THE GOSPEL ACORDING TO CHALE

Charles Milton Hale <-- very cool guy

Dan Courses – Cisco Practice

CISCO DEV NET IS VERY VERY GOOD

WRITE STUFF DOWN

https://networkproguide.com/cidr-subnet-mask-ipv4-cheat-ssheet/

To start using the router or whatever your doing, you must type “enable” without quotes.

Network – a group of PC’s connected together. Different networks are on oa different sides of the router.

Ethernet Cable – connects the PC’s together physically (The blue cable)

Switch – PC's connect to the switch through ethernet cables.

A group of switch's can connect to a router. Switch’s deal with the I.P’s. (Internet Protocol) address while router deal with a M.A.C (Media access control)

Ethernet Cable plugs into the switch. The main purpose of the switch is so the PC’s can talk.

C.L.I - command line interface (this is where you put the code but in Cisco.)

Conf t – this code is short for “configure global” This means that you can configure the router, switch, PC whatever, it can be changed. This is critical to Cisco.

When dealing with the native vlan, (ex vlan 99), go to its sub interface or interfcae and type the following command,

“encapsulation do 99 native”

Subnetting – Small networks below larger networks

Netting-networking

Sub-below

Bit- 0 or a 1

Binary starts at 2 to the 0 power (right to left)

ACL – ACCESS CONTROL LIST : iT EITHER PREMITS OR DENYS A NEWTWOKRS TRAFFIC

2 TYPES OF ACLS. STANDARD IS 0-99, EXTENDED IS 100-INFINATE

Standard acls only take source address

“SHIFT ?”!!! This means that you can see what your next move is. It shows the commands that you can do at that time. F

When you want to see what you are configuring, you go to options at the top left, preferences, always show port labels.

Command – tells the CLI what to do. The first word that you type. (Ip, conf t, etc.)

Sub-command – the stuff that you type after the command. (address, Gig0/1. Etc.)

Subnet Mask – it helps the router to differentiate where to send the data. One subnet can contain multiple I.P address, so the router can figure out what group to send the data to.

“<cr>” - meanFs that the command is complete, and you can’t do anymore.

How to save – do write mem -> copy run start ->

RED MEANS BAD!

GREEN MEANS GOOD!

YELLOW MEANS KINDA!

HOW TO CONFIG/ASSIGN AN IP!!

1.enable

2.conf t

3.interface Gig0/1 (Or whatever you need to configure)

4.ip address “IP” “SUBNET”

5. No shutdown

6.exit

Info gets to one place to another by I.P address

Default gateway – where a device sends something if it does not know where to put it]

It checks if you are directly connected to the PC, if not, it will send it to a gateway and 9 times out of 10 it will be a router.

Routing table – It shows all the possible routers/routes that it can take. If not, it will take the default static route.

What does passive interface do - it sets it so that no ospf traffic is sent down that interface.

Default static route – Always is at the bottom of the routing table. You would make the destination IP and the Subnet mask 0.0.0.0 0.0.0.0 (next hop).

OSPF tells the router the shortest way to send something there, and then packets can flow through.

Do not send all your data to the sever.

Network Address = 172.16.8.**0**

First Usable Address = 172.16.8.**1**

Last Usable Address = 172.16.8.**254**

Broadcast Address = 172.16.8.**255**

HOW TO ASSIGN A DEFAULT GATEWAY

1.enable

2.conf t

3.ip default-gateway (enter the address)

https://learningnetwork.cisco.com/thread/46034

For more help check out the URL

ASSIGN IPS

1.go to the PC

2.desktop

3.Ip Configuration

Bit – a small unit of data; can be 1 or 0.

11111111.11111111.11111111.11111111

That is a basic I.P in binary. You solve that by added power of two.

128 64 32 16 8 4 2 1, that would be the first section of numbers.

Ping - very common method for troubleshooting the accessibility of devices. It uses a series of Internet Control Message Protocol (ICMP) Echo messages to determine: Whether a remote host is active or inactive. The round-trip delay in communicating with the host.

MOTD – message of the day

What is the difference between “show run” and “do show run”?

The difference is that “show run” is before conf t and “do show run” is after conf t.

VLAN 1 – Virtual LAN

SHH – a secure shell to access your switch remotely

RSA – a crypto system that takes data and cyphers it for transport and then decrypt it.

If it ever asks you for RSA keys, say 1024

The Purpose of RIP is to send everything, everywhere inside of the network

Always do no router rip unless it says to configure rip

CREATE USER

1. Enable
2. Conf t
3. Username _____ password _____

HOW TO ADD A VTY PASSWORD

1. Enable
2. Conf t
3. Line vty 0 15

ADD VTY LINES

1. Enable
2. Conf t
3. line vty _____ - _____
4. Transport input _____

MANAGEMENT INTERFACE ADDRESSING

1. Enable
2. Conf t
3. INT _____ (interface)
4. Ip address _____ (IP) _____ (subnet mask)
5. No shutdown

6. Exit

HOW TO GET HOST NAME

1.enable

2.conf t

3. hostname ____

HOW TO ADD BANNER

1. Enable
2. Conf t
3. Banner motd %
4. Warning %

HOW TO ADD CONSOLE PASSWORD

1. Enable
2. Conf tF
3. Line con 0
4. Password _____ (cisco)
5. Login

(THAT ADDS CONSOLE LINE)

auto-summary is what tells v2 that it can use other subnets than 8,16, etc

Do auto-summary unless told not to

HOW TO DO RIP V2

1. Enable
2. Conf t
3. Router rip
4. Veriosn 2

Console line – a line that adds to the console

HOW TO ADD A SECRET (encrypted password)

1. Enable
2. Conf t
3. Enable secret _____ (whatever its going to be) (class)

ENCRYPT PLAIN TEXT PASSWORDS

1. Enable
2. Conf t
3. Service password-encryption

ADD DOMAIN NAME

1. Enable
2. Conf t
3. Ip domain name _____(Whatever)

Before you enable SSH, you have to enable RSA

HOW TO DENY/BAN/NO ADD AN NETWORK THROUGH ACL

1. Enable
2. Conf t
3. Ip access-list extended _____ (name
4. Deny ip _____ (source address) (this is the port that it asks for.) On the ACL lab, it asks for g0/0. SPLIT Ip address of the port that it asks for.) _____ (wildcard) _____ (the ip of the thing that it asks for. Like the server.) host _____ (the thing that it wants you to go to)

HOW TO ASSIGN AN ACL ACCESS LIST TO A PORT

1. Enable
2. Conf t
3. Int (this is the interface of the incoming traffic of the router that is going into the thing that you made the list for.) int the ACL lab it is g0/0
4. Ip access-list HQServer in

HOW TO ADD AN ACL

1. Enable
2. Conf t
3. Ip access-list exteneded _____ (the name of what it wants you to be)

HOW TO PREVENT ANY COMPUTERS ATTACHED TO A PORT FROM ACCESSING THINGS

1. Enbale
2. Conf t
3. Ip access-list exteneded _____(the name)
4. Deny tcp (the network

HOW TO CREATE RSA

1. Enable
2. Conf t
3. Crypto key generate RSA
4. However many bits is in that system or version of SSH (version 2 has 768 bits)

HOW TO ENABLE SSH

1. Enable
2. Conf t
3. Ip SSH version 2 (1024 unless told otherwise)

HOW TO DISABLE ALL UNUSED PORTS

1.enable

2. conf t

3.int range F0/3-24 (or whatever ports that you have to disable)

4.shutdown

HOW TO SWITCH PORT TO ACCESS

1. Enable
2. Conf t
3. Int ____ (What ever is connected to the switch)
4. Switchport mode access

HOW TO SET INTERFACE MODE TO ACCESS

1. Enable
2. Conf t
3. Int range (ex. F0/1-24 – the ports that want to access.)
4. Switchport mode access

HOW TO ENABLE PORT SECURITY

1. Enable
2. Conf t
3. Int _____
4. Switchport port-security

HOW TO ENABLE PORT SECURITY FOR TWO HOSTS PER PORT

1. Enable
2. Conf t
3. Int _____
4. Switchport port-security max _ (whatever number you want)

HOW TO RECORD THE MAC ADDRESS

1. Enable
2. Conf t
3. Int _____
4. Switchport port-security mac-address sticky

HOW TO SET MAX AMOUNT OF DEVICES ON MAC ADDRESS

1. En
2. Conf t

3. Int _____
4. Switchport port-security maximum ___

HOW TO ENSURE THAT PORT VIOLATIONS DISABLE PORTS (Secure interface)

1. Enable
2. Conf t
3. Int _____
4. Switchport port-security violation shutdown

AFTER YOU FINISH EVERYTHING DO THE COMMANDS "DO WRITE MEM" AND THEN "DO COPY RUN START"

HOW TO ADD VLAN NAME

1. Enable
2. Conf t
3. Vlan (vlan number/id)
4. Name _____

HOW TO UNAME VLAN

1. No vlan ___

HOW TO ASSIGN VLANS TO INTERAFACES

1. Enable
2. Conft
3. Int range __/_-_
4. Switchport access vlan ___

HOW TO ADD NATIVE VLAN TO INTERFACE

1. Enable
2. Conf t
3. Int ____
4. Switchport trunk native vlan ____ (number)

TRUNK PORTS ARE FROM SWITCH TO ROUTER

HOW TO DO TRUNK PORTS

1. Enable
2. Conf t
3. Int ____
4. Switchport Mode trunk

HOW TO DO A STATIC ROUTE

1. Enable
2. Conf t
3. Ip route (ip of the thing your going to) (subnet mask of the thing your going to) (the WAM. This is the port that shows the outside world. It is mostly the closest port to the thing)
4. **REMEMBER THAT NETWORK IP ROUTES HAVE A .0 AT THE END**

HOW TO RESTRCIT TRUNK

1. Enable
2. Conf t
3. Int ____
4. Switchport trunk allowed vlan add ____(vlan number) (use commas if multiple vlans)

HOW TO CONFIGURE TRUNKING

1. Enable
2. Conf t
3. Int range (G1/1 or something like that).
4. Switchport mode trunk

WHEN DEALING WITH A SWITCH AND PORTS FACING PC'S, ITS SWITCHPORT ACCESS AND DEALIGN WITH VLANS AND SWITCHSPORTS ITS 'SWITCHPORT ACCESS VLAN"

You do switchport mode access on access ports and switchport mode trunk on trunk ports

To cancel a command you type “No” in front of it.

IOT – internet of things (just google it)

Trunk – the port on a back of the switch that where the PCs branch off

Static Routing
Go into sub interface
encapsulation dot1q (vlan ID)
Ip address
Trunking
Go into trunk interface
No shutdown
switchport mode trunk
switchport trunk native vlan 99
Vlans to address
switchport mode access
switchport access vlan 10
Static route lets switches know about devices that aren’t next to them
Ip route (network address) (subnet mask) interface it goes through
I.e. ip route 172.31.10.0 255.255.255.0 172.31.1.2
Outside network=everything outside of internet
Inside network=internet
Outside host
Ip route (outside host) (subnet mask of the destination network) (Next IP.)
The port
I.e. ip route 209.165.200.0 255.255.255.224 172.17.45.248

Ip route (Network ID of destined network) (Subnet mask of the destination

Network) (next hop)

Default route – 0.0.0.0 0.0.0.0 and then the exit

Destination address is always a network.

The point of VLANS is like a mini network inside of your main network. For example, the PC's on both sides of the router.

The Two rules of routing.

1. The router only knows its next hop
2. The computer only does what you tell it to do

How to get rid of translating – Control + Shift + 6

ENCAPSOLATION

1. Enbale
2. Conf t
3. Interface _____
4. Enc _____ (tab it) vlan number

Inter vlan routing – Pretty much just static routing

Default route – 0.0.0.0

Always turn off R.I.P "No router rip"

RIP – routing info protocol

How to create a default I.P - 0.0.0.0 0.0.0.0 _____

How to disable summarization of networks - "no auto-summary"

To enter rip confg mode "router rip"

Wildcard- inverse of a subnet mask

HOW TO GET TO A VERISON OF THE RIP

1. Enable
2. 2. conf t
3. Router rip
4. Version 2

HOW TO CONFIGURE THE LAN PORT THAT CONTAINS NO ROUTERS SO THAT IT DOES NOT SEND OUT ANY INFO

1. En
2. Conf t
3. Router rip
4. Version 2
5. Passive-interface (full port name plus number, not IP. EX. Gigabit ethernetport 0/0)

HOW TO DISABLE SUMMERIZATION OF NETWORKS

1. Enable
2. Conf t
3. Router rip
4. No auto-summary

HOW TO CONF PASSIVE INTERFACES ON RIP

1. Enbale
2. Conf t
3. Router rip
4. Passive-interface _____ (interface)

HOW TO CONFIGURE RIP FOR THE NETWROKS THAT CONNECT TO _

1. Conf t
2. En
3. Router rip
4. Verson 2
5. Network (ip address)

HOW TO ADVERTISE DEFAULT ROUTE

1. Enable
2. Conf t
3. Router rip
4. Deafult-information Originate

SAVING INFO!!!! 1. “do write mem” 2. “do copy run start”

HOW TO CONF NETWORKS IN RIP

1. Enable
2. Conf t
3. Router rip
4. Network _____(network number)

HOW TO DO ENTER PROCESS ID (ospf confg mode)

1. Enable
2. Conf t
3. Router ospf (process id) “1”

HOW TO CONFG A NETWORK ON OSPF

1. Enable
2. Conf t
3. Router ospf
4. Network _____ (network id) _____-(wild card) area __- (0 unless told otherwise)

HOW TO ADD ROUTER ID

1. Enable
2. Conf t
3. Router ospf _____ ‘1”
4. Router-id 1.1.1.1

HOW TO RENAME VLANS

1. Enable
2. Conf t
3. Vlan ____ (20)
4. Name _____

HOW TO PREVENT ADDRESS FROM BEING DISTRUBTED

1. Enable

2. Conf t
3. Ip address dhcp

HOW TO SET DEFAULT-GATEWAY ON DHCP POOL

1. Enable
2. Conf t
3. Ip dhcp pool _____
4. Default-router _____(ip address)

HOW TO SET THE LAN INTERFACE TO PASSIVE

1. Enable
2. Conf t
3. Router osfp _____ (1)
4. Passive-interface _____

HOW TO SET ROUTE BETWEEN VLANS USING SUBINTERFACES

1. Enable
2. Conf t
3. Int _____
4. Encapsulation ___(vlan number)
5. Ip address ____ subnet mask _____

CONFIG A DHCP POOL

1. Enbale
2. Conf t
3. Ip dhcp pool _____(pool name)

HOW TO ASSIGN ADDRESS TO EACH POOL

1. Enable
2. Conf t
3. Dhcp pool ____-(pool name)

DHCP = DYNAMIC HOST CONFIG PROTOCAL

SSH V2 AUTHRNTICATION RETIRES

1. Enable
2. Conf t
3. Ip ssh authentication-retries (_____) number

SSH TIMEOUT

1. Enable
2. Conf t
3. Ip ssh time-out (____) number

HOW TO ALLOW MAC ADDRESS (Learn mac address)

1. Enable
2. Conf t
3. Int _____
4. Switchport port-security f-address sticky

HOW TO REDISTRBIUTE AN IP ROUTE TO SOMEWHERE ELSE (AKA A ROUTER)

1. Enable
2. Conf t
3. Router ospf 1
4. default-information originate

HOW TO HANDOUT IP ADDRESS ON A POOL

1. Enable
2. Conf t
3. Ip dhcp pool (poolname)
4. Network (ip address) (subnet mask)

HOW TO DO A DEFAULT ROUTE

1. Enable
2. Conf t
3. Ip route 0.0.0.0 0.0.0.0

HOW TO CONFIG ADDRESS AS PASSIVE USING OSPF

1. Enable

2. Conf t
3. Router ospf 1
4. Passive-interface _____ (any interface NOT facing the router)

HOW TO ASSIGN A DEFAULT GATEWAY TO A DHCP POOL

1. Enable
2. Conf t
3. Default router (ip address)

HOW TO MAKE A DHCP POOL NOT USE A CERTAN ADRESS

1. Enable
2. Conf t
3. Ip dhcp excluded-address (excluded ip)

Configure standard acl

R1(config)# ip access-list standard (_____)

R1(config-std-nw)# permit host _____

R1(config-std-nacl)# deny any

R1(config-if)# ip access-group File_Server_Restrictions out

Configure an ACL to permit FTP and ICMP.

a. From global configuration mode on R1, enter the following command to determine the first valid number for an extended access list.

```
R1(config)# access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
```

b. Add 100 to the command, followed by a question mark.

```
R1(config)# access-list 100 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
```

c. To permit FTP traffic, enter permit, followed by a question mark.

```
R1(config)# access-list 100 permit ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
```

d. This ACL permits FTP and ICMP. ICMP is listed above, but FTP is not, because FTP uses TCP. So you enter TCP. Enter tcp to further refine the ACL help.

R1(config)# access-list 100 permit tcp ?

A.B.C.D Source address

any Any source host

host A single source host

e. Notice that we could filter just for PC1 by using the host keyword or we could allow any host. In this case, any device is allowed that has an address belonging to the 172.22.34.64/27 network. Enter the network address, followed by a question mark.

R1(config)# access-list 100 permit tcp 172.22.34.64 ?

A.B.C.D Source wildcard bits

f. Calculate the wildcard mask determining the binary opposite of a subnet mask.

11111111.11111111.11111111.11100000 = 255.255.255.224

00000000.00000000.00000000.00011111 = 0.0.0.31

g. Enter the wildcard mask, followed by a question mark.

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?

A.B.C.D Destination address

any Any destination host

eq Match only packets on a given port number

gt Match only packets with a greater port number

host A single destination host

lt Match only packets with a lower port number

neq Match only packets not on a given port number

range Match only packets in the range of port numbers

h. Configure the destination address. In this scenario, we are filtering traffic for a single destination, the server. Enter the host keyword followed by the server's IP address.

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?

dscp Match packets with given dscp value

eq Match only packets on a given port number

established established

gt Match only packets with a greater port number

lt Match only packets with a lower port number

neq Match only packets not on a given port number

precedence Match packets with given precedence value

range Match only packets in the range of port numbers

<cr>

i. Notice that one of the options is <cr> (carriage return). In other words, you can press Enter and the statement would permit all TCP traffic. However, we are only permitting FTP traffic; therefore, enter the eq keyword, followed by a question mark to display the available options. Then, enter ftp and press Enter.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
  <0-65535>  Port number
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp
```

j. Create a second access list statement to permit ICMP (ping, etc.) traffic from PC1 to Server. Note that the access list number remains the same and a specific type of ICMP traffic does not need to be specified.

```
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62
```

k. All other traffic is denied, by default.

Step 2: Apply the ACL on the correct interface to filter traffic.

From R1's perspective, the traffic that ACL 100 applies to is inbound from the network connected to Gigabit Ethernet 0/0 interface. Enter interface configuration mode and apply the ACL.

R1(config)# interface gigabitEthernet 0/0

R1(config-if)# ip access-group 100 in

Step 3: Verify the ACL implementation.

a. Ping from PC1 to Server. If the pings are unsuccessful, verify the IP addresses before continuing.

b. FTP from PC1 to Server. The username and password are both cisco.

PC> ftp 172.22.34.62

c. Exit the FTP service of the Server.

ftp> quit

d. Ping from PC1 to PC2. The destination host should be unreachable, because the traffic was not explicitly permitted.

Part 2: Configure, Apply and Verify an Extended Named ACL

Step 1: Configure an ACL to permit HTTP access and ICMP.

a. Named ACLs start with the ip keyword. From global configuration mode of R1, enter the following command, followed by a question mark.

R1(config)# ip access-list ?

extended Extended Access List

standard Standard Access List

b. You can configure named standard and extended ACLs. This access list filters both source and destination IP addresses; therefore, it must be extended. Enter HTTP_ONLY as the name. (For Packet Tracer scoring, the name is case-sensitive.)

R1(config)# ip access-list extended HTTP_ONLY

c. The prompt changes. You are now in extended named ACL configuration mode. All devices on the PC2 LAN need TCP access. Enter the network address, followed by a question mark.

R1(config-ext-nacl)# permit tcp 172.22.34.96 ?

A.B.C.D Source wildcard bits

d. An alternative way to calculate a wildcard is to subtract the subnet mask from 255.255.255.255.

255.255.255.255

- 255.255.255.240

= 0. 0. 0. 15

R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 ?

e. Finish the statement by specifying the server address as you did in Part 1 and filtering www traffic.

R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

f. Create a second access list statement to permit ICMP (ping, etc.) traffic from PC2 to Server. Note: The prompt remains the same and a specific type of ICMP traffic does not need to be specified.

R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

g. All other traffic is denied, by default. Exit out of extended named ACL configuration mode.

Step 2: Apply the ACL on the correct interface to filter traffic.

From R1's perspective, the traffic that access list HTTP_ONLY applies to is inbound from the network connected to Gigabit Ethernet 0/1 interface. Enter the interface configuration mode and apply the ACL.

R1(config)# interface gigabit 0/1

R1(config-if)# ip access-group HTTP_ONLY in

Step 3: Verify the ACL implementation.

a. Ping from PC2 to Server. If the pings unsuccessful, verify the IP addresses before continuing.

b. FTP from PC2 to Server. The connection should fail.

c. Open the web browser on PC2 and enter the IP address of Server as the URL. The connection should be successful.

HOW TO SET UP MANAGEMENT INTERFACE ADDRESSING

1. Enable
2. Conf t
3. Int _____(vlan 1)

4. Assign ip address

HOW TO SET UP VTY LINES/ACCPET ONLY STUFF

1. Enable
2. 2. conf t
3. Line vty ____ (Number 0-15)(0)
4. Login local
5. Transport input ssh

HOW TO GET RID OF NONNEGOTIATE

1. Enbale
2. Conf t
3. Int _____
4. Switchport nonegotiate

ON A PORT, THE PORT FACING THE OUTSIDE IS TRUNKED, AND THE PORTS ON THE INSIDE ARE ACCESS. YOU HAVE TO TELL THE PORTS THAT YOU MAKE TRUNK OR ACCESS TO LET THE VLANS YOU ASSIGN TO LET THEM THROUGH.

RIP V2 CAN USE EVERY SINGLE SUBNET (/23 FOR EXAMPLE)

RIP V1 CAN ONLY USE /8,/16,/29,/32

Saving work is very imporant,

DO WRITE MEM

DO COPY RUN START

-Eigrp
On a router, if you want things on the system to only send things to certain things on the system, you must use the command

Router egirp (number)

If you want to trouble shoot, you should look to the bottom right hand corner of the packet tracer, look for the “Simulation” tab, and click it.

DHCP automatically assigns ip address to the end devices on the network, (for example to PC). So, if you say the dhcp pool is to assign the ip 192.1680.0/24, then it will assign that ip to all the end devices.

- Hello There

- Static Routing
    - Ip route *network ip address {ip address w/ 0 at end}* *subnet mask* *ip address of where to go through*
    - Do show ip route
- In pc
    - Ping router
    - Need to make sure ip/gateway/dns set
    - Need to make sure all routers know route
- From routers make sure you send to PC not router PC is connected to
- Make sure you send to correct port on router/switch/server
- RIP Routing
    - Type router rip
    - Put in network id + subnet mask
    - Make sure if subnet mask not /8 /16 or /24 on version 2
        - Command is version 2
        - Auto-summary allows ripv2 to use not /8 /16 /24 or /32
- Eigrp
    - Router eigrp 1
    - Kind of same as rip, but put same # to share *must be connected*
    -
        - Type passive interface to receive but not send
- Dhcp
    - If have dhcp server in subnet, pc will contact server for ip address, will send ip address
    - Router has help address, will tell pc where dhcp server is
    - Can make router into dhcp “server”
    - Command ip dhcp pool (pool name)
        - Default-router (ip address)
            - Makes default gateway
    - Ip dhcp excluded-address (ip address you don’t want to use)

- VLAN
    - On router
    - To put ip on vlan
        - Type inter fa(#)
            - Type ip address (ip address)
        - Type .(vlan #) after fa name to enter subif mode
            - Type ip address (ip address and subnet)
            - No shut
            - Encapsulation dot1Q (VLAN #)
    - On switch
    - Vlan (#)
    - Inter vlan (#)
    - Inter fa(#)
        - THIS NEEDS TO BE WHERE IT CONNECTS TO ROUTER
        - Type switchport mode trunk
        - Type switchport trunk allowed vlan add (#)
        - Need to switch ports to PCs to access
            - Type switchport mode access
            - Type switchport access vlan (#)
- In router
    - To make ports have ip addresses, type ip address (ip address and subnet)
- ACL
    - In router
        - Type access-list 100 permit (thing you want to permit) (ip address and wildcard of thing) [host (ip address)]
        - Type ip access-list extended/standard HTTP_ONLY
            - Permit tcp (ip address and wildcard) host (ip address) eq www
        - Type access-list (#) permit ahp (source wildcard) (destination wildcard)
        - “ “esp” “
        - “ “udp “ “ eq isakmp
- OSPF
    - Router ospf (process id)
    - Network (ip address) (wildcard mask) area (area id {usually 0})
    - Passive-inter gig(gig #)
- NAT
    - Static, dynamic, overload
    - Static
        - Ip nat source static (internal ip address) (external ip address)
    - Dynamic bm
        - Access-list (ACL#) allow (network’s ip address) (wildcard)

        - Ip nat pool (name of pool) (start of ip range) (end of ip range) netmask (subnet mask)
        - Ip nat inside source list (ACL#) pool (name of pool)
    - Overload
        - Access-list (ACL#) allow (network's ip address) (wildcard)
        - Ip nat pool (name of pool) (start of ip range) (end of ip range) netmask (subnet mask)
        - Ip nat inside source list (ACL#) pool (name of pool) overload
            - OR
        - Access-list (ACL#) allow (network's ip address) (wildcard)
        - Ip nat inside source list (ACL#) inter (name of interface) overload
- AAA
    - Authentication
        - Username (username) secret (password)
        - Aaa new-model
        - Aaa authentication login default local
    - Authorization
        - Aaa authorization (network/exec/commands (level)) default (group/local) (radius/tacas+)
    - Accounting
        - Aaa accounting (network/exec/connection) default (start-stop/stop-only/none) (group/broadcast) (radius/tacas+)
- ALWAYS DO
    - Do write mem
    - Do copy run start
- VPN commands
    - Gre
        - Inter tunnel (# or 0)
        - Ip address (address)
        - Tunnel source (ip address of source)
        - Tunnel destination (ip address of destination)
        - Tunnel mode gre ip
- ISAKMP
    - Crypto isakmp policy (1-10000) {usually 1} {For ipsec vpn}
        - Authentication pre-share
        - Encryption des
        - Group 1
        - Hash md5
        - Lifetime (# of seconds) {default is 86400}
        - Authentication (should tell what to do)
        - Crypto isakmp key (keystring) address (peer address)

        - Crypto isakmp key (keystring) hostname (hostname)
        - Crypto isakmp identity hostname
        - Crypto ipsec transform-set (transform set name) {should tell what to do after}
        - Crypto map (name) (#) ipsec-(manual/dynamic)
- general
    - Auto secure
    - Erase startup-config
    - Do sho run [include username]
- Console security
    - Line con 0
    - Password (password)
    - Login
    - Login local
    - Transport input ssh
- Telnet security
    - Line vty 0 4
    - Password (password)
    - Login
    - Login local
    - Transport input ssh
- Aux port access security
    - Line aux 0
    - Password (password)
    - Login
    - Login local
    - Transport input ssh
- Privileged exec access
    - Enable secret (password)
- Change minimum length of password
    - Security passwords min-length (length) {default 6}
- Change timeout time after inactivity
    - Exec-timeout (mins)
- Disable exec process for line
    - No exec {while in line config)
- Encrypt all passwords
    - Service password-encryption
- username/password
    - Username (username) password/secret (password)
- Enhanced login config
    - Login block-for (seconds) attempts (failed tries) within (seconds)

        - Ip access-list standard (PERMIT-ADMIN {name})
            - Remark permit only administrative hosts
            - Permit (ip address)
            - Ex
        - Login quiet-mode access-class (PERMIT-ADMIN {name})
        - Login delay (seconds)
        - Login on-success log [every login]
        - Login on-failure log [every login]
        - Security authentication failure rate (threshold rate) log
        - Sho login
- Router config
    - Hostname (hostname)
    - Domain (domain name)
    - Line-desc
    - Banner motd/exec/login (symbol message symbol)
- Ssh config
    - Ip domain-name (domain name)
    - Crypto key generate rsa general-keys modulus (modulus size)
    - Sho crypto key mypubkey rsa
    - Crypto key zeroize rsa
    - Sho ip ssh {before conf t}
    - Ip ssh version 1 or 2
    - Ip ssh time-out (seconds)
    - Ip ssh authentication-retries (integer)
    - Sho ssh
- Config privilege level
    - Privilege (mode) [level (level) or reset] [command]
    - Username (username) privilege (level) secret (password)
    - Enable secret level (level) (password)
    - Sho privilege {before enable}
    - Enable secret level (level) (password)
    - {before enable} enable (level)
- View config
    - Aaa new-model
    - Enable view [(view name)]
    - Parser view (view name)
        - Secret (password)
        - Commands (parser mode) include/include-exclusive/exclude [all] int(int name)/(command)

Alternative

- Parser view (superview name) superview
    - Secret (password)
    - View (view name)

- Verify user view
    - {before conf t} Enable view (view name)
    - {before conf t} show parser view
    - “ “ enable view
    - “” show parser view all
- Router Security
    - Secure boot-image
    - Secure boot-config
    - {bct} show secure bootset
    - If enable password forgotten
        - {be} show version
        - Confreg0x2142
        - Reset
        - Copy startup-config running-config
        - config-register (configuration register setting)
    - Disable password recovery
        - No service password-recovery
- Syslog
    - {in line config}
        - Logging host (hostname) (ip address)
    - Logging trap (level)
    - Logging source-interface (int name and #)
    - Logging on
    - Logging host (ip address)
- Setting time
    - {bct} clock set (hr:min:sec) (mon) (#) (yr)
- Ntp servers
    - Ntp master (stratum)
    - Ntp server (ip address)/(hostname) [version (#)/key (key id)/source (int)/prefer]
        - Ntp broadcast client
    - Ntp authenticate
    - Ntp authentication-key (key #) md5 (key value)
    - Ntp trusted-key (key #)
    - {bct} sho ntp association detail [include (ip address)]

- {bct} auto secure [no-interact/full] [forwarding/management] [ntp/login/ssh/firewall/tcp-intercept]

- Protocol
  - Like a language
- RIP vs static
  - Static you need to say “connect to this”
  - Rip automates routing
- OSPF
  - Open shortest path first
- VPN
  - Virtual private network
  - Called tunnel

- ASA
  - Enable password {not secret}
  - Domain-name
  - Write erase {not erase startup-config)
  - Show route {no ip}
  - Route outside/inside {not ip route}
  - Q {not Ctrl C}
  - Security-level (level)
  - Ip address dhcp [setroute]
  - {to make vlan description} description (description)
  - Switchport access vlan (vlan id)
  - No shut {enables int}
  - Route (interface name) 0.0.0.0 0.0.0.0 (next hop address)
  - Show route
  - Passwd (password) {for telnet/ssh}
  - Telnet (ip address) (sub mask) inside/outside
  - Telnet timeout (minutes)
  - Aaa authentication ssh console [LOCAL]

- Crypto key generate rsa modulus (#)
- Ssh (ip address) (sub mask) (int name)
- Ssh timeout (minutes)
- Show ssh
- Ntp server (ip address)
- Ntp authentication-key (#) (type) (password)
- Ntp trusted-key (#)
- Ntp authenticate
- Dhcpd enable inside/outside
- Dhcpd address (start of pool address) (end of pool address) inside/outside
- Dhcpd domain (domain name)
- Dhcpd dns (dns ip address)
- Dhcpd wins (wins ip address)
- Dhcpd lease (seconds)
- Dhcpd option (value)
- Show dhcpd state
- Show dhcpd binding
- Show dhcpd statistics

NAT – the most basic way to change an I.P address, it changes you ip into a different one, but that IP is only viewed by people on the outside. It Is only on routers.

Static NAT – you must manually change all the ips

Dynamic NAT is automatic

PAT -

HOW TO PERMIT STANDARD ACLS

1. En
2. Conf t
3. Ip access-list (If it says standard, then do that) standard _____(Name)
4. Permit _____ (ip address and wildcard)

HOW TO MAKE A NAT POOL

1. Make an ACL
2. Ip nat pool _____ (name) _____ (Ip address or what is specifies, the end of the ip range.) netmask _____ (Subnet)

HOW TO ENABLE PAT

1. En
2. Conf t
3. Ip nat inside source list ____ (name) pool ____(name) overload

HOW TO ASSOCIATE ACL'S WITH NAT POOLS

1. En
2. Conf t
3. Ip nat inside source list ____ (name) pool ____(name)

HOW TO MAKE A PORT INSIDE OR OUTSIDE

1. En
2. Conf t
3. Ip nat inside/outside

HOW TO TURN INSIDE SOURCE STATIC ON A NAT

1. En
2. Conf t
3. Ip nat inside the source static

HOW TO CONIFG OUTSIDE AND INSIDE STATIC SOURCE

1. En
2. Conf t
3. Ip nat inside source static (inside Ip) (outside ip)

TCP PORT IS 80

OSI LAYERS (7)

Please do not take south park away – we mostly use 2 and 3

7 - APPLICATION

6 - PRESNTATION

5 - SESSION

4 – TRANSPORT (HTTP)

3 – NETWORK (IP) routers

2 – DATALINK (ETHERNET) switches

1 – PYSICAL

HOW TO TURN ON AAA

1. En
2. Conf t
3. Aaa new-model

HOW TO CONFIGURE AUTHENCATION LOGIN DEFAULT AAA

1. En
2. Conf t
3. Aaa authencation login default login

HOW TO CONFIG AAA AUTHENCATIN CONSOLE ACCESS

1. En
2. Conf t
3. Aaa authencation login

HOW TO CONFIG AAA FOR VTY

1. En
2. Conf t

3. Aaa authencation login TELNET-LOGIN local

HOW TO CONFIG VTY PORTS AAA

1. En
2. Conf t
3. Line vty 0.4 or 0.15

HSRP COMMANDS

HSRP VERISON

1. En
2. Conf t
3. Int (VLAN #)
4. Standby version 2

HSRP CONFIGURE DIFFERENT VLANS / SET ACTIVE IP

1. En
2. Conf t
3. Int vlan(VLAN #)
4. Standby (vlan int #) ip (IP #) (remember to do any spefic commands if asked such as a .1)

HOW TO SET PRIOROTY IN HSRP

1. En
2. Conf t
3. Int vlan (vlan #)
4. Standby (vlan int #) priority (priority #((100 is default #)

HOW TO CONFIG ACTIVE ROUTER TO RUN IF DOWN HSRP

1. En
2. Conf t
3. Int vlan (vlan #)
4. Standby (vlan #) prempt

Spanning tree notes 9/20/21

Why we need STP?

What happens when three switches are connected to each other?

Endless loop.

STP STATES

- Forwarding state – interface activity forwarding network traffic
- Blocking state – interface currently blocked but is a backup if a forwarding interface fails
- Port roles
    - Root
    - Designated
    - Non designated

BPDU – bridge protocol data unit – info sent to the switch

Bridge ID field – used to elect root bridge for the network

If root bridge, all ports will be in forward state

BPDU – Bridge ID field; lowest priority used to elect root bridge, info sent to each other

32768 is max, mac address will be tie breaker

1. Determine root bridge
2. Select root port
3. Select designed ports
4. Block ports with loops

SHOW SPANNING-TREE COMMAND IS VERY IMPORTANT!!!!

Cost -

Ethernet (10mbps) = 100

Fast Ethernet (100mbps) = 19

1gig (1000mbps) = 4

10gig (10000mbps) = 2

Spanning tree commands

Portfast – enables on end hosts to forward right away. Never connected to the switch

Spanning-tree portfast – for a singular interface

Spanning-tree portfast default – enables STP portfast on all access ports

BPDU Guard – will shut down interface id a BPDU is received

Pvst – per vlan spanning tree (a mode of STP on a vlan)

Spanning-tree vkan # root (primary/secondary)