CISCO™

CCNA 200-301

Lesson 8

- SSH Configuration
- Switch Interface configuration
- Autonegotiation
- Physical Layer problems

SSH Configuration

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated.

IOS uses the three SSH-specific configuration commands in the figure to create the SSH encryption keys.

- Switch(config)# hostname S1
- S1(config)# ip domain-name example.com
- S1(config)# crypto key generate rsa

RSA is the algorithm. (Rivest, Shamir, Adelman)

SSH Configuration cont.

After crypto key generate rsa command the IOS prompts the user to enter key modulus in the form of bits. More bits more encrypted. The default size of modulus is 512 bits. The interval is [360 – 2048].

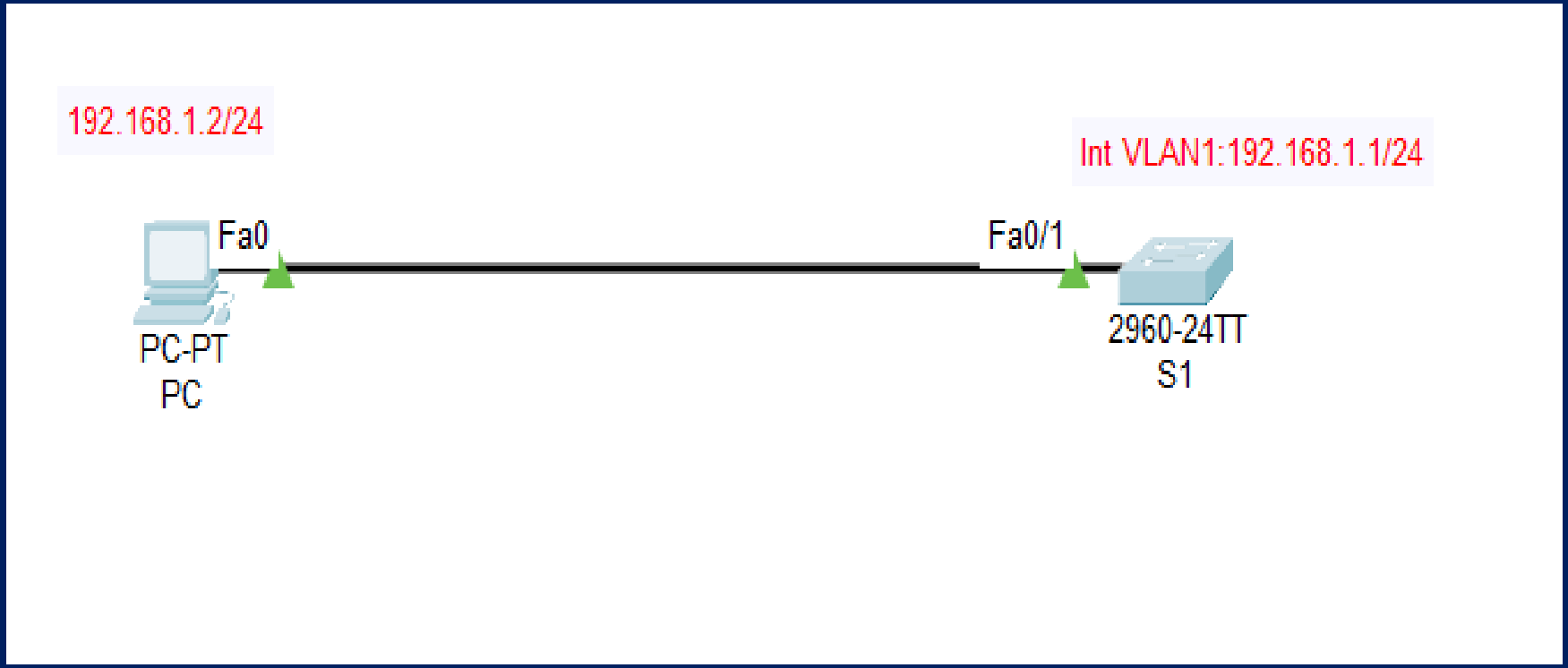
```
How many bits in the modulus [512]: 1024
```

Generating an RSA key pair for the Switch automatically enables SSH.

After creating rsa key pairs we can configure the left that is analogy to telnet.

- S1(config)#username cisco password cisco
- S1(config)#line vty 0 15
- S1(config-line)#login local
- S1(config-line)#transport input ssh
- S1(config-line)#transport output ssh
- S1(config-line)#end
- S1(config)#ip ssh version 1|2 is a optional command, by default the IOS uses the latest version supported itself.

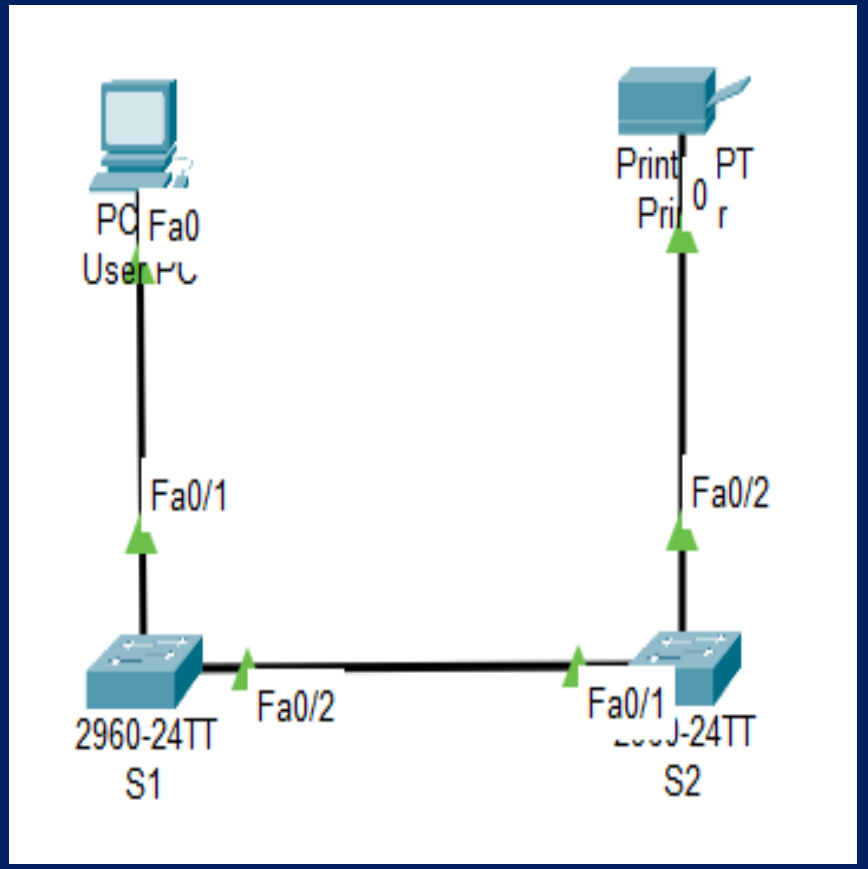
SSH configuration cont__Practice. Packet Tracer



Switch Interface configuration

- Description
- Speed
- Duplex
- Configuring Multiple Interfaces
- Switch Interface Status
- Removing Interface Configuration

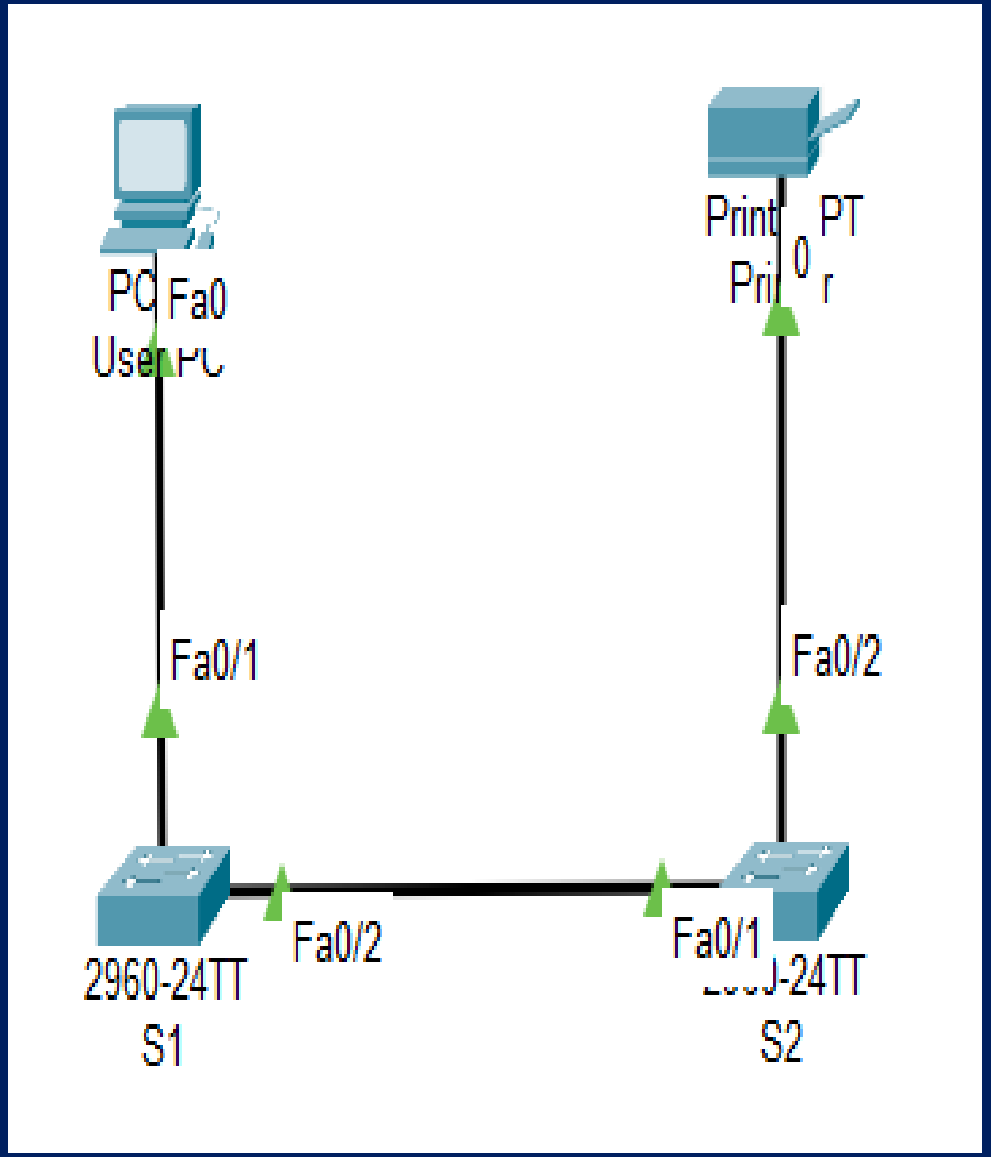
To implement these commands we'll use the topology on the image



Description, Speed, Duplex

- S1(config)#inter fastEthernet 0/1
- S1(config-if)#description to User PC
- S1(config-if)#speed 10 | 100 | auto
- S1(config-if)#duplex half | full | auto
- S1(config-if)#exit
- S1(config)#interface fastethernet 0/2
- S1(config-if)#description to S2
- S1(config-if)#speed 10 | 100 | auto
- S1(config-if)#duplex half | full | auto
- S1(config-if)#exit
- S1(config)#

Task for lab: Configure the same for S2.



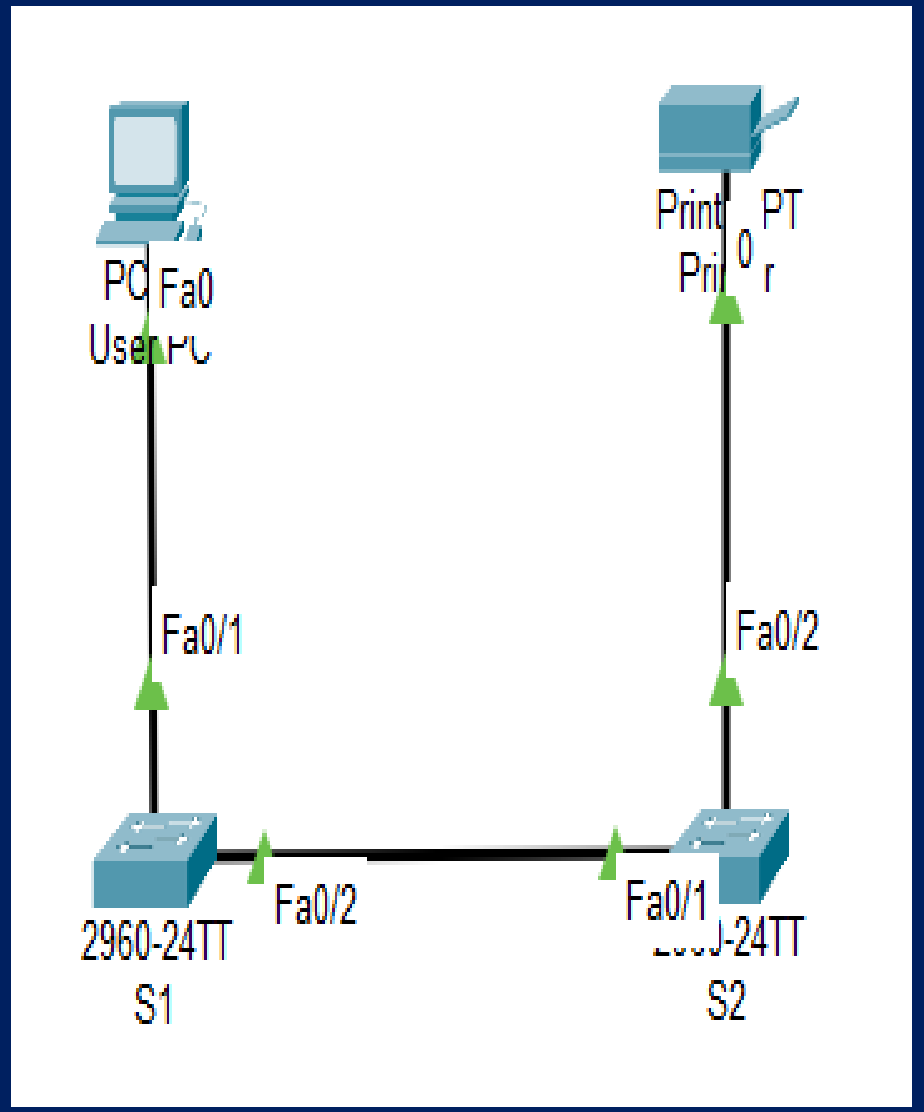
Switch Interface configuration

To configure multiple switch interfaces we use next command.

- S1(config)#interface range fastEthernet 0/1 -2
- S1(config-if-range)#

To confirm switch interface status we use next command.

```
S1#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          auto    auto  10/100BaseTX
Fa0/2                        connected    1          auto    auto  10/100BaseTX
Fa0/3                        notconnect   1          auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        notconnect   1          auto    auto  10/100BaseTX
Fa0/7                        notconnect   1          auto    auto  10/100BaseTX
```



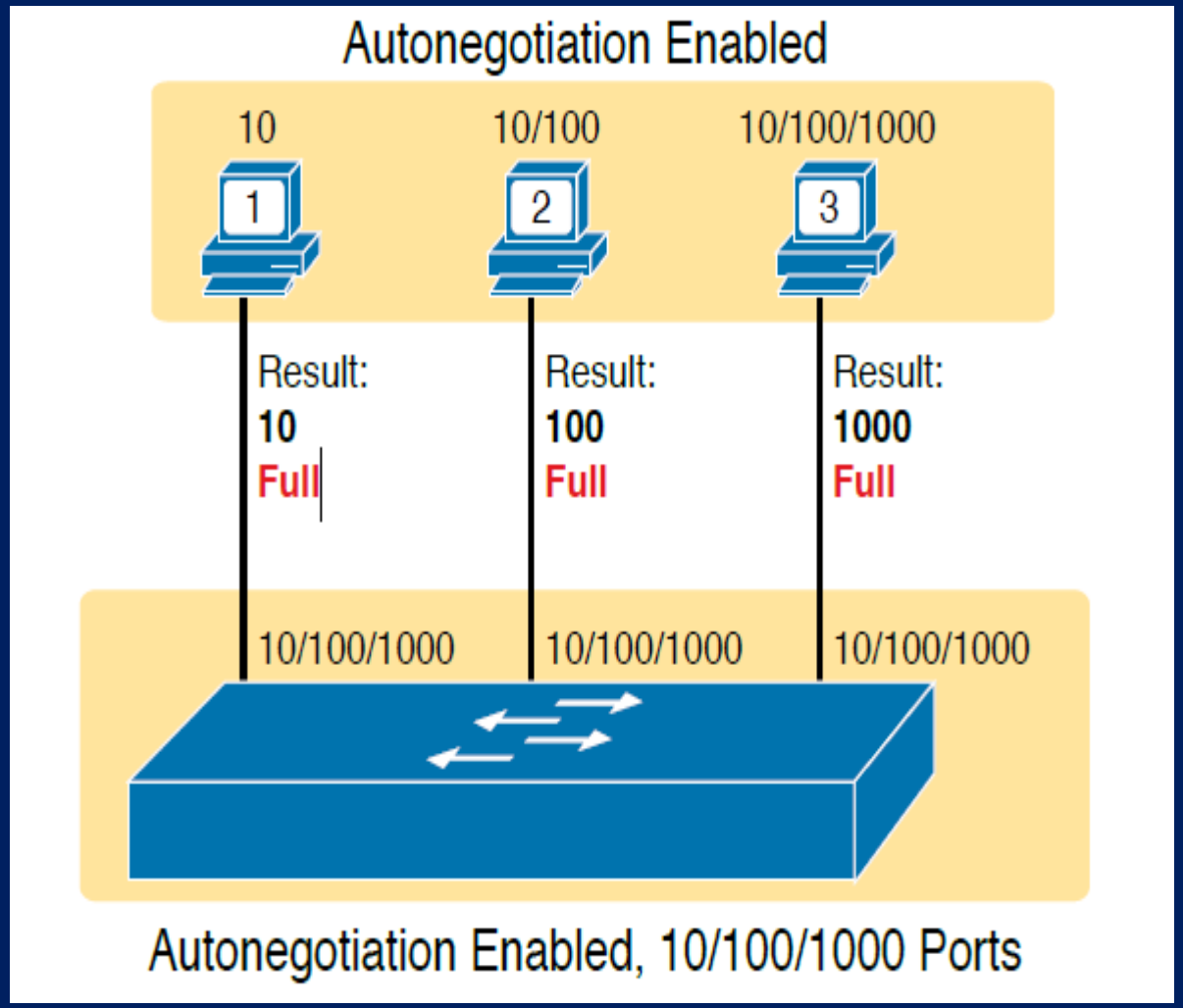
LAN Switch Interface status codes

Line Status	Protocol Status	Interface Status	Typical Root Cause
administratively down	down	disabled	The shutdown command is configured on the interface.
down	down	notconnect	No cable; bad cable; wrong cable pinouts; speed mismatch; neighboring device is (a) powered off, (b) shutdown, or (c) error disabled.
up	down	notconnect	Not expected on LAN switch physical interfaces.
down	down (err-disabled)	err-disabled	Port security has disabled the interface.
up	up	connected	The interface is working.

Autonegotiation

Auto-negotiation is an optional function of the IEEE 802.3u Fast Ethernet standard that enables devices to automatically exchange information over a link about speed and duplex abilities.

For any 10/100 or 10/100/1000 interfaces—that is, interfaces that can run at different speeds—Cisco Catalyst switches default to a setting of **duplex auto** and **speed auto**. As a result, those interfaces attempt to automatically determine the speed and duplex setting to use. Alternatively, we can configure most devices, switch interfaces included, to use a specific speed and/or duplex.

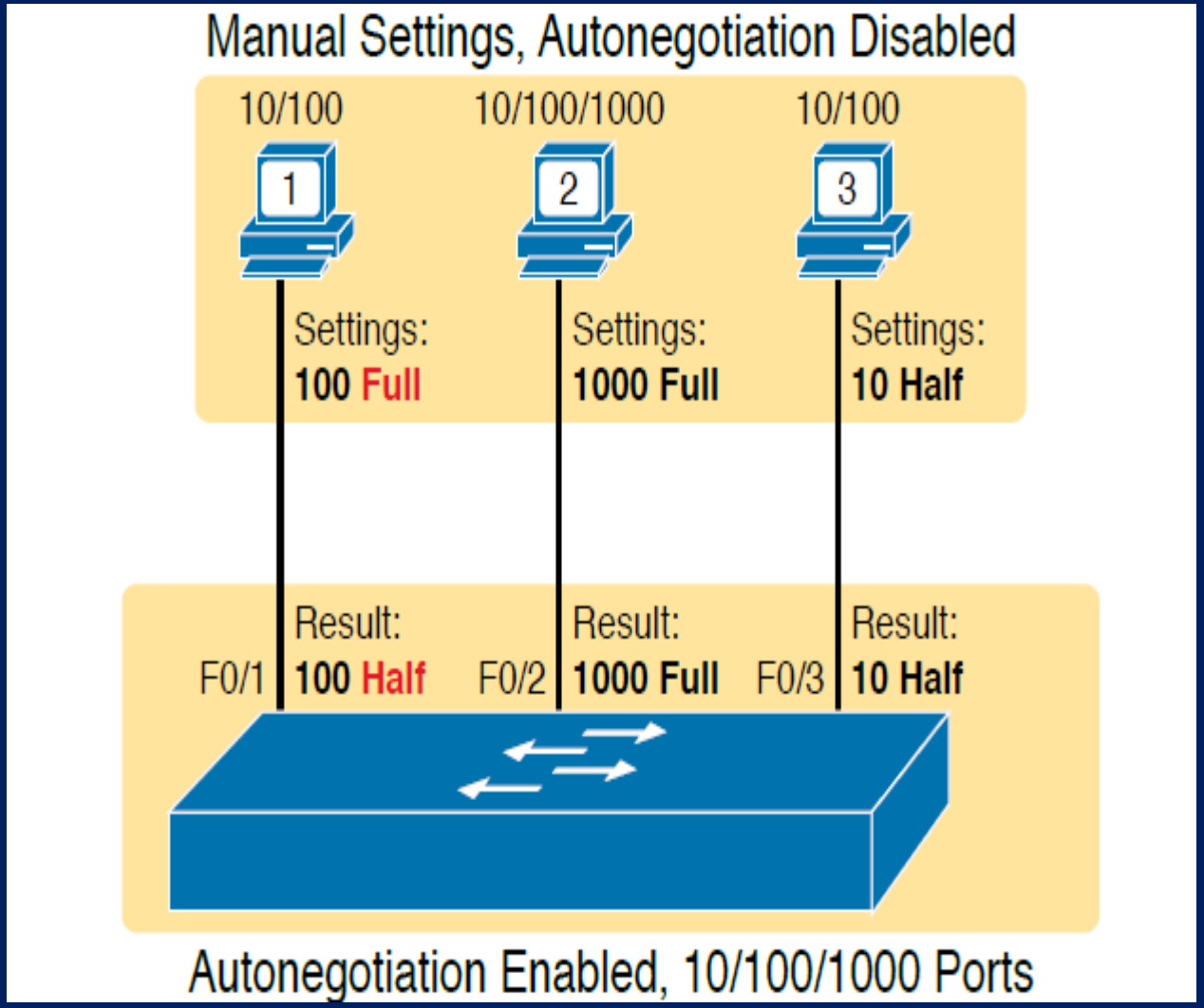


Autonegotiation Enabled, 10/100/1000 Ports

Autonegotiation cont.

If autonegotiation is failed, IEEE has three default rules for speed and duplex.

- Speed: Use your slowest supported speed (often 10 Mbps).
- Duplex: If your speed = 10 or 100, use half duplex; otherwise, use full duplex.



Autonegotiation cont.

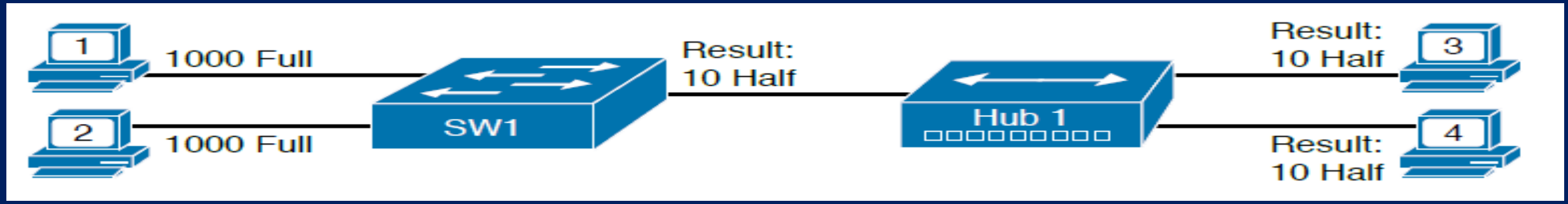
Let’s suppose that we have topology that is shown in the image.

Autonegotiation is enabled in switchports, and as a result the operation mode for PCs are full duplex, speed 1000, for hub is half duplex, speed 10.

If we change the switchport configuration to full duplex, the interface will go down.

Configuration commands:

- SW1(config)#inter fa0/1
- SW1(conf-if)#duplex full



Interface Layer 1 issues (problems)

If the frames don't pass error detection logic of FCS that is implemented in ethernet trailer, there is physical transmission problem. The receiving device discard frame and count input errors. These errors are known as a CRC (Cyclic Redundancy Check) errors.

Using show interfaces command in enable CLI mode we can observe the physical layer problems.

```
SW1# show interfaces fa0/13
! lines omitted for brevity
     Received 284 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 281 multicast, 0 pause input
     0 input packets with dribble condition detected
     95226 packets output, 10849674 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

Interface Layer 1 issues (problems)

- **Runts:** Frames that did not meet the minimum frame size requirement (64 bytes, including the 18-byte destination MAC, source MAC, type, and FCS). Can be caused by collisions.
- **Giants:** Frames that exceed the maximum frame size requirement (1518 bytes, including the 18-byte destination MAC, source MAC, type, and FCS).
- **Input Errors:** A total of many counters, including runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
- **CRC:** Received frames that did not pass the FCS math; can be caused by collisions.
- **Frame:** Received frames that have an illegal format, for example, ending with a partial byte; can be caused by collisions.
- **Packets Output:** Total number of packets (frames) forwarded out the interface.
- **Output Errors:** Total number of packets (frames) that the switch port tried to transmit, but for which some problem occurred.
- **Collisions:** Counter of all collisions that occur when the interface is transmitting a frame.
- **Late Collisions:** The subset of all collisions that happen after the 64th byte of the frame has been transmitted. (In a properly working Ethernet LAN, collisions should occur within the first 64 bytes; late collisions today often point to a duplex mismatch.)

That is all for Lesson 8

The key is :

Learn

Repeat

Practice

You will be able to reach your goals.

GOOD LUCK !!!!!...