



Chapter 5: Switch Configuration

Instructor Materials

CCNA Routing and Switching

Routing and Switching Essentials v6.0



Chapter 5 - Sections & Objectives SMB

5.1 Basic Switch Configuration

5.2 Basic Device Configuration

- Configure the management virtual interface on a switch.
- Configure the port security feature to restrict network access.

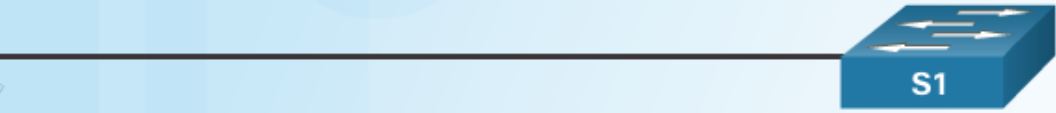
5.1 Configure a Switch with Initial Settings

Switch Boot Sequence





- 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.
- The IOS image can be defined within the BOOT environment variable.
- If the variable is not set, the switch scours through the flash file system searching for an executable image file, loading it into **RAM**, and launching it if found.
- If an executable image file is not found, the switch shows the prompt **switch:** where a few commands are allowed in order to provide access to operating system files found in flash memory and files used to load or reload an operating system.
- If an IOS operating system loads, the switch interfaces are initialized and any commands stored in the **startup-config file** load.

The startup-config file is stored in NVRAM.

Switch Boot Sequence (Cont.)



```
S1 (config) # boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin
```

-  Command
-  Storage Device
-  Path to location in file system
-  Filename of IOS

Recovering From a System Crash

- The boot loader prompt can be accessed through a console connection to the switch:
 1. Cable the PC to the switch console port.
 2. Configure the terminal emulation software on the PC.
 3. Unplug the switch power cord.
 4. 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.

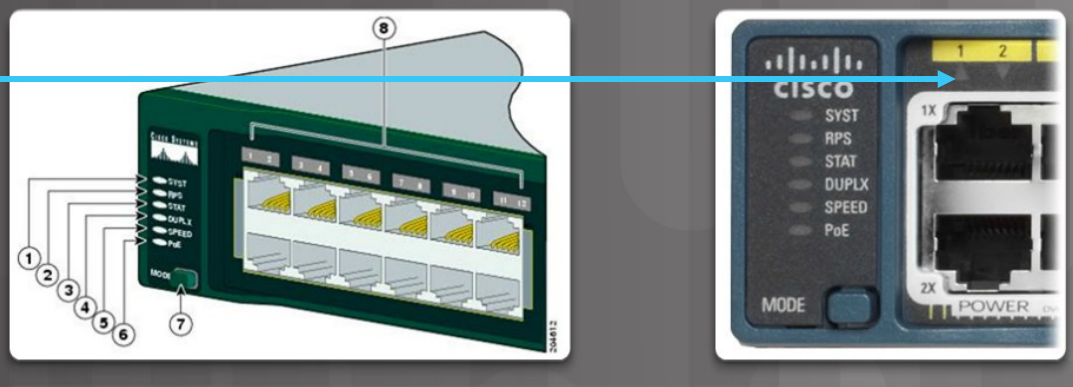
```
switch: dir flash:
Directory of flash:/

 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)
```

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



The diagram shows a Cisco Catalyst 2960 switch with numbered callouts 1 through 8. Callout 1 points to the system LED, 2 to the RPS LED, 3 to the port status LED, 4 to the duplex mode LED, 5 to the speed LED, 6 to the PoE LED, 7 to the mode button, and 8 to the port LEDs. A blue arrow points from the text 'Port LED states:' to the port LEDs. To the right is a close-up of a port with callouts 1 and 2 pointing to the top LEDs.

1	The system LED
2	The RPS LED (if RPS is supported on the switch)
3	The port status LED (This is the default mode.)
4	The port duplex mode LED
5	The port speed LED
6	The PoE status LED (if PoE is supported on the switch)
7	The Mode button
8	The port LEDs

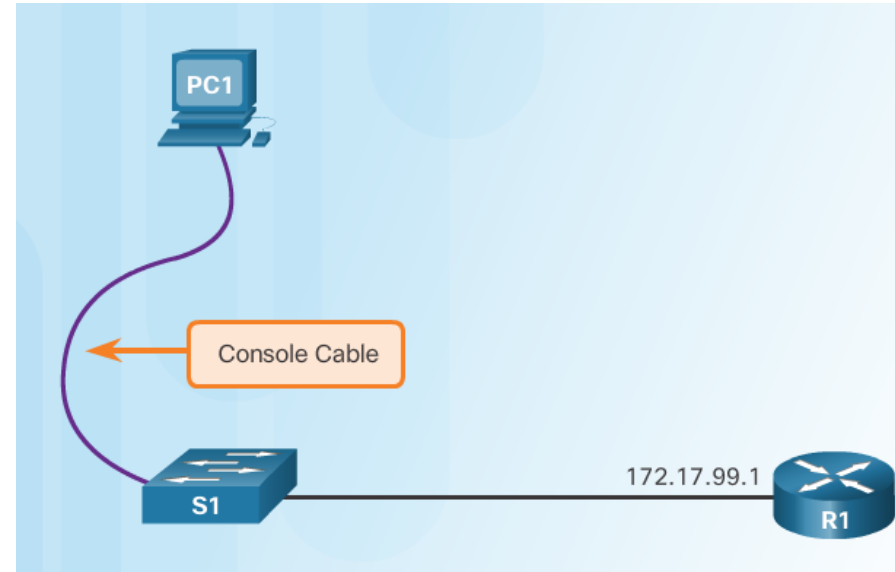


Preparing for Basic Switch Management

- 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.



Remember that the switch console port is on the back of the switch.

Switching Process: Learn

- Examining the Source MAC Address
- Switches examine all incoming frames for new source MAC address information to learn.
- If the source MAC address is unknown, it is added to the table along with the port number.
- If the source MAC address does exist, the switch updates the refresh timer for that entry.
- By default, most Ethernet switches keep an entry in the table for **5 minutes**.

Switching Process: Forward

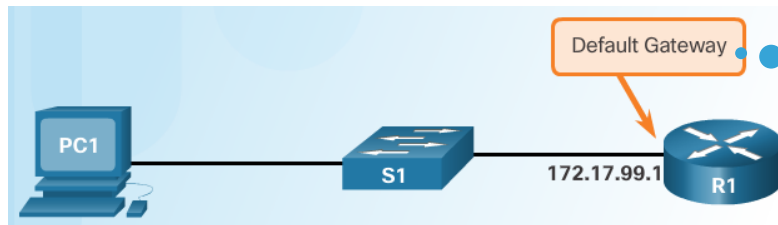
- Examining the Destination MAC Address
- If the destination MAC address is a **broadcast or a multicast**, the frame is also flooded out all ports except the incoming port.
- If the destination MAC address is a **unicast** address, the switch will look for a match in its MAC address table.
- If the destination MAC address **is in the table**, it will forward the frame out the specified port.
- If the destination MAC address **is not in the table** (i.e., an unknown unicast) the switch will **forward** the frame out all ports except the incoming port.

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



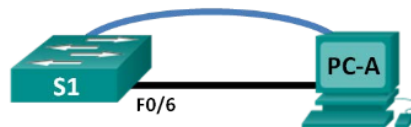
The default gateway is the router address and is used by the switch to communicate with other networks.

Basic Switch Configuration



Lab – Configuring Basic Switch Settings

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Cable the Network and Verify the Default Switch Configuration

Part 2: Configure Basic Network Device Settings

- Configure basic switch settings.
- Configure the PC IP address.

Part 3: Verify and Test Network Connectivity

- Display device configuration.
- Test end-to-end connectivity with ping.
- Test remote management capabilities with Telnet.
- Save the switch running configuration file.

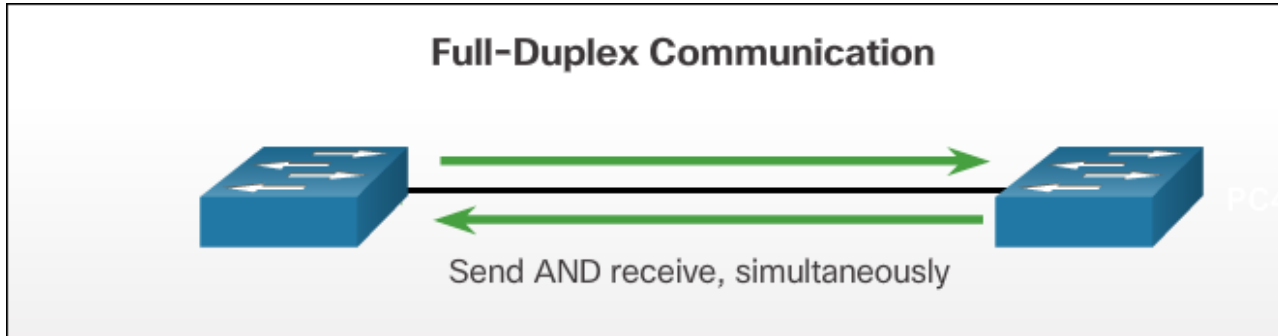
Part 4: Manage the MAC Address Table

- Record the MAC address of the host.
- Determine the MAC addresses that the switch has learned.
- List the `show mac address-table` command options.

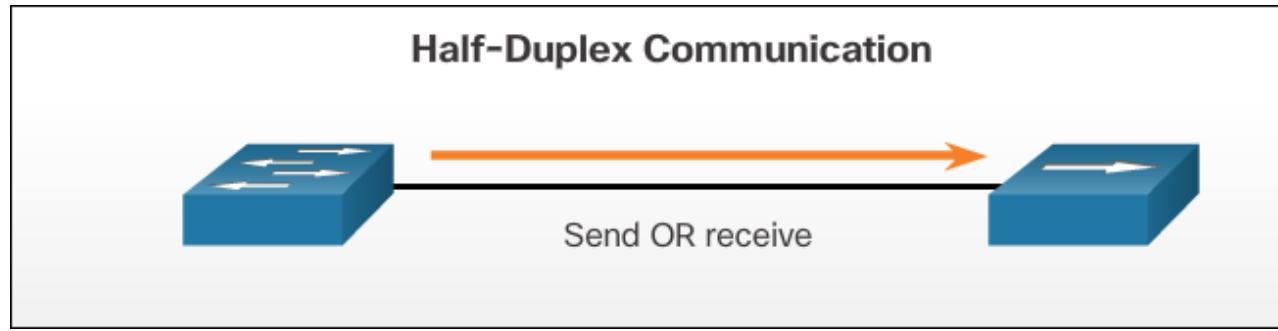
Duplex Communication

- Gigabit Ethernet and 10Gb Ethernet NICs require full-duplex connections to operate.

Bidirectional communication



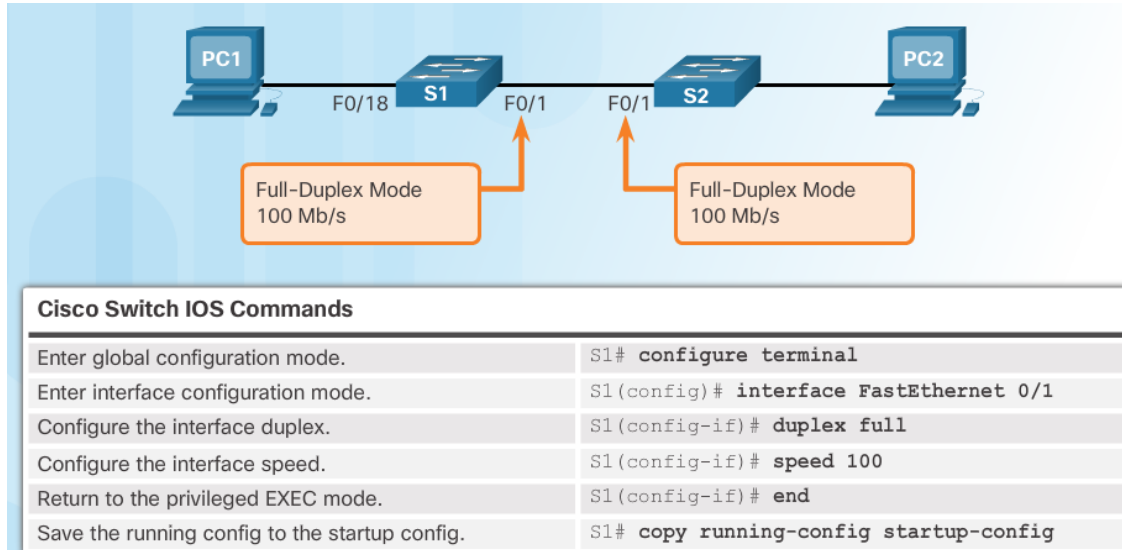
Unidirectional communication



Obvody pro detekci kolize jsou vypnuty

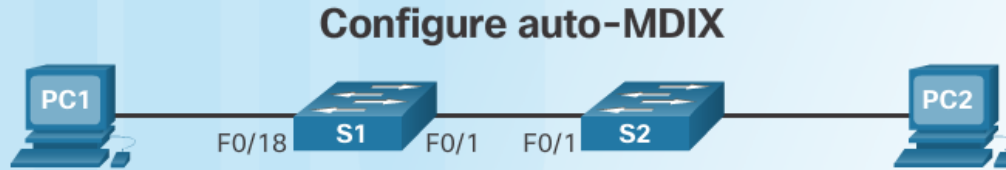
Configure Switch Ports at the Physical Layer

- Some switches have the default setting of auto for both duplex and speed.
- Mismatched duplex and/or speed settings can cause connectivity issues.
- Always 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.

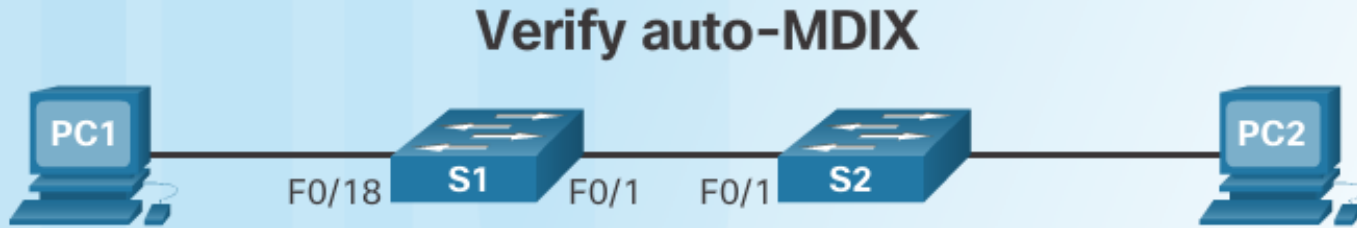


Cisco Switch IOS Commands

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

Auto-MDIX (Cont.)

- Use the **show controllers Ethernet-controller** command to verify auto-MDIX settings.



```
S1# show controllers ethernet-controller fa 0/1 phy | include Auto-MDIX
Auto-MDIX      : On   [AdminState=1   Flags=0x00056248]
S1#
```


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
```

Verifying Switch Port Configuration (Cont.)

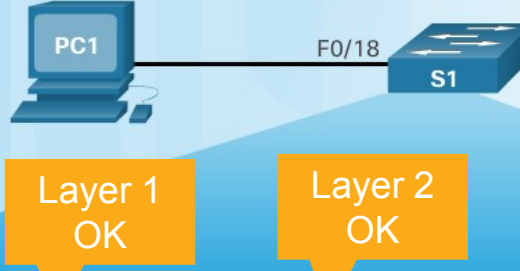
Running Configuration



```
S1# show running-config
Building configuration...
<output omitted>
Current configuration : 1664 bytes
!
!
interface FastEthernet0/18
  switchport access vlan 99
  switchport mode access
!
<output omitted>
!
interface Vlan99
  ip address 172.17.99.11 255.255.255.0
!
```

Verifying Switch Port Configuration (Cont.)

Interface Status



PC1 — F0/18 — S1

Layer 1 OK

Layer 2 OK

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.8a01
  (bia 0cd9.96e8.8a01)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes);
  Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

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

Network Access Layer Issues (Cont.)

```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast Ethernet, address is
0022.91c4.0e01 (bia 0022.91c4.0e01)MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0
  throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 multicast, 0 pause input
  0 input packets with dribble condition detected
  3594664 packets output, 436549843 bytes, 0 underruns
  8 output errors, 1790 collisions, 10 interface resets
  0 unknown protocol drops
  0 babbles, 235 late collision, 0 deferred
<output omitted>
```

Error Type	Description
Input Errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1,518 bytes is considered a giant.
CRC	CRC errors are generated when the calculated checksum is not the same as the checksum received.
Output Errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
Collisions	Number of messages retransmitted because of an Ethernet collision.
Late Collisions	A collision that occurs after 512 bits of the frame have been transmitted.

Late collision

```
CSW1# show interface FastEthernet 0/1 | include duplex
Half-duplex, 10Mb/s, media type is 10/100Base TX
```

```
CSW1# show interfaces FastEthernet 0/1 counters errors
```

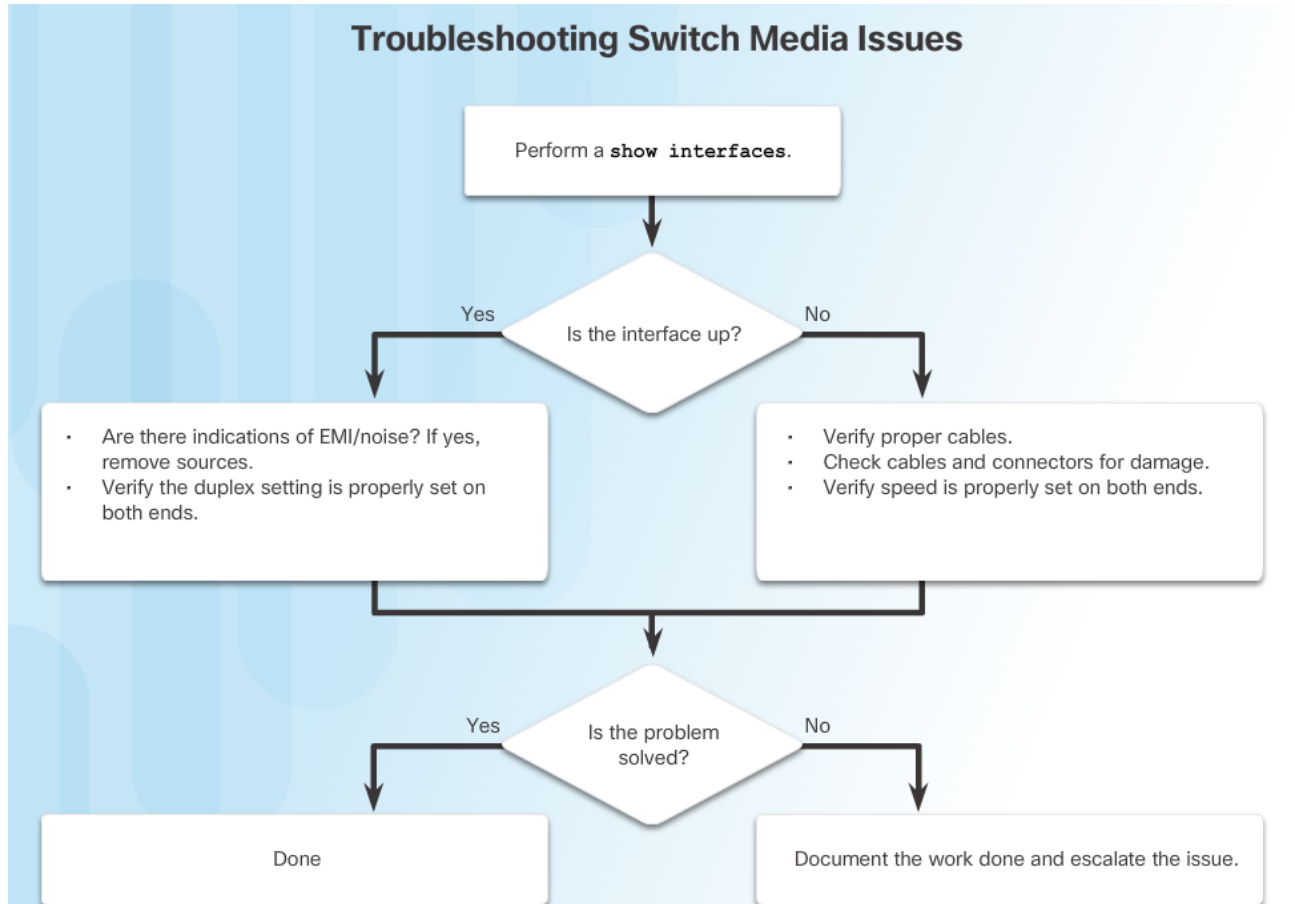
Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize	OutDiscards
Fa0/1	0	0	0	0	0	0

Port	Single-Col	Multi-Col	Late-Col	Excess-Col	Carri-Sen	Runts	Giants
Fa0/1	664	124	12697	0	0	0	44

Pozdní kolize jsou problémem, protože jakmile NIC zmešká skutečnost, že došlo ke kolizi, zotavení a opakovaný přenos jsou ponechány na horních vrstvách a doba zotavení drasticky vzroste. Zatímco síťová karta obvykle obnoví a znovu vysílá rámeček za **2 –3 ms**, u horních vrstev trvá obvykle **10x až 100x déle**.

Troubleshooting Network Access Layer Issues

Troubleshooting Switch Media Issues



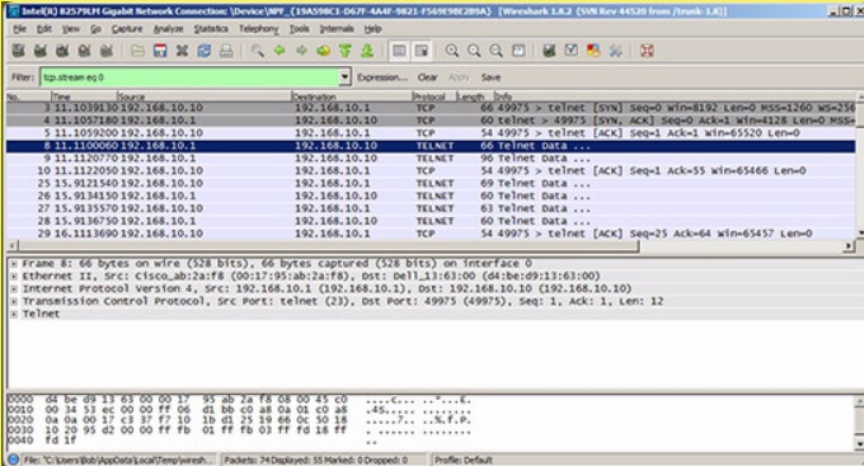
5.2 Switch Security

SSH Operation

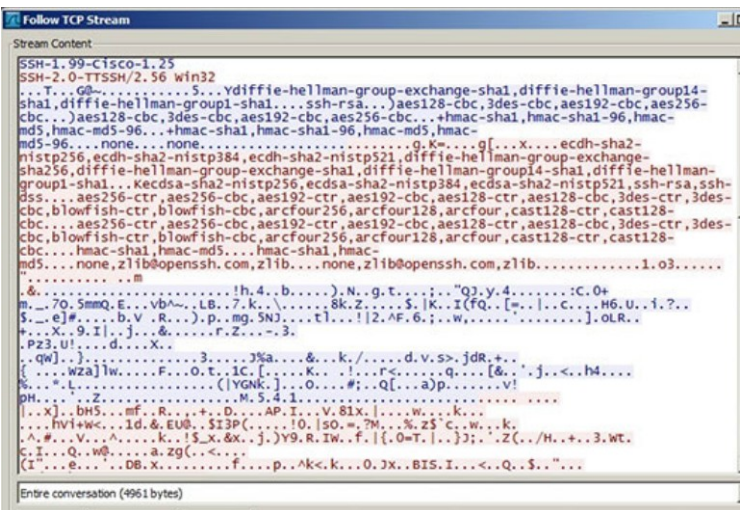
- Secure Shell (SSH)

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

Wireshark Capture of Telnet




Wireshark Capture of SSH



SSH Operation (Cont.)

- A switch must have an IOS version (**k9 at the end of the IOS file name**) that includes cryptographic capabilities in order to configure and use SSH.
- Use the **show version** command to see the IOS version.

```
S1> show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M),
Version 15.0(2)SE, RELEASE SOFTWARE (fc1)
<output omitted>
```



Configuring SSH

- 1. Verify SSH support.
- 2. Configure the IP domain name.
- 3. Generate RSA key pairs.
- 4. Configure user authentication.
- 5. Configure the vty lines.
- 6. Enable SSH version 2.

The `login local` command forces the use of the local database for username/password.

Commonly forgotten command that is used in key generation

```
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin secret ccna
S1(config-line)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)# exit
S1#
```

Default is to accept both Telnet and SSH (transport input all)

Configure PuTTY SSH Client Connection Parameters



Verifying SSH

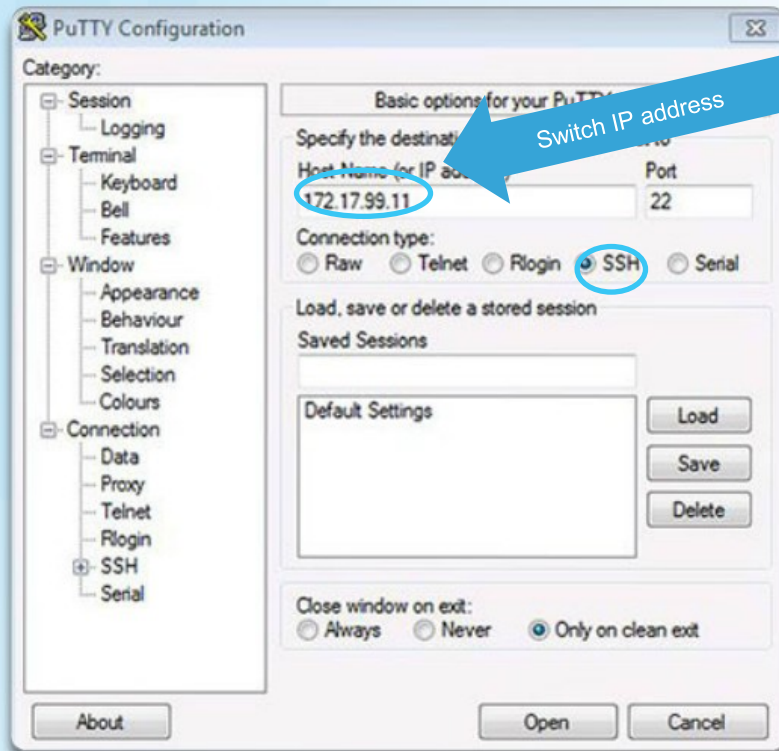
- On the PC, connect to the switch using SSH.

Packet Tracer: `ssh -l 172.17.99.11`

172.17.99.11 - PuTTY

```
Login as: admin
Using keyboard-interactive
authentication.
Password:

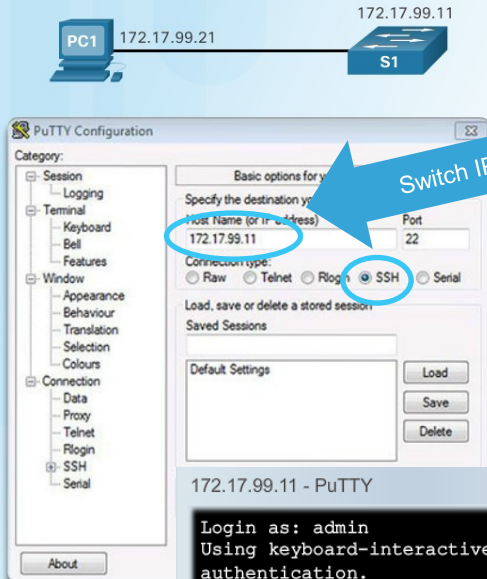
S1>enable
Password:
S1#
```



Verifying SSH

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

Configure PuTTY SSH Client Connection Parameters



172.17.99.11 - PuTTY

```
Login as: admin
Using keyboard-interactive
authentication.
Password:
```

```
S1>enable
Password:
S1#
```

Verify SSH Status and Settings

172.17.99.21

172.17.99.11

PC1

S1

```
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 AAAAB3NzaC1yc2EAAAADAQABAAQgQCdLksVz2Q1REsoZt2f2scJHbW3aMDM8 /8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVN1QhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAaP3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO880UJL3Q==

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#
```

The PC is using SSH to communicate and issue commands on the switch.

Packet Tracer – Configuring SSH

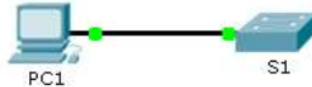


Cisco Networking Academy®

Mind Wide Open™

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

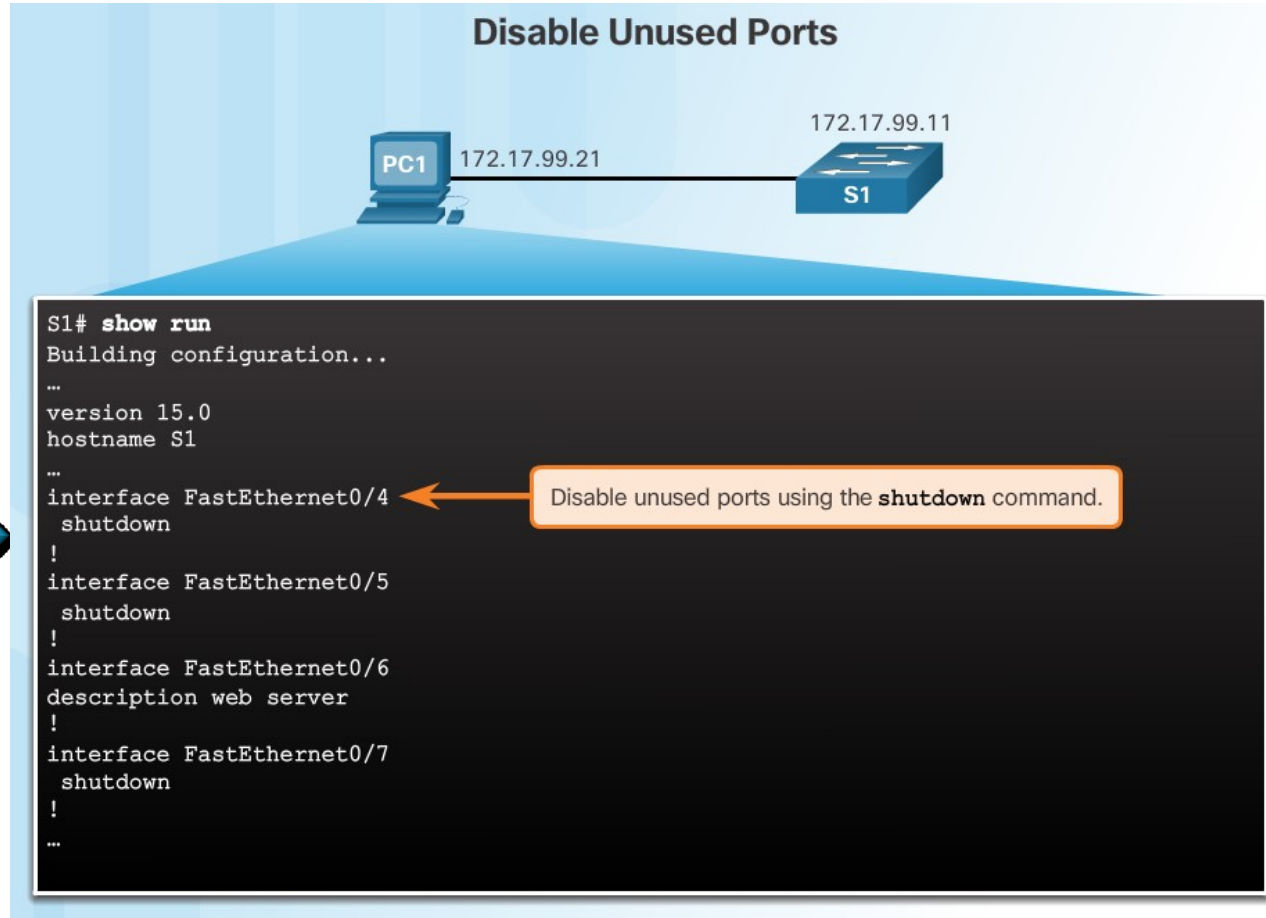
Part 2: Encrypt Communications

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.

Secure Unused Ports



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

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**
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*

Note: **Disabling sticky learning converts sticky MAC addresses to dynamic secure addresses and removes them from the running-config.**

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 example: 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 to enable port security on an interface.

Configure Dynamic Port Security



Cisco IOS CLI Commands

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

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
```

Port Security: Verifying

- Use the **show port-security interface** command to verify the maximum number of MAC addresses

```
S1# show port-security interface fastethernet 0/19
```

```
Port Security           : Enabled
Port Status             : SecureSticky-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
```

Port Security: Verifying (Cont.)

- Use the **show running-config** command to see learned MAC addresses added to the configuration.

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
  switchport mode access
  switchport port-security maximum 10
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0025.83e6.4b02
```


Port Security: Verifying (Cont.)

- The **show port-security address** command shows how MAC addresses were learned on a particular port.

```
S1# show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address          Type                Ports      Remaining Age
-----  -
1       0025.83e6.4b01      SecureDynamic       Fa0/18     -
1       0025.83e6.4b02      SecureSticky        Fa0/19     -
-----
```

Ports in Error Disabled State

- Switch console messages display when a port security violation occurs. Notice the port link status changes to down.

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18,
putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

Ports in Error Disabled State (Cont.)

- Check the port status and the port security settings.

```
S1# show interface fa0/18 status
```

Port Name	Status	Vlan	Duplex	Speed	Type
Fa0/18	err-disabled	1	auto	auto	10/100BaseTX

```
S1# show port-security interface fastethernet 0/18
```

```
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 0
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 000c.292b.4c75:1
Security Violation Count : 1
```

Ports in Error Disabled State (Cont.)

- Do not re-enable a port until the security threat is investigated and eliminated.
- Notice that you must first **shut** the port down and **then** issue the **no shutdown** command in order to use the particular port again after a security violation has occurred.

```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/18, changed state to up
```

Hrátky s časem

Parameter	Description
<code>static</code>	Enable aging for statically configured secure addresses on this port.
<code>time <i>time</i></code>	Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
<code>type absolute</code>	Set absolute aging type. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
<code>type inactivity</code>	Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Typická konfigurace



Switch(config-if)#

```
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security violation shutdown
switchport port-security mac-address sticky
switchport port-security aging time 120
```

Jiný typický příklad

```
Switch(config)#hostname S2
```

```
S2(config)#interface fastEthernet 0/1
```

```
S2(config-if)#switchport mode access
```

```
S2(config-if)#switchport port-security
```

```
S2(config-if)#switchport port-security maximum 1
```

```
S2(config-if)#switchport port-security mac-address sticky
```

```
S2(config-if)#switchport port-security violation shutdown
```

```
S2(config-if)#exit
```

```
S2(config)#
```

Packet Tracer – Configuring Switch Port Security

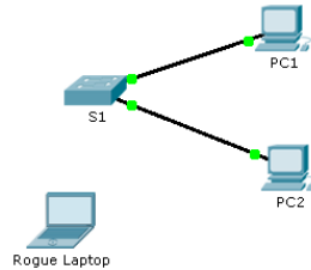


Cisco Networking Academy®

Mind Wide Open™

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

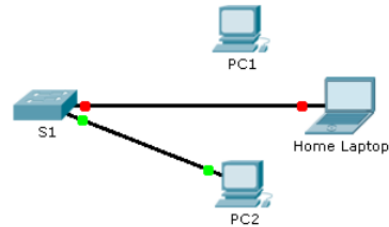
In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

Packet Tracer – Troubleshooting Switch Port Security



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 – Configuring Switch Security Features



Cisco Networking Academy®

Mind Wide Open™

Lab – Configuring Switch Security Features

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Objectives

Part 1: Set up the Topology and Initialize Devices

Part 2: Configure Basic Device Settings and Verify Connectivity

Part 3: Configure and Verify SSH Access on S1

- Configure SSH access.
- Modify SSH parameters.
- Verify the SSH configuration.

Part 4: Configure and Verify Security Features on S1

- Configure and verify general security features.
- Configure and verify port security.

5.3 Chapter Summary

Packet Tracer - Skills Integration Challenge

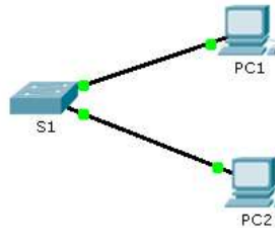


Cisco Networking Academy®

Mind Wide Open™

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.

Nutné k zapamatování

```
config t
interface vlan 99
ip address 172.17.99.11
255.255.255.0
no shutdown
ip default-gateway 172.16.99.1
(address on the router that is on the
same 172.17.99.0 network)
vlan 99
name Management
exit
```

? is a KEY to IOS. Prompts

- Switch> (User EXEC mode that is shown when a switch first boots)
- Switch# (Privileged EXEC mode that is shown after someone types **enable**)
- switch: (Boot loader mode shown when a switch does not have, or cannot find, an operating system)

sh boot

```
Switch#show boot
BOOT path-list      :
Config file        : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break       : no
Manual Boot        : no
HELPER path-list   :
Auto upgrade       : yes
NVRAM/Config file
    buffer size:    65536
Switch#
```

