

ABSTRACT

In today network management becomes very important in the growth of computer-networks. An person is needed with critical skill and full knowledge of managing networks, His different thinking about network admin. Or admins ,that gives a best net environment .This environment is called IP Sub netting. This knowledge can be taken by various medium and terms of network management or sub netting. These are the individual views arise in the from of peoples are in the team of net. management. These cases shows different selected groups of members or network engineers. They are not complete, but summary of the level complicated of network finding paper discussion for why sub netting is important why we need sub netting IP add , decimal notation and binary notation conversion and sub netting. Internet Protocol Sub netting, network class ,Fixed Length Variable Mask, Subnet Length Subnet Mask ,CIDR, Advantages and disadvantages of FLSM ,VLSM ,Sub netting with Class A,B and C, Routing ,Switching , Network Securities

Contents

Sr. No..	Contents	Page No.
1.	Introduction	3
2.	Introduction To IP	3-6
3.	Decimal To Binary Conversion	6-7
4.	Subnet Mask	7-8
5.	CIDR/Super Netting	8-9
6.	Need Of Sub Netting & Methods	9-12
7.	Priority Bit	12
8.	Wild Card Mask	13
9.	Sub Netting With Classis	13-14
10.	Routing	15
11	Switching	`16-17
12.	Network Security	17-18
13.	Result	18
14.	Evaluation	18
15.	Abbreviations Used	19
17.	Preferences	19

Introduction

Sub Netting :-

This report proposal is based on the basic Sub netting .Sub netting is a term of IP addressing in which one large network is divided into some smaller subnets. In other words sharing ip addresses in a same network to different uses is called sub netting .The process of dividing a network into subparts is known as sub netting. Sub netting . The theory is called Sub netting .If an company or enterprise is large or Their system are more spreader then , it is an better sense to make network into smaller ones and attached routers. Another term after sub netting is the routing .Routing is for defining best and shortest path for route. There are many routing types and terms used for better communication. All of those terms are mention in this Proposal. This is for importance of sub netting , why we need sub netting and their methods or other terms .Sub netting is very use full and secure term in the computer networking . This allows to better management of IP's .

Literature Review

How Does Subnet Works :Subnet allows its connected devices to communicate with routers are used to communicate between the subnets. The size of an Subnet varies on the requirement needed in any network. A node to node subnet authenticate two devices to communicate each other .when a data subnet is designed for connect many systems or devices . Every org. is responsible for assign. the no. of the subnets and also its size .This size is within the limits of the address given for its use. In other words , the data of subnet in a enterprise remain local to that present enterprise.

Why Sub netting is important :-

1. **Reduce Network Traffic** –By sub netting we can divide network into as many smaller networks according to our need. This also helps to network traffic and hides toughness of the network.
2. **Optimize Performance** – Reduce in network traffic results in optimized network performance.
3. **Security** – Sub netting can helps to improve security .When exchange of information between computers on the same subnet while disabling authorization from other computer or subnet leads to network security.

Introduction To IP :-

Full Form of IP is Internet Protocol. It is a numbered address through which any system can be identified over the internet or a network .IP Address helps to share information between two systems or users . IP addresses is an internetworking address. This is The address to identify various Devices over any network is known as IP.IP maintain the addressing packets with multiple standards.

History of IP :-

The development of IP began from 1974 by Bob Kahn and Vint Cerf .This is generally using TCP/IP architecture. The First edition of the Internet Protocol came in 1983 in the ARPANET (Advance Research Project Agency Network). The 1st edition of the Internet, is Internet Protocol version 4 (IPv4).

IP Addresses :-

1.IPv4 :-The Length of the IPv4 is of 32 bits (4bytes) .The maximum value for 32 bits is $(2)^{32}$ or 4,29,49,67,296. So The maximum value for IPv4 address is 4.3 billion.

2.IPv6 :- This Version is also of 128 bits long. The range of this is 2 raise to power 128. The size of IPv6's address range space — 340 duo decillion — it is very high than IPv4

Classes of IP Address :-

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.

Types of IP Addressing :-

- 1. Static :-** A static IP address is that do not change after some time. If once static Ip is given to the device remain same until device is removed from network or other changes to the network. Static IP Add. are mainly used to servers of Enterprises or Company and also other devices.

Advantages :-

- **Good DNS :** Static IP add. are very easy to set up and communicate with DNS servers.
- **Server hosting :** If a user is hosting a Server then static IP address is best option for this .Static IP made easy for customers to locate a device through Domain Name Server (DNS). In simple to get websites and services of dns when they have a static IP address.
- **Remote access:** A static IP add. allows users to work from any location through the Virtual Private Network (VPN) / other remote login program like telnet.
- **Stability :** All the Static IP address are said to be stable until they are restricted from changes in a Network .It does not undergo frequent lapses similar to dynamic addressing. When the computer is rebooted , or restarted then it will get to same ip address that given by the network admin.

- **Accuracy :-** Static IP is highly accurate .It helpful for Teleconferencing and videoconferencing and also helpful for physical location of static device.

Disadvantages :-

- **Cost :-** Static IP is more costly . ISPs charge more form the users for static Ip address.
- **Security :-** Static IPs are insecure because hackers know about the static Ip address and where it is . So it is easier for them to attack on servers for stealing information.
- **Allocation :-** Through static ip device or system easily allocated or tracked by the Hackers .
- **Time :-** In static every device has to be addressed by the network admin . So this process takes more time than other . So ,this is an disadvantage of static IP address.

2. **Dynamic :-**Dynamic IP add. Given by the servers .Those servers are called DHCP (Dynamic Host Configuration Protocol). Dynamic ip address is not remain same as to static . Dynamic IP add. Are mainly given by the Internet Service Providers. Whenever it compared to the static IP addresses, dynamic IP addresses are temporary they change after some interval of time.When a system is removed or restarted then the system will get new ip from that network . .One of the main reasons behind is having dyna. IP add. is the requirement IP add. on IP version 4. Dyna. IP add. Allow single IP to be shuffled in many diff. ends to overcome that problem..

Advantages :-

- **Easy Automatic Configuration :-** Dynamic IP Addressing easy to use. The DHCP server automatically assigns IP address for devices attached to that network . DHCP assign IP's to devices according to their class and also their range.
- **Less Expensive :-** Dynamic IP addressing is less expensive as compared to staic IP addressing.
- **Lots of Ip Addressing :-** Dynamic Ip address allow to reuse ip address with in a network . When you attached a new device it will get new fresh new ip address.
- **Better Security :-** Dynamic addressing results better security. Because it provide every time new ip to a device. Through this it is impossible to find out device 's ip to attacker . this term leads to better security.
- **Physical Security :-** It's very tough for a monitor to find out exact location where you're . A VPN may be helpful for this as well.

Disadvantages :-

- **Not work well :-**Dynamic IP Address do not work well for hosted services like for a website or email server as DNS not work good with dyna. IP addr. because the address is shuffled.
- **Limit Remote Access :-** Dyna. IP Add. , this may limit your remote access as your program find errors in connecting. VPN programs can help you in this situation.

- **Interruption In Connection :-** In Some Condition ISP(Internet Service Provider) cannot be able to give you a dyna. IP add. and it will be results in interruption in your internet connections.
- **Less accuracy :-**Dynamic IP address gives you less accurate geo-location as it does not reflects your real-world location.

Types of IP :-

1. **Public :-** A public IP is and IP add. that accessed directly on the Internet. This address provided By ISP to router of organization. Through Public class ip address a user can share data and information through the internet. The scope of the public class ip is global .This is also used to communicate outside network. It is used to get access for using internet .To use Public class IP we need to pay some amount according to plans of ISP .The Management of Public IP is under the Internet Service Providers. The range of public IP beside Private IP rest are all public.

Private :- The private ip address is used to communicate with in a network. The scope of public IP is local. This ip is controlled by the network operator. This only work in a LAN .This ip is free of cost. Private ip is known by entering command in command prompt “ipconfig”.

Range of Pvt. IP Add. :- Class A -10.0.0.0 to 10.255.255.255

Class B - 17.16.0.0 to 17.31.255.255

Class C 192.168.0.0 to 192.168.255.255

Methods :-

Decimal And Binary Conversion :-

In IP Sub netting ,it is imp. to know about decimal and binary conversion .How IP Address and subnet mask is converted from decimal to binary form. Because 0s and 1s are most important according to their locations.

Let's. Take an example of a public class ip i.e. 172.16.10.15 and represent it into Binary form. The result will be 101011100.00010000.00001010.00001111. =\

Converting binary notation to decimal notation .if first octate example is taken .it look like this

Binary	$2^7=128$	$2^6=64$	$2^5=32$	$2^4=16$	$2^3=8$	$2^2=4$	$2^1=2$	$2^0=1$
IP Add.	1	0	1	0	1	1	0	0

Now according to the conversion of Binary we get $128+0+32+8+0+4 = 172$.

conversion from binary notation to decimal notation. Taking an e.g from above section . The below formula is given for conversion is as follows.

1. 1st Step of binary to decimal conversion is divide the number by 2
2. When division by 2 is done then remainder will be either 0 or 1.
3. Divide the number with our remainder and value will be 0 or 1.
4. Now write down the output Value to the left side of the last remaining value.
5. Loop this process until the output value is zero.

For 172,

the formula is given below :

When 172 is divided by 2 = 86c0

When 86 / 2 = 43 Value 0

When 43 / 2 = 21 Value 1

When 21 / 2 = 10 Value 1

When 10 / 2 = 5 Value 0

When 5 / 2 = 2 Value 1

When 2 / 2 = 1 Value 0

When 1 / 2 = 0 Value 1

Binary number for 172 = 10101100. Every part of IP add. having length of 8B long. In the last e.g. , The conversion up to 8B is accurate and easy to convert. If lesser no. is 12 it will get upto 0 before 8 bits. If this happens the remaining bit are filled with 0s.

Let's e.g. : when $12 \div 2 = 6$ remainder 0

$6 \div 2 = 3$ remainder 0

After division of six by two $3 \div 2 = 1$ remainder 1

Now, last step and we have output 1 is divided by 2 = 0 The output value is 1

We get zero value in just 4 steps, Hence, the remained bits are 0 — then the binary value of 12 is 00001100.

Sub net mask :- .This is a 32 bit value of IP add. to separate the network ID of the IP add. from the host ID . A subnet mask identifies the net. add. and the host add. .of any IP . They never displayed in the data packets on the internet. They takes values destination IP add. to match with a subnet . Subnet mask is of two types:

Default Subnet mask :- This is the mask reversed through the address class. Through Default mask We can create subnets according to our need.

E.g. - 255.255.255.0

Custom Subnet Mask :- This Mask can be expressed by admin. to accommodate multiple networks network.

E. g. - 255.255.255.254

Classis of Subnet mask

Class A- 11111111.00000000.00000000.00000000. 255.0.0.0

Class B- 11111111.11111111.00000000.00000000. 255.255.0.0

Class C- . 11111111.11111111.11111111.00000000. 255.255.255.0

1 Denotes For Network ID

0 Denotes For Host ID

Here are some special subnets given below:-

/24 is	used	in	the	local	networks	by	default.
/32 is	for	Loopback	and	System	interfaces.		
/31 is	used	on	point-to	–	point	connection	links over the network.
/30 is used by Service Provider for point-to-point connections.							

Subnet ID :- All subnet has own different network value called Subnet ID. Subnet Id is made through bits of the Host ID of the IP to the network part . The no of bits taken from the Host id leads to make subnets.

CIDR / Super netting – The full name of CIDR is Classless Inter Domain Routing. This is the way that ISP (Internet service providers) use to locate a no. of add. to a company . The officially development of CIDR or SUPPERNETTING in September 1993. CIDR also known as Super netting. Super netting is opponent to the Sub netting. Sub netting divides One large network into smaller subnets. But super netting make one large network form small Sub nets. Sol. for routing table problem is the temp. sol. to Internet add. space allocation . Anybody can't expect that an Growth of Internet and their appliances will leads to a network terrific impact. Proj.(RFC 1752) of the add. Use between 2k5 and 2k11 takes optimum solution that is IPv6 (128 bit). ISP arrange add. in a special block example 192.168.10.32/28. We recognize the subnet mask through the block size. The / sign shows no. of bits that are on .

e.g. a class C's mask 255.255.255.0 , which is means twenty four bits are for network part of other for sub nets.

The image given below shows notion of the subnets and their masks.

Subnet Mask	CIDR Value	Subnet Mask	CIDR Value
255.0.0.0	/8	255.255.240.0	/20
255.128.0.0	/9	255.255.248.0	/21
255.192.0.0	/10	255.255.252.0	/22
255.224.0.0	/11	255.255.254.0	/23
255.240.0.0	/12	255.255.255.0	/24
255.248.0.0	/13	255.255.255.128	/25
255.252.0.0	/14	255.255.255.192	/26
255.254.0.0	/15	255.255.255.224	/27
255.255.0.0	/16	255.255.255.240	/28
255.255.128.0	/17	255.255.255.248	/29
255.255.192.0	/18	255.255.255.252	/30
255.255.224.0	/19		

Need Of Sub netting :-

- When a company is using Two or more Different technologies (like Ethernet or token ring) in their different LAN Segments.
- When hosts dominating most of the LAN bandwidth need to be isolated.
- Breakdown network to decrease latency.
- Breakdown broadcast domain to reduce network congestion.
- To restrict Two network segments by distance limitations.
- To Reduce Network traffic .
- To reduce wastage of ip address in big network

Types of Sub netting :-

1.FLSM (Fixed Length Subnet Mask) /Class full Sub netting.

2.VLSM (Variable Length Subnet Mask) / Classless Sub netting.

Formula of dividing network based on requirement:

- Host part : $2^{(h-2)} = \text{req. add.}$ where h= no. of host bits .
- Network part : $2^{(n)} = \text{req. add.}$ where n=no of network bits.

Addressing format with network & host bits as

Class & Format	Network Bits (N)	Host Bits (H)
A: N/W.HOST.HOST.HOST	Eight	Twenty Four
B: N/W.N/W.HOST.HOST	Sixteen	Sixteen
C: N/W.N/W.N/W.HOST	Twenty Four	Eight

FLSM (Fixed Length Subnet Mask) /Class full Sub netting:-

This is define as class full sub netting that make sub parts of the network into the subnets .Where each part is same value .All the parts have equal numbers of hosts required .All the parts (subnets) have saved subnet mask. Fixed-length subnet masking does not use the entire subnet address space, the method is not sufficiently efficient. Therefore, the variable-length address method, variable-length subnet mask (VLSM), was developed, in which the subnet address space is adapted to the required subnet addresses. This method is an improvement on the original fixed-length subnet mask.

Mathematical calculation : -

Example. Calculate subnet mask using Host Bits , each having 12 hosts or nodes or devices. Also provide IP addresses of all devices. How many subnets available. Given network id as 199.1.1

Solution: Step I: Calculation of host bits For h host bits $2^{(h-2)} \geq \text{requirement}$

Here requirement=12

Hence h=4 as $2^{(h-2)}=16-2=14 \geq 12$

Hence host bits required is 4

Step II: Calculation of subnet mask Given class C address, which has format N.N.N.H or 11111111.11111111.11111111.00000000 (24 network bits & 8 host bits).

From the host bit calculation h=4, hence 4 Least Significant Bits are host bits & remaining 4 bits of are for network bits.

When arranging 11111111.11111111.11111111.11110000 24 Bits used for host part and 4 bits for network part , i.e is subnet mask for that network. This might be expressed as 28 n/w/4 host (N/W bits/host bits). Now changing the subnet mask to decimal notation , output value is 255.255.255.240.

Step III: Now cal. for number of sub-networks

No of networks=2 raise to power number of bits taken borrow from host bit = $2^{(8-4)}=2^4=16$ subnets.

Step IV: IP Range Given IP is 199.1.1 Range is equal to $2^4=16$ (group of 16 is one sub network) & every one have 16 users

199.1.1.0, 199.1.1.1, 199.1.2 up to 199.1.1.15

199.1.1.16,199.1.1.17 up to 199.1.1.31

199.1.1.32 up to 199.1.1.48

199.1.1.240, 199.1.1.241 up to 199.1.1.255

Network ID (here 199.1.1.0, 199.1.1.16.....199.1.1.240)

B/C ID (here 199.1.1.15, 199.1.1.31.....199.1.1.255)]

N/W ID & B/C ID are one type of reserved addressed .That cannot be assigned to any device in an network. IP's except board cast and network id all other are assigned to any device or user.

This subnet mask is for above ip address of class c 255.255.255.240.

Total devices or users for 16 subnets are $16*16-16*2=224$

VLSM (Variable Length Subnet Mask) / Classless Subnet. :-

This methods is also defined as classless method through which b big n/w divided into sub net using a unspecified class format .The value of every subnet is not same but little bit of difference .All the sub nets don't have same limit of the hosts parts some having more some having less .Also in case of subnet every host has different subnets sometimes more or some times less.. Variable Length Subnet Mask is designed to use a one mask of subnet in network .Which means one mask used w.r.t to their classis . It is used to increase the usage of variable length . It is known as the process of getting sub netting of a subnet.

Comparison Between VLSM and FLSM –

1. In Fixed length subnet mask sub netting (FLSM), all subnets are of same size .the values of those are approximetly same .But in VLSM it is opposite .
2. In FLSM Mamixm IP add. Are wasted but in VLSM maximum IP add. Are being used by some one.
3. FLSM is Best suitable for Private connection /IP and VLSM is for always public.

Mathematical Cal. (Variable Length Subnet Mask)

The length of Variable block

For example :- the no. of hosts as 100, 50 20 & 6. Find out IP add. & Sub. Mask with class C

Answer : For given 100 hosts: $2^{(h-2)}=100$,

H equal to 7 are (host bits)

The output value is adding 8 three times+ $(8-7)=25$

subnet mask 11111111.11111111.11111111.10000000 that is 255.255.255.128 Block size is $2^7=128$

the range is of IP add. 192.168.1.0/25 to 192.168.1.127/25 for given hosts

Now fifty hosts are given

$$2^{(h-2)}=50, h=6 \text{ (host bits)}$$

Now the output value is adding 8 three times $+(8-6)=26$

11111111.11111111.11111111.11000000 that is 255.255.255.192

Size Block is $2^{(6)}=64$ the range is 192.168.1.128/26 to 192.168.1.191/26

for fifty hosts

Ans :For Twenty hosts: 2 Raise to power h-2 is equal to 20

hence $h=5$ (host bits)

Now the output value is adding 8 three times $+(8-5)=27$

After that 11111111.11111111.11111111.11100000 that is 255.255.255.224

The size block is two raise to power 5=32

192.168.1.192/27 to 192.168.1.223/27 Twenty hosts

For six hosts: two raise to power h-2 is equal to 6,

Hosts is equal to 3\

Now the output value is adding 8 three times $+(8-3)=29$

11111111.11111111.11111111.11111000 that is 255.255.255.248

size $2^3=8$

Range is equal to

192.168.1.224/29 to 192.168.1.231/29 for 6 hosts

Here range of class c ip addresses given below :

For 100 host the range of ip address is 192.168.1.0/25 to 192.168.1.127/25

For 50 host the range of ip address is 192.168.1.128/26 to 192.168.1.191/26

For 20 hosts the range of ip address is 192.168.1.192/27 to 192.168.1.223/27

For 6 hosts the range of ip address is 192.168.1.224/29 to 192.168.1.231/29

Priority Bit :- The left most bit of the first octet of IP add. Is called priority bit..

Priority Bit For Class A :- In first octet of class A value of priority bit is always zero . Other Seven bits of first octet are for N/w part. Other 24 bits for host id.

Priority Bit For Class B:- Priority Bit of class b is -2. Network Address is represented by zero bits in host id part.

Priority Bit For Class C :- The priority bit for class C always **110**. The 21 bits are used for network ID. The 8 bits of host ID is used to find the host in any network.

Important formulas

2s – 2 formula:

- Class full routing method is also used for determining subnet.
- Routing Information Protocol version 1 is used to determine subnet
- Through configuration of no IP subnet-zero cmd. on the router helps to determine subnet.

2s formula

- In 2s formula classless routing and VLM is used for determine subnet.
- RIPv2, EIGRP or OSPF is used in 2s formula.
- Through configuration of IP subnet-zero command.

Wildcard Mask

A wildcard mask is a numbers of sequences that maintain packets in routing inside a network's subnets. Another name of wild card mask is Inverse mask. The reason behind this is that is not look like subnet mask which means , binary 1, is equal to a value, and binary 0 is null value However, in the wildcard mask, the opposite is true.

Sub netting With Class A :- The Class A network address is for govt. and MNC's for different hosts .The Class A is only 254 network addresses, it gives space approx. 17 million unique hosts. Subnet mask of class is 255.0.0.0 .First eight bits are for N/w add. and other 24 bits are for hosts .That remaining bits makes many subnet as per to their maximum limit of subnets or hosts.

Now the image given below shows the full module of class according to their network id or host id.

Class A Table :-				
Subnet	Subnet Mask	Effective Subnet	Number of Hosts	Number of Subnet
1	255.0.0.0	1	16777216	1
2	255.128.0.0	2	8388608	2
3	255.192.0.0	3	5592448	3
4	255.224.0.0	4	4194304	4
5	255.240.0.0	5	3980160	5
6	255.248.0.0	6	3801600	6
7	255.252.0.0	7	3642240	7
8	255.254.0.0	8	3498240	8
9	255.255.128.0	9	3368960	9
10	255.255.192.0	10	3252480	10
11	255.255.224.0	11	3157760	11
12	255.255.240.0	12	3080960	12
13	255.255.248.0	13	3016960	13
14	255.255.252.0	14	2964480	14
15	255.255.254.0	15	2922240	15

Figure shows: class A sub netting charts with max hosts and subnets.

Above image shows all the bits used for number of hosts borrowed from the portion .In class A maximum number of subnets and hosts for sub netting is 8388608.

Sub netting with class B IP add. :-

The class B IP add. is an numbered address having variable length of 32 bits. Whose first 16 bits are used for network id identification . Rest of other 16 bits are used for hosts id identification. Class B subnet mask 255.255.0.0 .Here 255 in this address are network id and 0 for host id. Now image given below shows the full detail of the Class B IP address sub netting.

Class B # bits	Mask	Effective Subnets	Effective Hosts
1	255.255.128.0	2	32766
2	255.255.192.0	4	16382
3	255.255.224.0	8	8190
4	255.255.240.0	16	4094
5	255.255.248.0	32	2046
6	255.255.252.0	64	1022
7	255.255.254.0	128	510
8	255.255.255.0	256	254
9	255.255.255.128	512	126
10	255.255.255.192	1024	62
11	255.255.255.224	2048	30
12	255.255.255.240	4096	14
13	255.255.255.248	8192	6
14	255.255.255.252	16384	2

Figure shows: class B Sub netting charts with max hosts and subnets.

The above image shows Class B sub netting Table .First column is for number of bits used. 2nd column shows subnet masks according to their bits used.3rd column is for effective subnets available and last row is for their hosts. Maximum number of subnets in class B is 16384 and maximum subnets are 32766.

Sub netting With Class C :-

The class C address is an numbered address having variable length of 32 bits. Whose first 24 bits are used for network id identification . Rest of other 8Bits for hosts id identification. The class B subnet mask is 255.255.255.0 .Here 255 in this address are network id and 0 for host id. In class C sub netting there is 6 bits available for use because first bit is for network address and last bit is for broadcast address. Now image given below shows the full detail of the class C IP address sub netting

Class C # bits	Mask	Effective Subnets	Effective Hosts
1	255.255.255.128	2	126
2	255.255.255.192	4	62
3	255.255.255.224	8	30
4	255.255.255.240	16	14
5	255.255.255.248	32	6
6	255.255.255.252	64	2

*Subnet all zeroes and all ones included. These might not be supported on some legacy systems.
 *Host all zeroes and all ones excluded.

Figure shows: class C Sub netting charts with max hosts and subnets.

Class c have maximum number of subnet is 64 and number of host is 126.

Sub netting Rules :

1. Minimum two bits must be borrowed
2. Minimum of 2 bits must be left over
3. We cannot use last created subnet because it is the broadcast address for that entire network.

Routing :- Routing is the process of the providing a route to our network system. According to the OSI model for networking routing works on the Network layer in that layer data is travel through data packets .Routing is term used for providing the best path to the transmission line or to the host. Routing selects a best path to communication .Routing checks route with less traffic and the shortest distance covered. Routing includes circuit switched network and public switched networks.

Types of Routing :- There is many types of routing terms used for data transmission are given below.

1.Static Routing :- Static routing the type of routing in which path is decided by the network admin. In this type of routing every path and their gateway are statically assigned by the network admin to the network. In this routing no special router is needed for selecting a route. Only admin is accessible for routing the network. No band width is used for the route.

Type of Static Routing :-

a).Default Static Route :- The default static routing is the type of static routing that matches all the data/IP packets .This route identify the IP address of that router to which sends all of the data packets and do not have static route.

b).Floating Static Route :- This route is also the type of static routing that is used for taking Backup for the static or dynamic route, during the failure of link. This route is used when primary route is unavailable. This route is configured with higher administrative distance than primary route.

c) Summary Static Routing :- This routing protocol works as an exit door when there is no any other router is important or available.

2 .Default Routing : - The default routing is term in which there is only one path for data transmission in a route. The data travels through next hop sub router or IP .No matter data packet from which router or which path. Every data packet is travel only through the given default router. This routing is based on the sub router routing. Sub router is used for next hop IP .

3. Dynamic Routing :- Dynamic Routing is used for automating adjustment of route in the routing table .In this type of routing router send data or gives best path according to the current situation. Dynamic Routing is also known as Adaptive Routing. Dynamic Routing allows different routes in an network.

Types of Dynamic Routing Protocols :-

1. RIP
2. OSPF
3. LSR
4. IGP
5. EIGRP
6. IGRP
7. ISIS

1.RIP :-Routing Information Protocol .This is type of distance vector routing .That shares all information with their routing table to every neighbor as routing-update message. Through RIP we can use configure hosts as the part of RIP. RIP shares full table of routing to all active interfaces in every half minute . Hop count of RIP is best way to remote access method. By default RIP has maximum number of hop count available is 15.

2. OSPF :- Full Form of OSPF is Open Shortest Path .This is a dynamic routing protocol that gives open and shortest path to the router or data packet to be transmitted. g OSPF. a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information. Unlike the RIP in which the entire routing table is sent.The host using OSPF sends only the part that has changed. With RIP, the routing table is sent to a neighbor host every 30 seconds

3.LSR :- (Link State Routing) In this routing every router shares its neighbor knowledge with every router in the internal network or internetwork.

4. IGP :- IGP stands for Interior Gateway Routing. IGP shares their routing table information in the network .

5. EIGRP :-Enhance Interior Gateway Routing Protocol allows exchange information more quickly and in a efficient way than other protocols.

6.IGRP :- Interior Gateway Routing Protocol is a routing protocol . That is used for managing the route flow of connected devices to the network. IGRP also deny routing loops by updating itself.

7. IS-IS :- This stands for Intermediate Systems to Intermediate Systems . This is the protocol used for moving information easily or in a efficiently way through same network or group of networks.

Switching

Switching is the process of selecting path for the direction of data or signal towards the destination address. This is forwarding process to specific points of a network . Layer-3 forwarding can occur in hardware because switch has cache traffic flows . Many older modular switches support Layer-3 route processors – this alone does not qualify as Layer-3 switching. Layer-2 and Layer-3 processors can act independently within a single switch chassis, with each packet requiring a route-table lookup on the route processor. Layer-3 switches leverage ASICs to perform Layer-3 forwarding in hardware. For the first packet of a particular traffic flow, the Layer-3 switch will perform a standard route-table lookup. This flow is then *cached* in hardware – which preserves required routing information, such as the destination network and the MAC address of the corresponding next-hop. Subsequent packets of that flow will bypass the route-table lookup, and will be forwarded based on the cached information, reducing latency. This concept is known as *route once, switch many*.

VLAN Switching: -VLAN is a concept of breaking down the large LAN network in small LAN networks of broadcast domain. Mainly VLAN is used to creates groups of computer for reduces traffic, and conflicts..

VTP(VLAN Trunking Protocol)- This is protocol used to share VLAN information. VTP used for reducing the admin.in a switched network. When VTP is configured on the VLAN then VTP self distributed to the all domains of that network .But it is very important to understand where you want to use VTP in a network. Through The VTP we can make changes to multiple devices centrally who are automatically attached to the network. Without VTP it is impossible to send information of VLAN to other switches.so VTP is important for sharing VLAN information to other VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.

Inter-VLAN :-Some time ago the VLAN was used where the two vlan was created and than these two vlan does not communicate to each other but can communicate with group users .So we want to get communicate to each other groups we can create it between sub dividing fast Ethernet port of router where it connected to switch. In intervlan we internally subdivided the router port. we can also communicate two vlans without intervlan but this method does not have more security

NETWORK SECURITIES

NAT (NETWORK ADDRESS TRANSLATION)

The network address translation is a technique that translate private class ip address with public class address .NAT provides a security to our internal network because it make our internal network hidden behind the public class ip address .NAT helps in protecting the depletion of IPV4 ip address .there are two type of NAT.

STATIC :-In static nat one to one mapping of ip address is done that is network admin has to allocate a different public class ip address for every host in the router. The static NAT provides the high security.

DYNAMIC :-In dynamic NAT we can create a pool of public class ip address.In our home router and our router randomly selects or translate internal network ip address with the address range define in a pool. Extend NAT provide the less security as compared to static nat.

Access Lists:-It is a fire wall that is configured on a router to filter the content of network access control list is consist of rules .That are applied on the home router and router every time checks the incoming and outgoing packets according to their condition.

There are two type of ACL

STANDARD ACL : - The value of access list is from one to ninety Nine, to create a standard access list. Standard access lists is implement on the Third layer . The source and destination address is known as logic criteria of the list. IP access lists uses source address only but work very moderately.

EXTENDED ACL :-The same rules are applied for every access List .Extended access decisions are taken at very high level of OSI Model it provides best controlling..

.

Result

As the result sub netting allows you to a simplified administration for your own network. Sub netting also improves the security of a network nobody can access that network until the part of that network. Also as result sub netting allows restricting of the ip's with the network .in simple words without affecting or going to other network

Evaluation

Sub netting in an IP network can be \used for many reasons. In an organization .There may be one large network and their users\ or hosts are more that that network .So to good and meaning full use of the network ,sub netting is used. To use of different physical media through the sub netting we can different physical media as per to our need .Sub netting allows us many subnets as ip address for those devices .sub netting is also used for preservation of the address space. When there is shortage of ip or maximum of IP's are used . Then for preserving some address to special purpose sub netting is used . The sub netting allows addresses as like a departmental .So for preservations sub netting is used. For secure connection , sub netting is more secure as compared to other addressing .Sub netting also controls network traffic .When we

use sub netting there is no need to new IP for every device .sub netting is part of on big network to small subnets. So this helps to reduce the network traffic.

Abbreviation's Used :

IP	–	Internet Protocol
Add.	–	Address
FLSM	-	Fixed Length Subnet Mask
VLSM	–	Variable Length Subnet Mask
CIDR	-	Classless Inter Domain Routing
LAN	–	Local Area Network
VPN	–	Virtual Private Network
ISP	–	Internet Service Provider
DHCP	–	Dynamic Host Configuration Protocol
DNS	–	Domain Name Server
NAT	-	Network Address Translation

References

1. <https://www.google.com>
2. <https://www.investopedia.com/>
3. <https://www.cisco.com>
4. <https://www.researchgate.net/>
5. <https://www.avast.com/>
6. Arihant Publications.Limited @arihantbooks.com
7. Loards Publications 36 Chandan Nagar ,Jalandhar city (PB)
8. Dhanpat Rai &Co.LTD. for Computer Networks.
9. Disha publication For www.dishapublication.com

