**CCNA - Cisco Certified Network Associate**

**ROUTING & SWITCHING**

Different other levels

CCNA

CCNP - Cisco Certified Network Professional

CISSP - Certified Information System Security Professional

CCIE - Cisco Certified Internetwork Expert

OSI LAYERS

NETWORKING PROTOCOLS

IP ADDRESS

SUBNETTING

ROUTING

SWITCHING

VLAN

PORT SECURITY

ACL

NAT

DHCP,DNS

PAT

IPV6

FIREWALL

OSI LAYERS

* Open System Interconnect

Explains :

How data is transferred from source to destination and how data gets converted into different format before reaching the destination.

Function :

It is a universal standard which all manufacturers should follow in order to connect with the internet.

OSI - 7 layer and each layer has a device placed.

|  |  |  |  |
| --- | --- | --- | --- |
| LAYERS | DEVICES | ENCAPSULATION DATA | FUNCTIONS |
| APPLICATION | COMPUTER | DATA | In built system app or 3rd party apps |
| PRESENTATION | COMPUTER | DATA | Encryption/Decryption & Data Integrity |
| SESSION | COMPUTER | DATA | Authentication, Authorisation |
| TRANSPORT | CABLES | SEGMENTS | Segmentation, Flow Control, Error Control |
| NETWORK | ROUTER | PACKETS | IP Addressing, Path Determination |
| DATALINK | SWITCH | FRAMES | Mac Addressing, Multiplexing |
| PHYSICAL | NIC, HUB | BITS | Converting to 0’s and 1’s |

PACKET TRACER 4 or 5

**NETWORKING PROTOCOLS**

Protocols - set of rules for two computers to communicate with each other.

1. TCP/IP
2. UDP
3. DNS
4. DHCP

TCP/IP - TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL

UDP - USER DATAGRAM PROTOCOL

Normally, a computer communication happens in packets. All these packets are like courier packets with a from and to address.

These two protocols are responsible for two computer to communicate with each other.

|  |  |
| --- | --- |
| TCP | UDP |
| Will always check if the recipient is available or not. | Will not check |
| Will always expect an acknowledgement from the recipient | Will not expect |
| Will be slow | Will be fast |
| No data loss | Data loss will occur |
| It is called heavy weighted protocol | It is called light weighted protocol |
| Ex : normal browser communication | Ex: Whatsapp, voip calls. |

TCP FLAGS

RST - RESET

ACK - ACKNOWLEDGE

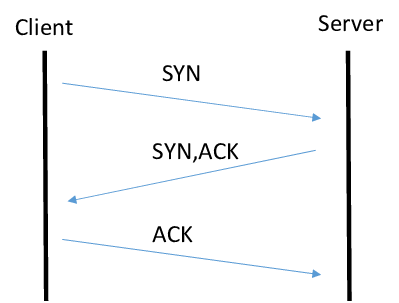
SYN - SYNCHRONIZE

FIN - FINISH

URG - URGENT

PSH - PUSH

TCP 3 WAY HANDSHAKE



TCP PORTS

Every protocol will have a port number assigned to it.

Range = 0 - 65535

HTTP : 80

**TODO Set of protocols with port numbers (commonly used 15)**

|  |  |
| --- | --- |
| **PROTOCOLS** | **PORT.NO** |
| FTP | 20/21 |
| SSH | 22 |
| TELNET | 23 |
| SMTP | 25 |
| DNS | 53 |
| DHCP | 67/68 |
| TFTP | 69 |
| HTTPS | 43 |
| POP3 | 110 |
| NTP | 123 |
| IMAP | 143 |
| SNMP | 161/162 |
| BGP | 179 |
| IPSec | 50,51 |
| TFTP | 69 |

**PORT NUMBERS WILL HAVE A PORT STATUS - OPEN OR CLOSED**

In case if the port is open, it will allow traffic. If not it will not allow traffic.

**TCP HEADER**

Source Port no | Destination Port No

SEQ NO | ACK NO

FLAG STATUS - RST | FIN | URG

Data

Options(any)

**IP ADDRESS - IPV4**

**IP - INTERNET PROTOCOL**

CONTENTS

1. IP RANGE
2. DECIMAL TO BINARY CONVERSIONS
3. WHY IP IS 32 BIT
4. WHY RANGE IS 255
5. CLASSES OF IP
6. SUBNET MASK
7. NID & BID
8. PRIVATE IP RANGE
9. DEFAULT SUBNET MASK
10. CALC OF NO OF N/W AND HOST PORTIONS

**IP RANGE**

IP Range is from 0 to 255

An IP looks something like 192.168.1.23

IP range starts from

0.0.0.0

0.0.0.1

0.0.0.2

.

.

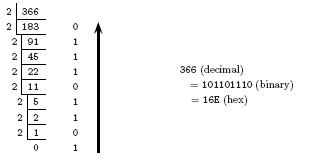
.

.

255.255.255.255

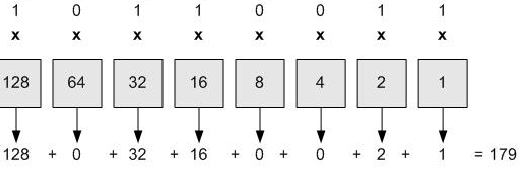
**DECIMAL TO BINARY CONVERSIONS**

366 is a decimal number which has to be converted to binary.



**BINARY TO DECIMAL CONVERSION**

10110011 is the binary number which has to be converted into decimal



**WHY IP IS 32 BIT?**

0.0.0.0 - 00000000.00000000.00000000.00000000

.

.

.

255.255.255.255 - 11111111.11111111.11111111.11111111

8 BITS 8BITS 8BITS 8BITS = 32 BITS

8 BITS = 1 OCTET, TOTAL 4 OCTETS WHICH IS 32 BITS. THIS IS WHY IP IS 32 BITS.

**WHY IP RANGE IS 255?**

Can we extend the range to 455, 855, 955

The maximum IP address which we can obtain using IPV4 is 4.2 billion

0.0.0.0

0,0,0,1

0.0.0.2

.

.

.

.

4.2 billion ip

Calculation - 2 power n

When 2 power 8 = 256

00000000

00000001

00000010

00000100

.

.

.

We take from 0 so range is 0-255

CLASSES OF IP

Important

CLASS RANGE

A 0 - 127

B 128 - 191

C 192 - 223

-------

D 224 - 239 MILITARY & RESERVED PURPOSE

E 240 -254 Reserved for Future uses and also R&D Process

CLASS A

0.0.0.0

0.0.0.1

.

127.255.255.255

CLASS B

128.0.0.0

128.0.0.1

.

.

191.255.255.255

CLASS C

192.0.0.0

192.0.0.1

.

.

223.255.255.255

Ex :

100.0.0.1 - A

132.10.0.2 - B

192.168.1.3 - C

**SUBNET MASK**

**Assgined to**

**CLASS A** Larger MNC **N.H.H.H**

**CLASS B** Midlevel comp **N.N.H.H**

**CLASS C** Small Comp & Home Users **N.N.N.H**

**Network and Host portion**

**\_ . \_ .\_ .\_**

Network portion means / related to network **N**

Host refers to computers **H**

**DEFAULT SUBNET MASK**

We have to assign the following

N = 255

H = 0

To get the default subnet mask for each class

**CLASS A N.H.H.H 255.0.0.0**

**CLASS B** N.N.H.H 255.255.0.0

**CLASS C** N.N.N.H 255.255.255.0

**NID & BID**

Network ID

Its like ur department name

Ex: Computer Science Department - It represents all the students studying in that department

Its the collective representation of all computers in ur network or lan - usually in IP

To find NID

1. Find class
2. Get number of network and host portions
3. Make host portions zero.

192.168.1.10

Class - C

SM - N.N.N.H

NID - 192.168.1.0 **FIRST IP ADDRESS**

DG - 192.168.1.1 **SECOND IP ADDRESS**

BID - 192.168.1.255 **LAST IP ADDRESS**

100.10.10.5

Class - A

SM - N.H.H.H

NID - 100.0.0.0

DG - 100.0.0.1

BID - 100.255.255.255

128.15.10.10

Class - B

SM - N.N.H.H

NID - 128.15.0.0

DG - 128.15.0.1

BID - 128.15.255.255

Broadcast ID

When we need to send a single msg to all the computers in our LAN. Then ill use broadcast ID

EX: 192.168.1.10 is my computer IP, then we can identify the following

192.168.1.0 - the first IP will be my NID

192.168.1.1 - the second IP will be my Default gateway IP / Modem IP / Router IP

192.168.1.255 - the last IP will be my BID

IMPORTANT

We cannot use/assign the above 3 IP address to any computer.

PRIVATE IP ADDRESS

Is Ip address UNIQUE ?

Private IP

Used only inside a LAN

When this IP goes out of LAN, it becomes invalid and it changes to public IP

Ex: INdia being our LAN, We use INR only inside INdia, when go abroad, we convert INR to USD.

We can view, edit, change

It is assigned by user or admin

Public IP

Used only outside a LAN

When this IP comes inside LAN, it becomes invalid and it changes to private IP

Ex: INdia being our LAN, We use INR only inside INdia, when go abroad, we convert INR to USD.

We can view but cannot edit, change

It is assigned by ISP (internet service provider)

CLASS Public IP Range Private IP

A 0.0.0.0 - 127.255.255.255 10.0.0.0 - 10.255.255.255

B 128.0.0.0 - 191.255.255.255 172.16.0.0 - 172.31.255.255

C 192.0.0.0 - 223.255.255.255 192.168.0.0- 192.168.255.255

Public IP is unique everywhere.

Private IP is unique inside a LAN but not between LAN.

CALCULATION OF NUMBER OF NETWORK AND HOST FOR EACH CLASS

EX: CLASS A uses more number of computers. - How Much?

CLASS priority bit (p)

A N.H.H.H 1

B N.N.H.H 2

C N,N,N,H 3

To find no of n/w = 2 power n-p

To find no of hosts = 2 power h and -2

A

NO of n/w = 2 power 8-1 = 127 n/w

No f host = 2 power 24 and -2 = 16777216 hosts

B Network 16384 Host 65536

C Network 2097152 Host 256

No of host = 2 power 8 and -2 = 254 hosts

**SUBNETTING**

1. IMPORTANCE OF SUBNET MASK
2. USES OF SUBNETTING
3. HOW SUBNETTING WORKS
4. SCENARIO 1, 2, 3

**IMPORTANCE OF SUBNET MASK**

192.168.1.2 - our computer

CLASS C

NID : 192.168.1.0 - A

DG : 192.168.1.1

PING - PACKET INTERNET GROPER

We are trying to ping another ip from our computer

PING 192.168.1.3

SWITCH - PERFORMS BOOLEAN AND’ING OPERATION.

DEST IP

192.168.1.3 11000000.10100000.00000001.00000011

SUB MASK

255.255.255.0 11111111.11111111.11111111.00000000

BOOLEAN AND 11000000.10100000.00000001.00000000

RESULT 192.168.1.0 - B

A=B, SWITCH DECIDES THAT PACKET BELONGS INSIDE LAN AND WILL NOT SEND IT TO ROUTER

A NOT EQUAL TO B, SWITCH DECIDES PACKET BELONGS TO ANOTHER LAN, SO IT WILL FORWARD IT TO THE ROUTER.

USES OF SUBNETTING

* TO MINIMIZE COST
* TO MINIMIZE IP WASTAGE

COMPANY - SALES, HR, DEVELOPERS, SUPPORT - 100, 200, 300, 400

HOME - DESKTOP,LAPTOP - 2 COMPUTER.

CLASS C = 254 -2 = 252 HOSTS WASTED.

THIS CAN BE PREVENTED BY SUBNETTING.

EX : 255.255.255.0 - 11111111.11111111.11111111.000000**00** - 2 COMPUTERS

111111 - CONVERTING TO N/W

11111111.11111111.11111111.11111100

255.255.255.248 - CUSTOM SUBNET MASK

**HOW SUBNETING WORKS**

IS THE PROCESS OF CALCULATING WASTED HOST BITS AND

CONVERTING THE WASTED HOST BIT TO NETWORK BITS.

**SCENARIO 1**

SALES - 120

HR - 120

**STEP 1 : TO FIND CLASS**

NO OF COMPUTERS = 120+120 = 240 < 254

WE CAN USE CLASS C

**STEP 2 : TO FIND ‘n’**

‘N’ - no of bits to be borrowed

2 power n >= Req No of Network

2 power n >= 2

n=0

2 power 0 = 1>=2 false

n=1

2 power 1 = 2>=2 true

n=1 (no of bits to borrow)

**STEP 3 : TO FIND CSM**

CLASS C

DSM - 255.255.255.0 - 11111111.11111111.11111111.**0**0000000

CSM - 11111111.11111111.11111111.10000000 - 255.255.255.128

**STEP 4 : CALCULATING NO OF N/W AND HOST**

NO OF N/W = 2 power n

NO OF HOST = 2 power h and -2

No of N/w = 2 power 1 = 2 network

No of Host = 2 power 7 and -2 = 128-2 = 126 hosts.

**STEP 5 : IP ASSIGNING**

A + B = C + 2 = D - 1 = E

SALES

192.168.1.0 -------------- 192.168.1.127

0 - A

126 - B

0+126 = 126 + 2 = 128 - 1 = 127

HR

192.168.1.128 ----------------192.168.1.255

128 - A

126 - B

128+126 = 254+2 = 256-1 + 255

**SCENARIO 2**

LAB 1 - 30

LAB 2 - 30

LAB 3 - 30

LAB 4 - 30

LAB 5 - 30

PACKET TRACER 4 OR 5

SCENARIO 1 & 2

* SAME COMPANY
* SAME NO OF HOSTS

WE FOUND ‘n’ - NO OF N/W TO BE BORROWED

In Scenario 3

* Different company
* Different no of hosts
* We need to find ‘h’

SBI - 120

HDFC - 30

ICICI - 60

HSBC - 30

SBI - 120

FIND CLASS

FIND ‘h’

2 power h and -2 >= Req no of host

FIND CSM

CALC NO OF N/W AND HOST

You will or you should get 2 networks and 126 hosts each

IP ASSIGNING

ICICI - 60

FIND CLASS

FIND ‘h’

FIND CSM

You will not take the default subnet mask, you will take the previous custom subnet mask and use the host bits and convert the remaining to network bits.

CALC NO OF N/W AND HOST

You will or you should get 2 networks and 62/60 hosts each

IP ASSIGNING

HSBC - 30

FIND CLASS

FIND ‘h’

FIND CSM

You will not take the default subnet mask, you will take the previous custom subnet mask and use the host bits and convert the remaining to network bits.

CALC NO OF N/W AND HOST

You will get 2 networks with 30 hosts each. You will use one 30 host for HSBC and other 30 host for hdfc

IP ASSIGNING

**ROUTER**

A. INTRODUCTION

B. ROUTER PORTS

C. ROUTER RULES

D. ROUTER MODES

E. ROUTER BASIC CONFIGURATION

INTRODUCTION

THE MAIN FUNCTION OF A ROUTER IS TO FIND THE BEST PATH.

WHAT DIFFERENCE DOES IT MAKE TO HAVE A ROUTER?

Bandwidth utilisation - We use router to use maximum of our bandwidth without any loss. If our internet speed is 10 mbps, we can use the maximum of that with router, and incase if we use a modem we will have loss.

Incase if we dont have a router, our isp will take care of routing needs.

ROUTER PORTS

**INTERFACE** - used to connect a router with other devices (router, Switch)

Ex:

-Ethernet interface - Old and Slow - Et

-Fast ethernet interface - Fast and new - Fe

-Gigabit ethernet interface - Very fast and advanced - Ge

All the above 3 will look the same. (RJ45 port), but differs in speed -

-Serial Interface

Used to connect two routers.

**LINE** - used to configure a router

Types of line

- Console port (CON)

used for direct configuration

- Auxiliary port (AUX)

used for remote configuration

C. ROUTER RULES

Rule 1 - All interfaces of a router should be in different network | should have different NID

Rule 2 - A serial interface connecting two routers should be in same network | should have same NID.

D. ROUTER MODES

Router Modes - User Mode, Previledge Mode, Global Configuration Mode

1.User Mode

**Router >**

Its just a login mode, we cannot configure anything in this mode.

To enter into next mode,

Router > enable or

Router > en

2.Previledge mode

**Router #**

This mode we cannot configure anything in router, but we can see what is already configured in router using SHOW command

We use this mode for Troubleshooting

In order to go to the next mode

Router # show ? / ? is for help, it wil display what possible commands can come after show

Router # show version

Router # show clock

Router # show vlan

To go to next mode

Router # configure terminal

Router # conf t

3.Global Configuration Mode

**Router(config) #**

All router configurations can be made in this mode.

TO DO

1. Assign password for USER MODE

2. Command to rename the NAME OF ROUTER

3. TELNET configuration for router

4. Router Basic Configuration

1. Assign password

router>en

type password:

router#

4. Basic Configuration

Router> enable

Router# configure terminal

Router(config)# Interface fastethernet 0/0

int fas

tab tab tab is to complete the command

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

Verify

PC 192.168.1.2

CMD

ping 192.168.1.1

reply from 192.168.1.1 / Configuration is right

Request timed out

Destination host unreachable / Error in configuration

**ROUTING**

Process of making two routers communicate with each other.

Or

Process of filling IP tables either manually or automatically.

TO DO

1. Create Template in Packet tracer with 3 routers

2. Identify Master and Slave end of Serial cable in packet tracer

3. Set Clock rate as "64000" for master end and "not set" for slave end

**TYPES OF ROUTING**

A. STATIC ROUTING

-Process of filling ip tables with UNKNOWN NID / NETWORKS.

-Configured for smaller networks

B. DYNAMIC ROUTING

-Process of filling ip tables with KNOWN NID / NETWORKS.

-Configured for larger networks

STATIC ROUTING

We need to enter Unknown network ids

When we configure static routing in router, we get the following options

Network - Network ID

Mask - Subnet Mask

Next Hop - IP address

TODO

1. Open template in packet tracer

2. Configure Static routing

3. Verify configuration

4. Save As - Static routing

DYNAMIC ROUTING

In dynamic we configure router with KNOWN NETWORK ID's

TYPES OF DYNAMIC ROUTING PROTOCOLS

A. DISTANCE VECTOR PROTOCOL

- RIP (Routing Information Protocol)

B. LINK STATE PROTOCOL

- OSPF (Open Shortest Path First)

C. ADVANCED DISTANCE VECTOR PROTOCOL

- EIGRP (Enhanced Interior Gateway Protocol)

-All the above routing protocols will identify best path differently.

-This is based on METRIC (based on what criteria best path is identified)

-Based on the purpose, we use any one of routing protocol

WORKING OF PROTOCOLS

RIP (Routing Information Protocol)

Metric - Hop Count

Best Path - Minimum Hop Count will be considered as best path.

Its an old protocol and not commonly used now a days due to false positive.

OSPF (Open Shortest Path First)

Metric - Bandwidth

Bandwidth is the channel width, (Like roadsize, bigger the road size faster we can travel) more the bandwidth, speed of internet will be more.

Best Path - Maximum Bandwidth is considered as best path

Used commonly for router configuration

EIGRP (Enhanced Interior Gateway Protocol)

Metric - Bandwidth & Delay

Delay is the time taken for the packet to reach the destination and come back.

Best Path - Maximum Bandwidth & Minimum delay is best path

Most commonly used routing protocol.

CONFIGURATION COMMANDS

RIP

#ROUTER RIP

#NETWORK (NETWORK ID)

EIGRP

#ROUTER EIGRP (AUTONOMOUS NUMBER)

#NETWORK (NETWORK ID)

OSPF

#ROUTER OSPF (PROCESS ID)

#NETWORK (NETWORK ID) (WILD CARD MASK) AREA (AREA NUMBER)

AUTONOMOUS NUMBER(EIGRP) / AREA NUMBER (OSPF)

-Both are numbers

-Number range is from 0 - 65535 (we can assign any number)

-It should be same for all 3 routers

-It is like STD code

PROCESS ID

-Its a number

-Number range is from 0 - 65535 (we can assign any number)

-It should be different for all 3 routers

-It is like Landline Number.

WILD CARD MASK

-It is inverse of ur subnet mask

Calculation

Global Subnet mask - 255.255.255.255

Default Subnet mask - 255.255.255.0 (-)

Wild card mask - 0 . 0 . 0. 255

TO DO

- Open Template

- Configure RIP

- Verify

- Save as Routing RIP

Repeat the same for OSPF and EIGRP

OSPF

ROUTER A

#ROUTER OSPF **PROCESSID(600)**  
#NETWORK 192.168.1.0 **WILDCARDMASK** **AREA 100**

#NETWORK 192.168.2.0 0.0.0.255 AREA 100

ROUTER B

#ROUTER OSPF 700

#NETWORK 192.168.2.0 0.0.0.255 AREA 100

#NETWORK 192.168.3.0 0.0.0.255 AREA 100

#NETWORK 192.168.4.0 0.0.0.255 AREA 100

ROUTER C

#ROUTER OSPF 800

#NETWORK 192.168.4.0 0.0.0.255 AREA 100

#NETWORK 192.168.5.0 0.0.0.255 AREA 100

EIGRP

ROUTER A

#ROUTER EIGRP 100(AUTONOMOUS NO)

#NETWORK 192.168.1.0

#nETWORK 192.168.2.0

ROUTER B

#ROUTER EIGRP 100

#NETWORK 192.168.2.0

#NETWORK 192.168.3.0

#NETWORK 192.168.4.0

ROUTER C

------------------------------------------------------------------------------

SWITCHING

-SWITCH PORTS

-SWITCH RULES

-SWITCH MODES

-BASIC CONFIG

SWITCH PORTS

-BASED ON FUNCTIONALITY

1. ACCESS PORT

-used for connecting a switch with another device(comp,router)

1. TRUNK PORT

-used to connect two switches

SWITCH RULES

* When you are trying to connect a switch to a router, you will connect in 0/1 to router’s 0/0 port.
* When you are trying to connect a switch with another switch, you will connect in 0/24 to another switch’s 0/1

SWITCH MODES

* Similar to router modes
* We have 24 port switch
* We have to assign the ports manually.

BASIC CONFIGURATION

#INTERFACE FASTETHERNET 0/2

#SWITCHPORT MODE ACCESS

#EXIT

If you have many ports that has to be assigned as access mode, then you can use the RANGE command

#INTERFACE RANGE FA0/1-20

#SWITCHPORT MODE ACCESS

#EXIT

---------------------------------------------------------------------------------

18-03-2020

VLAN - VIRTUAL LAN

Disadvantages of Subnetting

- its time consuming - when we have more number of computers

- it is configured at user end, so users can change the ip configuration of computers any time,. this is a security issue.

VLAN

- Subnetting depends on two factors - IP RANGE & CUSTOM SUBNET MASK

- vlan doesnt depend on both of these, because we configure the ports of a switch and not computers.

Steps to create VLAN

1. Create vlan name and number

2. Configure switch port - Access port / Trunk port

3. VLAN membership - link the port with created vlan

PACKET TRACER 1

Create two VLANs

SALES 100 & HR 200

SWITCH>EN

#SHOW VLAN

#CONF T

#VLAN 100 //STEP1

#NAME SALES //STEP1

#EXIT

#EXIT

#SHOW VLAN

#CONF T

#INTERFACE FA0/2 //STEP 2

#SWITCHPORT MODE ACCESS //STEP 2

#SWITCHPORT ACCESS VLAN 100 //STEP 3

#EXIT

#SHOW VLAN

Repeate the same for HR 200

Verify

PING

192.168.1.2 -- 192.168.1.3

No reply

PACKET TRACER 2

SWITCH 1:CREATE SALES(500),HR(600) AND MARKETING(700)

SWITCH 2:CREATE SALES(500),HR(600) AND MARKETING(700)

SWITCH 3:CREATE SALES(500),HR(600) AND MARKETING(700)

0/24 OF SWITCH 1

SWITCH>EN

#CONF T

#INT FA0/24

#SWITCHPORT MODE TRUNK

#SWITCHPORT TRUNK ALLOWED VLAN ALL

0/1 OF SWITCH 2

SWITCH>EN

#CONF T

#INT FA0/1

#SWITCHPORT MODE TRUNK

#SWITCHPORT TRUNK ALLOWED VLAN ALL

Verify

Ping from Sales of switch1 to sales of switch2

Sales of switch1 to hr of switch2

---------------------------------------------------------------

**PORT SECURITY**

Disadvantages of VLAN

When attacker computer from outside our LAN tries to connect to sales vlan 100 of switch 1, what will happen?

He will be able to connect and he can access all the documents of sales vlan, this is a security risk and port security is used to stop this.

- Port security assigns a particular mac address to a particular port.

- Only computer with that mac address can access that port.

- If a computer with different mac address tries to access, the port will be either blocked or shut down

Steps to configure PORT SECURITY

1. CHOOSE PORT/INTERFACE OF SWITCH

2. CONFIGURE PORT - ACCESS PORT / TRUNK PORT

3. ENTER PORT SECURITY CONFIGURATION

4. CHOOSE MAXIMUM NO OF COMPUTERS THAT CAN ACCESS THE PORT

5. ASSIGNING MAC ADDRESS - AUTOMATIC(STICKY) OR MANUAL

6. CONFIGURING VIOLATION RULE - RESTRICT,SHUTDOWN

RESTRICT - PACKET TRACER WILL KEEP THE PORT ON - GREEN, BUT ATTACKER WONT BE ABLE TO ACCESS ANYTHING FROM SALES VLAN

SHUTDOWN - PORT WILL BE DOWN, PACKET TRACER - RED

PACKET TRACER 1

#INT FA0/2

#SWITCHPORT MODE ACCESS

#SWITCHPORT PORT SECURITY

#SWITCHPORT PORT-SECURITY MAXIMUM 1

#SWITCHPORT PORT-SECURITY MAC ADDRESS STICKY

#SWITCHPORT PORT-SECURITY VIOLATION SHUTDOWN

VERIFY

REMOVE THE CONNECTION FROM 0/2, CONNECT A NEW COMPUTER TO 0/2,

PORT WILL TURN RED

------------------------------------------------------------------

**ACL - ACCESS CONTROL LIST**

It's a configuration done at router

It is used to control traffic of all computers in our lan

It permits / denies traffic based on the rules which we create.

TYPES OF ACL

A. STANDARD ACL

B. EXTENDED ACL

A. STANDARD ACL

- Its old and used in smaller networks

- It is permits / denies traffic based on "SOURCE IP ADDRESS"

- Configured close to "DESTINATION"

- Number Range 0 - 99

B. EXTENDED ACL

- Its new and used in larger networks

- It is permits / denies traffic based on

"SOURCE IP ADDRESS"

"DESTINATION IP ADDRESS"

"PROTOCOL"

"PORT NUMBER"

- Configured close to "SOURCE"

- Number Range 100 - 199

STEPS TO CONFIGURE ACL

1. ACL CREATION

2. SELECT AN INTERFACE

3. IMPLEMENTATION OF ACL

4. VERIFICATION OF ACL

STANDARD ACL CONFIGURATION

1.ACL CREATION

#ACCESS-LIST <NO>PERMIT/DENY <SOURCE IP><SOURCE WILDCARD MASK>

2.IMPLEMENTATION OF ACL

#INTERFACE<TYPE><NO>

#IP ACCESS-GROUP<NO> IN/OUT

3.VERIFICATION OF ACL

#SHOW IP ACCESS-LIST

4.VERIFICATION-IMPLEMENTATION OF ACL

#SHOW IP INTERFACE <TYPE><NO>

router A,

#access-list 10 deny 192.168.3.2 0.0.0.0

#interface fast ethernet 0/0

ip access-group 10 in

verify

3.2 - > 1.2 ping

NOTE -

WILD CARD MASK FOR ACL WILL HAVE THE FOLLOWING CRITERIA

NORMAL WILD CARD MASK WILL BE THE INVERSE OF UR SUBNET MASK

BUT HERE WE HAVE TWO SCENARIOS

SCENARIO 1 - WHEN WE CONFIGURE FOR A SINGLE HOST / IP

i.e 192.168.1.2, then Wild card mask will be all zeros 0.0.0.0

SCENARIO 2 - WHEN WE CONFIGURE FOR A ENTIRE NETWORK

i.e 192.168.1.0, then Wild card mask will be 0.0.0.255

WHEN IMPLEMENTING ACL , WE HAVE TWO OPTIONS

IN & OUT

IN blocks the incoming traffic

OUT block the outgoing traffic

THE OUTPUT VARIES LIKE BELOW WHEN WE PING

IN :REQUEST TIMEOUT

OUT :DESTINATION HOST UNREACHABLE

-----------------------------------

EXTENDED ACL

ACL CREATION

#ACCESS-LIST <NO>PERMIT/DENY<PROTOCOL><SOURCE IP><SOURCE WILDCARD MASK><DESTINATION IP><DESTINATION WILDCARD MASK><OPERATOR><PORT NO>

IMPLEMENTATION OF ACL

#INT <TYPE><NO>

#IP ACCESS-GROUP <NO>IN/OUT

Note:

1. More specific statements should be at top

2. More generic statements should be at bottom

access-list 110 permit 192.168.1.2 .......... (1)

access-list 110 deny 192.168.1.0 ....... (2)

The above statement will permit only 1.2 and deny all other computers

access-list 110 deny 192.168.1.0 ....... (2)

access-list 110 permit 192.168.1.2 .......... (1)

The above statement will deny all computers including 1.2,

so statement number (2) will not work.

**BGP - BORDER GATEWAY PROTOCOL**

THIS COMES UNDER EGP - EXTERIOR GATEWAY PROTOCOL

IN CCNA WE SAW IGP - INTERIOR GATEWAY PROTOCOL, AND THAT'S THE REASON WHEN WE CONFIGURED 3 ROUTERS, THE AUTONOMOUS NUMBER FOR THE THREE ROUTERS WERE SAME, BECAUSE IGP WILL ONLY CONFIGURE ROUTERS IN SAME AREA.

WHEREAS BGP CAN PROVIDE ROUTING TO ROUTERS WITH DIFFERENT AUTONOMOUS NUMBER.

CONFIGURATION

ROUTER A

#ROUTER BGP (AUT NO- A)

#NETWORK (NID)

#NEIGHBOR (NEXT HOP IP ADDRESS) REMOTE-AS (REMOTE ROUTER AUT NO- B)

**DHCP - DYNAMIC HOST CONFIGURATION PROTOCOL**

if we need to change ip of our computer

adapter settings - ip configuration

0r ncpa.cpl

A. obtain automatically - Dynamic

B. use the below ip - Static

If we go for the first option A. and save the config and restart ur computer.

When computer restarts and login, whether ur computer will have ip assigned or not. NO

IP will be assigned only after completion of DORA Process

How to access ur wifi modem from ur computer?

ur computer ip is 192.168.1.2

ur modem ip is 192.168.1.1

from ur computer browser, give the ip of ur modem and login

Login to any modem and check the following

1. DHCP SERVER - on / off

dhcp scope - 192.168.1.\_ to 192.168.1.\_

dhcp lease time

dhcp reservations

Lease time is the time period for which a particular mac address is linked to an ip address. usually in minutes.

Scenario 1 - we have 50 ip in our dhcp server.our lan has 10 computers

our comp ip is 192.168.1.8, even if our lease time expires, we will have the same ip assigned

Scenario 2 - suddenly our lan has 45 computer logged in.and our comp is powered off(192.168.1.8), now when we power on our computer, even if lease time is not over, our ip will change.

incase if u want to change ip manually, use the following commmand

> ipconfig /release

> ipconfig /renew

DHCP Reservations - reserving ip for special computers or servers

if we have 2 servers, for which we dont want the ip to change.

hence ill choose my reservation range in my dhcp server

Reservation range - 192.168.1.1 - 192.168.1.3

so the first computer wil get 192.168.1.4.

Wireless Options

SSID

BSSID

FREQUENCY

CHANNEL

SECURITY - WEP, WPA, WPA2

AUTHENTICATION - AES, TKIP

ADMIN / MAINTENACE

find option to change default username and password for modem

(admin - admin, admin - password, admin - )

**PAT - PORT ADDRESS TRANSLATION**

- COMMONLY KNOWN AS "NAT OVERLOAD"

- IT IS MAPPING MANY INTERNAL LAN COMPUTERS PRIVATE IP TO A SINGLE PUBLIC IP ADDRESS, BUT USING DIFFERENT PORT NUMBERS.

- IT IS ONE WAY OF IMPLEMENTING NAT

- 3 WAYS OF IMPLEMENTING NAT

- PAT

- POOLED NAT

- STATIC NAT

- EACH INTERNAL LAN COMPUTER(PRIVATE IP) WILL HAVE A SINGLE IP ADDRESS(PUBLIC IP) MAPPED BUT USES DIFFERENT PORTS TO DIFFERENTIATE EACH SESSION

- NAT CONFIGURATION DEFINES WHICH IP SHOULD RESPOND WHEN SOMEONE PINGS TO A SERVER (EX: WHEN WE PING GOOGLE.COM, GOOGLE.CO.IN RESPONDS)

- PAT CONFIGURATION DEFINES WHICH IP SHOULD BE SHOWN WHEN WE PING TO ANY COMPUTER OR SERVER (EX: WHEN WE PING GOOGLE.COM, PRIVATE IP WILL BE MASKED AND PUBLIC IP WILL BE DISPLAYED TO GOOGLE SERVER)

**CONFIGURATION**

1. CONFIGURE IP TO ROUTERS & COMPUTERS

2. CONFIGURE ROUTING

3. CONFIGURE TELNET TO 2 ROUTERS

4. CONFIGURE GENERAL NAT IN ROUTERS

5. CREATE NAT POOL

6. CREATE ACL

7. APPLY NAT RULE

8. VERIFY

**-CONFIGURE TELNET TO ROUTERS**

ROUTER A & B

ROUTER(CONFIG)#LINE VTY 0 4

verify from pc

telnet 192.168.1.1

router>

**-CONFIGURE GENERAL NAT IN ROUTERS**

ROUTER A

#INTERFACE FASTETHERNET 0/0

#IP NAT INSIDE

#EXIT

#INTERFACE SERIAL 0/0/0

#IP NAT OUTSIDE

#EXIT

**-CREATE NAT POOL**

#IP NAT POOL TEST 20.0.0.1 20.0.0.1 NETMASK 255.0.0.0

TEST is the name of NAT POOL

and since we have only one router, our NAT POOL RANGE will be 20.0.0.1 to 20.0.0.1

**-CREATE ACL (STD)**

#ACCESS-LIST 10 PERMIT 10.0.0.0 0.255.255.255

**-APPLY NAT RULE**

in order to create NAT rule we need two things to be configured

NAT POOL

ACL

#IP NAT INSIDE SOURCE LIST 10 POOL TEST OVERLOAD

**-VERIFY**

FROM COMPUTER 10.0.0.2

> TELNET 20.0.0.2 /IT WILL LOGIN TO ROUTER B

ROUTER> ENABLE

ROUTER# SHOW USER /IT WILL NOT DISPLAY 10.0.0.2 IP

GO TO ROUTER A

ROUTER# SHOW IP NAT TRANSLATIONS

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

FIREWALL

Security Device - Both Hardware & Software

Implements all the configurations of Router & Switch.

1. HARDWARE FIREWALL MANUFACTURERS

2. STATEFUL & STATELESS FIREWALL

3. CISCO ASA FIREWALL

4. CISCO ASA MODELS

5. FIREWALL RULES

6. KEY POINTS OF CISCO ASA

7. CONFIGURATION STEPS

1. HARDWARE FIREWALLS MANUFACTURERS

Different Firewall manufacturers are as follows

-Check Point.

-FortiGate.

-Palo Alto Networks.

-WatchGuard.

-Seqrite Firewall.

-Cisco Asa Firepower.

-Cisco PIX.

-Mcafee Firewall.

2. STATEFUL & STATELESS FIREWALL

3.CISCO ASA FIREWALL

ASA - Adaptive Security Appliance

-Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, virtual private network (VPN) & SSL capabilities.

4.CISCO ASA MODELS

ASA models are all in the 5500 series

The ASA 5500 series has the following models:

Cisco ASA 5505 // We will configure this in Packet Tracer

Cisco ASA 5510

Cisco ASA 5520

Cisco ASA 5525-X

Cisco ASA 5540

Cisco ASA 5550

Cisco ASA 5580-20

Cisco ASA 5580-40

5.FIREWALL RULES

- Inbound Rules

- Outbound Rules

6.KEY POINTS OF CISCO ASA

1. We cant assign ip directly to any interface of a firewall

2. we have to assign ip to the vlan and then link the vlan to any interface. so the ip gets indirectly assigned to the interface

3. INSIDE network is inside ur LAN

4. OUTSIDE network will be out of LAN

5. VLAN 1 will always be linked with INSIDE network

6. VLAN 2 will always be linked with OUTSIDE network

7. Security level of INSIDE network will be 100 and OUTSIDE will be 0.

8. Ethernet 0/1 of firewall wil be assigned to VLAN 1

9. Ethernet 0/0 of firewall wil be assigned to VLAN 2

7. CONFIGURATION STEPS

--------------------------------------------------------

STEPS TO CONFIGURE FIREWALL

STEP 1 - REMOVE DEFAULT IP ADDRESS AND DHCP SCOPE RANGE

STEP 2 - ASSIGN IP,NAME AND SECURITY LEVEL TO VLAN 1 & 2

STEP 3 - LINK CORRESPONDING VLAN 1& 2 WITH THE RESPECTIVE INTERFACE

STEP 4 - CONFIGURE DHCP & DNS SERVER

STEP 5 - CONFIGURE DEFAULT ROUTE

STEP 6 - OBJECT NETWORK CREATION & ENABLING NAT

STEP 7 - CREATE ACCESS CONTROL LIST

---------------------------------------------------------

STEP 1 - REMOVE DEFAULT IP ADDRESS AND DHCP SCOPE RANGE

ciscoasa(config)#interface vlan 1

ciscoasa(config-if)#no ip address

ciscoasa(config-if)#exit

ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.35 inside

(We can find this using SHOW command

SHOW RUNNING-CONFIG)

------------------------------------------------------------

STEP 2 - ASSIGN IP,NAME AND SECURITY LEVEL TO VLAN 1 & 2

ciscoasa(config)#interface vlan 1

ciscoasa(config-if)#ip address 172.16.1.1 255.255.255.0

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#nameif inside

ciscoasa(config-if)#security-level 100

ciscoasa(config)#interface vlan 2

ciscoasa(config-if)#ip address 210.2.2.2 255.255.255.0

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#nameif outside

ciscoasa(config-if)#security-level 0

----------------------------------------------------------------

STEP 3 - LINK CORRESPONDING VLAN 1& 2 WITH THE RESPECTIVE INTERFACE

ciscoasa(config)#interface ethernet 0/1

ciscoasa(config-if)#switchport access vlan 1

ciscoasa(config-if)#exit

ciscoasa(config)#interface ethernet 0/0

ciscoasa(config-if)#switchport access vlan 2

----------------------------------------------------------------

STEP 4 - CONFIGURE DHCP & DNS SERVER

we can give dhcp range as much as we want, here we give 6 ip's

starting from 1.5 to 1.10

ciscoasa(config)#dhcpd address 172.16.1.5-172.16.1.10 inside

ciscoasa(config)#dhcpd dns 20.20.20.2 interface inside

The above command allows all the computer from inside network to communicate with the DNS server

----------------------------------------------------------------

STEP 5 - CONFIGURE DEFAULT ROUTE

The command will let the firewall communicate with the outside network. 0.0.0.0 means any source ip can communicate with any destination ip through router ip 210.2.2.1

ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 210.2.2.1

----------------------------------------------------------------

STEP 6 - OBJECT NETWORK CREATION & ENABLING NAT

This will allow the INSIDE network to communicate with OUTSIDE network (& vice versa) with the public ip address

ciscoasa(config)#object network LAN

ciscoasa(config-network-object)#subnet 172.16.1.0 255.255.255.0

ciscoasa(config-network-object)#nat (inside,outside) dynamic interface

----------------------------------------------------------------

STEP 7 - CREATE ACCESS CONTROL LIST

This is the EXTENDED NAMED ACL (3rd type of ACL, apart from Standard & extended ACL) where we use Alphabets instead of Number.

This ACL will allow both TCP and ICMP traffic to be allowed in outside network

ciscoasa(config)#access-list inside\_to\_internet extended permit tcp any any

ciscoasa(config)#access-list inside\_to\_internet extended permit icmp any any

ciscoasa(config)#access-group inside\_to\_internet in interface outside

----------------------------------------------------------------

STEP 8 - STEPS TO CONFIGURE ROUTER

ASSIGN IP ADDRESS TO ROUTER

Configure OSPF for ISP Router

Router(config)#router ospf 1

Router(config-router)#network 210.2.2.0 0.0.0.255 area 0

Router(config-router)#network 20.20.20.0 0.0.0.255 area 0

----------------------------------------------------------------

VERIFY

1.Change ip of computers from inside network to Dynamic

2.Ip should be automatically assigned by firewall.

Ex: 172.16.1.5

3. Now ping from 172.16.1.5 to 20.20.20.2 (DNS Server)

we should get reply.