* Telnet Configuration Command *.

step1: Configure IP Address to router and Computer interface

```
(Config)# interface fastethernet 0/1
        # Ip address 192.168.10.1  255.255.255.0
```

step 2: Virtual line for concurrent terminal.

```
(Config)#  line vty  0  4
         # password  abc@123
         #     login
```

step 3: Configure enable password

```
        # enable secret  abc@123
```

step 4: Access Telnet from pc.

```
      telnet  192.168.10.1
```

* Configure DHCP server on Router *.

```
 # ip dhcp pool  dhcpserver
(dhcp-conf)# network  192.168.10.1  255.255.255.0
       # default-router  192.168.10.2  255.255.255.0
       #   exit
       # ip exclude-address   192.168.10.10  192.168.10.20
```

* Configure SSH Server

step1: Assign hostname to router.

```
    # hostname  Aniket
```

step2: Assign domain name to router

```
    # ip domain name  cdac.com
```

step 3: Generate RSA key pair.

```
      # crypto key generate rsa
                  or
    # crypto key generate rsa general-key modulus 1024
```

Page No. :
Date :

Step 4: Create local user and Assign password
username Admin Secret Cisco@123
Step 5: Apply SSH on VTY line
line vty 0 4
transport input SSh
login local
Step 6: Also Assign enable password.
enable password 123@abc.

Router and Routing Command.

interface fastethernet 0/0
ip address 192.168.10.1 255.255.255.0
exit
interface serial 0/1/1
* At DCE end give the clock rate
# clock rate 64000
* At every end give encapsulation type.
# encapsulation ppp
* To see routing table.
#Show ip route

* Static routing Command

ip route Dest N/w Dest SM Next hop (outgoing interface)

* Code for Routing Table.

1) C → Connected Network
2) L → Local interface ID
3) S → Static route
4) R → Routing Information Protocol
5) D → EIGR
6) O → OSPF
7) B → BGP.

* VLAN / VTP Server Configuration *

1) one broadcast domain to many i.e break the broadcast domain
2) VLAN To enhance security

Vlan 1 → Netive Vlan

Show Vlan brief

→ vlan is store under flash memory (vlan.dat).

Create Vlan

Vlan 10
name sales

Assign port to vlan

interface range fa 0/0-3
make port in access mode
Switchport mode access
* Assign port in respective vlan
# Switchport access vlan 10

* VTP server.

1) make one server by setting domain Name & Password

Vtp domain vtp_Server.
Vtp password 123
Vtp mode server/client/transpaket.
Show vtp status.
Show vtp couter
Show vtp password

TACACS+ - Terminal Access Controller Access Control System is also a Security server that's cisco proprietory and uses TCP including multiprotocol support

Authentication includes messaging support in addition to login and password function.

Authorization enables explicit control over user capabilities

Accounting supplies the detailed information about user activities

Configuration of TACACS+

aaa new-model

step 2) Configure host and key for TACACS+

tacacs-server host 10.0.0.1

tacacs-server key password

Step 3) create local user

username aniket password 123

Step 4) Add TACACS server to AAA group of any name

aaa authorization login cdac group tacacs+ local

Backup using TFTP Server

Step 1: Copy startup configuration to TFTP

```
# Copy startup-config tftp
```

address of server: 192.168.10.1

Destination file name: a-ro-config

Step 2: Recover Configuration from TFTP.

```
# Copy tftp running-config 192.168.10.1
```

Inter Vlan Routing

Step 1: Turn on the interface

```
# Interface fa 0/0
# no shutdown
```

Step 2: make the sub interfaces and encapsulate

```
# Interface fa 0/0.1
# encapsulation dot1q <Vlan-ID>
# ip address 10.0.0.1 255.0.0.0
```

* Access control list
  i) Used for filter traffic
  ii) To define intensity of traffic

* Two type of ACl

Standard access list: 1) These ACls use only the source ip address in an ip packet as the condition test. All decisions are made based on the source IP

2) This means that ACl list basically permit or deny an entire suite of protocol. They do not distinguish between any of the many type of IP traffic.

3) 0-99 number are for standard ACl.

Step 1 # access-list 10 deny/permit host/n/w
access-list 10 permit any

Step 2: Apply ACL to Interface of router.
interface fa 0/0
ip access-group 10. in/out
.

* Extended ACL : 1) They can evaluate source and destination, IP address, the protocol field in network layer header, and the port number at the transport layer header.
# 100-199 is extended acl #

Step 1: # access-list 150 deny icmp 10.0.0.0 0.255.255.255 host 20.0.0.2
access-list 150 permit any any

Step 2: Apply ACL to interface of router
Interface fa 0/0
ip access-group 150 in/out.

Named ACL are either standard or extended

* Inbound ACL: 1) When ACL is applied to inbound packet on an interface, those packet are processed through the access list before being routed to outbound interface
2) Any packet that are denied won't be routed because they are discarded before the routing process are invoked.

outbound ACL: 1) when the acl is applied to outbound packet on an interface, packet are routed to the outbound interface and then prossed through acl before being queued

* NAT (Network Address Translation)
is a also useful tool for network migration and mergers server load sharing, and creating virtual server.
1) when you need to connect to the internet and your host don't have globally unique IP address
2) when you need to merge two intranets with duplicate address.

Static (NAT) - allows one to one mapping between local and global address. (one to one)

Dynamic NAT - (many to many) ability to map local IP address to a globle ip address from pool of registred IP address.

Overloading (one to many) - Overloading really is a form dynamic NAT that map multiple private IP address. to a single public IP address. by using different source port. It also known as port address translation (PAT) also refered as NAT overload.

Page No. :
Date :

Static NAT configuration
#ip nat inside source static 10.0.0.1 172.16.0.2
Apply NAT To interfaces.
interface fa 0/0
ip nat inside
interface serial 0/0
#ip nat outside
check NAT Table
show ip nat translation

Dynamic NAT Translation
1) create pool of public IP address.
#ip nat pool mypool 10.0.0.4 10.0.0.8
netmask 255.255.255.0
2) Choose NAT Type
#ip nat inside source list 1 pool mypool
3) Apply NAT on interfaces.
#interface fa all
ip nat inside
4) Create a access-list.
access list 1 permit 20.0.0.1 0.0.0.255

PAT configuration
1) create pool which have same starting and end ip or use interface IP
ip nat inside source interface serial 0/0 overload.
2) Apply NAT on interface
3) create access list.

Page No.
Date :

* Spanning Tree protocol (STP) *

1) If the switches are in the loop in each every 2 second it sends BPDU (Bridge protocol Data unit) and give its mac address and its priority
2) Due to which switch communicates is not get over so it is in constinous move in the loop called broadcast storm.
3) To make communication we have to break the loop it get break by STP which is inbuild in switch
4) With the spanning tree protocol one redundant port is going to block in.
5) But thing is which switch port is going to block in multiple switch network and for this root bridge comes into focus.
6) root-bridge tell the other non-root switches either keep their port in blocking state or in forwarding state

* Root Bridge is selected by priority or by mac address.
* 32768 default priority
* the forwarding and blocking of port is decided by STP cost to reach root.
* we can set priority in increment of 4096.

show spanning-tree vlan 1
Spanning tree vlan 1 priority 8192
Spanning-tree vlan 1 root primary.

Page No. :
Date :

* Spanning-Tree port States

1) Disabled : A port in administratively disabled state doesn't participate in in frame forwarding or STP

2) Blocking : A Blocked port doesn't forward frame it just listen to BPDUS. The purpose of Blocking state is to prevent the use of loop path

3) Listening : This port listen to BPDU to make sure no loop occur on the network before passing data frames. A port in listening state prepares to forward data frames without populating the mac add table

4) Learning : The switch port listen to BPDU's and learn all the path in switched network
A port in learning state populates the mac address table but still doesn't forward data frame

5) forwarding : This port send and receive all data frames on switch port. If the port is still designated or root port at end of learning state it will enter the forwarding state.

* Types of Spanning tree protocol

IEEE 8021.d the original standard for switching and STP, which is really slow but requires very little switch resource. It also refered to as common Spanning tree

PVST+ (cisco default version) pre VLAN Spanning tree+ is the cisco proprietary enhancement for STP that provides seperate 802.1d Spanning tree instance for each VLAN.

IEEE 802.1w Also called Rapid Spanning tree protocol (RSTp), this iteration enhanced the BPDU exchanged and paved the way for much faster network convergence. but it will only allow for one root bridge per Network like CST

802.1s (MSTP) IEEE standard out as cisco proprietary MISTP. maps multiple VLAN's into the same ST instance to save the processing on switch. It's basically a Spanning tree protocol that rides on top of another spanning tree protocol.

Rapid PVST+ provides a seperate instance of 802.1w per VLAN. It gives us really fast convergence time and optimal traffic flow but predictably require the most CPU and memory of all.

Page No. :
Date :

* Ip Addresses And Subnetting

Class	Range	Subnet Mask
A	0 - 126	/8 255.0.0.0
B	128 - 191	/16 255.255.0.0
C	192 - 223	/24 255.255.255.0
D	224 - 229	used for multicasting
E	240 - 255	Research & Developmet

Note: 127 is reserved for loop back testing that mean for self testing NIC

IP Address has

- Network bits — on bit i.e 1
- Host bits — off bit i.e '0'

* Host-bit = 32 - Network bit
* Block Size = $2^{host\ bit}$
* valid IP = Block Size - 2

Find Network And Broad cast ID

Step 1: Convert IP to binary

Step 2: Convert Subnet into binary

Step 3: Perform ① & ② (Anding)
Get NID

p 4: After by using Subnet calculate Number of host and find BID

: If we to connect two router in a same network ben we have to use /30 subnet mask

① It has 30 N/w bit

② It has 2 host bit

Block size is 4 Vallid host is 2

* Private IP range *

Class A

10.0.0.0 - 10.255.255.255

Class B

172.16.0.0 - 172.31.255.255

Class C

192.168.0.0 - 192.168.0.0

Note → where the magic number the increment occur in that octet only.

Page No. :
Date :

Magic No	128	64	32	16	8	4	2	1
Borrow Bit	1	2	3	4	5	6	7	8
Subnet	128	192	224	240	248	252	254	255

* MAC Address

48 : 27 : 5A : B6 : CA : 8F

24 bit | 24 bit

Assigned by IEEE to identify vendor

Assinged to vendor and manufacturer.

* OUI (organisation of unique identification).

* ASIC → (Application Specific integrated circuit) which handle the building of mac table