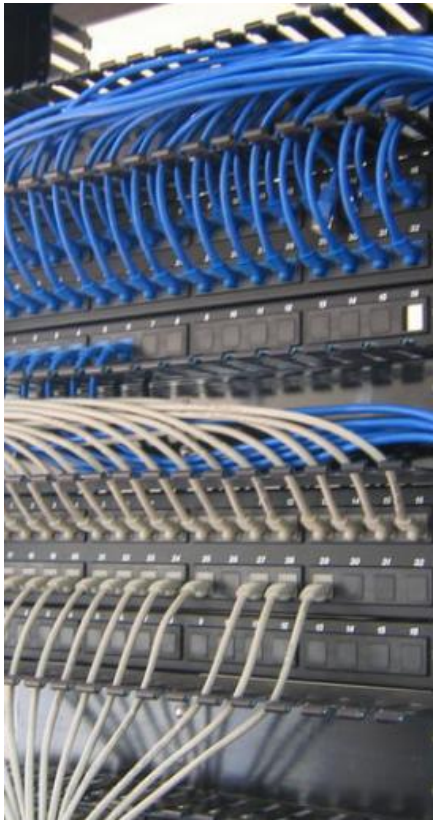
Redes de Información

Diseño LAN – Switch LAN



Temario

- Características deseables de una LAN
  - Escalabilidad
  - Disponibilidad
  - Seguridad
- Configuración básica de switch
  - Modos
  - Nombre del dispositivo
  - Contraseña modo privilegiado
  - Contraseña de acceso por consola
  - Contraseña de acceso remoto
  - Configuración interfaces
  - Configuración de la VLAN de administración
  - Verificación de configuración
  - Guardar la configuración
  - Eliminar la configuración
  - Seguridad de puerto
  - Configuración de seguridad de puerto
  - Verificación de la seguridad de puerto

Características deseables de una LAN

Escalabilidad

- La escalabilidad es una propiedad deseable de una red, que indica su habilidad para reaccionar y adaptarse sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida, o bien para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.
- En el momento del diseño, hay que tener en cuenta esta propiedad, para que la red se adapte a nuevos cambios, sin mayores modificaciones y costos en la infraestructura.

Disponibilidad

- La disponibilidad hace referencia a la probabilidad de que un sistema o red funcione adecuadamente en todo momento, las 24 horas del día y en las condiciones que el usuario necesite.
- Una red debe encontrarse siempre disponible, cuando un usuario la necesite utilizar. Por ello, en el momento del diseño, debe tenerse en cuenta los requerimientos del usuario y del sistema, del ancho de banda, etc.
- Este término se encuentra muy relacionado a otro, Redundancia, que veremos en el capítulo 6.

Seguridad

- Muchos de los ataques o vulnerabilidades de la redes LAN se deben a la errónea configuración o ubicación de los dispositivos de la misma.
- Algunas de las pautas referidas a la seguridad son:
  - Los dispositivos intermedios, como switches, deben encontrarse ubicados en racks o centros de cableado, bajo llave y solo accesibles al personal autorizado.
  - La configuración de los dispositivos intermedios, se debe implementar con las características de seguridad que ellos posean, como por ejemplo deshabilitar todos los puertos no utilizados.
  - Los dispositivos finales, entre otras implementaciones de seguridad, deberían contar con software antivirus actualizados que prevengan el ataque de virus, gusanos y troyanos.

Políticas de seguridad de una organización

- El objetivo de la Política de Seguridad de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.
- Se debe disponer de un documento formalmente elaborado sobre el tema y que debe ser divulgado entre todos los empleados.
- No es necesario un gran nivel de detalle, pero tampoco ha de quedar como una declaración de intenciones. Lo más importante para que estas surtan efecto es lograr la concientización, entendimiento y compromiso de todos los involucrados.
- Las políticas deben contener claramente las prácticas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.

Políticas de seguridad de una organización (cont.)

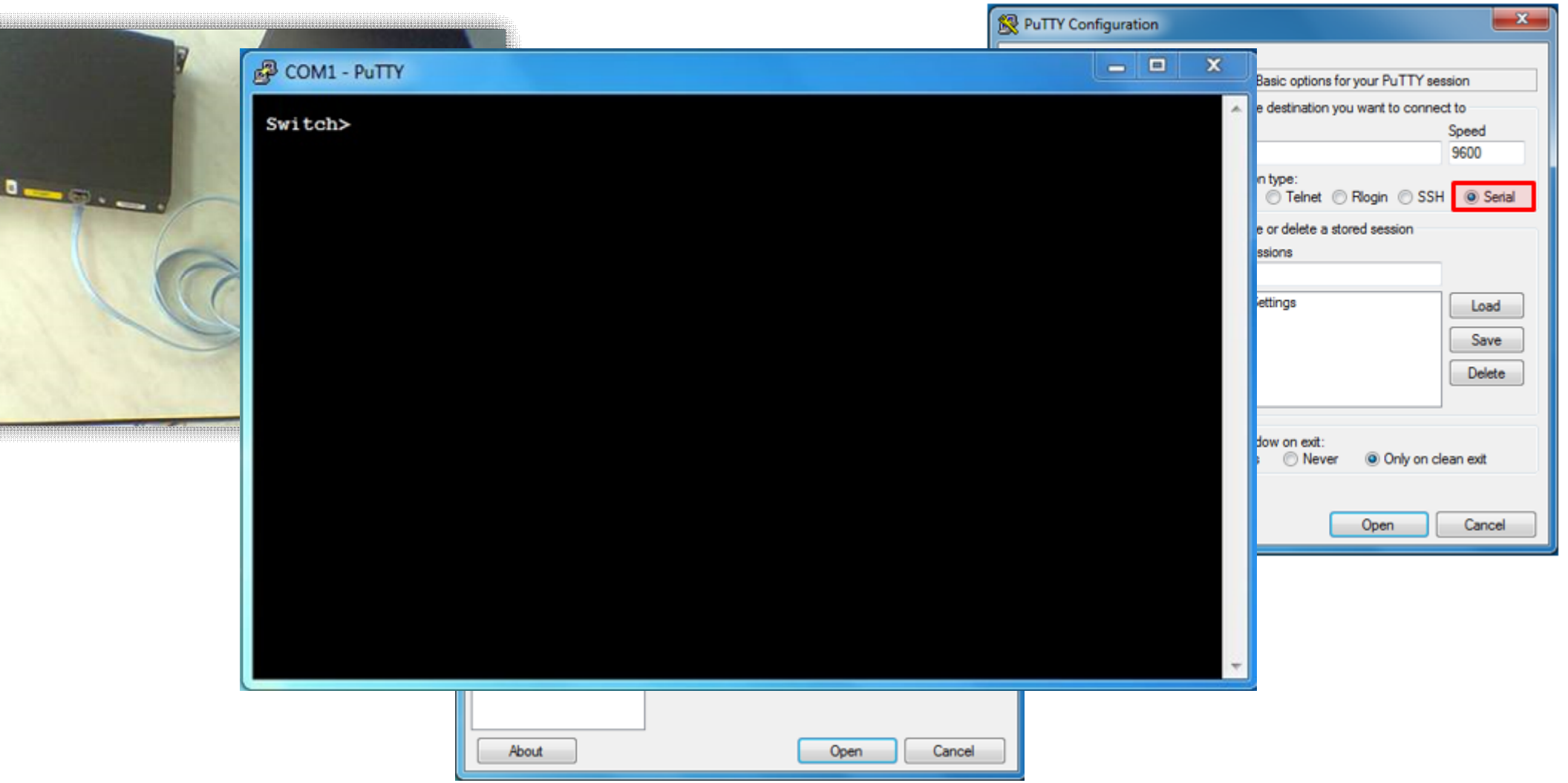
- Las políticas deben:
  - Definir qué es seguridad de la información, cuáles son sus objetivos principales y su importancia dentro de la organización
  - Mostrar el compromiso de sus altos cargos con la misma
  - Definir la filosofía respecto al acceso a los datos
  - Establecer responsabilidades inherentes al tema
  - Establecer la base para poder diseñar normas y procedimientos referidos a:
    - Organización de la seguridad
    - Clasificación y control de los datos
    - Seguridad de las personas
    - Seguridad física y ambiental
    - Plan de contingencia
    - Prevención y detección de virus
    - Administración de los computadores

Configuración básica de Switch

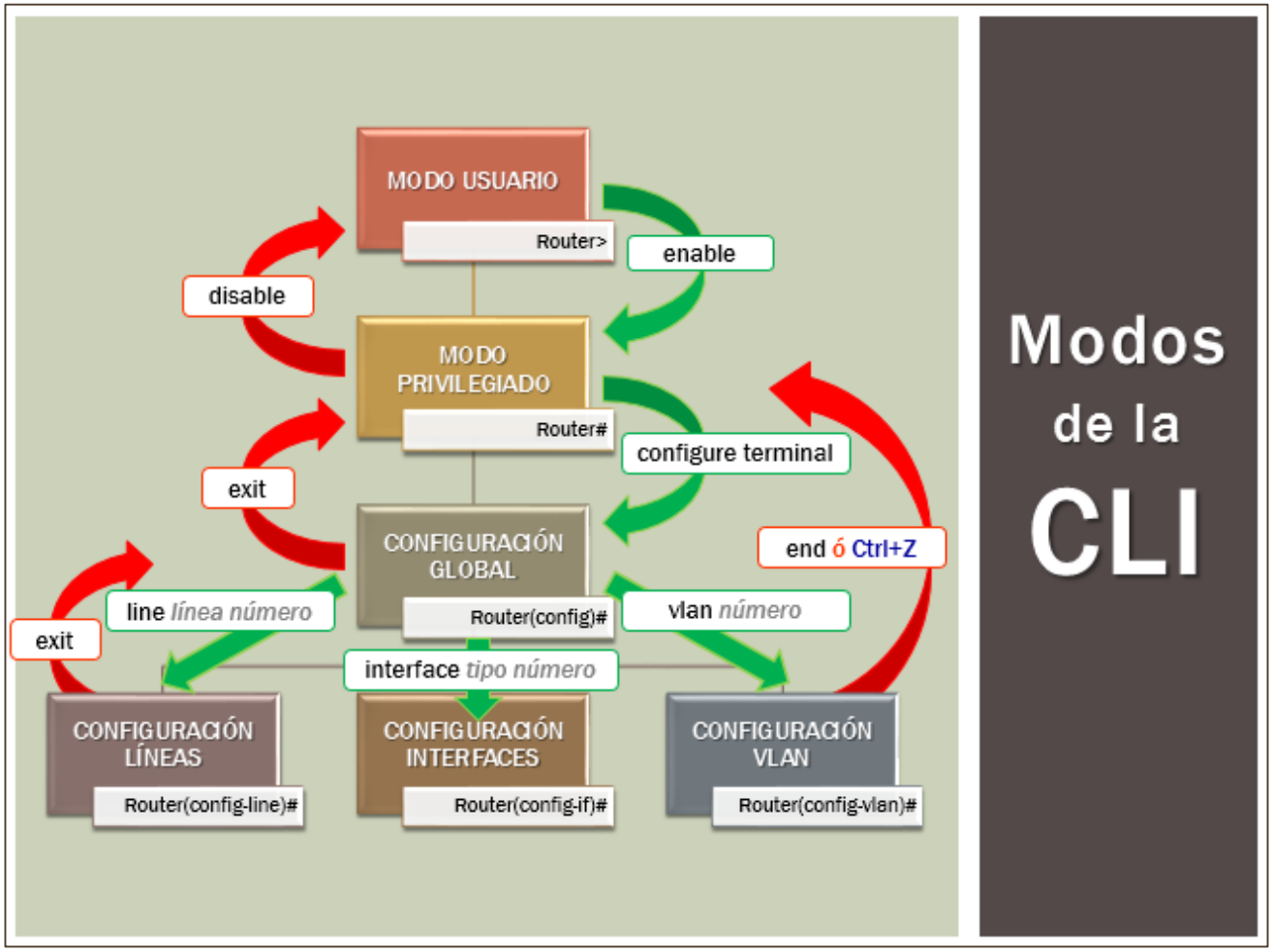
Conectándonos al Switch Administrable

- La administración de los switches, en la mayoría de los casos se puede llevar a cabo mediante una interfaz gráfica accesible a través de un navegador web. En otros, como los fabricados por la empresa Cisco Systems, vienen provisto de un sistema operativo propietario de línea de comandos (CLI), a través del cual también puede ser configurados y administrados.
- A la CLI se puede acceder de dos formas:
  - Remotamente a través de TELNET o SSH, con una aplicación como Putty.
  - Localmente por el puerto de consola. Para llevar a cabo esta conexión se necesita un cable de consola o rollover, un adaptador RJ45/DB9 y un puerto serial DB9 (computadora). La configuración inicial debe realizarse a través de este puerto, debido a que por configuración predeterminada, la administración remota se encuentra deshabilitada.

Conexión serial al puerto de consola



Modos


MODO USUARIO
Router>
enable
disable
MODO PRIVILEGIADO
Router#
configure terminal
exit
CONFIGURACIÓN GLOBAL
Router(config)#
end ó Ctrl+Z
line línea número
vlan número
exit
interface tipo número
CONFIGURACIÓN LÍNEAS
Router(config-line)#
CONFIGURACIÓN INTERFACES
Router(config-if)#
CONFIGURACIÓN VLAN
Router(config-vlan)#
Modos de la CLI

Particularidades de la CLI

- Permite la abreviatura de comandos y parámetros. Por el ejemplo el comando **enable** se puede abreviar a **ena**. La regla es que la abreviatura le permita al intérprete de comandos diferenciar un comando de otro similar. Caso contrario, informará con un error de comando ambiguo.
- Permite autocompletar comandos y parámetros usando la tecla de Tabulación (Tab).
- La CLI posee un sistema de ayuda de comandos y sintaxis, utilizando el caracter **?**
  - A continuación del prompt indica todos los comandos disponibles en ese modo.
  - Dejando un espacio después del comando o parámetro e introduciendo el **?** indica los parámetros adicionales que se deben o pueden ingresar.
- Las teclas de las flechas hacia arriba y hacia abajo permite navegar por el historial de los comandos ingresados previamente en ese modo, para facilitar entre otras cosas la corrección de comandos ingresados incorrectamente.
- La negación de un comando (anteponiendo el **no**), en algunos casos con la sintaxis completa y en otras parcial, elimina o desconfigura el comando o parámetro guardado o reconfigura los valores por defecto.

Nombre del dispositivo

Predeterminadamente el dispositivo tiene como nombre **Switch**.

Para cambiarlo debe ingresar al modo de Configuración global y con el comando **hostname** *nombre* indicar el nombre que desea. Este nombre le permite diferenciar los diferentes dispositivos. No admite espacios.

```
Switch> enable

Switch# config t

Switch(config)# hostname Switch_Piso_3

Switch_Piso_3(config)#
```

Los cambios que uno realice a la configuración, se implementan inmediatamente aunque no quedan guardados para el próximo reinicio del dispositivo. Más adelante veremos el comando para guardar permanentemente los cambios

Contraseña de modo Privilegiado

El acceso al modo Privilegiado debería estar protegido por una contraseña. Por defecto, no lo está.

Para configurar una contraseña utilice el comando **enable secret** *contraseña.* Este comando acepta espacios en la contraseña. En el momento de guardar la contraseña en el archivo de configuración, la misma queda encriptada para que no pueda ser visualizada por alguien indebido.

```
Switch(config)# enable secret admin12345
```

Contraseña de Acceso por Consola

Esta contraseña restringe el acceso a la CLI a través del puerto de consola. En forma predeterminada no posee. Se recomienda la configuración de ella. Para ello debe ingresar al submodo de configuración de la línea de consola y luego configurar la contraseña y habilitarla con los comandos mostrados a continuación.

```
Switch(config)# line console 0
Switch(config-line)# password Pass1234
Switch(config-line)# login
```

Contraseña de Acceso Remoto

Restringe el acceso a la CLI pero a través de las conexiones remotas, también llamadas VTY. El switch soporta hasta 16 conexiones remotas entrantes simultáneas, pero se recomienda configurar solo unas pocas.

Por defecto no tiene configurada una contraseña, aunque está habilitada la solicitud de la misma con el comando **login**, por lo cual inhabilita este tipo de conexión.

```
Switch(config)# line vty 0 4

Switch(config-line)# password Pass1234

Switch(config-line)# login
```

Configuración de interfaces

- Las interfaces o puertos de un switch, en forma predeterminada están habilitados. Y tanto el dúplex como la velocidad se encuentran en configurados para autonegociar contra el dispositivo al cual se lo conecte.
- Para ingresar a la configuración del puerto debe utilizar el comando **interface** *tipo número*. En *tipo* debe especificar si es **fastethernet**, **gigabitethernet**, etc. Los switches, más comunes generalmente tienen 24 o 48 puertos. Se numeran 0/1, 0/2, 0/3, etc.
- Para cambiar el dúplex, utilice el comando **duplex** {auto|half|full}
- Para modificar la velocidad, use el comando **speed** {auto|100|1000}
- Para deshabilitar el puerto, se usa el comando **shutdown**. Para activarlo, **no shutdown**

Configuración de interfaces (cont.)

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# duplex full
Switch(config-if)# speed auto
Switch(config-if)# no shutdown
```

Un parámetro del comando **interface** que se puede utilizar para configurar varios puertos en forma simultánea, es el parámetro **range**.

```
Switch(config)# interface range fastethernet 0/2 - 4
Switch(config-if-range)# shutdown
```

Configuración de la VLAN de administración

- Para que se pueda llevar a cabo una conexión remota, habrá que dotar al switch con una dirección IP a la que el administrador pueda conectarse. Para ello, hay que configurar la vlan de administración.
- Primero deberemos ingresar al modo de configuración de la vlan administrativa con el comando **interface vlan** *número*. Por defecto todos los puertos de un switch se encuentran asociados a la vlan 1. Por cuestiones de seguridad y rendimiento, se recomienda no utilizar la vlan 1, como vlan de administración.
- En el modo de configuración de la vlan de administración, debemos configurarle una dirección IP y su respectiva máscara de subred, con el comando **ip address** *dirección_ip máscara_subred* y habilitarla con el comando **no shutdown**.
- En el caso de que quiera administrar remotamente el switch desde una conexión fuera de su red IP, deberá configurar desde el modo de configuración global, el Gateway (Router) que va enrutar los datos salientes de la red en la que se encuentra el switch. Para ello utilice el comando **ip default-gateway** *dirección_ip*

Configuración de la VLAN de administración (cont.)

```
Switch(config)# interface vlan 50
Switch(config-if)# ip address 192.168.10.5 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway 192.168.10.1
```

Verificación de configuración (show running-config)

```
Switch_Piso_3#show running-config
Building configuration...

Current configuration : 1269 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch_Piso_3
!
enable secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 duplex full
!
interface FastEthernet0/2
 shutdown
!
 --More--
```

Verificación de configuración (show interface)

```
Switch_Piso_3# show interfaces fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0001.c9dc.da01 (bia 0001.c9dc.da01)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, 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
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Verificación de configuración (show interface vlan)

```
Switch_Piso_3#show interface vlan 50
Vlan50 is down, line protocol is down
  Hardware is CPU Interface, address is 0002.163c.7e0d (bia 0002.163c.7e0d)
  Internet address is 192.168.10.5/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, 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
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Guardar la configuración

Los cambios que se van ingresando en la configuración del Switch se aplican a la configuración en ejecución (running-config). Para que los mismos sean guardados definitivamente para futuros reinicios del dispositivo, debe ingresar el comando de modo Privilegiado **copy running-config startup-config**

Una vez ingresado este comando solicitará la confirmación del nombre del archivo a guardar. Entre **[]** aparece el nombre que le dará si presiona Enter directamente (en este caso **startup-config**). Presione Enter para proceder.

```
Switch_Piso_3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Guardar la configuración (cont.)

- El comando **show startup-config** mostrará el archivo de configuración de inicio o respaldo, guardado en la memoria NVRAM. Con él puede confirmar que se hayan guardado los cambios o verificar la configuración de inicio.
- De no haber ninguna configuración de inicio guardada, mostrará el siguiente resultado:

```
Switch_Piso_3#show startup-config
startup-config is not present
```

Eliminar la configuración

Si desea eliminar la configuración de inicio guardada, ingrese el siguiente comando:

```
Switch_Piso_3#erase startup-config
Erasing the nvram filesystem will remove all configuration
files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

Para eliminar la configuración activa o ejecución, una vez borrada la configuración de inicio, deberá reiniciar el dispositivo. Puede hacerlo, quitándole la energía al dispositivo y reconectándola o bien ejecutando el comando **reload** desde el modo privilegiado.

Seguridad de puerto

Con el objetivo de incrementar la seguridad en una red LAN es posible implementar seguridad de puertos en los switches de capa de acceso, la que permite:

- Restringir la o las direcciones MAC que se pueden conectar a través de un puerto del Switch.
- Restringir el número de direcciones MAC que se pueden conectar (simultáneamente) a un puerto del Switch. (Por defecto: 1 - Máximo: 132).
- Configurar el tiempo en que determinada MAC permanece registrada (en minutos).
- Definir la acción a tomar cuando una violación es detectada.

Configuración de seguridad de puerto

1. Para definir manualmente (estática) la dirección MAC segura que tendrá permitido conectarse utilice el comando:

```
Switch(config-if)# switchport port-security mac-address DirecciónMAC
```

2. Para que el dispositivo aprenda dinámicamente las direcciones MAC seguras, utilice el siguiente comando:

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

3. Para permitir que el Switch aprenda dinámicamente la o las direcciones MAC del o los equipos que se conecten al puerto y aplique esas direcciones MAC a la configuración en ejecución (running-config), utilice el siguiente comando:

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

4. Si hay un switch o un hub, conectado a un puerto del switch que quiere asegurar, puede configurar un máximo de direcciones MAC asociadas a ese puerto, por ejemplo si quiere configurar un máximo de 3 direcciones MAC, use el siguiente comando:

```
Switch(config-if)# switchport port-security maximum 3
```

Configuración de seguridad de puerto (cont.)

5. En el caso de que la seguridad de puerto sea violada, puede configurar las siguientes acciones:

- **Protección**: una vez que se alcanzó el máximo de direcciones MAC en un puerto, todo el tráfico de orígenes desconocidos (es decir, de direcciones MAC que no sean válidas para ese puerto) es descartado. No obstante, se continúa enviando el tráfico legal normalmente. No se notifica al administrador de esta situación.

```
Switch(config-if)# switchport port-security violation protect
```

- **Restricción**: el mismo comportamiento que el caso anterior pero con la diferencia que se envía un aviso al administrador mediante SNMP, se registra el evento en el syslog y se incrementa el contador de violaciones.

```
Switch(config-if)# switchport port-security violation restrict
```

- **Desactivación** (default): en este caso el puerto se da de baja dejándolo en estado *err-disabled* (deshabilitado por error). Además se envía un aviso al administrador mediante SNMP, se registra el evento en el syslog y se incrementa el contador de violaciones. Para reactivar el puerto una vez identificada la causa de la violación, el administrador debe desactivarlo (shutdown) y volver a reactivarlo (no shutdown)

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

Configuración de seguridad de puerto (cont.)

```
Switch# configure terminal
Switch(config-if)# interface FastEthernet 0/20
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security violation shutdown
```

Verificación de la seguridad de puerto

Switch# show port-security interface *Tipo Número*

```
Switch#show port-security interface fastEthernet  0/20
Port Security               : Disabled
Port Status                 : Secure-down
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    : 0000.0000.0000:0
Security Violation Count    : 0
```

Verificación de la seguridad de puerto (cont.)

Switch# show running-config

```
Switch#show running-config
Building configuration...
!

[--Salida omitida---]

interface FastEthernet0/19
!
interface FastEthernet0/20
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.5C34.E888
!
```

Preguntas