

Section 7:TCP/IP Basics

37. Introduction to IP Addressing and Binary

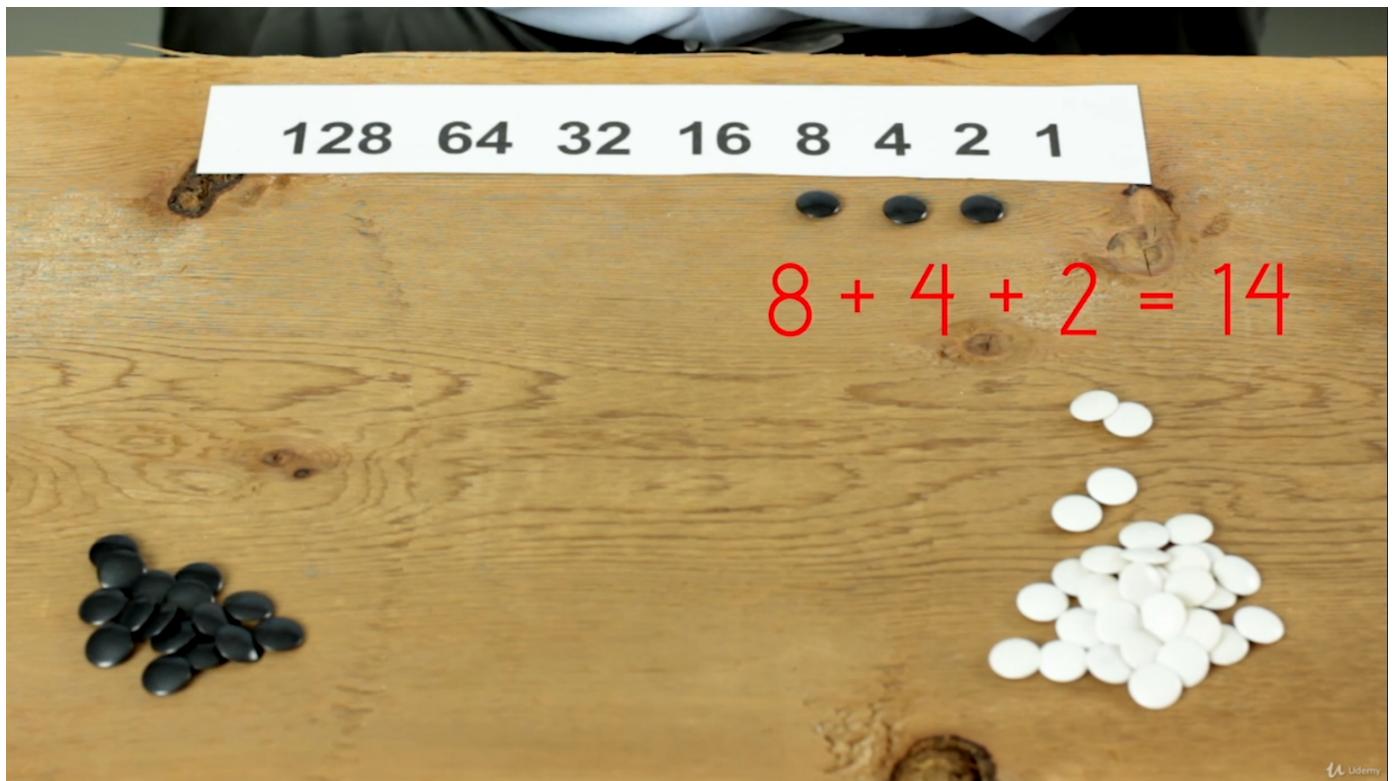
Dotted Decimal Notation -> 172.168.20.3

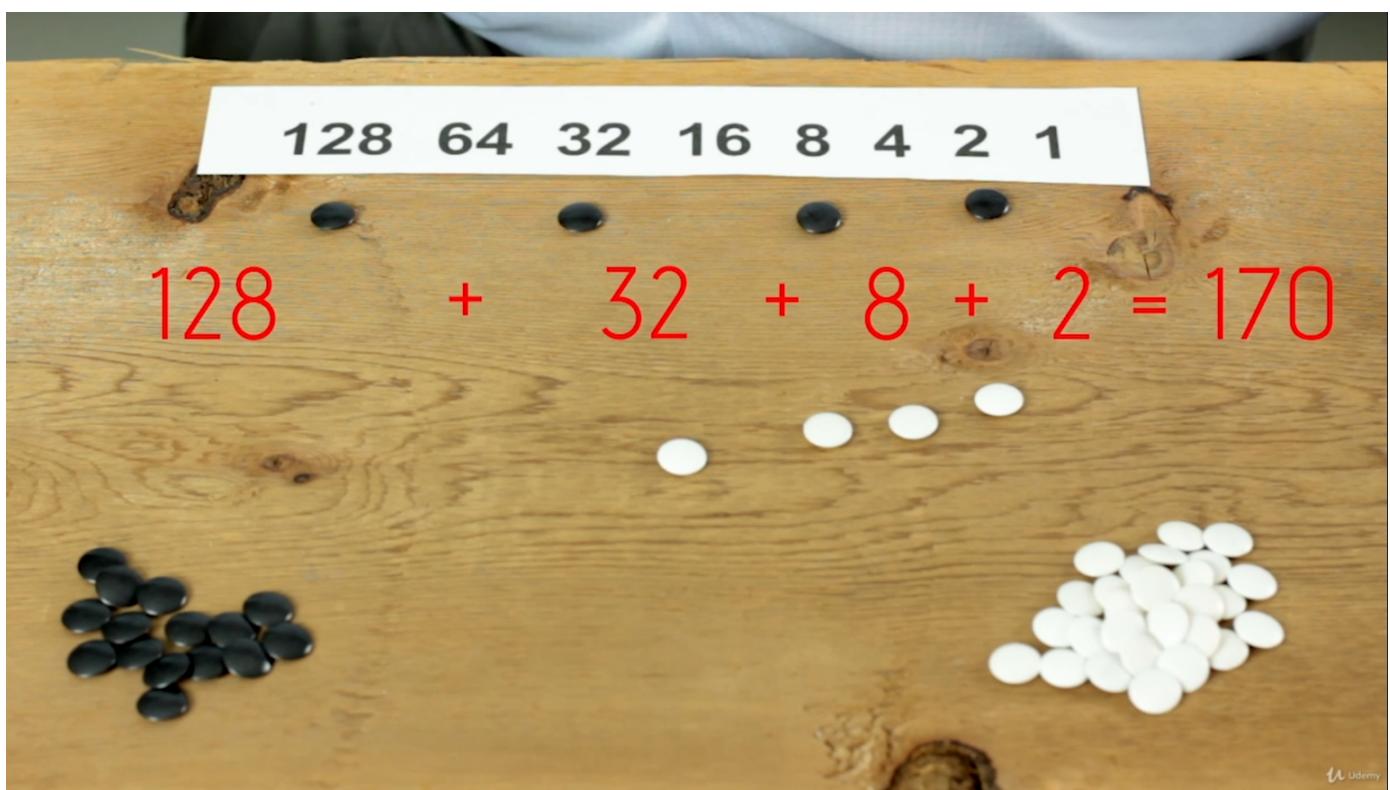
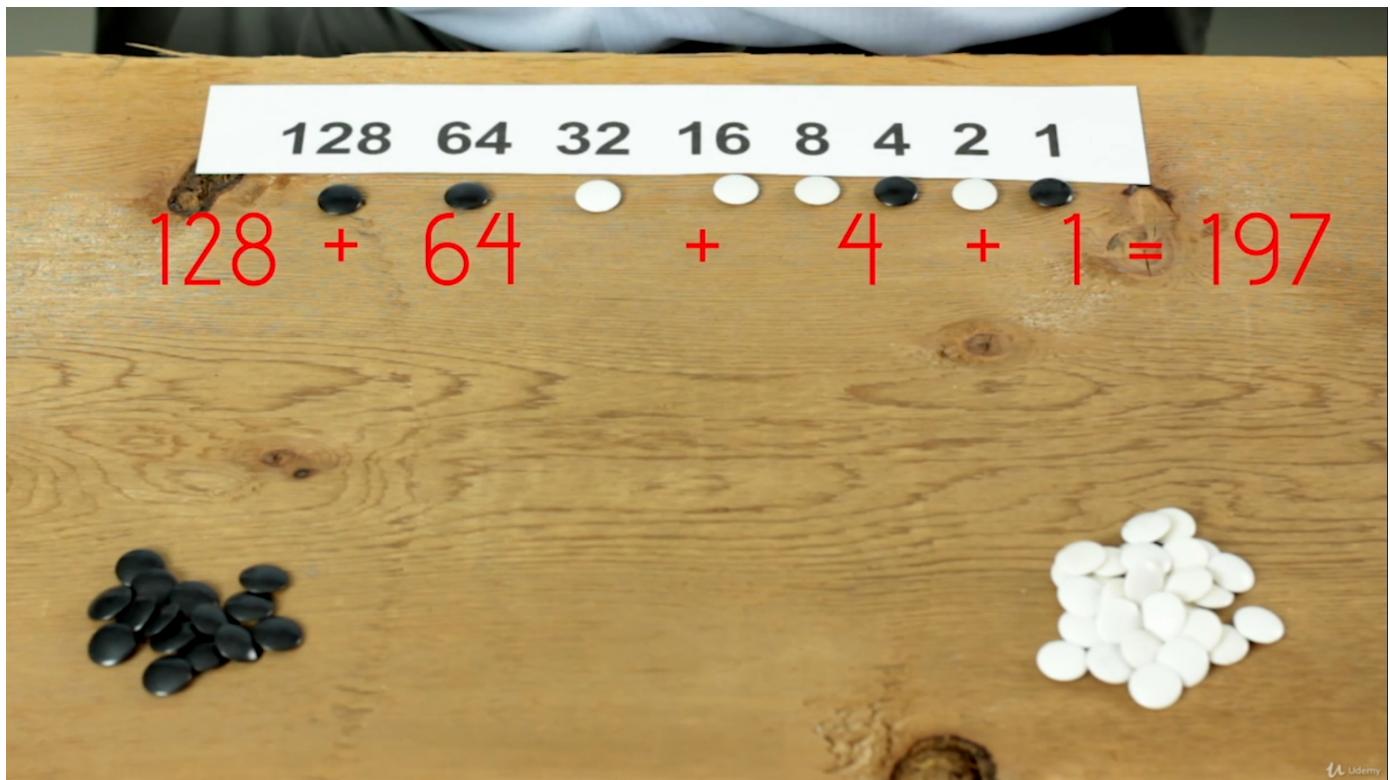
There are exactly 256 combinations of 8 1's and 0's. -> This is "0-255"

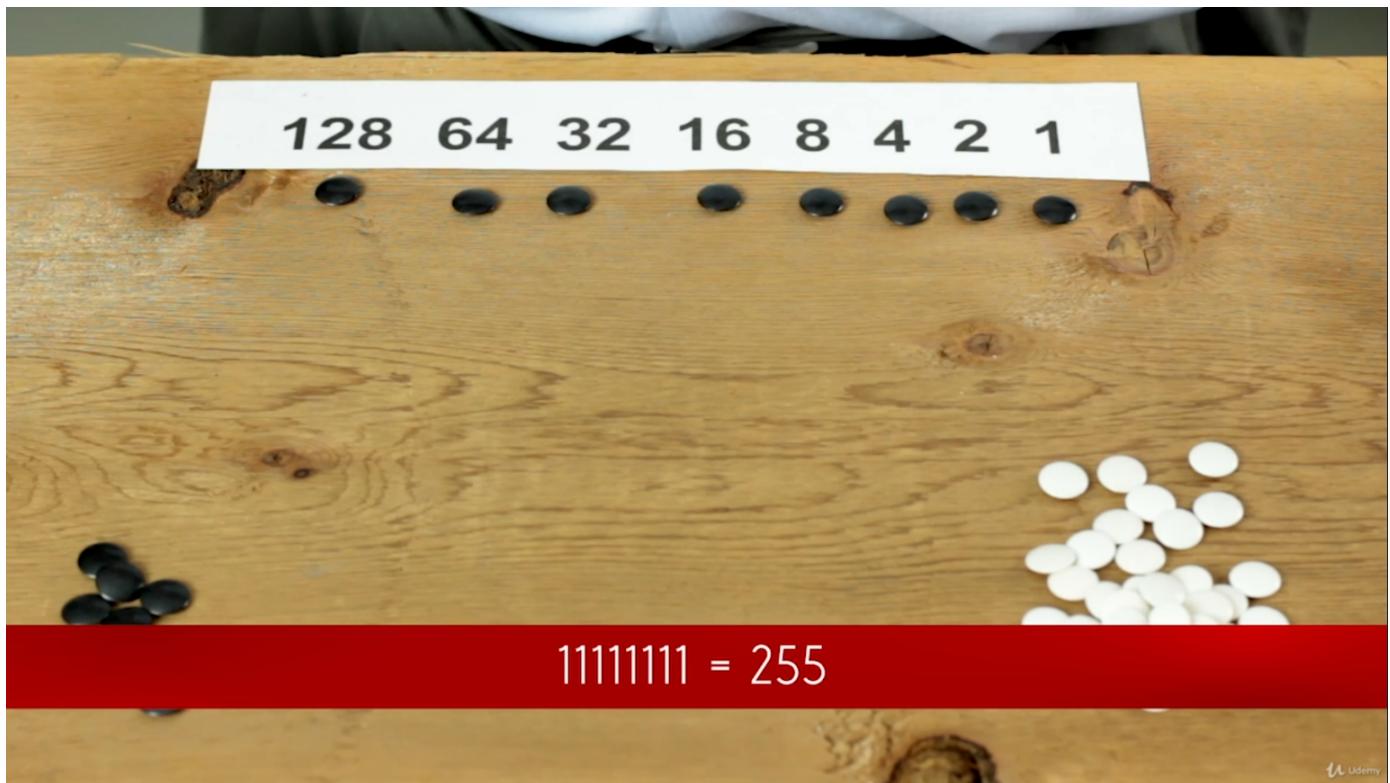
Converting a binary to dotted Decimal notation octet by adding each number that has a 1. Blacks are 1, White is zero

REMEMEBER "128"

Examples:







Udemy

Reversing by taking dotted decimal notation octet and converting to binary:

Using 171: how many 128's are in 171 (1) with a remainder of 43, 64 is larger than 43 (0). how many 32 are in 43 (1) remainder of 11, how many 16's are in 11 (0), how many 8's in 11 (1), how many 4's are in 3 (0), how many twos in 3 (1), how many 1's in 1's is (1)



Udemy

ARP(Address Resolution Protocol) -> ARP resolves MAC addresses from IP Addresses

ARPing is sending out a broadcast asking who has the sought after IP, but only one computer is going to respond and say "it's me" and send its MAC Address.

Know for NET+ - If you want to see your ARP cache you have to use the "arp -a" command

39. Classful Addressing

Every computer has to have a unique IP address.

IANA-(Internet Assigned Numbers Authority)

IANA does not pass out IPs to people. They Pass them out to the RIR (Regional Internet Registry)

The RIR passes out IP's to ISP (Internet Service Provider) who passes out Network ID's (IP's) to people who need them.

Class Licenses: (used for organization) *Memorize these, these are the first OCTET*

Class A: 0-126 /8

Class B: 128-191 /16 (65534 IP addresses 'hosts')

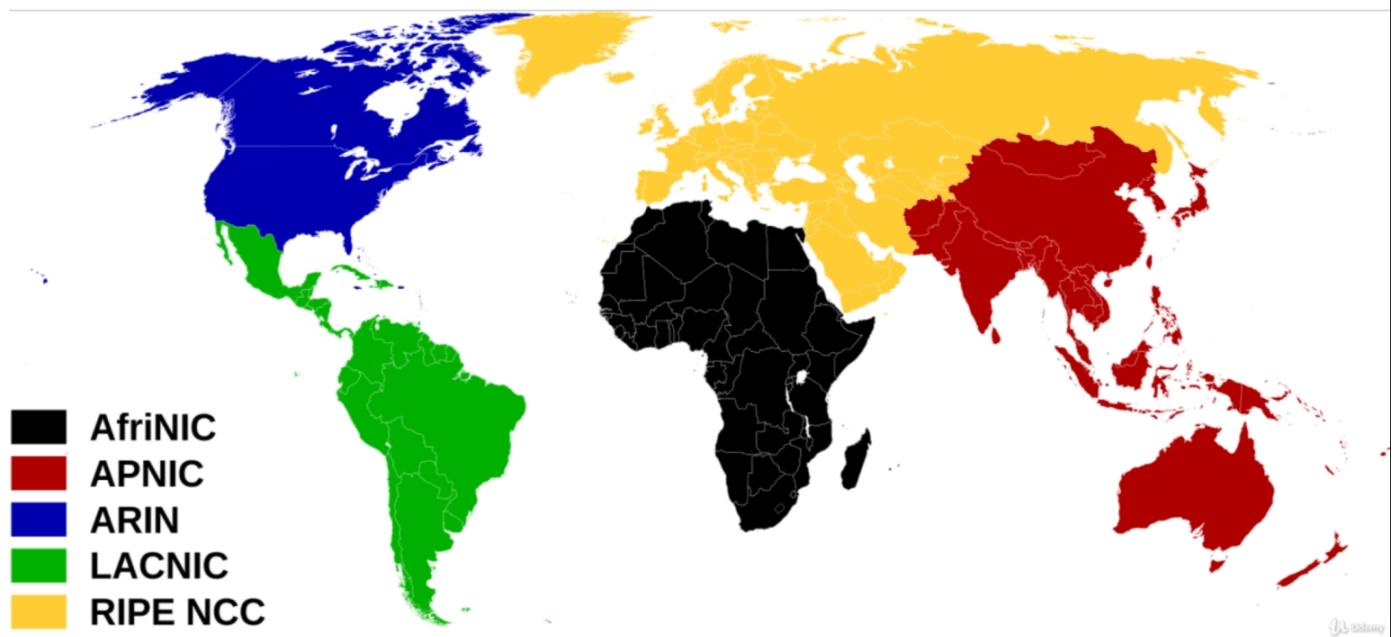
Class C: 192-223 /24 (254 IP addresses 'hosts')

Wack '/' is the subnet

Subnetting divides Network ID's (IP's) into two or more networks

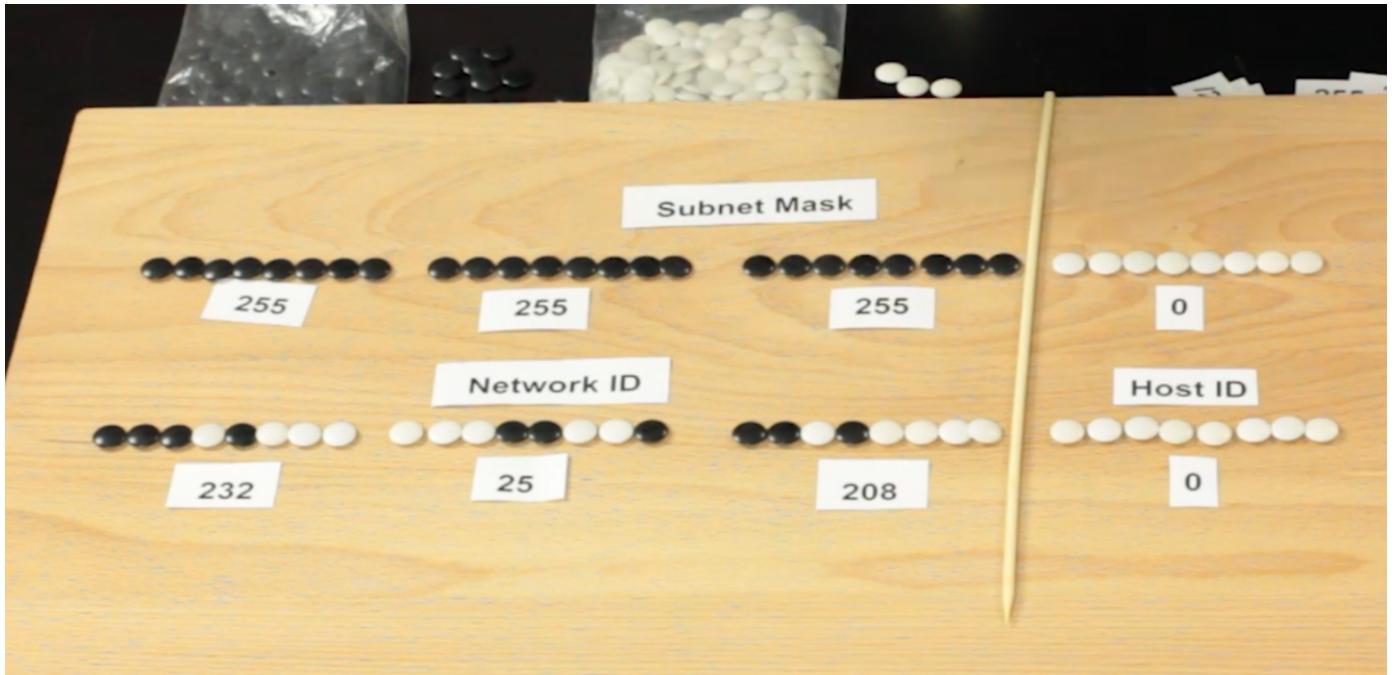
IP's cannot end in a 1 or a 255, However subnets can end in a 1 or a 255
subnets do not have to be on the dots.

Regional Internet Registry (RIR)

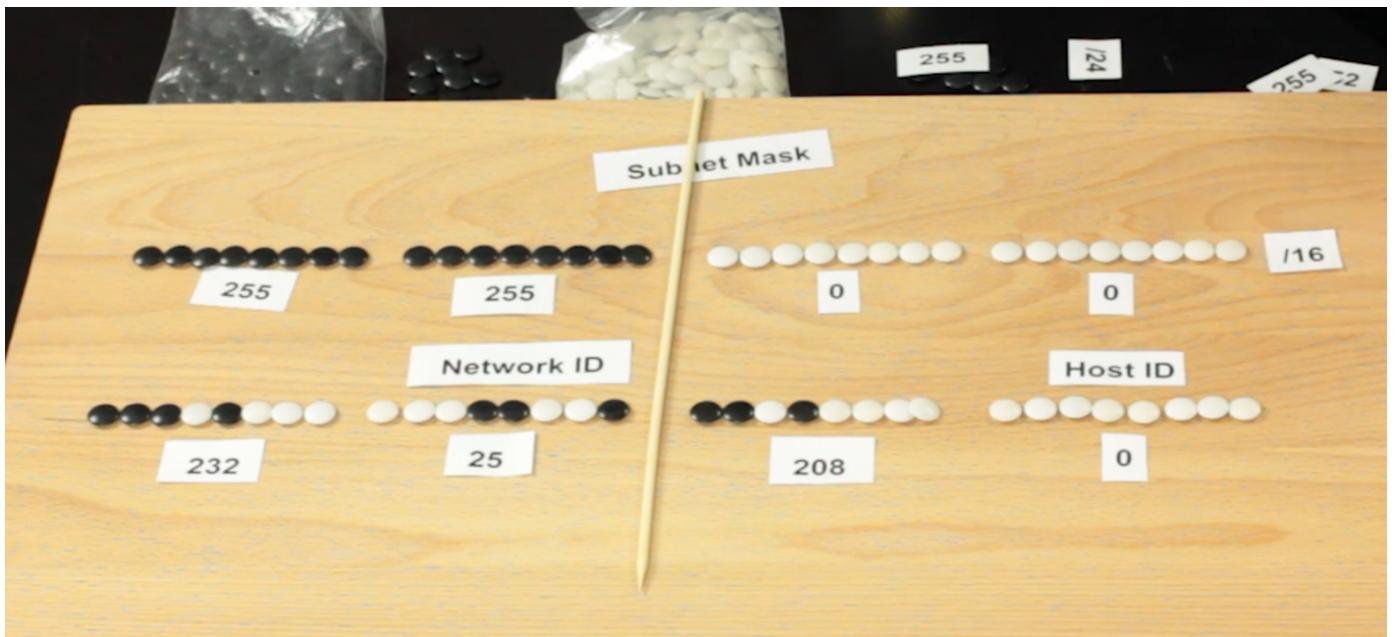


40. Subnet Masks

Anywhere there is a 1 the Net ID stays the same. The zeros can change and that is the amount of host on the network.



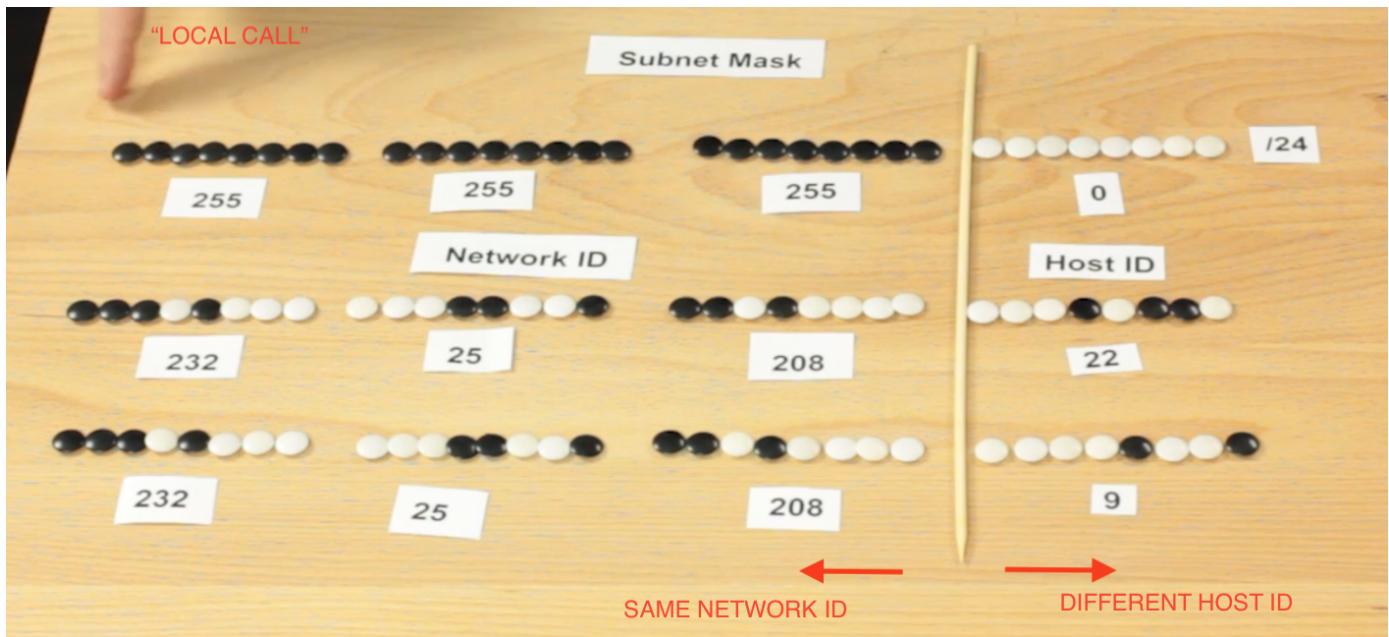
"Wack 16" or /16 subnet the "16" is the number of zeros. Only the first two digits need to be the same for all the computers. So the smaller the subnet mask the larger the networks, the larger the smaller the networks



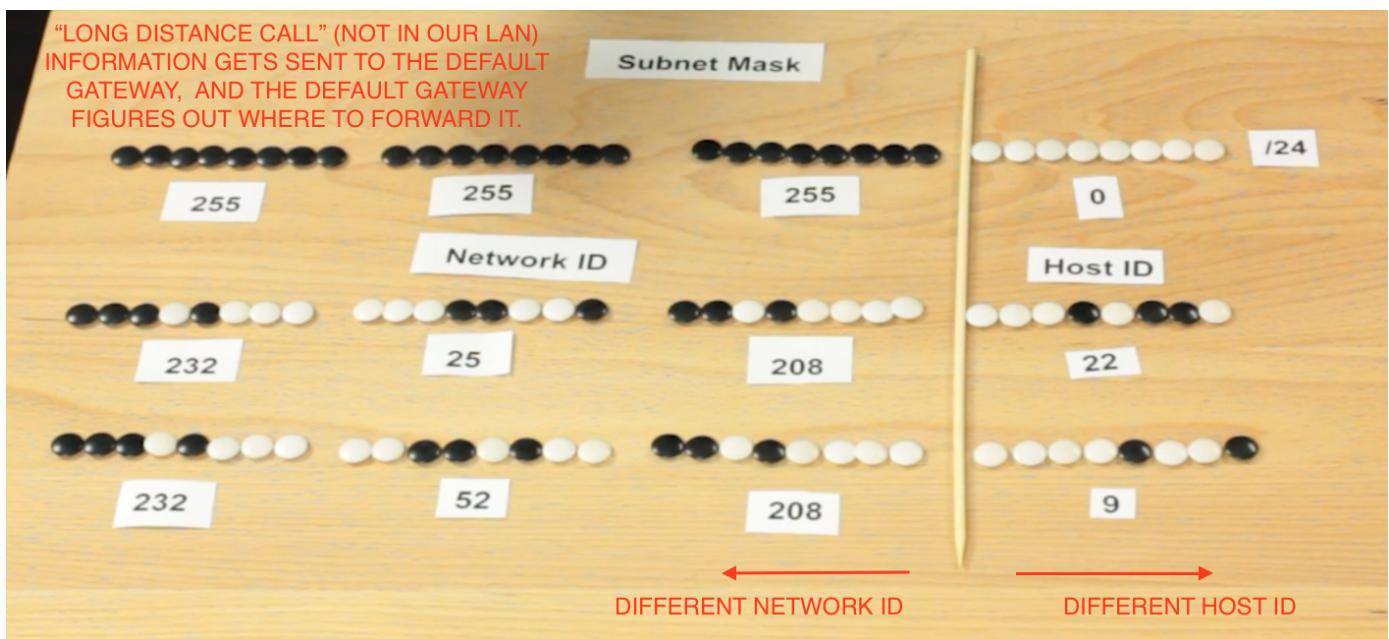
The subnet can only be used by the computer. It cannot be sent out.

The subnet mask can determine using the subnet mask if one computer talking to another is a "local call" so it just sends an ARP gets the MAC and sends information.

LOCAL CALL (SAME NETWORK ID): SUBNETMASK LOOKS AT THE ADDRESS AND DETERMINES IF IT IS A LOCAL CALL



LONG DISTANCE CALL (DIFFERENT NETWORK ID):



1. EACH HOST NEEDS AN IP
2. EACH HOST NEEDS A SUBNET MASK
3. NEEDS A DEFAULT GATEWAY.

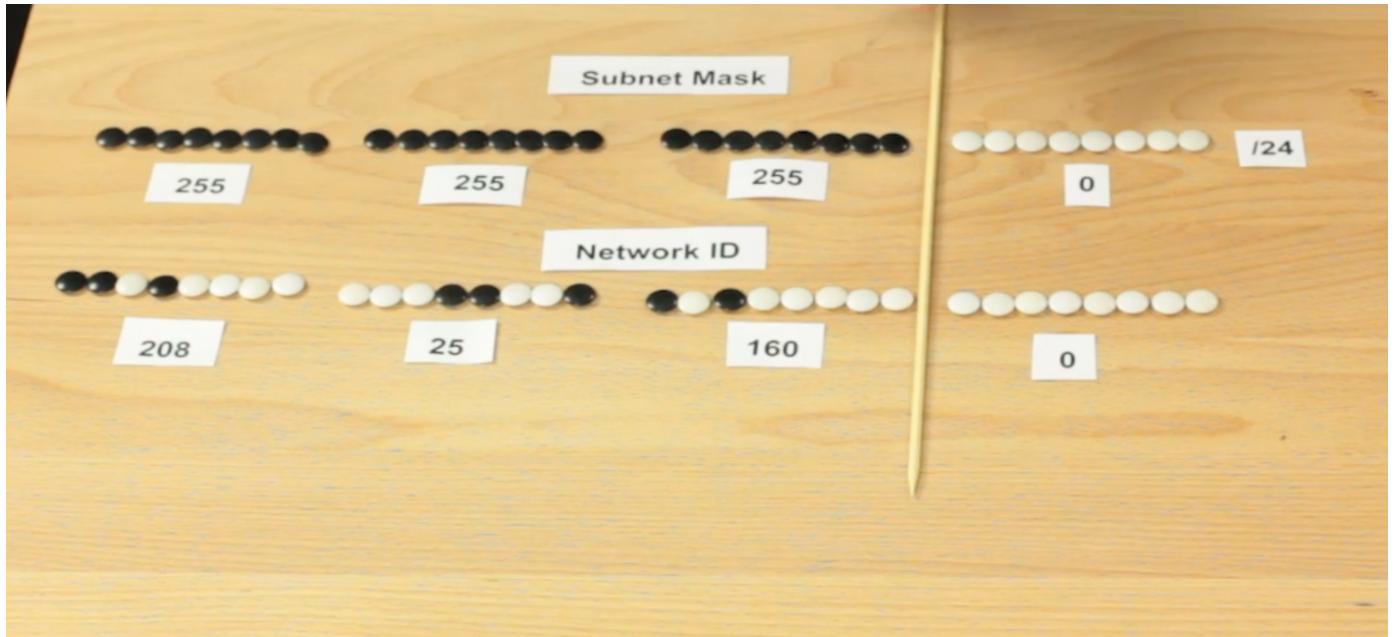
41. Subnetting with CIDR

Classless Inter-Domain Routing (CIDR)

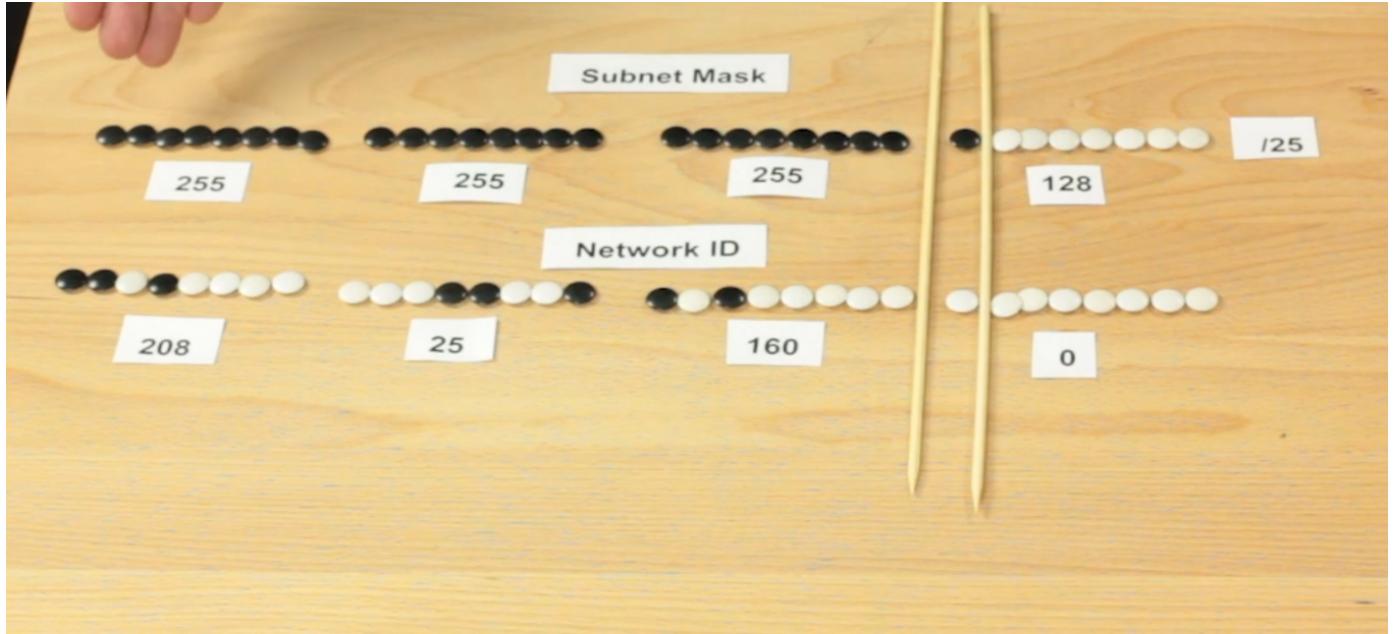
Subnets only have to be a string of 1's and then 0's. So you can break subnets up by the amount of 1's and 0's. 1'S ON THE RIGHT, 0'S ON THE LEFT

Example:

/24:



/25:



*REWATCH FOR REVIEW-GREAT EXPLANATION

42. More CIDR Subnetting Practice

Memorize the number of Hosts each /# Has

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:	<ul style="list-style-type: none"> *Hosts double each increment of a CIDR *Always subtract 2 from host total: Network ID - First Address Broadcast - Last Address 																																															
	<p style="text-align: center;">/8= Wack 8 /16 = Wack 16 /24 = Wack 24 /32= Wack 32</p>																																															
	<p style="text-align: center;">CIDR= # First available Last Available</p>																																															
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th></th><th>IP</th><th>Hosts</th><th>Network</th><th>Broadcast</th><th></th><th></th><th></th></tr> </thead> <tbody> <tr><td>192.168.1.0/24</td><td>255.255.255.0</td><td>254</td><td>192.168.1.0</td><td>192.168.1.255</td><td></td><td></td><td></td></tr> <tr><td>192.168.1.0/28</td><td>255.255.240.0</td><td>14</td><td>192.168.1.0</td><td>192.162.1.15</td><td></td><td></td><td></td></tr> <tr><td>192.168.1.16/28</td><td>255.255.240.0</td><td>14</td><td>192.168.1.16</td><td>192.162.1.31</td><td></td><td></td><td></td></tr> <tr><td>192.168.0.0/23</td><td>255.255.254.0</td><td>510</td><td>192.168.0.0</td><td>192.162.1.255</td><td></td><td></td><td></td></tr> </tbody> </table>									IP	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	255.255.240.0	14	192.168.1.0	192.162.1.15				192.168.1.16/28	255.255.240.0	14	192.168.1.16	192.162.1.31				192.168.0.0/23	255.255.254.0	510	192.168.0.0	192.162.1.255			
	IP	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	255.255.240.0	14	192.168.1.0	192.162.1.15																																												
192.168.1.16/28	255.255.240.0	14	192.168.1.16	192.162.1.31																																												
192.168.0.0/23	255.255.254.0	510	192.168.0.0	192.162.1.255																																												
Practice	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th></th><th>IP</th><th>Hosts</th><th>Network</th><th>Broadcast</th><th></th><th></th><th></th></tr> </thead> <tbody> <tr><td>192.168.0.0/22</td><td>255.255.252.0</td><td>1022</td><td>192.168.0.0</td><td>192.168.3.255</td><td></td><td></td><td></td></tr> <tr><td>192.168.1.0/26</td><td>255.255.255.192</td><td>62</td><td>192.168.0.0</td><td>192.168.1.63</td><td></td><td></td><td></td></tr> <tr><td>192.168.1.0/27</td><td>255.255.255.224</td><td>30</td><td>192.168.1.0</td><td>192.168.1.31</td><td></td><td></td><td></td></tr> </tbody> </table>									IP	Hosts	Network	Broadcast				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	192.168.0.0	192.168.1.63				192.168.1.0/27	255.255.255.224	30	192.168.1.0	192.168.1.31											
	IP	Hosts	Network	Broadcast																																												
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	192.168.0.0	192.168.1.63																																												
192.168.1.0/27	255.255.255.224	30	192.168.1.0	192.168.1.31																																												
	<p style="text-align: center;">16 HOSTS in /28</p> <p style="text-align: center;">NETWORK ID= Host 0 Broadcast is 0-15= Host 16 Total Hosts available after Network ID and Broadcast = 14 (16-2=14)</p>																																															

Static IP: You always have an IP address for our router.

Watch Subnetting in 7 Seconds.

Subnetting in 7 Seconds:

<https://www.youtube.com/watch?v=ZxAwQB8TZsM>

43. Dynamic and Static IP Addressing

DHCP (Dynamic Host Configuration Protocol)

BOOTP (Bootstrap Protocol)

DHCP most time manifests as a server.

Computer starts without IP address or any information and it sends out a broadcast that is "DHCP Discover" with a MAC of all F's to find a DHCP Server.

The DHCP server sends a DHCP offer (Unicast traffic gets sent back to machine)

The Offer has everything in it. IP, Subnet mask, default gateway, etc.

The computer then sends a DHCP Request back to the server for all of that information.

Then the server sends a DHCP Acknowledgement to the Computer and does it and then keeps track of all all the clients that are using DHCP.

**Almost all home routers have DHCP server in them

**Only have one DHCP Server.

**DHCP servers have to be withing the broadcast domain

Static IP Addressing - is when you manually type in your IP information on the machine.

When setting a DHCP server you have to start with a scope (manually):

Then input a starting IP

Then input an ending IP

Then input the subnet

Then lease duration (default on windows is 8 days)

Input the default gateway

Input DNS Servers

NEED TO REVIEW THIS SECTION

44. Rogue DHCP Servers

Common DHCP Errors:

They all manifest in the same way: you cannot get "on" the internet

APIPA - Automatic Private IP Addressing - built into all DHCP clients and designed as a fallback if you cannot find a DHCP Server (169.254 APIPA ADDRESS) <-- Cannot connect to the DHCP Server. This is on the exam (the APIPA Address)

-If all computers on broadcast domain suddenly lose the dhcp server they will all spin up an APIPA address.

ROGUE DHCP Server

Anytime your IP address is not putting out your known IP address you have a rogue DHCP.

*APIPA Address

*Know your network ID - If yours is different than the known you have a Rouge DHCP Server.

*45. Special IP Addresses - Need to recognize these for the exam

-Private IP addresses: 3 IP addresses that are only used on internal networks that are never going to share on the Internet

1. 10.x.x.x (Private)
2. 172.16.x.x or 172.31.x.x (Private)
3. 192.168.x.x (private) (NAT Device - Hides you from the internet)

-Loop Back IP Addresses:

1. 127.0.0.1 (IPv4)
2. ::1 (IPv6)

-APIPA (Automatic Private IP Address) - Cannot get on the internet but can talk locally if DHCP is down.

1. Always start with 169.254.x.x (Each computer randomly generates the next two values)

Make sure you are comfortable with all of these for the exam

46. IP Addressing Scenarios

Issues that come up on the Exam:

1. Duplicate IP Address: Standard NAT Router/DHCP Server passing to two computers (Win 10, and Ubuntu Linux)

If there was a rogue DHCP Server it could pass out two identical IPs

Statically Addressing IPs you could accidentally duplicate them (windows will fix it on its own)

*Know your network

*Good Book Keeping (Anytime you set static IP's track it)

2. Duplicate MAC Addresses (Happens with Virtual Machines)

Could accidentally type in two identical MAC addresses.

You will not connect to the net, or the local network

**It's very hard to detect.

3. Incorrect gateway

*You will not be able to get out of your LAN

*Need to know your default gateway

*Main reason this gets messed up is because we type things incorrectly statically

4. Incorrect Subnet Mask

*Remember that all computers within the same broadcast domain will have the same subnet mask.

* Sometimes you can get sometimes get through to other machines if the subnet is the same on two machines but they're typed in differently.

Machine 1 - 255.255.255.0

Machine 2 - 255.255.255.00

One machine will be able to ping the other but not vice versa.

5. Expired IP Address

*Computers always ask the DHCP server to renew its lease after half the allowed time and the DHCP will renew. However, if the DHCP server dies it cannot renew and by default the lease is expired. Easy to detect because it will work or it won't and you will get an APIPA address.

there are a lot of scenarios questions like this on the exam, and COMPTIA will give you lots of pictures and things like that to use.

QUIZ

1. Which decimal number is represented by the binary number 10110110?

- a. **182**
- b. 176
- c. 73
- d. 182.176.73.0

2. What does ARP stand for and what does it do?

- a. Advanced Routing Protocol determines routes between MAC addresses
- b. Altenate Routing Protocal determines backup routes between MAC addresses
- c. Address Resolution Protocol resolves MAC Addresses with IP Addresses**
- d. Advanced Resolution Protocol resolves network names to IP addresses

3. Which statment is not true of a subnet mask?

- a. Subnet masks are used by a computer to determine the network ID
- b. Subnet masks are sent out as one of the fields in the IP packet**
- c. Subnt masks are made up of ocntiguous 1s starting at the leftmost (Most significant bit) of an IP address
- d. Subnet masks are never sent out of a host

4. Here are three IP addresses: 216.53.12.11, 130.222.255.170, 223.255.6.88. What class of addresses are each one (in order)?

- a. c,b,c**
- b. b,a,c
- c. c,a,b
- d. a,c,a

5. An organization has five campus buildings. They want each building to be on its own subnet. Each campus will need a minimum of twenty-five IP addresses. The organization has the Class C network address 217.105.2.0 assigned to it. Using CIDR, what subnet mask will yield the minimum number of subnetworks with the maximum number of hosts per network that will meet the requirements of the organization?

- a. /26
- b. /27** (Need to review subnetting)
- c. /28
- d. /29

6. A company has subnetted their Class C network address into four subnets with a /26 subnet mask. What are the addresses of the four subnets?

- a. 0,1,2,3
- b. 128,64,32,16
- c. 0,64,128,192**
- d. 1,2,4,8

0, 64, 128, and 192 represent all of the possible values of 1s and 0s in the first two columns of the fourth octet in a Class C address: 0 0, 0 1, 1 0, and 1 1. Place those values under a 128 and a 64 and calculate the results. The leftmost two bits of the fourth octet are masked - the 128 and 64 column - using any combination of 1s and 0s in those columns, it would not be possible to generate a 1, 2, 3, 4 or 8. It would also be impossible to generate a 32 or 16 so the other choices are incorrect.

7. What service does not automatically assign an IP address to a host?

- a. **Static**
- b. DHCP
- c. Bootp
- d. APIPA

8. Which choice is true of a rogue DHCP server?

- a. A rogue DHCP server increases the speed of the DHCPO service
- b. A rogue DHCP server increases the pool of available IP addresses
- c. **A rogue DHCP server can assign incompatible IP addresses to hosts**
- d. A rogue DHCP server ensures that hosts will get compatible APIPA addresses

9. Which of the following is not a "special" IP address?

- a. 10.255.1.1
- b. 169.253.4.185 (APIPA is 169.254.x.x)**
- c. 192.168.70.70
- d. 127.0.0.1

10. Which symptom is not a result of an IP addressing problem?

- a. Duplicate IP address
- b. Static IP address**
- c. Duplicate MAC address
- d. Incorrect Gateway