



Operating Cisco LAN switches

Catalyst Switch Devices

Trần Tuấn Toàn



Objective

- Cơ bản về Catalyst Switches
- Mô tả LAN switches
- LAN Switching
- Cấu hình cơ bản Switches
- Tính năng Port Security trên Cisco Switches
- VLAN

Switch & Physical layout



Figure 2-3 Catalyst 2970 Switch Rear Panel



1	RJ-45 console port
2	Fan exhaust
3	AC power connector
4	RPS connector



Catalyst switch: Physical

- Switches:
 - Được thiết kế chuyên dụng
 - Giống như một chiếc máy tính đặc biệt:
 - Central Processing Unit (CPU)
 - Random Access Memory (RAM)
 - Operating System
 - Có thể kết nối qua **console port** để cấu hình
 - Switch thường không có nút Power



LAN Switching

Cisco LAN Switching Basic



Transparent Bridging

- Transparent Bridges:
 - Kết nối 2 hay nhiều Ethernet với nhau
 - “*Transparent*”: thiết bị đầu cuối không biết đến sự tồn tại của bridge(s)
- LAN switches (bridges) phải quyết định chuyển tiếp hay không chuyển tiếp các *Ethernet frames*
 - Quá trình chuyển tiếp dựa trên MAC Addr.



Type of MAC Address

- IEEE định nghĩa 3 loại MAC addr. trên Eth.:
 - Unicast address:
 - Xác định một giao tiếp LAN card duy nhất
 - Broadcast address:
 - Có giá trị FFFF.FFFF.FFFF
 - Tất cả các thiết bị trong LAN đều nhận và xử lý *frame* dữ liệu này
 - Multicast address:
 - Một nhóm các thiết bị trong LAN sẽ nhận và xử lý
- Sự khác nhau giữa 3 loại MAC addr. là cơ sở cho Bridge(s) hay Switch(es) có cách thức chuyển mạch khác nhau

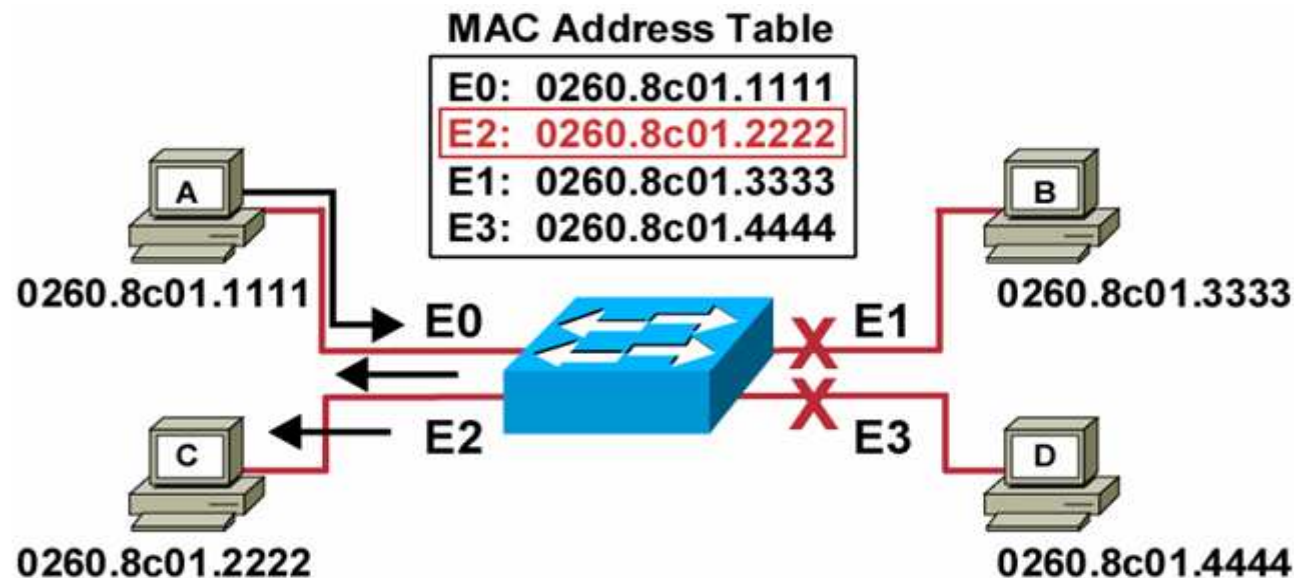


LAN Switches Operation

- Switch lắng nghe các *frames* dữ liệu đi vào từ tất cả các *interfaces*, sau đó quyết định có chuyển tiếp hay không và chuyển đến cổng nào
- Switches (Bridges) thực hiện 3 nhiệm vụ:
 - Learning
 - Forwarding/Filtering
 - Loop prevent

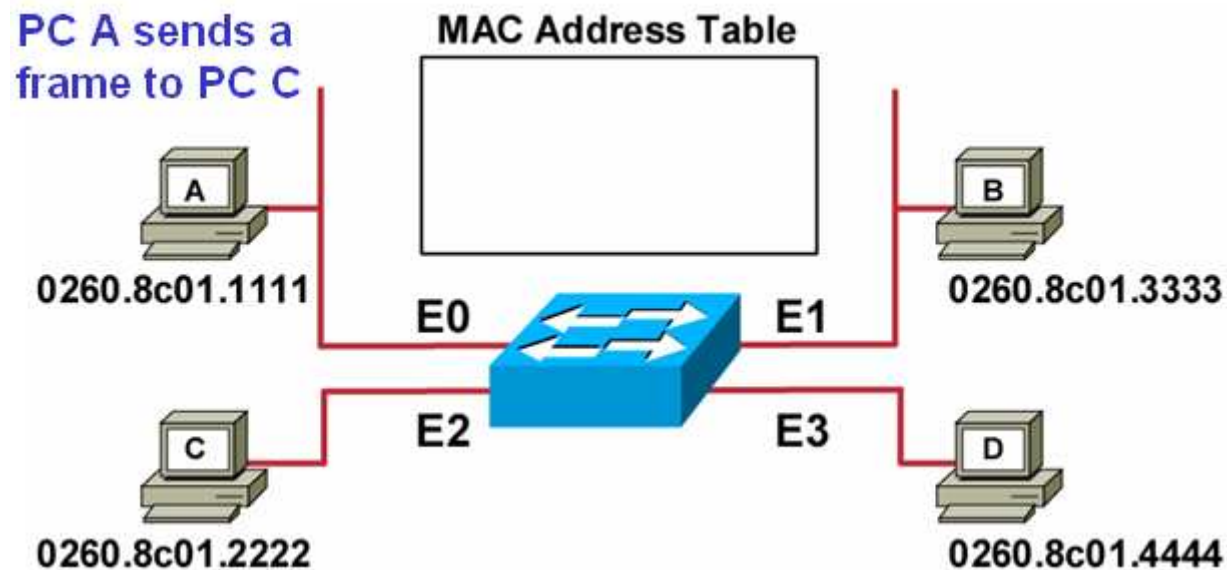
The Forward versus Filter Decision

- Switches sẽ làm giảm sự quá tải trong mạng bằng cách chỉ chuyển tiếp các gói tin từ phân đoạn mạng này sang phân đoạn khác thực sự khi cần thiết
- Để quyết định được Forward / Filter, switches sử dụng:
 - *Bridge table* hoặc *MAC address table*



Learning MAC Addresses (1)

- Switches xây dựng **MAC address table**:
 - Lắng nghe tất cả các frames dữ liệu đến
 - Kiểm tra **frame's source MAC address**

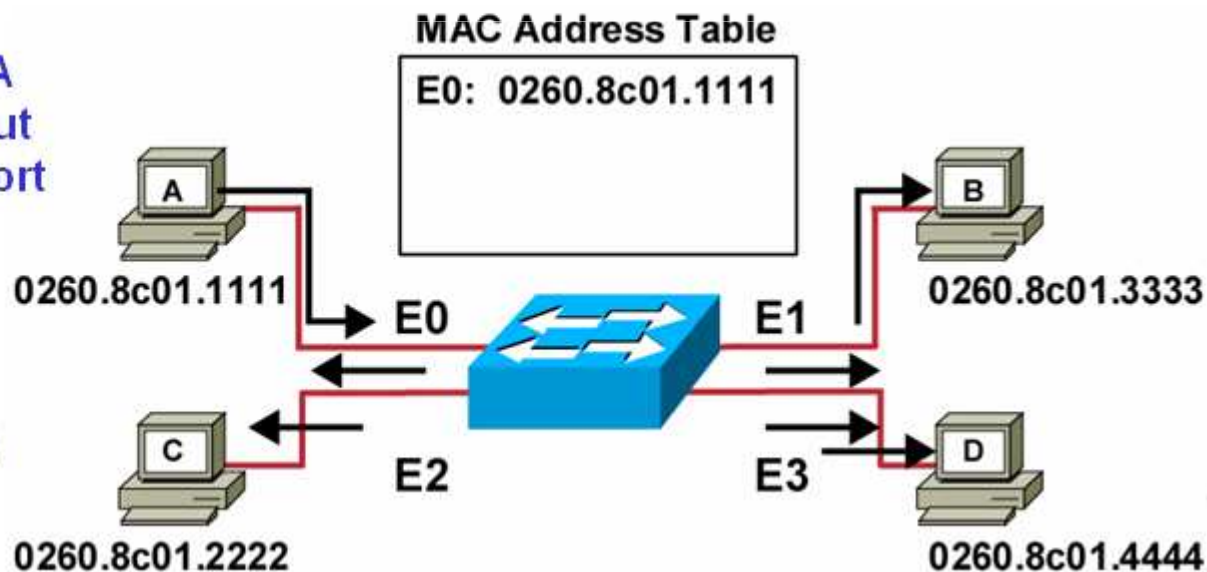


Learning MAC Addresses (2)

- Khi một frame đi đến Switch, nếu **Source MAC addr.** chưa tồn tại trong **M.A.T** \Rightarrow Switch sẽ tạo một entry mới gồm:
 - **Port** mà frame đi vào
 - **Source MAC addr.** của thiết bị đầu cuối

The frame from PC A to PC C is flooded out to all ports except port E0

When PC C replies, the switch can learn PC C's MAC address





The basic Forwarding Logic

1. Một Frame dữ liệu được gửi đến switch
2. Nếu đích là **broadcast** / **multicast**:
 - Switch **chuyển tiếp Frame đến tất cả các Port** trừ Port Source
3. Nếu đích là **unicast** và MAC addr. không nằm trong MAC table:
 - Switch **chuyển tiếp Frame đến tất cả các Port** trừ Port Source
4. Nếu đích là **unicast**, MAC addr. có trong MAC table và interface tương ứng không phải là interface trong Frame được gửi đến:
 - Switch **chuyển tiếp Frame đến đúng một Port cần chuyển**
5. Các trường hợp còn lại:
 - Switch thực hiện **lọc Frame (không chuyển tiếp)**



Basic Configuration

Basic LAN Switch Configuration Guide

Initial bootup Output

```
Cisco C2950

C2950 POST: System Board Test : Passed
C2950 POST: Ethernet Controller Test : Passed
C2950 POST: MII TEST : Passed

cisco WS-C2950-12 (RC32300) processor (revision
B0) with 22260K bytes of memory.
Processor board ID FOC0605W0BH
Last reset from system-reset

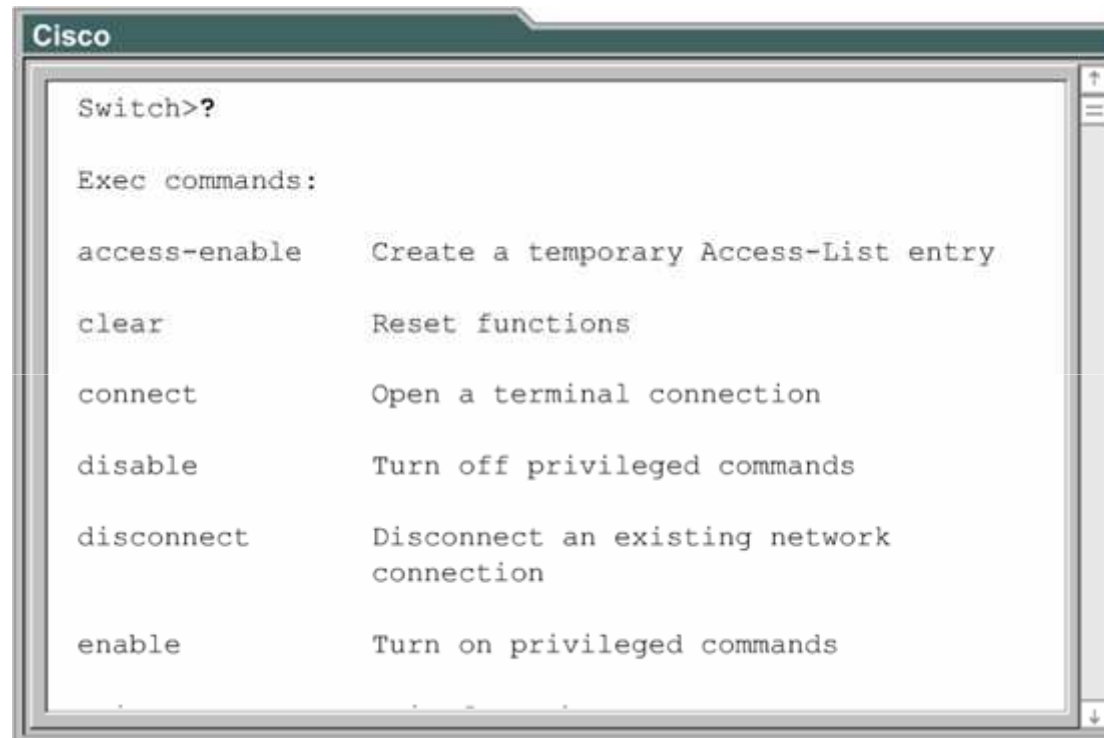
Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
12 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile
configuration memory.
Base ethernet MAC Address: 00:08:E3:2E:E6:00
```

Device with Console



CLI on Switch



```
Cisco
Switch>?
Exec commands:
access-enable    Create a temporary Access-List entry
clear            Reset functions
connect          Open a terminal connection
disable          Turn off privileged commands
disconnect       Disconnect an existing network
                  connection
enable           Turn on privileged commands
```

CLI trên Cisco Switch cơ bản giống CLI trên Cisco Router



Switch command modes

Commands	Description
<code>show version</code>	Gives version information for software and hardware. Used to see exactly which modules and software are in use.
<code>show running-config</code>	Displays the current configuration file of the switch.
<code>show interface</code>	Displays the administrative and operational status of a switching port, packets in/out, and errors.
<code>show interface status</code>	Display the operational mode of the port.
<code>show controllers ethernet-controller</code>	Gives discarded frames, deferred frames, alignment errors, collisions, and so on.
<code>show post</code>	Tells if the switch passed the Power-On Self Test (POST).

enable/disable command
User Mode/Privilege Mode



show running-configure

```
Switch#show running-config
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!<OUTPUT OMITTED>
!
interface VLAN1
  no ip directed-broadcast
```



show interface

```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is down, line protocol is down
  Hardware is Fast Ethernet, address is
0008.e32e.e501 (bia 0008.e32.e.e601)
  MTU 1500 bytes, BW 0 Kbit, DLY 100 usec,
    reliability 255/25, txlead 1/255, rxlead 1/255
  Encapsulation ARPA, Loopback not set
  Keepalive not set
  Auto-duplex, AutoSpeed , 100BaseTX/TX
  ARP type: ARPA, ARP TImeout 04:00:00
  Last Input never, output 00:31:54, output hang
never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  . . . . .
```



show flash

```
Switch#show flash or Switch#dir flash:
Directory of flash:/

 2  -rwx      1674921   Apr 30 2001 15:09:51  c2950-
c3h2s-mz.120-5.3.WC.1.bin
 3  -rwx           269   Jan 01 1970 00:00:57
env_vars
 4  drwx       10240   Apr 30 2001 15:09:52  html

7741440 bytes total (4780544 bytes free)
```



show version

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-C3H2S-M), Version
12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 07:56 by devgoyal
Image text-base: 0x80010000, data-base: 0x8031A000

ROM: Bootstrap program is CALHOUN boot loader

Switch uptime is 1 hour, 24 minutes
System returned to ROM by power-on
System image file is "flash:c2950-c3h2s-mz.120-
5.3.WC.1.bin"
cisco WS-C2950-12 (RC32300) processor (revision B0) with
22260K bytes of memory.
Processor board ID FOC0605W0BH
```



Reset all Configurations & Reload

- Xóa CSDL VLAN
- Xóa bản sao lưu cấu hình startup-config
- Reload Switch

Catalyst 2950

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]?  
Delete flash:vlan.dat? [confirm]  
Switch#erase startup-config  
<output omitted>  
Switch#reload
```

Catalyst 1900

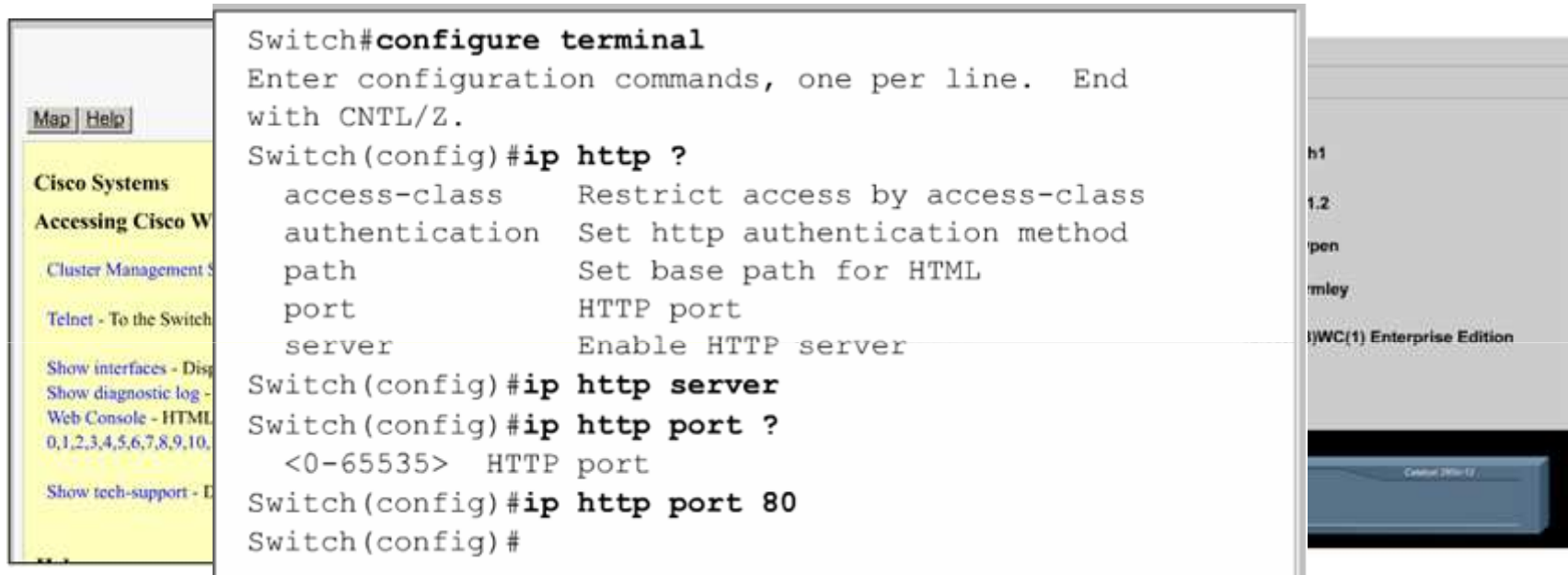
```
Switch#delete nvram
```



Security Remote Control

```
Switch(config)#hostname ALSwitch
ALSwitch(config)#line con 0
ALSwitch(config-line)#password <your-choice>
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 4
ALSwitch(config-line)#password <your-choice>
ALSwitch(config-line)#login
```

HTTP Service & Port



The image shows a Cisco switch configuration terminal window and a web browser interface. The terminal window displays the following commands and output:

```
Switch#configure terminal
Enter configuration commands, one per line.  End
with CNTL/Z.
Switch(config)#ip http ?
    access-class      Restrict access by access-class
    authentication     Set http authentication method
    path               Set base path for HTML
    port               HTTP port
    server              Enable HTTP server
Switch(config)#ip http server
Switch(config)#ip http port ?
    <0-65535> HTTP port
Switch(config)#ip http port 80
Switch(config)#
```

The web browser interface on the left shows the Cisco Systems logo and a list of links: Accessing Cisco W, Cluster Management S, Telnet - To the Switch, Show interfaces - Disp, Show diagnostic log - Web Console - HTML, 0,1,2,3,4,5,6,7,8,9,10, Show tech-support - D. The right side of the image shows a partial view of a web browser window with a search bar and a list of results.

- Sử dụng WebBrowser để có thể truy cập vào Switch qua IP addr. và Port của HTTP Service
- HTTP Service có thể được bật / tắt và lựa chọn Port tùy biến

Managing the MAC address table

```
Switch#show mac-address-table
Dynamic Address Count:          2
Secure Address Count:          0
Static Address (User-defined) Count: 0
System Self Address Count:     13
Total MAC addresses:           15
Maximum MAC addresses:         8192
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination
Port
-----
0010.7a60.ad7e      Dynamic      1     FastEthernet0/2
00e0.2917.1884      Dynamic      1     FastEthernet0/5
```

- Switch **learning** MAC addr. của PC/Workstation theo phương pháp của mình
- PC có thể bị ngắt kết nối tới Switch Port, cũng có thể bị tắt nguồn hay kết nối tới Switch qua một Port khác
 - Có thể gây ra nhầm lẫn trong quá trình chuyển tiếp các Frame
- MAC address sẽ tự động bị loại bỏ hay hết hạn trong khoảng thời gian sau **300 giây**



Managing the MAC address table

```
Switch#clear mac-address-table
Switch#show mac-address-table
Dynamic Address Count:                0
Secure Address Count:                 0
Static Address (User-defined) Count:  0
System Self Address Count:            13
Total MAC addresses:                  14
Maximum MAC addresses:                 8192
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination
Port
-----
```

- Thay vì phải chờ khoảng thời gian một entry trong MAC table hết hiệu lực, người quản trị hoàn toàn có thể xóa bỏ hoàn toàn MAC table:
 - **clear mac-address-table** command



Configure static MAC addresses

- Lý do:
 - MAC addr. Không bị hết hiệu lực tự động bởi Switch
 - Một vài Server / Workstation cần phải kết nối vào một Port nhận biết được
 - Vấn đề Security được nâng cao hơn
- Command:

```
Switch(config)#mac-address-table ?
  aging-time  Set MAC address table entry maximum
age
  secure      Configure a secure address
  static      Configure a static 802.1d static
address
Switch(config)#mac-address-table static
0010.7a60.1884 interface FastEthernet0/5 VLAN1
Switch(config)#no mac-address-table static
0010.7a60.1884 interface FastEthernet0/5 VLAN1
```



Configure Port Security

- Bất kỳ ai cũng có thể cắm PC/Laptop vào các outlet
 - Tạo thêm các điểm cuối không hợp pháp
 - ⇒ Switch cung cấp khả năng Security đến từng Port
- Có thể cấu hình *Static MAC address*, tuy nhiên khi đó việc quản lý sẽ trở nên khá phức tạp
- ⇒ Security MAC address



Security MAC Address

- Một Security Port có thể được cấu hình cho 1→132 MAC address
- Các bước thực hiện Security MAC Address:
 - Step 1: *Lựa chọn Interface cần Security Port*
 - Step 2: **switchport mode access**
 - Step 3: **switchport port-security**
 - Step 4: **switchport port-security maximum** *value*
 - Step 5: **switchport port-security violation** *shutdown*
 - Step 6: **switchport port-security mac-address** *mac-address*
 - Step 7: **switchport port-security mac-address** *sticky*
- Kiểm tra:
 - **show port-security**



Summary

- Catalyst Switches
- Cơ chế hoạt động trong LAN Switches
- Điều khiển/Cấu hình Switches từ xa
- Security Port trên Catalyst Switches ?