

## Capítulo 11: Es una red



## Introducción a redes

**Ing. Aníbal Coto Cortés**

Cisco | Networking Academy®  
Mind Wide Open™



# Capítulo 11

11.1 Crear y crecer

11.2 Cómo mantener la seguridad de la red

11.3 Rendimiento básico de la red

11.4 Administración de los archivos de configuración de IOS

11.5 Servicios de enrutamiento integrados

11.6 Resumen



# Capítulo 11: Objetivos

- Identificar los dispositivos y protocolos utilizados en una red pequeña.
- Explicar la forma en que una red pequeña sirve como base de redes más grandes.
- Explicar la necesidad de contar con medidas de seguridad básicas en los dispositivos de red.
- Identificar las vulnerabilidades de seguridad y las técnicas de mitigación generales.



# Capítulo 11: Objetivos (continuación)

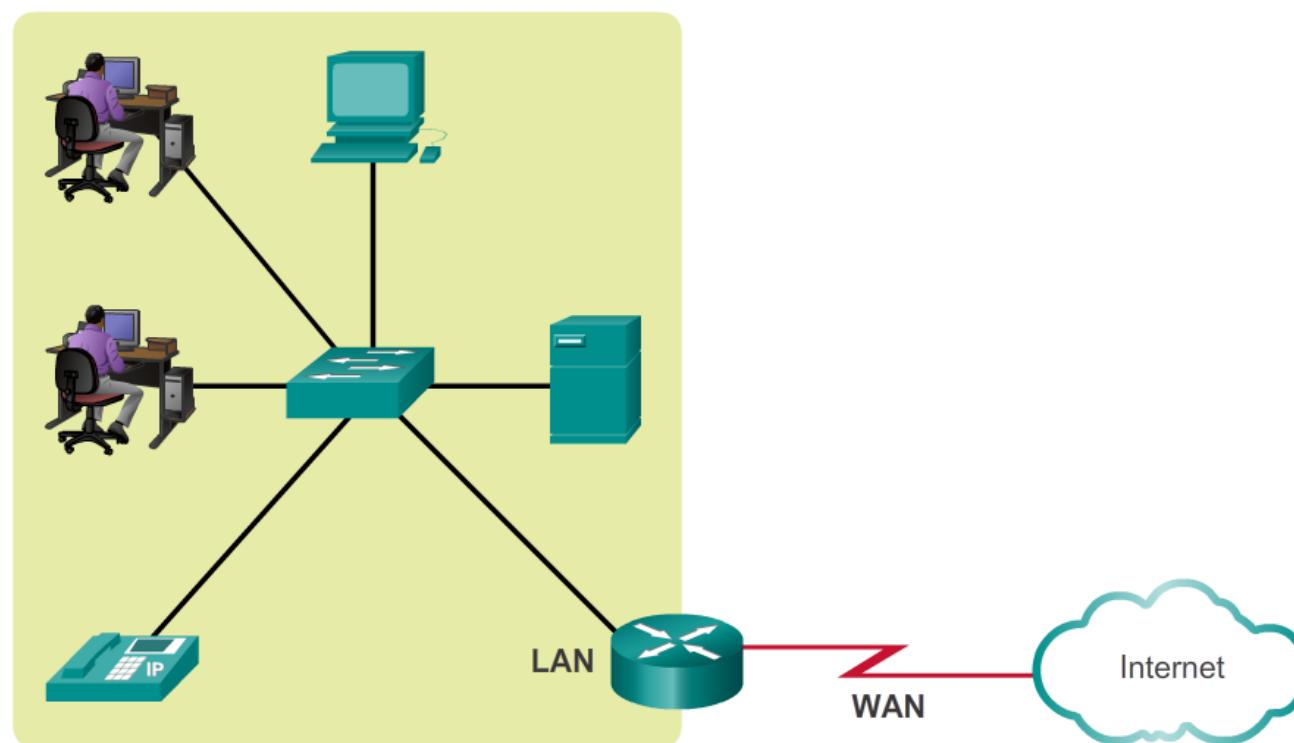
- Utilizar el resultado de los comandos ping y tracert para establecer el rendimiento relativo de la red.
- Utilizar comandos show básicos para verificar la configuración y el estado de una interfaz de dispositivo.
- Explicar los sistemas de archivos de los routers y los switches.
- Aplicar los comandos para realizar copias de seguridad de un archivo de configuración de IOS y restaurarlo.



Dispositivos en redes pequeñas

# Topologías de redes pequeñas

- Topología de red pequeña típica





## Dispositivos en redes pequeñas

# Selección de dispositivos para redes pequeñas

- Factores que se deben tener en cuenta al seleccionar dispositivos intermedios



Costo



Puertos



Velocidad



Expansibilidad/Modularidad



Facilidad de administración



## Dispositivos en redes pequeñas

# Direccionamiento IP para redes pequeñas

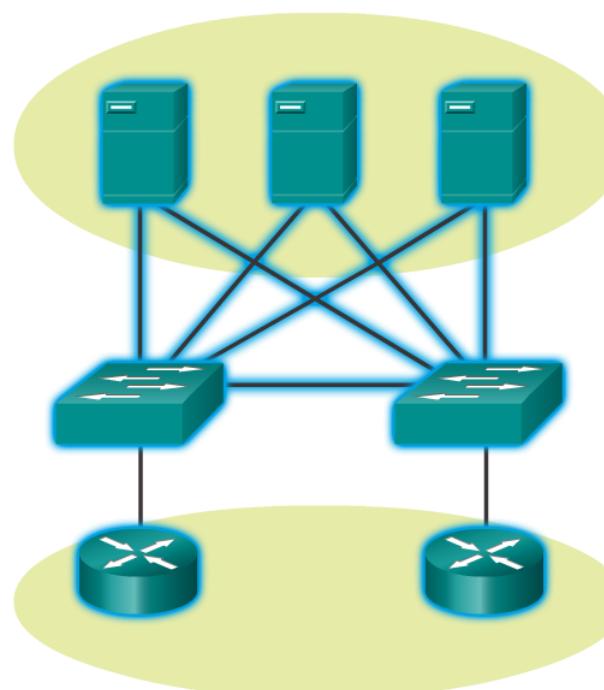
- Se debe planificar, registrar y mantener un esquema de direccionamiento IP basado en los tipos de dispositivos que reciben la dirección.
- Los siguientes son ejemplos de dispositivos que forman parte del diseño de IP:
  - Dispositivos finales para usuarios
  - Servidores y periféricos
  - Hosts a los que se accede desde Internet
  - Dispositivos intermediarios
- Los esquemas de IP planificados ayudan al administrador a realizar lo siguiente:
  - Realizar un seguimiento de los dispositivos y resolver problemas.
  - Controlar el acceso a los recursos.

## Dispositivos en redes pequeñas

# Redundancia en redes pequeñas

- La redundancia ayuda a eliminar puntos de error únicos.
- Mejora la confiabilidad de la red.

Redundancia a una granja de servidores





## Dispositivos en redes pequeñas

# Consideraciones de diseño para redes pequeñas

- En el diseño de red, se deben incluir los siguientes aspectos:

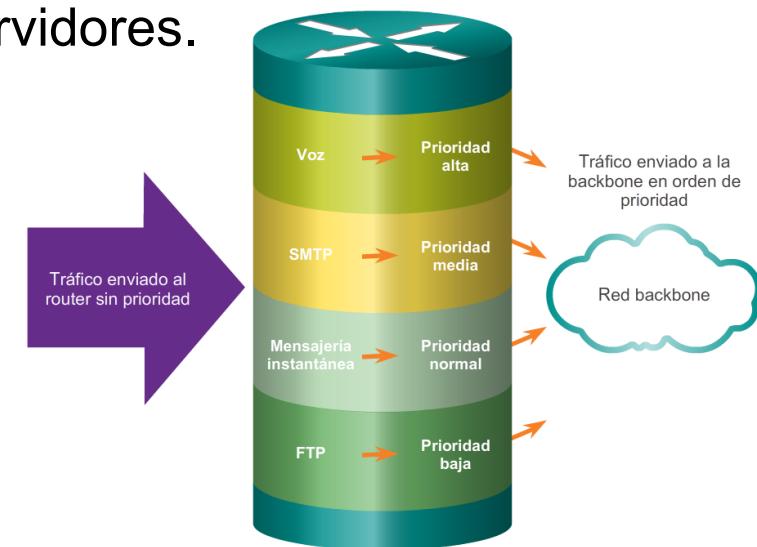
Aportar seguridad a los servidores de archivos y de correo en una ubicación centralizada.

Proteger la ubicación con medidas de seguridad física y lógica.

Crear redundancia en la granja de servidores.

Configurar rutas redundantes a los servidores.

Establecimiento de prioridades de tráfico





Protocolos en redes pequeñas

# Aplicaciones comunes en redes pequeñas

- **Aplicaciones que reconocen a la red:** programas de software utilizados para comunicarse a través de la red.
- **Servicios de la capa de aplicación:** programas que interactúan con la red y preparan los datos para su transferencia.

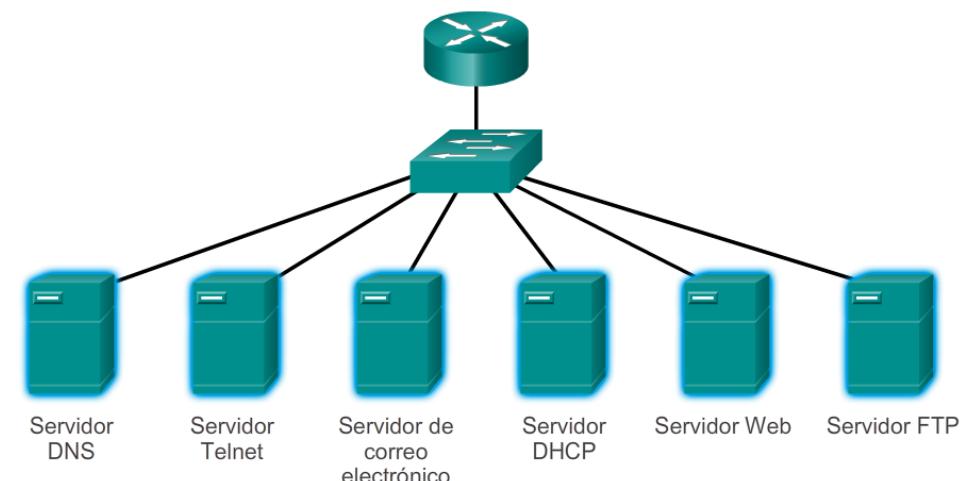


## Protocolos en redes pequeñas

# Protocolos comunes en redes pequeñas

- Los protocolos de redes definen lo siguiente:
  - Procesos en cualquier extremo de una sesión de comunicación.
  - Tipos de mensajes.
  - Sintaxis de los mensajes.
  - Significado de los campos informativos.
  - Cómo se envían los mensajes y la respuesta esperada.
  - Interacción con la capa inferior siguiente.

Servicios de red





# Aplicaciones en tiempo real para redes pequeñas

- **Infraestructura:** se debe evaluar para asegurar que admitirá las aplicaciones en tiempo real propuestas.
- VoIP se implementa en organizaciones que todavía utilizan teléfonos tradicionales.
- Telefonía IP: el teléfono IP propiamente dicho realiza la conversión de voz a IP.
- Protocolos de video en tiempo real: utilizan el protocolo de transporte en tiempo real (RTP) y el protocolo de control de transporte en tiempo real (RTCP).



Crecimiento hacia redes más grandes

## Escalamiento de redes pequeñas

Consideraciones importantes al crecer hacia una red más grande:

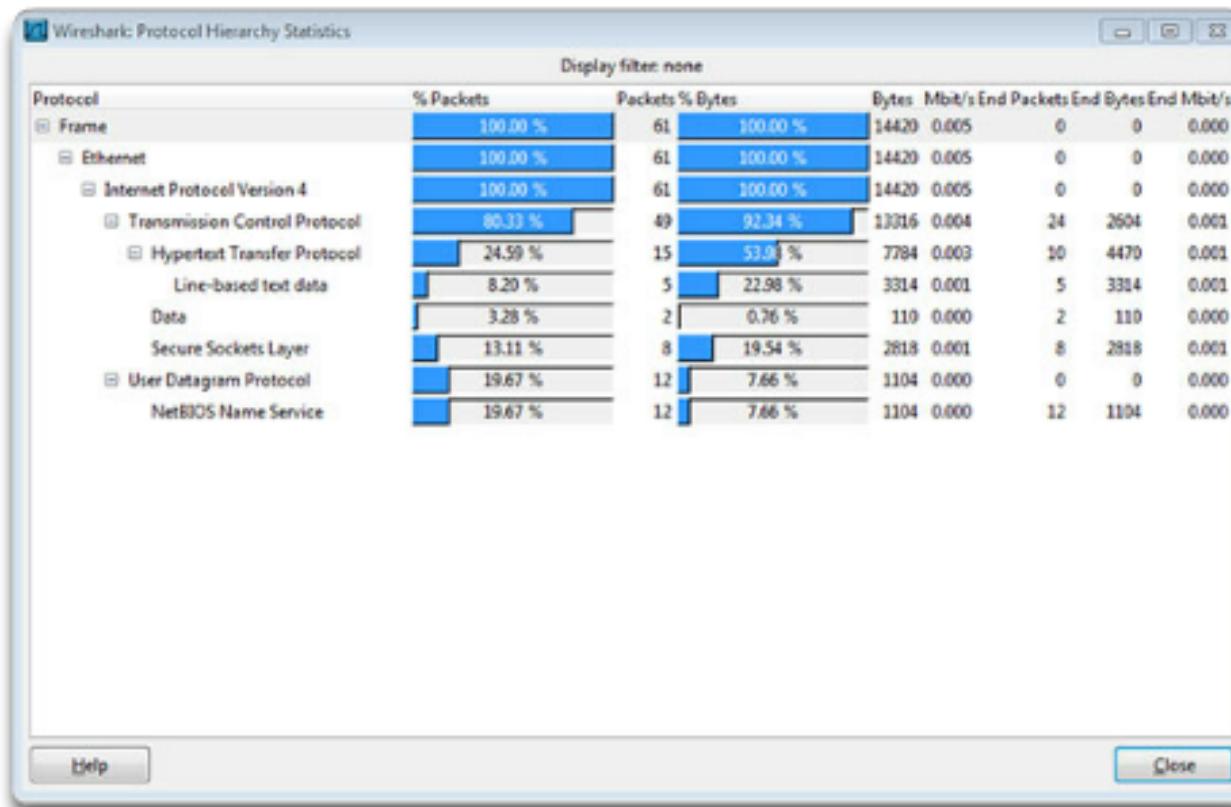
- Documentación: topología física y lógica.
- Inventario de dispositivos: lista de dispositivos que utilizan o conforman la red.
- Presupuesto: presupuesto de TI detallado, incluido el presupuesto de adquisición de equipos para el año fiscal.
- Análisis de tráfico: se deben registrar los protocolos, las aplicaciones, los servicios y sus respectivos requisitos de tráfico.



Crecimiento hacia redes más grandes

## Análisis de protocolos de redes pequeñas

- La información recopilada por el análisis de protocolos se puede utilizar para tomar decisiones acerca de cómo administrar el tráfico de forma más eficiente.

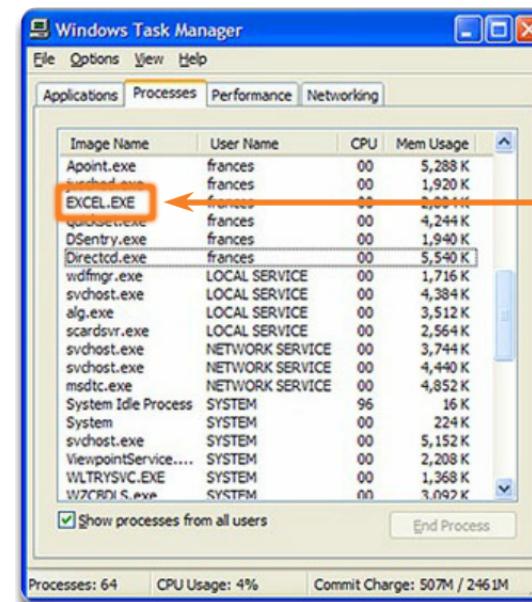




Crecimiento hacia redes más grandes

## Evolución de los requisitos de los protocolos

- El administrador de red puede obtener “instantáneas” de TI del uso de aplicaciones por parte de los empleados.
- Las instantáneas realizan un seguimiento de los requisitos de utilización y de flujo de tráfico de la red.
- Las instantáneas contribuyen a dar forma a las modificaciones de red necesarias.



Los procesos son programas de software individuales que se ejecutan simultáneamente.

Los procesos pueden ser:

1 Aplicaciones

2 Servicios

3 Operaciones del sistema

4 Un programa puede estar en ejecución varias veces en simultáneo, cada una en su propio proceso.

## Medidas de seguridad para dispositivos de red

# Amenazas a la seguridad de red

- Categorías de amenazas a la seguridad de red



Robo de información



Pérdida y manipulación de datos



Robo de identidad



Interrupción del servicio



## Medidas de seguridad para dispositivos de red

# Seguridad física

Las cuatro clases de amenazas físicas son las siguientes:

- **Amenazas de hardware:** daño físico a servidores, routers, switches, planta de cableado y estaciones de trabajo
- **Amenazas ambientales:** extremos de temperatura (demasiado calor o demasiado frío) o extremos de humedad (demasiado húmedo o demasiado seco)
- **Amenazas eléctricas:** picos de voltaje, suministro de voltaje insuficiente (apagones parciales), alimentación sin acondicionamiento (ruido) y caída total de la alimentación
- **Amenazas de mantenimiento:** manejo deficiente de componentes eléctricos clave (descarga electrostática), falta de repuestos críticos, cableado y etiquetado deficientes



## Medidas de seguridad para dispositivos de red

# Tipos de vulnerabilidades de seguridad

- Debilidades tecnológicas
- Debilidades de la configuración
- Debilidades de la política de seguridad

### Debilidades de la seguridad de red:

#### Debilidad del protocolo TCP/IP

- El protocolo de transferencia de hipertexto (HTTP), el protocolo de transferencia de archivos (FTP) y el protocolo de mensajes de control de Internet (ICMP) son inseguros por naturaleza.
- El protocolo simple de administración de red (SNMP) y el protocolo simple de transferencia de correo (SMTP) se relacionan con la estructura intrínsecamente insegura sobre la que se diseñó TCP.

#### Debilidades de los sistemas operativos

- Cada sistema operativo tiene problemas de seguridad que se deben resolver.
- UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8.
- Estos están registrados en los archivos del Computer Emergency Response Team (CERT) disponibles en <http://www.cert.org>.

#### Debilidades de los equipos de red

Existen diversos tipos de equipos de red, como routers, firewalls y switches, que tienen debilidades de seguridad que se deben reconocer y de las cuales se deben proteger a los dispositivos. Sus debilidades incluyen la protección de contraseñas, la falta de autenticación, los protocolos de enrutamiento y los agujeros de firewall.



## Vulnerabilidades y ataques de red

# Virus, gusanos y caballos de Troya

- **Virus:** tipo de software malintencionado que se asocia a otro programa para ejecutar una función no deseada específica en una estación de trabajo.
- **Caballo de Troya:** toda la aplicación se creó con el fin de que aparente ser otra cosa, cuando en realidad es una herramienta de ataque.
- **Gusanos:** programas autónomos que atacan un sistema e intentan explotar una vulnerabilidad específica del objetivo. El gusano copia su programa del host atacante al sistema atacado recientemente para volver a iniciar el ciclo.

# Vulnerabilidades y ataques de red

## Ataques de reconocimiento



Consultas a través de Internet



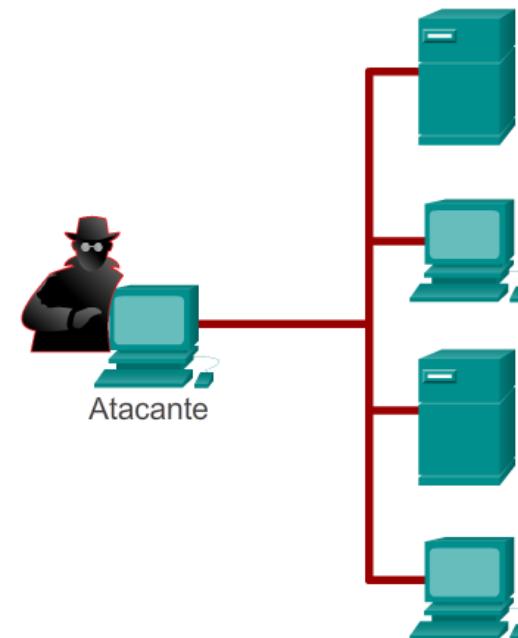
Barridos de ping



Escaneos de puertos



Programas detectores de paquetes





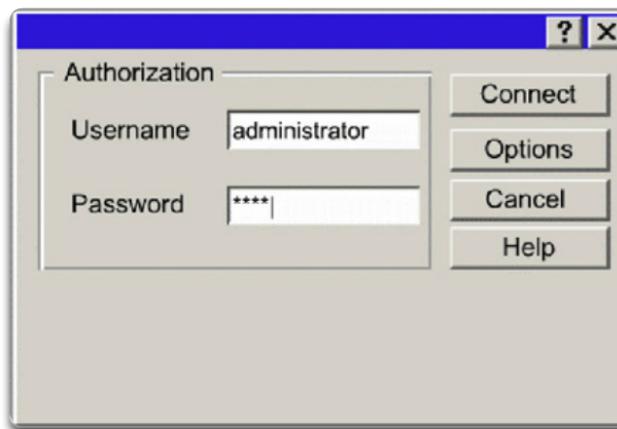
# Vulnerabilidades y ataques de red

## Ataques de acceso

## Ataque a la contraseña

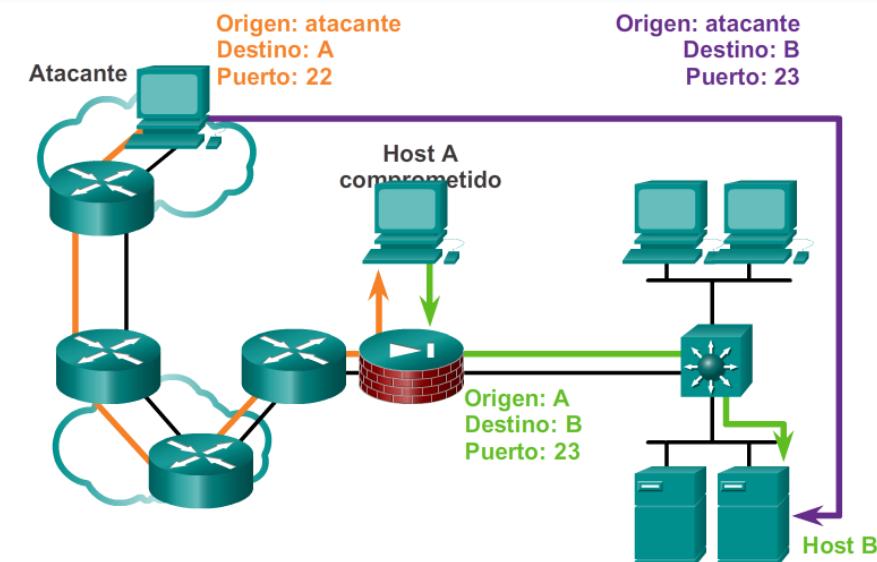
Los atacantes pueden implementar ataques a contraseñas mediante diversos métodos:

- Ataques por fuerza bruta
  - Programas de caballos de Troya
  - Programas detectores de paquetes



## Redirección de puertos

La redirección de puertos es un tipo de ataque de explotación de confianza que utiliza un host comprometido para pasar tráfico que de otra manera se descartaría a través un firewall. Se mitiga principalmente con el uso de modelos de confianza adecuados. Los softwares antivirus y los IDS basados en host pueden ayudar a detectar si un atacante instala utilidades de redirección de

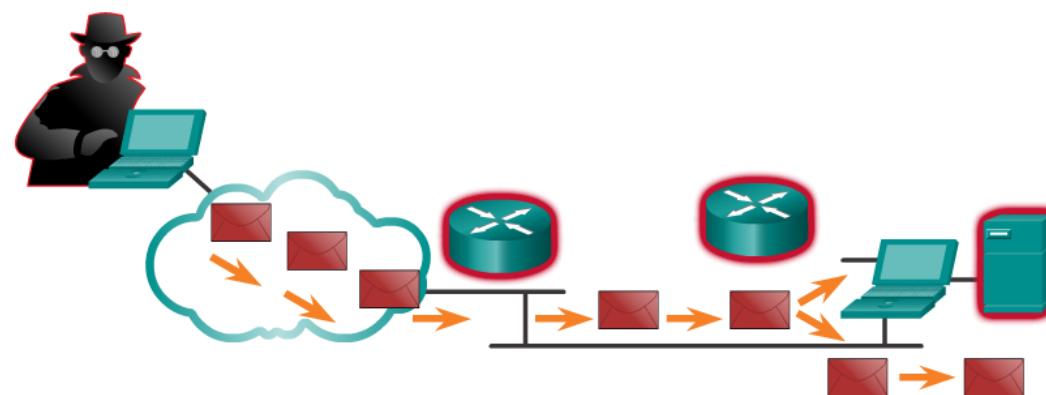


## Vulnerabilidades y ataques de red

# Ataques por denegación de servicio (DoS)

### Ataque de DoS

Sobrecargas de recursos	Datos mal formados
Espacio en disco, ancho de banda, búferes	Paquetes de tamaños excesivos como el ping de la muerte
Saturación de ping como el smurf	Paquete superpuesto como el winuke
Tormentas de paquetes como las bombas UDP y fraggle	Datos no gestionados como el teardrop



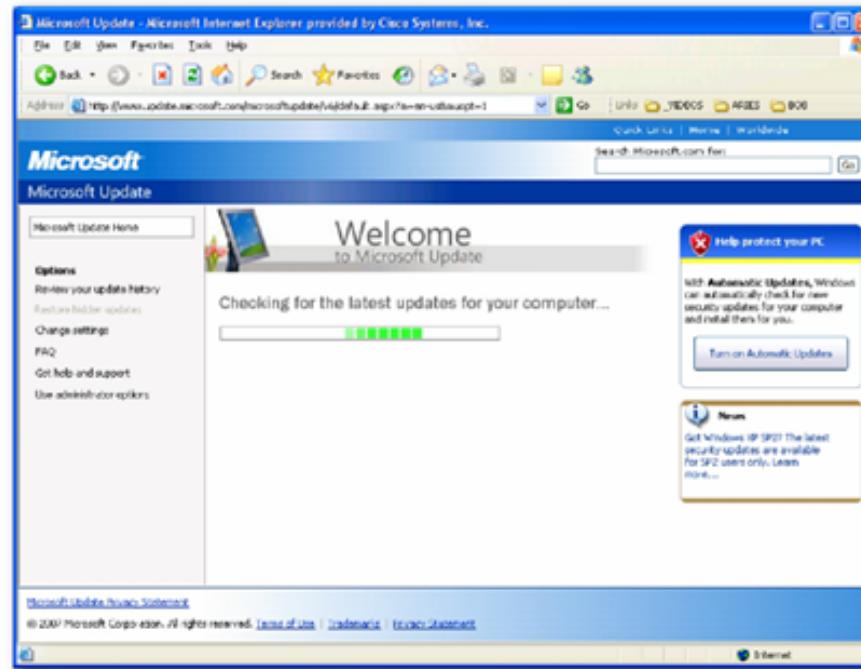
Los ataques de DoS evitan que el personal autorizado use un servicio mediante la utilización de los recursos del sistema.



## Mitigación de ataques de red

# Copias de seguridad, actualizaciones y parches

- Mantenerse al día con las versiones más recientes del software antivirus.
- Instalar parches de seguridad actualizados.





## Mitigación de ataques de red

# Autenticación, autorización y contabilidad

Autenticación, autorización y contabilidad (AAA o “triple A”)

- **Autenticación:** los usuarios y administradores deben probar su identidad. La autenticación se puede establecer utilizando combinaciones de nombre de usuario y contraseña, preguntas de desafío y respuesta, tarjetas token y otros métodos.
- **Autorización:** recursos a los que puede acceder el usuario y operaciones que tiene permitido realizar.
- **Contabilidad:** registra los recursos a los que accedió el usuario, la cantidad de tiempo que accedió al recurso y todos los cambios realizados.



## Mitigación de ataques de red

# Firewalls

Los firewalls residen entre dos o más redes. Controlan el tráfico y contribuyen a evitar el acceso no autorizado.

Los métodos utilizados son los siguientes:

- Filtrado de paquetes
- Filtrado de aplicaciones
- Filtrado de URL
- Inspección de paquetes con estado (SPI, Stateful Packet Inspection): los paquetes entrantes deben ser respuestas legítimas de los hosts internos.



Aplicaciones de seguridad de Cisco



Firewall basado en servidor



Router inalámbrico Linksys con firewall integrado



Firewall personal



## Mitigación de ataques de red

# Seguridad de las terminales

- Las terminales comunes son computadoras portátiles, computadoras de escritorio, servidores, smartphones y tablet PC.
- Los empleados deben cumplir las políticas de seguridad registradas de las compañías para proteger los dispositivos.
- En general, estas políticas incluyen el uso de software antivirus y la prevención de intrusión de hosts.





## Protección de dispositivos

# Introducción a la protección de dispositivos

- Parte de la seguridad de la red consiste en proteger los dispositivos, incluidos los dispositivos finales y los intermediarios.
- Se deben cambiar de inmediato los nombres de usuario y las contraseñas predeterminados.
- Se debe restringir el acceso a los recursos del sistema solamente a las personas que están autorizadas a utilizar dichos recursos.
- Siempre que sea posible, se deben desactivar y desinstalar todos los servicios y las aplicaciones innecesarios.
- Realizar actualizaciones con parches de seguridad a medida que estén disponibles.



# Protección de dispositivos

# Contraseñas

Contraseña no segura	Por qué no es segura
secreto	Contraseña simple de diccionario
smith	Apellido de soltera de la madre
toyota	Marca de automóvil
bob1967	Nombre y cumpleaños de un usuario
Blueleaf23	Palabras y números simples

Contraseña segura	Por qué es segura
b67n42d39c	Combina caracteres alfanuméricos
12^h u4@1p7	Combina caracteres alfanuméricos, símbolos y además incluye un espacio



## Protección de dispositivos

# Prácticas de seguridad básicas

- Encriptar las contraseñas.
- Requerir contraseñas con una longitud mínima.
- Bloquear los ataques de fuerza bruta.
- Utilizar mensajes de aviso.
- Establecer el tiempo de espera de ejecución.

```
Router(config)#service password-encryption
Router(config)#security password min-length 8
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#line vty 0 4
Router(config-vty)#exec-timeout 10
Router(config-vty)#end
Router#show running-config
-more-
!
line vty 0 4
password 7 03095A0F034F38435B49150A1819
exec-timeout 10
login
```

# Protección de dispositivos

## Habilitación de SSH



```
R1#conf t
R1(config)#ip domain-name span.com
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable... [OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#username Bob secret cisco
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
```

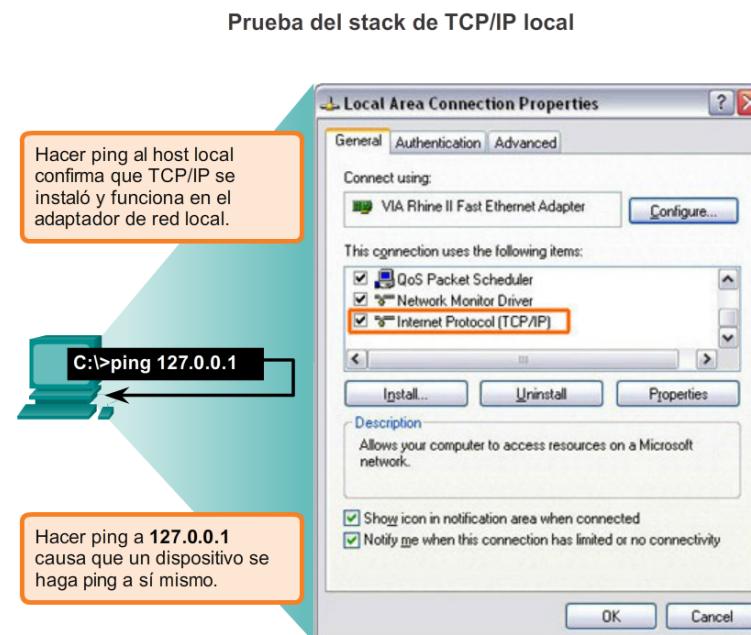
- Paso 1. Configurar el nombre de dominio IP.
- Paso 2. Generar claves secretas unidireccionales.
- Paso 3. Verificar o crear una entrada de base de datos local.
- Paso 4. Habilitar las sesiones SSH entrantes por VTY.



## Ping

# Interpretación de mensajes de ICMP

- ! : indica la recepción de un mensaje de respuesta de eco ICMP.
- . : indica que se agotó el tiempo mientras se esperaba un mensaje de respuesta de eco ICMP.
- U: se recibió un mensaje de ICMP de destino inalcanzable.





## Ping

# Uso de ping extendido

- Cisco IOS ofrece un modo “extendido” del comando ping.

R2# **ping**

Protocol [ip]:

Target IP address: **192.168.10.1**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **10.1.1.1**

Type of service [0]:



## Ping

# Línea de base de red

### Ejecute la misma prueba

8 de febrero de 2013, 08:14:43

```
C:\>ping 10.66.254.159
Pinging 10.66.254.159 with 32 bytes of data:
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128

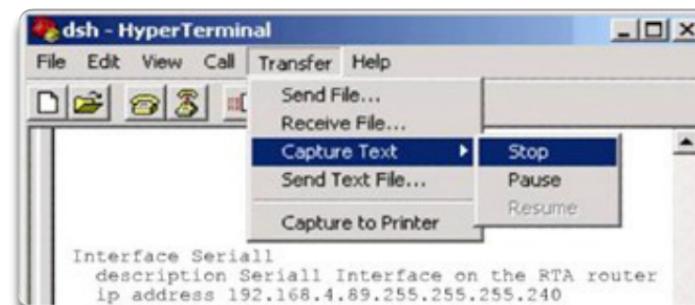
Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

17 de marzo de 2013, 14:41:06

```
C:\>ping 10.66.254.159
Pinging 10.66.254.159 with 32 bytes of data:
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

### Cómo guardar una captura de ping del router en un archivo de texto



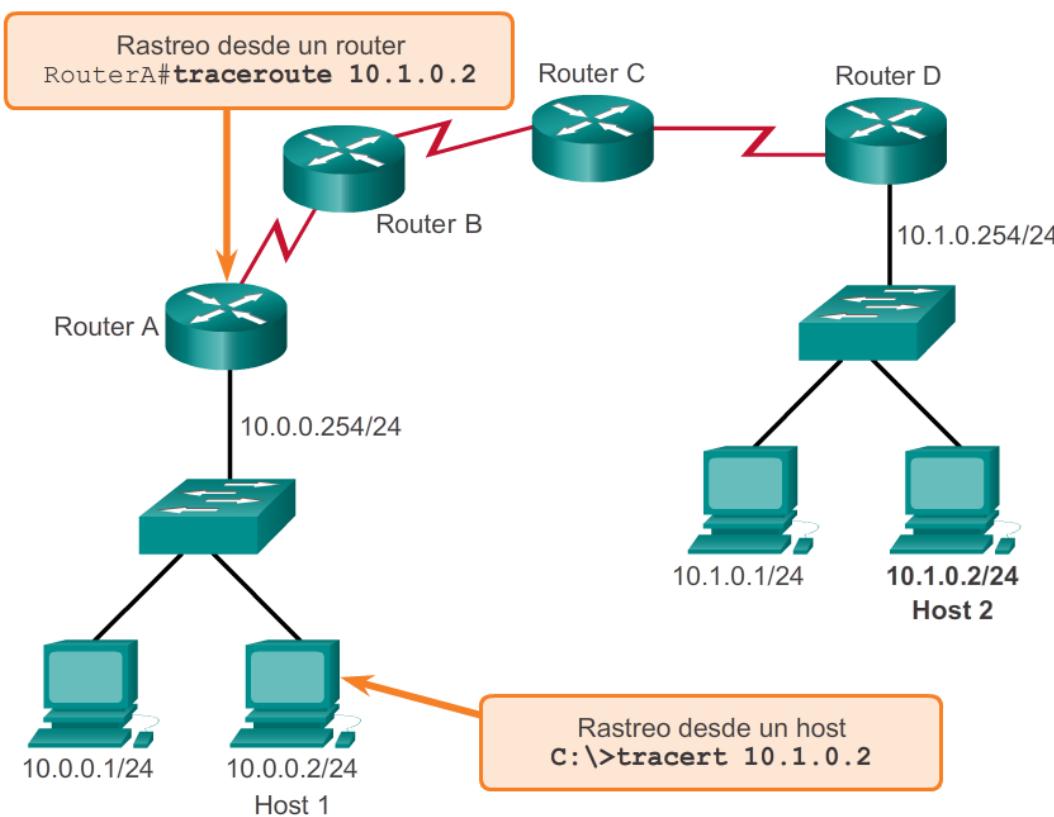
#### En la sesión de terminal:

1. Inicie el proceso de captura de texto.
2. Emite un comando **ping <dirección ip>**.
3. Detenga el proceso de captura.
4. Guarde el archivo de texto.

## Tracert

## Interpretación de mensajes de tracert

Prueba de la ruta hacia un host remoto





## Comandos show

# Repaso de comandos show comunes

- Se puede mostrar el estado de casi todos los procesos o funciones del router mediante un comando **show**.
- Los comandos show de uso frecuente son los siguientes:
  - show running-config**
  - show interfaces**
  - show arp**
  - show ip route**
  - show protocols**
  - show version**



## Comandos show

# Visualización de la configuración del router mediante show version

Versión de Cisco IOS

Bootstrap del sistema

Imagen de Cisco IOS

CPU y RAM

Cantidad y tipo de interfaces físicas

Cantidad de NVRAM

Cantidad de memoria flash

Config. register

```
Router#show version
Cisco Internetwork Operating System Software
IOS(tm)2500 Software (C2500-I>L), Version 12.0(17a), RELEASE
SOFTWARE (fc1)
Copyright (c)1986-2002 by cisco Systems, Inc.
Compiled Mon 11-Feb-02 05:55 by kellythw
image text-base:0x00001000
ROM:system Bootstrap,Version 11.0(10c),SOFTWARE
BOOTFLASH :3000 Bootstrap Software (IGS-BOOT-R),Version
11.0(10c),RELEASE SOFTWARE(fc1)
System image file is "flash:c2500-i-1.120-17a.bin"
cisco 2500 (68030 processor(revision N) With 2048K/2048K
bytes of memory.
processor bord ID 08860060,with hardware revision 00000000
Bridging software.
X.25 software,version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)

32K bytes of non-volatile Configuration memory.

8192K bytes of processor board system flash (Read ONLY)

Configuration register is 0x2102
Router#
```



## Comandos show

# Visualización de la configuración del switch mediante show version

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE2,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 04:33 by yenanh
Image text-base: 0x00003000, data-base: 0x00AA2F34

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE
SOFTWARE (fc1)

Switch uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-25.SEE2/c2960-lanbase-
mz.122-25.SEE2.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 61440K/4088K
bytes of memory.
Processor board ID FOC1107Z9ZN
Last reset from power-on
1 Virtual Ethernet interface
```



## Host y comandos de IOS

# Opciones del comando ipconfig

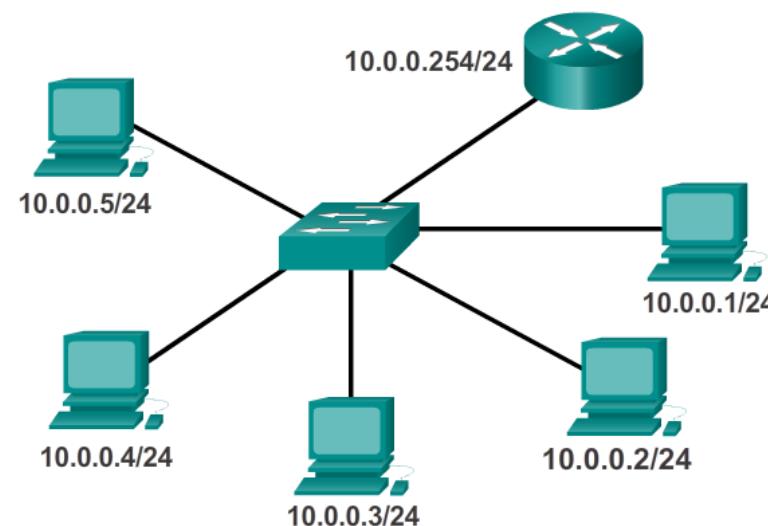
- ipconfig: muestra la dirección IP, la máscara de subred y el gateway predeterminado.
- ipconfig /all: también muestra la dirección MAC.
- Ipconfig /displaydns: muestra todas las entradas DNS en caché en un sistema Windows.

```
C:\>ipconfig /all
Ethernet adapter Network Connection:
  Connection-specific DNS Suffix: example.com
  Description . . . . . : Intel(R)
  PRO/Wireless 3945ABG Network Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-FB
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.2.3.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.2.3.254
    DHCP Server . . . . . : 10.2.3.69
    DNS Servers . . . . . : 192.168.226.120
    Lease Obtained. . . . . : Thursday, May 03,
                               2007 3:47:51 PM
    Lease Expires . . . . . : Friday, May 04,
                               2007 6:57:11 AM
C:\>
```



## Host y comandos de IOS

# Opciones del comando arp



```
C:\>arp -a
Internet Address Physical Address Type
10.0.0.2          00-08-a3-b6-ce-04 dynamic
10.0.0.3          00-0d-56-09-fb-d1 dynamic
10.0.0.4          00-12-3f-d4-6d-1b dynamic
10.0.0.254        00-10-7b-e7-fa-ef dynamic
```

Par de direcciones  
IP y MAC



## Host y comandos de IOS

# Opciones del comando show cdp neighbors

```
R3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID      Local Intrfce     Holdtme   Capability  Platform  Port ID
S3            Fas 0/0          151        S I       WS-C2950  Fas 0/6
R2            Ser 0/0/1        125        R         1841     Ser 0/0/1
```

```
R3#show cdp neighbors detail
```

```
Device ID: R2
Entry address(es):
  IP address : 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/1,  Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec
```

```
Version :
```



## Host y comandos de IOS

# Uso del comando show ip interface brief

- Se puede utilizar para verificar el estado de todas las interfaces de red en un router o un switch.

```
Router1#show ip interface brief
Interface          IP-Address      OK?   Method    Status           Protocol
FastEthernet0/0    192.168.254.254  YES   NVRAM     up                up
FastEthernet0/1/0  unassigned       YES   unset     down              down
Serial0/0/0        172.16.0.254   YES   NVRAM     up                up
Serial0/0/1        unassigned       YES   unset     administratively down  down
```

```
Router1#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Router1#traceroute 192.168.0.1
Type escape sequence to abort.
Tracing the route to 192.168.0.1
 1 172.16.0.253 8 msec 4 msec 8 msec
 2 10.0.0.254 16 msec 16 msec 8 msec
 3 192.168.0.1 16 msec * 20 msec
```



## Sistemas de archivos del router y del switch

# Sistemas de archivos del router

- Comando **show file systems**: enumera todos los sistemas de archivos disponibles en un router Cisco 1941.

```
Router# show file systems
File Systems:

  Size (b)      Free (b)     Type   Flags  Prefixes
  -           -    opaque  rw    archive:
  -           -    opaque  rw    system:
  -           -    opaque  rw    tftpvs:
  -           -    opaque  rw    null:
  -           -    network rw    tftp:
* 256487424  183234560   disk   rw    flash0: flash:#*
  -           -    disk   rw    flash1:
  262136      254779    nvram  rw    nvram:
  -           -    opaque  wo    syslog:
  -           -    opaque  rw    xmodem:
  -           -    opaque  rw    ymodem:
  -           -    network rw    rcp:
  -           -    network rw    http:
  -           -    network rw    ftp:
  -           -    network rw    scp:
  -           -    opaque  ro    tar:
  -           -    network rw    https:
  -           -    opaque  ro    cns:
```

- \* El asterisco indica que este es el sistema de archivos predeterminado actual.



## Sistemas de archivos del router y del switch

# Sistemas de archivos del switch

- Comando **show file systems**: enumera todos los sistemas de archivos disponibles en un switch Catalyst 2960.

```
Switch#show file systems
File Systems:

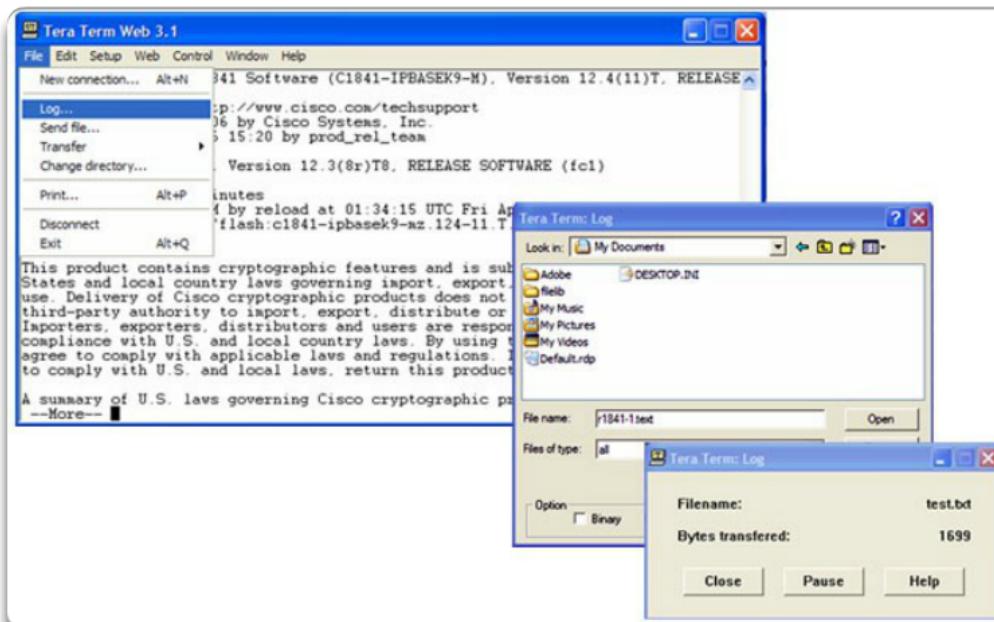
  Size(b)    Free(b)   Type  Flags  Prefixes
* 32514048  20887552  flash  rw     flash:
      -        -       opaque  rw     vb:
      -        -       opaque  ro     bs:
      -        -       opaque  rw     system:
      -        -       opaque  rw     tmpsys:
  65536     48897    nvram  rw     nvram:
      -        -       opaque  ro     xmodem:
      -        -       opaque  ro     ymodem:
      -        -       opaque  rw     null:
      -        -       opaque  ro     tar:
      -        -       network rw     tftp:
      -        -       network rw     rcp:
      -        -       network rw     http:
      -        -       network rw     ftp:
      -        -       network rw     scp:
      -        -       network rw     https:
      -        -       opaque  ro     cns:
```



# Creación de copias de seguridad y restauración de archivos de configuración

# Creación de copias de seguridad y restauración mediante archivos de texto

Cómo guardar en un archivo de texto en Tera Term



1. Inicie el proceso de registro.
2. Emite un comando **show running-config**.
3. Cierre el registro.



## Creación de copias de seguridad y restauración de archivos de configuración

# Creación de copias de seguridad y restauración mediante TFTP

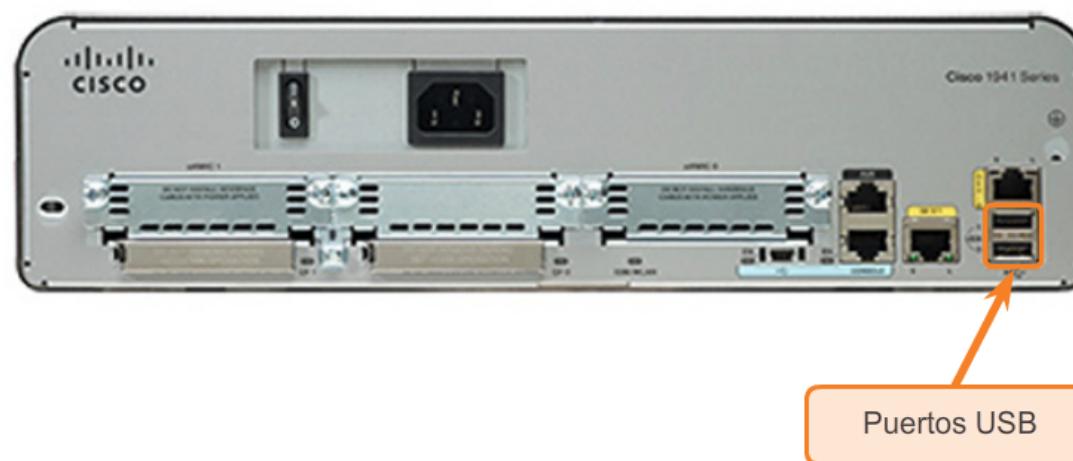
- Los archivos de configuración se pueden almacenar en un servidor de protocolo trivial de transferencia de archivos (TFTP).
- **copy running-config tftp:** guarda la configuración en ejecución en un servidor tftp.
- **copy startup-config tftp:** guarda la configuración de inicio en un servidor tftp.

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm]
Writing tokyo.2 !!!!!!! [OK]
```

## Creación de copias de seguridad y restauración de archivos de configuración

# Uso de interfaces USB en un router Cisco

- La unidad flash USB debe tener formato FAT16.
- Puede contener varias copias de las configuraciones de Cisco IOS y varias configuraciones del router.
- Permite que el administrador pase fácilmente las configuraciones de router a router.





## Creación de copias de seguridad y restauración de archivos de configuración

# Creación de copias de seguridad y restauración mediante USB

```
R1#copy running-config usbflash0:  
Destination filename [running-config]? R1-Config  
5024 bytes copied in 0.736 secs (6826 bytes/sec)
```

Copia a la unidad flash USB; no hay ningún archivo existente.

```
R1#copy running-config usbflash0:  
Destination filename [running-config]? R1-Config  
%Warning:There is a file already existing with this name  
Do you want to over write? [confirm]  
5024 bytes copied in 1.796 secs (2797 bytes/sec)
```

Copia a la unidad flash USB; ya existe en la unidad el mismo archivo de configuración.



## Router integrado

# Dispositivo multifunción

- Incorpora un switch, un router y un punto de acceso inalámbrico.
- Proporciona enrutamiento, conmutación y conectividad inalámbrica.
- Los routers inalámbricos Linksys son de diseño simple y se utilizan en redes domésticas.
- La familia de productos de router de servicios integrados (ISR) de Cisco ofrece una amplia gama de productos, diseñados para redes de oficinas pequeñas y redes más grandes.

Linksys, modelo WRT300N2

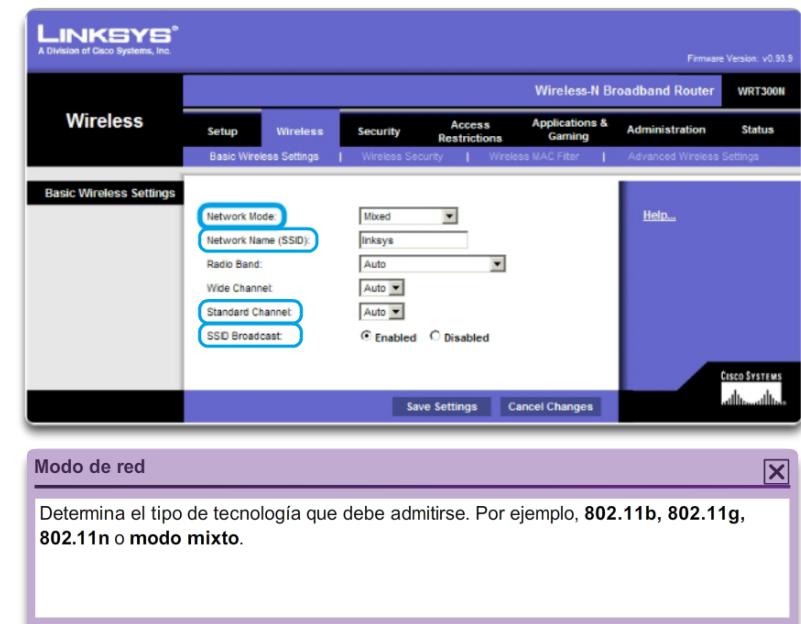




## Router integrado

# Capacidad inalámbrica

- **Modo inalámbrico:** la mayoría de los routers inalámbricos integrados son compatibles con las versiones 802.11b, 802.11g y 802.11n
- **Identificador de conjunto de servicios (SSID):** nombre alfanumérico que distingue mayúsculas de minúsculas para la red inalámbrica doméstica.
- **Canal inalámbrico:** espectro de RF dividido en canales.





## Router integrado

# Seguridad básica de la tecnología inalámbrica

- Cambiar los valores predeterminados.
- Deshabilitar la transmisión del SSID.
- Configurar la encriptación mediante WEP o WPA.
- **Protocolo de equivalencia por cable (WEP):** utiliza claves preconfiguradas para encriptar y descifrar datos. Cada dispositivo inalámbrico que está autorizado a acceder a la red debe tener introducida la misma clave WEP.
- **Acceso protegido Wi-Fi (WPA):** también utiliza claves de encriptación de 64 a 256 bits. Se generan nuevas claves cada vez que se establece una conexión al AP. Por lo tanto, es más seguro.



## Router integrado

# Configuración del router integrado

- Para acceder al router, conecte un cable de una PC a uno de los puertos Ethernet para LAN del router.
- El dispositivo que se conecta obtendrá automáticamente la información de direccionamiento IP del router integrado.
- Por cuestiones de seguridad, cambie el nombre de usuario y contraseña predeterminados y la dirección IP predeterminada de Linksys.

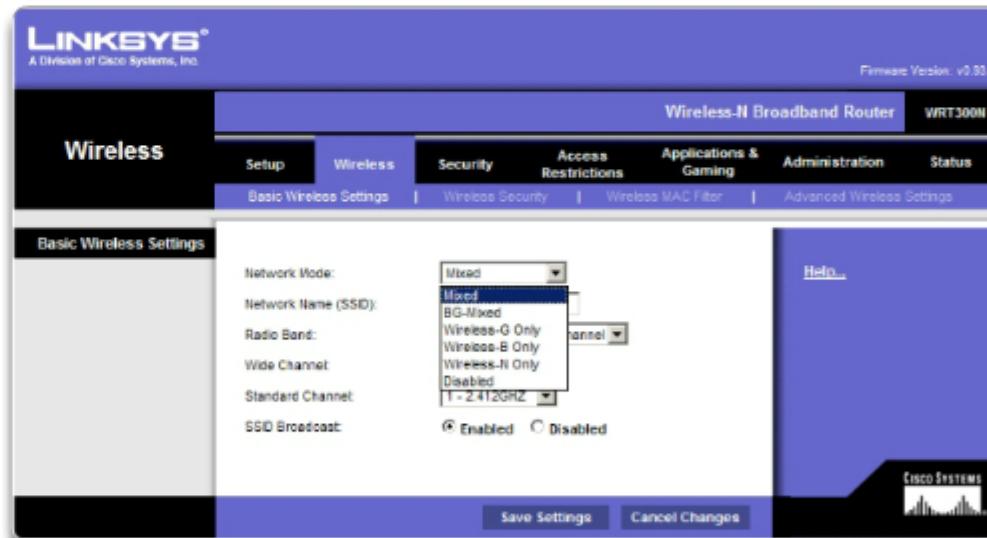




## Router integrado

# Habilitación de la conectividad inalámbrica

- Configurar el modo inalámbrico.
- Configurar el SSID.
- Configurar el canal de RF.
- Configurar cualquier mecanismo de encriptación de seguridad deseado.





## Router integrado

# Configuración de un cliente inalámbrico

- Las opciones de configuración del cliente inalámbrico deben coincidir con la del router inalámbrico.

SSID

Parámetros de seguridad

Canal

- El software de cliente inalámbrico puede estar integrado al sistema operativo del dispositivo o puede ser un software de utilidad inalámbrica, independiente y que se puede descargar.





# Capítulo 11: Resumen

- Un buen diseño de red incorpora confiabilidad, escalabilidad y disponibilidad.
- Se deben proteger las redes de virus, caballos de Troya, gusanos y ataques de red.
- Documente el rendimiento básico de la red.
- Pruebe la conectividad de red mediante ping y traceroute.
- Utilice los comandos de IOS para controlar y visualizar información acerca de la red y los dispositivos de red.
- Realice copias de seguridad de los archivos de configuración mediante TFTP o USB.
- Las redes domésticas y las pequeñas empresas suelen utilizar routers integrados, que proporcionan las características de un switch, un router y un punto de acceso inalámbrico.

# Cisco | Networking Academy®

Mind Wide Open™