# Lecture (04)

# VTP - Ports Security

**By:**

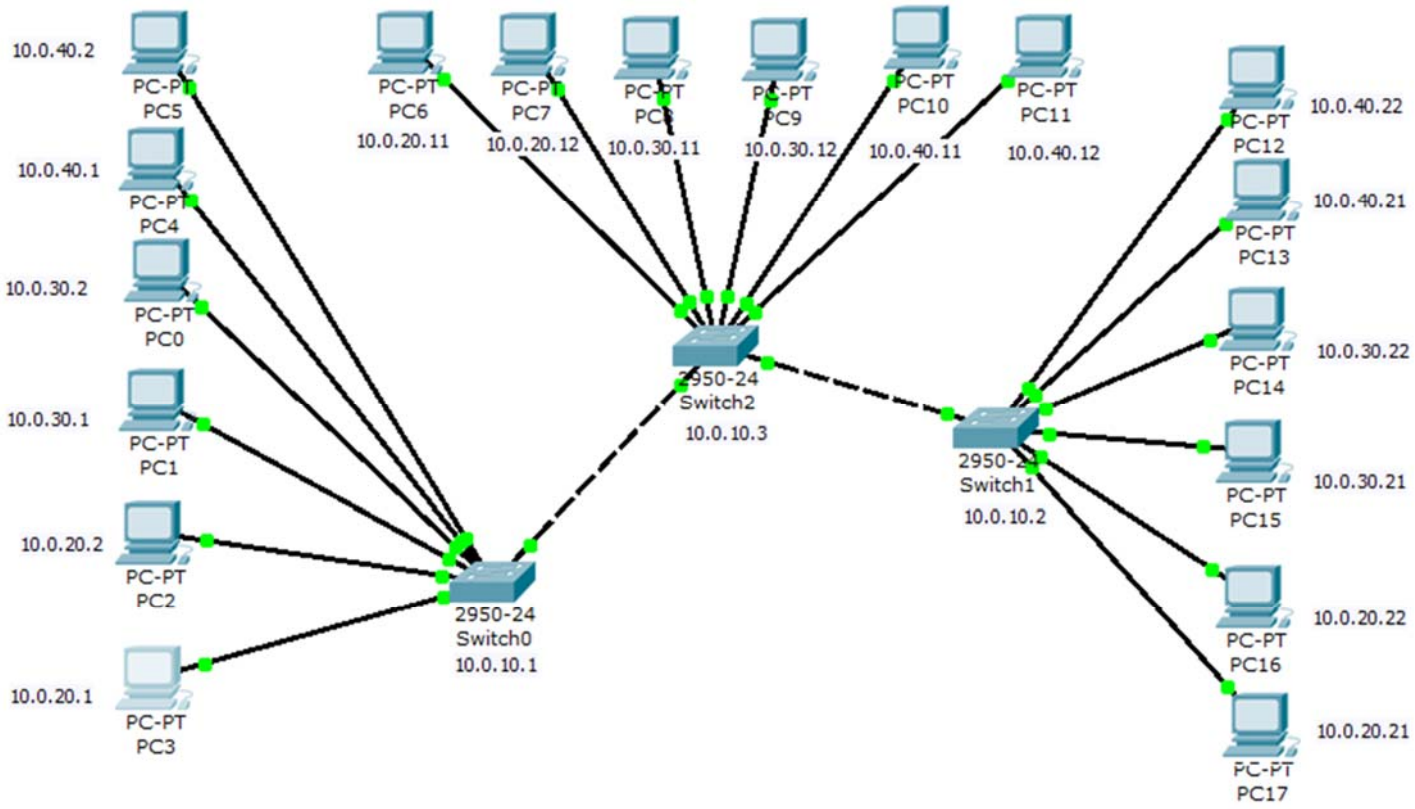
**Dr. Ahmed ElShafee**



## VTP

- VLAN Trucking Protocol (VTP) is a Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks (VLAN) on the whole local area network
- To do this, VTP carries VLAN information to all the switches in a VTP domain.
- VTP advertisements can be sent LAN trunks.
- VTP is available on most of the Cisco Catalyst Family products.
- Their are three versions of vtp, namely version 1 , version 2, version 3.
- The comparable IEEE standard in use by other manufacturers.

# VTP 6.10






```
SW01
****
enabl
config t
hostname FL01-R01-SW01
banner motd #FL01-R01-
SW01 - 10.0.10.1#

line vty 0 4
password cisco
login

line console 0
password cisco
login

enable password cisco

enable secret cisco1

vtp domain ACU
vtp mode server
```

```
interface vlan 1
ip address 10.0.10.1
255.255.255.0
no shutdown

vlan 2
name Finance

vlan 3
name HR

vlan 4
name Administration

interface range fa0/1-24
speed auto
duplex auto

interface range fa0/1-5
switchport mode access
switchport access vlan 2

interface range fa0/6-10
switchport mode access
```

```
switchport access vlan 3

interface range fa0/11-15
switchport mode access
switchport access vlan 4

interface range fa0/23-24
switchport mode trunk

end

copy running-config
startup-config
```

```
SW02
****
enabl
config t
hostname FL01-R02-SW02
banner motd #FL01-R02-
SW02 - 10.0.10.2#

line vty 0 4
password cisco
login

line console 0
password cisco
login

enable password cisco

enable secret cisco1

vtp domain ACU
vtp mode client
```

```
interface vlan 1
ip address 10.0.10.2
255.255.255.0
no shutdown

interface range fa0/1-24
speed auto
duplex auto


interface range fa0/1-5
switchport mode access
switchport access vlan 2

interface range fa0/6-10
switchport mode access
switchport access vlan 3

interface range fa0/11-15
switchport mode access
switchport access vlan 4
```

```
interface fa0/24
switchport mode trunk

interface fa0/23
switchport mode trunk

end

copy running-config
startup-config
```

```
SW03
****
enabl
config t
hostname FL01-R03-SW03
banner motd #FL01-R03-
SW03 - 10.0.10.3#

line vty 0 4
password cisco
login

line console 0
password cisco
login

enable password cisco

enable secret cisco1

vtp domain ACU
vtp mode client
```

```
interface vlan 1
ip address 10.0.10.3
255.255.255.0
no shutdown

interface range fa0/1-24
speed auto
duplex auto


interface range fa0/1-5
switchport mode access
switchport access vlan 2

interface range fa0/6-10
switchport mode access
switchport access vlan 3

interface range fa0/11-15
switchport mode access
switchport access vlan 4
```

```
interface fa0/24
switchport mode trunk

interface fa0/23
switchport mode trunk

end

copy running-config
startup-config
```

Test SW01
**********

FL01-R01-SW01#**show vtp status**
VTP Version : 2
Configuration Revision : 6
Maximum VLANs supported locally : 255
Number of existing VLANs : **8**
VTP Operating Mode : **Server**
VTP Domain Name : **ACU**
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xED 0x01
0xC6 0x30 0xE0 0x1F 0x98 0x2A
Configuration last modified by 10.0.10.1 at 3-1-93 00:32:14
Local updater ID is 10.0.10.1 on interface Vl1 (lowest numbered VLAN interface found)

Test SW02
**********

FL01-R02-SW02#**show vtp status**
VTP Version : 2
Configuration Revision : 6
Maximum VLANs supported locally : 255
Number of existing VLANs : **8**
VTP Operating Mode : **Client**
VTP Domain Name : **ACU**
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xED 0x01
0xC6 0x30 0xE0 0x1F 0x98 0x2A
Configuration last modified by **10.0.10.1** at 3-1-93 00:32:14
FL01-R02-SW02#

Test SW03
**********

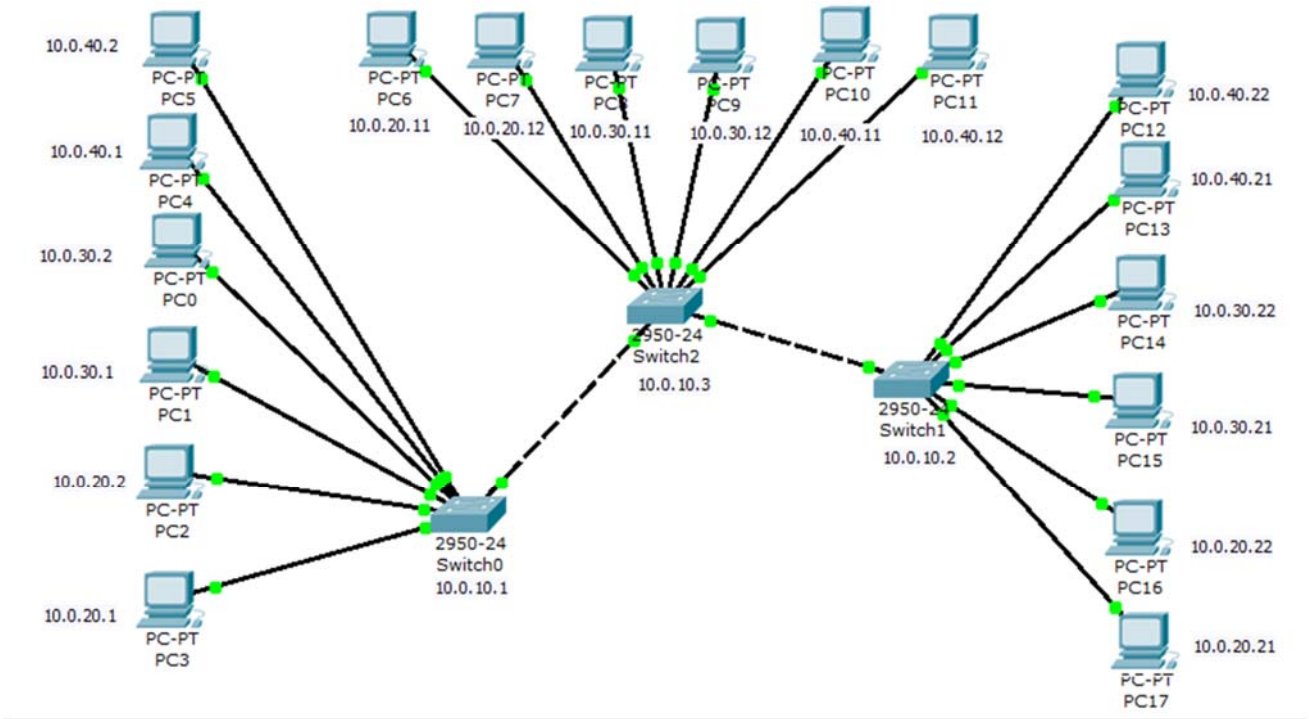
FL01-R03-SW03#show vtp status
VTP Version : 2
Configuration Revision : 6
Maximum VLANs supported locally : 255
Number of existing VLANs : **8**
VTP Operating Mode : **Client**
VTP Domain Name : **ACU**
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xED 0x01
0xC6 0x30 0xE0 0x1F 0x98 0x2A
Configuration last modified by 1**0.0.10.1** at 3-1-93 00:32:14

# 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

```
PC>ping 10.0.20.1

Pinging 10.0.20.1 with 32 bytes of data:

Reply from 10.0.20.1: bytes=32 time=13ms TTL=128
Reply from 10.0.20.1: bytes=32 time=8ms TTL=128
Reply from 10.0.20.1: bytes=32 time=8ms TTL=128
Reply from 10.0.20.1: bytes=32 time=8ms TTL=128

Ping statistics for 10.0.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 13ms, Average = 9ms
```



- 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

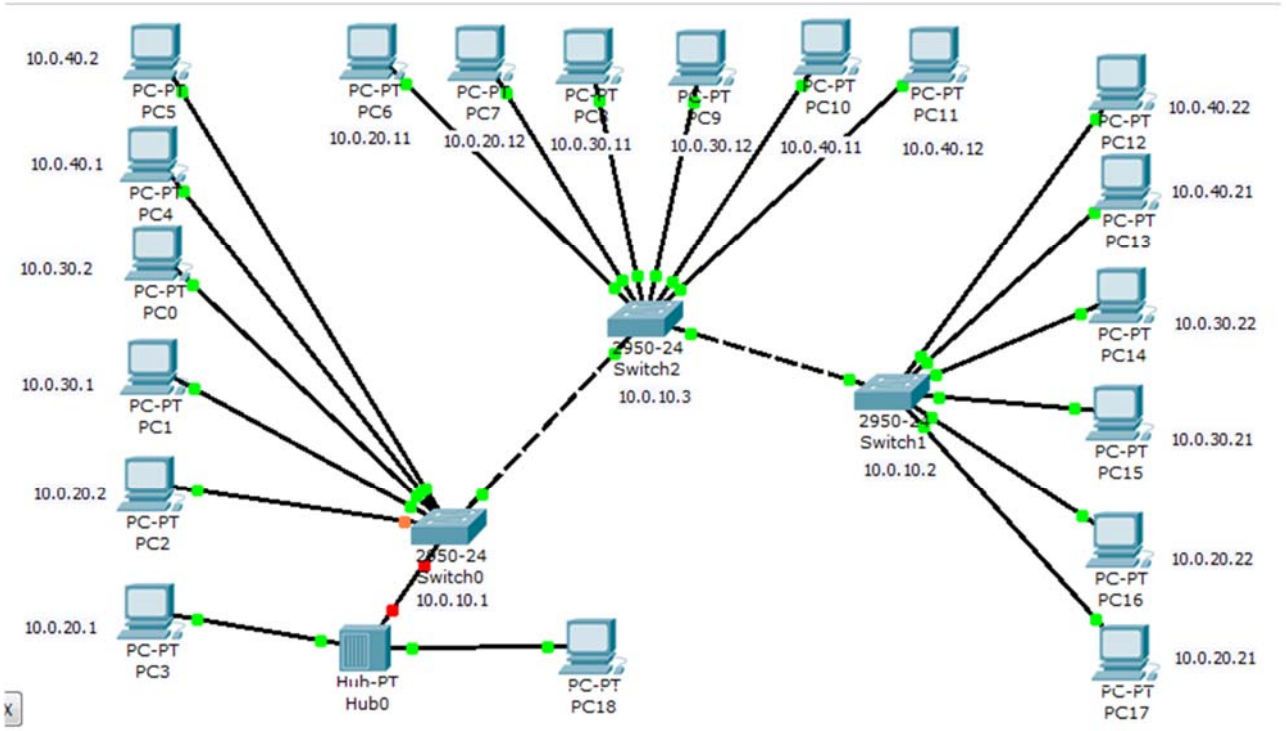
```
FL01-R01-SW01#config t
Enter configuration commands, one per line.  End with CNTL/Z.
FL01-R01-SW01(config)#interface fa0/1
FL01-R01-SW01(config-if)#switchport port-security
FL01-R01-SW01(config-if)#end
```



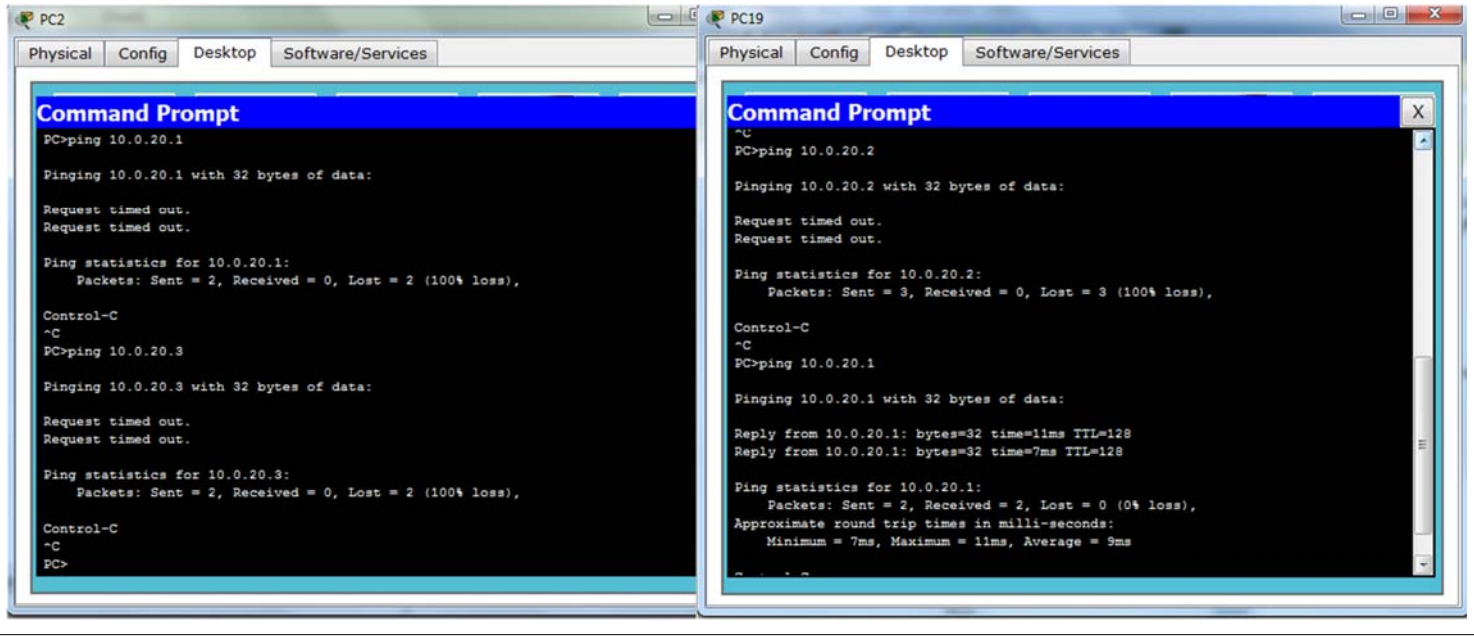
- show

```
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#
```

- 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#
```



- 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
```

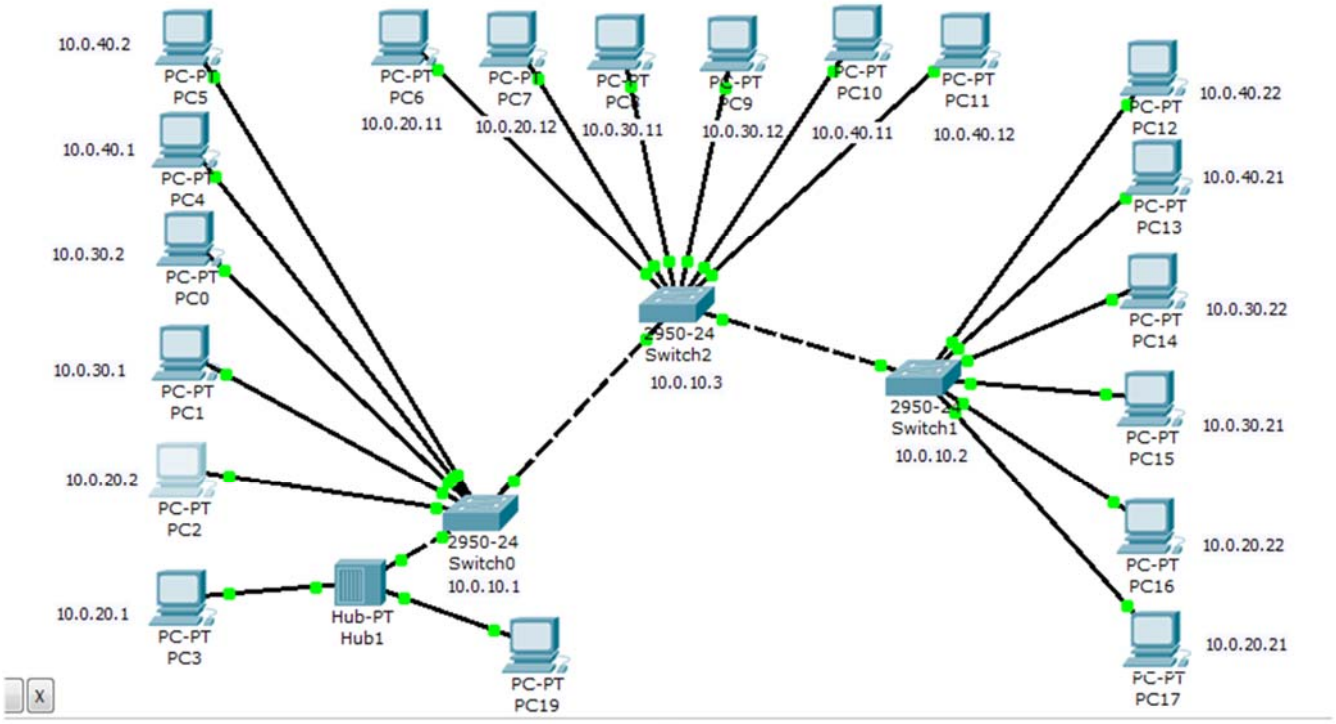
- **Change violation mode**
- **Protect** - when the port receives the traffic from the MAC addresses which are not configured as secure, it silently drops those transmissions. There is NO notification logged about the violation occurring on a port.
- **Restrict** - similar to 'protect' only the switch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



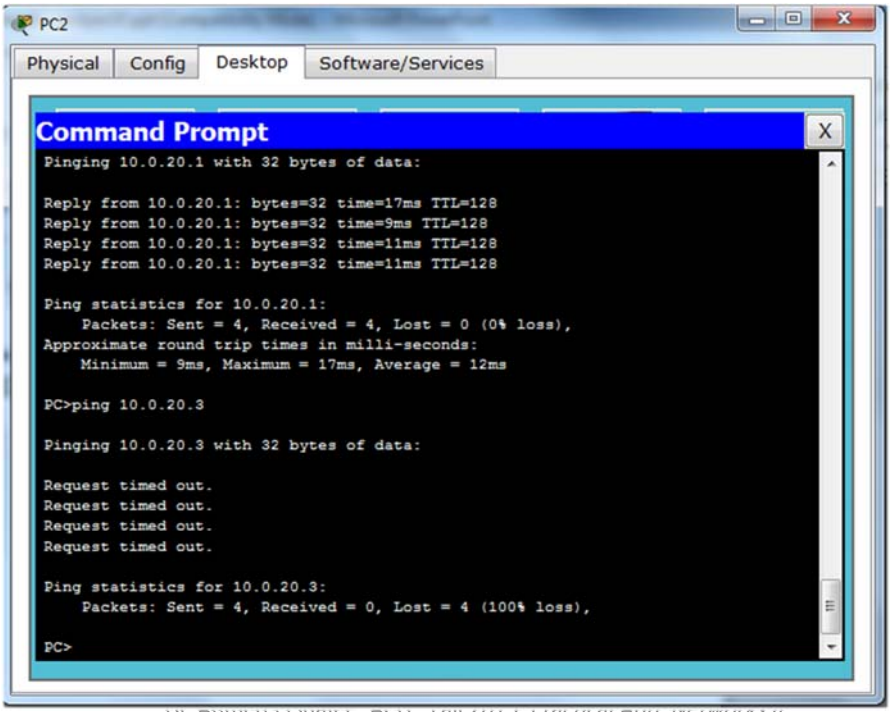
- Change violation to protect, and enable security

```
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#
```

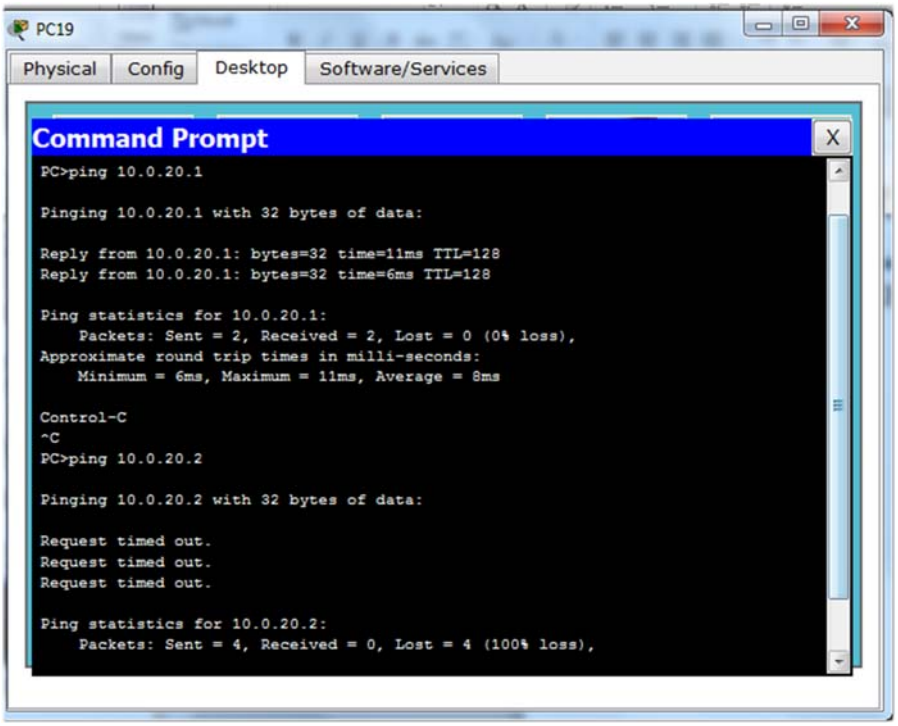
- Connect two PCs to fa0/1




- 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#
```

- 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
```

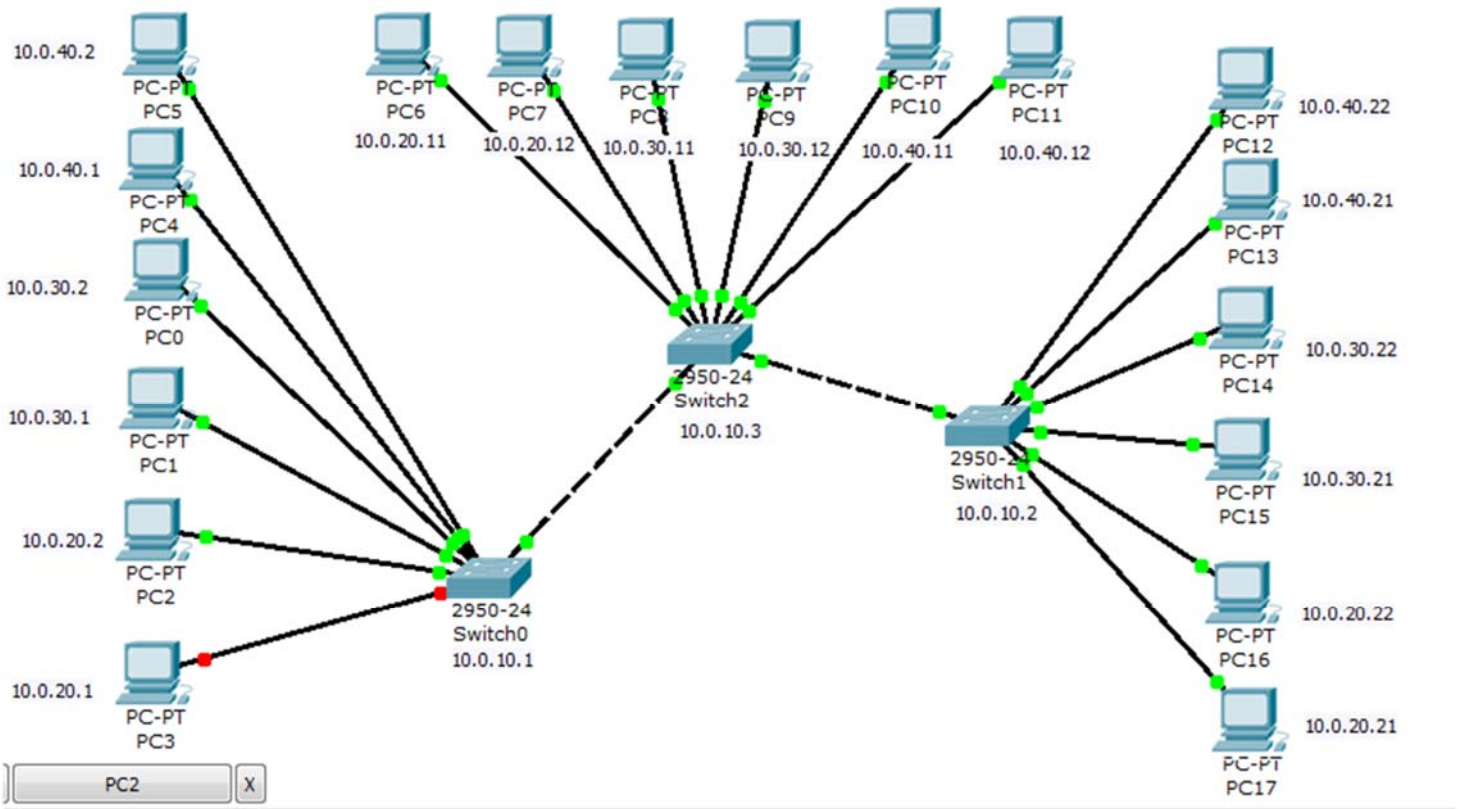


- Show

```
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#
```






# Thanks,..

# See you next week (ISA),…