Lecture (07)
Ports Security

Dr. Ahmed M. ElShafee

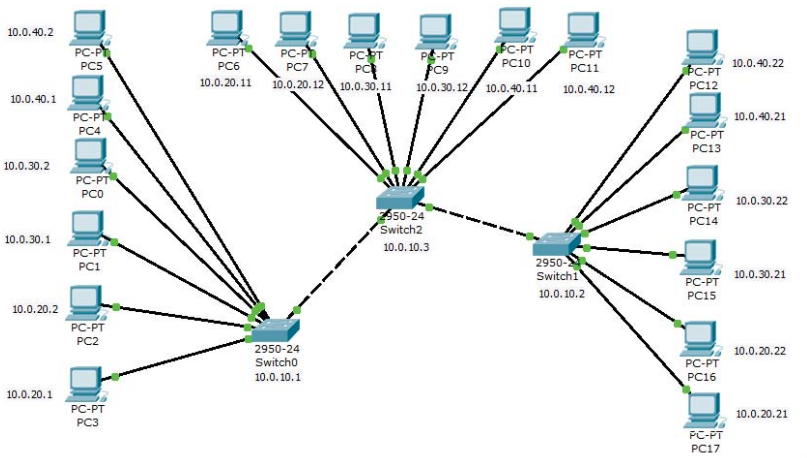
Agenda

- Security

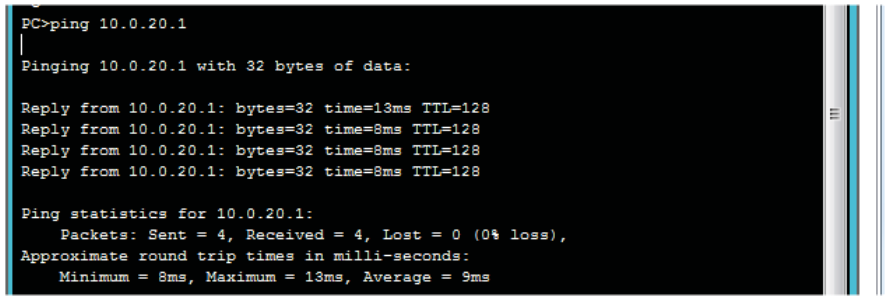
Ports Security

- This IOS feature (switch only) allows you to limit the number of MAC addresses that will be serviced on a given port. It comes with multiple options such as which MAC address(es) is/are going to be allowed on a given port, and what action should be taken when the violation of the policy occurs.
- This way, you can further protect your entry point in the network (access switches).
- By default, the port security is turned off on all interfaces. In order to turn it on, a port **must be in an access mode**.
- Otherwise the command will be rejected.

Security 6.30



- From PC 10.0.20.2 ping 10.0.20.1



- Show mac-address-table
- Show mac-address-table interface fa0/1

```
FL01-R01-SW01#show mac-address-table
        Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  1    000c.cfe6.2718    DYNAMIC     Fa0/24
  2    0001.c747.0835    DYNAMIC     Fa0/2
  2    00e0.f9d2.1239    DYNAMIC     Fa0/1
FL01-R01-SW01#show mac-address-table interface fa0/1
        Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  2    00e0.f9d2.1239    DYNAMIC     Fa0/1
FL01-R01-SW01#
```

- Default port security

```
FL01-R01-SW01#config t
Enter configuration commands, one per line.  End with CNTL/Z.
FL01-R01-SW01(config)#interface fa0/1
FL01-R01-SW01(config-if)#switchport port-security
FL01-R01-SW01(config-if)#end
```

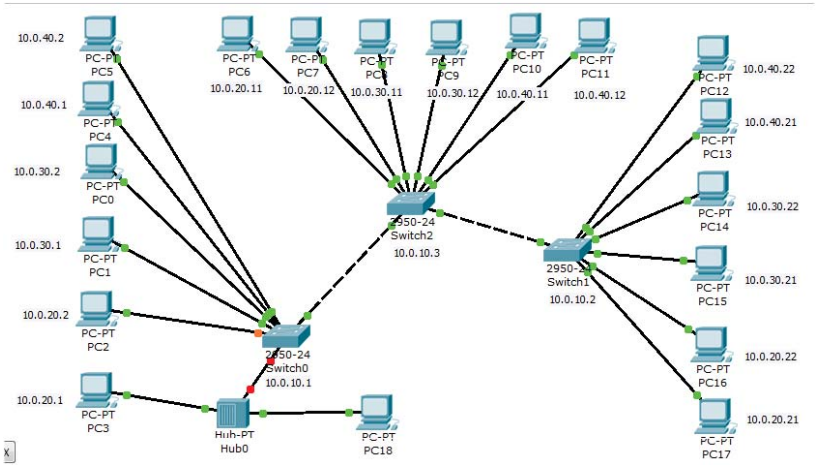

- show

```
FL01-R01-SW01#show port-security
Secure Port        MaxSecureAddr CurrentAddr          SecurityViolation  Security Action
             (Count)       (Count)       (Count)
---------------------------------------------------------------------------
      Fa0/1          1                    0                  0                  Shutdown
---------------------------------------------------------------------------

FL01-R01-SW01#show mac-address-table interface fa0/1
        Mac Address Table
-------------------------------------------

Vlan       Mac Address       Type                Ports
----       -----------       --------             -----

  2        00e0.f9d2.1239    STATIC              Fa0/1
FL01-R01-SW01#
```

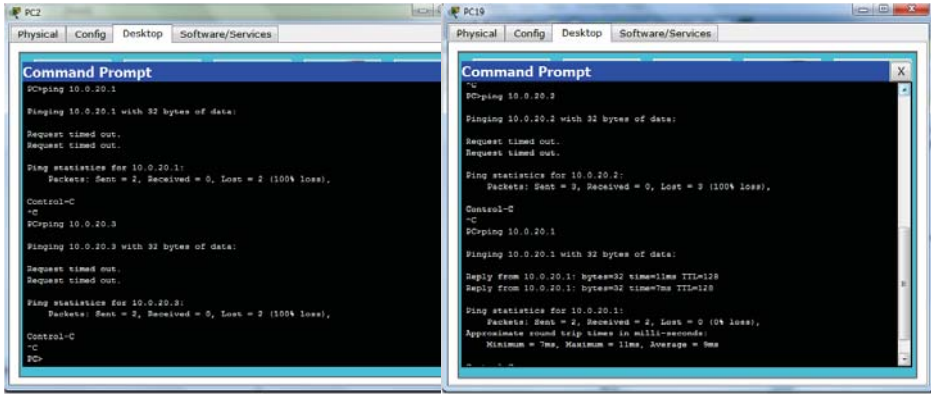
- Swap 10.0.20.1 with 10.0.20.2

```
FL01-R01-SW01#show mac-address-table interface fa0/1
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   2    0001.c747.0835    STATIC      Fa0/1

FL01-R01-SW01#show mac-address-table interface fa0/2
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   2    00e0.f9d2.1239    DYNAMIC     Fa0/2
FL01-R01-SW01#show port-security
Secure Port            MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)       (Count)
---------------------------------------------------------------------------
       Fa0/1               1                     1              0                    Shutdown
---------------------------------------------------------------------------
```

- Connect fa0/1 to two PCs



- Ping 10.0.20.3 & 10.0.20.1 from 10.0.20.2
- Ping 10.0.20.1 & 10.0.20.2 from 10.0.20.3



- Check interfaces

```
FL01-R01-SW01#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/1        unassigned      YES manual down                  down

FastEthernet0/2        unassigned      YES manual up                    up

.......

Vlan1                  10.0.10.1       YES manual up                    up
FL01-R01-SW01#
```

- Assign mac to port

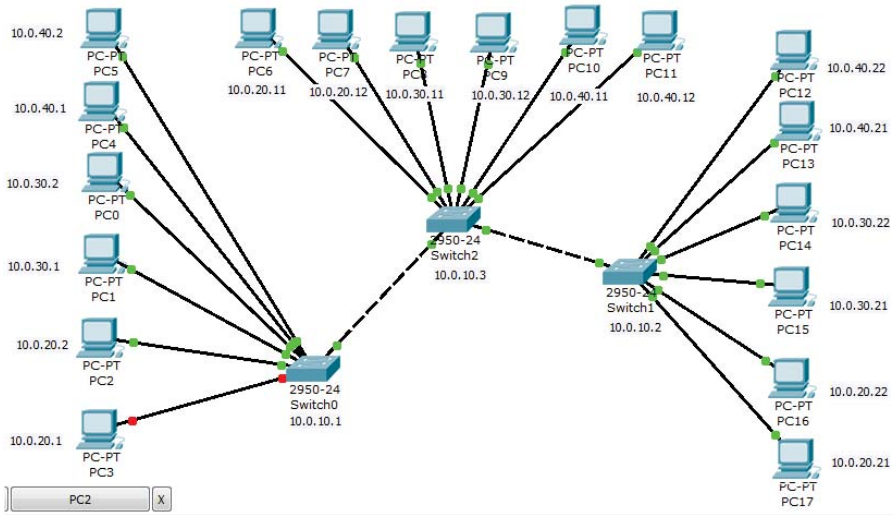
```
FL01-R01-SW01#show mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000c.cfe6.2718    DYNAMIC     Fa0/24
   2    0001.c747.0835    DYNAMIC     Fa0/2
   2    00e0.f9d2.1239    STATIC      Fa0/1
FL01-R01-SW01#config t
Enter configuration commands, one per line.  End with CNTL/Z.
FL01-R01-SW01(config)#interface fa0/1
FL01-R01-SW01(config-if)#sh
FL01-R01-SW01(config-if)#switchport port-security mac-address 0001.c747.0835
FL01-R01-SW01(config-if)#No sh
FL01-R01-SW01(config-if)#end
```


- Show

```
FL01-R01-SW01#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
            (Count)       (Count)        (Count)
---------------------------------------------------------------------------
       Fa0/1        1          1               0         Shutdown
---------------------------------------------------------------------------
FL01-R01-SW01#
```

- From 10.0.20.2 ping 10.0.20.1

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
FL01-R01-SW01#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
            (Count)       (Count)        (Count)
---------------------------------------------------------------------------
       Fa0/1        1          1               1         Shutdown
---------------------------------------------------------------------------
FL01-R01-SW01#
```



- Cancelling security

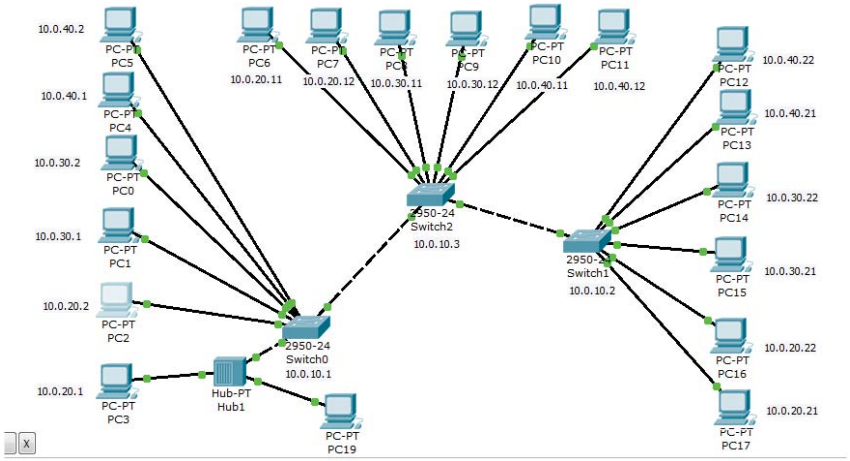
```
FL01-R01-SW01#config t
Enter configuration commands, one per line.  End with CNTL/Z.
FL01-R01-SW01(config)#interface fa0/1
FL01-R01-SW01(config-if)#sh

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
FL01-R01-SW01(config-if)#switchport port-security
FL01-R01-SW01(config-if)#no switchport port-security
FL01-R01-SW01(config-if)#no sh

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

FL01-R01-SW01(config-if)#end
FL01-R01-SW01#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Change violation mode**
- **Protect** - when the port receives the traffic from the MAC addresses which are not configured as secure, it silently drops those transmissions. There is NO notification logged about the violation occurring on a port.
- **Restrict** - similar to 'protect' only the switch logs the violations detected.
- **Shutdown** (default) - the port will transition to err-disable upon detecting the violation.

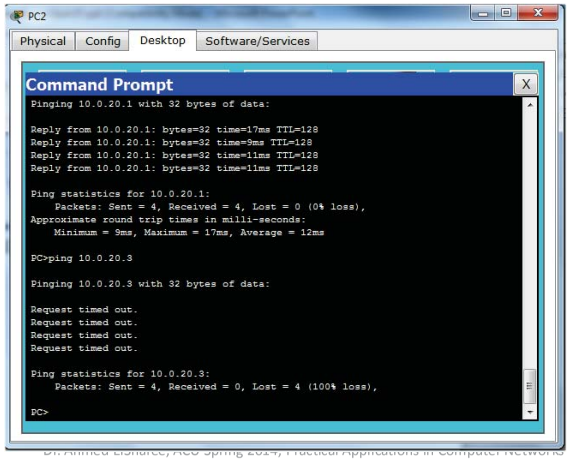
- Change violation to protect, and enable security

```
FL01-R01-SW01#config t
Enter configuration commands, one per line.  End with CNTL/Z.
FL01-R01-SW01(config)#interface fa0/1
FL01-R01-SW01(config-if)#switchport port-security
FL01-R01-SW01(config-if)#switchport port-security violation protect
FL01-R01-SW01(config-if)#end
FL01-R01-SW01#
%SYS-5-CONFIG_I: Configured from console by console
FL01-R01-SW01#
FL01-R01-SW01#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
            (Count)       (Count)       (Count)
---------------------------------------------------------------------
      Fa0/1       1           1              0          Protect
---------------------------------------------------------------------
FL01-R01-SW01#
```

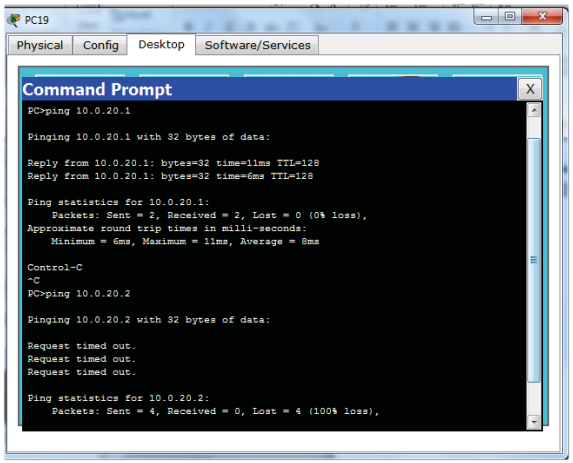
- Connect two PCs to fa0/1



- Ping 10.0.20.1 & 10.0.20.3 from 10.0.20.2



- Ping 10.0.20.1 & 10.0.20.2 from 10.0.20.3



- show

```
FL01-R01-SW01#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000c.cfe6.2718    DYNAMIC     Fa0/24
   2    0001.c747.0835    DYNAMIC     Fa0/2
   2    00e0.f9d2.1239    STATIC      Fa0/1
FL01-R01-SW01#
```


Thanks,..

See you next week (ISA),…