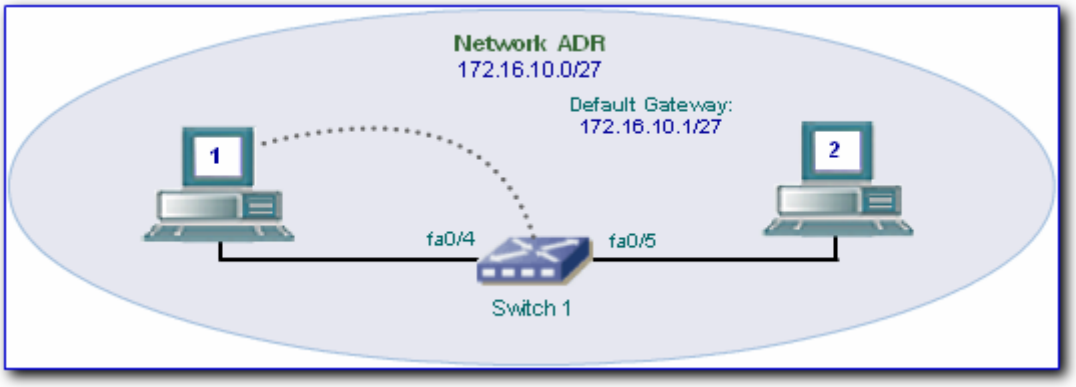
Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

Objectives

- Carry out basic configuration of a switch
- Implement basic security measures, including static MAC addresses and port security
- *Collect portfolio evidence for part of Grading Criteria P3*

Scenario



As a technician for the ADR company, you have been asked to configure a new switch and implement basic security measures. Although you are comfortable with basic switch configuration commands, it has been some time since you set security options. So you have decided to review security related commands by setting up the switch as shown above and reviewing the necessary commands.

Task 1: Document the Configuration

a. Specify the configuration of the switch and the hosts

Using the diagram above for reference, fill in the table below. Some of the detail such as the switch name you may decide for yourself.

	Switch 1
Name	
Enable Secret Password	
VTY and Console Password	
VLAN IP Address and Subnet Mask	
Gateway IP Address and Subnet Mask	

Now decide on and IP address for the hosts and fill the table below. Determine each of your hosts Mac address and add that information to the table.

	IP Address/CIDR	**Default Gateway**	**Mac Address**
Host 1			
Host 2			

Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

Task 2: Configure the Switch and Hosts

You will need to configure the switch as follows:-

- Set the switch name and the enable, console and VTY passwords
- Configure the VLAN management port with an IP address and subnet mask.
- Specify the default gateway IP address and subnet mask.

a. Configure the switch

As a reminder, the various configuration commands are specified below. You will need remember which mode to be in for yourself, e.g. global configuration mode etc.

Delete any existing configuration including the startup configuration and any **`vlan`** database information stored in a **`vlan.dat`** file.

Set the switch's name using the **hostname** command

Set the enable password using the **enable secret** command

Set the line console and vty passwords using the **password** and **login** command

Set the IP address and subnet mask on the VLAN port using the **ip address** command and activate the port using the **no shutdown** command

Specify the default gateway IP address and subnet mask.

b. Configure the hosts

Configure each host with the IP address, subnet mask and default gateway as specified in your documentation.

c. Verify Connectivity

If you have configured the switch and hosts correctly you should be able to ping between the following devices:-

- Ping the Switch from Host 1
- Ping the Switch from Host 2

*Don't forget to save your configuration using the **copy run start** command*

Task 3: Secure Unused Ports

*By default, all port states on a switch are **down** until a live device is attached. Then the port automatically changes state to **up**. You have decided to secure all unused ports on the switch so they are in the state of **administratively down**.*

a. Shutdown unused ports

For each interface except for Ethernet or Fast Ethernet ports 0/4 and 0/5, disable the interface using the **shutdown** command. You will need to go into each interface in turn unless the switch supports the **range** command, e.g.

```
Switch(config)#interface range fa0/1 – 3
```

Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

Task 3: Manage the MAC Address Table

You have decided to review the commands for managing a switch's MAC address table.

a. View and Clear Mac Address Table Information

You have decide to familiarize yourself with the options for the **show mac-address-table** command using the **?** help function. At the privileged EXEC mode prompt try the following:-.

```
Switch#show mac-address-table ?
```

Which option would be useful for viewing dynamic Mac addresses? _____

Which option would be useful for viewing static Mac addresses? _____

Using the appropriate commands determine the following:-

How many total MAC addresses are there? _____

How many dynamic MAC addresses are there? _____

Do the MAC addresses match the host MAC addresses? _____

What is shown if you don't specify any options, e.g. `Switch#show mac-address-table`

_____

You have now decided to familiarize yourself with the options for the **clear mac-address-table** command using the **?** help function. At the privileged EXEC mode prompt try the following:-.

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

Now issue the following command:

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

Using the appropriate command to view the MAC address table, determine the following.

How many dynamic MAC addresses are there now? _____

What do you think might be cleared from the MAC address table if you did not specify any options?

_____

Ping the switch from the hosts a few time. Then view the MAC address table again. Has it changed? If so explain why.

_____

_____

Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

Task 4: Set a Static Mac Address

*As you have now seen, a switch stores in the address table all addresses learned by monitoring traffic. You can also manually configure **static** addresses and bind them to a specific port. Static addresses have the following characteristics:*

- *Static addresses are bound to the assigned interface. They are not removed from the address table if the interface link goes down.*
- *If a static address bound to one interface is seen on another interface, the address will be ignored and will not be written to the address table.*
- *Dynamic entries will be added to static entries for an interface up to the maximum number of entries allowed on that interface.*

*To prepare yourself for configuring the switch to meet the requirements of network ADR, you have decided to experiment with setting **static MAC addresse**s using your two hosts attached to the switch on ports 0/4 and 0/5.*

a. Set a static MAC address on an interface

Setup a static MAC address on the interface 0/4 as follows. **Note**: Use the MAC address that you recorded for Host 1. The address 0000.1111.2222 is used as an example only.

2900:

```
Switch(config)#mac-address-table static 0000.1111.2222 vlan 1
fastethernet 0/4
```

1900:

```
Switch(config)#mac-address-table permanent 0000.1111.2222 ethernet 0/4
```

b. Verify Connectivity

Verify the results using the **show mac-address-table** command

How many MAC addresses are there? Total: _____ Static: _____

You should be able to ping the switch from Host 1. Did your ping succeed? _____

Now connect Host 2 onto Host 1's port 0/4. Can you ping the switch from Host 2? _____

View the address table again using the **show mac-address-table** command. Explain the address table and ping results. Examine the statements at the beginning of this section if you need to.

_____

_____

Now reconnect Host 1 to port 0/4 and Host 2 to port 0/5. Clear any existing *dynamic* entries using the appropriate option with the **clear mac-address-table** command. If you accidentally clear your static entry for interface 0/4 you will have to set the static entry back again.

Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

Task 5: Configure Port Security

Port security can be used to prevent the unauthorized use of a switch by allowing an administrator to specify a list of MAC addresses that can connect to a port. This can be used to stop users connecting unauthorized devices to a network. If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, a security violation occurs if any device with a MAC address not in the secure list attempts to access the port. A violation also occurs if any device with a secure MAC address configured or learned on one secure port attempts to access another secure port.

Port security can be configured in various ways:-

- A secure port can have from 1 to 132 associated secure addresses
- You can configure a secure port by specifying the MAC addresses of devices allowed to connect statically.
- You can allow a secure port to dynamically add MAC addresses until the maximum number of allowed addresses is reached.
- You can specify some addresses statically and allow the rest to be dynamically determined.
- You can set port security so that if the switch sees a MAC address that is not on the secured list, it discards the traffic and takes action such as shutting the port down or sending an alert.

a. Explore port security options

*To prepare yourself for configuring the switch to meet the requirements of network ADR, you have decided to experiment with **port security** using your two hosts attached to the switch on ports 0/4 and 0/5.*

First you need to determine the options for setting port security on an interface. Go into the interface mode for the Ethernet or Fast Ethernet port 0/4. E.g.

```
Switch(config)#interface fa0/4
```

Now familiarize yourself with the options for the port security command using the **?** help function. At the interface mode prompt try the following:-.

2950:

```
Switch(config-if)# switchport port-security ?
```

1900:

```
Switch(config-if)#port secure ?
```

Which option can be used to …

specify the number of addresses allowed on a port? _____

specify static MAC addresses allowed on a port? _____

specify the action to be taken when a security violation is detected? _____

Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

To set a static address on switchport 0/4 to accept a particular device, enter port security commands as follows:

2950:

```
Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address 0000.1111.2222
```

1900:

```
Switch(config-if)#port secure
```

b. Verify port security

Use the **show mac-address-table** command to view the MAC address table entries:

View the port security settings using the following command:-

2950:

```
Switch#show port-security
```

1900:

```
Switch#show mac-address-table security
```

Now view your running configuration. List any statements related to port security.

_____

_____

c. Limit the number of connections

You can specify the maximum number of connections allowed for a port. On interface 0/4 you can set the port security maximum to 1 as follows. First go into the interface mode for the Ethernet or Fast Ethernet port 0/4. E.g.

```
Switch(config)#interface fa0/4
```

2950:

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

1900:

```
Switch(config-if)#port secure max-mac-count 1
```

Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

d. Verify your port security maximum count

Now check that only the Host 1's static address configured on port 0/4 is acceptable to the switch.

Ensure Host 1 is connected to Port 1. Ping the switch from host 1.

Record any observations. _____

_____

Now disconnect Host 1 from port 0/4 and connect Host 2 to the port. Ping the switch from Host 2.

Record any observations. _____

_____

e. Configure shutdown for a security violation

Now you are going to configure the port to shut down if there is a security violation.

First reconnect Host 1 to port 0/4.

In the interface mode for port 0/4, enter the following to set the port security action to shutdown:-

2950:

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

1900:

```
Switch(config-if)#port security action shutdown
```

What other violation action options are available with port security? _____

_____

With Host 1 connected to port 0/4, the interface should be up and running. Check this using the following at the Privileged EXEC mode prompt::

2950:

```
Switch#show interface fastethernet 0/4
```

1900:

```
Switch#show interface ethernet 0/4
```

What is the state of the interface? _____

Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

f. Invoke a security violation

Disconnect Host 1 from port 0/4 and connect Host 2 to the port. Ping the switch from Host 2.

Record any observations. _____

_____

What is the state of the interface? _____

g. Reactivate the port

If a security violation occurs and the port is shut down, you can use the **shutdown** then the **no shutdown** command to reactivate it.

Reconnect Host 1 to port 0/4. Ping the switch from Host 1 a few times to generate traffic.

Record any observations. _____

_____

What is the state of the interface? _____

h. Now remove all previous port security entries

Remove all static entries in the MAC address table and remove port security. In configuration mode you can reverse a command by putting a **no** in front of the old command as follows. (*Don't forget to use your own host's MAC address.*)

2950:

```
Switch(config)#no mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4

Switch(config)#int fa0/4

Switch(config-if)#no switchport port-security mac-address
0000.1111.2222
```

1900:

```
Switch(config)#no mac-address-table permanent 00e0.2917.1884 ethernet
0/4

Switch(config)#int e0/4

Switch(config-if)# no port secure
```

Check you have removed all MAC address and port security configurations by viewing the MAC address table and your running configuration file.

Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

i. Review port security options

Some of the option for port security are:-

```
switchport port-security maximum 1

switchport port-security mac-address aMacAddress

switchport port-security mac-address sticky
```

The options for port security relate to the following types of secure MAC addresses:

Static secure MAC addresses - these are manually configured static addresses that will be stored in the address table and added to the switch's running configuration.

Dynamic secure MAC addresses - these are dynamically configured addresses that will be stored in the address table but will be removed when the switch restarts.

Sticky secure MAC addresses - these are dynamically configured addresses that will be stored in the address table and added to the running configuration. If the running configuration is saved, when the switch restarts, the dynamically learnt addresses are restored.

Hypothesis: **-** Suppose an administrator wishes to configure a switch port so up to 10 addresses are dynamically learned. Which two *port-security* commands should be used?

_____

_____

Hypothesis: **-** Suppose an administrator wishes to configure a switch port with one static address and up to 10 dynamic addresses dynamically learned but will not saved if the switch restarts. Which two *port-security* commands should be used?

_____

_____

Hypothesis: **-** Suppose an administrator wishes to configure a switch port with one static address and up to 10 dynamic addresses dynamically learned that will be saved if the switch restarts. Which three *port-security* commands should be used?

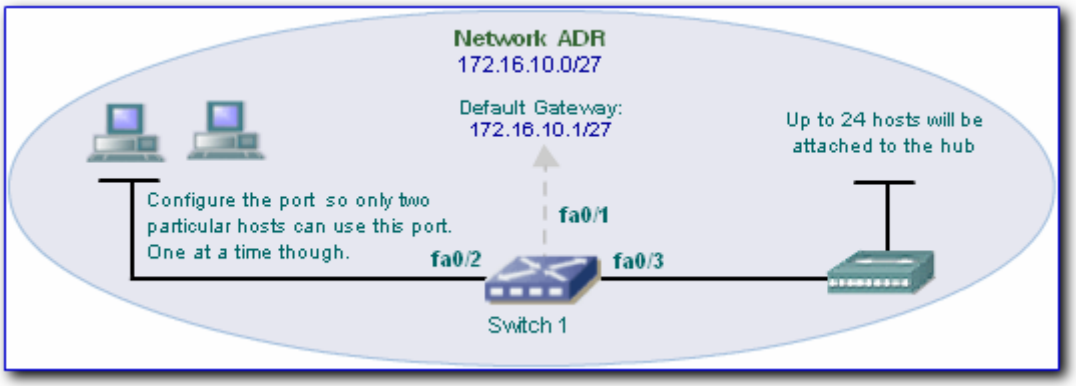
_____

_____

_____

Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

Task 6: Configure the Switch to Meet Requirements



You have now been given the switch to configure for the company as shown above. You have been given a list of security requirements:-

1. Administratively shut down all unused ports
2. Set port 0/2 to accept ONLY the MAC addresses listed below

Port	→	**Mac Addresses of Allowed Devices**
fa0/2 or e0/2	→	00c0.1111.2222 and 00c0.3333.4444

3. Set port 0/3 to accept the following static address and dynamically accept up to 23 other addresses. The dynamic addresses should be restored if the switch ever restarts.

Port	→	**Mac Address of Allowed Device**
fa0/3 or e0/3	→	00c0.5555.6666

4. Set both ports 0/2 and 0/3 to shutdown if a security violation occurs.

You will not need to connect all the hosts and devices to the switch to be able to configure it properly. Just connect a console cable from a single host to say port 0/2 on the switch.

a. Prepare to configure security on the switch

Which command will you use to meet requirement 1?

_____

Which four port security commands will you use to meet requirement 2?

_____

_____

_____

_____

Portfolio Exercise 3b: Switch MAC Address and Port Security Configuration

Which four port security commands will you use to meet requirement 3?

_____

_____

_____

_____

Which command will you use on both port interfaces to meet requirement 4?

_____

b. Configure security on the switch to meet requirements

Using the appropriate commands configure security on the switch to meet all the requirements listed above. *Don't forget to save your configuration using the **copy run start** command*

c. Verify the configuration

When you have finished configuring security on the switch. Examine the running configuration.

Do you feel confident that you have configured the switch correctly? _____

~~A printout of your running configuration is required~~

Examine the MAC address table to see if it contains the correct number of static address entries?

~~Screenshot of your mac address table is required~~

d. Erase the configuration

Clear the switch so it can be used by others. Erase the startup configuration. Reload the switch and view the startup configuration to ensure you have removed your configuration.

~~Printout of cleared startup configuration is required~~

Evidence

Please supply the following evidence to support your implementation of this task

~~Screenshots and configuration files required~~

- Printout of the switch's configuration file, with annotation pointing out parts you specifically configured
- Screenshots showing your **MAC address table**
- Printout showing that you cleared the switch's startup configuration

Please annotate, sign, date, put the portfolio exercise number and task number on all evidence pages