

La importancia de la seguridad en las capas 2 y 3 de la red. Aplicación en granjas web.

Juan Carlos Gámez Granados



Who am I?

Juan Carlos Gámez Granados

Doctor en Informática

Máster en Tecnologías Multimedia

Ingeniero en Informática



Instructor CISCO

Responsable Academia CISCO de la Universidad de Córdoba

Coordinador del Aula de Ciberseguridad y Redes de la Universidad de Córdoba

Director Centro Universitario de Desarrollo Tecnológico de Puente Genil (Universidad de Córdoba)



Tabla de contenidos

- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - Configuración de switchs:
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - Práctica 1
- Seguridad en capa 2: Segmentación de redes (VLAN)
 - Práctica 2
- Enrutamiento inter-VLAN:
 - Práctica 3
- Seguridad en capa 3: ACL
 - Práctica 4



Elección de Switch (I)

- Plataforma de Switch
 - Seleccionar el hardware adecuado para cumplir con los requisitos de la red actual es fundamental durante el diseño de una red.
 - Existen cinco categorías de switches para las redes empresariales:
 - Switches LAN en campus
 - Switches administrados en la nube
 - Switches para centros de datos
 - Switches del proveedor de servicios
 - Redes virtuales
 - Varios factores para tener en cuenta al seleccionar los switches incluyen:
 - Configuración fija frente a modular
 - Apilable frente a no apilable
 - Grosor del switch (unidades de rack)
 - Costo, densidad de puertos, potencia, confiabilidad

Switches de configuración modular



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados

Elección de Switch (II)

- **Densidad de puertos del Switch**
 - La densidad de puertos de un switch hace referencia al número de puertos en un único switch.
 - Los switches de configuración fija admiten una variedad de configuraciones de densidad de puertos:
 - Switches de 24 y 48 puertos.
 - Switches con opción de puertos adicionales SFP.
 - Más de 1000 puertos.
 - Los switches modulares generalmente son más apropiados en las redes grandes, dado que reducen los problemas de energía y espacio.

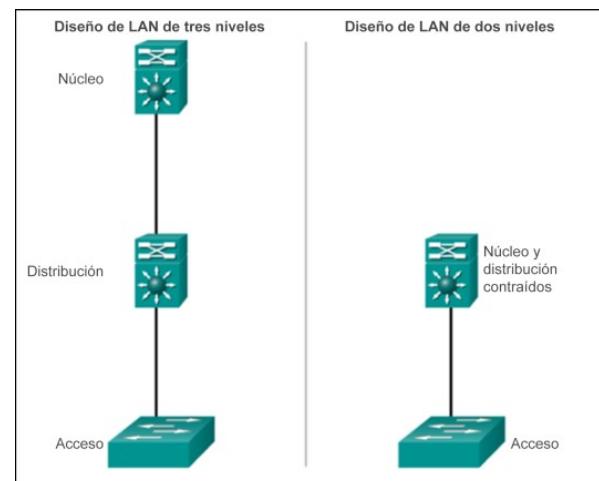


La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Elección de Switch (III)

- **Velocidad de reenvío del Switch**
 - Las líneas de productos de switching se clasifican según las velocidades de reenvío.
 - Las velocidades de reenvío definen las capacidades de procesamiento de un switch mediante la estimación de la cantidad de datos que puede procesar por segundo el switch.
 - Los switches básicos presentan velocidades de reenvío inferiores que los switches de nivel empresarial.
 - Las velocidades de reenvío son un factor importante al seleccionar un switch porque, si la velocidad es demasiado baja, no será capaz de admitir la comunicación a la máxima velocidad del cable en todos sus puertos de switch.
 - Los switches de capa de acceso por lo general no necesitan funcionar a la máxima velocidad del cable, debido a que están limitados físicamente por uplinks en la capa de distribución.
 - Se necesitan switches de mayor rendimiento en las capas principales y de distribución.

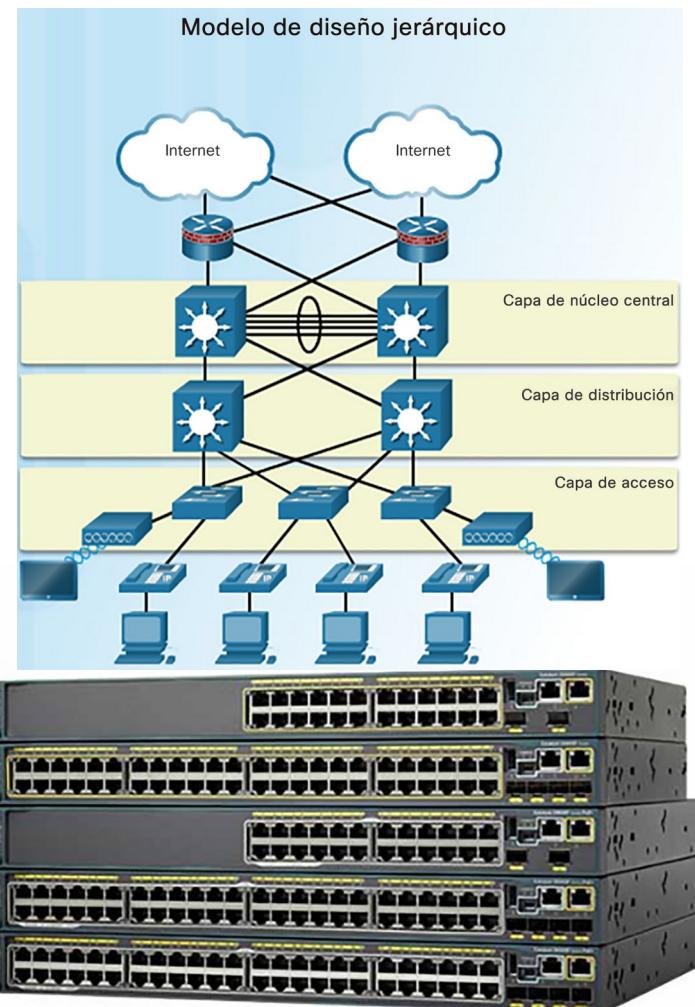


La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Elección de Switch (IV)

- **Switching multicapa:**
 - Por lo general, los switches multicapa se implementan en la capa principal y de distribución.
 - Los switches multicapa pueden hacer lo siguiente:
 - Armar una tabla de routing y admitir protocolos de routing.
 - Reenviar los paquetes IP a una velocidad cercana a la velocidad de reenvío de capa 2.
 - Los switches multicapa suelen admitir hardware especializado, llamado circuitos integrados de aplicación específica (ASIC).
 - Los ASIC, junto con el software dedicado, pueden simplificar el reenvío de los paquetes IP de forma independiente de la CPU.



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Tabla de contenidos

- **Switch**
 - Elección de switchs
 - **Funcionamiento de switchs**
 - Configuración de switchs:
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - Práctica 1
- Seguridad en capa 2: Segmentación de redes (VLAN)
 - Práctica 2
- Enrutamiento inter-VLAN:
 - Práctica 3
- Seguridad en capa 3: ACL
 - Práctica 4



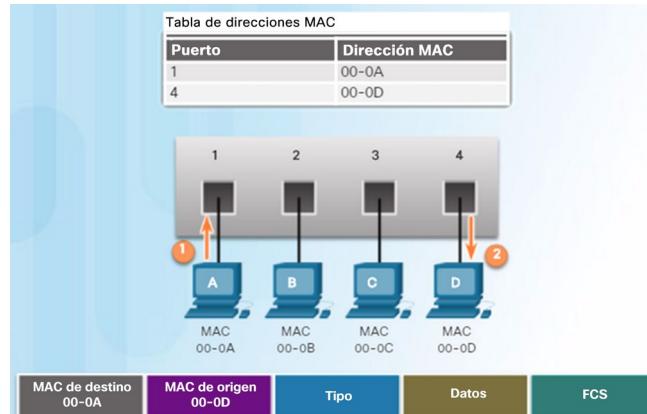
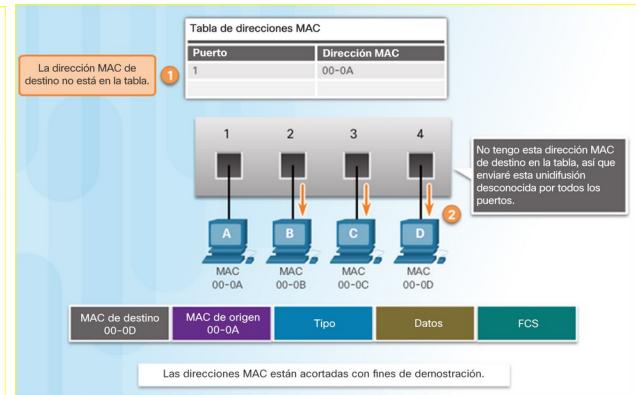
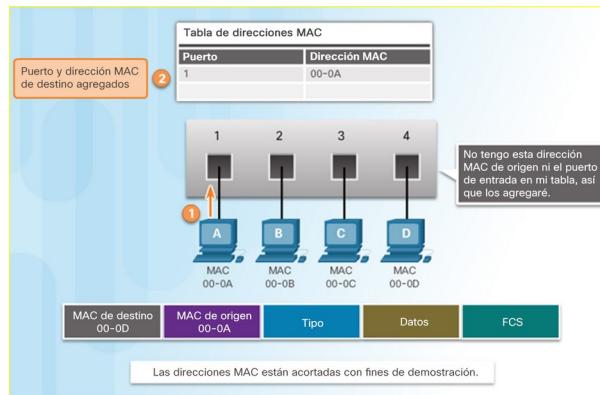
Funcionamiento del switch (I)

- Reenvío de tramas (Switching)
 - Un switch toma una decisión sobre la base del puerto de entrada y de destino.
 - Los switches LAN mantienen una tabla que usan para determinar cómo reenviar el tráfico a través del switch.
 - Los switches LAN reenvían tramas de Ethernet según la dirección MAC de destino de las tramas.
 - Para transmitir una trama, el switch primero debe averiguar qué dispositivos hay en cada puerto.
 - A medida que el switch detecta la relación entre puertos y dispositivos, crea una tabla denominada "tabla de direcciones MAC" o "tabla de memoria de contenido direccionable" (CAM).
 - CAM es un tipo de memoria especial que se usa en las aplicaciones de búsqueda de alta velocidad.
 - La información en la tabla de direcciones MAC se utiliza para enviar tramas.
 - Cuando un switch recibe una trama entrante con una dirección MAC que no figura en la tabla CAM, satura todos los puertos con la trama, excepto el puerto que la recibió.



Funcionamiento del switch (II)

- ARP (Protocolo de resolución de direcciones):



- Ejercicio: Obtener la MAC y ARP de vuestro equipo

La importancia de la seguridad en las capas 2 y 3 de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados

Funcionamiento del switch (III)

- **Métodos de Reenvío de tramas (Switching)**

Almacenamiento y reenvío



Un switch de almacenamiento y envío recibe la trama completa y calcula la CRC. Si la CRC es válida, el switch busca la dirección de destino, que determina la interfaz de salida. A continuación, se envía la trama por el puerto correcto.

Método de corte

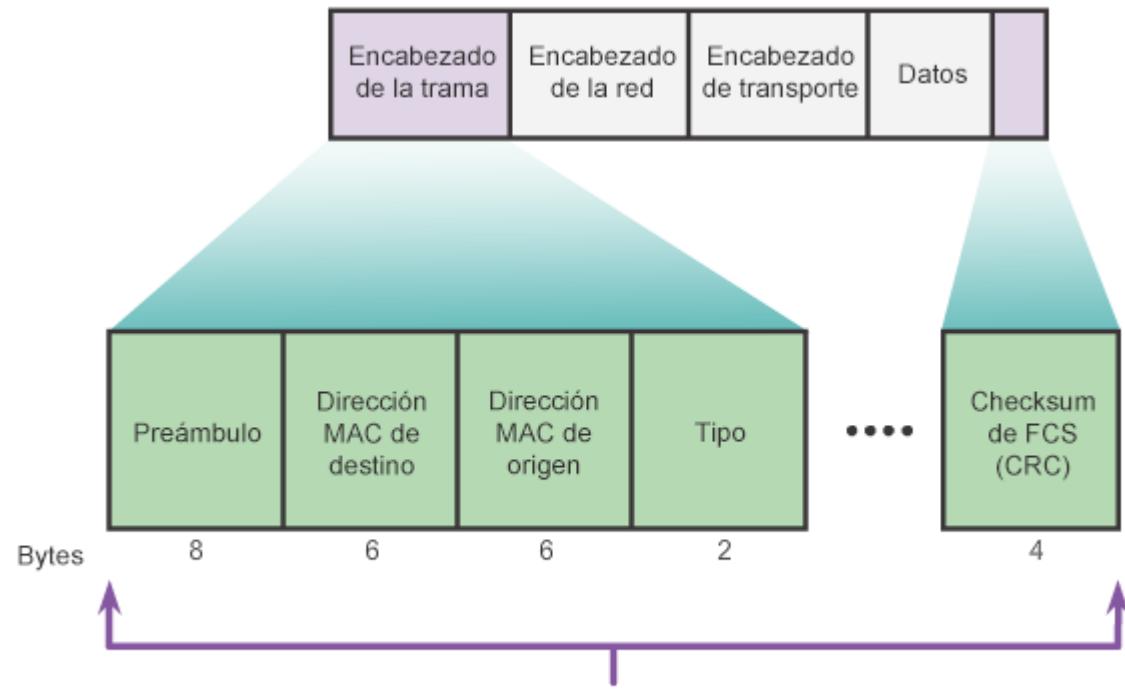


El switch que utiliza el método de corte envía la trama antes de recibirla en su totalidad. Como mínimo, se debe leer la dirección de destino para que la trama se pueda enviar.



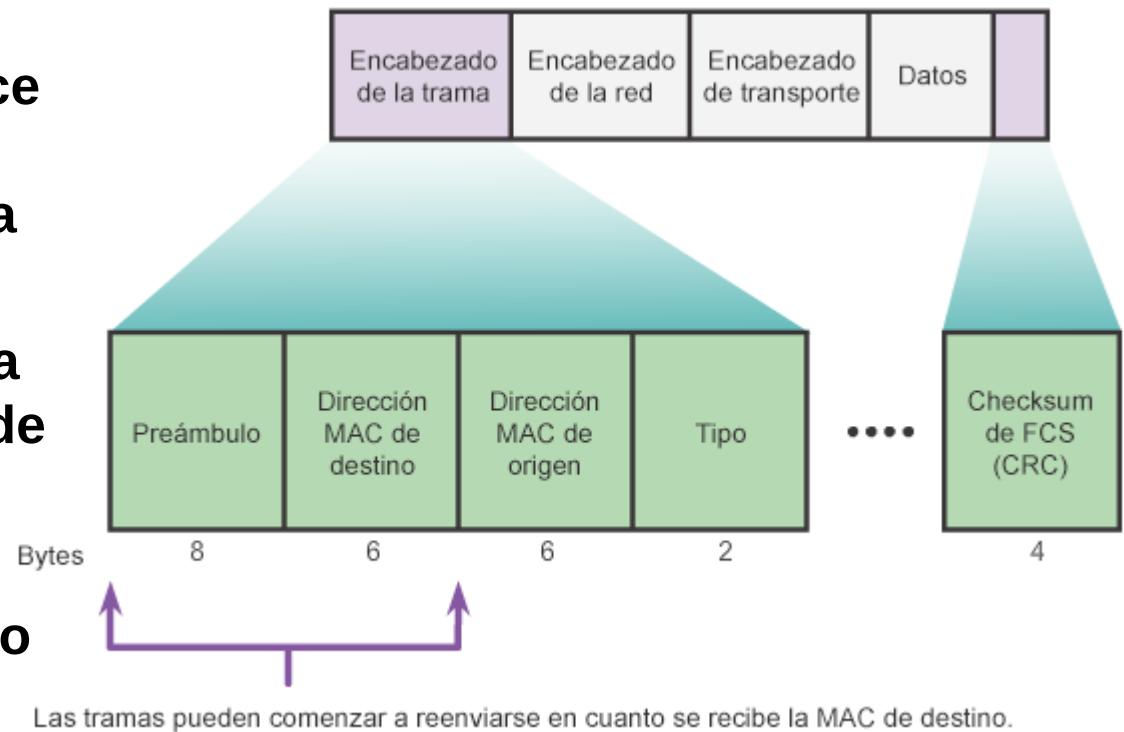
Funcionamiento del switch (IV)

- **Método de almacenamiento y reenvío:**
 - Permite que el switch haga lo siguiente:
 - Verificar si hay errores (mediante la verificación de FCS)
 - Realizar el almacenamiento en búfer automático
 - Proceso de reenvío más lento



Funcionamiento del switch (V)

- **Método de corte:**
 - Permite que el switch comience a reenviar en cuanto conozca el destino.
 - No es necesaria la verificación de FCS.
 - No hay almacenamiento en búfer automático.



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Tabla de contenidos

- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - **Configuración de switchs:**
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - Práctica 1
- Seguridad en capa 2: Segmentación de redes (VLAN)
 - Práctica 2
- Enrutamiento inter-VLAN:
 - Práctica 3
- Seguridad en capa 3: ACL
 - Práctica 4



Acceso al dispositivo (I)

- Métodos de acceso:
 - Las tres formas más comunes de acceder al IOS son las siguientes:
 - Puerto de consola: puerto serial fuera de banda que se utiliza principalmente para propósitos de gestión como la configuración inicial del router.
 - Shell seguro (SSH): método en banda para establecer en forma remota y segura una sesión de CLI en una red. Se cifran la autenticación de usuario, las contraseñas y los comandos que se envían por la red. Se recomienda utilizar el protocolo SSH en lugar de Telnet, siempre que sea posible.
 - Telnet: interfaces en banda para establecer una sesión CLI de manera remota a través de una interfaz virtual por medio de una red. La autenticación de usuario, las contraseñas y los comandos se envían por la red en texto no cifrado.
 - Nota: El puerto AUX es un método más antiguo de establecer una sesión CLI en forma remota a través de una conexión por acceso telefónico a través de un módem.
 - Independientemente del método de acceso, se requerirá un programa de emulación de terminal. Entre los programas de emulación de terminal populares, se incluyen PuTTY, Tera Term, SecureCRT y OS X Terminal.

La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados

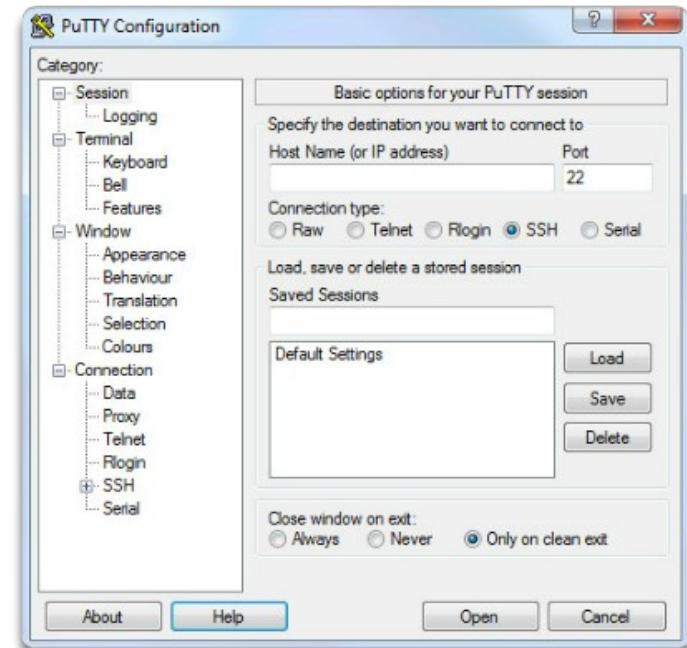


Acceso al dispositivo (II)

Puerto de consola



PuTTY



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Tabla de contenidos

- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - **Configuración de switchs:**
 - Acceso al dispositivo
 - **Modos de funcionamiento**
 - Comandos de configuración
 - Práctica 1
- Seguridad en capa 2: Segmentación de redes (VLAN)
 - Práctica 2
- Enrutamiento inter-VLAN:
 - Práctica 3
- Seguridad en capa 3: ACL
 - Práctica 4



Modos de funcionamiento (I)

- Los modos Cisco IOS utilizan una estructura de mando jerárquica.
- Cada modo tiene una petición de entrada distinta y se utiliza para realizar tareas determinadas con un conjunto específico de comandos que están disponibles solo para el modo en cuestión.
- El ‘modo EXEC de usuario’ permite solo una cantidad limitada de comandos de monitoreo básicos.
 - A menudo, se lo describe como un modo de “visualización solamente”.
 - En forma predeterminada, no se requiere autenticación para acceder al modo EXEC de usuario, pero debería obtenerse.
- El ‘modo EXEC con privilegios’ permite la ejecución de comandos de administración y configuración.
 - A menudo, se lo describe como "modo enable" porque requiere el comando EXEC de usuario enable.
 - En forma predeterminada, no se requiere autenticación para acceder al modo EXEC con privilegios, pero debería obtenerse.

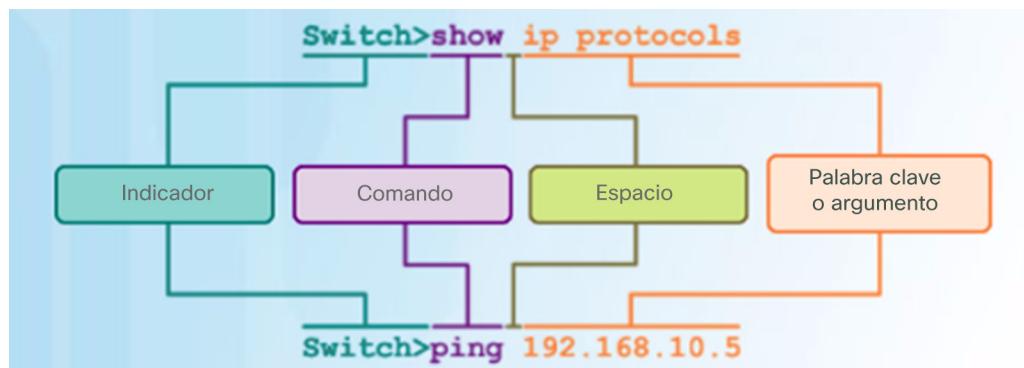
Modo de comando	Descripción	Indicador de dispositivo predeterminado
Modo EXEC de usuario	<ul style="list-style-type: none">Permite el acceso solamente a una cantidad limitada de comandos básicos de monitoreo.A menudo se le describe como un modo de “visualización solamente”.	Switch> Router>
Modo EXEC con privilegios	<ul style="list-style-type: none">Permite el acceso a todos los comandos y funciones.El usuario puede utilizar cualquier comando de monitoreo y ejecutar comandos de configuración y de administración.	Switch# Router#

La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Modos de funcionamiento (II)

- Los dispositivos Cisco IOS admiten muchos comandos.
- Cada comando de IOS tiene una sintaxis o formato específico y puede ejecutarse solamente en el modo adecuado.
- La sintaxis para un comando es el comando seguido de las palabras clave y los argumentos correspondientes:
 - Palabra clave: un parámetro específico que se define en el sistema operativo (en la figura ip protocols)
 - Argumento: no está predefinido; es un valor o variable definido por el usuario, (en la figura, 192.168.10.5)
- Después de ingresar cada comando completo, incluso cualquier palabra clave y argumento, presione la tecla Enter para enviar el comando al intérprete de comandos.
- Ayuda contextual de IOS:
 - La ayuda contextual proporciona una lista de comandos y los argumentos asociados con esos comandos en el contexto del modo actual.
 - Para acceder a la ayuda contextual, introduzca un signo de interrogación, ?, en cualquier petición de entrada.



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Tabla de contenidos

- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - **Configuración de switchs:**
 - Acceso al dispositivo
 - Modos de funcionamiento
 - **Comandos de configuración**
 - Práctica 1
- Seguridad en capa 2: Segmentación de redes (VLAN)
 - Práctica 2
- Enrutamiento inter-VLAN:
 - Práctica 3
- Seguridad en capa 3: ACL
 - Práctica 4



Comandos de configuración (I)

Sintaxis de comando de la CLI del IOS de Cisco	
Cambia de modo EXEC usuario a modo EXEC privilegiado.	switch> enable
Si una contraseña ha sido configurada para modo EXEC privilegiado, se le solicitará que la ingrese ahora.	password: Contraseña
La petición de entrada # significa modo EXEC privilegiado.	switch#
Cambia de modo EXEC privilegiado a modo EXEC usuario.	switch# disable
La petición de entrada > significa modo EXEC usuario.	switch>

Sintaxis de comando de la CLI del IOS de Cisco	
Habilite el historial del terminal. Este comando se puede ejecutar desde el modo EXEC privilegiado o usuario.	switch# terminal history
Configura el tamaño del historial del terminal. El historial del terminal puede mantener de 0 a 256 líneas de comando.	switch# terminal history size 50
Restablece el tamaño del historial del terminal al valor predeterminado de 10 líneas de comando.	switch# terminal no history size
Inhabilita el historial del terminal.	switch# terminal no history



Comandos de configuración (II)

Sintaxis de comando de la CLI del IOS de Cisco	
Cambia de modo EXEC privilegiado a modo de configuración global.	<code>switch#configure terminal</code>
La petición de entrada (config)# significa que el switch está en modo de configuración global.	<code>switch(config) #</code>
Cambia de modo de configuración global a modo de configuración de interfaz para la interfaz 0/1 fast ethernet.	<code>switch(config)#interface fastethernet 0/1</code>
La petición de entrada (config-if)# significa que el switch está en modo de configuración de interfaz.	<code>switch(config-if) #</code>
Cambia de modo de configuración de interfaz a modo de configuración global.	<code>switch(config-if)#exit</code>
La petición de entrada (config)# significa que el switch está en modo de configuración global.	<code>switch(config) #</code>
Cambia de modo de configuración global a modo EXEC privilegiado.	<code>switch(config)#exit</code>
La petición de entrada # significa que el switch está en modo EXEC privilegiado.	<code>switch#</code>

La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Comandos de configuración (III)

- Específico para el Switch

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	S1# configure terminal
Ingrese al modo de configuración de interfaz para la interfaz de VLAN 99.	S1(config)# interface vlan 99
Configurar la dirección IP de la interfaz.	S1(config-if)# dirección IP 172.17.99.11 255.255.255.0
Habilitar la interfaz.	S1(config-if)# no shutdown
Regrese al modo EXEC privilegiado.	S1(config-if)# end
Ingrese al modo de configuración global.	S1# configure terminal
Ingrese la interfaz para asignar la VLAN.	S1(config)# interface fastethernet 0/18
Defina el modo de membresía de la VLAN para el puerto.	S1(config-if)# switchport mode access
Asigne el puerto a una VLAN.	S1(config-if)# switchport acces vlan 99
Regrese al modo EXEC privilegiado.	S1(config-if)# end
Guardar la configuración en ejecución en la configuración de inicio del switch.	S1# copy running-config startup-config



Comandos de configuración (IV)

Uso de los comandos Show

Sintaxis del comando de CLI IOS de Cisco	
Muestra el estado de la interfaz y la configuración para una o todas las interfaces disponibles del switch.	<code>show interfaces [id de la interfaz]</code>
Muestra el contenido de la configuración de inicio.	<code>show startup-config</code>
Muestra la configuración de funcionamiento actual.	<code>show running-config</code>
Muestra información acerca de flash: sistema de archivos.	<code>show flash:</code>
Muestra el estado del hardware y el software del sistema.	<code>show version</code>
Muestra el historial de comandos de sesión.	<code>show history</code>
Muestra información de IP. La opción interface muestra el estado de la interfaz de IP y la configuración. La opción http muestra información de HTTP acerca del administrador de dispositivos que se ejecuta en el switch. La opción arp muestra la tabla ARP de IP.	<code>show ip {interface http arp}</code>
Muestra la tabla MAC de envío.	<code>show mac-address-table</code>

La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.

Juan Carlos Gámez Granados



Comandos de configuración (V)

Configuraciones de respaldo y restauración del switch

Sintaxis del comando de CLI IOS de Cisco	
Versión formal del comando copy de IOS de Cisco. Confirmar el nombre de archivo de destino. Presione la tecla Enter para aceptar y utilice la combinación de teclas Ctrl+C para cancelar.	S1#copy system:running-config flash:startup-config Destination filename [startup-config] ?
Versión informal del comando copy. Se supone que running-config se está ejecutando en el sistema y que el archivo startup-config se almacenará en NVRAM flash. Presione la tecla Enter para aceptar y utilice la combinación de teclas Ctrl+C para cancelar.	S1#copy running-config startup-config Destination filename [startup-config] ?
Hace una copia de respaldo de startup-config en un archivo almacenado en NVRAM flash. Confirmar el nombre de archivo de destino. Presione la tecla Enter para aceptar y utilice la combinación de teclas Ctrl+C para cancelar.	S1#copy startup-config flash:config.bak1 Destination filename [config.bak1] ?



Comandos de configuración (V)

Configuraciones de respaldo y restauración del switch

Sintaxis del comando de CLI IOS de Cisco	
Copia el archivo config.bak1 almacenado en flash a la configuración de inicio supuestamente almacenada en flash. Presione la tecla Enter para aceptar y utilice la combinación de teclas Ctrl+C para cancelar.	<pre>S1#copy flash:config.bak1 startup-config Destination filename [startup-config] ?</pre>
Permite que IOS de Cisco ejecute el reinicio del switch. Si se ha modificado el archivo de configuración en ejecución se le solicitará que lo guarde. Confirme con 'y' o con 'n'. Para confirmar la recarga presione la tecla Enter para aceptar y utilice la combinación de teclas Ctrl+C para cancelar.	<pre>S1#reload System configuration has been modified. Save? [yes/no] : n Proceed with reload? [confirm] ?</pre>



Comandos de configuración (VI)

- **Respaldo en un servidor TFTP**

```
S1#copy system:running-config tftp://172.16.2.155/tokyo-config  
Write file tokyo-config on host 172.16.2.155? [confirm] y  
Writing tokyo-config!!! [OK]
```

- **Borrado del archivo de configuración**

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



Comandos de configuración (VII)

- **Configuración acceso a consola**

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	S1# configure terminal
Cambio del modo de configuración global a modo de configuración de línea para la consola 0.	S1(config)# line con 0
Establece cisco como contraseña para la línea de la consola 0 del switch.	S1(config-line)# password cisco
Establece la linea de consola para que solicite el ingreso de la contraseña antes de conceder el acceso.	S1(config-line)# login
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	S1(config-line)# end



Comandos de configuración (VIII)

- Configuración acceso a terminal

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	S1# configure terminal
Cambio del modo de configuración global a modo de configuración de línea para las líneas vty de 0 a 4.	S1(config)# line vty 0 4
Establezca cisco como contraseña para las líneas vty del switch.	S1(config-line)# password cisco
Establezca las líneas vty para que soliciten el ingreso de la contraseña antes de conceder el acceso.	S1(config-line)# login
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	S1(config-line)# end

La importancia de la seguridad en las capas 2 y 3 de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Comandos de configuración (IX)

- Configuración de contraseñas para el modo EXEC

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	S1# configure terminal
Configura la enable password para ingresar al modo EXEC privilegiado.	S1(config)# enable password contraseña
Configura la enable secret para ingresar al modo EXEC privilegiado.	S1(config)# enable secret contraseña
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	S1(config)# end

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	S1# configure terminal
Configurar un título de MOTD de inicio de sesión.	S1(config)# banner motd "Device maintenance will be occurring on Friday!"



Comandos de configuración (X)

- Configuración de Telnet

```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

- Configuración SSH

```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```



Comandos de configuración (XI)

Guión de configuración de seguridad de puerto

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global. Use este comando del IOS de Cisco:	S1# configure terminal
Especificar el tipo y número de interfaz física a configurar. Use este comando del IOS de Cisco:	S1(config)# interface fastEthernet 0/18
Establecer el modo de interfaz como acceso. Use este comando del IOS de Cisco:	S1(config-if)# switchport mode access
Activar la seguridad de puerto en la interfaz. Use este comando del IOS de Cisco:	S1(config-if)# switchport port-security
Establecer el número máximo de direcciones seguras en 50. Use este comando del IOS de Cisco:	S1(config-if)# switchport port-security maximum 50
Activar el aprendizaje sin modificaciones. Use este comando del IOS de Cisco:	S1(config-if)# switchport port-security mac-address sticky
Volver al modo EXEC privilegiado. Use este comando del IOS de Cisco:	S1(config-if)# end

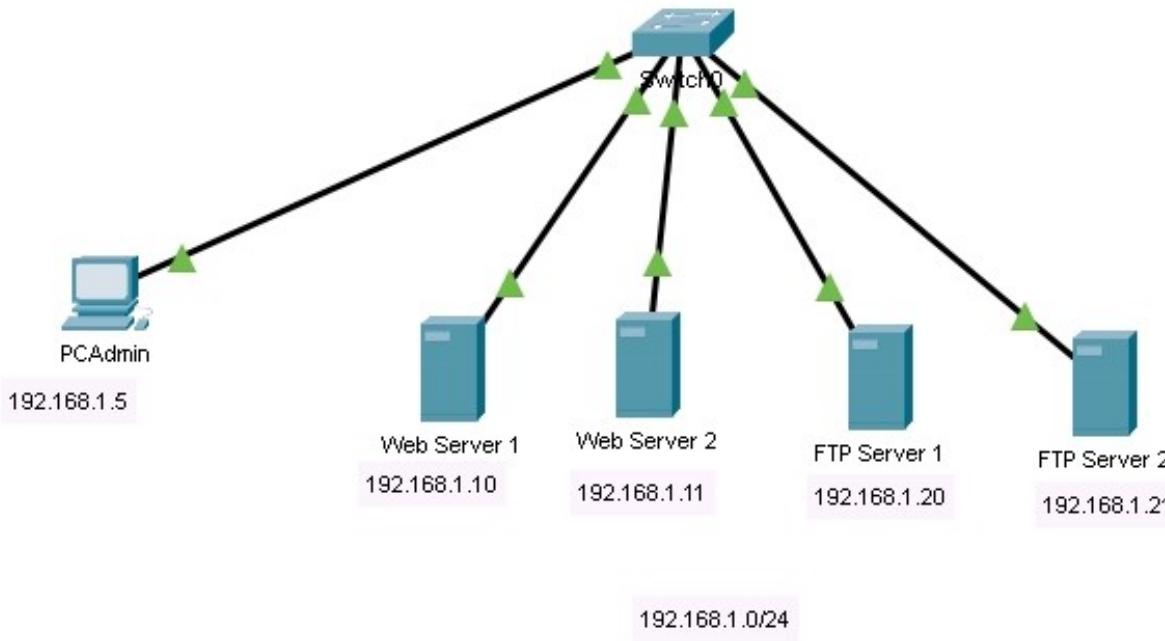


Tabla de contenidos

- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - Configuración de switchs:
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - **Práctica 1**
- **Seguridad en capa 2: Segmentación de redes (VLAN)**
 - **Práctica 2**
- **Enrutamiento inter-VLAN:**
 - **Práctica 3**
- **Seguridad en capa 3: ACL**
 - **Práctica 4**



Práctica 1: Seguridad de puertos



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Tabla de contenidos

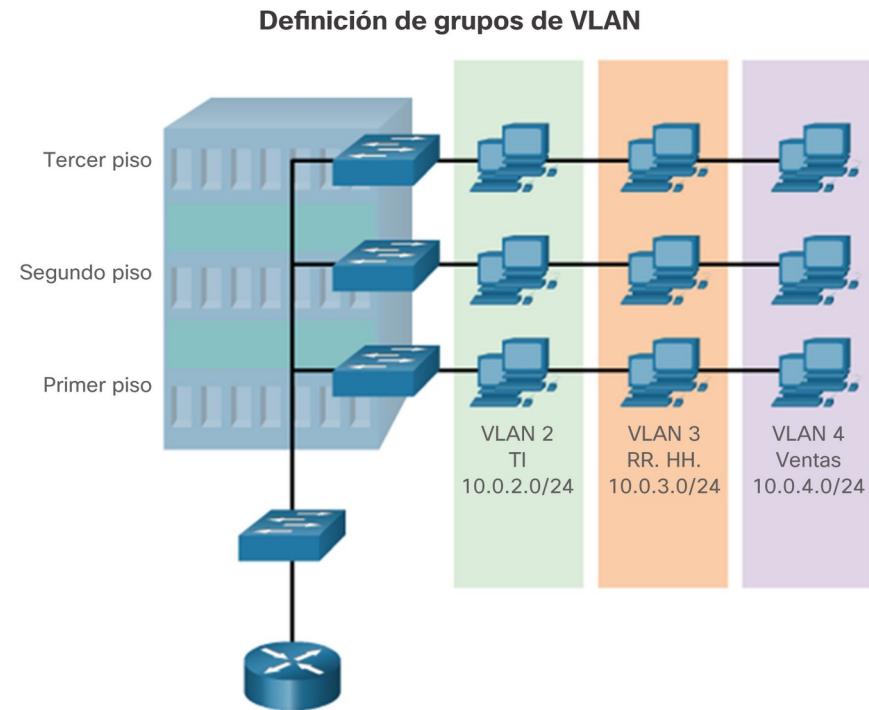
- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - Configuración de switchs:
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - Práctica 1
- **Seguridad en capa 2: Segmentación de redes (VLAN)**
 - Práctica 2
- **Enrutamiento inter-VLAN:**
 - Práctica 3
- **Seguridad en capa 3: ACL**
 - Práctica 4



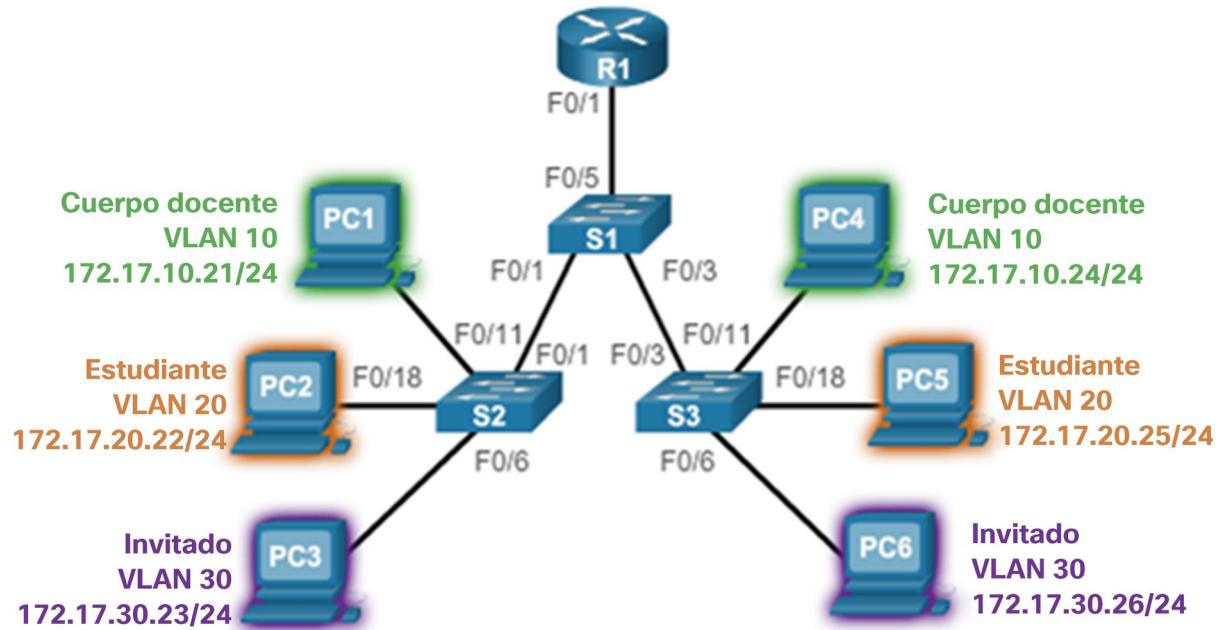
VLAN (I)

- **Definiciones:**

- Es una subred IP separada de manera lógica.
- Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada.
- Para que los equipos informáticos se comuniquen en la misma VLAN, deben tener una dirección IP y una máscara de subred consistente con esa VLAN.
- En el switch deben darse de alta las VLAN y cada puerto asignarse a la VLAN correspondiente. Un puerto de switch con una VLAN singular configurada en el mismo se denomina puerto de acceso



VLAN (II)



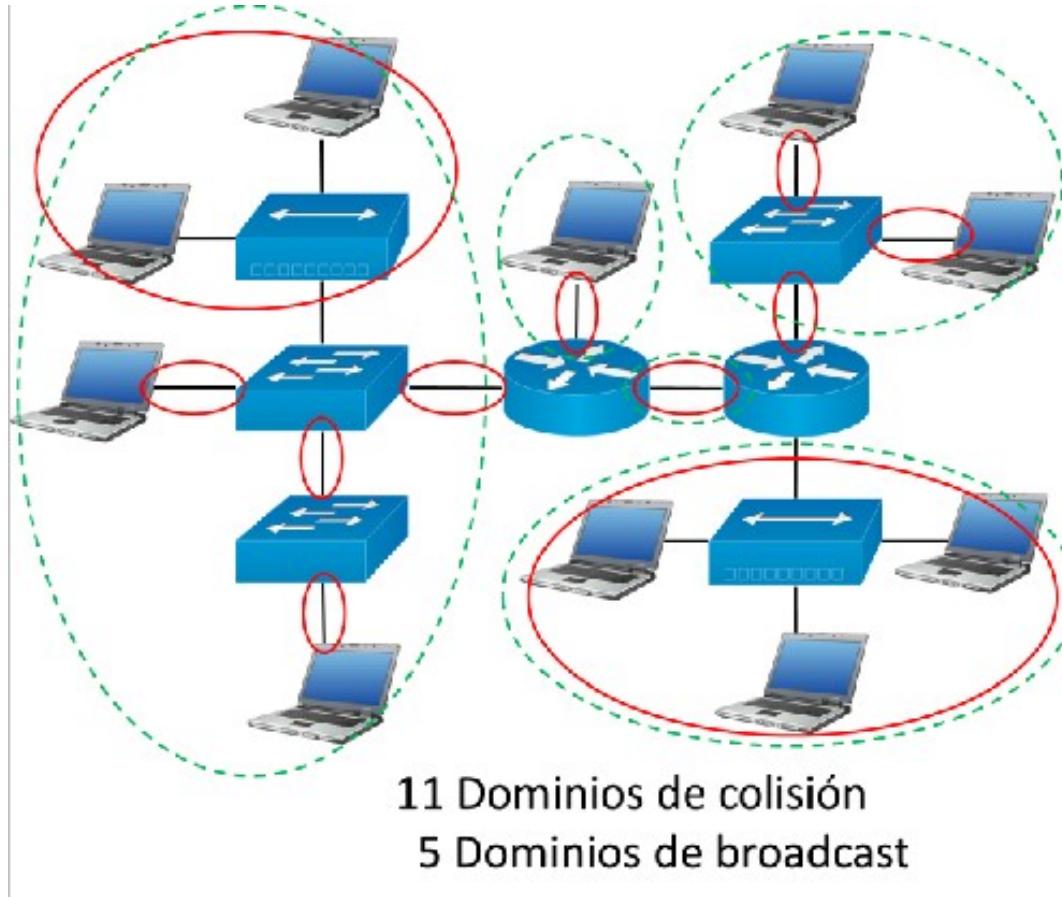
- Seguridad mejorada
- Reducción de costos
- Mejor rendimiento
- Dominios de difusión más pequeños
- Eficacia de TI
- Eficacia administrativa
- Administración más simple de proyectos y aplicaciones

La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



VLAN (III)

- Dominio de colisión y difusión (II):



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



VLAN (IV)

- **Tipos (I):**
 - **Red VLAN de datos:**
 - Tráfico generado por el usuario
 - **Red VLAN predeterminada:**
 - Todos los puertos de switch se convierten en un miembro de la VLAN predeterminada tras el arranque inicial del switch.
 - Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch.
 - La VLAN predeterminada para los switches de Cisco es la VLAN 1. La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no la puede volver a denominar y no la puede eliminar.
 - **Red VLAN nativa:**
 - Se utiliza para tráfico no etiquetado
 - Admite el tráfico que llega de diferentes VLAN (tráfico etiquetado) así como el tráfico que no llega de una VLAN (tráfico no etiquetado).



VLAN (V)

- **Tipos (II):**
 - **Red VLAN de administración:**
 - Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades administrativas de un switch.
 - La VLAN 1 serviría como VLAN de administración si no definió proactivamente una VLAN única para que sirva como VLAN de administración.
 - Se asigna una dirección IP y una máscara de subred a la VLAN de administración.
 - **VLAN de voz:**
 - Ancho de banda garantizado para asegurar la calidad de la voz
 - Alta prioridad de la transmisión sobre otros tipos de tráfico de la red
 - Posibilidad de routing en áreas congestionadas de la red.
 - Demora inferior a 150 ms en toda la red.



VLAN (VI)

- **Enlaces troncales (I):**
 - Un enlace troncal de VLAN es un enlace punto a punto que transporta datos de más de una red VLAN.
 - Generalmente, se establece entre switches para que los dispositivos de una misma red VLAN se puedan comunicar, incluso si están conectados físicamente a switches diferentes.
 - Un enlace troncal de VLAN no está asociado a ninguna red VLAN; tampoco se utilizan los puertos de enlace troncal para establecer el enlace troncal.
 - Cisco IOS admite IEEE802.1q, un protocolo de enlace troncal VLAN muy utilizado.



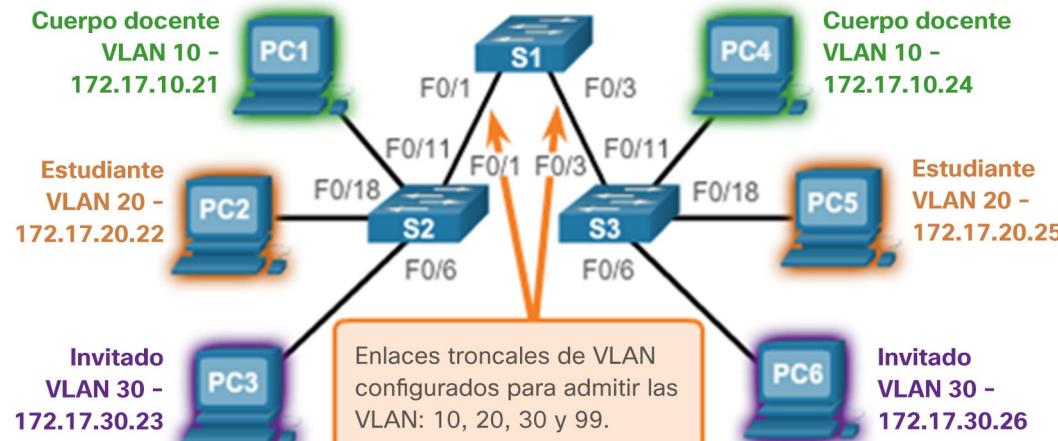
VLAN (VII)

- **Enlaces troncales (II):**

- Los enlaces entre los switches S1 y S2, y entre S1 y S3, se configuraron para transmitir tráfico proveniente de las redes VLAN 10, 20, 30 y 99 a través de la red. Esta red no podría funcionar sin los enlaces troncales de VLAN.

VLAN 10 Cuerpo docente/Personal –
172.17.10.0/24
VLAN 20 Estudiantes – 172.17.20.0/24
VLAN 30 Invitado – 172.17.30.0/24
VLAN 99 Management and Native –
172.17.99.0/24

F0/1 son interfaces de enlaces troncales
802.1Q con VLAN 99 nativa.
F0/11-17 están en VLAN 10.
F0/18-24 están en VLAN 20.
F0/6-10 están en VLAN 30.



de la red. Aplicación en granjas web.

Juan Carlos Gámez Granados



VLAN (VIII)

- **Dominios de difusión (I):**
 - Las redes VLAN se pueden utilizar para limitar el alcance de las tramas de difusión.
 - Una red VLAN es un dominio de difusión propio.
 - Una trama de difusión enviada por un dispositivo en una red VLAN específica se reenvía solamente dentro de esa red VLAN.
 - Las redes VLAN ayudan a controlar el alcance de las tramas de difusión y su impacto en la red.
 - Las tramas de unidifusión y multidifusión también se reenvían dentro de la red VLAN de origen.

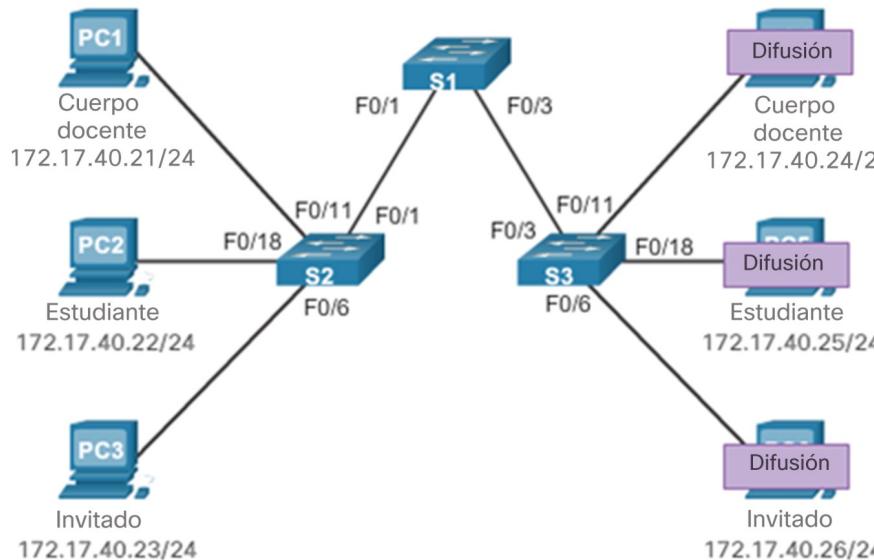


VLAN (IX)

- ## Dominios de difusión (II):

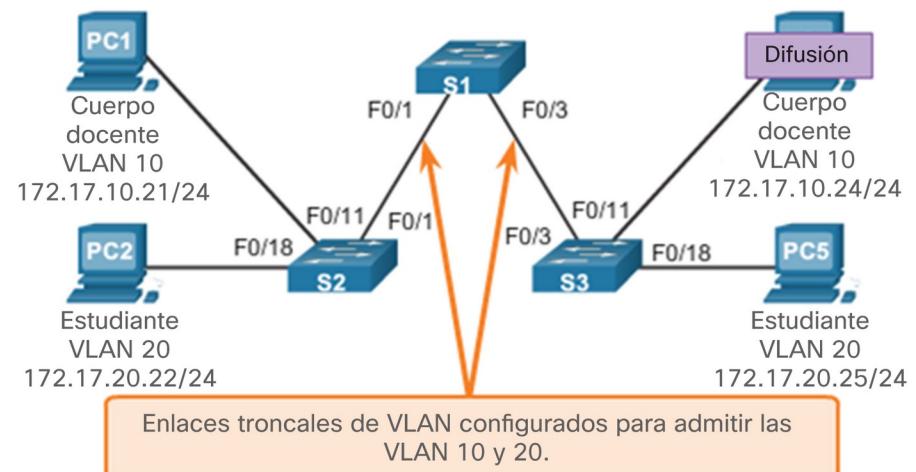
Sin segmentación de VLAN

La PC1 envía una difusión de capa 2 local. Los switches reenvían la trama del broadcast a todos los puertos disponibles.



Con segmentación de VLAN

La PC1 envía una difusión de capa 2 local. Los switches reenvían la trama de la difusión solamente a los puertos configurados para VLAN 10.



La importancia de la seguridad en las capas 2 y 3 de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados

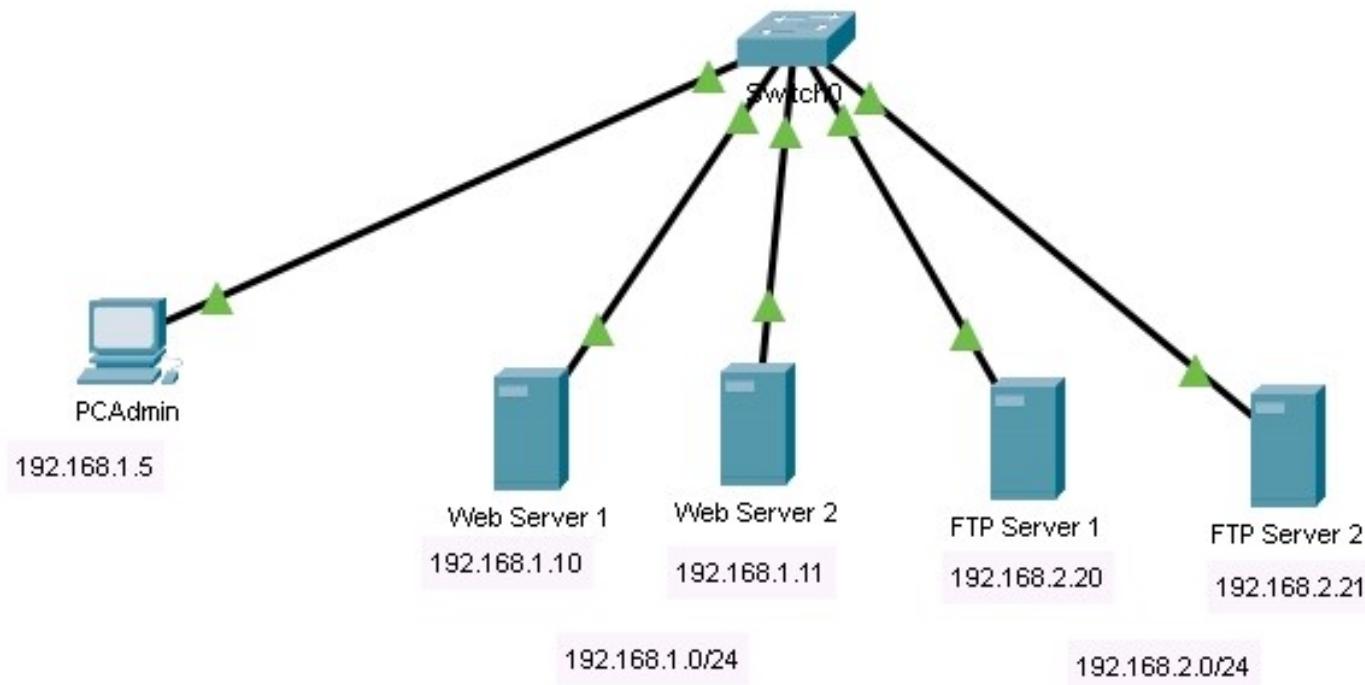


Tabla de contenidos

- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - Configuración de switchs:
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - Práctica 1
- Seguridad en capa 2: Segmentación de redes (VLAN)
 - Práctica 2
- Enrutamiento inter-VLAN:
 - Práctica 3
- Seguridad en capa 3: ACL
 - Práctica 4



Práctica 2: Segmentación VLAN



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Tabla de contenidos

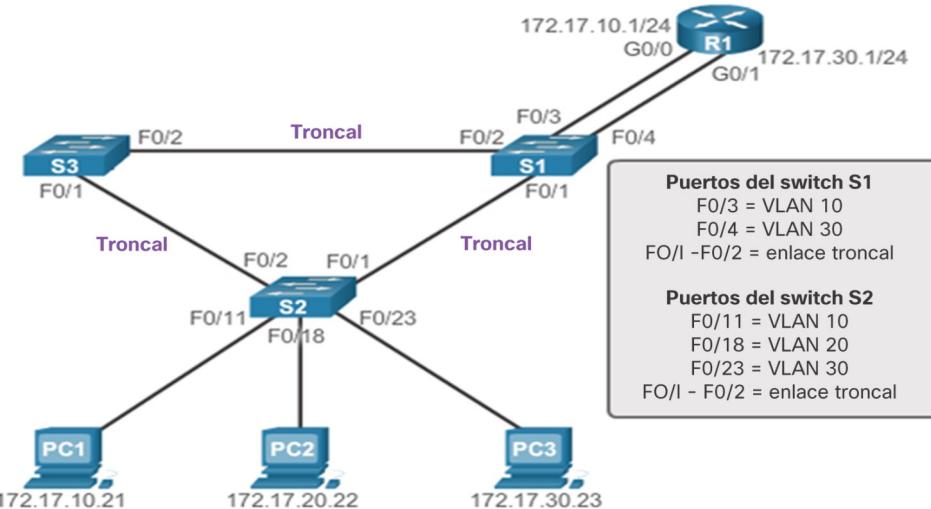
- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - Configuración de switchs:
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - Práctica 1
- **Seguridad en capa 2: Segmentación de redes (VLAN)**
 - Práctica 2
- **Enrutamiento inter-VLAN:**
 - Práctica 3
- **Seguridad en capa 3: ACL**
 - Práctica 4



Enrutamiento inter-VLAN (I)

- Routing entre VLAN Antiguo:
 - Se usaban routers físicos para el routing entre redes VLAN.
 - Cada red VLAN se conectaba a una interfaz de router física diferente.
 - Los paquetes llegaban al router a través de una interfaz, se enrutaban y salían por otra interfaz.
 - Como las interfaces del router estaban conectadas a redes VLAN y tenían direcciones IP provenientes de esa red VLAN específica, se hacía posible el routing entre redes VLAN.
 - Las redes grandes con una gran cantidad de redes VLAN necesitaban muchas interfaces de router.

Routing entre VLAN antiguo



Enrutamiento inter-VLAN (II)

- Routing entre VLAN Router-on-a-stick:
 - El enfoque router-on-a-stick utiliza solo una de las interfaces físicas del router.
 - Una de las interfaces físicas del router se configura como un puerto de enlace troncal 802.1Q para que pueda comprender las etiquetas de las redes VLAN.
 - Se crean subinterfaces lógicas, una por cada red VLAN.
 - Cada subinterfaz se configura con una dirección IP proveniente de la red VLAN que representa.
 - Los miembros de las VLAN (hosts) se configuran para utilizar la dirección de subinterfaz como gateway predeterminado.

Routing entre redes VLAN con un "Router-on-a-Stick"

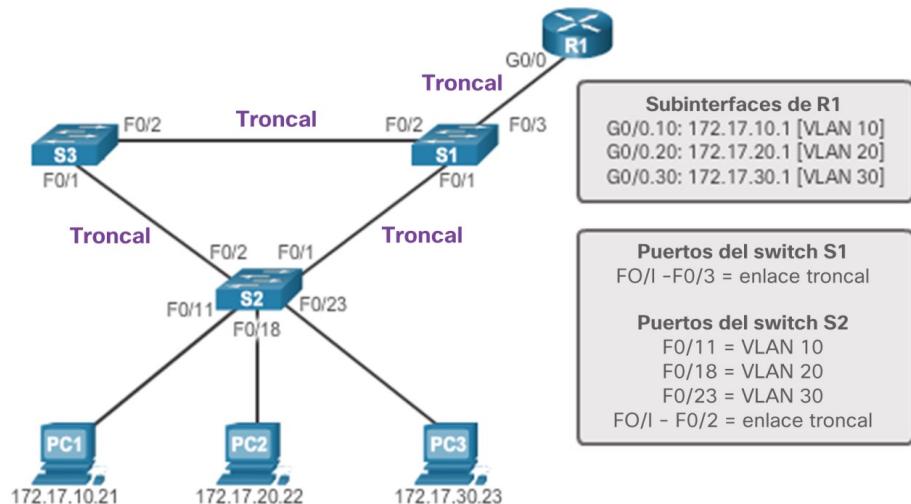
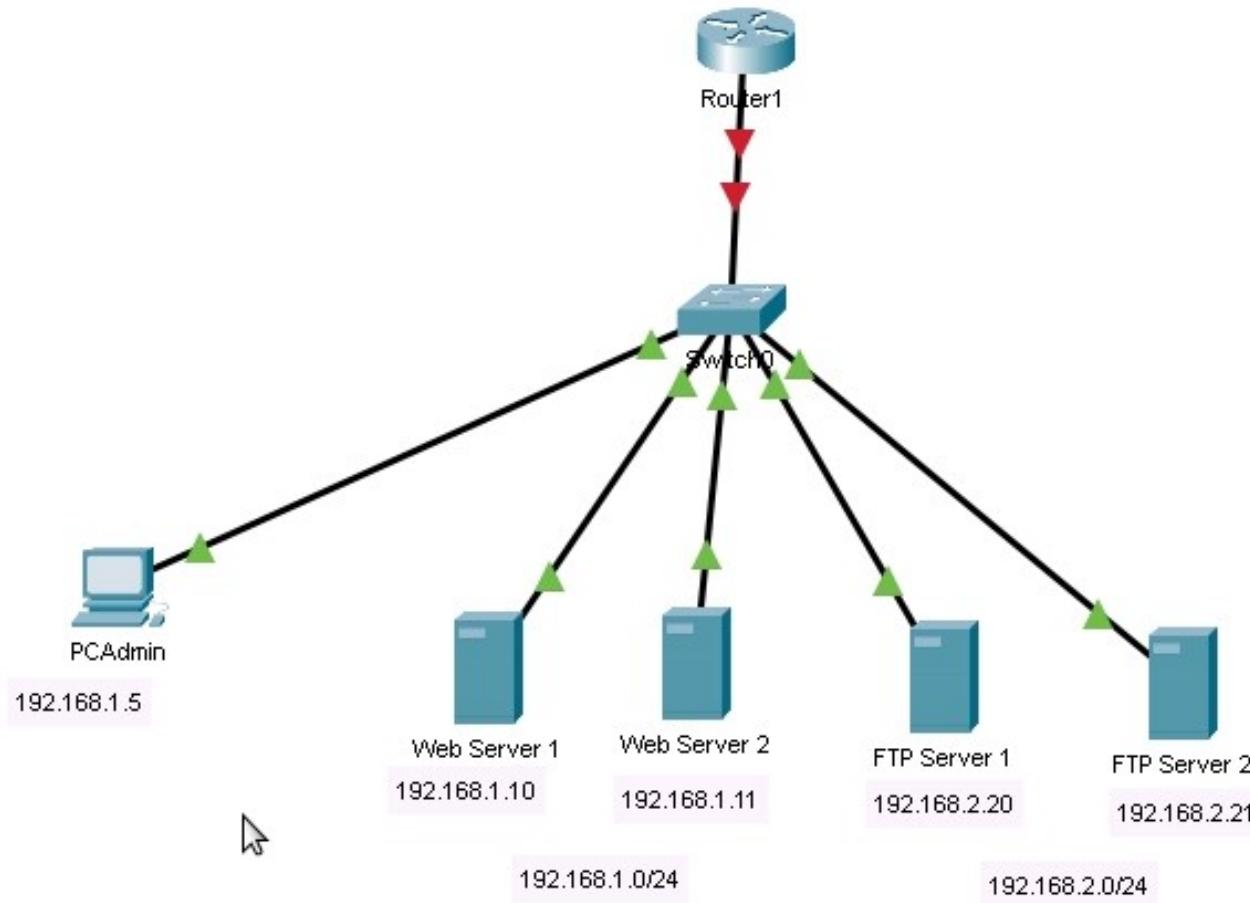


Tabla de contenidos

- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - Configuración de switchs:
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - Práctica 1
- **Seguridad en capa 2: Segmentación de redes (VLAN)**
 - Práctica 2
- **Enrutamiento inter-VLAN:**
 - **Práctica 3**
- **Seguridad en capa 3: ACL**
 - Práctica 4



Práctica 3: Acceso entre servers



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Tabla de contenidos

- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - Configuración de switchs:
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - Práctica 1
- **Seguridad en capa 2: Segmentación de redes (VLAN)**
 - Práctica 2
- **Enrutamiento inter-VLAN:**
 - Práctica 3
- **Seguridad en capa 3: ACL**
 - Práctica 4



Implementación de la Seg. (I)

- Control de acceso:
 - Configuración de contraseñas para acceso a Router y Switch mediante ssh.
 - AAA: Autenticación, Autorización y Contabilidad
 - Es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y qué acciones realizan mientras acceden a la red (contabilizar).

```
S1#configure terminal  
  
S1(config)#line con 0  
  
S1(config-line)#password cisco  
  
S1(config-line)#login  
  
S1(config-line)#end
```

```
S1#configure terminal  
  
S1(config)#enable password contraseña  
  
S1(config)#enable secret contraseña  
  
S1(config)#end
```

```
R1(config)# ip domain-name example.com  
R1(config)# crypto key generate rsa general-keys modulus 2048  
R1(config)# username Admin secret Str0ng3rPa55w0rd  
R1(config)# ssh version 2  
R1(config)# line vty 0 4  
R1(config-line)# transport input ssh  
R1(config-line)# login local
```

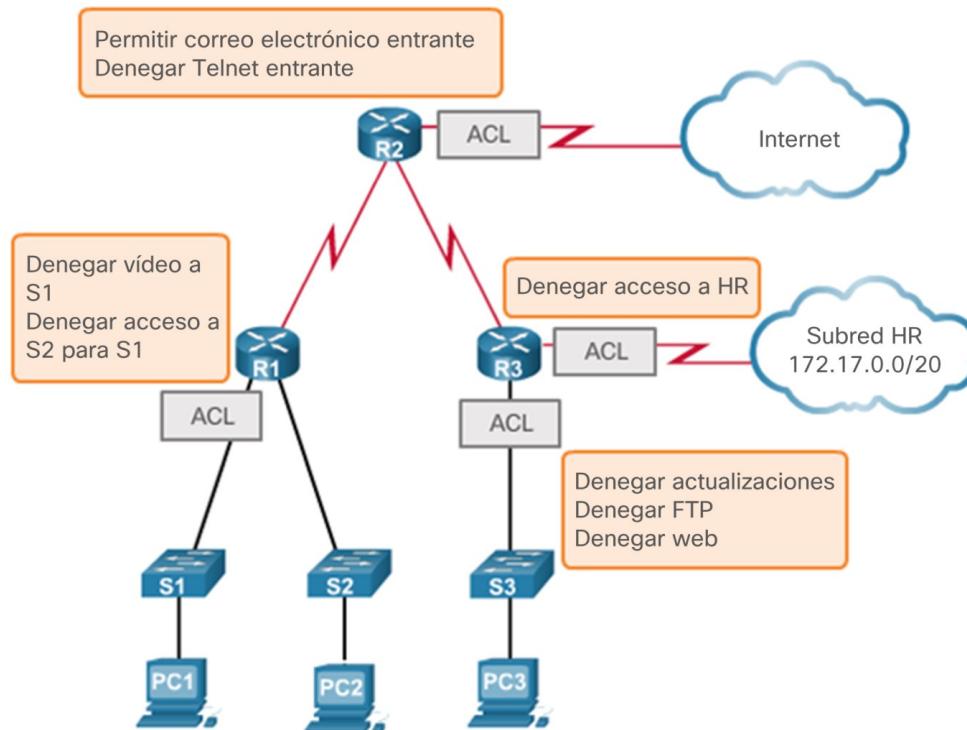
```
S1#configure terminal  
  
S1(config)#line vty 0 4  
  
S1(config-line)#password  
cisco  
  
S1(config-line)#login  
  
S1(config-line)#end
```

La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Implementación de la Seg. (II)

- Listas de control de acceso (ACL) (I):
 - Una ACL es una lista secuencial de sentencias de permiso o denegación que se aplican a direcciones IP o protocolos de capa superior.
 - Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar), conocidas como “entradas de control de acceso” (ACE).

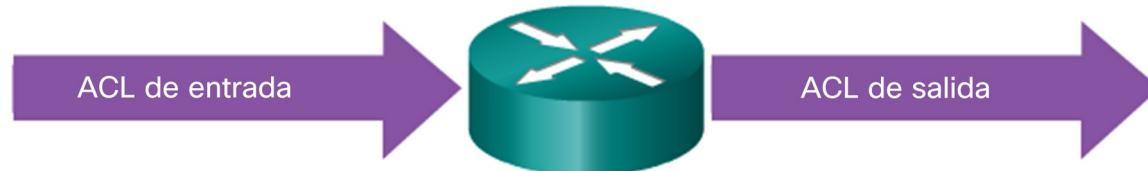


La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Implementación de la Seg. (III)

- Listas de control de acceso (ACL) (II):
 - El filtrado de paquetes, a veces denominado “filtrado de paquetes estático”, controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según determinados criterios, como la dirección IP de origen, la dirección IP de destino y el protocolo incluido en el paquete.
 - Cuando reenvía o deniega los paquetes según las reglas de filtrado, un router funciona como filtro de paquetes.



Las ACL de entrada filtran los paquetes que ingresan a una interfaz específica y lo hacen antes de que se enruten a la interfaz de salida.

Las ACL de salida filtran los paquetes después de que se enrutan, independientemente de la interfaz de entrada.



Implementación de la Seg. (IV)

- Listas de control de acceso (ACL) (III):
 - Las ACL realizan las siguientes tareas:
 - Limitar el tráfico de red para mejorar el rendimiento de ésta.
 - Por ejemplo, si la política corporativa no permite el tráfico de video en la red, pueden configurarse y aplicarse las ACL que bloquean el tráfico de video. Esto reduce considerablemente la carga de la red y aumenta su rendimiento.
 - Brindar control de flujo de tráfico.
 - Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
 - Proporcionar un nivel básico de seguridad para el acceso a la red.
 - Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, el acceso a la red de Recursos Humanos puede restringirse a determinados usuarios.
 - Se debe decidir qué tipos de tráfico enviar o bloquear en las interfaces del router.
 - Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de Telnet.
 - Controlar las áreas de la red a las que puede acceder un cliente.
 - Analizar los hosts para permitir o denegar su acceso a los servicios de red.
 - Las ACL pueden permitir o denegar el acceso de un usuario a tipos de archivos, como FTP o HTTP.

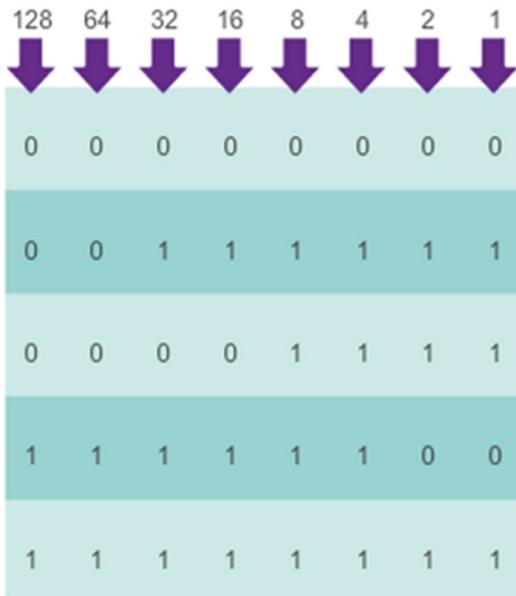


Implementación de

- Listas de control de acceso (ACL) (IV):

Máscaras de wildcard

Posición del bit de octeto y valor de dirección para el bit



0 significa hacer coincidir el valor del bit de dirección correspondiente

1 significa ignorar el valor del bit de dirección correspondiente

Ejemplo 1:

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
!OR
R1(config)# access-list 1 permit any
```

Ejemplo 2:

```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
!OR
R1(config)# access-list 1 permit host 192.168.10.10
```

Máscaras de comodín para establecer coincidencias con hosts y subredes IPv4

Ejemplo 1

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara de comodín	0.0.0.0	00000000.00000000.00000000.00000000
Resultado	192.168.1.1	11000000.10101000.00000001.00000001

Ejemplo 2

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara de comodín	255.255.255.255	11111111.11111111.11111111.11111111
Resultado	0.0.0.0	00000000.00000000.00000000.00000000

Ejemplo 3

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara de comodín	0.0.0.255	00000000.00000000.00000000.11111111
Resultado	192.168.1.0	11000000.10101000.00000001.00000000



Implementación de la Seg. (VI)

- Listas de control de acceso (ACL) (V):
 - Reglas para aplicar ACL

Filtrado de tráfico en un router mediante ACL



Una lista por interfaz, por dirección y por protocolo

Con dos interfaces y dos protocolos en ejecución, este router podría tener un total de ocho ACL distintas aplicadas.

Reglas para aplicar las ACL

Solo se puede tener una ACL por protocolo, por interfaz y por sentido:

- Una ACL por protocolo (p. ej., IPv4 o IPv6)
- Una ACL por sentido (es decir, de entrada o de salida)
- Una ACL por interfaz (p. ej., GigabitEthernet0/0)



Implementación de la Seg. (VII)

- Listas de control de acceso (ACL) (VI):
 - Tipos de ACL (I):
 - Estándar
 - Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan.
 - Extendida
 - Las ACL extendidas filtran paquetes IPv4 según varios atributos:
 - » Tipo de protocolo
 - » Dirección IPv4 de origen
 - » Dirección IPv4 de destino
 - » Puertos TCP o UDP de origen
 - » Puertos TCP o UDP de destino
 - » Información optativa de tipo de protocolo para un control más preciso



Implementación de la Seg. (VIII)

- Listas de control de acceso (ACL) (VII):
 - Tipos de ACL (II):

ACL denominada:

Asignar un nombre para identificar la ACL.

- Los nombres pueden contener caracteres alfanuméricos.
- Se sugiere escribir el nombre en MAYÚSCULAS.
- Los nombres no pueden contener espacios ni signos de puntuación.
- Se pueden agregar o eliminar entradas dentro de la ACL.

ACL numerada:

Asignar un número según el protocolo que se debe filtrar.

- (1 a 99) y (1300 a 1999): ACL de IP estándar
- (100 a 199) y (2000 a 2699): ACL de IP extendida

La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



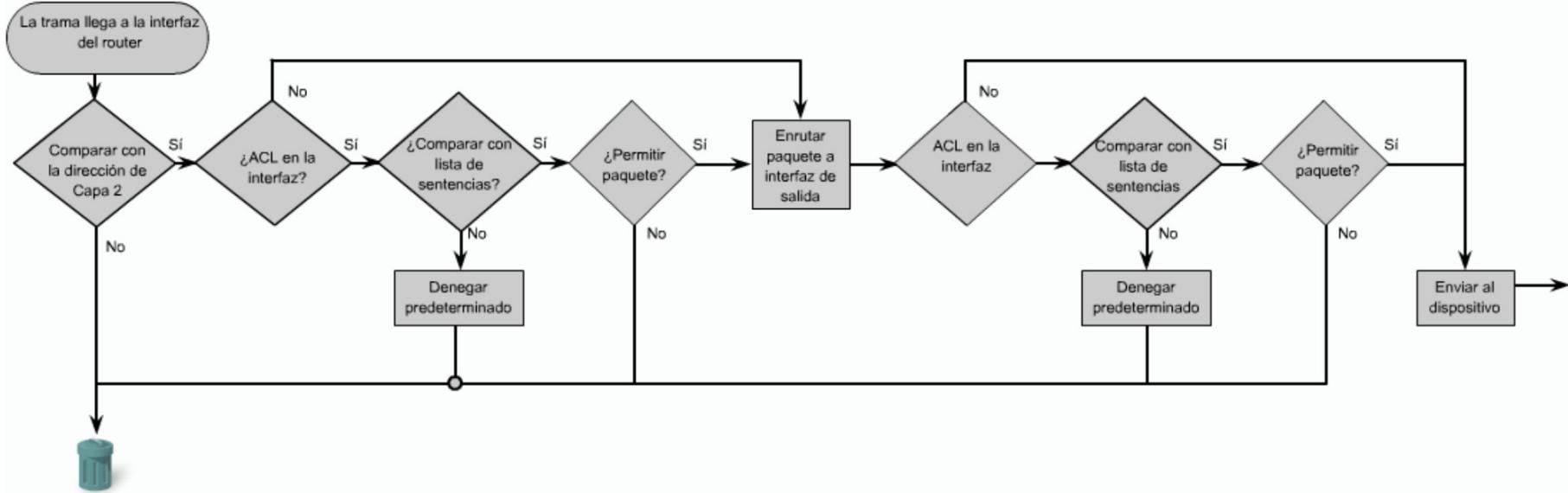
Implementación de la Seg. (IX)

- Listas de control de acceso (ACL) (VIII):
 - Funcionamiento (I):
 - Las ACL no actúan sobre paquetes que se originan en el mismo router.
 - Las ACL se configuran para ser aplicadas al tráfico entrante o saliente.
 - Las sentencias de la ACL operan en orden secuencial.
 - Una sentencia implícita final cubre todos los paquetes para los cuales las condiciones no resultan verdaderas (implicit deny any statement/deny all traffic).
 - ACL de salida, antes de reenviar un paquete a una interfaz de salida, el router verifica la tabla de enrutamiento para ver si el paquete es enrutable.



Implementación de la Seg. (X)

- Listas de control de acceso (ACL) (IX):
 - Funcionamiento (II):

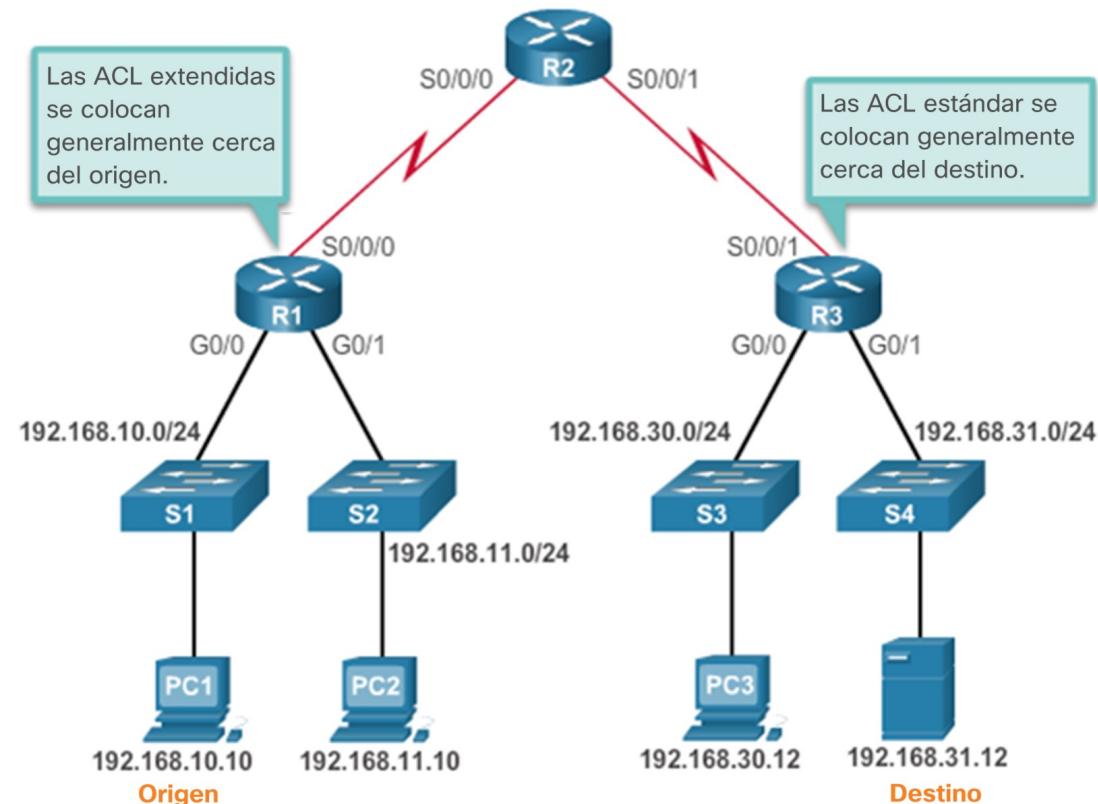


La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Implementación de la Seg. (XI)

- Listas de control de acceso (ACL) (XI):
 - ¿Dónde ubicar las ACL? (I):



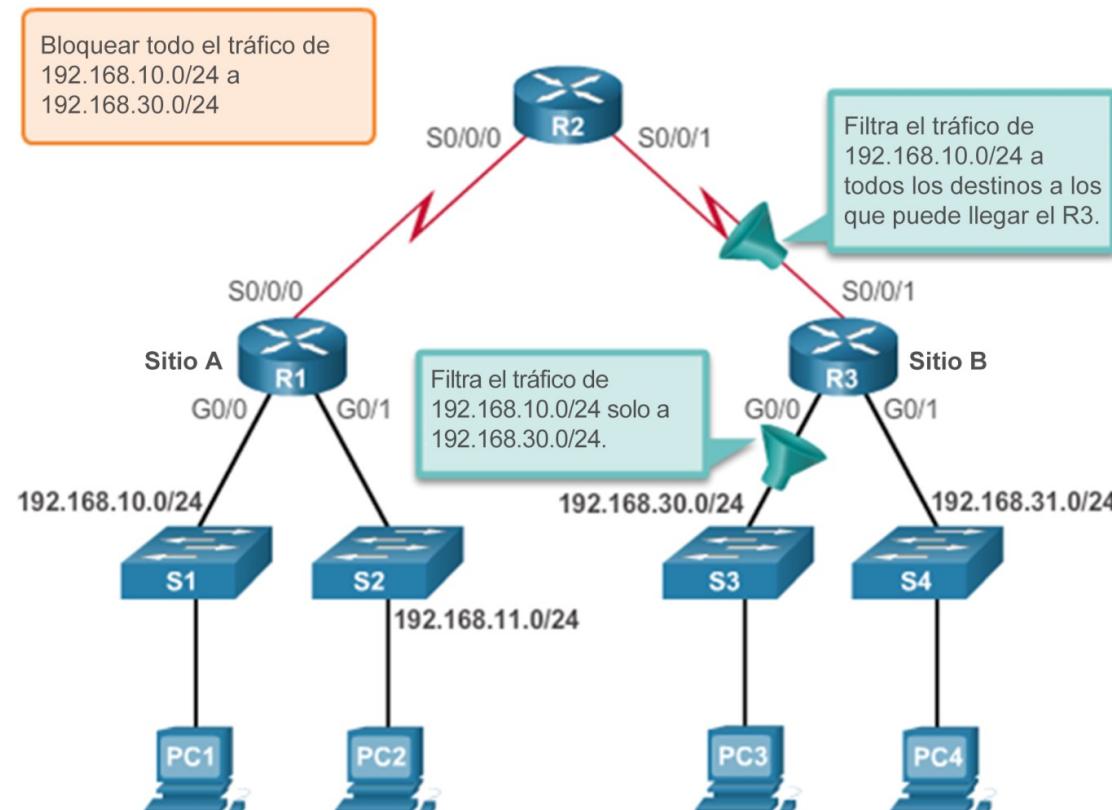
La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.

Juan Carlos Gámez Granados



Implementación de la Seg. (XII)

- Listas de control de acceso (ACL) (XII):
 - Ejemplo ACL estándar: El administrador desea impedir que el tráfico que se origina en la red 192.168.10.0/24 llegue a la red 192.168.30.0/24.

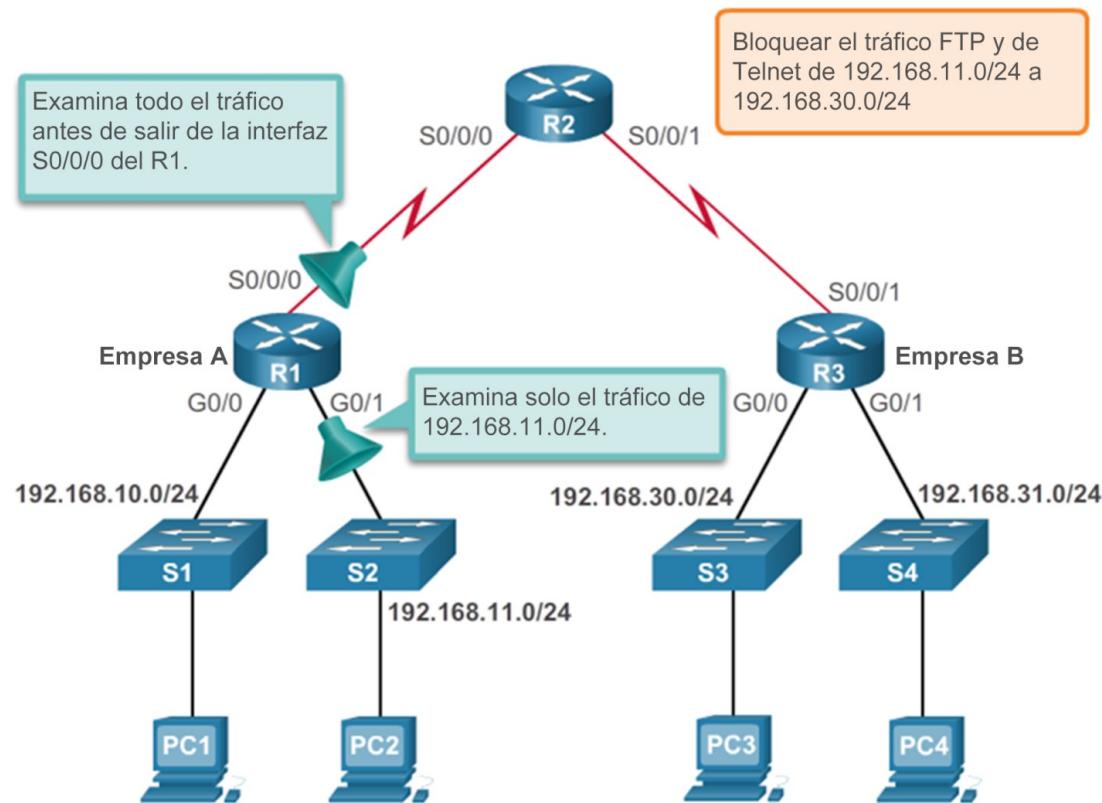


La importancia de la seguridad en las capas 2 y 3 de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Implementación de la Seg. (XIII)

- Listas de control de acceso (ACL) (XIII):
 - Ejemplo ACL extendida: Lo que el administrador desea es denegar el tráfico de Telnet y FTP de la red 192.168.11.0/24 a la red 192.168.30.0/24 de la empresa B. Se debe permitir que el resto del tráfico de la red .11 salga de la empresa A sin restricciones.

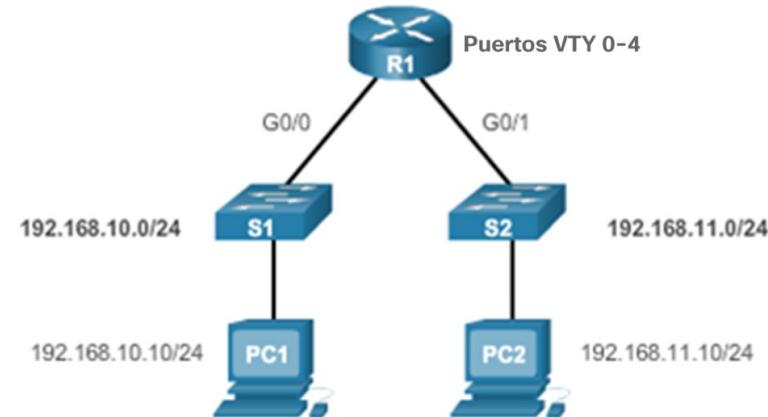


La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados



Implementación de la Seg. (XIV)

- Listas de control de acceso (ACL) (XIV):
 - ACL para terminal: El comando access-class configurado en el modo de configuración de línea restringe las conexiones entrantes y salientes entre una VTY determinada (en un dispositivo de Cisco) y las direcciones incluidas en una lista de acceso.



```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados

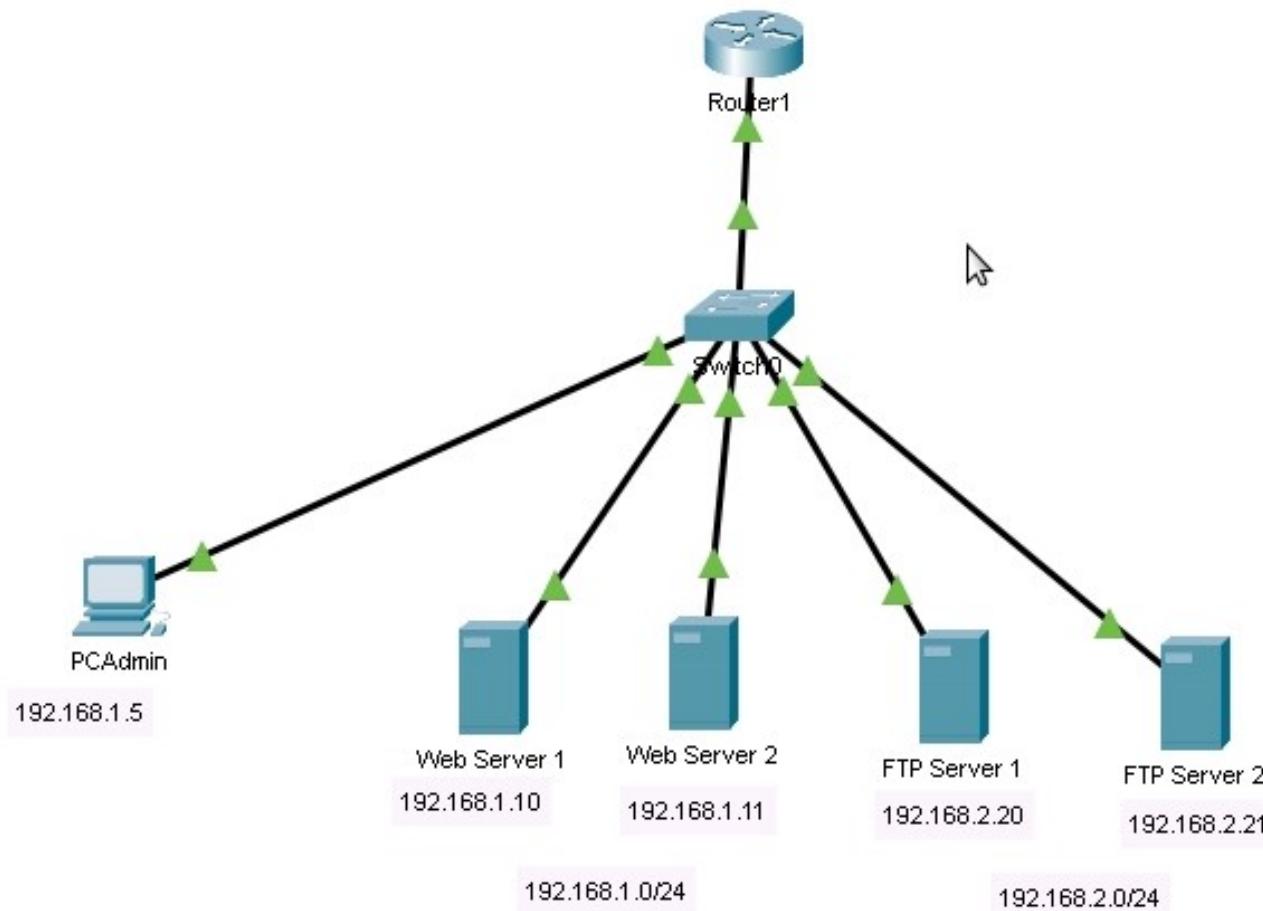


Tabla de contenidos

- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - Configuración de switchs:
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - Práctica 1
- **Seguridad en capa 2: Segmentación de redes (VLAN)**
 - Práctica 2
- **Enrutamiento inter-VLAN:**
 - Práctica 3
- **Seguridad en capa 3: ACL**
 - Práctica 4



Práctica 4: Restringir acceso



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados

Tabla de contenidos

- **Switch**
 - Elección de switchs
 - Funcionamiento de switchs
 - Configuración de switchs:
 - Acceso al dispositivo
 - Modos de funcionamiento
 - Comandos de configuración
 - Práctica 1
- **Seguridad en capa 2: Segmentación de redes (VLAN)**
 - Práctica 2
- **Enrutamiento inter-VLAN:**
 - Práctica 3
- **Seguridad en capa 3: ACL**
 - Práctica 4



La importancia de la seguridad en las capas 2 y 3 de la red. Aplicación en granjas web.



La importancia de la seguridad en las capas 2 y 3
de la red. Aplicación en granjas web.
Juan Carlos Gámez Granados