

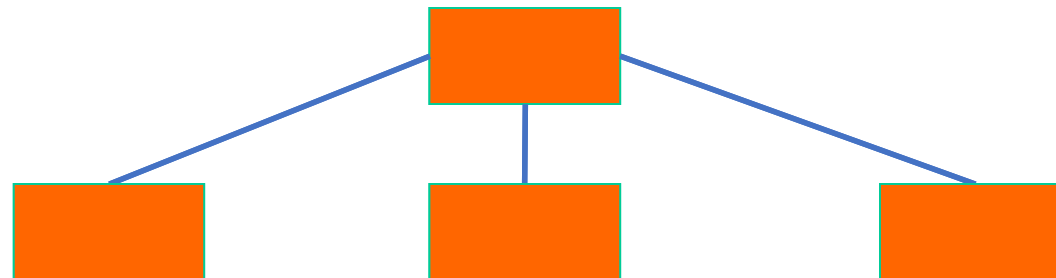
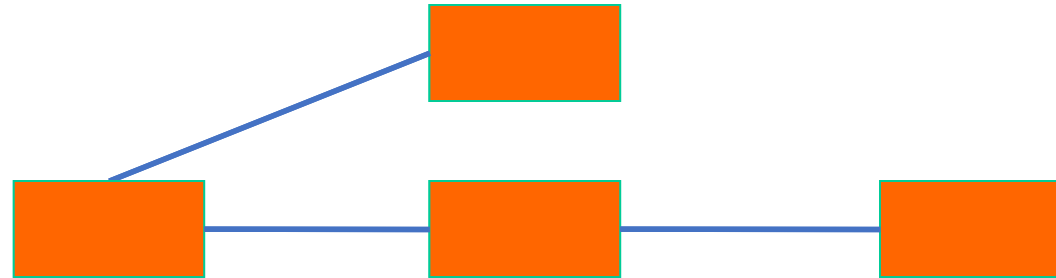
Switch Configuration

Faculty of Technology
University of Sri Jayewardenepura
2019

Layer 2 Network Design Guidelines

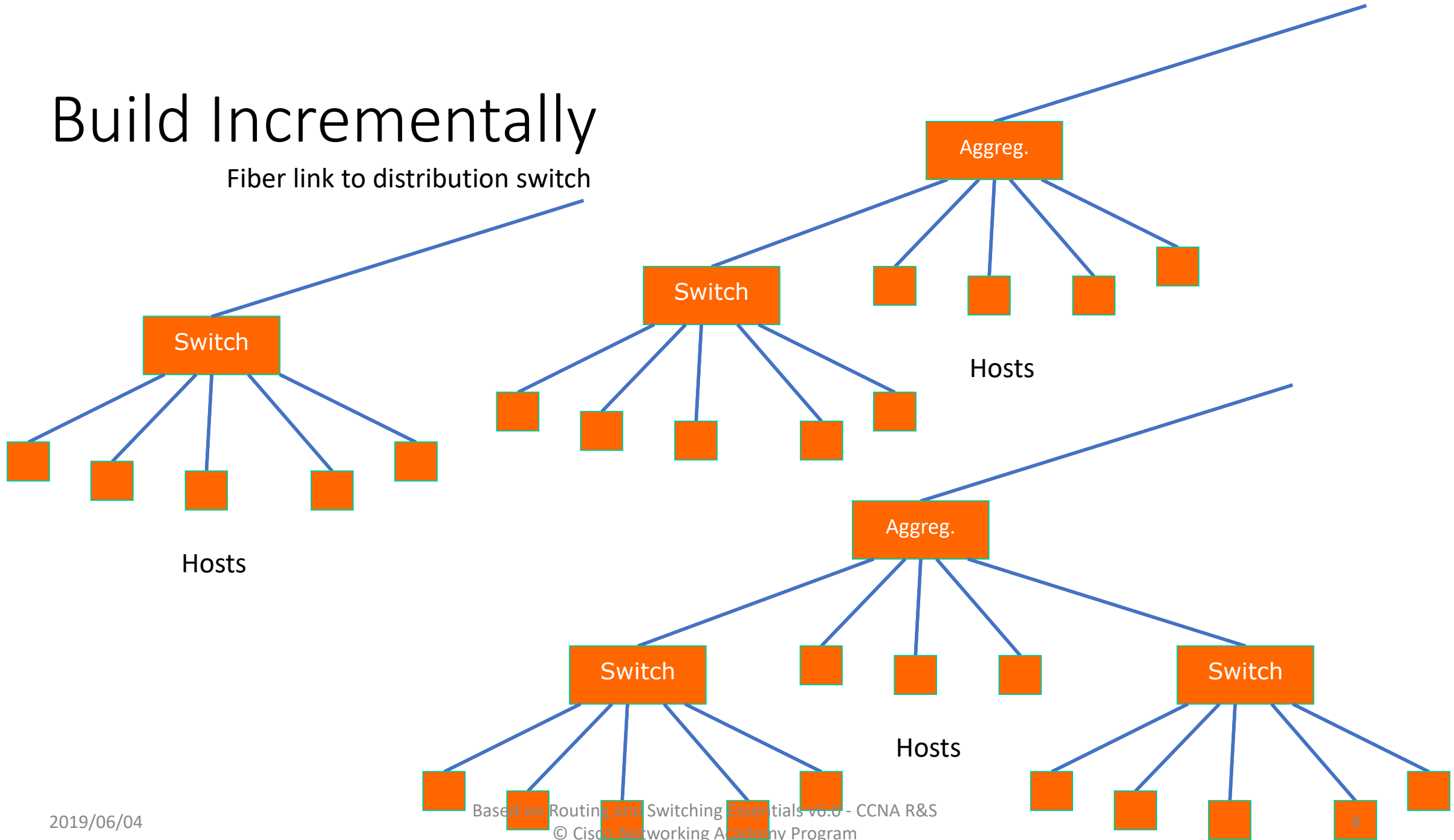
- Always connect hierarchically
 - If there are multiple switches in a building, use an aggregation switch
 - Locate the aggregation switch close to the building entry point (e.g. fiber panel)
 - Locate edge switches close to users (e.g. one per floor)
 - Max length for Cat 5 is 100 meters

Minimize Path Between Elements



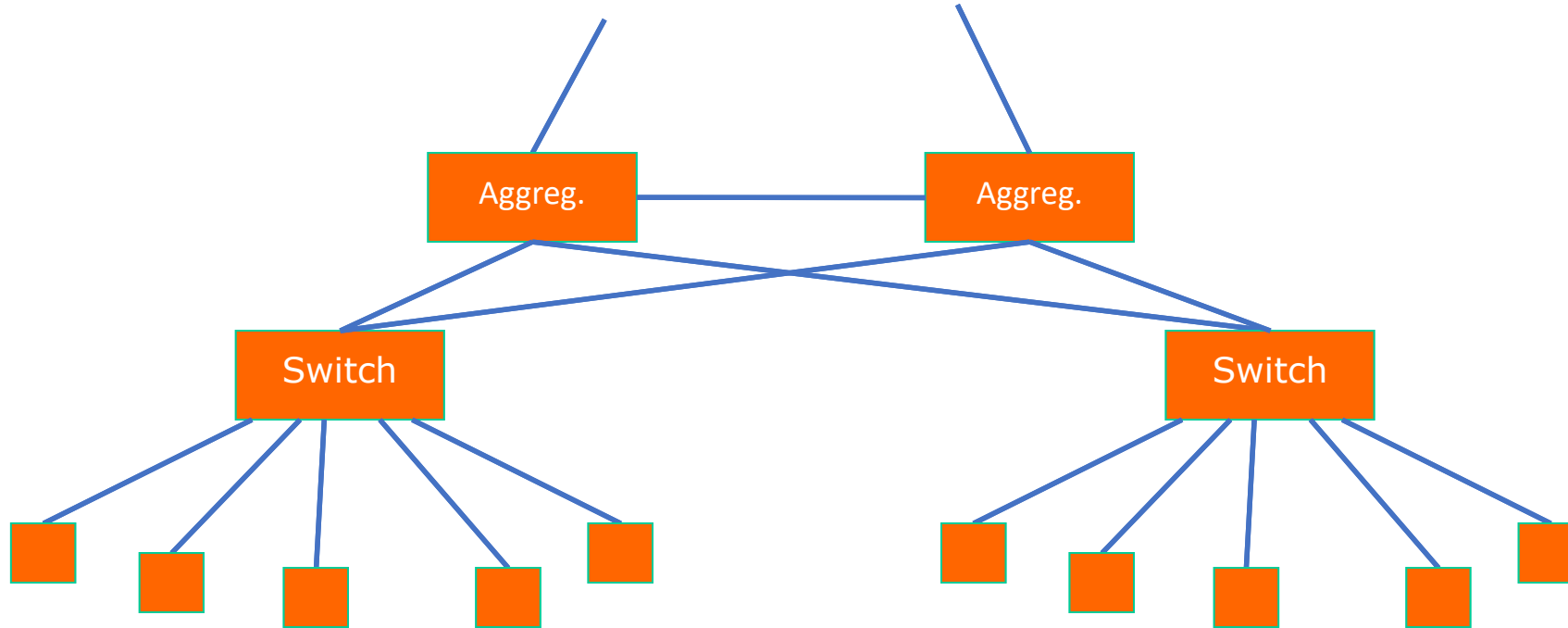
Build Incrementally

Fiber link to distribution switch



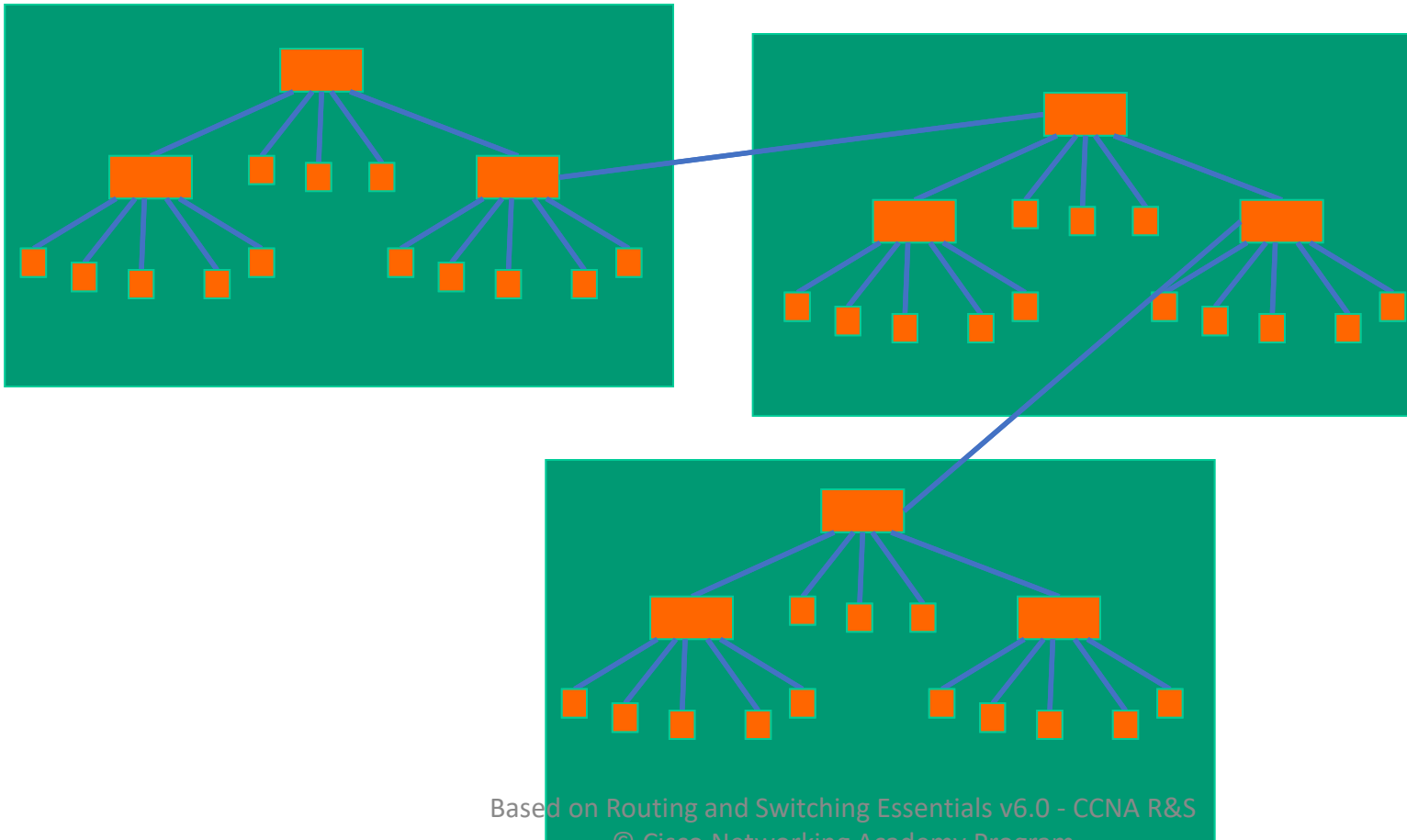
Build Incrementally

- At this point, you can also add a redundant aggregation switch:

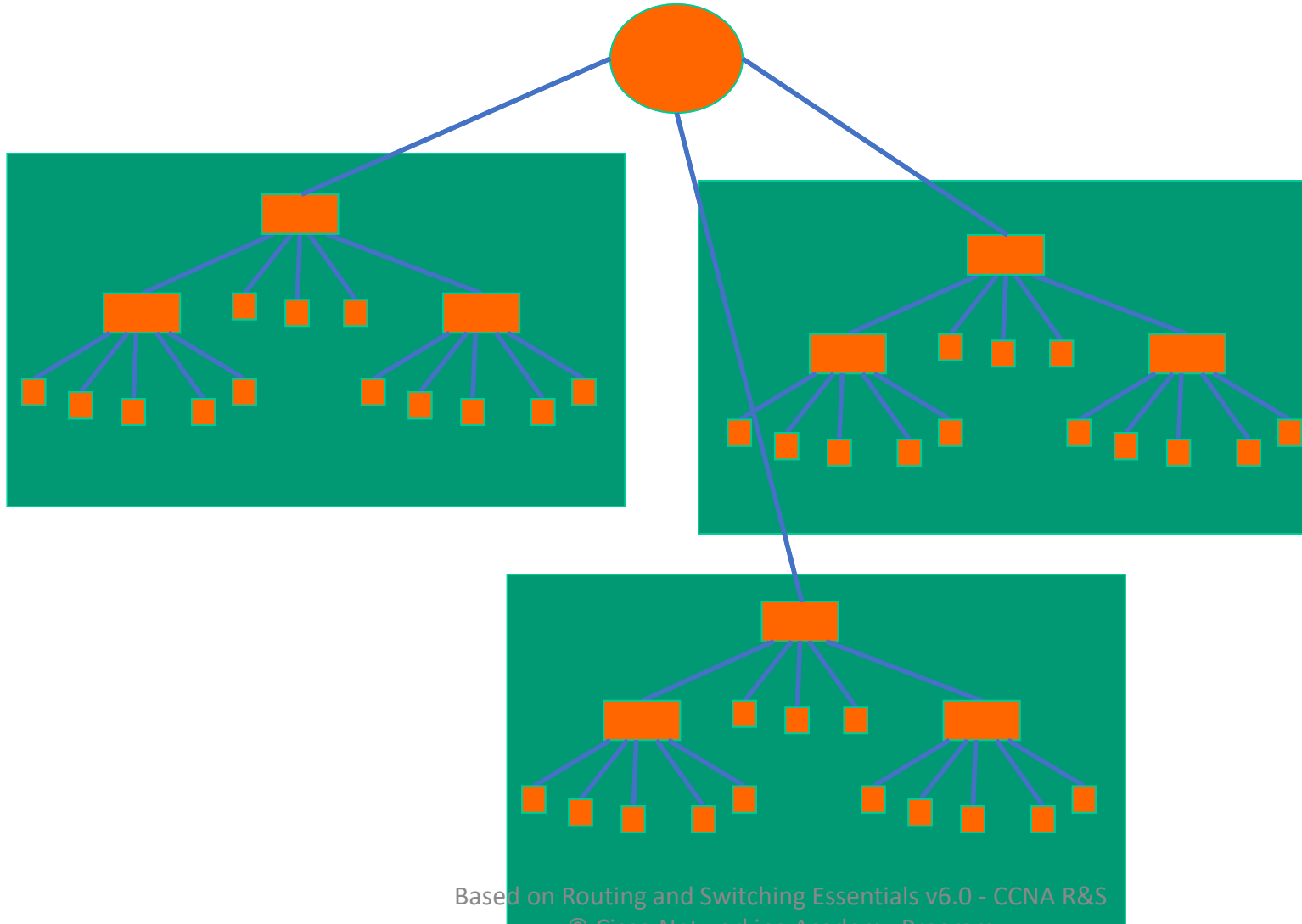


Do not daisy-chain

- Resist the temptation of doing this:



Connect buildings hierarchically



Unmanaged Switches

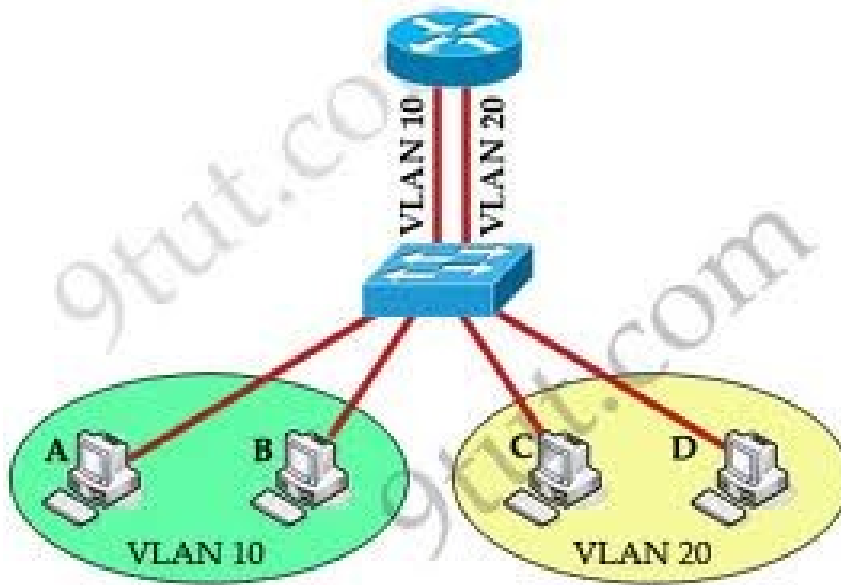
- Basic IEEE 802.3 MAC based switching functions
- No configurable parameters
- Cannot be configured to optimize LAN traffic
- Unmanaged switches offer plug and play operation
- Can't be used in a redundant config (Ring, Mesh)

Managed Switches

- Managed switches provide all of the features of an unmanaged switch and provide the ability to configure and monitor your network
- Managed switches support protocols such as SNMP (Simple Network Management Protocol) that provides information about the switch to facilitate remote management
- Additional advanced management features include:
 - QoS (Quality of Service)
 - VLANs (Virtual LAN) which allows network segmentation
 - STP/RSTP (Spanning Tree and Rapid Spanning Tree Protocol) which for redundancy
 - Port Mirroring

Layer 3 Switches

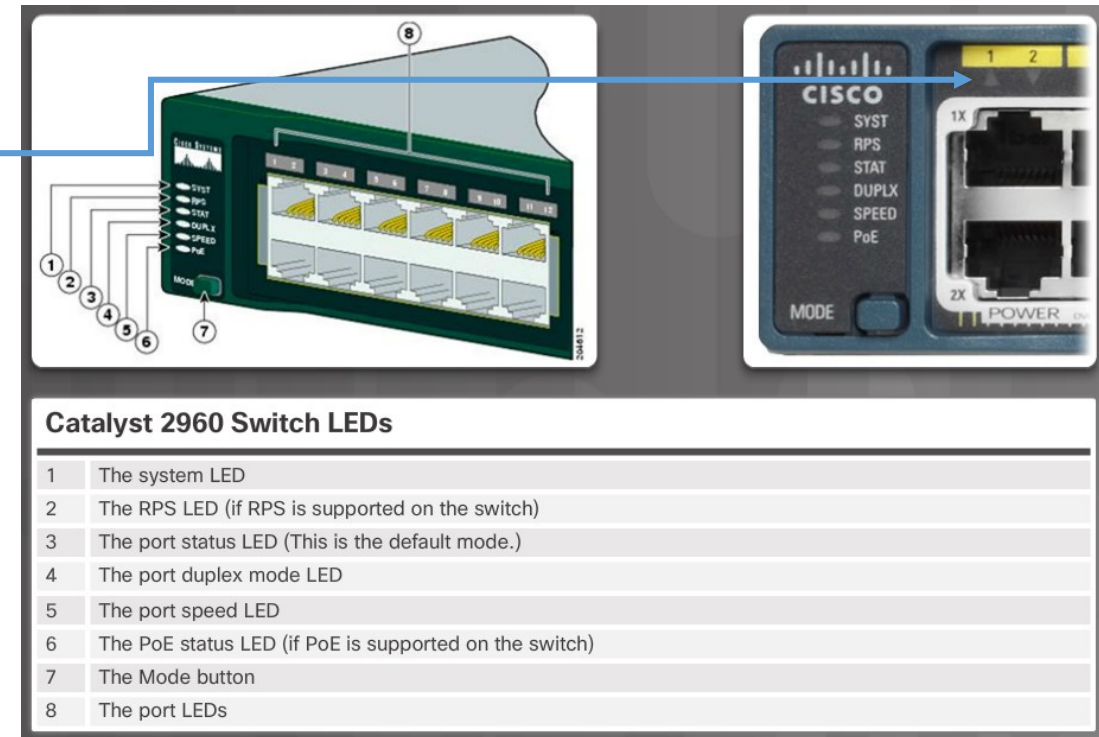
- Layer 3 adds routing capability
- Allows packets to cross network domains
- VLAN to VLAN connections



Can be accomplished in a single unit
Layer 3 switch

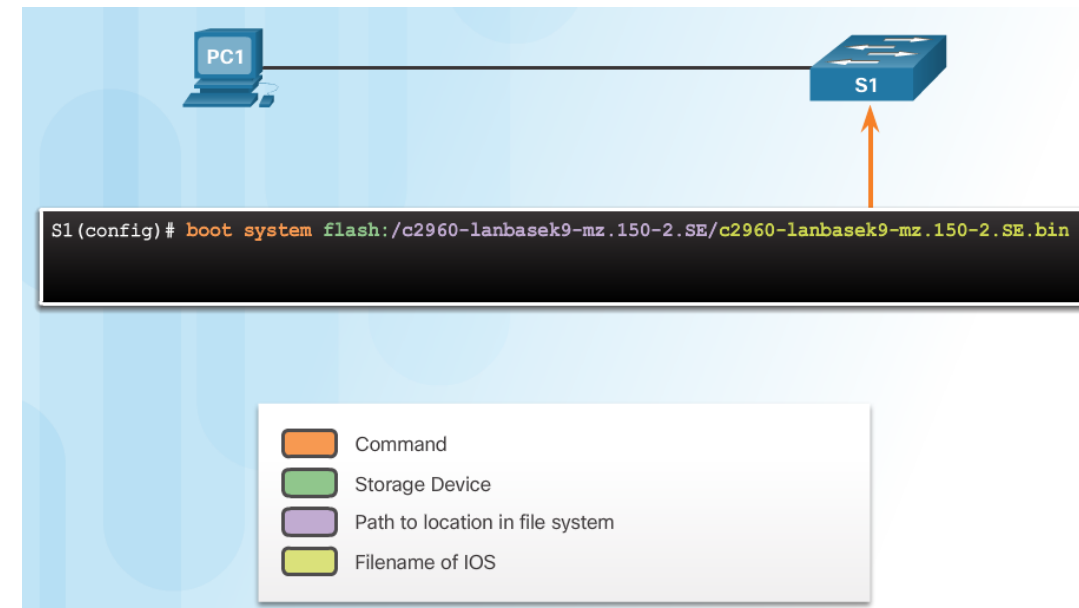
Switch LED Indicators

- System LED shows if the switch has power applied.
- Port LED states:
 - Off – no link or shut down
 - Green – link is present
 - Blinking green – data activity ▲
 - Alternating green and amber – link fault ▲→▲→▲→▲
 - Amber – port is not sending data; common for first 30 seconds of connectivity or activation ▲
 - Blinking amber – port is blocking to prevent a switch loop



Configure a Switch with Initial Settings

- When a switch is powered on, the boot sequence occurs.
 - Power-on self-test (POST), a program stored in ROM, executes and checks hardware like CPU and RAM.
 - The boot loader, also stored in ROM, runs and initializes parts within the CPU, initializes the flash file system, and then locates and loads an IOS image.
 - If an IOS operating system loads, the switch interfaces are initialized and any commands stored in the startup-config file load.
 - The boot system command is use to set the BOOT environment variable.



Recovering From a System Crash

- The boot loader prompt can be accessed through a console connection to the switch:
 - Cable the PC to the switch console port.
 - Configure the terminal emulation software on the PC.
 - Unplug the switch power cord.
 - Reconnect the power cord and at the same time or within 15 seconds, press and hold the Mode button on the front of the switch until the System LED turns an amber color briefly and then turns a solid green.
- The boot loader command prompt is switch: (instead of Switch>).
 - The commands available through the boot loader command prompt are limited.
 - Use the help command to display the available commands.

```
switch: dir flash:
Directory of flash:/

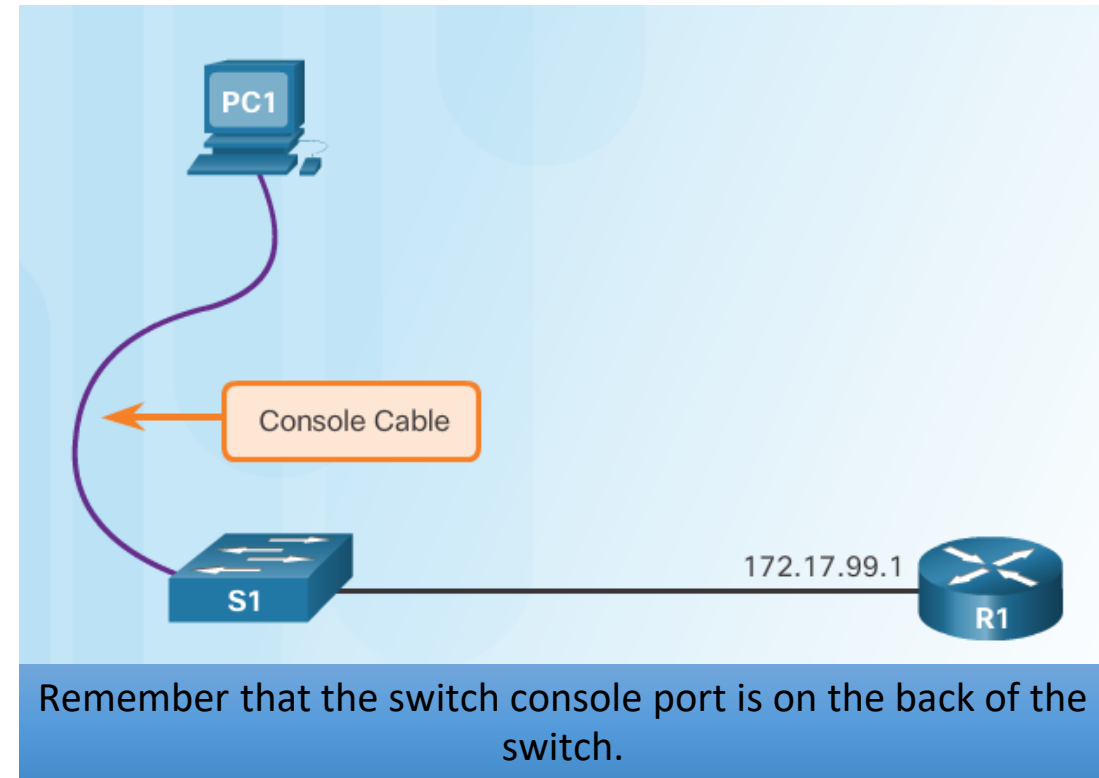
 2  -rwx      11607161   Mar 1 2013 03:10:47 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
 3  -rwx         1809   Mar 1 2013 00:02:48 +00:00  config.text
 5  -rwx         1919   Mar 1 2013 00:02:48 +00:00  private-config.text
 6  -rwx         59416   Mar 1 2013 00:02:49 +00:00  multiple-fs

32514048 bytes total (20841472 bytes free)
```

Based on Routing and Switching Essentials v6.0 - CCNA R&S
© Cisco Networking Academy Program

Preparing for Basic Switch Management

- To configure a switch for remote access, the switch must be configured with an IP address, subnet mask, and default gateway.
- One particular switch virtual interface (SVI) is used to manage the switch:
 - A switch IP address is assigned to an SVI.
 - By default the management SVI is controlled and configured through VLAN 1.
 - The management SVI is commonly called the management VLAN.
- For security reasons, it is best practice to use a VLAN other than VLAN 1 for the management VLAN.

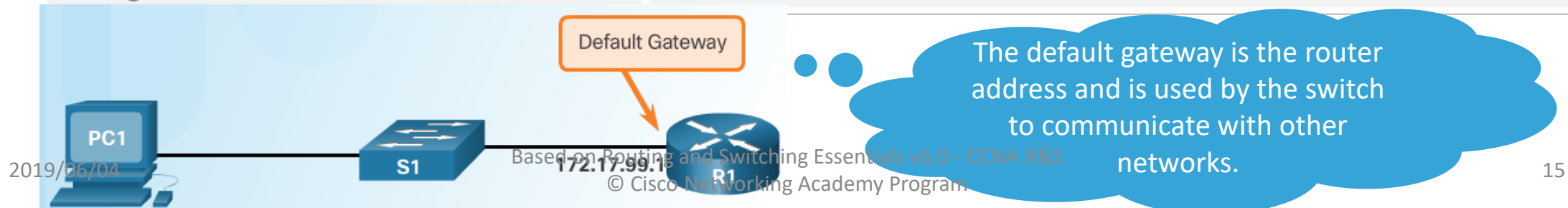


Configuring Basic Switch Management Access with IPv4

Cisco Switch IOS Commands

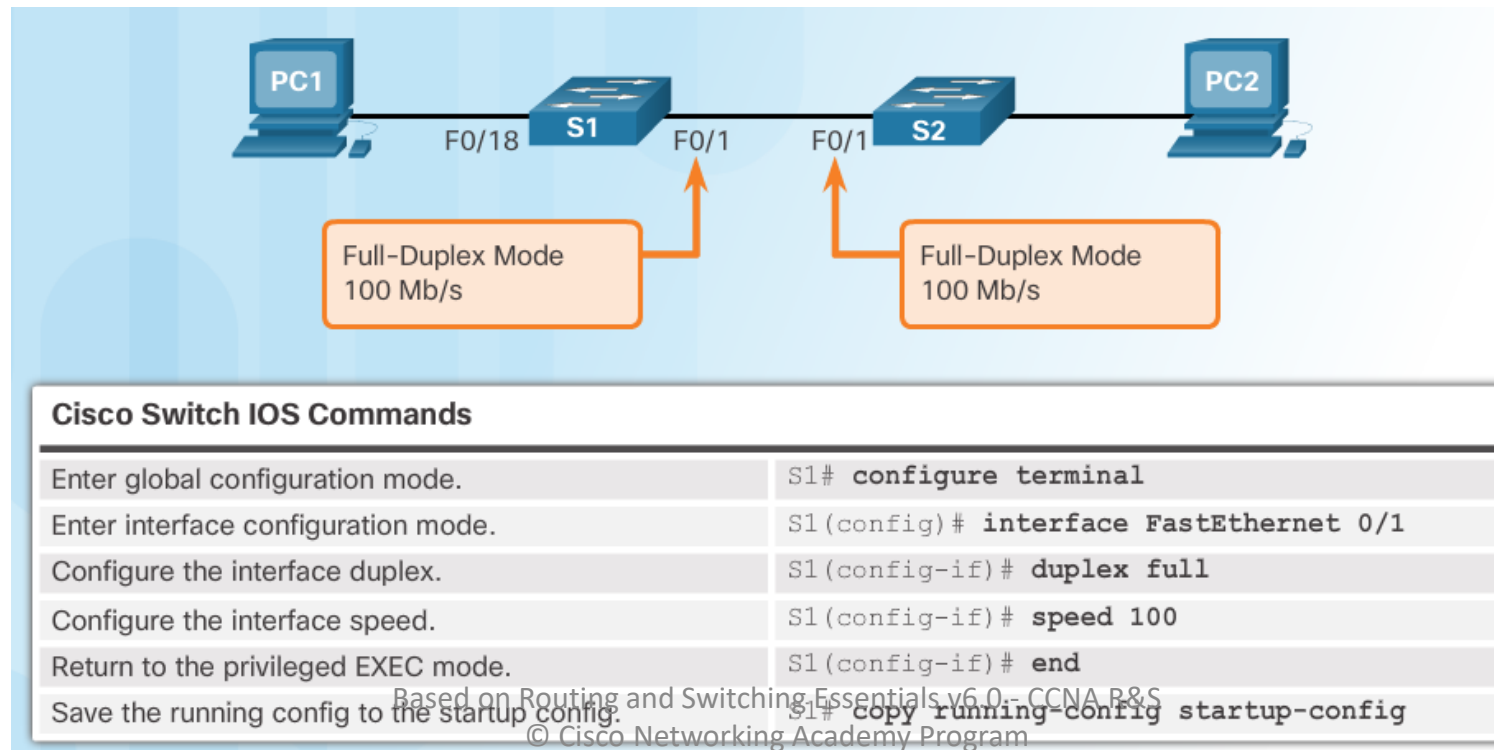
| | |
|---|---|
| Enter global configuration mode. | S1# configure terminal |
| Enter interface configuration mode for the SVI. | S1(config)# interface vlan 99 |
| Configure the management interface IP address. | S1(config-if)# ip address 172.17.99.11 255.255.255.0 |
| Enable the management interface. | S1(config-if)# no shutdown |
| Return to the privileged EXEC mode. | S1(config-if)# exit |
| Configure the default gateway for the switch. | S1(config)# ip default-gateway 172.17.99.1 |
| Return to the privileged EXEC mode. | S1(config)# end |
| Save the running config to the startup config. | S1# copy running-config startup-config |

Important Concept



Configure Switch Ports at the Physical Layer

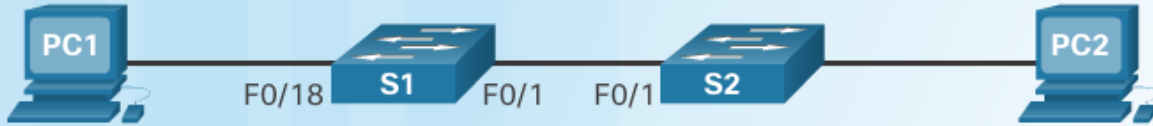
- Some switches have the default setting of auto for both duplex and speed.
- Mismatched duplex and/or speed settings can cause connectivity issues.
- Check duplex and speed settings using the `show interface interface_id` command.
- All fiber ports operate at one speed and are always full-duplex.



Auto-MDIX

- Some switches have the automatic medium-dependent interface crossover (auto-MDIX) feature that allows an interface to detect the required cable connection type (straight-through or crossover) and configure the connection appropriately.

Configure auto-MDIX



The diagram illustrates a network setup for configuring auto-MDIX. PC1 is connected to switch S1 at interface F0/18. Switch S1 is connected to switch S2 at interface F0/1. Switch S2 is connected to PC2 at interface F0/1.

| Cisco Switch IOS Commands | |
|--|---|
| Enter global configuration mode. | S1# configure terminal |
| Enter interface configuration mode. | S1(config)# interface fastethernet 0/1 |
| Configure the interface to autonegotiate duplex with the connected device. | S1(config-if)# duplex auto |
| Configure the interface to autonegotiate speed with the connected device. | S1(config-if)# speed auto |
| Enable auto-MDIX on the interface. | S1(config-if)# mdix auto |
| Return to the privileged EXEC mode. | S1(config-if)# end |
| Save the running config to the startup config. | S1# copy running-config startup-config |

Based on Routing and Switching Essentials v6.0 – CCNA R&S

Verifying Switch Port Configuration

Cisco Switch IOS Commands

Display interface status and configuration.

```
S1# show interfaces [interface-id]
```

Display current startup configuration.

```
S1# show startup-config
```

Display current operating config.

```
S1# show running-config
```

Display information about flash file system.

```
S1# show flash
```

Display system hardware and software status.

```
S1# show version
```

Display history of commands entered.

```
S1# show history
```

Display IP information about an interface.

```
S1# show ip [interface-id]
```

Display the MAC address table.

```
S1# show mac-address-table  
OR  
S1# show mac address-table
```

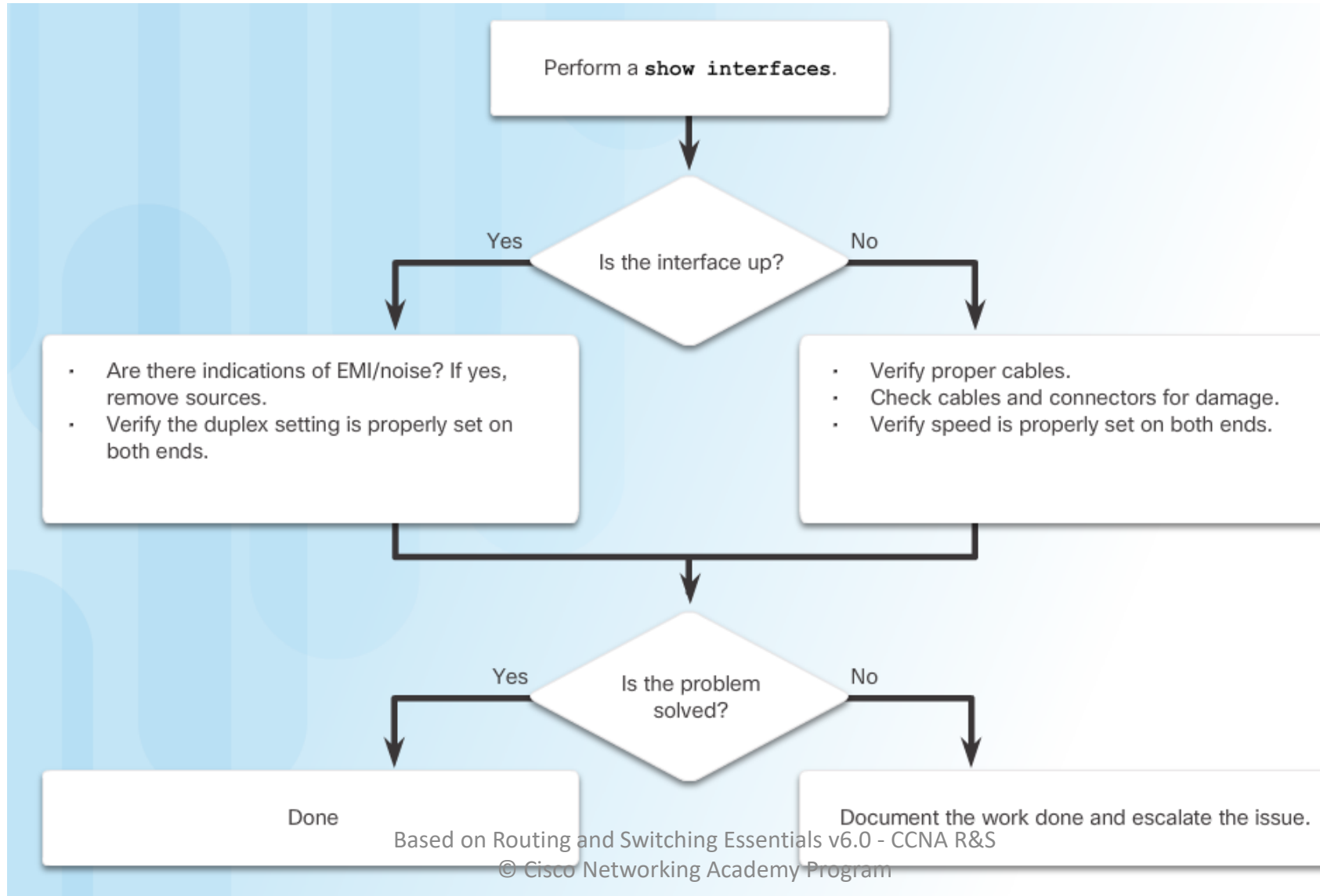
Network Access Layer Issues

- Use the show interfaces command to detect common media issues.
- The first parameter refers to Layer 1, the physical layer, and indicates if the interface is receiving a carrier detect signal.
- The second parameter (protocol status) refers to the data link layer and indicates whether the data link layer protocol has been configured correctly and keepalives are being received.

```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
```

| Interface Status | Line Protocol Status | Link State |
|------------------|----------------------|-------------------|
| Up | Up | Operational |
| Down | Down | Interface Problem |

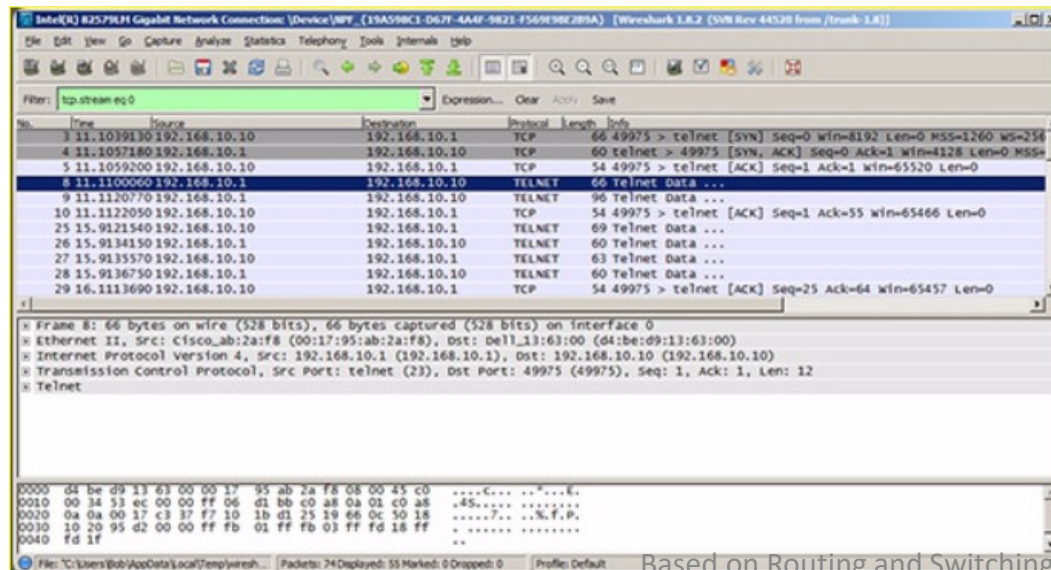
Troubleshooting Network Access Layer Issues



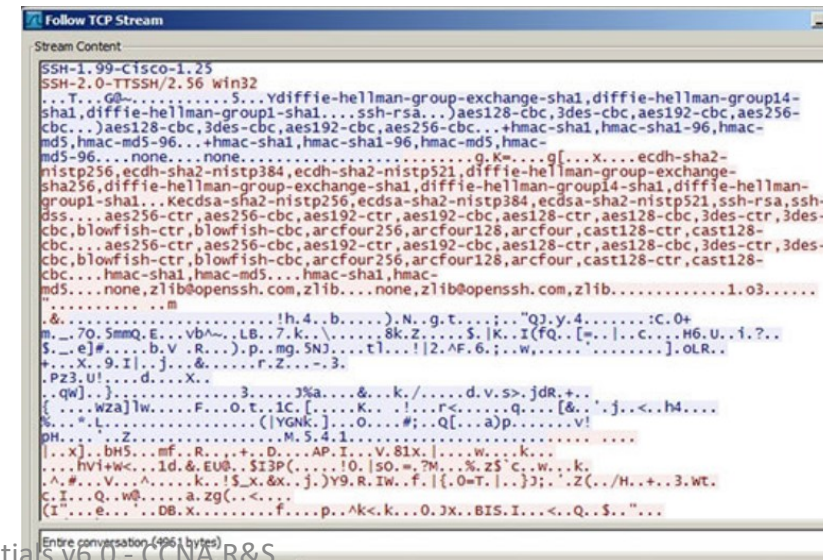
Switch Security

- Secure Shell (SSH)
 - An alternative protocol to Telnet. Telnet uses unsecure plaintext of the username and password as well as the data transmitted.
 - SSH is secure because it provides an encrypted management connection.

Wireshark Capture of Telnet



Wireshark Capture of SSH



Secure Remote Access

- On the PC, connect to the switch using SSH.

Verify SSH Status and Settings

```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCdLksVz2Q1REsoZt2f2scJHbW3aMDM8 /8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVN1QhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAaP3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption Hmac State Username
0 2.0 IN aes256-cbc hmac-sha1 Session started admin
0 2.0 OUT aes256-cbc hmac-sha1 Session started admin
%No SSHv1 server connections running.
S1#
```

Based on Routing and Switching Essentials v6.0 - CCNA R&S
© Cisco Networking Academy Program

Secure Unused Ports

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

Disable Unused Ports

```
S1# show run
Building configuration...
...
version 15.0
hostname S1
...
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6
description web server
!
interface FastEthernet0/7
shutdown
!
...
```

Disable unused ports using the **shutdown** command.

Based on Routing and Switching Essentials v6.0 - CCNA R&S
© Cisco Networking Academy Program

Port Security: Operation

- 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
 - 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)

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 |

Port Security: Configuring

Configure Dynamic Port Security



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 |

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 |

Packet Tracer - Configuring SSH

Topology



Addressing Table

| Device | Interface | IP Address | Subnet Mask |
|--------|-----------|-------------|---------------|
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |

Objectives

Part 1: Secure Passwords

Part 2: Encrypt Communications

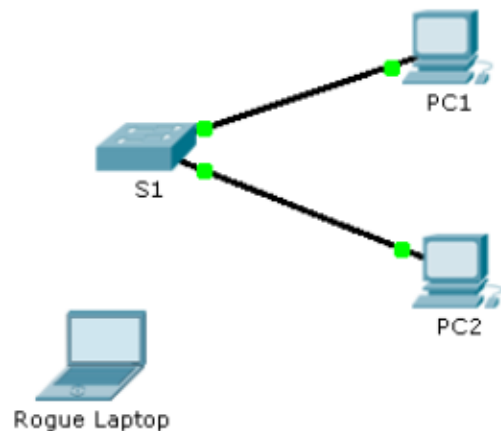
Part 3: Verify SSH Implementation

Background

SSH should replace Telnet for management connections. Telnet uses insecure plain text communications. SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In this activity, you will secure a remote switch with password encryption and SSH.

Packet Tracer - Configuring Switch Port Security

Topology



Addressing Table

| Device | Interface | IP Address | Subnet Mask |
|--------------|-----------|-------------|---------------|
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |
| PC2 | NIC | 10.10.10.11 | 255.255.255.0 |
| Rogue Laptop | NIC | 10.10.10.12 | 255.255.255.0 |

Objective

Part 1: Configure Port Security

Part 2: Verify Port Security

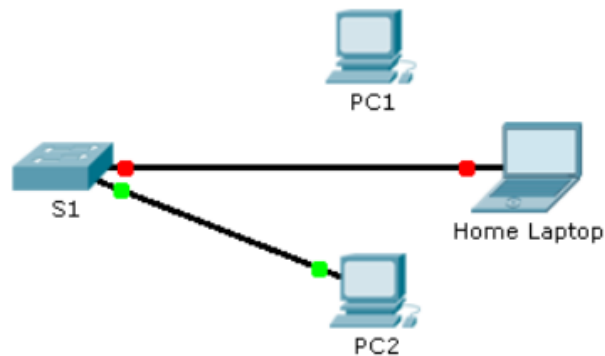
Background

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

Based on Routing and Switching Essentials v6.0, CCNA R/S

Packet Tracer - Troubleshooting Switch Port Security

Topology



Scenario

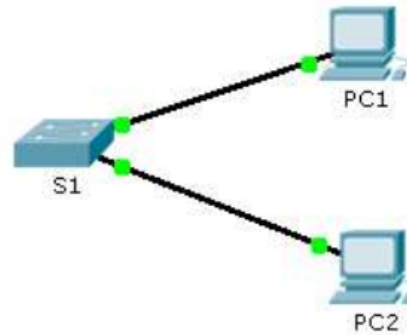
The employee who normally uses PC1 brought his laptop from home, disconnected PC1 and connected the laptop to the telecommunication outlet. After reminding him of the security policy that does not allow personal devices on the network, you now must reconnect PC1 and re-enable the port.

Requirements

- Disconnect **Home Laptop** and reconnect **PC1** to the appropriate port.
 - When **PC1** was reconnected to the switch port, did the port status change?
 - Enter the command to view the port status. What is the state of the port?
 - Which port security command enabled this feature?
- Enable the port using the necessary command.
- Verify connectivity. **PC1** should now be able to ping **PC2**.

Packet Tracer - Skills Integration Challenge

Topology



Addressing Table

| Device | Interface | IP Address | Subnet Mask |
|--------|-----------|-------------|---------------|
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |
| PC2 | NIC | 10.10.10.11 | 255.255.255.0 |

Scenario

The network administrator asked you to configure a new switch. In this activity, you will use a list of requirements to configure the new switch with initial settings, SSH, and port security.