IPAddress

==============

Computer understand only 0 and 1's.ip address is a 32 bit ocatl number.it will be devided into 4 segments.each segment is called octet.

IP address is a combination of network id and Host ID.

why we need IP?

if we want to communicate from computer-computer we need IP.

it is 32-bit format and it will be devided into 5 types.

Class A,B,C,D,E

Class A:

out of 4 octets first octet can be newwork and remaining 3 are host ID.

8bits : 8bit:8bits:8Bits

n/wId : hostId

0

In networkid first bit is 0.so max value is 255-128=127 max value.127 and 0 cannot be used for network address so Class A network Address range between 1 and 126.

in any IP address range ,first starting address is network addresss and last one is broadcast address.

eg:1.0.0.0-->network address and

1.255.255.255.255 broadcast address

so we will not give initial network address and broadcast address to any device.

Class B:

8:8 : 8:8

N/w : Host

10

and in network id ,in first octet,first and 2nd bit is 1 and 0 repsectively.

so 2^6=64.SO 255-64=191.so class B ip address range is 128-191.

Class C:

8:8:8: 8

n/w : host.

110

range 192:0:0:0--223.0.0.0.

Class D:

224:0.0.0--239.0.0.0

Subnet mask:

==============

the computer cannot identify what is networkid and hostid.to understand compueter we have concept called subnet mask..

based on this it will understand what type of class IP's we are using.

for networkid it will take all 1's and host id's it will take 0's.

so for class A ,first 8 bits are network id so we will take all 1's .now subnetmask for class A is 255:0:0:0

same way class B,subnet mask is 255:255:0:0

class C is 255:255:255:0

class D is 255:255:255:255

mac address is fixed for all computers.

in windows command prompt we can find using below command.

ipconfig /all

physical address

Network

a)PAN-->personal Area Network

b)CAN-->Campus Area Network

c)LAN

d)MAN

e)WAN

on top of above networks,we will use topology how systems are connected internally.

bus opology,mesh topology,tree topology.

to estrablsih a computer network we need devices i.e n/w devices.

switch :

========

all clients connected to one switch throgh cables.and this switch finally connected to one centralized server.

clients computers,printers.

Repeater:

suppose i have two LAN n/ws.suppose from one system of LAN A should be sned data to one system of LAN B.the distance may very

long then we will use Repeater to amplify the signal means it will strenghten the weak signal.

Bridge:To send data from two diffrent LAN's we need one medium called Bridge.

HUB:All devices connected to central one server.

Router:after network is established between computers if we want to conect to inernet we need router.

ROuter->network switch1-->1machine,2 machine,3 machine.

->network switch2-->4machine,5 machine,6 machine.

to establish wired connection we will use below cables.

a)Co-axial(1990's-T connector,copper made)

b)Twisted Pair(8 cables-combination of two cables.)

c)Fiber Optics(data transimission in the from of light)

depending on type of cable it will send data in particular with certain data transfer rate.

VLAN:Virtual LAN.

it is private set of LAN.

LAN local area network consists within a building connected with network devices like switches, routers etc.

and VLAN VIRTUAL LOCAL AREA network is a concept of virualy logical domain's connectivity and communication.

VLAN's are created in a SWITCH to seperated the goups and join the same domain like, sale department ,

purchase department etc etc to communicate each other. For example there is VLAN Named sale department ,

in this case any computer we join to sale department can only communicate each other within sale department vlan.

secure , fast and reduced the burdon of more switches purchasing.

Spanning tree:

switch to switch -->cross cable.

Advanced port scanner.-->to check which software is working on which port.

in windows -->Device driver-->update device driver-->networkadapter-->

here it will list all installed drivers related to network.

Protocols

========================

specific rules for communication on the net.

it is a set of rules and procedures used for communication.

1)TCP Protocols-->Transmission Control Protocols

2)UDP--user Datagram protocol(gaming,video conference)

3)SMTP(simple mail tranfer protocol)

4)POP3-(Post office protocol)

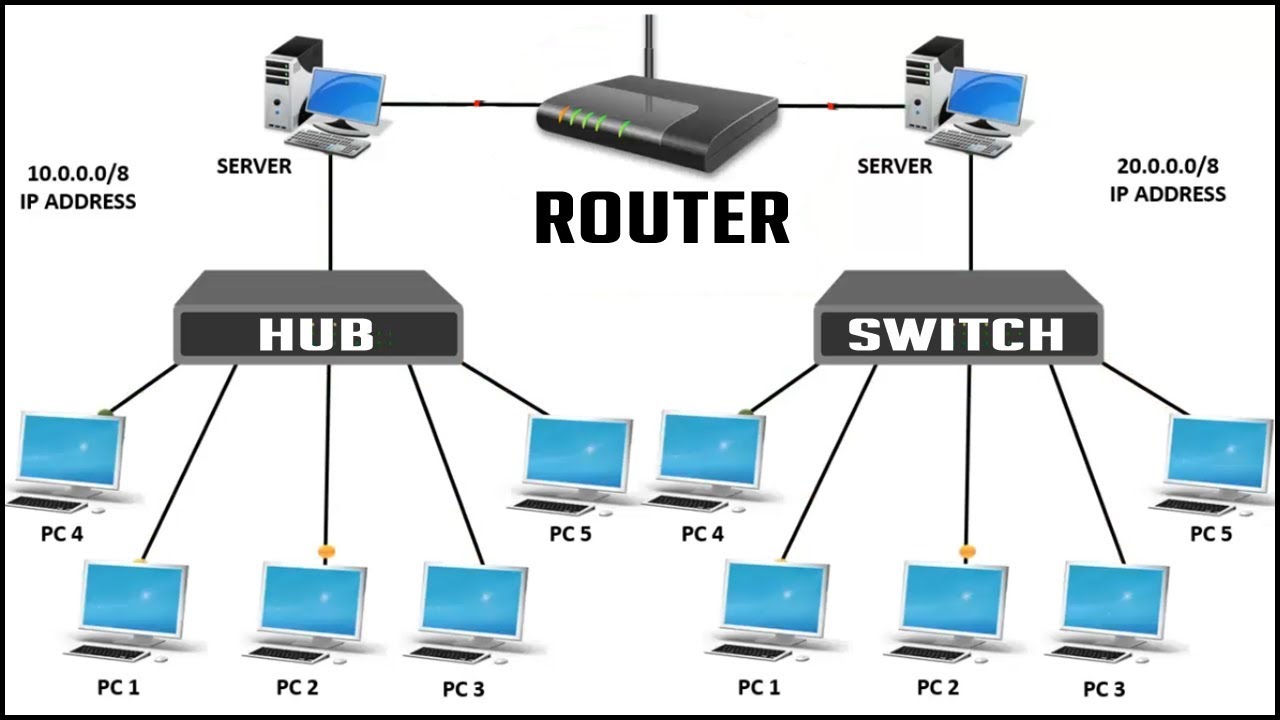
5)IMAP(internet Message Access Protocol)

6)HTTP ,HTTPS

7)FTP

Ethernet-->a system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.

Router is used to connect two or more diffrent networks.



Hub sends data in the form of packets.switch sends data in the form of frames.router sends data in the form of packets.

Hub works on physical layer,switch works on data link layer ,and router work on network layer.

Hub does not store any mac or ip address to transfer data,switch stores and uses mac address of a devices to transfer data,Router uses IP address to transfer data.

Hub is broadcast device,switch is multicast device,router is routing device use to create route for transmitting data packets.

Ethernet-->a system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.

Router is used to connect two or more diffrent networks.

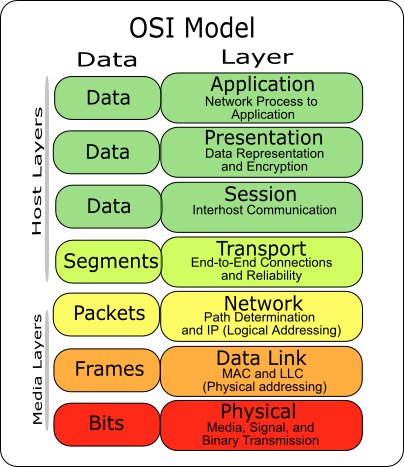
Packet-->A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

OSI model

==============

why osi model?-->to proper communication between devices.

OSI-->OpenSystem InterConnection.it consists of 7 layers.



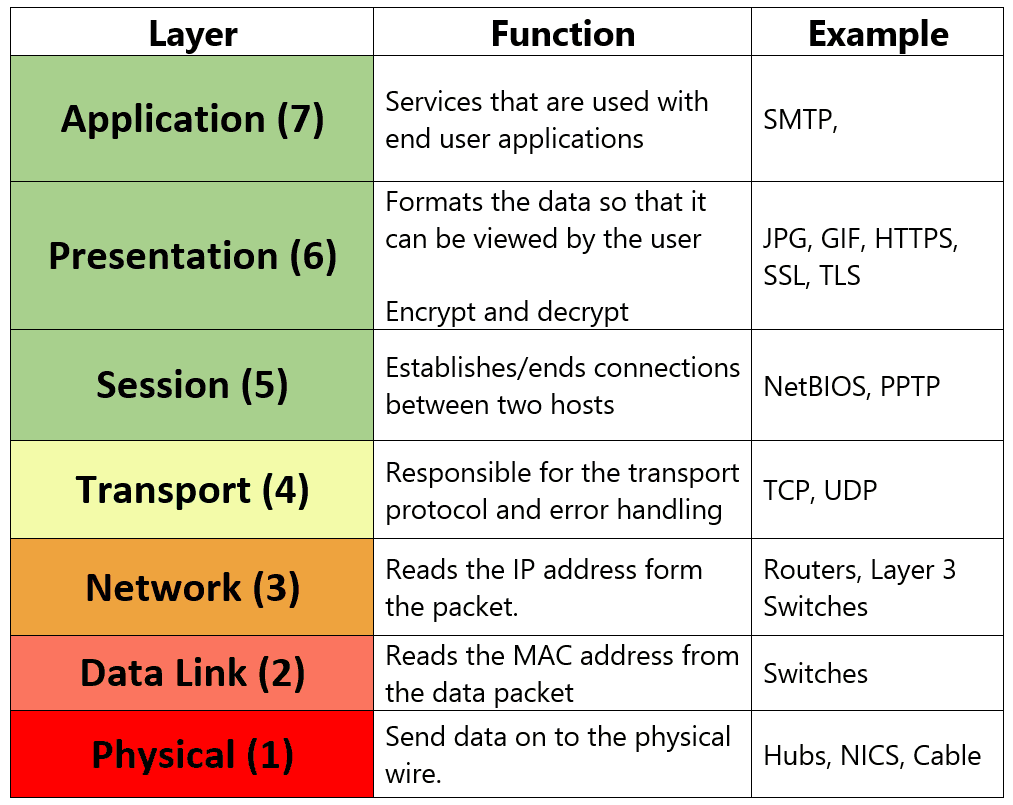
Top 3 layers are software layers because it will work based on software ,

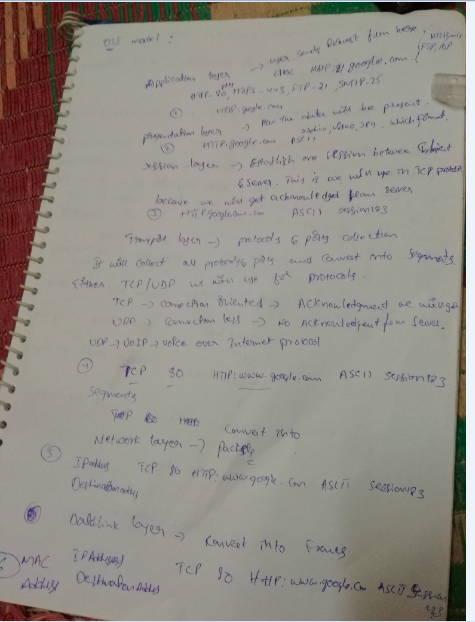
Application,Presentation, and session layers

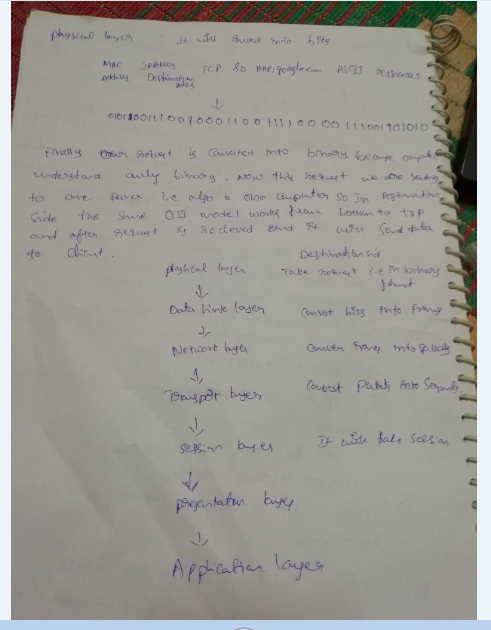
and bottom 3 are hardware layers.

N/w,Data Link and Physical Layes.these are all working with hardware components.

Trnasport layer🡪heart of OSI model.







Modem:Modulation and Demodulation.In olden days we have telephone lines ,through this we will get internet.but it is in the form of analog.but computer can understand only digital so we should convert this signals from telephone wire to computer and vice versa.

Processor 32-bit and 64-bit:

2^32=4GB

2^64=16Exa Bytes stores data in RAM.

Suppose for 32-bit system,if we give more than 4GB data it will not use because the max it will store 4GB only.

Operating system also 32-bit and 64 bit.

Subnet: A single network is divided into multiple networks is called sub net.

In a company we have 4 departments each department we required 50 hosts,so total 200 hosts we required but each department can not access other department host .so we should maintain 4 networks.so that we can provide security.but we need to buy 4 networks.its a very cost.so we have concept called subnet.

Suppose for 200 hosts,if we buy class C IP address public IP i.e192.168.1.0

For first 50 users we can give 192.16.1.1

192.16.1.2, 192.16.1.3 like this up to 50 .but for another 50 users we can’t use after 50 becauese security issue so we need to buy one more network.

Now this problem we can overcome by using subnet.

Subnetting can be performed in two ways.

FLSM:Fixed Length Subnet Mask.

VLSM:Variable length Sub net Mask.

Subnetting can be done based on requirement.

--no.of n/w’s required

--no.of hosts required

Based on no.of networks

2^n-2

No.of host

2^h-2>=2.

I have requirement for 4 departments A,B,C,D.

for Department A required 90 hosts,

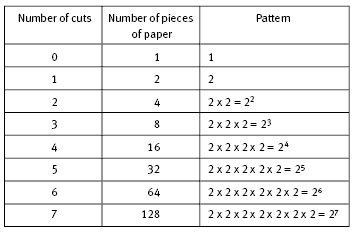
B required 40 hosts,C required 20 hosts,D required 10 hosts.

So for this Class C address is fine max 160 .in Class for one single public Ip we will get max 250 hosts.based on subnet we will devide them into 4 categories.

Suppose I bought Class C IP address is 192.168.0.0

192.168.0.1-192.168.0.254 this range ip’s I can assign to above 4 departments.

Take first highest number 90 and then 40,30,10.



90 value is nearer to 128 so 2^7-2=126>=90(1 network id and broadcast id).now host value is 7 .so in that position we will replace with 1.

Subnet mask🡪11111111: 11111111: 11111111:1000000/25🡪255.255.255.128/25

For department A IP range is 192.168.0.0-192.168.0.127/25(192.168.0.0, 192.168.0.127 not used for this is dedicated for network and broadcast=126 we can use).

So for department A network range is 0-127 with subnet mask /25.all network id is replaced with 1’s.so in that 8 th position means 2^7 we have taken 1.so that’s why subnet mask is 25.

Like this for Department B required 40 hosts.if we go to 2 table above we have to take 2^6.

Like this we have to apply above concept for all deprtment.finally the ip range of all departments are,

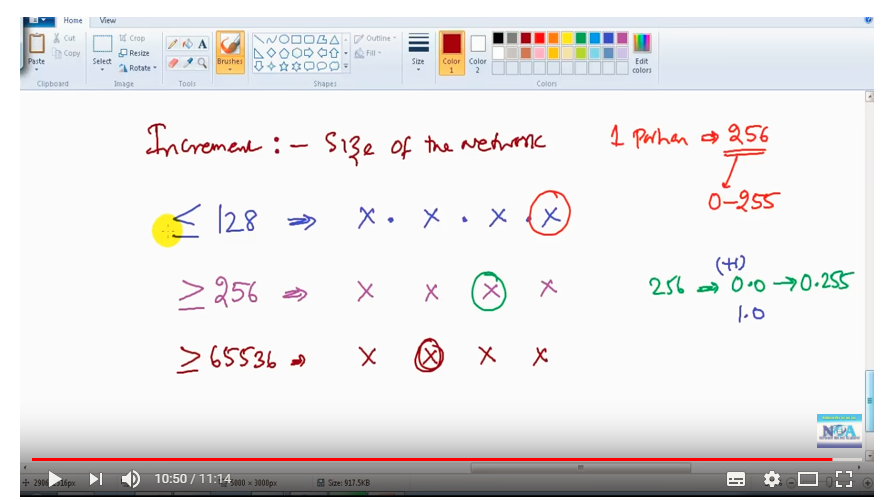
DEPT A-192.168.0.0-192.168.0.127/25(for 90 hosts)

DEPT B-192.168.0.128-192.168.0.191/26(40 hosts)

DEPT C-192.168.0.192-192.168.0.223/27(20 hosts)

DEPT D-192.168.0.224-192.168.0.239/28(10 hosts)

Wastage of ips will be less in VLSM.



FLSM: Requirement 50 hosts.

2^6=64-2>=50

62>=50.

I’m using 6 bits so remaining 2 bits are not using. That two bits are converted to network bits.

So

In class C N:N:N:H

Network always represented with 1’s.

1111111: 1111111: 1111111:11000000

Total network bits are 26 now.by default Class C supports 24 n/w bits and 8 host bits.

Subnet mask is 255:255:255:192

Take Class C example 192.168.1.0

Range 2^h=2^6=64.

256/64=4 subnets.

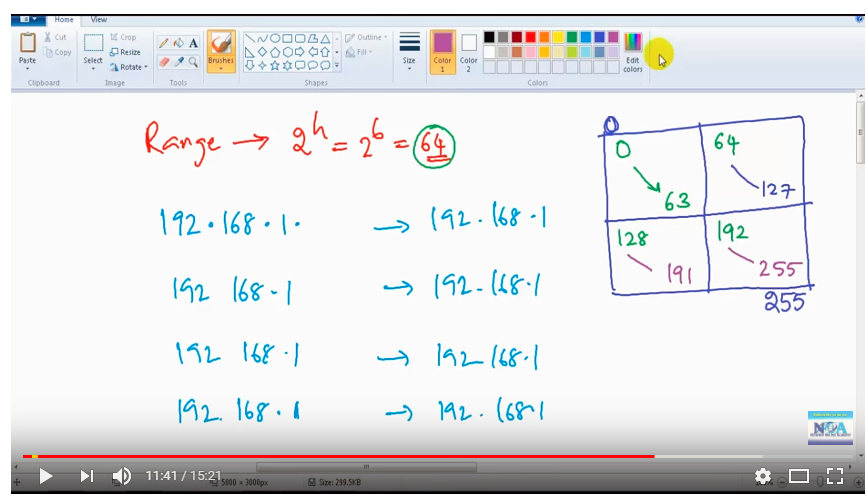
So ip ranges should be in 4 ranges.

192.168.1.0 -- 192.168.1.63

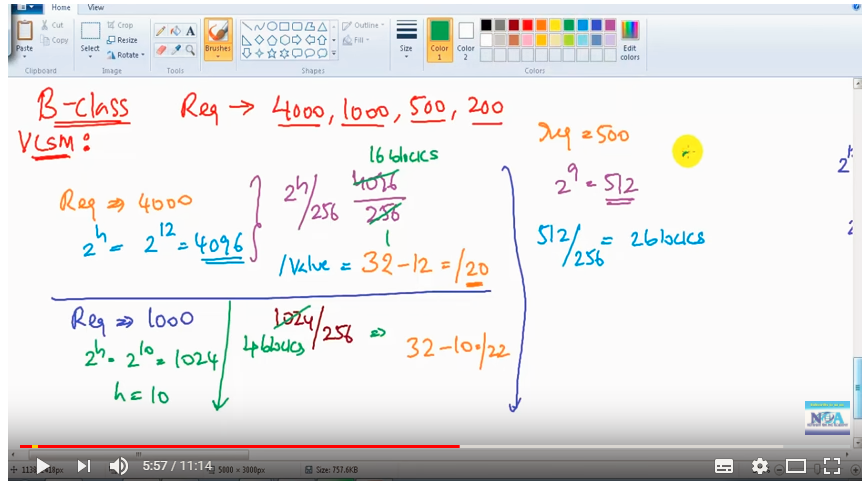
192.168.1.64 -- 192.168.1.127

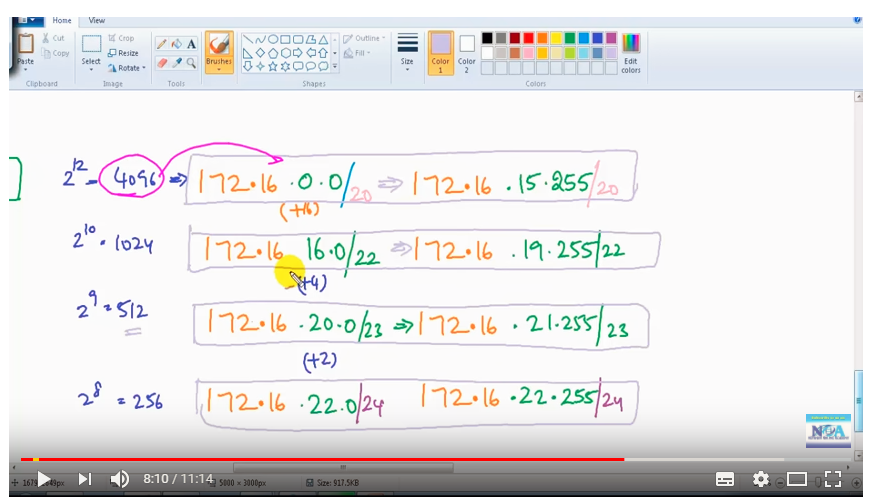
192.168.1.128 -- 192.168.1.191

192.168.1.192 -- 192.168.1.255

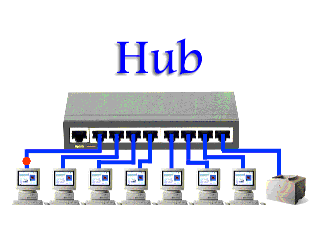


Class B VLSM example:





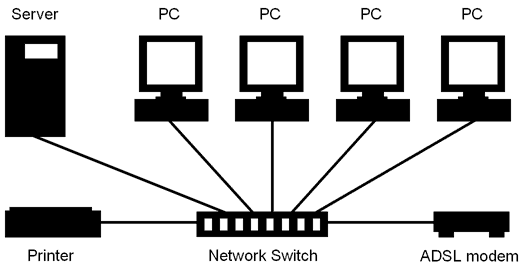
Network devices:

Hub:it is not an intelligent device,before switches we are using hub for data transmission. 

A D G

Suppose if computer A sends data to computer D.first computer will inform hub to im sending data to computer D.now hub will send broadcast packets to every computer .all computers will reject except D.now A will transfer data but hub will send this packets to every computer but D only Accept.because of bandwidth and n/w traffic will b more.in this A can send data to computer D at the same time D cannot send data to computer A.so that’s y its half duplex.

Switch:switch is an intelligent device ,it will maintain mac addresses of all computers.



Now pc1 sends data to pc3.first pc1 sends broadcast packet to switch,this switch will send packets to all devices.now D will give reply to Switch,in this point swich will store both mac address of pc1 and pc3.these are all store in switch table.in next time pc1 sends data to pc3 ,this time it will sends directly because it will store in switching table and no need to send broadcast packets for communication.

DHCP:Dynamic Host Configuration protocol.it will automatically assign ip address to connected to devices.DHCP is a service installed in every operating system.

Ipconfig –all

It wll show ip address starting leasing time an expiry time,it is done by automatically bydhcp server.

We can see this dhcp client service which installed in windows service.

Services.msc🡪DHCP client.

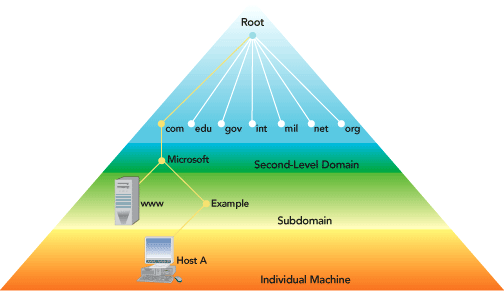
Router:WAN port for internet connection and LAN ports to connect devices.

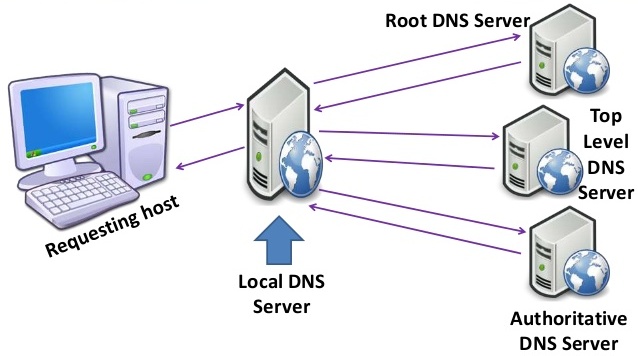
DNS:Domain Naming Service.in router we have dns address .in this maintain all addresses of URL and with their IP’s.

At the starting of internet we don’t have dns so at that time ,suppose we want google.com ,how we will get this one means we have host file in our machine based on this one it will take that ip.

C:\Windows\System32\drivers\etc\hosts.

Dns is zone file it will contain all records.





Suppose im requesting [www.yahoo.com](http://www.yahoo.com)

First my host will request this to local dns is nothing but whatever dns provided by ISP.internet service provicder like beam,hatchway.they provided already one DNS when im using internet means they provided DHCP router and DNS serverIP also.so first request will go to my local dns server.if its fine my [www.yahoo.com](http://www.yahoo.com) then it will return that ipaddress to me .but if it is not find means my dns again connected to one authorized dns server their also we didn’t fine means then it will send to root level dns server.thier we have all info about our requested url info.again root level will send that ip address of yahoo.com to us.in this process our local dns server will maintain caching data of yahoo.com data into our dns sevrer.next time any request coming for yahoo.com it will take from cache.

VPN:Virtual Private Network .Accessing other network resources by using internet in secured way.

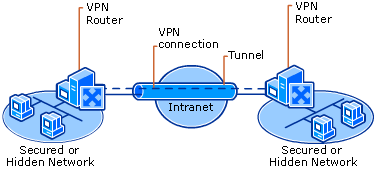
It will create one tunnel between two networks in secured manner by using some encryption algorithms.

i.e aes—advanced encryption standard.

des –data encryption standrad

3des

protocols:IPSec(internet security protocol),L2tp,Ssh,SSL.



ACL:Access Control List.

Access control list (in further text: ACL) is a set of rules that controls network traffic and mitigates network attacks. More precisely, the aim of ACLs is to filter traffic based on a given filtering criteria on a router or switch interface.

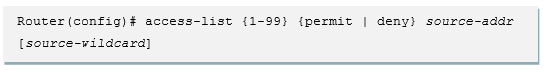
Reasons why you should use ACLs:

* Limit network traffic to increase network performance
* Provide traffic flow control
* Provide a basic level of security for network access by defining which part of the network/server/service can be accessed by a host and which cannot
* Granular control over traffic entering or existing the network

Types of Access Control Lists

ACLs are primarily divided into two types: **standard** and **extended**. We also differentiate between **numbered** and **named** ACLs.

**Standard** ACLs allow filtering traffic solely based on Layer 3 source address written in the header of the IP (*Internet Protocol*) packet.  
The command syntax for configuring a **standard** numbered ACL:



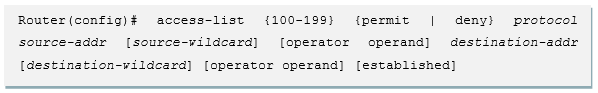
The first value {**1-99** or **1300-1999**} specifies the standard ACL number range.

The second value specifies whether to **permit** or **deny** the configured source IP address traffic.

The third value is the source IP address that must be matched.

The fourth value is the wildcard mask to be applied to the previously configured IP address to indicate the range.

**Extended ACLs** filter traffic based on Layer 3 and 4 source and destination information thus giving greater flexibility and control over network access than standard ACLs. The Cisco Extended ACL command guide can be found [here](https://www.cisco.com/c/en/us/td/docs/app_ntwk_services/waas/waas/v401_v403/command/reference/cmdref/ext_acl.pdf).  
The command syntax for configuring an extended numbered ACL:



The first value {**100-199** or **2000-2699**} specifies the extended ACL number range.

The second value specifies whether to **permit** or **deny** traffic according to the criteria that follows.

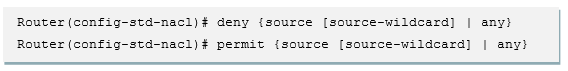
The third value indicates protocol type, that is, IP, TCP, UDP, ICMP or other IP-sub protocol

The source and destination IP address and their associated wildcard masks determine where traffic originates and its final destination, respectively.

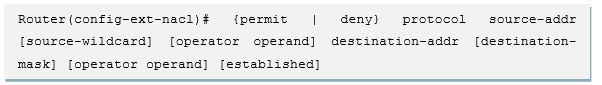
As already mentioned, it is also possible to create a **named** ACL, which must be specified as either standard or extended.  
The command syntax for configuring a **named** standard or extended ACL:

*Router(config)# ip access-list [standard | extended] ACL\_name*

Upon executing this command, a user is placed into subconfiguration mode where permit and deny commands are entered:



An extended named ACLs offer additional parameters:



After creating the standard or extended ACL, you must apply it to the appropriate interface (or to a VTY line). The command to apply the ACL to an interface:

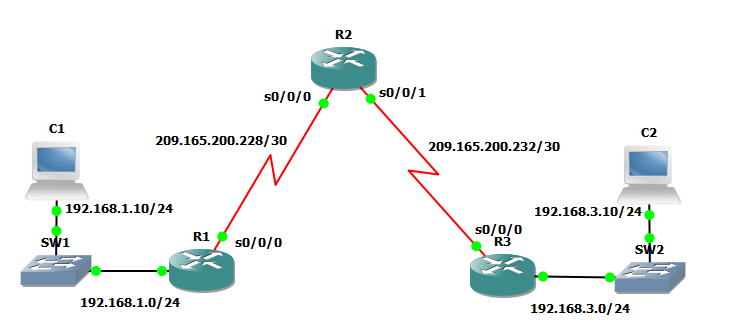
ACL apply syntax

## ACL Configuration Guidelines

When working with ACL or preparing the CCNA exam, it’s important to remember the following guidelines:

* Only one ACL per interface, per protocol, per direction is allowed.
* ACLs are processed top-down; the most specific statements must go at the top of the list. Once a packet meets the ACL criteria, the ACL processing stops and the packet is either permitted or denied.
* ACLs are created globally and then applied to interfaces.
* An ACL can filter traffic going through the router, or traffic to and from the router.
* All ACLs have an implicit “deny all” statement at the end. Therefore, every ACL must have at least one permit statement to allow any traffic to pass.

## ACL Example

[](http://www.routerfreak.com/wp-content/uploads/2014/10/acl_diagram.png)

The idea of this example is to demonstrate the usage of standard and extended numbered ACLs.

On this network, you want to block all remote access to the routers except from PC C2.  
First, you should create a numbered ACL on all three routers and then apply it to incoming traffic on the VTY lines as follows:

*R1(config)# access-list 10 permit 192.168.3.10 0.0.0.0  
R2(config)# access-list 10 permit 192.168.3.10 0.0.0.0  
R3(config)# access-list 10 permit 192.168.3.10 0.0.0.0*

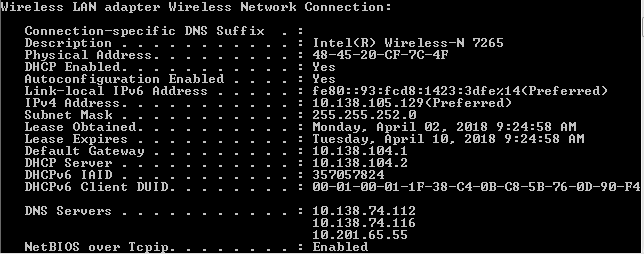
*R1(config-line)# access-class 10 in  
R2(config-line)# access-class 10 in  
R3(config-line)# access-class 10 in*

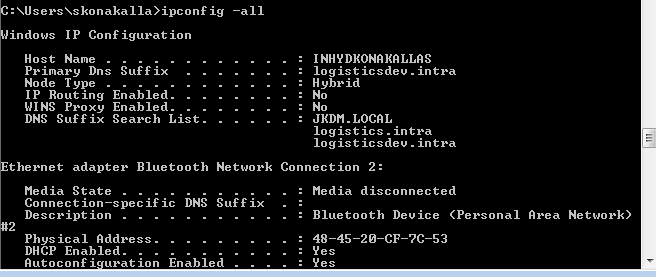
Then suppose you want to block all packets containing the source IP address from the following pool of addresses on R1: any RFC 1918 private addresses and 127.0.0.0/8. The solution is as follows:

*R1(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any  
R1(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any  
R1(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any  
R1(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any  
R1(config)# access-list 100 permit ip any any*

*R1(config)# interface s0/0/0  
R1(config-if)# ip access-group 100 in*

Myip: 219.65.68.2





tracert [www.google.com](http://www.google.com)

it will show how data packets are travelling at different levels.

Security group vs NACL

Vs Internet gateway

Vpc peering

Firewall vs cpl

NAT

Internet gateway vs NAT

Amazon vpc.