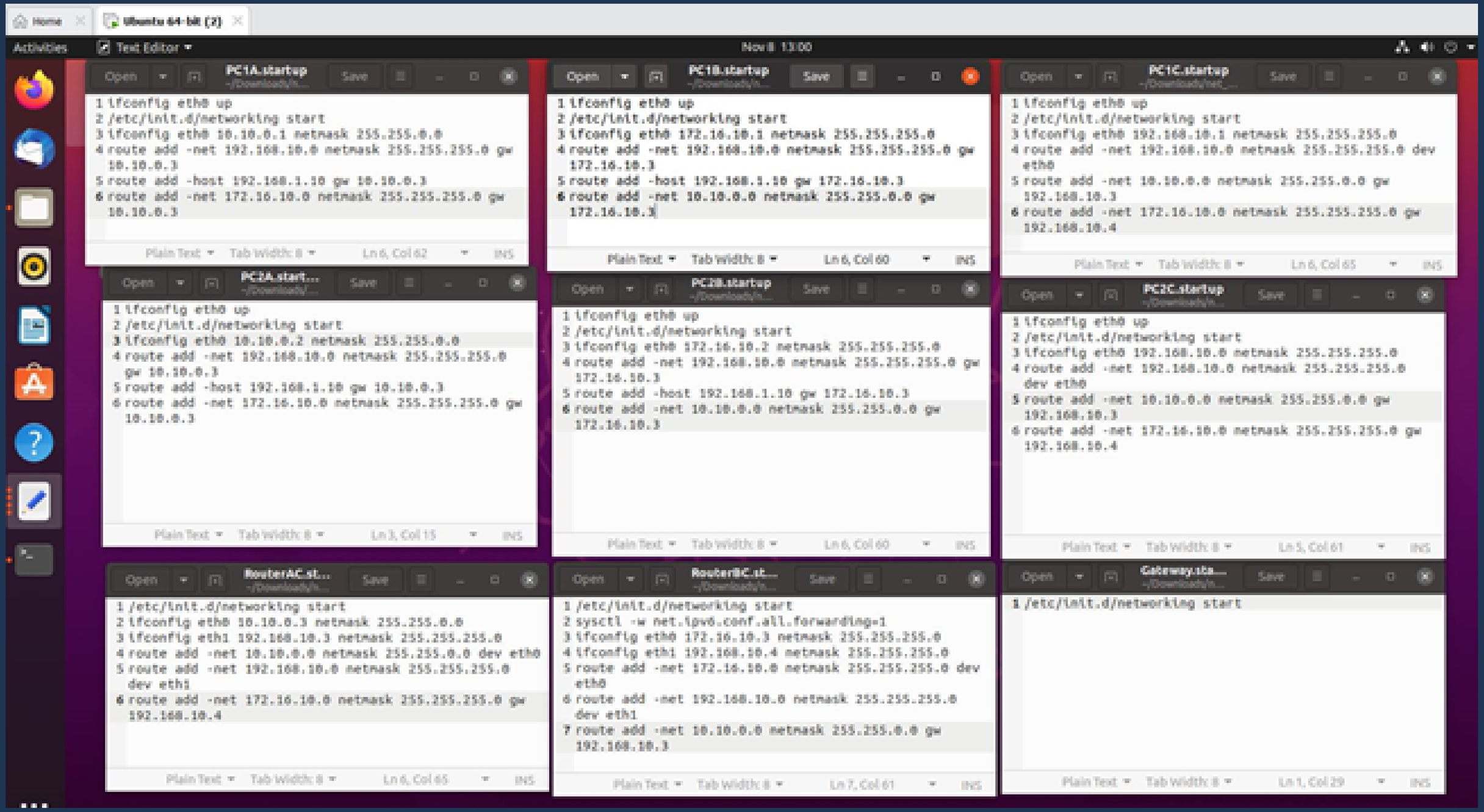
WEEK 9

IP ROUTING



STATIC VS DYNAMIC ROUTING

Static routing follows a manually defined routing protocol and routing table, will generally be unchanging unless changed directly by the network administrator. It is generally used in small networks. Dynamic routing is an automated process which allows for changes in the routing table once any network updates occur. It is generally used in larger networks (such as a company office space, schools, etc.)


Home
Ubuntu 64-bit (2)
Activities
Text Editor
Nov 8 13:00
PC1A.startup
1 ifconfig eth0 up
2 /etc/init.d/networking start
3 ifconfig eth0 10.10.0.1 netmask 255.255.0.0
4 route add -net 192.168.10.0 netmask 255.255.255.0 gw 10.10.0.3
5 route add -host 192.168.1.10 gw 10.10.0.3
6 route add -net 172.16.10.0 netmask 255.255.255.0 gw 10.10.0.3
PC1B.startup
1 ifconfig eth0 up
2 /etc/init.d/networking start
3 ifconfig eth0 172.16.10.1 netmask 255.255.255.0
4 route add -net 192.168.10.0 netmask 255.255.255.0 gw 172.16.10.3
5 route add -host 192.168.1.10 gw 172.16.10.3
6 route add -net 10.10.0.0 netmask 255.255.0.0 gw 172.16.10.3
PC1C.startup
1 ifconfig eth0 up
2 /etc/init.d/networking start
3 ifconfig eth0 192.168.10.1 netmask 255.255.255.0
4 route add -net 192.168.10.0 netmask 255.255.255.0 dev eth0
5 route add -net 10.10.0.0 netmask 255.255.0.0 gw 192.168.10.3
6 route add -net 172.16.10.0 netmask 255.255.255.0 gw 192.168.10.4
PC2A.start...
1 ifconfig eth0 up
2 /etc/init.d/networking start
3 ifconfig eth0 10.10.0.2 netmask 255.255.0.0
4 route add -net 192.168.10.0 netmask 255.255.255.0 gw 10.10.0.3
5 route add -host 192.168.1.10 gw 10.10.0.3
6 route add -net 172.16.10.0 netmask 255.255.255.0 gw 10.10.0.3
PC2B.startup
1 ifconfig eth0 up
2 /etc/init.d/networking start
3 ifconfig eth0 172.16.10.2 netmask 255.255.255.0
4 route add -net 192.168.10.0 netmask 255.255.255.0 gw 172.16.10.3
5 route add -host 192.168.1.10 gw 172.16.10.3
6 route add -net 10.10.0.0 netmask 255.255.0.0 gw 172.16.10.3
PC2C.startup
1 ifconfig eth0 up
2 /etc/init.d/networking start
3 ifconfig eth0 192.168.10.0 netmask 255.255.255.0
4 route add -net 192.168.10.0 netmask 255.255.255.0 dev eth0
5 route add -net 10.10.0.0 netmask 255.255.0.0 gw 192.168.10.3
6 route add -net 172.16.10.0 netmask 255.255.255.0 gw 192.168.10.4
RouterAC.st...
1 /etc/init.d/networking start
2 ifconfig eth0 10.10.0.3 netmask 255.255.0.0
3 ifconfig eth1 192.168.10.3 netmask 255.255.255.0
4 route add -net 10.10.0.0 netmask 255.255.0.0 dev eth0
5 route add -net 192.168.10.0 netmask 255.255.255.0 dev eth1
6 route add -net 172.16.10.0 netmask 255.255.255.0 gw 192.168.10.4
RouterBC.st...
1 /etc/init.d/networking start
2 sysctl -w net.ipv6.conf.all.forwarding=1
3 ifconfig eth0 172.16.10.3 netmask 255.255.255.0
4 ifconfig eth1 192.168.10.4 netmask 255.255.255.0
5 route add -net 172.16.10.0 netmask 255.255.255.0 dev eth0
6 route add -net 192.168.10.0 netmask 255.255.255.0 dev eth1
7 route add -net 10.10.0.0 netmask 255.255.0.0 gw 192.168.10.3
Gateway.sta...
1 /etc/init.d/networking start

WEEK 9

WHAT DID WE DO?

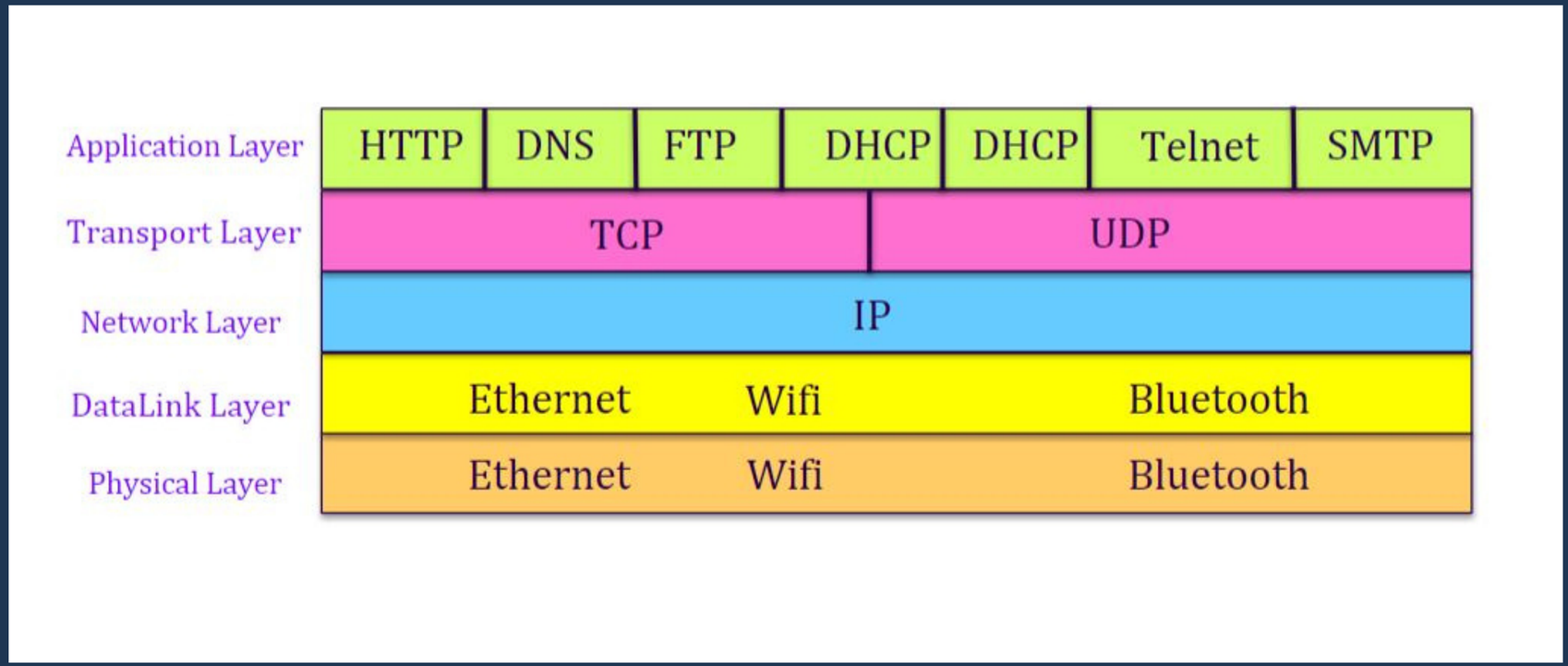
IP ROUTING

1. We added a route for every PC to connect to another corresponding PC from the routers through route add -net
2. We made the routers connect to each corresponding PCs in its domain (ex: Router A to PC1A, PC2A)

This is the basis of static routing!

WEEK 10

TCP/UDP PROTOCOLS

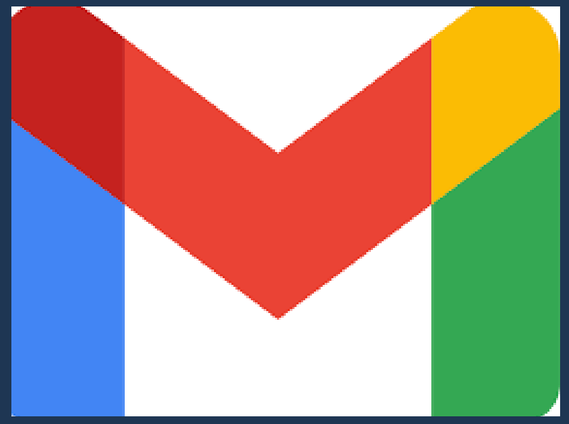


WHAT ARE TRANSPORT PROTOCOLS?

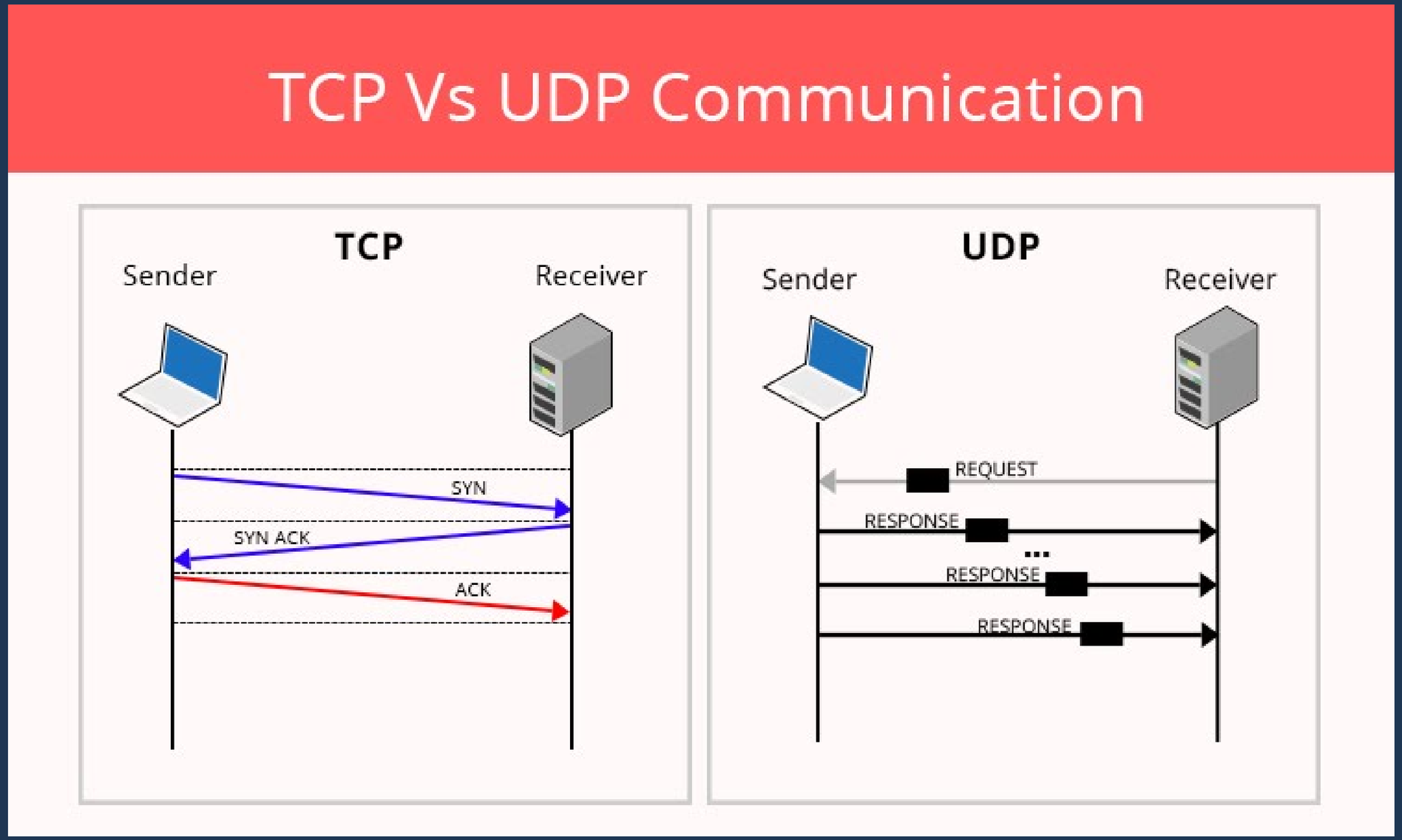
So we connected to each other through routing, now what?

We transport data!

The transport layer ensures that data can be transported through different networks, with different protocols depending on the type of transfer you want to execute.



TCP AND UDP



source:
https://sites.google.com/site/ciscoch9/_/rsrc/1525977696865/home/tcp-vs-udp/TCP%20VS%20UDP.jpeg

TCP SCENARIO 1: HTTPS

.105.38.147	91.198.174.192	TLSv1.2	160	Application Data
.105.38.147	91.198.174.192	TLSv1.2	93	Application Data
198.174.192	217.105.38.147	TCP	60	443 → 52212 [ACK] Seq=1 Ack=107 Win=83 Len=0
198.174.192	217.105.38.147	TCP	60	443 → 52212 [ACK] Seq=1 Ack=146 Win=83 Len=0
198.174.192	217.105.38.147	TLSv1.2	93	Application Data
198.174.192	217.105.38.147	TLSv1.2	154	Application Data
.105.38.147	91.198.174.192	TCP	54	52212 → 443 [ACK] Seq=146 Ack=140 Win=510 Len=0
.105.38.147	91.198.174.192	TLSv1.2	154	Application Data
198.174.192	217.105.38.147	TLSv1.2	198	Application Data
.105.38.147	91.198.174.192	TCP	54	52212 → 443 [ACK] Seq=246 Ack=284 Win=516 Len=0
.105.38.147	91.198.174.192	TLSv1.2	194	Application Data
198.174.192	217.105.38.147	TLSv1.2	1320	Application Data
.105.38.147	91.198.174.192	TCP	54	52212 → 443 [ACK] Seq=386 Ack=1550 Win=511 Len=0

ire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3BD00995-1D4D-4198-B8E7-B50643E6FF14}, id 0
erN_03:a2:00 (30:7c:5e:03:a2:00), Dst: Dell_f2:1e:4e (f4:8e:38:f2:1e:4e)
1e:4e (f4:8e:38:f2:1e:4e)
a2:00 (30:7c:5e:03:a2:00)

TCP SCENARIO 2: SMTP

	Source	Destination	Protocol	Length	Info
5	217.105.38.147	173.194.79.108	TCP	66	52301 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	173.194.79.108	217.105.38.147	TCP	66	587 → 52301 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
0	217.105.38.147	173.194.79.108	TCP	54	52301 → 587 [ACK] Seq=1 Ack=1 Win=131328 Len=0
9	173.194.79.108	217.105.38.147	SMTP	108	S: 220 smtp.gmail.com ESMTP op24sm9440680ejb.56 - gsmtp
8	217.105.38.147	173.194.79.108	TCP	54	52301 → 587 [ACK] Seq=1 Ack=55 Win=131328 Len=0
1	217.105.38.147	173.194.79.108	TCP	55	52301 → 587 [PSH, ACK] Seq=1 Ack=55 Win=131328 Len=1 [TCP segment of a reassembled PDU]
7	173.194.79.108	217.105.38.147	TCP	60	587 → 52301 [ACK] Seq=55 Ack=2 Win=65536 Len=0
3	217.105.38.147	173.194.79.108	TCP	55	52301 → 587 [PSH, ACK] Seq=2 Ack=55 Win=131328 Len=1 [TCP segment of a reassembled PDU]
1	173.194.79.108	217.105.38.147	TCP	60	587 → 52301 [ACK] Seq=55 Ack=3 Win=65536 Len=0
5	217.105.38.147	173.194.79.108	TCP	55	52301 → 587 [PSH, ACK] Seq=3 Ack=55 Win=131328 Len=1 [TCP segment of a reassembled PDU]
6	173.194.79.108	217.105.38.147	TCP	60	587 → 52301 [ACK] Seq=55 Ack=4 Win=65536 Len=0
4	217.105.38.147	173.194.79.108	TCP	55	52301 → 587 [PSH, ACK] Seq=4 Ack=55 Win=131328 Len=1 [TCP segment of a reassembled PDU]
3	173.194.79.108	217.105.38.147	TCP	60	587 → 52301 [ACK] Seq=55 Ack=5 Win=65536 Len=0

ytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{3BD00995-1D4D-4198-B8E7-B50643E6FF14}, id 0

rc: JuniperN_03:a2:00 (30:7c:5e:03:a2:00), Dst: Dell_f2:1e:4e (f4:8e:38:f2:1e:4e)

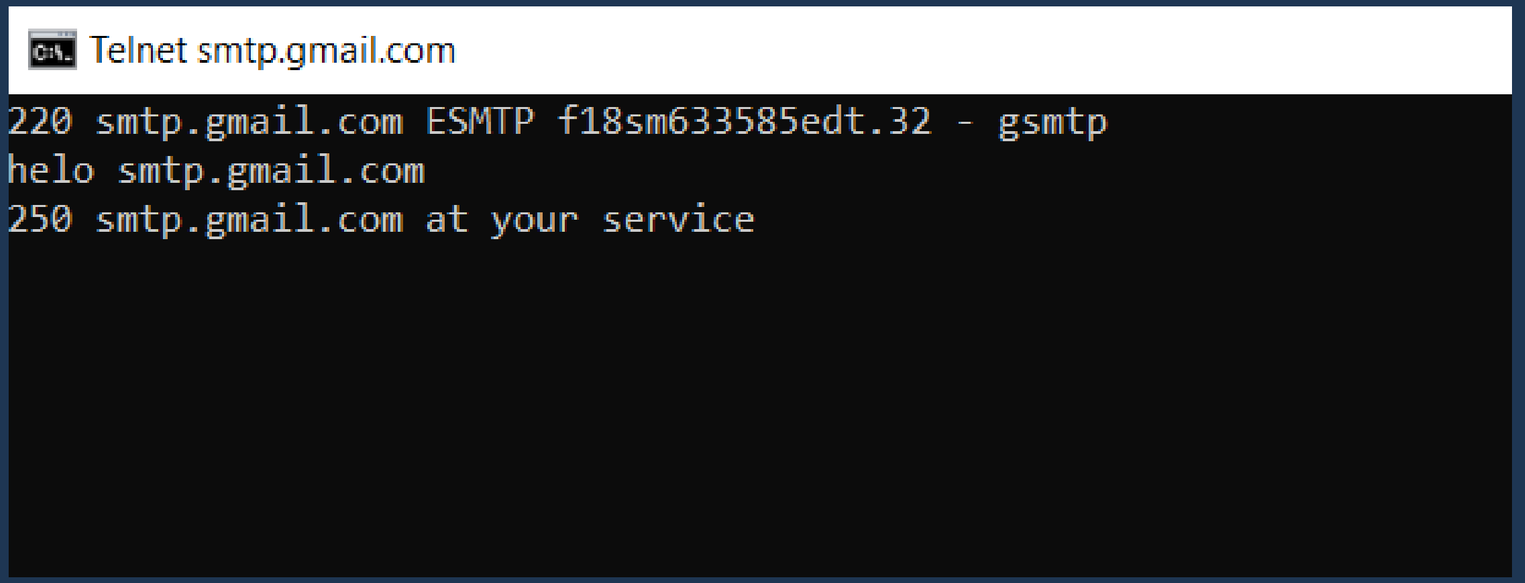
Dell_f2:1e:4e (f4:8e:38:f2:1e:4e)

perN_03:a2:00 (30:7c:5e:03:a2:00)

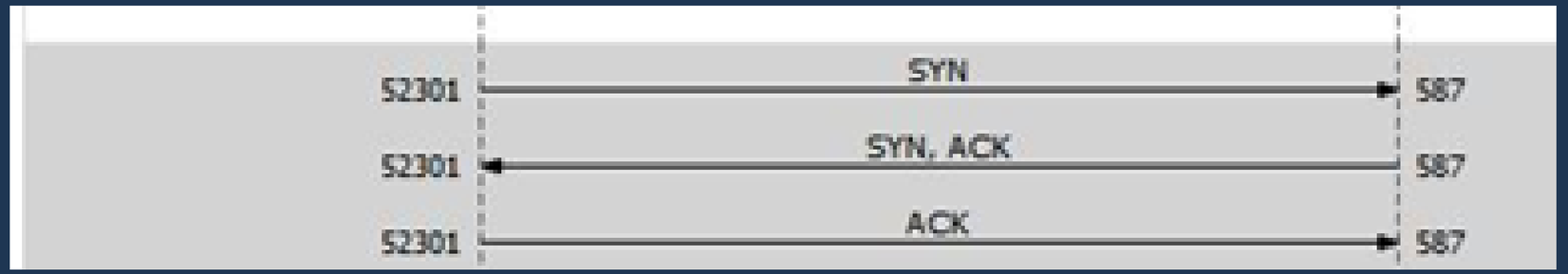
0x0800)

ol Version 4, Src: 173.194.79.108, Dst: 217.105.38.147

ntrol Protocol, Src Port: 587, Dst Port: 52301, Seq: 0, Ack: 1, Len: 0


Telnet smtp.gmail.com
220 smtp.gmail.com ESMTP f18sm633585edt.32 - gsmtp
helo smtp.gmail.com
250 smtp.gmail.com at your service

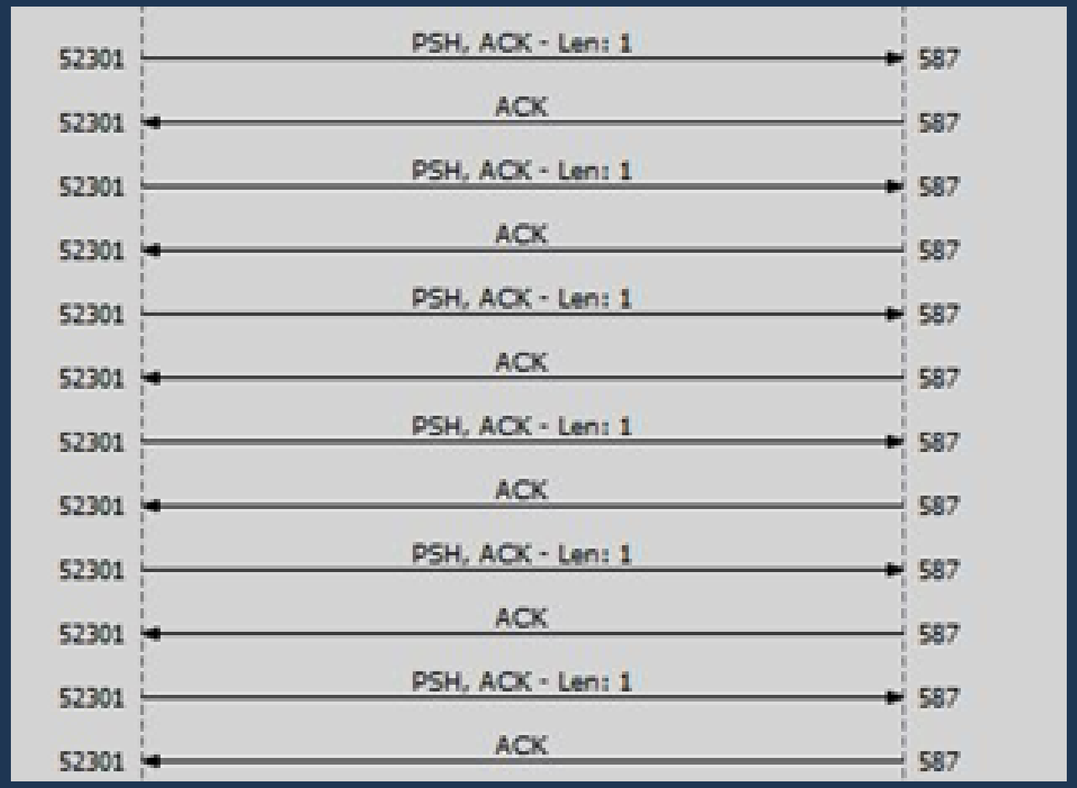
THREE WAY HANDSHAKE: THE ESSENTIAL FEATURE OF TCP!

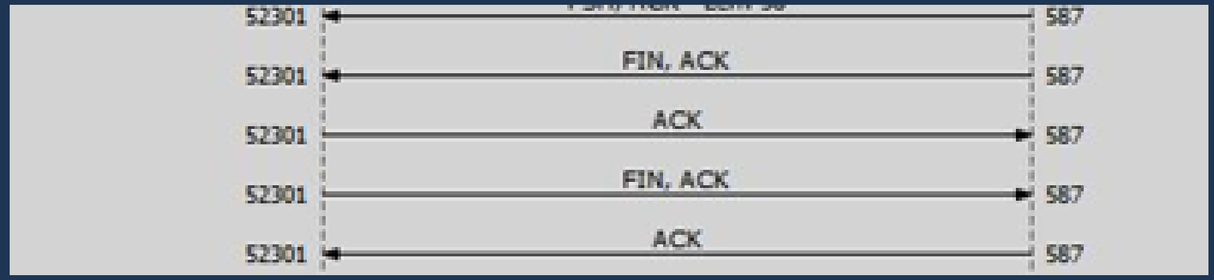


Seq = 0

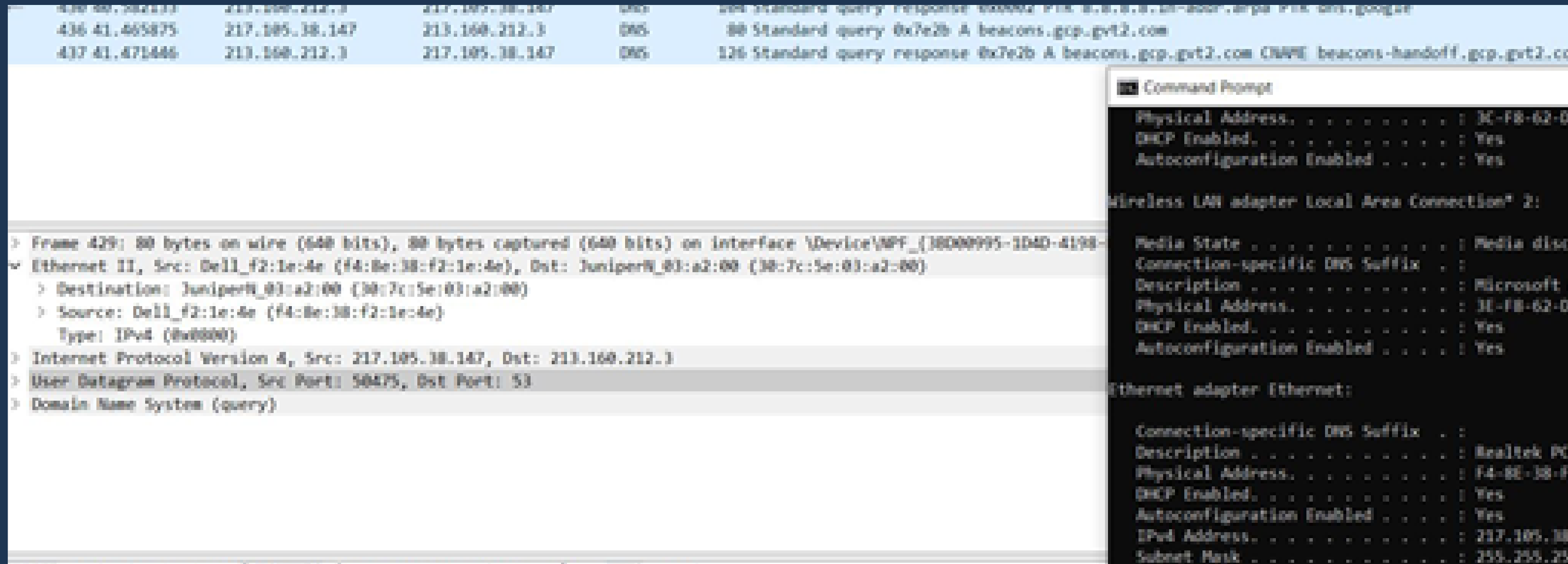
Seq = 0 Ack = 1

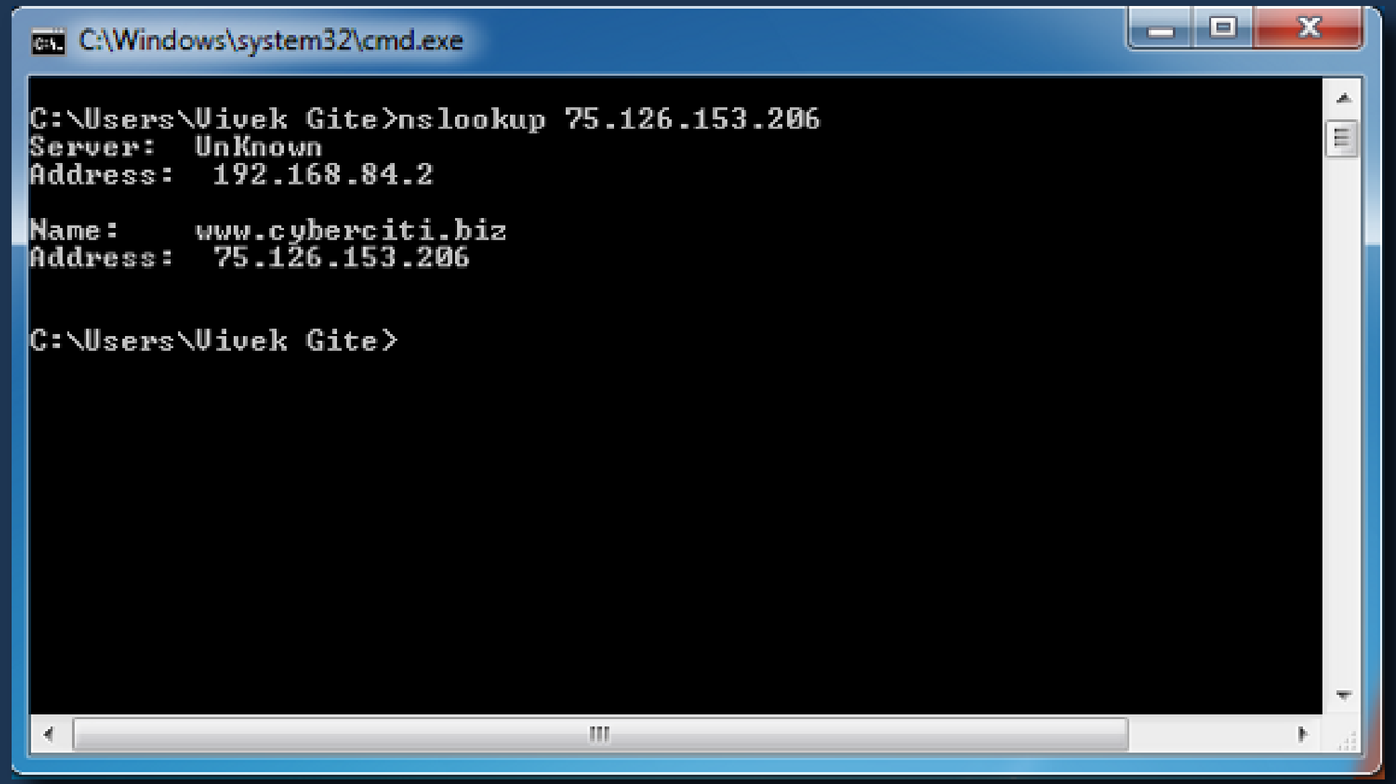
Seq = 1 Ack = 1


52301
587
PSH, ACK - Len: 1
ACK
PSH, ACK - Len: 1
ACK
PSH, ACK - Len: 1
ACK
PSH, ACK - Len: 1
ACK
PSH, ACK - Len: 1
ACK
PSH, ACK - Len: 1
ACK


52301
587
FIN, ACK
ACK
FIN, ACK
ACK

UDP SCENARIO 1: REVERSE DNS LOOKUP





source:
https://www.cyberciti.biz/media/new/faq/2010/12/windows-nslookup-reverse-lookup.png

UDP SCENARIO 2: DHCP IP ADDRESS RENEWAL

udp.port == 68

No.	Time	Source	Destination	Protocol	Length	Info
31	8.065626	217.105.38.147	213.124.208.3	DHCP	358	DHCP Request - Transaction ID 0xd19a5640
32	8.128564	213.124.208.3	217.105.38.147	DHCP	342	DHCP ACK - Transaction ID 0xd19a5640
33	8.129994	213.124.208.3	217.105.38.147	DHCP	342	DHCP ACK - Transaction ID 0xd19a5640

```
> Frame 31: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{3BD0099
v Ethernet II, Src: Dell_f2:1e:4e (f4:8e:38:f2:1e:4e), Dst: JuniperN_03:a2:00 (30:7c:5e:03:a2:00)
  > Destination: JuniperN_03:a2:00 (30:7c:5e:03:a2:00)
  > Source: Dell_f2:1e:4e (f4:8e:38:f2:1e:4e)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 217.105.38.147, Dst: 213.124.208.3
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)
```

```
0000  30 7c 5e 03 a2 00 f4 8e  38 f2 1e 4e 08 00 45 00   0|^·····  8··N··E·
0010  01 58 50 61 00 00 80 11  43 b7 d9 69 26 93 d5 7c   ·XPa····  C··i&··|
```

Command Prompt

```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual
   Physical Address. . . . . . . . . : 3E-F8-62-D9-C5-7E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Control
   Physical Address. . . . . . . . . : F4-8E-38-F2-1E-4E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 217.105.38.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.192
   Lease Obtained. . . . . . . . . . : 15 November 2020 18:18:53
   Lease Expires . . . . . . . . . . : 15 November 2020 21:56:21
   Default Gateway . . . . . . . . . : 217.105.38.129
   DHCP Server . . . . . . . . . . . : 213.124.208.3
   DNS Servers . . . . . . . . . . . : 213.160.212.3
                                       213.160.223.35
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

CHALLENGES

Computer networks are more complicated than what we usually think!

But we incidentally managed to overcome hard problems by using the internet itself!

Week 8 challenge is in applying binary AND operations to yield the routing number.
Week 9 challenge is in configuring the routes based on our network flow diagram and understanding route tables.
Week 10 challenge is in figuring out the uses of TCP and UDP in our daily networking operations.

THANK YOU!

Any questions?