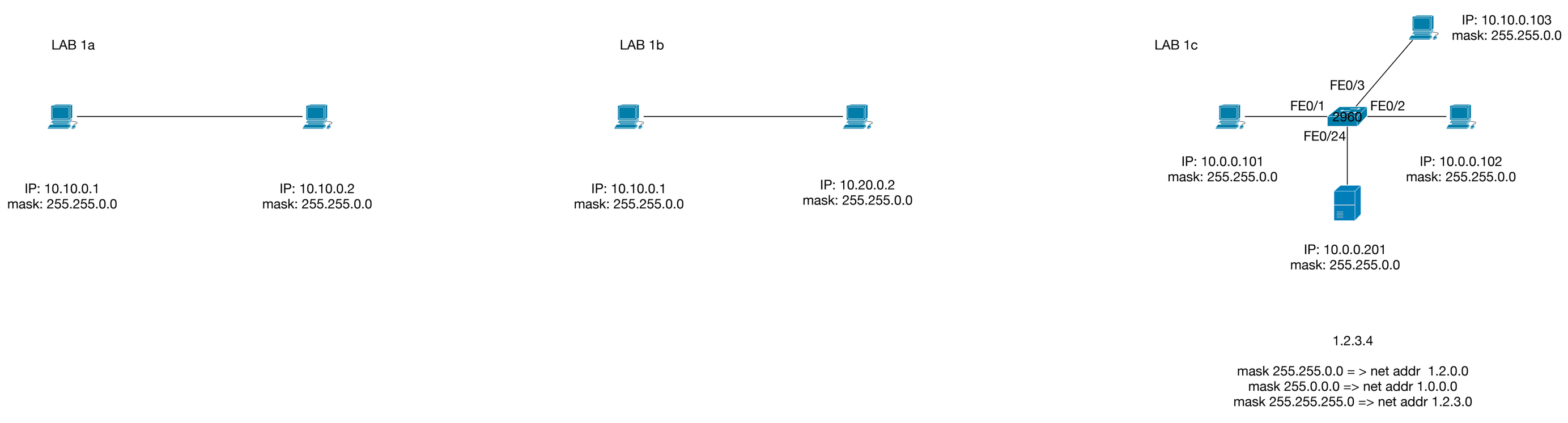
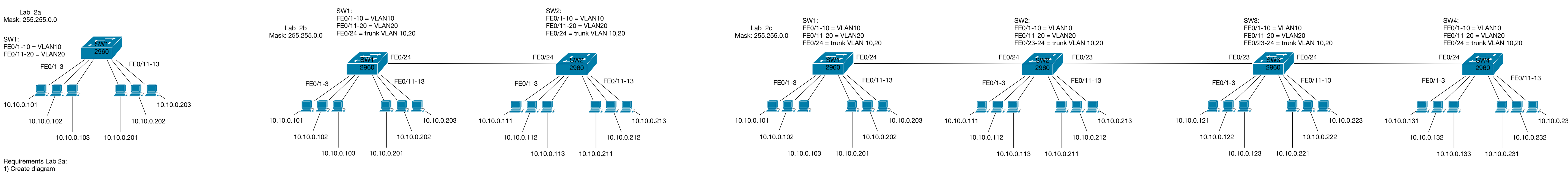
PLEASE USE SWITCHES type 2960 and ROUTERS type 1841, PacketTracer is buggy and we need to stick to these.



1.2.3.4

mask 255.0.0.0 => net addr 1.0.0.0
mask 255.0.0.0 => net addr 1.0.0.0
mask 255.255.255.0 => net addr 1.2.3.0

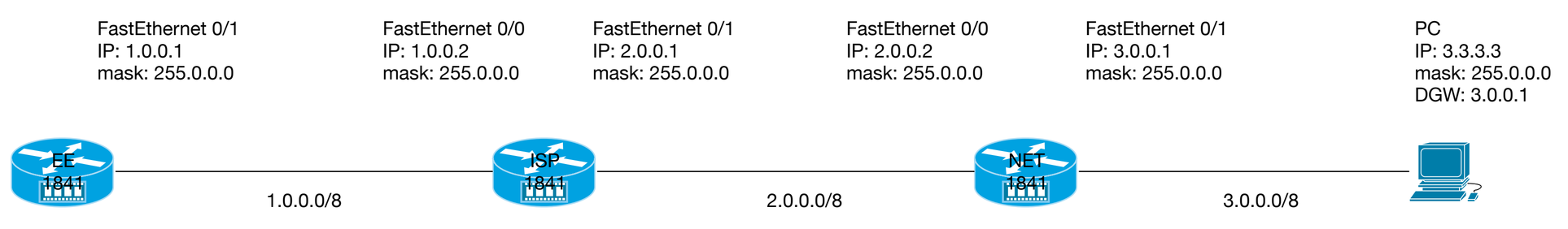
Lab 2: Switching

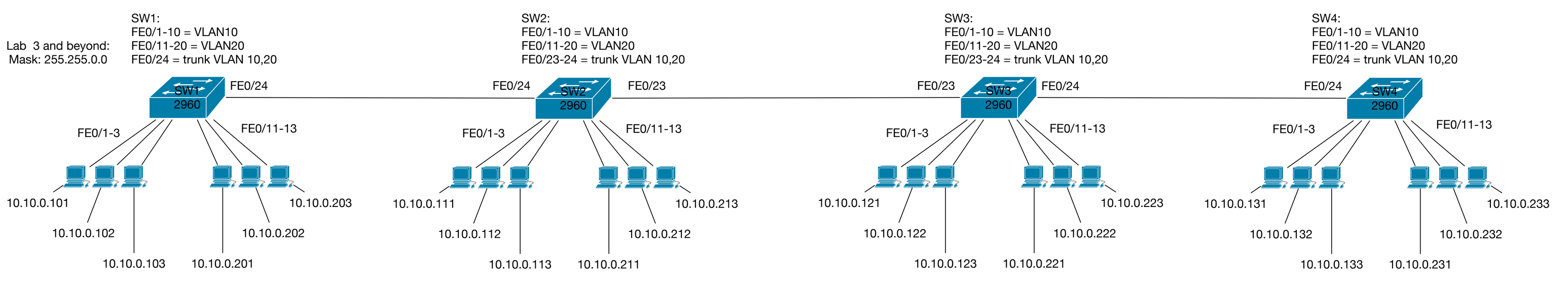


Requirements Lab 2a:
1) Create diagram
2) Rename the switch as SW1
3) Assign ports to the appropriate VLANs
4) Access switchports have to be STP portfast
5) Assign the proper IP addresses and masks to the PCs
6) Test connectivity. What you expect vs what happens.

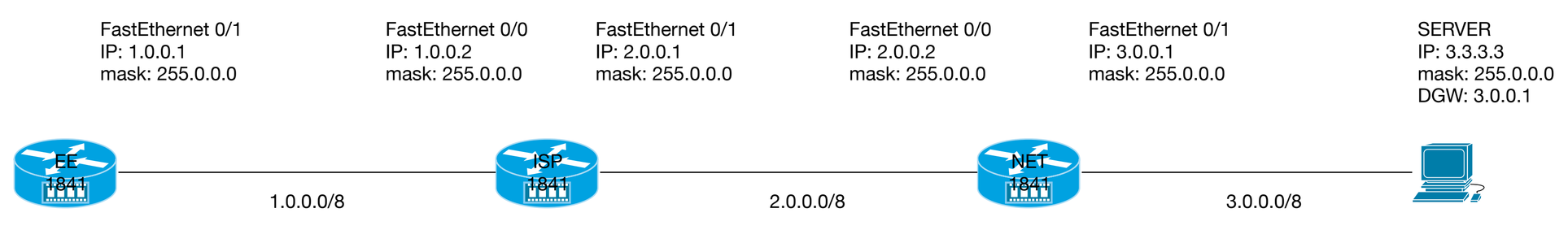
Requirements Lab 2b:
1) Create diagram
2) Rename the switches as SW1 and SW2
3) Assign ports to the appropriate VLANs on each switch
4) Access switchports have to be STP portfast
5) Assign a trunk port carrying VLANs 10 and 20 on FE0/24 on both switches
6) The trunk port must be portfast trunk on both sides
7) Assign the proper IP addresses and masks to the PCs
8) Test connectivity. What you expect vs what happens.

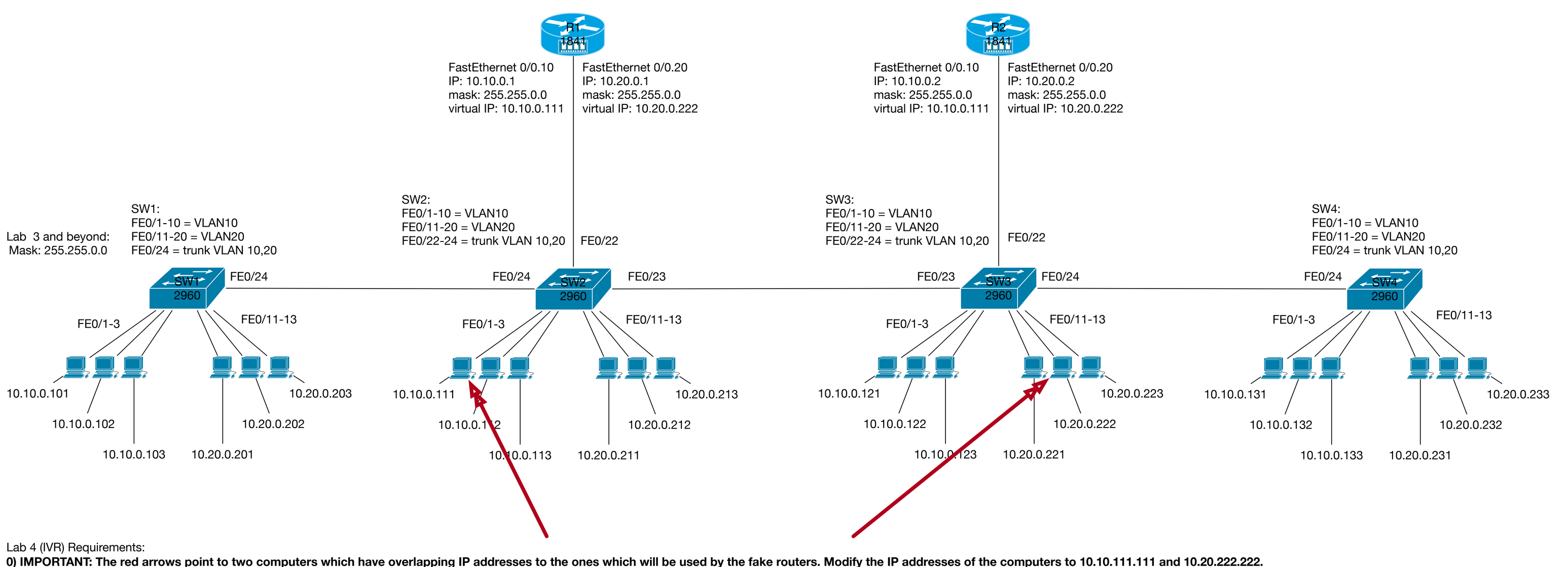
Requirements Lab 2c:
1) Create diagram
2) Rename the switches
3) Assign ports to the appropriate VLANs on each switch
4) Access switchports have to be STP portfast
5) Assign the proper switchport trunks on each switch
6) The trunk ports must be portfast trunk
7) Assign the proper IP addresses and masks to the PCs
8) Test connectivity. What you expect vs what happens.



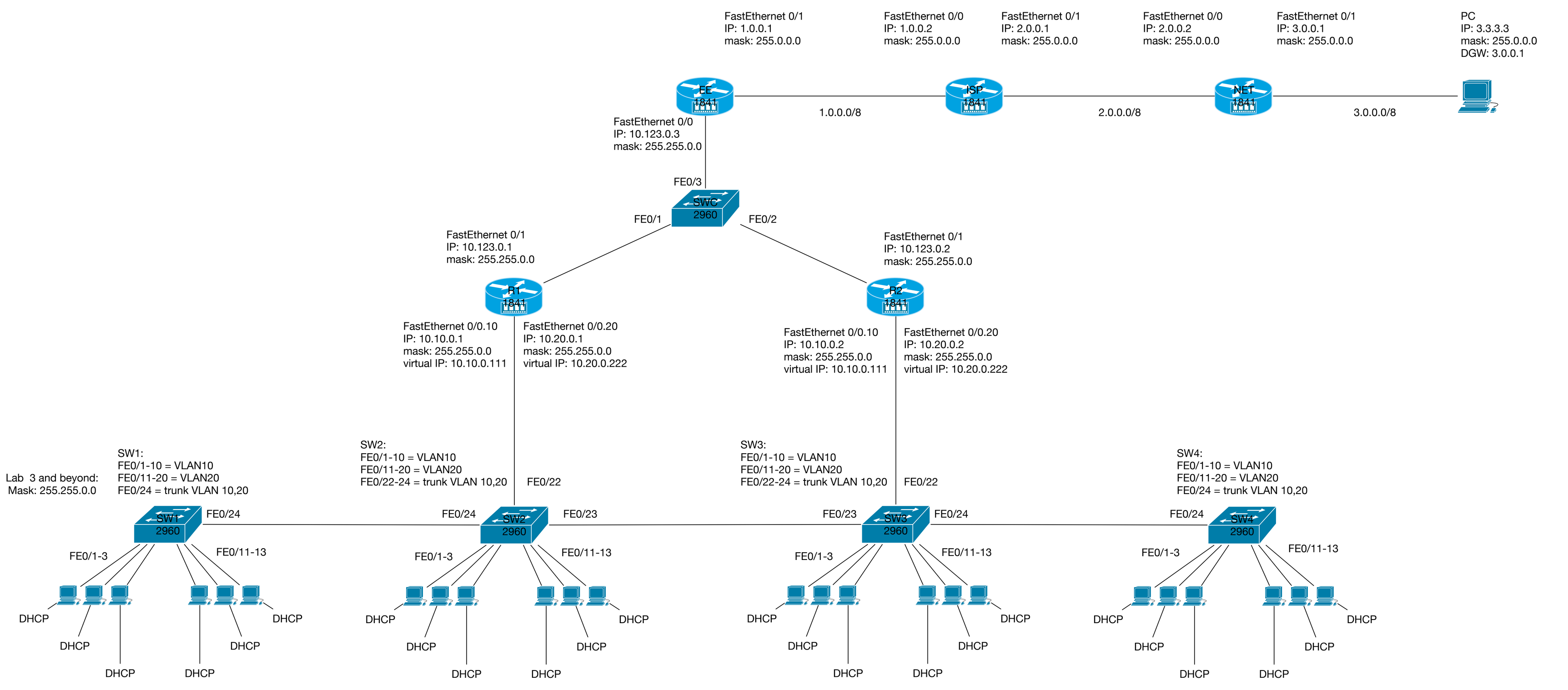


Lab 3 (routing) Requirements:
1) Note: mask /8 means 255.0.0.0 (8 bits of 1)
2) Add 3 routers 1841 and connect them accordingly to this diagram
3) Rename the routers as: EE (Enterprise Edge); ISP (Internet Service Provider) and NET (InterNET)
4) Assign the correct IP addresses and masks to the required interfaces and turn them on
5) Ping from router to router. You should get !. Try to explain the first . preceding the !.
6) Configure dynamic routing as asked by your instructor, on all the 3 routers, on all active interfaces:
Either EIGRP on Autonomous System 10 OR OSPF in Area 0
7) Test ping from EE to 2.0.0.2 and then 3.0.0.1
8) Add the PC, configure the appropriate IP, mask and default gateway.
9) Test from the PC ping to EE





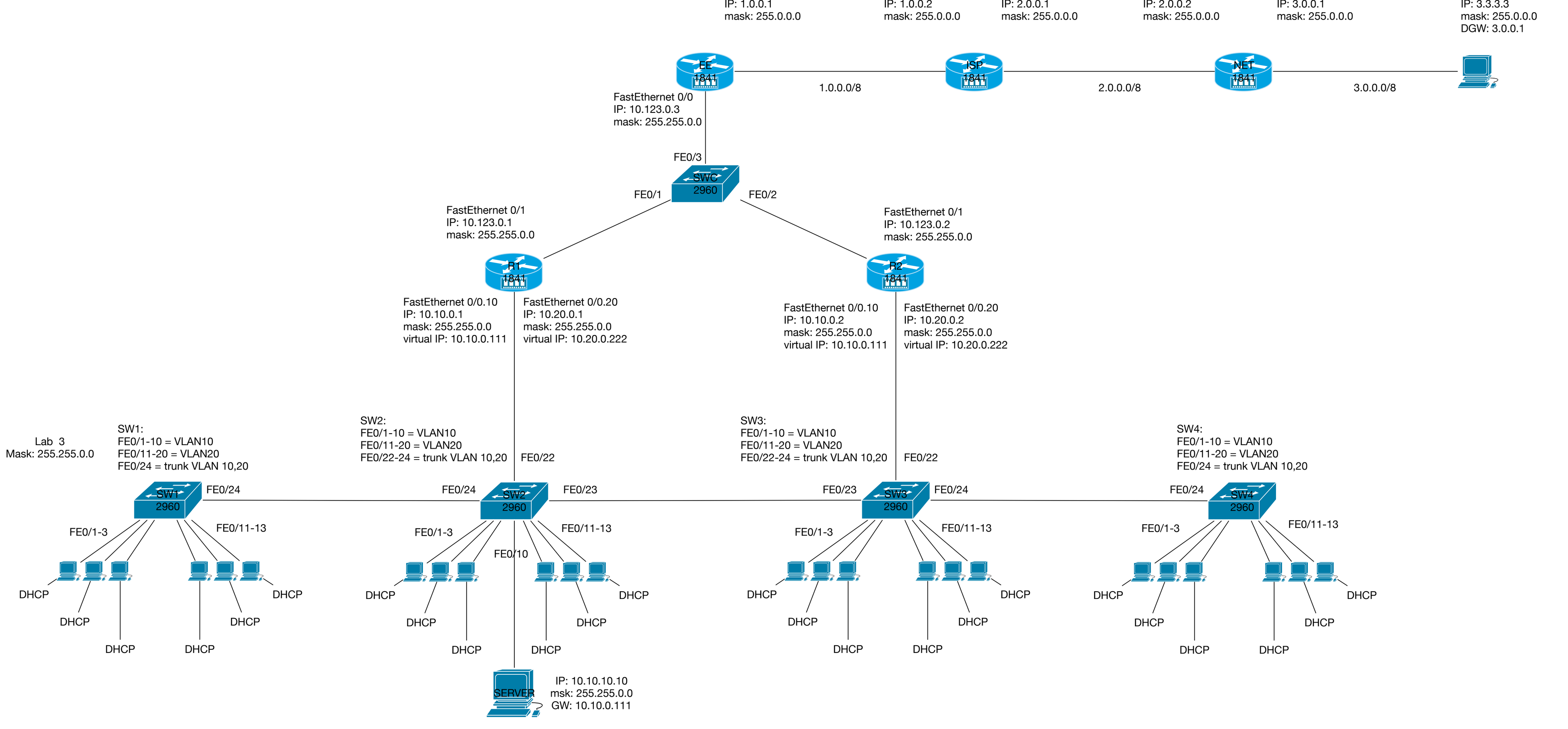
Lab 4 (IVR) Requirements:
0) IMPORTANT: The red arrows point to two computers which have overlapping IP addresses to the ones which will be used by the fake routers. Modify the IP addresses of the computers to 10.10.111.111 and 10.20.222.222.
It is only a temporary measure as, in the future, the IP addresses of the computers will be issued on a DHCP basis.
1) Add the 1841 routers R1 and R2 and connect them accordingly to the diagram.
2) On switches SW2 and SW3 the interfaces FE0/22 must be trunk in VLANs 10 and 20 and spanning-tree portfast trunk.
3) On routers R1 and R2 turn on the interfaces FastEthernet 0/0 and 0/1.
4) On router R1, create the subinterface FastEthernet 0/0.10. Activate encapsulation dot1q for VLAN 10 and assign the IP address 10.10.0.1 mask 255.255.0.0 to that SUBinterface.
5) Ping from router to one computer in VLAN 10. You should get ! (success).
6) On router R1, create the subinterface FastEthernet 0/0.20. Activate encapsulation dot1q for VLAN 20 and assign the IP address 10.20.0.1 mask 255.255.0.0 to that SUBinterface.
7) Ping from router to one computer in VLAN 20. You should get ! (success).
8) On router R2, create the subinterface FastEthernet 0/0.10. Activate encapsulation dot1q for VLAN 10 and assign the IP address 10.10.0.2 mask 255.255.0.0 to that SUBinterface.
9) Ping from router to one computer in VLAN 10. You should get ! (success).
10) On router R2, create the subinterface FastEthernet 0/0.20. Activate encapsulation dot1q for VLAN 20 and assign the IP address 10.20.0.2 mask 255.255.0.0 to that SUBinterface.
11) Ping from router to one computer in VLAN 20. You should get ! (success).
12) NOTE: We shall next activate first hop redundancy between routers R1 and R2. This is done in the following points.
13) On router R1, on the subinterface FastEthernet 0/0.10 create a standby group 1 with the virtual IP address 10.10.0.111.
14) On router R2, on the subinterface FastEthernet 0/0.10 create a standby group 1 with the virtual IP address 10.10.0.111.
15) NOTE: As you can see, now the routers R1 and R2 share the same virtual IP address. If one fails, the other one takes the traffic.
16) On router R1, on the subinterface FastEthernet 0/0.20 create a standby group 2 with the virtual IP address 10.20.0.222 mode on.
17) On router R2, on the subinterface FastEthernet 0/0.20 create a standby group 2 with the virtual IP address 10.20.0.222 mode on.
18) NOTE: As you can see, now the routers R1 and R2 share the same virtual IP address. If one fails, the other one takes the traffic.
19) On EACH SWITCH (SW1 to SW4) perform the following changes:
20) On the computers in VLAN 10 leave the IP addresses unchanged and put the default gateway as 10.10.0.111 - the virtual IP shared by multiple routers acting as default gateways.
21) On the computers in VLAN 20 change the IP addresses from 10.10.x.x to 10.20.x.x and put the default gateway as 10.20.0.222 - the virtual IP shared by multiple routers acting as default gateways.
22) NOTE: You achieved Inter VLAN routing using routing on a stick with redundant routers. Test by pinging between computers in different VLANs.



Lab 5 (DHCP and routing) Requirements:
1) Add a core switch 2960 and rename it SWC. Make all ports of the switch spanning tree portfast. Leave them in the VLAN 1.
2) Connect the routers R1, R2 and EE accordingly to the diagram.
3) Assign the proper addresses of routers R1, R2 and EE connecting to the SWC. Ping all 3 addresses between themselves. You should have success.
4) On router R1, create a default gateway to 10.123.0.3. The command is ip route 0.0.0.0 0.0.0.0 ….
5) On router R2, create a default gateway to 10.123.0.3. The command is ip route 0.0.0.0 0.0.0.0 ….
6) On router EE create gateways to the networks 10.10.0.0 mask 255.255.0.0 and 10.20.0.0 mask 255.255.0.0 via 10.123.0.1 and 10.123.0.2. You thus need to write 4 lines of code here.
ip route 10.10.0.0 255.255.0.0 10.123.0.1
ip route 10.10.0.0 255.255.0.0 10.123.0.2
ip route 10.20.0.0 255.255.0.0 10.123.0.1
ip route 10.20.0.0 255.255.0.0 10.123.0.2
7) Ping from any computer the address 10.123.0.3. You should have success.

8) NOTE: The IP addresses 10.x.x.x are called private (alongside 172.16.x.x and 192.168.0.x IP addresses). What does it mean? They are NOT routable in the internet.
Thus, from router EE (the Enterprise Edge) you can reach the internet (3.3.3.3) but not from the internal network. To solve this, we will activate NAT, but not today, in the future.

9) NOTE: We shall now activate DHCP for the computers. This will be done in the following points.
10) On both routers R1 and R2 define 2 DHCP pools POOL10 and POOL20 having:
-POOL10: network 10.10.0.0 mask 255.255.0.0 gateway 10.10.0.111
-POOL20: network 10.20.0.0 mask 255.255.0.0 gateway 10.20.0.222
11) On all the computers EXCEPT the server 10.10.10.10 set the IP address on automatic. The computers should receive IP addresses automatically.



Lab 6 (NAT) Requirements:
1) NOTE: On router EE we shall enable NAT. This is done in the following steps.
2) On router EE activate ip nat inside on the interface FastEthernet 0/0.
3) On router EE activate ip nat outside on the interface FastEthernet 0/1.
4) On router EE create an ip ACL extended called NAT-ACL permitting traffic from 10.0.0.0 wildcard 0.255.255.255 to go anywhere. This will match traffic from the private block corresponding to our network to be matched when going to the internet.
5) On router EE create a pool of public addresses called NAT-POOL containing only one public address: our inside global 1.0.0.1 mask 255.0.0.0.
6) Activate PAT: ip nat inside source list NAT-ACL pool NAT-POOL overload
7) NOTE: In this moment all computers should be able to go to the internet by pinging 3.3.3.3. or visiting the webpage at 3.3.3.3.
8) NOTE: we shall now filter traffic with an ACL.
9) On the switch SW2 add a server on the interface FE 0/10. The IP address of the server will be 10.10.10.10 with a 255.255.0.0 mask and with 10.10.0.111 as default gateway. We shall make this server accessible from the internet and isolated from VLAN 20.
==!!!==DO NOT IMPLEMENT POINT 10, BUG IN PACKETTRACER, NAT WILL STOP WORING==!!!==
10) On router EE let us permit access from the internet to the server.
ip nat inside source static tcp 10.10.10.10 80 1.0.0.1 80
ip nat inside source static tcp 10.10.10.10 443 1.0.0.1 443
11) NOTE: On the server 3.3.3.3 open a web browser and test if you can see a webpage on the address 1.0.0.1 on protocols http and https. It should be fine.
==!!!==CONTINUE IMPLEMENTING WITH 12==!!!==
12) NOTE: In order to isolate VLAN 10 from VLAN 20 but permit the server access we need to create an ACL. On which device? On the devices responsible for routing between the VLANs 20 and 10, thus R1 and R2.
13) On router R1 create an ip extended ACL called SERVER in which you permit access from network 10.20.0.0 WC 0.0.255.255 to the host 10.10.10.10 ; you then deny access from network 10.20.0.0 WC 0.0.255.255 to network 10.10.0.0 WC 0.0.255.255 and then you permit anything. Why do you to permit anything (permit ip any any)? Because of access to the Internet.
14) Apply on router R1 the access list (with the IP access group) on the IN direction of the interface FastEthernet 0/0.20.
15) Do the points 13 and 14 on router R2, in the same way.
16) NOTE: Test ping between any computer of VLAN 10 or VLAN 20 and the server 10.10.10.10. This should be successful.
17) NOTE: Test ping from the server 10.10.10.10 to 3.3.3.3 it should be success.
18) NOTE: Test ping between any computer of VLAN 20 and any other computer of VLAN 10 (except the server). This should NOT be successful. Congrats, you have just built a basic firewall.

Lab 7 (remote management) Requirements:
1) On SW1 assign the interface 10.10.10.1 for VLAN10.
2) On SW2 assign the interface 10.10.10.2 for VLAN10.
3) On SW3 assign the interface 10.10.10.3 for VLAN10.
4) On SW4 assign the interface 10.10.10.4 for VLAN10.
5) On SWC assign the interface 10.123.0.4 for VLAN1.
6) O ALL SWITCHES and on routers R1, R2 and EE execute 7-10:
7) define a username “moucha” with privilege level 15 and secret “cisco”
8) define an ip domain-name moucha.org
9) create a crypto key size 2048
10) on lines vty 0 15 activate the transport as ssh and login local
11) From the server 10.10.10.10 a network administrator should be able to remotely connect to any enterprise networking device.

END OF LABS