Laboratory commands 2:

# Virtual LAN

Can use **show vlan brief** to view configurations.

Can use **show running-config** to show all other things.

**VLAN: configuration:**

* **Switch (config)#** vlan x
* **Switch (config-vlan)#** name <**NAME**>(optional) => DO ONLY IF ASKED AT EXAM
* **Switch (config-vlan)#** exit

**Example:**

* **Switch (config)#** vlan 10
* **Switch (config-vlan)#** name student
* **Switch (config-vlan)#** exit

**Access port:** connected to hosts belonging to a single VLAN.

* **Switch (config)#** interface FastEthernet 1/0
* **Switch (config-if)#** switchport mode access
* **Switch (config-if)#** switchport access vlan <**ID**>

**Trunk port:** receiving and forwarding frames belonging to different VLANs.

* **Switch (config)#** interface FastEthernet o/x
* **Switch (config-if)#** switchport mode trunk

* **Switch (config-if)#** switchport trunk native vlan <ID> => This command is optional and permits the vlan <ID> messages to not be tagged and reduce overhead. => **NO FOR ROUTER LINKS**

To configure the trunk port so that only a subset of VLANs is allowed:

* **Switch (config-if)# switchport trunk allowed vlan y**

**Example:**

* **Switch (config)#** interface FastEthernet 0/13
* **Switch (config-if)#** switchport mode trunk
* **Switch (config-if)#** switchport trunk native vlan 99
* **Switch (config-if)#** switchport trunk allowed 10-20

FOR EXAM: **Management VLAN** where ip of switches are taken, VLAN 99 must be used to take ip of switches. VLAN 99 (Management) → IP of switches.

**Example:**

* **Switch (config)#** interface vlan 99
* **Switch(config-if)#** ip address <**A.B.C.D.**>

FOR EXAM: when is asked that all **switches must be accessible** from PCs of management VLAN must do these command in all switches:

Define ip address of switch from vlan 99, like this only PCs of management VLAN can access to it:

* **Switch (config)#** vlan 99
* **Switch(config-vlan)#** exit
* **Switch (config)#** interface vlan 99
* **Switch(config-if)#** ip address <**A.B.C.D.**>

Permit to PCs of management VLAN to access to switches with telnet:

* **Switch (config)#** line vty 0 15
* **Switch(config-line)#** password <**NAME**>
* **Switch(config-line)#** login
* **Switch(config-line)#** exit

If text ask that switches must be also **configurable** and accessible:

* **Switch (config)#** enable password <**NAME**>

# Inter-VLAN Routing

Now we configure connection between router and switch.

**IMPORTANT**: always set default-router in each host for permit inter-VLAN

**Traditional inter-VLAN:**

* The number of router-to-switch physical links is equal to the number of VLANs able to communicate with each other.
* Each router interface is associated with a VLAN; an IP address of the VLAN block must be assigned to it.
* The switch ports connected to the router must be **configured in access mode**.

**Example:** only VLAN 10 and VLAN 30 are allowed to communicate with each other.

*Router: interfaces configuration*

* R1(config)# interface Fa 0/0
* R1(config-if)#ip address 172.17.10.1 255.255.255.0 → IP of vlan 10
* R1(config-if)# no shutdown → **IMPORTANT**
* R1(config)# interface Fa 0/1
* R1(config-if)#ip address 172.17.30.1 255.255.255.0 → IP of vlan 30
* R1(config-if)# no shutdown

*Switch: configuration of the ports* → **ACCESS MODE**

* S1(config)# interface Fa 0/6
* S1(config-if)# switchport access vlan 10
* S1(config)# interface Fa 0/5
* S1(config-if)# switchport access vlan 30

**“Router-on-a-stick” inter-VLAN:**

* The router is connected to a switch by means of a single physical interface.
* The physical interface of the router is split into virtual interfaces (subinterfaces): the number of virtual interfaces is equal to the number of VLANs able to communicate with each other.
* Each virtual interface (subinterface) of the router is associated to a single VLAN (it must have an IP address of the VLAN block).
* The switch port connected to the router must be **configured in trunk mode**.

**Example:** only VLAN 10 and VLAN 30 are allowed to communicate with each other.

*Router: the interface connected to the switch must be split in two subinterfaces, one belonging to VLAN 10 and one to VLAN 30*

* R1(config)# interface Fa 0/1.10 → subinterface for vlan 10
* R1(config-subif)# encapsulation dot1q 10
* R1(config-subif)#ip address 172.17.10.1 255.255.255.0 → IP address of vlan 10
* R1(config)# interface Fa 0/1.30 → subinterface for vlan 30
* R1(config-subif)# encapsulation dot1q 30
* R1(config-subif)# ip address 172.17.30.1 255.255.255.0 → IP address of vlan 30
* R1(config)# interface Fa 0/1 → real interface
* R1(config-if)# no shutdown

*Switch: the port connected to the router is configured in* ***TRUNK MODE***

* S1(config)# interface Fa 0/5
* S1(config-if)# switchport mode trunk

# Access Control List

To check can use **show ip interface,** **show access-list**, **show running-config**

**Important:**

* The packets direction on an interface:

**Inbound**: incoming packets. → in

**Outbound**: outgoing packets. → out

* When associating an ACL to an interface, the direction must be specified.
* An ACL can be associated also to a sub-interface. If the sub-interfaces are defined on an interface, the ACL must be associated to subinterfaces, not to the original interface.
* Order of rules is fundamental, when we add a rule the default rule becomes DROP, always add another rule to permit all.

**Wildcard:**

* The wildcard mask is a 32 bits string
* A wildcard define the matching of an ACL rule regarding IP addresses
  + 0 the corresponding value of the IP address must be checked
  + 1 the corresponding value of the IP address doesn’t have to be checked
* Example
  + 172.16.0.0 ⇔ 0.0.255.255:
  + 172.16.2.3 matching
  + 172.15.0.1 no matching
* Two keywords to be used; **any** and **host:**
  + **any:** means 255.255.255.255 for the wildcard mask: Always a matching, independently of the IP address.
  + **host:** means 0.0.0.0 for the wildcard mask: All the bits of the IP address must be checked.

**Standard ACL:**

* filters on the basis of the source IP address.
* access-list number must be in the range [1, 99].
* Create list of rules, and after associate to an interface in or out channel::
* **Router(config)#** access-list <**NUMBER**> {deny | permit} source [source-wildcard ]
* **Router(config)#** access-list <**NUMBER**> {deny | permit} any → to deny|permit all source traffic
* **Router(config)#** interface <**NAME**>
* **Router(config-if)#** ip access-group <**NUMBER**> {in | out}
* **Router(config)#** no access-list <**NUMBER**> → TO DELETE

**Extended ACL:**

* Extended ACLs allow filtering traffic considering IP source and destination addresses, the protocol and the destination port number.

.

* access-list number must be in the range [101, 199].
* Create list of rules, and after associate to an interface in or out channel::
* **Router(config)#** access-list <**NUMBER**> {deny | permit} protocol source [source-wildcard] destination [destination -wildcard] eq port
* **Router(config)#** access-list 1 {deny | permit} ip any any → to deny|permit all type of traffic

**protocol**: tcp, udp and icmp -> use always eq

**port:** www (must use tcp and is equal to http), ping is in icmp, dns uses udp, ecc.

Applying the extended list:

* **Router(config)#** interface <**NAME**>
* **Router(config-if)#** ip access-group <**NUMBER**> {in | out}

**Named ACL:**

* named ACLs are identified by a name.
* named ACL can be standard or extended
* possible to remove a single statement and to add a new one in any position.
* create a named ACL is < **ip access-list** >
* each rule added has a number 10, 20, 30, …

To set a Named ACL:

* **Router(config)#** ip access-list { extended I standard } <**NAME**>
* **Router(config-ext-nacl)#** { permit l deny } protocol source source-wildcard destination destination-wildcard **eq** port [established?]

To add/change a rule in a Named ACL:

* **Router(config)#** ip access-list extended example
* **Router(config-ext-nacl)#** no 20 → To delete rule number 20 (second rule added)
* **Router(config-ext-nacl)#** 20 permit ip host 192.168.1.77 any → Add rule in position number 20.
* **Router(config-ext-nacl)#** 25 ip host 192.168.1.88 any → Add rule in position number 25.

Important is rule order 25 will be checked after rule 20!

**Limiting the telnet access:**

Must create a **STANDARD ACL** in the router:

* **Router(config)#** access-list 2 permit 172.16.1.0 0.0.0.255
* **Router(config)#** access-list 2 permit 172.16.2.0 0.0.0.255
* **Router(config)#** access-list 2 deny any

Applying the access list:

* **Router(config)#** line vty 0 4
* **Router(config-...)#** access-class 2 in

Example**:**

* **Router(config)#** ip access-list extended server-access
* **Router(config-ext-nacl)#** permit TCP any host 131.108.101.99 eq smtp
* **Router(config-ext-nacl)#** permit UDP any host 131.108.101.99 eq domain
* **Router(config-ext-nacl)#** deny ip any any log

Applying the named list:

* **Router(config)#** interface fastethernet 0/0
* **Router(config-if)#**  ip access-group server-access out
* **Router(config-if)#** exit

IMPORTANT**:**

* The **standard ACLs should be put as close as possible to the destination** (since it is not possible to specify the destination).
* The **extended ACLs should be put as close as possible to the source** (to filter earlier the traffic, and so reducing routers work).
* Sometimes we can n**ot follow these rules for example because of NAT or other configurations.** For example if the destination is a host that is private we can’t use a rule in the router near to the source host, we must set a rule in the router near the private host that knows that ip address.
* We can set **maximum one rule for in/out for each interface**, this means that for an interface Fa0/0 we can set an ACL for in and one for out, we must carefully read the text before building an ACL.

# LAN Security

Now we configure security on switches.

For show configuration of Port security use **show port-security interface** <**NAME**> , **show port-security address**

**Port security: MUST BE DONE ONLY ON ACCESS SWITCHPORT**

* This command must always be done for enable port security:
* **Switch(config-if)#** switchport port-security

*Static configuration:*

* **Switch(config-if)#** switchport port-security mac-address <**MAC-ADDRESS**>
* To see MAC-ADDRESS of an host from **Command Prompt** of the host use: **ipconfig /all**

*Dynamic configuration:* specify number of allowed MAC addresses

* **Switch#** configure terminal
* **Switch(config)#** interface fastEthernet 0/18
* **Switch(config-if)#** switchport mode access → *must be access the interface*
* **Switch(config-if)#** switchport port-security
* **Switch(config-if)#** switchport port-security **maximum 50**

For *Sticky Dynamic configuration:*

Like this saved MAC are visible in **show running-config**

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

**Violation management:**

* Once a violation occurs on a port, the port will transition to an error disabled state. Can see red triangles on the link.
* To recover from an error disabled state, a **shutdown** command and then a **no shutdown** on the interface (manual intervention by an administrator) must be executed. For example if we have a violation on Fa0/2 must do:
  + **Switch(config)#** interface Fa0/2
  + **Switch(config-if)#** shutdown
  + **Switch(config-if)#** — messages —
  + **Switch(config-if)#** no shutdown
* Error disabled ports can be configured to automatically recover from port security violations:
* **Switch(config-if)#** errdisable recovery interval <**Time\_Interval**>
* The **Time\_Interval** is an integer value in the range [30-86400] seconds

**DHCP-Snooping:**

* With DHCP snooping enabled on an interface, the switch will deny packets containing:
  + Unauthorized DHCP server messages coming from an untrusted port.
* DHCP snooping recognizes two types of ports:
  + **Trusted DHCP ports** - Only ports connecting to upstream DHCP servers should be trusted.
  + **Untrusted ports** - These ports connect to hosts that should not be providing DHCP server messages.
* Command to use are:
* **Switch(config)#**  ip dhcp snooping
* **Switch(config)#** ip dhcp snooping vlan <**vlan-id**> #if no one use always 1
* **Switch(config)#** no ip dhcp snooping information option
* **Switch(config)#** interface <**NEAR:DHCP:SERVER/ROUTER:TO:TRUST**> and also on interfaces that are linked to the switch connected to the server.
* **Switch(config-if)#** ip dhcp snooping trust

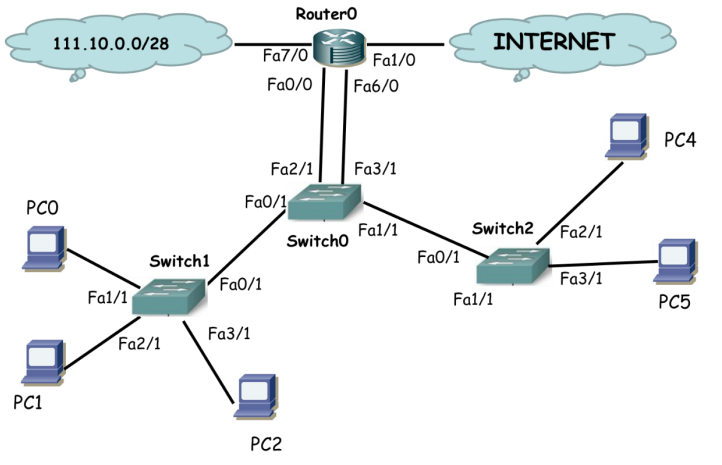
**Configuring GRE:**

* Create a tunnel interface:
  + **Router(config)#** interface Tunnel <**ID**> #typically can use 0
* Configure GRE as the tunnel interface mode:
  + **Router(config-if)#** tunnel mode gre ip
* Assign an IP address to the tunnel interface (Better an available private address and /30)
* Specify the tunnel source physical interface:
  + **Router(config-if)#** tunnel source <ID>
* Specify the tunnel destination IP address (IP address of the physical interface of the tunnel end point):
  + **Router(config-if)#** tunnel destination <A.B.C.D.>

**Example of tunnel configuration:**

* **Router(config)#**interface Tunnel 0
* **Router(config-if)#** tunnel mode gre ip
* **Router(config-if)#** ip address 192.168.2.1 255.255.255.252
* **Router(config-if)#** tunnel source S0/0/0 (physical connected to internet)
* **Router(config-if)#** tunnel destination 198.133.219.87 (ip of physical destination)
* **Router(config)#** ip route 10.0.0.0 255.0.0.0 192.168.2.2 (ip of tunnel destination)
* To check all work send a ping to a private host in 10.0.0.0

# EXAM 1



**1)** IP addresses of PC considering the following table:

* PC0, PC4 → vlan 10 → 11.0.0.0/16
* PC1, PC5 → vlan 30 → 30.0.0.0/18
* PC2 → vlan 99 → 99.0.0.0/26

**2)** VLANs on switches.

**3)** VLAN 99 as Management VLAN. All Switches must be accessible from PCs of management

VLAN.

**4)** VLAN 10 as Native VLAN for all network trunks.

**5)** Traditional inter-VLAN routing among hosts of VLAN 10 and VLAN 30.

**6)** Sticky dynamic port security on interfaces of switch Switch2, fixing the maximum number of

allowed MAC addresses to 2.

**7)** ACLs so that only these traffic flows are blocked:

* HTTP traffic from Internet to VLAN 10 hosts;
* ICMP traffic from hosts of network 111.10.0.0/28 to PC0;
* UDP traffic from PC5 to PC4.

**Answers:**

**1)** In each host set an ip address from the block given.

**2)** Only switch2, for other Switches is the same:

Configure VLANs:

* **Switch2(config)#** vlan 10
* **Switch2(config-vlan)#** exit
* **Switch2(config)#** vlan 30
* **Switch2(config-vlan)#** exit
* **Switch2(config)#** vlan 90
* **Switch2(config-vlan)#** exit

Configure each interface:

* **Switch2(config)#** interface Fa2/1
* **Switch2(config-if)#** switchport mode access
* **Switch2(config-if)#** switchport access vlan 10
* **Switch2(config-if)#** exit
* **Switch2(config)#** interface Fa3/1
* **Switch2(config-if)#** switchport mode access
* **Switch2(config-if)#** switchport access vlan 30
* **Switch2(config-if)#** exit
* **Switch2(config)#** interface Fa0/1
* **Switch2(config-if)#** switchport mode trunk
* **Switch2(config-if)#** switchport trunk native vlan 10 → **4)**
* **Switch2(config-if)#** exit

**3)** Only switch2, for other Switches is the same:

Set ip address from management vlan:

* **Switch2(config)#** interface vlan 99
* **Switch2(config-if)#** ip address 99.0.0.10

configure telnet:

* **Switch2(config)#** line vty 0 15
* **Switch2(config-line)#** password exam1
* **Switch2(config-line)#** login
* **Switch2(config-line)#** exit

**5)** Commands for Switch0:

* **Switch0(config)#** interface Fa2/1
* **Switch0(config-if)#** switchport mode access
* **Switch0(config-if)#** switchport access vlan 10
* **Switch0(config)#** interface Fa3/1
* **Switch0(config-if)#** switchport mode access
* **Switch0(config-if)#** switchport access vlan 30

Commands for Router0:

* **Router0(config)#** interface Fa0/0
* **Router0(config-if)#** ip address 11.0.0.10
* **Router0(config-if)#** no shutdown
* **Router0(config)#** interface Fa6/0
* **Router0(config-if)#** ip address 30.0.0.10
* **Router0(config-if)#** no shutdown

Must set for all PCs of vlan 10 the default-router as 11.0.0.10, while for all PCs of vlan 30 the default-router as 30.0.0.10.

**6)** Commands for Switch2 only on access ports:

* **Switch0(config)#** interface Fa2/1
* **Switch0(config-if)#** switchport port-security
* **Switch0(config-if)#** switchport port-security maximum 2
* **Switch0(config-if)#** switchport port-security mac-address sticky
* **Switch0(config)#** interface Fa3/1
* **Switch0(config-if)#** switchport port-security
* **Switch0(config-if)#** switchport port-security maximum 2
* **Switch0(config-if)#** switchport port-security mac-address sticky

**7)** Commands for Router0 using named access-list:

HTTP traffic from Internet to VLAN 10 hosts:

* **Router(config)#** ip access-list extended first
* **Router(config-ext-nacl)#** deny tcp any 11.0.0.0 0.0.255.255 eq www
* **Router(config-ext-nacl)#** permit ip any any
* **Router(config-ext-nacl)#** exit
* **Router(config)#** interface Fa1/0
* **Router(config-if)#**  ip access-group first in
* **Router(config-if)#** exit

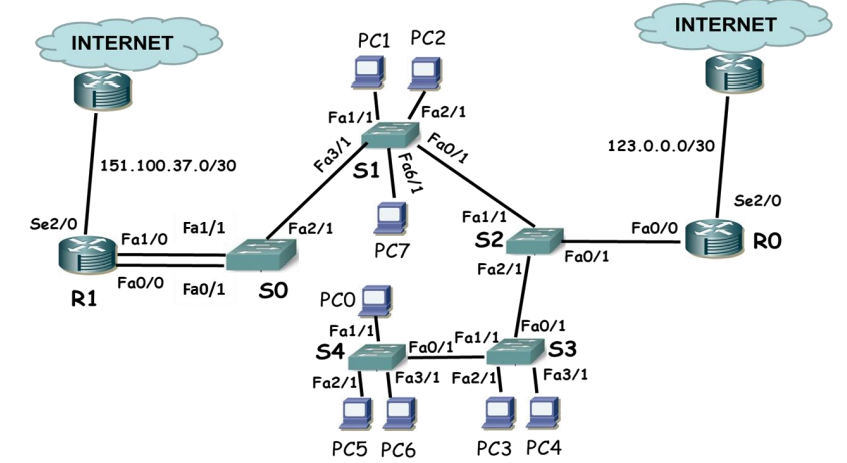
ICMP traffic from hosts of network 111.10.0.0/28 to PC0:

* **Router(config)#** ip access-list extended second
* **Router(config-ext-nacl)#** deny icmp any host 11.0.0.1
* **Router(config-ext-nacl)#** permit ip any any
* **Router(config-ext-nacl)#** exit
* **Router(config)#** interface Fa7/0
* **Router(config-if)#**  ip access-group second in
* **Router(config-if)#** exit

UDP traffic from PC5 to PC4:

* **Router(config)#** ip access-list extended third
* **Router(config-ext-nacl)#** deny udp host 30.0.0.2 host 11.0.0.2
* **Router(config-ext-nacl)#** permit ip any any
* **Router(config-ext-nacl)#** exit
* **Router(config)#** interface Fa6/0
* **Router(config-if)#**  ip access-group third in
* **Router(config-if)#** exit

# EXAM 2



**1)** The student has to configure the network reported in the figure, following the requirements

reported below. If a password must be configured, you can use the following one: netlab. PCs must belong to the following VLANs:

* Hosts → VLAN → Indirizzo VLAN
* PC0, PC1 → 10 → 11.0.10.0/24
* PC2, PC5 → 20 → 11.0.20.0/24
* PC3, PC4 → 99 → 11.0.99.0/24
* PC6, PC7 → 80 → 11.0.80.0/24

**2)** Switches must have interfaces properly configured.

**3)** VLAN 99 is the Management VLAN for switches and the Native VLAN for trunks; switches must

be accessible and configurable via telnet.

**4)** Hosts of VLAN 10 and hosts of VLAN 20 must communicate by means of router R0; hosts of

VLAN 80 and hosts of VLAN 99 must communicate by means of router R1.

**5)** Configure sticky dynamic port security for VLAN 99.

**6)** Router R1 must be accessible only by hosts of VLAN 99 and VLAN 80.

**7)** The following traffic flows must be blocked (minimizing routers processing):

* UDP traffic from PC0 to PC5;
* ICMP traffic from Internet to all VLANs;
* http traffic from VLAN 10 to VLAN 80;
* all bidirectional traffic among VLAN 99 and Internet.

**Answers:**

**1)** In each host set an ip address from the block given, leave the first ip for the router.

**2)** Only switch2, for other Switches is the same:

Configure VLANs:

* **Switch3(config)#** vlan 10
* **Switch3(config-vlan)#** exit
* **Switch3(config)#** vlan 20
* **Switch3(config-vlan)#** exit
* **Switch3(config)#** vlan 99
* **Switch3(config-vlan)#** exit
* **Switch3(config)#** vlan 80
* **Switch3(config-vlan)#** exit

Configure each interface:

* **Switch3(config)#** interface Fa0/1
* **Switch3(config-if)#** switchport mode trunk
* **Switch3(config-if)#** switchport trunk native vlan 99 → **3)**
* **Switch3(config-if)#** exit
* **Switch3(config)#** interface Fa1/1
* **Switch3(config-if)#** switchport mode trunk
* **Switch3(config-if)#** switchport trunk native vlan 99 → **3)**
* **Switch3(config-if)#** exit
* **Switch3(config)#** interface Fa2/1
* **Switch3(config-if)#** switchport mode access
* **Switch3(config-if)#** switchport access vlan 99
* **Switch3(config-if)#** exit
* **Switch3(config)#** interface Fa3/1
* **Switch3(config-if)#** switchport mode access
* **Switch3(config-if)#** switchport access vlan 99
* **Switch3(config-if)#** exit

**3)** Only switch2, for other Switches is the same:

Set ip address from management vlan:

* **Switch2(config)#** interface vlan 99
* **Switch2(config-if)#** ip address 11.0.99.5

configure telnet:

* **Switch2(config)#** line vty 0 15
* **Switch2(config-line)#** password netlab
* **Switch2(config-line)#** login
* **Switch2(config-line)#** exit
* **Switch2(config)#** enable password netlab

**4)** Commands for Switch0:

* **Switch0(config)#** interface Fa2/1
* **Switch0(config-if)#** switchport mode trunk
* **Switch0(config-if)#** switchport trunk native vlan 99 → **3)**
* **Switch0(config-if)#** exit
* **Switch0(config)#** interface Fa1/1
* **Switch0(config-if)#** switchport mode access
* **Switch0(config-if)#** switchport access vlan 99
* **Switch0(config-if)#** exit
* **Switch0(config)#** interface Fa0/1
* **Switch0(config-if)#** switchport mode access
* **Switch0(config-if)#** switchport access vlan 80
* **Switch0(config-if)#** exit

Commands for Router1:

* **Router1(config)#** interface Fa1/0
* **Router1(config-if)#** ip address 11.0.99.1 255.255.255.0
* **Router1(config-if)#** no shutdown
* **Router1(config-if)#** exit
* **Router1(config)#** interface Fa0/0
* **Router1(config-if)#** ip address 11.0.80.1 255.255.255.0
* **Router1(config-if)#** no shutdown
* **Router1(config-if)#** exit

Commands for Switch2:

* **Switch2(config)#** interface Fa2/1
* **Switch2(config-if)#** switchport mode trunk
* **Switch2(config-if)#** switchport trunk native vlan 99 → **3)**
* **Switch2(config-if)#** exit
* **Switch2(config)#** interface Fa1/1
* **Switch2(config-if)#** switchport mode trunk
* **Switch2(config-if)#** switchport trunk native vlan 99 → **3)**
* **Switch2(config-if)#** exit
* **Switch2(config)#** interface Fa0/1
* **Switch2(config-if)#** switchport mode trunk => “Router on stick”, NO NATIVE TRUNK ON LINK TO ROUTER
* **Switch2(config-if)#** exit

Commands for Router0:

* **Router0(config)#** interface Fa0/0.10
* **Router0(config-if)#** encapsulation dot1Q 10
* **Router0(config-if)#** ip address 11.0.10.1 255.255.255.0
* **Router0(config-if)#** exit
* **Router0(config)#** interface Fa0/0.20
* **Router0(config-if)#** encapsulation dot1Q 20
* **Router0(config-if)#** ip address 11.0.20.1 255.255.255.0
* **Router0(config-if)#** exit
* **Router0(config)#** interface Fa0/0
* **Router0(config-if)#** no shutdown
* **Router0(config-if)#** exit

Must set for all PCs of vlan N the default-router as 11.0.N.1.

**5)** Commands for Switch2 only on access ports:

* **Switch0(config)#** interface Fa2/1 → *must be access the interface*
* **Switch0(config-if)#** switchport port-security
* **Switch0(config-if)#** switchport port-security mac-address sticky
* **Switch0(config)#** interface Fa3/1 → *must be access the interface*
* **Switch0(config-if)#** switchport port-security
* **Switch0(config-if)#** switchport port-security mac-address sticky

Like this saved MAC are visible in **show running-config**

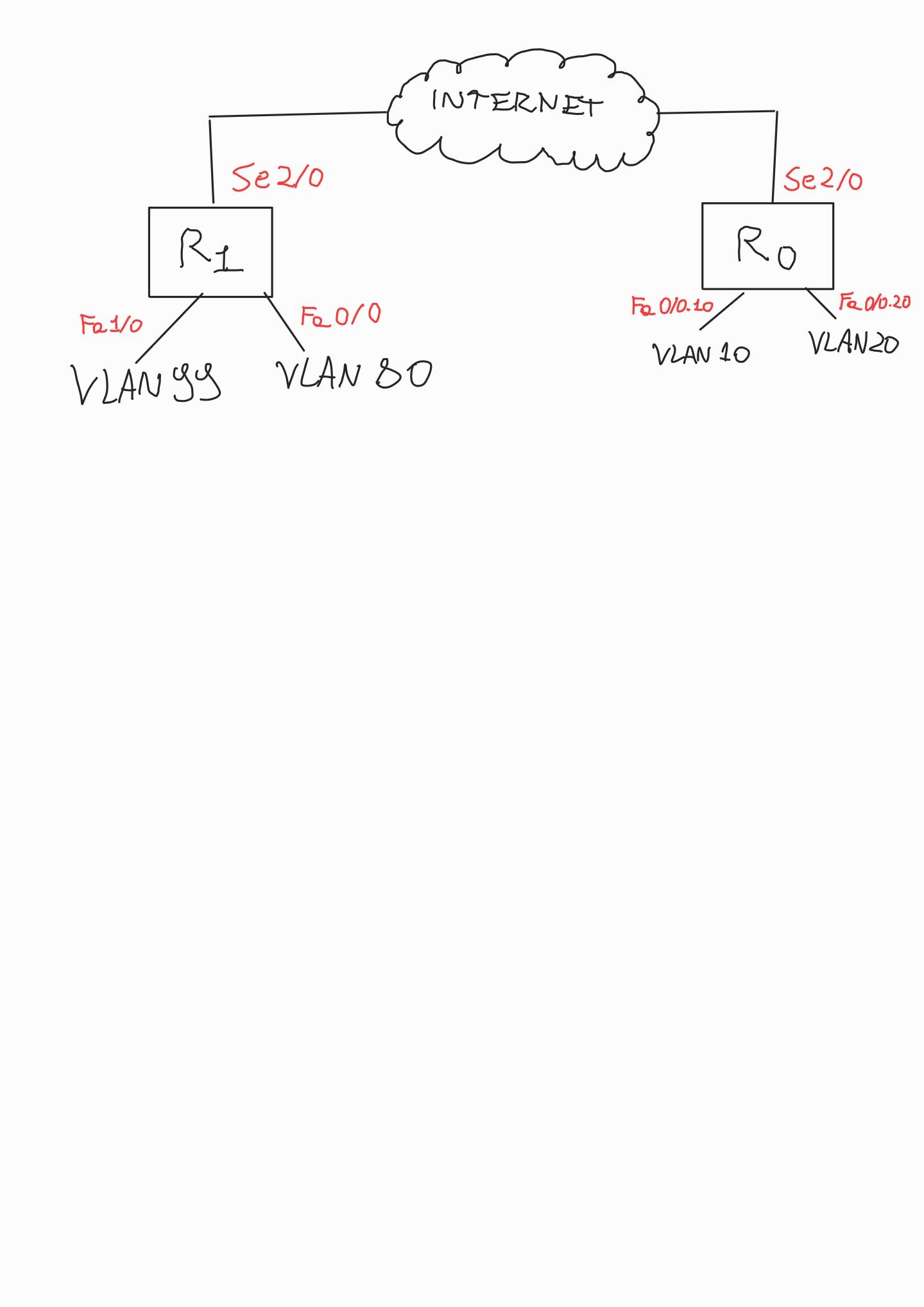
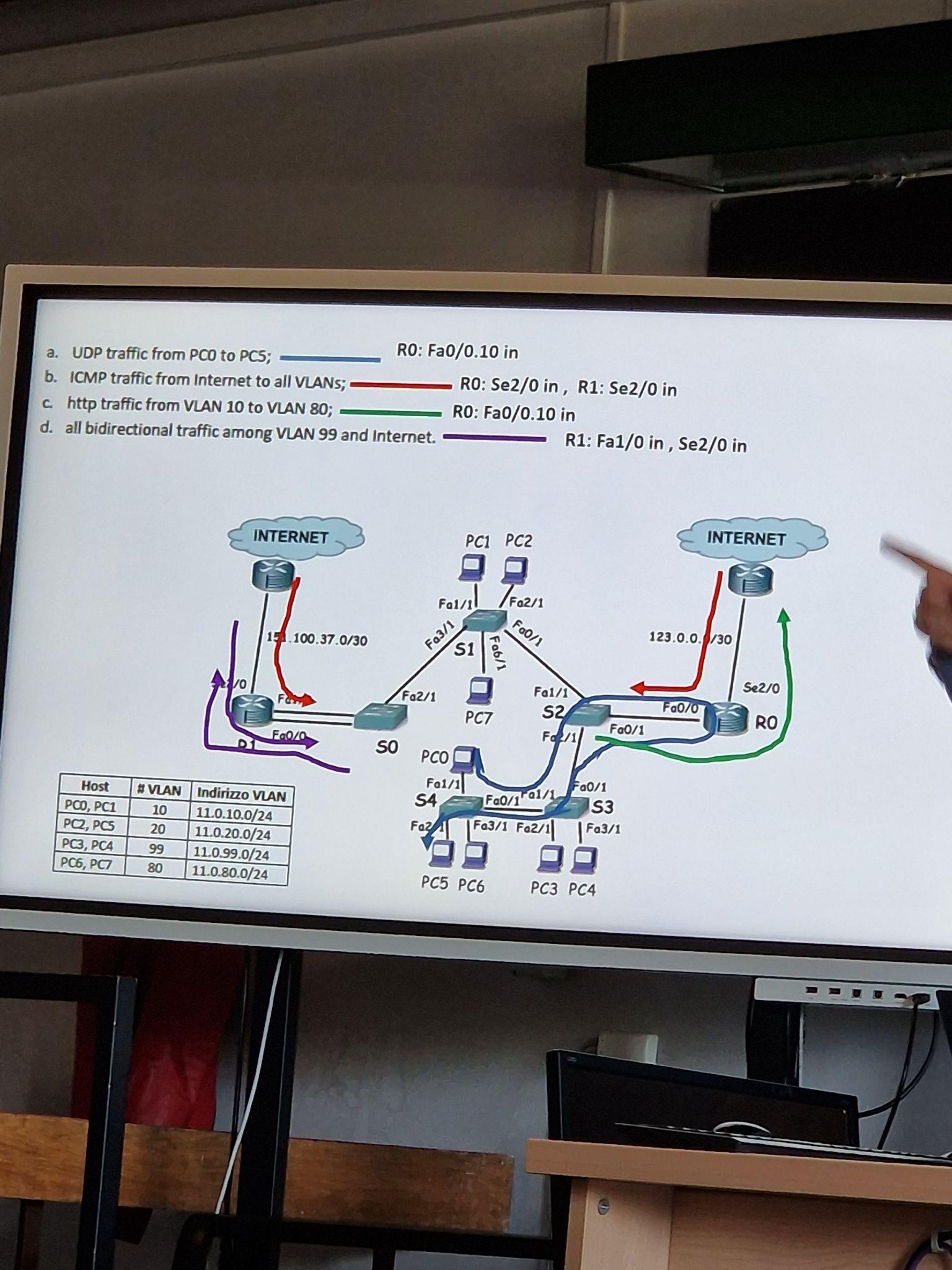
**6)** Commands for R1 for be accessible only by vlan 80 and vlan 99:

* **Router1(config)#** access-list 2 permit 11.0.99.0 0.0.0.255
* **Router1(config)#** access-list 2 permit 11.0.80.0 0.0.0.255
* **Router(config)#** access-list 2 deny any

Applying the access list:

* **Router1(config)#** line vty 0 4
* **Router1(config-...)#** access-class 2 in

**7)** Commands for Router0 using named access-list:



first and third rule:

* **Router0(config)#** ip access-list extended ac
* **Router0(config-ext-nacl)#** deny udp host 11.0.10.3 host 11.0.20.3
* **Router0(config-ext-nacl)#** deny tcp 11.0.10.0 0.0.0.255 11.0.80.0 0.0.0.255 eq www
* **Router0(config-ext-nacl)#** permit ip any any
* **Router0(config-ext-nacl)#** exit
* **Router0(config)#** interface Fa0/0.10 => ON DOT INTERFACE
* **Router0(config-if)#**  ip access-group ac in
* **Router0(config-if)#** exit

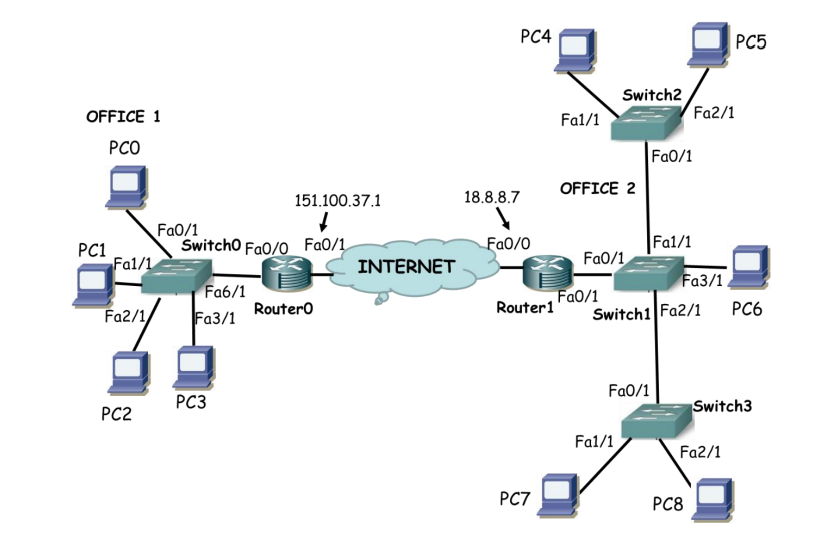
second rule R0:

* **Router0(config)#** ip access-list extended b
* **Router0(config-ext-nacl)#** permit icmp 11.0.99.0 0.0.0.255 any
* **Router0(config-ext-nacl)#** permit icmp 11.0.80.0 0.0.0.255 any
* **Router0(config-ext-nacl)#** deny icmp any any
* **Router0(config-ext-nacl)#** permit ip any any
* **Router0(config-ext-nacl)#** exit
* **Router0(config)#** interface Se2/0
* **Router0(config-if)#**  ip access-group b in
* **Router0(config-if)#** exit

second rule and fourth for R1:

* **Router1(config)#** ip access-list extended b
* **Router1(config-ext-nacl)#** permit icmp 11.0.10.0 0.0.0.255 any
* **Router1(config-ext-nacl)#** permit icmp 11.0.20.0 0.0.0.255 any
* **Router1(config-ext-nacl)#** deny icmp any any
* **Router1(config-ext-nacl)#** permit ip 11.0.10.0 0.0.0.255 11.0.99.0 0.0.0.255
* **Router1(config-ext-nacl)#** permit ip 11.0.20.0 0.0.0.255 11.0.99.0 0.0.0.255
* **Router1(config-ext-nacl)#** deny ip any 11.0.99.0 0.0.0.255
* **Router1(config-ext-nacl)#** permit ip any any
* **Router1(config-ext-nacl)#** exit
* **Router1(config)#** interface Se2/0
* **Router1(config-if)#**  ip access-group b in
* **Router1(config)#** ip access-list extended d
* **Router1(config-ext-nacl)#** permit ip any 11.0.80.0 0.0.0.255
* **Router1(config-ext-nacl)#** permit ip any 11.0.10.0 0.0.0.255
* **Router1(config-ext-nacl)#** permit ip any 11.0.20.0 0.0.0.255
* **Router1(config-ext-nacl)#** deny ip any any
* **Router1(config-ext-nacl)#** exit
* **Router1(config)#** interface Fa1/0
* **Router1(config-if)#**  ip access-group d in

# EXAM 3



**1)** The student has to configure the network reported in the figure. If a password must be configured,

you can use the following one: netlab. A network is composed of two different physical networks. The first one (Office 1) is connected to R0 and the second one (Office 2) is connected to R1. The two physical networks are managed by the same network administrator and are organized in the following VLANs:

* Hosts → VLAN → Indirizzo VLAN
* PC0, PC1 → 10 → 10 10.0.0.0/8
* PC2, PC3 → 20 → 192.168.0.0/24
* PC4 – PC8 → 1 → 192.168.10.0/24

Hosts of Office 1 network must be configured in a static way; hosts of Office 2 network must

be configured in a dynamic way.

**2)** Switches must have interfaces properly configured.

**3)** IP addresses of R0 and R1, and OSPF protocol have been already configured in the routers.

**4)** VLAN 20 is the Management VLAN for Office 1 network, while VLAN1 is the Management

VLAN for Office 2 network; switches must be accessible and configurable via telnet.

**5)** Hosts of VLAN 10, VLAN 20 and VLAN1 must communicate without using NAT.

**6)** R0 must be accessible and configurable only by hosts of VLAN 20.

**7)** DHCP Snooping must be enabled in the Office 2 network.

**8)** The following traffic flows must be blocked on Router0 minimizing router processing:

* ICMP traffic from Internet to VLAN 10 and VLAN 20 (supposing that NAT overload on interface Fa0/1 is used for both VLANs);
* ICMP traffic from VLAN 1 to VLAN 20;

**Answers:**

**1)** In each host of BLOCK-1 set an ip address from the vlan given, leave the first ip for the router. For the second block must set dhcp and set PC dynamic ip. Form point **7)** there is another server dhcp, set ip after that point.

* **Router1(config)#** ip dhcp pool exam2
* **Router1(config-if)#** network 192.168.10.0 255.255.0
* **Router1(config-if)#** default-router 192.168.10.1
* **Router1(config-if)#** exit
* **Router1(config)#** ip dhcp excluded-address 192.168.10.1 192.168.10.4 → Must fix ip of switches

**2)** For switch 1-2-3 must do nothing on interfaces because there is only one vlan, for switch 0:

* **Switch0(config)#** vlan 10
* **Switch0(config-vlan)#** exit
* **Switch0(config)#** vlan 20
* **Switch0(config-vlan)#** exit

Configure each interface:

* **Switch0(config)#** interface Fa0/1
* **Switch0(config-if)#** switchport mode access
* **Switch0(config-if)#** switchport access vlan 10
* **Switch0(config-if)#** exit
* **Switch0(config)#** interface Fa1/1
* **Switch0(config-if)#** switchport mode access
* **Switch0(config-if)#** switchport access vlan 10
* **Switch0(config-if)#** exit
* **Switch0(config)#** interface Fa2/1
* **Switch0(config-if)#** switchport mode access
* **Switch0(config-if)#** switchport access vlan 20
* **Switch0(config-if)#** exit
* **Switch0(config)#** interface Fa3/1
* **Switch0(config-if)#** switchport mode access
* **Switch0(config-if)#** switchport access vlan 20
* **Switch0(config-if)#** exit
* **Switch0(config)#** interface Fa6/1
* **Switch0(config-if)#** switchport mode trunk
* **Switch0(config-if)#** exit

**3)** For Router0: also **5)**

* **Router0(config)#** interface Fa0/0.10
* **Router0(config-if)#** encapsulation dot1Q 10
* **Router0(config-if)#** ip address 10.0.0.1 255.0.0.0
* **Router0(config-if)#** exit
* **Router0(config)#** interface Fa0/0.20
* **Router0(config-if)#** encapsulation dot1Q 20
* **Router0(config-if)#** ip address 192.168.0.1 255.255.255.0
* **Router0(config-if)#** exit
* **Router0(config)#** interface Fa0/0
* **Router0(config-if)#** no shutdown
* **Router0(config-if)#** exit

Must set for all PCs of vlan N the default-router.

For Router1:

* **Router1(config)#** interface Fa0/1
* **Router1(config-if)#** ip address 192.168.10.1 255.255.255.0
* **Router1(config-if)#** no shutdown
* **Router1(config-if)#** exit

**4)** For Switch0:

Set ip address from management vlan:

* **Switch2(config)#** interface vlan 20
* **Switch2(config-if)#** ip address 192.168.0.5

configure telnet:

* **Switch2(config)#** line vty 0 15
* **Switch2(config-line)#** password netlab
* **Switch2(config-line)#** login
* **Switch2(config-line)#** exit
* **Switch2(config)#** enable password netlab

For Switch 1-3:

Set ip address from management vlan:

* **Switch1(config)#** interface vlan 1
* **Switch1(config-if)#** ip address 192.168.10.(2 - 4)

configure telnet:

* **Switch1(config)#** line vty 0 15
* **Switch1(config-line)#** password netlab
* **Switch1(config-line)#** login
* **Switch1(config-line)#** exit
* **Switch1(config)#** enable password netlab

**5)** For communicate vlan 10 and 20 we set in point **3)** Router0, for communicate also with vlan 1 we must set a Tunnel:

* **Router0(config)#**interface Tunnel 0
* **Router0(config-if)#** tunnel mode gre ip
* **Router0(config-if)#** ip address 192.168.20.1 255.255.255.252
* **Router0(config-if)#** tunnel source Fa0/1 (physical connected to internet)
* **Router0(config-if)#** tunnel destination 18.8.87 (ip of physical destination)
* **Router0(config)#** ip route 192.168.10.0 255.255.255.0 192.168.20.2 (ip of tunnel destination)
* **Router1(config)#**interface Tunnel 0
* **Router1(config-if)#** tunnel mode gre ip
* **Router1(config-if)#** ip address 192.168.20.2 255.255.255.252
* **Router1(config-if)#** tunnel source Fa0/0 (physical connected to internet)
* **Router1(config-if)#** tunnel destination 151.100.37.1 (ip of physical destination)
* **Router1(config)#** ip route 192.168.0.0 255.255.255.0 192.168.20.1
* **Router1(config)#** ip route 10.0.0.0 255.0.0.0 192.168.20.1

**6)** Commands for R0 for be accessible only by vlan 20:

* **Router0(config)#** access-list 2 permit 192.168.0.0 0.0.0.255
* **Router0(config)#** access-list 2 deny any

Applying the access list:

* **Router0(config)#** line vty 0 4
* **Router0(config-...)#** access-class 2 in

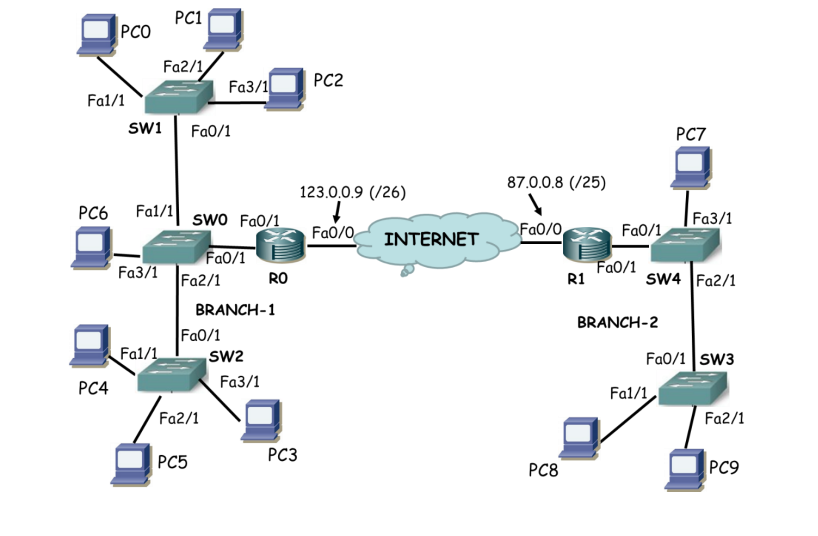
**7)** Commands for enable dhcp snooping:

* **Switch1(config)#**  ip dhcp snooping
* **Switch1(config)#** ip dhcp snooping vlan 1
* **Switch1(config)#** no ip dhcp snooping information option
* **Switch1(config)#** interface Fa0/1
* **Switch1(config-if)#** ip dhcp snooping trust
* **Switch2(config)#**  ip dhcp snooping
* **Switch2(config)#** ip dhcp snooping vlan 1
* **Switch2(config)#** no ip dhcp snooping information option
* **Switch2(config)#** interface Fa0/1
* **Switch2(config-if)#** ip dhcp snooping trust
* **Switch3(config)#**  ip dhcp snooping
* **Switch3(config)#** ip dhcp snooping vlan 1
* **Switch3(config)#** no ip dhcp snooping information option
* **Switch3(config)#** interface Fa0/1
* **Switch3(config-if)#** ip dhcp snooping trust

**8)** Commands for Router0 using named access-list:

* **Router0(config)#** ip access-list extended a
* **Router0(config-ext-nacl)#** permit icmp host 18.8.8.7 any
* **Router0(config-ext-nacl)#** deny icmp any any
* **Router0(config-ext-nacl)#** exit
* **Router0(config)#** interface Fa0/1
* **Router0(config-if)#**  ip access-group a in
* **Router0(config-if)#** exit
* **Router0(config)#** ip access-list extended b
* **Router0(config-ext-nacl)#** deny icmp 192.168.10.0 0.0.0.255 192.168.0.0 0.0.0.255
* **Router0(config-ext-nacl)#** permit ip any any
* **Router0(config-ext-nacl)#** exit
* **Router0(config)#** interface Fa0/0.20
* **Router0(config-if)#**  ip access-group b out
* **Router0(config-if)#** exit

# EXAM MIDTERM



**1)** The student has to configure the network reported in the figure. Password to use: netlab. A network is composed of two different physical networks. The first one (BRANCH-1) is connected to R0 and the second one (BRANCH-2) is connected to R1. The two physical networks are managed by the same network administrator and are organized in VLANs:

* Host Physical → Network →VLAN → Indirizzo VLAN
* PC0, PC4 → BRANCH-1 → 10 → 192.168.10.0/24
* PC1, PC5 → BRANCH-1 → 20 → 10.0.20.0/24
* PC2, PC3 → BRANCH-1 → 30 → 192.168.30.0/24
* PC6 → BRANCH-1 → 98 → 10.0.98.0/24
* PC7, PC8, PC9 →BRANCH-2 → 1 → 10.0.1.0/24

Hosts of BRANCH-1 must be configured in a static way; hosts of BRANCH-2 must be configured

in a dynamic way. Switches must have interfaces properly configured.

**2)** IP addresses of R0 and R1 must be configured on the basis of the figure. OSPF has been

already configured in the routers.

**3)** VLAN 98 is the Management VLAN for BRANCH-1 network, while VLAN1 is the Management

VLAN for BRANCH-2 network; switches must be accessible and configurable via telnet.

**4)** Hosts of VLAN 10, VLAN 30 and VLAN1 must communicate. NAT is NOT enabled.

**5)** R0 must be accessible and configurable only by hosts of VLAN 30.

**6)** DHCP Snooping must be enabled in BRANCH-2. Static port security must be enabled on SW4.

**7)** The following traffic flows must be blocked in R0 minimizing router processing:

* ICMP traffic from VLAN1 to VLAN 30;
* HTTP traffic from VLAN 10 to VLAN 30;
* UDP traffic from PC3 to PC8

**SOLUZIONE MIA (NON CORRETTA):**

**2)** In each host of BLOCK-1 set an ip address from the vlan given, leave the first ip for the router. For the second block must set dhcp and set PC dynamic ip. Form point **6)** there is another server dhcp, set ip after that point.

* **Router1(config)#** interface Fa0/1
* **Router1(config-if)#** ip address 10.0.1.1 255.255.255.0
* **Router1(config-if)#** no shutdown
* **Router1(config-if)#** exit
* **Router1(config)#** ip dhcp pool mid
* **Router1(config-if)#** network 10.0.1.0 255.255.255.0
* **Router1(config-if)#** default-router 10.0.1.1
* **Router1(config-if)#** exit
* **Router1(config)#** ip dhcp excluded-address 10.0.1.1 10.0.1.3
* **Router0(config)#** interface Fa0/1.10
* **Router0(config-if)#** encapsulation DOT1Q 10
* **Router0(config-if)#** ip address 192.168.10.1 255.255.255.0
* **Router0(config-if)#** exit
* **Router0(config)#** interface Fa0/1.30
* **Router0(config-if)#** encapsulation DOT1Q 30
* **Router0(config-if)#** ip address 192.168.30.1 255.255.255.0
* **Router0(config-if)#** exit
* **Router0(config)#** interface Fa0/1
* **Router0(config-if)#** no shutdown
* **Router0(config-if)#** exit

**1)** For switch 3-4 must do nothing on interfaces because there is only vlan 1, for switch 0-1-2:

SWITCH0:

* **Switch0(config)#** vlan 10
* **Switch0(config-vlan)#** exit
* **Switch0(config)#** vlan 20
* **Switch0(config-vlan)#** exit
* **Switch0(config)#** vlan 30
* **Switch0(config-vlan)#** exit
* **Switch0(config)#** vlan 98
* **Switch0(config-vlan)#** exit

Configure each interface:

* **Switch0(config)#** interface Fa0/1
* **Switch0(config-if)#** switchport mode trunk
* **Switch0(config-if)#** exit
* **Switch0(config)#** interface Fa1/1
* **Switch0(config-if)#** switchport mode trunk
* **Switch0(config-if)#** exit
* **Switch0(config)#** interface Fa2/1
* **Switch0(config-if)#** switchport mode trunk
* **Switch0(config-if)#** exit
* **Switch0(config)#** interface Fa3/1
* **Switch0(config-if)#** switchport mode access
* **Switch0(config-if)#** switchport access vlan 98
* **Switch0(config-if)#** exit

SWITCH1:

* **Switch1(config)#** vlan 10
* **Switch1(config-vlan)#** exit
* **Switch1(config)#** vlan 20
* **Switch1(config-vlan)#** exit
* **Switch1(config)#** vlan 30
* **Switch1(config-vlan)#** exit
* **Switch1(config)#** vlan 98
* **Switch1(config-vlan)#** exit

Configure each interface:

* **Switch1(config)#** interface Fa0/1
* **Switch1(config-if)#** switchport mode trunk
* **Switch1(config-if)#** exit
* **Switch1(config)#** interface Fa1/1
* **Switch1(config-if)#** switchport mode access
* **Switch1(config-if)#** switchport access vlan 10
* **Switch1(config-if)#** exit
* **Switch1(config)#** interface Fa2/1
* **Switch1(config-if)#** switchport mode access
* **Switch1(config-if)#** switchport access vlan 20
* **Switch1(config-if)#** exit
* **Switch1(config)#** interface Fa3/1
* **Switch1(config-if)#** switchport mode access
* **Switch1(config-if)#** switchport access vlan 30
* **Switch1(config-if)#** exit

SWITCH2:

* **Switch2(config)#** vlan 10
* **Switch2(config-vlan)#** exit
* **Switch2(config)#** vlan 20
* **Switch2(config-vlan)#** exit
* **Switch2(config)#** vlan 30
* **Switch2(config-vlan)#** exit
* **Switch2(config)#** vlan 98
* **Switch2(config-vlan)#** exit

Configure each interface:

* **Switch2(config)#** interface Fa0/1
* **Switch2(config-if)#** switchport mode trunk
* **Switch2(config-if)#** exit
* **Switch2(config)#** interface Fa1/1
* **Switch2(config-if)#** switchport mode access
* **Switch2(config-if)#** switchport access vlan 10
* **Switch2(config-if)#** exit
* **Switch2(config)#** interface Fa2/1
* **Switch2(config-if)#** switchport mode access
* **Switch2(config-if)#** switchport access vlan 20
* **Switch2(config-if)#** exit
* **Switch2(config)#** interface Fa3/1
* **Switch2(config-if)#** switchport mode access
* **Switch2(config-if)#** switchport access vlan 30
* **Switch2(config-if)#** exit

**3)** Set ip addresses and telnet and enable passwords:

SWITCH0:

* **Switch0(config)#** interface vlan 98
* **Switch0(config-if)#** ip address 10.0.98.5 255.255.255.0
* **Switch0(config-if)#** exit
* **Switch0(config)#** line vty 0 15
* **Switch0(config-if)#** password netlab
* **Switch0(config-if)#** login
* **Switch0(config-if)#** exit
* **Switch0(config)#** enable password netlab

SWITCH1:

* **Switch1(config)#** interface vlan 98
* **Switch1(config-if)#** ip address 10.0.98.6 255.255.255.0
* **Switch1(config-if)#** exit
* **Switch1(config)#** line vty 0 15
* **Switch1(config-if)#** password netlab
* **Switch1(config-if)#** login
* **Switch1(config-if)#** exit
* **Switch1(config)#** enable password netlab

SWITCH2:

* **Switch2(config)#** interface vlan 98
* **Switch2(config-if)#** ip address 10.0.98.7 255.255.255.0
* **Switch2(config-if)#** exit
* **Switch2(config)#** line vty 0 15
* **Switch2(config-if)#** password netlab
* **Switch2(config-if)#** login
* **Switch2(config-if)#** exit
* **Switch2(config)#** enable password netlab

SWITCH3:

* **Switch3(config)#** interface vlan 1
* **Switch3(config-if)#** ip address 10.0.1.2 255.255.255.0
* **Switch3(config-if)#** exit
* **Switch3(config)#** line vty 0 15
* **Switch3(config-if)#** password netlab
* **Switch3(config-if)#** login
* **Switch3(config-if)#** exit
* **Switch3(config)#** enable password netlab

SWITCH4:

* **Switch4(config)#** interface vlan 1
* **Switch4(config-if)#** ip address 10.0.1.3 255.255.255.0
* **Switch4(config-if)#** exit
* **Switch4(config)#** line vty 0 15
* **Switch4(config-if)#** password netlab
* **Switch4(config-if)#** login
* **Switch4(config-if)#** exit
* **Switch4(config)#** enable password netlab

**4)** For VLAN 10 and 30 already set Router0 in point 2) and set interfaces on Switch0 in point 1), must set the default-router of PCs. For communicate with VLAN 1 use a Tunnel:

* **Router0(config)#** interface Tunnel 0
* **Router0(config-if)#** tunnel mode gre ip
* **Router0(config-if)#** ip address 192.168.20.1 255.255.255.252
* **Router0(config-if)#** tunnel source Fa0/0
* **Router0(config)#** tunnel destination 87.0.0.8
* **Router0(config-if)#** exit
* **Router0(config)#** ip route 10.0.1.0 255.255.255.0 192.168.20.2
* **Router1(config)#** interface Tunnel 0
* **Router1(config-if)#** tunnel mode gre ip
* **Router1(config-if)#** ip address 192.168.20.2 255.255.255.252
* **Router1(config-if)#** tunnel source Fa0/0
* **Router1(config)#** tunnel destination 123.0.0.9
* **Router1(config-if)#** exit
* **Router1(config)#** ip route 192.168.10.0 255.255.255.0 192.168.20.1
* **Router1(config)#** ip route 192.168.30.0 255.255.255.0 192.168.20.1

**5)** Commands for R0 for be accessible only by vlan 30:

* **Router0(config)#** access-list 2 permit 192.168.30.0 0.0.0.255
* **Router0(config)#** access-list 2 deny any

Applying the access list:

* **Router0(config)#** line vty 0 4
* **Router0(config-...)#** access-class 2 in

**6)** Commands for enable dhcp snooping:

**DHCP SNOOPING:**

* **Switch4(config)#**  ip dhcp snooping
* **Switch4(config)#** ip dhcp snooping vlan 1
* **Switch4(config)#** no ip dhcp snooping information option
* **Switch4(config)#** interface Fa0/1
* **Switch4(config-if)#** ip dhcp snooping trust
* **Switch4(config-if)#** exit

STATIC PORT SECURITY:

PC7->prompt-> c:> ipconfig /all -> <MAC>

* **Switch4(config)#** interface Fa3/1
* **Switch4(config-if)#** switchport port-security
* **Switch4(config-if)#** switchport port security mac-address <MAC>
* **Switch3(config)#**  ip dhcp snooping
* **Switch3(config)#** ip dhcp snooping vlan 1
* **Switch3(config)#** no ip dhcp snooping information option
* **Switch3(config)#** interface Fa0/1
* **Switch3(config-if)#** ip dhcp snooping trust

**7)** Commands for Router0 using named access-list:

* **Router0(config)#** ip access-list extended a
* **Router0(config-ext-nacl)#** deny icmp 10.0.1.0 0.0.0.255 any
* **Router0(config-ext-nacl)#** permit ip any any
* **Router0(config-ext-nacl)#** exit
* **Router0(config)#** interface Fa0/1.30
* **Router0(config-if)#**  ip access-group a out
* **Router0(config-if)#** exit
* **Router0(config)#** ip access-list extended b
* **Router0(config-ext-nacl)#** deny tcp any 192.168.30.0 0.0.0.255 eq www
* **Router0(config-ext-nacl)#** permit ip any any
* **Router0(config-ext-nacl)#** exit
* **Router0(config)#** interface Fa0/0.10
* **Router0(config-if)#**  ip access-group b in
* **Router0(config-if)#** exit
* **Router0(config)#** ip access-list extended c
* **Router0(config-ext-nacl)#** deny udp host 192.168.30.3 host 10.0.1.0.5
* **Router0(config-ext-nacl)#** permit ip any any
* **Router0(config-ext-nacl)#** exit
* **Router0(config)#** interface Fa0/1.30
* **Router0(config-if)#**  ip access-group ac in
* **Router0(config-if)#** exit