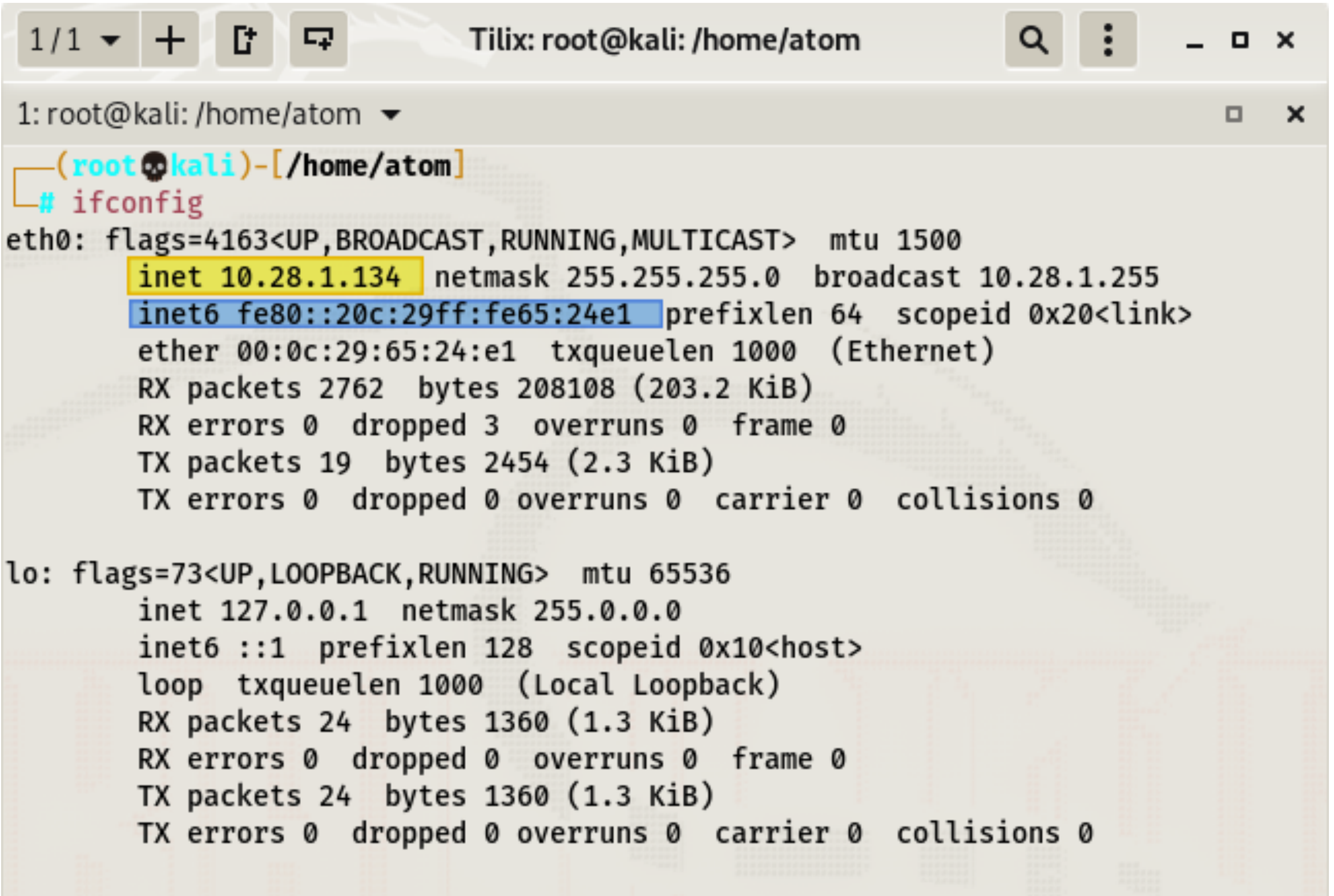
NETWORKING INTRODUCTION

Tuesday, July 20, 2021 7:19 PM

1. IP ADDRESSES-

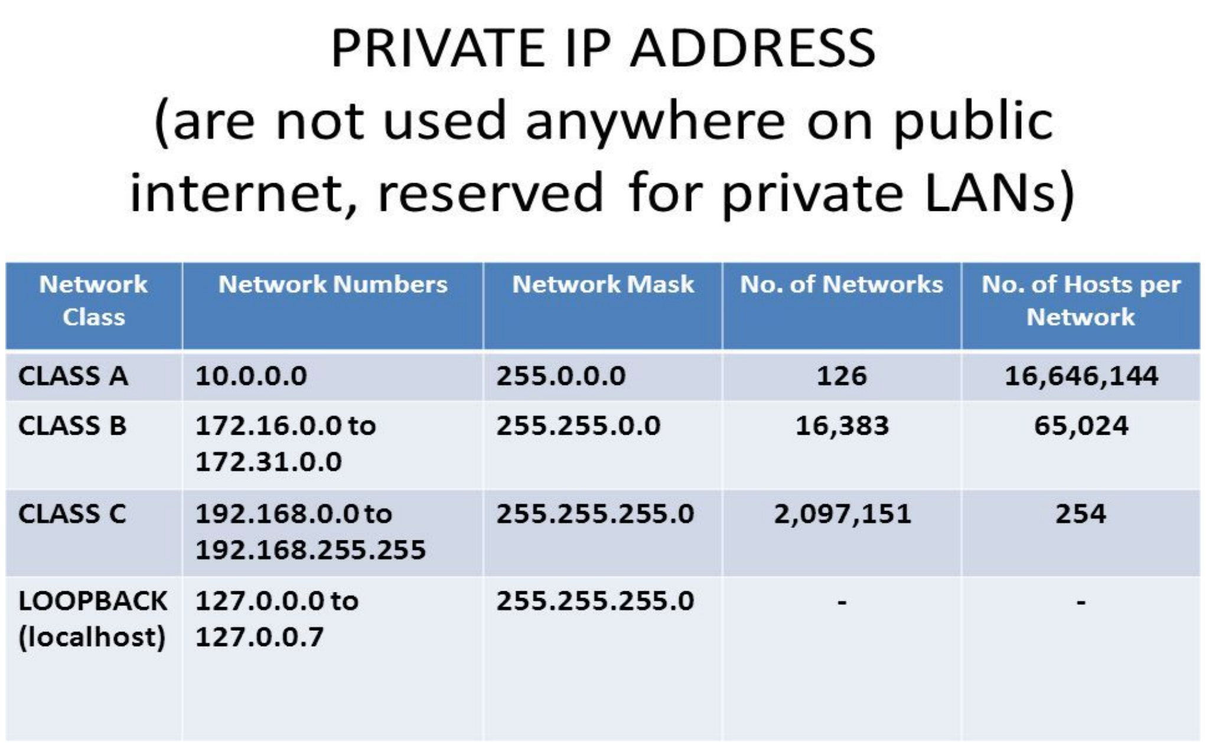
- ifconfig
    - ipv4 (32bits -> 4bytes) YELLOW
        - 128 64 32 16 8 4 2 1 -> 255
        - 0 0 0 0 1 1 1 1 -> 7. 7. 7. 7
        - MY IP- 10.28.1.134 (CLASS A) {BIG OFFICES AND BUSSINESSES}
        - Possible amount of IP Addresses(ipv4) -> 2^{32}
        - Possible amount of IP Addresses(ipv6) -> 2^{128}



```
┌──(root💀kali)-[/home/atom]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.28.1.134  netmask 255.255.255.0  broadcast 10.28.1.255
        inet6 fe80::20c:29ff:fe65:24e1  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:65:24:e1  txqueuelen 1000  (Ethernet)
        RX packets 2762  bytes 208108 (203.2 KiB)
        RX errors 0  dropped 3  overruns 0  frame 0
        TX packets 19  bytes 2454 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 24  bytes 1360 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1360 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

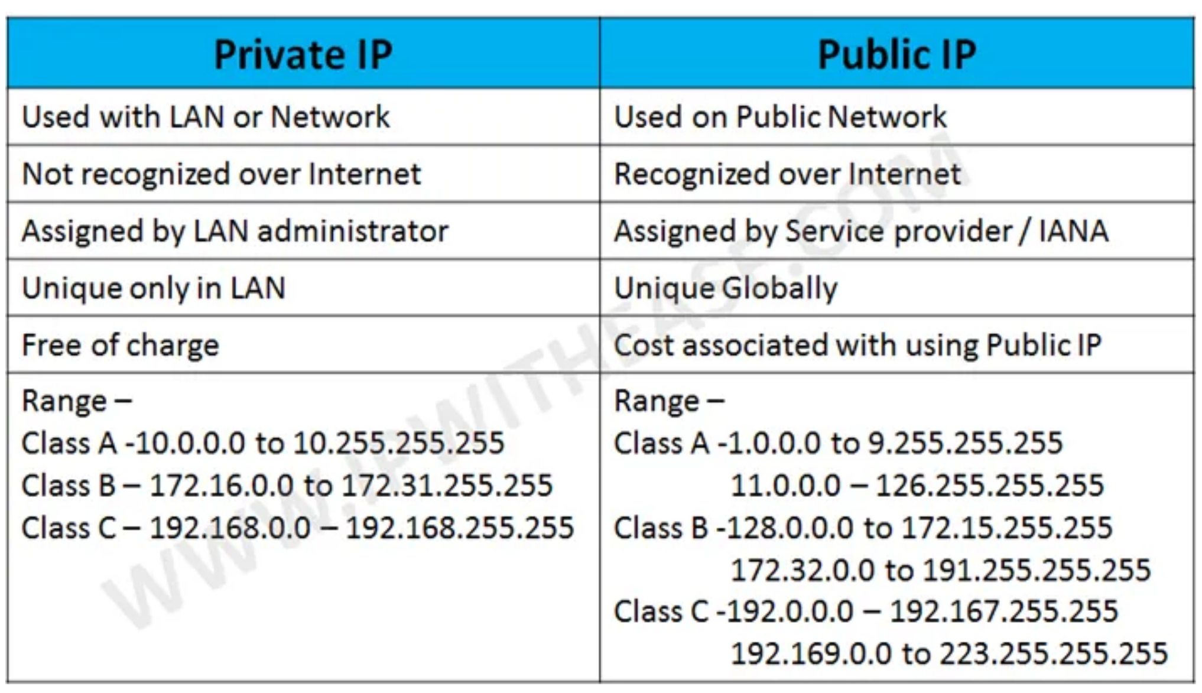
- NAT- [NETWORK ADDRESS TRANSLATION]-
- PUBLIC IP ADDRESSES



PRIVATE IP ADDRESS
(are not used anywhere on public internet, reserved for private LANs)

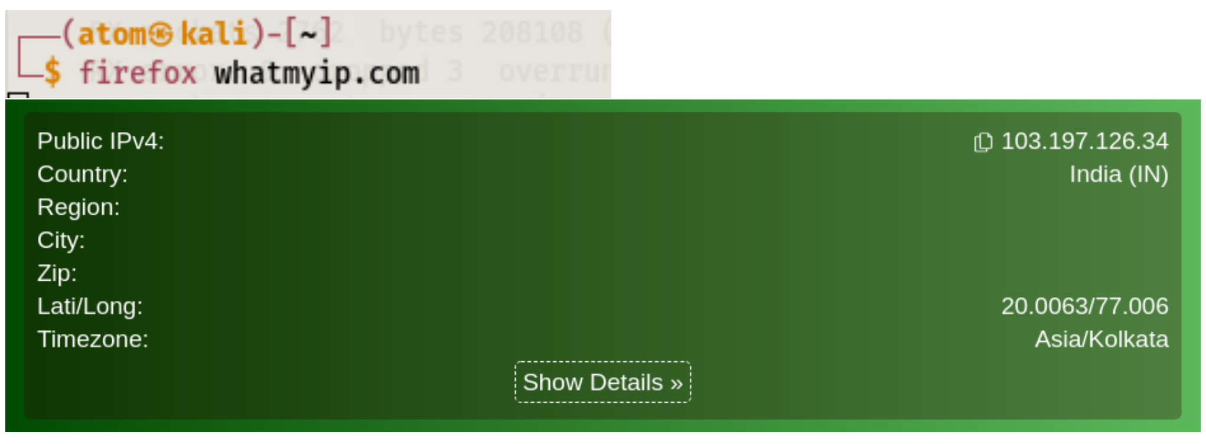
Network Class	Network Numbers	Network Mask	No. of Networks	No. of Hosts per Network
CLASS A	10.0.0.0	255.0.0.0	126	16,646,144
CLASS B	172.16.0.0 to 172.31.0.0	255.255.0.0	16,383	65,024
CLASS C	192.168.0.0 to 192.168.255.255	255.255.255.0	2,097,151	254
LOOPBACK (localhost)	127.0.0.0 to 127.0.0.7	255.255.255.0	-	-

- PUBLIC IP ADDRESSES



Private IP	Public IP
Used with LAN or Network	Used on Public Network
Not recognized over Internet	Recognized over Internet
Assigned by LAN administrator	Assigned by Service provider / IANA
Unique only in LAN	Unique Globally
Free of charge	Cost associated with using Public IP
Range – Class A -10.0.0.0 to 10.255.255.255 Class B – 172.16.0.0 to 172.31.255.255 Class C – 192.168.0.0 – 192.168.255.255	Range – Class A -1.0.0.0 to 9.255.255.255 11.0.0.0 – 126.255.255.255 Class B -128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255 Class C -192.0.0.0 – 192.167.255.255 192.169.0.0 to 223.255.255.255

- MY Public IP Address-

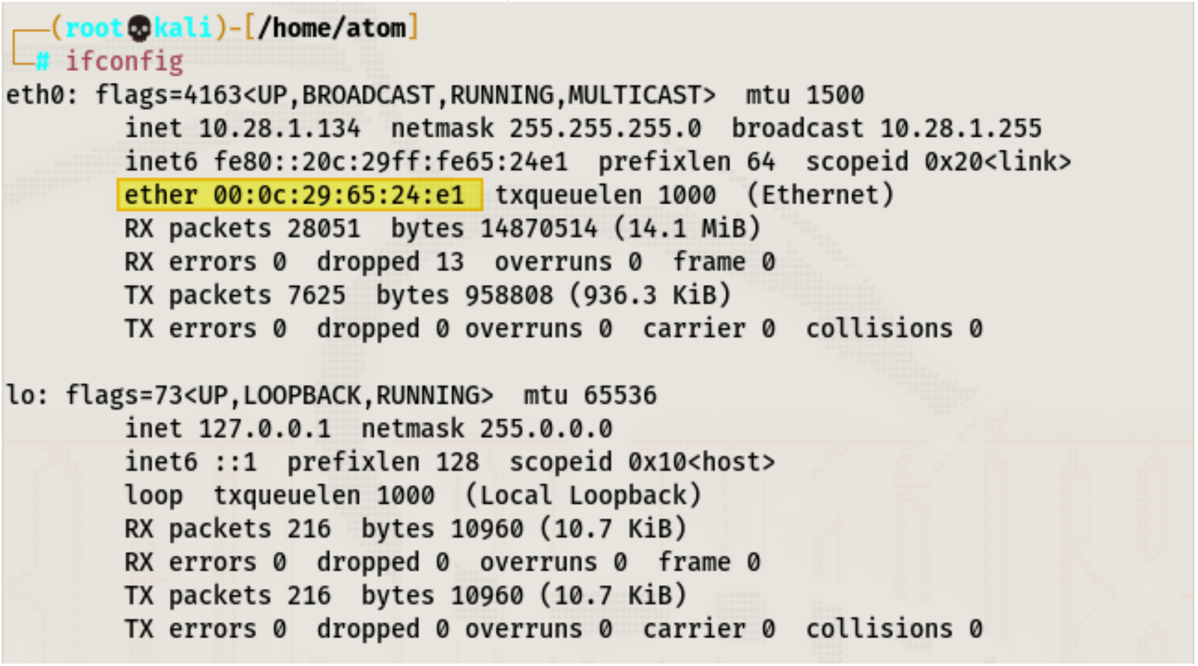


```
┌──(atom㉿kali)-[~]
└─$ firefox whatmyip.com
```

Public IPv4: 103.197.126.34
Country: India (IN)
Region:
City:
Zip:
Lati/Long: 20.0063/77.006
Timezone: Asia/Kolkata

2. MAC ADDRESS-

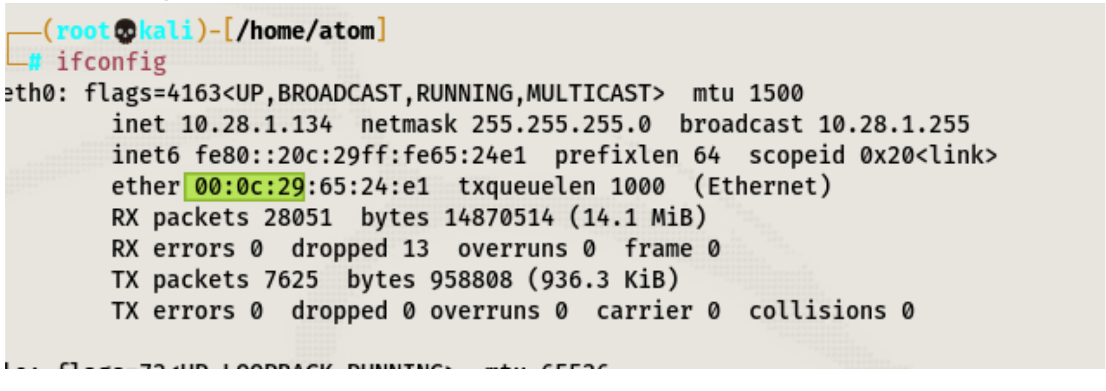
- SWITCHES
    - Mac addresses are used by switches to identify the specific devices over the network
        - Permanent Addresses - (YELLOW)



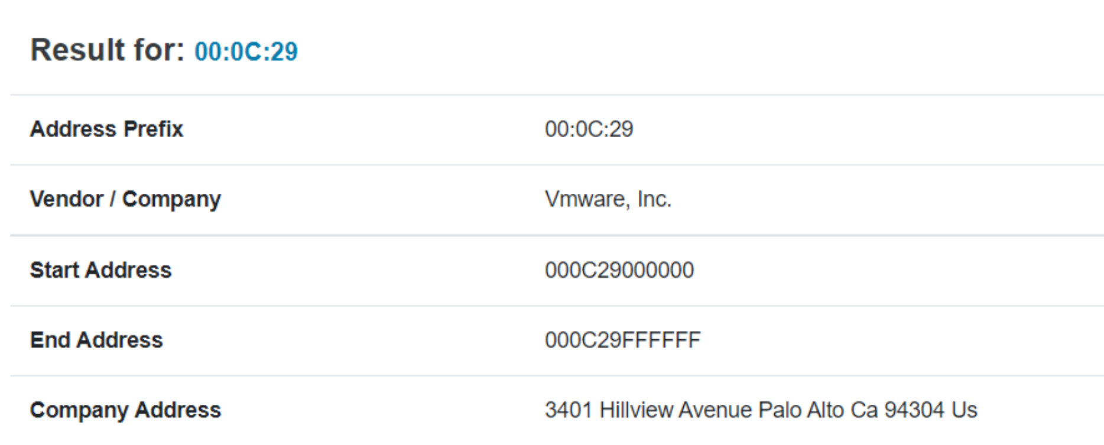
```
┌──(root💀kali)-[/home/atom]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.28.1.134  netmask 255.255.255.0  broadcast 10.28.1.255
        inet6 fe80::20c:29ff:fe65:24e1  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:65:24:e1  txqueuelen 1000  (Ethernet)
        RX packets 28051  bytes 14870514 (14.1 MiB)
        RX errors 0  dropped 13  overruns 0  frame 0
        TX packets 7625  bytes 958808 (936.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 216  bytes 10960 (10.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 216  bytes 10960 (10.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- (ADDRESS PREFIX) Identifiers-
    - The first three pairs of the MAC Address



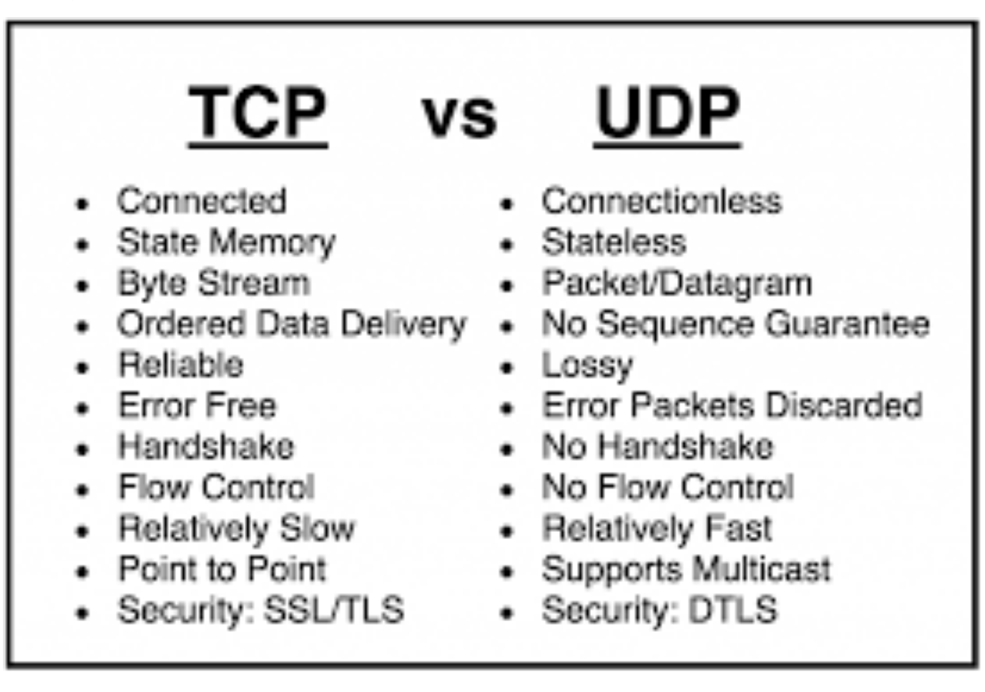
```
┌──(root💀kali)-[/home/atom]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.28.1.134  netmask 255.255.255.0  broadcast 10.28.1.255
        inet6 fe80::20c:29ff:fe65:24e1  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:65:24:e1  txqueuelen 1000  (Ethernet)
        RX packets 28051  bytes 14870514 (14.1 MiB)
        RX errors 0  dropped 13  overruns 0  frame 0
        TX packets 7625  bytes 958808 (936.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



Result for: 00:0C:29

Address Prefix	00:0C:29
Vendor / Company	Vmware, Inc.
Start Address	000C29000000
End Address	000C29FFFFFF
Company Address	3401 Hillview Avenue Palo Alto Ca 94304 Us

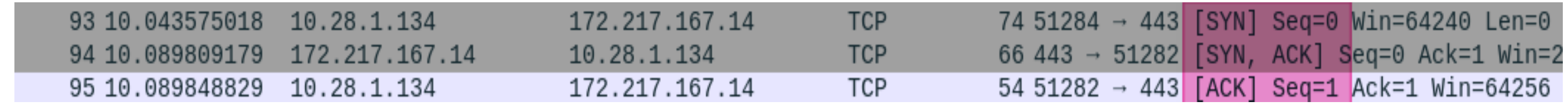
3. TCP & UDP-



TCP vs UDP

TCP	UDP
Connected	Connectionless
State Memory	Stateless
Byte Stream	Packet/Datagram
Ordered Data Delivery	No Sequence Guarantee
Reliable	Lossy
Error Free	Error Packets Discarded
Handshake	No Handshake
Flow Control	No Flow Control
Relatively Slow	Relatively Fast
Point to Point	Supports Multicast
Security: SSL/TLS	Security: DTLS

- TCP
    - [Transmission Control Protocol]
        - Connection oriented protocol
            - THREE WAY HANDSHAKE- {port are for connection}
                - [SYN] > [SYN ACK] > [ACK]



```
93 10.043575018  10.28.1.134      172.217.167.14   TCP   74 51284 → 443 [SYN] Seq=0 Win=64240 Len=0
94 10.089809179  172.217.167.14   10.28.1.134      TCP   66 443 → 51282 [SYN, ACK] Seq=0 Ack=1 Win=2
95 10.089848829  10.28.1.134      172.217.167.14   TCP   54 51282 → 443 [ACK] Seq=1 Ack=1 Win=64256
```

- Website{http, https}, SSH, FTP

- UDP
    - [User Datagram Protocol]
        - Connectionless protocol
            - Streaming service, DNS, Voice over IP

4. COMMON PORTS AND PROTOCOLS-

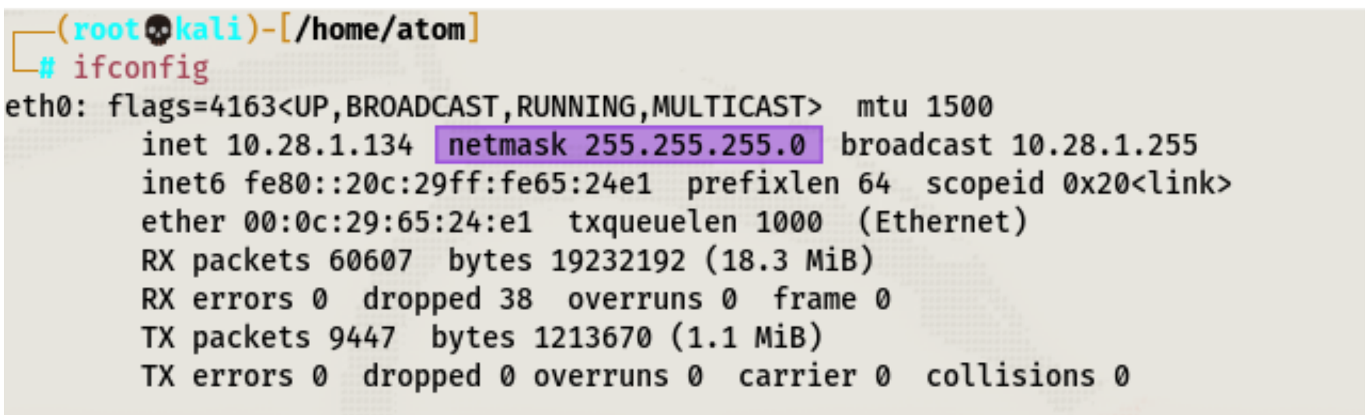
TCP	UDP
FTP (21)	DNS (53)
SSH (22)	DHCP (67, 68)
Telnet (23)	TFTP (69)
SMTP (25)	SNMP (161)
DNS (53)	
HTTP (80) / HTTP (443)	
POP3 (110)	
SMB (139 + 445)	
IMAP (143)	

5. THE OSI MODEL-

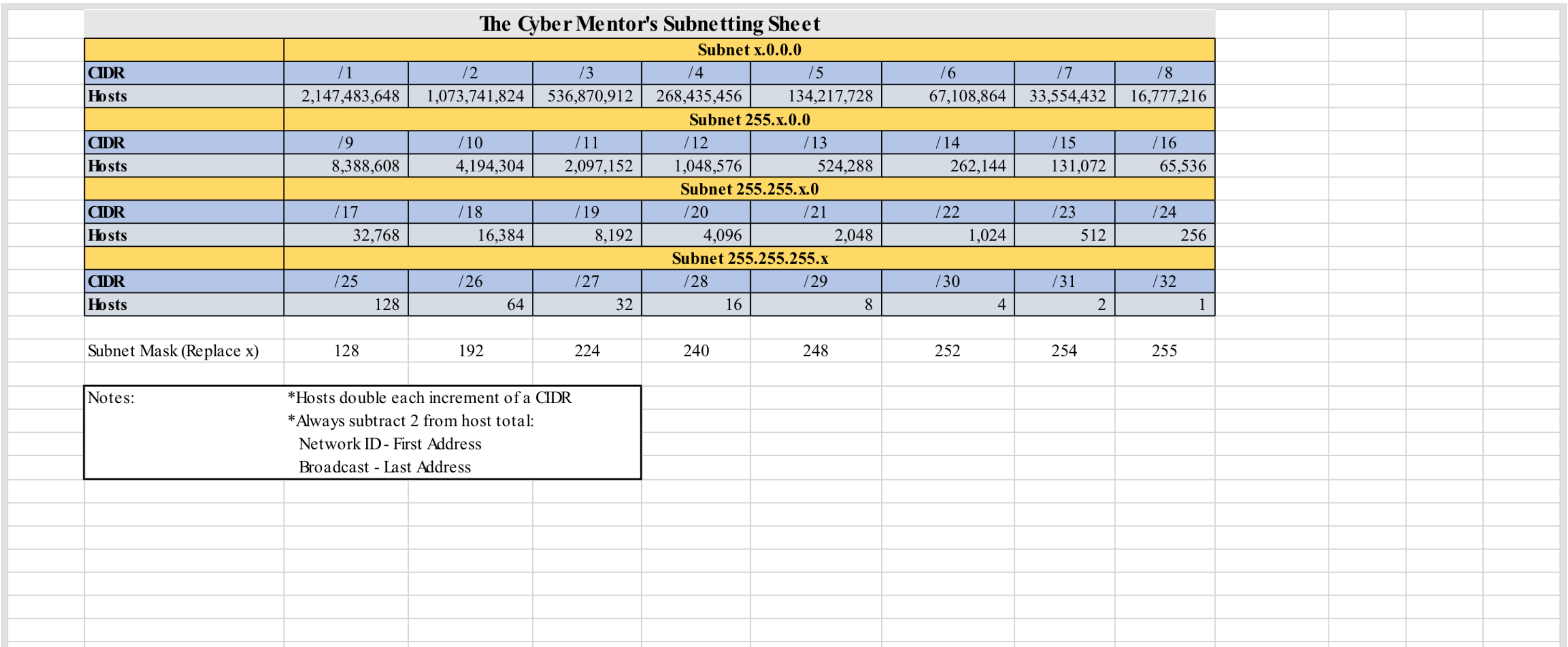
1. P (PHYSICAL LAYER) - Data Cable, Cat6 [LAYER 1] -> PLEASE
2. D (DATA) - Switching, Mac Addresses [LAYER 2] -> DO
3. N (NETWORK) - IP Addresses, Routing [LAYER 3] -> NOT
4. T (TRANSPORT) - TCP, UPD [LAYER 4] -> THROW
5. S (SESSEION) - Session, Management [LAYER 5] -> SOUSAGE,
6. P (Presentation) - WMV, JPEG, MOV [LAYER 6] -> PIZZA
7. A (APPLICATION) -HTTP, SMTP [LAYER 7] -> AWAY.

6. SUBNETTING-

- Netmask , subnet mask, subnet (PURPLE)
- {8bit}:{8bit}:{8bit}:{8bit}
- 128:64:32:16:8:2:1



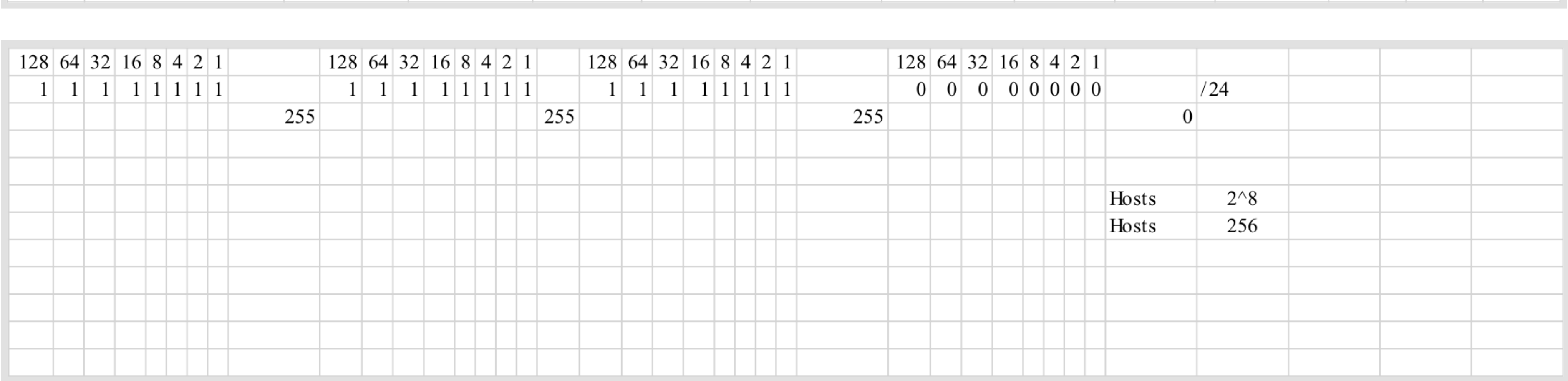
```
┌──(root💀kali)-[/home/atom]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.28.1.134  netmask 255.255.255.0  broadcast 10.28.1.255
        inet6 fe80::20c:29ff:fe65:24e1  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:65:24:e1  txqueuelen 1000  (Ethernet)
        RX packets 60607  bytes 19232192 (18.3 MiB)
        RX errors 0  dropped 38  overruns 0  frame 0
        TX packets 9447  bytes 1213670 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



The Cyber Mentor's Subnetting Sheet

	Subnet x.0.0.0							
CIDR	/1	/2	/3	/4	/5	/6	/7	/8
Hosts	2,147,483,648	1,073,741,824	536,870,912	268,435,456	134,217,728	67,108,864	33,554,432	16,777,216
	Subnet 255.x.0.0							
CIDR	/9	/10	/11	/12	/13	/14	/15	/16
Hosts	8,388,608	4,194,304	2,097,152	1,048,576	524,288	262,144	131,072	65,536
	Subnet 255.255.x.0							
CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Hosts	32,768	16,384	8,192	4,096	2,048	1,024	512	256
	Subnet 255.255.255.x							
CIDR	/25	/26	/27	/28	/29	/30	/31	/32
Hosts	128	64	32	16	8	4	2	1
Subnet Mask (Replace x)	128	192	224	240	248	252	254	255

Notes:
*Hosts double each increment of a CIDR
*Always subtract 2 from host total:
Network ID - First Address
Broadcast - Last Address



128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1		
1	1	1	1	1	1	1	1		1	1	1	1	1	1	1	1		1	1	1	1	1	1	1	1		0	0	0	0	0	0	0	0		/24
								255									255									255									0	
																																			Hosts	2^8
																																			Hosts	256

IP	SUBNET	HOSTS	NETWORK	BROADCAST
192.168.1.0/24	255.255.255.0	254	192.168.1.0	192.168.1.255
192.168.1.0/28	255.255.255.240	14	192.168.1.0	192.168.1.15
192.168.1.16/28	255.255.255.240	14	192.168.1.16	192.168.1.31
192.168.0.0/23	255.255.254.0	510	192.168.0.0	192.168.1.255
192.168.2.0/23	255.255.254.0	510	192.168.2.0	192.168.3.255
192.168.0.0/22	255.255.252.0	1022	192.168.0.0	192.168.3.255
192.168.1.0/26	255.255.255.192	62	192.168.1.0	192.168.1.63
192.168.1.0/27	255.255.255.222	30	192.168.1.0	192.168.1.31

Need Help -> CIDR to ipv4 convertor- www.ipaddressguide.com/cidr