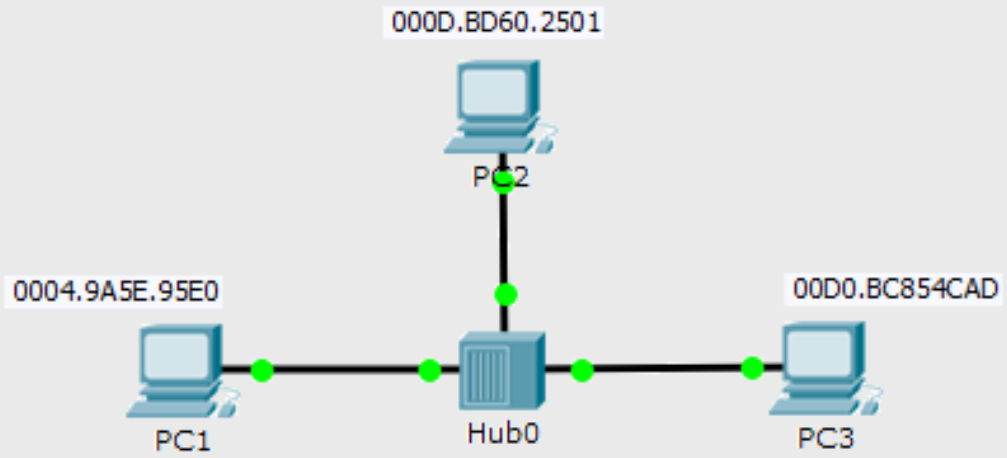
Lab8

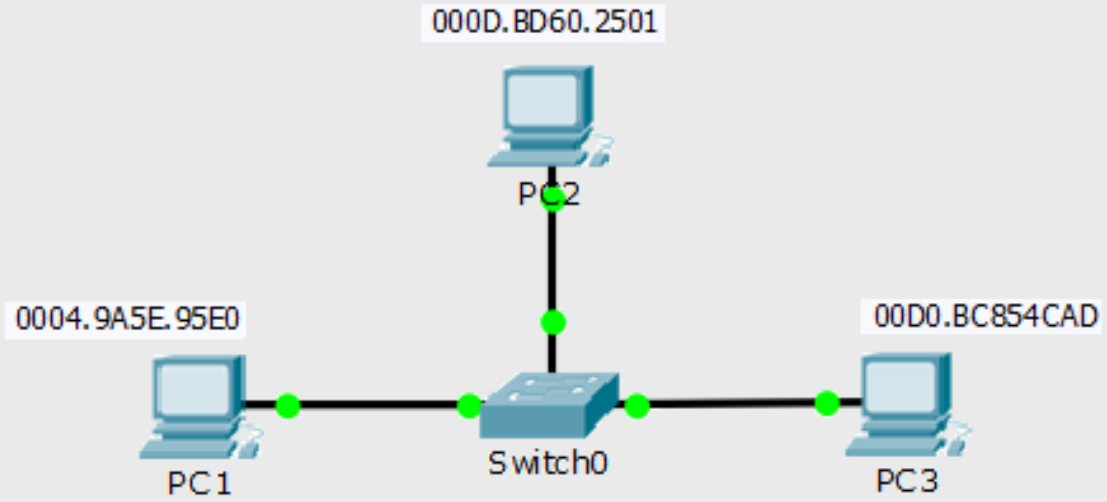
LAN Switching

Basic IOS switch configuration

LAN switching recap



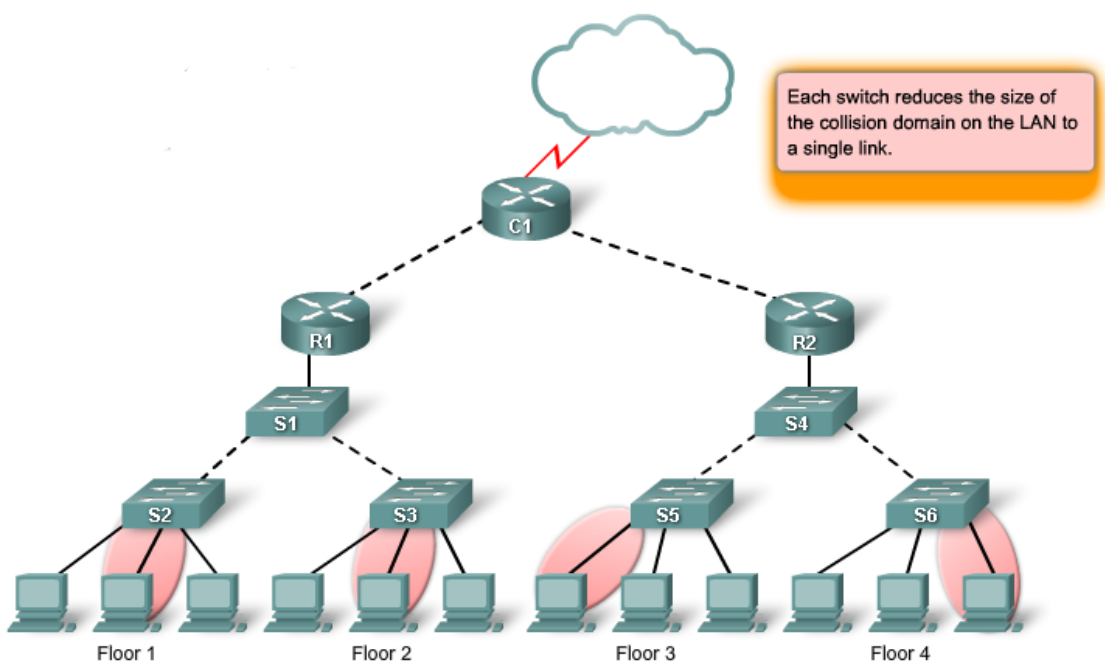
collision domain
=
broadcast domain



collision domain
≠
broadcast domain

LAN switching recap

- Switched Ethernet (transparent bridging)



LAN switching recap

- Ethernet physical layer (Wikipedia)

Ethernet Name	Cable Type	Maximum Speed	Maximum Transmission Distance	Cable Name
100Base-TX	UTP	100Mbps	100 Meters	CAT5, CAT5e, CAT6
1000Base-T	UTP	1000Mbps	100 Meters	CAT5e, CAT6
1000Base-SX	Fiber	1000Mbps	550 Meters	Multimode and Singlemode Fiber
1000Base-LX	Fiber	1000Mbps	550 Mbps MMF, 2000 Meters SMF	Singlemode Fiber
1000Base-ZX	Fiber	1000Mbps	70000 Meters (70 Kilometers)	Singlemode Fiber
10GBase-T	UTP	10Gbps	100 Meters	CAT5e, CAT6
10GBase-SR	Fiber	10Gbps	300 Meters	Multimode Fiber
10GBase-LR	Fiber	10Gbps	10000 Meters (10 Kilometers)	Singlemode Fiber
10GBase-ER	Fiber	10Gbps	40000 Meters (40 Kilometers)	Singlemode Fiber
10GBase-SW	Fiber	10Gbps	300 Meters	Multimode Fiber
10GBase-LW	Fiber	10Gbps	10000 Meters (10 Kilometers)	Singlemode Fiber
10GBase-EW	Fiber	10Gbps	40000 Meters (40 Kilometers)	Singlemode Fiber

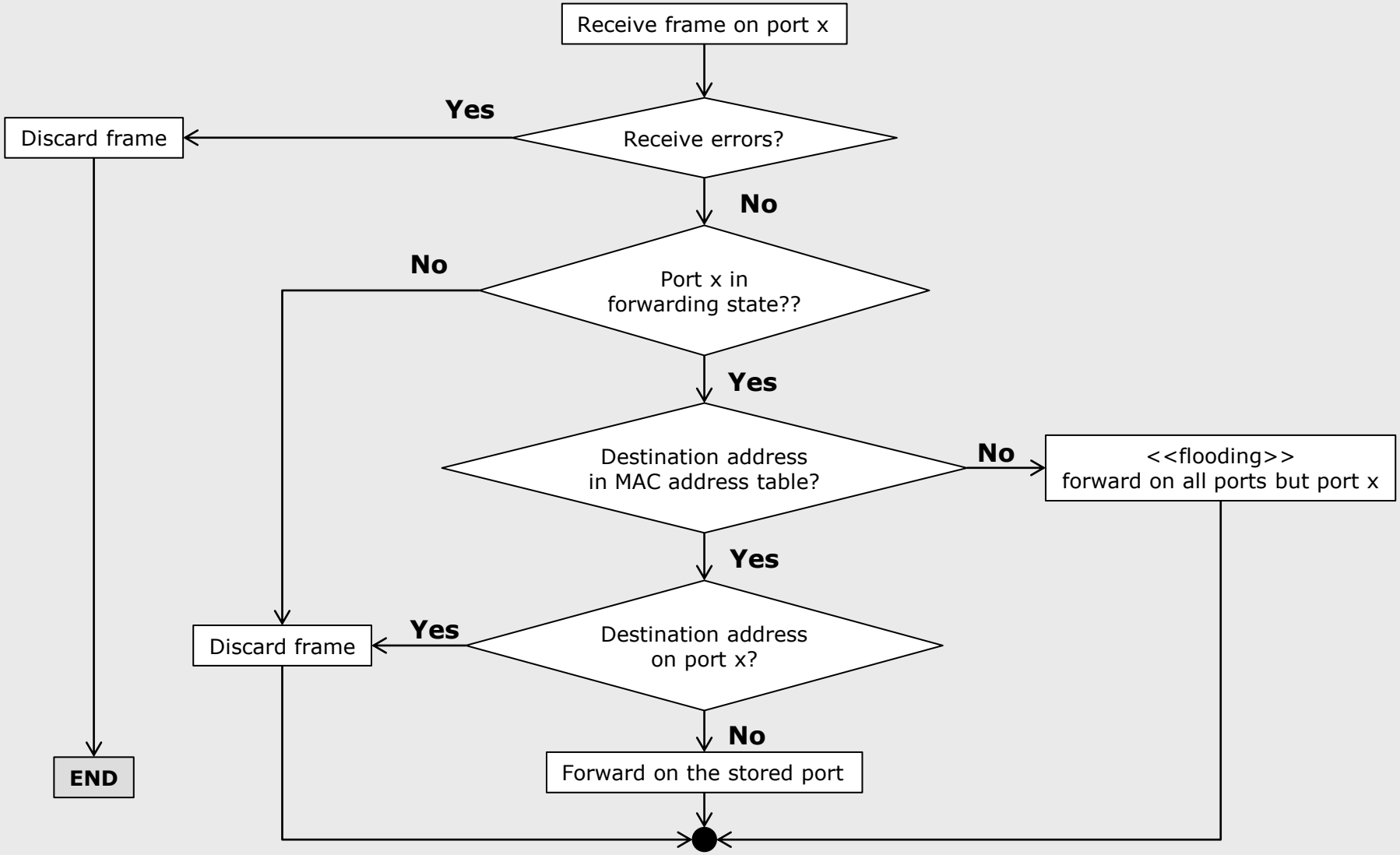
LAN switching recap

- MAC address database
  - Is the forwarding table of the switch
- Entry data
  - MAC address
  - Port id
  - Vlan id
  - Type
    - Static
    - Dynamic
  - Ageing
  - STP state

```
Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c20000d      STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    000c.7671.7534    DYNAMIC     Fa0/2
   1    0013.e809.7695    DYNAMIC     Fa0/2
   1    0017.9a51.d339    DYNAMIC     Fa0/2
   1    0019.5b0a.a951    DYNAMIC     Fa0/2
   1    0060.b0af.7be4    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 25
```

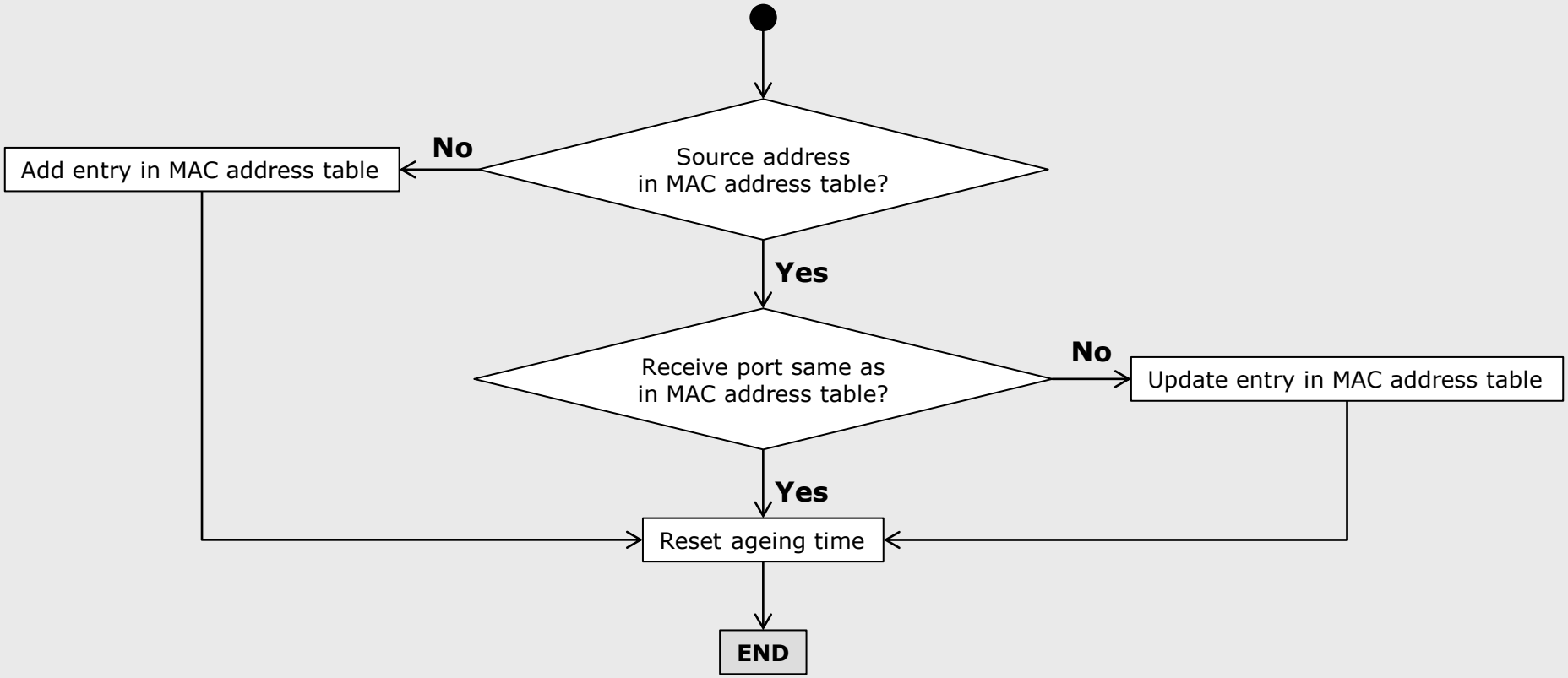
LAN switching recap

- Forwarding process

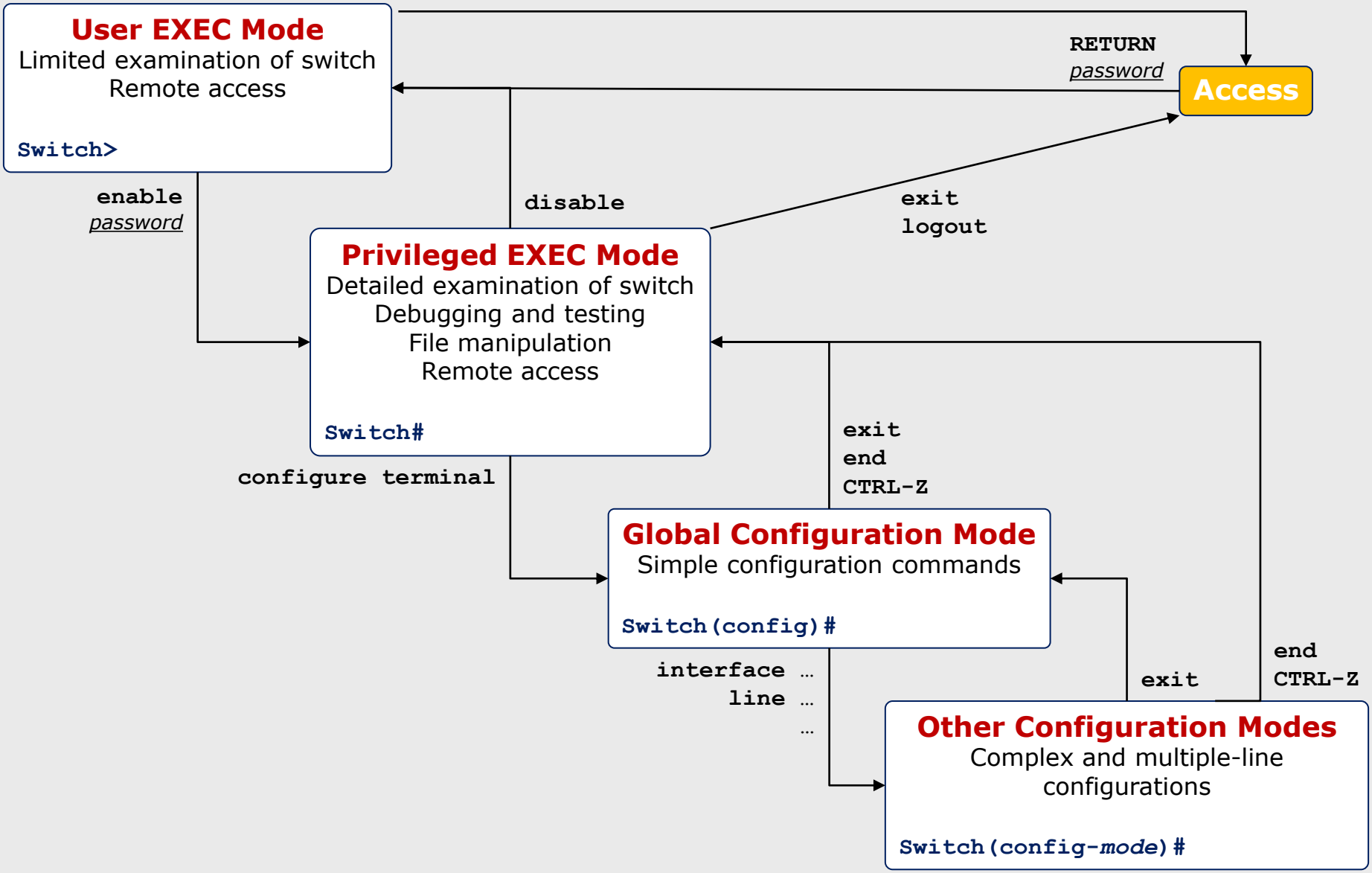


LAN switching recap

- Learning process

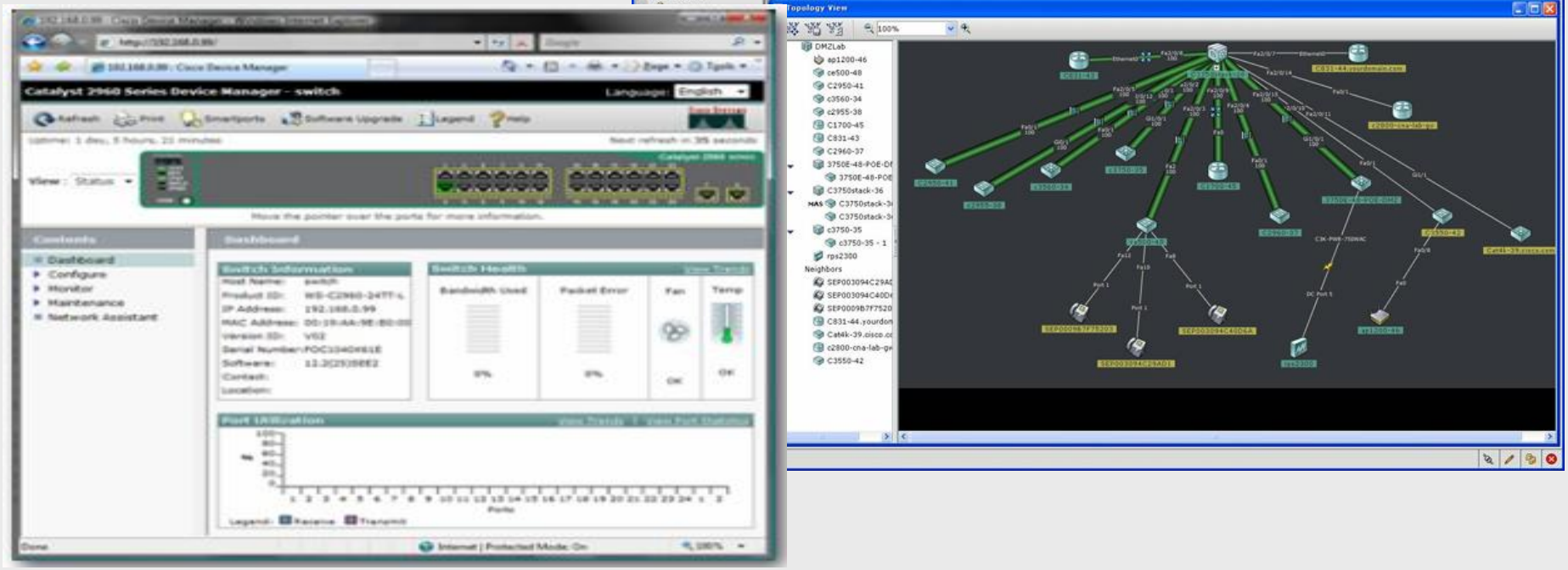


Switch management configuration (IOS)



Switch management configuration (IOS)

- GUI-based alternatives exist (usually require IP reachability)
  - Network Management Applications
    - Cisco Network Assistant
    - Cisco View (SMNP-based)
    - …
  - Web-based device built-in configuration software



Switch management configuration (IOS)

- IOS command structure

- Context-sensitive help

Example of a sequence of commands using the CLI context sensitive help

```
Cisco#cl?
clear  clock
Cisco#clock ?
  set  Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
  hh:mm:ss  Current Time
Cisco#clock set 19:50:00
% Incomplete command.
```

```
Cisco#clock set 19:50:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year
Cisco#clock set 19:50:00 25 6
                            ^
Invalid input detected at '^' marker.
Cisco#clock set 19:50:00 25 June
% Incomplete command.
Cisco#clock set 19:50:00 25 June ?
  <1993-2035>  Year
Cisco#clock set 19:50:00 25 June 2007
Cisco#
```

Command explanations
Incomplete Command messages
Invalid input messages
Variable formats

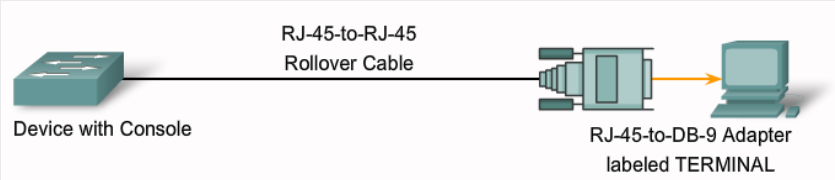
Switch boot-up sequence

- Load the boot-loader from ROM

- Boot-loader
  - Perform low-level CPU initialization
  - Perform POST (Power-On Self-Test)
  - Initialize the flash file system
  - Load a default operating system software image into memory and boots the switch
    - Default rules to locate the Cisco IOS image

- IOS
  - Initialize the switch executing commands

Switch boot-up sequence

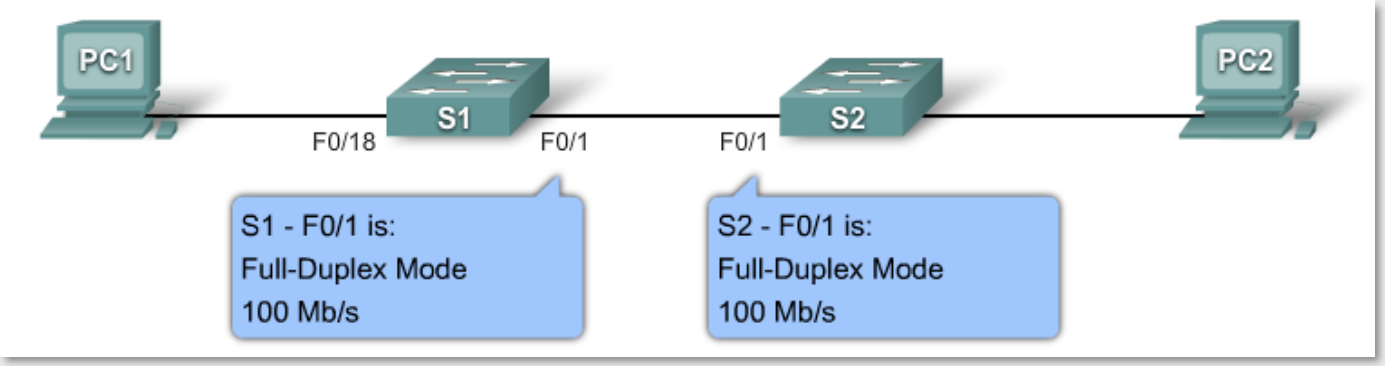



```
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 04:33 by yenanh
Image text-base: 0x00003000, data-base: 0x00AA2F34
flashfs[1]: 602 files, 19 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 32514048
flashfs[1]: Bytes used: 7715328
flashfs[1]: Bytes available: 24798720
flashfs[1]: flashfs fsck took 1 seconds.
flashfs[1]: Initialization complete....don
flashfs.

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC PortASIC interface Loopback Tests : Begin
POST: CPU MIC PortASIC interface Loopback Tests : End, Status
Passed

POST: PortASIC RingLoopback Tests : Begin
POST: PortASIC RingLoopback Tests : End, Status Passed

POST: PortASIC CAM Subsystem Tests : Begin
```

POST ok: SYST LED rapidly blinks green
POST fails: SYST LED turns amber

Basic configuration

- Configure duplex and speed, enable automatic MDI-crossover




```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface Fa0/1
S1(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation
S1(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
S1(config-if)#mdix ?
  auto  Enable automatic MDI crossover detection on this interface
S1(config-if)#end
S1#
```

Basic configuration

- Manage the MAC Address Table

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

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

  99    0003.e4ea.0b02    DYNAMIC     Fa0/5
  99    00d0.baed.1acb    DYNAMIC     Fa0/18
```

- Configure a static MAC address (not aged out)

```
Switch(config)#mac-address-table static mac_address vlan vlan-id interface-id
```

- Modify the default aging time (300 s)

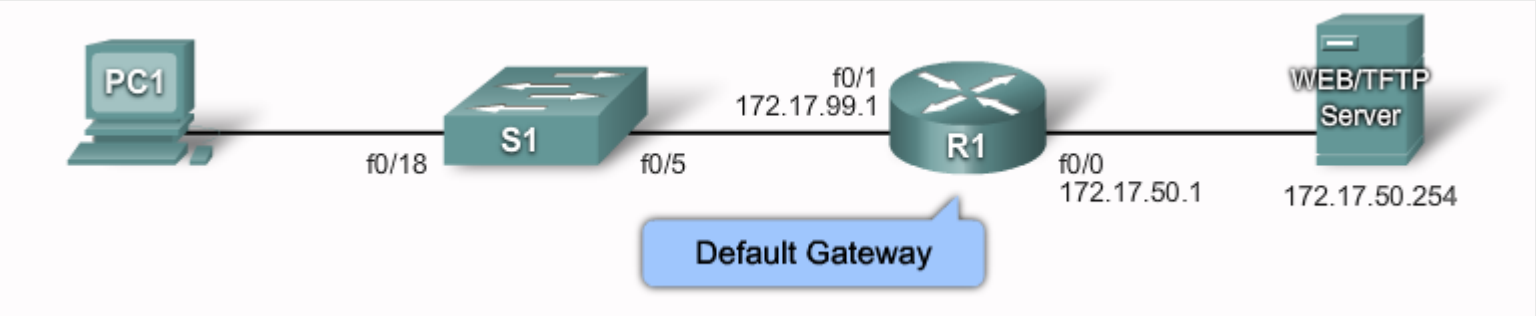
```
Switch(config)#mac-address-table aging-time seconds [vlan vlan_id]
```

Verifying configuration

Cisco IOS CLI Command Syntax	
Displays interface status and configuration for a single or all interfaces available on the switch.	`show interfaces [interface-id]`
Displays contents of startup configuration.	`show startup-config`
Displays current operating configuration.	`show running-config`
Displays information about flash: file system.	`show flash:`
Displays system hardware and software status.	`show version`
Display the session command history.	`show history`
Displays IP information. The interface option displays IP interface status and configuration. The http option displays HTTP information about device manager running on the switch. The arp option displays the IP ARP table.	`show ip {interface | http | arp}`
Displays the MAC forwarding table.	`show mac-address-table`

Assign IP address (basic)

- Enable remote configuration using TCP/IP
  - Assign the switch an IP address




```
S1#configure terminal
S1(config)#interface vlan 1
S1(config-if)#ip address 172.17.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1#ip default-gateway 172.17.99.1
S1#end
```

Configuration management

- Backup and restore *switch* configurations

```
SW-lab#copy running-config startup-config
```

```
SW-lab#copy startup-config flash:
Destination filename [startup-config]? startup-config.bak

551 bytes copied in 0.416 secs (1324 bytes/sec)
```

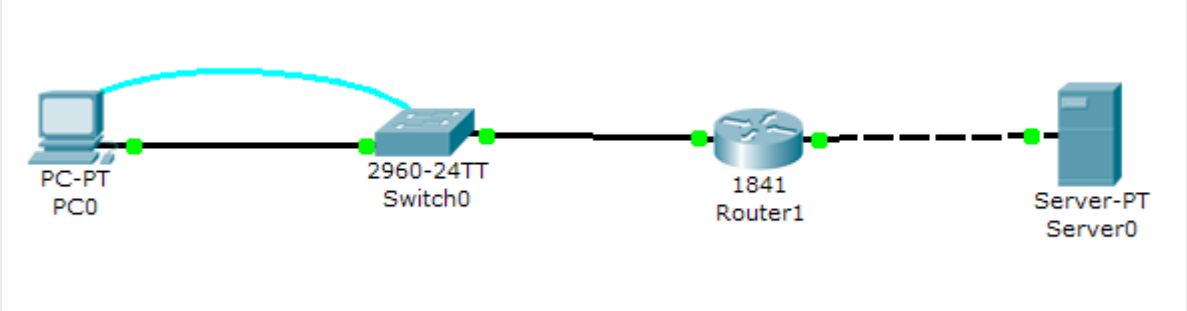
```
SW-lab#copy running-config flash:
Destination filename [running-config]? running-config.bak
Building configuration...
[OK]
```

```
SW-lab#copy flash: startup-config
Source filename []? startup-config.bak
Destination filename [startup-config]?
[OK]

551 bytes copied in 0.416 secs (1324 bytes/sec)
```

```
SW-lab#reload
Proceed with reload? [confirm]
```

Configuration management

- Backup and restore on the network




```
Switch0#copy running-config tftp:
Address or name of remote host []?
Destination filename [Switch-confg]?

Switch#copy startup-config tftp:
```

```
Switch0#copy tftp: startup-config
...
```

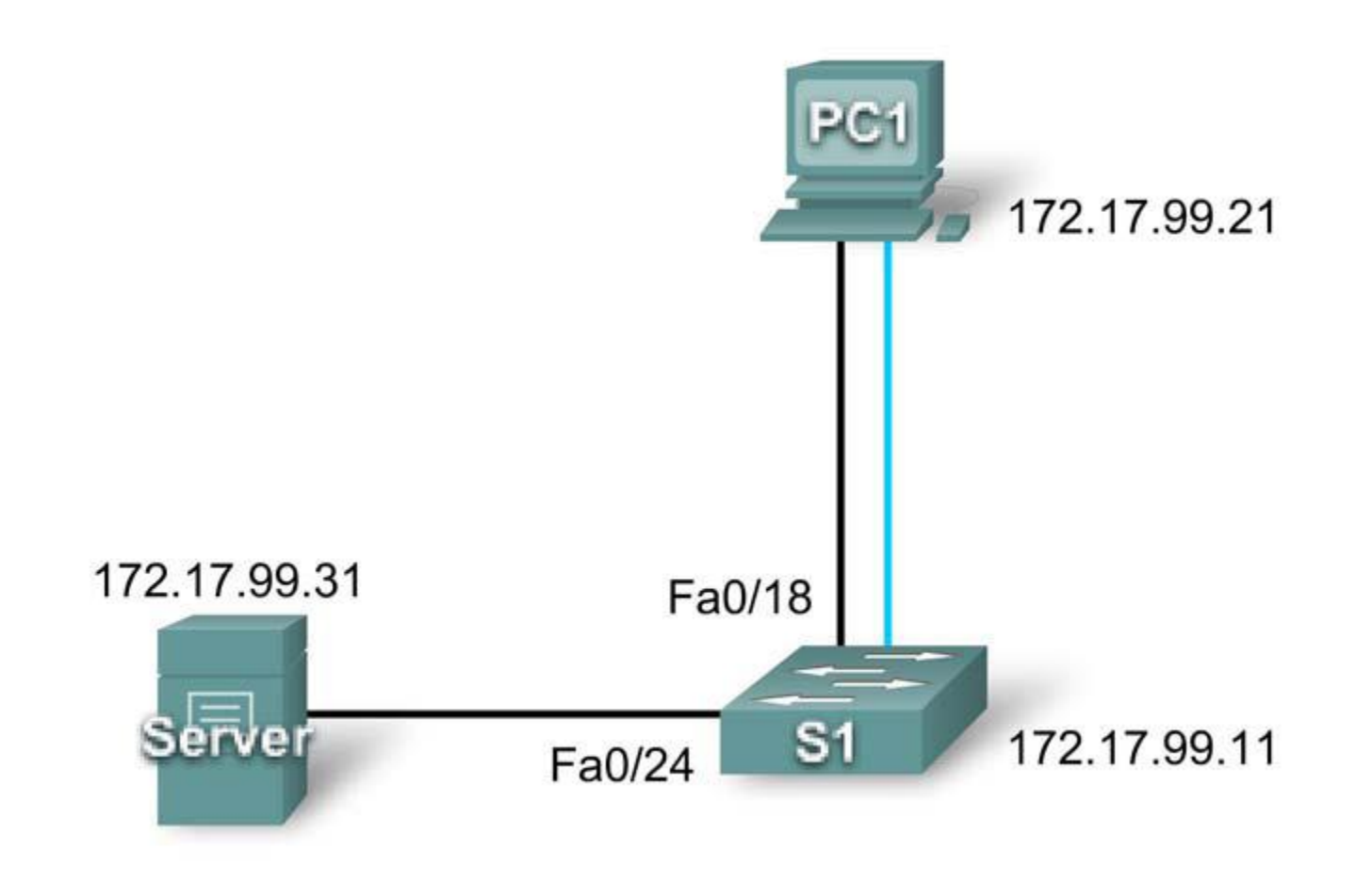
```
Switch0#copy tftp: running-config
```

Attenzione!!!

- Clearing configuration

```
Switch0#erase startup-config

Switch0#delete flash:
Delete filename []?
```

Lab activity



Configuring basic switch security

- Console password

```
Switch(config)#line console 0
Switch(config-line)#password password
Switch(config-line)#login
```

- Virtual Terminal password (telnet)

```
Switch(config)#line vty 0 15
Switch(config-line)#password password
Switch(config-line)#login
```

- Privileged EXEC mode authentication

```
Switch(config)#enable secret password
```

- Encrypting password display (show commands)

```
Switch(config)#service password-encryption
```

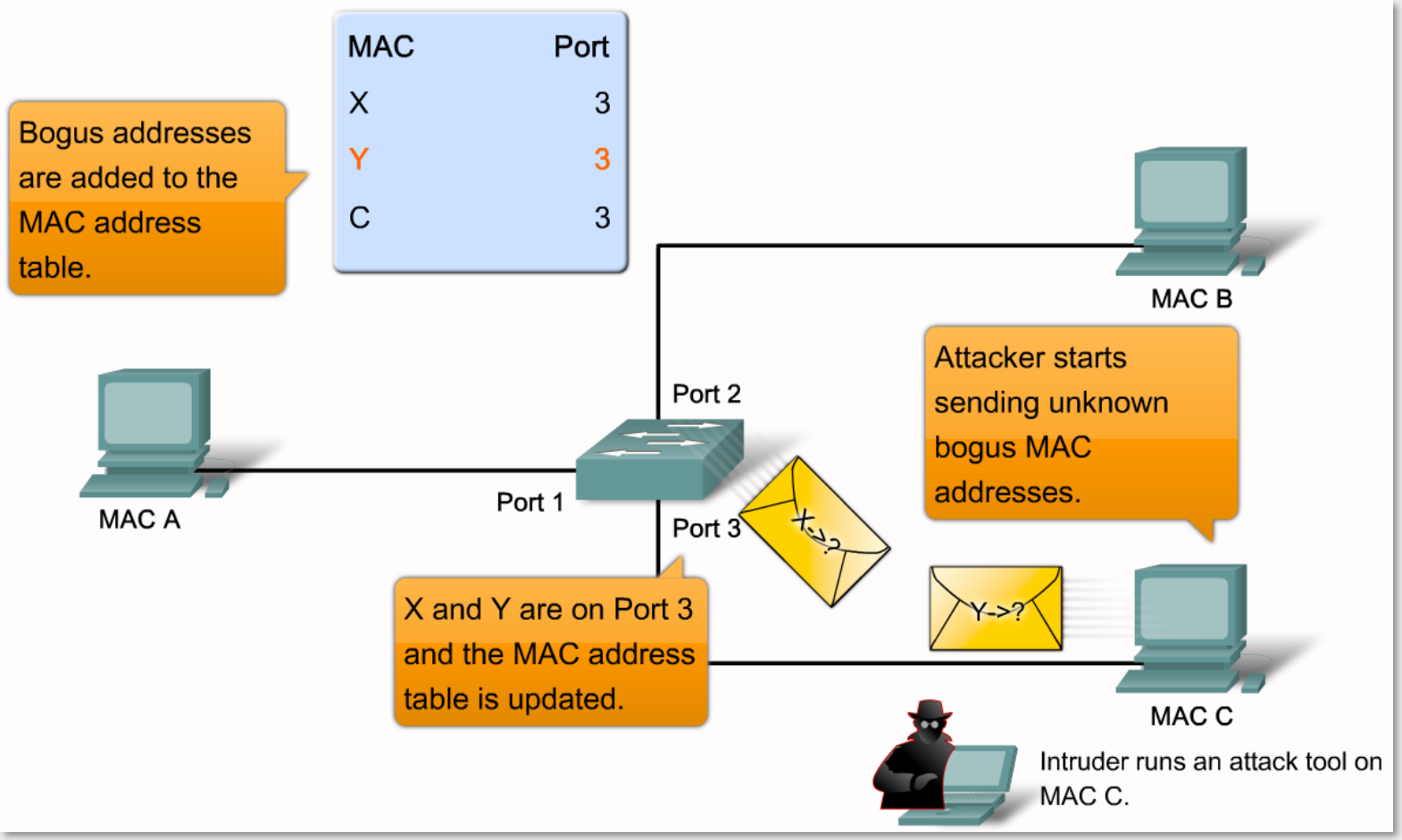
Configuring basic switch security

- Enabling SSH access (instead of telnet)

```
Sw1#conf t
Sw1(config)#ip domain-name mydomain.com
Sw1(config)#crypto key generate rsa
The name for the keys will be: Sw1.mydomain.com
...
How many bits in the modulus [512]: 1024
...
Sw1(config)#end
Sw1#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
Sw1#conf t
Sw1(config)#username admin secret cisco
Sw1(config)#line vty 0 15
Sw1(config-line)#transport input ssh
Sw1(config-line)#login local
Sw1(config-line)#exit
Sw1(config)#ip ssh version 2
Sw1(config)#ip ssh time-out 60
Sw1(config)#ip ssh authentication-retries 5
Sw1(config-line)#^Z
Sw1#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 5
```

Switch security: common attacks

- MAC address flooding



Configuring switch security

- Port security
  - Limit the number of **valid** (secure) MAC addresses allowed on each port
  - Packets with source addresses outside the group of allowed addresses on that port are not forwarded
  - Example: max number = 1, i.e. single secure MAC address assigned
    - The port is reserved for use by the workstation with that particular MAC address
- Secure MAC address types
  - Static
    - manually configured (using the **`switchport port-security mac-address`** ***`mac-address`*** interface configuration command)
    - stored in the address table and saved to the running configuration
  - Dynamic
    - dynamically learned
    - stored in the address table only, removed when the switch restarts
  - Sticky
    - dynamically learned
    - stored in the address table and saved to the running configuration

Configuring switch security

- Configure port security

```
Sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#interface fa0/18
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport port-security ?
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>
Sw1(config-if)#switchport port-security
Sw1(config-if)#switchport port-security maximum ?
  <1-132>  Maximum addresses
Sw1(config-if)#switchport port-security maximum 5
Sw1(config-if)#switchport port-security mac-address ?
  H.H.H    48 bit mac address
  sticky   Configure dynamic secure addresses as sticky
Sw1(config-if)#switchport port-security mac-address sticky
Sw1(config-if)#end
```

Enables port security

Specify the # of allowed addresses

Configure secure MAC addresses

Configuring switch security

- Sticky MAC addresses
  - enabled by using the **`switchport port-security mac-address sticky`** interface configuration command
  - the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration
  - If you disable sticky learning by using the **`no switchport port-security mac-address sticky`** interface configuration command, the sticky secure MAC addresses remain part of the address table but are removed from the running configuration.
  - When you configure sticky secure MAC addresses by using the **`switchport port-security mac-address sticky mac-address`** interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration
  - If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost

Configuring switch security

- Security violation
  - The maximum number of secure MAC addresses has been reached on an interface, and a station whose MAC address is not in the address table attempts to access the interface
  - An address is being used on two secure interfaces in the same VLAN

- Security violation modes
  - **`protect`**
  - **`restrict`**
  - **`shutdown`** (default mode)

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	Yes	No	Yes	Yes

Configuring switch security

- Configure port security violation mode

```
Sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#interface fa0/18
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport port-security
Sw1(config-if)#switchport port-security maximum 5
Sw1(config-if)#switchport port-security mac-address sticky
Sw1(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
Sw1(config-if)#switchport port-security violation restrict
Sw1(config-if)#end
```

Configuring switch security

- Port security defaults

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, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

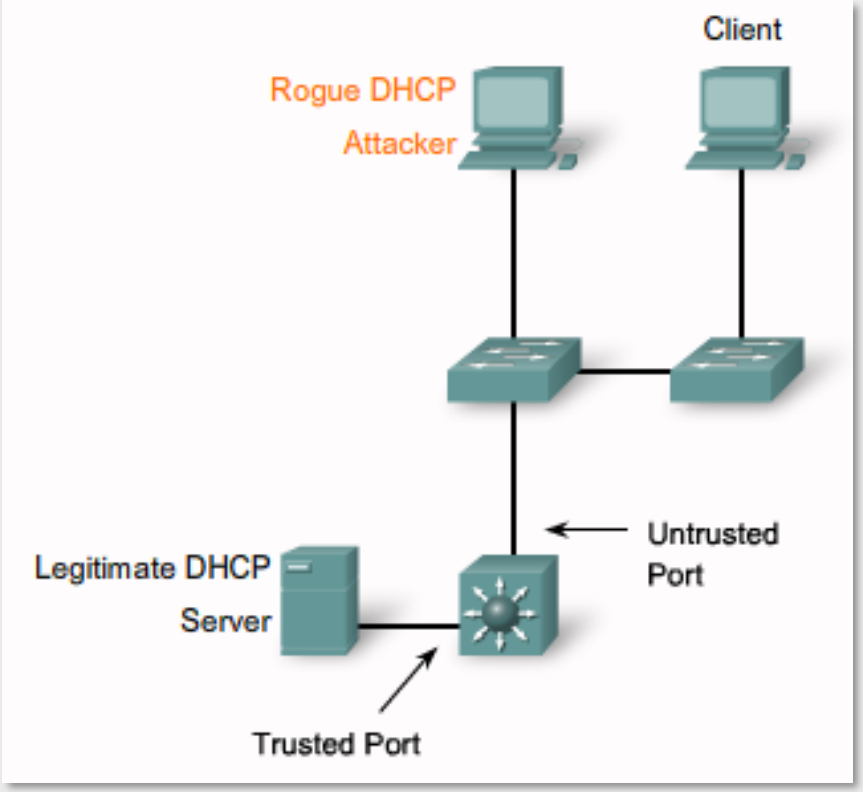
Configuring switch security

- Verify port security

```
Sw1#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       : 1
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

Sw1#show port-security address
                           Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address         Type                          Ports                Remaining Age
                                                                               (mins)
----    -----------         ----                          -----                -------------
99      00D0.BAED.1ACB      SecureSticky                  FastEthernet0/18             -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Sw1#
```

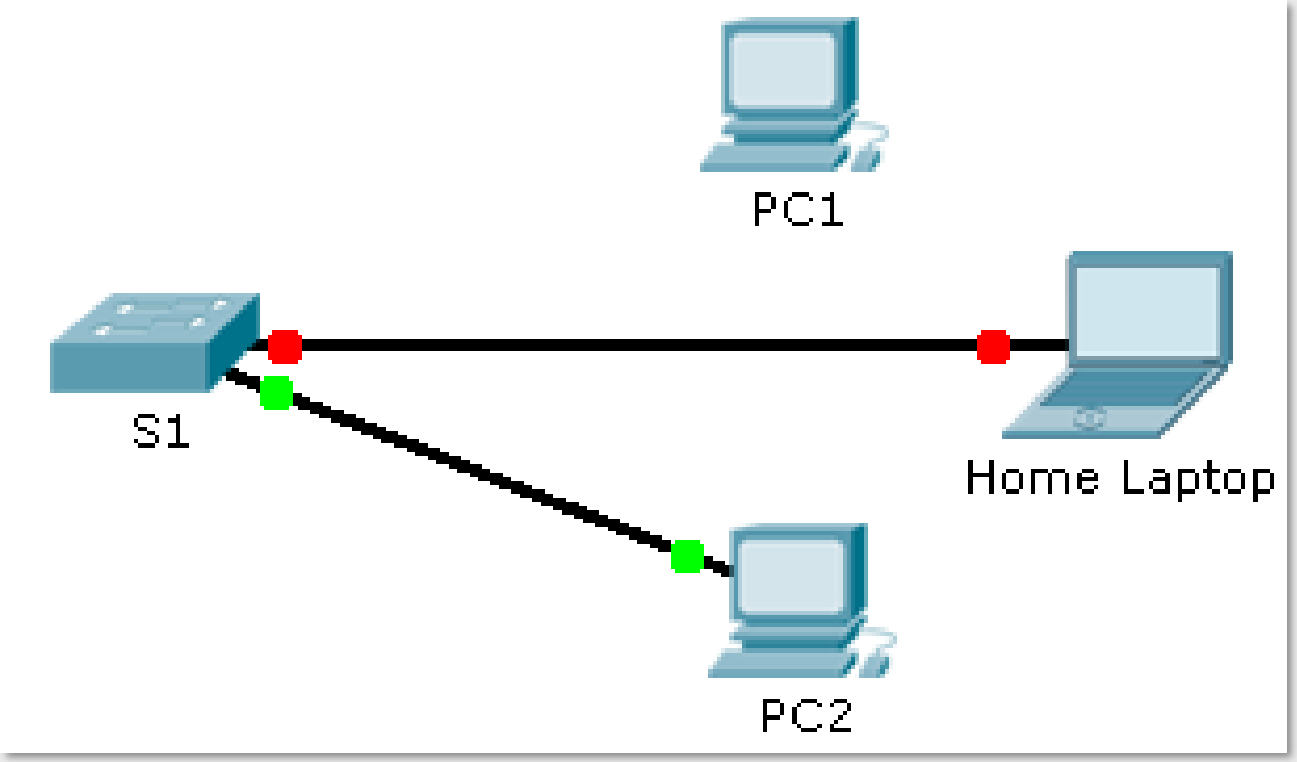
Switch security: common attacks

- DHCP spoofing
- DHCP starvation



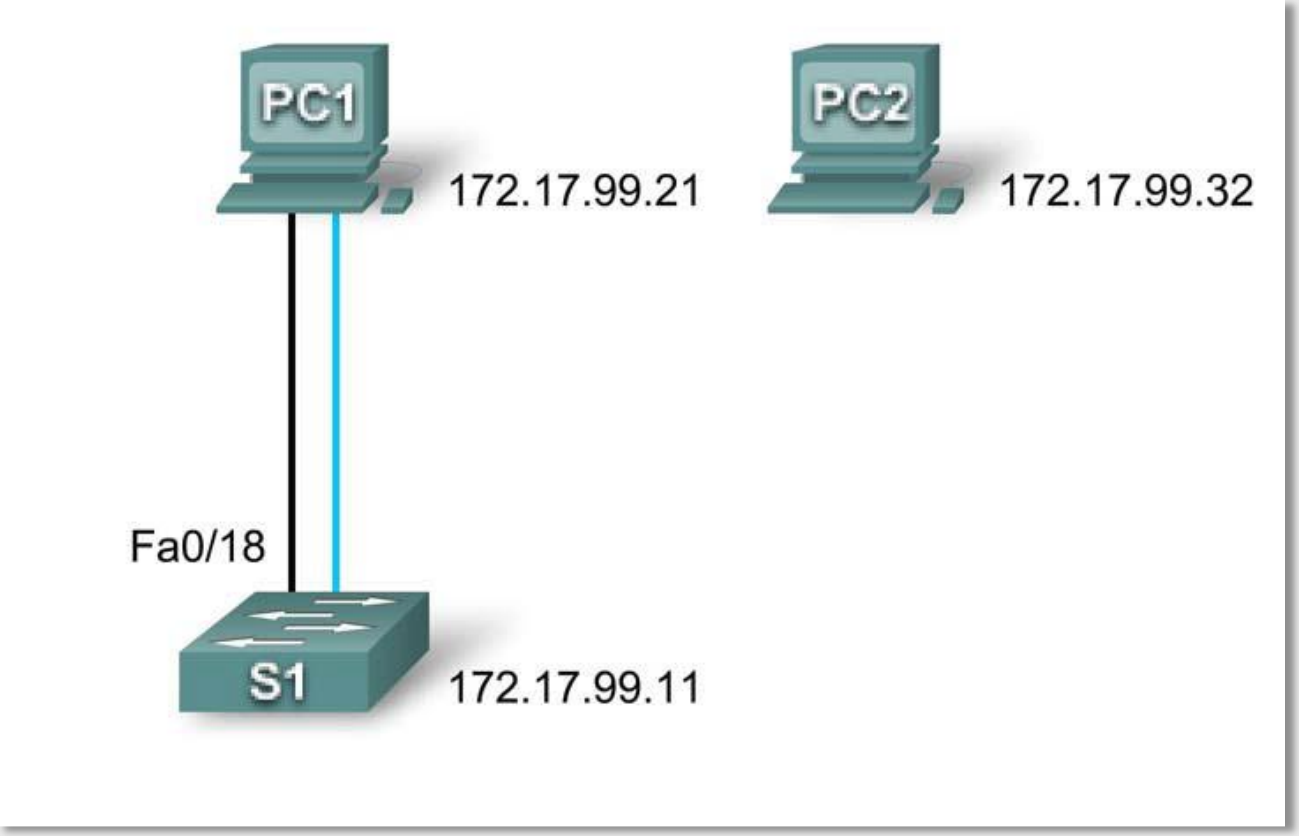
Lab activity

- Troubleshooting switch port security



Lab activity

- Configure Switch Security



Lab activity

- Configure Switch Security

Lab activity

- Basic Switch configuration