5/31/2021

Nadir Hussain

023-18-0025

Computer Networks

Lab 10

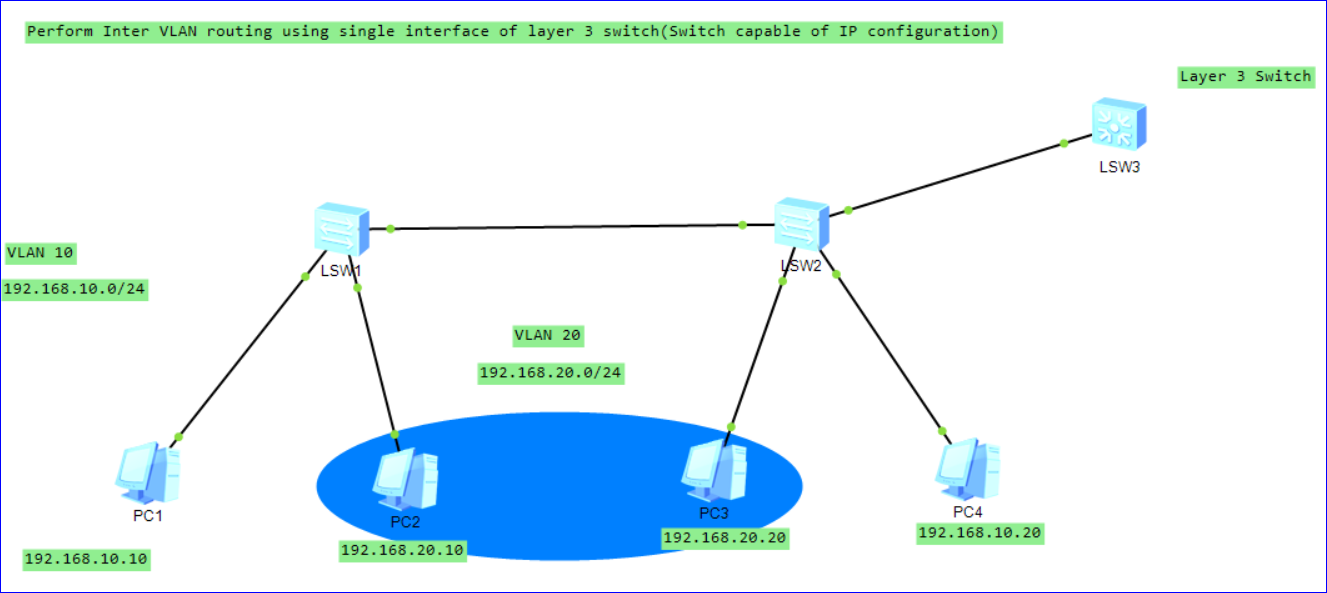
**Lab Objectives:**

* Perform Inter VLAN routing using single interface of layer 3 switch (Switch capable of IP configuration)
* Configure Access control list (ACL), practice it’s commands

**Perform Inter VLAN routing using single interface of layer 3 switch(Switch capable of IP configuration)**

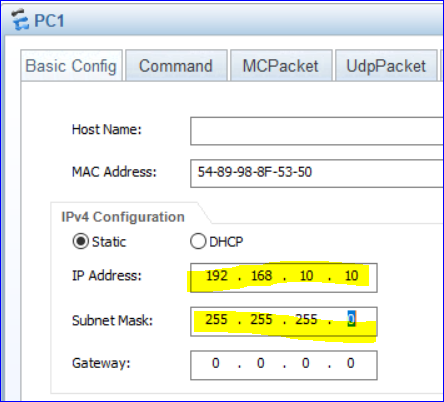
We have to configure VLAN for single interface layer 3 switch first.

**Network Design**



**Configure PCs with subnet mask**

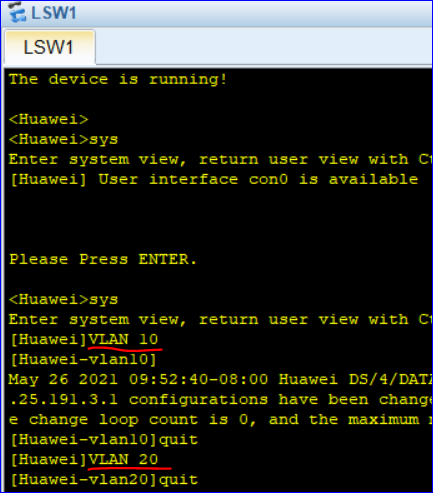
On Pc1



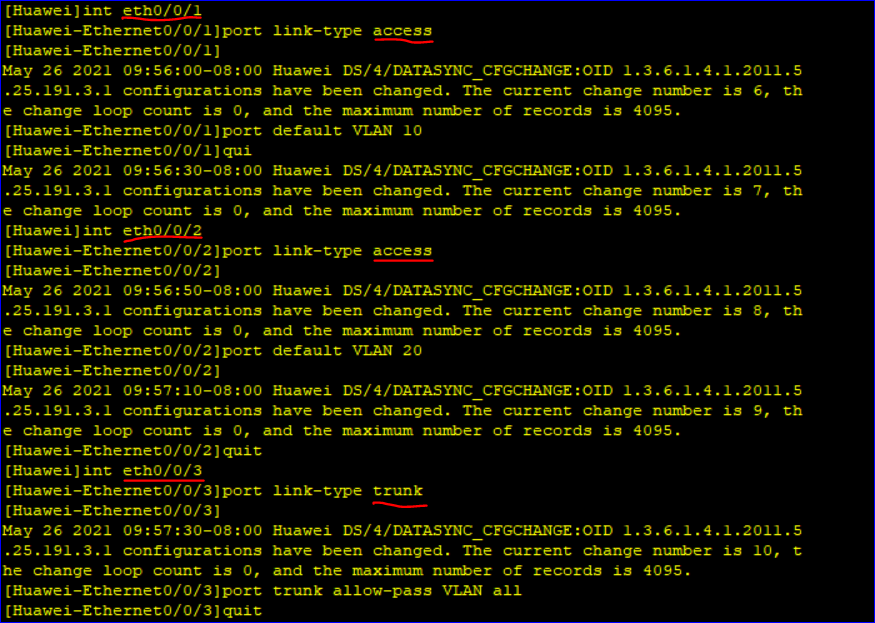
Similarly configure all PCs with their respective VLAN IPs, note we don’t provide gateway address yet.

**Create 2 VLANs i.e 10 and 20 on switch 1 and switch 2**

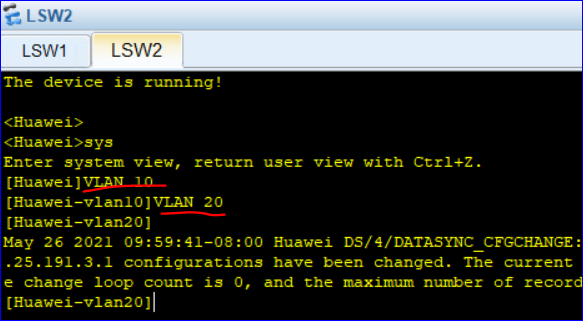
On Switch1



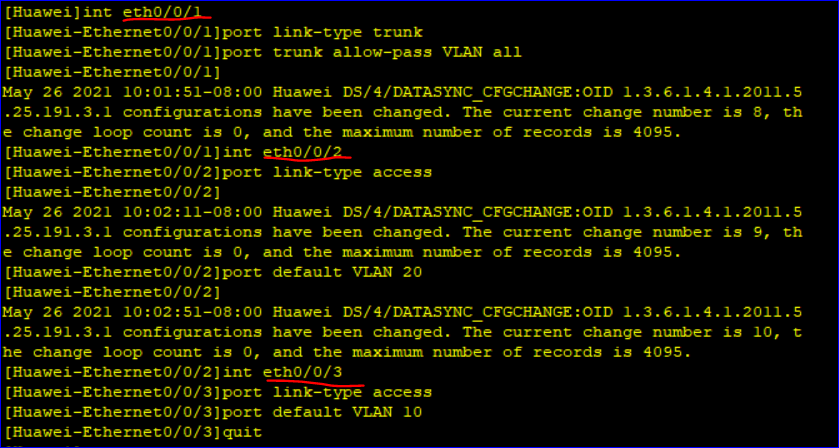
**Now configure All interfaces and add them to their respective VLANs**



**Similarly we create VLANs on switch 2 and add interface to their VLANs**

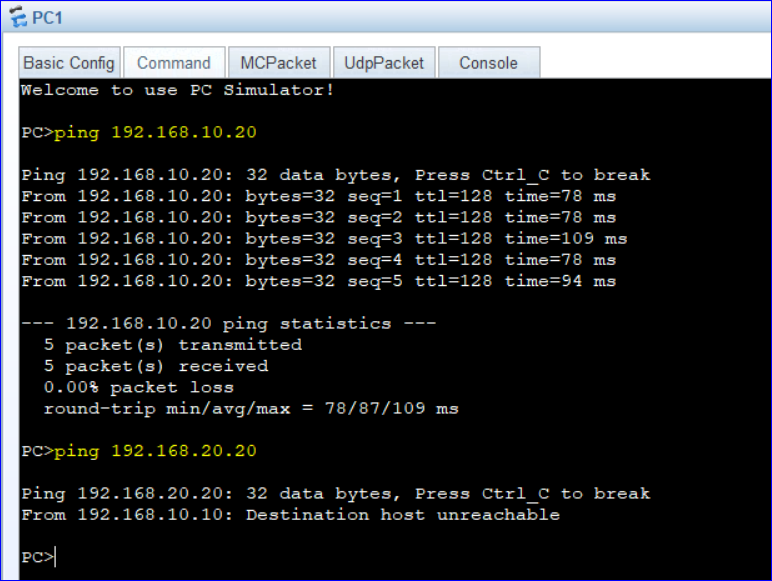


**Now add interfaces to VLANs**



**Let’s ping if we have configured correctly both of our VLANs**

PC1 should ping to PC4 but not to 3 and 2.



So our VLANs are working correctly.

**But we want to make VLANs communicate! What to do?**

Use Inter VLAN using single interface of Router or layer3 switch.

Previously we use router for Inter VLAN, but now we use Layer3 switch, that is cheaper and cost-effective solution to connect VLANs.

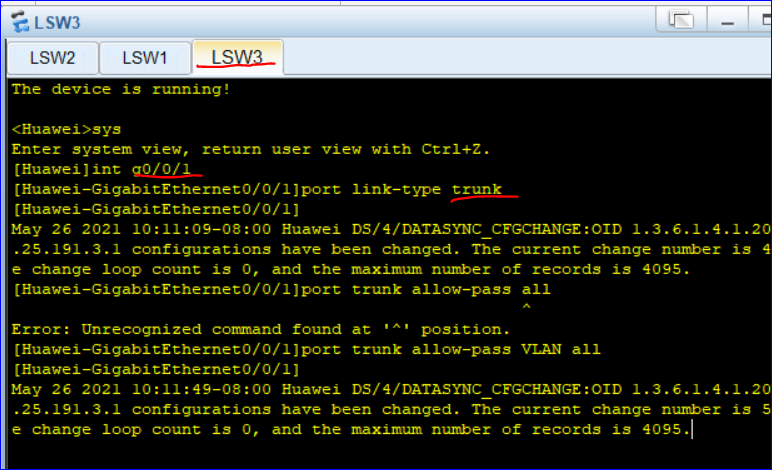
**Layer3 Switch:**

* S5700 is layer 3 switch
* Layer 3 switch is connected with GE, While Layer 2 switches are connected to Ethernet
* Switches number start from 1, while routers start from 0 but layer 3 switch starts from 1 though.

 Layer3 Switch

**Now we perform VLAN on layer 3 using switch**

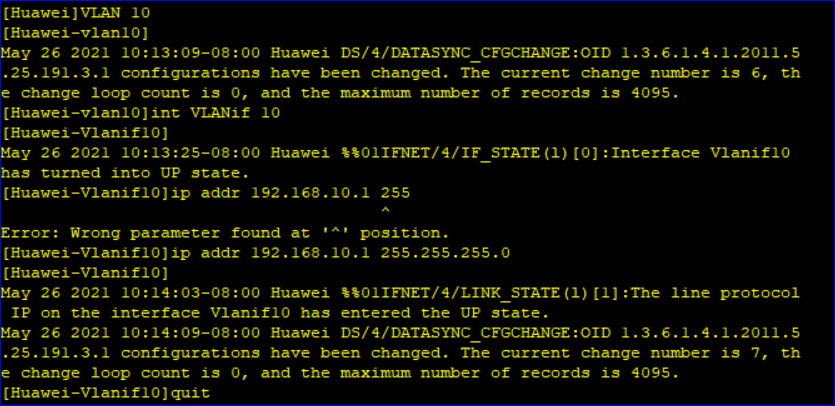
**On switch layer 3**



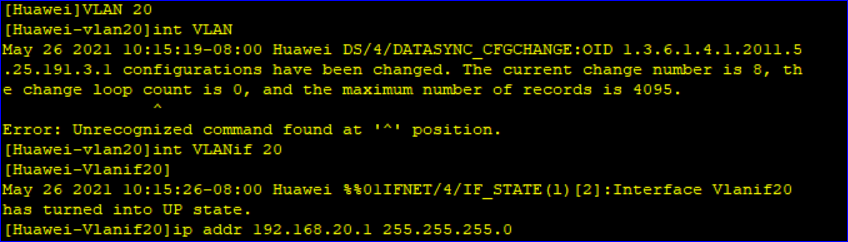
*Now we have created trunk*

We should create VLAN on this switch and configure IPs

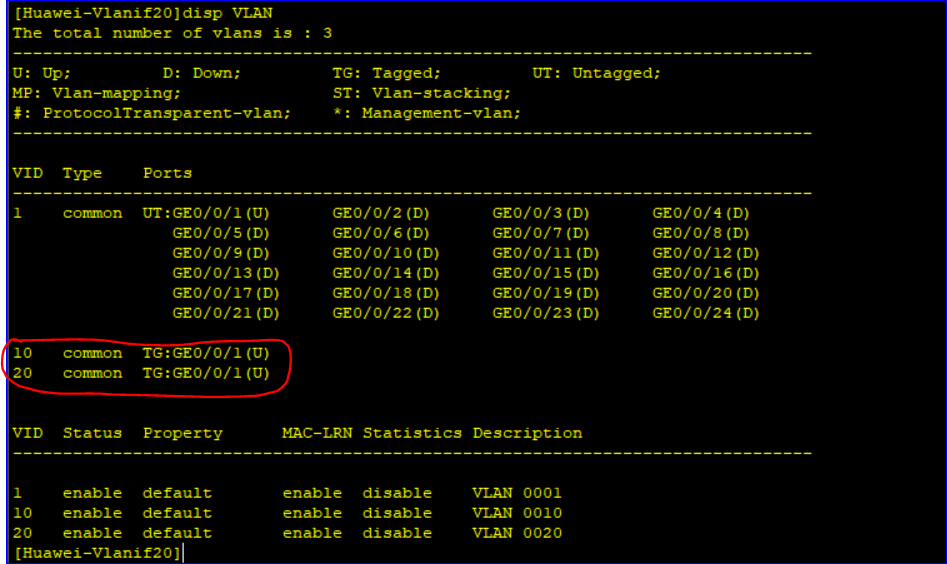
**Configure VLAN 10 on Layer3 switch as**



**Configure VLAN 20 on layer 3 switch as**



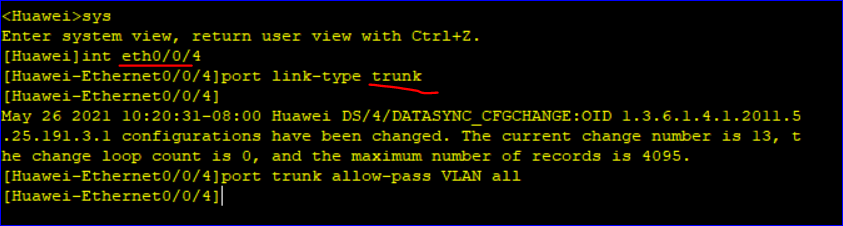
**Now display all VLANs on switch**



So we have added both VLANs to Inter VLAN switch

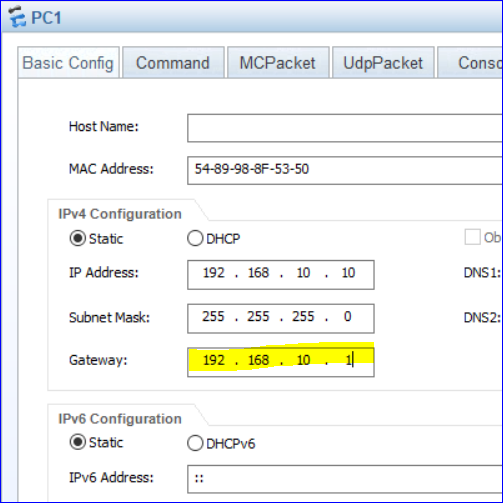
Now on Switch2 we should allow traffic from both VLANs to pass through interface eth0/0/4

**There make eth0/0/4 as trunk**



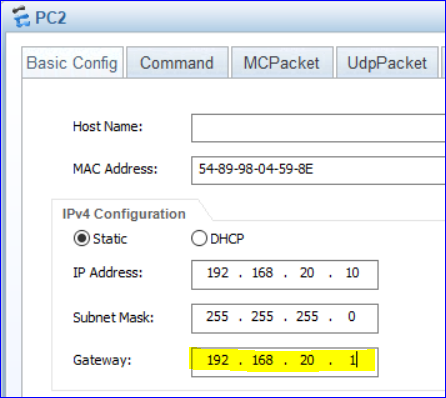
Upto here we have configured tha LANs with inter VLAN interface using Layer3 switch.

Now as our traffic will need to move to layer3 switch, so we assign Gateways to all PCs as

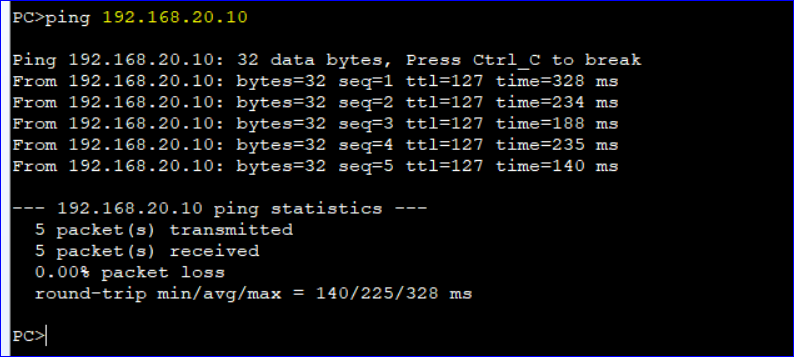


***Same gatway will be for PC4***

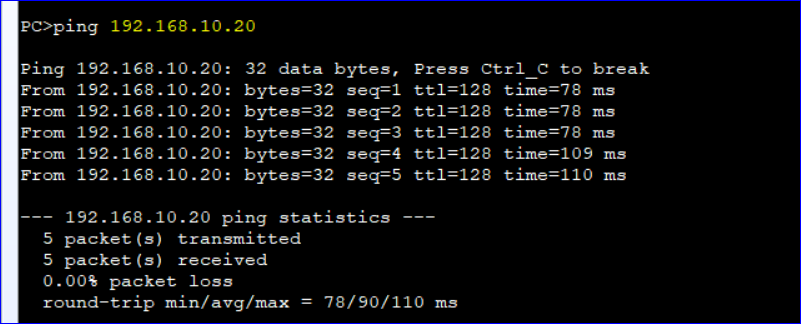
**On PC2 and PC3, gateway will be gateway**



**Now our 2 LANs must be connected. Let’s ping from PC1(VLAN 10) to PC2 (VLAN 20)**



**And test PC1 and PC4 connection as well.**



So we have finally configured Inter VLAN using layer3 switch rather than expensive routers.

**But How does it work?**

Switch1 and Switch 2 are broadcast domains, they both have 2 pcs in their physical broadcast, but we have created virtual broadcast and override the physical broadcast.

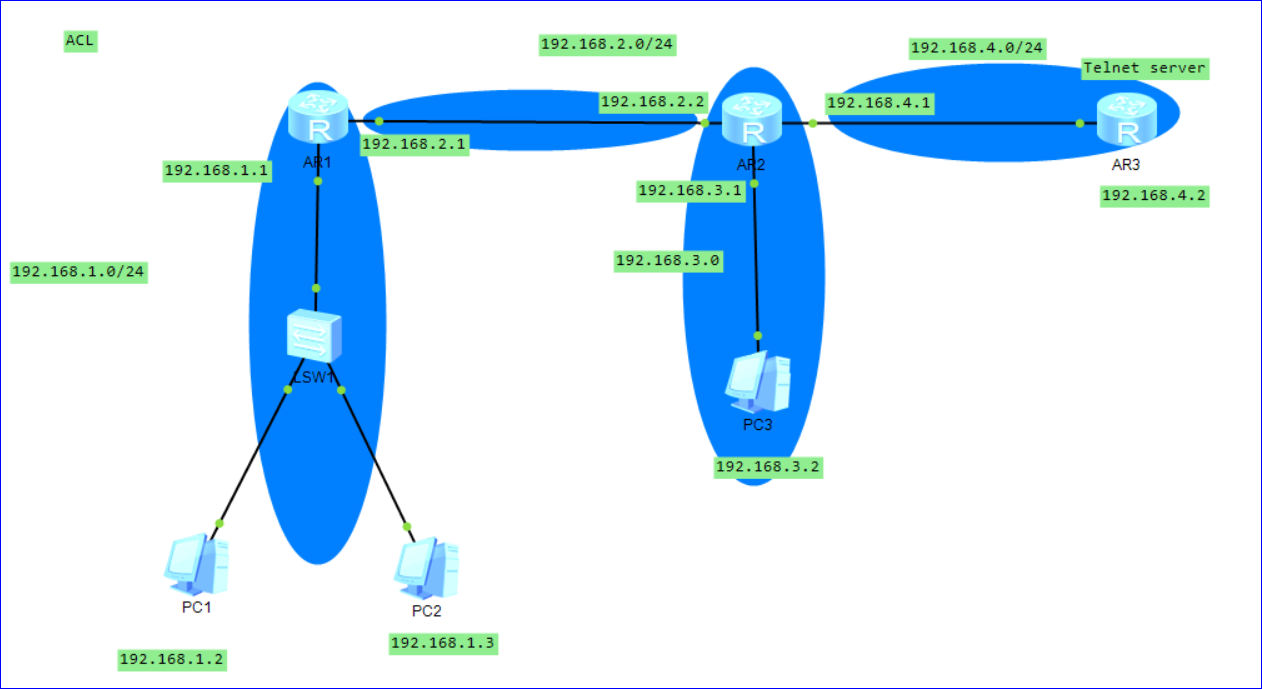
Now when we ping from 10.10 to 20.10, then ARP messages are received to Switch 3, then they are connected to VLAN 20 and messages are broadcast toward another VLAN.

**Configure Access control list (ACL), practice it’s commands**

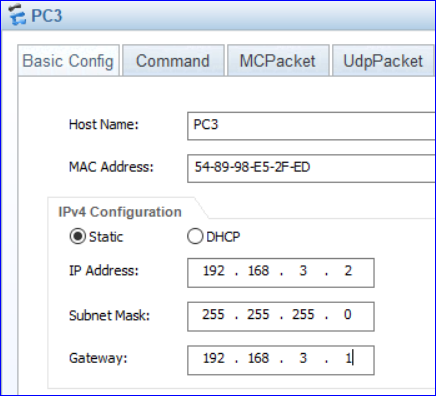
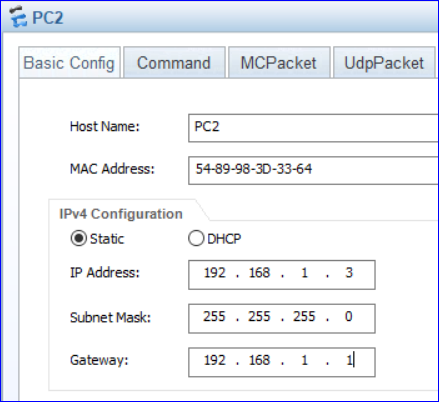
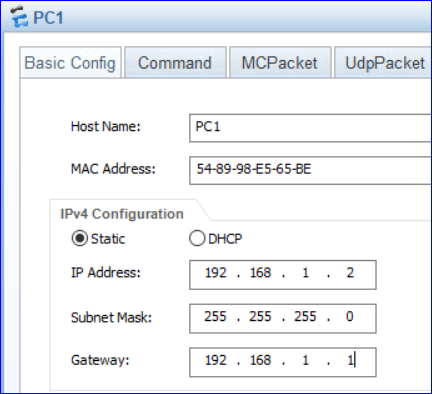
Topology

* Take 3 AR2220 routers, 3 Pcs and 1 3700 Switch
* Connect Switch to router 1, and 2 PCs to Switch
* Connect PC to router 2
* Connect all routers

**Network design**

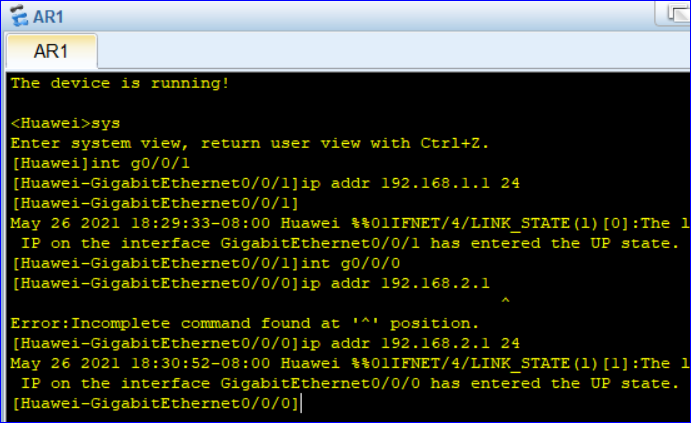


**Configure PCs with their gateways**

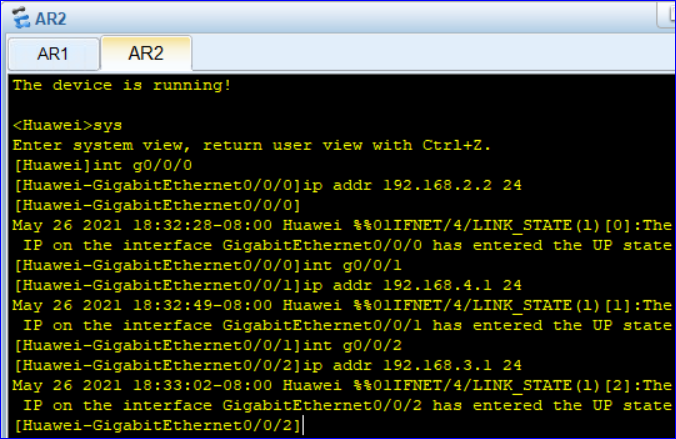


**Configure interface on each router**

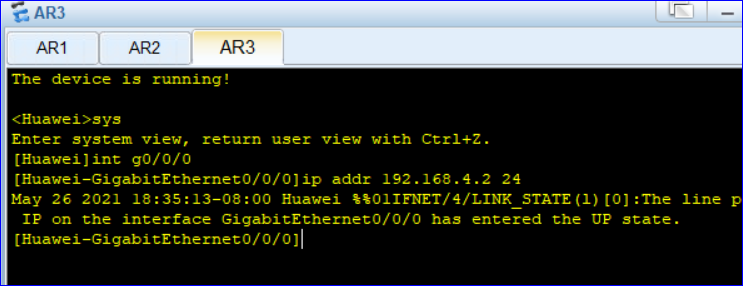
**On Router1**



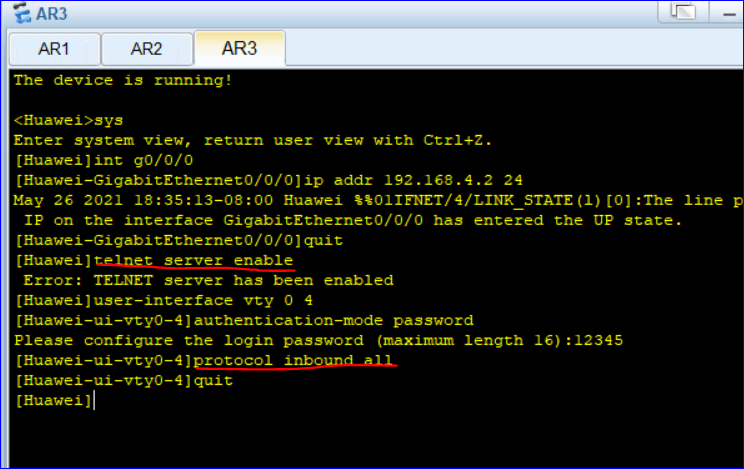
**Router2**



**Router3**

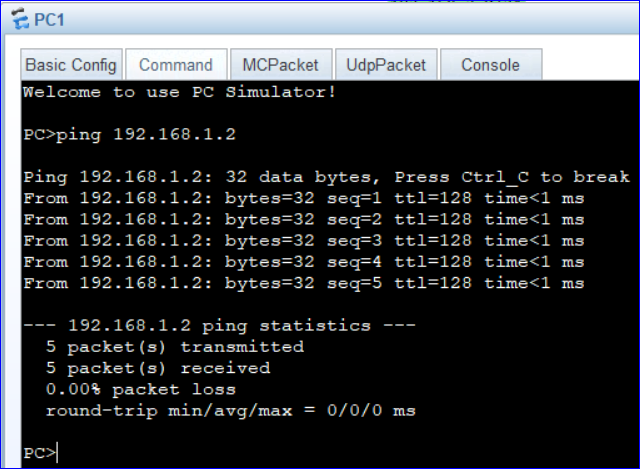


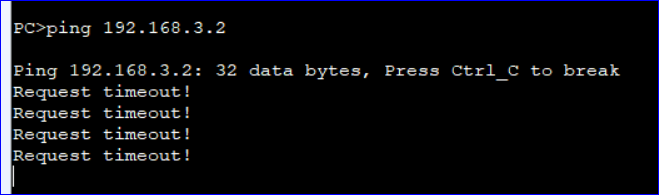
*Router 3 will be used as Telnet server so we Enable telnet and create user*



Now let us ping from PC1 to other PCs

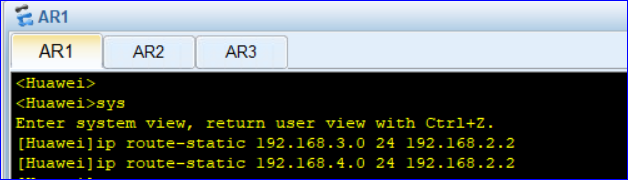
PC1 to PC2, and PC1 to PC3



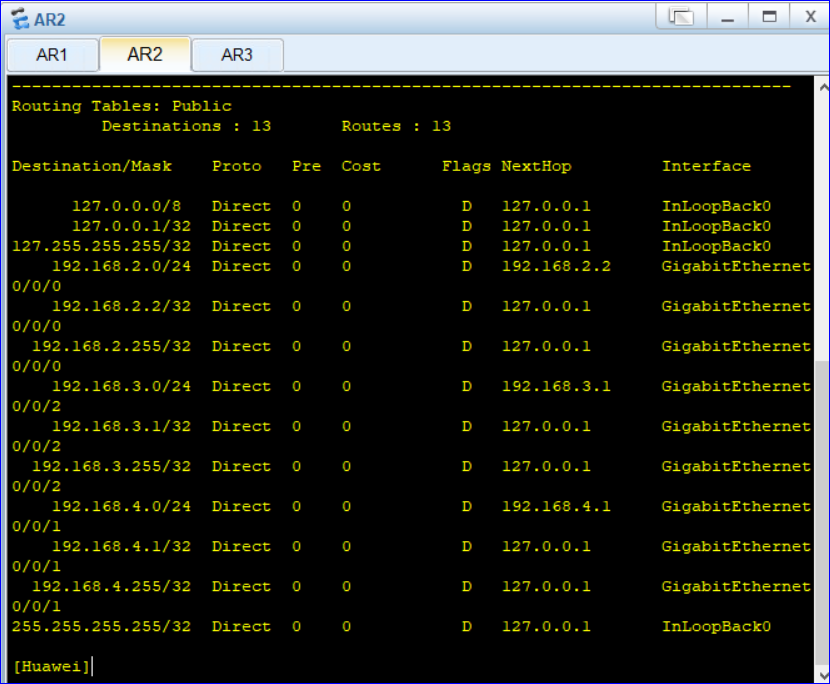


We could not reach PC2 which is on network 3.0, so we need to define routes first, by static routing.

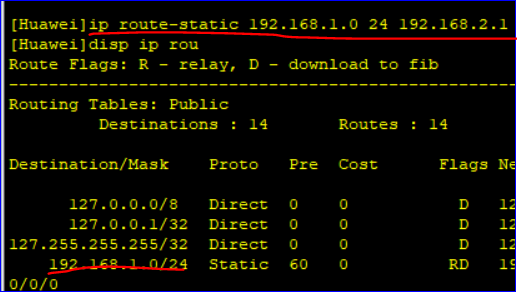
On router1



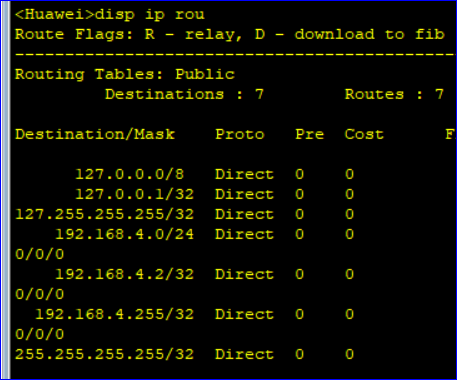
On Router 2



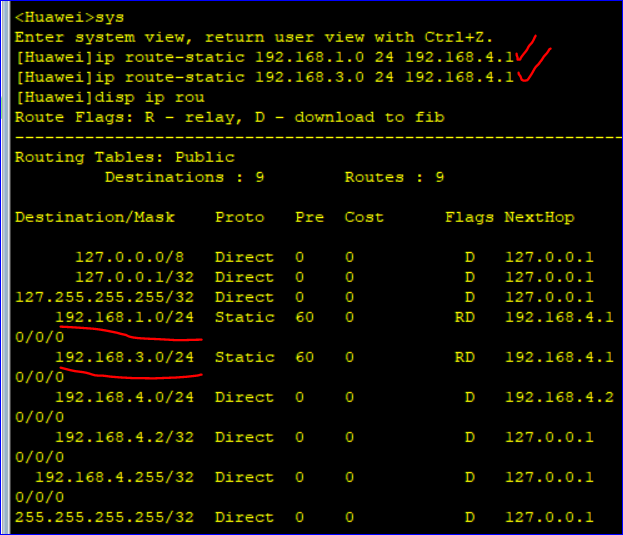
We can’t find 192.168.1.0, so add route to that



On router3

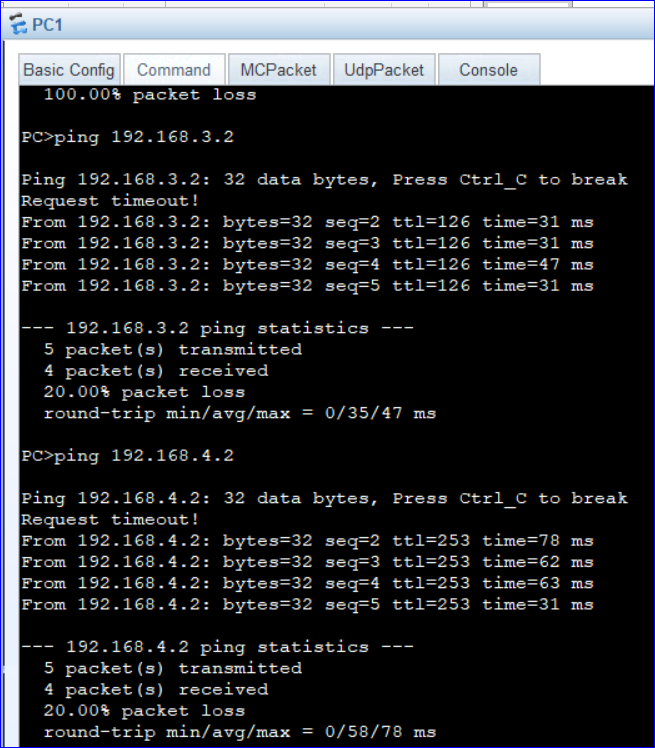


We can’f find 3.0 and 1.0, so we add path to them



Now we can ping from PC1 to all other interface and PCs

Lets try



So our network is all set.

We can confirm from routing table of each router as well.

**Remember that we can’t telnet from one PC to another PC in ensp.**

Now we want to apply filter on packets over each router. So we use Access control list.

Each router can decide whether to forward or deny packets.

**There are 2 Levels of ACL**

1. 2000-2999 basic level ACL
2. 3000-4999 basic Advanced ACL

**ACL is set of rules that are stored in configuration file. There are two actions**

1. Deny
2. Permit

**Further we can apply ACL on two types of traffic**

1. Inbound
2. Out bound

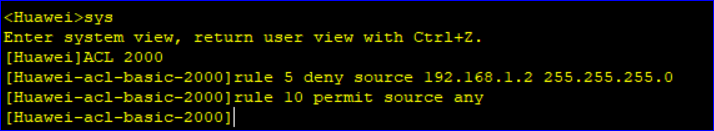
Traffic coming to interface G0/0/1 or 192.168.1.1 from PC1 and PC2 is inbound.

Traffic coming from outside of network is outbound.

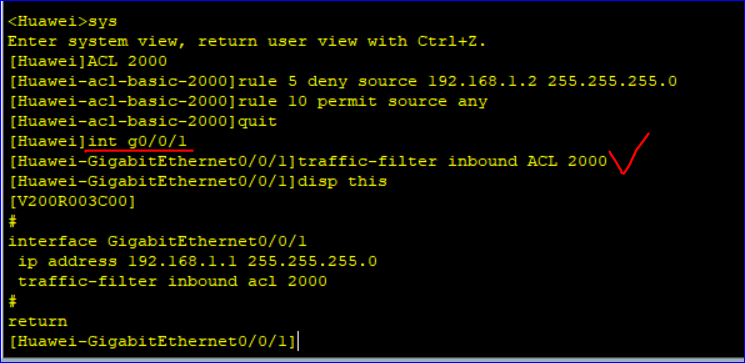
**Suppose Router1 want to deny traffic flow of PC1 to other networks, but permit flow from PC1 to PC2. Then what to do?**

* Create basic ACL
* Create rules
* Apply on interface

**On Router1**

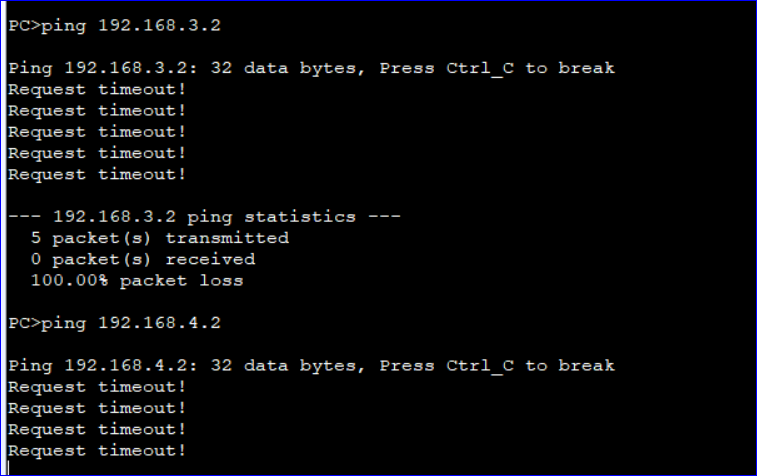


We have created ACL and two rules, now we want to apply them on interface 192.168.1.1 of router 1



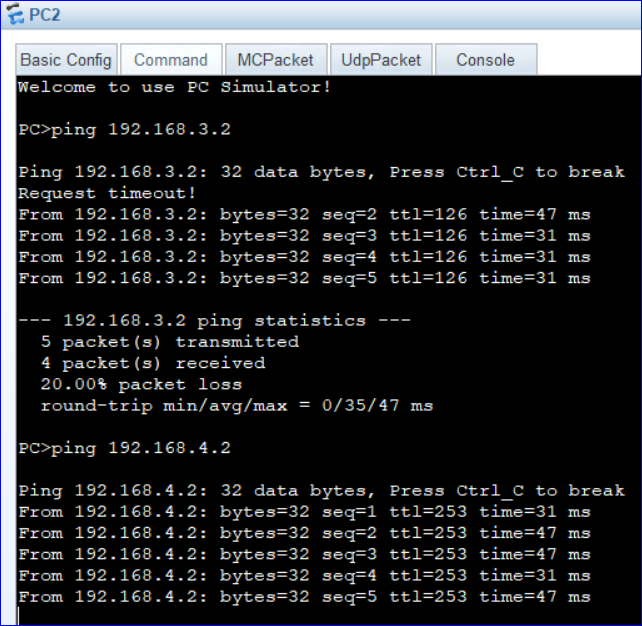
So it will not allow PC1 to transfer data

Now ping from PC1 to PC3 and PC1 to 192.168.4.2

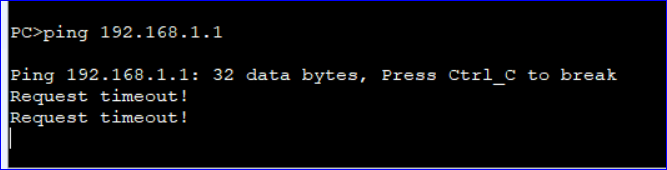


So we can’t send traffic out of network by PC1, but can send from PC2

From PC2 to PC3 and PC2 to 192.168.4.2



PC1 can’t even reach it’s gateway.

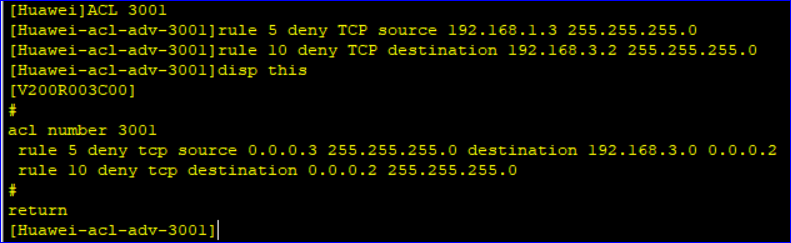


**ACL Task2:**

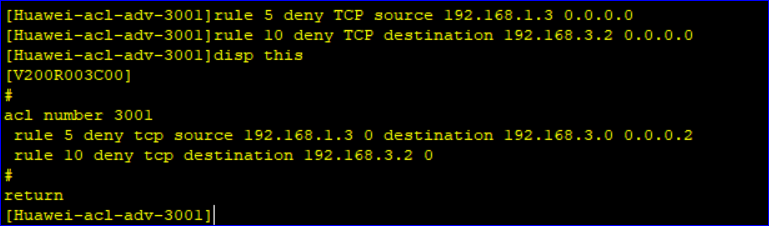
**Now suppose we want Router 3 to not allow TCP packets from PC2 i.e 192.168.1.3, and want to deny TCP traffic from PC3 to other networks**

* Create advanced level ACL
* Define rules
* Apply on interface

On Router2

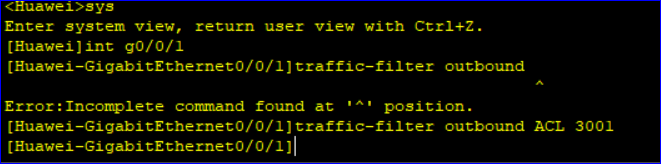


We can note that it has made source 0.0.0.3 in rule 5, while destination as 0.0.0.4 in rule 10 due to subnet mask. So we edit our rules and make as



So if we want to keep values fixed before the last digit, we put 0s.

Now we apply our created rules on interface of router2. We apply on g0/0/1 so that it will not allow outer traffic having source 192.168.1.3 toward destination 192.168.3.2 i.e interface 192.168.3.1 will block TCP packets from PC2 to PC3.



Now if we use TCP connection and send packets from PC2 to PC3 then we will be denied at interface 192.168.3.1. And communication will fail.

**The End**