

Fundamentos de Redes CCNA1

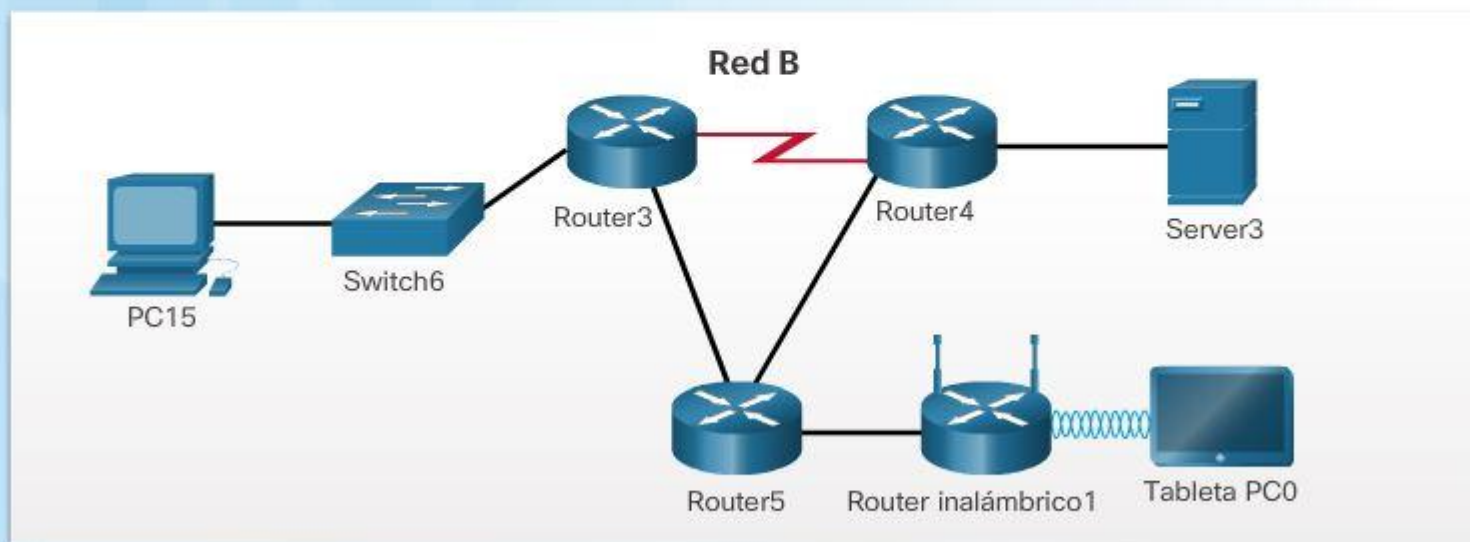
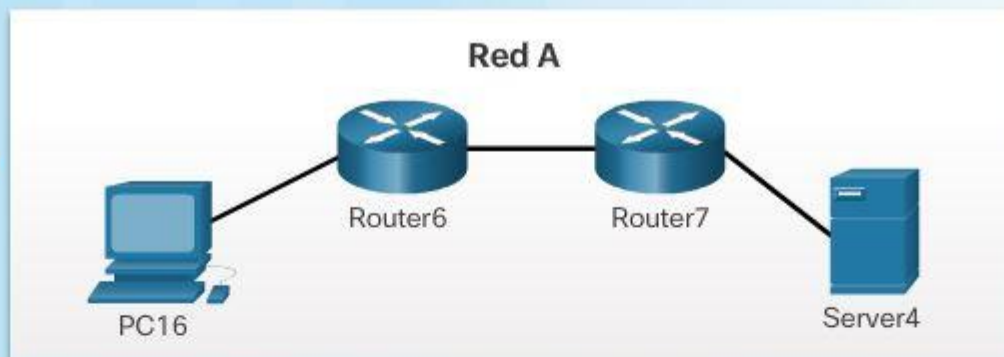
Clase “13”

Para cumplir con los requisitos de los usuarios, incluso las redes pequeñas requieren planificación y diseño.

La planificación asegura que se consideren debidamente todos los requisitos, factores de costo y opciones de implementación.

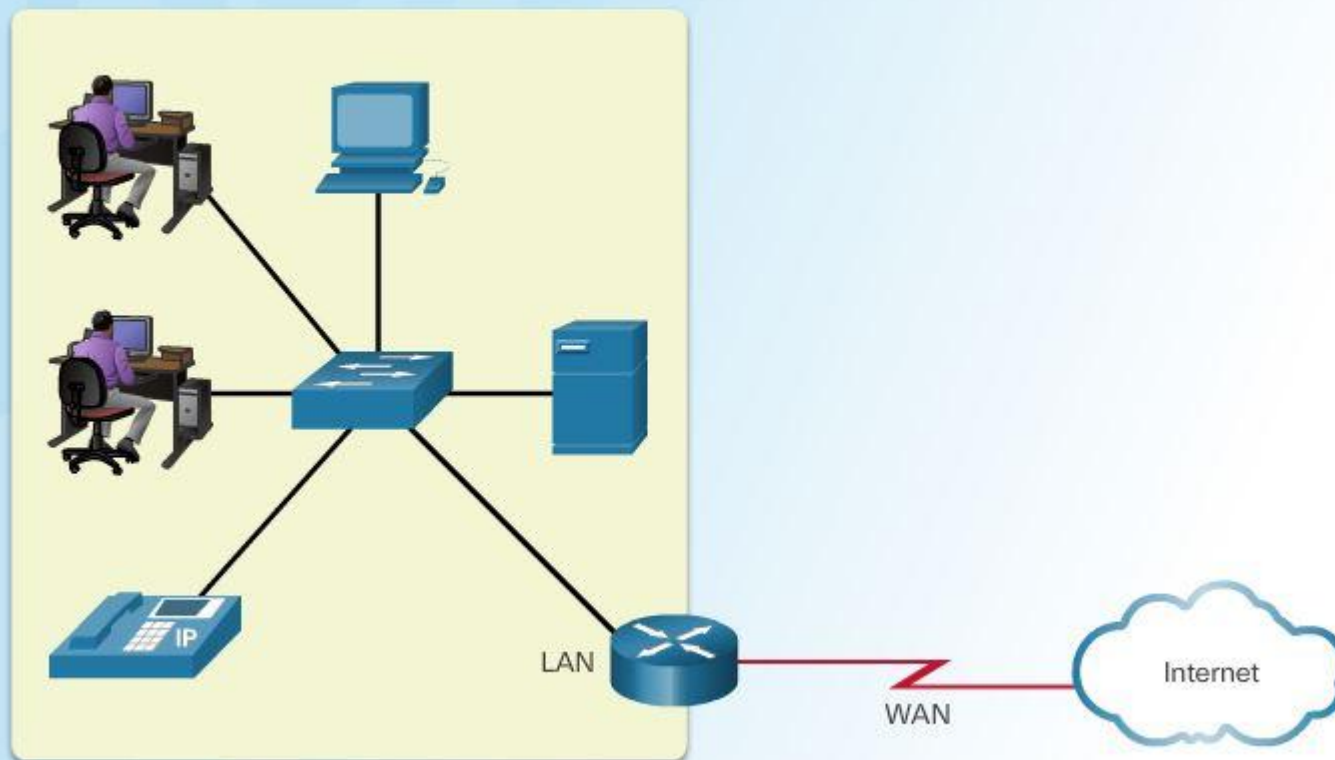
La confiabilidad, la escalabilidad y la disponibilidad son partes importantes del diseño de una red.

Cree y...



... ¡crezca!

Red típica de una pequeña empresa



Factores a considerar al elegir un dispositivo



Costo



Puertos



Velocidad



Si es modular o tiene capacidad de expansión



Si es fácil de administrar

Planificación y asignación de direcciones IPv4



Departamento

Ventas

Ubicación

RR. HH.

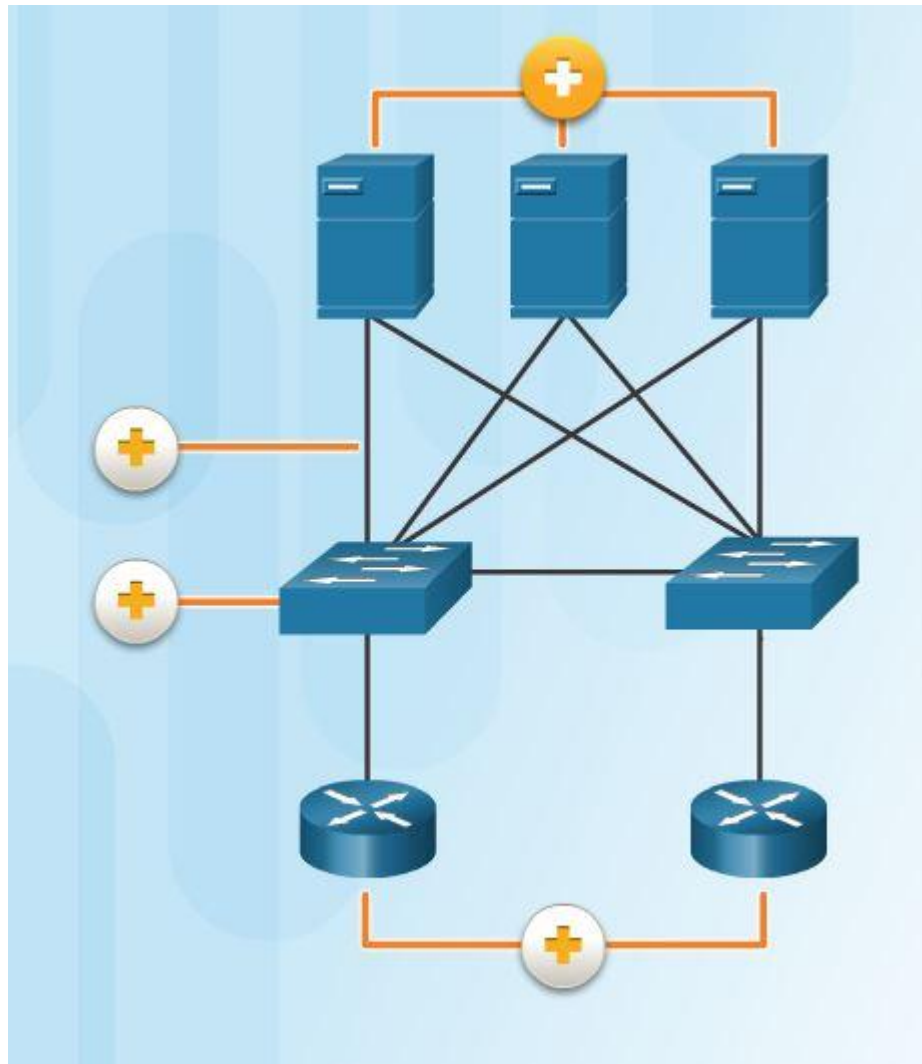
Legales

Dispositivo

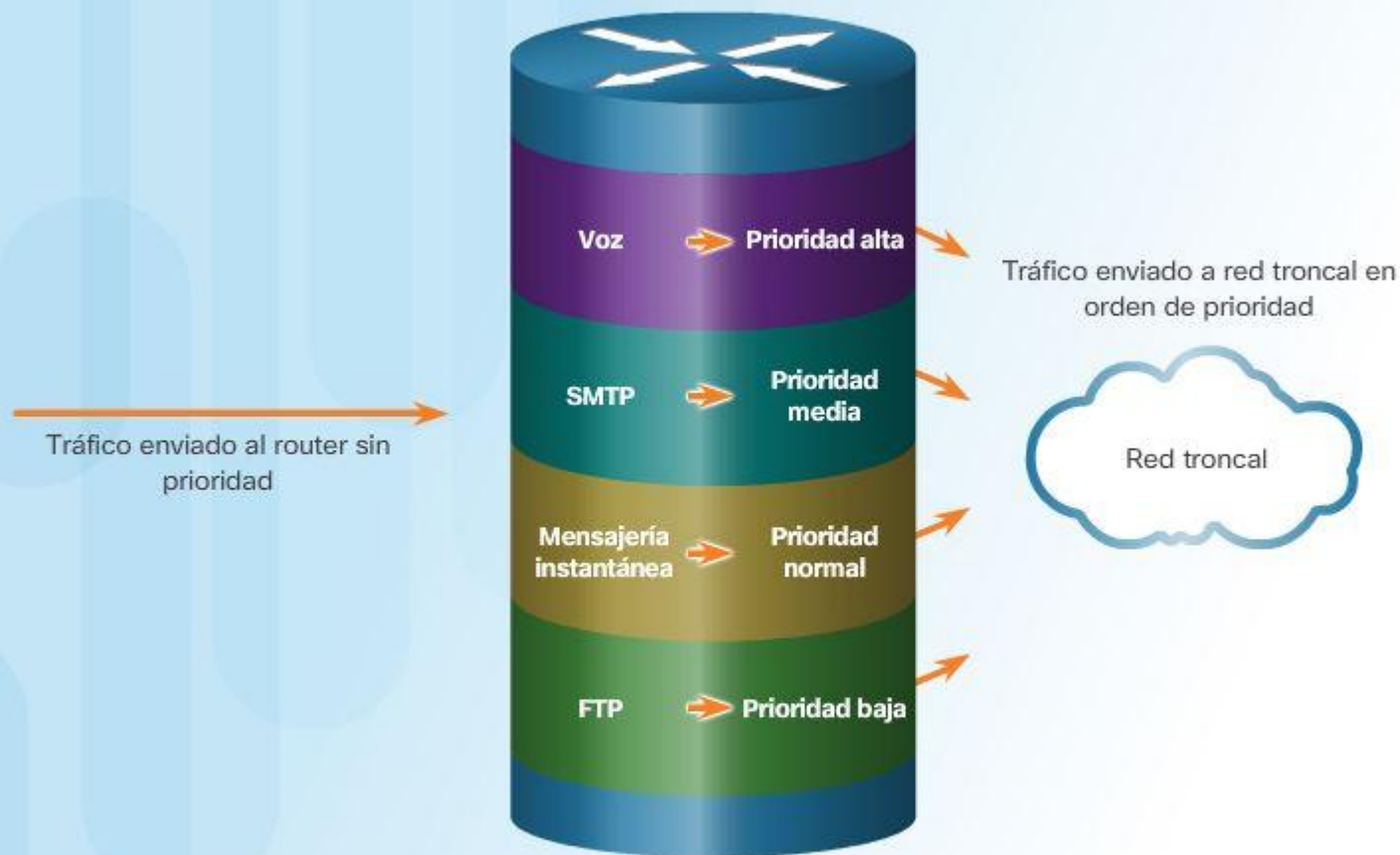
Impresora

Servidor

Equipo

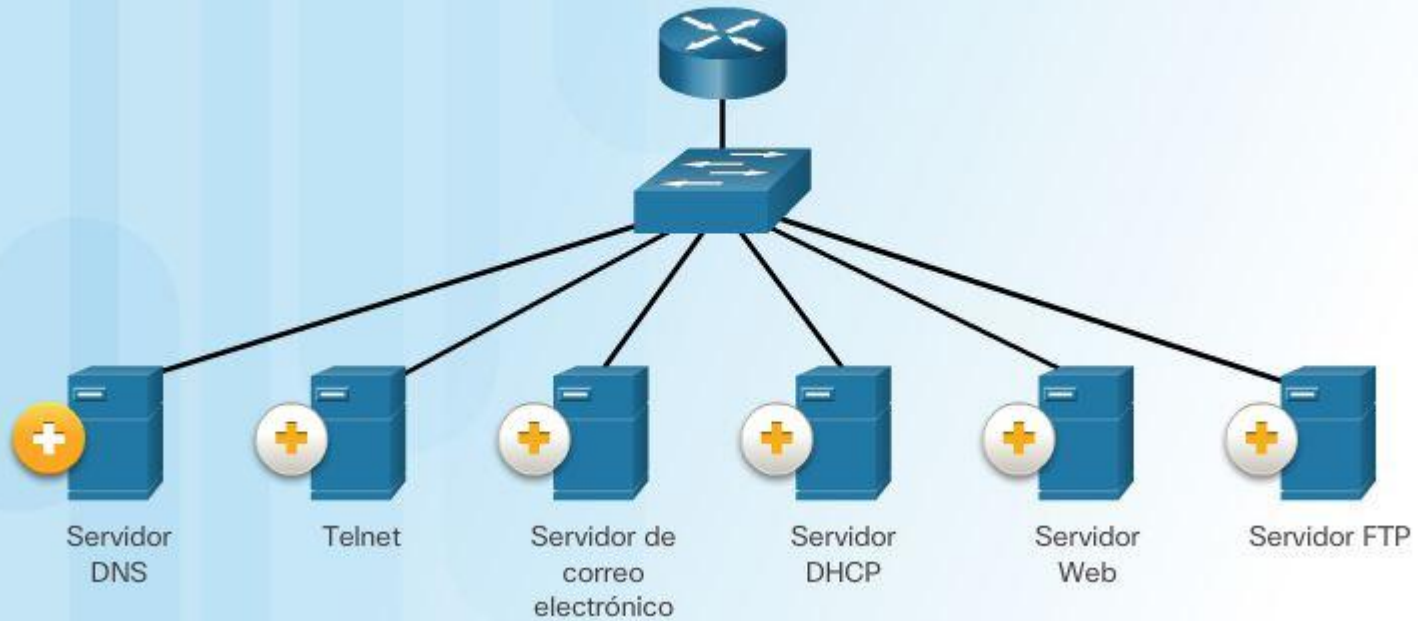


Priorización del tráfico



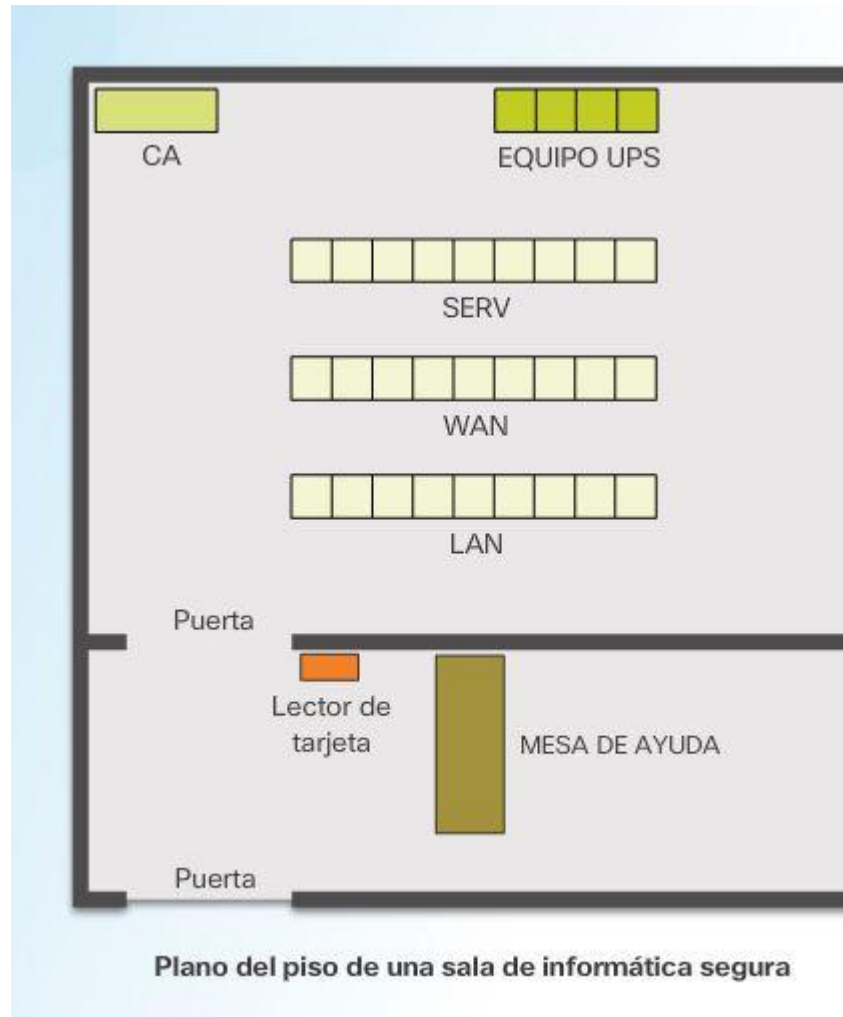
Hay cuatro colas de prioridad. La cola de prioridad alta siempre se vacía primero.

Servicios de red



Crecimiento de las redes pequeñas





Vulnerabilidades: tecnología

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 redes (SNMP) y el protocolo simple de transferencia de correo (SMTP) se relacionan con la estructura intrínsecamente insegura sobre la que se diseñó TCP.

Debilidad 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
- Están registrados en los archivos del Computer Emergency Response Team (CERT) en <http://www.cert.org>.

Debilidad de los equipos de red

Los diversos tipos de equipos de red, como routers, firewalls y switches, tienen debilidades de seguridad que deben identificarse y evitarse. Sus debilidades incluyen la protección de contraseñas, la falta de autenticación, los protocolos de routing y los agujeros de firewall.

Vulnerabilidades: configuración

Debilidad en la configuración	Cómo se aprovecha la debilidad
Cuentas de usuario no seguras	La información de la cuenta de usuario se puede transmitir de manera insegura a través de la red. Esto expone nombres de usuario y contraseñas a los curiosos.
Cuentas del sistema con contraseñas fáciles de adivinar	Este problema común se debe a la elección de contraseñas de usuario deficientes y fáciles de adivinar.
Servicios de Internet mal configurados	Un problema común es activar JavaScript en los navegadores web, lo que permite ataques mediante scripts hostiles cuando se accede a sitios no confiables. Otras posibles fuentes de debilidades incluyen los servicios de terminal mal configurados, FTP o los servidores web (p. ej., Microsoft Internet Information Services (IIS), servidor HTTP Apache).
Configuraciones predeterminadas no seguras dentro de productos	Muchos productos tienen configuraciones predeterminadas que habilitan los agujeros de seguridad.
Equipos de red mal configurados	Las malas configuraciones del propio equipo pueden causar problemas de seguridad importantes. Por ejemplo, las listas de acceso mal configuradas, los protocolos de routing o las cadenas comunitarias SNMP pueden abrir enormes agujeros de seguridad.

Vulnerabilidades: política

Debilidad en las políticas	Cómo se aprovecha la debilidad
Falta de políticas de seguridad por escrito	Una política no escrita no se puede aplicar sistemáticamente ni se puede hacer cumplir.
Política	Las batallas políticas y las luchas territoriales pueden dificultar la implementación de una política de seguridad sistemática.
Falta de continuidad de autenticación	Las contraseñas mal elegidas, las contraseñas fáciles de decodificar o las contraseñas predeterminadas pueden permitir el acceso no autorizado a la red.
Controles de acceso lógico no aplicados	El monitoreo y la auditoría inadecuados permiten que los ataques y el uso no autorizado continúen. Esto hace que la empresa desperdicie recursos. Esto puede ocasionar acciones legales o despidos de los técnicos de TI, de la administración de TI o hasta de los directores de la empresa que permiten que estas condiciones no seguras persistan.
La instalación de software y hardware y los cambios no respetan la política	Los cambios no autorizados que se realizan en la topología de la red o la instalación de aplicaciones no aprobadas crean agujeros de seguridad.
No existe plan de recuperación tras un desastre	La falta de un plan de recuperación tras un desastre produce caos, pánico y confusión cuando alguien ataca la empresa.

Robo de información



Robar informes de una investigación científica



Robar la base de datos de usuarios de una empresa

Robo de identidad



Hacerse pasar por otra persona para obtener crédito



Hacer compras ilegales en línea

Pérdida/manipulación de datos



Alterar registros de datos



Enviar un virus para reformatar un disco duro

Interrupción del servicio



Sobrecargar una red para que los usuarios no puedan ingresar



Impedir que los usuarios legales accedan a servicios de datos

avanzado

- ✓ Bloquear dispositivos; impedir el acceso no autorizado
- ✓ Usar cámaras de seguridad

Consideraciones ambientales

- ✓ Controlar la temperatura y la humedad
- ✓ Generar un flujo de aire positivo

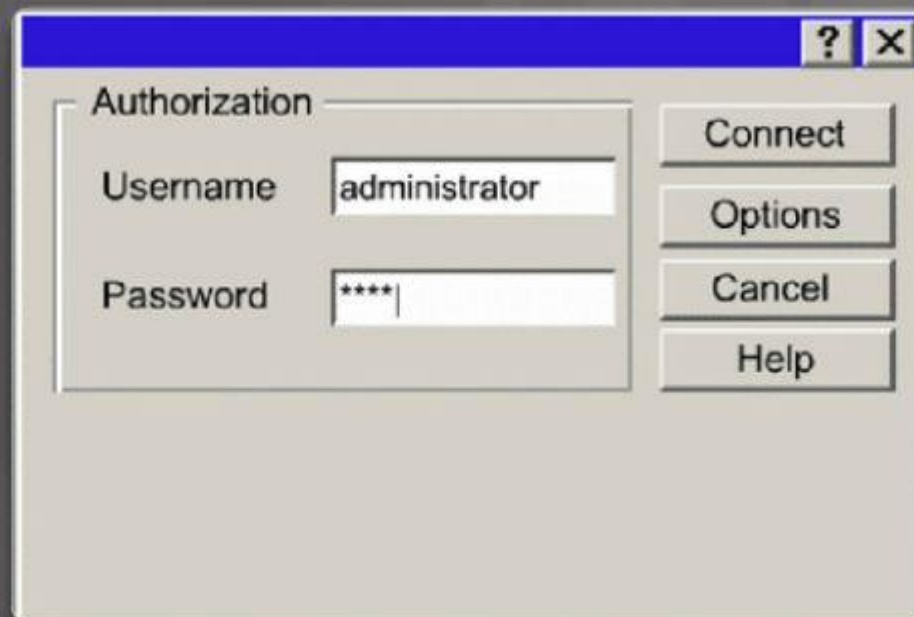
Eléctrico

- ✓ Instalar fuentes de alimentación redundantes
- ✓ Instalar sistemas UPS

Mantenimiento

- ✓ Controlar el acceso a los puertos de la consola
- ✓ Etiquetar cables y componentes fundamentales

Ataque a la contraseña

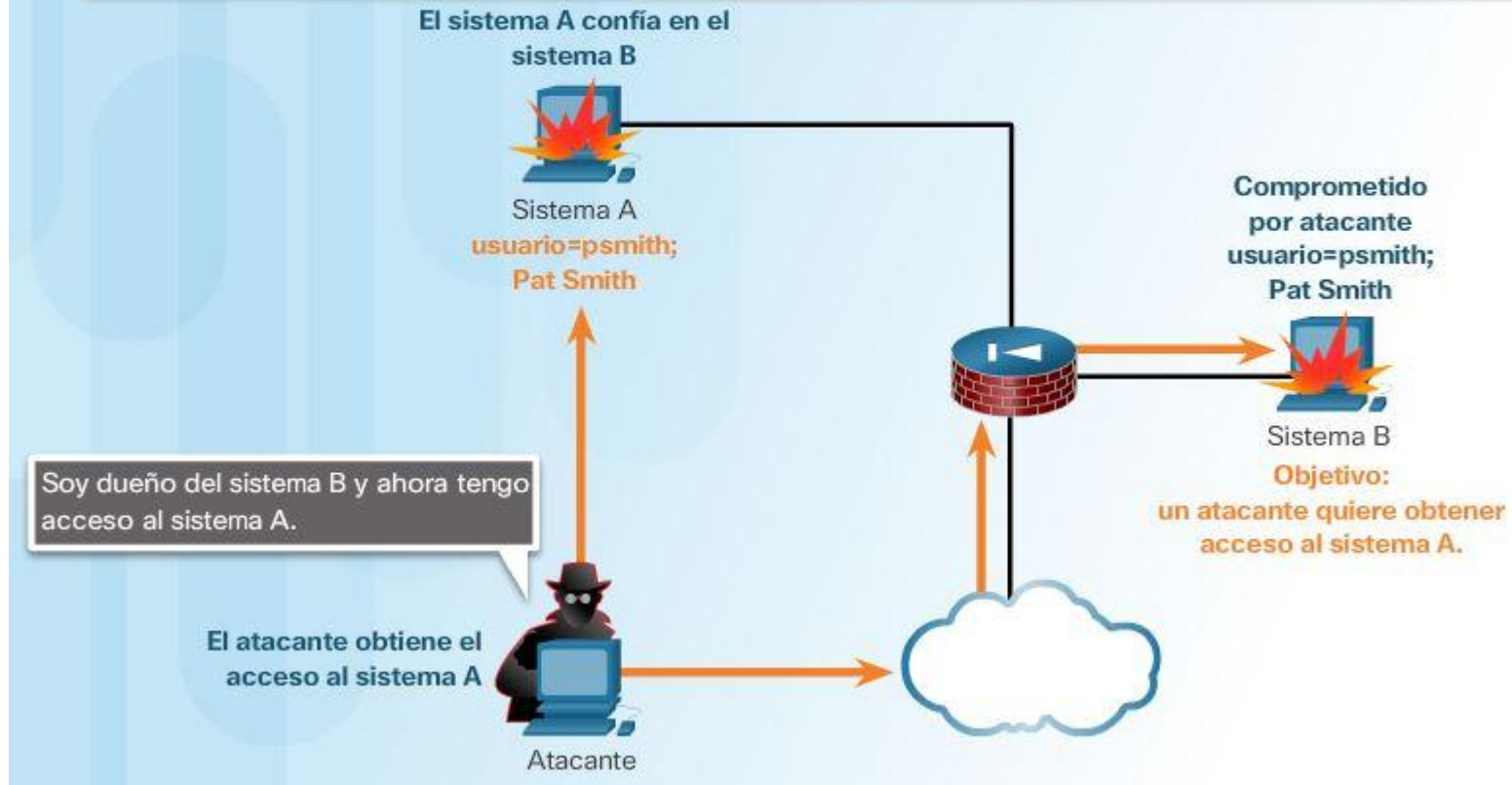


Los atacantes pueden implementar ataques a la contraseña mediante diversos métodos:

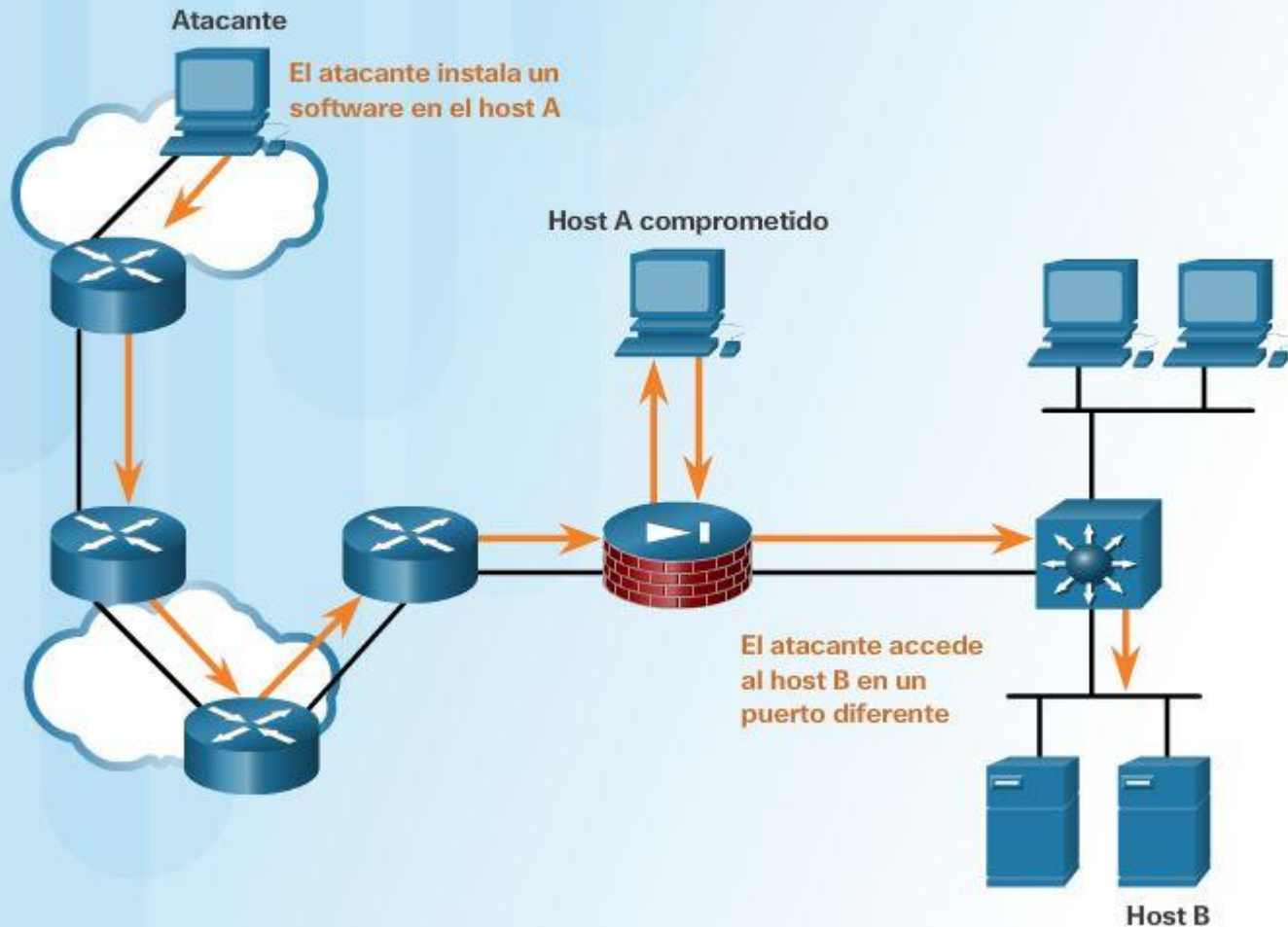
- Ataques por fuerza bruta
- Caballos de Troya
- Programas detectores de paquetes

Explotación de confianza

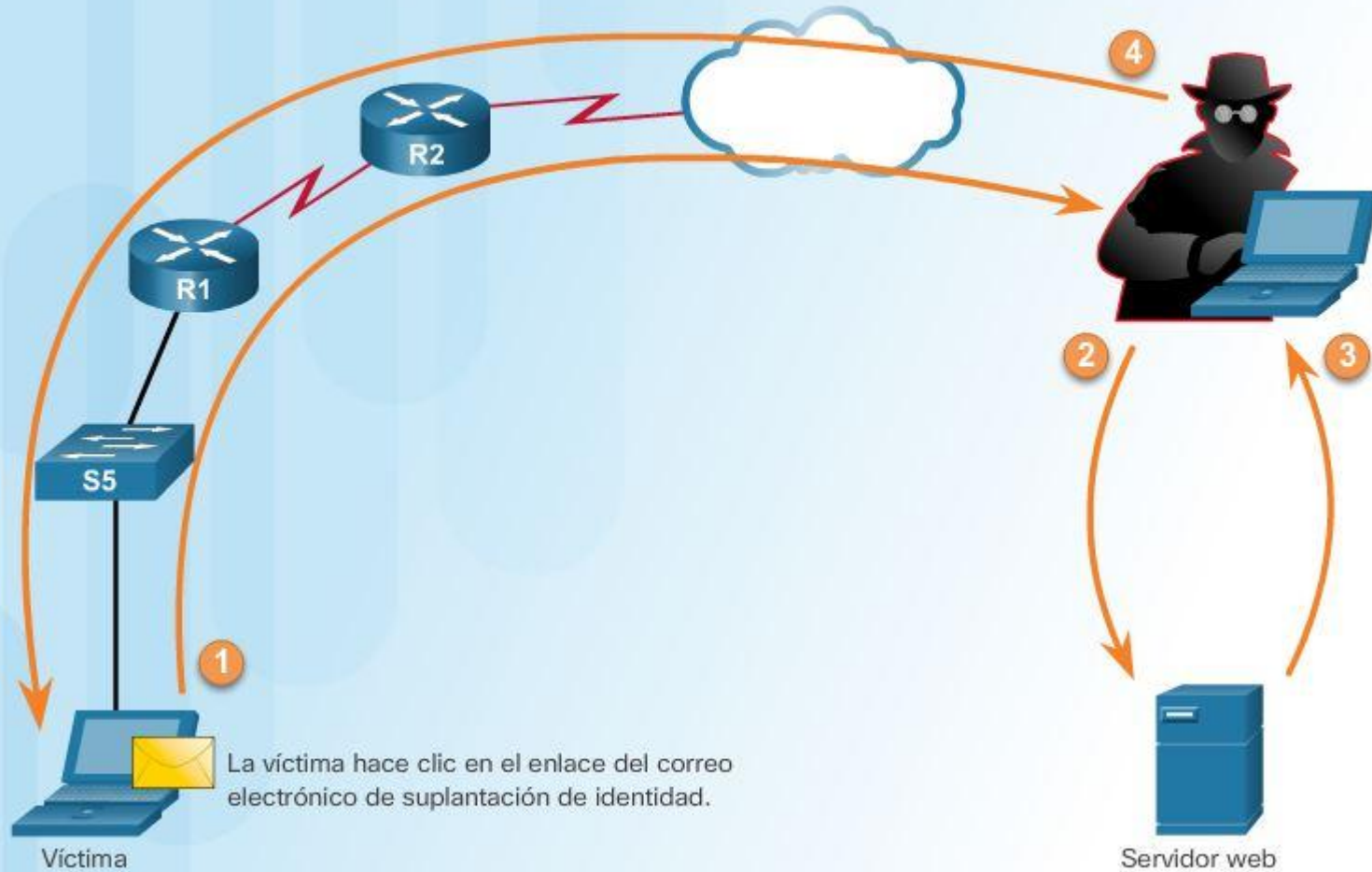
Network OS	Trust Models
Windows	Domains Active Directory (AD)
Linux and UNIX	Network File System (NFS) Network Information Service Plus (NIS+)



Redireccionamiento de puertos

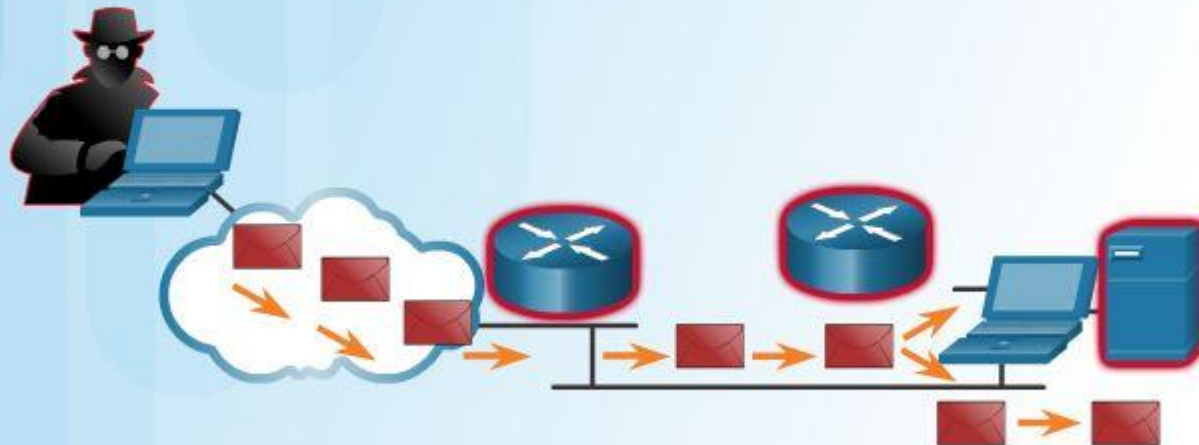


Ataque man-in-the-middle



Ataque de DoS

Sobrecargas de recursos	Datos con formato incorrecto
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 impiden que el personal autorizado use un servicio porque consumen los recursos del sistema.

Ping de la muerte



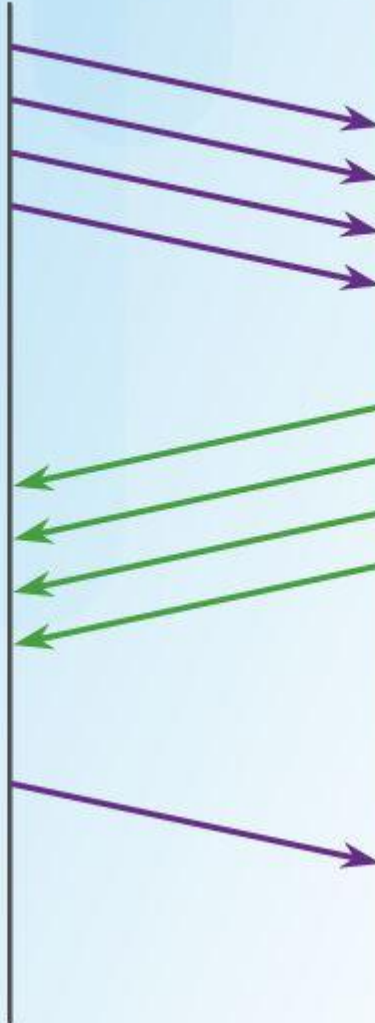
Equipo atacante

El atacante envía un ping mal formado o muy grande.



Saturación SYN

El atacante envía varios pedidos SYN a un servidor web



Un servidor web envía respuestas SYN-ACK



Servidor web

Un servidor web espera para completar un enlace de tres vías



Servidor web

Un usuario válido envía un pedido SYN

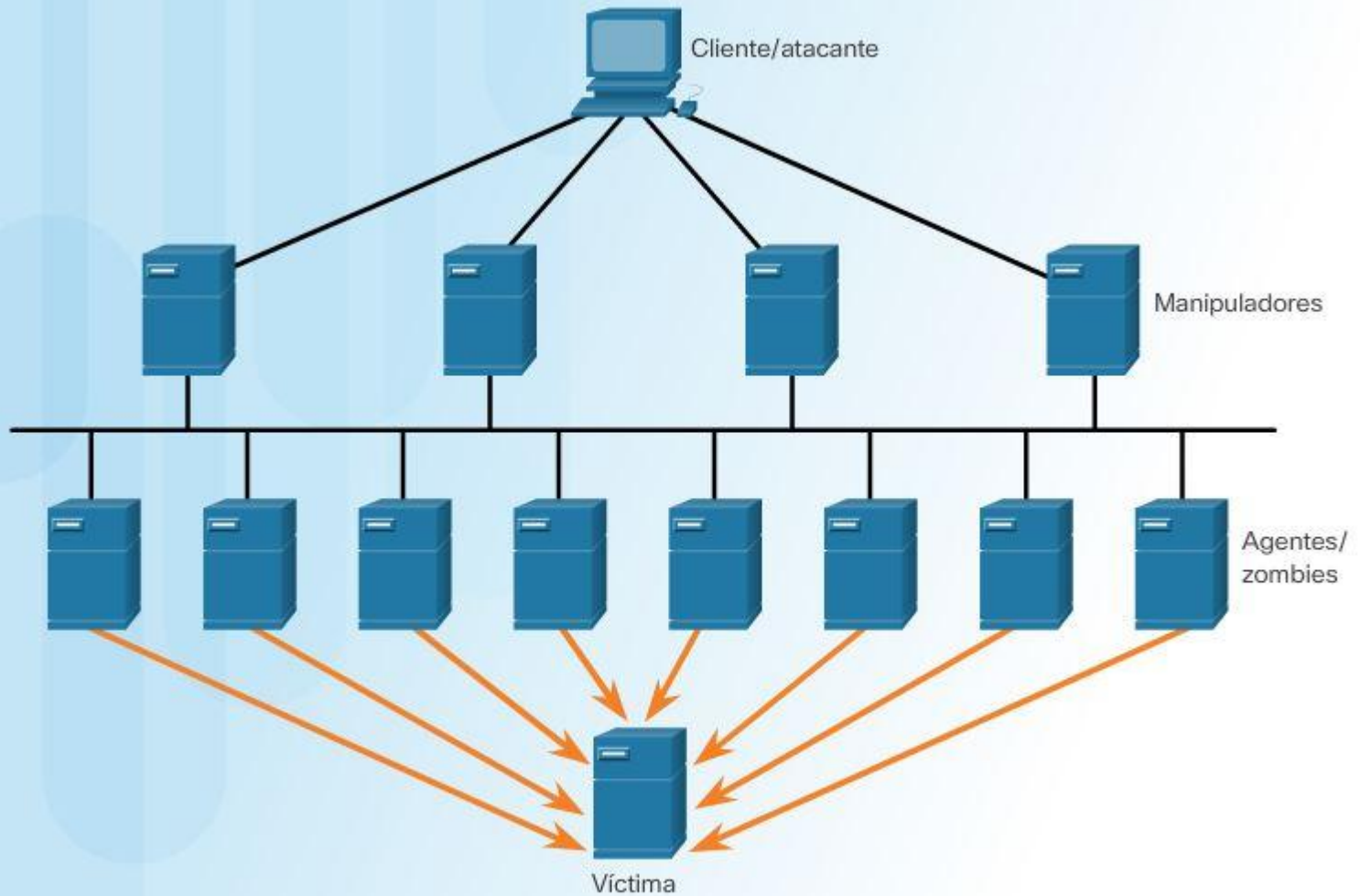


El servidor web no está disponible



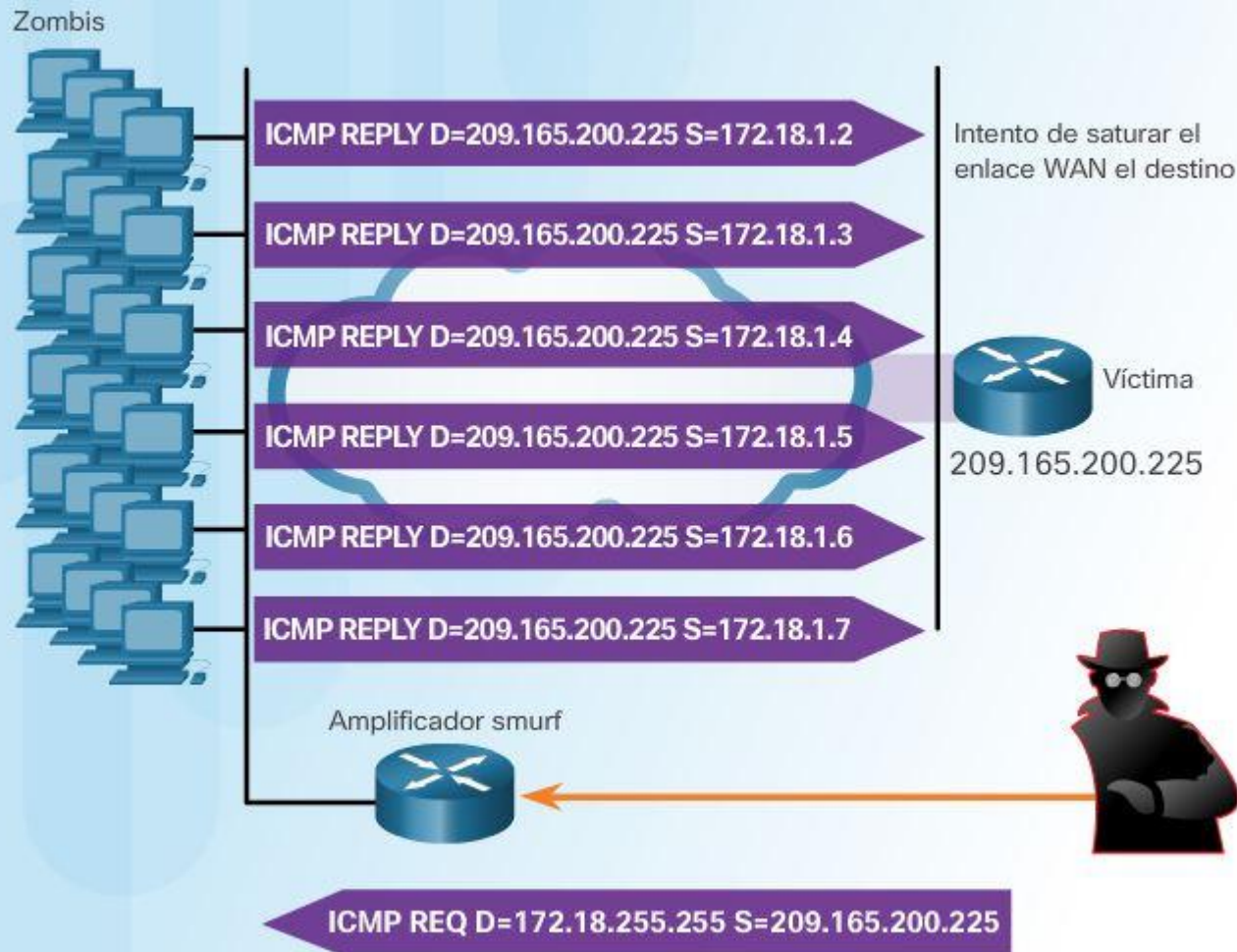
Servidor web

DDoS

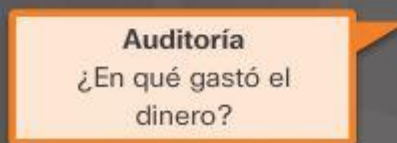


El atacante utiliza muchos hosts intermediarios, denominados "zombis", para iniciar el ataque.

Ataque Smurf



El concepto de AAA es similar al uso de una tarjeta de crédito



Account Number: 1234-567-890 Statement Closing Date: 01-31-01 Current Amount Due: \$278.50

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234
872919345 00178255000000003

MAIL PAYMENT TO:
THE BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

Detach here and return upper portion with check or money order. Do not staple or fold.

Platinum Credit Card Account **THE BANK**

Statement Closing Date: 01-31-01

Statement Date: 02-01-01 Payment Due Date: 03-01-01
Closing Date: 01-31-01
Credit Limit: \$1,500.00 Credit Available: \$1221.50
New Balance: \$278.50 Minimum Payment Due: \$20.00

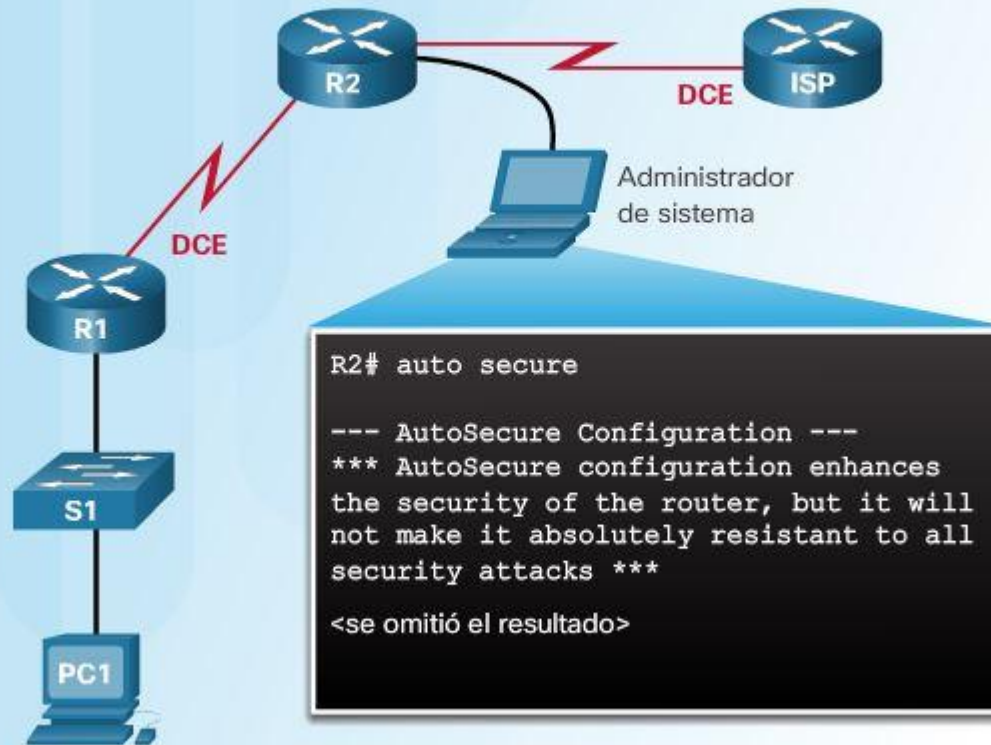
Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	\$278.50

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
78543210	01-29	01-30	Electronic World Anytown, USA	\$89.25
2345678		01-30	Transaction Fees	\$3.00
1234567890		01-01	Annual Fee	\$25.00

PAGE 1 OF 1

Restringir función del router



Contraseñas débiles y seguras

Contraseña débil	Por qué es débil
secreto	Contraseña de diccionario simple
perez	Apellido de soltera de una mujer
toyota	Marca de un auto
bob1967	Nombre y fecha de nacimiento de un usuario
Blueleaf23	Palabras y números simples

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

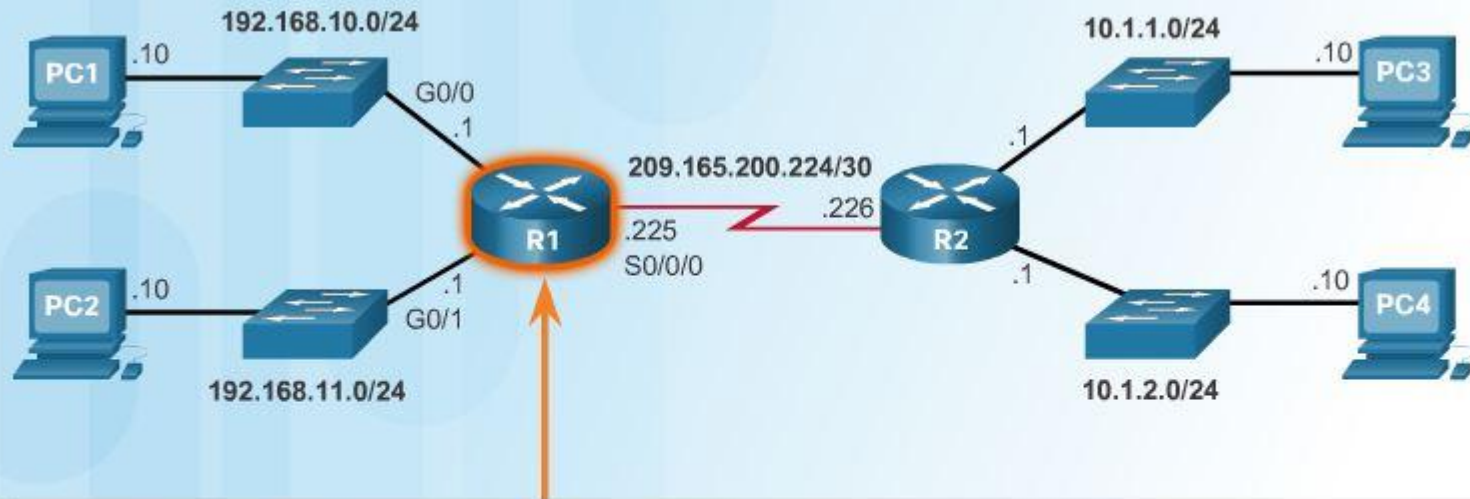
```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# exec-timeout 10
Router(config-line)# end
Router# show running-config
-
-
!
line vty 0 4
 password 7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



```
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.

Indicadores de ping IOS



```
R1# ping 209.165.200.226
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout  
is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max =  
3/3/4 ms
```

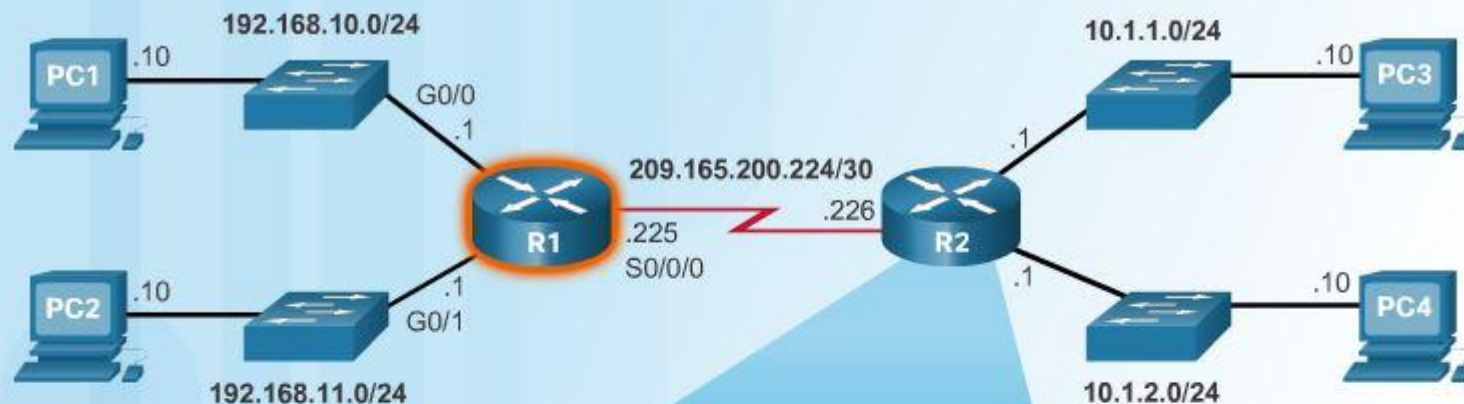
```
R1#
```


Prueba de loopback



```
C:\> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time=0ms TTL=128
Reply from 127.0.0.1: bytes=32 time=4ms TTL=128
Reply from 127.0.0.1: bytes=32 time=3ms TTL=128
Reply from 127.0.0.1: bytes=32 time=3ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 2ms
```

```

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]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

```

Ejecute la misma prueba

8 FEB 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
```

```
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
```

```
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
```

```
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 MAR 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
```

```
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
```

```
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
```

```
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
```

En diferentes momentos

8 FEB 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
```

```
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
```

```
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
```

```
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 MAR 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
```

```
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
```

```
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
```

```
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
```

Compare valores

8 FEB 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  
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128  
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 MAR 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  
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
```

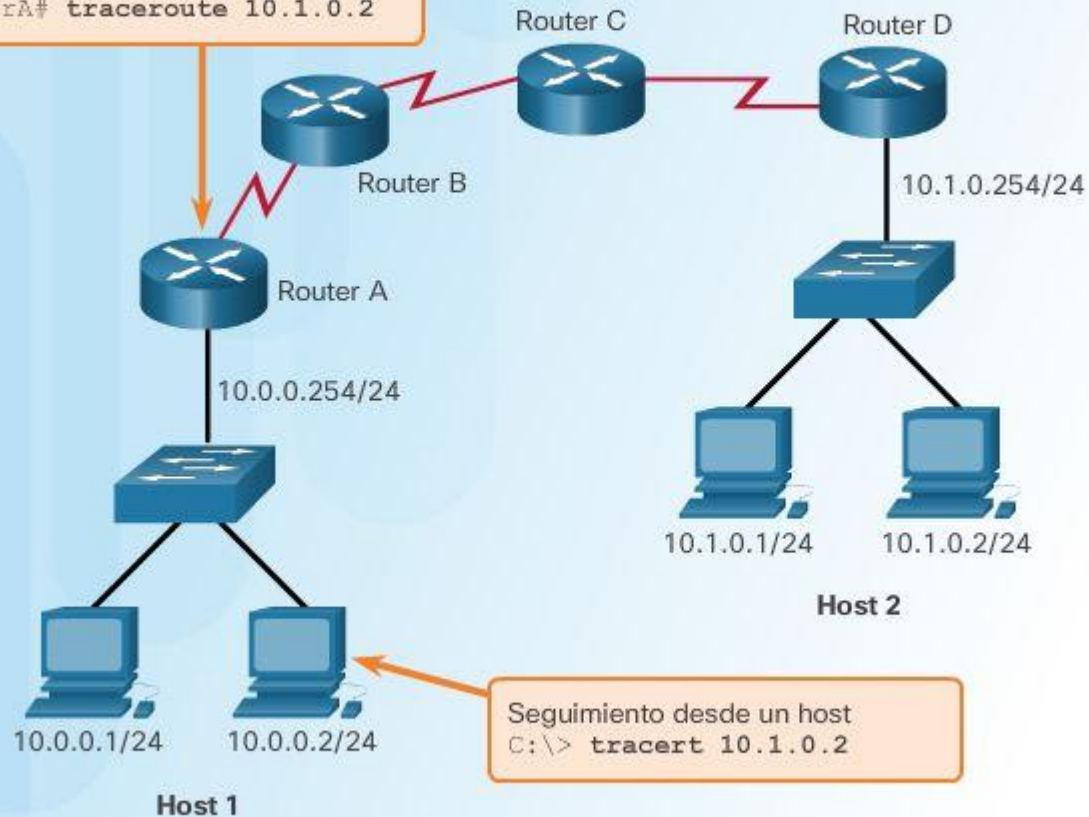
```
Ping statistics for 10.66.254.159:
```

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


Prueba de la ruta a un host remoto

Seguimiento desde un router

```
RouterA# traceroute 10.1.0.2
```



Seguimiento desde un host
C:\> tracert 10.1.0.2

Seguimiento de la ruta del host 1 al host 2

```
C:\> tracert 10.1.0.2
Tracing route to 10.1.0.2 over a maximum of 30 hops
 1  2 ms  2 ms  2 ms  10.0.0.254
 2  * * * Request timed out.
 3  * * * Request timed out.
 4  ^C
C:\>
```

Opciones de traceroute extendido

Opción	Descripción
Protocol [ip]:	Indicadores para un protocolo admitido. El predeterminado es IPv4
Target IP address:	Debe ingresar un nombre de host o una dirección IPv4. No hay predeterminado.
Source address:	La interfaz o la dirección IPv4 del router para utilizarla como dirección de origen para los sondeos. El router habitualmente elige la dirección IPv4 de la interfaz saliente que va a utilizar.
Numeric display [n]:	De manera predeterminada hay una pantalla simbólica y una numérica; sin embargo, puede eliminar la pantalla simbólica.
Timeout in seconds [3]:	Cantidad de segundos de espera para una respuesta a un paquete de sondeo. El valor predeterminado es 3 de segundos.
Probe count [3]:	La cantidad de sondeos a enviar en cada nivel de TTL. El valor predeterminado es 3.
Minimum Time to Live [1]:	El valor TTL para los primeros sondeos. El valor predeterminado es 1, pero puede estar configurado en un valor más alto para evitar mostrar saltos conocidos.
Maximum Time to Live [30]:	El valor TTL más grande que pueda utilizarse. De manera predeterminada, es 30. El comando traceroute finaliza cuando se llega al destino o se alcanza este valor.
Port Number [33434]:	El puerto de destino utilizado por los mensajes del sondeo UDP. De manera predeterminada, es 33434.
Loose, Strict, Record, Timestamp, Verbose [none]:	Opciones de encabezado IP. Puede especificar cualquier combinación. El comando traceroute emite peticiones para los campos obligatorios. Observe que el comando traceroute colocará las opciones solicitadas en cada sondeo; sin embargo, no hay garantía de que todos los routers (o nodos finales) procesarán las opciones.

Opciones de tracert de Windows

```
C:\> tracert
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name
Options:
    -d                Do not resolve addresses to hostnames.
    -h maximum_hops   Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                Force using IPv4.
    -6                Force using IPv6.
C:\>
```

Show running-config

```
R1# show running-config
<Resultado omitido>
Building configuration...
Current configuration : 1063 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$i6w9$dvdpmVM6zV10E6tSyLdkR5/
no ip domain lookup
!
interface FastEthernet0/0
 description LAN 192.168.1.0 default gateway
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
interface Serial0/0/0
  description WAN link to R2
  ip address 192.168.2.1 255.255.255.0
  encapsulation ppp
  clock rate 64000
  no fair-queue
!
interface Serial0/0/1
  no ip address
  shutdown
!
interface Vlan1
  no ip address
!
router rip
  version 2
  network 192.168.1.0
  network 192.168.2.0
!
banner motd ^CUnauthorized Access Prohibited^C
!
ip http server
!
line con 0
  password cisco
  login
line aux 0
line vty 0 4
  password cisco
  login
```


Show interfaces

```
R1# show interfaces
<Resultado omitido>
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256e
    (bia 001b.5325.256e)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:17, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes);
  Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    196 packets input, 31850 bytes
    Received 181 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
    392 packets output, 35239 bytes, 0 underruns
    0 output errors, 0 collisions, 3 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

```
FastEthernet0/1 is administratively down,  
line protocol is down  
  
Serial0/0/0 is up, line protocol is up  
  Hardware is GT96K Serial  
  Internet address is 192.168.2.1/24  
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,  
    reliability 255/255, txload 1/255, rxload 1/255  
  Encapsulation PPP, LCP Listen, loopback not set  
  Keepalive set (10 sec)  
  Last input 00:00:02, output 00:00:03, output hang never  
  Last clearing of "show interface" counters 00:51:52  
  Input queue: 0/75/0/0 (size/max/drops/flushes);  
  Total output drops: 0  
  Queueing strategy: fifo  
  Output queue: 0/40 (size/max)  
  5 minute input rate 0 bits/sec, 0 packets/sec  
  5 minute output rate 0 bits/sec, 0 packets/sec  
    401 packets input, 27437 bytes, 0 no buffer  
    Received 293 broadcasts, 0 runts, 0 giants, 0 throttles  
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort  
    389 packets output, 26940 bytes, 0 underruns  
    0 output errors, 0 collisions, 2 interface resets  
    0 output buffer failures, 0 output buffers swapped out  
    6 carrier transitions  
  DCD=up DSR=up DTR=up RTS=up CTS=up  
  
Serial0/0/1 is administratively down, line protocol is down
```

Show arp

```
R1# show arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.17.0.1	-	001b.5325.256e	ARPA	FastEthernet0/0
Internet	172.17.0.2	12	000b.db04.a5cd	ARPA	FastEthernet0/0

Show protocols

```
R1# show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24
FastEthernet0/1 is administratively down, line protocol is down
FastEthernet0/1/0 is up, line protocol is down
FastEthernet0/1/1 is up, line protocol is down
FastEthernet0/1/2 is up, line protocol is down
FastEthernet0/1/3 is up, line protocol is down
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.2.1/24
Serial0/0/1 is administratively down, line protocol is down
Vlan1 is up, line protocol is down
```

Show version

```
R1# show version
<Resultado omitido>
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M),
Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
R1 uptime is 43 minutes
System returned to ROM by reload at 22:05:12 UTC Sat Jan 5 2008
System image file is "flash:c1841-advipservicesk9-mz.124-10b.bin"

Cisco 1841 (revision 6.0) with 174080K/22528K bytes of memory.
Processor board ID FTX1111W0QF
 6 FastEthernet interfaces
 2 Serial(sync/async) interfaces
 1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```


ipconfig

```
C:\>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:
```




```
    Connection-specific DNS Suffix  . :
```

```
    IP Address. . . . . : 192.168.1.2
```

```
    Subnet Mask . . . . . : 255.255.255.0
```

```
    Default Gateway . . . . . : 192.168.1.254
```

Leyenda

-  Dirección IP para este equipo host
-  Máscara de subred de la red local
-  Dirección del gateway predeterminado para este equipo host

Ejemplo de resultado de `ipconfig` que muestra la dirección del gateway predeterminado

ipconfig /all

```
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:\>
```

ipconfig /displaydns

```
C:\> ipconfig /displaydns
```

```
Windows IP Configuration
```

```
cisco-tags.cisco.com
```

```
-----
```

```
Record Name . . . . . : cisco-tags.cisco.com
```

```
Record Type . . . . . : 1
```

```
Time To Live . . . . . : 44024
```

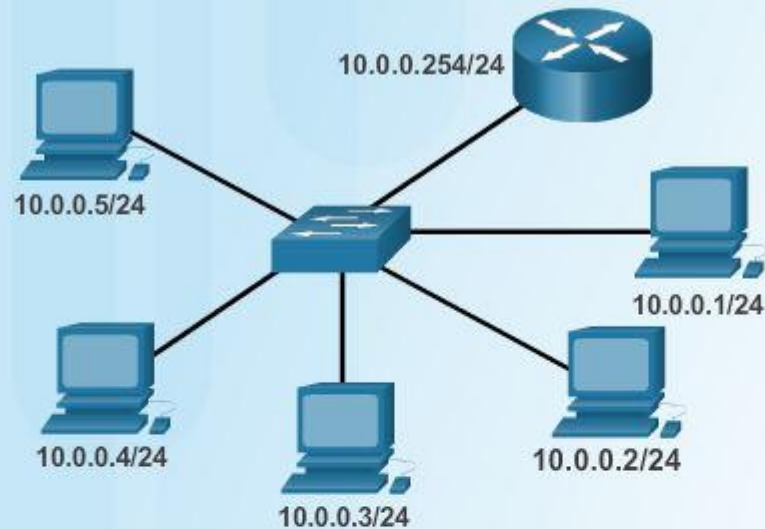
```
Data Length . . . . . : 4
```

```
Section . . . . . : Answer
```

```
A (Host) Record . . . : 72.163.10.10
```

```
<se omitió el resultado>
```

Nociones sobre los nodos de la red



```
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

Examining the 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	Holdtime	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 :
```

```
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M),
```

```
Version 12.4(10b), RELEASE SOFTWARE (fc3)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2007 by Cisco Systems, Inc.
```

```
Compiled Fri 19-Jan-07 15:15 by prod_rel_team
```



```
advertisement version: 2
VTP Management Domain: ''

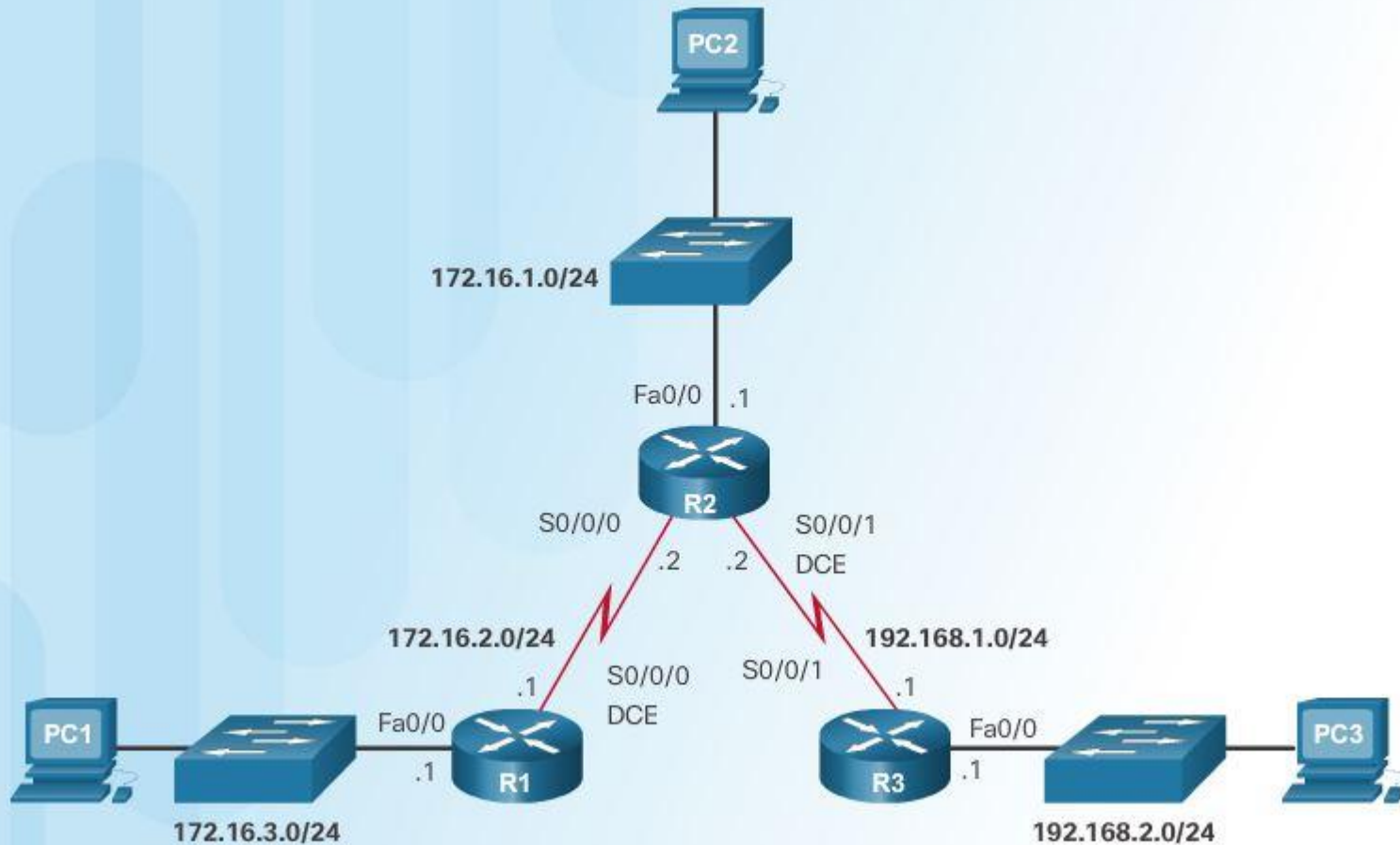
-----
Device ID: S3
Entry address(es):
Platform: cisco WS-C2950-24, Capabilities: Switch IGMP
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/11
Holdtime : 148 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(9)EA1,
RELEASE SOFTWARE (fcl)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 24-Apr-02 06:57 by antonino

advertisement version: 2
Protocol Hello: OUI=0x000000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFFF0
10231FF00000000000000000AB769F6C0FF0000
VTP Management Domain: 'CCNA3'
Duplex: full

R3#
```

Análisis de vecinos CDP



Prueba de interfaz



Interface Testing

R1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.254.254	YES	NVRAM	up	up
FastEthernet0/1	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

R1

S1

Interface Testing

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.254.250	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up

R1

S1

Comando show

Situaciones de comandos show



`show
startup-config`

Sospecha que hay un problema con la configuración actual del switch. Desea ver la configuración guardada, a fin de poder compararla con la que está en ejecución en ese momento.



`show version`

Está hablando por teléfono con el personal de asistencia de Cisco. Le solicitan el nombre del IOS y la RAM, la NVRAM y la memoria flash disponible del switch. También le solicitan la ubicación de arranque en sistema hexadecimal.



`show arp`

Está ejecutando el protocolo de routing EIGRP y necesita saber los intervalos de actualización y qué redes e interfaces activas anuncia el router.



`show ip
protocols`

No puede conectarse a Internet. Necesita saber si el router tiene una ruta a Internet y qué protocolos se utilizan para proporcionar las rutas.



`show ip route`

Debe actualizar la documentación de red. Una enumeración rápida de las direcciones IP de los routers en relación con las direcciones MAC ayudaría a terminar la tarea para fines de registro.



`show ip int
brief`

El dispositivo intermediario más cercano es un switch. Tiene 24 puertos. Desea ver una lista simple de los puertos utilizados, el estado de estos y la dirección IP de la VLAN del switch.

Resultado del comando debug ip icmp

```
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.0.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
*Nov 13 12:56:08.147: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
R1# undebug all
All possible debugging has been turned off
R1#
```

Ejecute el comando para permitir que los mensajes de registro sean enviados a su sesión remota.

```
R1# terminal monitor
```

```
R1#
```

Ejecute los siguientes comandos para la solución de problemas:

- Ejecute el comando debug que supervisará el estado de los mensajes ICMP en el R1.
- Haga ping a un dispositivo con una dirección IP de 10.0.0.10.
- Desconecte todas las depuraciones.

```
R1# debug ip icmp
```

```
R1# ping 10.0.0.10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
*Nov 13 12:56:08.147: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,  
topology BASE, dscp 0 topoid 0
```

```
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,  
topology BASE, dscp 0 topoid 0
```

```
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,  
topology BASE, dscp 0 topoid 0
```

```
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,  
topology BASE, dscp 0 topoid 0
```

```
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,  
topology BASE, dscp 0 topoid 0
```

```
R1# undebug all
```

```
All possible debugging has been turned off
```

```
R1#
```

Utilizó correctamente los comandos terminal monitor y debug para solucionar problemas.

Seis pasos de la metodología de solución de problemas

Paso	Título	Descripción
1	Identificación del problema	El primer paso del proceso de solución de problemas consiste en identificar el problema. Aunque se pueden usar herramientas en este paso, una conversación con el usuario suele ser muy útil.
2	Establecer una teoría de causas probables	Después de hablar con el usuario e identificar el problema, puede probar y establecer una teoría de causas probables. Este paso generalmente permite ver más causas probables del problema.
3	Poner a prueba la teoría para determinar la causa	Según las causas probables, pruebe sus teorías para determinar cuál es la causa del problema. El técnico aplica a menudo un procedimiento rápido para probar y ver si resuelve el problema. Si el problema no se corrige con un procedimiento rápido, quizá deba continuar investigando el problema para establecer la causa exacta.
4	Establecer un plan de acción para resolver el problema e implementar la solución	Una vez que haya determinado la causa exacta del problema, establezca un plan de acción para resolver el problema e implementar la solución.
5	Verificar la funcionalidad total del sistema e implementar medidas preventivas	Una vez que haya corregido el problema, verifique la funcionalidad total y, si corresponde, implemente medidas preventivas.
6	Registrar hallazgos, acciones y resultados	El último paso del proceso de solución de problemas consiste en registrar los hallazgos, las acciones y los resultados. Esto es muy importante para referencia futura.

Prueba de conectividad satisfactoria con el comando ping



```
R1# ping 10.0.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#
```


Rastreo de una ruta hacia el destino con el comando traceroute



```
R1# traceroute 10.3.0.1
Type escape sequence to abort.
Tracing the route to 10.3.0.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.1.0.2 12 msec 12 msec 16 msec
 2 10.2.0.2 24 msec * 24 msec
R1#
```

El comando show ip interface brief

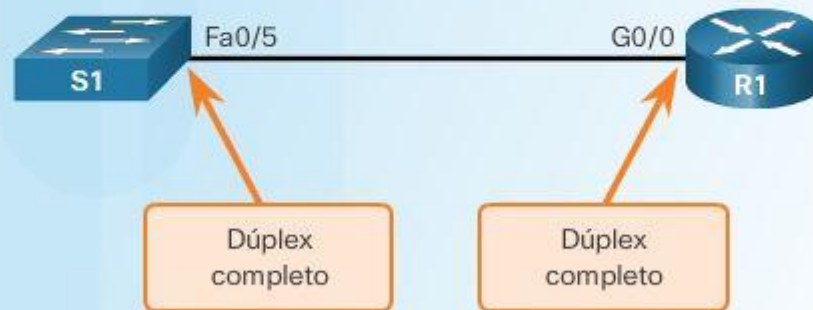


```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	10.0.0.1	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	10.1.0.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down

```
R1#
```

Autonegociación dúplex completo satisfactoria



Topología de diferencia entre dúplex



```
S1#  
*Mar 1 01:01:03.858: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on  
FastEthernet0/5 (not half duplex), with R1 GigabitEthernet0/0 (half duplex).  
*Mar 1 01:01:04.856: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on  
FastEthernet0/5 (not half duplex), with R1 GigabitEthernet0/0 (half duplex).  
*Mar 1 01:01:05.855: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on  
FastEthernet0/5 (not half duplex), with R1 GigabitEthernet0/0 (half duplex).  
S1#
```

Topología de diferencia entre dúplex



```
S1# show interfaces fastethernet 0/5
FastEthernet0/5 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, Auto-speed, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
<se omitió el resultado>
```


Topología de diferencia entre dúplex



```
R1# show interfaces gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0 (bia
fc99.4775.c3e0)
  Internet address is 10.0.0.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
<se omitió el resultado>
```

El comando show ip interface



```
R1# show ip interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 10.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
<se omitió el resultado>
```

El comando ipconfig



```
C:\> ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::fd4c:6609:6733:c5cc%11  
IPv4 Address. . . . . : 10.0.0.10  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.0.0.1
```

```
C:\>
```

Verificación del gateway predeterminado en una PC con Windows



```
C:\> ipconfig

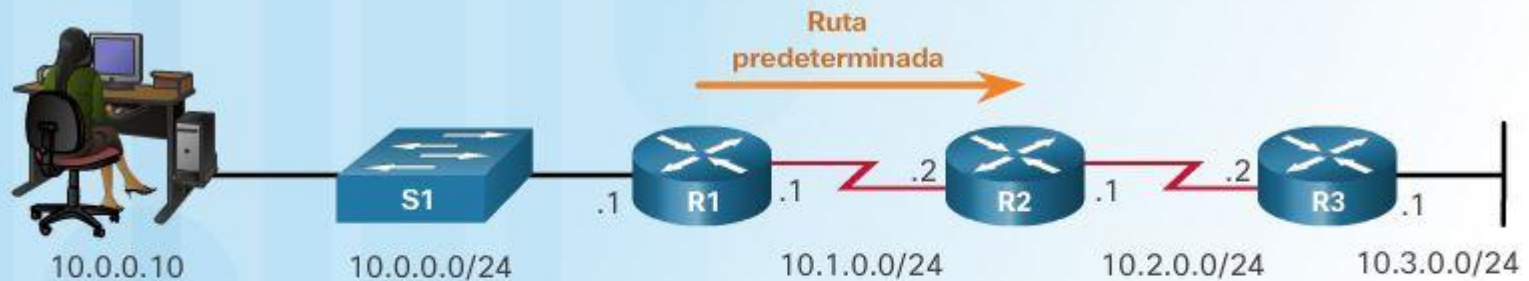
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::fd4c:6609:6733:c5cc%11
    IPv4 Address. . . . . : 10.0.0.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

C:\>
```

Verifique la ruta predeterminada del router



```
R1# show ip route
<se omitió el resultado>

Gateway of last resort is 10.1.0.2 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 10.1.0.2
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C     10.0.0.0/24 is directly connected, GigabitEthernet0/0
L     10.0.0.1/32 is directly connected, GigabitEthernet0/0
C     10.1.0.0/24 is directly connected, Serial0/0/0
L     10.1.0.1/32 is directly connected, Serial0/0/0
R1#
```


Información del servidor DNS en una PC

```
C:\> ipconfig /all
```

```
Ethernet adapter Local Area Connection:
```

```
<se omitió parte del resultado>
```

```
Connection-specific DNS Suffix . :  
Description . . . . . : Realtek PCIe GBE Family Controller  
Physical Address. . . . . : F0-4D-A2-DD-A7-B2  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::449f:c2:de06:ebad%10 (Preferred)  
IPv4 Address. . . . . : 10.0.0.10 (Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : Monday, November 09, 2015 7:49:48 PM  
Lease Expires . . . . . : Thursday, November 19, 2015 7:49:51 AM  
Default Gateway . . . . . : 10.0.0.1  
DHCP Server . . . . . : 10.0.0.1  
DNS Servers . . . . . : 8.8.8.8  
NetBIOS over Tcpip. . . . . : Enabled
```

El comando nslookup

```
C:\> nslookup  
Default Server:  dns-cac-lb-01.rr.com  
Address:  209.18.47.61
```

```
> cisco.com  
Server:  dns-cac-lb-01.rr.com  
Address:  209.18.47.61
```

```
Non-authoritative answer:  
Name:      cisco.com  
Addresses: 2001:420:1101:1::a  
           72.163.4.161
```

```
> quit
```

```
C:\>
```