CCNA Exploration 4 – Acceso a la WAN

Capítulo 4: Seguridad de la Red Empresarial

Ricardo José Chois Antequera

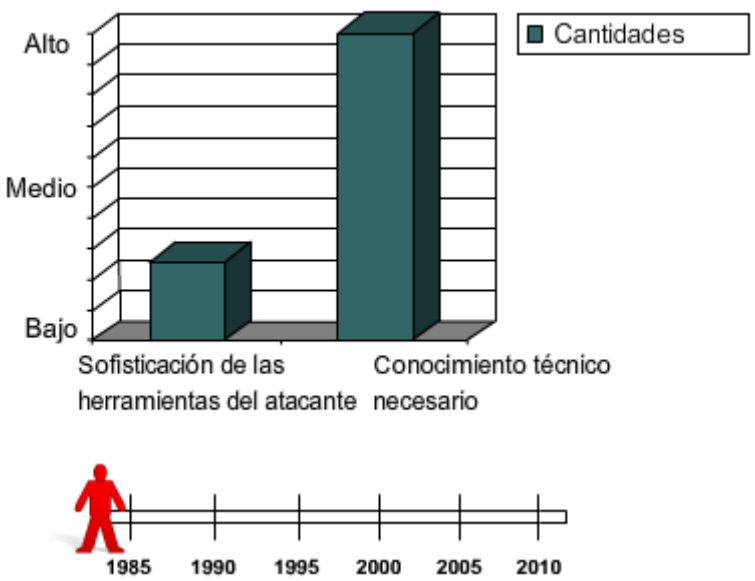
INSTITUTO TECNOLÓGICO DE SOLEDAD ATLÁNTICO - ITSA

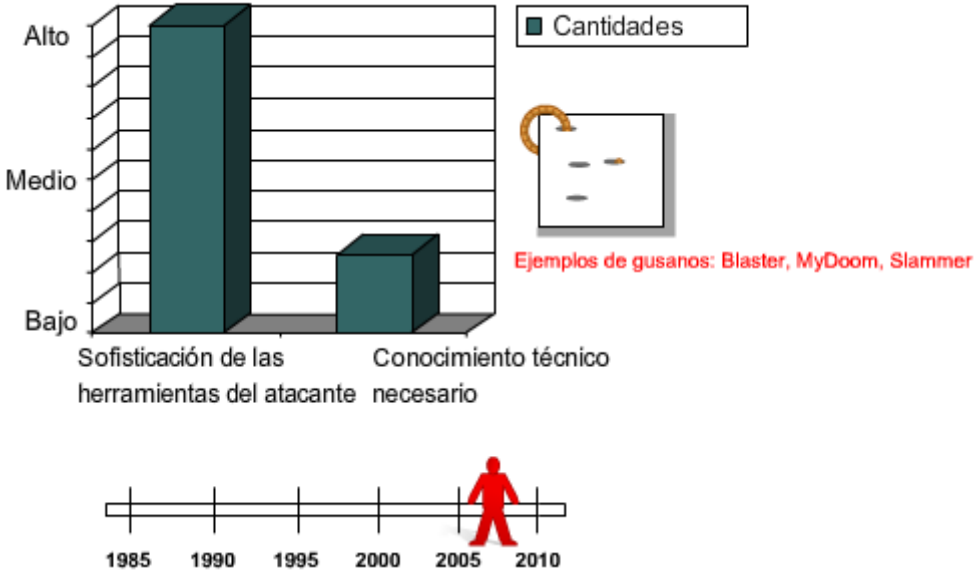
Objetivos

- Describir los métodos generales para mitigar los ataques de seguridad a las redes empresariales.
- Configurar la seguridad básica del router.
- Explicar como deshabilitar servicios e interfaces no utilizadas en routers Cisco.
- Explicar como usar el SDM de Cisco.
- Administrar el IOS de los routers Cisco.

Creciente amenaza…

- Términos usados para describir personas atacantes:
  - Hacker de sombrero blanco → Busca vulnerabilidades e informa para corrección.
  - Hacker → Término general para describir expertos en programación.
  - Hacker de Sombrero negro → Busca beneficio personal o económico. p.e: Cracker
  - Cracker → Busca acceso a la red con intención maliciosa.
  - Phreaker → Manipula red telefónica. Llamadas de larga distancia gratuitas.
  - Spammer → Envió de correo no solicitado.
  - Phisher (Estafador) → Engaña por algún medio para obtener información confidencial.





Piense como un agresor…

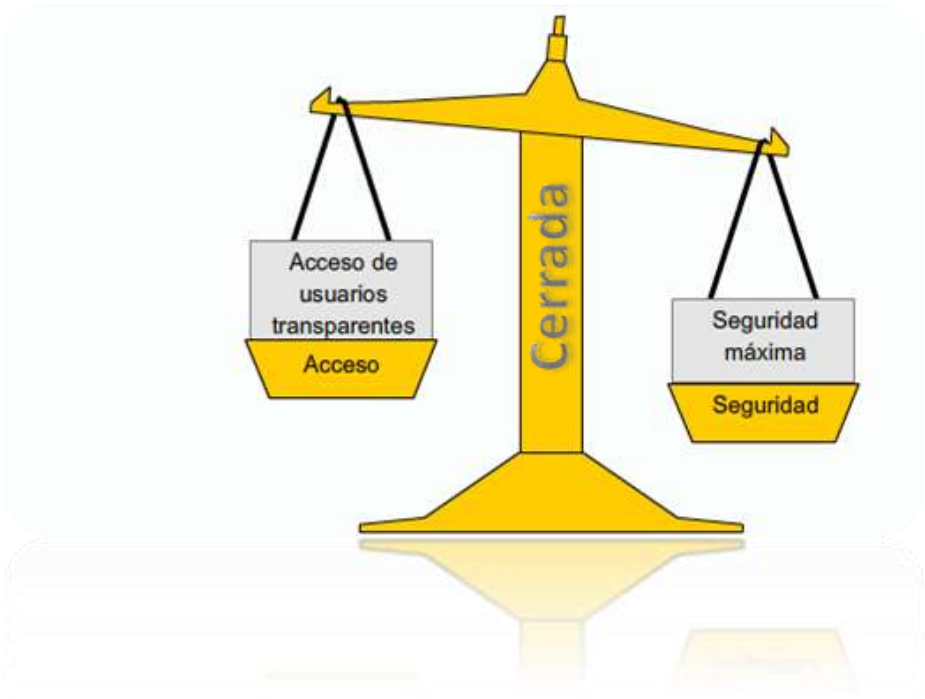
1. Realizar un análisis del perfil (reconocimiento)
   - Por la página web de la empresa, pueden saber la IP del servidor.
2. Enumerar los datos
   - Amplían información buscando versiones de los servidores y buscan vulnerabilidades conocidas de éstas versiones.
3. Manipular a los usuarios para obtener acceso
   - Se aprovechan de contraseñas simples o engañan a los empleados.
4. Aumentar los privilegios
   - Utilizando sus habilidades aumentan privilegios en la red.
5. Recopilar más contraseñas y secretos
   - Utilizan su talento para acceder a información confidencial bien protegida.
6. Aprovecharse del sistema comprometido
   - Utilizan el equipo comprometido para perpetuar otros equipos de la red.

Redes Abiertas Vs. Redes Cerradas

- Abierta → Permite todo lo que no esta explícitamente denegado.
- Cerrada → Se deniega lo que no esta explícitamente permitido.
- Restrictiva → Combinación de permisos específicos y restricciones específicas.

- Fácil de configurar y administrar
- Fácil para los usuarios finales acceder a los recursos de la red
- Menos costoso

- Más difícil de configurar y administrar
- Más difícil para los usuarios finales acceder a los recursos de la red
- El más costoso

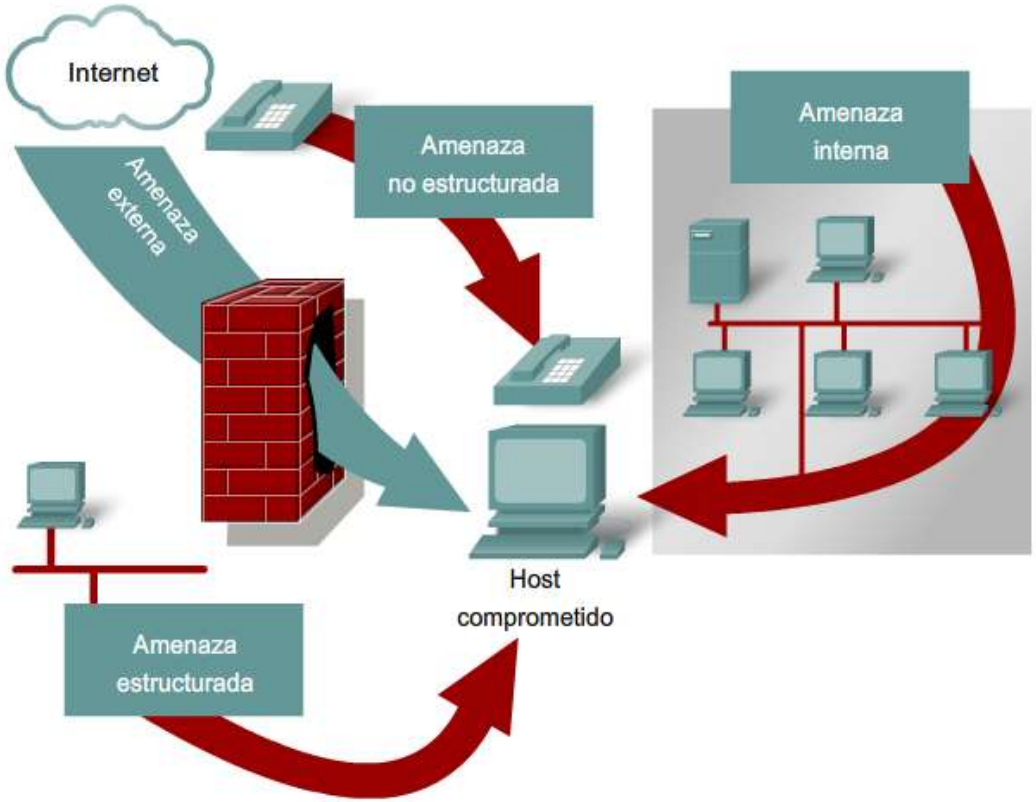


Amenazas comunes de seguridad

- En el análisis de la seguridad de la red, los tres factores comunes son:
  - Vulnerabilidad → Grado de debilidad inherente a cada red y cada dispositivo.
  - Amenaza → Personas interesadas y calificadas para aprovechar cada una de las debilidades en materia de seguridad
  - Ataque → Acción tomada por la amenaza.
- Existen 3 tipos de vulnerabilidades o debilidades:
  - Tecnológicas → TCP/IP, Sistemas Operativos, Equipos de red, etc.
  - De Configuración → Cuentas de usuario, Servicios de Internet, Valores Predeterminados, Equipos de red mal configurados, etc.
  - En la Política de Seguridad → No hay políticas de seguridad, Falta de continuidad, no hay plan de recuperación de desastres, etc.
- Hay 4 tipos de amenazas físicas:
  - Hardware → Evitar accesos no autorizados a través de puerta, cielorraso, monitoreo, cámaras de seguridad, etc.
  - Ambientales → Controles de temperatura, humedad. Alarmas ambientales.
  - Eléctricas → Sistemas de UPS, planes de mantenimiento preventivo, fuentes de energía redundantes, sistemas de alarma y vigilancia.
  - Mantenimiento → Control de acceso a puertos de consola, provisiones de repuestos, etiquetar cables y componentes fundamentales.

Amenazas a las redes

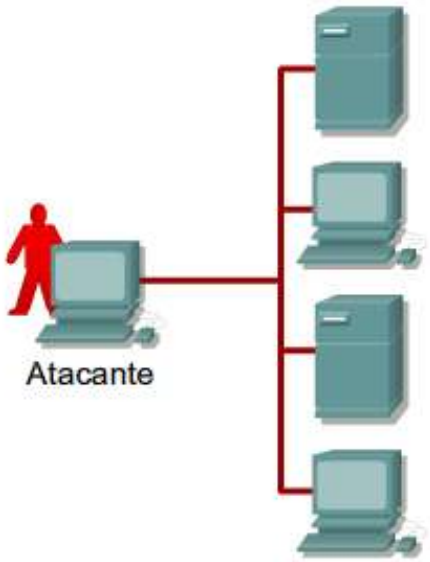
- Tipos de amenazas a las redes:
  - No Estructuradas → Personas sin experiencia con herramientas de piratería.
  - Estructuradas → Personas técnicamente más competentes. Herramientas más sofisticadas.
  - Externas → Personas u organizaciones fuera de la empresa.
  - Internas → Personas con acceso autorizado a la red.



La Ingeniería Social, consiste en engañar a los empleados de una organización para obtener información valiosa. No requiere habilidad informática

Tipos de ataques a las redes

- Ataques de reconocimiento
  - Consultas a través de Internet
  - Barridos de Ping
  - Escaneo de Puertos
  - Programas detectores de paquetes
- Ataques de Acceso
  - Ataque de contraseñas
  - Explotación de confianza
  - Reorientación de puertos
  - Man-in-the-middle
- Ataques de Denegación de Servicio (DoS)
  - Ping de la muerte
  - Saturación SYN
  - DDoS
  - Smurf
- Gusanos, Virus y Troyanos



Técnicas de mitigación de ataques a las redes

- Aseguramiento de dispositivos (Hardening)
- Software Antivirus
  - Detectar virus conocidos
  - Controlar procesos sospechosos
- Firewall Personal
  - Intentan impedir ataques.
- Parches para Sistemas Operativos
  - Del proveedor del SO
  - Con un servidor central. P.e: WSUS
- Detección y Prevención de Intrusiones
  - IDS → Sólo detectan. Existen HIDS (para los Hosts)
  - IPS → Previenen y Reaccionan. HIPS (para los Hosts)
- Aplicaciones y dispositivos.

Cisco ASA 5500

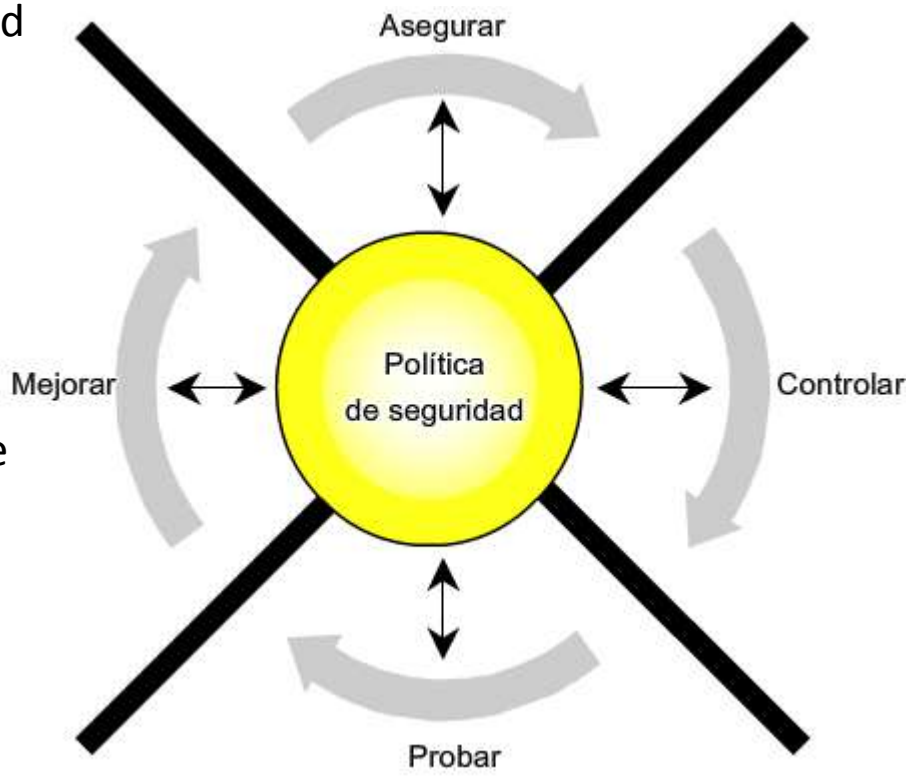
Reemplazan los anteriores firewall PIX. Contienen: firewall, seguridad de voz, VPN de SSL e IPSec, IPS y servicios.

Appliance Cisco NAC

Sensores Cisco serie IPS 4200

La rueda de seguridad de la red

- Paso 1. Asegurar
  - Defensa contra amenazas
  - Inspección de estado y filtrado de paquetes.
- Paso 2. Controlar
  - Métodos activos (IPS) y pasivos (IDS) de detección. Auditoría de archivos.
- Paso 3. Probar
  - Se prueban las soluciones de seguridad
  - Herramientas a nivel de Host como:
    - SATAN
    - Nessus
    - Nmap
- Paso 4. Mejorar
  - Análisis de datos recuperados durante el control y las pruebas
  - Como consecuencia de este paso se adicionan ítems al paso 1.



Política de seguridad de la Empresa

"Una política de seguridad es una declaración formal de las reglas a las cuales se debe adherir el personal que tiene acceso a los bienes tecnológicos y de información de una organización".
(RFC 2196, Manual de seguridad de sitio)

- Es un documento dinámico que tiene los siguientes componentes básicos:
  - Declaración de autoridad y alcance.
  - Política de Uso Aceptable
  - Política de Identificación y Autenticación.
  - Política de Acceso a Internet
  - Política de Acceso al campus.
- Además puede contener en algunos casos:
  - Política de solicitud de cuentas de acceso.
  - Política de evaluación de adquisiciones
  - Política de auditoría.
  - Política de confidencialidad de la información.
  - Política de contraseñas
  - Etc.

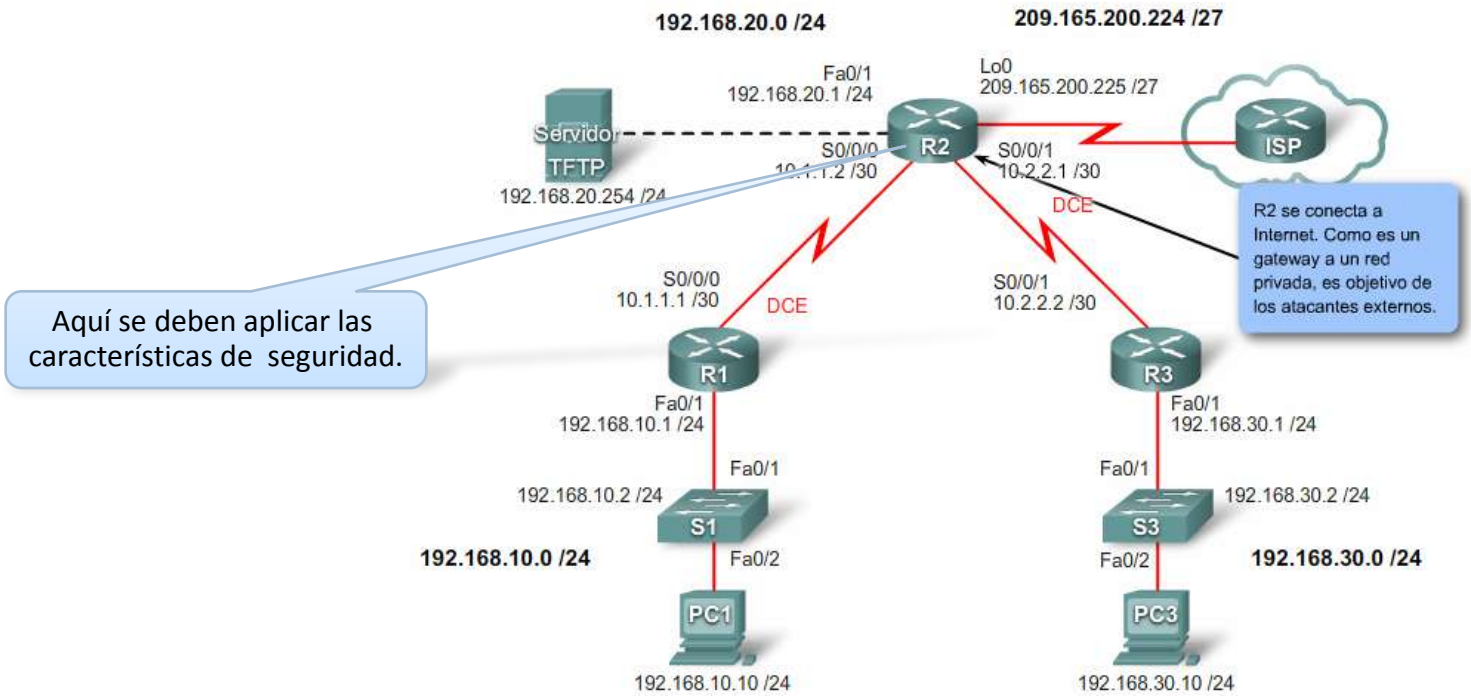
Sitio recomendado para ejemplos:
www.sans.org

Funciones

- Proteger a las personas y a la información
- Establecer la normas de comportamiento esperadas de los usuarios, de los administradores del sistema, de la dirección y del personal de seguridad
- Autorizar al personal de seguridad a monitorear, sondear e investigar
- Definir y autorizar las consecuencias de las violaciones

Configuración básica de seguridad en el router

- Recuerde que los routers:
  - Publican las redes y filtran a quienes pueden utilizarlas.
  - Proporcionar acceso a los segmentos de las redes y a las subredes.
- Por lo anterior son el principal objetivo de ataques.
  - Control de Acceso → Puede exponer los detalles de configuración de la red.
  - Tablas de enrutamiento → Disminuir rendimiento, DoS, exponer información.
  - Configuración incorrecta de filtros → Expone la red a escaneos y ataques.



Aplicación de las características de seguridad del IOS

- Planifique los pasos de la configuración de seguridad del IOS.

Pasos que se deben seguir para proteger un router:
Paso 1. Administre la seguridad del router
Paso 2. Proteja el acceso administrativo remoto a los routers
Paso 3. Registro de la actividad del router
Paso 4. Proteja los servicios y las interfaces del router vulnerables
Paso 5. Proteja los protocolos de enrutamiento
Paso 6. Controle y filtre el tráfico de la red

- Paso 1 → Consiste en la configuración de contraseñas.
  - Aplique las mejores prácticas (frecuencia de cambio, combinaciones, longitud…).
  - Se recomienda contraseñas con frases. Por ejemplo: “Mi espía favorito es James Bond 007” se traduce como *MefeJB007*
- Paso 2 → A medida que crece la red se hace necesario.
  - Utilice SSH en lugar de Telnet, ya que éste último envía el texto no cifrado.
- Paso 3 → Consiste en tener un host dedicado a registrar la actividad.
  - Considere la posibilidad de enviar a un segundo dispositivo.
  - Un ejemplo de servidor syslog es el *Kiwi Syslog Deamon*.
- Paso 4 → Consiste en deshabilitar interfaces y servicios innecesarios.

Configuración de SSH

- **Paso 1.** Configure los parámetros del router

```
Router(config)#hostname R2
```

- **Paso 2.** Configure el nombre de dominio

```
R2(config)#ip domain-name cisco.com
```

- **Paso 3.** Genere claves asimétricas

```
R2(config)#crypto key generate rsa
```

- **Paso 4.** Configure la autenticación local y VTY.

```
R2(config)#username student secret cisco
R2(config)#line vty 0 4
R2(config-line)#transport input ssh
R2(config-line)#login local
```

- **Paso 5.** Configure los tiempos de espera (Opcional)

```
R2(config)#ip ssh time-out 15
R2(config)#ip ssh authentication-retries 2
```

Servicios vulnerables en el router.

Los routers Cisco admiten una gran cantidad de servicios, en la siguiente tabla se muestran algunos y las recomendaciones asociadas.

Característica	Descripción	Predeterminado	Recomendación
Protocolo de descubrimiento de Cisco (CDP)	Protocolo de capa 2 patentado entre dispositivos de Cisco.	Habilitado	El CDP no se necesita casi nunca, deshabilítelo.
Servidores pequeños TCP	Servicios de red TCP estándar: echo, chargen, etc.	>=11.3: deshabilitado 11.2: habilitado	Esta es una característica de versiones anteriores; deshabilítela de manera explícita.
Servidores UDP pequeños	Servicios de red UDP estándar: echo, discard, etc.	>=11.3: deshabilitado 11.2: habilitado	Esta es una característica de versiones anteriores; deshabilítela de manera explícita.
Finger	Servicio de búsqueda de usuario UNIX, permite listado remoto de usuarios.	Habilitado	Las personas sin autorización no deben conocer esto; deshabilítelo.
Servidor HTTP	Algunos dispositivos de Cisco del sistema operativo Internetwork (IOS, Internetwork Operating System) ofrecen una configuración basada en Web.	Varía según el dispositivo	Si no está en uso, deshabilítelo de manera explícita; de lo contrario, restrinja el acceso.
Servidor BOOTP	Realice el mantenimiento para permitir que otros routers arranquen desde éste.	Habilitado	Esto se necesita con poca frecuencia y puede abrir un agujero en la seguridad; deshabilítelo.

Servicios vulnerables en el router (Continuación).

Carga automática de la configuración	El router intentará cargar su configuración mediante TFTP.	Deshabilitado	Esto se utiliza con poca frecuencia; deshabilítelo si no se encuentra en uso.
Enrutamiento IP de origen	Característica IP que permite que los paquetes especifiquen sus propias rutas.	Habilitado	Esta característica, muy poco usada, puede ser beneficiosa en ataques; deshabilítela.
ARP proxy	El router actuará como un proxy para una resolución de dirección de capa 2.	Habilitado	Deshabilite este servicio salvo que el router esté funcionando como puente LAN.
Broadcast dirigido IP	Los paquetes pueden identificar un LAN objetivo para broadcasts.	>=11.3: habilitado	El broadcast dirigido se puede utilizar para ataques; deshabilítelo.
Comportamiento del enrutamiento sin clase	El router enviará paquetes que no tengan una ruta concreta.	Habilitado	Ciertos ataques se pueden beneficiar de éste; deshabilítelo salvo que su red lo solicite.
Notificaciones de IP inalcanzables	El router notificará a los emisores, de manera explícita, acerca de direcciones IP incorrectas.	Habilitado	Puede ayudar con la asignación de red; deshabilitado en interfaces para redes que no son confiables.
Respuesta de la máscara IP	El router enviará una máscara de dirección IP de la interfaz en respuesta a una solicitud de máscara del protocolo de mensajes de control de Internet (ICMP, Internet Control Messaging Protocol).	Deshabilitado	Puede ayudar con la asignación de dirección IP; deshabilítela explícitamente en interfaces de redes que no son confiables.
Redireccionamientos IP	El router enviará un mensaje de redirección ICMP en respuesta a ciertos paquetes IP ruteados.	Habilitado	Puede ayudar con la asignación de red; deshabilítelo en interfaces de redes que no son confiables.
Servicio NTP	El router puede actuar como un servidor de tiempo para otros dispositivos y hosts.	Habilitado (siempre que NTP esté configurado)	Si no está en uso, deshabilítelo de manera explícita; de lo contrario, restrinja el acceso.
Protocolo de administración de red simple	Los routers pueden admitir consulta y configuración remota del protocolo de administración de red simple (SNMP, Simple Network Management Protocol).	Habilitado	Si no está en uso, deshabilítelo de manera explícita; de lo contrario, restrinja el acceso.
Servicio de nombres de dominio	Los routers pueden realizar la resolución de nombre servicio de nombre de dominio (DNS, Domain Name Service).	Habilitado (broadcast)	Configure la dirección del servidor DNS de manera explícita o deshabilite DNS.

Servicios de administración vulnerables en el router

- SNMP
  - Protocolo estándar de monitoreo y la administración remota.
  - Las versiones anteriores a la 3, transportan texto sin cifrar.
  - Utilice versión 3.
- NTP
  - Lo utilizan para mantener relojes con la hora del día exacta
  - Normalmente hay una jerarquía NTP, un temporizador maestro que da la hora al resto. Si no hay jerarquía. Mejor desactivar.
- DNS
  - No ofrece autenticación
  - De manera predeterminada se envían a 255.255.255.255
  - Utilice explícitamente la dirección del servidor "*ip domain-server 192.168.1.254*"
  - De lo contrario, "*no ip domain-lookup*"

Vulnerabilidades de SNMP, NTP y DNS

Protocolo	Vulnerabilidad
SNMP	Las versiones 1 y 2 pasan información de administración y cadenas de comunidad (contraseñas) en texto sin cifrar
NTP	El NTP deja los puertos de escucha abiertos y vulnerables
DNS	Puede ayudar a los atacantes a conectar las direcciones IP a nombres de dominio

Configurar la protección de protocolos de enrutamiento

- RIPv2
  - Paso 1. Evitar propagación de actualizaciones de enrutamiento.

```
Router(config)#router rip
Router(config-router)#passive-interface default
Router(config-router)#no passive-interface s0/0/0
```

  - Paso 2. Evitar recepción de actualizaciones sin autorización.

```
Router(config)#key chain RIP_KEY
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string “clave”

Router(config)#int s0/0/0
Router(config-if)#ip rip authentication mode md5
Router(config-if)#ip rip authentication key-chain RIP_KEY
```

  - Paso 3. Verificar el enrutamiento

```
Router(config)#sh ip route rip
```

Configurar la protección de protocolos de enrutamiento

- EIGRP
  - **Paso 1.** Evitar propagación de actualizaciones de enrutamiento.

```
Router(config)#router eigrp 1
Router(config-router)#passive-interface default
Router(config-router)#no passive-interface s0/0/0
```

  - **Paso 2.** Evitar recepción de actualizaciones sin autorización.

```
Router(config)#key chain EIGRP_KEY
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string “clave”

Router(config)#int s0/0/0
Router(config-if)#ip authentication mode eigrp 1 md5
Router(config-if)#ip authentication key-chain eigrp 1 EIGRP_KEY
```

  - **Paso 3.** Verificar el enrutamiento

```
Router(config)#sh ip route eigrp
```

Configurar la protección de protocolos de enrutamiento

- OSPF
  - Paso 1. Evitar propagación de actualizaciones de enrutamiento.

```
Router(config)#router ospf 10
Router(config-router)#passive-interface default
Router(config-router)#no passive-interface s0/0/0
```

  - Paso 2. Evitar recepción de actualizaciones sin autorización.

```
Router(config)#int s0/0/0
Router(config-if)#ip ospf message-digest-key 1 md5 “clave”
Router(config-if)#ip ospf authentication message-digest

Router(config)#router ospf 10
Router(config-router)#area 0 authentication message-digest
```

  - Paso 3. Verificar el enrutamiento

```
Router(config)#sh ip route ospf
```

Bloqueo del router con AutoSecure de Cisco

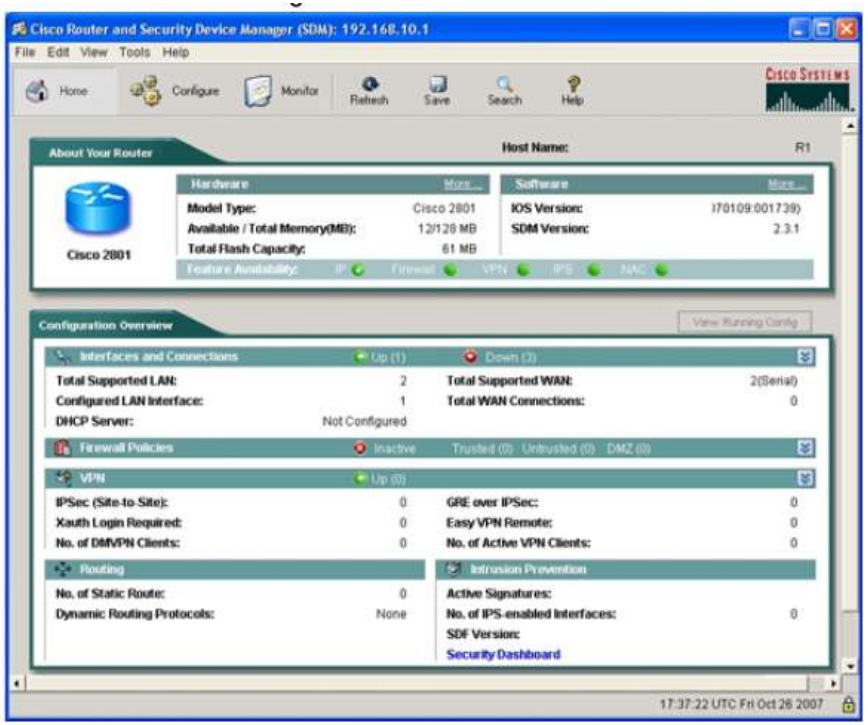
- Utiliza un único comando para desactivar procesos y servicios no esenciales del sistema y elimina amenazas de seguridad potenciales.
- Tiene 2 modos:
  - Modo interactivo: Le indica opciones para activar y desactivar servicios y otras características de seguridad. Es el modo predeterminado.
  - Modo no interactivo: Ejecuta automáticamente el comando auto secure con la configuración predeterminada recomendada de Cisco. Este modo se activa con la opción del comando *no-interact*.

```
R1#auto secure
Is this router connected to internet? [no]:y
Enter the number of interfaces facing internet [1]:1
Enter the interface name that is facing internet:Serial0/1/0
Securing Management plane services..

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
(output omitted)
```

SDM (Security Device Manager)

- Herramienta Web de administración.
- Proporciona asistentes inteligentes de configuración
- Admite una amplia gama de versiones de IOS de Cisco.
- Esta preinstalado en los nuevos routers.
- Los archivos se pueden instalar en el router o un el PC o en ambos.
- En el PC ahorra la memoria del router

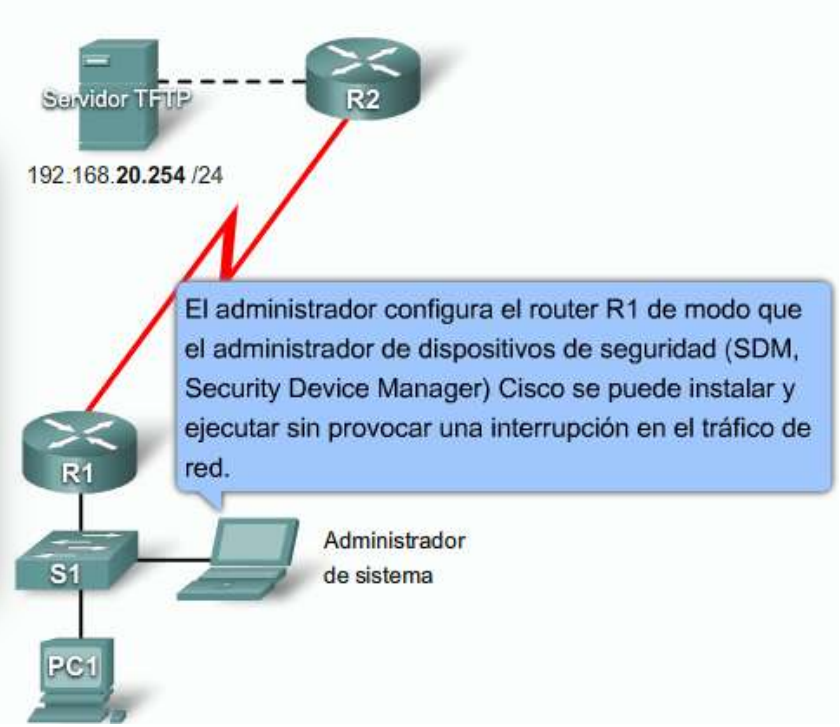


- Herramienta para usuarios más avanzados:
  - ACLs
  - El editor de cryto maps para VPNs
  - Firewall
  - IPS
  - Vista preliminar de la CLI de Cisco

Configuración del router para usar SDM

- Paso 1. Obtenga acceso a la interfaz CLI de Cisco del router mediante la conexión Telnet o de consola
- Paso 2. Active los servidores HTTP y HTTPS en el router
- Paso 3. Cree una cuenta de usuario configurada con nivel de privilegio 15 (active los privilegios)
- Paso 4. Configure SSH y Telnet para la conexión local y nivel de privilegio 15

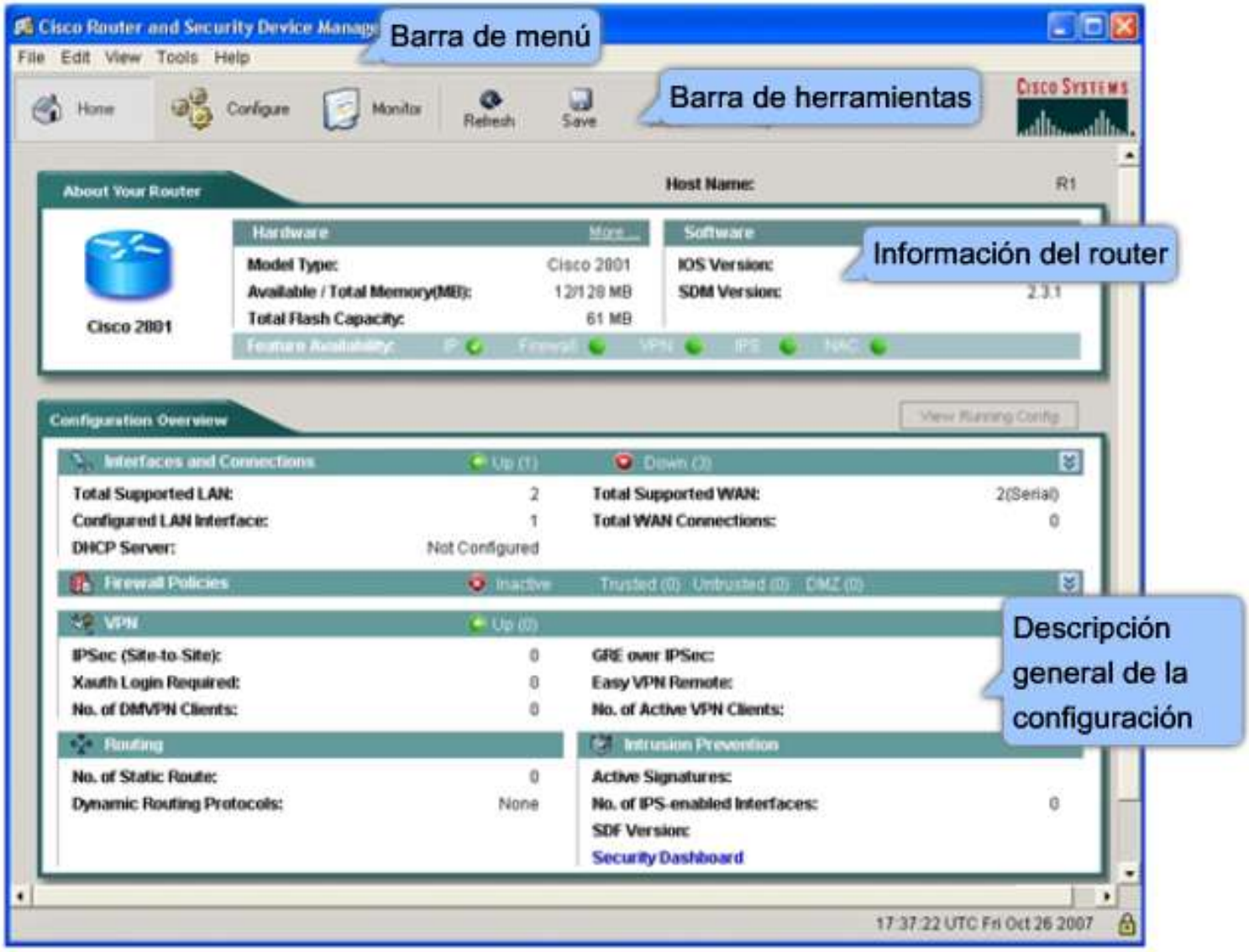
```
R1# configure terminal
Enter configuration commands, one per line. End with CNT
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ip http authentication local
R1(config)# username Student privilege 15 secret cisco
R1(config)# line vty 0 4
R1(config-line)# privilege level 15
R1(config-line)# login local
R1(config-line)# transport input telnet ssh
R1(config-line)# exit
```



- Luego inicie el SDM desde el navegador con la dirección https://198.162.20.1

Página de inicio del SDM

Descripción general de la página de inicio del SDM Cisco



Sistemas de Archivos

- Los dispositivos con el IOS de Cisco cuentan con una característica denominada Sistema de archivos integrados (IFS).
- Permite crear, navegar y manipular directorios en un dispositivo Cisco
- El comando "*show file system*" roporciona información útil, como la cantidad de memoria disponible y libre, el tipo de sistema de archivos y sus permisos. Sólo lectura (ro), sólo escritura (wo) y lectura y escritura (rw).

```
R1# show file system
File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     rw   archive:
           -           -    opaque     rw   system:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
      196600      194247     nvram     rw   nvram:
*   31932416      462848      disk     rw   flash:#
           -           -    opaque     wo   syslog:
           -           -    opaque     rw   xmodem:
           -           -    opaque     rw   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   pram:
           -           -   network     rw   ftp:
           -           -   network     rw   http:
           -           -   network     rw   scp:
           -           -   network     rw   https:
           -           -    opaque     ro   cns:

R1#
```

Sistemas de Archivos

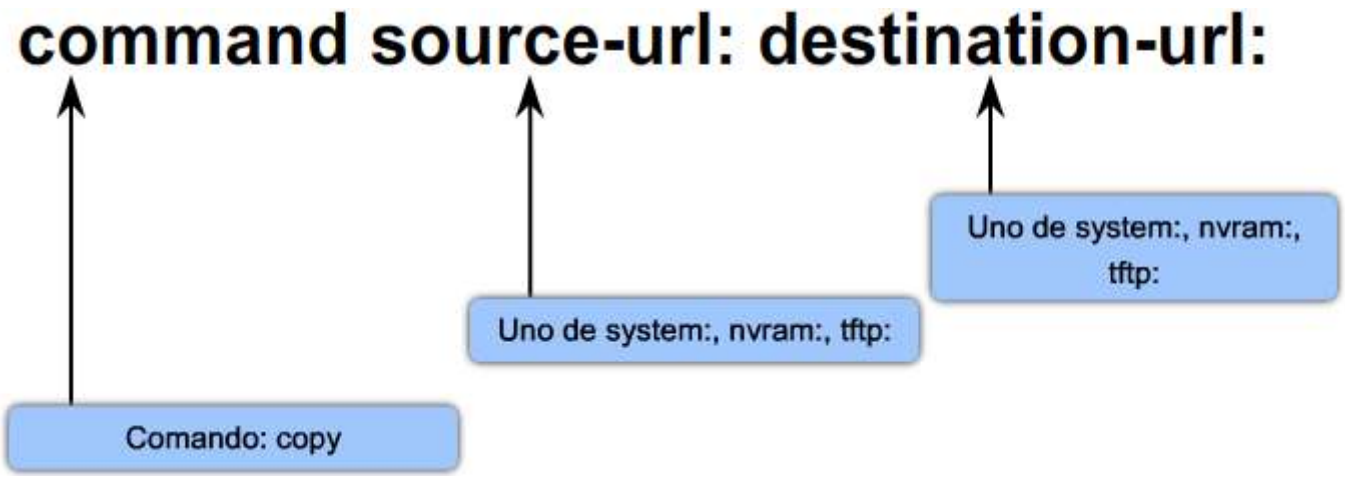
- Asegúrese de mantener copias de seguridad de los archivos de configuración de inicio y del IOS del dispositivo.

```
R2# copy running-config startup-config
R2#copy system:running-config nvram:startup-config
```

```
R2# copy running-config tftp:
R2# copy system:running-config tftp:
```

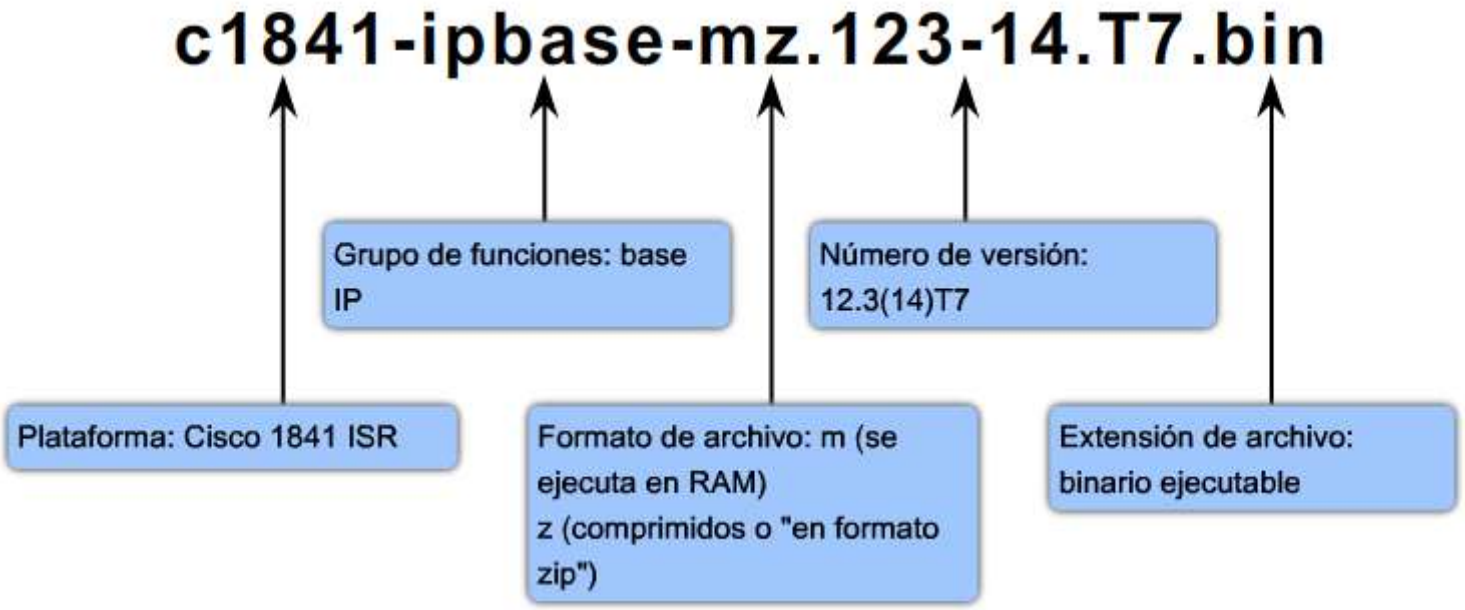
```
R2# copy tftp: running-config
R2# copy tftp: system:running-config
```

```
R2# copy tftp: startup-config
R2# copy tftp: nvram:startup-config
```



Normas de denominación de archivos del IOS de Cisco

- Otros posibles conjuntos de características son:
  - **i**: designa el conjunto de características IP
  - **j** : designa el conjunto de características empresariales (todos los protocolos)s: designa un conjunto de características PLUS (más colas, manipulación o traducciones)
  - **56i**: designa la encriptación DES de IPsec de 56 bits
  - **3**: designa el firewall/IDS
  - **k2**: designa la encriptación 3DES de IPsec (168 bits)

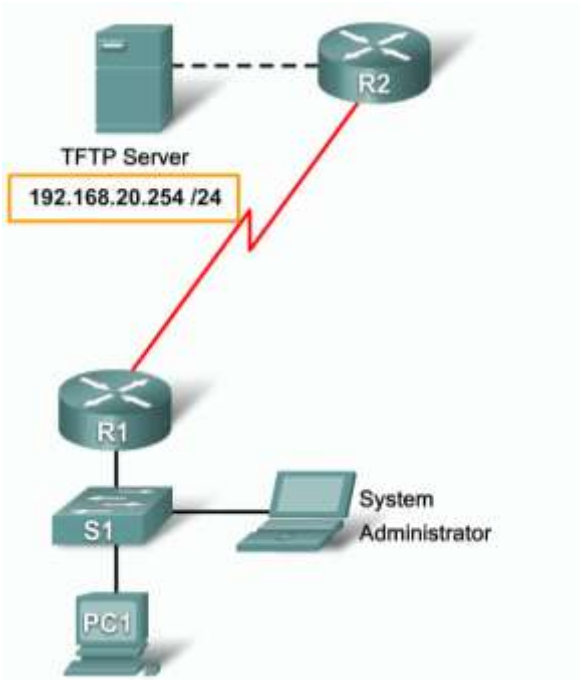


Hacer copia de seguridad del IOS del dispositivo

- Paso 1. Haga ping al servidor TFTP
- Paso 2. Verifique el tamaño del IOS y si el servidor tiene el espacio.
- Paso 3. Copie el archivo de la flash del router al servidor tftp

```
R1#show flash
System flash directory:
File  Length   Name/status
  1   13832032 c1841-ipbase-mz.123-14.T7.bin
[13832032 bytes used, 18682016 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)
```

```
R1#copy flash: tftp:
Source filename []? c1841-ipbase-mz.123-14.T7.bin
Address or name of remote host []? 192.168.20.254
Destination filename [c1841-ipbase-mz.123-14.T7.bin]? <CR>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!<output omitted>
13832032 bytes copied in 113.061 secs (122341 bytes/sec)
R1#
```

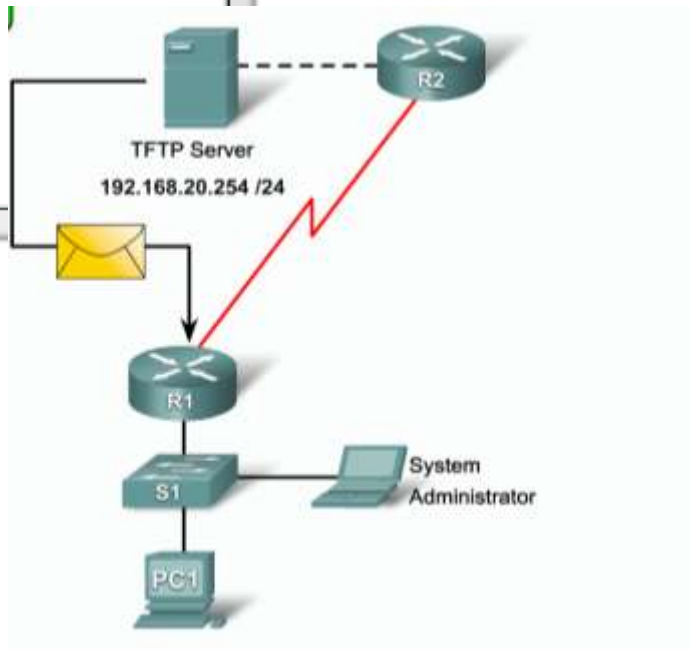


Actualización de imagen de IOS del dispositivo

- Cada signo de exclamación (!) significa que un segmento del UDP se ha transferido con éxito.

```
R1#copy tftp: flash:
Address or name of remote host [192.168.20.254]? <CR>
Source filename []? c1841-ipbase-mz.123-14.T7.bin
Destination filename [c1841-ipbase-mz.123-14.T7.bin]?<CR>
Accessing tftp://192.168.20.254/c1841-ipbase-mz.123-14.T7.bin…

Erase flash: before copying? [confirm] <CR>
Erasing the flash filesystem will remove all files! Continue? [confirm] <CR>
Erasing device… eeeeeee (output omitted) erased
Erase of flash: complete
Loading c1841-ipbase-mz.123-14.T7.bin from 192.168.20.254 (via Serial 0/0/0):
!!!!!! (output omitted)
```



- Si no hay espacio suficiente el dispositivo le pedirá borrar la flash para liberar espacio.

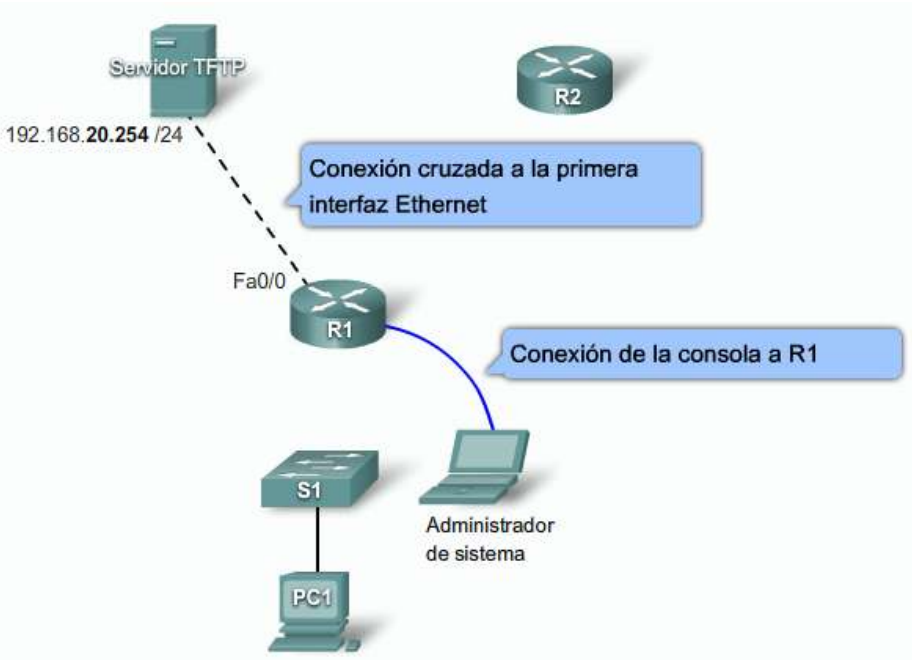
Restauración de imagen del software IOS desde ROMmon

- Paso 1. Conecte los dispositivos
  - Conecte la PC del administrador del sistema al puerto de consola del router afectado.
  - Conecte el servidor TFTP al primer puerto Ethernet del router. En la figura, R1 es un router Cisco 1841; por lo tanto, el puerto es Fa0/0. Active el servidor TFTP y configúrelo con la dirección IP estática 192.168.1.1/24.
- Paso 2. Inicie el router y defina las variables de ROMmon.
- Paso 3. Introduzca el comando *tftpdnld* en el indicador de ROMmon.

```
rommon1> IP_ADDRESS=192.168.1.2
rommon2> IP_SUBNET_MASK=255.255.255.0
rommon3> DEFAULT_GATEWAY=192.168.1.1
rommon4> TFTP_SERVER=192.168.1.1
rommon5> TFTP_FILE=c1841-ipbase-mz.123-14.T7.bin
rommon7> tftpdnld

          IP_ADDRESS: 192.168.1.2
      IP_SUBNET_MASK: 255.255.255.0
     DEFAULT_GATEWAY: 192.168.1.1
         TFTP_SERVER: 192.168.1.1
           TFTP_FILE: c1841-ipbase-mz.123-14.T7.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:  [n]:
Do you wish to continue? y/n:  [n]: y <CR>

Receiving c1841-ipbase-mz.123-14.T7.bin from 192.168.1.1
!!!!!!!!!(output omitted)!!!!!!!
File reception completed.
Copying file c1841-ipbase-mz.123-14.T7.bin to flash.
Erasing flash at 0x607c0000
program flash location 0x605a0000
```



Restauración de imagen del software IOS con Xmodem

1

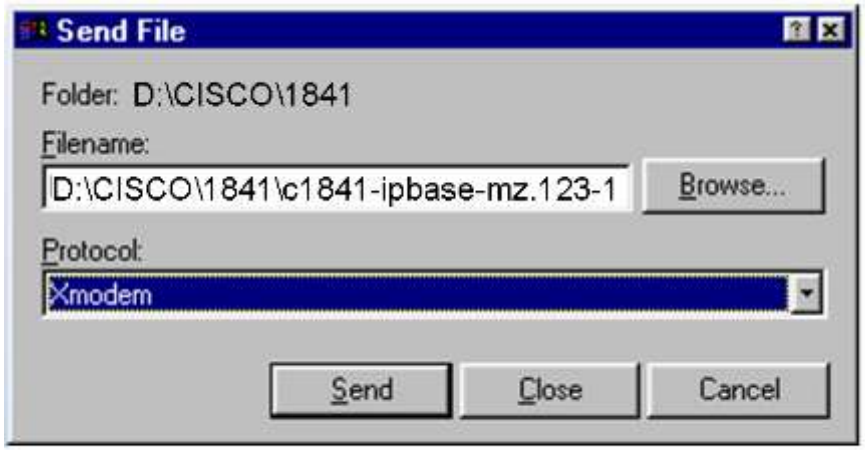
```
rommon1>xmodem -c c1841-ipbase-mz.123-14.T7.bin
Do not start the sending program yet...
device does not contain a valid magic number
dir: cannot open device "flash:"

WARNING: All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n  [n]:y <CR>

Ready to receive file c1841-ipbase-mz.123-14.T7.bin
```

2

3



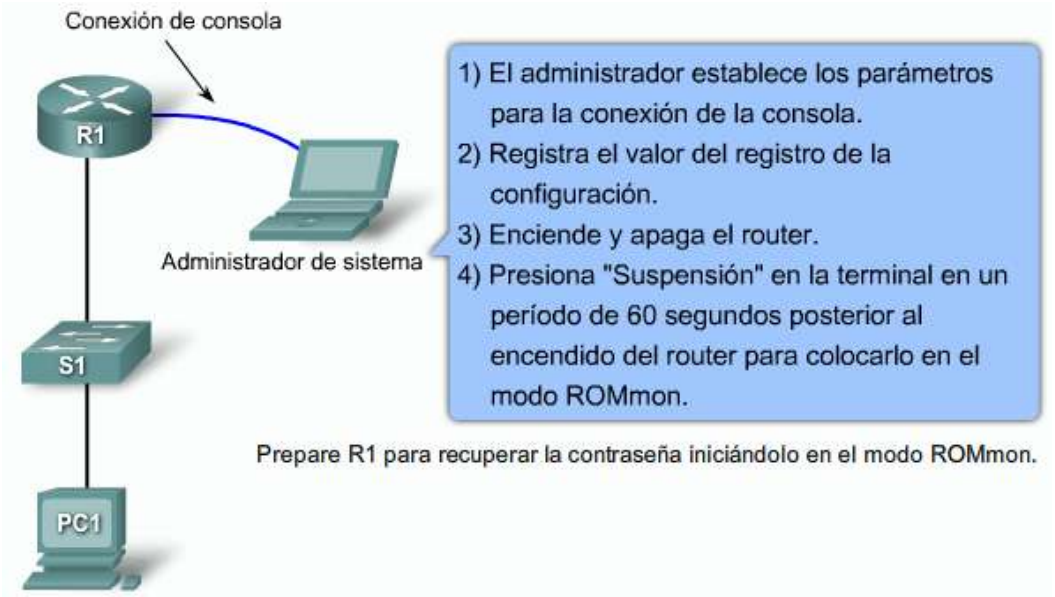
Haga clic en el botón Send para ver el "archivo Xmodem enviado por cisco"

Comandos para la resolución de problemas

- La figura resume las características de los comandos show y debug.

	show	debug
Característica de procesamiento	Estática	Dinámica
Proceso de carga	Baja sobrecarga	Alta sobrecarga
Uso principal	Recopilar hechos	Observar los procesos

Recuperación de contraseñas



1) El administrador establece los parámetros para la conexión de la consola.
2) Registra el valor del registro de la configuración.
3) Enciende y apaga el router.
4) Presiona "Suspensión" en la terminal en un período de 60 segundos posterior al encendido del router para colocarlo en el modo ROMmon.

Prepare R1 para recuperar la contraseña iniciándolo en el modo ROMmon.

5) Cambie la configuración config register.
6) Reinicie. Ignore la configuración guardada.
7) Salte el procedimiento de configuración inicial.
8) Ingrese **`enable`** para obtener el indicador de configuración.

9) Copie la configuración de inicio de NVRAM a la configuración en ejecución en RAM.
10) Vea las contraseñas mediante el comando **`show running-config`** .

11) Habilite el modo de configuración global.
12) Configure una nueva contraseña secreta.
13) Ejecute el comando `no shutdown` para cada interfaz operacional en el router.
14) Configure la ubicación del registro de configuración.
15) Salga del modo de configuración.
16) Confirme los cambios.

Resumen

- Los ataques de seguridad a la red empresarial incluyen:
  - Ataques No Estructurados
  - Ataques Estructurados
  - Ataques Externos
  - Ataques Internos
- Métodos para mitigar los ataques:
  - Hardening de dispositivos
  - Uso de software antivirus
  - Firewalls personales
  - Descargar actualizaciones de seguridad

Resumen

- La seguridad básica del router involucra:
  - Seguridad física
  - Actualizar y hacer copia de seguridad al IOS
  - Hacer copia de seguridad a los archivos de configuración
  - Configuración de contraseñas
  - Llevar registro de la actividad del router.
- Deshabilitar interfaces y servicios no usados para minimizar los ataques de los intrusos.
- Cisco SDM
  - Una herramienta de administración web para configurar la seguridad de los routers Cisco.
- Cisco IOS Integrated File System (IFS)
  - Permite la creación, navegación y manipulación de directorios en un dispositivo Cisco.