Introduccion a redes Conmutadas

RAUL BAREÑO GUTIERREZ

Cisco | Networking Academy®
Mind Wide Open™

Objetivos

- Explicar las ventajas y desventajas del enrutamiento estático
- Configuración de los ajustes iníciales en un switch Cisco
- Configurar puertos del switch
- Configurar la interfaz de administración del switch y la interface virtual
- Describir los ataques de seguridad básicos
- Describir las mejores prácticas de seguridad
- Configurar la función de seguridad del puerto para restringir el acceso de red

Secuencia de arranque del Switch

1. Arranca el POST
2. Ejecuta el software de gestor de arranque
3. El gestor de arranque hace la inicialización de bajo nivel de la CPU.
4. El gestor de arranque inicializa el sistema de archivos en la flash.
5. El gestor de arranque localiza y carga la imagen de software por defecto del sistema operativo IOS en la memoria y pasa el control de switch al IOS.

Cambie la secuencia de arranque

El switch pasa por los siguientes pasos.

1. Realiza una búsqueda de arriba hacia abajo a través del sistema de archivos flash. Se carga y ejecuta el primer archivo ejecutable, si puede

2. El IOS inicializa las interfaces que se encuentran en el archivo de configuración de inicio (startup-config), almacenado en la NVRAM.

3. Nota: el sistema de comandos de arranque (**boot system)** se puede utilizar para establecer las condiciones de entorno de arranque

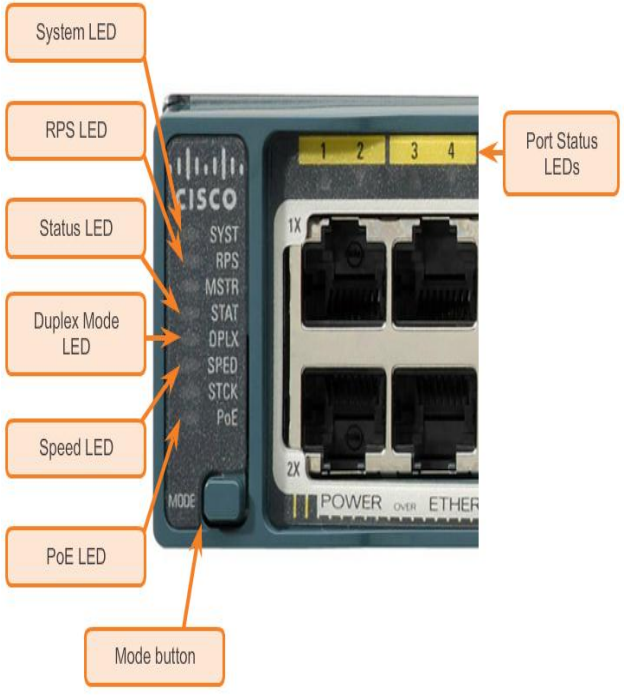
Recuperación de un fallo del sistema

- Si el IOS no puede ser cargado.
- El gestor de arranque se puede acceder a través de la conexión de la consola usando:
  1. Conectando el PC y un cable de consola al puerto de consola del switch. Desconecte el cable de alimentación del switch.
  2. Vuelva a conectar el cable de alimentación al switch y presione y manténgalo presionado el botón Mode.
  3. El LED del Sistema enciende brevemente, y toma el color ámbar y verde. Suelte el botón Mode
- El interruptor de arranque del switch: prompt aparece en el emulador de terminal (consola) en el PC.

Cambios Indicadores de LED

- Cada puerto de los switches tiene un indicador de luces de estado LED.
- Estas luces LED reflejan la actividad portuaria también otra información sobre el switch a través del botón mode
- Los modos que están disponibles

  LED del sistema
  LED Sistema de alimentación redundante (RPS)
  LED de estado del puerto
  LED de puerto Duplex
  LED de Velocidad de puerto
  LED Alimentación a través de (PoE)



Preparación para la administración del switch

- **Para la administración remota** switch, tiene que ser configurado para acceder a la red

- Una dirección IP y la máscara de subred deben configurarse. Y la puerta de enlace predeterminada también debe configurarse.

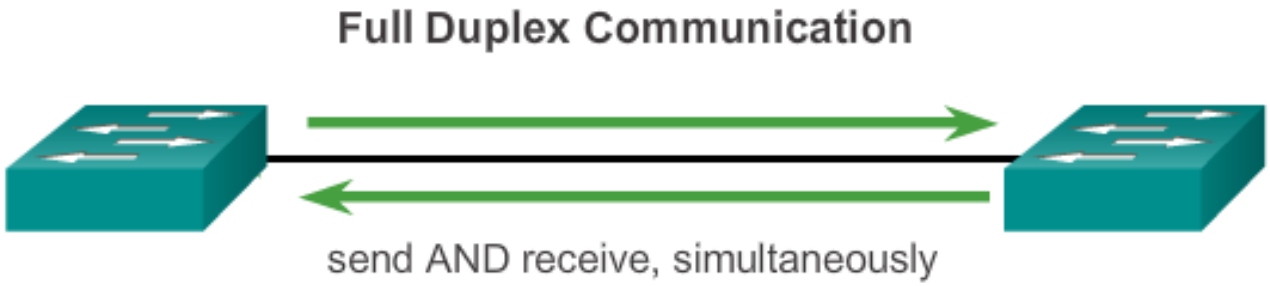
- La información IP (la dirección IP, máscara de subred, y la puerta de enlace) se va a asignar a la SVI (interfaz virtual del switch).

Preparación para la administración del switch

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for the SVI.	S1(config)# **interface vlan99**
Configure the management interface IP address.	S1(config-if)# **ip address 172.17.99.11**
Enable the management interface.	S1(config-if)# **no shutdown**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

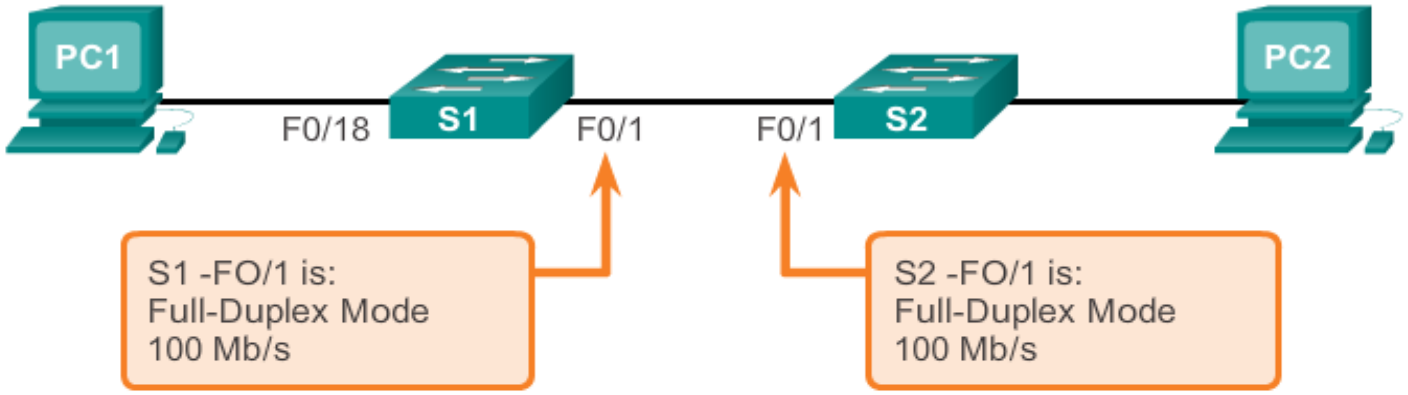
Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Configure the default gateway for the switch.	S1(config)# **ip default-gateway 172.17.99.**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Comunicación Dúplex



Configurar Puertos del switch en la capa física

Configure Duplex and Speed



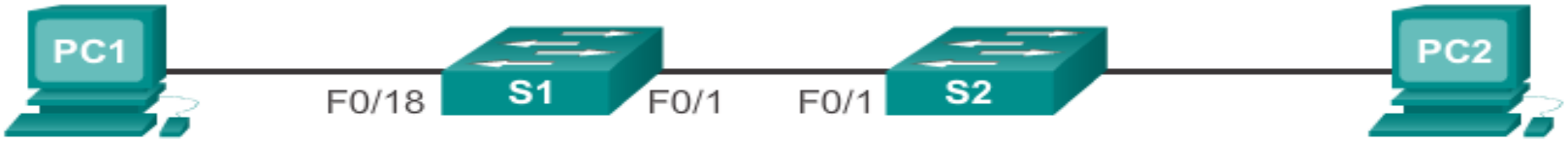
Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface fastethernet 0/1**
Configure the interface duplex.	S1(config-if)# **duplex full**
Configure the interface speed.	S1(config-if)# **speed 100**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Caracteristicas de auto MDIX

- Se requieren ciertos tipos de cable (directo o cruzado) para conectar dispositivos.
- El medio automáticamente depende de la interface cruzada (auto-MDIX).
- Cuando el auto-MDIX se habilita, la interfaz detecta y configura automáticamente la conexión.
- Al usar auto-MDIX en una interfaz, la velocidad de la interfaz y el dúplex se deben establecer en auto

Caracteristicas de auto MDIX

Enable auto-MDIX



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**

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

Verificando la configuración de Switch

Verification Commands

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**
Displays info about flash filesystem.	S1# **show flash**
Displays system hardware & 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**

Asuntos de la capa de acceso de red

Display interface status and statistics.

```
S1# show interface 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>
```

Asuntos de la capa de acceso de red

Pequeños

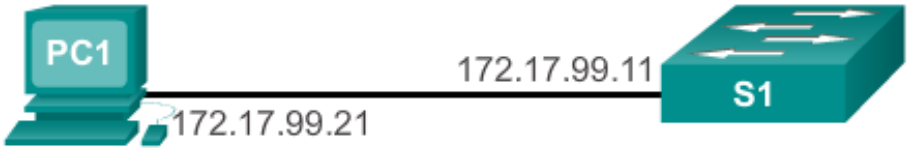
Grandes

Parameter	Description
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 1518 bytes is considered a giant.
Input errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
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	Jammed signal could not reach to ends.

Acceso remoto seguro **SSH**

- SSH es un protocolo que Proporciona una conexión segura (cifrada) a un dispositivo remoto
- SSH se utiliza comúnmente en sistemas basados en UNIX.
- Se requiere una versión del software IOS con las características y capacidades de cifrado (cifrado) para permitir SSH
- Debido a sus fuertes características de cifrado, SSH debe reemplazar a Telnet para conexiones de administración.
- SSH utiliza el puerto TCP 22 por defecto. Telnet utiliza el puerto TCP 23

SSH Operación

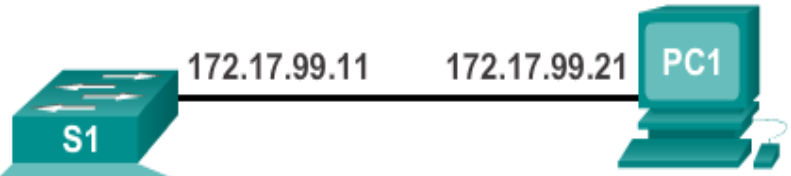


172.17.99.11 - PuTTY

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

S1>enable
Password:
S1#
```

Configuración de SSH y verificación




```
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 password ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config)# end
```

```
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
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

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

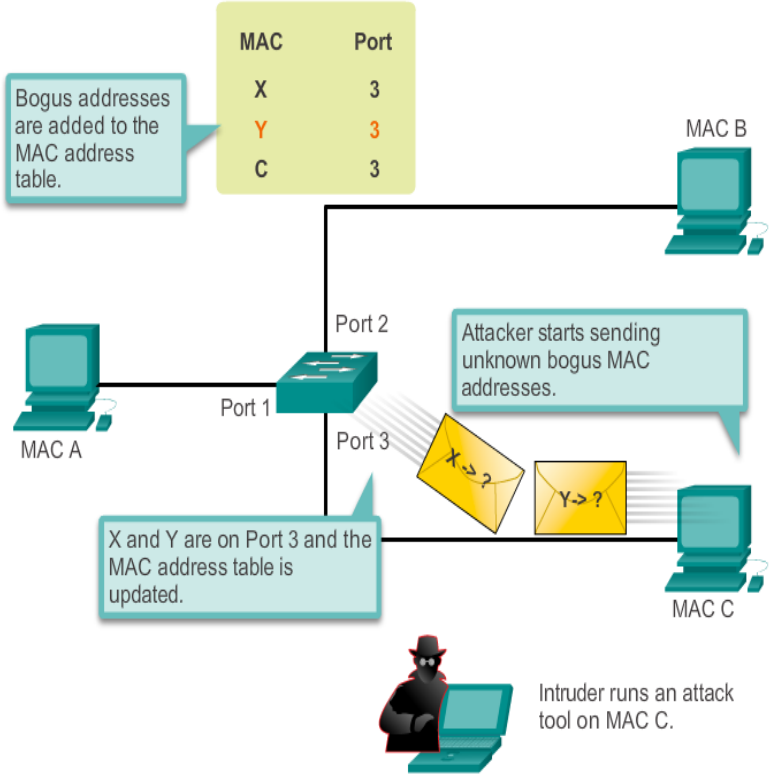
Problemas de seguridad en LAN? Inundaciones de las direcciones MAC

- Los switch automáticamente llenan sus tablas CAM por inundación del tráfico que entran a sus puertos.
- Los switch enviarán tráfico a todos los puertos si no puede encontrar el destino de la MAC en su tabla CAM.

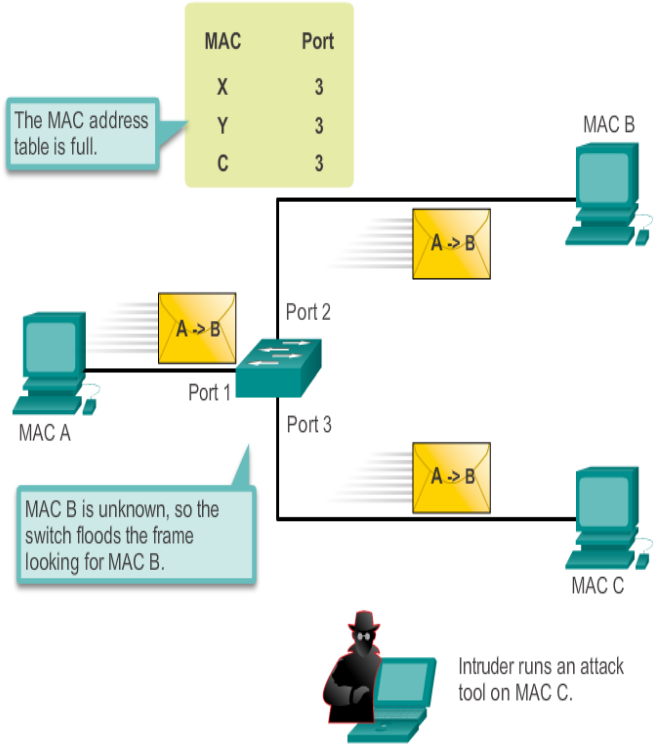
- El switch actúa como un hub. El Tráfico unicast puede ser visto por todos los dispositivos conectados.
- Un atacante podría utilizarlo para obtener acceso al tráfico, normalmente controlado por el switch. puede ejecutar una herramienta de inundaciones MAC

Problemas de seguridad en LAN? Inundaciones de las direcciones MAC

- Atacante inundando la tabla CAM con entradas falsas



- Ahora se comporta como un hub



Problemas de seguridad en LAN? Suplantación de DHCP

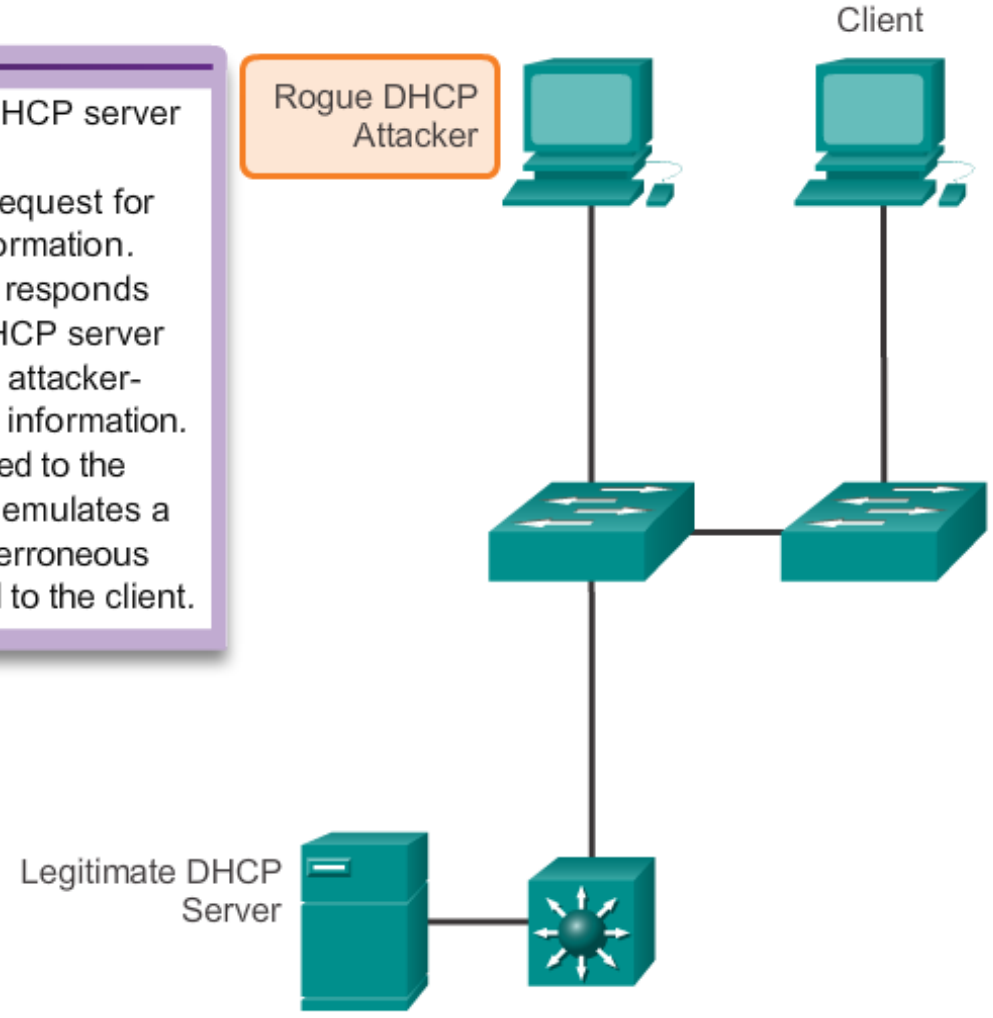
- DHCP se utiliza para asignar automáticamente información IP.
- Existen dos tipos de ataques de DHCP:
  1. Suplantación de DHCP
- 2. Reservación de DHCP

- En suplantación, el servidor DHCP falso se coloca en la red para emitir direcciones DHCP a los clientes.
- En reservación de DHCP utilizado para saturar las IP del servidor DHCP legítimo.

Suplantación de DHCP

- Ataque de suplantacion de DHCP

1) An attacker activates a DHCP server on a network segment.
2) The client broadcasts a request for DHCP configuration information.
3) The rogue DHCP server responds before the legitimate DHCP server can respond, assigning attacker-defined IP configuration information.
4) Host packets are redirected to the attacker's address as it emulates a default gateway for the erroneous DHCP address provided to the client.



Aprovechando CDP

- CDP es un protocolo propietario de Cisco de Capa 2 utilizado para descubrir otros dispositivos de Cisco que están conectados directamente.
- Diseñado para permitir a los dispositivos auto-configurar sus conexiones.
- Si un atacante está escuchando mensajes CDP, pueda aprender información importante, como el modelo del dispositivo, la versión del software que se ejecuta.
- Se recomienda deshabilitar CDP cuando sea posible.

Aprovechando Telnet

- Como se ha mencionado el protocolo Telnet es inseguro y debería ser sustituido por SSH.
- A pesar de que un atacante puede utilizar parte de Telnet para otros ataques. Dos ataques son ataque de fuerza bruta, para la contraseña y de ataque de DoS para Telnet .
- la contraseña se conoce como ataque de fuerza bruta a la contraseña.
- Telnet se puede utilizar para testear la contraseña al iniciar el sistema.

Aprovechando Telnet

- **En el ataque DoS Telnet**, el atacante explota un fallo en el software del servidor de Telnet.

- ataque impide que un administrador Acceda remotamente a cambiar las funciones de gestión del switch. Durante un tiempo.

- Las Vulnerabilidades en el servicio telnet permite el ataque de denegación se minimiza generalmente con parches de seguridad Que se incluyan en las nuevas revisiones de Cisco IOS.

Prácticas recomendadas de seguridad? 10 Mejores Prácticas

- Crear una política de seguridad por escrito en la organización.
- Deshabilite los servicios y los puertos no utilizados.
- Utilice contraseñas seguras y cámbielas con frecuencia.
- Controlar el acceso físico a los dispositivos.
- Utilizar HTTPS en lugar de HTTP.
- Realizar las operaciones de copia de seguridad regularmente.
- Educar a los empleados sobre los ataques de ingeniería social.
- Encriptar y proteger con contraseña los datos sensibles.
- Implemente firewalls.
- Mantenga actualizado el software al día

Herramientas de seguridad de red: Opciones

- Son muy importantes para los administradores de red.
- Permiten revisar las medidas de seguridad.
- Un administrador puede lanzar un ataque contra la red y analizar los resultados.
- Determina cómo ajustar las políticas de seguridad para mitigar esos tipos de ataques.
- **La auditoría de seguridad y pruebas de penetración** son dos funciones básicas que las herramientas de seguridad de red realizan.

Herramientas de seguridad de red: Auditorías

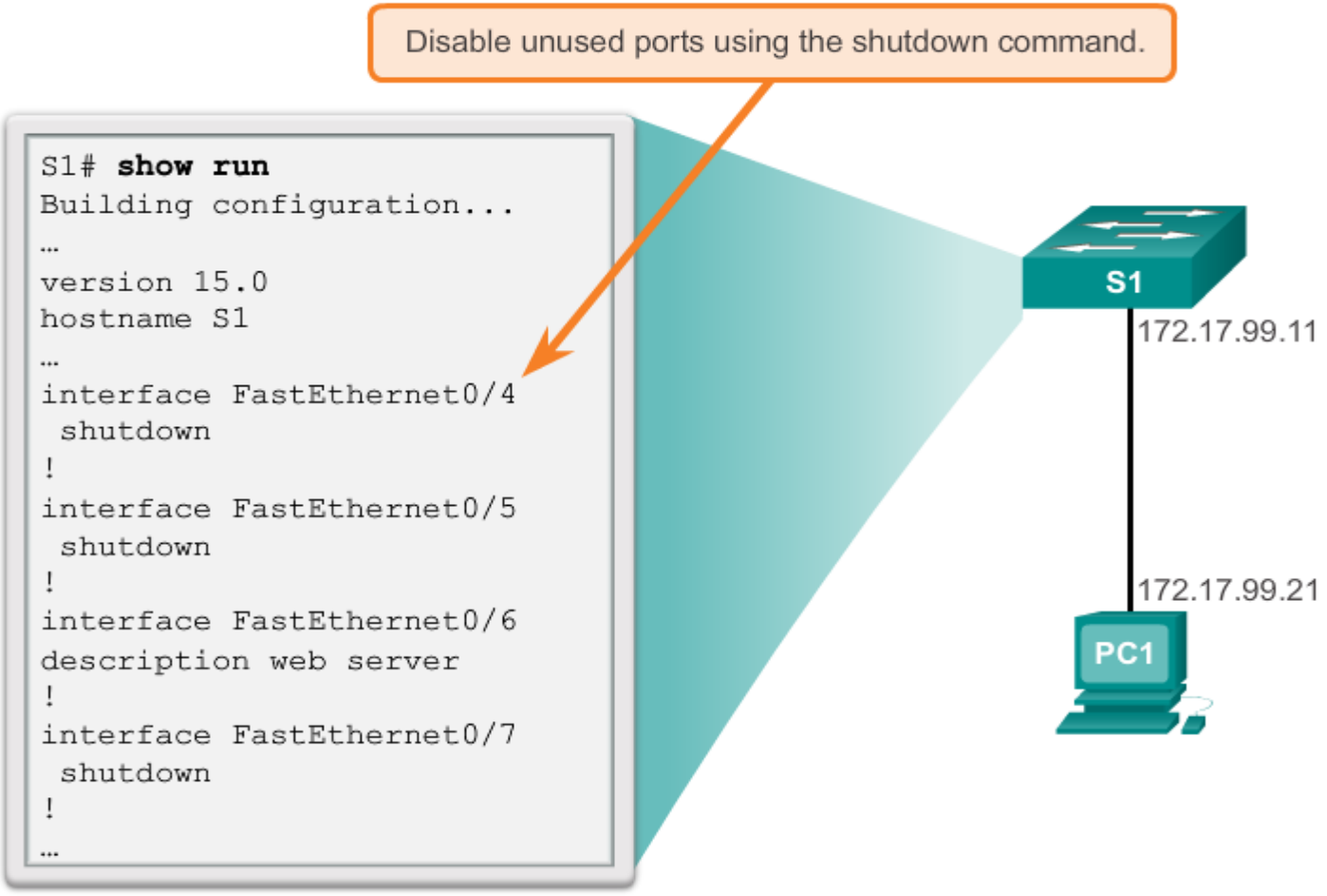
- Se puede utilizar para auditar la red.
- Mediante el control de la red, se evalua qué tipo de información un atacante sería capaz de reunir.
- Al atacar e inundar la tabla CAM del switch, un administrador podría saber qué puertos de switch son vulnerables a las inundaciones MAC y corregir el problema.
- Se pueden utilizar son las herramientas de **pruebas de penetración.**

Herramientas de seguridad de red: Auditorías

- Las pruebas de penetración es un ataque simulado.
- Determina la vulnerabilidad de la red Cuando se encuentra bajo un ataque real.
- Las debilidades en la configuración de dispositivos de red pueden ser problemas identificados sobre la base de los resultados de las pruebas realizadas.
- Se pueden hacer cambios para hacer los dispositivos más resistentes a los ataques.
- Estas pruebas pueden dañar la red y debe llevarse a cabo bajo condiciones muy controladas.

Deshabilite los puertos no utilizados

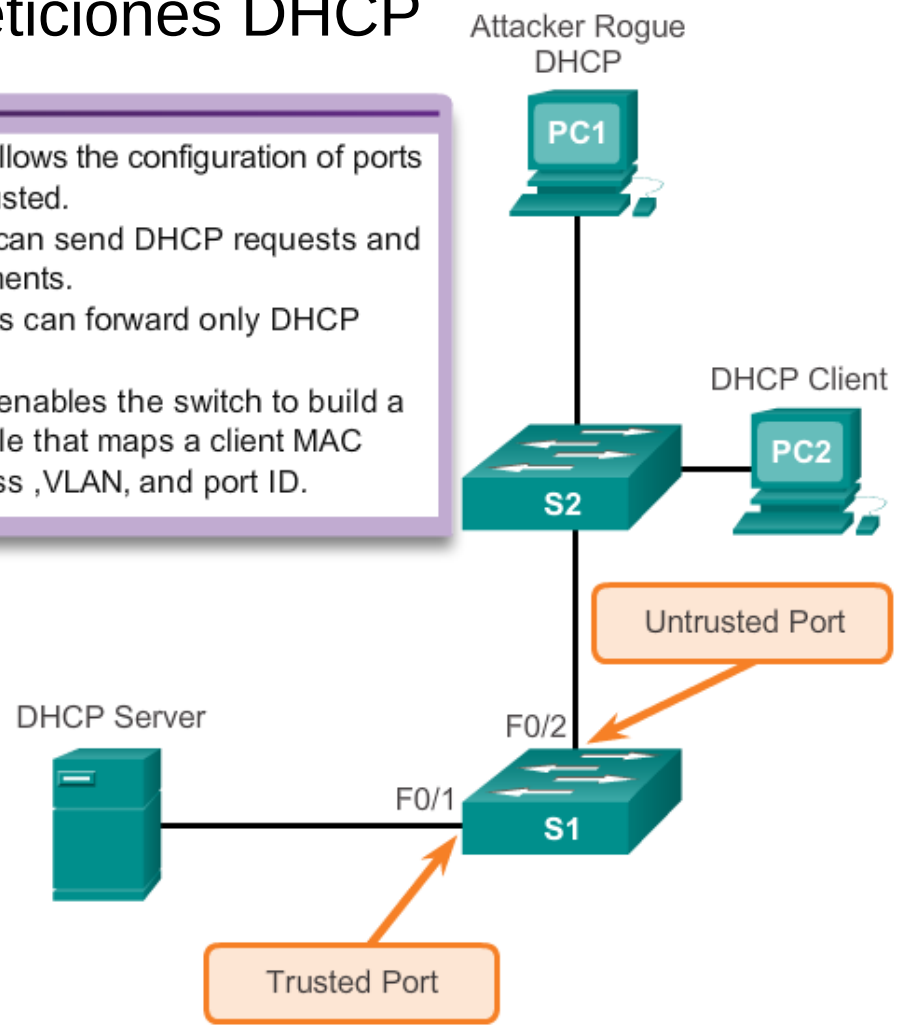
- Es un simple pero eficiente guía de seguridad



DHCP observando (fisgonear)

- DHCP Snooping especifica qué puertos del switch pueden responder a peticiones DHCP

- DHCP snooping allows the configuration of ports as trusted or untrusted.
  - Trusted ports can send DHCP requests and acknowledgements.
  - Untrusted ports can forward only DHCP requests.
- DHCP Snooping enables the switch to build a DHCP binding table that maps a client MAC address, IP address ,VLAN, and port ID.




```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20
S1(config)# interface fastethernet 0/1
S1(config-if)# ip dhcp snooping trust
S1(config)# interface fastethernet 0/2
S1(config-if)# ip dhcp limit rate 5
```

Seguridad de puertos: Operación

- Limita el número de direcciones MAC válidas permitidas en el puerto.
- Las MAC de los PC legítimos se permite el acceso, mientras que se les niega a otras direcciones MAC.
- Cualquier intento de MAC desconocidas generarán una Violación de la seguridad.
- Las MAC seguras se pueden configurar de varias maneras:

  - **Direcciones MAC seguras estáticas**
  - **Direcciones MAC seguras dinámicas**
  - **Direcciones MAC seguras adheridas (Sticky)**

Seguridad de puertos: Modos de Violación

- Cuando se dan cualquiera de estas situaciones:
- El número máximo de MAC seguras exceden las que la interfaz ha añadido a la CAM, y la estación cuya dirección MAC no está en la tabla de direcciones e intenta acceder a la interfaz.
- Una dirección conocida o configurado en una interfaz segura es visto en otra interfaz segura de la misma VLAN

- Hay tres posibles acciones cuando se detecta una Violación: **Proteger, Restringir, o cerrar**

Seguridad de puertos: Configuración

- Por defecto se hace de manera dinámica y esta deshabilitada.

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.

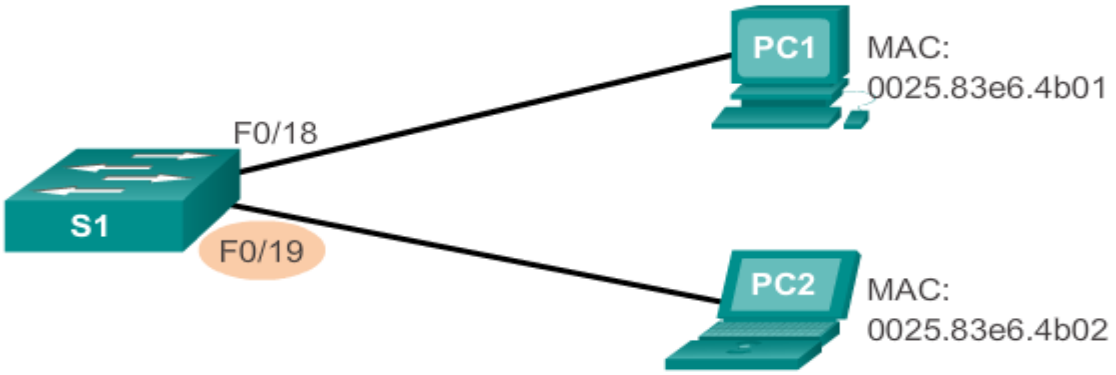
Seguridad de puertos: Configuración

- Configuración Dinámica de la Seguridad de puertos

Cisco IOS CLI Commands	
S1(config)#**interface fastethernet 0/18**	Specify the interface to be configured for port security.
S1(config-if)#**switchport mode access**	Set the interface mode to access.
S1(config-if)#**switchport port-security**	Enable port security on the interface.

Seguridad de puertos: Configuración

- Configuración de Seguridad de puertos adheridos o Sticky



Cisco IOS CLI Commands	
S1(config)#**interface fastethernet 0/18**	Specify the interface to be configured for port security.
S1(config-if)#**switchport mode access**	Set the interface mode to access.
S1(config-if)#**switchport port-security**	Enable port security on the interface.
S1(config-if)#**switchport port-security maximum 50**	Set the maximum number of secure addresses allowed on the port.
S1(config-if)#**switchport port-security mac-address sticky**	Enable sticky learning.

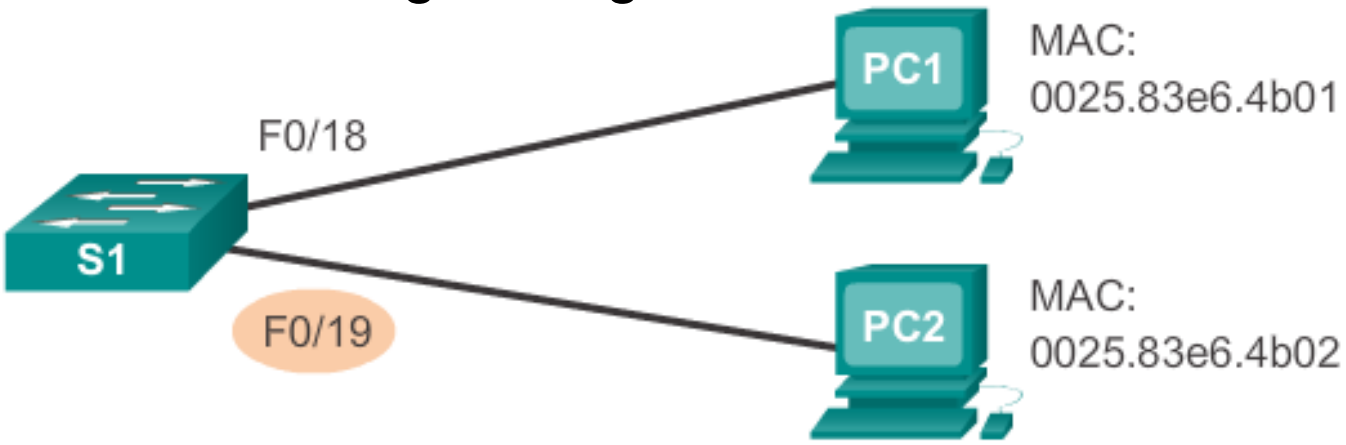
Seguridad de puertos: Verificación

- Verificando la Seguridad de puertos adheridos o Sticky


```
S1# show port-security interface fastethernet 0/19
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 50
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```

Seguridad de puertos: Verificación

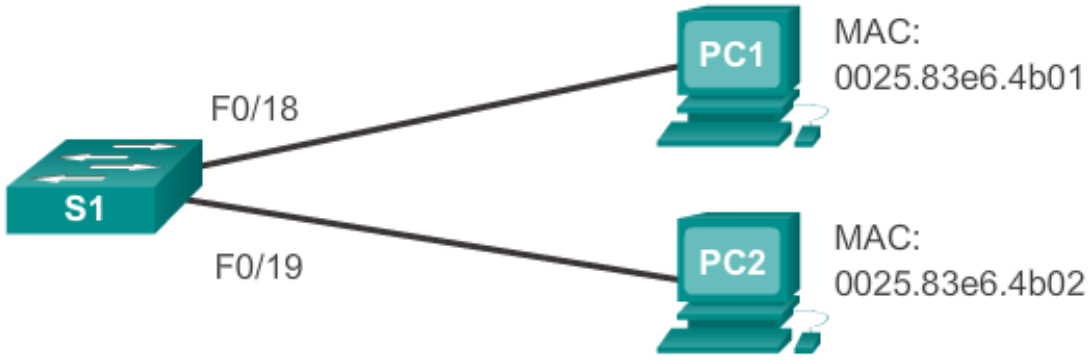
- Verificación de la Seguridad de puertos Sticky con el comando Running Config




```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Seguridad de puertos: Verificación

- Verificando la Seguridad de puertos Seguros con sus direcciones MAC




```
S1# show port-security address
Secure Mac Address Table
-----------------------------------------------------------
Vlan    Mac Address       Type              Ports   Remaining Age
                                                      (mins)
----    -----------       ----              -----   -------------
1       0025.83e6.4b01    SecureDynamic     Fa0/18      -
1       0025.83e6.4b02    SecureSticky      Fa0/19      -
-----------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port
```

Puertos de seguridad deshabilitados generan un mensaje de error.

- Puede generar un mensaje de error en el switch generando el estado deshabilitado del puerto.
- El puerto está desactivado y se cerró efectivamente.
- El switch genera eventos de comunicación a través de mensajes en la consola.

```
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
```

Puertos de seguridad deshabilitados generan un mensaje de error.

- Show interface revela que el puerto del switch en estado desactivado por error

```
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
```

Puertos de seguridad deshabilitados generan un mensaje de error.

- El comando shutdown y no shutdown deben ser emitidos para volver a habilitar el puerto

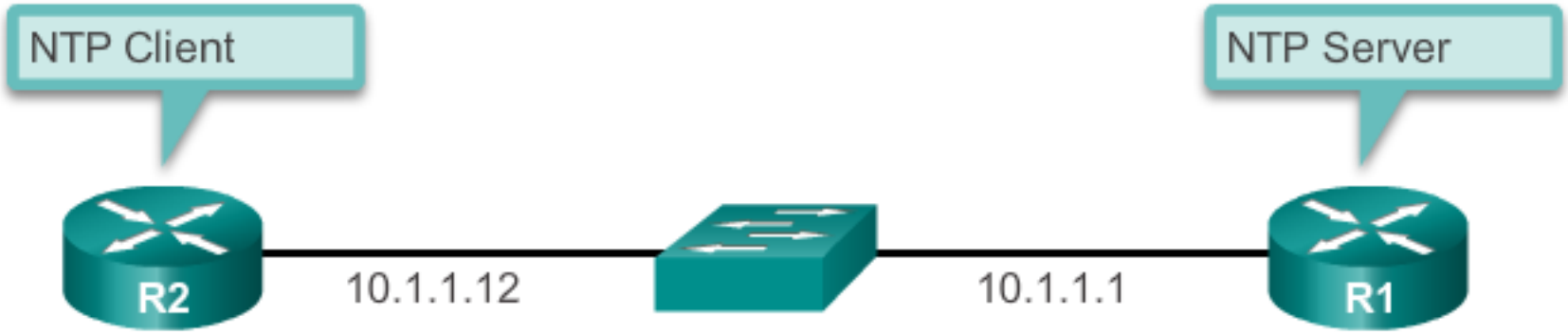
```
S1(config )#interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: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

Network Time Protocol (NTP)

- Es un protocolo utilizado para sincronizar los relojes de las redes de datos de los sistemas informáticos.
- Puede obtener el tiempo correcto desde un equipo de origen interno o externo.
- Las fuentes de tiempo pueden ser: **Reloj maestro local**
- **Reloj maestro en Internet**
- **GPS o reloj estándar**
- Un dispositivo de red puede ser configurado para ya sea un servidor NTP o un cliente NTP.

Network Time Protocol (NTP)

- Configurando NTP




```
R2(config)# ntp master 1
```

```
R2(config)# ntp server 10.1.1.1
```

Network Time Protocol (NTP)

- Verificando NTP

```
R2# show ntp associations
  address         ref clock       st   when   poll reach   delay   offs
*~10.1.1.1        .LOCL.           1     13     64   377    1.472   6.07
sys.peer,    # selected,    + candidate, - outlyer,   x falsetick
```

```
R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.1.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz,
precision is 2**17reference time is D40ADC27.E644C776
(13:18:31.899 UTC Mon Sep 24 2012)clock offset is 6.0716
msec,
root delay is 1.47 msecroot dispersion is 15.41 msec,
peer dispersion is 3.62 msecloopfilter state is 'CTRL'
(Normal Controlled Loop), drift is 0.000000091 s/ssystem poll
interval is 64, last update was 344 sec ago.
```

Resumen

- Secuencia de arranque o Boot de un switch LAN.
- Los diferentes modos LED del Switch.
- Cómo acceder y gestionar remotamente Switch LAN a través de una conexión segura.
- Modos de los puertos LAN de modos dúplex.
- Seguridad de puertos LAN switch, modos y acciones y Violación.
- Las mejores prácticas para redes conmutadas

Cisco | Networking Academy®

Mind Wide Open™

MUCHAS GRACIAS
CONSTRUIMOS FUTURO