Port Security

- *Port security is a security feature of Cisco switches.*
- *It allows you to control which source MAC address(es) are allowed to enter the switchport.*
- *If an unauthorized source MAC address enters the port, an action will be taken. The default action is to place the interface in an* **'err-disabled'** *state.*

Port Security Working

- *Port security supports private VLAN (PVLAN) ports.*
- *Port security supports IEEE 802.1Q tunnel ports.*
- *Port security does not support Switch Port Analyzer (SPAN) destination ports.*
- *Port security does not support EtherChannel port-channel interfaces.*

Port Security Types

Port security implements two traffic filtering methods,

Dynamic locking
Static locking

Dynamic locking

You can specify the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform dependent and is given in the software Release Notes. After the limit is reached, additional MAC addresses are not learned. Only frames with an allowable source MAC addresses are forwarded.

Static locking

You can manually specify a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

- *When you enable port security on an interface with the default settings, one MAC address is allowed.*
- *You can configure the allowed MAC address manually.*
- *If you don't configure it manually, the switch will allow the first source MAC address that enters the interface.*
- *You can change the maximum number of MAC addresses*

allowed.

- *A combination of manually configured MAC address and dynamically learned address is possible.*

Violation Modes

There are three different violation modes that determine what the switch will do if an unauthorized frame enters an interface configured with port security.

Shutdown : *When a violation occurs in this mode, the switchport will be taken out of service and placed in the err-disabled state. The switchport will remain in this state until manually removed; this is the default switchport security violation mode.*

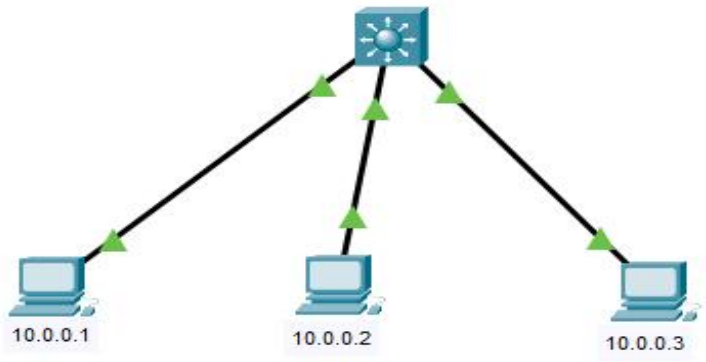
- *Effectively shuts down the port by placing it in an err-disabled state.*
- *Generates a Syslog and/or SNMP message when the interface is disabled.*
- *The violation counter is set to 1 when the interface is disabled.*

Protect: *When a violation occurs in this mode, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses. When using this mode, no notification message is sent when this violation occurs.*

- *The switch discards traffic from unauthorized MAC addresses.*
- *The interface is NOT disabled.*
- *It does NOT generate Syslog/SNMP messages for unauthorized traffic.*

Restrict: *When a violation occurs in this mode, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses. However, unlike the protect violation type, a message is also sent indicating that a violation has occurred.*

- *The switch discards traffic from unauthorized MAC addresses.*
- *The interface is NOT disabled.*
- *Generates a Syslog and/or SNMP message each time an unauthorized MAC is detected.*
- *The violation counter is incremented by 1 for each unauthorized frame.*



*Note:- Before Check MAC Address Table Ping PC IP with each other. Switch#***show mac address-table**

Mac Address Table

Vla Mac Address Type Ports

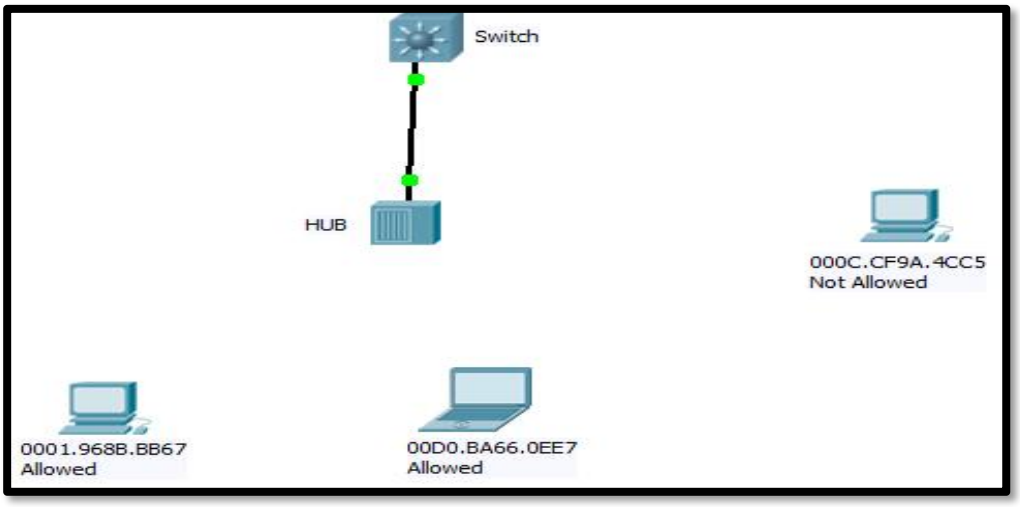
- -
n

- - - - - - - - - - - - -

1	000b.be68.d 274	DYNAM IC	Fa0/ 1
1	000d.bd3d.6 de8	DYNAM IC	Fa0/ 2
1	0050.0f1d.a1 63	DYNAM IC	Fa0/ 3

Switch#

Switch Port Security LAB



Switch(config)#interface f 0/1

Switch(config-if)#switchport mode

access Switch(config-if)#switchport

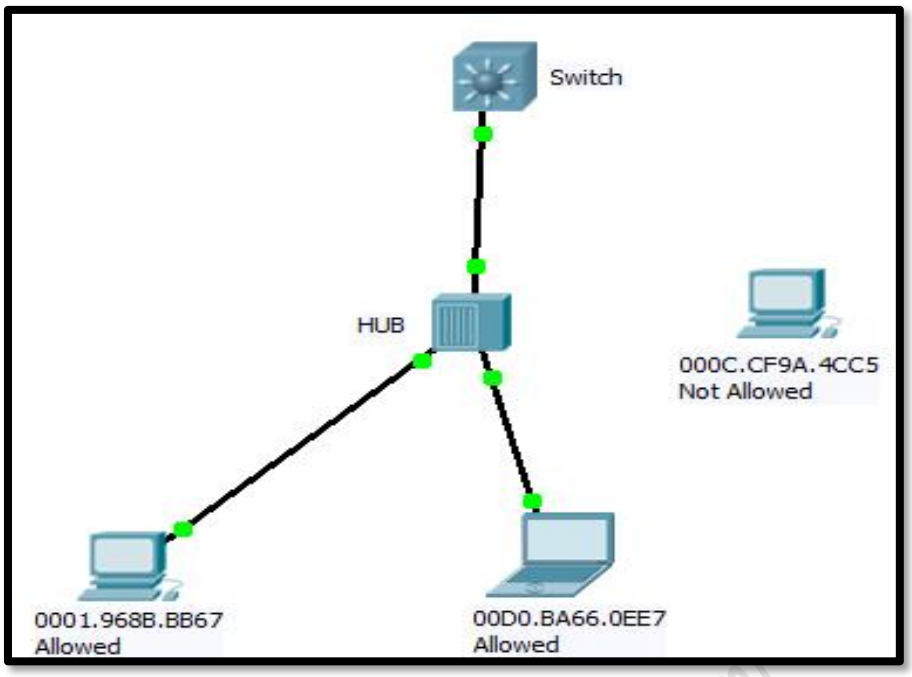
port-security

Switch(config-if)#switchport port-security maximum 2

Switch(config-if)#switchport port-security mac-address 0001.968B.BB67 Switch(config-if)#switchport port-security mac-address 00D0.BA66.0EE7 Switch(config-if)#switchport port-security mac-address 000C.CF9A.4CC5

Total secure mac-addresses on interface FastEthernet0/1 has reached maximum limit.

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



Verification

3560_A#show port-security address

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	0001.968B.BB67	SecureConfigured	Fa0/1	-
1	00D0.BA66.0EE7	SecureConfigured	Fa0/1	-

3560_A#

3560_A#show port-security interface fastEthernet 0/1

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging :

Disabled Maximum MAC

Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses :

2 Sticky MAC Addresses :

0

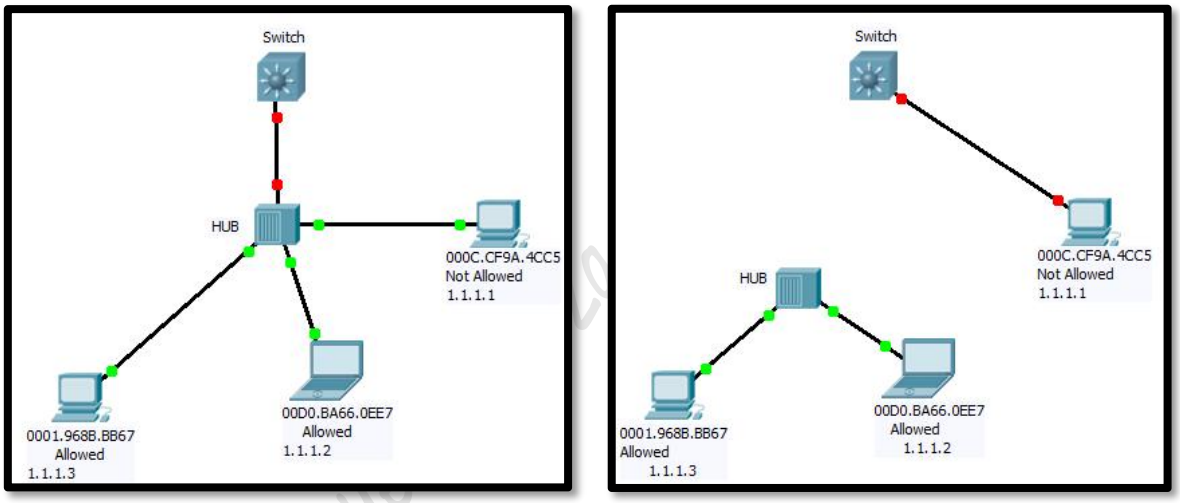
Last Source Address:Vlan :

0000.0000.0000:0 Security Violation Count

: 0

3560_A#

After connecting Not Allowed PC the Port Automatically will shut down.



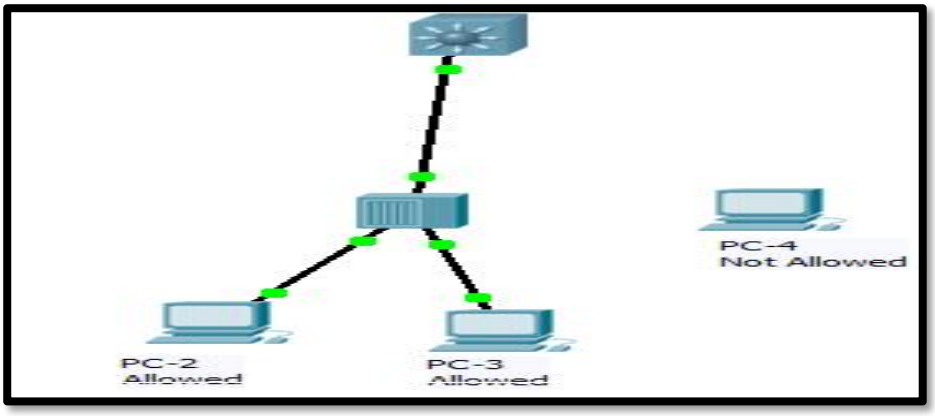
Restoring interface Fast-Ethernet f

0/1 Switch(config)#interface f 0/1

Switch(config-if)#shutdown

Switch(config-if)#no shutdown

Switch(config-if)#exit



Port Security with STICKY MAC-Address with Shutdown

3560_A(config)#int f 0/1

3560_A(config-if)#switchport mode access

3560_A(config-if)#switchport port-security

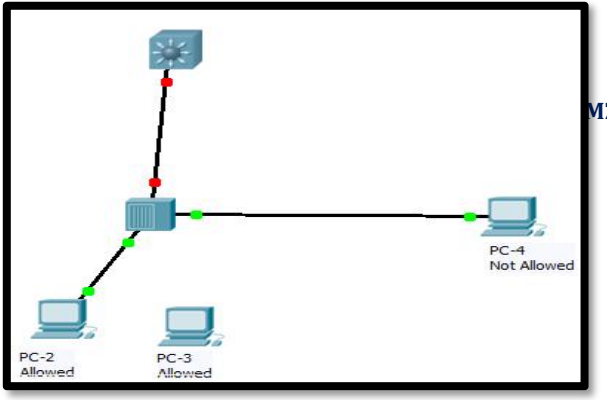
3560_A(config-if)#switchport port-security
maximum 2

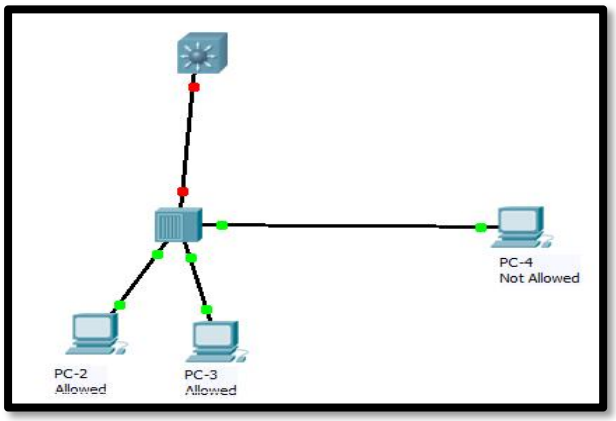
3560_A(config-if)#switchport port-security violation shutdown

3560_A(config-if)#switchport port-security mac sticky

Note: This command converts all dynamic port-security learned MAC addresses to sticky secure MAC address. This command cannot be used on ports where Voice VLANs are configured.

Now, All the devices to be allowed (E.g. PC-2, PC-3), will be attached to the interface 0/1 of Swtich. The MAC- address of these devices will be stored in the NVRAM.





If any device, (E.g. PC-4 having MAC-address other than the devices which were

attached earlier to fa 0/1 (E.g PC-2 & PC-3) is attached to F 0/1 causes this interface to go into err-disable mode.

Restoring interface Fast-Ethernet f

0/1 Switch(config)#interface f 0/1

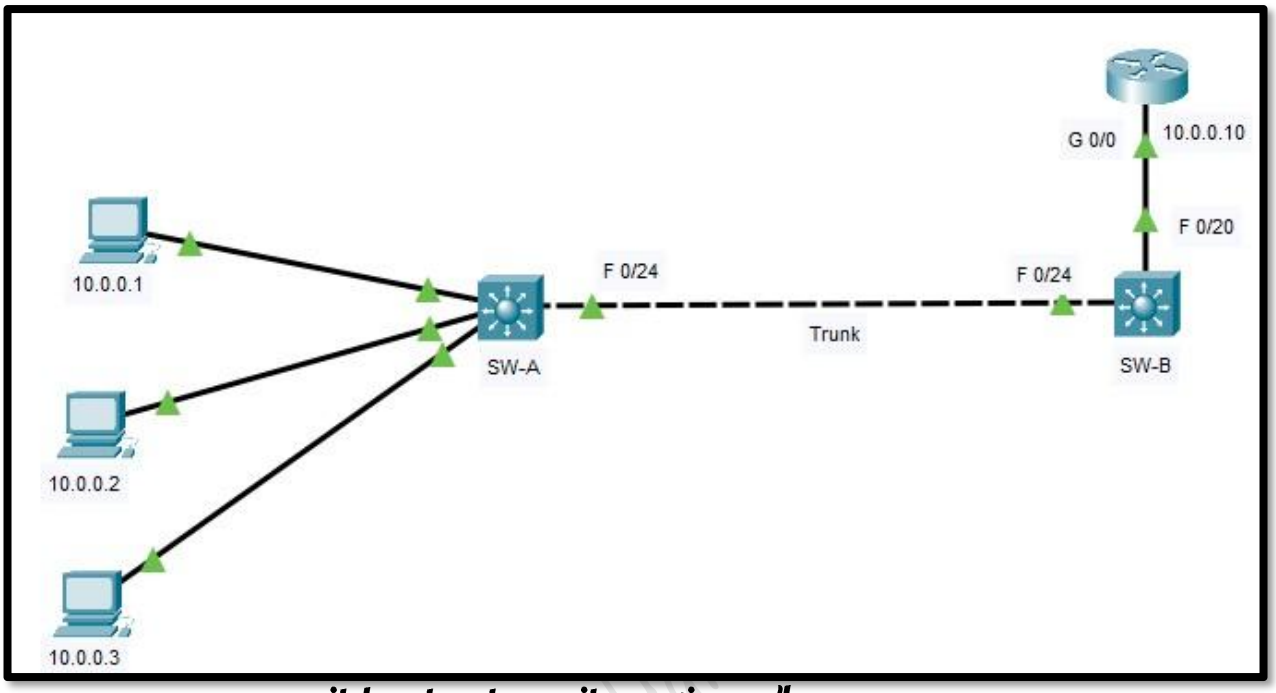
Switch(config-if)#shutdown

Switch(config-if)#no shutdown

Switch(config-if)#exit

LAB

Port Security with STICKY MAC-Address (Protect & restrict Violations)



SW-B(config)#
SW-B(config-if)# SW-B(config-if)# SW-B(config-if)# SW-B(config-if)#

switchport port-security maximum 4
switchport port-security violation Protect
switchport port-security mac sticky

Note: This command converts all dynamic port-security learned MAC addresses to

sticky secure MAC address. This command cannot be used on ports where Voice VLANs are configured.

Now, All the devices to be allowed (E.g. PC-2, PC-3), will be attached to the interface 0/24 of Swtich. The MAC- address of these devices will be stored in the NVRAM.

If any device, (E.g. PC-4 having MAC-address other than the devices which were attached earlier to fa 0/1 (E.g PC-2 & PC-3) is attached to F 0/24 causes this interface to go into err-disable mode.

Note:- Before Check MAC Address Table Ping PC IP with Router.

```
SW-B#show port-security address
Secure Mac Address Table
------------------------------------------

Vlan  Mac Address       Type            Ports      Remaining Age
                                                   (mins)
----  -----------       ----            -----      -------------
1     0001.6381.09E2    SecureSticky    FastEthernet0/24    -
1     0090.0C97.85A4    SecureSticky    FastEthernet0/24    -
1     00D0.972A.1727    SecureSticky    FastEthernet0/24    -
1     0060.7004.8A18    DynamicConfigured FastEthernet0/24  -
------------------------------------------
Total Addresses in System (excluding one mac per port) : 3
Max Addresses limit in System (excluding one mac per port) : 1024
SW-B#

SW-B#show mac address-table
          Mac Address Table
-------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

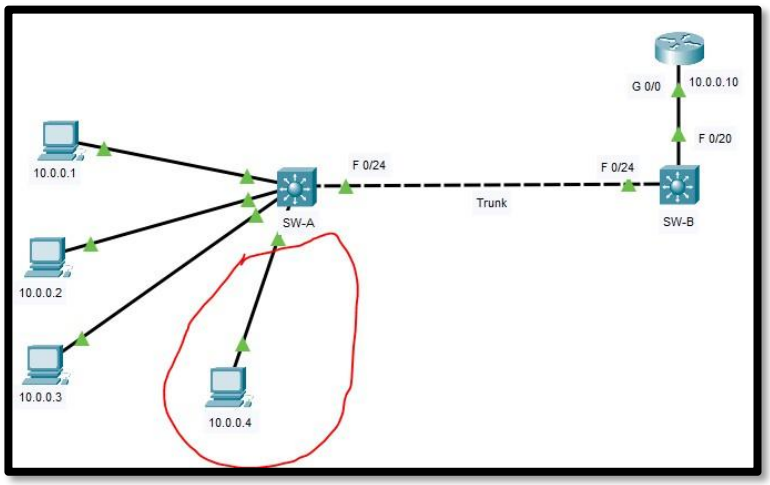
1	0001.6381.09e2	STATIC	Fa0/24
1	0060.7004.8a18	STATIC	Fa0/24
1	0090.0c97.85a4	STATIC	Fa0/24
1	00d0.972a.1727	STATIC	Fa0/24

SW-B#

SW-B# **Show Run**

```
interface FastEthernet0/24
switchport trunk encapsulation
dot1q switchport mode trunk
switchport port-security
switchport port-security maximum 4
switchport port-security mac-
address sticky switchport port-
security violation protect
switchport port-security mac-address sticky
0001.6381.09E2 switchport port-security mac-
address sticky 0090.0C97.85A4 switchport
port-security mac-address sticky
00D0.972A.1727
```

After That All Tree Current PC can Ping with Router, Add one new PC



10.0.0.4 PC will not able to ping with Router IP, but can ping with other PCs. *C:\>ping 10.0.0.10*

Pinging 10.0.0.10 with 32 bytes

of data: Request timed out.

Request timed

out. Request

timed out.

Request timed

out.

Ping statistics for 10.0.0.10:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32

time=1ms TTL=128 Reply from 10.0.0.1: bytes=32 time<1ms TTL=128 Reply from 10.0.0.1: bytes=32 time<1ms TTL=128 Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\>

SW-B# **show port-security interface fastEthernet 0/24**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Protect

Aging Time : 0 mins

Aging Type :

Absolute SecureStatic

Address Aging : Disabled

Maximum MAC Addresses

4

Total MAC Addresses 4

Configured MAC Addresses 0

Sticky MAC Addresses 3

Last Source Address:Vlan: 0060 7004.8A18:1

Security Violation Count0

Just Change the Violation Mode from Protect to Restrict, aS Protect Mode Already Configured.

SW-B(config)#**interface fastEthernet 0/24**

SW-B(config-if)# **switchport port-security violation restrict**

SW-B#

After that Add new PC and Try to Ping from new PC.

Verification

SW-B#**show port- security interface fastEthernet 0/24**

Port Security	*: Enabled*
Port Status	*: Secure-up*
Violation Mode	*: Restrict*
Aging Time	*: 0 mins*
Aging Type	*: Absolute*
SecureStatic Address Aging	*: Disabled*
Maximum MAC Addresses	*: 4*
Total MAC Addresses	*: 4*
Configured MAC Addresses	*: 0*
Sticky MAC Addresses	*: 3*
Last Source Address:Vlan	*: 0060.7004.8A18:1*
Security Violation Count	*: 9*
