Instruction for lab 09 (rev. 201202)

**legend:**blue color (006699) - additional remarks  
green color (006600) { ... }- outside of curriculum  
red color (FF0000) - important fragments  
orange color (FF9900) - alternatives tasks for extra points  
grey color (999999) - could be omitted, should be used in special cases, especially in case of problem (wrong [IOS](https://eportal.pwr.edu.pl/mod/folder/view.php?id=56895), lack of commands, ...)  
  
1 point - the number of points possible to receive for particular task  
[2.2.5.1] CCNA1 v. 5.0 - refers to the number of Cisco Academy labs, course name, course semester number and curriculum version.  
\*[1.2.3.4] - refers to older version of Cisco Academy curriculum  
Recommended printout - the exercise recommended for printing  
Obligatory print - compulsory exercise for printing (1 copy per group)

For self preparation before lab

* What is duplex/halfduplex?
* How works the assignment of static and dynamic MAC addresses to the port of the switch?
* How to configure the switch port to accept only specific client traffic (hosts)?

Suggested bibliography:

* Cisco Academy CCNA2 curriculum materials

Lab topology schema

PC1 ---------- |S\_X |---------- PC2

Each group configure switch S\_X and router R\_X  
PC1 and PC2 should be connected to port s Fa 0/1 and Fa 0/11, Roter R\_X to port Fa 0/23.

[IP addresses](https://eportal.pwr.edu.pl/mod/resource/view.php?id=56957) and names used in Lab 10

**Switch**  
name: S\_X  
management VLAN: 99  
  
Ports assigments to VLANS  
Fa 0/1 - Fa 0/24: VLAN 99  
  
IP address of management VLAN (99)  
192.168.X.X9/24, gateway: 192.168.X.X0  
  
**PC**  
[IP addresses](https://eportal.pwr.edu.pl/mod/resource/view.php?id=56957) of local computers  
PC1: 192.168.X.X1/24, brama: 192.168.X.X0  
PC2: 192.168.X.X2/24, brama: 192.168.X.X0  
...  
X - group number.

Task 1 - Managing the MAC address table on the switch.

\*[2.5.1] CCNA ver. 4  
[5.1.1.6] CCNA R&S2 ver. 6.0 (Part 4 MAC management)  
  
2 points

PC configuration

- Check the PC connection to the switch.

PC1 to port 1  
PC2 to port 11

- Set IPv4 addresses on computers in the group

[IP addresses](https://eportal.pwr.edu.pl/mod/resource/view.php?id=56957) assigned to interfaces of individual computers:  
PC1: 192.168.X.X1 / 24, gateway: 192.168.X.X0  
PC2: 192.168.X.X2 / 24, gateway: 192.168.X.X0

Router configuration

- erase old configuration  
- make base router configuration  
- configure IP address on LAN interface

R\_X(config)#interface FastEthernet 0/0 (or FastEthernet 0/2/0)  
R\_X(config-if)#ip address 192.168.X.X0 255.255.255.0  
R\_X(config-if)#no shutdown

**Switch configuration**

- Remove the VLAN data base from the switch.

S\_X>enable  
S\_X#delete flash:vlan.dat  
Delete filename [vlan.dat]? [Enter]  
Delete flash: vlan.dat? [Confirm] [Enter]

- Remove the startup configuration from the switch.

S\_X#erase startup-config

- Restart the switch.

S\_X#reload

During reload do not save the current configuration.  
For the question: Do you want save the changes? - answer no.

- After reloading do not enter into the setup wizard,  
Would you like to enter the initial configuration dialog? [yes/no]: no <ENTER>  
Would you like to terminate autoinstall? [Yes]: yes <ENTER> or <ENTER>  
  
- Assign a switch name

Switch#configure terminal  
Switch(config)#hostname S\_X  
S\_X(config)#exit

X - replace by the group number (switch number).

- Set passwords for vty and console lines

S\_X#configure terminal  
S\_X(config)#line console 0  
S\_X(config-line)#password cisco  
S\_X(config-line)#login  
S\_X(config-line)#line vty 0 15  
S\_X(config-line)#password cisco  
S\_X(config-line)#login  
S\_X(config-line)#exit

- Set password to privileged mode.

S\_X(config)#enable password class  
...don't use encrypted password (enable secret)

- Layer 3 address configuration for the switch.  
To be able to remotely manage the switch, you must assign the correct IP configurations to the appropriate interfaces. By default, all switch ports are assigned to VLAN1, which is also a default management VLAN. For security reasons, a VLAN different than VLAN1 should be configured as managemt VLAN.

Set VLAN99 as the management VLAN.  
For VLAN 99 set the IP address 192.168.X.X9 / 24, where X is the switch number (should correspond to the group number).

S\_X(config)#vlan 99  
S\_X(config-vlan)#exit  
S\_X(config)#interface vlan99  
S\_X(config-if)#ip address 192.168.X.X9 255.255.255.0 (192.168.6.69 - example for the group no 6)  
S\_X(config-if)#no shutdown  
S\_X(config-if)#exit  
S\_X(config)#

- Port assignments to VLAN99.  
All ports are assigned by default to VLAN1, which is a management VLAN. Access to the switch and its configuration is possible only from ports assigned to the management VLAN. If you change the managemnt VLAN number the management ports should be also assigned to this VLAN number. Configuration from other ports will not be available.

For the purpose of this exercise all ports are selected as management ports.

S\_X(config)#interface range fa0/1 - 24  
S\_X(config-if-range)#switchport access vlan 99  
S\_X(config-if-range)#exit  
S\_X(config)#

- Set default gateway

S\_X(config)#ip default-gateway 192.168.X.X0 (192.168.6.60 - for the switch no 6)  
S\_X(config)#exit

- Check created IP configuration.

S\_X#show interface vlan 99

- Check the connection between devices. Use the ping command.

PC1, PC2 - S\_X  
Does the switch answers?

- Save the configuration into NVRAM

S\_X#copy running-config startup-config

- Display the startup configuration (NVRAM)

S\_X#show startup-config

- Check and save the MAC addresses of cisco NIC from both PC.

c:\>ipconfig /all

Save it into notepad document.

- Test the communication between the devices:

- PC1 - PC2  
- PC1- S\_X  
- PC2 - S\_X

- Verify what MAC addresses the switch has learned.

S\_X#show mac address-table  
S\_X#show mac address-table ?  
S\_X#show mac address-table dynamic  
S\_X#show mac address-table address (write here mac address of your PC)

- Clean the mac address table.

S\_X#clear mac address-table dynamic

Check the mac table, it is realy empty?  
Which entries still exists?

- **Set static MAC address of PC2 to port Fa 0/1 (port connected to PC1)**

S\_X(config)#mac address-table static xxxx.yyyy.zzzz vlan 99 interface FastEthernet 0/1  
xxx.yyy.zzz - represents the MAC address of PC2 in short notation

- Check communication between PC1 and PC2 and the switch

Check mac address table.  
Is communication PC1 - switch possible? Why?  
Is communicatio PC2 - switch possible? Why?

- **Swap the computer cables** connected to switch  
  
- Check communication between PC1 and PC2 and the switch

Did something change?

Check the content of the mac table.  
Can communication from PC1 be possible, why?  
Can communication from PC2 be possible, why?

- Delete the static entry and check configuration

S\_X(config)#no mac address-table static xxxx.yyyy.zzzz vlan 99 interface FastEthernet 0/1

Check contents of the mass address table.  
Check communication between PC1, PC2 and switch.  
**Swap computer cables on the switch to correct ports.**  
Test the connections.

Task 2 - Switch port configuration. Securing the switch ports.

\*[2.5.1] CCNA ver. 4  
[5.2.2.9] CCNA R&S2 ver. 6.0 (Part 4: Configure and Verify Security Features on Switch )  
2 points  
  
- Check the communication between PCs and switch. In case of problem diagnose and repair the connections.  
  
-Check the configuration of PC1 port

S\_X#show interface FastEthernet 0/1

It the interface enabled?  
How to enable it?  
Check port MAC address.  
Check the speed and duplex mode.

-**Configure the speed of the Fa 0/2 to 10 Mb/s and full duplex mode**.

S\_X#configure terminal  
S\_X(config)#interface FastEthernet 0/2  
S\_X(config-if)#speed 10  
S\_X(config-if)#duplex full  
S\_X(config-if)#end  
S\_X#show interface FastEthernet 0/2

Remark: configuration of Fa0/1 in speed 10 and full duplex cause the connection problem with the router in the task 2.

- **Disable unused ports**

S\_X(config)#interface range Fa 0/12-22, Gi 0/1-2  
S\_X(config-if)#shutdown

- **Configure the Fa 0/1 port security. Allow only two sticky secure mac addresses**.**Use the restrict mode of port security.**

S\_X#configure terminal  
S\_X(config)#interface FastEthernet 0/1  
S\_X(config-if)#switchport mode access  
S\_X(config-if)#switchport port-security  
S\_X(config-if)#switchport port-security maximum 2  
S\_X(config-if)#switchport port-security mac-address sticky  
S\_X(config-if)#switchport port-security violation **restrict**  
S\_X(config-if)#end  
S\_X#show port-security

- Check the configuration.

Was the MAC address of the connected computer memorized?

**Connect repeatedly the second and third devices to the secured Fa0/1 port :**

- Disconnect the PC1 cable from Fa 0/1 switch port. Then connect to this port any second device.

For example: connect the router R\_X cable from the port Fa 0/23 (to port Fa 0/1) or any computer cable from the neighbor group (do it for a while, inform the neighbors).  
In the time of connection make the connectivity test to force the connected devices to send to switch any frame. Switch will memorize the device physical address from Ethernet frame.

- Check if mac address of second device (computer/router) was memorized on the switch port.

S\_X#show run

S\_X#show mac address-table

- Connect PC2 to port Fa 0/1

Check if communication from it is possible? Why?  
Was the third MAC address memorized?

S\_X#show run

S\_X#show mac address-table

- **Repeat this step for different security option. Enable the port shutdown after security violation.**

S\_X(config)#interface FastEthernet 0/1  
S\_X(config-if)#switchport port-security violation **shutdown**

What happen after connection of second and third device to the Fa 0/1 port?

- Check status of Fa 0/1 port

S\_X#show ip interface brief FastEthernet 0/1

- Try to enable the blocked port

Only one way to unblock the port is to shutdown it and activate again

S\_X(config)#interface Fa 0/1  
S\_X(config-if)#shutdown  
S\_X(config-if)#no shutdown

- Ask instructor to check your results.  
  
- Erase the switch and router configuration.

The "violation shutdown" option on the Catalyst 2960 switch is the default option and does not show up in the configuration (running-config). If this option is set, the port will be blanked when the intruder is connected. The Compueter is treated as an intruder, when the number of connected computers to the port with the restriction "port-security maximum n" has been exceeded. In the case of using the "violation protect" option, the switch does not shutdown the port if an intruder computer interferes with it. However, the communication of this computer is blocked. The computer of the intruder can not communicate through this port. MAC addresses memorized by the "mac-address-sticky" command are added to the configuration of the current port. If the current configuration is remembered for the nvram, then after restarting the switch through a given port, only those sockets that could be remembered before the restart could be connected..

Task 3 - Switch IPv6 configuration. SSH service configuration.

Points: 1

**Switch**  
name: S\_X  
management VLAN: 99  
  
Ports assigments to VLANS  
Fa 0/1 - Fa 0/24: VLAN 99  
  
IPv6 address of management VLAN (99)  
fc00:99::X9/64  
fe80::19 link-local

gateway  
fc00:99::X0  
  
**PC**  
[IP addresses](https://eportal.pwr.edu.pl/mod/resource/view.php?id=56957) of local computers  
PC1: fc00:99::X1/64  
fe80::X1 link-local

PC2: fc00:99::X2/64  
fe80::X2 link-local

X - group number.

- Make the IPv6 configuration on the PCs.

- Prepare the switch to IPv6 configuration. Change the default working tamplate.

S\_X(config)#sdm prefer dual-ipv4-and-ipv6 default

After this change reload the switch and proceed.

- Make the IPv6 configuration on the switch: IPv6 address and the gateway.

int vlan 99  
ipv6 address ...

ipv6 address ... link-local

ipv6 route ::/0 fc:99::X0

- Check if PCs switch port are configured in VLAN 99

- Configure SSH server on the switch.  
Configure SSH in version 2.  
Create users:  
stud - password cisco (privilidge level0)  
admin - password class (priviledge level 15)  
Configure domain name: pwr.edu.pl  
Set the correct date and time.  
Crypto key lenght: 1024

S\_X(config)#ip ssh version 2

- test SSH connection to switch from the PCs.

Task 3 - Router and switch IP configuration. SSH service configuration.

\* [2.5.1] CCNA ver. 4  
[5.1.1.6] CCNA R&S2 ver. 6.0  
[5.2.2.9] CCNA R&S2 ver 6.0 (Part 3: Configure and Verify SSH Access on Switch)  
  
2 points

PC configuration

- Check the PC connection to the switch.

PC1 to port 1  
PC2 to port 11

- Set IPv4 addresses on computers in the group

[IP addresses](https://eportal.pwr.edu.pl/mod/resource/view.php?id=56957) assigned to interfaces of individual computers:  
PC1: 192.168.X.X1 / 24, gateway: 192.168.X.X0  
PC2: 192.168.X.X2 / 24, gateway: 192.168.X.X0

Router configuration

- erase old configuration  
- make base router configuration  
- configure IP address on LAN interface

R\_X(config)#interface FastEthernet 0/0 (or FastEthernet 0/2/0)  
R\_X(config-if)#ip address 192.168.X.X0 255.255.255.0  
R\_X(config-if)#no shutdown

Switch configuration

- Remove the VLAN data base from the switch.

S\_X>enable  
S\_X#delete flash:vlan.dat  
Delete filename [vlan.dat]? [Enter]  
Delete flash: vlan.dat? [Confirm] [Enter]

- Remove the startup configuration from the switch.

S\_X#erase startup-config

- Restart the switch.

S\_X#reload

During reload do not save the current configuration.  
For the question: Do you want save the changes? - answer no.

- After reloading do not enter into the setup wizard,  
Would you like to enter the initial configuration dialog? [yes/no]: no <ENTER>  
Would you like to terminate autoinstall? [Yes]: yes <ENTER> or <ENTER>  
  
- Assign a switch name

Switch#configure terminal  
Switch(config)#hostname S\_X  
S\_X(config)#exit

X - replace by the group number (switch number).

- Set passwords for vty and console lines

S\_X#configure terminal  
S\_X(config)#line console 0  
S\_X(config-line)#password cisco  
S\_X(config-line)#login  
S\_X(config-line)#line vty 0 15  
S\_X(config-line)#password cisco  
S\_X(config-line)#login  
S\_X(config-line)#exit

- Set password to privileged mode.

S\_X(config)#enable password class  
...don't use encrypted password (enable secret)

- Layer 3 address configuration for the switch.  
To be able to remotely manage the switch, you must assign the correct IP configurations to the appropriate interfaces. By default, all switch ports are assigned to VLAN1, which is also a default management VLAN. For security reasons, a VLAN different than VLAN1 should be configured as managemt VLAN.

Set VLAN99 as the management VLAN.  
For VLAN 99 set the IP address 192.168.X.X9 / 24, where X is the switch number (should correspond to the group number).

S\_X(config)#vlan 99  
S\_X(config-vlan)#exit  
S\_X(config)#interface vlan99  
S\_X(config-if)#ip address 192.168.X.X9 255.255.255.0 (192.168.6.69 - example for the group no 6)  
S\_X(config-if)#no shutdown  
S\_X(config-if)#exit  
S\_X(config)#

- Port assignments to VLAN99.  
All ports are assigned by default to VLAN1, which is a management VLAN. Access to the switch and its configuration is possible only from ports assigned to the management VLAN. If you change the managemnt VLAN number the management ports should be also assigned to this VLAN number. Configuration from other ports will not be available.

For the purpose of this exercise all ports are selected as management ports.

S\_X(config)#interface range fa0/1 - 24  
S\_X(config-if-range)#switchport access vlan 99  
S\_X(config-if-range)#exit  
S\_X(config)#

- Set default gateway

S\_X(config)#ip default-gateway 192.168.X.X0 (192.168.6.60 - for the switch no 6)  
S\_X(config)#exit

- Check created IP configuration.

S\_X#show interface vlan 99

- Check the connection between devices. Use the ping command.

PC1, PC2 - S\_X  
Does the switch answers?

- Save the configuration into NVRAM

S\_X#copy running-config startup-config

- Display the startup configuration (NVRAM)

S\_X#show startup-config

SSH configuration on the switch

- Cofigure the domain name of the switch as cisco.lab128.pwr.edu.pl

S\_X(config)#ip domain-name cisco.lab128.pwr.edu.pl

- Create the local data base of the SSH users

S\_X(config)#username admin privilege 15 secret adminpass  
S\_X(config)#username stud privilege 1 secret studpass

- Configure VTY terminal to support SSH and telnet connections. Force authentication based on local user database.

S\_X(config)#line vty 0 15   
S\_X(config-line)#transport input **telnet ssh**   
S\_X(config-line)#login **local**   
S\_X(config-line)#exit

- Configure a 1024 bit RSA key

S\_X(config)#crypto key generate rsa modulus 1024

- Check the ability to log on via the telnet service to the switch from PC computer. Try to connect via telnet to admin and stud account.

Note in notepad the difference between this two connections.

- Check the ability to log on via the SSH service. As an SSH client, use the putty program.

- Check the SSH configuration settings on the switch.

S1#show ip ssh

What version of SSh is configured by default?

What is the maximum number of logon errors?  
What is the default idle time?

Note in notepad the SSH default settings.

- Change the SSH version

S\_X#config t   
S\_X(config)#ip ssh version ?  
S\_X(config)#ip ssh version 1

- Check the configuration changes

S1#show ip ssh

- Test the SSH login possibilities with putty. Does any changes appear during log on.  
In case of the problem change the SSH version in putty  
  
- Change SSH version to 2

S\_X(config)#ip ssh version 2

- Change the default time-out and authentication settings

S\_X#config t   
S\_X(config)#ip ssh time-out 10  
S\_X(config)#ip ssh authentication-retries 1

- Check if the new setting function correctly. Connect with putty SSH and wait 30 seconds

Test the SSH connection to switch. Use the Windows clock to calculate the elapsed time.  
Save in notepad the real exec time.

- Try to overwrite SSH time-out settings with VTY lines settings

S\_X(config)#line vty 0 15  
S\_X(config-line)#exec-timeout 0 20

- Check if the new setting function correctly. Connect with putty SSH and wait about 30 seconds

Test the telnet and SSH connection to switch. Use the Windows clock to calculate the elapsed time.  
Save in notepad the real exec time for both connections.

- Change exec-timeout to 1 minute

S\_X(config-line)#exec-timeout 1 0

- Check if the new setting function correctly. Connect with putty SSH and wait about 60 seconds

Test the telnet and SSH connection to switch. Use the Windows clock to calculate the elapsed time.  
Save in notepad the real exec time for both connections.

Remark:  
Usage: exec-timeout minutes [seconds]  
  
Back to default settings  
no exec-timeout  
  
To specify no timeout  
exec-timeout 0 0  
  
Defaults exec timeout  
10 minutes  
  
 If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.  
  
- Back SSH and VTY to the default settings

S\_X(config-line)#no exec-timeout  
S\_X(config-line)#exit  
S\_X(config)#no ip ssh version  
S\_X(config)#no ip ssh time-out  
S\_X(config)#no ip ssh authentication-retries