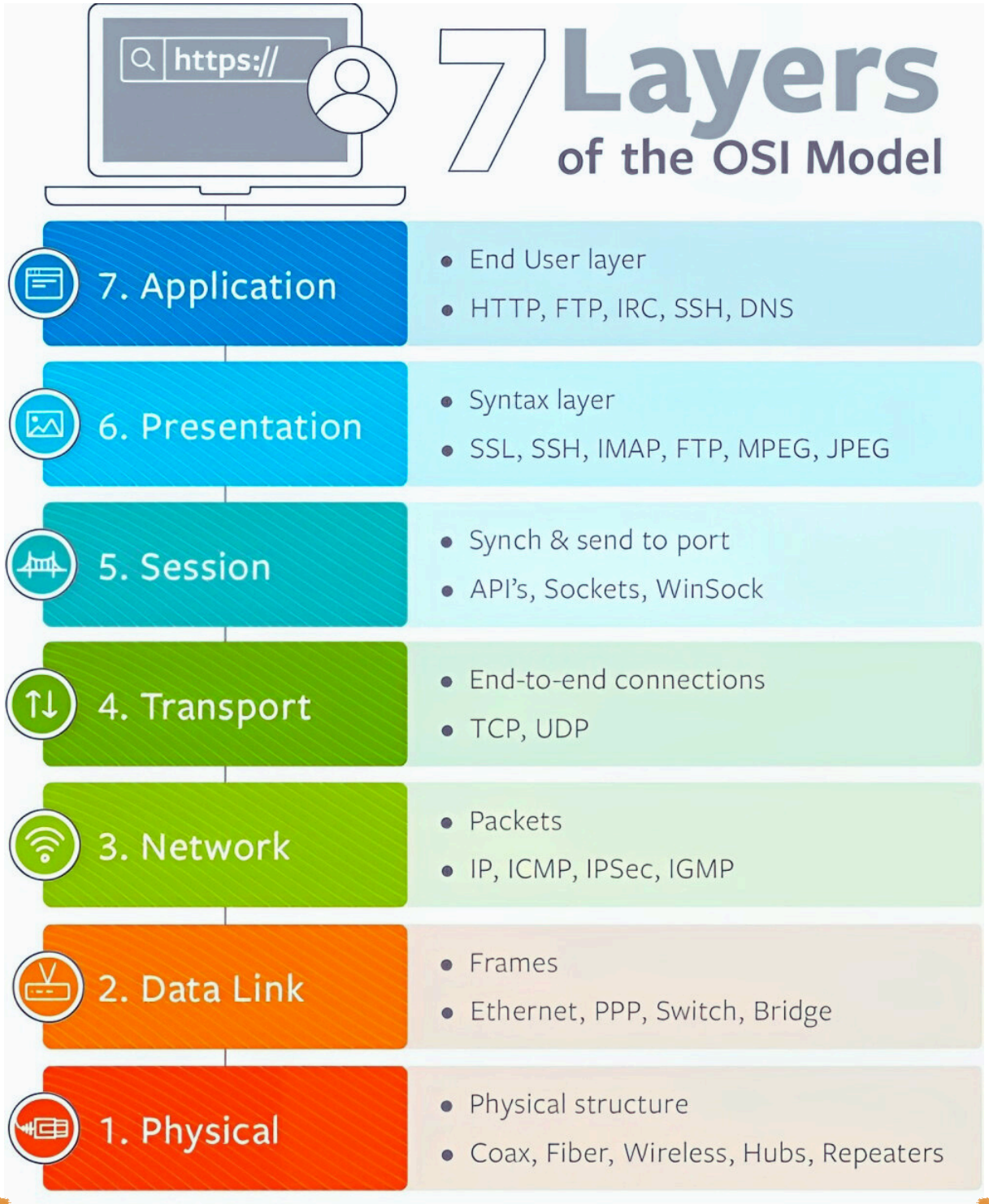
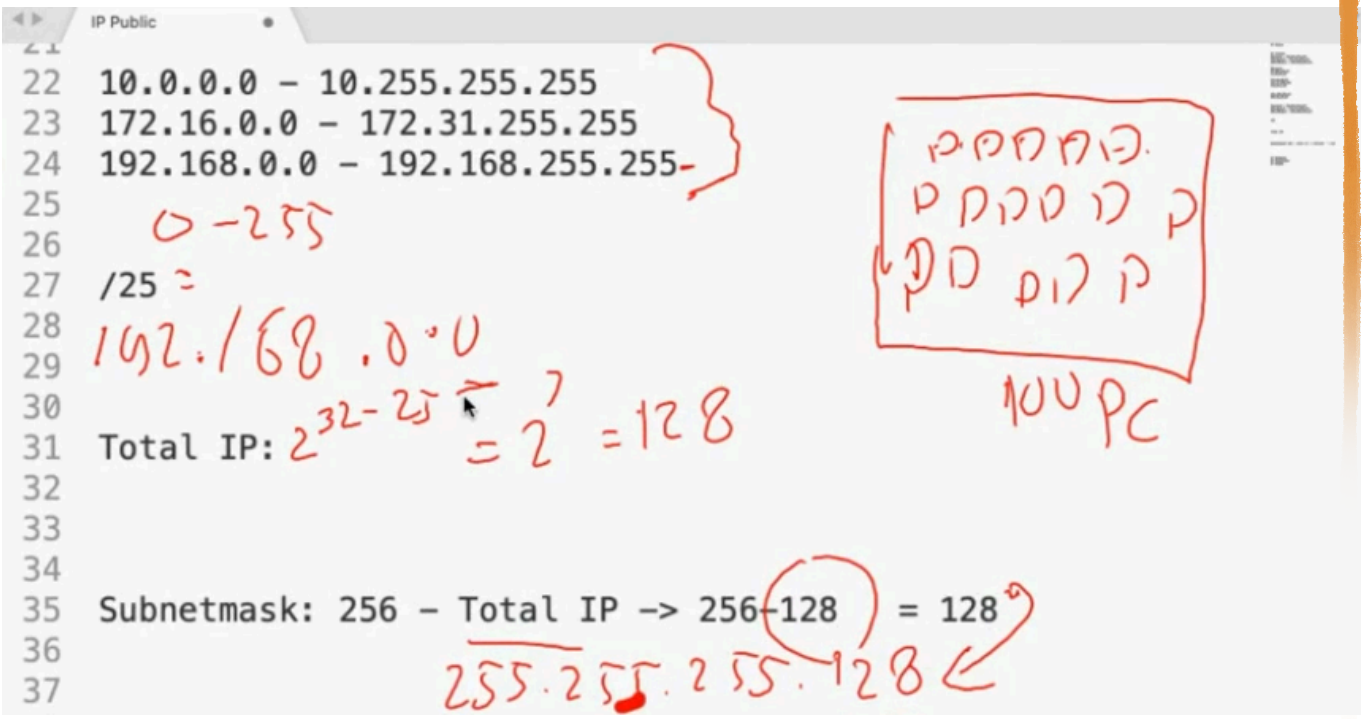
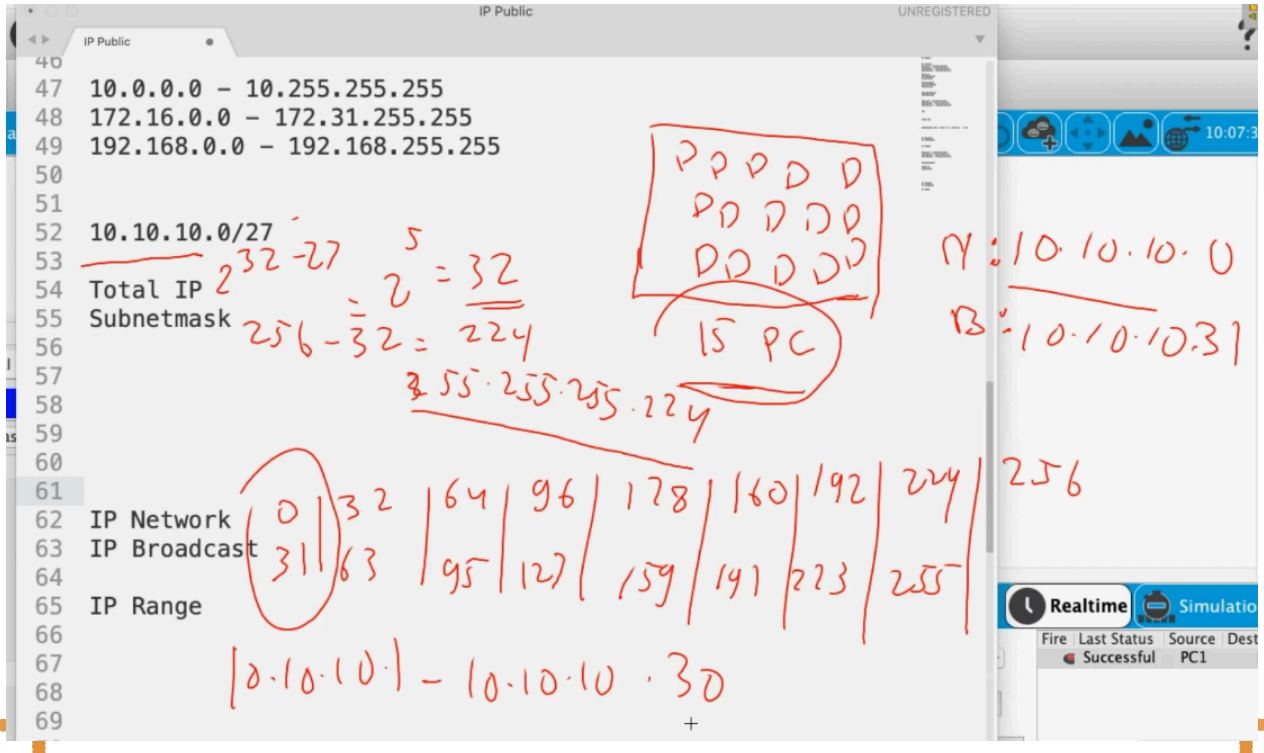
CISCO CCNA SUMMARY



PREFIX SUBNETTING

Prefix & Subnetting





Interface

Change Interface fa

```
Router1(config)#int fa0/0
Router1(config-if)#no shutdown

Router1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up

Router1(config-if)#ip address 192.168.1.1
255.255.255.0
```

Commands to End (privilege) and to Config

```
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#
Router1(config)#
Router1(config)#int fa0/1
Router1(config-if)#
Router1(config-if)#end
Router1#
%SYS-5-CONFIG_I: Configured from console by console
```

BASIC COMMAND

Change Hostname

```
Router(config)#hostname R
```

Perintah Menyimpan Konfig

```
R(config)#enable secret cisco
R(config)#
R(config)#
R(config)#do write
Building configuration...
[OK]
```

Command Basic CLI Cisco

```
enable
exit
configure terminal
hostname Router1
enable password 123
enable secret cisco
show running-config
do show running-config
```

SHOW INTERFACE

Command Show Interface

```
Switch#show interface
FastEthernet0/1 is down, line protocol is down (disabled)
  Hardware is Lance, address is 000a.f3d7.ab01 (bia 000a.f3d7.ab01)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
```

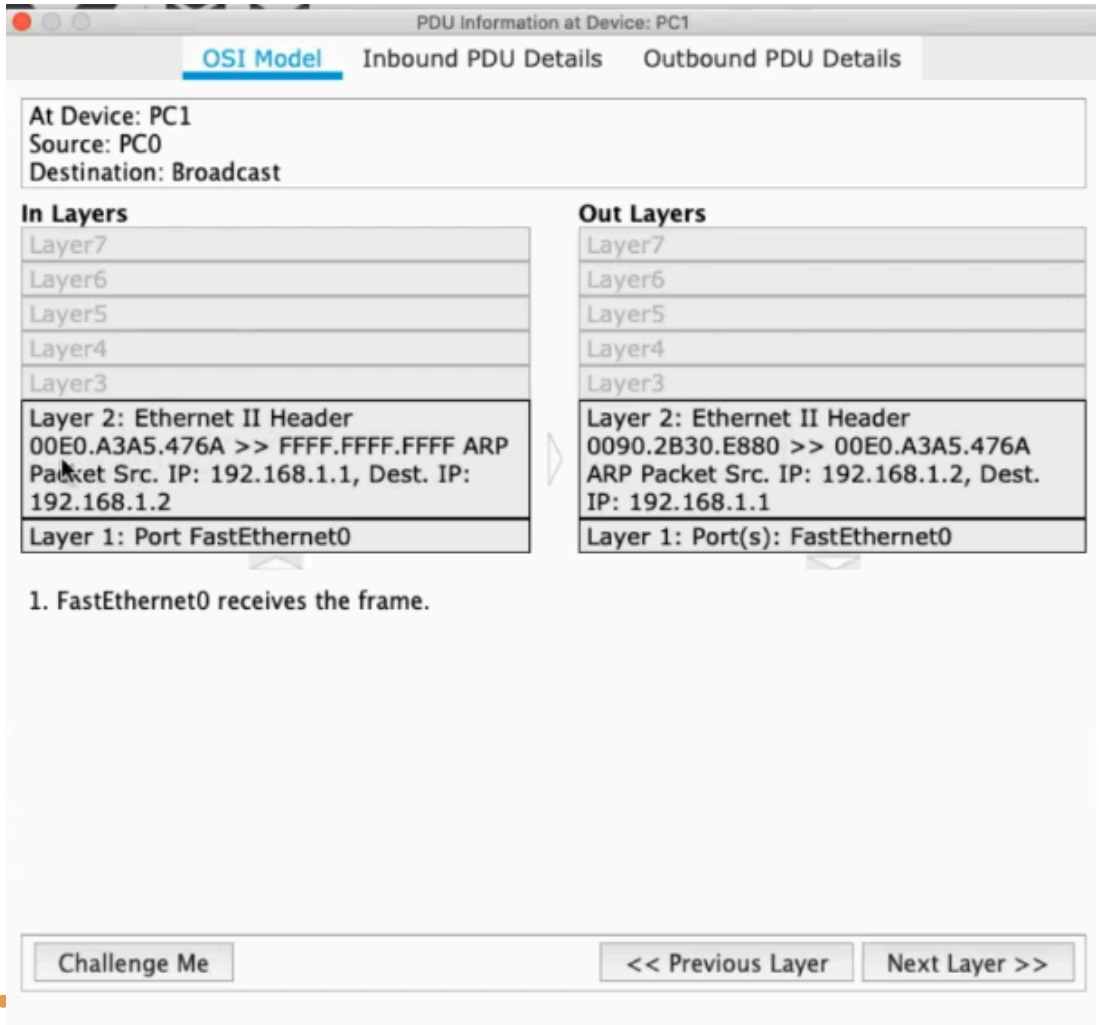
Show Port Interface

```
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual down                  down
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
```

SHOW ARP

Command to see Mac Address and IP in Command that has been Pinged

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.2           0090.2b30.e880        dynami
```



SHOW ARP

On a PC it is called an ARP table, if on a switch it is called a MAC address table (for mapping IP and MAC addresses on each interface)

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0010.1146.3b67    DYNAMIC     Fa0/3
   1    0090.2b30.e880    DYNAMIC     Fa0/2
Switch#
```

Description: records the Mac address of the interface connected to the PC.

Clear

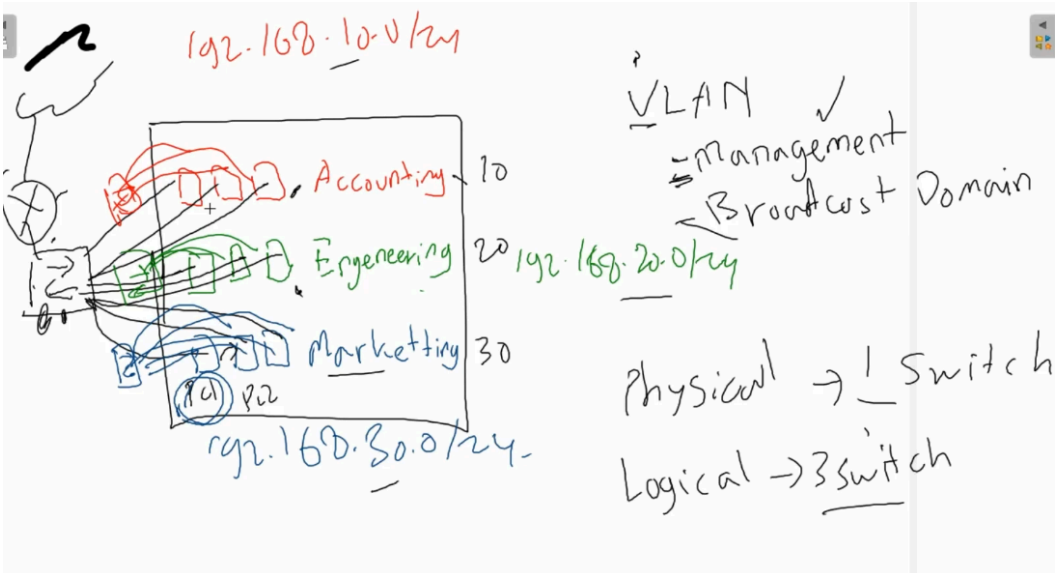
```
Switch#clear mac-address-table
```

VLAN

Add Vlan On Switch and Manage VLAN

```
Switch(config)#vlan 10
Switch(config-vlan)#
Switch(config-vlan)#name Accounting
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#do show vlan brief
```

Description: The VLAN number can be any number! The VLAN's job is to broadcast to the selected VLAN and not broadcast to other VLANs.



Description: Physically we have 1 switch, logically we can have several switches in a VLAN.

MANAGE VLAN

To Enter the Fa Interface into the VLAN

```
Switch(config)#interface fa0/2
Switch(config-if)#
Switch(config-if)#switchport mode access
Switch(config-if)#
Switch(config-if)#switchport access vlan 10
```

Description: Insert Interface Fa0/2 into the Vlan that we created earlier. Then you exit. Then go to do show

```
Switch(config-if)#exit
Switch(config)#
Switch(config)#do show vlan brief
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
10   Accounting                        active    Fa0/2
20   Marketting                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch(config)#
```

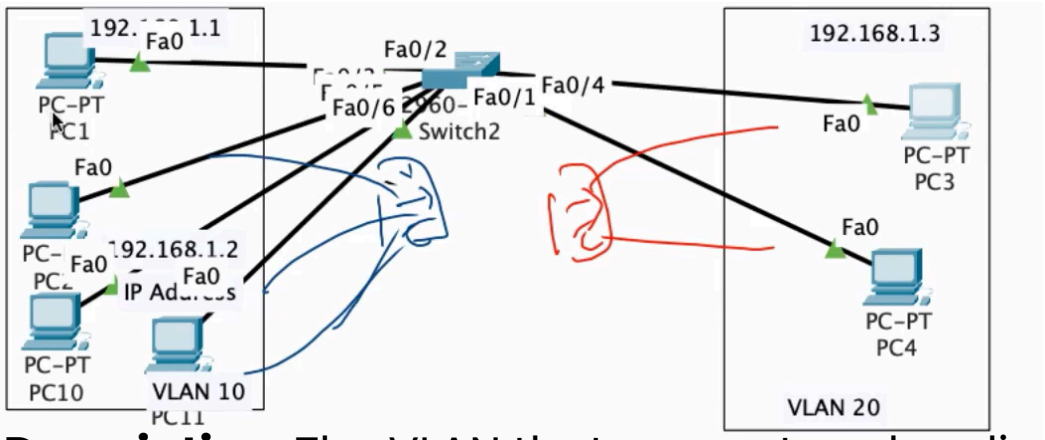
Description: The VLAN that was entered earlier has appeared

MANAGE VLAN

To enter the Fa interface into the VLAN briefly and all interfaces are included

```
Switch(config)#interface range fa0/1-2
Switch(config-if-range)#
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#
```

Description: Insert Interface Fa0/1 and Fa0/2 into the VLAN that we created earlier. Then you exit. Then go to do show



Description: The VLAN that was entered earlier has appeared

```
#switchport mode access
```

Description: Access mode is only connected to VLAN points.

MANAGE VLAN

If you want to combine VLAN 10 on switch1 and switch2, the Int on switch2 FA matches the VLAN, for the default trunk it's just on VLAN 1

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Accounting                       active    Fa0/1, Fa0/2
20   Marketting                       active    Fa0/3, Fa0/4
30   Engineering                      active    Fa0/6
```

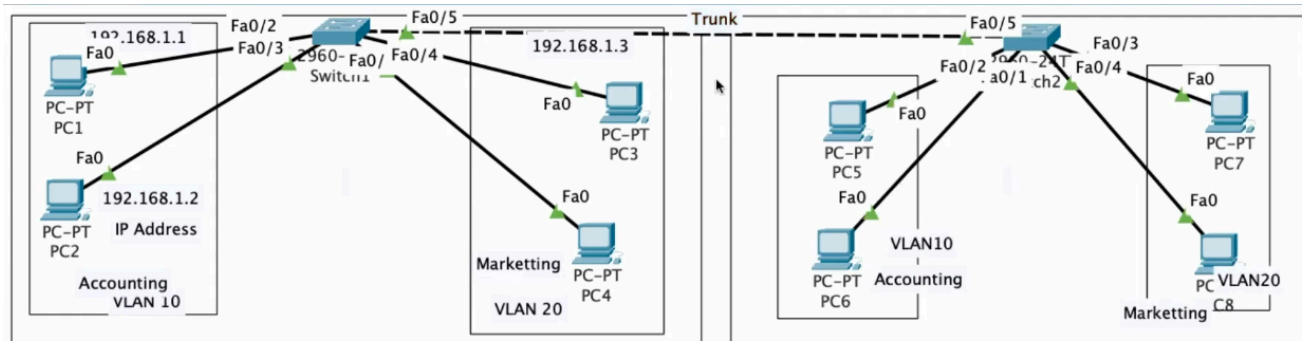
Description: If there are 2 switches in the same VLAN and we want to send packets from Int on switch1 and Int on switch2. we can use (Trunk)

Description: This is a quick way to no shutdown in int which connects between switches. **do show vlan brief**

```
Switch(config)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Accounting                       active    Fa0/2, Fa0/3
20   Marketting                       active    Fa0/1, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
```

TRUNK

Trunk (Connecting multiple switches) that is connected to the Interface and passes through VLANs



Description: If there are 2 switches on the VLAN, we will use Trunk. And here is the code for Trunk

```
Switch(config-if)#int fa0/5
Switch(config-if)#
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state
to up

Switch(config-if)#
```

Description: We call the interface on Switch 1 and Switch 2 to use Trunk Mode.

```
Switch(config-if)#do show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/5       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/5       1-1005

Port        Vlans allowed and active in management domain
Fa0/5       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/5       none

Switch(config-if)#
```

Description: To find out which Show Trunk has been activated.

TRUNK

Allowed Trunk is to allow and secure the VLAN that we are going to as below. We will use Allow

```
Switch(config-if)#switchport trunk allowed vlan 10,20
```

Description: If there are 2 LANs that you want to secure and allow, we can use Allowed Trunk.

```
Switch(config-if)#do show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/5       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/5       10,20

Port        Vlans allowed and active in management domain
Fa0/5       10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/5       20
```

Note: Only VLAN 10 and 20 are allowed which we have configured

```
Switch(config-if)#switchport trunk allowed vlan add 30
```

Description: add 30 to the Allowed Trunk with the word “add” 30

```
#switchport trunk allowed vlan remove 10
```

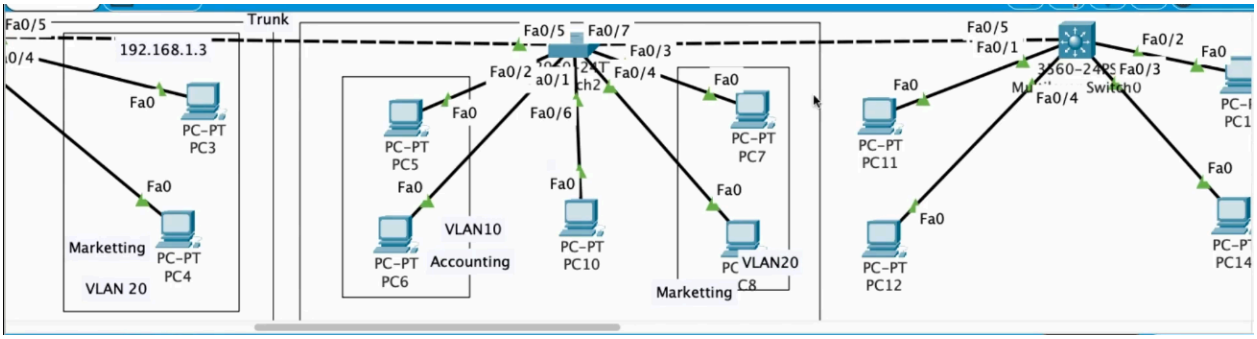
Description: delete Vlan 10 on allowed trunk using “remove” 10

```
Switch(config)#int rang fa0/1,fa0/4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#
Switch(config-if-range)#switchport access vlan 10
```

Description: if we want to enter a non-consecutive int range into VLAN 10

TRUNK

Trunk connects 3 switches with MLS configuration and not ISL



Description: If there are 3 switches in the VLAN, we will trunk using the MLS method

```
Switch(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured
to "trunk" mode.
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
```

Description: on other switches, the trunk configuration to fellow Cisco can use the default ISL. For the trunk configuration to open standard, we use 802.1q.

```
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport mode trunk
```

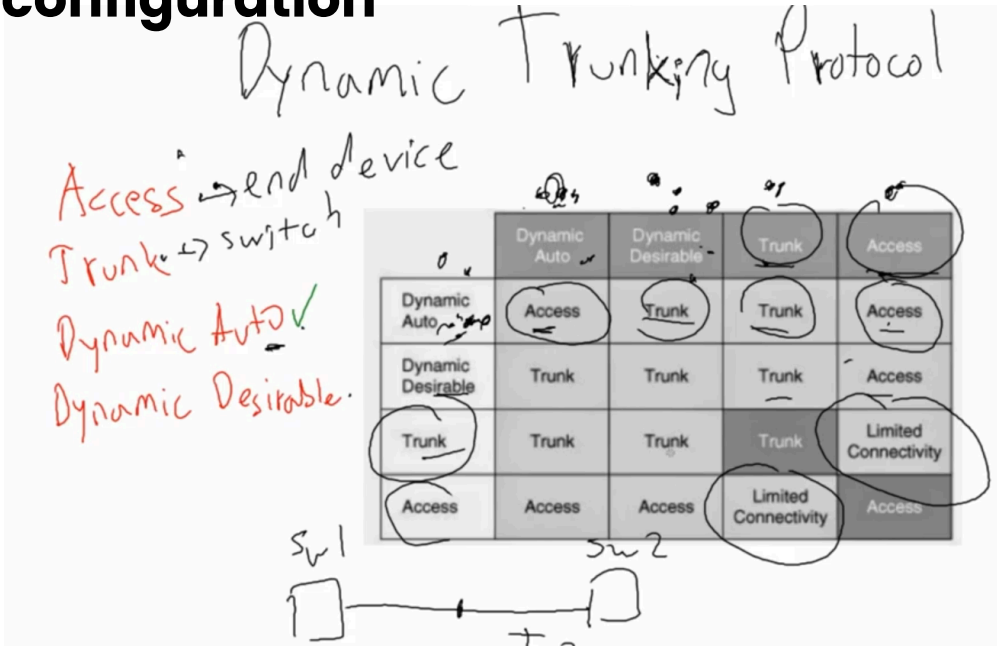
Description: To change the Trunk configuration to an open standard MLS using dot1q encapsulation.

```
Port        Vlans allowed on trunk
Fa0/5       10,20,30
Fa0/7       1-1005
```

Description: The following are 3 switches that have been configured with ISL and MLS trunks

DTP

Dynamic Trunking Protocol for Switch configuration



Description: Can be seen in the image above

```
Switch#show int fa0/5 switchport
```

Description: To view Int fa0/5

```
Administrative Mode: trunk
Operational Mode: trunk
```

Description: administrative mode is the mode that we configure, and operation mode is the final mode.

```
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode dy
Switch(config-if)#switchport mode dynamic de
Switch(config-if)#switchport mode dynamic
desirable

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/5, changed state to up
```

Description: Invites to go to the trunk on the switch

DTP

DTP configuration results from desirable to trunk mode!

```
Name: Fa0/5
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
```

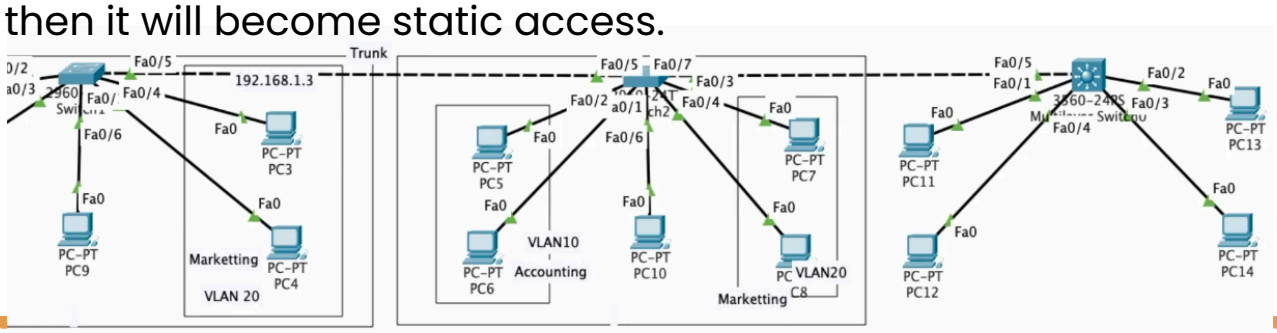
Description: Change the trunk configuration to desirable.

```
Switch(config)#int fa0/5
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode dy
Switch(config-if)#switchport mode dynamic au
Switch(config-if)#switchport mode dynamic auto

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/5, changed state to up
```

Description: Change Int trunk switch 2 to its dynamic auto DTP mode.

```
Administrative Mode: dynamic auto
Operational Mode: static access
```

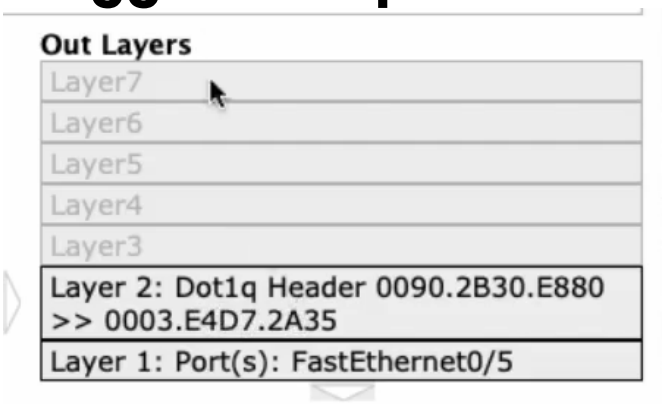
Description: Change both switches to dynamic auto trunk, then it will become static access.



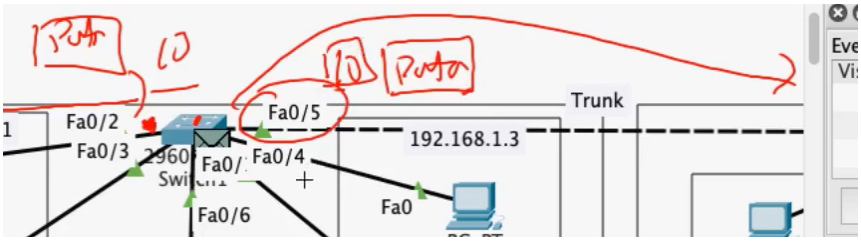
Description: dynamic auto: waiting (and cannot be interconnected from switch 1 to other switches) dynamic desirable: forced to become a trunk (can be interconnected)

Tagged

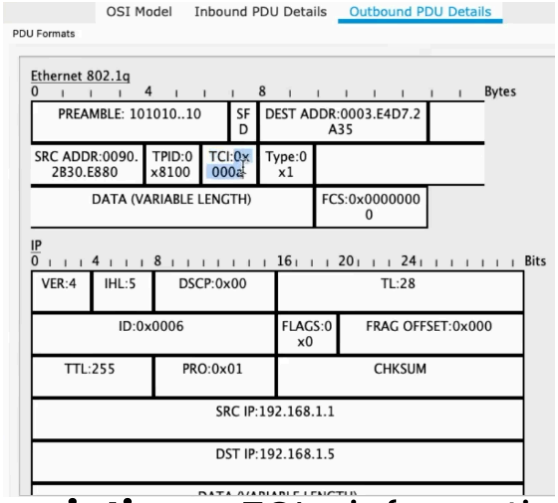
Tagged dot1q Header

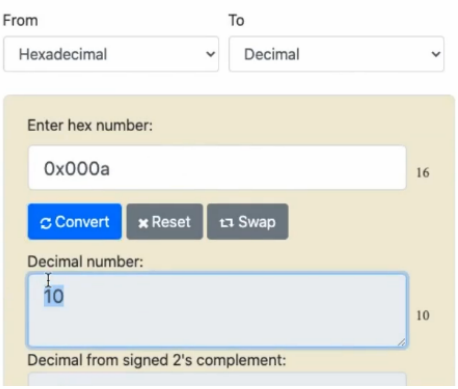


Description: So the tagged packets that pass through the trunk are tagged packets.



Description: Tagged trunk to identify the target VLAN to be accessed.





Description: TCI information for the VLAN number in hexadecimal in the outbound.. we are targeting VLAN 10.

Native VLAN

Changing Native Vlan on trunk

```
Switch(config-if)#switchport trunk native vlan 20
```

Description: Change the Native VLAN on the trunk

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/5       on           802.1q         trunking      20

Port        Vlans allowed on trunk
Fa0/5       1,10,20,30

Port        Vlans allowed and active in management domain
Fa0/5       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/5       1,10,20,30
```

Description: Native Vlan has been changed to 20

```
Switch(config-if)#switchport trunk native vlan 1
```

Description: restore native vlan to default native vlan

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/5       on           802.1q         trunking      20
Fa0/7       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/5       1,10,20,30
Fa0/7       1-1005

Port        Vlans allowed and active in management domain
Fa0/5       1,10,20,30
Fa0/7       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/5       10,30
Fa0/7       1,10,20,30
```

Description: on int 0/7 the vlan has returned to native vlan 1, which is the default vlan.

VLAN ON ROUTER

To configure VLAN on Router

```
VLAN1 : 192.168.1.0/24
VLAN10: 192.168.10.0/24
VLAN20: 192.168.20.0/24
VLAN30: 192.168.30.0/24
```

Description: Configuring VLANs on a Router

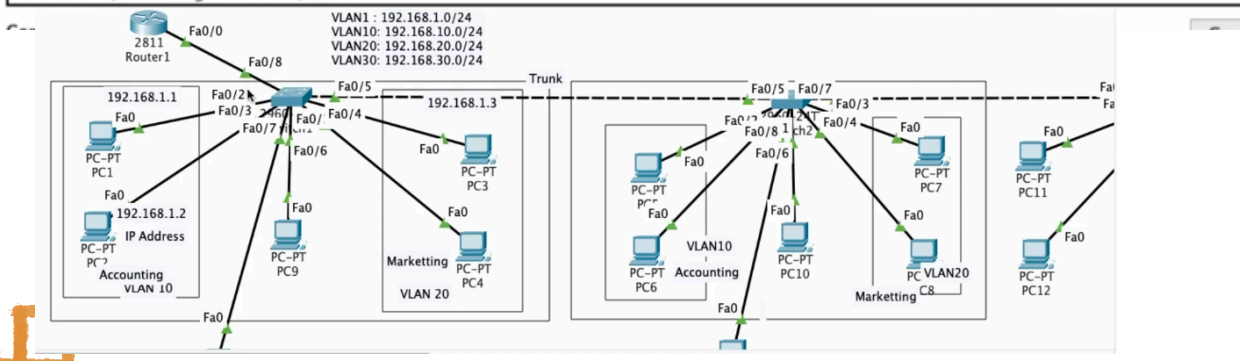
```
Router(config-if)#int fa0/0.10
Router(config-subif)#
```

Description: we enter the sub-interface VLAN fa0/0.10 (sub interface)

```
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#ip address 192.168.10.1
255.255.255.0
```

Description: defines VLAN 10 and its IP address and subnet mask.

```
Router(config-subif)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/0.10     192.168.10.1    YES manual up                    up
FastEthernet0/0.20     192.168.20.1    YES manual up                    up
FastEthernet0/0.30     192.168.30.1    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router(config-subif)#
```



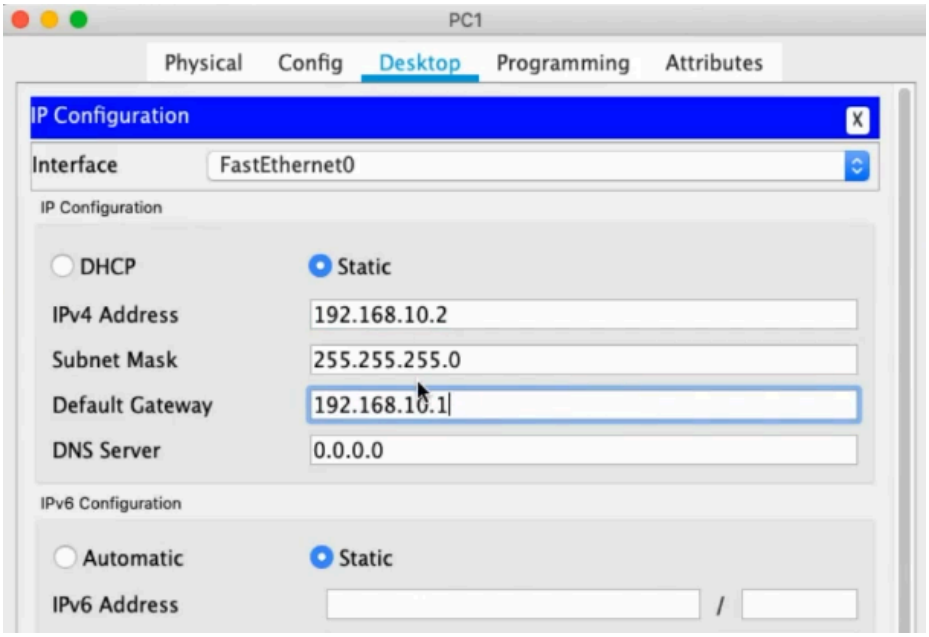
Description: displays the interface that has been configured on the router to the switch

Trunk Router

to use trunk on router by connecting int out to switch, namely fa0/8

```
Switch(config)#int fa0/8
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport mode trunk\
                                    ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up
```

Description: we can insert int fa0/8 into the trunk so that it can connect to the switch.



Description: configure for Vlan 10 the default gateway that we will use... the IP address must not be the same as the router, that's why on PC 1 it becomes 10.2

DHCP SERVER

Setting DHCP Server

```
Router(config)#ip dhcp pool VLAN1
Router(dhcp-config)#
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
```

Description: configure Vlan 1 (default) for all end users, IP addresses, subnet masks, default gateways and DNS servers**.**

```
Router(config)#ip dhcp pool VLAN20
Router(dhcp-config)#
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#
Router(dhcp-config)#exit
```

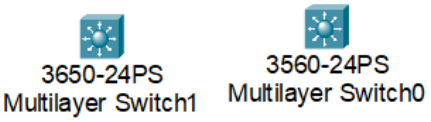
```
Router(config)#ip dhcp pool VLAN30
Router(dhcp-config)#
Router(dhcp-config)#network 192.168.30.0 255.255.255.0
Router(dhcp-config)#
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#exit
```

Description: Configure Vlan 20 and 30 for all end users, IP addresses, subnet masks, default gateways and DNS servers**.**

SVI

setting up a virtual switch interface using a multilayer switch (SVI)

```
Switch(config)#int vlan 1
Switch(config-if)#
Switch(config-if)#ip address 192.168.1.1
255.255.255.0
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#
```



Description: configure directly to Vlan 1 IP address and its subnet mask, we do not need to use encapsulation to configure SVI on the switch.

```
Switch(config)#int vlan 10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interfac
Vlan10, changed state to up

Switch(config-if)#ip address 192.168.10.1
255.255.255.0
```

```
Switch(config)#do show ip interface brief
```

```
Vlan1                  192.168.1.1     YES manual administratively down down
Vlan10                 192.168.10.1    YES manual up                    up
Vlan20                 192.168.20.1    YES manual up                    up
Vlan30                 192.168.30.1    YES manual up                    up
Switch(config)#
```

```
Switch(config)#int vlan 1
Switch(config-if)#
Switch(config-if)#no shutdown
```

```
Vlan1                  192.168.1.1     YES manual up                    up
Vlan10                 192.168.10.1    YES manual up                    up
Vlan20                 192.168.20.1    YES manual up                    up
Vlan30                 192.168.30.1    YES manual up                    up
```

Description: fill in the VLAN on the switch using the SVI method, then to check you can go to do show ip int brief, and for VLAN1 we will do no shutdown

SVI

set layer 2 to layer 3

```
Switch#show ip route
Default gateway is not set

Host                 Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty
```

Description: Multi layerswitch switch virtual interface by default Multi layerswitch is layer 2 _*show ip route*_ if it is still layer 2 the description is still there *ICMP redirect cache is empty" setting up the switch virtual interface using a multilayer switch (SVI) we will change to layer 3 so that the inter-vlan can be connected using a multilayer switch we will change to layer 3

```
Switch(config)#ip routing
Switch(config)#
Switch(config)#
Switch(config)#exit
```

Description: to change from layer 2 to layer 3

```
Switch#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, Vlan1
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.30.0/24 is directly connected, Vlan30
```

Description: Layer 3 is now out

SVI

DHCP with SVI

```
Switch(config)#ip dhcp pool VLAN1
Switch(dhcp-config)#
Switch(dhcp-config)#
Switch(dhcp-config)#
Switch(dhcp-config)#network 192.168.1.0 255.255.255.0
Switch(dhcp-config)#
Switch(dhcp-config)#default-router 192.168.1.1
Switch(dhcp-config)#
Switch(dhcp-config)#dns-server 8.8.8.8
Switch(dhcp-config)#
Switch(dhcp-config)#exit
```

Description: Change the IP address, default gateway and DNS using DHCP so that they are filled in automatically.

```
Switch(config)#ip dhcp pool VLAN10
Switch(dhcp-config)#
Switch(dhcp-config)#network 192.168.10.0 255.255.255.0
Switch(dhcp-config)#
Switch(dhcp-config)#default-router 192.168.10.1
Switch(dhcp-config)#
Switch(dhcp-config)#dns-server 8.8.8.8
Switch(dhcp-config)#
Switch(dhcp-config)#exit
```

Description: Change the IP address on Vlan 10, default gateway and DNS using DHCP so that it is filled automatically.

Remote Telnet

Remote Access with Telnet

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#line vty 0 ?
  <1-15>  Last Line number
  <cr>
Router(config)#line vty 0 2
Router(config-line)#password telnet123
Router(config-line)#login
Router(config-line)#transport input telnet
```

Description: Enter line (login entry) to remote telnet, telnet input transport is only used using telnet client

```
Router(config-line)#transport input all
```

Description: input can be either SSH or Telnet.

```
Router(config-line)#transport input ssh
```

Description: There are two input methods, namely SSH.

```
Router(config)#enable secret
```

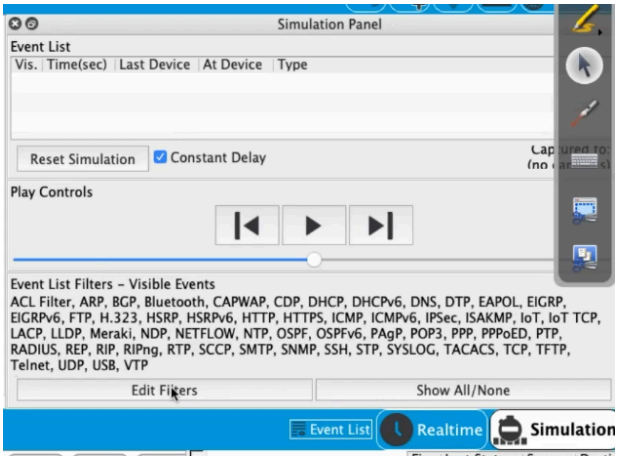
Description: on the remote we must use enable secret to be able to enter config or privilege mode on the router.

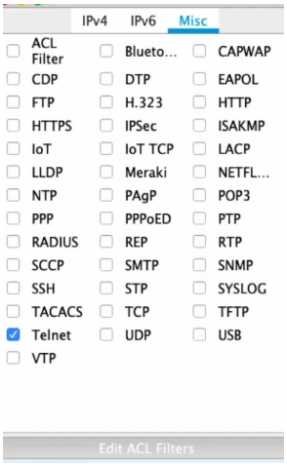
```
Router(config)#username user1 secret password1
Router(config)#
Router(config)#
Router(config)#line vty 0 2
Router(config-line)#login local
Router(config-line)#exit
```

Description: add username and password to telnet

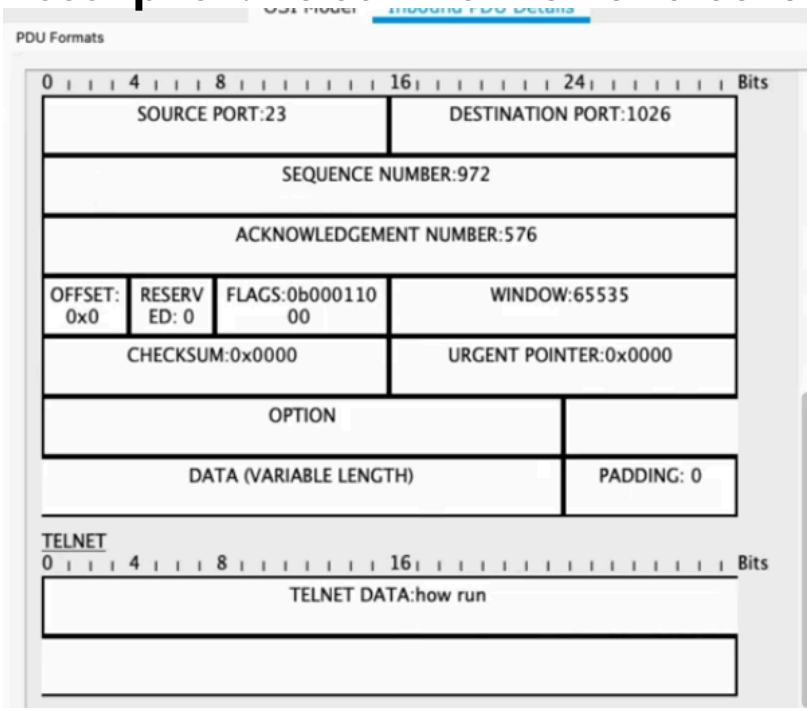
Remote Telnet

Using Telnet is not secure and can be spoofed/wiretapped





Description: we edit the filter towards telnet only



Description: on inbound telnet, it is very easy to tap because you can see the cli that we type.

Remote SSH

Remote Access SSH

```
Router(config)#enable secret
Router(config)#username user1 secret password1
Router(config)#hostname Core-Router
Core-Router(config)#line vty 0 15
Core-Router(config-line)#transport input ssh
Core-Router(config)#ip domain-name agunacourse.com
```

Description: First we will create an enable secret for the router, and second for the username and password on the client. Then create the path, a maximum of 15 paths (0-15). Enter the domain IP and transport input ssh

```
Core-Router(config)#crypto key generate rsa
The name for the keys will be: Core-Router.agunacourse.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
```

Description: Enter the RSA key generate to perform remote SSH, and enter the ideal modulus of 1024.

```
Switch(config)#int vlan 10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed st

Switch(config-if)#ip address 192.168.10.30 255.255.255.0
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#exit
```

SWITCH!!

Description: to do it remotely using a router, we will enter the VLAN IP address on the switch first, be free and choose one!

Remote SSH

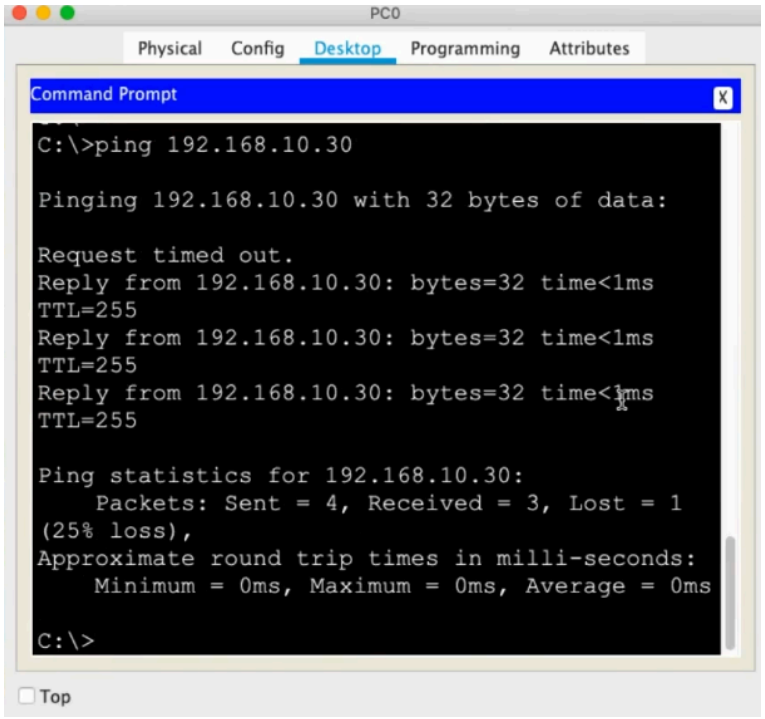
Ping from switch to router, switch configuration

```
Switch(config)#do show ip interface brief
Vlan10                 192.168.10.30   YES manual up                    up
```

Description: IP vlan has been issued on the switch

```
Switch(config)#do ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms
```

Description: Ping test to fellow VLAN10, we see it has succeeded! (success) . (failed)...at first failed then requested and succeeded!



Description: We try to ping from the end user to the switch.

Remote SSH

Setting Default Gateway IP on Switch

```
Switch(config)#ip default-gateway 192.168.10.1
```

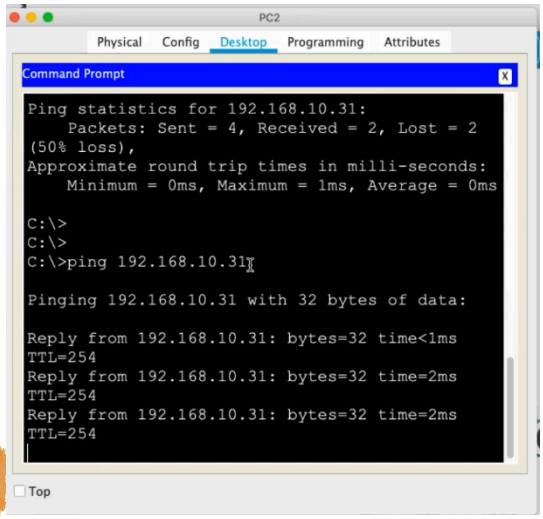
Description: to send packets between VLANs and switches

```
C:\>ping 192.168.10.30

Pinging 192.168.10.30 with 32 bytes of data:

Reply from 192.168.10.30: bytes=32 time=1ms
TTL=254
Reply from 192.168.10.30: bytes=32 time<1ms
TTL=254
Reply from 192.168.10.30: bytes=32 time<1ms
TTL=254
```

Description: Ping test between VLANs

```
Switch(config)#int vlan 10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state

Switch(config-if)#ip address 192.168.10.31 255.255.255.0

Switch(config)#ip default-gateway 192.168.10.1
```

Description: We do the configuration to another Switch



Description: We test the ping on the switch that has been configured!

Konfigurasi SSH pada switch

Remote SSH

```
Switch(config)#int vlan 10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, chan
Switch(config-if)#ip address 192.168.10.30 255.255.255.0

Switch(config)#ip default-gateway 192.168.10.1
Switch(config)#username user1 secret password1
```

Description: add username and password

```
Switch(config)#hostname SW1
SW1(config)#
SW1(config)#
SW1(config)#ip domain-name agunacourse.com
```

Description: change hostname and domain

```
SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.agunacourse.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW1(config)#
*Mar 2 6:29:20.618: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

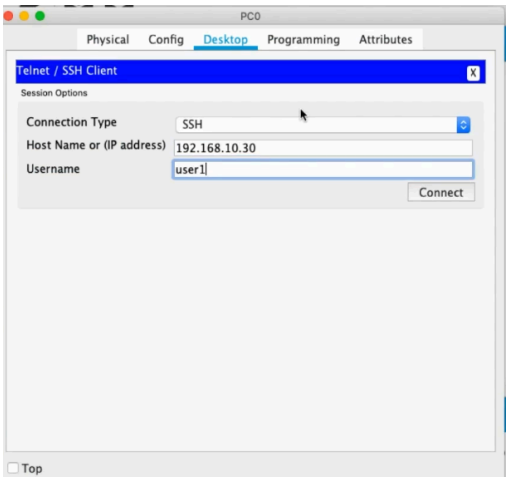
Description: we do the key and its bits

```
SW1(config)#line vty 0 4
SW1(config-line)#login local
SW1(config-line)#transport input ssh
SW1(config-line)#
SW1(config-line)#exit
SW1(config)#enable secret cisco
```

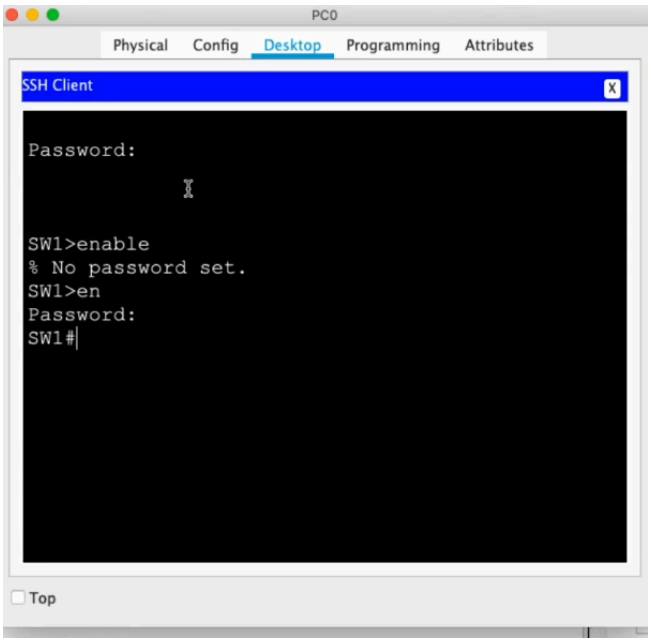
Description: We enter the login path, namely 0 4 and local login so that login uses username and password. then transport input ssh. and enable secret

Remote SSH

Konfigurasi SSH pada switch



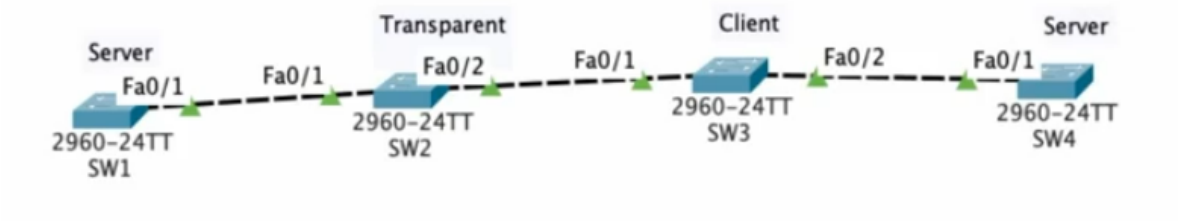
Description: SSH client input, namely SSH, IP address and username.



Description: We enter the password that we created earlier, namely "password1". Then enter privilege mode by entering the password that we created earlier, namely "cisco".

VTP

Configuration VTP (Vlan trunk protocol)



Description: We prepare the topology that is already in trunk mode to perform VTP

- **Server :** Switches in this mode can create, delete, and modify VLANs across the VTP domain. Any changes made to this switch will be propagated to all other switches in the same domain.
- **Transparent:** Switches in this mode do not participate in VLAN management directly via VTP. They do not broadcast VLAN information received from other switches, but forward it to other switches. However, VLANs created on this switch are not propagated to other switches.
- **Client:** Switches in this mode only accept and apply VLAN information received from switches in server mode. They cannot create, delete, or modify VLANs.

VTP

Configuration VTP Server, VTP Transparent, VTP Client

```
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#
Switch(config)#vtp domain AGUNACOURSE
Changing VTP domain name from NULL to
AGUNACOURSE
Switch(config)#
Switch(config)#vtp password 123
Setting device VLAN database password to 123
```

```
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)#
Switch(config)#vtp domain AGUNACOURSE
Domain name already set to AGUNACOURSE.
Switch(config)#
Switch(config)#vtp password 123
Setting device VLAN database password to 123
Switch(config)#
```

```
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#
Switch(config)#vtp domain AGUNACOURSE
Changing VTP domain name from NULL to
AGUNACOURSE
Switch(config)#
Switch(config)#vtp password 123
Setting device VLAN database password to 123
```

Description: We enter vtp mode, then enter the domain name and vtp password. the domain name and password must be the same! with other vtp

VTP

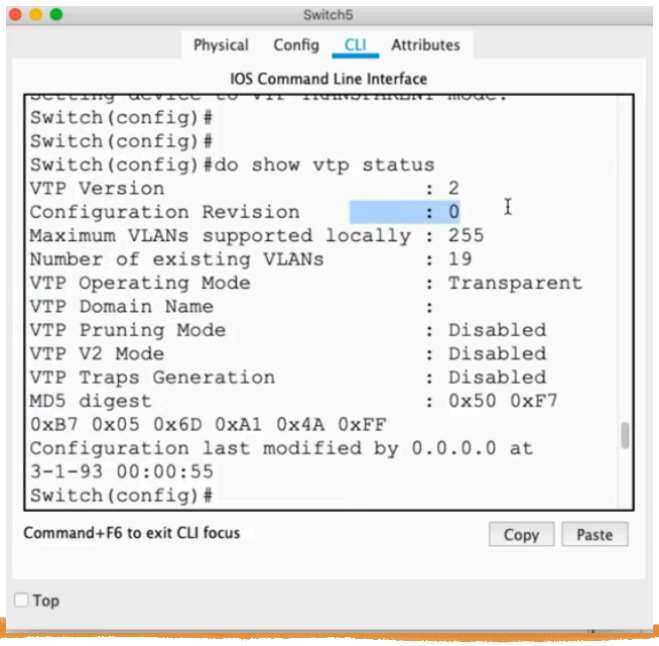
Solving Revision Number

```
Switch(config)#do sho vtp status
VTP Version                     : 2
Configuration Revision          : 14
Maximum VLANs supported locally : 255
Number of existing VLANs        : 19
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x28 0x8F
0x5B 0xDD 0x72 0xED 0xA1 0x33
Configuration last modified by 0.0.0.0 at
3-1-93 00:00:55
Local updater ID is 0.0.0.0 (no valid interface
found)
```

Description: Example case. when we insert a new switch that has VLAN. that configuration revision takes from the largest revision number.

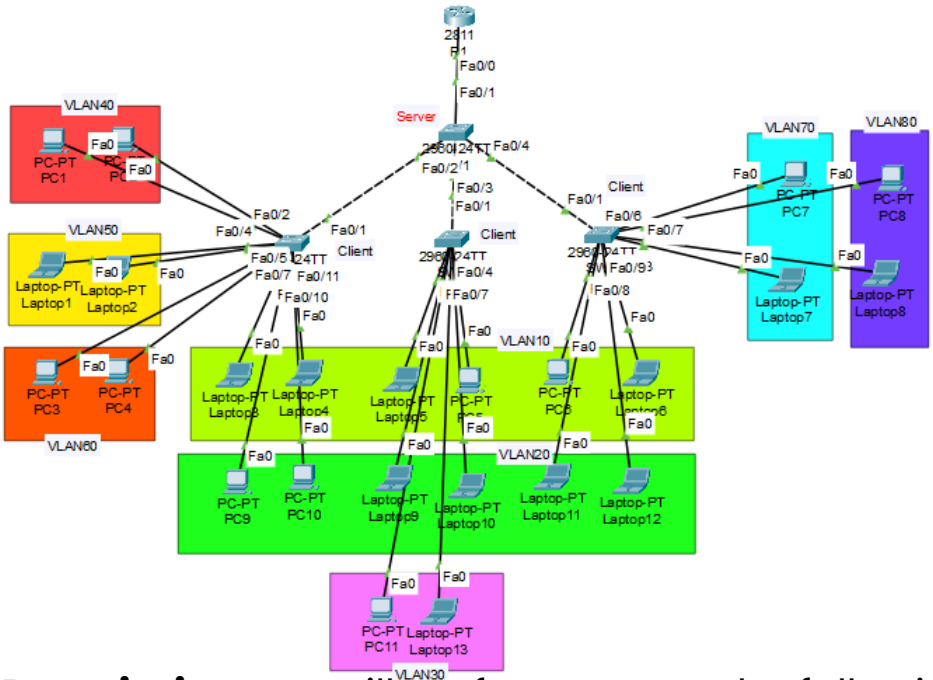
```
Switch(config)#vtp mode transp
Setting device to VTP TRANSPARENT mode.
```

Description: For the latest switch, we will make it transparent mode first so that the configuration revision changes to 0.



VTP

Practice Using VTP



Description: We will perform VTP on the following topology.

```
Router(config-if)#int fa0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interfac
FastEthernet0/0.10, changed state to up

Router(config-subif)#
Router(config-subif)#enc do 10
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#ip address 192.168.10.1
255.255.255.0
```

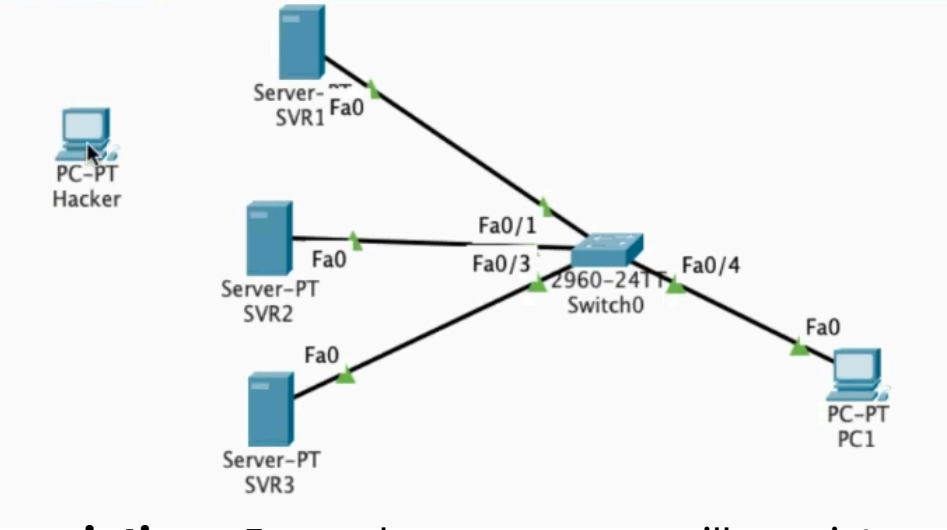
Description: perform VLAN configuration on the router

```
Router(config)#ip dhcp pool VLAN10
Router(dhcp-config)#
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
```

Description: DHCP configuration on the router

PORT SECURITY

Practice Using Port Security



Description: Example case, we will register the end user interface connected to the switch..using port security. then our PC1 will play a role in combining the interface to the switch that has not been registered. and hackers try to enter the interface

```
Switch(config)#int fa0/1
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#do show int fa0/1 switchpor
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
```

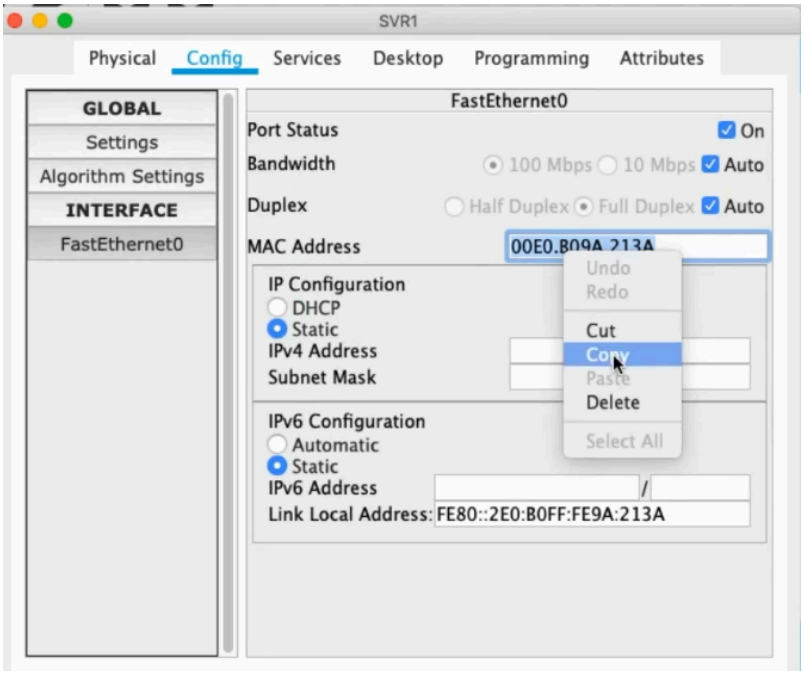
Description: we will change it to access mode

```
Switch(config-if)#switchport mode access
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#swit
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security
```

Description: switchport port-security

PORT SECURITY

Practice Using Port Security



Description: We copy the MAC address of the end user.

```
Switch(config-if)#switchport port-security mac-address
00E0.B09A.213A
```

Description: we enter the MAC address into the port-security

```
Switch(config-if)#switchport port-security maximum 1
```

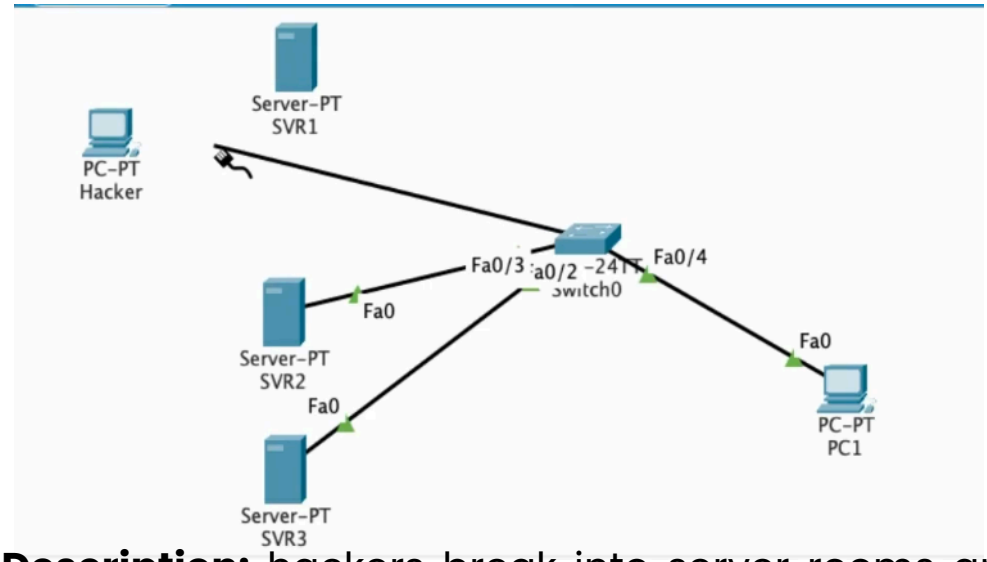
Description: we enter the MAC address into the port-security, maximum 1 end user on 1 interface.

```
Switch(config-if)#switchport port-security violation
shutdown
```

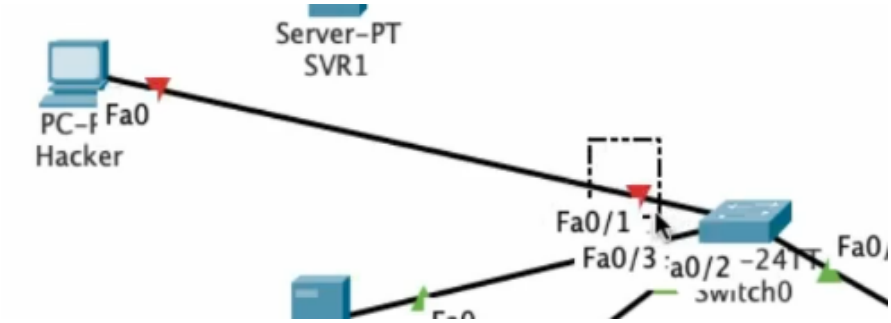
Description: We enter the action that occurs on the interface if an end user tries to enter another interface whose MAC address is not registered. if someone tries to break in. will be shutdown!

PORT SECURITY

Test Port Security



Description: hackers break into server rooms and connect to interfaces



Description: we see the interface is immediately shut down

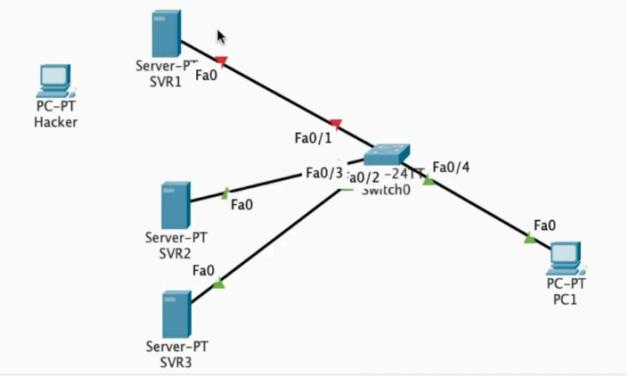
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
```

```
Switch(config-if)#do show port-security int fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
```

Description: fa0/1 changed to down

PORT SECURITY

Test Port Security



Description: we connect the interface to the server again. The cable that was just used by the hacker

```
Switch(config-if)#int fa0/1
Switch(config-if)#
Switch(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
down
```

Description: we see the interface to the server is still down

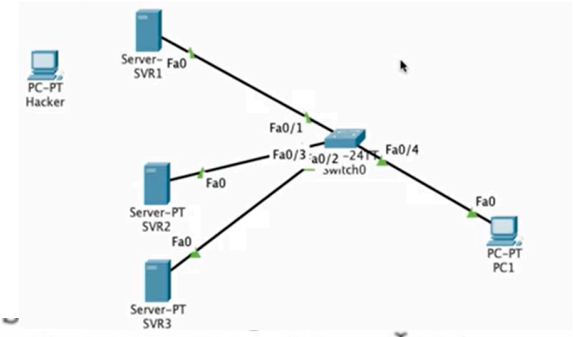
```
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
Switch(config-if)#
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
```

Description: SOLUTION! We shutdown to enable port security again to the server. After that we do no shutdown

```
Switch(config-if)#do show port-security int fa0/1
Port Security              : Enabled
Port Status                : Secure-up
```

MAC STICKY

Mac Adress Sticky



Description: we will try to connect fa0/2 with the security port using sticky Mac address (recorded automatically)

```
Switch(config)#int fa0/2
Switch(config-if)#
Switch(config-if)#switchport mode access
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security
```

```
Switch(config-if)#do show port-security int fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
```

Description: We activate port security

```
Switch(config-if)#switchport port-security mac-address
sticky
```

Description: We activate sticky mac-address

```
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#
Switch(config-if)#swi
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security vi
Switch(config-if)#switchport port-security violation shu
Switch(config-if)#switchport port-security violation
shutdown
```

Description: We enter the maximum and violation shutdown.

Description: We will send a packet so that the sticky MAC address can be read!

```
Total MAC Addresses          : 1
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 1
Last Source Address:Vlan     : 00E0.8F10.23C1:1
```

SWITCHPORT SECURITY

Penjelasan 3 Switchport security

switchport port-security violation { **protect** | **restrict** | **shutdown** }

no switchport port-security violation { **protect** | **restrict** | **shutdown** }

Syntax Description

protect	Drops all the packets from the insecure hosts at the port-security process level but does not increment the security-violation count.
restrict	Drops all the packets from the insecure hosts at the port-security process level and increments the security-violation count.
shutdown	Shuts down the port if there is a security violation.

Protect : if the security-violation count is not entered, it will still block hacker access to the hacker interface. and will not shutdown the interface.

```
Switch(config-if)#do show port-security int fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00E0.8F10.23C1:1
Security Violation Count   : 0
```

- **Protect:** If an unknown device tries to connect, packets from that device are dropped without notification or logging. The port remains active and is not affected by the violation.
- **Restrict:** If an unknown device tries to connect, packets from that device are dropped, and the violation is logged. However, the port remains active and can be used by legitimate devices.
- **Shutdown**: If a violation occurs, the port is immediately shut down, so no devices can connect to it until the port is manually re-enabled.

VIOLATION PROTECT

Practice Violation Protect

```
Switch(config-if)#int fa0/3
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport mode access
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#swi
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security mac-ad
Switch(config-if)#switchport port-security mac-address st
Switch(config-if)#switchport port-security mac-address
sticky
```

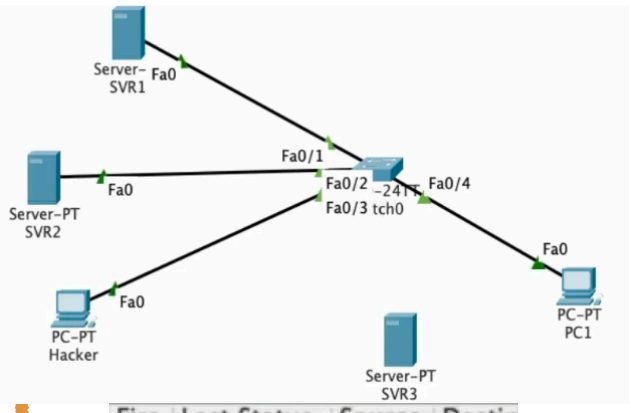
```
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#
Switch(config-if)#sw
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security vi
Switch(config-if)#switchport port-security violation pro
Switch(config-if)#switchport port-security violation protect
```

Protect: we put the switch port fa0/3 into access mode then into the security port, and give the mac adrss sticky. we create a maximum of 1 end user and we put it in protect

```
Switch(config-if)#do show port-security int fa0/3
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.42E9.619C:1
Security Violation Count   : 0
```

```
Last Source Address:Vlan   : 000A.4150.9C57:1
Security Violation Count   : 0
```

Protect : the output after sending the package will display the Mac address. and the empty visualization count is not added.



Fire	Last Status	Source	Destin
	Failed	Hacker	SV
	Failed	Hacker	SV

```
Switch(config-if)#do show port-security int fa0/3
Port Security              : Enabled
Port Status                : Secure-up
```

Protect: when hackers keep trying to get in. interface up but send packet down.. but when connected to the server. will not shutdown!

VIOLATION RESTRICT

Practice Violation Restrict

```
Switch(config-if)#int fa0/5
Switch(config-if)#
Switch(config-if)#sw
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security
Command rejected: FastEthernet0/5 is a dynamic port.
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport mode access
Switch(config-if)#
Switch(config-if)#swi
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security
```

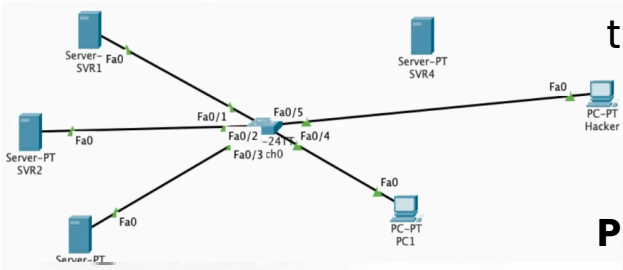
```
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#
Switch(config-if)#sw
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security vi
Switch(config-if)#switchport port-security violation r
Switch(config-if)#switchport port-security violation
restrict
```

Restrict: we put the switch port fa0/5 into access mode then into the security port, and give the mac adrss sticky. we create a maximum of 1 end user and we put it in restrict

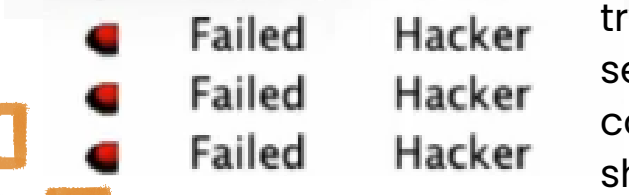
```
Switch(config-if)#do show port-security int fa0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 000A.4150.9C57:1
Security Violation Count   : 4
```

```
Source Address:Vlan    : 000A.4150.9C57:1
ity Violation Count    : 4
```

Protect: we see the output after sending the packet, the Mac address will appear. and the visualization count is added 4 (4 times the hacker sent the packet)



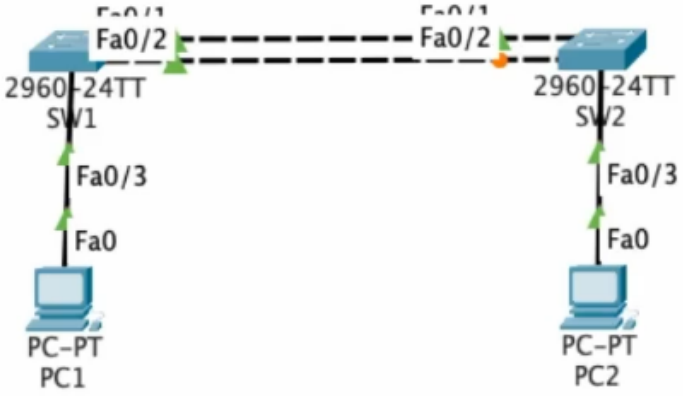

```
Switch(config-if)#do show port-security int fa0/3
Port Security              : Enabled
Port Status                : Secure-up
```



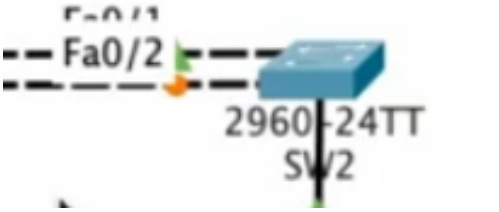
Protect: when hackers keep trying to get in. interface up but send packet down.. but when connected to the server. will not shutdown!

STP

Spanning Tree Protocol (STP)

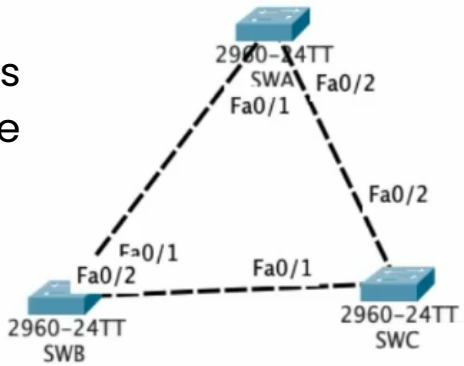


STP : STP in this topology ensures that only one of the two paths between Switch1 and Switch2 is used to avoid loops. The other path remains ready to be used in case the primary path experiences problems. This keeps the network stable and free from disruptions that can be caused by loops.



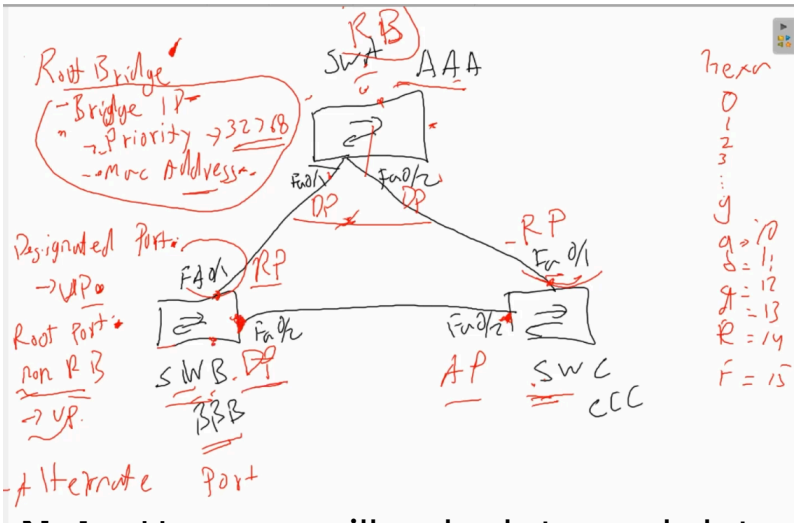
Fa0/2 : On Fa0/2 connected to switch2 orange means it is blocked. STP is blocking...STP is already active by default

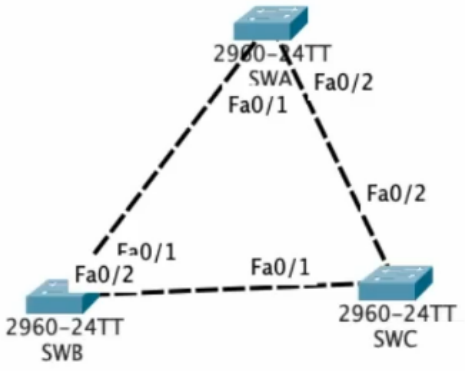
STP: In the following 3 switches we can see, and we will calculate which int is blocked by STP.



BLOCKING STP

Choose Blocking STP





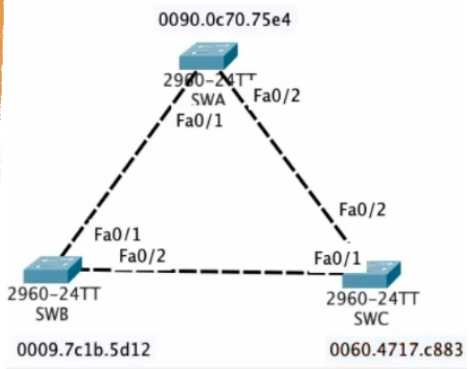
Note: Here we will calculate and determine the right Blocking. We determine which is the Root Bridge, Designed Port and Root Port (Non Root Bridge) and Alternate Port. In determining RB, DP, RP and AP we look at the MAC address, Bridge IP or Priority (32768)

In the above case

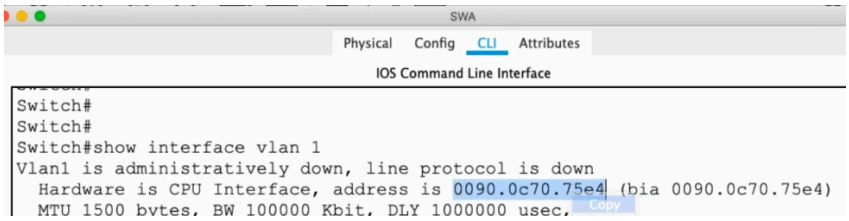
- **Switch A** has the smallest Mac Address AAA then it will RB status UP
- **Fa0/1 and 0/2** will automatically DP Status Up Switch B has the next smallest Mac Address BBB then it will DP and its Int will RP status UP
- **Switch C** has the largest Mac Address CCC then its AP status will be DOWN

BLOCKING STP

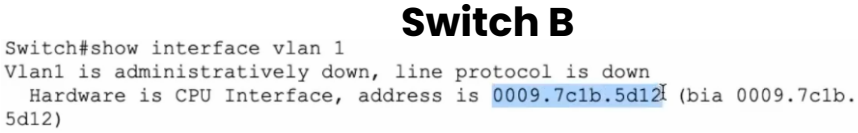
Latihan Menentukan Block Port



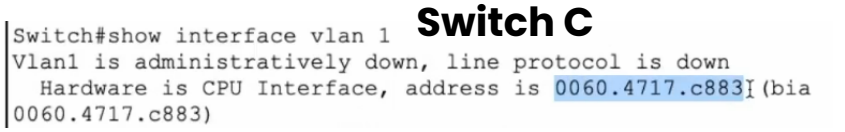
Switch A



Switch B



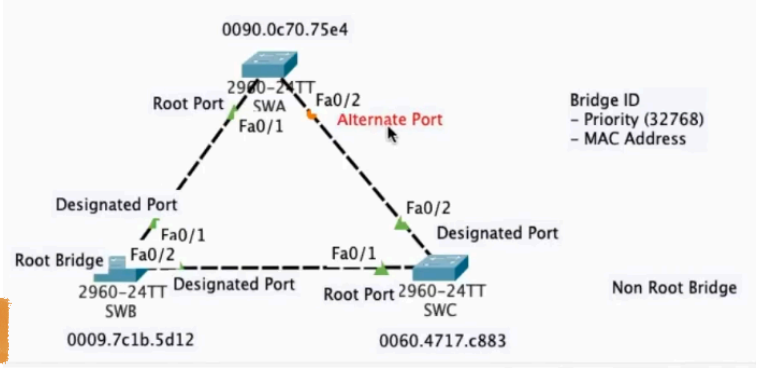
Switch C



Note: in SW.A, SW.B and SW.C we will note the MAC address. In determining RB, DP, RP and AP we look at the MAC address, Bridge IP or Priority (32768)

In The Case Above

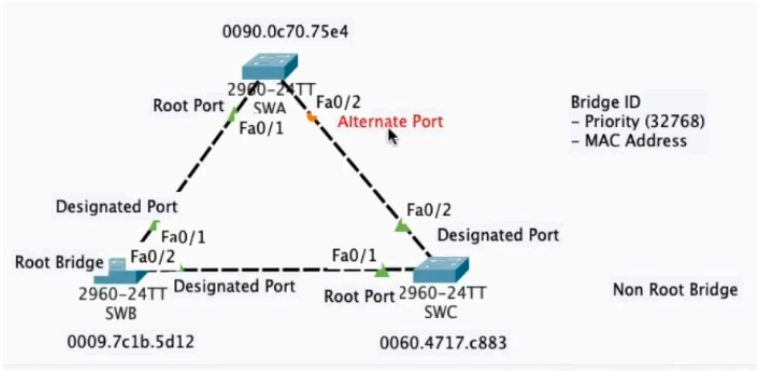
- **Root Bridge :** To Lower Switch B 0009 (Up)
- **Designated Port :** Switch B (Fa0/1, Fa0/2) (Up)
- **Root Port (The Closest to Designated Port) :** Switch C Fa0/1 dan Switch A Fa0/1 (Up)
- **Designated Port :** Fa0/2 Switch C (Up) Mac Adress lebih kecil dan menang 0060
- **Alternate Port :** Switch A Fa0/2 (Block)



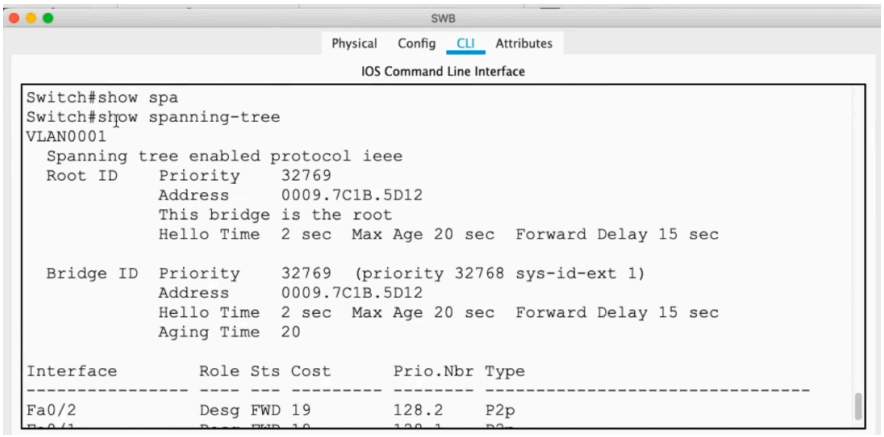
Final : Here we have calculated which block ports and it is correct that the alternate port is blocked by the interface!

STP VERIFY

Verify STP



Note: Here we can see the root bridge is on switch B.



Note : On switch B, the spanning tree is connected to Vlan 1. We only have Vlan 1.

- **Root ID :** root bridge information mac address information on root bridge
- **Bridge ID :** Information related to Priority is 32769 (Priority 32768 is added to the Vlan, which is **1**)

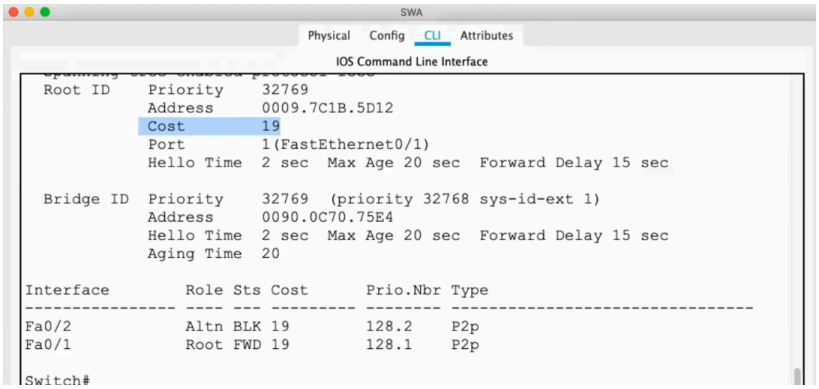
Example Case *Vlan 30 means (32768 + 30) : Priority 32799*
Mac address : Mac address information on the switch

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
```

Note: the entire interface role is Design Port, because on switch B it is Root Bridge, forward status (not blocked)

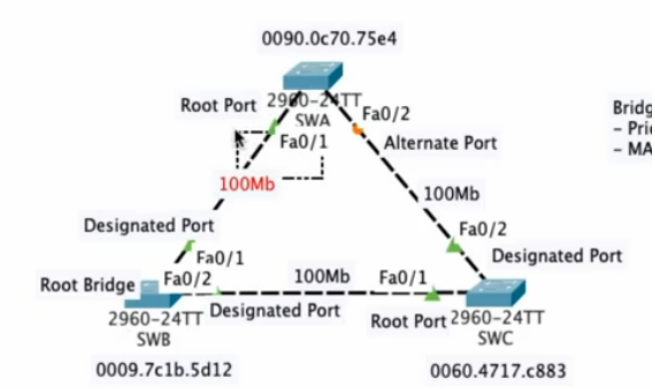
COST STP

Cost STP

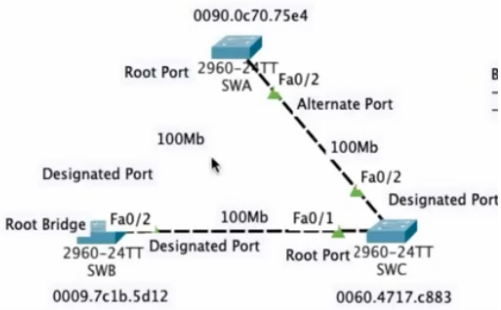


COST
10Mb -> 100
100Mb -> 19
1Gb -> 4
10Gb -> 2

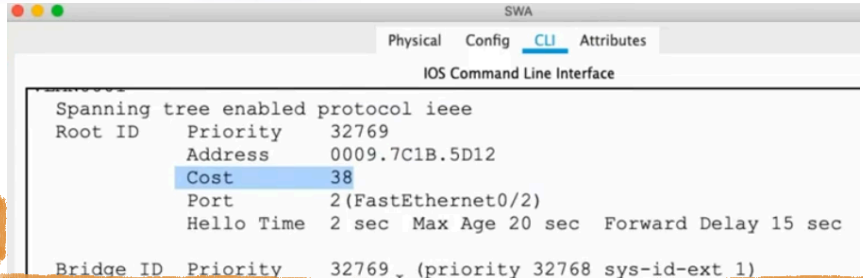
Cost : Switch A is the fastest route to Switch B (Root Bridge), Cost is based on Bandwidth on the interface



Cost : We see here that the closest cost is from switch B to switch A.



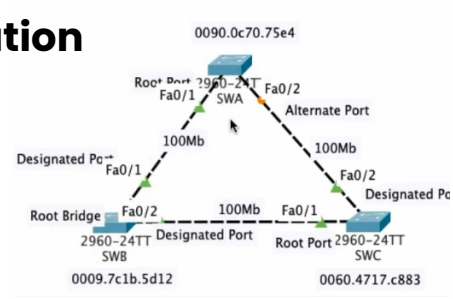
Cost is : In the case where the interface cable is unplugged, the route changes to 19 + 19, namely: 38



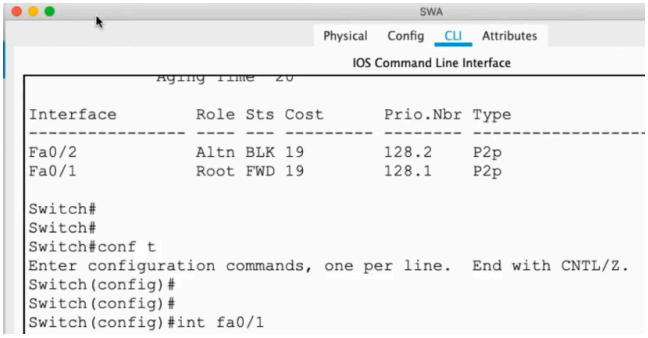
BANDIWITH

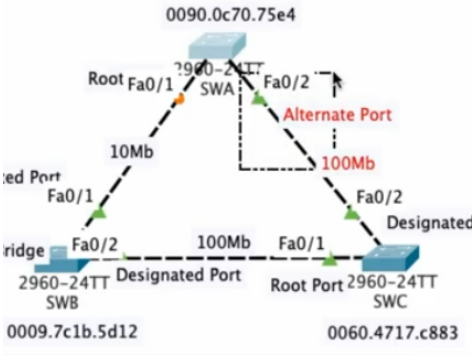
Bandwidth Manipulation

```
COST
10Mb -> 100
100Mb -> 19
1Gb -> 4
10Gb -> 2
```



Change Bandwith : In the above case, we will change the speed bandwidth on fa0/1 from switch A to switch B from 100MBPS to 10 MBPS.



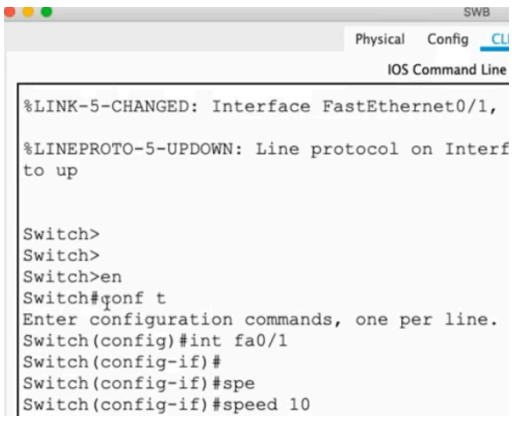



```
Switch(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
Switch(config-if)#speed 10
Switch(config-if)#
```

Change Bandwith : this case we have changed the bandwidth on int fa0/1 from switch B to A. from 100mbps to 10mbps.

from switch A to B the cost changed from 19 to 100

we see the alternate port changed to a higher cost of 100




```
Interface        Role Sts Cost
---------------- ---- --- ---------
Fa0/2            Root FWD 19
```

PVSTP

Per Vlan Spanning Tree (PVSTP)

```
Switch(config)#int rang fa0/1-2
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#switchport mode trunk
```

Switch Mode Trunk: we can connect int trunk

```
Switch(config)#vlan 2
Switch(config-vlan)#vlan 3
```

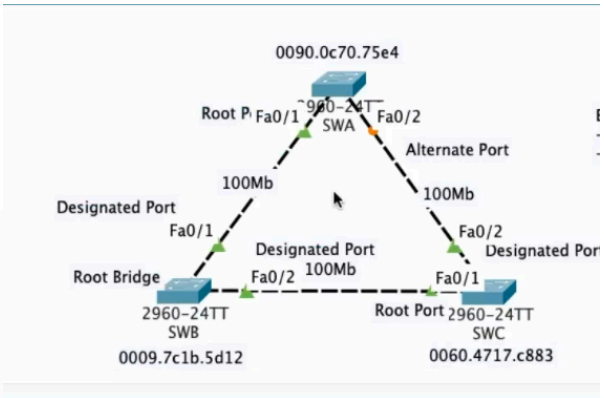
Switch Mode Trunk: we make vlan on switch

```
Switch#show spanning-tree
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0009.7C1B.5D12
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0090.0C70.75E4
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
```

```
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    32770
             Address     0009.7C1B.5D12
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32770  (priority 32768 sys-id-ext 2)
             Address     0090.0C70.75E4
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

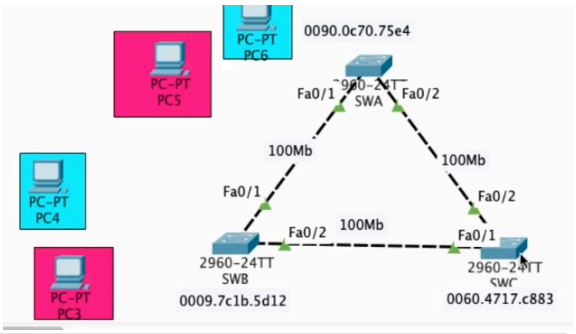
```
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID    Priority    32771
             Address     0009.7C1B.5D12
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32771  (priority 32768 sys-id-ext 3)
             Address     0090.0C70.75E4
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/2            Altn BLK 19        128.2    P2p
```

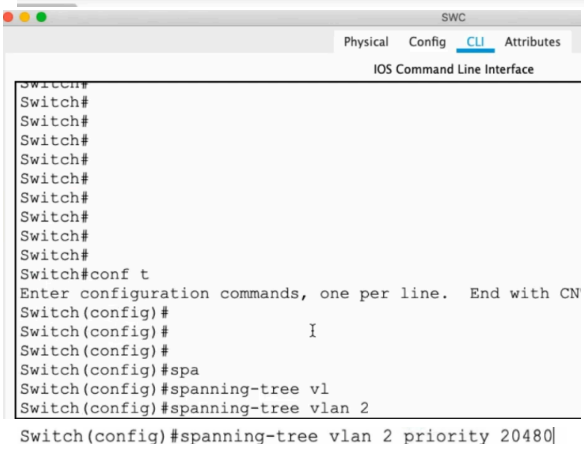


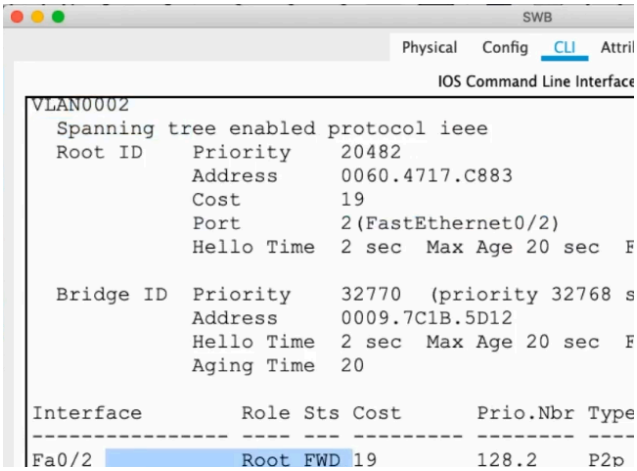
Show Spanning-tree : After we create a VLAN and connect between Interfaces with trunk mode. we can see information related to the spanning tree. Each VLAN has its own Spanning tree information

PVSTP

Manipulation Root Bridge In PVSTP





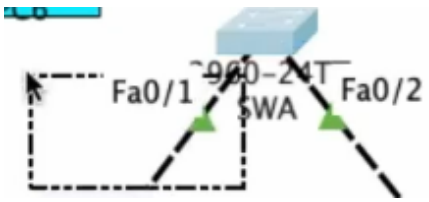


Note : there are 3 switches that are already connected by trunk and PVSTP. and in it there are already 3 Vlans namely Vlan 1 2 and 3. on Vlan 1 will be connected PC 3,5 (Pink) and Vlan 2 namely PC 4,6 (Blue).

Simulation: create a simulation, namely on Vlan 2 we will go through Switch C and Switch C will become the Root Bridge. and Vlan 1 through the Root Bridge

Spaning Vlan 2 : Spanning tree uses priority method so 20480. Remember if priority is lower it will win and Up. Fa0/1 and Fa0/2 it will be DP

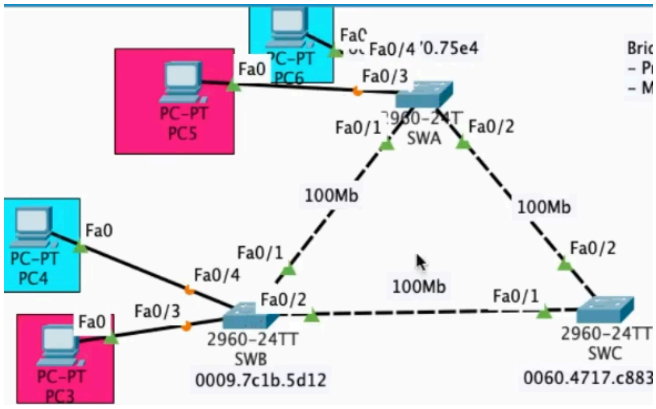
Spaning Vlan 2 SWB : On Switch B for VLAN Fa0/2 it is the root port.



Blocking Vlan 2 : Switch A Fa0/1

PVSTP

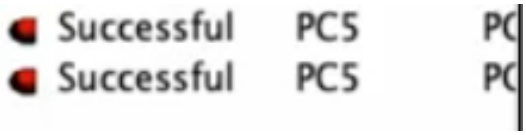
Simulation PVSTP



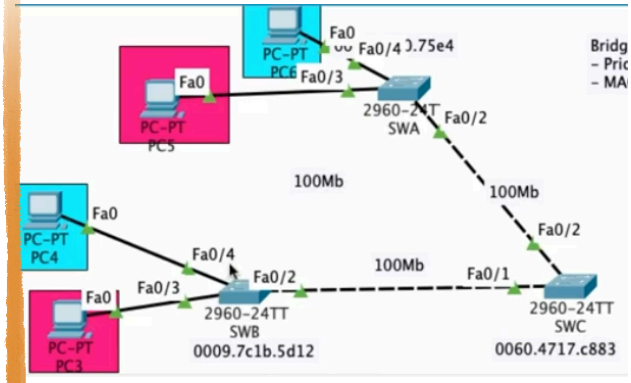
Test VLan 2: From PC 4 to PC 6, here we will see. From PC 4 it will go to Switch B then broadcast and be blocked on Fa0/1 switch A. which is in PVSTP Switch B - Switch C (Fa0/2) then - Switch A (Fa0/2).

Fa0/4 : On PC Fa0/4 we will connect the access mode to Vlan 2. PC 6 and PC 4

Test VLan 1: PC 3 (Vlan1) we will do a test sending a packet to PC 5. Via Switch B - Switch A. From PC 5 it will resend the packet to Switch B then resend it to Switch A and back to PC 3 and it will be successful.



Simulation PVSTP

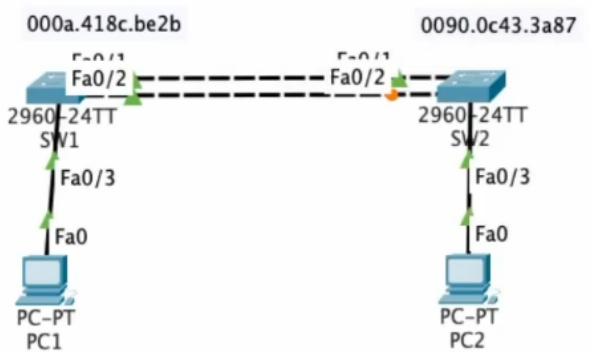


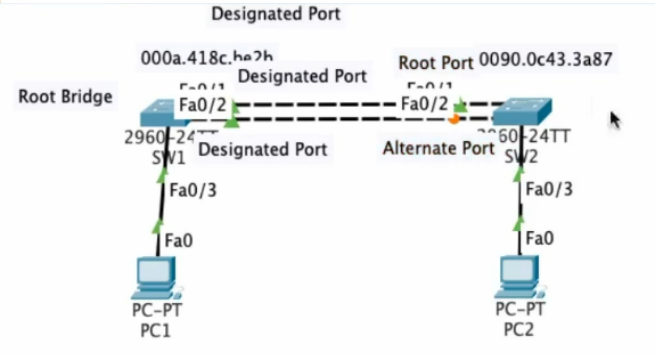
Test : What if we delete one of the interfaces? VLAN 1 and 2 will also pass through Switch C and will have no effect

PExplain: When the main is off. he will move to another switch which is connected automatically.

STP 2 SWITCH

Simulation STP 2 Switch





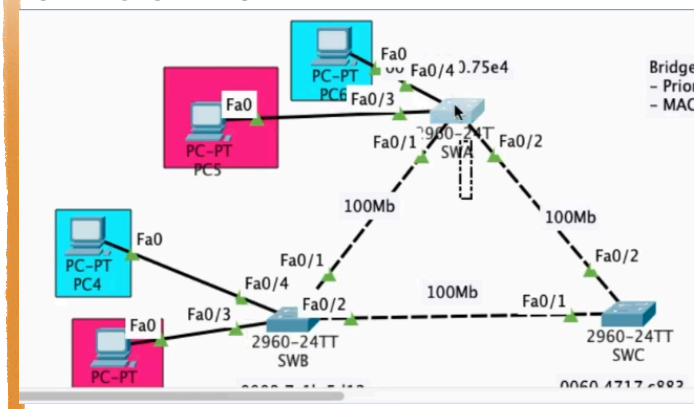
Root Bridge : 'See in our switch, we will look for the smallest Mac Address, which is 000a (Switch 1)

Designated Port : There is a topology where Switch 1 is already RB, then the interface connected to Switch 1 is the Designated Port (Fa0/1, and Fa0/2)

Root Port : In this topology we will see the one closest to the root bridge, the winner is the one closest to the root bridge, namely Fa0/1 on Switch 2.

Alternative Port: and the last one who loses will become an alternative port

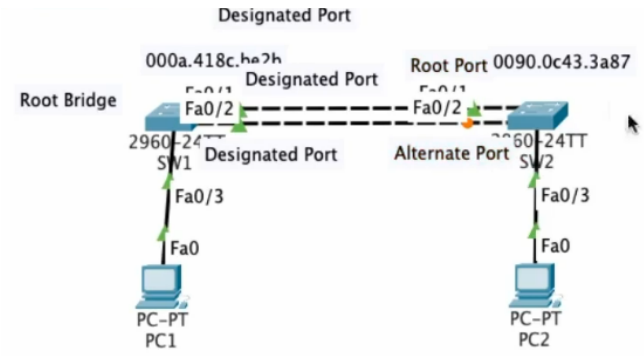
STP 3 Switch



Explanation: this case we can see, the cost is different and we can see that if SW B to SW A the cost is 19 and SW B to SW C to SW A the cost is 19+19+19 : 57

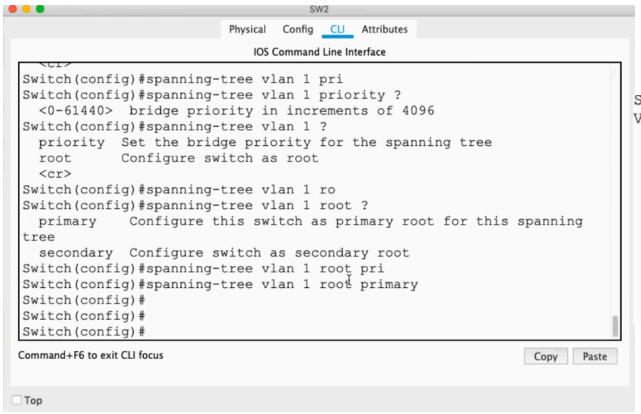
STP 2 Switch

Manipulate 2 STP Switches (change fa0/1 on switch 1 to blocking)



Case : Here we will change Switch 2 to Root Bridge. Here we will change the blocking on Switch 1 Fa0/1

Primary : switch 2 we will change to vlan 1 Spanning tree root primary. and will change to root bridge. and will make switch 2 become root bridge




```
Switch(config)#do show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0090.0C43.3A87
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0090.0C43.3A87
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
```

Priority : we see the priority changes to 24576. (This bridge is the root)

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

Switch 2 : We see on do show span. for Vlan it is connected Designated port (fa0/1-3) and forward (Up)

Switch 1 & 2 change bandwith (Fa0/1)

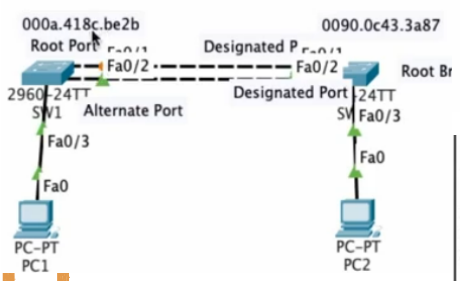
```
Switch(config)#int fa0/1
Switch(config-if)#
Switch(config-if)#spe
Switch(config-if)#speed 10
```

Bandwith : In this case it is visible. because we want a blocking switch on fa0/1 on switch 1. we will change the bandwidth (cost)

```
Switch(config)#int fa0/1
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#spe
Switch(config-if)#speed 10
```

Switch 1 Fa0/1

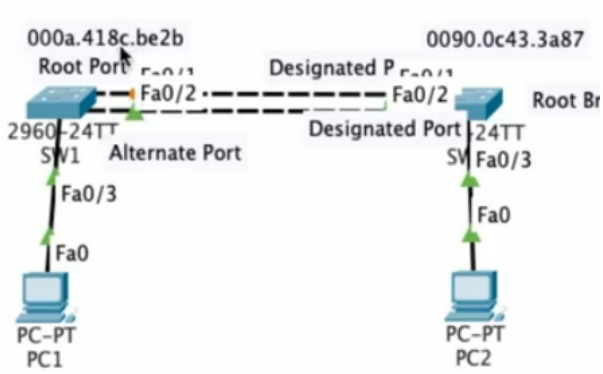
```
Spanning tree enabled protocol ieee
Root ID     Priority    24577
            Address     0090.0C43.3A87
            Cost        19
            Port        2(FastEthernet0/2)
            Hello Time  2 sec  Max Age 20
```




```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
Fa0/1            Altn BLK 100       128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/2            Root FWD 19        128.2    P2p
```

STP 2 Switch

STP Port States (Status Port) ON STP

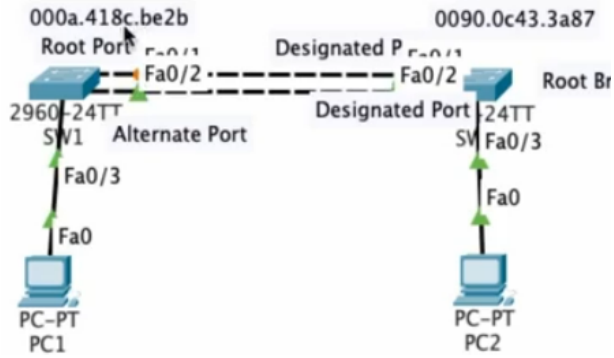


:

- **Listening:** Stages when we connect a cable, there will be a status stage.
- **Learning**: learning Spanning treee + mac addres (15 second)
- **Forward :** Finish and Up or running stages.
- because Root port will in **Blocking on** spanning tree (20 Second)

STP 2 Switch

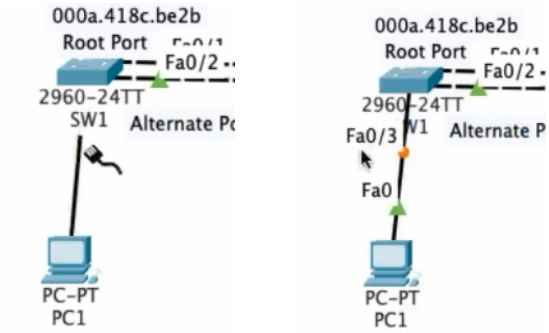
Spanning Tree Portfast (skip listening learning int connect to PC)



Case: Here we will see that Fa0/3 (PC) does not need to do listening and learning spanning tree. because spanning tree applies only for switch to switch.

```
Switch(config-if)#do show span
```

```
-------------------------------
Fa0/1           Altn BLK 100
Fa0/3           Desg LSN 19
Fa0/2           Root FWD 19
```




```
Fa0/1           Altn BLK 100
Fa0/3           Desg LRN 19
Fa0/2           Root FWD 19
```

Fa0/3 Switch 1: We can see that when we unplug the interface cable connected to the end (PC) it experiences Listening and learning. The point is to get forward it takes a long time, it has to take 15+15 = 30 seconds.

```
Switch(config-if)#int fa0/3
Switch(config-if)#
Switch(config-if)#spa
Switch(config-if)#spanning-tree por
Switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
```

Explanation: that portfast is used only for switchport interfaces connected to clients and should not be connected between switches. portfast has been configured to interface fa0/3. portfast will work in non-trunking mode! conclusion portfast will immediately forward without a pause!

```
Switch(config-if)#do show span
```

```
Fa0/1           Altn BLK 100
Fa0/3           Desg FWD 19
Fa0/2           Root FWD 19
```

ETHERCHANNEL

Etherchannel

Explanation: we will need 300MBPS in the switch, and there are 3 interface cables but on the existing interface. 1 cable (100MBPS). the switch is only connected with 1 interface cable, the remaining 2 are blocked by STP or also backup link. Etherchannel aims to combine 3 cables (physical) into 1 virtual cable. if all are active, the bandwidth changes to 300MBPS

Types of Etherchannel

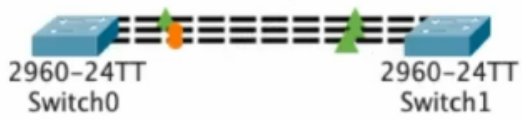
- **LACP (Link Aggregation Control Protocol):** An open standard protocol (IEEE 802.3ad) that combines multiple physical links into a single logical path to increase bandwidth and provide redundancy. Flexible for devices from multiple vendors. (For all vendors) ***(Layer2)***
- **PAgP (Port Aggregation Protocol):** A proprietary protocol from Cisco that functions similarly to LACP, but only on Cisco devices. Used to manage and aggregate physical links. (Cisco Only) ***(Layer2)***
- **Layer 3 EtherChannel:** EtherChannel that works in layer 3 (network). Used to combine links that can perform routing between networks or between VLANs, not just switching. (Multilayer switch only) ***(Layer3)***

Note: network engineers are increasingly using LACP (Link Aggregation Control Protocol) for several main reasons:

- **Open Standard:** LACP is an open standard protocol (IEEE 802.3ad), which makes it compatible with devices from various vendors. This provides flexibility in multi-vendor environments, where network devices from different manufacturers are used together.
- **Flexibelity:** LACP allows automatic merging of multiple physical links into a single logical path, with the ability to dynamically add or remove links as needed without disrupting network traffic..
- **Redundancy and Accurate:** LACP automatically determines which links are active and which are backup, so that if one link fails, traffic will automatically be redirected to the other active link. This increases network reliability.
- **Easy to Management:** LACP simplifies link aggregation management by providing an automated mechanism to manage and optimize bandwidth usage, thereby reducing the workload of engineers in monitoring and configuring the network.

ETHERCHANNEL LACP

Etherchannel LACP (All vendor)
(Layer2) **Configuration Trunk!**



LACP (Link Aggregation Control Protocol): An open standard protocol (IEEE 802.3ad) that combines multiple physical links into a single logical path to increase bandwidth and provide redundancy. Flexible for devices from multiple vendors. (For all vendors)

Konfigurasi Etherchannel LACP

Switch 0

```
Switch(config)#int rang fa0/1-3
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#sw
Switch(config-if-range)#switchport mod
Switch(config-if-range)#switchport mode trunk



Switch(config-if-range)#
```

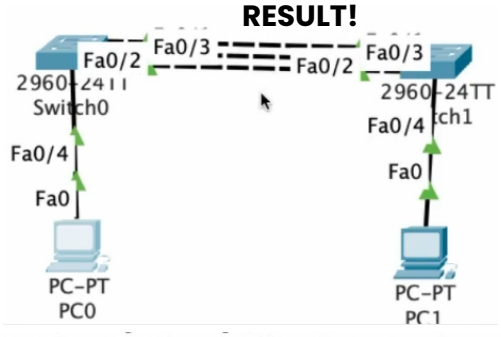
```
Switch(config-if-range)#channel-group ?
  <1-6>  Channel group number
Switch(config-if-range)#channel-group 1 ?
  mode  Etherchannel Mode of the interface
Switch(config-if-range)#channel-group 1 mode ?
  active     Enable LACP unconditionally
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected
```

```
Switch(config-if-range)#channel-group 1 mode active
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1
```

Switch 1

```
Switch(config-if-range)#channel-group 1 mode passive
```

RESULT!




```
Switch(config-if-range)#do show etherchannel sum

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+----------------------------------------------

1      Po1(SU)           LACP    Fa0/1(P) Fa0/2(P) Fa0/3(P)
```

Step by Step

- We will create a trunk mode first for connecting between switches
- we create a channel group, here there are channel groups 1-6. we can create etherchannel up to 6 groups. the connector for each switch must have a different group! For example SW0-SW1 (Group 1) then SW1 to SW2 must be other than group 1
- channel group mode Active/Passive

Mode LACP

- **LACP Active :** So one of the switches must be active
- **LACP Passive :** Waiting (Not Active)
- **Active to Active :** Berhasil
- **Passive to Passive** : Failed
- **Active to Passive** : Succeed

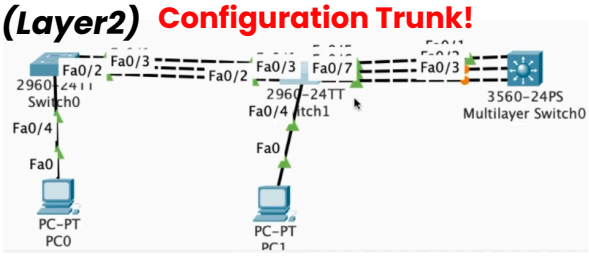
Noted : The connected ones must be the same! For example, switch 0 is in group 1, then the connected switch 1 must also use group 1. And for the connected port when switch 0 is active, then the connected switch is free to be active or passive. For other ether connectors, the groups must be different!

Conclusion Results: The results of the etherchannel are:

- Po1 : Port Channel, and 1 is Group 1
- SU : S (Layer 2) and U (In Use) digunakan
- Protocol : LACP
- P : In Port Channel
- Three Cabel speed 300MBPS

ETHERCHANNEL PAGP

Etherchannel PAGP (ONLY CISCO) *(Layer2)* Configuration Trunk!



Konfigurasi Etherchannel PAGP

Switch 1

```
Switch(config-if-range)#int range fa0/5-7
Switch(config-if-range)#
Switch(config-if-range)#sw mod trunk
```

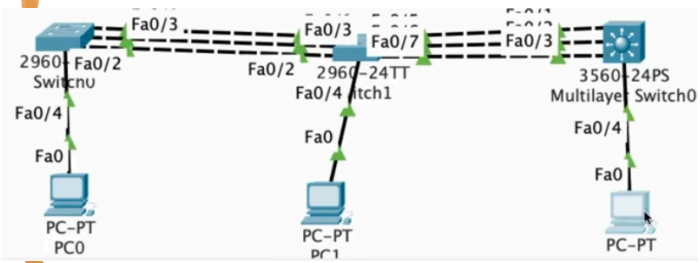
```
Switch(config-if-range)#channel-group ?
  <1-6>  Channel group number
Switch(config-if-range)#channel-group 2 mod
Switch(config-if-range)#channel-group 2 mode ?
  active     Enable LACP unconditionally
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected

Switch(config-if-range)#channel-group 2 mode desirable
```

Multi layer switch

```
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#channel-group 2 mode desirable
```

Catatan : In multilayer switch we have to encapsulate first!

Hasil!




```
Switch(config-if-range)#do show etherchannel sum

Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

1      Po1(SU)           LACP    Fa0/1(P) Fa0/2(P) Fa0/3(P)
2      Po2(SU)           PAgP    Fa0/5(P) Fa0/6(P) Fa0/7(P)
```

PAGP: An open standard protocol (IEEE 802.3ad) that combines multiple physical links into a single logical path to increase bandwidth and provide redundancy. Flexible for devices from multiple vendors. (For all vendors)

Step by Step

- We will create a trunk mode first for connecting between switches we create a channel group, here there are channel groups 1-6.
- we can create etherchannel up to 6 groups. the connector for each switch must have a different group! For example SW0-SW1 (Group 1) then SW1 to SW2 must be other than group 1 channel group mode auto/desirable

Mode PAGP

- **Auto :** Waiting
- **Desirable :** Invite
- **Desirable to Auto :**Succed
- **Auto to Auto :** Failed
- **Desirable to Desirable :Succed**

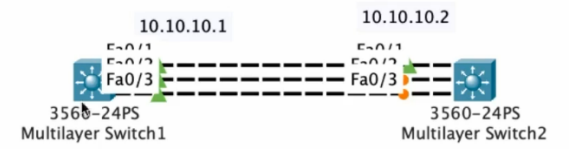
Note: The point is that the connected ones must be the same! For example, switch 1 is in group 2, then the connected multi-layer switch must also use group 2. And for the connected port when switch 1 is desirable, then the connected switch is free, can be desirable or auto. **For other ether connectors, the group must be different!**

Explain Result: Result From etherchannel

- Po2 : Port Channel, and 2 is Group 2
- SU : S (Layer 2) dan U (In Use)
- Protocol : PAgP
- P : In Port Channel
- Three Cabel Total 300MBPS

ETHERCHANNEL LAYER 3

Ethernet Layer 3 **No Trunk! Config IP Address!**



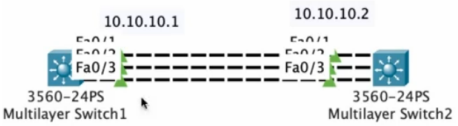
Layer 3 EtherChannel: EtherChannel that works at layer 3 (network). Used to combine links that can do routing between networks or between VLANs, not just switching.

Konfigurasi Etherchannel PAGP

Multilayer switch1

```
Switch(config)#int rang fa0/1-3
Switch(config-if-range)#
Switch(config-if-range)#no switchport
Switch(config-if-range)#channel-group ?
  <1-48>  Channel group number
Switch(config-if-range)#channel-group 1 mode ?
  active      Enable LACP unconditionally
  auto        Enable PAgP only if a PAgP device is detected
  desirable   Enable PAgP unconditionally
  on          Enable Etherchannel only
  passive     Enable LACP only if a LACP device is detected
Switch(config-if-range)#channel-group 1 mode on
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1,
changed state to up
Switch(config-if-range)#int po1
Switch(config-if)#ip address 10.10.10.1 255.255.255.0
```

Result!!




```
Switch(config-if)#do show etherchannel sum
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+----------------------------------------------

1      Po1(RU)          -      Fa0/1(P) Fa0/2(P) Fa0/3(P)
Switch(config-if)#
```

Step By Step

- **no switchport :** disabled interface switch, so we can configure the IP address
- **channel-group 1 mode on :** we can enter mode 1-48, and configure it to all connected multilayer switches. cttn (for configuration do not be the same on 1 topology)
- **int po1 :** Interface port1
- **Configuration IP Address**

Explain Mode Etherchannel Layer 3

- **On :** Mode active to configure IP address on multilayer switch

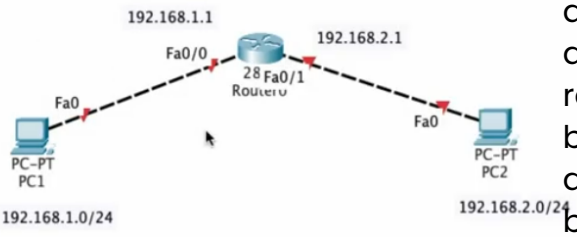
Note: Etherchannel layer 3 can only be used on multilayer switches. On this etherchannel we configure using the IP address on the switch.

Result : Hasil from etherchannel tersebut is

- Po2 : Port Channel, and 2 adalah Group 2
- RU : S (Layer 3) dan U (In Use)
- Protocol : - (Nothing)
- P : In Port Channel
- Three Cable 300MBPS

STATIC ROUTING

Static Routing 1 Router



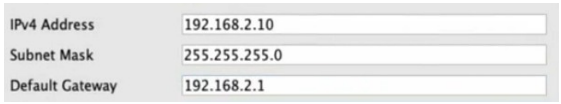
Static Routing : Method for static routing and cannot be changed except by the administrator. static routing unlike dynamic routing, which automatically updates routes based on network conditions, static routing does not change unless manually updated by the administrator.

Config Router

```
Router(config)#int fa0/0
Router(config-if)#
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.1
255.255.255.0
```

Default gateway : ip address router

Config PC



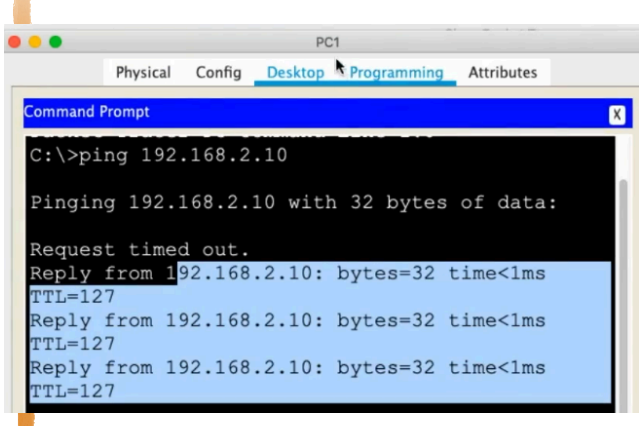
Step by Step

- **Configurasi PC : in** PC Config IP and Subnetmask
- **Default Gateway :** Default gateway use ip address on router
- **Confif Router :** We configure our router to have no shutdown on the interface, then enter the IP address

Result : The result of this routing is

- When pinging from PC 1 to PC 2, it will ask the gateway to the router. Is there a gateway for PC 2 on the router?
- The router gateway is the IP address of the interface on the router that we just configured
- If it is successful, then the ping is successful!

Result!

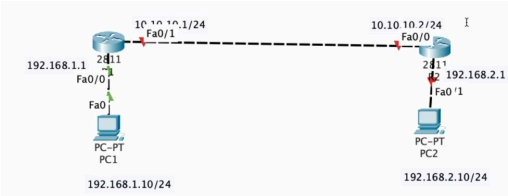



```
Router(config-if)#do show ip inter brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        192.168.1.1     YES manual up
FastEthernet0/1        192.168.2.1     YES manual up
```

STATIC ROUTING

Static Routing 2 Router

TEST PING WITH TERMINAL!



Config Router 1

C 10.10.10.0/24 -> fa0/1
C 192.168.1.0/24 -> fa0/0

```
Router(config)#int fa0/0
Router(config-if)#
Router(config-if)#no shutdown

Router(config-if)#ip address 192.168.1.1
255.255.255.0
Router(config-if)#int fa0/1
Router(config-if)#
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config)#ip route 192.168.2.0 255.255.255.0 10.10.10.2
```

Config Router 2

C 10.10.10.0/24 -> fa0/0
C 192.168.2.0/24 -> fa0/1

```
Router(config-if)#ip address 10.10.10.2
255.255.255.0

Router(config-if)#ip address 192.168.2.1
255.255.255.0
Router(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1
```

Default gateway : ip address router

Config PC

IPv4 Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1

RESULT!

Router 1

```
Router(config)#do show ip route

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 [1/0] via 10.10.10.2
```

Router 2

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 10.10.10.1
C    192.168.2.0/24 is directly connected, FastEthernet0/1
```

Explanation: Here we will enter the IP address on the Router to determine the default gateway on the router. on router 1 & 2 we enter the IP address

Step By Step

- **Config PC :** Our PC configures IP and Subnetmask
- **Default Gateway :** Default gateway here use ip address on router
- **Config Router :** router we configuration no shutdown on interface next input Ip address
- **Input static routing :** to Ip address destination and destination default gateway!

Explanation: Here we have connected 2 routers to the client, we will use static routing!

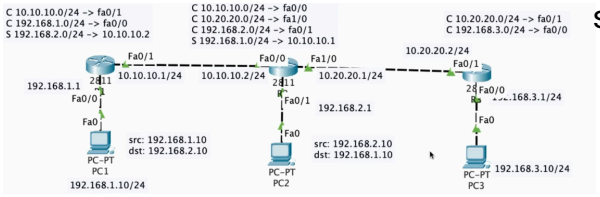
in router 1 config: we will enter the default gateway! which is on router 2, and vice versa!

if you want to go to 192.168.2.0 please ask 10.10.10.2

STATIC ROUTING

Static Routing 3 Router

TEST PING WITH TERMINAL!



Config Router 1

```
Router(config)#ip route 10.20.20.0 255.255.255.0 10.10.10.2
Router(config)#
Router(config)#ip route 192.168.3.0 255.255.255.0 10.10.10.2
```

Config Router 2

```
Router(config)#do write
```

NM-1FE-TX

```
Router(config)#int fa1/0
Router(config-if)#
Router(config-if)#no shutdown
Router(config-if)#ip address 10.20.20.1 255.255.255.0
Router(config-if)#ip route 192.168.3.0 255.255.255.0 10.20.20.2
```

Config Router 3

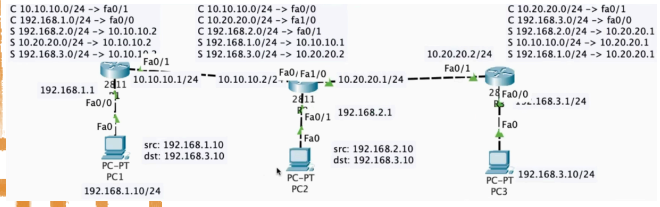
int fa0/1

```
Router(config-if)#ip address 10.20.20.2
255.255.255.0
```

int fa0/0

```
Router(config-if)#ip address 192.168.3.1
255.255.255.0

Router(config-if)#no shutdown
Router(config)#ip route 192.168.2.0 255.255.255.0 10.20.20.1
Router(config)#ip route 10.10.10.0 255.255.255.0 10.20.20.1
Router(config)#ip route 192.168.1.0 255.255.255.0 10.20.20.1
```

RESULT!!



Explanation: add interface on router 2! by going to physical then to modules and select NM-FE-TX

Step By Step

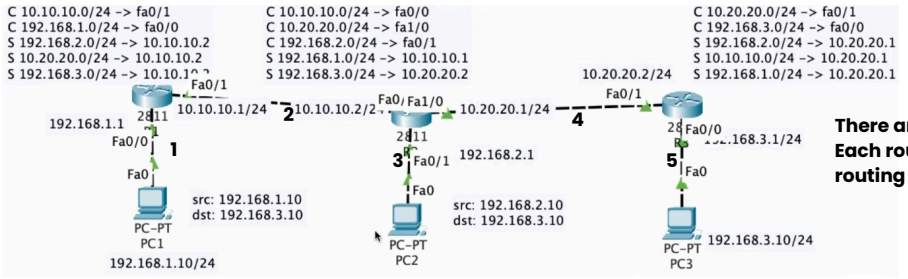
- **static routing 2 router** : continuation of static routing 2 routers: On router 2 we add an interface! don't forget to save do write! (shutdown the router first!)
- no shutdown: to all connected interfaces! on all routers
- add ip address to interface
- on all routers we add all static routing information from all routers
- on router 1 connected to 2 and will go to router 3 we ask for information on router 2!
- to ask for information from router 1 to router 3, we will still use the first cable information! connected
- for router 2 we ask for gateway information from router 3

Explanation: ip route "destination" "netmask" "where to go"? let's see from the example of the 3 routing topologies!!

Router 1

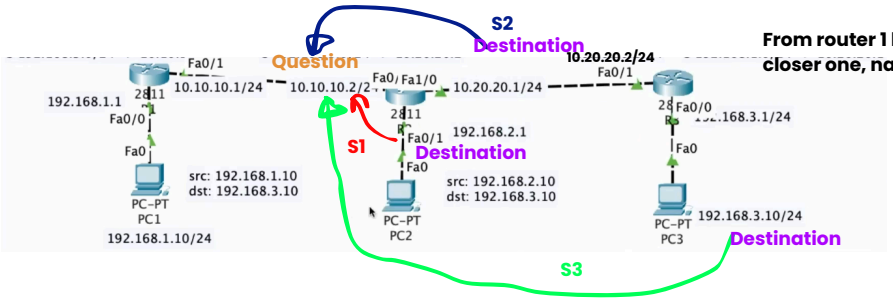
- **Static** : 192.168.2.0/24 to 10.10.10.2 explains that our destination is router 2 and passes through 10.2
- **Static** : 10.20.20.0/24 to 10.10.10.2 explains that the destination is to the interface that wants to connect to router 3 and passes through 10.2
- **Static** : 192.168.3.0/24 to 10.10.10.2 explains that the destination is to the default gateway passing through 10.2

ROUTING STATIC 3 ROUTER



There are 5 paths here! Each router has 5 paths in the routing table

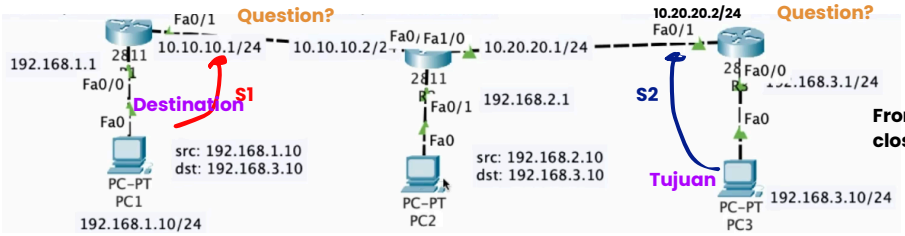
Explanation: "destination" "netmask" "where to go"? let's see from the example of the 3 routing topologies!



From router 1 he wants to ask the closer one, namely router 2?

Router 1

- **Static 1**: The destination is 192.168.2.0/24 asking 10.10.10.2 explaining that our destination is router 2 and passing through then asking 10.2
- **Static 2 :** The destination is 10.20.20.0/24 asking 10.10.10.2 explaining that the destination is to the interface that wants to connect to router 3 and passing through then asking 10.2
- **Static 3** : The destination is 192.168.3.0/24 asking 10.10.10.2 explaining that the destination is to Router 3 which is the default gateway! passing through and asking 10.2

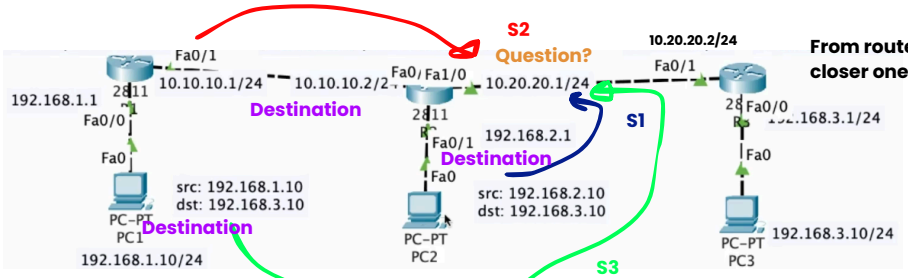


From router 2 he wants to ask the closer ones, namely router 1 & 3?

Router 2

- **Static 1 :** The destination is 192.168.1.0/24 asking 10.10.10.1 explaining that the destination is to identify router 1. That's why it asks for router 1's default gateway!. And then it passes and asks 10.1
- **Static 2 :** The destination is 192.168.3.0/24 asking 10.20.20.2 explaining that the destination is to identify router 3, That's why it asks for router 3's default gateway. And then it passes and asks 20.2

(If it's in the middle it asks the router next to it!)



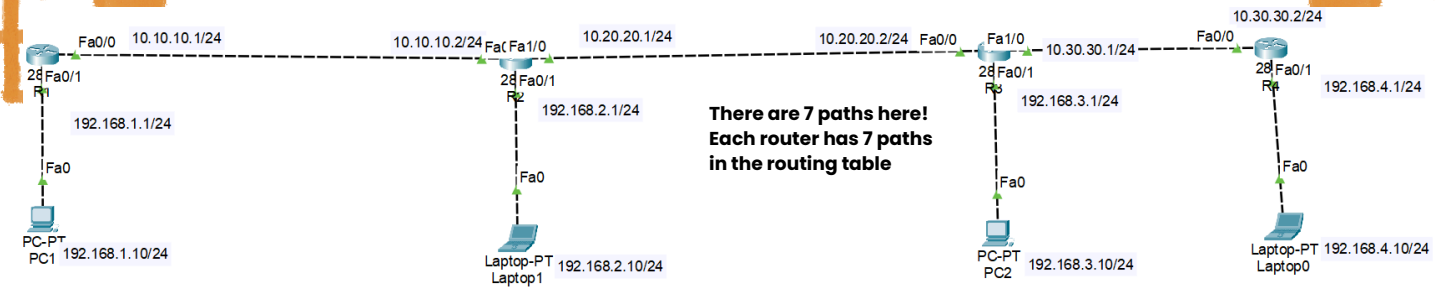
From router 3 he wants to ask the closer one which is router 2?

Router 3

- **Static 1:** The destination is 192.168.2.0/24 asking 10.20.20.1 explaining that the destination is to recognize router 2, it will pass through then ask 20.1.
- **Static 2:** The destination is 10.10.10.0/24 asking 10.20.20.1 explaining that the destination is to the interface that wants to router 3, it will pass through then ask 20.1
- **Static 3:** The destination is 192.168.1.0/24 asking 10.20.20.1 explaining that the destination is to recognize router 1, it will pass through then ask 20.1

Note: For that purpose is the router ip or interface ip and the destination asked is the closest destination from the router and asks the cable. for example. from router 3, the closest is router 2 so it uses the nearest router 2 interface cable ip.

ROUTING STATIC 4 ROUTER



Penjelasan : ip route "destination" "netmask" "where to go"? let's see from the example of the 4 routing topology! there are 7 paths!

ROUTING ROUTER 1

1. **Connect :** 10.10.10.0/24 -> fa0/1
2. **Connect :** 192.168.1.0/24 -> fa0/0
3. **Static :** 192.168.2.0/24 -> 10.10.10.2
4. **Static :** 10.20.20.0/24 -> 10.10.10.2
5. **Static :** 192.168.3.0/24 -> 10.10.10.2
6. **Static :** 192.168.4.0/24 -> 10.10.10.2
7. **Static :** 10.30.30.0/24 -> 10.10.10.2

ROUTING ROUTER 2

1. **Connect :** 10.10.10.0/24 -> fa0/0
2. **Connect :** 10.20.20.0/24 _> fa1/0
3. **Connect :** 192.168.2.0/24 -> fa0/1
4. **Static :** 192.168.1.0/24 -> 10.10.10.1
5. **Static :** 192.168.3.0/24 -> 10.20.20.2
6. **Static :** 192.168.4.0/24 -> 10.20.20.2
7. **Static :** 10.30.30.0/24 -> 10.20.20.2

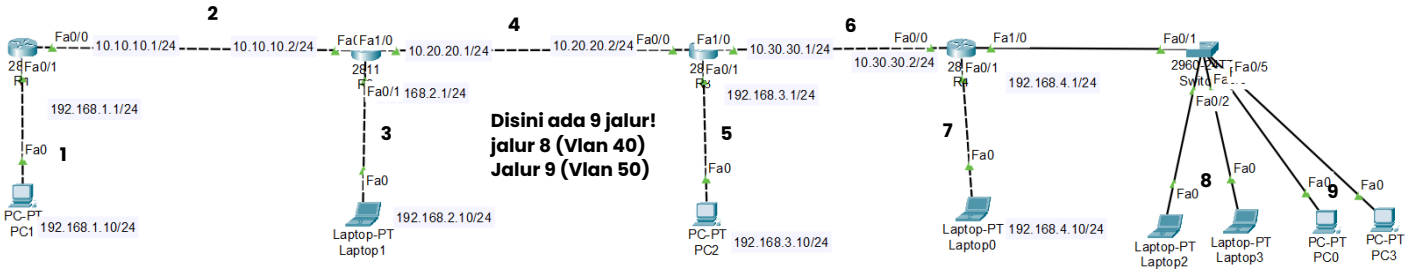
ROUTING ROUTER 3

1. **Connect :** 10.20.20.0/24 -> fa0/1
2. **Connect :** 10.30.30.0/24 -> fa1/0
3. **Connect :** 192.168.3.0/24 -> fa0/0
4. **Static :** 192.168.2.0/24 -> 10.20.20.1
5. **Static :** 10.10.10.0/24 -> 10.20.20.1
6. **Static :** 192.168.1.0/24 -> 10.20.20.1
7. **Static :** 192.168.4.0/24 -> 10.30.30.2

ROUTING ROUTER 4

1. **Connect :** 10.30.30.0/24 -> fa0/0
2. **Connect :** 192.168.4.0/24 -> fa0/1
3. **Static :** 192.168.3.0/24 -> 10.30.30.1
4. **Static :** 10.20.20.0/24 -> 10.30.30.1
5. **Static :** 192.168.2.0/24 -> 10.30.30.1
6. **Static :** 10.10.10.0/24 -> 10.30.30.1
7. **Static :** 192.168.1.0/24 -> 10.30.30.1

EXPLANATION ROUTING STATIC 4 ROUTER + VLAN



Penjelasan : ip "destination" "netmask" "where to go"? let's see from the example of the 4 routing topology! there are 9 paths! Path 8 (Vlan40) Path 9 (Vlan50)

ROUTING ROUTER 1

1. **Connect :** 10.10.10.0/24 -> fa0/1
2. **Connect :** 192.168.1.0/24 -> fa0/0
3. **Static :** 192.168.2.0/24 -> 10.10.10.2
4. **Static :** 10.20.20.0/24 -> 10.10.10.2
5. **Static :** 192.168.3.0/24 -> 10.10.10.2
6. **Static :** 192.168.4.0/24 -> 10.10.10.2
7. **Static :** 10.30.30.0/24 -> 10.10.10.2
8. **Static :** 192.168.40.0/24 -> 10.10.10.2 (destination vlan 40)
9. **Static :** 192.168.50.0/24 -> 10.10.10.2 (destination vlan 50)

ROUTING ROUTER 2

1. **Connect :** 10.10.10.0/24 -> fa0/0
2. **Connect :** 10.20.20.0/24 _> fa1/0
3. **Connect :** 192.168.2.0/24 -> fa0/1
4. **Static :** 192.168.1.0/24 -> 10.10.10.1
5. **Static :** 192.168.3.0/24 -> 10.20.20.2
6. **Static :** 192.168.4.0/24 -> 10.20.20.2
7. **Static :** 10.30.30.0/24 -> 10.20.20.2
8. **Static :** 192.168.40.0/24 -> 10.20.20.2 (destination vlan 40)
9. **Static :** 192.168.50.0/24 -> 10.20.20.2 (destination vlan 50)

ROUTING ROUTER 3

1. **Connect :** 10.20.20.0/24 -> fa0/1
2. **Connect :** 10.30.30.0/24 -> fa1/0
3. **Connect :** 192.168.3.0/24 -> fa0/0
4. **Static :** 192.168.2.0/24 -> 10.20.20.1
5. **Static :** 10.10.10.0/24 -> 10.20.20.1
6. **Static :** 192.168.1.0/24 -> 10.20.20.1
7. **Static :** 192.168.4.0/24 -> 10.30.30.2
8. **Static :** 192.168.40.0/24 -> 10.30.30.2 (destination vlan 40)
9. **Static :** 192.168.50.0/24 -> 10.30.30.2 (destination vlan 50)

ROUTING ROUTER 4

1. **Connect :** 10.30.30.0/24 -> fa0/0
2. **Connect :** 192.168.4.0/24 -> fa0/1
3. **Static :** 192.168.3.0/24 -> 10.30.30.1
4. **Static :** 10.20.20.0/24 -> 10.30.30.1
5. **Static :** 192.168.2.0/24 -> 10.30.30.1
6. **Static :** 10.10.10.0/24 -> 10.30.30.1
7. **Static :** 192.168.1.0/24 -> 10.30.30.1
8. **Static :** 192.168.40.0/24 -> fa1/0 (destination vlan 40)
9. **Static :** 192.168.50.0/24 -> fa1/0 (destination vlan 50)

DYNAMIC ROUTING
EIGRP, OSPF & BGP

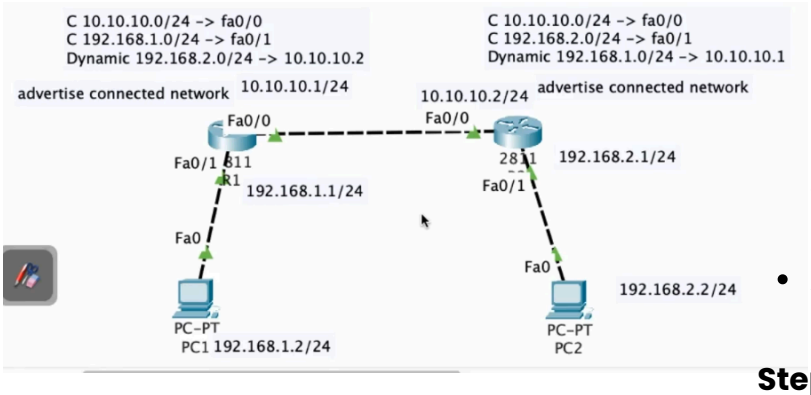
1. **EIGRP (Enhanced Interior Gateway Routing Protocol): [Only Cisco)**
   - **Why Use:** Widely used in networks that use Cisco devices, because EIGRP is a protocol developed by Cisco and has advanced features such as fast convergence, bandwidth efficiency, and the ability to handle paths with unequal costs (unequal-cost load balancing).
   - **Advantages:**Easy to configure, scalable, and optimal for complex environments
2. **OSPF (Open Shortest Path First): [Open Source]**
   - **Why Use:** OSPF is a link-state based protocol that is widely used in large and complex networks. It supports large network scales and can be implemented across multiple device vendors, making it more flexible than EIGRP which is limited to Cisco devices.
   - **Advantages:**Reliable, scalable, and supports hierarchical structures in networks (with areas and backbones).
3. **BGP (Border Gateway Protocol): [Open Source]**
   - **Why Use:** BGP is the primary routing protocol used for routing between networks or between AS (Autonomous Systems), especially on the internet. It is essential for Network Engineers working at ISPs or handling connections to multiple service providers.
   - **Advantages:**Supports very complex routing policies and is scalable for global networks.
4. **IS-IS (Intermediate System to Intermediate System): [Open Source]**
   - **Why Used:** Used primarily by ISPs and in very large networks because of its excellent scalability. IS-IS is less common than OSPF, but is very efficient and reliable in very large networks.
   - **Advantages:**Very scalable and reliable in large networks.

Conclusion:

- EIGRP and OSPF are the most commonly used protocols in enterprise networks, depending on the vendor of the equipment used.
- BGP is the primary choice for routing between different networks, especially in ISP environments or for Internet routing.
- IS-IS is used in environments with very large networks, although it is not as popular as OSPF in enterprise environments.

DYNAMIC ROUTING
EIGRP (2 Router)

Topology



Router 1

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router eigrp ?
  <1-65535>  Autonomous system number
Router(config)#router eigrp 10
Router(config-router)#network 10.10.10.0
Router(config-router)#network 192.168.1.0
```

Router 2

```
Router(config)#router eigrp 10
Router(config-router)#
Router(config-router)#
Router(config-router)#
Router(config-router)#network 10.10.10.0
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.10.10.1 (FastEthernet0/0) is up:
new adjacency

Router(config-router)#
Router(config-router)#network 192.168.2.0
```

RESULT!!

```
Router(config-router)#do show ip eigrp neighbor
IP-EIGRP neighbors for process 10
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)        Cnt Num
0   10.10.10.1      Fa0/0           11   00:00:59  40     1000  0   3
```

RESULT! Router 2

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:01:23, Null0
C       10.10.10.0/24 is directly connected, FastEthernet0/0
D    192.168.1.0/24 [90/30720] via 10.10.10.1, 00:01:27, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
```

RESULT! Router 1

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:04:46, Null0
C       10.10.10.0/24 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
D    192.168.2.0/24 [90/30720] via 10.10.10.2, 00:03:18, FastEthernet0/0
```

EIGRP (Enhanced Interior Gateway Routing Protocol): [Only Cisco)

- **Why Use:** Widely used in networks that use Cisco devices, because EIGRP is a protocol developed by Cisco and has advanced features such as fast convergence, bandwidth efficiency, and the ability to handle paths with unequal costs (unequal-cost load balancing).
- **Advantages:** Easy to configure, scalable, and optimal for complex environments.

Step by Step EIGRP

- **advertise :** we enter the router that we want to advertise. which is advertised (Connected) on the router. and the autonomous **number of the entire router must be the same!**
- **EIGRP Router 1 :** network 10.10.10.0 & network 192.168.1.0
- **EIGRP Router 2 :** network 10.10.10.0 & network 192.168.2.0

Explanation

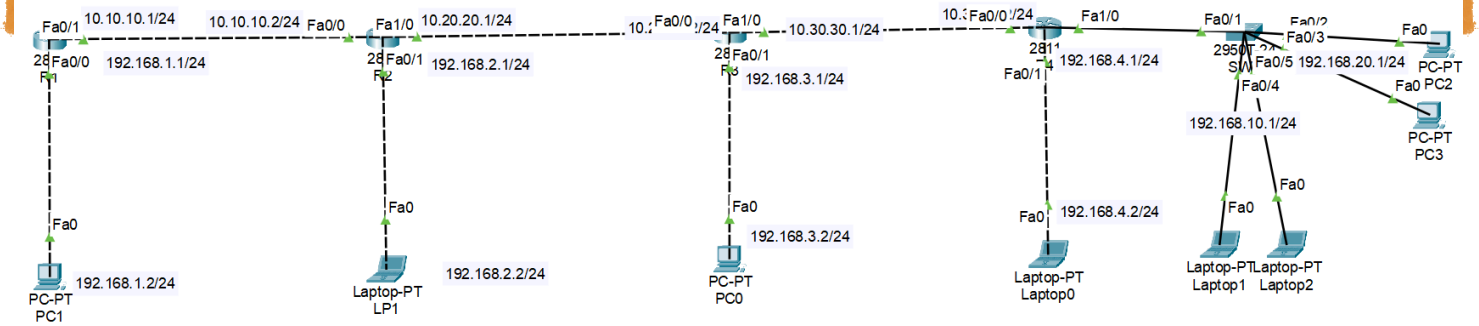
IP-EIGRP 10 : Neighbor 10.10.10.1 fa0/0 is up artinya EIGRP 10.10.10.0 sudah up melalui fa0/-0

RESULT!:

- **do show ip eigrp neighbor :** ip address well done advertise id 10.10.10.1
- **do show ip route (router 2) :** we enter the router that we want to advertise. which is advertised (Connected) on the router. and the autonomous number of the entire router must the same! 1 ***D (EIGRP)***
- **do show ip route (router 1):** that D has been automatically added, namely advertise routing from router 2.

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time<1ms
TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms
TTL=126
```

DYNAMIC ROUTING
EIGRP (4 Router + VLAN)



Penjelasan : EIGRP advertise connected router

DYNAMIC ROUTING ROUTER 1

1. **Connect :** 10.10.10.1/24 -> fa0/1
2. **Connect :** 192.168.1.1/24 -> fa0/0
3. **Dynamic :** 192.168.2.0/24 -> 10.10.10.2
4. **Dynamic :** 192.168.3.0/24 -> 10.10.10.2
5. **Dynamic :** 192.168.4.0/24 -> 10.10.10.2
6. **Dynamic :** 192.168.10.0/24 -> 10.10.10.2
7. **Dynamic :** 192.168.20.0/24 -> 10.10.10.2

DYNAMIC ROUTING ROUTER 2

1. **Connect :** 10.10.10.2/24 -> fa0/0
2. **Connect :** 10.20.20.1/24 -> fa1/0
3. **Connect :** 192.168.2.1/24 -> fa0/1
4. **Dynamic :** 192.168.1.0/24 -> 10.10.10.1
5. **Dynamic :** 192.168.3.0/24 -> 10.20.20.2
6. **Dynamic :** 192.168.4.0/24 -> 10.20.20.2
7. **Dynamic :** 192.168.10.0/24 -> 10.20.20.2
8. **Dynamic :** 192.168.20.0/24 -> 10.20.20.2

DYNAMIC ROUTING ROUTER 3

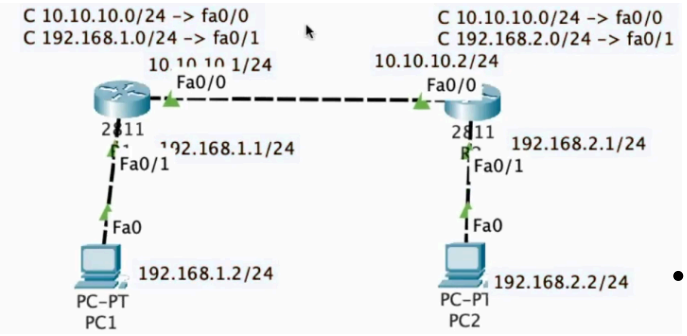
1. **Connect :** 10.20.20.2/24 -> fa0/0
2. **Connect :** 192.168.3.1/24 -> fa0/1
3. **Connect :** 10.30.30.1/24 -> fa1/0
4. **Dynamic :** 192.168.1.0/24 -> 10.20.20.1
5. **Dynamic :** 192.168.3.0/24 -> 10.20.20.1
6. **Dynamic :** 192.168.4.0/24 -> 10.30.30.2
7. **Dynamic :** 192.168.10.0/24 -> 10.20.20.1
8. **Dynamic :** 192.168.20.0/24 -> 10.20.20.1

DYNAMIC ROUTING ROUTER 4

1. **Connect :** 10.30.30.2/24 -> fa0/0
2. **Connect :** 192.168.4.1/24 -> fa0/1
3. **Dynamic :** 192.168.3.0/24 -> 10.30.30.1
4. **Dynamic :** 192.168.2.0/24 -> 10.30.30.1
5. **Dynamic :** 192.168.1.0/24 -> 10.30.30.1
6. **Dynamic :** 192.168.10.0/24 -> 10.30.30.1
7. **Dynamic :** 192.168.20.0/24 -> 10.30.30.1

DYNAMIC ROUTING
OSPF (2 Router)

Topology



Router 1

```
Router(config)#router ospf ?
  <1-65535>  Process ID
Router(config)#router ospf
```

```
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 10.10.10.0 ?
  A.B.C.D  OSPF wild card bits
Router(config-router)#network 10.10.10.0 0.0.0.255 ?
  area  Set the OSPF area ID
Router(config-router)#network 10.10.10.0 0.0.0.255 area ?
  <0-4294967295>  OSPF area ID as a decimal value
  A.B.C.D         OSPF area ID in IP address format
Router(config-router)#network 10.10.10.0 0.0.0.255 area 0
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

Router 2

```
Router(config)#router ospf 1

Router(config-router)#network 10.10.10.0
0.0.0.255 area 0

Router(config-router)#network 192.168.2.0
0.0.0.255 area 0
```

RESULT!!

```
Router(config-router)#do show ip eigrp neighbor
IP-EIGRP neighbors for process 10
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)       Cnt Num
0   10.10.10.1      Fa0/0          11   00:00:59  40     1000  0   3
```

RESULT! Router 2

```
00:15:46: %OSPF-5-ADJCHG: Process 2, Nbr
192.168.1.1 on FastEthernet0/0 from LOADING to
FULL, Loading Done
are
Router(config-router)#do show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time
Address         Interface
192.168.1.1       1   FULL/DR         00:00:33
10.10.10.1      FastEthernet0/0
```

do show ip route

```
Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/0
O    192.168.1.0/24 [110/2] via 10.10.10.1, 00:01:10, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1

Router(config-router)#
```

OSPF (Open Shortest Path First): [Open Source]

- **Why Use It:** OSPF is a link-state based protocol that is widely used in large and complex networks. It supports large network scales and can be implemented across multiple device vendors, making it more flexible than EIGRP which is limited to Cisco devices.
- **Advantages:** Reliable, scalable, and supports hierarchical structures in networks (with areas and backbones).

Step by Step OSPF

- **advertise:** we enter the router that we want to do OSPF. on the router. and the **ID for the OSPF router as a whole may or may not be the same!**
- **input network, wilcard mask & area :** 10.10.10.0 0.0.0.255 area 0 & 192.168.1.0 0.0.0.255 area 0

Explanation:

- **wilcard mask :** prefix subnetmask is /24 = 255.255.255.0 and reduced wilcard mask is 0.0.0.255
- **area :** area on each network must start from 0! **all router areas must be the same!**

on router 2 we have got the ip information from router 1! which was initially loading now it is FULL/UP

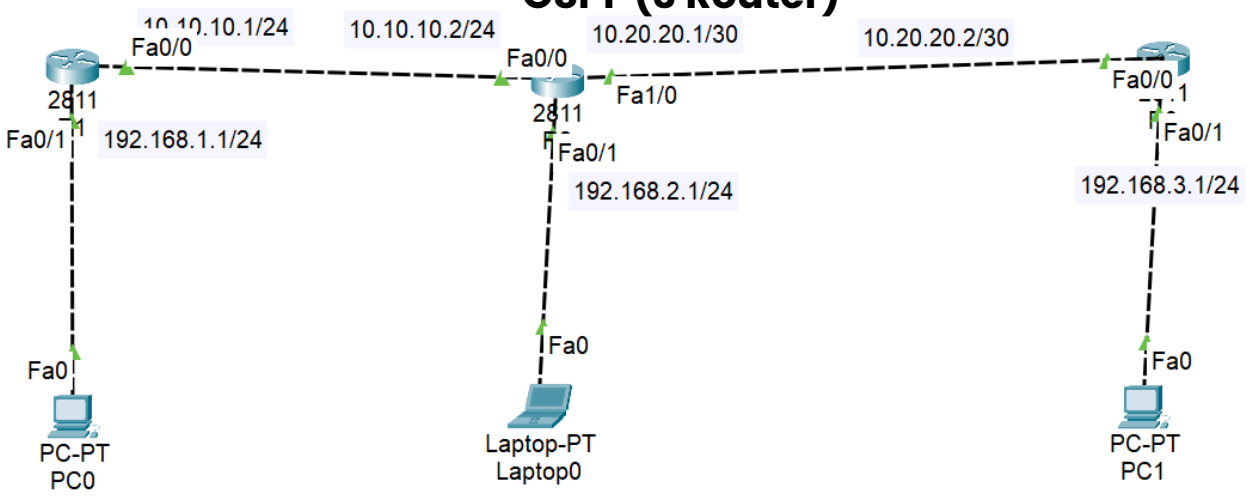
RESULT!:

- **do show ip ospf neighbor (Router2) :** ip address The ones that have been advertised are 10.10.1 0.1, and the full 192.168.1.1
- **do show ip route (router 2) :** It can be seen that O has been automatically added, namely advertise routing from the router1 . ***O (OSPF)***

Result Ping OSPF!

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time<1ms
TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms
TTL=126
```

DYNAMIC ROUTING
OSPF (3 Router)



DYNAMIC ROUTING ROUTER 1 (OSPF)

1. **C** 10.10.10.0/24 -> fa0/0
2. **C** 192.168.1.0/24 -> fa0/1
3. **Dynamic** 192.168.2.0/24 -> 10.10.10.2
4. **Dynamic** 192.168.3.0/24 -> 10.10.10.2
5. **Dynamic** 10.20.20.0/30 -> 10.10.10.2

DYNAMIC ROUTING ROUTER 2 (OSPF)

1. **C** 10.10.10.0/24 -> fa0/0
2. **C** 192.168.2.0/24 -> fa0/1
3. **C** 10.20.20.1/30 -> fa1/0
4. **Dynamic** 192.168.1.0/24 -> 10.10.10.1
5. **Dynamic** 192.168.3.0 -> 10.20.20.2

DYNAMIC ROUTING ROUTER 3 (OSPF)

1. **C** 10.10.10.0/24 -> fa0/0
2. **C** 192.168.2.0/24 -> fa0/1
3. **C** 10.20.20.1/30 -> fa1/0
4. **Dynamic** 192.168.1.0/24 -> 20.20.20.1
5. **Dynamic** 192.168.2.0/24 -> 20.20.20.1
6. **Dynamic** 10.10.10.0/24 -> 20.20.20.1

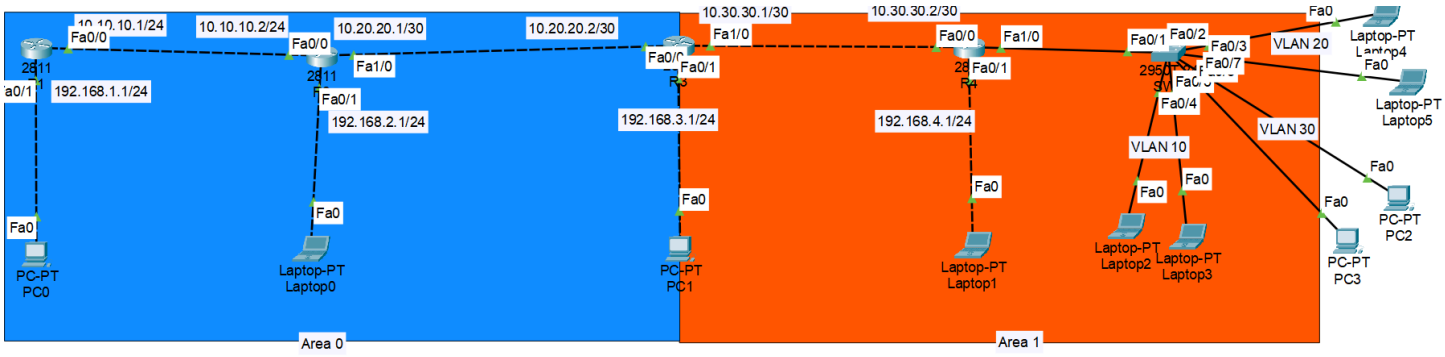
Step by Step OSPF

- **advertise:** we enter the router that we want to do OSPF. on the router. and the **ID for the OSPF router as a whole may or may not be the same!**
- **input network, wilcard mask & area :** 10.10.10.0 0.0.0.255 area 0 & 192.168.1.0 0.0.0.255 area 0 ***(prefix /24)***

Penjelasan :

- **wilcard mask :** is the prefix of the subnet mask which is /24 = 255.255.255.0 and minus the wildcard mask which is 0.0.0.255
- **On Router 2:** Here we have a different prefix which is 10.20.20.1/30 then we add the ospf /30 = 255.255.255.252 and the wildcard mask is 255.255.255.255 minus 255.255.255.252. the result of the wildcard mask is 0.0.0.3
- **area :** area network start from 0! **all area routers must be the same**

DYNAMIC ROUTING
OSPF (Multi Area)



Router 3

Do show Run

```
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 10.20.20.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 1
 network 10.30.30.0 0.0.0.3 area 1
!
```

Step by Step Multilayer

- **Router 3:** Here we can see that we will create 2 areas in router 3 to integrate in areas 0 and 1. This router 3 is the mediator!
- **Router 4:** In router 4, we also change it to area 1
- **Router 1-2:** it remains area 0

Router 4

```
 network 10.30.30.0 0.0.0.3 area 1
 network 192.168.4.0 0.0.0.255 area 1
 network 192.168.10.0 0.0.0.255 area 1
 network 192.168.30.0 0.0.0.255 area 1
 network 192.168.20.0 0.0.0.255 area 1
!
```

Router 2

```
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 10.20.20.0 0.0.0.3 area 0
!
```

Router 2

```
 router ospf 1
  log-adjacency-changes
  network 10.10.10.0 0.0.0.255 area 0
  network 192.168.1.0 0.0.0.255 area 0
 !
```

Explanation
DYNAMIC ROUTING BGP

IGP (Interior Gateway Protocol)
IGP is a type of routing protocol used to discover and maintain routes within an Autonomous System (AS), which is a single network or group of networks managed by a single organization.

Kegunaan: IGP used for routing within internal networks, such as within a company, organization, or internet service provider (ISP) within a single administrative domain.

Contoh Protokol:

1. **OSPF (Open Shortest Path First) [Open Source]: Protocol** A link-state based protocol that is widely used in internal networks due to its reliability and scalability.
2. **EIGRP (Enhanced Interior Gateway Routing Protocol) [Only Cisco]:** A vector-metric based protocol, developed by Cisco, and widely used in Cisco-based networks.
3. **IS-IS (Intermediate System to Intermediate System) [Open Source]: Protocol** scalable link-state based, often used in large ISP networks.

EGP (Exterior Gateway Protocol):
EGP adalah jenis protokol routing yang digunakan untuk routing antar Autonomous Systems (AS), seperti routing antar jaringan yang berbeda di internet.

menghubungkan inter/antar AS

Kegunaan: EGP digunakan untuk routing di antara berbagai jaringan yang dimiliki oleh organisasi berbeda, terutama di tingkat penyedia layanan internet (ISP) atau perusahaan besar yang memiliki lebih dari satu AS.

Example Protocol :

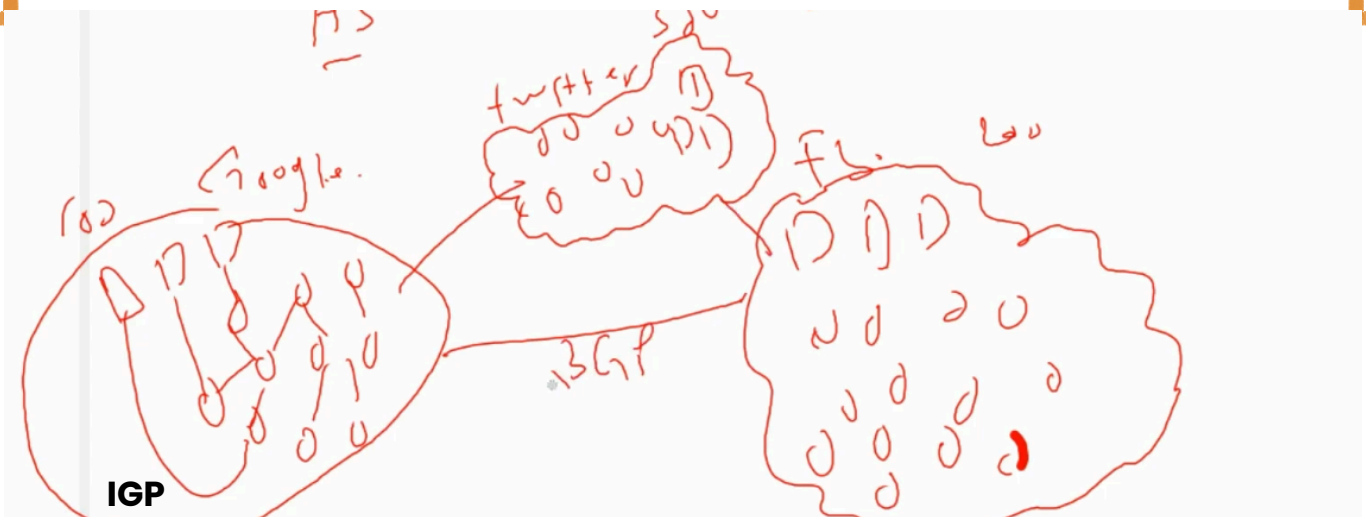
- **BGP (Border Gateway Protocol):** The only EGP in use today. BGP is a path-vector routing protocol that manages routes between ASs on the internet, allowing complex routing policies and efficient handling of thousands of routes.

Conlusion:

- **IGP :** are used for routing within a network or AS, ensuring that all devices on the network can communicate with each other.
- **EGP :** are used for routing between networks or ASs, allowing communication between different networks around the world, such as the Internet.

BGP is a prime example of an EGP, while OSPF, EIGRP, IS-IS, and RIP are examples of IGPs used in internal networks.

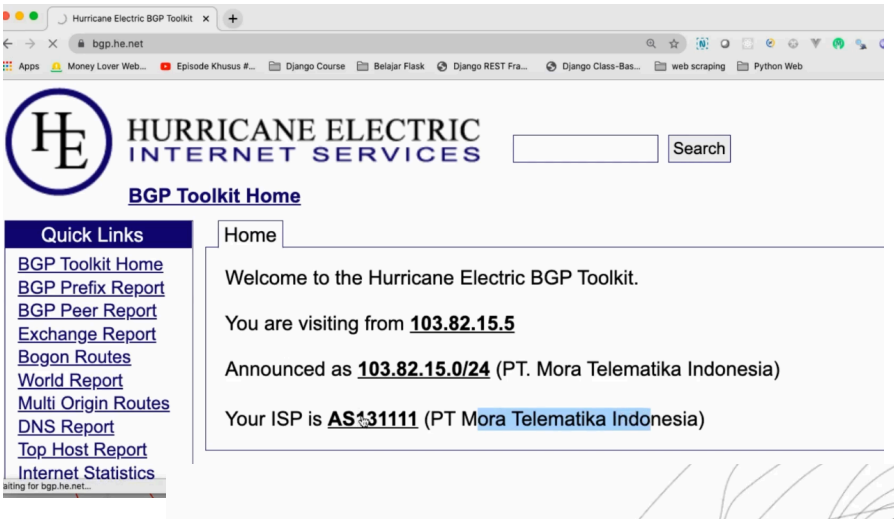
EXAMPLE IGP AND EGP

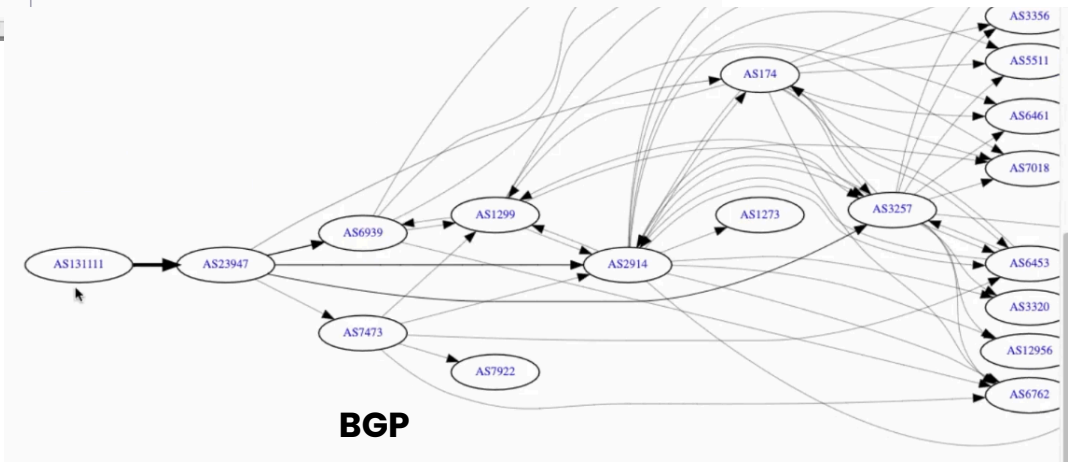


Explanation

- **IGP** : are used for routing within a network or AS, ensuring that all devices on the network can communicate with each other.
- **EGP**: are used for routing between networks or ASs, allowing communication between different networks around the world, such as the Internet.

BGP is a prime example of an EGP, while OSPF, EIGRP, IS-IS, and RIP are examples of IGPs used in internal networks.



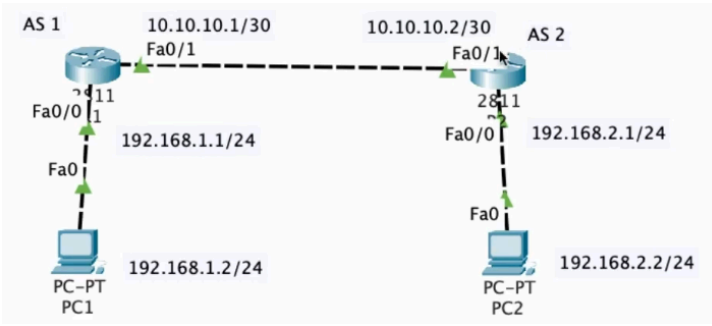


BGP

EXAMPLE BGP (BORDER GATEWAY PROTOCOL)
TOPOLOGY 2 ROUTER

AS : Autonomus System

Topology 2 router



BGP (Border Gateway Protocol): The only EGP in use today. BGP is a path-vector routing protocol that manages routes between ASs on the internet, allowing complex routing policies and efficient handling of thousands of routes.

Router 1

```
Router(config)#router bgp ?
  <1-65535>  Autonomous system number
Router(config)#router bgp 1

Router(config-router)#neighbor 10.10.10.2
remote-as 2

Router(config-router)#network 10.10.10.0 mask ?
  A.B.C.D  Network mask
Router(config-router)#network 10.10.10.0 mask
255.255.255.252

Router(config-router)#network 192.168.1.0 mask
255.255.255.0
```

Router 2

```
Router(config)#router bgp 2
Router(config-router)#neighbor 10.10.10.1
remote-as 1
Router(config-router)#%BGP-5-ADJCHANGE:
neighbor 10.10.10.1 Up

Router(config-router)#network 10.10.10.0 mask
255.255.255.252

Router(config-router)#network 192.168.2.0 mask
255.255.255.0
```

Step by Step

- **Router 1:** Here we enter the OS on router 1, namely "router bgp 1"
- **Configure Neighbor:** Enter Neighbor, namely the remote IP address and neighbor AS! The IP address and AS connected to router 2! "neighbor 10.10.10.2 remote-as 2"
- **Enter the network and mask in router 1:** "network 10.10.10.0 mask 255.255.255.252" & "192.168.1.0 mask 255.255.255.0"

RESULT!

- **Router 2:** Here the BGP neighbor connected to Router 1 is already connected and up 10.10.10.1 Up
- **ip bgp sum:** already received, namely the neighbor of router 1 is 10.10.10.1 and the prefix received is 4 / received 4 networks!
- **do show ip route:** here BGP is already active, the ip received from Router 2 is 192.168.2.0/24

RESULT Router 2

```
Router(config-router)#%BGP-5-ADJCHANGE:
neighbor 10.10.10.1 Up
```

do show ip bgp sum

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.1      4     1       6       3        5    0    0 00:01:31        4
```

Prefix

RESULT Router 1

do show ip bgp sum

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.2      4     2       6       4        5    0    0 00:02:08        4
```

Prefix

do show ip route

```
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
B    192.168.2.0/24 [20/0] via 10.10.10.2, 00:00:00
```

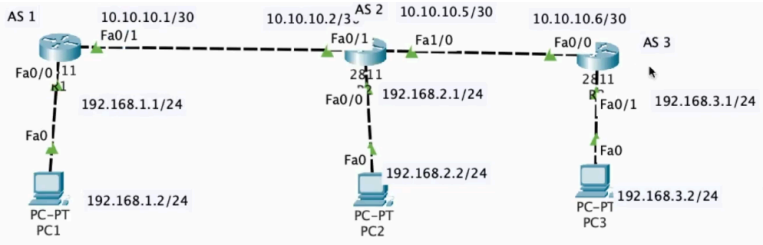
```
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/1
B    192.168.1.0/24 [20/0] via 10.10.10.1, 00:00:00
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Note: if the prefix is not running, the state is active

EXAMPLE BGP (BORDER GATEWAY PROTOCOL)
TOPOLOGY 3 ROUTER

AS : Autonomus System

Topology 3 Router



Router 2

```
Router(config-if)#router bgp 2
Router(config-router)#neighbor 10.10.10.6
remote-as 3
Router(config-router)#network 10.10.10.4 mask
255.255.255.252
```

Router 3

```
Router(config-if)#router bgp 3
Router(config-router)#neighbor 10.10.10.5
remote-as 2
Router(config-router)#network 10.10.10.4 mask
255.255.255.252
Router(config-router)#network 192.168.3.0 mask
255.255.255.0
```

Why does the 2-3rd Router Mask use mask 4?

Prefix	IP Addresses	Subnet Mask	Bits
/32	1	255.255.255.255	0
/31	2	255.255.255.254	1
/30	4	255.255.255.252	2
/29	8	255.255.255.248	3

RESULT Router 3

```
Router(config-router)#%BGP-5-ADJCHANGE:
neighbor 10.10.10.5 Up
```

RESULT Router 1

do show ip Route

```
     10.0.0.0/30 is subnetted, 2 subnets
C       10.10.10.0 is directly connected, FastEthernet0/1
B       10.10.10.4 [20/0] via 10.10.10.2, 00:00:00
C    192.168.1.0/24 is directly connected, FastEthernet0/0
B    192.168.2.0/24 [20/0] via 10.10.10.2, 00:00:00
B    192.168.3.0/24 [20/0] via 10.10.10.2, 00:00:00
```

BGP (Border Gateway Protocol):

The only EGP in use today. BGP is a path-vector routing protocol that manages routes between ASs on the internet, allowing complex routing policies and efficient handling of thousands of routes.

Step by Step

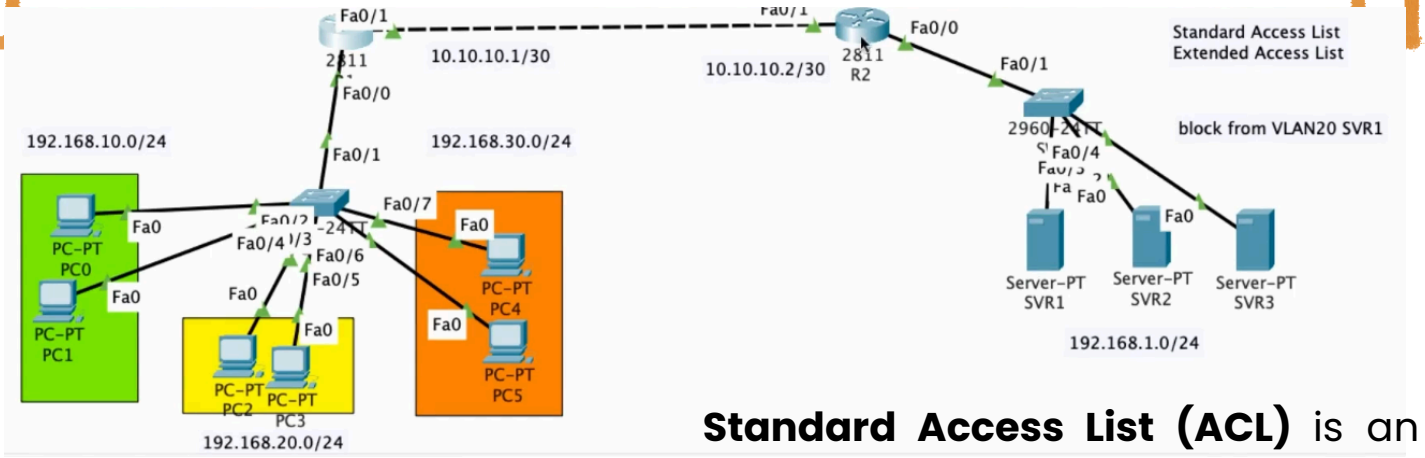
- **Router 2:** Here we enter the OS on router 1, namely "router bgp 3"
- **Configure Neighbor:** Enter Neighbor, namely the remote IP address and neighbor AS! The IP address and AS connected from router 2 to 3, why use 10.10.10.4? because in subnetting prefix 30, it gets an IP address of 4! and must start with 0 and end with 4!

Enter the network and mask in the router connected to the end service

RESULT

- **BGP :** Connected

STANDARD ACCESS LIST
CASE (BLOKIR VLAN 20 TO SERVER 1)

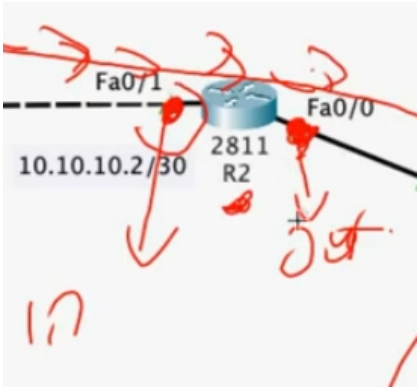


Standard Access List (ACL) is an access control list used in network devices, such as routers, to filter traffic based on the source IP address. Using standard ACLs, you can allow or deny traffic from specific IP addresses without checking other details such as protocols or ports.

Router 2

```
Router(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
Router(config)#access-list 1 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
Router(config)#access-list 1 de
Router(config)#access-list 1 deny ?
  A.B.C.D  Address to match
  any      Any source host
  host     A single host address
Router(config)#access-list 1 deny 192.168.20.0 ?
  A.B.C.D  Wildcard bits
  <cr>
Router(config)#access-list 1 deny 192.168.20.0 0.0.0.255
```

```
Router(config)#access-list 1 permit any
Router(config)#
Router(config)#do show access-list
Standard IP access list 1
    10 deny 192.168.20.0 0.0.0.255
    20 permit any
```

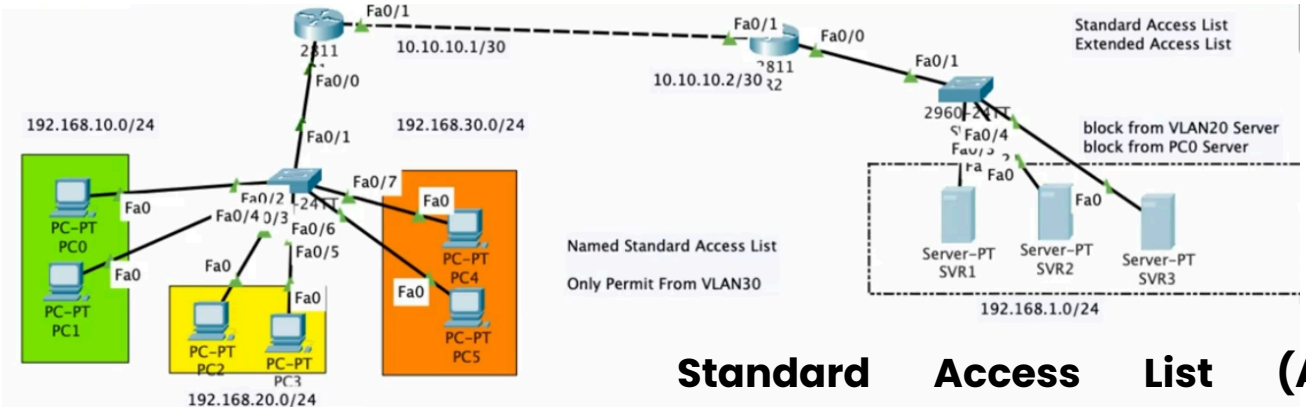



```
Router(config-if)#ip access-group 1 ?
  in    inbound packets
  out   outbound packets
Router(config-if)#ip access-group 1 out
```

Explanation

- Access-list : there we choose the standard range from range 1-99 (free) and must start with 1!
- deny : block, permit : allow, remark : with comment
- A.B.C.D (Network uses wildcard mask)
- Any : from anywhere is blocked
- Host : to end user only
- in : enter the interface, if in it will block entry including the router
- out : where is the exit? we go to server 1, and choose one may be in may be out

STANDARD ACCESS LIST (SEQUENCE NUMBER)
ONLY FROM CLIENT TO DESTINATION!
CASE EXAMPLE (ONLY VLAN30 ALLOWS ACCESS TO SERVER)



Standard Access List (ACL) access control list used in network devices, such as routers, to filter traffic based on the source IP address. Using standard ACLs, you can allow or deny traffic from specific IP addresses without checking other details such as protocols or ports.

Router 2 (This is the default result of Sequence Number)

```
Router(config)#do show access-list
Standard IP access list 1
    10 deny 192.168.20.0 0.0.0.255 (10 match(es))
    20 permit any (23 match(es))
    30 deny host 192.168.10.2
```

Router 2 (Change Sequence Number for in priority)

```
Router(config)#ip access-list standard 1
Router(config-std-nacl)#?
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
```

```
Router(config)#ip access-list standard 1
Router(config-std-nacl)#
Router(config-std-nacl)#no 30

Router(config-std-nacl)#15 deny host 192.168.10.2
```

Router 2 (With ACL Name)

```
Router(config)#ip access-list standard ?
  <1-99>  Standard IP access-list number
  WORD    Access-list name
Router(config)#ip access-list standard PermitVLAN30

Router(config-std-nacl)#permit 192.168.30.0 0.0.0.255
Router(config-std-nacl)#
Router(config-std-nacl)#do show access-list
Standard IP access list 1
    10 deny 192.168.20.0 0.0.0.255 (10 match(es))
    15 deny host 192.168.10.2 (2 match(es))
    20 permit any (24 match(es))
Standard IP access list PermitVLAN30
    10 permit 192.168.30.0 0.0.0.255
```

Explanation

- **Input ACL :** We enter a standard ACL, we can use a name or a number.

Explanation

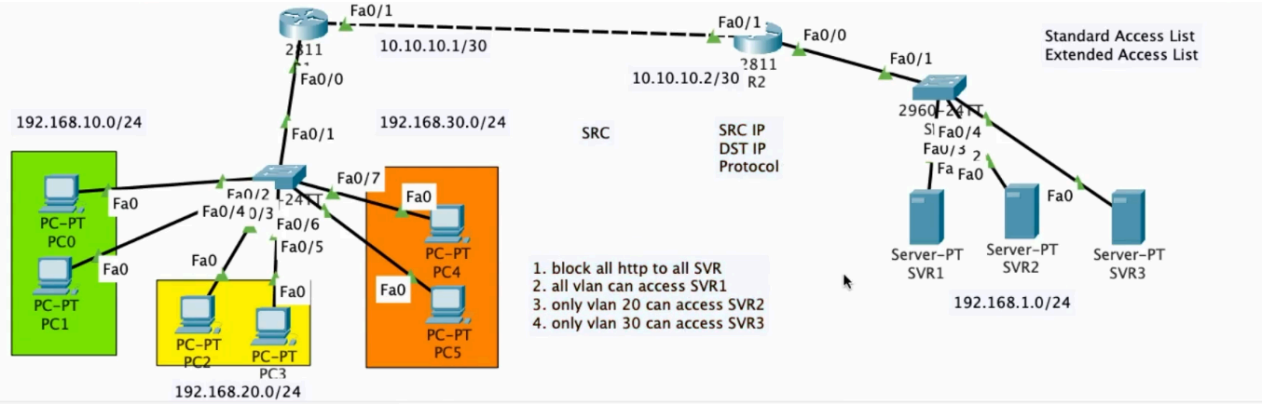
- **sequence number :** can enter sequence number, or can be added automatically deny : block permit : permission
-

Router 2 (ending with out) is out when adding ACL, whether number or name ACL, because number 1 ACL is already out, so Name ACL is also out!

```
Router(config-if)#ip access-group PermitVLAN30 out
```

```
Router(config-std-nacl)#do show access-list
Standard IP access list 1
    10 deny 192.168.20.0 0.0.0.255 (10 match(es))
    15 deny host 192.168.10.2 (2 match(es))
    20 permit any (24 match(es))
Standard IP access list PermitVLAN30
    10 permit 192.168.30.0 0.0.0.255
```

STANDARD ACCESS LIST VS EXTENDED ACCESS LIST



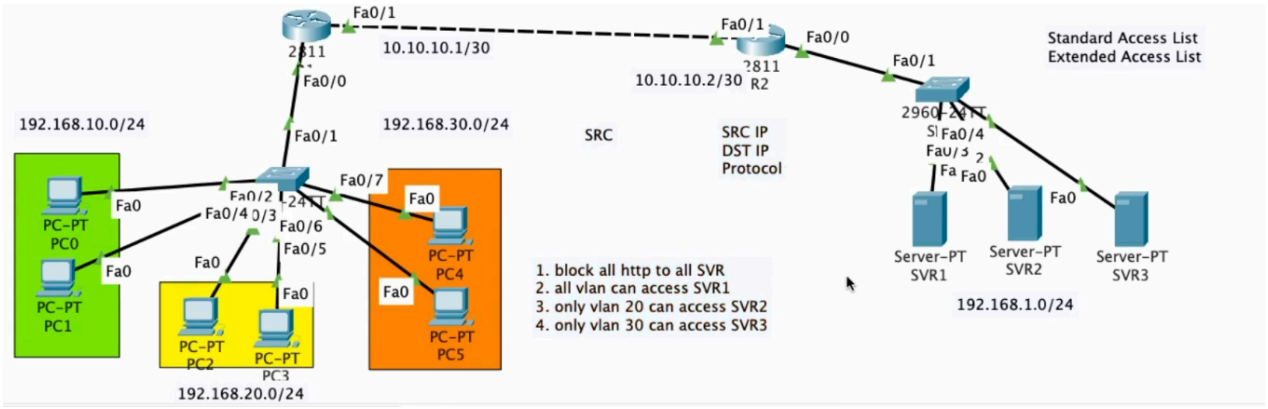
Standard Access List (Source)

- Standard ACL Features for Packet Filtering
- Standard ACL can only filter based on Source IP/Network (host, network)
- Standard ACL uses numbering 1-99
- Implementation/Applied as close as possible to Destination
- Using the IF – THEN concept
- There are only 2 Actions “Permit” & “Deny”
- The implementation of Direction IN & OUT is determined based on the direction of the packet from Source to Destination

Extended Access List (Source, Destination, Protocol)

- Extended Access-List can do Filtering based on source address, destination address, protocol, & port number
- Extended Access-List uses number 100-199
- Extended Access-List is used for more specific purposes in applications such as blocking telnet services
- Implementation/Applied as close as possible to the Source
- The implementation of Direction IN & OUT is determined based on the direction of the packet from the Source to the Destination

EXTENDED ACCESS LIST
(CASE BLOCK ALL HTTP TO ALL SERVER)



Router 1

```
Router(config)#access-list 100 deny ?
  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
Router(config)#access-list 100 deny tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
Router(config)#access-list 100 deny tcp any ?
  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
Router(config)#access-list 100 deny tcp any
```

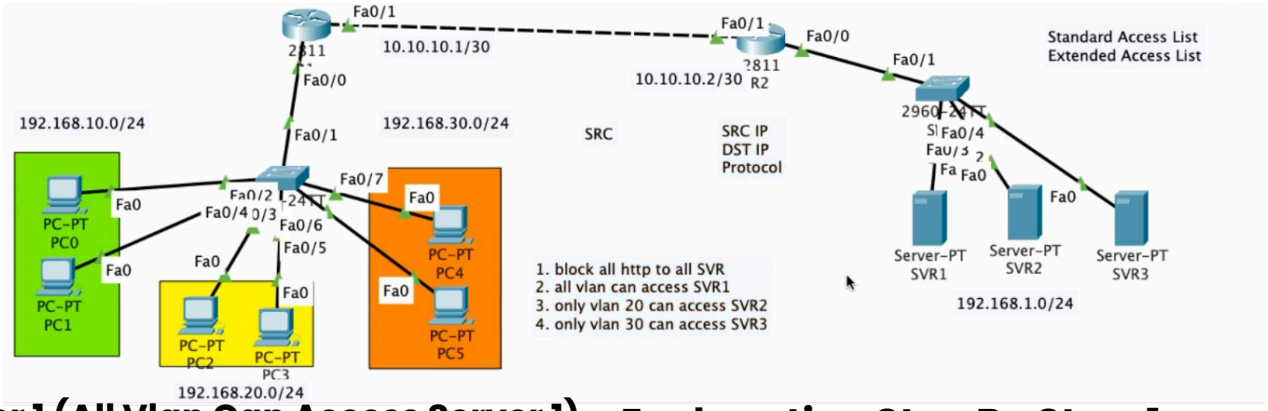
```
Router(config)#access-list 100 deny tcp any 192.168.1.0
0.0.0.255 ?
  dscp          Match packets with given dscp value
  eq            Match only packets on a given port number
  established   established
  gt            Match only packets with a greater port number
  lt            Match only packets 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
```

```
Router(config)#access-list 100 deny tcp any 192.168.1.0
0.0.0.255 eq 80
```

Explanation Step by Step

- access-list 100 : we create ACL 100 (can range from 100-199 and freely)
- deny : block
- tcp (http)
- any (source from anywhere)
- destination (where to go), we aim for the network server
- eq 80 : port 80 is the http port

EXTENDED ACCESS LIST
(CASE ALL VLAN ACCESS SERVER 1)
(ONLY VLAN 20 CAN ACCESS SERVER 2)
(ONLY VLAN 30 CAN ACCESS SERVER 3)



Router 1 (All Vlan Can Access Server 1)

```
Router(config)#access-list 100 permit ip any host
192.168.1.10
```

Router 1 (Only Vlan 20 Can Access Server 2)

```
Router(config)#access-list 100 permit ip 192.168.20.0
0.0.0.255 ?
  A.B.C.D  Destination address
  any      Any destination host
  host     A single destination host
Router(config)#access-list 100 permit ip 192.168.20.0
0.0.0.255 hos
Router(config)#access-list 100 permit ip 192.168.20.0
0.0.0.255 host 192.168.1.20
Router(config)#
```

Router 1 (Only Vlan 30 Can Access Server 3)

```
Router(config)#access-list 100 permit ip 192.168.30.0
0.0.0.255 host 192.168.1.30
```

It must be out!
here we use number 100

```
Router(config)#int fa0/1
Router(config-if)#ip ac
Router(config-if)#ip access-group 100 out
```

RESULT Extended Access List

```
Router(config)#do show access-list
Standard IP access list 1
    10 deny 192.168.20.0 0.0.0.255 (3 match(es))
    20 permit any
Extended IP access list 100
    10 deny tcp any 192.168.1.0 0.0.0.255 eq www
    20 permit ip any host 192.168.1.10
    30 permit ip 192.168.20.0 0.0.0.255 host 192.168.1.20
    40 permit ip 192.168.30.0 0.0.0.255 host 192.168.1.30
```

Explanation Step By Step 1

- **access-list 100 :** we create ACL 100 (can range from 100-199 and freely)
- **permit :** allow
- **ip :** any (all vlan)
- **host :** the destination is server 1

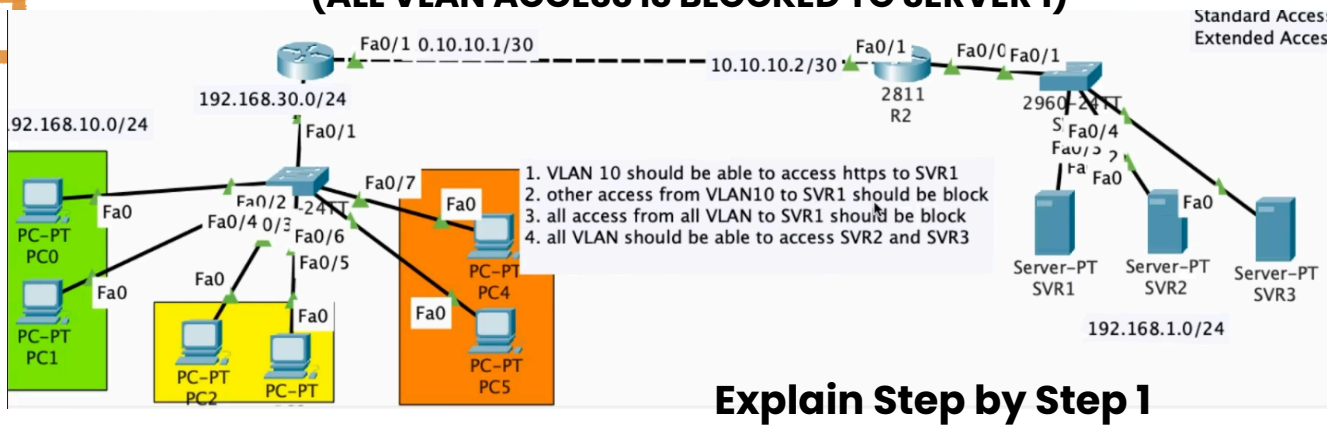
Explanation Step By Step 2

- **access-list 100 :** we create ACL 100 (can range from 100-199 and freely)
- **permit :** allow
- **ip :** ip VLAN 10
- **host :** the destination is server 2

Explanation Step By Step 3

- **access-list 100 :** we create ACL 100 (can range from 100-199 and freely)
- **permit :** allow
- **ip :** Vlan 30
- **host :** the destination is server 3

EXTENDED ACCESS LIST
(VLAN 10 IS ALLOWED FOR HTTPS TO SERVER 1)
(ALL VLAN ACCESS IS BLOCKED TO SERVER 1)



Router 1 (Deleting Previous ACL)

```
Router(config)#int fa0/1
Router(config-if)#no ip access-group 100 out
```

Router 2 (Vlan 10 is allowed for HTTPS to Server 1)

```
Router(config)#ip access-list extended ?
  <100-199>  Extended IP access-list number
  WORD         name
Router(config)#ip access-list extended ACL
Router(config-ext-nacl)#
```

```
Router(config-ext-nacl)#permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
Router(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 ?
  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
Router(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255
```

```
Router(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 host
192.168.1.10 eq 443
```

Router 2 (All VLAN Access Blocked To Server 1)

```
Router(config-ext-nacl)#deny ip any host 192.168.1.10
```

Router 2 (All VLAN access is allowed to Server 2 and 3)

```
Router(config-ext-nacl)#permit ip any any
```

Router 2 (RESULT Extended ACL)

```
Extended IP access list ACL
    10 permit tcp 192.168.10.0 0.0.0.255 host 192.168.1.10 eq 443
    20 deny ip any host 192.168.1.10
    30 permit ip any any
```

Note

- Why does he permit any any? because previously we have blocked and can be seen from the sequence number that is prioritized, namely 10 and 20. Here we don't need to exit again because we have exited on ACL 100

Explain Step by Step 1

- delete previous ACL
- **permit :** permission
- **tcp :** https
- **source :** VLAN 10
- **Host :** destination to server 1
- **eq :** port 443 is the https port

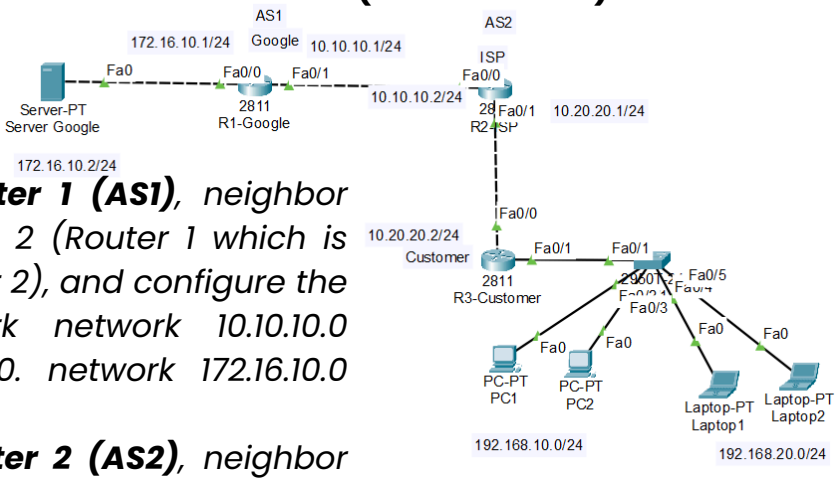
Explain Step by Step 2

- Block All VLANs to Host Server 1

Explain Step by Step 3

- Permit All VLANs to Host Server 2 & 3

NETWORK ADDRESS TRANSLATION (NAT)
DYNAMIC NAT (MANY TO ONE)



Routing BGP

- ***Router 1: BGP Router 1 (AS1)***, *neighbor 10.10.10.2 remote-as 2 (Router 1 which is connected to router 2), and configure the connected Network network 10.10.10.0 mask, 255.255.255.0. network 172.16.10.0 mask 255.255.255.0*
- ***Router 2: BGP Router 2 (AS2)***, *neighbor 10.10.10.1 remote-as 1 (Router 2 which is connected to router 1), and configure the connected Network network 10.10.10.0 mask 255.255.255.0, network 10.20.20.0 mask 255.255.255.0*
- ***Google Server:*** *Using Gateway, OK! 172.16.10.1*

Explanation of NAT in the Topology Above

Example

Source : 192.168.10.2/24 (PC1) [Ip Private]
Destination : 172.16.10.2/24 (Server Google)

Untuk konfigurasi Ip Private ke IP Public R3-Customer

Before

Source : 192.168.10.2/24
Destination : 172.16.10.2/24

Config NAT

After in Router 3

Source : 10.20.20.2/24 (Ip Public)
Destination : 172.16.10.2/24

Here we see that the Private IP changes to a public IP available on Router 3 using NAT.

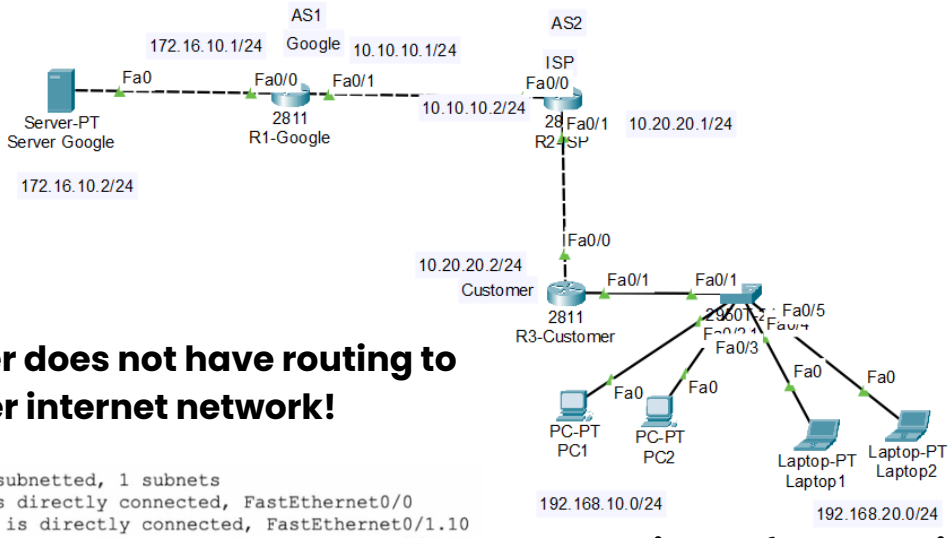
Types NAT:

- **Static NAT:** Each private IP is translated to a fixed public IP. This is used when devices on the local network need to be accessed from outside with a specific public IP.
- **Dynamic NAT:** A set of private IPs is translated to a set of dynamically available public IPs. The public IP is selected from the available pool when a device on the local network accesses the internet.
- **PAT (Port Address Translation) or NAT Overloading:** Multiple devices with private IPs share a single public IP, but are differentiated by port numbers. This is the most common type of NAT used in homes or offices.

Note

- Why don't we use BGP on Router 3? Because on Router 3 it is the customer/router at home. And on Router 3 it will be the NAT path and Default Router

DEFAULT ROUTER (ROUTER 3) CUSTOMER



From Customer does not have routing to google, or other internet network!

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.20.20.0 is directly connected, FastEthernet0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1.10
C    192.168.20.0/24 is directly connected, FastEthernet0/1.20
```

Default Routing Configuration on Router 3 (Customer)

```
R3-Customer(config)#ip route 0.0.0.0 0.0.0.0 10.20.20.1
```

- ***ip route 0.0.0.0 0.0.0.0 10.20.20.1*** **:** All networks on the internet and their subnet mask is 0.0.0.0, the customer's gateway is the ISP's router.

RESULT Default Routing!

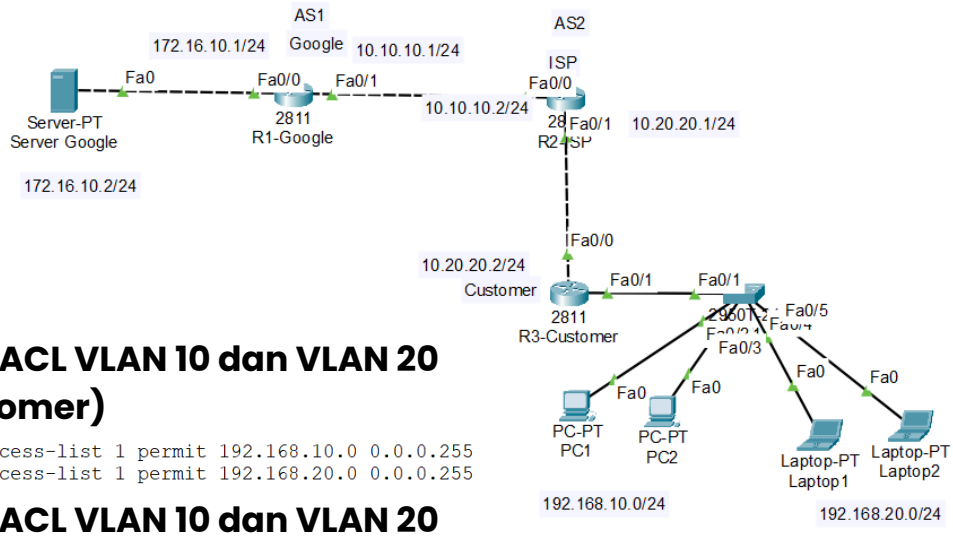
```
S*    0.0.0.0/0 [1/0] via 10.20.20.1
```

```
R3-Customer#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3-Customer(config)#do ping 172.16.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/1/9 ms
```

Explanation Default Routing

- **Default routing** is a concept in computer networking where a router is configured with a default route that is used to forward data packets to destinations that do not have a specific route in the routing table. The default route is used when no more specific route is available for the packet's destination.
- **Default Routing Topology above:** Because in Router 3 it is the customer. adding routing manually but the destination router is not specific to a particular router. but we go to all routers. we configure it to the customer router to go to the internet. it is impossible for him to static routing one by one!

NAT (Router 3) Customer



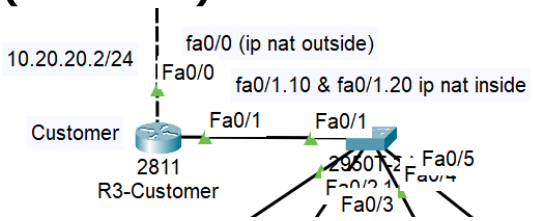
Configuration ACL VLAN 10 dan VLAN 20 Router 3 (Customer)

```
R3-Customer(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R3-Customer(config)#access-list 1 permit 192.168.20.0 0.0.0.255
```

Configuration ACL VLAN 10 dan VLAN 20 Router 3 (Customer)

```
R3-Customer(config)#ip nat inside source list 1 interface fa0/0 overload
```

Configuration Inside Outside Router 3 (Customer)

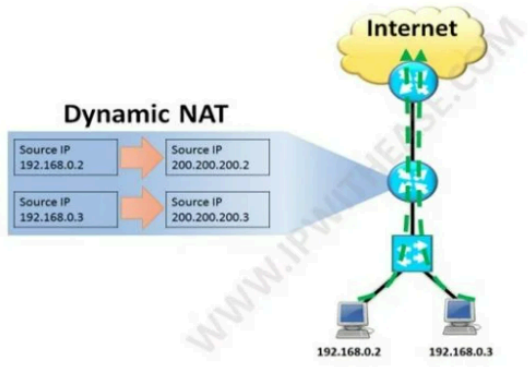


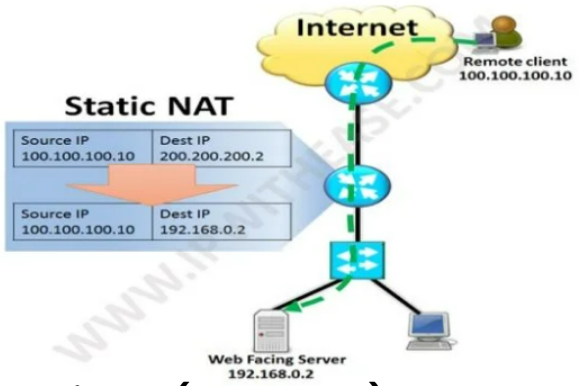

```
R3-Customer(config)#int fa0/0
R3-Customer(config-if)#ip nat outside

R3-Customer(config)#int fa0/1.10
R3-Customer(config-subif)#ip nat inside

R3-Customer(config)#int fa0/1.20
R3-Customer(config-subif)#ip nat inside
```

Step By Step Configuration NAT

- **Network to be NAT (ACL):** here we will enter VLAN 10 and VLAN 20 into NAT. We enter it with Standard ACL
- **NAT:** which comes from list 1 (VLAN 10 and VLAN 20) will be translated to the IP on fa0/0. So when it becomes an internet client, the source changes to the source on fa0/0 (public IP)
- **overload:** means translating a private IP into 1 public IP
- **Inside**: which leads to the ISP
- **Outside**: which leads to the VLAN

DYNAMIC NAT (MANY TO ONE) VS STATIC NAT (ONE TO ONE)





Dynamic Nat (Many to One)

- **Many to One:** Many Private IPs are translated into one public IP
- **Dynamic NAT:** more efficient in the use of public IP addresses and suitable for networks with many devices that only require outbound access to the internet.
- **Definition:** Dynamic NAT translates private IP addresses to public IP addresses dynamically, from the available public IP pool. With dynamic NAT, the public IP address used by internal devices can change every time the device accesses the internet.

When to use?

- When you have many devices that want to access the internet but only have a limited number of public IP addresses.
- **Example:** In an office with an internal network, dynamic NAT allows employee devices to access the internet using public IPs taken from a pool, without having to assign a public IP address to each device.

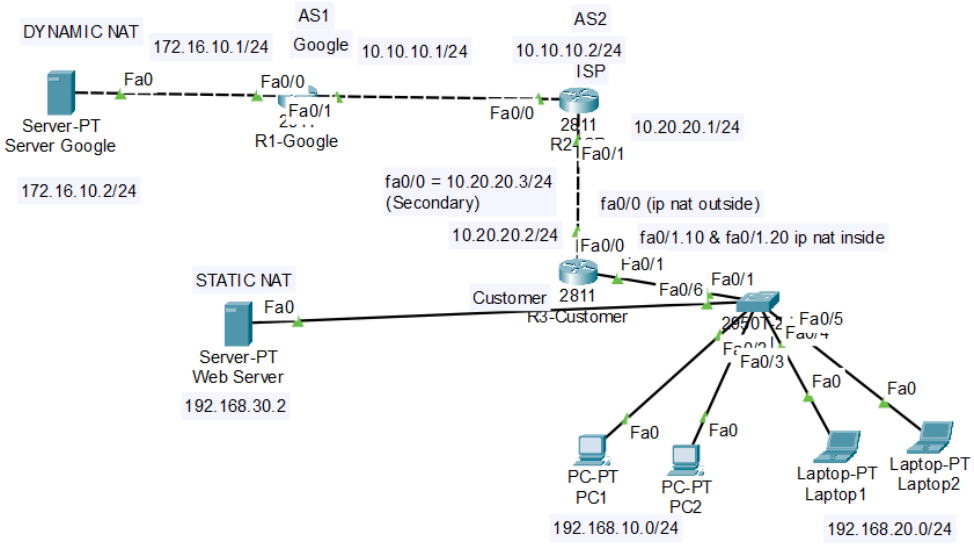
Static Nat (One to One)

- **One to One:** One Private IP is translated into one Public IP
- static NAT case: used when having a web server locally, so that the local web server can be accessed publicly. which accesses the internet is not the web server's private IP but its public IP
- **Static NAT:** suitable for devices that require a fixed public IP address and must be accessible from the internet, such as servers.
- **Definition:** Static NAT translates one private IP address into one fixed (static) public IP address. This means that every device on the local network always has the same public IP address when accessing the internet.

When to use?

- When a device on a local network needs to be constantly accessible from the internet via a specific public IP address.
- **Example:** If you have a web server on your internal network, static NAT allows you to map a fixed public IP address to that server so that it can be accessed from the outside.

CONFIGURATION STATIC NAT (ONE TO ONE)



Adding Public IP on Router 3

Real Device

```
R3-Customer(config-if)#ip add 10.20.20.3 255.255.255.0 secondary
```

If you are using Cisco Packet Tracer, just configure the STATIC NAT!

```
R3-Customer(config)#ip nat inside source static 192.168.30.2 10.20.20.3
```

Configure Nat Inside at fa0/1.30

```
R3-Customer(config)#int fa0/1.30
R3-Customer(config-subif)#ip nat insi
R3-Customer(config-subif)#ip nat inside
```

Test Web Server to Public Web IP which has been NAT from 192.168.30.2 (private IP) to Public IP 10.20.20.3

Static Nat (One to One)

- **Local Web Server:** Before we configure STATIC NAT, we will use a Local Web Server!
- **Local Web Server:** Access to the Internet!
- **One to One:** one Private IP is translated into One Public IP
- Here Public IP: 10.20.20.2 is already used by Dynamin NAT
- **Router 3:** Here we add the Public IP, which is 10.20.20.3
- **Flow:** Private IP 192.168.30.2 is made into Public IP, which is 10.20.20.3 using Static NAT
- **Adding Public IP to Router 3 (Real Device):** On the Real Device we can use the IP address 10.20.20.3 255.255.255.0 secondary
- **Router 3 Cisco Packet Tracer:** Let's go straight to the STATIC NAT!
- **Static Nat Router 3:** ip nat inside source static 192.168.30.2 10.20.20.3 here we directly STATIC NAT on router 3

Note

- Why not use outside? because we use **STATIC NAT directly on the router and not on the interface because Cisco packet tracer does not support secondary.** then it will be written as ip nat inside source static 192.168.30.2 10.20.20.3

TYPE IPv6 ADDRESS

Type	Range
Link Local	FE80::/10
Global Unicast	2000::/3
Unique Local	FC00::/7

Link Local

- **Prefix:** Link-local addresses always start with FE80::/10 (i.e., FE80 to FEBF).
- **Function:** Used for communication within a local network (link), such as within a subnet. Not routable to other networks or the Internet. Every device on the network must have a link-local address for basic operations.
- **Example**: FE80::1A2B:3C4D:5E6F:789A

Main Uses:

- Used for communication between devices in a local network without the need for a router.
- In the IPv6 autoconfiguration (SLAAC) process to generate globally routable IP addresses.
- Used in protocols such as Neighbor Discovery Protocol (NDP) to identify devices in a single link.
-

Global Unicast

- Prefix: This address is similar to the Public IP in IPv4, it can be routed to the internet. Global unicast addresses always start with 2 or 3 (for example, prefix 2000::/3).
- **Function**: This address is used for routable communication on the global internet network. Like the public IP in IPv4, every device connected to the internet has a global unicast address.
- **Example**: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Main Uses

- Used for communication between devices on the internet.
- Used in enterprise networks that require communication between subnets and to the internet.

Unique Local Address (ULA)

- **Prefix:** Unique Local Address is an address similar to Private IP in IPv4 (for example, 192.168.x.x or 10.x.x.x). This address starts with FC00::/7, but generally uses the prefix FD00::/8.
- **Function:** This address is used for local communication within an internal network. Cannot be routed on the internet, only used for private communication within an organization or network.
- **Example:** FD12:3456:789A:1::1

Main Uses:

- Used on an organization's internal network to ensure that addresses do not collide with addresses outside the network.
- As an alternative to using global unicast, but still ensures that devices inside the network remain inaccessible from outside.

Functions and comparisons

Tipe Alamat	Prefix	Routable	Kegunaan
Link Local	FE80::/10	Tidak	Komunikasi antar perangkat dalam satu link (tanpa router).
Global Unicast	2000::/3	Ya	Alamat untuk komunikasi di internet/global.
Unique Local	FC00::/7 (FD00::/8)	Tidak	Komunikasi dalam jaringan privat/internal (mirip IP Private IPv4).

IPv4 VS IPv6

	IPv4	IPv6
Address Space	32 bits	128 bit
Address Format	Decimal	Hexa Decimal
Possible Address	4.294.467.295	340282366920938463463374607431768211456
Example	192.168.1.1	2001:0db8:aaaa:bbbb:cccc:1111:2222:3333

IPv4

- **Prefix:** 0-32
- **Example:** 192.168.10.1/24
- **Explanation:** An IPv4 address consists of 32 bits divided into 4 parts, with each part containing 8 bits. This address is usually written in decimal format separated by periods. In the example 192.168.10.1/24, the number /24 indicates that the first 24 bits are part of the network identifier, while the rest are the host identifier.
- **Subnet Mask (Prefix):** For the /24 prefix, this means that the first 3 parts (192.168.10) are the network address, and the fourth part (1) is the host address. All devices on the same network must have the same first 3 parts, while the last part is different for each device.
  - **PC 1:** 192.168.10.1/24
  - **PC 2:** 192.168.10.2/24
- **This means that both devices are on the same network,** but have different host addresses.

IPv6

- **Prefix:** 0-128
- **Example:** 2001:db8:12:34:56:78:90:11/64
- **Explanation:** An IPv6 address consists of 128 bits divided into 8 sections, with each section containing 16 bits. The address is written in hexadecimal format and separated by colons. The example 2001:db8:12:34:56:78:90:11/64 shows that the first 64 bits are part of the network identifier, and the last 64 bits are the host identifier.
- **Subnet Mask (Prefix):** With a /64 prefix, the first 4 sections (2001:db8:12:34) are part of the network address, and the last 4 sections are used to identify hosts on the network.
  - PC 1: 2001:db8:12:34:56:78:90:11/64
  - PC 2: 2001:db8:12:34:56:78:90:12/64
- Both have the same network address, but different host addresses, indicating that they are on the same network but with unique host identities.

Conclusion:

- **IPv4 =** uses 32-bit addresses divided into 4 parts with each part containing 8 bits. In the /24 prefix, the first three parts specify the network, while the last part is the host.
- **IPv6 =** uses 128-bit addresses divided into 8 parts with each part containing 16 bits. In the /64 prefix, the first four parts specify the network, and the last four parts specify the host.

IPV6 ADDRESS COMPRESSION UNCOMPRESSION

2001:0db8:0be0:75a2:0000:0000:0000:0001

2001:db8:be0:75a2:0:0:0:1

2001:db8:be0:75a2::1

Explanation:

- **There are 8 parts! :** Each network has 8 parts, 4 network parts 4 host parts
- **There are 4 characters :** Each part has 4 main characters
- We abbreviate by reducing the 0 in front = Each part can be abbreviated by reducing the 0 in front
- **we replace it with "::"** : If we have a lot of 0000 we can replace it with "::"

2001:0db8:0000:0000:0010:0000:0000:0001

Wrong

2001:db8::10::1

Correct

2001:db8::10:0:0:1

2001:db8:0:0:10::1

Explanation:

- **There are 0000 more than 2 parts :** We can only choose one part to be used as "::"

Exercise Address Compression

2001:0db8:0ab0:0d00:0000:0000:0000:8c01

2001:0db8:0000:4c05:0000:0000:05ad:0bb1

2001:0db8:0000:0000:1234:0000:0000:da61

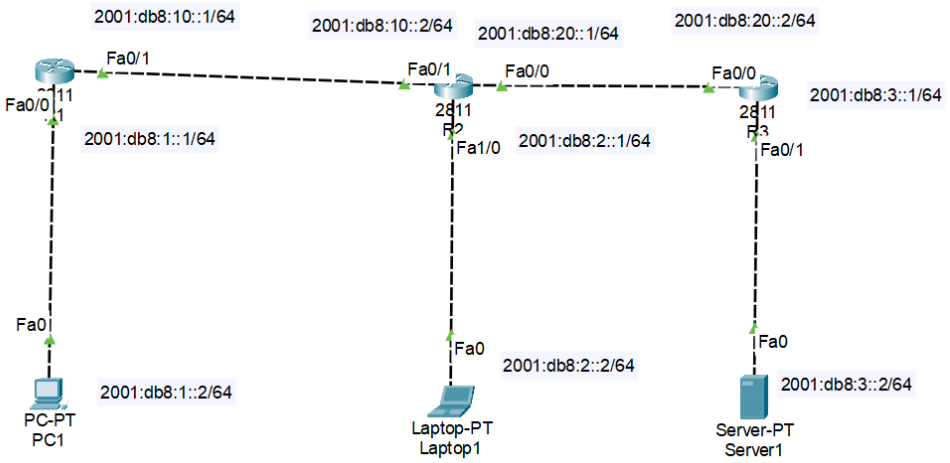
Exercise Address Uncompression

2001:db8:ab::bc0:c1ab

2001:db8:a000:c05:b0::1

2001:db8:0:1234::61

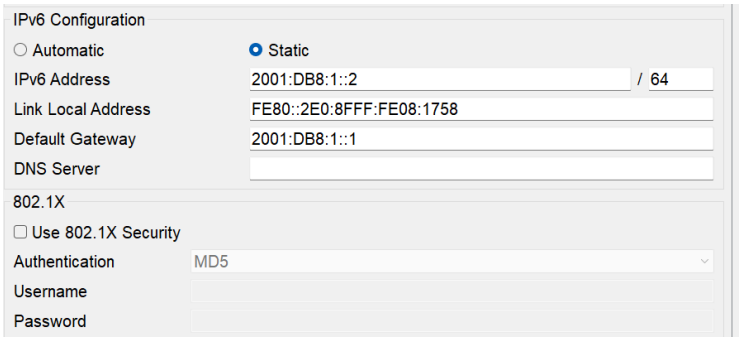
Configuration IPv6



Adding IP Address to Interface

```
R1(config)#int fa0/1
R1(config-if)#ipv
R1(config-if)#ipv6 add
R1(config-if)#ipv6 address 2001:db8:10::1/64
```

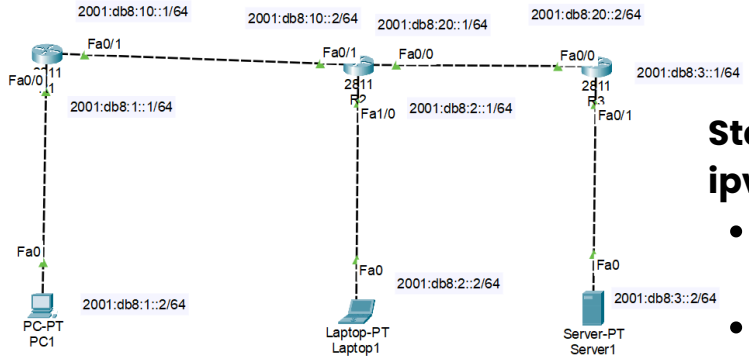
Configuration IP Static Our Client



Step By Step :

- **Input the interface:** Fa0/1 etc.
- **Input the IPv6 Address:** 2001:db8:10::1/64 etc.
- **No subnet mask:** in IPv6 there is no subnet mask like IPv6, it goes straight to the prefix
- **Here we use Static IP first for IPv6**: That is the IP from the Router (Public IP) and the prefix and gateway

IPV6 STATIC ROUTING CONFIGURATION IP ROUTE "DESTINATION" "PREFIX" "WHERE TO GO"?



Route 1 (Static Routing)

```
R1(config)#ipv6 route 2001:db8:2::/64 2001:db8:10::2
R1(config)#ipv6 route 2001:db8:20::/64 2001:db8:10::2
R1(config)#ipv6 route 2001:db8:3::/64 2001:db8:10::2
```

Router 2 (Static Routing)

```
R2(config)#ipv6 route 2001:db8:1::/64 2001:db8:10::1
R2(config)#ipv6 route 2001:db8:3::/64 2001:db8:20::2
```

Router 3 (Static Routing)

```
R3(config)#ipv6 route 2001:db8:2::/64 2001:db8:20::1
R3(config)#ipv6 route 2001:db8:10::/64 2001:db8:20::1
R3(config)#ipv6 route 2001:db8:1::/64 2001:db8:20::1
```

Router (unicast-routing) fungsinya untuk menghubungkan routing di Router

```
R1(config)#ipv6 unicast-routing
R2(config)#ipv6 unicast-routing
R3(config)#ipv6 unicast-routing
```

Static Routing (Router 1)

ipv6 route 2001:db8:2::/64 2001:db8:10::2

- **Destination:** Network Router 2 connected to the Client Interface
- **Through which way? :** It will pass through the interface connected from router 1 to router 2

ipv6 route 2001:db8:20::/64 2001:db8:10::2

- **Destination :** Network interface Router 2 yang terhubung ke Router 3
- **Lewat mana? :** Router 2 interface connected to Router 3

ipv6 route 2001:db8:3::/64 2001:db8:10::2

- **Destination:** Network Router 3 connected to interface server
- **Through which way?:** It will pass through the interface connected from router 1 to router 2

Explain Unicast Routing

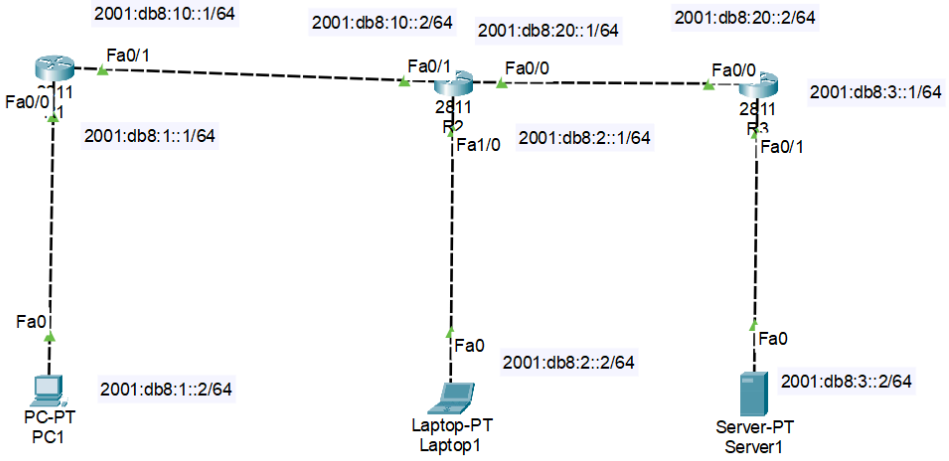
Unicast routing in the context of IPv6 is the process of routing data packets from one device to another directly based on unique IPv6 addresses. In IPv6, unicast routing is used to send data from a single source to a specific destination, meaning one source IP address to one destination IP address..

Function Unicast Routing IPv6:

- **Data Delivery:** Directs data packets from one node to another node that has a unique IPv6 address. Packets sent in unicast mode will go to one specific recipient address.
- **Routing Protocols:** Allows the use of routing protocols such as OSPFv3, EIGRP for IPv6, and BGP to determine the best path and direct packets to the right destination based on the IPv6 routing table.
- **Network Management:** Assists in network management and setup by providing a method for efficient and accurate data packet routing at scale.
- **User Experience:** Ensures that data sent from one device reaches the right device, enabling consistent and reliable communication between devices on an IPv6 network.

Unicast routing in IPv6 functions to send data packets directly from one device to another based on the destination IPv6 address.

CONFIGURATION OSPF IPv6



Router 1 add Ospf 1 and router id

```
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please
configure manually
R1(config-rtr)#router
R1(config-rtr)#router-id 10.10.10.1
```

Router 1 menambahkan ospf 1 dan area 0 pada interface

```
R1(config-rtr)#int fa0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#int fa0/1
R1(config-if)#ipv6 ospf 1 area 0
```

Router 2

```
R2(config)#ipv6 router ospf 2
R2(config-rtr)#router-id 10.10.10.2
R2(config-rtr)#int fa0/0
R2(config-if)#ipv6 ospf 2 area 0
R2(config-if)#int fa1/0
R2(config-if)#ipv6 ospf 2 area 0
R2(config-if)#ipv6 ospf 2 area 0
R2(config-if)#
00:24:15: %OSPFv3-5-ADJCHG: Process 2, Nbr 10.10.10.1 on
FastEthernet0/1 from LOADING to FULL, Loading Done
```

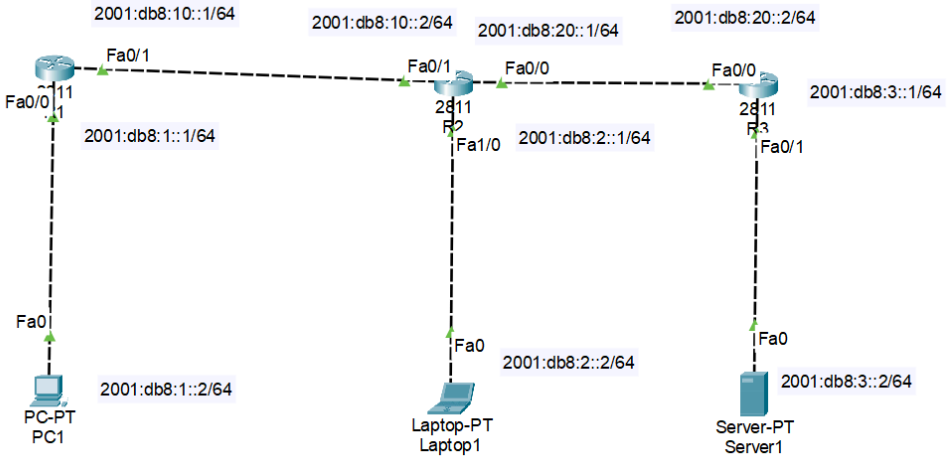
Router 3

```
R3(config)#ipv6 router ospf 3
%OSPFv3-4-NORTRID: OSPFv3 process 3 could not pick a router-
id,please configure manually
R3(config-rtr)#router-id 10.10.10.3
R3(config-rtr)#int fa0/0
R3(config-if)#ipv6 ospf 3 area 0
R3(config-if)#int fa0/1
R3(config-if)#ipv6 ospf 3
00:25:44: %OSPFv3-5-ADJCHG: Process 3, Nbr 10.10.10.2 on
FastEthernet0/0 from LOADING to FULL, Loading Done

R3(config-if)#ipv6 ospf 3 area 0
```

Step by Step :

- **We configure the router ospf:** ipv6 router ospf 1 (why does it start with 1? because ospf must start with 1
- **Why area 0?:** area 0 must exist at the beginning of every time we use OSPF! (the area of each router must be the same!) (except multilayer)
- **Why do we have to enter the router id?:** Router ID is needed in OSPFv3 to provide unique identification on the router, support DR/BDR election, and ensure integrity and consistency in the exchange of routing information. Although OSPFv3 works with IPv6, the basic principles of identification and management remain relevant by using the Router ID. **(the router id of each router must be with the same network! but different hosts!)**

CONFIGURATION EIGRP IPv6



Router 1

```
R1(config)#ipv6 router eigrp 10
R1(config-rtr)#eigrp router-id 10.10.10.1
R1(config-rtr)#no shutdown
R1(config-rtr)#int fa0/0

R1(config-if)#ipv6 eigrp 10
R1(config-if)#int fa0/1
R1(config-if)#ipv6 eigrp 10
```

Router 2

```
R2(config)#ipv6 router eigrp 10
R2(config-rtr)#eigrp router-id 10.10.10.2
R2(config-rtr)#no shutdown
R2(config-rtr)#int fa0/1
R2(config-if)#ipv6 eigrp 10
R2(config-if)#
%DUAL-5-NBRCHANGE: IPv6-EIGRP 10: Neighbor
FE80::260:47FF:FE22:6002 (FastEthernet0/1) is up: new adjacency

R2(config-if)#int fa1/0
R2(config-if)#ipv6 eigrp 10
R2(config-if)#int fa0/0
R2(config-if)#ipv6 eigrp 10
```

Router 3

```
R3(config)#ipv6 router eigrp 10
R3(config-rtr)#eigrp router-id 10.10.10.3
R3(config-rtr)#no shutdown
R3(config-rtr)#int fa0/0
R3(config-if)#ipv6 eigrp 10
R3(config-if)#
%DUAL-5-NBRCHANGE: IPv6-EIGRP 10: Neighbor FE80::2D0:97FF:FEAC:
7A01 (FastEthernet0/0) is up: new adjacency

R3(config-if)#int fa0/1
R3(config-if)#ipv6 eigrp 10
```

Explanation:

- **We configure the router ospf:** ipv6 router EIGRP 10 (why does it start with 10 because the ID is 10) each ID on the router must be the same!
- **Why area 0?:** area 0 must exist at the beginning of each time we use OSPF! (the area of each router must be the same!) (except multilayer)
- **Why do we have to enter the router id?:** In short, the Router ID in EIGRP for IPv6 ensures that each router has a unique identity in the routing process, which allows EIGRP to operate effectively and stably on the IPv6 network. (the router id of each router must be with the same network! but different hosts!)
- **Why must there be no shutdown:** because in EIGRP IPv6 it is off by default and must be in no shutdown!