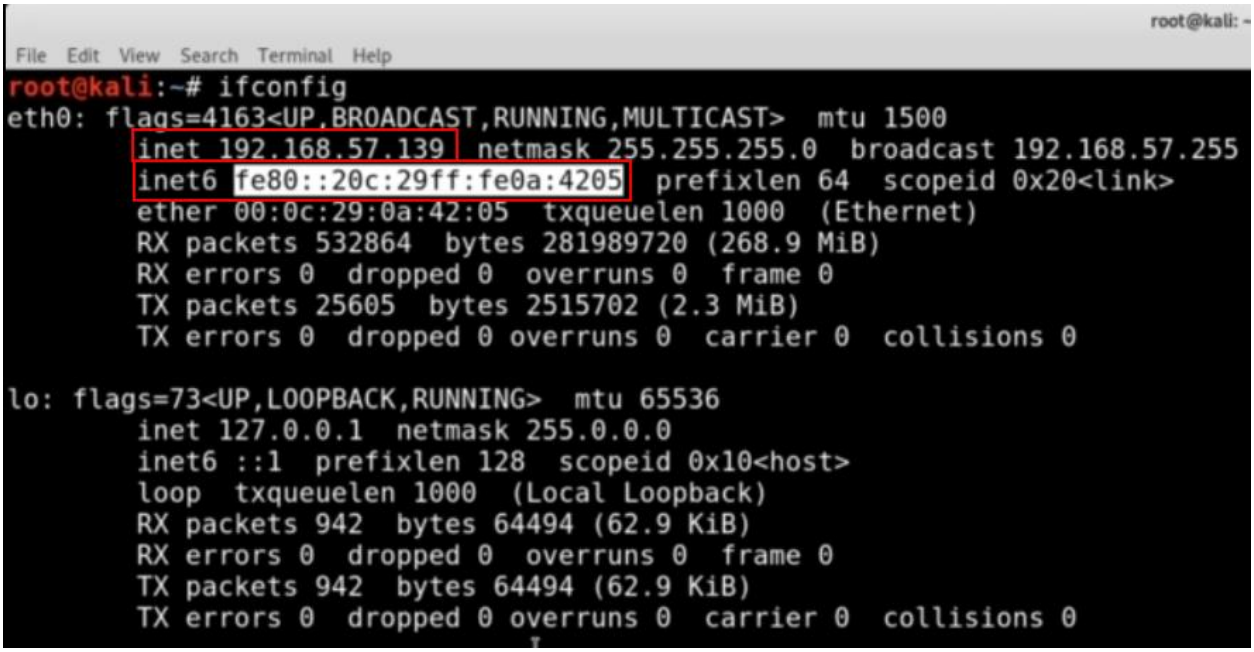
Networking concept.

1. Introduction.

Introduction

- IP Addresses
- MAC Addresses
- TCP, UDP, and the Three-Way Handshake
- Common Ports and Protocols
- The OSI Model
- Subnetting
- Demo Network Build with Cisco Packet Tracer

2. IP Address



IP address:
>> inet address - is decimal address - ipv4
>> inet6 is hexadecimal address - ipv6

IP address - we communicate over layer 3.

192.168.57.139

192 is the first octet. Of 8 bits, we got the range of 8 1's and 0's,

- This all ipv4 bits & it made 32 bits. 8+8+8+8 = 4bytes

This all adds up and it adds them.

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

1 1 1 1 1 1 1 1 = 255

>> There is range of ip company buy in chunks it and sells to ISP and ISP sell to us.

Covers almost 2 ^ 32 = 4,296,967,296 4BILLION range of ip.

However, ipv6 covers hex-dec number

2 ^ 128 = 3.402823669094354565678789879645343 5+38

How we use IPAddress but we are out of address.

We use NAT (**Network Address Translation**)

Like device connected to one network.

- We sign this ip address with this NAT.

PRIVATE IP ADDRESS

192.168.44.104

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

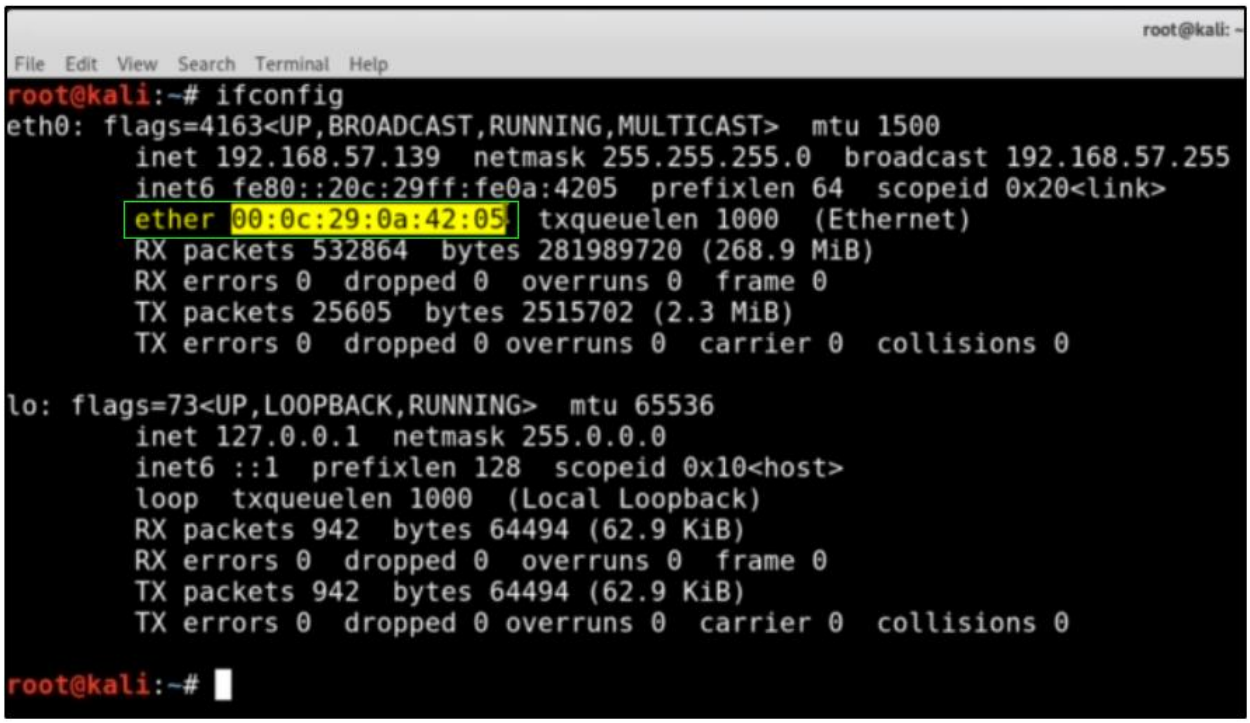
Network Class	Network Numbers	Network Mask	No. of Networks	No. of Hosts per Network
CLASS A	10.0.0.0	255.0.0.0	126	16,646,144
CLASS B	172.16.0.0 to 172.31.0.0	255.255.0.0	16,383	65,024
CLASS C	192.168.0.0 to 192.168.255.255	255.255.255.0	2,097,151	254
LOOPBACK (localhost)	127.0.0.0 to 127.0.0.7	255.255.255.0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

This way we can fix the range ip address usage to our network.

---

3. MAC Addresses - layer 2 Switching

Media access control. It can identify this way. This is the physical address and we can communicate with switches

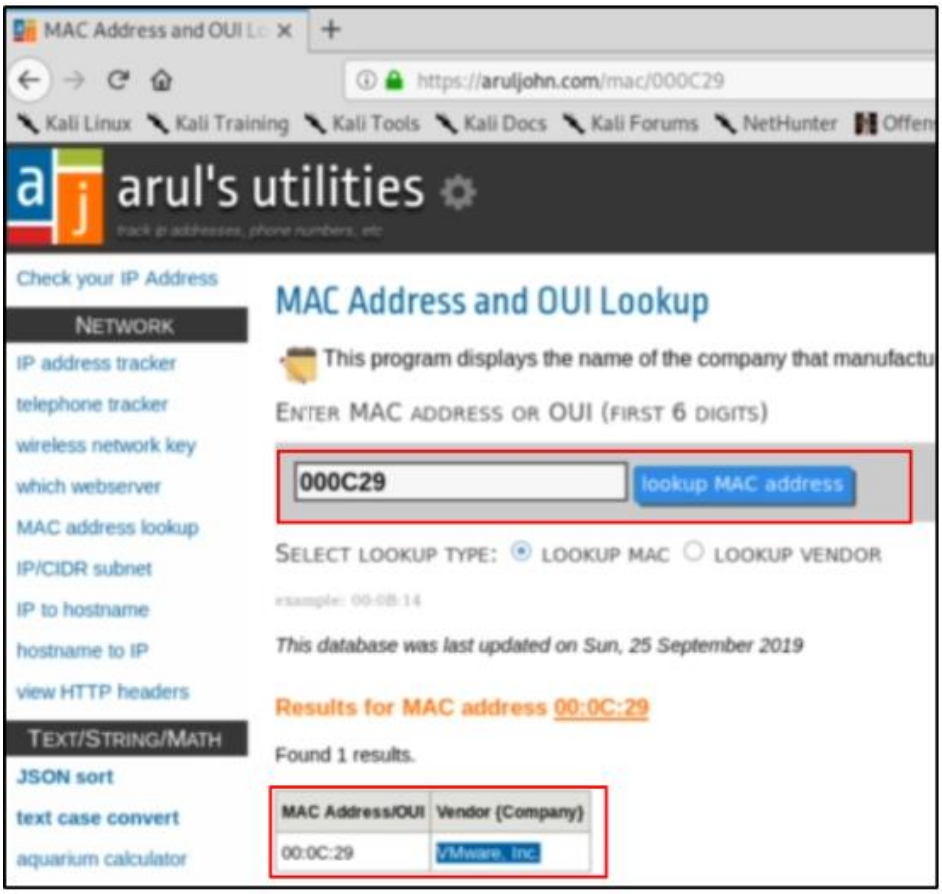


Switch is communicate over this physical address and this is how to get to know which is device has what.

This mac address are useful and use over layer 2 switching. Switches

This mac address have 6 different pairs 2's of identifiers

We can copy the first 3 pairs of address and search google for **mac address lookup**



Therefore, the first 3 pairs are the identifiers

-- Our home network perform both switching and routing so it comes in layer 2/3 device

4. TCP, UDP, and the Three-Way Handshake

Moving to Layer 4 - which is transport layer of OSI Model.

--> What is TCP and UDP?
-- TCP - transmission control protocol - connection oriented protocol
-- if we want to make connection with high reliability - use TCP

Ex - HTTP or HTTPS WEBSITE. SSH, FTP those all utilize TCP

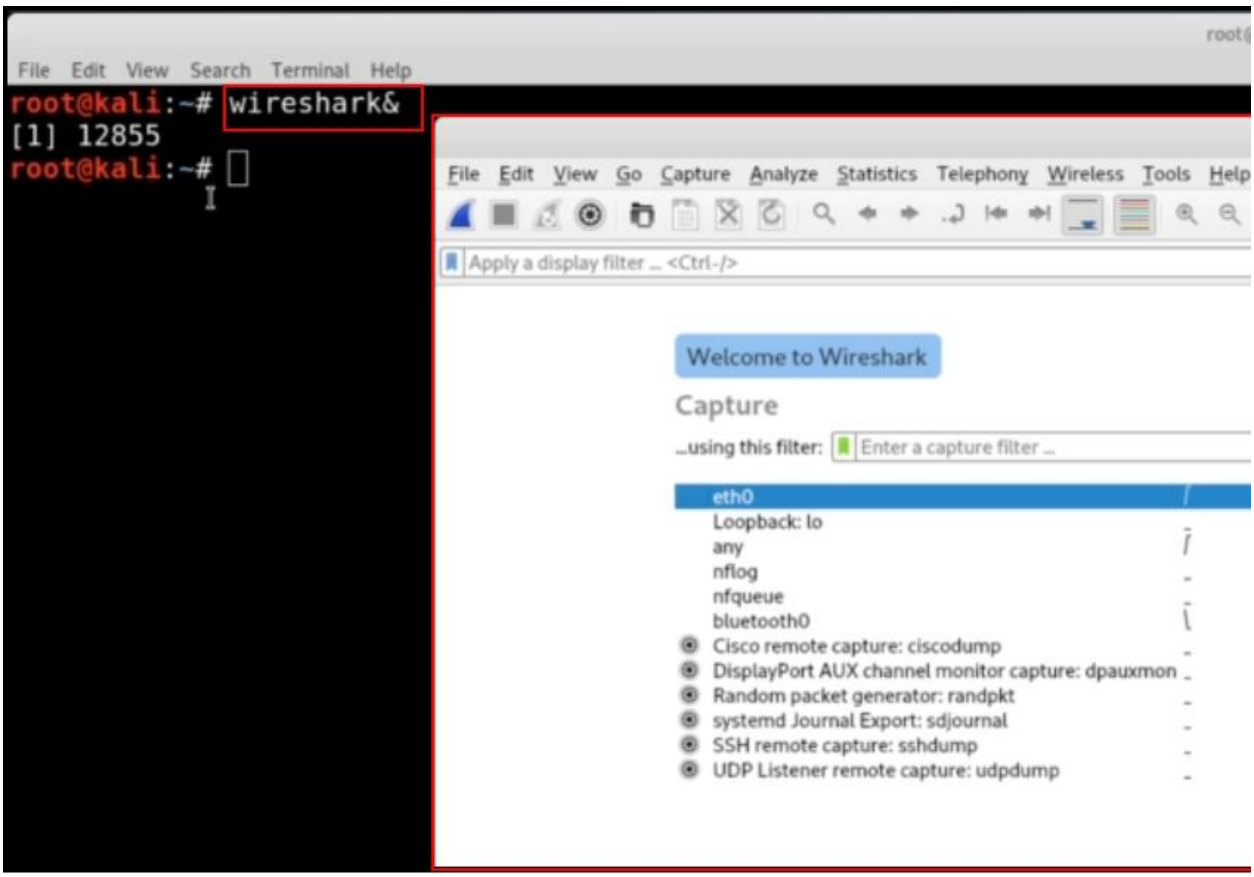
-- UDP - User datagram protocol - connection less protocol
Ex - Streaming service. DNS, VoIP.
-- Commonly used to scan the is TCP,

-- TCP is going to work on 3 way Handshake,

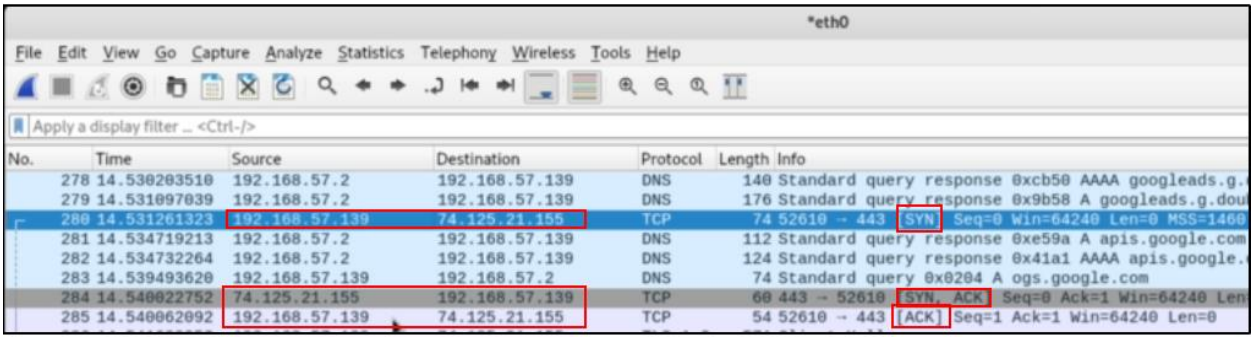
SYN > SYN ACK > ACK, \\ think like an interaction like human talking.

Run Wireshark tool,

>> Wireshark& \\ run this command in Terminal.



>> We can start capture the Wireshark. In addition, see the different packet coming through.



5. Common ports and protocol

Common Ports and Protocols

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

>> FTP (21) - log in to server we can put a file and we can get a file.

>> Telnet (23) - ability to login to machine remotely, identify in clear text & SSH (22) - it is does it but it is encrypted format of that.

>> SMTP (25), POP3 (110), IMAP (143) - all relate to mail.

>> DNS (53) - it resolved IP Address to names.

>> HTTP (80) / HTTPS (443) - it is normally website. Http is not secure and https is encrypted.

>> SMB (139 + 445) - it is originally 139, but it is later windows format is 445. It is file shares. Most recent one is - wanacry virus - also know eternal blue- ms17010. Utilize smb exploit smb over network to navigate through networks, and it is open so frequently on networks.

DHCP (67, 68) - DHCP associates with IP address and opposite is static ip address, so with http when you connect to internet probably running dhcp on backend. It is going to list the ip for some time. Like 8hr, week, or month.

Static ip is give specific ip to computer, when you are try to login to computer with same ip, or single ip called static ip. Most likely mac address

From layer 2 to layer 3 is how to assign it.

TFTP (69) - Trivial File Transfer Protocol - utilize the UDP instead of TCP

SNMP (161) - Simple network management protocol - utilize when strings when used community public strings, we will encounter snmp occasionally on networks, and there may be some information gathered.

6. The OSI Model

Mnemonic - Please Do Not Throw Sausage Pizza Away.

1 - P - PHYSICAL - Data cables, cat6

2 - D - DATALINK - Switching, MAC Addresses

3 - N - NETWORK - IP Addresses, Routing

4 - T - TRANSPORT - TCP, UDP

5 - S - SESSION - Session management

6 - P - PRESENTATION - WMV, JPEG, MOVIE FILES,

7 - A - APPLICATION - HTTP, SMTP

Why it is so important.

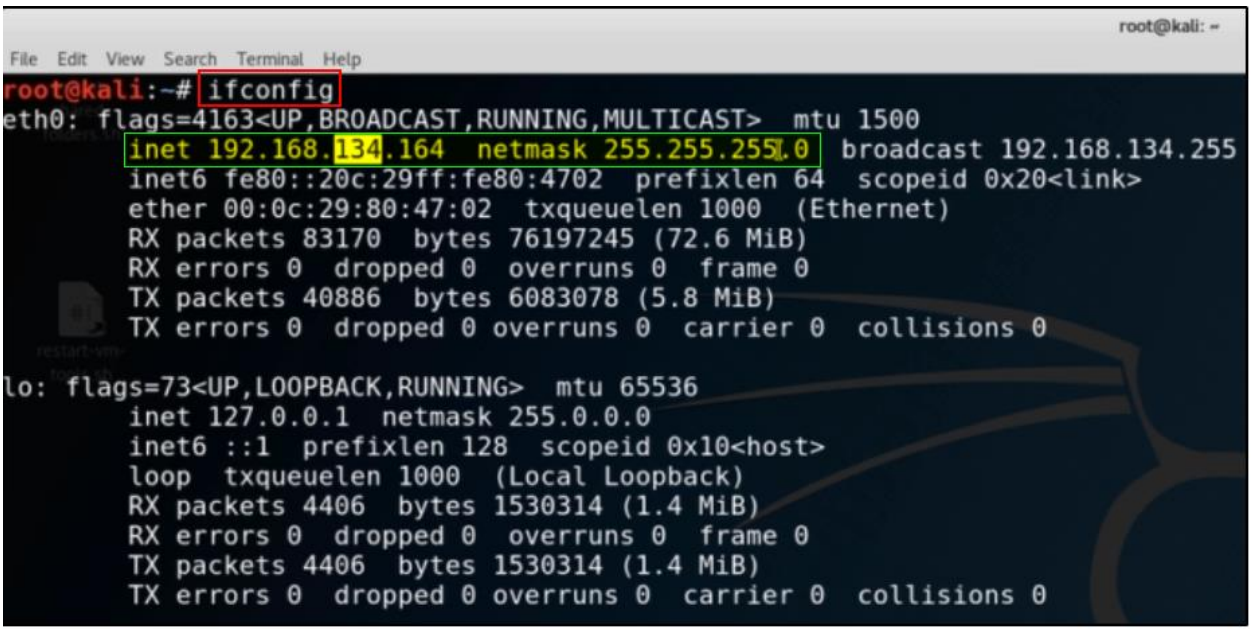
You can say like this - my home router is on 2 - 3 - it does switching and routing.

-- When we receive the data it is coming through = physical layer to application layer

-- When we transmit data is going through = application layer to physical layer,

Troubleshooting this - Starts with Physical to Application layer

7. Sub netting



>> We have IP Address of class c - 192.168.134.164 and subnet mask for class c is - 255.255.255.0

>> If you think in bits- we can see that 8bit.8bit.8bit.0 no bits turned on.

>> So the 24bits are turned on & last 8 bits no turned on.

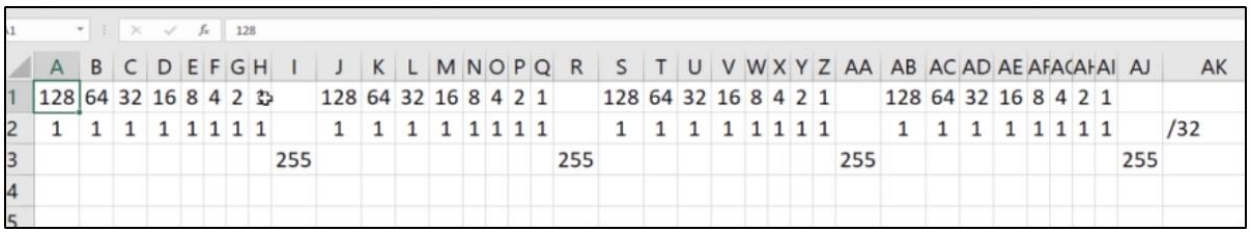
>> When your subnet mask is 255,255,255.0 means it is lockdown up to 255 and 0 is changeable.

>> 0 represent to movement on last octet.

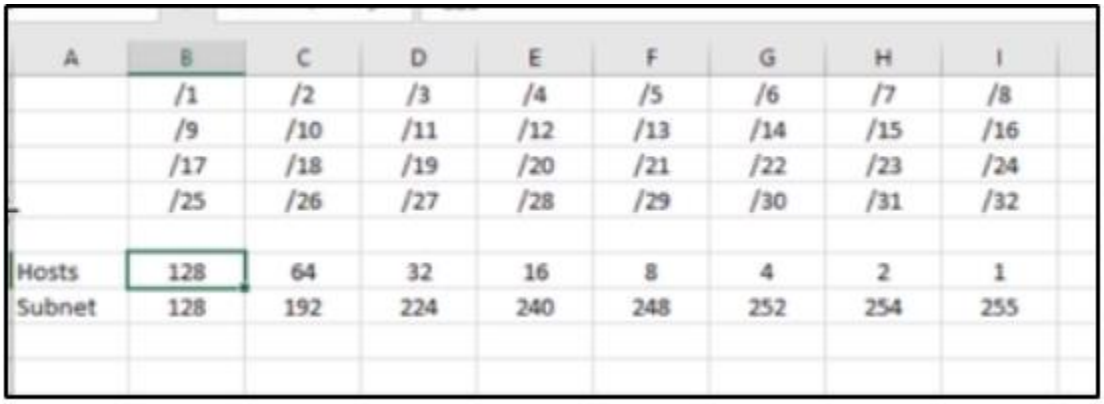
>> We have 256 ip address but 254 host.

>> Your host grows substantially as net mask reduces.

>> So the class 3 have wak24 network. 0/24, class 2 - wak 0/16 network, class 1 - wak 0/8 network.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK
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		128	64	32	16	8	4	2	1		
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	1	1	1	1	1	1		/32
3									255									255									255									255	
4																																					
5																																					



	A	B	C	D	E	F	G	H	I
		/1	/2	/3	/4	/5	/6	/7	/8
		/9	/10	/11	/12	/13	/14	/15	/16
		/17	/18	/19	/20	/21	/22	/23	/24
		/25	/26	/27	/28	/29	/30	/31	/32
	Hosts	128	64	32	16	8	4	2	1
	Subnet	128	192	224	240	248	252	254	255

/1 = 128.0.0.0

/25 = 255.255.255.128

/24 = 255.255.255.0

/9 = 255.128.0.0

/17 = 255.255.128.0

Broadcast - last address

Network id - first address