CCNA DIK عادل

Dete: 27 / 1 / 23 Lec 1 Day M T W T F S ①

External parts of Router.

→ Router is an intelligence device

→ Router is layer three "3" device.

→ console and auxilary is used for router configuration.

→ Serial port is used for the communication of Router to router.

→ Ethernet is able to communicate devices via protocols.

→ speed of ethernet is "10mb".

→ speed of gigethernet is "1000mb".

→ speed of fastethernet is "100mb".

→ switch is used to comunicate more then two devices.

→ In switch POE (power over ethernet) ports is used.

→ Repeater is used for signal regentration.

→ Router is use for path determination

→ SP (service provider) has no internet.

→ SP is more expensive

→ ISP has internet

→ ISP is less expensive.

→ SP is just connectivity

→ SP is more secure then ISP.

→ Data in rest is the data present in your pc

→ Data in motion is a data move or travel.

→ Line port is use for management.

→ interface port is used for data

→ Firewall is use for security.

→ Data in motion will be secured by VPN" virtual private network".

→ VPN create a logical path

→ Data in VPN is travel encrypted.

x————————x

Lec 2: 30-1-2023

## Modes of Router:

→ Router has three modes.

→ ① user Exac mode

→ router>

→ Limited verifications

→ ② privilage Exac mode

→ Router#

→ Full verification

→ ③ Global configuration mode

→ Router (config)#

→ Full configuration

→ In LAN communication will be perform due to MAC Address.

Internal Components of Router.

→ processor
- → processor is used for decision making
- → processor is used for data processing.

→ RAM
- → RAM stand for "Random access memory"
- → In cisco running configuration will be present in "RAM"
- → RAM is temporary memory
- → It works only during run time.
- → When device is off all the data in "RAM" will be erased.

→ NVRAM
- → It is use for permenent data.
- → In CISCO router data will be present in startup configuration.

→ Flash
- → In flash IOS are stored.
- → IOS stand for "Internetwork operating system.

→ ROM:
- → ROM stand for "Read only memory"
- → It is use for Boot sequence.
- → It is also use for "POST"
- → POST stand for "power ~~over~~ on self test"

## Addresses.

→ Address has two types
(i) physical Address
(ii) Logical address
→ physical adress is also called MAC Address.
→ MAC stand for "Media Access Control"
→ MAC Address is Globally unique.
→ MAC Address hass 48 bitz or 6byte.
→ 24 bits is for network portion.
→ 24 bits is for vendor portion.
→ MAC Address represented in Hexa-decimal formate. i.e 123456789ABCDEF.
→ MAC Address is assign by "IANA"
→ IANA stand for "Internet Assign number Authority".
→ Switch has unique MAC Address.
→ MAC Address of Router having each interface.

Logical Address

→ IP stand for "Internet protocol".
→ It has 32bit Logical address
→ Range of IP address is (0 – 255).
→ IP Address is formed from Network ID and Host ID.
→ In IPV4 there are ~~two~~ three types of communication.
→ unicast
→ Broadcast
→ Multicast

P.T.O

→ communication of one to one is called unicost.

→ Communication of one to all is called Broadcast

→ communication of one to group is called multicast.

→ Network portion represents nos of IPs.

→ Host portion represent specific users.

→ Network portion is same but Host portion is not same.

→ There are five clasess of IPv4

→ class "A".

→ Range of class A is 1–126

→ Network bits of class A is 8 while host bits is 24

→ class A IP is use for ~~b~~unicast and Broadcast

→ class "B".

→ Range of class B is 128 - 191.

→ Network bits of class B is 16 white host bits is 16.

→ class B IP is used for unicast and Broadcast.

→ class "C".

→ Range of class C is 192-223.

→ Network portion of class C is 24 bits while host portion is 8.

P.T.O

→ IPs of class C is used for unicast and Broadcast.

→ class "D"

→ Range of class D is 224-239.

→ there is no concept of Network and host portion.

→ it is used for multicast.

→ class "C".

→ Range of class C is 240-255.

→ No concept.

→ class "C" IP is use for research and development.

→ 0.0.0.0 this IP is use for default route.

→ 127.0.0.0 this IP is use for machine testing Loopback.

→ identity of classes is from first octate.

→ Network ID represent group of IP.S.

→ How to find Net ID.

→ formula ⇒ Network portion as it is and host portion all bitz off.

i.e 192.168.10.1 ⇒ Net ID ="192.168.10.0"

→ How to find Broadcast ID.

→ Network portion as it and host portion all bits on.

i.e 192.168.10.1 ⇒ B-ID "192.168.10.255"

→ How to find valid IP.

→ Network portion as it is and host portion is combination of 0,1.

→ $2^n - 2$

i.e 192.168.10.1

$2^8 - 2 = 256 - 2$

→ (254) this will be valid IP.

→ How to find subnet mask.

→ Subnet mask is also called prefix length.

→ Network portion all bitz ON and host portion all bitz off.

→ i.e 192.168.10.1

255.255.255.0

→ free IP i.e private IP from class A, B and C.

→ class A:

→ Network 10.0.0.0 free private IP

→ this IP will use in LAN.

→ class B

→ private IP from class B is.

172.16.0.0 to

172.31.0.0

→ 16 ~~of~~ private IP in class B.

→ class C.

→ private IP from class C is.

→ 192.168.0.0 to

192.168.255.0

→ 256 are free private network

DHCP

→ DHCP stand for "dynamic HOST ~~control~~ ~~@~~ configuration protocols."

→ Gateway use to communicate different networks.

→ DHCP performs DORA process.

→ DORA stand for " Discovery offer Request Acknoledgment."

→ How to enable DHCP:

→ IP DHCP pool Khan
→ Network 10.0.0.0 255.0.0.0
→ DNS server 8.8.8.8
→ Default router 10.0.0.100
→ Exit
→ Show IP DHCP binding.

→ What is DNS server

→ DNS stand for Domain name system"

→ It is use for ~~x~~ changing of name to IP and IP are change into name .. i.e IP to name and name to IP resolution.

→ when DHCP is down then PC obtained 169.254.234.66 directly this IP is assign by APIPA

→ APIPA stand for "Automatic private IP Addresing".

→ DNS is an aplication layer protocol.

→ DNS and DHCP use tcp and UDP (53) ports.

## telnet and SSH

→ we can access a cisco router remotely by telnet and SSH.

→ telnet is not secure.

→ SSH is more secure.

→ SSH stand for secure shell.

→ telnet is not use in real.

→ telnet will be use when VPN is runing.

→ virtual interface created in router is Line vty.

→ vty stand for (virtual telitype).

→ How to Enable telnet

→ Comands.

```
→ Hostname clinks
→ Enable password 123.
→ Line vty 0 4          : (0-988)
    → password 123
    → transport input telnet
    → Login
```

→ How to Enable SSH

```
→ username Khan password 123
→ IP Domain name Khan
→ crypto ~~key~~ Key generate rsa general-Keys
  modulus 1024
→ Line vty 0-4
→ transport input SSH
→ Login Local.
```

Date: 20/02/2022 Lec Day: M T W T F S

IOS BACKUP

→ Comands For Backup: IOS
→ show Flass: copy .bin file
→ cop FlASh: tftP: file name:

Backup Of Running configuration
→ copy Runn-config tftP: Remote address

→ Delete Flash
→ delete flash
→ Reload

→ Take Backup
→ tftpdnld
→ follow the step
→ tftp_dnld
→ Reset

→ Runn-config Backup
→ copy tftP: runn-conf: remote host: Sourcefilename

Date: 3 / 3 / 2022 Lec Day: M T W T F S

RIP

→ RIP stand for "Routing Information protocol"

→ Administrative distance of RIP is "120".

→ Redendency means fast convergance of Load when connected port is down.

→ What is protocols?

→ protocol is a rule defined that is enable on a ports.

→ RIP is a industry standard protocols.

→ RIP is made by "IETF".

→ In RIP you just advertise the connected network.

→ RIP send their updates to the neighbour routers.

→ update is also called information.

→ RIP send their update in every "30" sec.

→ If RIP cant reply then it will for the reply next "180sec.

→ RIP is always broadcast their updates.

→ RIP depend on metric.

→ RIP select their best path on hop counts.

→ Metric is a criteria by which a router select the best path.

RIP is use for a small network

→ RIP Support maximium 15 to 16 routers.

→ RIP version one support only classfull networks.

→ passive interface means to block hello msg.

→ RIP V2 supert classless IP, Authentication, Sumarization.

→ RIP Broadcast and multicast IP is 224.0.0.9

EIGRP

→ EIGRP stand for "Enhanced interior gateway Routing protocol".

→ Before 2014 it is "IGRP" and only a cisco property.

→ After 2014 it is enhanced to "EIGRP" and it is standard industry protocol.

→ EIGRP Support Authentication

→ EIGRP Support Summarization

→ EIGRP Support classless ~~net~~. IP

→ EIGRP is used for Large Net max "255"

→ EIGRP hello time is "5" sec

→ EIGRP hold time is 15 sec.

→ EIGRP multicost their update."

→ Authentication is used to check validity- It is used to denied ~~for~~ unauthorized person.

→ Summarization means to advertise many network as a single network.

→ classless IP mean those IP where subneting is performed.

→ EIGRP creates three types of table.

→ * Neighbour table: In neighbour table the information of neighbour will be present.

→ * Topology Table: All path of routing will be present in topology table.

→ * Routing table: Best path will be present in routing table.

→ To chose best path it is called 'metric".

Dely value 1—125

Date: / /  Day M T W T F S

→ Metric of EIGRP is depend on bandwidth, dely and Load e.t.c

→ Administrative distance of EIGRP is 90.

→ Formula of EIGRP is to find metric.

$$= \left( \frac{10^7}{B.W} + Dely \right) 256$$

→ Less metric value will be follow by router.

→ How To Enable EIGRP ON Router.

→ Comands

→ Router EIGRP A.S ∴ A.S will be same

→ No Auto Summary

→ Network 1.0.0.0 e.g

→ In EIGRP equal path Load balancing is performed.

→ How to Enable EIGRP

→ Comands.

→ Router EIGRP 1 (0—255)

→ NO Autosummary

→ Network.

→ Exit.

→ Multicast IP of EIGRP is "224.0.0.10".

→ External EIGRP A.D is "170".

Date: / / Lec Day: M T W T F S

OSPF

→ "open shortest path first"

→ OSPF is dynamic routing protocol.

→ OSPF is made by "IETF"

→ IETF stand for "Internet Engineering Task force"

→ OSPF is industry standard protocol.

→ protocols enable computer to communicate with one another.

→ OSPF is also use for large network maximum is 255 router.

→ OSPF is support Authintication

→ OSPF Suport Summarization

→ OSPF support Classless ip.

→ OSPF Hello time is 10 sec.

→ OSPF Hold time is 40 sec.

→ OSPF multicast their updates.

→ for multicost OSPF use 224.0.0.5 and 224.0.0.6 for ip address.

→ One IP is use for neighbourship 224.0.0.6

→ The other IP is use for "DRBDR" 224.0.0.5.

OSPF creates three types of table.

→ one table is called neighbour table.

→ Second is called Data base table.

→ Third is called Routing table.

→ Best path for OSPF we look for cost

→ cost only depend on bandwidth in OSPF.

→ Formula for cost in OSPF is

→ $\frac{10^8}{B.W-B.S}$

→ Low cost will be follow by router.

→ In OSPF there is a concept of Area.

→ OSPF will be perform in two types of Area "0" and "1". OR Single Area and multi Area.

→ Area zero will be consider as Backbone Area.

→ Other then zero area will be consider as regular area.

→ the advantages of Area is easy management, Routing table management.

→ there are four types of Router in OSPF

→ Backbone Internal router

→ Internal Router

→ ABR ⇒ Area Border Router

→ ASBR ⇒ Autonumus system border router.

→ Backbone IR is those whose interfaces are in Area zero.

→ Internal router (IR) is those router whose interfaces is in regular Area.

→ ABR is those router which is conected with both regular and backbone Area.

→ ASBR is those router where other protocol Like EIGRP is run from outside i.e redistribute.

→ updates has two types

→ periodic updates there is no changes.

→ Incrimental updates changes their update all time

→ OSPF use incrimentall updates.

→ In OSPF there is no updates only LSA are forword.

→ LSA stand for Link state advertisment.

→ there are five LSA in OSPF.

→ "LSA1" and "LSA2" is those updates which is ~~transfer~~ change in with in Area.

→ when $R_1$ ~~sto~~ send their updates to $R_2$ then it is "LSA1".

→ when $R_2$ send Information of $R_1$ to $R_3$ then it is LSA2.

→ LSA3 when updates send from one to another Area then it is "LSA3".

→ When the Information of "ASBR" is send to another router then it is "LSA4".

→ LSA5 is also called external LSA.

→ When any Information comes to "ASBR" then it is "LSA5". External router redistribute.

→ In OSPF wildcard mask is use

→ wildcard mask is opposite of Subnetmask

→ In OSPF process ID is used.

→ It is use for distinguish b/w Routes.

→ Router ID is use as router name.

→ highest ID will be select when no Loopback.

# ~~EIGRP~~ OSPF

How to Enable ~~EIG~~I OSPF

→ Router OSPF 1

→ Network 1.0.0.0 Area 10

→ Exit

How to perform redistribution.

→ Router EIGRP 1

→ Redistribute EIGRP 1 subnets

→ Router EIGRP 1

→ Redistribute OSPF 1 metric 1 1 1 1 1

Name of ~~SEA~~ LSA

→ LSA ~~SEA~~ stand for "Link state Advertisment"

→ LSA 1 is called router LSA.

→ LSA 2 is called Network LSA.

→ LSA 3 and LSA 4 is called Summary LSA.

→ LSA 5 is called External LSA.

→ Administrative distance of OSPF is "110"

ACL

→ ACl stand for "Access control List"

→ Access control List is used to create policies.

→ It is used to allow or denied any user in organization.

→ there are two types of ACL.

→ Standard ACL

→ value of standard ACL start from (1—99).

→ Extended ACL

→ value of extended Acl start from ~~200~~ (100-199).

→ In standard Acl decision will take only through source

→ In Extanded ACL desicion will take through Source + destination and port number.

→ port no of telnet is 23.

→ port no of SSH is 22.

→ port no of HTTP is 80.

→ port no of HTTPs is 443.

→ In standed ACL policy is created

→ for single user we use permit host

→ for multiple user we use permit

→ Same for deny, deny host

→ for network you must write wildcard mask.

P.T.O

→ How to Enable ACL.

→ Comands.

→ Access List one "1" deny host 10.1.1.1

→ Access List 1 permit host 10.1.1.2

→ Access List 1 deny 30.0.0.0 0.255.255.255

→ Access List 1 permit any

→ Do show Access List.

→ interface F 0/0

→ IP Access-group 1 out

* How To Enable extended ACL

→ port number of HttP is 80.

→ port number of HTTPs is 443.

→ TCP stand for "transmision control protocol".

→ UDP stand for "user data gram protocol".

→ TCP

→ TCP is reliable

→ TCP is connection oriented

→ TCP is 3 way hand shak

TCP is slow. because there is no ~~er~~ chance of error in TCP.

→ TCP is used by text, emails e.t.c.

→ UDP

→ UDP is fast.

→ UDP is connectionless.

→ UDP is unreliable.

→ UDP is used by audio, video and Streaming e.t.c.

→ ICMP = ping

→ ICMP stand for "internel control message protocol"

→ ping is use ICMP protocol.

→ ICMP has no port number because ICMP is not TCP OR UDP.

* How to Enable ACL extended Comands.

Deny

Access List 111 deny IP host 10.1.1.1 host 192.168.18.1

Date: 14/2/2023 Day M T W T F S

# NAT

What is NAT

→ NAT stand for "Network Address So Translation".

→ There are three types of NAT

① Static NAT

Dynamic NAT

PAT NAT

→ In static NAT one private network translate in to one public network i.e one to one.

→ Static NAT is very expensive.

→ In Dynamic NAT is one private complete network into one pool of public network.

→ In PAT the whole private network is translate into a single public network.

→ preiority of static NAT is greater then PAT NAT.

→ How to Enable NAT

Static

→ Interface se 0/0/0 ~~outside~~

→ IP NAT outside

→ Interface F0/0

→ IP NAT inside

→ IP NAT source static 192.168.10.1 195.1.1.3

Dynamic

→ Access List 1 permit 192.168.10.0 0.0.0.255.

P.T.O

→ IP NAT pool public-- IPS 195.1.1.6 195.1.1.10 netmask 255.255.255.249

→ IP NAT inside Source List 1 pool public-IPs overload

PAT

→ Access List 2 permit 192.168.10.0 0.0.0.255

→ IP NAT inside Source List 2 inside interface serial 0/0/0 overload

→ How to Enable Loopback

→ interface Loopback 0

→ Network 10.0.0.0

→ DNS 8.8.8.8 ✓

Day: M T W T F S

Date: 15/02/2022 Lec

## Switching:

→ switch work on Datalink layer.

→ Datalink layer work on IP and mac address.

→ HUB work on physical Layer.

⇒ Difference between HUB and switch.

→

| ⇒ HUB | switch |
|---|---|
| → Hub is non-intelligence device. | → Switch is intelligence device. |
| → HUB can,t read mac address. | → switch read mac address. |
| → ports of Hub is half duplex | → while ports of switch is half and full duplex. |
| → Speed of HUB ports is 10mb per second. | → while speed of switch is 10mb, 100mb, 1000mb, 10000mb. |
| → HUB is a broadcast Domain alltime/everytim broadcast | → In switch first time broadcast then unicast. |
| → HUB is single collision Domain | → Switch is multiple collision Domain. |

→ What is ARP.

→ ARP stand for "address resolution protocol".

→ ARP work on mac address.

→ In ARP catche the mac address is Stored for 4hours.

→ ARP translate 32bits IP adrress into 48bits mac address.

→ ARP find mac address of destination host from its Known IP address.

→ ARP is a layer 2 protocol, Data link layer.

→ ARP Request is broadcast, But ARP response is unicast.

→ ARP request will be generated only for the same network.

→ ARP concept use in IPV4 addreses only.

→ Types of ARP

→ ARP has four types
(1) ARP (2) Proxy ARP (3) Reverse ARP (4) Gratituous ARP

→ ARP

→

Date: 15/02/2023 Lec Day M T W T F S

VLANS

→ VLAN stand for "Virtual Local Area Network".

→ vlan create for broadcast Limitation and Limited ~~full~~ security.

→ VLAN 1 created default by switch.

→ Range of VLAN is (2 — 1001) (← standard VLANS)

→ 1002, 1003, 1004, 1005 this vlan is already created but this are not suported .

→ this VLAN are use for old technologies.

→ (1006 → 4094) this vlan are extanded VLANS.

→ How to Enable VLAN: Comands:

→ VLAN 10

→ Name sales

→ Exit

→ How to assign interface to VLAN:

→ interface Fa0/0

→ switchport mode-access

→ switchport access vlan 10

→ interface range ~~Fa0/~~ Fa0/4-6

→ clear mac address-table.

→ Access port is assign to End user.

Daber Paper Products

Date: 20/2/2023 Lec Day: M T W T F S

Trunk

→ Access port will assign to the end user.

→ Access port is always a member of vlan 1.

→ Some vlans are for Data.

→ Some VLANS are for voice.

→ In Access port two VLAN can perform, voice and Data.

→ management VLAN when we want to access switch.

→ Native VLAN is used to carry untag traffic.

→ untag trafic means no VLAN TAG.

→ VLAN 1 is Native VLAN.

→ What is trunk.

→ Two protocols are used in trunk

→ DOT1q

→ 802.1Q

→ this's protocols are industry standard.

→ ISL is also use in TRUNK Encapsulation.

→ ISL stand for "inter switch link".

→ ICL is a cisco property.

→ " When we want to connect Same networks accross two different switches.

→ " When we want to carry multiple VLANS on a Single Link. Link is called trunk

How to Enable Trunk.

→ Interface F0/1
Switchport mod trunk ( Layer2 SW)
For layer 3 switch.
→ Switchport trunk encapsulation dot1q
→ Switchport mode trunk.

Lec

→ InterVLAN via switch
→ In these case layer 3 switch needed.
→ these switch need defaultgateway.
→ first create VLAN
→ interface VLAN 10
→ IP address
→ no shutdown
→ Exit

For VLAN 20
→ Same comand for VLAN 20:

VTP

→ VTP stand for " viLAN Trunking Protocol".

→ VLAN is also called layer2 VPN

→ VTP is used for viLAN mannagement.

→ VTP has three modes.

→ (i) Server mode

→ this mode can create VLAN

→ It pass VLAN to another SW

→ It can accept VLAN from other.

→ It modify all VLAN.

~~→~~P

→ (2) client Mode

→ In client mode it is only accept VLAN from server mode

→ client mode cant modify, delete and change any type of VLAN.

→ (3) Transparent:

→ ~~trans~~ In transparent mode ~~it~~ you can modify, delete and change of a VLAN

→ But when you create a VLAN this VLAN will not go to other modes.

→ In VTP revision number are used.

→ revision number will be increased by creating VLANS.

→ Configuration:

→ VTP Domain Khan : It is must

→ VTP mode client

→ VTP mode transparent

→ VTP pasword Khan.

Date: 24/2/2023 Lec Day: M T W T F S

Port security:

→ port security will be used in Access port i.e end user.

→ Access port is a member of a Same VLAN.

→ violation will be three types.

→ ① shutdown
(2) restrick
(3) protect.

→ In shutdown violation the port will shutdown when third party access it.

→ In protect violation the port can,t give any response to third party user.

→ In Restrict mode when third party enter to the port all info of third party will be store.

→ In port security we can tell many mac Address.

→ How to Configure Port Security:

→ interaface Fo/o
→ Switchport Acc mode Access
→ switchport port security
→ switchport security maxim "1"
→ Switchport port security mac address sticky
→ Switchport port security violation, Shutdown, protect, restrict.

Date: 28/12/2023 Lec Day: M T W T F S

Spanning Tree protocol.

→ Spanning tree is used for the evodence of Loop in LAN.

→ Spanning tree block the port logicaly.

→ when a port is disable or down then the logical port is up.

→ In STP election will perform to block a Single port.

→ In STP the election will perform by three rules.

→ ① one root bridge or per VLAN:

→ ② one designated per ~~root bridge~~ segment.

→ ③ one root port non root bridge.

→ every switch take 30 sec for STP election:

→ In every Switch it has own mac address and preiority value.

→ preiority value for all switch is same 32768.

→ BPDU is a protocol that it contains all type of STP information.

→ root bridge is a centralize device.

→ In STP root bridge will made to check low preiority value will be root bridge

→ If preiority are same then it will check mac address.

→ Low mac Address Switch will be root swi

→ preiority will be changed manually.

→ when root bridge Send BPDU it is call best BPDU.

→ For down the port STP follow cost value.

→ cost value of ethernet (100).

→ cost value of F-ethernet (19).

→ cost of gigethernet (4).

→ cost of 10 gig ethernet (2).

→ Designated port will be low cost port this port regenerate Best BPDU.

→ Root port will received best BPDU.

→ When link is down the othe port will wait for (20 sec)

→ this 20sec is called max age.

→ when an indirect link is down the other link will take (50 sec).

→ Dired link down then the other link will up on (30 sec).

→ How to configure ~~VLAN~~ STP

→ spanning tree VLAN~~10~~ 10 preiority 0.

→ When manually preiority decreased

→ Spaning tree priority 32768

⇒ In Rapid spanning tree there is no election perform again and again.

→ Comands

→ spanning-tree mode rapid-pvst

→ Interface F0/0

→ Spanning-tree portfast

30|3|2023

Etherchannel Lec

Day M T W T F S

→ Etherchanel is used for the grouping
of Severals Ethernet link to create one
Single logical Ethernet port on switches.
→ Multiple port as a single port. logical.
→ In Etherchanel loop evidence perform.
→ more speed perform.
→ high availibility, redundence.
→ Etherchannel has two types of protocols.
→ PAGP ⇒ It stand for "port aggregation group
protocol".
→ LACP ⇒ It stand for "Link aggregation
control protocol."
→ PAGP is a cisco property.
→ LACP is an industry standard protocol.
→ In PAGP there is two modes
→ (1) Desirable (2) Auto
→ In LACP there is two types of modes.
→ (1) Active (2) Passive
→ In Etherchannel how many ports bundle?
→ In PAGP You can bundle maximum
8 ports.
→ In LACP you can bundle maximum
16 ports. In 16 ports 8 ports Active and
8 ports are in standby.
→ for Etherchanel port must be the same
i.e if Faste then fast ethernat.
→ Etherchannel is use as a trunk.
→ FS load balancer is use for
Loadbalancing.

Date: / /　　Day: M T W T F S

⇒ How to Enable Etherchannel PAGP Commands:

→ Interface Range F0/1-4

→ Shutdown

→ channel-Protocol PAGP.

→ channel-group 2 mode desireble.

→ Same comands for other router.

→ Show Etherchannel.

⇒ How to Enable trunkport in this case.

→ Interface port-channel 2

→ Switchport mode trunk.

→ Same Comands for other Switch

DTP

→ DTP stand for "dynamic trunking protocol".

→ DTP is a cisco property.

→ DTP is work only on cisco devices.

→ DTP has two modes.

→ (1) desirable (2) Auto

→ Desirable mode will be send and received DTP. OR Trunk.

→ While Auto mode will received

→ By default DTP is enable on cisco devices.

→ By default all ports of a switch is Access and Auto.

→ When both side mode is Auto then no trunk will be enable.

→ One side must desirable and the other will be Auto.

→ When both side is desirable then trunk will be enable.

GRE Tunnel:

→ GRE stand for "Generaic routing Encapsulation".

→ In GRE the data move in plain text.

→ GRE tunnel is unsecure.

→ GRE tunnel is use for site to site communication.

→ How to configure GRE Tunnel

→ Commands.

→ perform EIGRP between ISP.

→ Router EIGRP 1

→ No Auto-Summary

→ Network.

→ perform default route from LAN to ISP.

→ IP route 0.0.0.0 0.0.0.0 next hope

→ check ping:

→ Creating GRE tunnel.

→ Comands

→ interface tunnel 16

→ tunnel Source ethernet 1/0

→ tunnel destination → remote public IP

→ IP address 192.168.10.1 → any private IP.

→ no shutdow

-:→ tunnel IP must be Same network.

→ Same command for other edge router.

→ Now perform static route

→ IP route 10.0.0.0 255.0.0.0 tunnel 16

→ Same for other site.

→ In GRE two types of header attached.

(1) public header, (2) private header.

Date: 19 / 3 / 2023 Lec Day: M T W T F S

GRE OVER IPSEC

→ site to site ipsec is use for site to site security.

→ for data encryption there are three algorithem used to Encrypt data.

→ (1) DES (2) 3DES ,, (3) AES.

→ DES stand for "Data Encryption standard.

→ AES stand for "Advance Encryption standard.

→ Data integrity means when a hacker change the Source IP during communication.

→ By protecting integrity data we attached "HASH".

→ HASH has two types.

→ (1) MD5 (2) SHA

→ MD5 stand for "Message digest algorithem"

→ SHA stand for "secure shell algorithem".

→ When we want to secure SHA we use "HMAC".

→ HMAC stand for " Hash-Based Message Authentication cod".

→ IP sec will perform in two steps. OR Phase.

→ (1) phase "1".

→ In phase 1 we will secure key.

→ for Key security we use Isa-Kemp

→ ISAKMP stand for "Internet sec Associate Key Management protocol.

→ phase 2:

→ In phase two we secure Data.

→ Data will be secure by IPsec.

→ How to configure IPSEC over GRE.

→ Comands.

→ Phase "1" commands

→ Krypto isakmp enable.

→ crypto isakmp policy 20.

→ Authentication pre-share

→ Encryption aes

→ HASH SHA

→ group 2

→ Exit.

→ Crypto- isakmp key cisco123 address 23.1.1.1 ∴ remote site IP

→ Same configuration on other site.

→

→ Now Data security

→ Phase 2

→ crypto ipsec transform-set TEST esp-aes

~~→ crypto ipsec~~ esp-sha-hmac

→ Exit

→ Same comand for other site

→ Now again

→ crypto IPSEC profile VPN

→ set transform-set TEST

→ Exit

→ Same comands for other Site.

P.T.O

→ Now apply IPSEC on tunnel

→ interface tunnel 123

→ tunnel protection ipsec profile VPN

→ Exit

→ Same comand for other site.

→ ESP stand for "Encapsulation security payload".

## CIA

Date: 20/3/23 Lec Day: M T W T F S

Site to site IPsec VPN

→ IPsec is use for internet security.

→ For Data encryption following algorithem is used.

→ DES, 3DES AES

→ DES stand for "Data Encryption standard".

→ 3DES stand for "Data Encryption Standard."

→ AES stand for "Advance Encapsulation standard."

→ the following algorithem is use for Data Encryption.

→ When a hacker replace source IP and attached their own IP this type of attack is called Anti reply attack.

→ xTo protect such type of attack we use "HASH".

→ this type of Data is called data intigrity.

→ to protect Intigrity Data We use HASH value

→ HASH has two types.

(i) SHA (ii) MD5

→ SHA stand for "secure Hash ~~strell~~ algorithem."

→ MD5 stand for "Message digest algorithem".

→ this algorithem is use for ~~Dat~~ protection of Data intigrity.

→ SHA is not secure.

→ For the security of SHA we use "HMAC".

→ HMAC stand for "Hashing message Authentication Code".

P.T.O

→ IPSEC will perform in two steps phase.

→ (1) Phase 1 (2) phase 2

→ In phase 1 we exchange a Secure Key.

→ In phase two we secure the Data.

→ for phase 1 key security we ISAKMP.

→ For Data security we use IPSEC.

⇒ IPSEC Configuration Comands.

→ crypto ISAKMP enable

→ crypto ISAKMP policy 1.

→ Encryption AES

→ Authentication pre-share

→ group 2

→ HASH ShA

→ Exit

→ crypto ISAKMP Key cisco123 address 15.1.1.2

→ same comands on other site.

⇒ Now phase 2.

→ First permit intresting traffic in ACL

→ Access list 111 permit ip. 10.0.0.0 0.255.255.2
172.16.0.0 0.0.255.255

→ crypto IPSEC transform-set test ~~ESP-AE~~
ESP-AES esp-sha-hmac

→ same comand for other site.

⇒ Now create map

→ crypto map VPN 10 IPSEC-ISAKMP

→ match address 111

→ set transform-set test

→ set peer 15.1.1.2

→ P.T.O

→ Same comands for other site.

⇒ Now apply VPN to public interface.
→ interface e1/0
→ crypto map VPN

→ Same comand for other site.

→ Show crypto ipsec ~~is~~ SA

⇒ Remote VPN

⇒ DMVPN