SLIIT

Discover Your Future

IT2050 - Computer Networks

Lecture 7

Securing Switched Networks

MAC Address Table

- **Dynamic MAC addresses**
- **Sticky MAC addresses**
- **Permanent MAC addresses**

- Port security limits the number of valid MAC addresses allowed to transmit data through a switch port.
  - If a port has port security enabled and an unknown MAC address sends data, the switch presents a security violation.
  - Default number of secure MAC addresses allowed is 1.

- Methods use to configure MAC addresses within port security:
  - Static secure MAC addresses – manually configure

    switchport port-security mac-address *mac-address*
  - Dynamic secure MAC addresses – dynamically learned and removed if the switch restarts
  - Sticky secure MAC addresses – dynamically learned and added to the running configuration (which can later be saved to the startup-config to permanently retain the MAC addresses)

switchport port-security mac-address sticky *mac-address*

Dynamic MAC Addresses

- MAC addresses are added to the MAC address table through normal switch processing
- When a frame is received, the source MAC of the frame is associated with the incoming port/interface

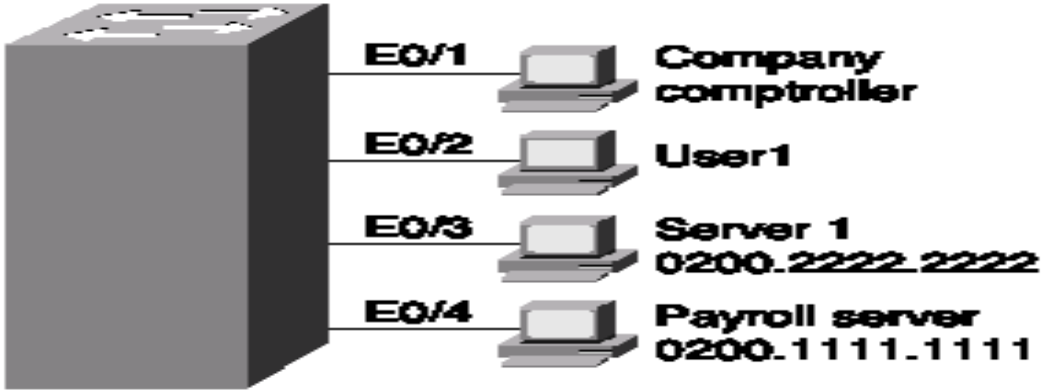
```
wg_sw_a#show mac-address-table
```

```
wg_sw_a#sh mac-address-table
Number of permanent addresses : 0
Number of restricted static addresses : 0
Number of dynamic addresses : 6

Address            Dest     Interface    Type    Source Interface List
-------------------------------------------------------------------
00E0.1E5D.AE2F   Ethernet      0/2     Dynamic        All
00D0.588F.B604   FastEthernet 0/26    Dynamic        All
00E0.1E5D.AE2B   FastEthernet 0/26    Dynamic        All
0090.273B.87A4   FastEthernet 0/26    Dynamic        All
00D0.588F.B600   FastEthernet 0/26    Dynamic        All
00D0.5892.38C4   FastEthernet 0/27    Dynamic        All
```

Permanent MAC addresses

- A MAC address is associated with a port



Switch(config-if)#switchport mode access

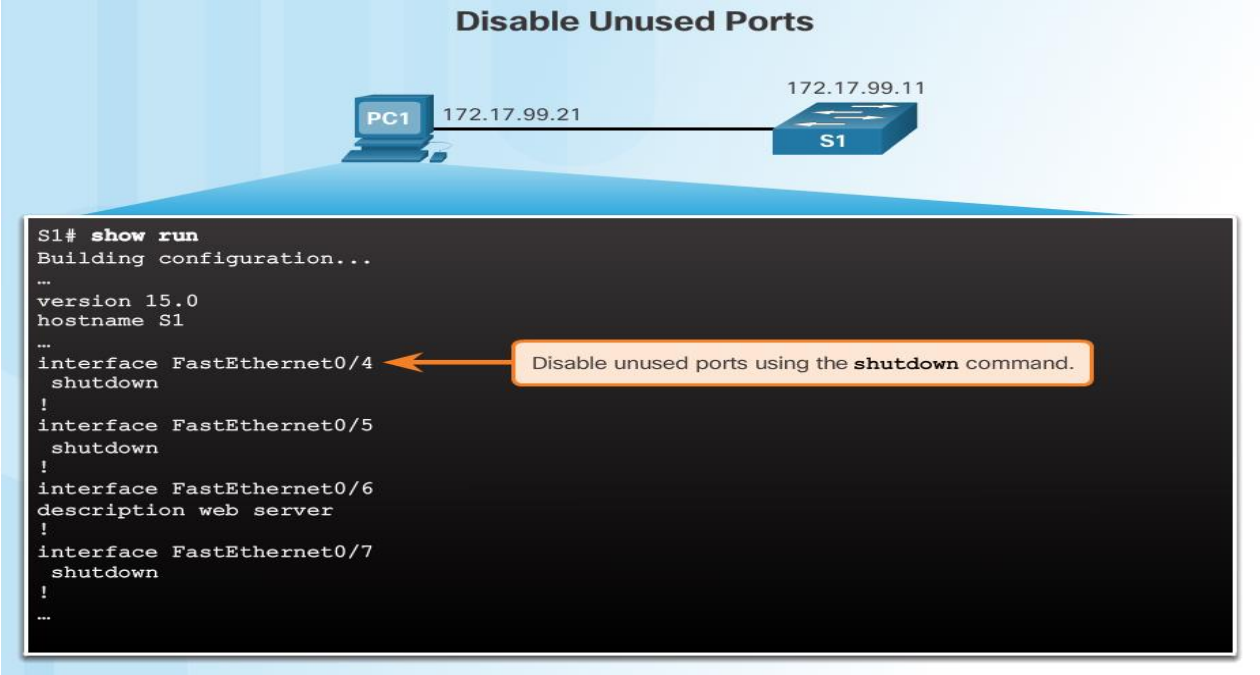
Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address 0200.1111.1111

Switch Port Security

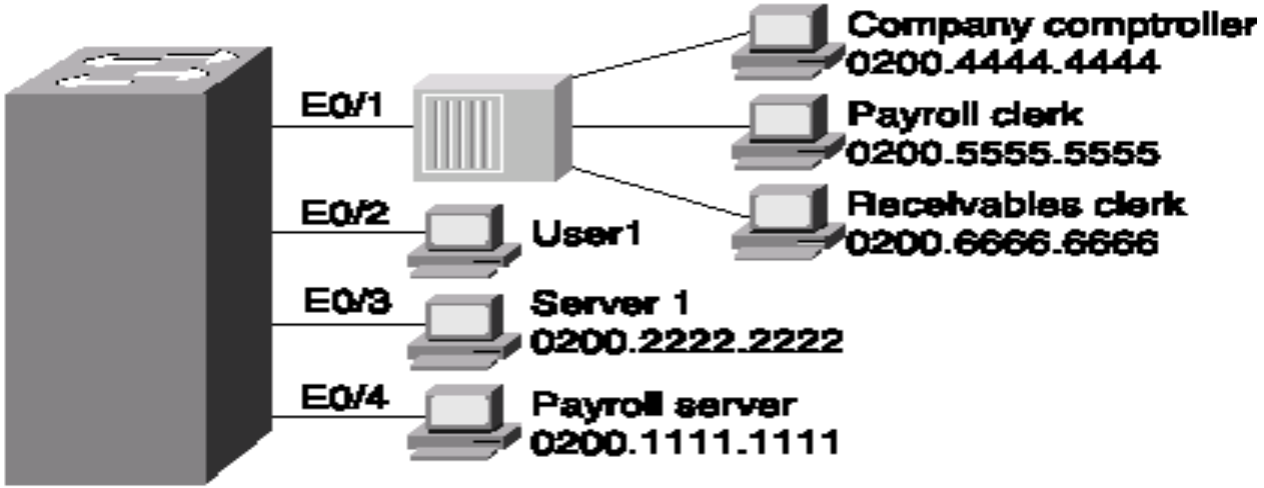
Secure Unused Ports

The **`interface range`** command can be used to apply a configuration to several switch ports at one time.



Port Security

- Limits the number of MAC addresses associated with a port (limits number of sources that can forward frames into that switch port)



Switch(config)#interface <interface name>

Switch(config-if)#switchport port-security maximum <number>

Port Security cont.

- Restrict port 0/1 so that only three MAC addresses can be learned on port 0/1

```
Switch(config)#interface Ethernet 0/1
Switch(config-if)# switchport port-security maximum 3
```

Address violation

- What should the switch do when a fourth MAC address sources a frame that enters E0/1?

An address violation occurs when a secured port receives a frame from a new source address that, if added to the MAC table, would cause the switch to exceed its address table size limit for that port

Port Security: Violation Modes

- **Protect**

– data from unknown source MAC addresses are dropped; a security notification IS NOT presented by the switch

- **Restrict –**

data from unknown source MAC addresses are dropped; a security notification IS presented by the switch and the violation counter increments.

- **Shutdown –**

(default mode) interface becomes error-disabled and port LED turns off. The violation counter increments. Issues the shutdown and then the no shutdown command on the interface to bring it out of the error-disabled state.

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

Security Violations Occur In These Situations

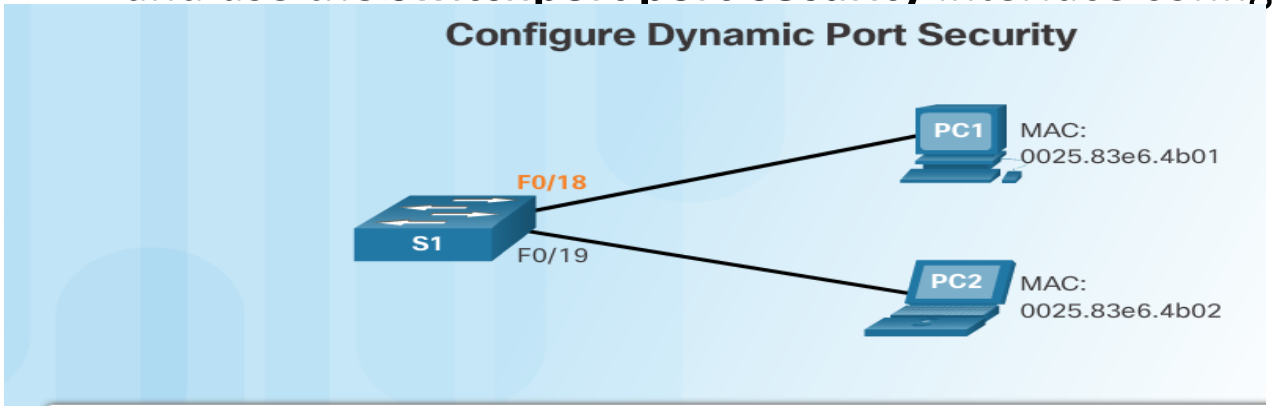
- A station with MAC address that is not in the address table attempts to access the interface when the table is full.
- An address is being used on two secure interfaces in the same VLAN.

Port Security: Configuring

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Sticky address learning	Disabled

Port Security: Configuring (Cont.)

- Before configuring port-security features, place the port in access mode and use the **switchport port-security** interface configuration command



Cisco IOS CLI Commands

Specify the interface to be configured for port security.	`S1(config)# interface fastethernet 0/18`
Set the interface mode to access.	`S1(config-if)# switchport mode access`
Enable port security on the interface.	`S1(config-if)# switchport port-security`

Most common configuration error is to forget this command!

Port Security: Configuring (Cont.)

Configure Sticky Port Security

Cisco IOS CLI Commands

Specify the interface to be configured for port security.	`S1(config)# interface fastethernet 0/19`
Set the interface mode to access.	`S1(config-if)# switchport mode access`
Enable port security on the interface.	`S1(config-if)# switchport port-security`
Set the maximum number of secure addresses allowed on the port.	`S1(config-if)# switchport port-security maximum 10`
Enable sticky learning.	`S1(config-if)# switchport port-security mac-address sticky`

Most common configuration error is to forget this command!

Port Security: Verifying

- Use the **show port-security interface** command to verify the maximum number of MAC addresses allowed on a particular port and how many of those addresses were learned dynamically using sticky.

Dynamic

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
```

Sticky

```
S1# show port-security interface fastethernet 0/19
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 10
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0025.83e6.4b02:1
Security Violation Count   : 0
```