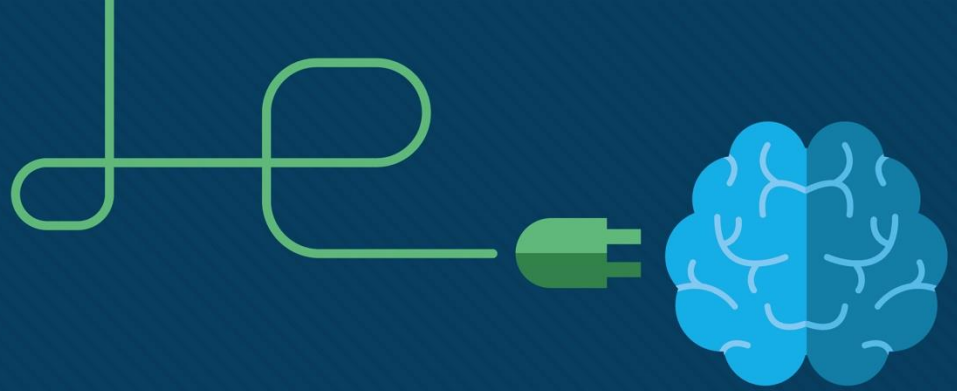


Modulo 9: Resolución de direcciones

Introduction to Networks v7.0
(ITN)

Objetivos

Titulo: Resolución de direcciones

Objetivo: Explicar como ARP y ND permiten la comunicación en una red.

Tema	Objectivo
MAC e IP	Comparar la función de las dirección MAC e IP .
ARP	Describir el próposito de ARP.
Neighbor Discovery	Describir la operación de IPv6 neighbor discovery.

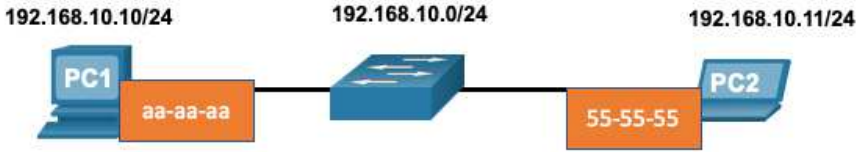
9.1 MAC e IP

Destino en la misma red

Hay dos direcciones principales asignadas a un dispositivo en una LAN Ethernet:

- **Dirección física de capa 2 (MAC)**: se utiliza para las comunicaciones NIC a NIC en la misma red Ethernet.
- **Dirección lógica de capa 3 (IP)**: se utiliza para enviar un paquete desde el dispositivo de origen al dispositivo de destino.

Las direcciones de capa 2 se utilizan para enviar tramas desde una NIC a otra NIC en la misma red. Si una dirección IP de destino está en la misma red, la dirección MAC de destino será la del dispositivo de destino.

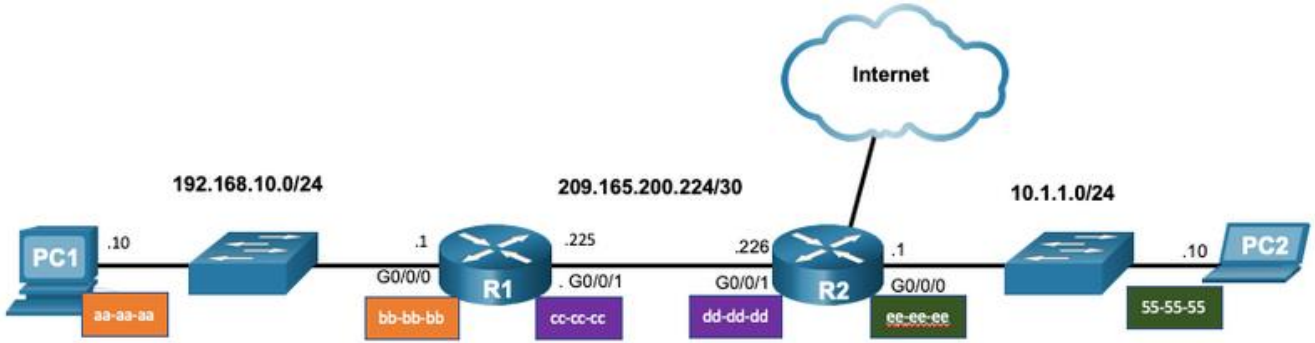


Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

Destino en una red remota

Cuando la dirección IP de destino está en una red remota, la dirección MAC de destino es la de la puerta de enlace predeterminada.

- IPv4 utiliza ARP para asociar la dirección IPv4 de un dispositivo con la dirección MAC de la NIC del dispositivo.
- IPv6 utiliza ICMPv6 para asociar la dirección IPv6 de un dispositivo con la dirección MAC de la NIC del dispositivo.



Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

Packet Tracer – Identifica las direcciones MAC e IP (9.1.3)

En este Packet Tracer, completará los siguientes objetivos:

- Recopilar información de la PDU para la comunicación de la red local
- Recopilar información de la PDU para la comunicación de red remota

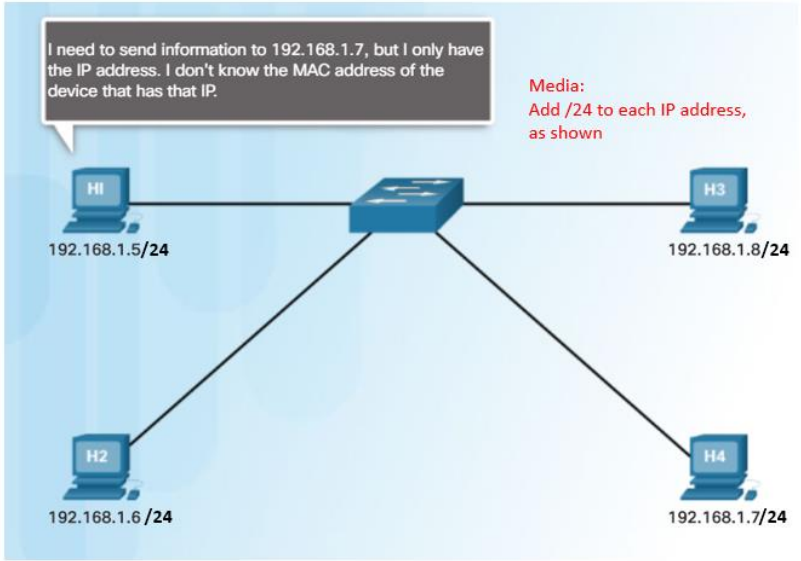
9.2 ARP

Descripción general de ARP

Un dispositivo usa ARP para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4.

ARP realiza dos funciones básicas:

- Resolución de direcciones IPv4 a direcciones MAC
- Mantener una tabla ARP que relaciona las direcciones IPv4 a MAC



Funciones ARP

Para enviar una trama, un dispositivo buscará en su tabla ARP una dirección IPv4 de destino y una dirección MAC correspondiente.

- Si la dirección IPv4 de destino del paquete está en la misma red, el dispositivo buscará en la tabla ARP la dirección IPv4 de destino.
- Si el dispositivo localiza la dirección IPv4, su dirección MAC correspondiente se utiliza como dirección MAC de destino en la trama.
- Si la dirección IPv4 de destino está en una red diferente, el dispositivo buscará en la tabla ARP la dirección IPv4 de la puerta de enlace predeterminada.
- Si no se encuentra ninguna entrada en la tabla ARP, el dispositivo envía una solicitud ARP.

Video - Petición ARP (9.2.3)

Este video presenta el proceso de una solicitud ARP.

Video – Operación ARP Operation – Respuesta ARP (9.2.4)

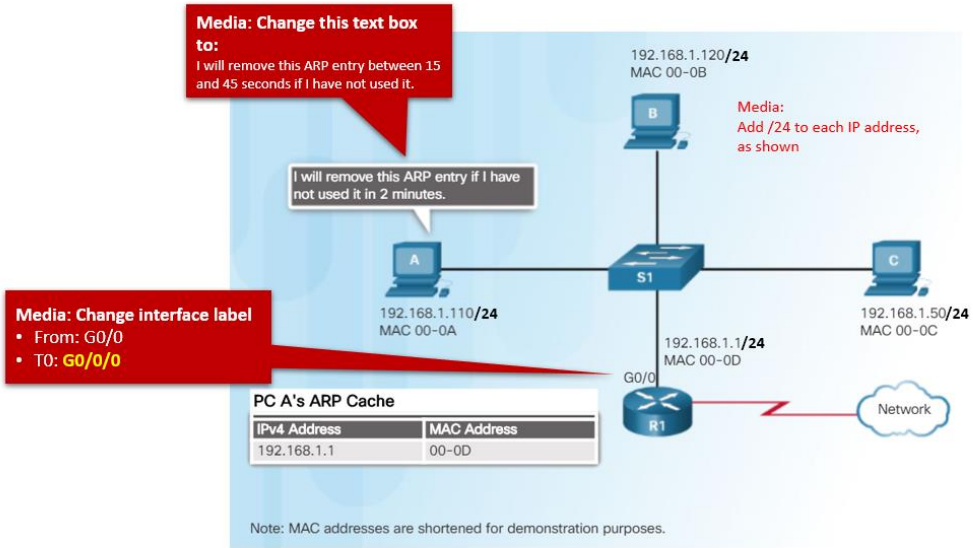
Este video describe como es la respuesta ARP a una solicitud ARP.

Video – El rol de ARP en comunicaciones remotas (9.2.5)

Este video presenta cómo la solicitud ARP proporciona a un host la dirección MAC de la puerta de enlace predeterminada.

Removiendo entradas de un tabla ARP

- Las entradas en la tabla ARP no son permanentes y se eliminan cuando un temporizador de caché ARP expira después de un período de tiempo especificado.
- La duración del temporizador de caché ARP varía según el sistema operativo.
- El administrador también puede eliminar manualmente las entradas de la tabla ARP.



Tablas ARP en dispositivos de red

- El comando **show ip arp** muestra la tabla ARP de un router Cisco.
- El comando **arp –a** muestra la tabla ARP table en una PC Windows 10.

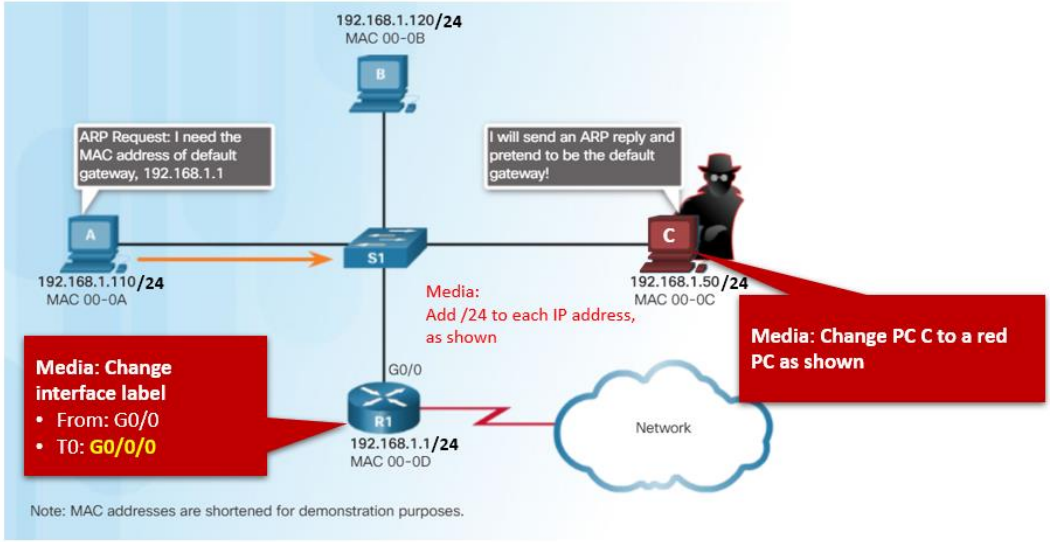
```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
```

```
C:\Users\PC> arp -a

Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
```

Problemas de ARP – Difusión y suplantación ARP

- Todos los dispositivos de la red local reciben y procesan las solicitudes de ARP.
- Las difusiones ARP excesivas pueden causar reducción en el rendimiento.
- Las respuestas ARP pueden ser falsificadas por un actor de amenazas para realizar un ataque de envenenamiento ARP.
- Los conmutadores de nivel empresarial incluyen técnicas de mitigación para proteger contra ataques ARP.



Packet Tracer – Examinado la tabla ARP (9.2.9)

En esta actividad Packet Tracer, se completarán los siguientes objetivos:

- Examinar una solicitud ARP
- Examinar la tabla de direcciones MAC de un conmutador
- Examinar el proceso ARP en comunicaciones remotas

9.3 Detección de vecinos IPv6

Video – Detección de vecinos IPv6 (9.3.1)

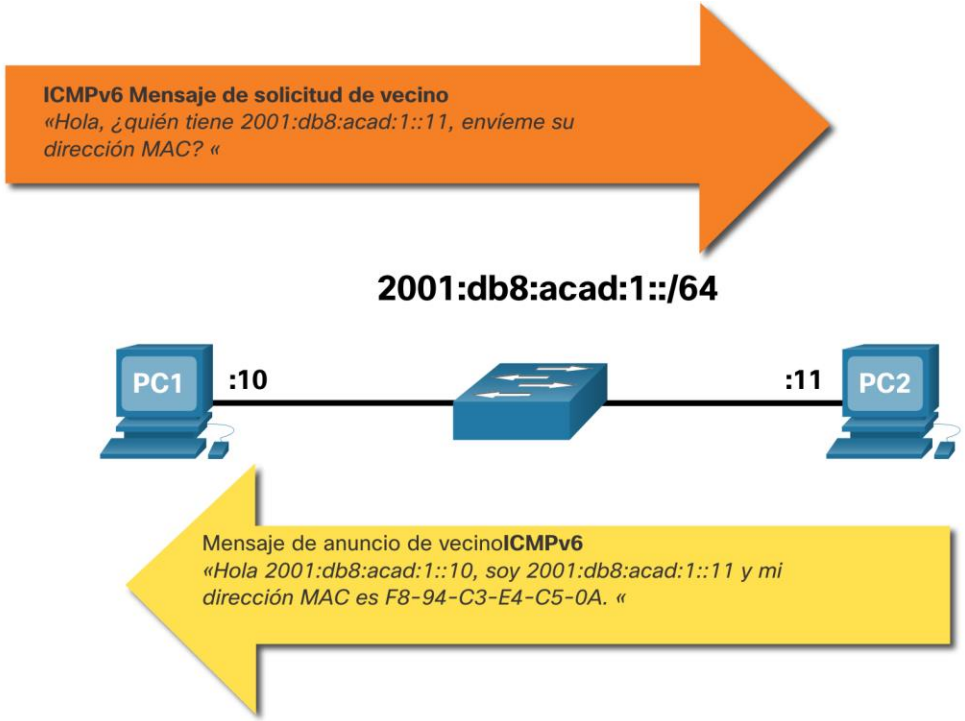
Este video explica el proceso que realiza IPv6 para la resolución de direcciones mediante la solicitud de vecinos ICMPv6 y los mensajes de descubrimiento de vecinos.

Mensajes de descubrimiento de vecinos IPv6

El protocolo IPv6 Neighbor Discovery (ND) proporciona:

- Resolución de direcciones
- Descubrimiento de enrutadores
- Servicios de redireccionamiento
- Los mensajes ICMPv6 de solicitud de vecino (NS) y de anuncio de vecino (NA) se utilizan para la mensajería de dispositivo a dispositivo, como la resolución de direcciones.
- Los mensajes de solicitud de enrutador (RS) y anuncio de enrutador (RA) ICMTPv6 se utilizan para enviar mensajes entre dispositivos y enrutadores para el descubrimiento de enrutadores.
- Los enrutadores utilizan los mensajes de redireccionamiento ICMPv6 para una mejor selección del siguiente salto.

Descubrimiento de vecinos IPv6 - resolución de direcciones



- Los dispositivos IPv6 utilizan ND para resolver la dirección MAC de una dirección IPv6 conocida.
- Los mensajes de solicitud de vecinos ICMPv6 se envían mediante direcciones especiales de multidifusión Ethernet e IPv6.

Packet Tracer – Descubrimiento de vecinos IPv6 (9.3.4)

En esta actividad, se completarán los siguientes objetivos:

- Parte 1: Red local de descubrimiento de vecinos IPv6
- Parte 2: Red remota de descubrimiento de vecinos IPv6

9.4 Módulo de práctica y prueba

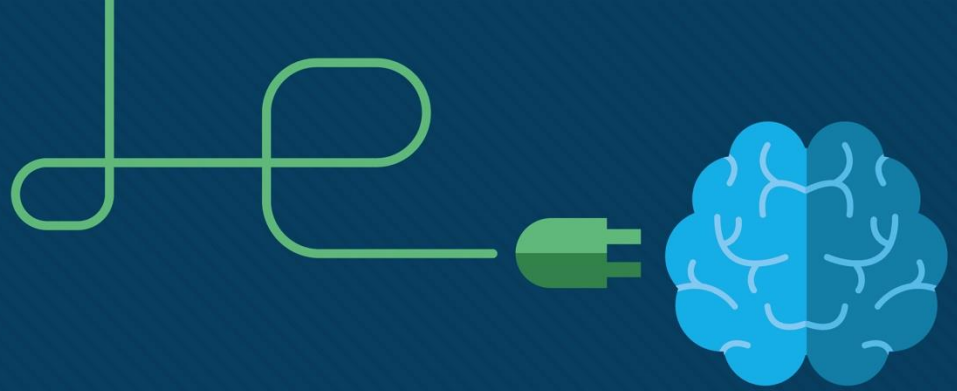
¿Que aprendimos en este módulo?

- Las direcciones físicas de capa 2 (es decir, direcciones MAC de Ethernet) se utilizan para entregar la trama de enlace de datos con el paquete IP encapsulado desde una NIC a otra NIC en la misma red.
- Si la dirección IP de destino está en la misma red, la dirección MAC de destino será la del dispositivo de destino.
- Cuando la dirección IP de destino (IPv4 o IPv6) está en una red remota, la dirección MAC de destino será la dirección de la puerta de enlace predeterminada del host (es decir, la interfaz del enrutador).
- Un dispositivo IPv4 usa ARP para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4.

¿Que aprendimos en este módulo?

- ARP proporciona dos funciones básicas: resolver direcciones IPv4 a direcciones MAC y mantener una tabla de asignaciones de direcciones IPv4 a MAC.
- Una vez recibida la respuesta ARP, el dispositivo agregará la dirección IPv4 y la dirección MAC correspondiente a su tabla ARP.
- Para cada dispositivo, un temporizador de caché ARP elimina las entradas ARP que no se han utilizado durante un período de tiempo específico.
- IPv6 no usa ARP, usa el protocolo ND para resolver direcciones MAC.
- Un dispositivo IPv6 utiliza ICMPv6 Neighbor Discovery para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv6.


CISCO



Módulo 10:
Configuración básica de router

Objectivos del módulo

Título: Configuración básica de router

Objetivo: Definir la configuración inicial del router.

Títilo	Objetivo
Configuración inicial del router	Configuración inicial en el. IOS del router Cisco.
Configuración de Interfaces	Configurar dos interfaces activas en el Cisco IOS.
Configurar el gateway default	Configurar dispotitivos para usar el gateway default.

Paso para la configuración inicial

- Configurar el nombre del dispositivo.

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

- Habilitar seguridad en el modo EXEC.

```
Router(config)# enable secret password
```

- Habilitar seguridad en el modo EXEC de usuario.

```
Router(config)# line console 0
Router(config-line)# password password
Router(config-line)# login
```

- Habilitar seguridad de acceso Telnet / SSH.

```
Router(config)# line vty 0 4
Router(config-line)# password password
Router(config-line)# login
Router(config-line)# transport input {ssh | telnet}
```

- Cifrar contraseñas .

```
Router(config)# service password encryption
```

- Habilitar mensaje de notificación legal.

```
Router(config)# banner motd # message #
Router(config)# end
Router# copy running-config startup-config
```

Ejemplo de configuraicón básica

- Comandos básicos para la configuración del router R1.
- Guardar la configuración en NVRAM.

```
R1(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password encryption
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
**********************************************
WARNING: Unauthorized access is prohibited!
**********************************************
R1(config)# exit
R1# copy running-config startup-config
```

Packet Tracer – Configuración inicial(10.1.4)

En esta actividad de Packet Tracer, se realiza lo siguiente:

- Configurar y verificar la configuración inicial del router.
- Guardar la configuación inicial.

10.2 Configuración de Interfaces

Configuración de interfaces del Router

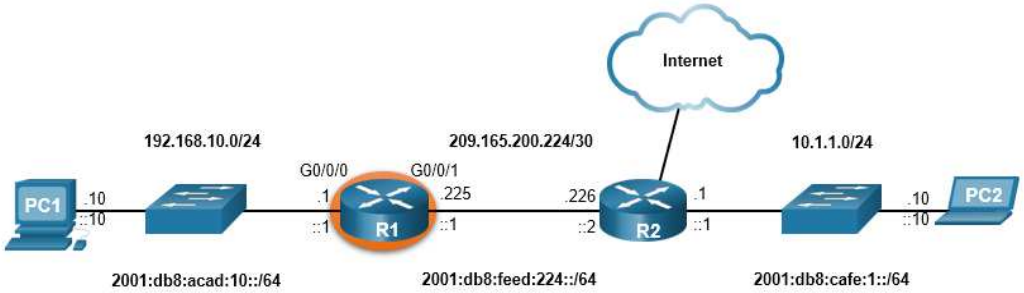
Configurar una interface se deben ejecutar los siguientes comandos:

```
Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-mask
Router(config-if)# ipv6 address ipv6-address/prefix-length
Router(config-if)# no shutdown
```

- E una buena práctica usar el comando **description** para agregar información acerca del dispositivo conectado a la interfaz.
- La interfaz se habilita con el comando **no shutdown.**

Ejemplo de configuración de interfaces

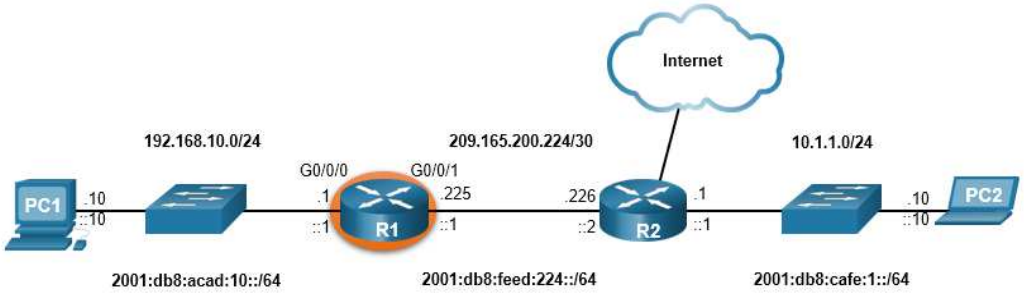
Secuencia de comandos para configurar la interfaz G0/0/0 en R1:




```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# description Link to LAN
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:10::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug  1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Aug  1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Aug  1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
```

Ejemplo de configuración de interfaces (Cont.)

Secuencia de comandos para configurar la interfaz G0/0/1 en R1:




```
R1(config)# interface gigabitEthernet 0/0/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:feed:224::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug  1 01:46:29.170: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Aug  1 01:46:32.171: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Aug  1 01:46:33.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
```

Verificar la configuración de la Interfaz

Para verificar la configuración se utiliza los comandos **show ip interface brief** y **show ipv6 interface brief:**

```
R1#  show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   209.165.200.225 YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

```
R1#  show ipv6 interface brief
GigabitEthernet0/0/0       [up/up]
    FE80::201:C9FF:FE89:4501
    2001:DB8:ACAD:10::1
GigabitEthernet0/0/1       [up/up]
    FE80::201:C9FF:FE89:4502
    2001:DB8:FEED:224::1
Vlan1                      [administratively down/down]
    unassigned
R1#
```

Comandos de verificación

La siguiente tabla resume los comandosd de verificación.

Commands	Description
`show ip interface brief` `show ipv6 interface brief`	Lista todas las interfaces, sus direcciones IP, y su estado actual.
`show ip route` `show ipv6 route`	Lista las tablas de ruteo almacenadas en memoria RAM.
`show interfaces`	Muestras las estadisticas de las interfaces del dispositivo. Solo muestra informaición IPv4.
`show ip interfaces`	Muestra las estadísticas IPv4 para todas las interfaces en el router.
`show ipv6 interfaces`	Muestra las estadísticas IPv9 para todas las interfaces en el router.

Comandos de verificación(Cont.)

Ver el estatus de todas las interfaces con **show ip interface brief** y **show ipv6 interface brief**:

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   209.165.200.225 YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

```
R1# show ipv6 interface brief
GigabitEthernet0/0/0       [up/up]
    FE80::201:C9FF:FE89:4501
    2001:DB8:ACAD:10::1
GigabitEthernet0/0/1       [up/up]
    FE80::201:C9FF:FE89:4502
    2001:DB8:FEED:224::1
Vlan1                      [administratively down/down]
    unassigned
R1#
```

Comandos de verificación(Cont.)

Mostrar el contenido de las tablas de ruteo IP utilizand los comandos **show ip route** y **show ipv6 route** :

```
R1# show ip route
< output omitted>
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

```
R1# show ipv6 route
<output omitted>
C   2001:DB8:ACAD:10::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:10::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:FEED:224::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:FEED:224::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

Comandos de verificación (Cont.)

Display statistics for all interfaces with the **show interfaces** command, as shown here:

```
R1# show interfaces gig0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4321-2x1GE, address is a0e0.af0d.e140 (bia  a0e0.af0d.e140)
  Description: Link to LAN
  Internet address is 192.168.10.1/24
  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 not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:35, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (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
     1180 packets input, 109486 bytes, 0 no buffer
     Received 84 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles

<output omitted>

R1#
```

Comandos de verificación (Cont.)

Mostrar información IPv4 para las interfaces del router utilizando **show ip interface**:

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  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 Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled

<output omitted>

R1#
```

Comandos de verificación (Cont.)

Mostrar información IPv6 **show ipv6 interface**:

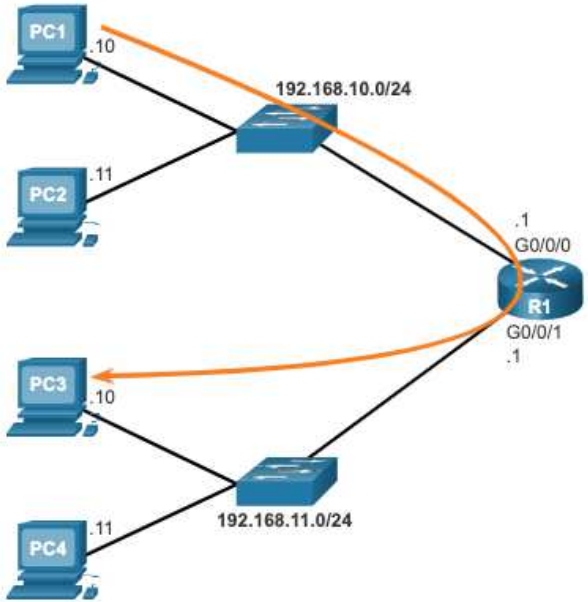
```
R1# show ipv6 interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::868A:8DFF:FE44:49B0
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:10::1, subnet is 2001:DB8:ACAD:10::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF44:49B0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds

R1#
```

10.3 Configuración de puerta de enlace predeterminada.

Configuración de puerta de enlace predeterminada
Host

- La puerta de enlace predeterminada se utiliza cuando un host envía un paquete a un dispositivo en otra red.
- La dirección de la puerta de enlace predeterminada es generalmente la dirección de la interfaz del enrutador adjunta a la red local del host.
- Para llegar a la PC3, la PC1 direcciona un paquete con la dirección IPv4 de la PC3, pero reenvía el paquete a su puerta de enlace predeterminada, la interfaz G0/0/0 de R1.



Nota: La dirección IP del host y la interfaz del enrutador deben estar en la misma red.

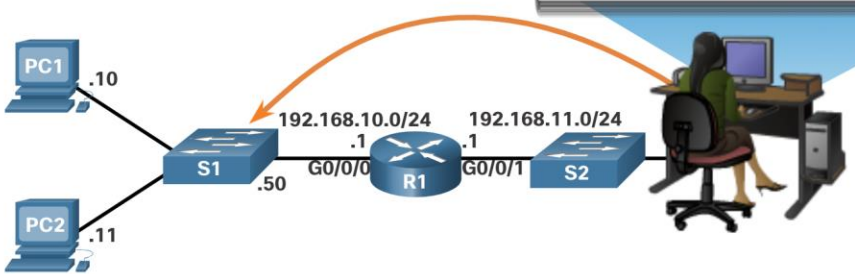
Configuración de puerta de enlace predeterminada
Switch

- Un conmutador debe tener una dirección de puerta de enlace predeterminada configurada para administrar de forma remota el conmutador desde otra red.
- Para configurar una puerta de enlace predeterminada IPv4 en un conmutador, en modo de configuación global utilice **ip default-gateway** *ip-address*

```
S1# configure terminal

S1(config)# ip default-gateway 192.168.10.1
```

```
S1# show running-config
Building configuration...
!
<Output Omitted>
service password-encryption
!
hostname S1
!
interface Vlan1
  ip address 192.168.10.50.255.255.255.0
!
<Resultado omitido>
!
ip default-gateway 192.168.10.1
<Resultado omitido>
```



Packet Tracer – Conexión de un router a la LAN (10.3.4)

En este Packet Tracer, hará lo siguiente:

- Mostrar la información del enrutador.
- Configurar las interfaces del enrutador.
- Verificar la configuración.

Packet Tracer – Solución de problemas

En este Packet Tracer, hará lo siguiente:

- Verificar la documentación de la red y utilizar pruebas para aislar problemas.
- Determinar una solución adecuada para el problema determinado.
- Implementa la solución.
- Verificar que el problema esté resuelto.
- Documentar la solución.

10.4 Práctica del módulo y cuestionario

Video – Diferencias de dispositivos de red: Parte 1 (10.4.1)

Este video cubrirá las diferentes configuraciones de los siguientes dispositivos:

- Cisco 4000 Series Router.
- Cisco 2900 Series Router.
- Cisco 1900 Series Router.

Video – Diferencias de dispositivos de red: Parte 2 (10.4.1)

Este video cubrirá las diferentes configuraciones de los siguientes dispositivos:

- Cisco 4000 Series Router.
- Cisco 2900 Series Router.
- Cisco 1900 Series Router.

Packet Tracer – Configuración básica de dispositivos (10.4.3)

En este Packet Tracer, hará lo siguiente:

- Completar la documentación de la red.
- Realizar configuraciones básicas de dispositivos en un router y un switch.
- Verificar la conectividad y solucionar problemas.

Lab – Armar una red con Switch y un Router

En este laboratorio, completará los siguientes objetivos:

- Configurar la topología e inicializar los dispositivos.
- Configurar dispositivos y verificar la conectividad.
- Mostrar la información del dispositivo.

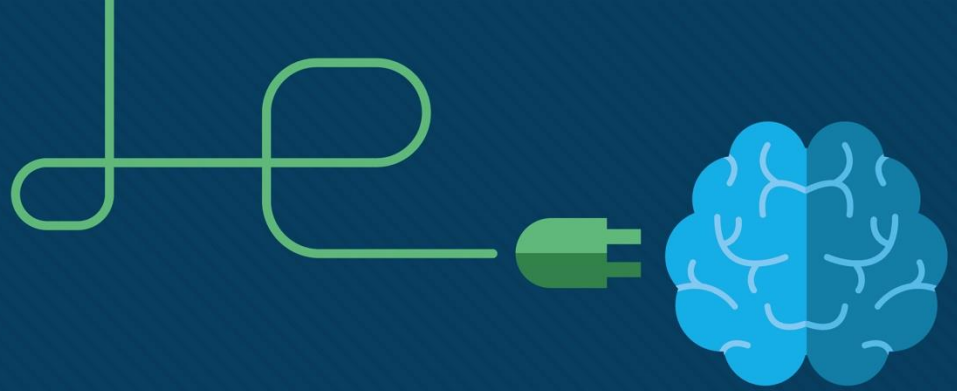
¿Qué aprendimos en el módulo?

- Las tareas que deben completarse al configurar los ajustes iniciales en un enrutador.
  - Configure el nombre del dispositivo.
  - Modo EXEC privilegiado seguro.
  - Modo EXEC de usuario seguro.
  - Asegure el acceso remoto Telnet / SSH.
  - Asegure todas las contraseñas en el archivo de configuración.
  - Proporcionar notificación legal.
  - Guarde la configuración.
- Para que los enrutadores sean accesibles, las interfaces del enrutador deben estar configuradas.
  - Usar el comabdo **no shutdown** para activar la interfaz. La interfaz dede estar conectado a otro dispositivo, como un switch o router. Hay muchos comoandos disponibles para verificar la configuración: **show ip interface brief, show ipv6 interface brief**, **show ip route, show ipv6 route**, así como **show interfaces**, **show ip interface** y **show ipv6 interface.**

¿Qué aprendimos en el módulo?

- Para que un dispositivo final llegue a otras redes, se debe configurar una puerta de enlace predeterminada.
  - La dirección IP del dispositivo host y la dirección de la interfaz del router deben estar en la misma red.
- Un conmutador debe tener una dirección de puerta de enlace predeterminada configurada para poder administrar de forma remota el conmutador desde otra red.
  - Para configurar una puerta de enlace predeterminada IPv4 en un conmutador, utilice el comando de configuración global **ip default-gateway** *ip-address*.


CISCO



Modulo 11: Direccionamiento IPv4

Introduction to Networks v7.0
(ITN)

Objetivos

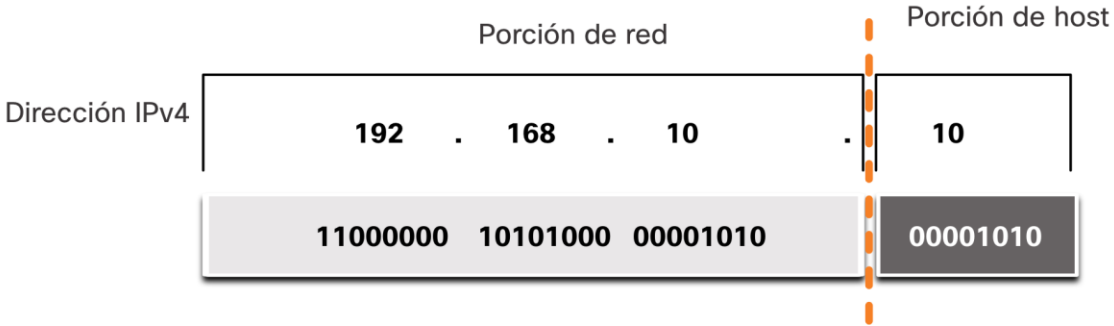
Calcular un esquema de direccionamiento IPv4 para segmentar una red de manera eficiente.

Tema	Objetivo
Estructura IPv4	Describir la estructura de una dirección IPv4, incluida la parte de la red, la parte del host y la máscara de subred.
IPv4 Unicast, Broadcast y Multicast	Comparar las características y usos de las direcciones IPv4 de unicast, broadcas y multicas.
Tipos IPv4 Addresses	Explicar las direcciones IPv4 públicas, privadas y reservadas.
Segmentación de red	Explicar cómo la división en subredes segmenta una red para permitir una mejor comunicación.
Subnetting IPV4	Calcular subredes IPv4 para un prefijo / 24.

11.1 Estructura IPv4

Porciónes de Red y Host

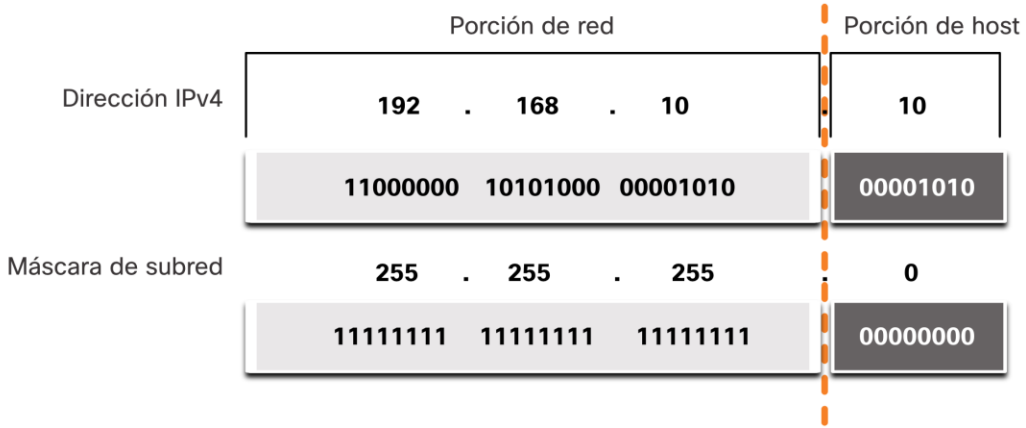
- Una dirección IPv4 es una dirección jerárquica de 32 bits que se compone de una parte de red y una parte de host.
- Al determinar la parte del host, debe observar el flujo de 32 bits.
- Se utiliza una máscara de subred para determinar las partes de la red y del host.



La máscara de subred

- Para identificar la porción red y host de una dirección IPv4, la máscara de subred se compara con la dirección IPv4 bit por bit, de izquierda a derecha.

- El proceso real utilizado para identificar las porciones de red y del host se denomina AND.



La longitud del prefijo

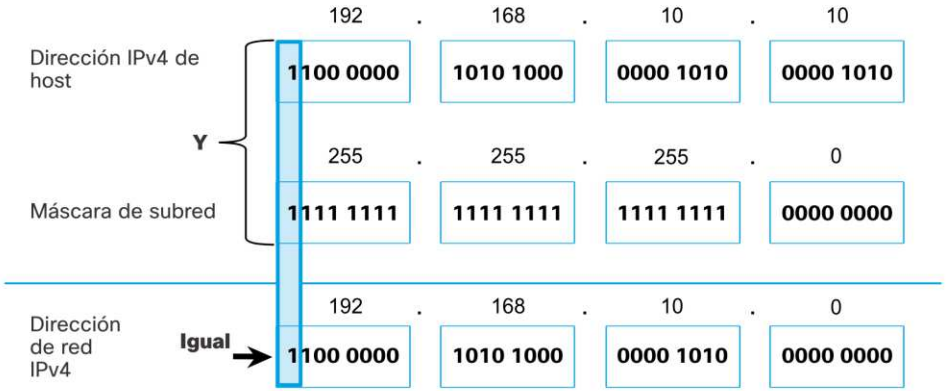
- La longitud de un prefijo es un método más simple que se utiliza para expresar una dirección de máscara de subred.
- La longitud del prefijo es el número de bits en 1 en la máscara de subred.
- Se escrobe en “notación de diagonal(slash)”. Se cuenta el número de bits en la máscara de subred y se antepone una diagonal (/).

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.1111110**1**.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Determinando la Red : AND Lógico

- Se utiliza una operación lógica AND booleana para determinar la dirección de red.
- AND lógico es la comparación de dos bits donde solo un 1 AND 1 produce un 1 y cualquier otra combinación da como resultado un 0.
- 1 AND 1 = 1, 0 AND 1 = 0, 1 AND 0 = 0, 0 AND 0 = 0
- 1 = Verdadero y 0 = Falso

- Para identificar la dirección de red, se realiza un AND lógico, bit a bit, con la máscara de subred y la dirección IPv4 del host.



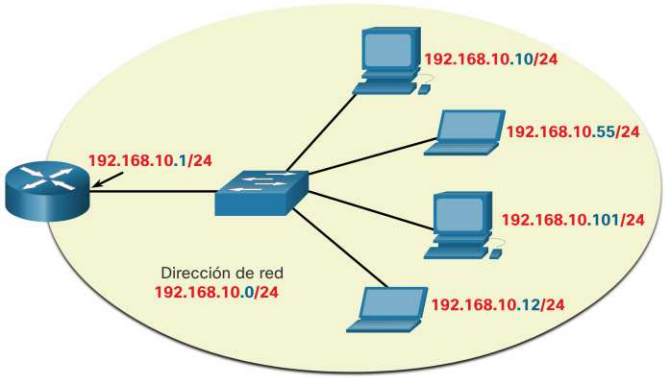
Video – Direcciones de red, host y broadcast

Este video describelo siguiente:

- Dirección de red
- Dirección de broadcast
- Primer host utilizable
- Último host utilizable

Direcciones de red, host y broadcast

- En una red exiten tres tipo de direcicones IP:
  - Dirección de red
  - Direcciónd e host
  - Dirección de broadcast

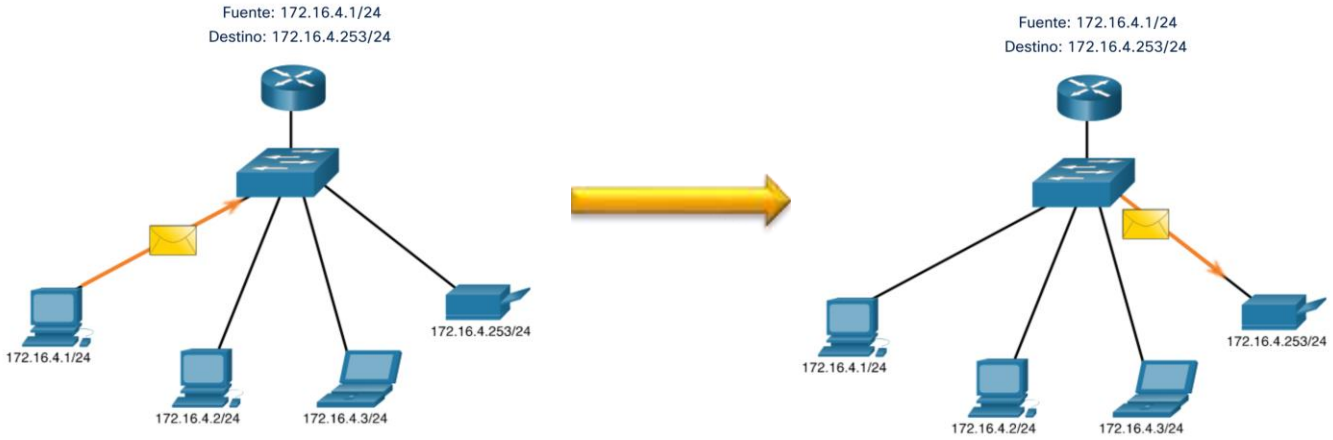


	Porción de red			Porción del host	Bits del host
Subnet mask **255.255.255.**0 or **/24**	255 11111111	255 11111111	255 11111111	0 00000000	
Network address **192.168.10.**0 or **/24**	192 11000000	168 10100000	10 00001010	0 00000000	Todos 0s
First address **192.168.10.**1 or **/24**	192 11000000	168 10100000	10 00001010	1 00000001	Todos 0s y un 1
Last address **192.168.10.**254 or **/24**	192 11000000	168 10100000	10 00001010	254 11111110	Todos 1s y un 0
Broadcast address **192.168.10.**255 or **/24**	192 11000000	168 10100000	10 00001010	255 11111111	Todos 1

11.2 IPv4 Unicast, Broadcast, y Multicast

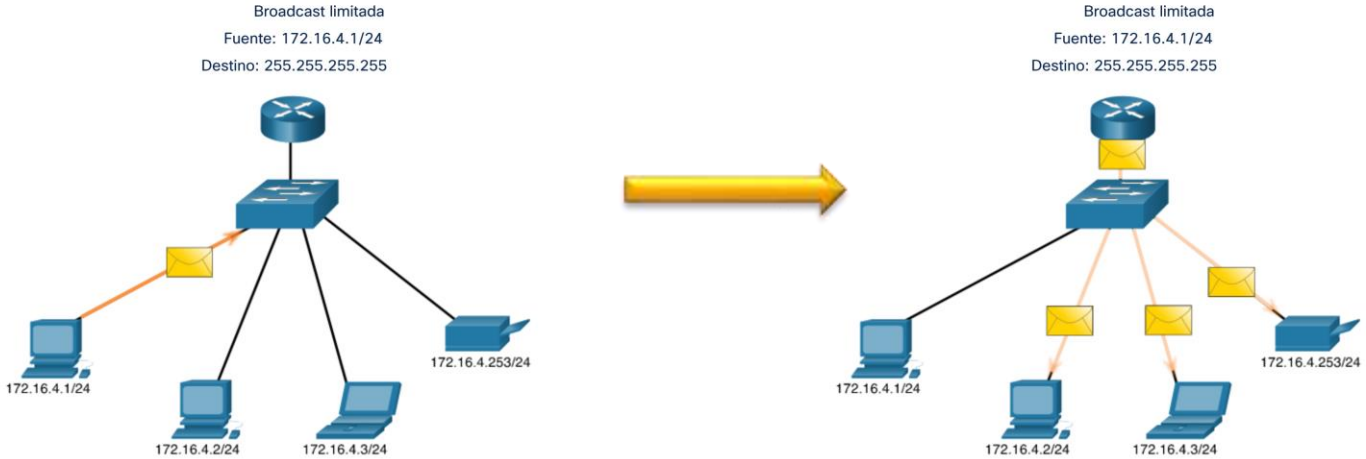
Unicast

- La transmisión unicast se envian un paquete a una dirección IP de destino.
- Por ejemplo, la PC 172.16.4.1 envía un paquete unicast a la impresora en 172.16.4.253.



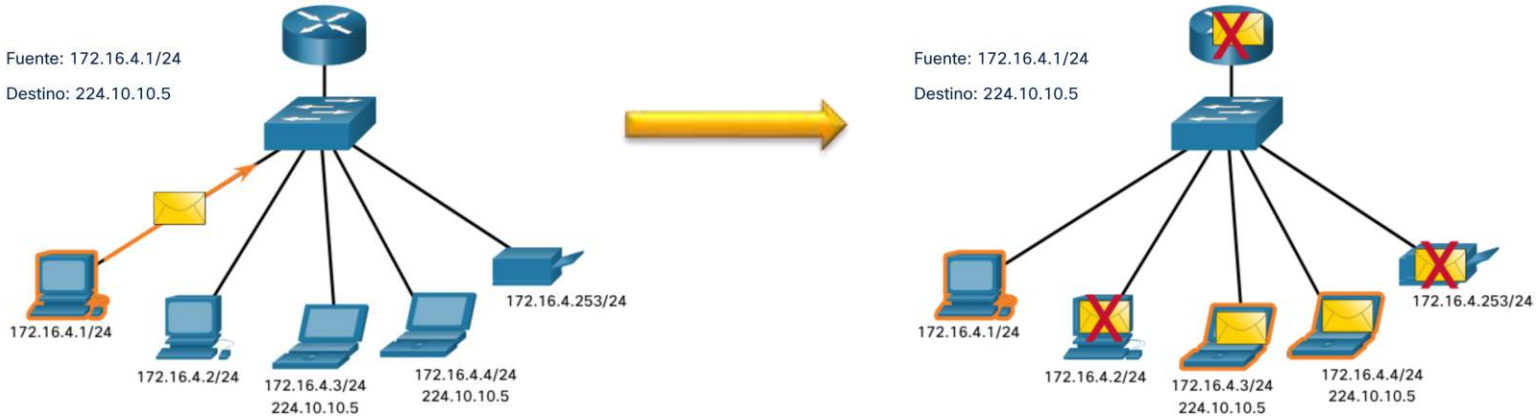
Broadcast

- La transmisión boradcast envia un paquete a todas las demás direcciones IP de destino.
- Por ejemplo, la PC e 172.16.4.1 envía un paquete broadcast a todos los hosts IPv4.



Multicast

- Multicast envia un paquete a un grupo de direcciones de multidifusión.
- Por ejemplo, la PC en 172.16.4.1 envía un paquete de multicast a la dirección del grupo 224.10.10.5.



11.3 Tipos de direcciones IPv4

Dirección IP públicas y privadas

- Como se define en RFC 1918, las direcciones IPv4 públicas se enrutan globalmente entre los enrutadores del proveedor de servicios de Internet (ISP).

- Las direcciones privadas son bloques comunes de direcciones que utilizan la mayoría de las organizaciones para asignar direcciones IPv4 a hosts internos.

- Las direcciones IPv4 privadas no son únicas y pueden usarse internamente dentro de cualquier red.

Dirección de red y prefijo	Rango de direcciones privadas (RFC 1918)
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

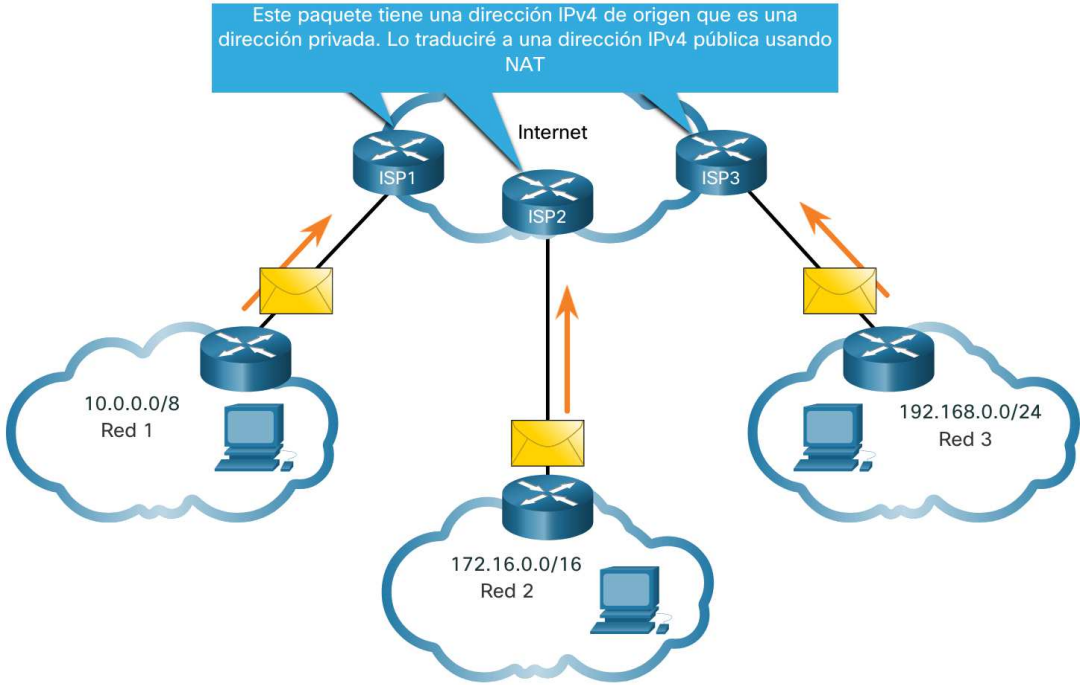
- Las direcciones privadas no son globalmente enrutables.

Enturando a Internet

- La traducción de direcciones de red (NAT) traduce las direcciones IPv4 privadas en direcciones IPv4 públicas.

- Normalmente, NAT se habilita en el router de frontera que se conecta a Internet.

- Traduce la dirección privada interna a una dirección IP pública global.



Uso especial de direcciones IPv4

Direcciones Loopback

- 127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)
- Comunmente solo se utiliza 127.0.0.1
- Se utiliza para probar si TCP/IP está habilitado.

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

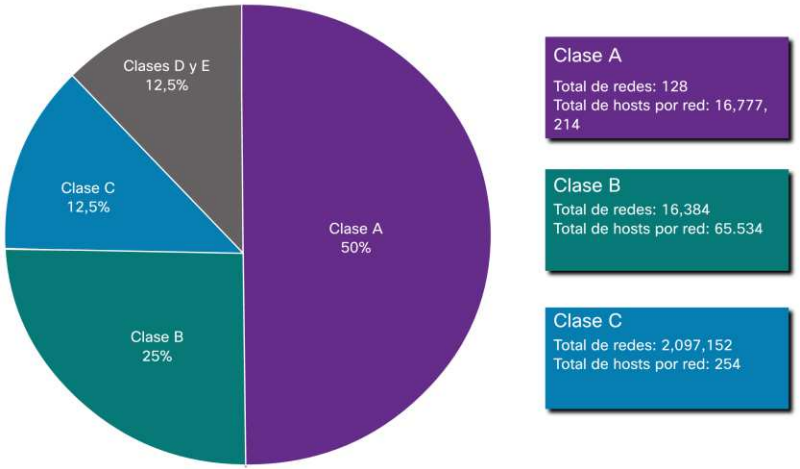
Direcciones Link-Local

- 169.254.0.0 /16 (169.254.0.1 to 169.254.255.254)
- Comúnmente conocidas como direcciones IP privadas automáticas (APIPA) o direcciones autoasignadas.
- Lo utilizan los clientes DHCP de Windows para autoconfigurarse cuando no hay servidores DHCP disponibles.

Direccionamiento con clase heredado

RFC 790 (1981) asignaba las direcciones IPv4 en clases

- Clase A (0.0.0.0/8 to 127.0.0.0/8)
- Clase B (128.0.0.0 /16 – 191.255.0.0 /16)
- Clase C (192.0.0.0 /24 – 223.255.255.0 /24)
- Clase D (224.0.0.0 to 239.0.0.0)
- Clase E (240.0.0.0 – 255.0.0.0)



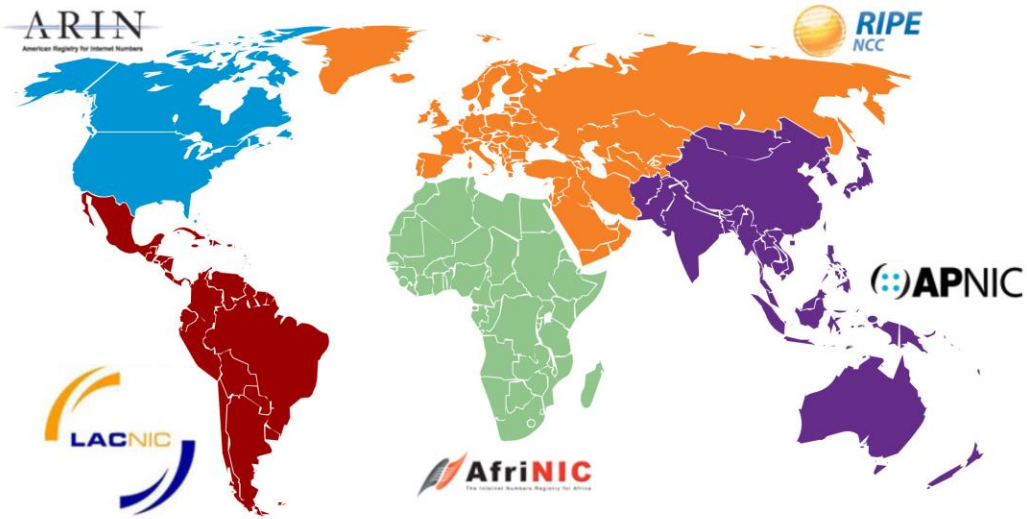
- Se desperdiciaban deirecciones IPv4.

La asignación de direcciones con clase se reemplazó por direcciones sin clases que ignoran las reglas de las clases (A, B, C).

Asignación de direcciones IP

- La Internet Assigned Numbers Authority (IANA) maneja y asigna los bloques de direcciones IPv4 e IPv6 en 5 Regional Internet Registries (RIRs).

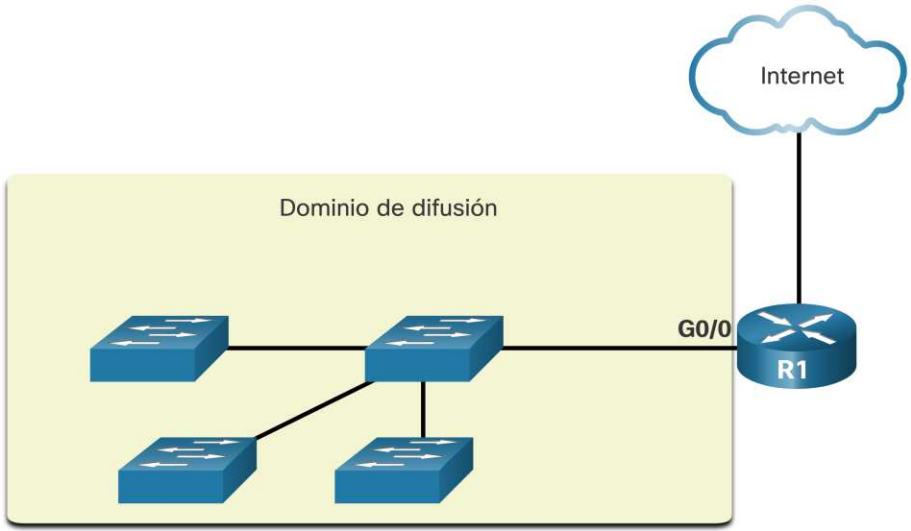
- Los RIR son responsables de asignar direcciones IP a los ISP que proporcionan bloques de direcciones IPv4 a ISP y organizaciones más pequeñas.



11.4 Segmentación de redes

Dominio de Broadcast y Segmentación

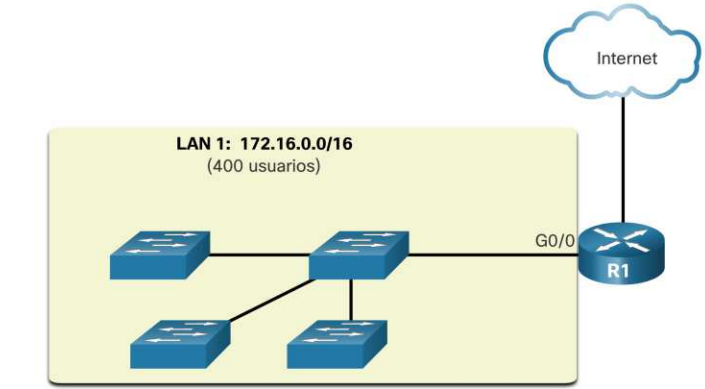
- Muchos protocolos utilizan broadcas o multicast (p. Ej., ARP utiliza broadcast para localizar otros dispositivos, los hosts hacen broadcast de descubrimiento DHCP para localizar un servidor DHCP).
- Los conmutadores hacen broadcast a todas las interfaces excepto la interfaz en la que recibieron.

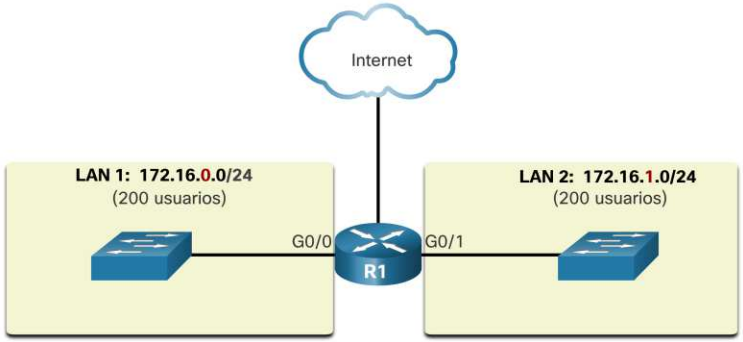


- El único dispositivo que detiene el boradcasts es un routerr.
- Los enrutadores no propagan los mensages broadcast.
- Cada interfaz del roeuter se conecta a un dominio de broadcast y los mensajes broadcast solo se propagan dentro de ese dominio de específico.

Problemas de dominios de Broadcast grandes

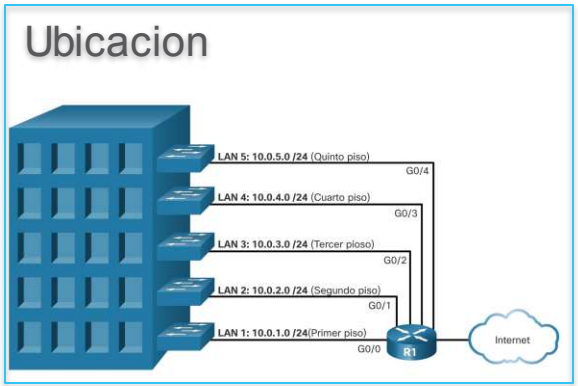
- Un problema con un dominio de difusión grande es que estos hosts pueden generar difusión excesiva y afectar negativamente a la red.
- La solución es reducir el tamaño de la red para crear dominios de difusión más pequeños en un proceso llamado división en subredes (subnetting).
- Dividiendo la dirección de red 172.16.0.0 / 16 en dos subredes de 200 usuarios cada una: 172.16.0.0 / 24 y 172.16.1.0 / 24.
- Las transmisiones solo se propagan dentro de los dominios de transmisión más pequeños.

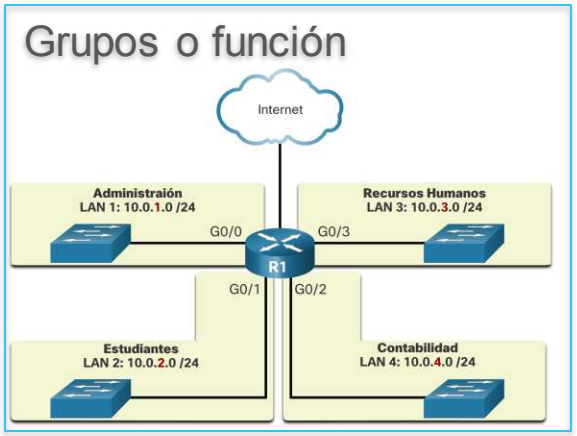




Razones para la segmentación de redes

- La división en subredes reduce el tráfico general de la red y mejora el rendimiento.
- Se puede utilizar para implementar políticas de seguridad entre subredes.
- La división en subredes reduce la cantidad de dispositivos afectados por el tráfico de transmisión anormal.
- Las subredes se utilizan por una variedad de razones, incluidas las siguientes:





11.5 División de subredes en una red IPv4

Subred en el límite de octeto

- Las redes se dividen más fácilmente en subredes en el límite de octetos de / 8, / 16 y / 24.
- Tenga en cuenta que el uso de longitudes de prefijo más largas reduce la cantidad de hosts por subred.

Longitud del prefijo	Máscara de subred	Máscara de subred en binario (n=network, h=host)	# de hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Subred en el límite de octeto (Cont.)

- En la primera tabla, 10.0.0.0/8 está dividido en subredes usando /16 y en la segunda tabla, una máscara / 24.

Direcciones de red (256 subredes)	**Rango del host** (65,534 hosts por red)	**Broadcast**
10.0.0.0/**16**	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0/**16**	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**.0.1 - **10.3**.255.254	**10.3**.255.255
10.4.0.0/**16**	**10.4**.0.1 - **10.4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 - **10.6**.255.254	**10.6**.255.255
10.7.0.0/**16**	**10.7**.0.1 - **10.7**.255.254	**10.7**.255.255
…	…	…
10.255.0.0/**16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Direccioens de red (65,536 redes)	**Rango del hosts** (254 por red)	**Broadcast**
10.0.0.0/**24**	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0/**24**	**10.0.1**.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255
…	…	…
10.0.255.0/**24**	**10.0.255**.1 - **10.0.255**.254	**10.0.255**.255
10.1.0.0/**24**	**10.1.0**.1 - **10.1.0**.254	**10.1.0**.255
10.1.1.0/**24**	**10.1.1**.1 - **10.1.1**.254	**10.1.1**.255
10.1.2.0/**24**	**10.1.2**.1 - **10.1.2**.254	**10.1.2**.255
…	…	…
10.100.0.0/**24**	**10.100.0**.1 - **10.100.0**.254	**10.100.0**.255
…	…	…
10.255.255.0/**24**	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

Subred en el límite de octeto

- Consulte la tabla para ver seis posibles formas de dividir en subredes una red /24.

Longitud del prefijo	Máscara de subred	Máscara de subred en binario (n = network, h = host)	# de subredes	# de hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

Video – La máscara de subred(11.5.3)

- Este video muestra el proceso de división en subredes.

Video – Subred con el número mágico(11.5.4)

- Este video muestra la división en subredes con el número mágico.

Packet Tracer – División de una red IPv4 (11.5.5)

En este Packet Tracer, hará lo siguiente:

- Diseñar un esquema de subredes de red IPv4
- Configurar los dispositivos
- Probar y solucionar problemas de la red

11.6 División de redes con prefijo /16 y /8

Crear subredes con longitud de prefijo 16

- La tabla muestra los escenarios posibles para dividir en subredes un prefijo / 16.

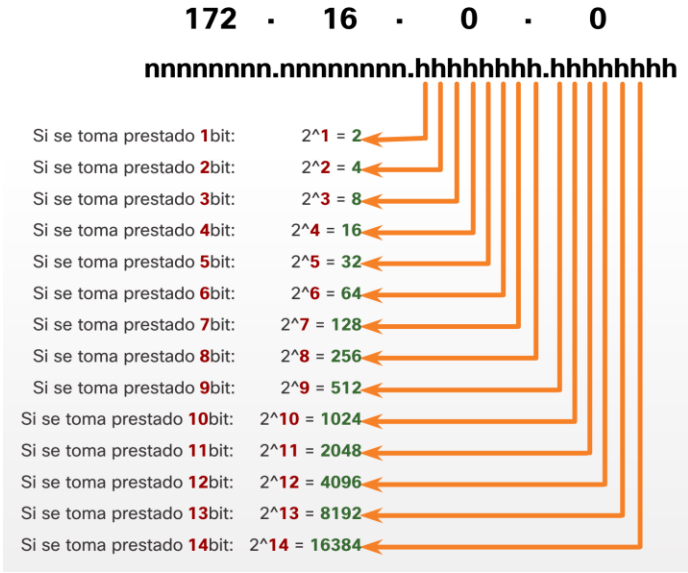
Longitud del prefijo	Máscara de subred	Dirección de red (n = network, h = host)	# de subredes	# de hosts
/17	255.255.**128**.0	nnnnnnnn.nnnnnnnn.**n**hhhhhhh.hhhhhhhh 11111111.11111111.**1**0000000.00000000	**2**	32766
/18	255.255.**192**.0	nnnnnnnn.nnnnnnnn.**nn**hhhhhh.hhhhhhhh 11111111.11111111.**11**000000.00000000	**4**	16382
/19	255.255.**224**.0	nnnnnnnn.nnnnnnnn.**nnn**hhhhh.hhhhhhhh 11111111.11111111.**111**00000.00000000	**8**	8190
/20	255.255.**240**.0	nnnnnnnn.nnnnnnnn.**nnnn**hhhh.hhhhhhhh 11111111.11111111.**1111**0000.00000000	**16**	4094
/21	255.255.**248**.0	nnnnnnnn.nnnnnnnn.**nnnnn**hhh.hhhhhhhh 11111111.11111111.**11111**000.00000000	**32**	2046
/22	255.255.**252**.0	nnnnnnnn.nnnnnnnn.**nnnnnn**hh.hhhhhhhh 11111111.11111111.**111111**00.00000000	**64**	1022
/23	255.255.**254**.0	nnnnnnnn.nnnnnnnn.**nnnnnnn**h.hhhhhhhh 11111111.11111111.**1111111**0.00000000	**128**	510
/24	255.255.**255.0**	nnnnnnnn.nnnnnnnn.**nnnnnnnn**.hhhhhhhh 11111111.11111111.**11111111**.00000000	**256**	254
/25	255.255.**255.128**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.n**hhhhhhh 11111111.11111111.**11111111.1**0000000	**512**	126
/26	255.255.**255.192**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nn**hhhhhh 11111111.11111111.**11111111.11**000000	**1024**	62
/27	255.255.**255.224**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnn**hhhhh 11111111.11111111.**11111111.111**00000	**2048**	30
/28	255.255.**255.240**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnn**hhhh 11111111.11111111.**11111111.1111**0000	**4096**	14
/29	255.255.**255.248**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnn**hhh 11111111.11111111.**11111111.11111**000	**8192**	6
/30	255.255.**255.252**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnnn**hh 11111111.11111111.**11111111.111111**00	**16384**	2

Crear 100 subredes con una red de prefijo /16

Considere una gran empresa que requiere al menos 100 subredes y ha elegido la dirección privada 172.16.0.0/16 como su dirección de red interna.

- La figura muestra la cantidad de subredes que se pueden crear al tomar prestados bits del tercer y cuarto octeto.
- Observe que ahora hay hasta 14 bits de host que se pueden tomar prestados (es decir, los dos últimos bits no se pueden tomar prestados).

Para satisfacer el requisito de 100 subredes para la empresa, se necesitarían tomar prestados 7 bits (es decir, 2^7 = 128 subredes, para un total de 128 subredes).

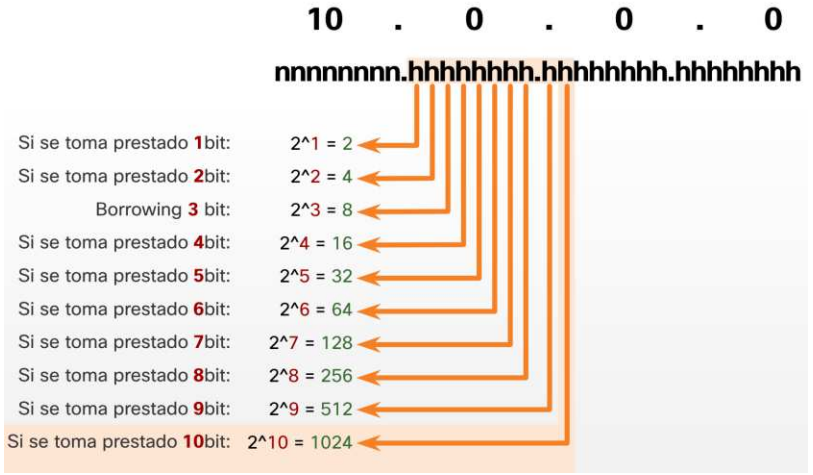


Crear 1000 redes con una red de prefijo 8

Considere un ISP pequeño que requiere 1000 subredes para sus clientes que usan la dirección de red 10.0.0.0/8, lo que significa que hay 8 bits en la porción de red y 24 bits de host disponibles para tomar prestados para la división en subredes.

- La figura muestra la cantidad de subredes que se pueden crear al tomar prestados bits del segundo y tercer octeto.
- Observe que ahora hay hasta 22 bits de host que se pueden tomar prestados.

Para satisfacer el requisito de 1000 subredes para la empresa, se necesitarían tomar prestados 10 bits (es decir, 2^{10} = 1024 subredes, para un total de 1024 subredes)



Video – División en varios octetos (11.6.4)

Este video muestra el proceso de creación de subredes en varios octetos.

Lab – Calcular subredes IPv4

En esta práctica de laboratorio, completará los siguientes objetivos:

- Parte 1: Determinar la división en subredes de direcciones IPv4
- Parte 2: Calcular la división en subredes de direcciones IPv4

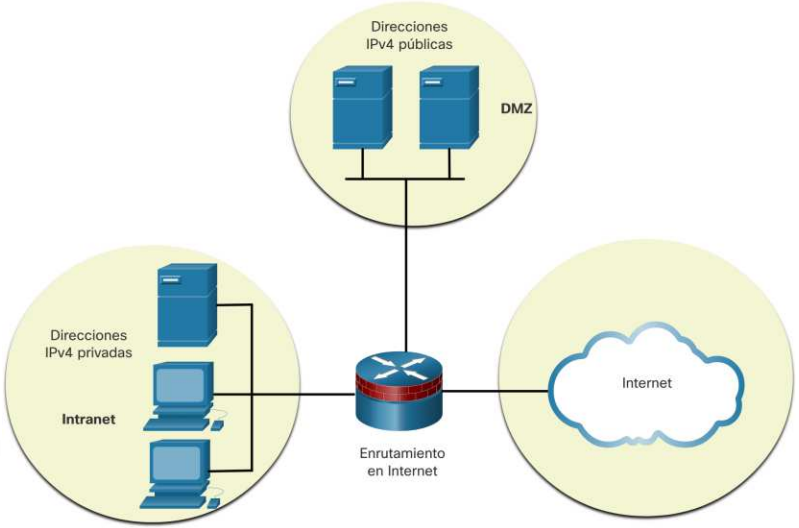
11.7 División en subredes para cumplir requerimientos

Espacio de direcciones IPv4 privado de subred frente al espacio público

Las redes empresariales tendrán:

- Intranet: red interna de una empresa que suele utilizar direcciones IPv4 privadas.
- DMZ - Servidores conectados a Internet de una empresa. Los dispositivos en la DMZ utilizan direcciones IPv4 públicas.
- Una empresa podría utilizar 10.0.0.0/8 y hacer subnetting en de una red /16 o /24.

Los dispositivos DMZ tendrían que configurarse con direcciones IP públicas.



División en subredes para cumplir requerimientos
Minimizar las direcciones de host no utilizables y maximizar el número de subredes

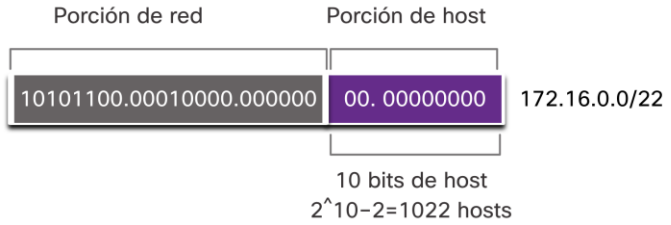
Hay dos consideraciones al planificar subredes:

- El número de direcciones de host necesarias para cada red.
- La cantidad de subredes individuales necesarias

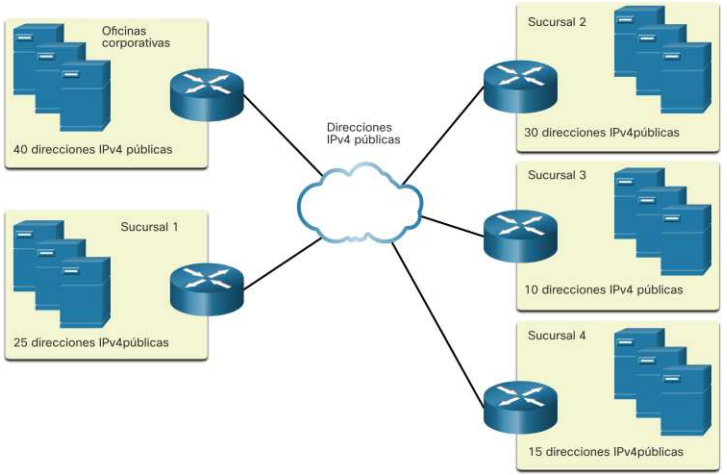
Longitud del prefijo	Máscara de red	Máscara de red en binario (n = network, h = host)	# de subredes	# de hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

Ejemplo de división eficiente de una red IPv4

- En este ejemplo, el ISP ha asignado una dirección de red pública de 172.16.0.0/22 (10 bits de host) a la sede corporativa, que proporciona 1022 direcciones de host.



- Hay cinco sitios y, por lo tanto, cinco conexiones a Internet, lo que significa que la organización requiere 10 subredes y la subred más grande requiere 40 direcciones.



- Asignó 10 subredes con una máscara de subred / 26 (es decir, 255.255.255.192).

División en subredes para cumplir requerimientos

Determinar la cantidad de bits que se deben tomar prestados(11.7.4)

Hosts necesarios	Máscara de subred (formato binario)	Máscara de subred (formato decimal)	Notación de prefijo (/x)
250	**11111111.11111111.11111111.00000000**	**255.255.255.0**	**/24**
25	. . .		/
1000	. . .		/
75	. . .		/
10	. . .		/
500	. . .		/

Packet Tracer – Escenario subnetting (11.7.5)

En este Packet Tracer, se realizará lo siguiente:

- Diseñar un esquema de direccionamiento IP
- Asignar direcciones IP a dispositivos de red y verificar la conectividad

11.8 VLSM

Video – VLSM básico(11.8.1)

- Este video explica los aspectos básicos de VLSM.

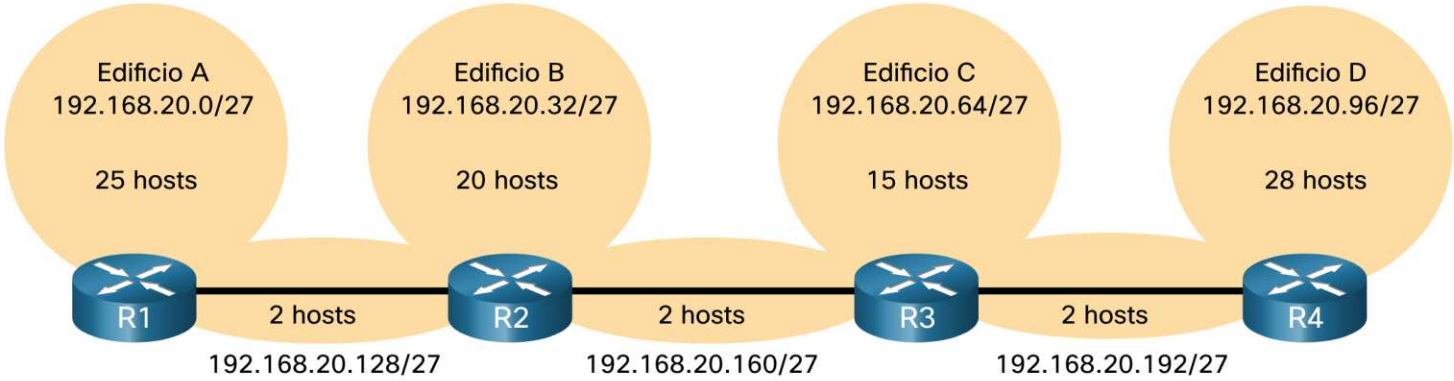
Video – Ejemplo VLSM(11.8.2)

- Este video demostrará la creación de subredes específicas para las necesidades de la red.

Conservación de direcciones IPv4

En la sig siguiente topología, se requieren 7 subredes (cuatro LAN y tres enlaces WAN) y la mayor cantidad de host se encuentra en el Edificio D con 28 hosts.

- Una máscara /27 proporcionaría 8 subredes de 30 direcciones IP de host y, por lo tanto, admitiría esta topología.



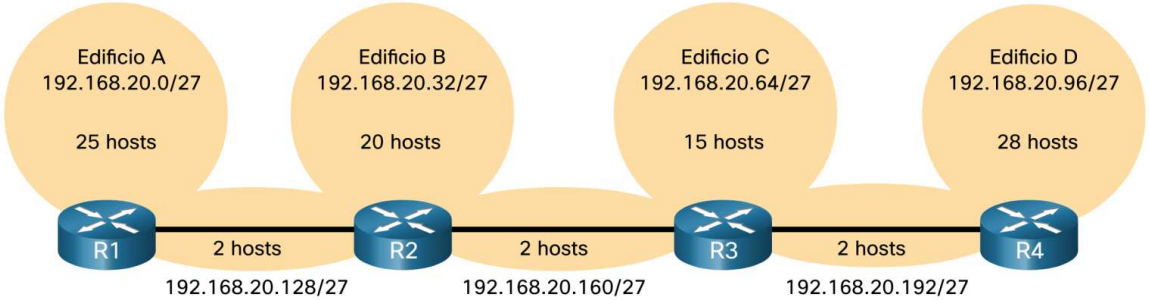
Conservación de direcciones IPv4 (Cont.)

Sin embargo, los enlaces WAN de punto a punto solo requieren dos direcciones y, por lo tanto, desperdician 28 direcciones cada uno para un total de 84 direcciones no utilizadas.

Porción de host
2^5-2=30 direcciones IP de host por subred

30-2=28
Cada subred WAN desperdicia 28 direcciones

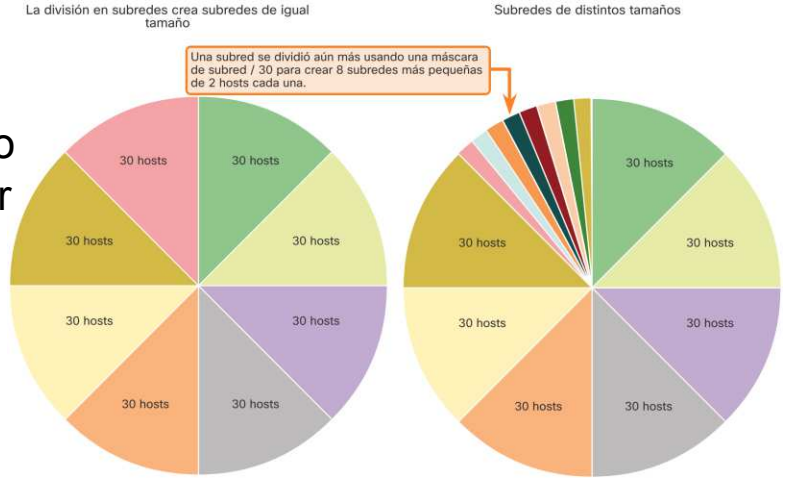
28x3=84
84 direcciones no se utilizan



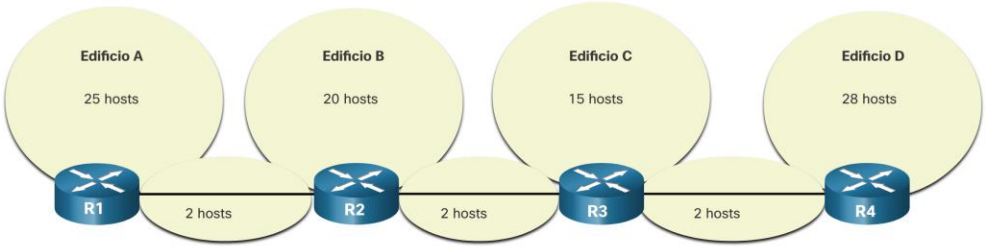
- Aplicar un esquema de división en subredes tradicional a este escenario no es muy eficiente.
- VLSM se desarrolló para evitar el desperdicio de direcciones al permitirnos dividir una subred en más subredes.

VLSM

- El lado izquierdo muestra el esquema de subred tradicional (es decir, máscara fija) mientras que el lado derecho ilustra cómo se puede usar VLSM para dividir una subred en subredes y dividir la última subred en ocho subredes /30.
- Cuando se utilice VLSM, comience siempre por satisfacer los requisitos de la subred más grande y continúe dividiendo en subredes hasta que se satisfagan los requisitos de host de la subred más pequeña.

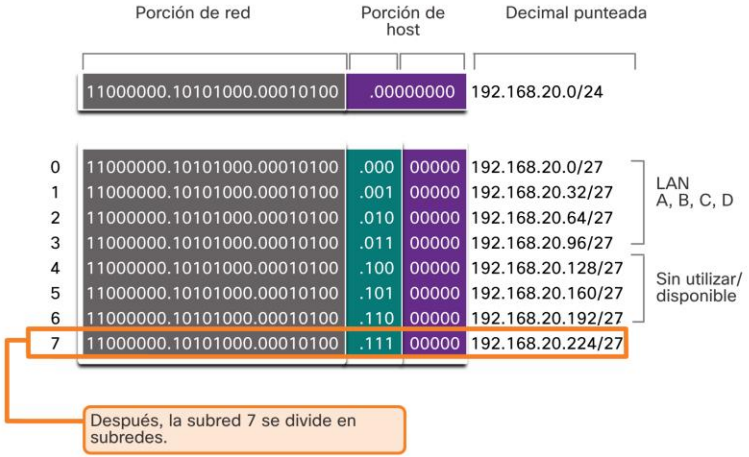


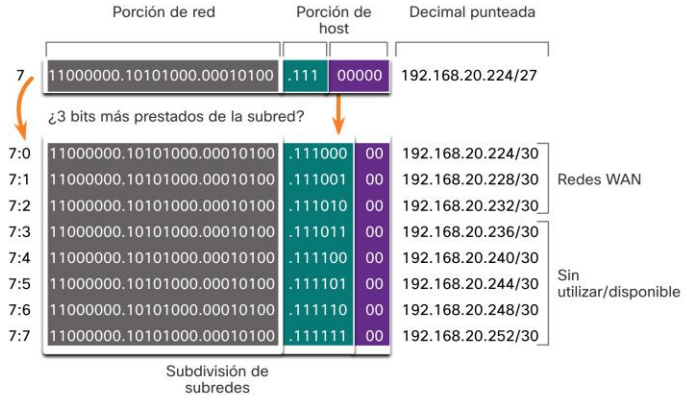
- La topología resultante usando VLSM.



Esquema de división VLSM

- Se divide una de las subredes /27. En este ejemplo, la última subred, 192.168.20.224/27, puede subdividirse aún más.

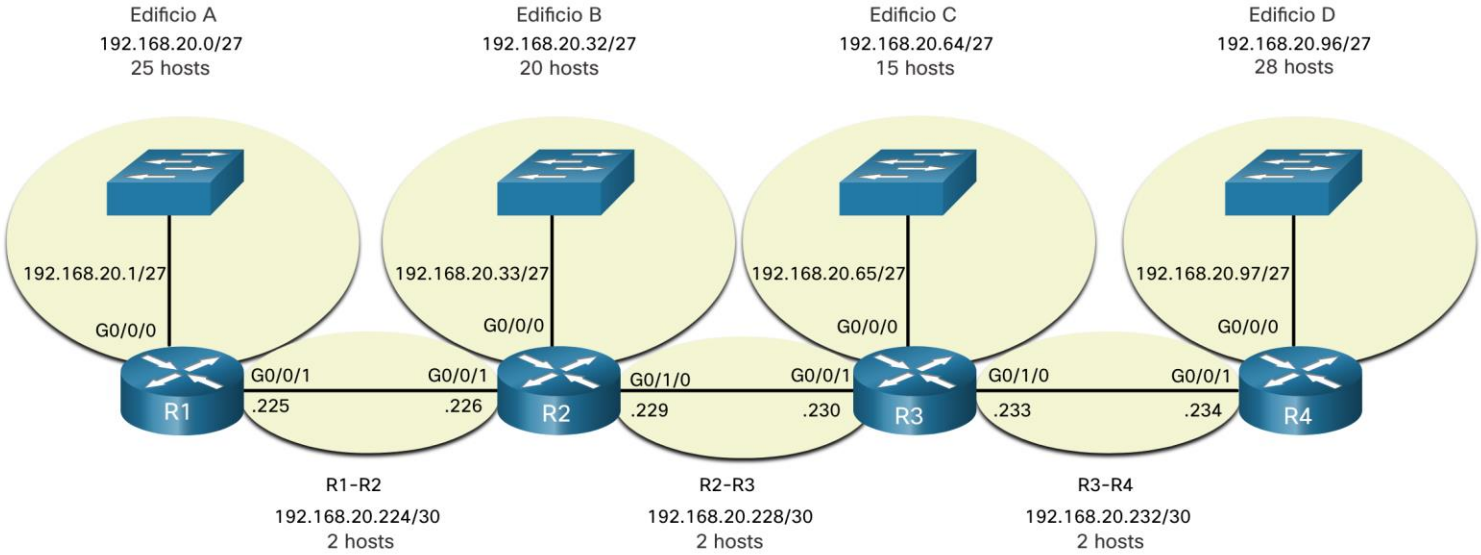




- Recuerde que cuando se conoce el número de direcciones de host necesarias, se puede usar la fórmula 2^n -2 (donde n es igual al número de bits de host restantes)

Asignación de direcciones de topología VLSM

- Usando las subredes VLSM, las redes LAN y entre routeres se pueden abordar sin desperdicio innecesario.



11.9 Diseño estructurado

Planificación de redes IPv4

La planificación de la red IP es fundamental para desarrollar una solución escalable para una red empresarial.

- Para desarrollar un esquema de direccionamiento para toda la red IPv4, necesita saber cuántas subredes se necesitan, cuántos hosts requiere cada subred, qué dispositivos son parte de la subred, qué partes de su red usan direcciones privadas y cuáles usan públicas, y muchos otros factores determinantes.

Examine las necesidades del uso de la red y cómo se estructurarán las subredes.

- Realice un estudio de requisitos de red observando toda la red para determinar cómo se segmentará cada área.
- Determine cuántas subredes se necesitan y cuántos hosts por subred.
- Determine los grupos de direcciones DHCP y los grupos de VLAN de capa 2.

Asignación de direcciones de dispositivos

Dentro de una red, existen diferentes tipos de dispositivos que requieren direcciones:

- **Clientes** : la mayoría usa DHCP para reducir los errores y la carga para el personal de soporte de la red. Los clientes de IPv6 pueden obtener información de direcciones mediante DHCPv6 o SLAAC.
- **Servidores y periféricos**: deben tener una dirección IP estática predecible.
- **Servidores a los que se puede acceder desde Internet**: los servidores deben tener una dirección IPv4 pública, a la que se accede con mayor frecuencia mediante NAT.
- **Dispositivos intermedios**: a los dispositivos se les asignan direcciones para la administración, el monitoreo y la seguridad de la red.
- **Puerta de enlace:** los enrutadores y los dispositivos de firewall son puertas de enlace para los hosts de esa red.

Al desarrollar un esquema de direccionamiento IP, generalmente se recomienda que tenga un patrón establecido de cómo se asignan las direcciones a cada tipo de dispositivo.

Packet Tracer – VLSM Práctica de diseño e implementación(11.9.3)

En este Packet Tracer, se realizará lo siguiente:

- Examinar los requisitos de la red
- Diseñar el esquema de direccionamiento utilizando VLSM
- Asignar direcciones IP a dispositivos y verificar la conectividad

11.10 Práctica del módulo y cuestionario

Packet Tracer – Diseño e implementacón de un esquema de direccionamiento VLSM(11.10.1)

En este Packet Tracer, hará lo siguiente:

- Diseñar un esquema de direccionamiento IP VLSM según los requisitos
- Configurar el direccionamiento en dispositivos y hosts de red
- Verificar la conectividad IP
- Solucionar problemas de conectividad según sea necesario.

Lab - Diseño e implementación un esquema de direccionamiento VLSM

En esta actividad de laboratorio, completará los siguientes objetivos:

- Examinar los requisitos de la red
- Diseñar el esquema de direcciones VLSM
- Cablear y configurar la red IPv4

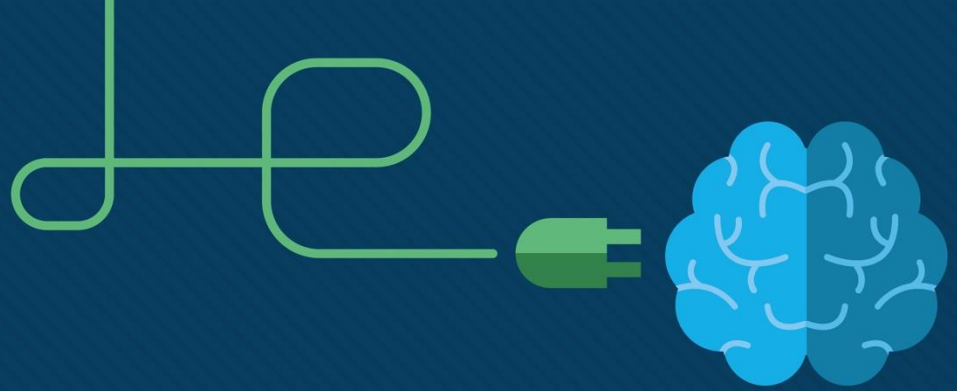
¿Qué se aprendió en el módulo?

- La estructura de direccionamiento IP consta de una dirección de red jerárquica de 32 bits que identifica las porciones de red y del host. Los dispositivos de red utilizan un proceso llamado AND usando la dirección IP y la máscara de subred para identificar las porciones de la red y del host.
- Los paquetes IPv4 de destino pueden ser de unidifusión, difusión y multidifusión.
- Hay direcciones IP enrutables globalmente asignadas por la IANA y hay tres rangos de direcciones de red IP privadas que no se pueden enrutar globalmente pero que se pueden usar en todas las redes privadas internas.
- Reduzca los dominios de transmisión mediante el uso de subredes para crear dominios de transmisión más pequeños, esto para reducir el tráfico general de la red y mejorar el rendimiento de la red.
- Crear subredes IPv4 utilizando uno o más de los bits de host como bits de red. Es más simple dividir subredes en el límite de octetos de /8, /16 y / 24.

¿Qué se aprendió en el módulo? (Cont.)

- Utilizar VLSM para reducir la cantidad de direcciones de host no utilizadas por subred.
- VLSM permite dividir un espacio de red en partes desiguales. Empiece siempre por satisfacer los requisitos de host de la subred más grande. Continúe dividiendo en subredes hasta que se satisfagan los requisitos de host de la subred más pequeña.
- Al diseñar un esquema de direccionamiento de red, tenga en cuenta los requisitos internos, DMZ y externos. Utilice un esquema de direccionamiento IP interno consistente con un patrón establecido de cómo se asignan las direcciones a cada tipo de dispositivo.


CISCO



Módulo 12: Direccionamiento IPv6

Objetivos

Título: Direccionamiento IPv6

Objetivo: Implementar un esquema de direccionamiento IPv6.

Tema	Objetivo
Limitaciones de IPv4	Explicar porque es necesario IPv6
Representación de direcciones IPv6	Explicar como se representan las direcciones IPv6.
Tipos de direcciones IPv6	Comparar los tipos de direcciones IPv6.
Configuración estática de GUA y LLA	Explicar como configurar una de how to Configure static global unicast and link-local IPv6 network addresses.
Direccióne IPv6 dinámicas GUAs	Explain how to configure global unicast addresses dynamically.

Objetivos (Cont.)

Titulo: IPv6 Addressing

Objetivo: Implement an IPv6 Addressing scheme.

Titulo	Objetivo
Direccionamiento dinámico IPv6 LLAs	Configurar direcciones link-local dinámicamente.
IPv6 Multicast	Identificar dirección IPv6.
Subneteo de redes IPv6	Implementar un esquema de direccionamiento IPv6.

12.1 Limitaciones IPv4

Necesidad de IPv6

- Se están agorando las direcciones IPv4. IPv6 es el sucesor de IPv4. IPv6 tiene un espacio de direcciones mucho más grande (128 bits).
- IPv6 también incluye correcciones a las limitaciones de IPv4 y otras mejoras.
- Con una población de Internet en aumento, un espacio de direcciones IPv4 limitado, problemas con NAT e IoT, ha llegado el momento de comenzar la transición a IPv6.

Coexistencia de IPv4 e IPv6

Tanto IPv4 como IPv6 coexistirán en un futuro próximo y la transición llevará varios años.

El IETF ha creado varios protocolos y herramientas para ayudar a los administradores de red a migrar sus redes a IPv6. Estas técnicas de migración se pueden dividir en tres categorías:

- Pila dual: los dispositivos ejecutan pilas de protocolos IPv4 e IPv6 simultáneamente.
- Tunelización: método de transporte de un paquete IPv6 a través de una red IPv4. El paquete IPv6 está encapsulado dentro de un paquete IPv4.
- Traducción: la traducción de direcciones de red 64 (NAT64) permite que los dispositivos habilitados para IPv6 se comuniquen con dispositivos habilitados para IPv4 mediante una técnica de traducción similar a NAT para IPv4.

Nota: La tunelización y la traducción son para la transición a IPv6 nativo y solo deben usarse donde sea necesario. El objetivo debe ser las comunicaciones IPv6 nativas desde el origen hasta el destino.

12.2 Representación de direcciones IPv6

Formatos de direcciones. IPv6

- Las direcciones Pv6 tienen 128 bits de longitud y se eesciben en hexadecimal.
- Las direcciones IPv6 puden escribirse en mayúsculas y minúsculas no distinguen entre mayúsculas y minúsculas.
- El formato preferido para escribir una dirección IPv6 es x: x: x: x: x: x: x: x, y cada "x" se compone de cuatro valores hexadecimales.
- En IPv6, un hexteto es el término no oficial utilizado para referirse a un segmento de 16 bits, o cuatro valores hexadecimales.

- Ejemplos de direcciones IPv6 en el formato preferido:

  2001:0db8:0000:1111:0000:0000:0000:0200

  2001:0db8:0000:00a3:abcd:0000:0000:1234

Regla 1 – Omitir los ceros a la izquierda

La primera regla para ayudar a reducir la notación de las direcciones IPv6 es omitir los 0 a la izquierda (ceros).

Ejemplos:

- 01ab puede escribirse como 1ab
- 09f0 puede escribirse como 9f0
- 0a00 puede escribirse como a00
- 00ab puede escribirse como s ab

Nota: Esta regla solo se aplica a los ceros iniciales, NO a los ceros finales; de lo contrario, la dirección sería ambigua.

Escritura	Formato
Preferida	2001 : **0**db8 : **000**0 : 1111 : **000**0 : **000**0 : **000**0 : **0**200
Sin ceros a la izquierda	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

Regla 2 – Double Colon

Dos puntos dobles (::) pueden reemplazar cualquier cadena única contigua de uno o más hextetos de 16 bits que constan de solo ceros.

Ejemplo:

- 2001:db8:cafe:1:0:0:0:1 (note que ya no tiene los zeros al inicio)se puede representar como 2001:db8:cafe:1::1

Nota: Los dos puntos dobles (: :) solo se pueden usar una vez dentro de una dirección; de lo contrario, habría más de una posible dirección resultante.s.

Escritura	Format
Preferida	2001 : **0**db8 : **000**0 : 1111 : **0000** : **0000** : **0000** : **0**200
Comprimida	2001:db8:0:1111::200

12.3 Tipos de direcciones IPv6

Unicast, Multicast, Anycast

Hay tres categorías amplias de direcciones IPv6:

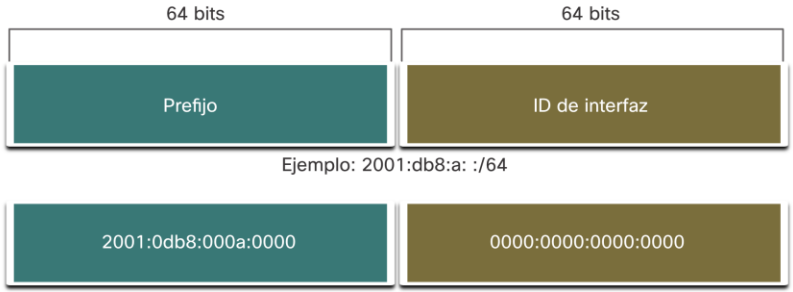
- **Unicast** – Unicast identifica de forma única una interfaz en un dispositivo habilitado para IPv6.
- **Multicast** – Multicast se utiliza para enviar un único paquete IPv6 a varios destinos.
- **Anycast** – Se trata de cualquier dirección de unidifusión IPv6 que se pueda asignar a varios dispositivos. Un paquete enviado a una dirección anycast se enruta al dispositivo más cercano que tenga esa dirección.

Note: A diferencia de IPv4, IPv6 no tiene una dirección de broadcast. Sin embargo, existe una dirección de multidifusión IPv6 para todos los nodos que básicamente da el mismo resultado.

Longitud de prefijo IPv6

La longitud del prefijo se representa en notación de barra y se utiliza para indicar la parte de red de una dirección IPv6.

La longitud del prefijo IPv6 puede oscilar entre 0 y 128. La longitud del prefijo IPv6 recomendada para las LAN y la mayoría de los otros tipos de redes es / 64.

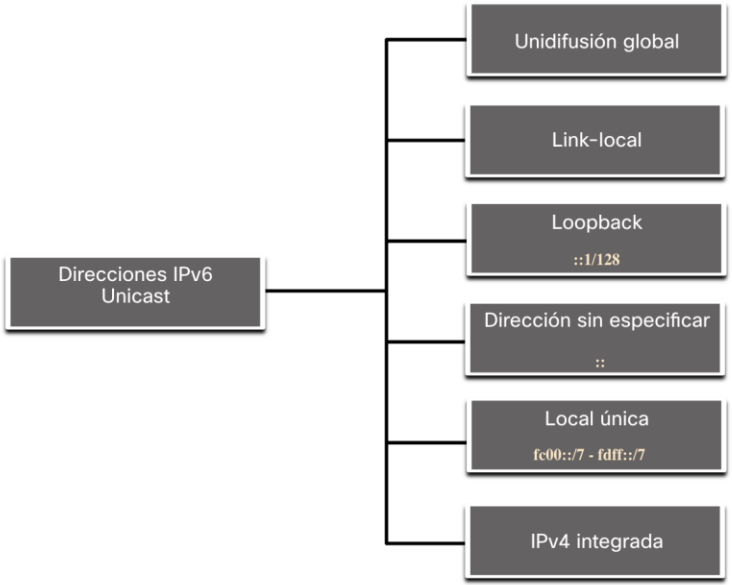


Nota: Se recomienda utilizar una ID de interfaz de 64 bits para la mayoría de las redes. Esto se debe a que la configuración automática de direcciones sin estado (SLAAC) utiliza 64 bits para el ID de interfaz. También hace que la división en subredes sea más fácil de crear y administrar..

Tipo de direccione IPv6 Unicast

A diferencia de los dispositivos IPv4 que tienen una sola dirección, las direcciones IPv6 suelen tener dos direcciones unicast:

- **Global Unicast Address (GUA)** – Esto es similar a una dirección IPv4 pública. Estas son direcciones enrutables a Internet, únicas a nivel mundial..
- **Link-local Address (LLA)** - Requerido para cada dispositivo habilitado para IPv6 y usado para comunicarse con otros dispositivos en el mismo enlace local. Los LLA no son enrutables y están confinados a un solo enlace.



Una nota sobre las dirección local única (ULA)

Las direcciones locales únicas IPv6 (rango fc00 :: / 7 a fdff :: / 7) tienen cierta similitud con las direcciones privadas RFC 1918 para IPv4, pero existen diferencias significativas:

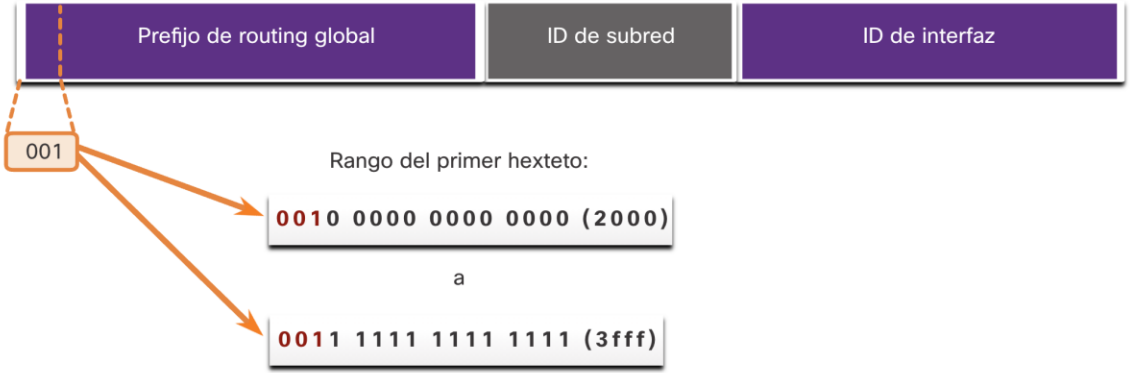
- Las direcciones locales únicas se utilizan para el direccionamiento local dentro de un sitio o entre un número limitado de sitios.
- Las direcciones locales únicas se pueden utilizar para dispositivos que nunca necesitarán acceder a otra red.
- Las direcciones locales únicas no se enrutan ni se traducen globalmente a una dirección IPv6 global.

Note: Muchos sitios utilizan la naturaleza privada de las direcciones RFC 1918 para intentar proteger u ocultar su red de posibles riesgos de seguridad. Este nunca fue el uso previsto de los ULA.

IPv6 GUA

Las direcciones de unidifusión global (GUA) IPv6 son globalmente únicas y enrutables en Internet IPv6.

- Actualmente, solo se asignan GUA con los primeros tres bits de 001 2000 :: / 3
- Las GUA disponibles actualmente comienzan con un decimal 2 o un 3 (esto es solo 1/8 del espacio total de direcciones IPv6 disponible).



Estructura IPv6 GUA

Prefijo de enrutamiento global:

- El prefijo de enrutamiento global es el prefijo, o parte de la red, de la dirección que asigna el proveedor, como un ISP, a un cliente o sitio. El prefijo de enrutamiento global variará según las políticas del ISP.

ID de subred:

- El campo ID de subred es el área entre el prefijo de enrutamiento global y el ID de interfaz. Una organización utiliza el ID de subred para identificar subredes dentro de su sitio.

ID de interfaz:

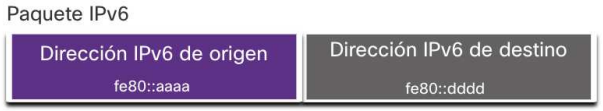
- El ID de la interfaz IPv6 es equivalente a la parte de host de una dirección IPv4. Se recomienda que, en la mayoría de los casos, se utilicen subredes / 64, lo que crea una ID de interfaz de 64 bits.

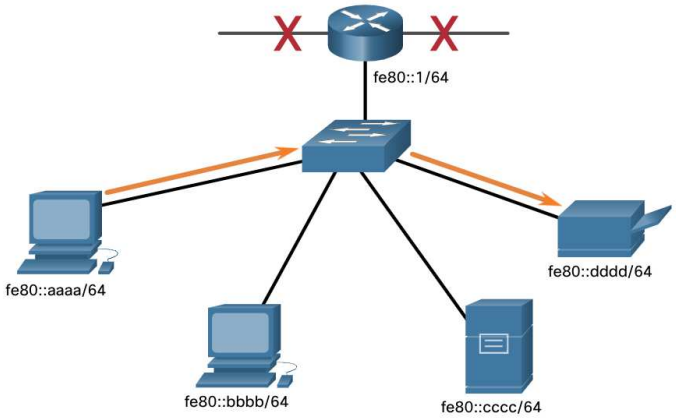
Nota: IPv6 permite que las direcciones de host todos 0 y todos 1 se puedan asignar a un dispositivo. La dirección todos ceros está reservada como una dirección anycast de subred-enrutador y debe asignarse solo a enrutadores.

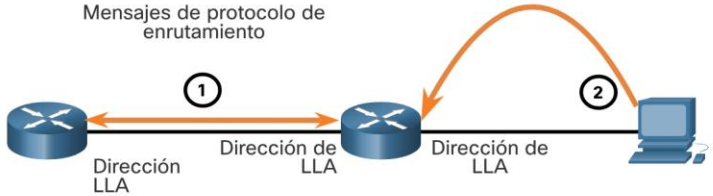
Tipo de direcciones IPv6
IPv6 LLA(revisar act 12.2.4)

Una dirección local de enlace IPv6 (LLA) permite que un dispositivo se comunique con otros dispositivos habilitados para IPv6 en el mismo enlace y solo en ese enlace (subred).

- Los paquetes con un LLA de origen o destino no se pueden enrutar.
- Cada interfaz de red habilitada para IPv6 debe tener un LLA.
- Si un LLA no se configura manualmente en una interfaz, el dispositivo creará uno automáticamente.
- Los LLA de IPv6 están en el rango fe80 :: / 10.







1. Los enrutadores usan el LLA de los enrutadores vecinos para enviar actualizaciones de enrutamiento.
2. Los hosts usan el LLA de un enrutador local como puerta de enlace predeterminada.

12.4 Configuración estática de GUA y LLA

Configuración estática de GUA en un router

La mayoría de los comandos de verificación y configuración de IPv6 en Cisco IOS son similares a sus contrapartes de IPv4. En muchos casos, la única diferencia es el uso de ipv6 en lugar de ip dentro de los comandos.

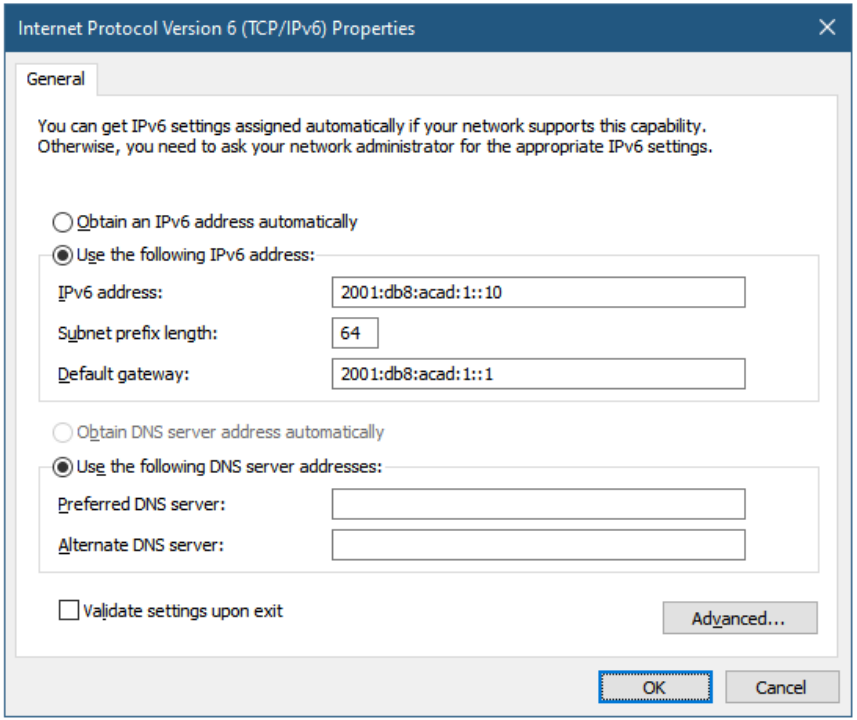
- El comando para configurar una GUA IPv6 en una interfaz es: dirección ipv6 dirección-ipv6 /longitud de prefijo.
- El ejemplo muestra comandos para configurar una GUA en la interfaz G0/0/0 en R1:

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```

Configuración estática GUA en un host Windows

- Configurar manualmente la dirección IPv6 en un host es similar a configurar una dirección IPv4.
- La GUA o LLA de la interfaz del enrutador se puede utilizar como puerta de enlace predeterminada. La mejor práctica es utilizar LLA.

Nota: Cuando se utiliza DHCPv6 o SLAAC, el LLA del enrutador se especificará automáticamente como la dirección de puerta de enlace predeterminada.



Configuración estática GUA de una dirección Link-Local Unicast

Configurar el LLA manualmente le permite crear una dirección que sea reconocible y más fácil de recordar.

- Los LLA se pueden configurar manualmente mediante el comando **ipv6 address** ipv6-link-local-address **link-local**.
- El ejemplo muestra comandos para configurar un LLA en la interfaz G0 / 0/0 en R1

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
```

Nota: El mismo LLA se puede configurar en cada enlace siempre que sea único en ese enlace. La práctica común es crear un LLA diferente en cada interfaz del enrutador para facilitar la identificación del enrutador y la interfaz específica.

12.5 Direccionamiento dinámico para GUAs IPv6

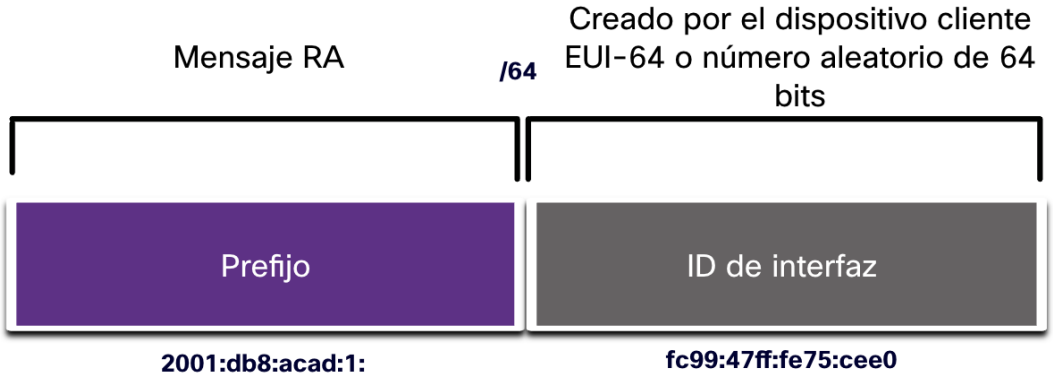
RS and RA Messages

Los dispositivos obtienen direcciones GUA dinámicamente a través de mensajes del Protocolo de mensajes de control de Internet versión 6 (ICMPv6).

- Los dispositivos host envían mensajes de solicitud de enrutador (RS) para descubrir enrutadores IPv6
- Los enrutadores envían mensajes de anuncio de enrutador (RA) para informar a los hosts sobre cómo obtener una GUA de IPv6 y proporcionar información de red útil, como:
  - Prefijo de red y longitud del prefijo
  - Dirección de puerta de enlace predeterminada
  - Direcciones DNS y nombre de dominio
- La RA puede proporcionar tres métodos para configurar una GUA IPv6:
  - SLAAC
  - SLAAC con servidor DHCPv6 sin estado
  - DHCPv6 con estado (sin SLAAC)

Método 1: SLAAC

- SLAAC permite que un dispositivo configure una GUA sin los servicios de DHCPv6.
- Los dispositivos obtienen la información necesaria para configurar una GUA a partir de los mensajes ICMPv6 RA del enrutador local.
- El prefijo lo proporciona el RA y el dispositivo utiliza el método EUI-64 o de generación aleatoria para crear una ID de interfaz.

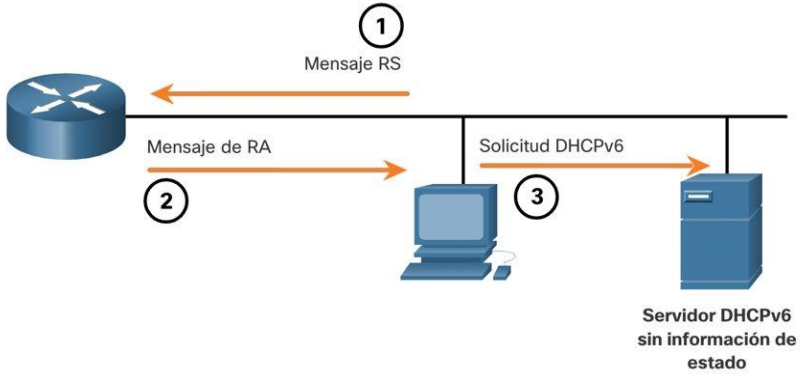


Método 2: SLAAC y DHCP sin estado

Un RA puede indicar a un dispositivo que utilice SLAAC y DHCPv6 sin estado.

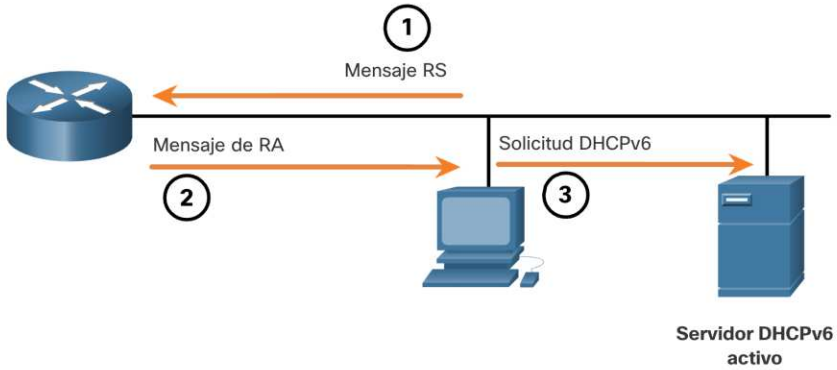
El mensaje RA sugiere que los dispositivos utilicen lo siguiente:

- SLAAC para crear su propia GUA IPv6
- El enrutador LLA, que es la dirección IPv6 de origen de RA, como la dirección de puerta de enlace predeterminada
- Un servidor DHCPv6 sin estado para obtener otra información, como una dirección de servidor DNS y un nombre de dominio



Método 3: DHCPv6 con estado

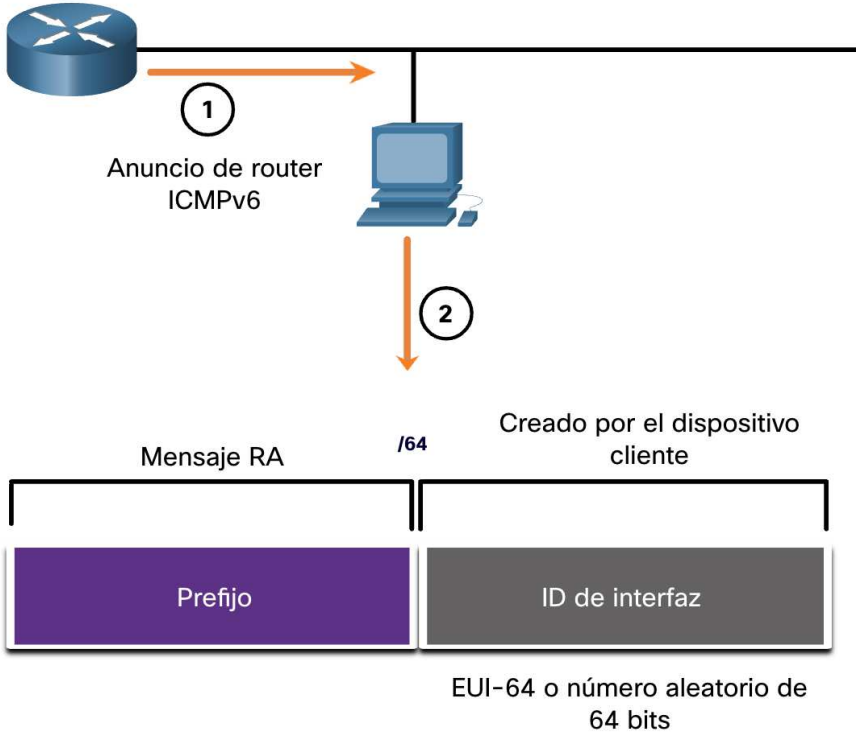
- Un RA puede indicarle a un dispositivo que utilice solo DHCPv6 con estado.
- El DHCPv6 con estado es similar al DHCP para IPv4. Un dispositivo puede recibir automáticamente una GUA, la longitud del prefijo y las direcciones de los servidores DNS de un servidor DHCPv6 con estado.
- El mensaje RA sugiere que los dispositivos utilicen lo siguiente:
  - El enrutador LLA, que es la dirección IPv6 de origen de RA, para la dirección de puerta de enlace predeterminada.
  - Un servidor DHCPv6 con estado para obtener una GUA, la dirección del servidor DNS, el nombre de dominio y otra información necesaria.



Proceso EUI-64 vs. Generación aleatoria

- Cuando el mensaje RA es SLAAC o SLAAC con DHCPv6 sin estado, el cliente debe generar su propia ID de interfaz.

- La ID de la interfaz se puede crear mediante el proceso EUI-64 o un número de 64 bits generado aleatoriamente.



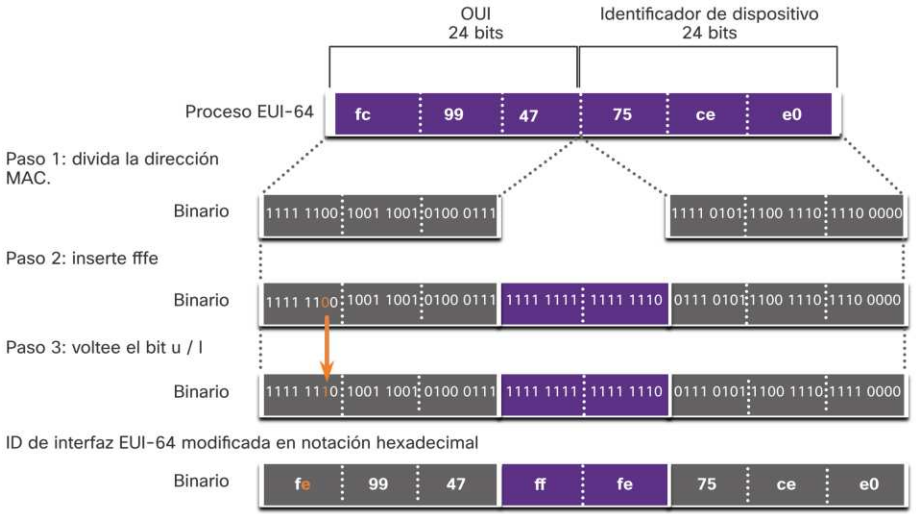
Proceso EUI-64

El IEEE definió el Identificador Único Extendido (EUI) o el proceso EUI-64 modificado que realiza lo siguiente:

- Se inserta un valor de 16 bits de fffe (en hexadecimal) en el medio de la dirección MAC de Ethernet de 48 bits del cliente.
- El séptimo bit de la dirección MAC del cliente se invierte de 0 a 1 binario.

Ejemplo:

48-bit MAC	fc:99:47:75:ce:e0
EUI-64 Interface ID	fe:99:47:ff:fe:75:ce:e0



Randomly Generated Interface IDs(ver act. 12.5.8)

- Dependiendo del sistema operativo, un dispositivo puede usar una ID de interfaz generada aleatoriamente en lugar de usar la dirección MAC y el proceso EUI-64.
- A partir de Windows Vista, Windows utiliza un ID de interfaz generado aleatoriamente en lugar de uno creado con EUI-64.

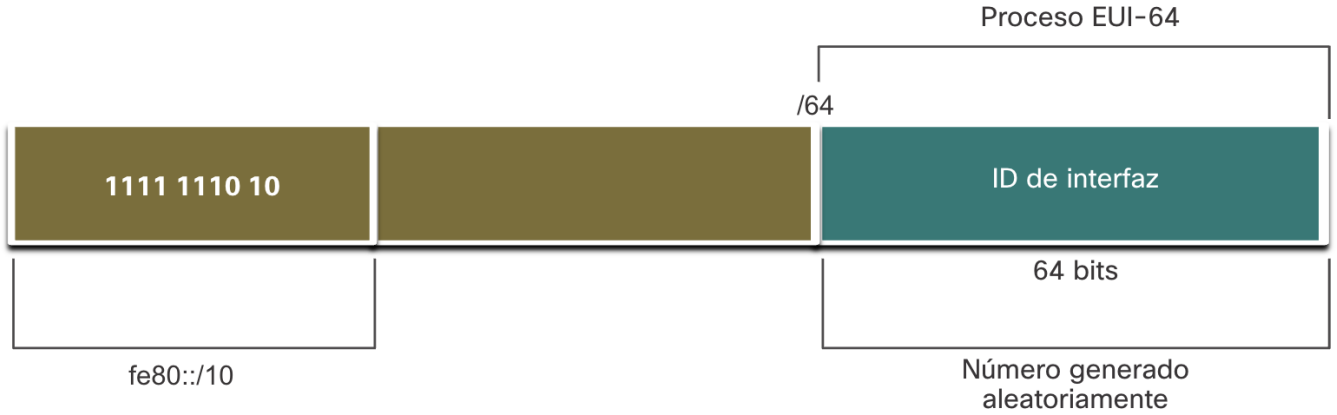
```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Nota: Para garantizar la unicidad de cualquier dirección unicast IPv6, el cliente puede utilizar un proceso conocido como Detección de direcciones duplicadas (DAD). Esto es similar a una solicitud ARP para su propia dirección. Si no hay respuesta, la dirección es única.

12.6 Direccionaniemto dinámico para IPv6 LLAs

LLAs Dinámicas

- Todas las interfaces IPv6 deben tener un LLA de IPv6.
- Al igual que las GUA de IPv6, las LLA se pueden configurar de forma dinámica.
- La figura muestra que el LLA se crea dinámicamente usando el prefijo fe80 :: / 10 y el ID de interfaz usando el proceso EUI-64, o un número de 64 bits generado aleatoriamente.



LLAs dinámicas en Windows

Los sistemas operativos, como Windows, normalmente utilizarán el mismo método tanto para una GUA creada por SLAAC como para una LLA asignada dinámicamente.

ID de interfaz generada con EUI-64 :

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

ID de intefaz generada aleatoriamente 64-bit:

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Verificar configuración IPv6 (ver act 12.6.5)

- Los enrutadores Cisco crean automáticamente un LLA IPv6 cada vez que se asigna una GUA a la interfaz. De forma predeterminada, los routers IOS de Cisco utilizan EUI-64 para generar el ID de interfaz para todos los LLA en las interfaces IPv6.
- A continuación, se muestra un ejemplo de un LLA configurado dinámicamente en la interfaz G0 /0/0 de R1:

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is ISR4221-2x1GE, address is 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
FE80::7279:B3FF:FE92:3640
2001:DB8:ACAD:1::1
```

Packet Tracer – Configurar direccionamiento IPv6 (12.6.6)

En este Packet Tracer, hará lo siguiente:

- Configurar el direccionamiento IPv6 en el enrutador
- Configurar el direccionamiento IPv6 en los servidores
- Configurar el direccionamiento IPv6 en los clientes
- Probar y verificar la conectividad de la red

12.7 Direcciones IPv6 multicast

Direcciones IPv6 de multidifusión asignadas

Las direcciones de multicast IPv6 tienen el prefijo ff00 :: / 8. Hay dos tipos de direcciones multicast IPv6:

- Direcciones multicast conocidas
- Direcciones multicast de nodo solicitadas

Note: Las direcciones multicast solo pueden ser direcciones de destino y no direcciones de origen.

Direcciones de multidifusión IPv6 bien conocidas

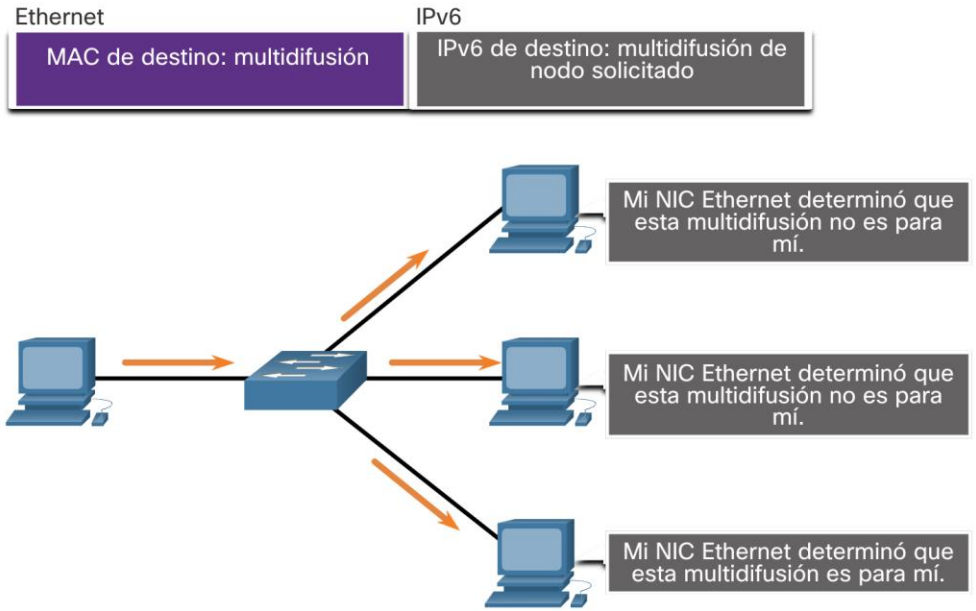
Se asignan direcciones de multidifusión IPv6 conocidas y se reservan para grupos predefinidos de dispositivos.

Hay dos grupos de multidifusión asignados de IPv6 comunes:

- **ff02 :: 1 Grupo de multidifusión de todos los nodos:** este es un grupo de multidifusión al que se unen todos los dispositivos habilitados para IPv6. Un paquete enviado a este grupo es recibido y procesado por todas las interfaces IPv6 en el enlace o la red.
- **ff02 :: 2 Grupo de multidifusión de todos los enrutadores:** este es un grupo de multidifusión al que se unen todos los enrutadores IPv6. Un enrutador se convierte en miembro de este grupo cuando se habilita como enrutador IPv6 con el comando de configuración global ***ipv6 unicast-routing*.**

IPv6 Multicast de nodo solicitado

- Una dirección de multidifusión de nodo solicitado es similar a la dirección de multidifusión de todos los nodos.
- Una dirección de multidifusión de nodo solicitado se asigna a una dirección de multidifusión Ethernet especial.
- La NIC Ethernet puede filtrar la trama examinando la dirección MAC de destino sin enviarla al proceso IPv6 para ver si el dispositivo es el objetivo previsto del paquete IPv6.



Lab – Identificar direcciones IPv6

En este lab, completará los siguientes objetivos:

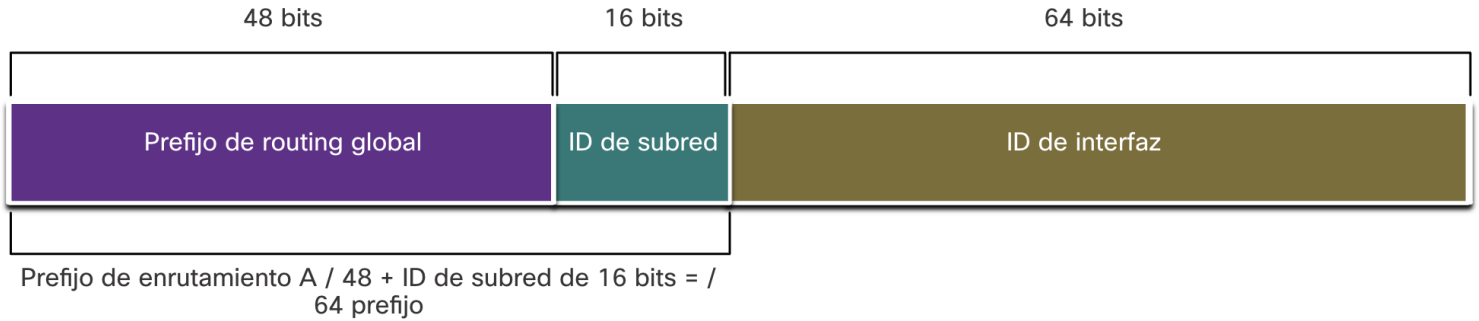
- Identificar los diferentes tipos de direcciones IPv6
- Examinar una dirección y una interfaz de red IPv6 de host
- Practicar la abreviatura de direcciones IPv6

12.8 Divisió de una red IPv6

Dividir usando el ID de subred

IPv6 considerando la división en subredes.

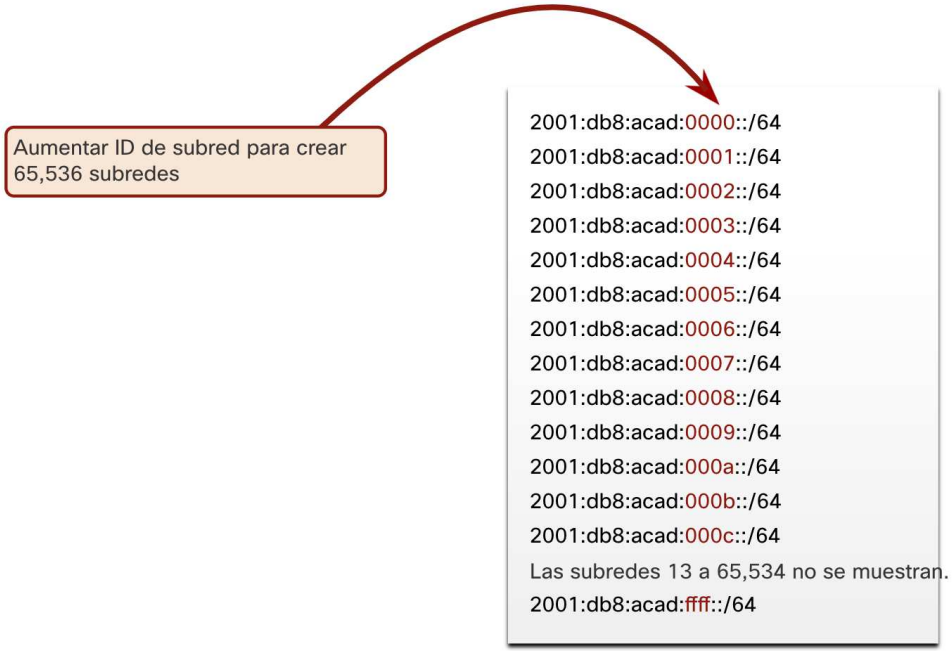
- Se utiliza un campo de ID de subred independiente en la GUA de IPv6 para crear subredes.
- El campo de ID de subred es el área entre el prefijo de enrutamiento global y el ID de interfaz.



Ejemplo de divisón de una red IPv6

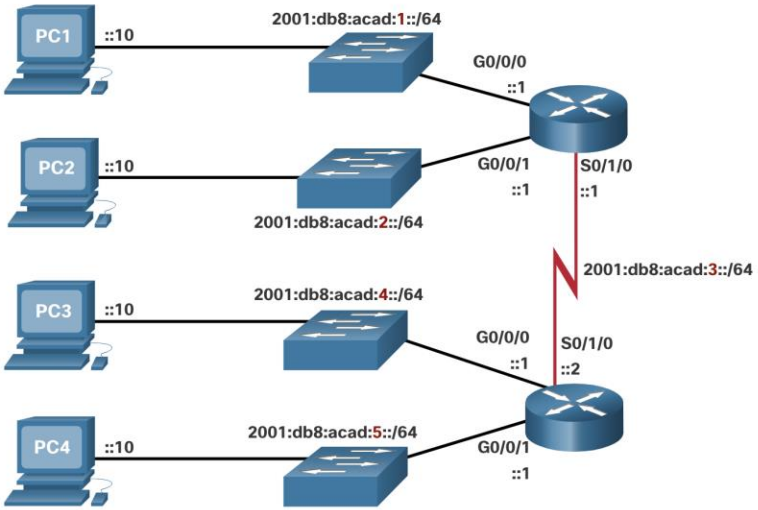
Dado el prefijo de enrutamiento global 2001: db8: acad :: / 48 con un ID de subred de 16 bits.

- Permite 65,536/64 subredes
- El prefijo de enrutamiento global es el mismo para todas las subredes.
- Solo el hexteto de ID de subred se incrementa en hexadecimal para cada subred.



Asignación de sunredes IPv6

- La topología de ejemplo requiere cinco subredes, una para cada LAN y para el enlace en serie entre R1 y R2.
- Se asignaron las cinco subredes IPv6, con el campo de ID de subred 0001 a 0005. Cada subred / 64 proporcionará más direcciones de las que nunca se necesitarán.



Bloque de direcciones: 2001:0 db8:acad: :/48

Cinco subredes asignadas a partir de 65 536 subredes disponibles

2001:db8:acad:**0000**::/64
2001:db8:acad:**0001**::/64
2001:db8:acad:**0002**::/64
2001:db8:acad:**0003**::/64
2001:db8:acad:**0004**::/64
2001:db8:acad:**0005**::/64
2001:db8:acad:**0006**::/64
2001:db8:acad:**0007**::/64
2001:db8:acad:**0008**::/64

2001:db8:acad:**ffff**::/64

Router configurado con subredes IPv6 (ver act 12.8.5)

El ejemplo muestra que cada una de las interfaces del enrutador en R1 se ha configurado para estar en una subred IPv6 diferente.

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

2.9 Práctica del módulo y custrionario

Packet Tracer – implemente un esquema de direccionamiento IPv6 subred(12.9.1)

En este Packet Tracer, hará lo siguiente:

- Determinar las subredes IPv6 y el esquema de direccionamiento
- Configurar el direccionamiento IPv6 en enrutadores y PC
- Verificar la conectividad IPv6

Lab – Configure IPv6 Addresses on Network Devices

In this lab, you complete the following objectives:

- Set up the topology and configure basic router and switch settings
- Configure IPv6 addresses manually
- Verify end-to-end connectivity

¿Qué se aprendió en el módulo?

- IPv4 tiene un máximo teórico de 4,3 mil millones de direcciones.
- El IETF ha creado varios protocolos y herramientas para ayudar a los administradores de red a migrar sus redes a IPv6. Las técnicas de migración se pueden dividir en tres categorías: doble pila, tunelización y traducción.
- Las direcciones IPv6 tienen una longitud de 128 bits y están escritas como una cadena de valores hexadecimales.
- El formato preferido para escribir una dirección IPv6 es x: x: x: x: x: x: x: x, y cada "x" consta de cuatro valores hexadecimales.
- Hay tres tipos de direcciones IPv6: unidifusión, multidifusión y anycast.
- Una dirección de unidifusión IPv6 identifica de forma exclusiva una interfaz en un dispositivo habilitado para IPv6.
- Las direcciones de unidifusión global (GUA) IPv6 son globalmente únicas y enrutables en Internet IPv6.

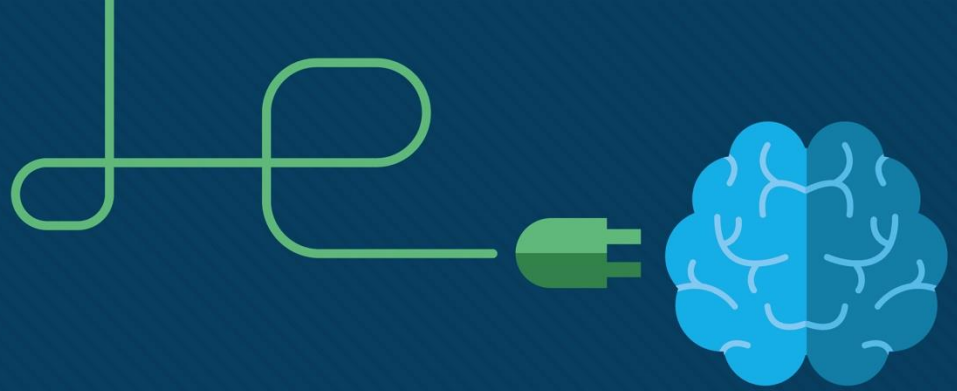
¿Qué se aprendió en el módulo? (Cont.)

- Una dirección local de enlace IPv6 (LLA) permite que un dispositivo se comunique con otros dispositivos habilitados para IPv6 en el mismo enlace y solo en ese enlace (subred).
- El comando para configurar una GUA IPv6 en una interfaz es dirección **ipv6** *dirección-ipv6/longitud de prefijo*.
- Un dispositivo obtiene una GUA de forma dinámica a través de mensajes ICMPv6. Los enrutadores IPv6 envían periódicamente mensajes ICMPv6 RA, cada 200 segundos, a todos los dispositivos habilitados para IPv6 en la red.
- Los mensajes RA tienen tres métodos: SLAAC, SLAAC con un servidor DHCPv6 sin estado y DHCPv6 con estado (sin SLAAC).
- La ID de la interfaz se puede crear mediante el proceso EUI-64 o un número de 64 bits generado aleatoriamente.
- El proceso EUIs utiliza la dirección MAC Ethernet de 48 bits del cliente e inserta otros 16 bits en el medio de la dirección MAC para crear una ID de interfaz de 64 bits.
- Dependiendo del sistema operativo, un dispositivo puede utilizar una ID de interfaz generada aleatoriamente.

¿Qué se aprendió en el módulo? (Cont.)

- Todos los dispositivos IPv6 deben tener un LLA IPv6. Un LLA se puede configurar manualmente o crear dinámicamente.
- Los enrutadores Cisco crean automáticamente un LLA IPv6 cada vez que se asigna una GUA a la interfaz.
- Hay dos tipos de direcciones de multidifusión IPv6: direcciones de multidifusión conocidas y direcciones de multidifusión de nodo solicitado.
- Dos grupos de multidifusión asignados por IPv6 comunes son: ff02 :: 1 grupo de multidifusión de todos los nodos y ff02 :: 2 grupo de multidifusión de todos los enrutadores.
- Una dirección de multidifusión de nodo solicitado es similar a la dirección de multidifusión de todos los nodos. La ventaja de una dirección de multidifusión de nodo solicitado es que se asigna a una dirección de multidifusión Ethernet especial.
- IPv6 se diseñó teniendo en cuenta la división en subredes. Se utiliza un campo de ID de subred independiente en la GUA de IPv6 para crear subredes.


CISCO



Módulo 13: ICMP

Objetivos

Titlulo: ICMP

Objetivo: Uso de herramientas de red para probar conectivida.

Tema	Objetivo
Mensajes ICMP	Explicar como ICMP es utilizado para probar conectividad
Utilidades ping y traceroute	Utilizar pong y traceroute para probar conectividad de res Use ping and traceroute utilities to test network connectivity.

13.1 Mensajes ICMP

Mensajes ICMPv4 y ICMPv6

- El Protocolo de mensajes de control de Internet (ICMP) proporciona información sobre problemas relacionados con el procesamiento de paquetes IP en determinadas condiciones.
- ICMPv4 es el protocolo de mensajería para IPv4. ICMPv6 es el protocolo de mensajería para IPv6 e incluye funcionalidad adicional.
- Los mensajes ICMP comunes a ICMPv4 e ICMPv6 incluyen:
  - Accesibilidad del host
  - Destino o servicio inalcanzable
  - Tiempo excedido

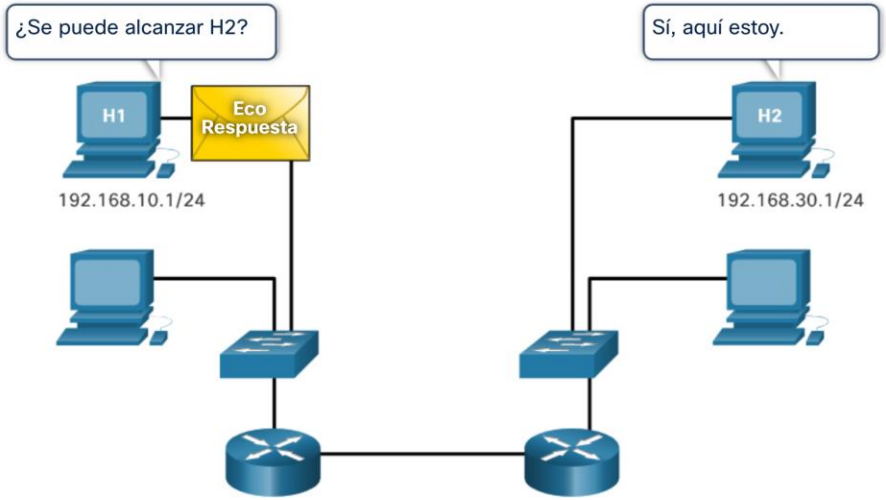
Nota: Los mensajes ICMPv4 no son obligatorios y, por lo general, no se permiten dentro de una red por razones de seguridad.

Accesibilidad del host

El mensaje de eco ICMP se puede utilizar para probar la accesibilidad de un host en una red IP.

Por ejemplo:

- Un host local envía una solicitud de eco ICMP a otro host remoto.
- Si el host está disponible, el host de destino responde con una respuesta de eco.



Destination or Service Unreachable

- Se puede utilizar un mensaje de destino inaccesible de ICMP para notificar al origen que un destino o servicio no está disponible.
- El mensaje ICMP incluirá un código que indica por qué no se pudo entregar el paquete.

Algunos códigos de destino inalcanzable para ICMPv4 son los siguientes:

- 0 - Net unreachable
- 1 - Host unreachable
- 2 - Protocol unreachable
- 3 - Port unreachable

Algunos códigos de destino inalcanzable para ICMPv6 son los siguientes:

- 0 - No route to destination
- 1 - Communication with the destination is administratively prohibited (e.g., firewall)
- 2 – Beyond scope of the source address
- 3 - Address unreachable
- 4 - Port unreachable

Nota: ICMPv6 tiene códigos similares pero ligeramente diferentes para los mensajes de destino inalcanzable.

Limite de tiempo excedido

- Cuando el campo Tiempo de vida (TTL) de un paquete se reduce a 0, se enviará un mensaje de tiempo excedido ICMPv4 al host de origen.
- ICMPv6 también envía un mensaje de Tiempo excedido. En lugar del campo TTL de IPv4, ICMPv6 utiliza el campo Límite de saltos de IPv6 para determinar si el paquete ha caducado.

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Nota: Los mensajes de tiempo excedido son utilizados por la herramienta **traceroute**.

Mensajes ICMPv6

ICMPv6 tiene nuevas características y funcionalidad mejorada que no se encuentran en ICMPv4, incluidos cuatro nuevos protocolos como parte del Protocolo de descubrimiento de vecinos (ND o NDP).

Los mensajes entre un enrutador IPv6 y un dispositivo IPv6, incluida la asignación dinámica de direcciones, son los siguientes:

- Mensaje de solicitud de enrutador (RS)
- Mensaje de anuncio de enrutador (RA)

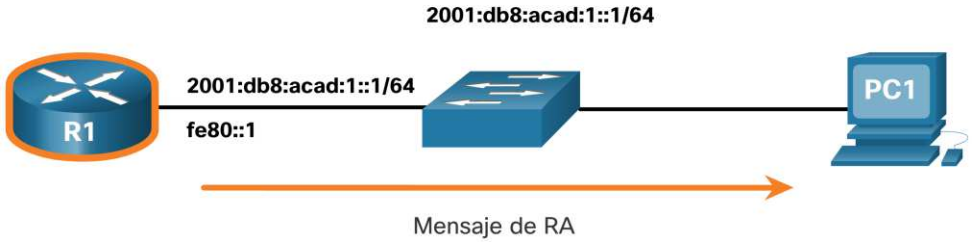
Los mensajes entre dispositivos IPv6, incluida la detección de direcciones duplicadas y la resolución de direcciones, son las siguientes:

- Mensaje de solicitud de vecino (NS)
- Mensaje de anuncio de vecino (NA)

Note: ICMPv6 ND también incluye el mensaje de redireccionamiento, que tiene una función similar al mensaje de redireccionamiento utilizado en ICMPv4.

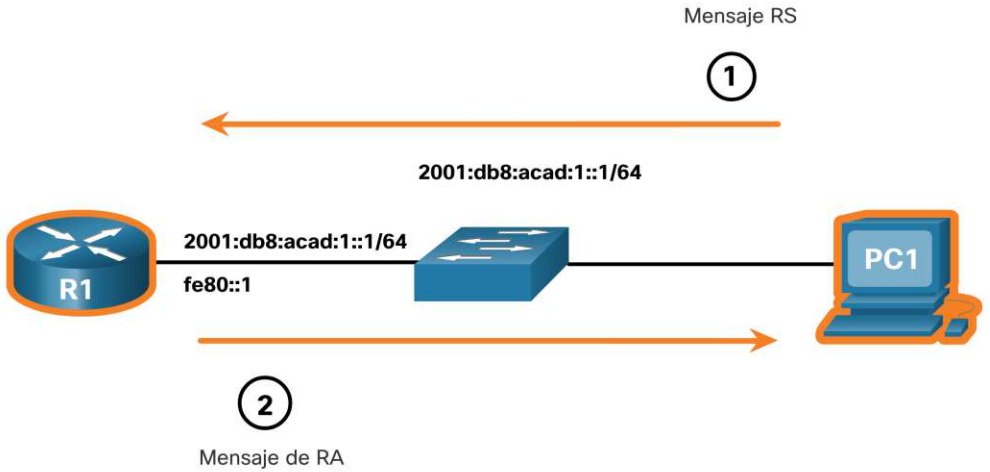
Mensajes ICMPv6 (Cont.)

- Los enrutadores habilitados para IPv6 envían mensajes RA cada 200 segundos para proporcionar información de direccionamiento a los hosts habilitados para IPv6.
- El mensaje RA puede incluir información de direccionamiento para el host, como el prefijo, la longitud del prefijo, la dirección DNS y el nombre de dominio.
- Un host que utilice la configuración automática de direcciones sin estado (SLAAC) establecerá su puerta de enlace predeterminada en la dirección local de enlace del enrutador que envió el RA.



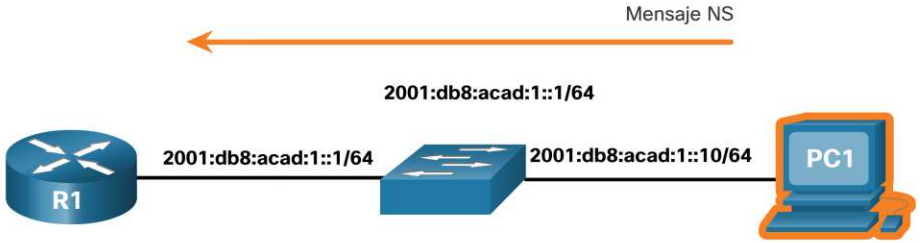
Mensajes ICMPv6 (Cont.)

- Un enrutador habilitado para IPv6 también enviará un mensaje RA en respuesta a un mensaje RS.
- En la figura, la PC1 envía un mensaje RS para determinar cómo recibir la información de su dirección IPv6 de forma dinámica.
- R1 responde al RS con un mensaje RA.
  - La PC1 envía un mensaje RS, "Hola, acabo de arrancar. ¿Hay un enrutador IPv6 en la red? Necesito saber cómo obtener la información de mi dirección IPv6 de forma dinámica ".
  - R1 responde con un mensaje RA. "Hola a todos los dispositivos habilitados para IPv6. Soy R1 y puedes usar SLAAC para crear una dirección de unidifusión global IPv6. El prefijo es 2001: db8: acad: 1 :: / 64. Por cierto, use mi dirección local de vínculo fe80 :: 1 como puerta de enlace predeterminada ".



Mensjaes ICMPv6 (Cont.)

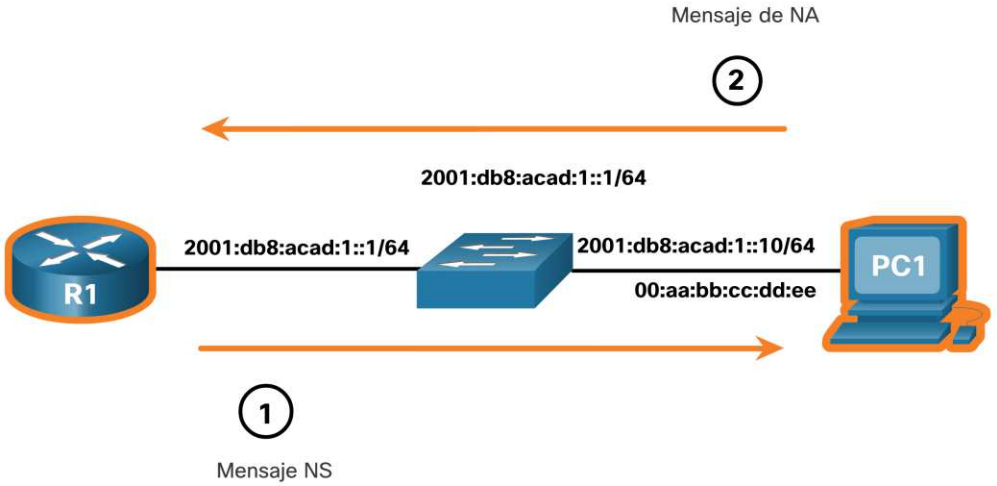
- Un dispositivo al que se le asigna una dirección de unicast IPv6 global o local de enlace puede realizar la detección de direcciones duplicadas (DAD) para garantizar que la dirección IPv6 sea única.
- Para verificar la unicidad de una dirección, el dispositivo enviará un mensaje NS con su propia dirección IPv6 como la dirección IPv6 de destino.
- Si otro dispositivo en la red tiene esta dirección, responderá con un mensaje NA notificando al dispositivo emisor que la dirección está en uso.



Nota: No se requiere DAD, pero RFC 4861 recomienda que DAD se realice en direcciones unicast.

Mensajes ICMPv6 (Cont.)

- Para determinar la dirección MAC del destino, el dispositivo enviará un mensaje NS a la dirección de nodo solicitada.
- El mensaje incluirá la dirección IPv6 conocida (dirigida). El dispositivo que tiene la dirección IPv6 de destino responderá con un mensaje NA que contiene su dirección MAC Ethernet.
- En la figura, R1 envía un mensaje NS a 2001: db8: acad:1::10 solicitando su dirección MAC.



13.2 Ping y Traceroute

Ping – Prueba de conectividad

- El comando **ping** es una utilidad de prueba de IPv4 e IPv6 que utiliza la solicitud de eco ICMP y los mensajes de respuesta de eco para probar la conectividad entre hosts y proporciona un resumen que incluye la tasa de éxito y el tiempo promedio de ida y vuelta al destino.
- Si no se recibe una respuesta dentro del tiempo de espera, ping proporciona un mensaje que indica que no se recibió una respuesta.
- Es común que se agote el tiempo de espera del primer ping si es necesario realizar la resolución de direcciones (ARP o ND) antes de enviar la solicitud de eco ICMP.

```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

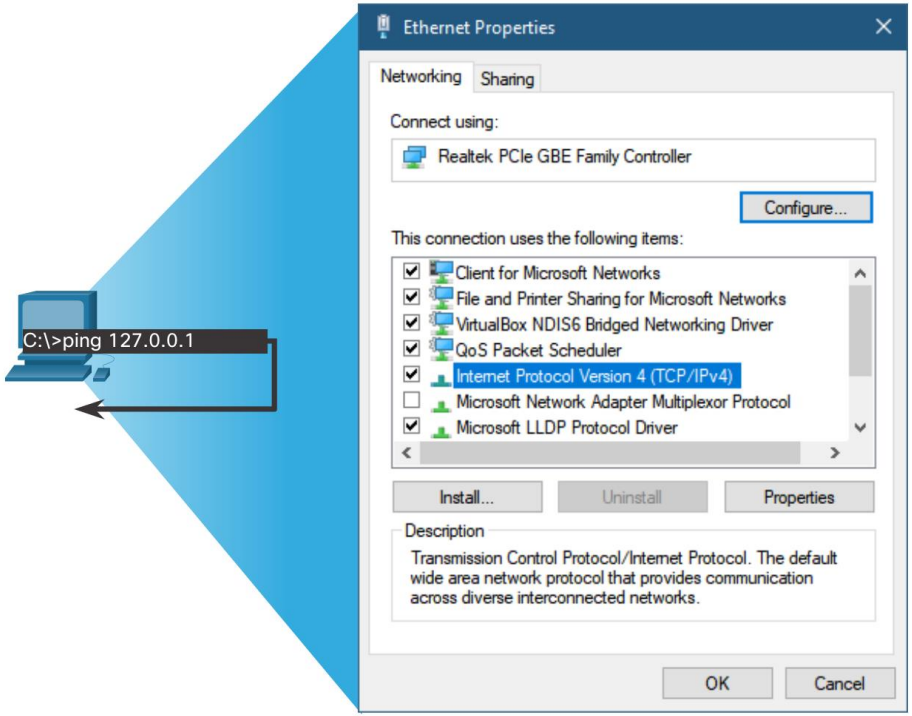
```
R1#ping 2001:db8:acad:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Ping a Loopback

Ping se puede utilizar para probar la configuración interna de IPv4 o IPv6 en el host local. Para hacer esto, haga **ping** a la dirección de loopback local de 127.0.0.1 para IPv4 (::1 para IPv6).

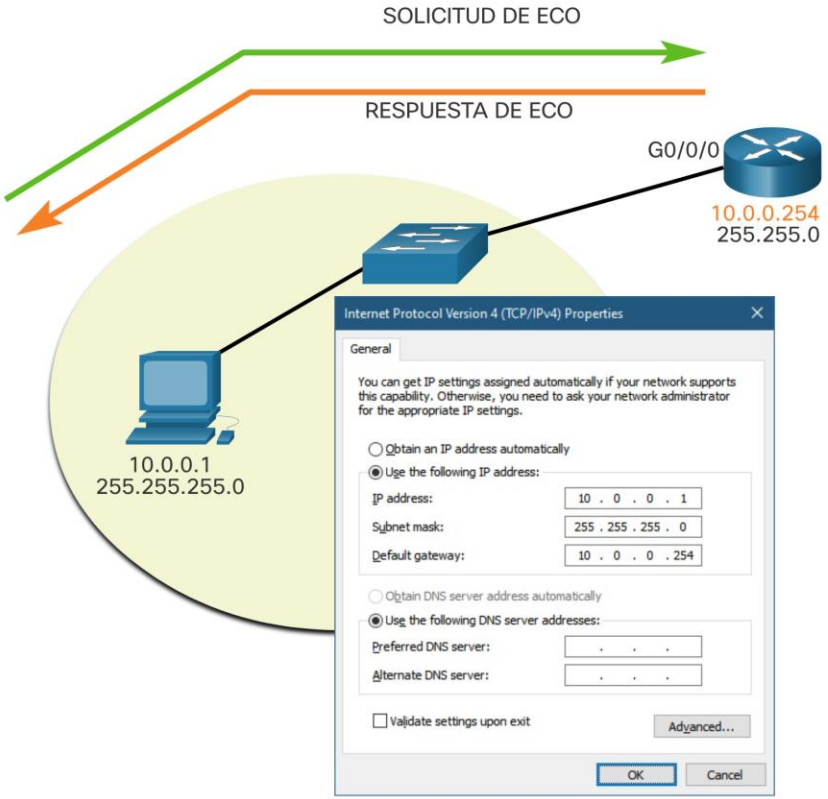
- Una respuesta de 127.0.0.1 para IPv4, o ::1 para IPv6, indica que IP está instalado correctamente en el host.
- Un mensaje de error indica que TCP/IP no está operativo en el host.



Ping al Gateway Default

El comando **ping** se puede utilizar para probar la capacidad de un host para comunicarse en la red local.

- La dirección de puerta de enlace predeterminada se utiliza con mayor frecuencia porque el enrutador normalmente siempre está operativo.
- Un ping exitoso a la puerta de enlace predeterminada indica que el host y la interfaz del enrutador que actúa como puerta de enlace predeterminada están operativos en la red local.
- Si la dirección de la puerta de enlace predeterminada no responde, se puede enviar un ping a la dirección IP de otro host en la red local que se sabe que está operativo.

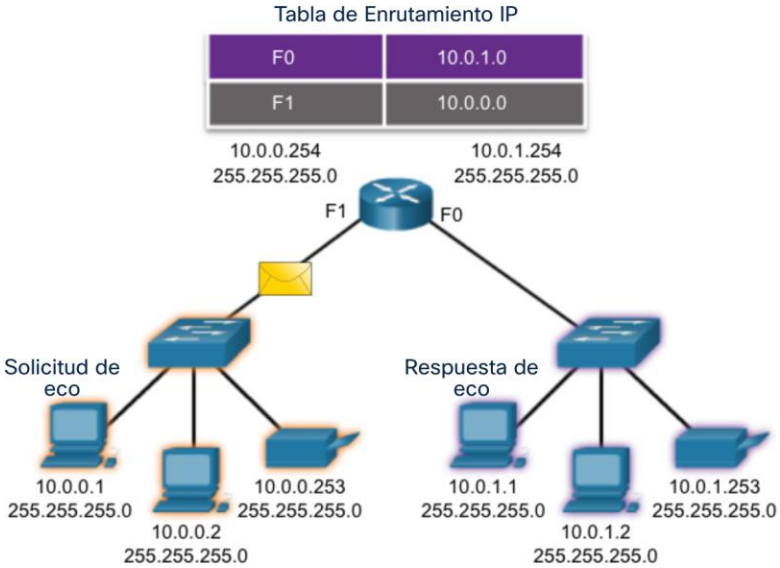


Ping a host remoto

Ping también se puede utilizar para probar la capacidad de un host local para comunicarse a través de una red.

Un host local puede hacer **ping** a un host en una red remota. Un ping exitoso a través de la red confirma la comunicación en la red local.

Nota: Muchos administradores de red limitan o prohíben la entrada de mensajes ICMP, por lo tanto, la falta de una respuesta de ping podría deberse a restricciones de seguridad.



Traceroute – probar la ruta

- Traceroute (**tracert**) es una utilidad que se utiliza para probar la ruta entre dos hosts y proporcionar una lista de los saltos que se alcanzaron con éxito a lo largo de esa ruta.
- Traceroute proporciona tiempo de ida y vuelta para cada salto a lo largo de la ruta e indica si un salto no responde. Se utiliza un asterisco (*) para indicar un paquete perdido o sin respuesta.
- Esta información se puede utilizar para localizar un enrutador problemático en la ruta o puede indicar que el enrutador está configurado para no responder.

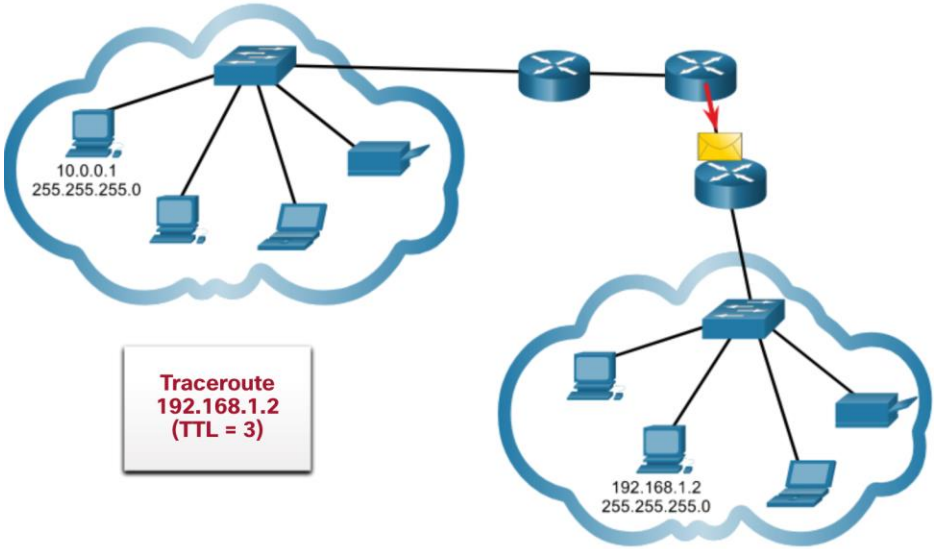
```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

  1   192.168.10.2    1 msec    0 msec    0 msec
  2   192.168.20.2    2 msec    1 msec    0 msec
  3   192.168.30.2    1 msec    0 msec    0 msec
  4   192.168.40.2    0 msec    0 msec    0 msec
```

Nota: Traceroute utiliza una función del campo TTL en IPv4 y el campo Hop Limit en IPv6 en los encabezados de Capa 3, junto con el mensaje ICMP Time Exceeded.

Traceroute – prueba la ruta (Cont.)

- El primer mensaje enviado tendrá un valor de campo TTL de 1. Esto hace que TTL expire el tiempo de espera en el primer enrutador. Luego, este enrutador responde con un mensaje de tiempo excedido ICMPv4.
- Luego, Traceroute incrementa progresivamente el campo TTL (2, 3, 4 ...) para cada secuencia de mensajes. Esto proporciona a la traza la dirección de cada salto a medida que los paquetes se agotan más adelante en la ruta.
- El campo TTL continúa aumentando hasta que se alcanza el destino, o se incrementa a un máximo predefinido.



Packet Tracer – Verificar direccionamiento IPv4 e IPv6

En este Packet Tracer, hará lo siguiente:

- Completar la documentación de la tabla de direccionamiento
- Probar la conectividad mediante ping
- Descubrir el camino trazando la ruta

Packet Tracer – Uso de ping y traceroute para probar coonectividad de red

En este Packet Tracer, hará lo siguiente:

- Probar y restaurar la conectividad IPv4
- Probar y restaurar la conectividad IPv6

13.3 Práctica del módulo y cuestionario

Packet Tracer – Uso de CMP para probar y corregir la conectividad de red

En este Packet Tracer, hará lo siguiente:

- Utilizar ICMP para localizar problemas de conectividad.
- Configurar los dispositivos de red para corregir problemas de conectividad.

Lab – Use Ping and Traceroute to Test Network Connectivity

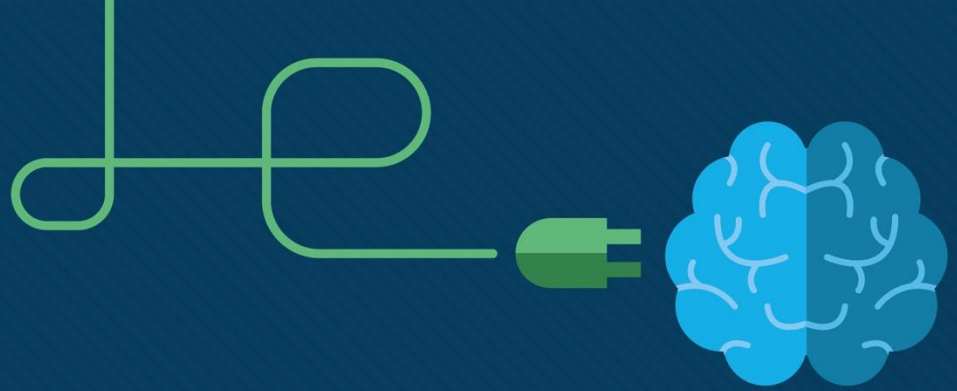
En este lab, completaras los siguientes objetivos:

- Construir y configurar una red
- Utilizar el comando **ping** para pruebas básicas de red
- Utilizar los comandos **tracert** y **traceroute** para pruebas de red básicas
- Solucionar problemas de topología

¿Qué aprendió en el módulo?

- El propósito de los mensajes ICMP es proporcionar información sobre problemas relacionados con el procesamiento de paquetes IP.
- Los mensajes ICMP comunes a ICMPv4 e ICMPv6 son: Accesibilidad del host, Destino o servicio inalcanzable y Tiempo excedido.
- Los mensajes entre un enrutador IPv6 y un dispositivo IPv6, incluida la asignación dinámica de direcciones, incluyen RS y RA. Los mensajes entre dispositivos IPv6 incluyen la redirección (similar a IPv4), NS y NA.
- Ping (utilizado por IPv4 e IPv6) utiliza la solicitud de eco ICMP y los mensajes de respuesta de eco para probar la conectividad entre hosts
- Ping se puede utilizar para probar la configuración interna de IPv4 o IPv6 en el host local.
- Traceroute (tracert) genera una lista de saltos que se alcanzaron con éxito a lo largo de la ruta.


CISCO



Módulo 14: Capa de transporte

Objetivos

Título: Capa de transporte

Objetivo: Compare the operations of transport layer protocols in supporting end-to-end communication.

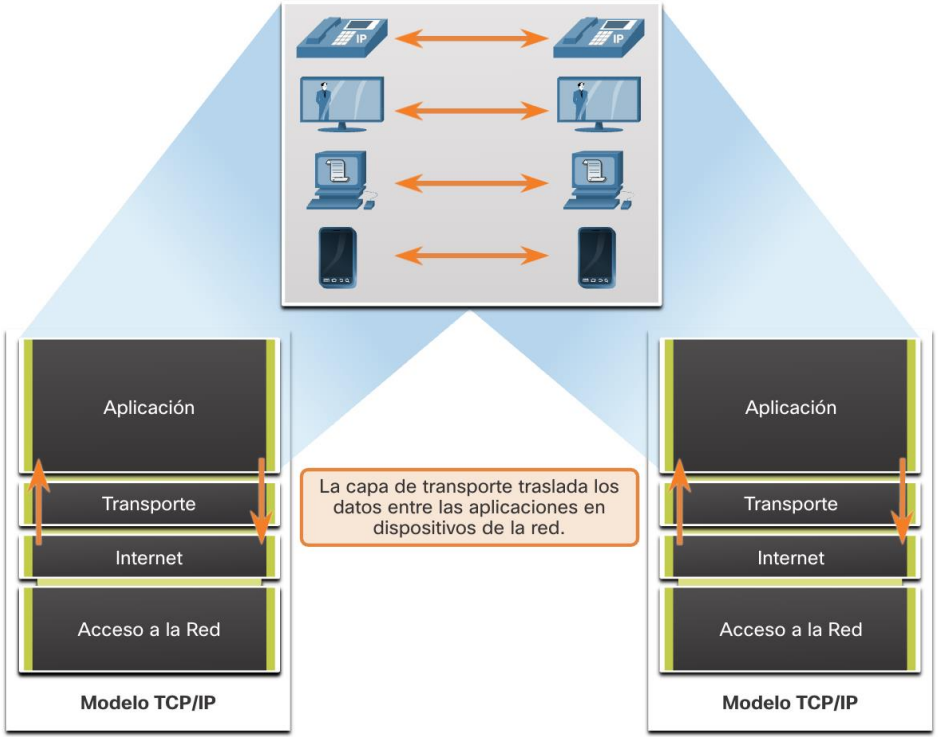
Título	Objetivo
Capa de transporte	Comparar las operaciones de los protocolos de la capa de transporte para admitir la comunicación de un extremo a extremo.
Descripción general de TCP	Explicar las características de TCP.
Descripción general de UDP	Explicar las características de UDP.
Números de puerto	Explica como utilizan los números de puertos TCP y UDP.
Procesos de comunicación TCP	Explicar como los procesos de establecimiento y terminación de sesiones TCP facilitan una comunicación confiable
Fiabilidad y control de flujo	Explicar cómo se transmiten y reconocen las unidades de datos del protocolo TCP para garantizar la entrega.
Comunicación UDP	Comparar las operaciones de los protocolos de la capa de transporte para admitir la comunicación de extremo a extremo.

14.1 Transporte de datos

Función de la capa de transporte

La capa de transporte es:

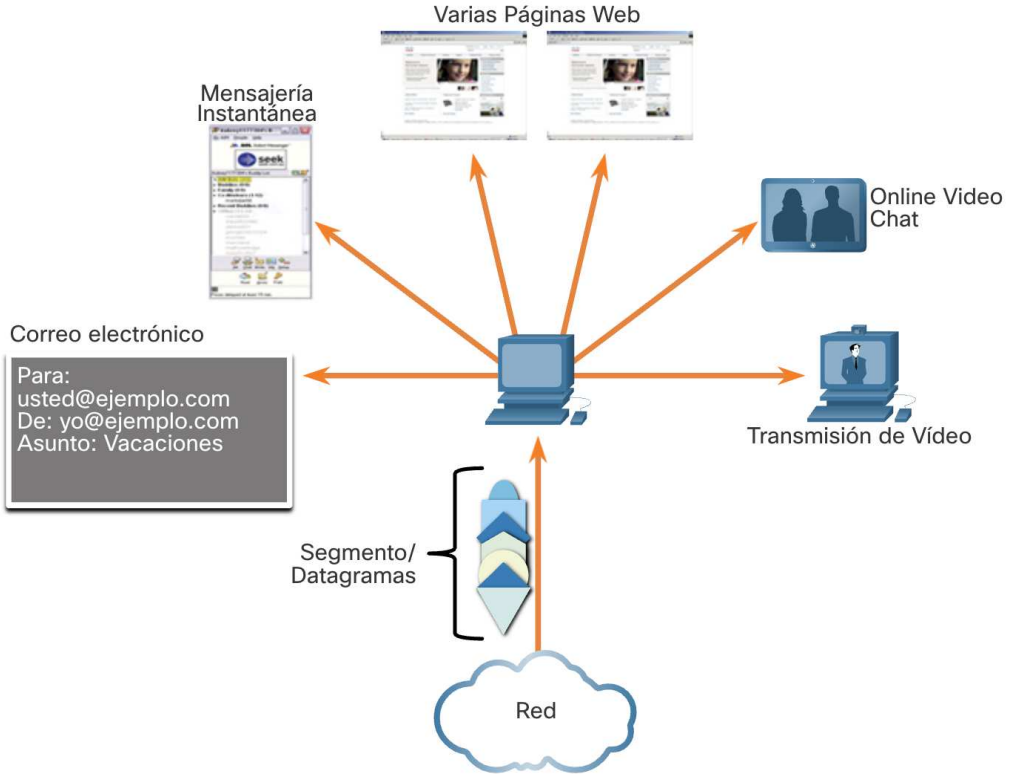
- responsable de las comunicaciones lógicas entre aplicaciones que se ejecutan en diferentes hosts.
- El enlace entre la capa de aplicación y las capas inferiores que son responsables de la transmisión de la red.



Responsibilidades de la capa de transporte

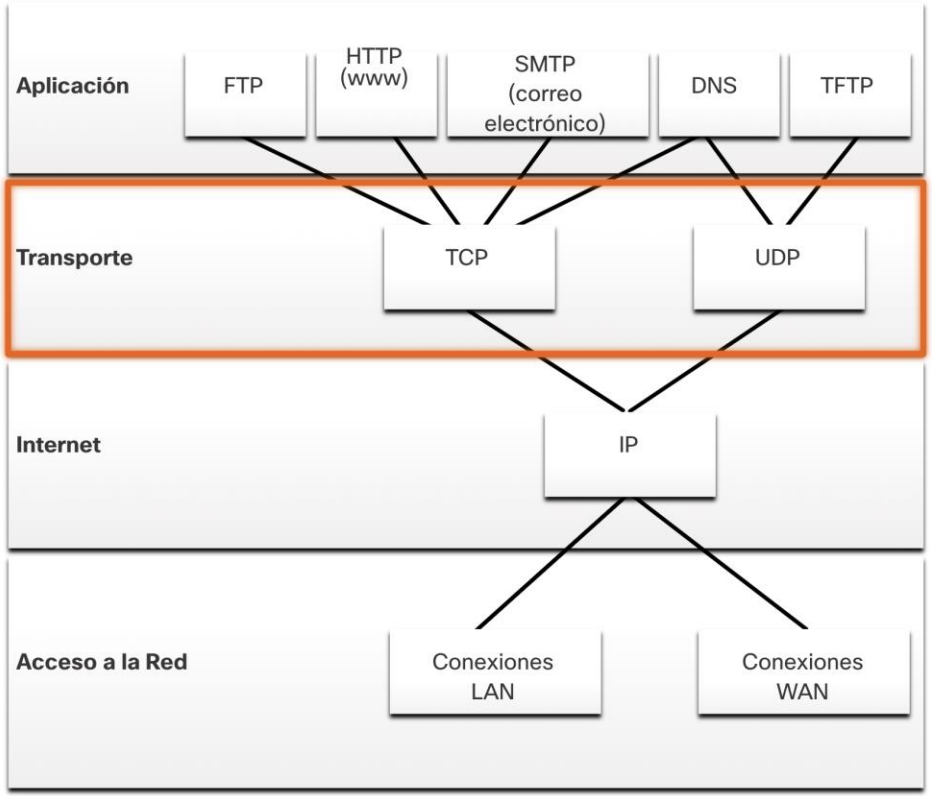
La capa de transporte tiene las siguientes responsabilidades:

- Seguimiento de conversaciones individuales
- Segmentar datos y reensamblar segmentos
- Agrega información de encabezado
- Identificar, separar y administrar múltiples conversaciones
- Utilizar la segmentación y multiplexación para permitir que diferentes conversaciones de comunicación se intercalen en la misma red.



Protocolos de capa de transporte

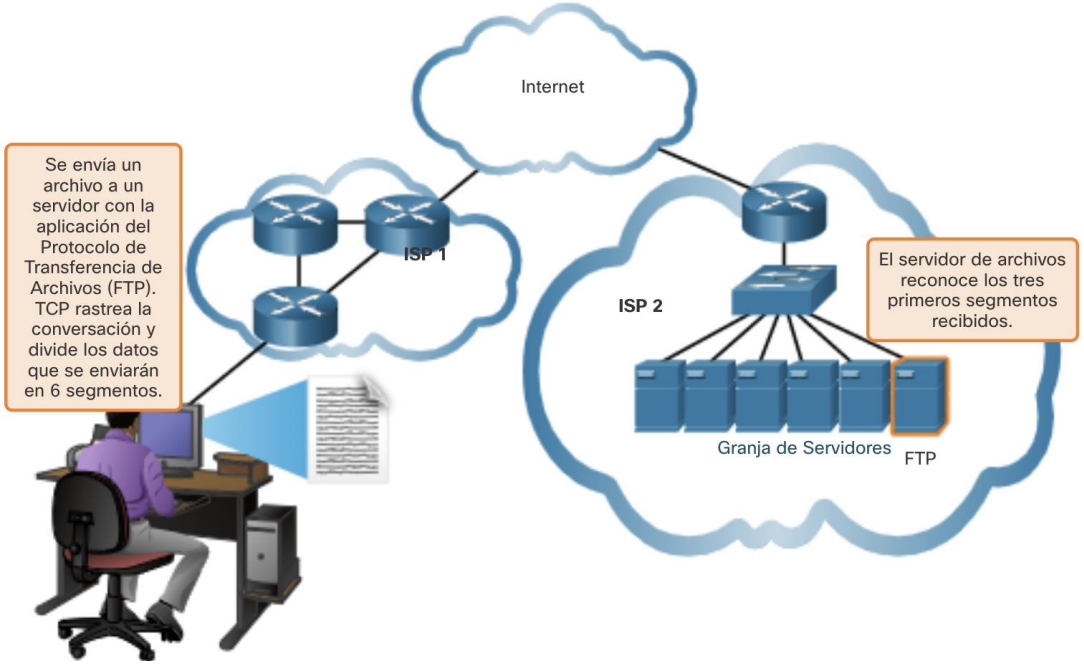
- IP no especifica cómo se realiza la entrega o transporte de los paquetes.
- Los protocolos de la capa de transporte especifican cómo transferir mensajes entre hosts y son responsables de administrar los requisitos de confiabilidad en una comunicación.
- La capa de transporte incluye los protocolos TCP y UDP.



Protocolo de transmisión y control (TCP)

TCP proporciona confiabilidad y control de flujo. Operaciones básicas de TCP:

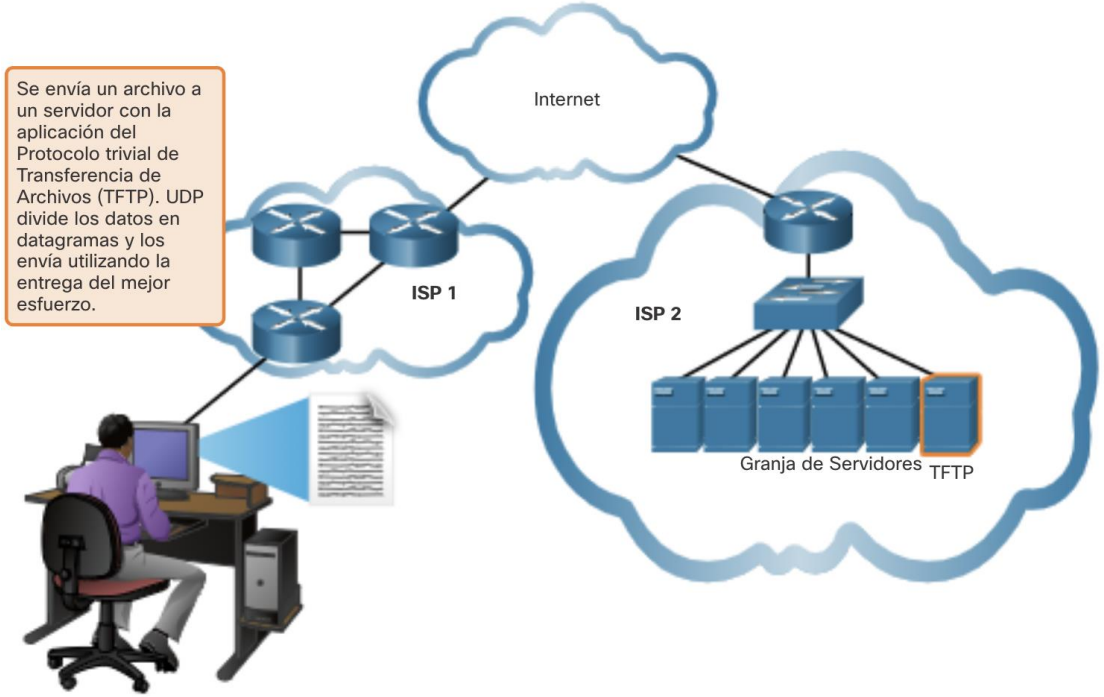
- Numera y rastrea segmentos de datos transmitidos a un host específico desde una aplicación específica
- Reconocer los datos recibidos
- Retransmitir los datos no reconocidos después de un cierto período de tiempo
- Secuencia de datos que pueden llegar en orden incorrecto
- Enviar datos a una velocidad eficiente que sea aceptable para el receptor



Protocolo de datagramas de usuario (UDP)

UDP proporciona las funciones básicas para entregar datagramas entre las aplicaciones apropiadas, con muy poca sobrecarga y poca verificación de datos.

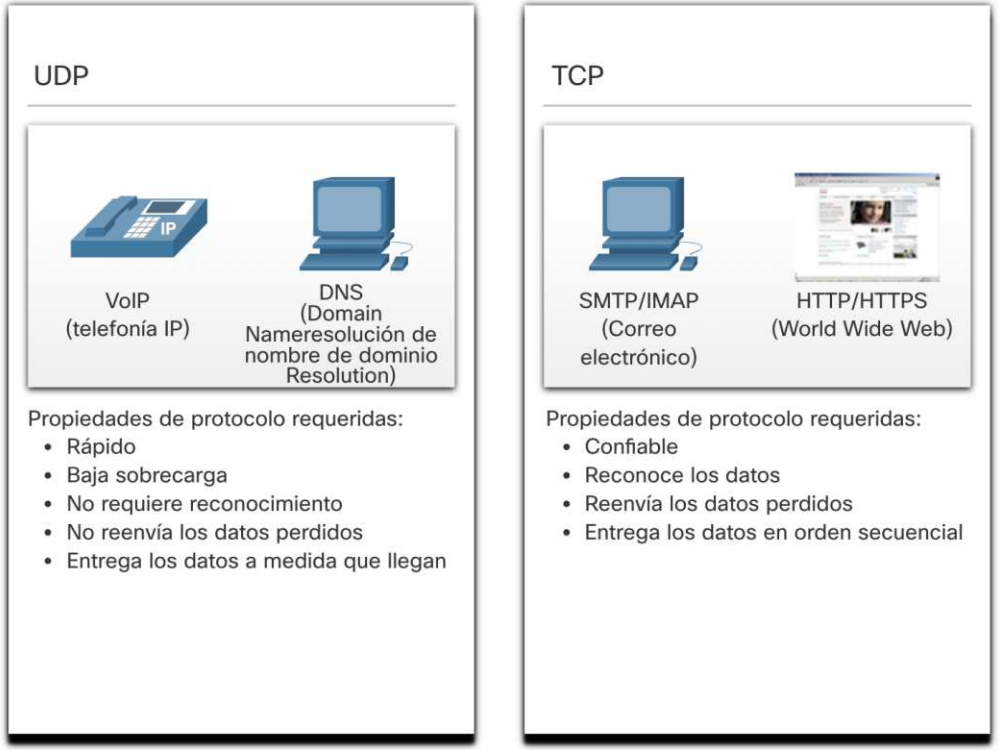
- UDP es un protocolo sin conexión.
- UDP se conoce como un protocolo de entrega best-effort porque no hay confirmación de que los datos se reciben en el destino.



El protocolo de capa de transporte adecuado para la aplicación adecuada

- UDP también se utiliza en aplicaciones de solicitud y respuesta en las que los datos son mínimos y la retransmisión se puede realizar rápidamente.

- Si es importante que lleguen todos los datos y que se puedan procesar en su secuencia adecuada, se utiliza TCP como protocolo de transporte.



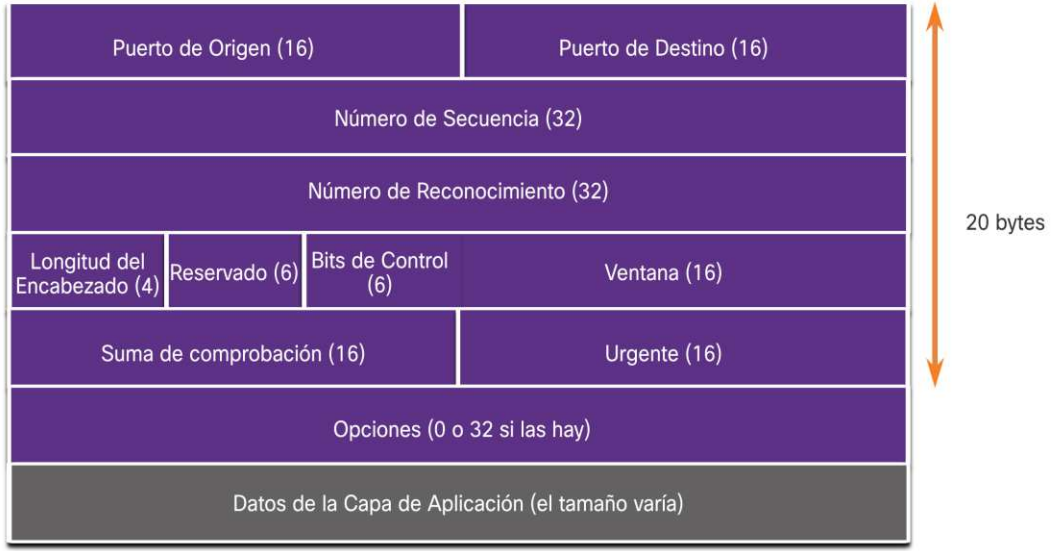
14.2 Descripción general de TCP

Características TCP

- **Establece una sesión:** TCP es un protocolo orientado a la conexión que negocia y establece una conexión (o sesión) permanente entre los dispositivos de origen y destino antes de reenviar el tráfico.
- **Garantiza una entrega confiable:** por muchas razones, es posible que un segmento se corrompa o se pierda por completo, ya que se transmite a través de la red. TCP asegura que cada segmento enviado por la fuente llegue al destino.
- **Proporciona entrega en el mismo orden:** debido a que las redes pueden proporcionar múltiples rutas que pueden tener diferentes velocidades de transmisión, los datos pueden llegar en el orden incorrecto.
- **Admite control de flujo:** los hosts de red tienen recursos limitados (i.e. memoria y potencia de procesamiento). Cuando estos recursos están sobrecargados, TCP puede solicitar que la aplicación emisora reduzca la tasa de flujo de datos.

Encabezado TCP

- TCP es un protocolo con estado, lo que significa que realiza un seguimiento del estado de la sesión de comunicación.
- TCP registra qué información ha enviado y qué información ha sido reconocida.

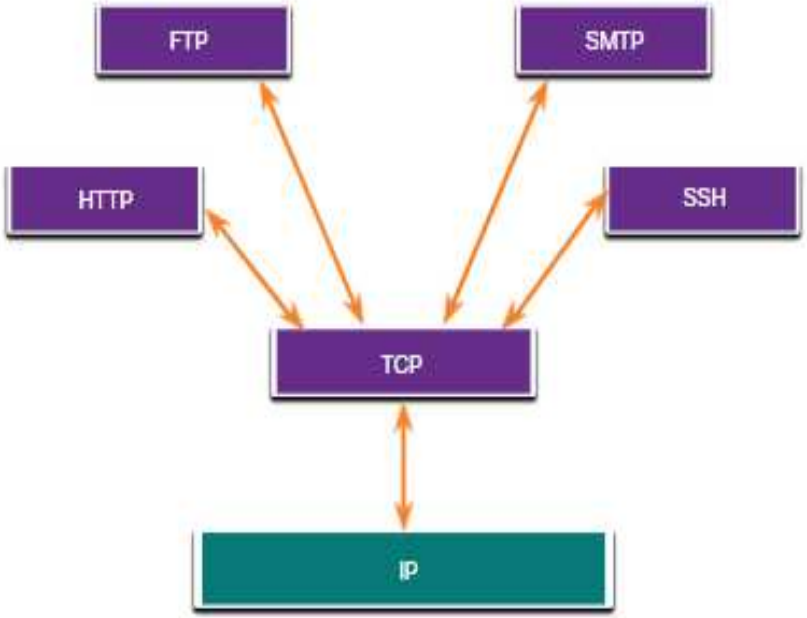


Campos en el encabezado TCP

Campo	Descripción
Puerto de origen	Campo de 16 bits para identificar la aplicación de origen por número de puerto.
Puerto de destino	Campo de 16 bits para identificar la aplicación de destino por número de puerto.
Número de secuencia	Campo de 32 bits que se utiliza para el reensamblaje de datos.
Número de acuse de recibo	Campo de 32 bits que se utiliza para indicar que se han recibido datos y el siguiente byte esperado de la fuente.
Longitud del encabezado	Campo de 4 bits conocido como "data-offset" que indica la longitud del encabezado del segmento TCP.
Reservado	Campo de 6 bits que está reservado para uso futuro.
Bits de control	Campo de 6 bits que incluye códigos de bits, o banderas, que indican el propósito y la función del segmento TCP.
Tamaño de ventana	Campo de 16 bits utilizado para indicar el número de bytes que se pueden aceptar a la vez.
Suma de comprobación	Caampo de 16 bits para la veridicación de errores en el segmento de datos y el header
Urgente	Campo de 16 bits que se utiliza para indicar si los datos contenidos son urgentes.

Applicaciones que utilizan TCP (act 14.10.7)

TCP maneja todas las tareas asociadas con la división del flujo de datos en segmentos, proporcionando confiabilidad, controlando el flujo de datos y reordenando segmentos.



14.3 Descripción general de UDP

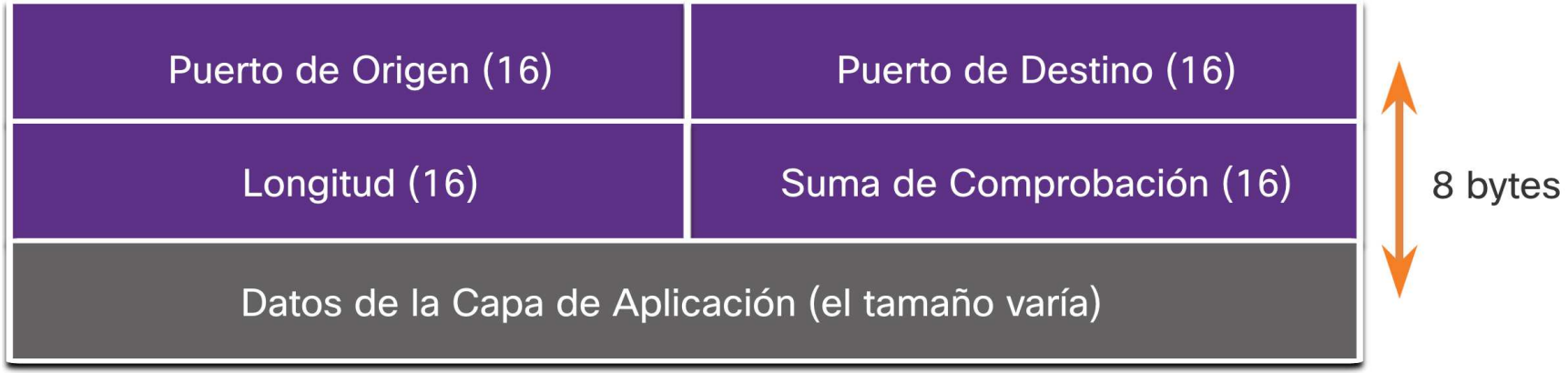
Características de UDP

Las características de UDP incluyen lo siguiente:

- Los datos se reconstruyen en el orden en que se reciben.
- Los segmentos que se pierden no se reenvían.
- No establece una sesión.
- El envío no está informado sobre la disponibilidad de recursos.

Encabezado UDP

El encabezado UDP es mucho más simple que el encabezado TCP porque solo tiene cuatro campos y requiere 8 bytes (es decir, 64 bits).

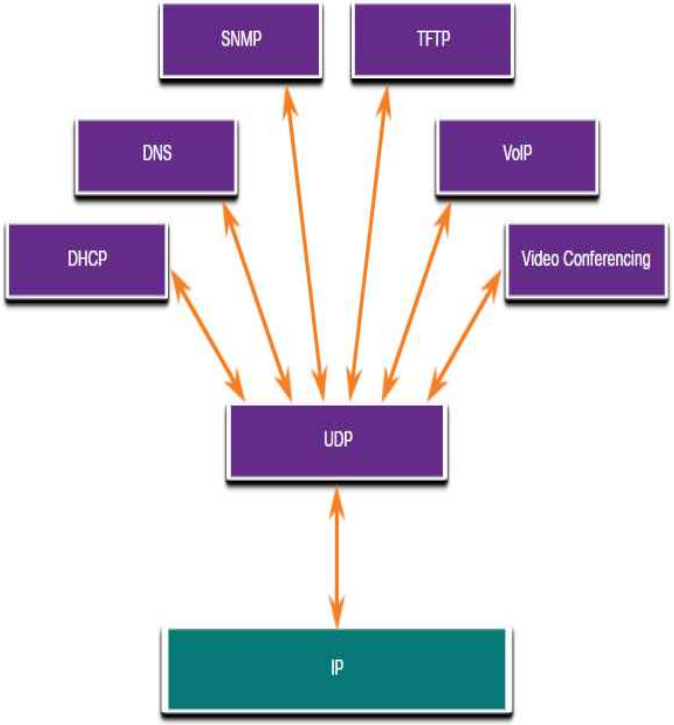


Campos del encabezado UDP

Campo UDP	Descrición
Puerto de origen	Campo de 16 bits para identificar la aplicación de origen por número de puerto.
Puerto de destino	Campo de 16 bits para identificar la aplicación de destino por número de puerto.
Longitud	Campo de 16 bits que indica la longitud del encabezado del datagrama UDP.
Suma de comprodación	Campo de 16 bits utilizado para la comprobación de errores del encabezado y los datos del datagrama.

Applicaciones que utilizan UDP

- Aplicaciones multimedia y de video en vivo: estas aplicaciones pueden tolerar cierta pérdida de datos, pero requieren poca o ninguna demora. Los ejemplos incluyen VoIP y transmisión de video en vivo.
- Aplicaciones de solicitud y respuesta simples: aplicaciones con transacciones simples en las que un host envía una solicitud y puede o no recibir una respuesta. Los ejemplos incluyen DNS y DHCP.
- Aplicaciones que manejan la confiabilidad por sí mismas: comunicaciones unidireccionales donde el control de flujo, la detección de errores, los reconocimientos y la recuperación de errores no son necesarios o pueden ser manejados por la aplicación. Los ejemplos incluyen SNMP y TFTP.



14.4 Números de puerto

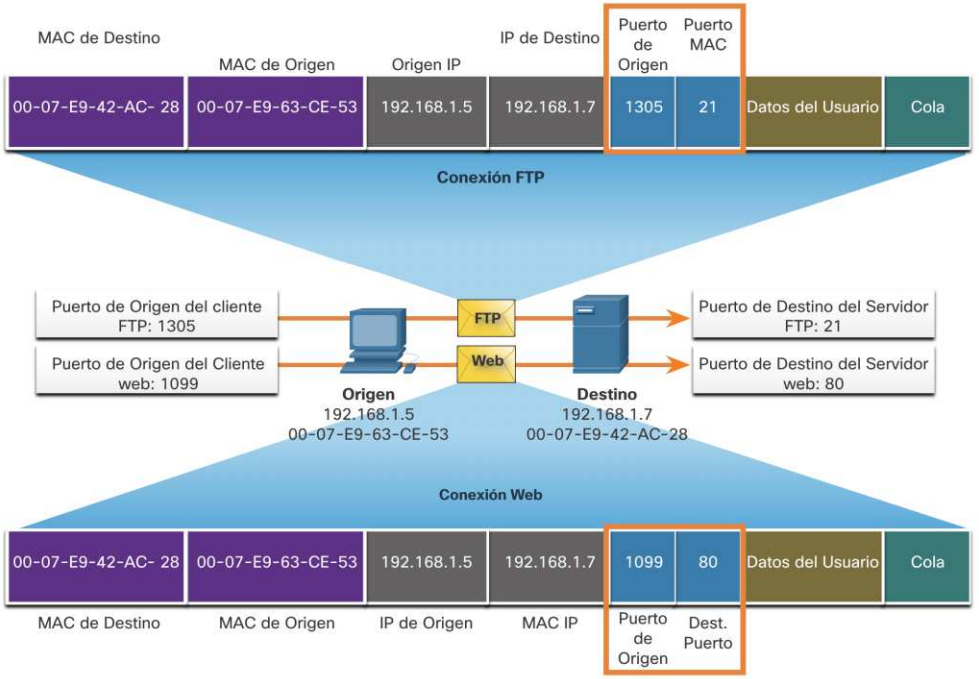
Comunicaciones múltiples separadas

Los protocolos de capa de transporte TCP y UDP utilizan números de puerto para administrar múltiples conversaciones simultáneas.

El número de puerto de origen está asociado con la aplicación de origen en el host local, mientras que el número de puerto de destino está asociado con la aplicación de destino en el host remoto.

Pares de Sockets

- Los puertos de origen y destino se colocan dentro del segmento.
- Luego, los segmentos se encapsulan dentro de un paquete IP.
- La combinación de la dirección IP de origen y el número de puerto de origen, o la dirección IP de destino y el número de puerto de destino se conoce como socket.
- Los sockets permiten que varios procesos, que se ejecutan en un cliente, se distingan entre sí, y que varias conexiones a un proceso de servidor se distingan entre sí.



Grupos de números de puerto

Grupo de puertos	Rango de números	Descripción
Puertos bien conocidos	0 to 1,023	•Números de puerto reservados para servicios comunes o populares y aplicaciones como navegadores web, clientes de correo electrónico y acceso remoto clientes. •Los puertos conocidos definidos para aplicaciones de servidor comunes permiten para identificar fácilmente el servicio asociado requerido.
Puertos registrados	1,024 to 49,151	•Asignados por IANA a una entidad solicitante para utilizar con procesos o aplicaciones específicos. •Principalmente aplicaciones individuales de usuario. Por ejemplo, Cisco ha registrado el puerto 1812 para el proceso de autenticación de su servidor RADIUS
Privados y/o puertos dinámicos	49,152 to 65,535	• Asignados dinámicamente por el SO cuando se inicia una conexión a un servicio. • El puerto dinámico se utiliza para identificar la aplicación del cliente. durante la comunicación

Grupos de números de puerto (Cont.)

Puertos bien conocidos

Port Number	Protocol	Application
20	TCP	File Transfer Protocol (FTP) - Data
21	TCP	File Transfer Protocol (FTP) - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP, TCP	Domain Name Service (DNS)
67	UDP	Dynamic Host Configuration Protocol (DHCP) - Server
68	UDP	Dynamic Host Configuration Protocol - Client
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol version 3 (POP3)
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)

El comando netstat(act 14.4.5)

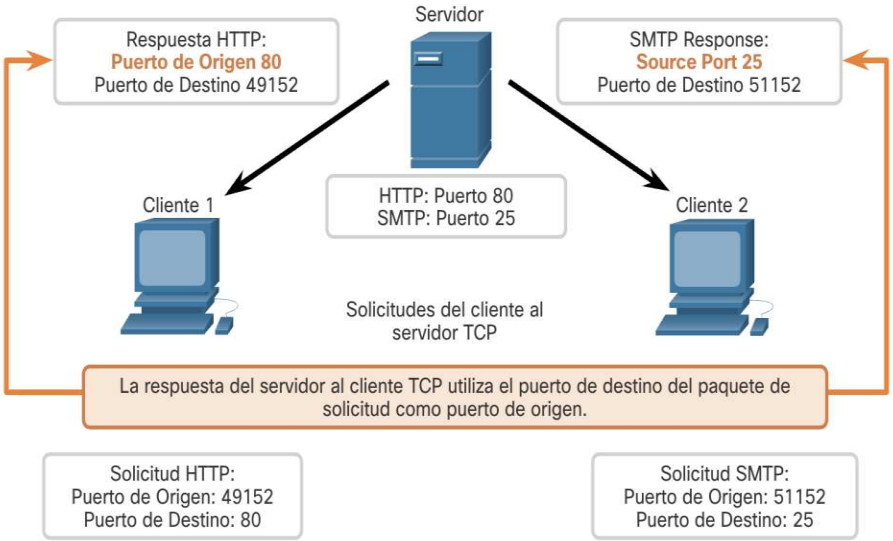
Las conexiones TCP no documentadas pueden representar una gran amenaza para la seguridad. Netstat es una herramienta importante para verificar conexiones.

```
C:\> netstat
Active Connections
Proto Local Address          Foreign Address          State
TCP   192.168.1.124:3126     192.168.0.2:netbios-ssn  ESTABLISHED
TCP   192.168.1.124:3158     207.138.126.152:http     ESTABLISHED
TCP   192.168.1.124:3159     207.138.126.169:http     ESTABLISHED
TCP   192.168.1.124:3160     207.138.126.169:http     ESTABLISHED
TCP   192.168.1.124:3161     sc.msn.com:http          ESTABLISHED
TCP   192.168.1.124:3166     www.cisco.com:http       ESTABLISHED
```

14.5 Proceso de comunicación TCP

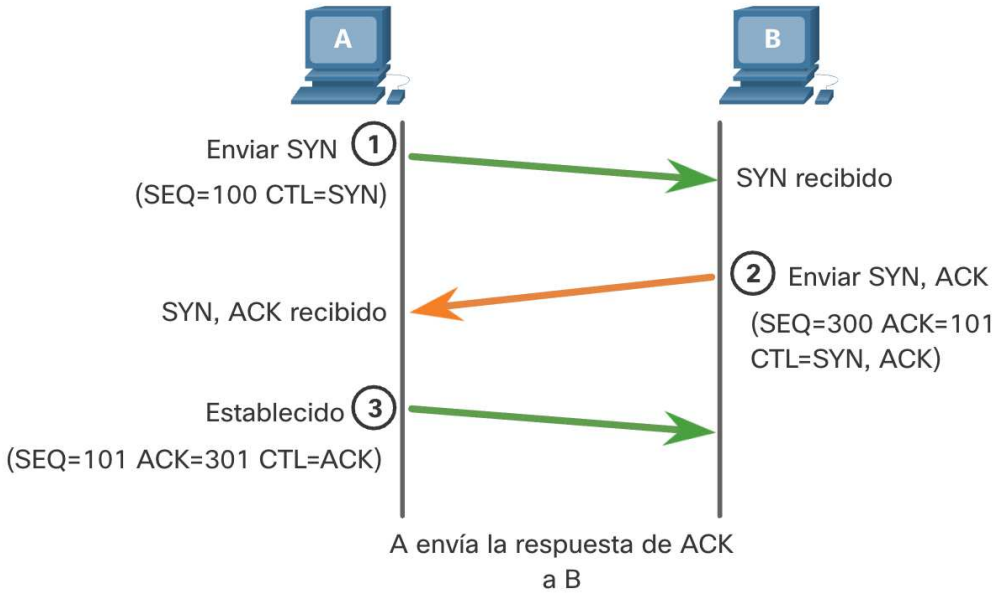
Procesos del servidor TCP

- Cada proceso de aplicación que se ejecuta en un servidor está configurado para usar un número de puerto.
- Un servidor individual no puede tener dos servicios asignados al mismo número de puerto dentro de los mismos servicios de capa de transporte.
- Una aplicación de servidor activa asignada a un puerto específico se considera abierta, lo que significa que la capa de transporte acepta y procesa los segmentos dirigidos a ese puerto.
- Se acepta cualquier solicitud de cliente entrante dirigida al socket correcto y los datos se pasan a la aplicación del servidor.



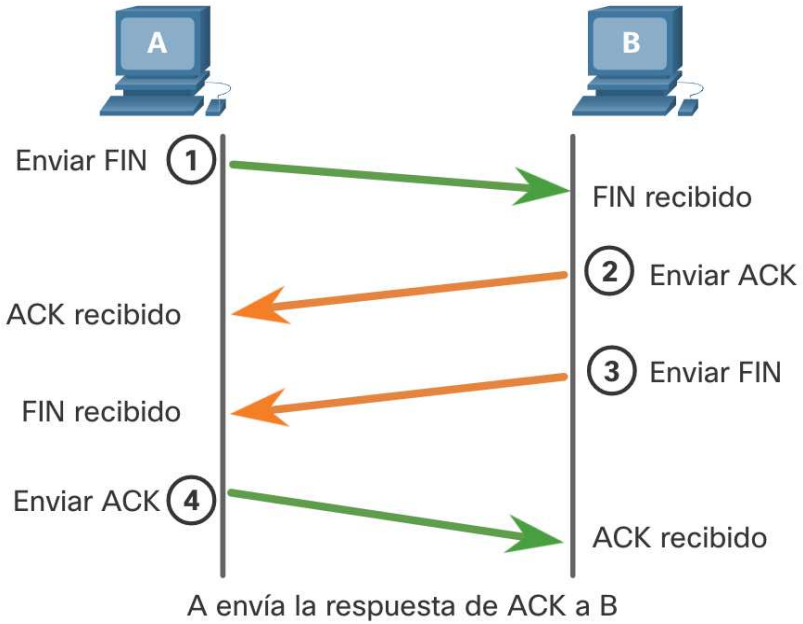
Establecimiento de conexiones TCP

- Paso 1: el cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor.
- Paso 2: el servidor reconoce la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.
- Paso 3: el cliente reconoce la sesión de comunicación de servidor a cliente.



Terminacion de sesión

- Paso 1: cuando el cliente no tiene más datos para enviar en el flujo, envía un segmento con la bandera FIN establecida.
- Paso 2: El servidor envía un ACK para acusar recibo del FIN para terminar la sesión de cliente a servidor.
- Paso 3: el servidor envía un FIN al cliente para finalizar la sesión de servidor a cliente.
- Paso 4: El cliente responde con un ACK para reconocer el FIN del servidor.



Análisis del enlace TCP de tres vías

Funciones del enlace de tres vías:

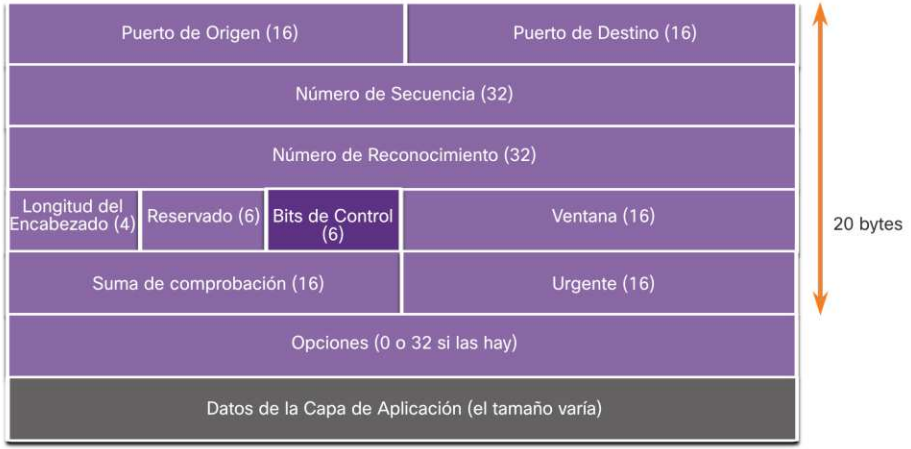
- Establecer que el dispositivo de destino está presente en la red.
- Verificar que el dispositivo de destino tiene un servicio activo y está aceptando solicitudes en el número de puerto de destino que el cliente iniciador tiene la intención de usar.
- Informar al dispositivo de destino que el cliente de origen tiene la intención de establecer una sesión de comunicación en ese número de puerto.

Una vez finalizada la comunicación, se cierran las sesiones y se termina la conexión. Los mecanismos de conexión y sesión habilitan la función de confiabilidad de TCP.

Análisis del enlace TCP de tres vías (Cont.)

Los seis indicadores de bits de control son los siguientes:

- **URG**: campo de puntero urgente significativo
- **ACK**: bandera de acuse de recibo utilizada en el establecimiento de la conexión y la terminación de la sesión
- **PSH** - Función Push
- **RST**: restablece la conexión cuando se produce un error o se agota el tiempo de espera
- **SYN**: sincroniza los números de secuencia utilizados en el establecimiento de la conexión
- **FIN**: no hay más datos del remitente y se utilizan en la terminación de la sesión



Video enlace TCP de tres vias(act 14.5.5)

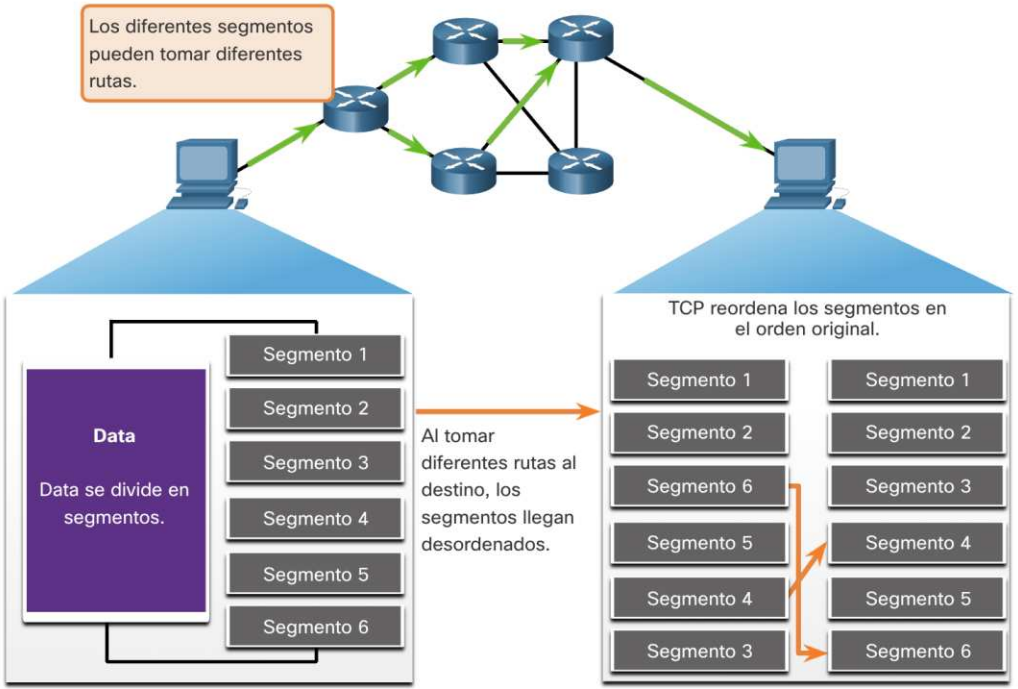
El video cubre lo siguiente:

- Protocolo de enlace de 3 vías TCP
- Terminación de una conversación TCP

14.6 Confiabilidad y control de flujo

Confiabilidad de TCP: entrega garantizada y en orden

- TCP también puede ayudar a mantener el flujo de paquetes para que los dispositivos no se sobrecarguen.
- Puede haber ocasiones en las que los segmentos TCP no lleguen a su destino o lleguen fuera de orden.
- Todos los datos deben recibirse y los datos de estos segmentos deben volver a ensamblarse en el orden original.
- Los números de secuencia se asignan en el encabezado de cada paquete para lograr este objetivo.

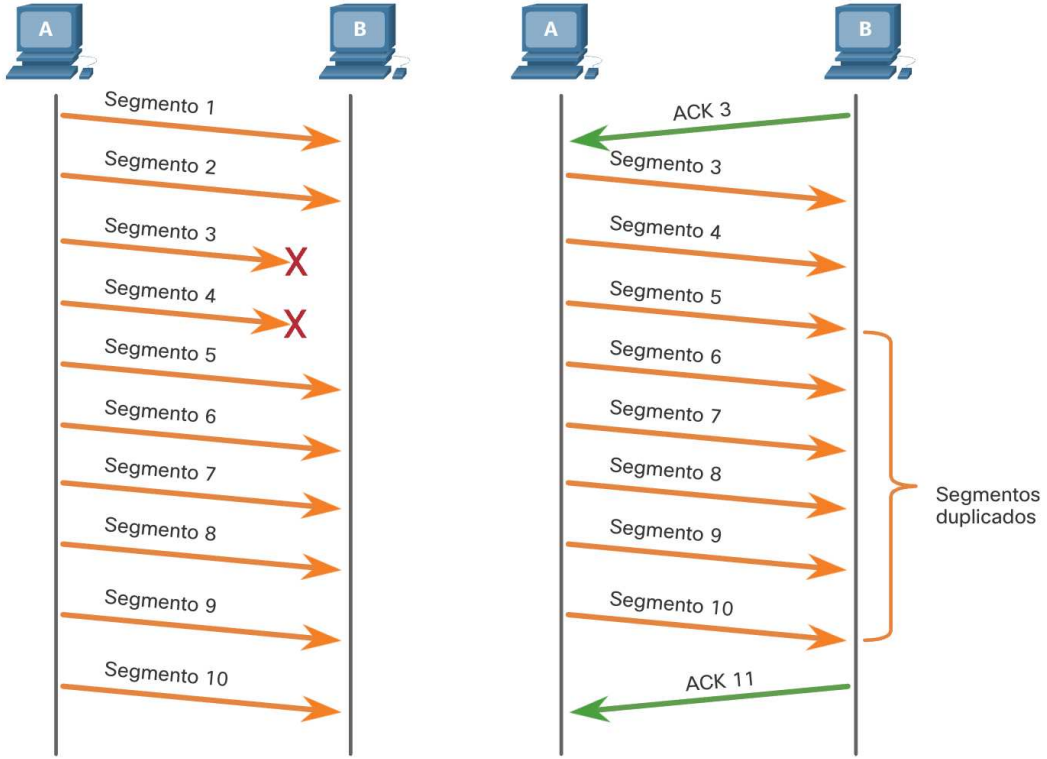


Video -Confiabilidad de TCP- Números de secuencia y acuse de recibo (act 14.6.4)

Este video muestra un ejemplo simplificado de las operaciones de TCP.

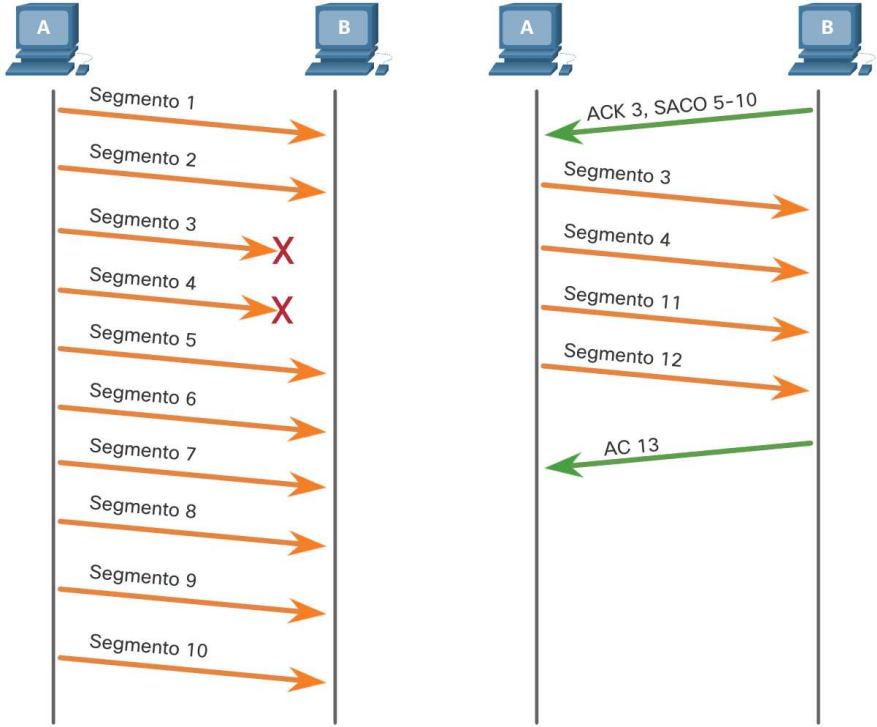
Confiabilidad de TCP – Retransmición y pérdida de datos

- No importa qué tan bien diseñada esté una red, ocasionalmente se producen pérdidas de datos.
- TCP proporciona métodos para gestionar estas pérdidas de segmentos. Entre estos se encuentra un mecanismo para retransmitir segmentos de datos no reconocidos.



Confiabilidad de TCP – Retransmición y pérdida de datos (Cont.)

- En la actualidad, los sistemas operativos de host suelen emplear una función TCP opcional denominada reconocimiento selectivo (SACK), que se negocia durante el protocolo de enlace de tres vías.
- Si ambos hosts admiten SACK, el receptor puede reconocer explícitamente qué segmentos (bytes) se recibieron, incluidos los segmentos discontinuos.

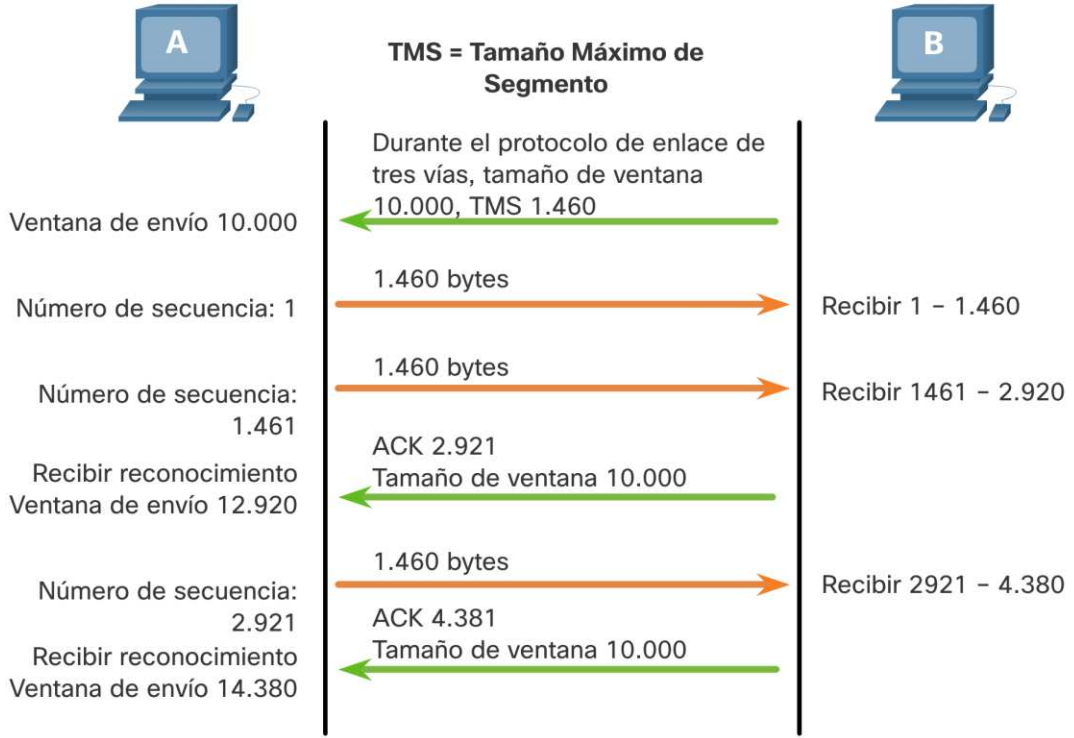


Video - Confiabilidad de TCP – Retransmición y pérdida de datos (14.6.4)

Este video muestra el proceso de reenvío de segmentos que el destino no recibió.

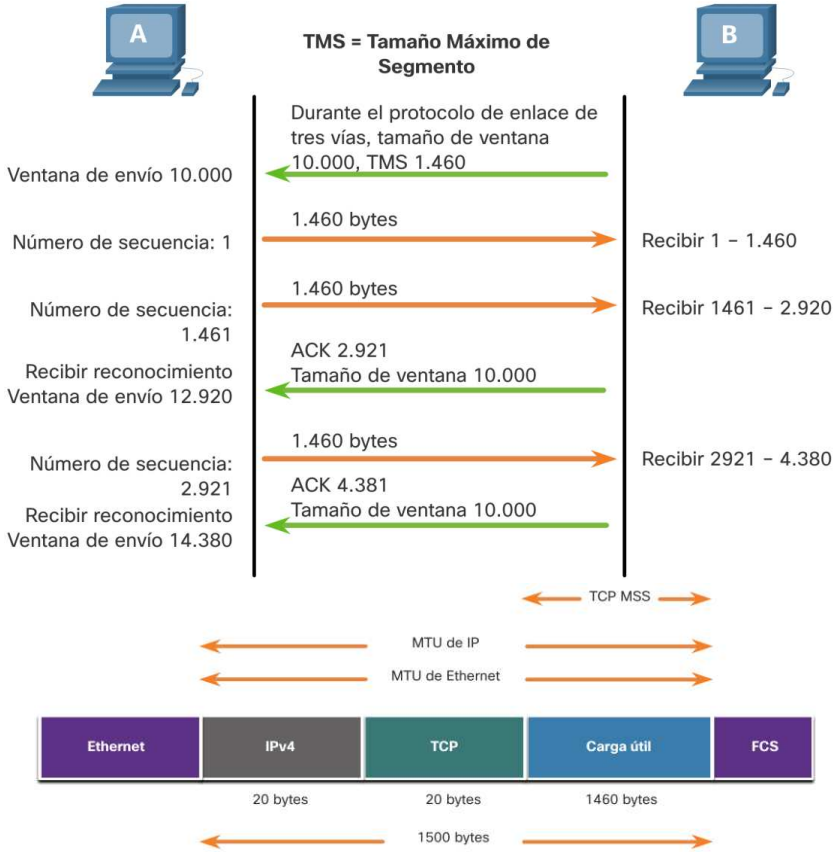
Control de flujo TCP – Tamaño de ventana y Acknowledgments

- TCP también proporciona los siguientes mecanismos para el control de flujo:
  - El control de flujo es la cantidad de datos que el destino puede recibir y procesar de manera confiable.
  - El control de flujo ayuda a mantener la confiabilidad de la transmisión TCP ajustando la tasa de flujo de datos entre el origen y el destino para una sesión determinada.



Control de flujo TCP – Tamaño máximo de segmento

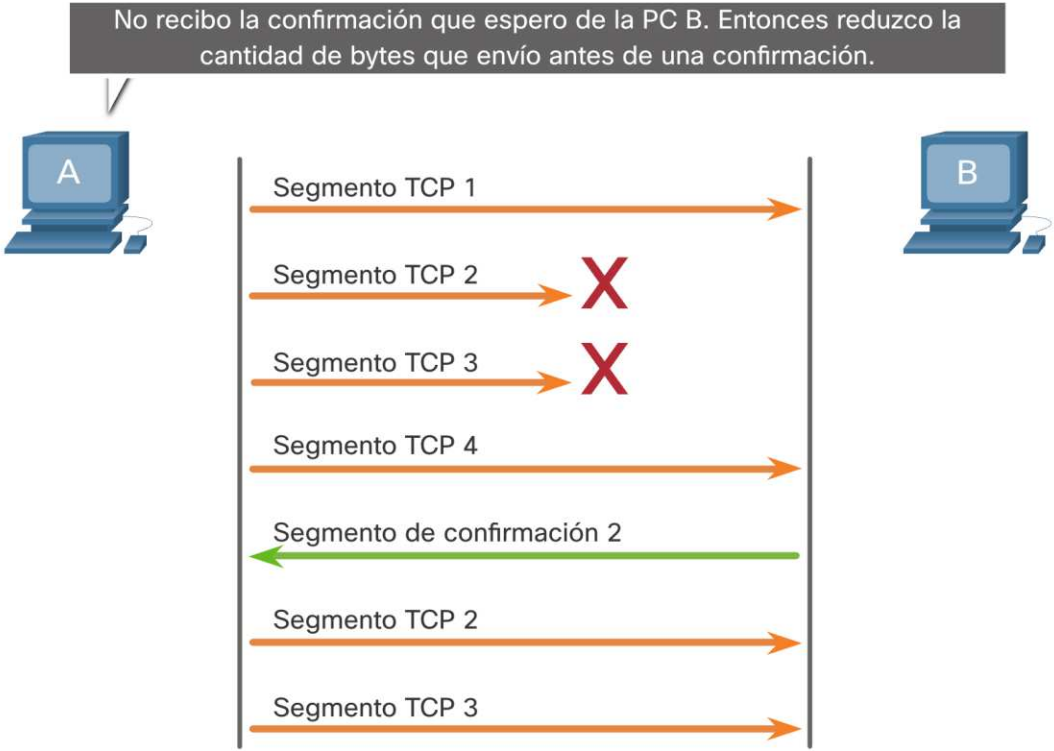
- El tamaño máximo de segmento (MSS) es la cantidad máxima de datos que puede recibir el dispositivo de destino.
- Un MSS común es de 1460 bytes cuando se usa IPv4.
- Un host determina el valor de su campo MSS restando los encabezados IP y TCP de la unidad de transmisión máxima de Ethernet (MTU), que es 1500 bytes por defecto.
- 1500 menos 40 (20 bytes para el encabezado IPv4 y 20 bytes para el encabezado TCP) deja 1460 bytes.



Control de flujo TCP – Prevención de congestiones (act 14.6.8)

- Cuando se produce una congestión en una red, el enrutador sobrecargado descarta paquetes.

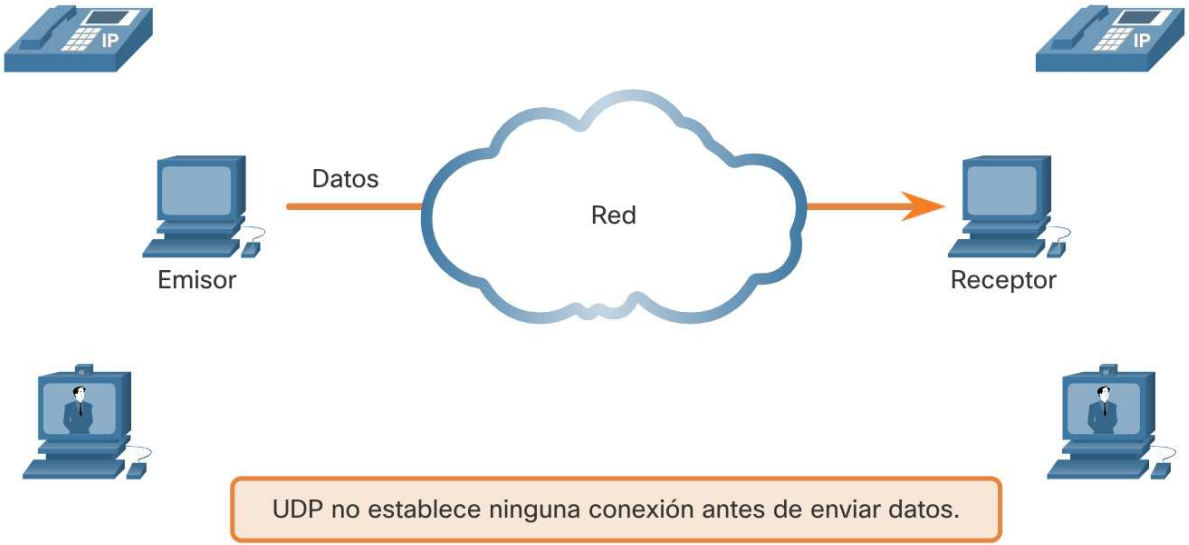
- Para evitar y controlar la congestión, TCP emplea varios mecanismos, temporizadores y algoritmos de manejo de la congestión.



14.7 Comunicación UDP

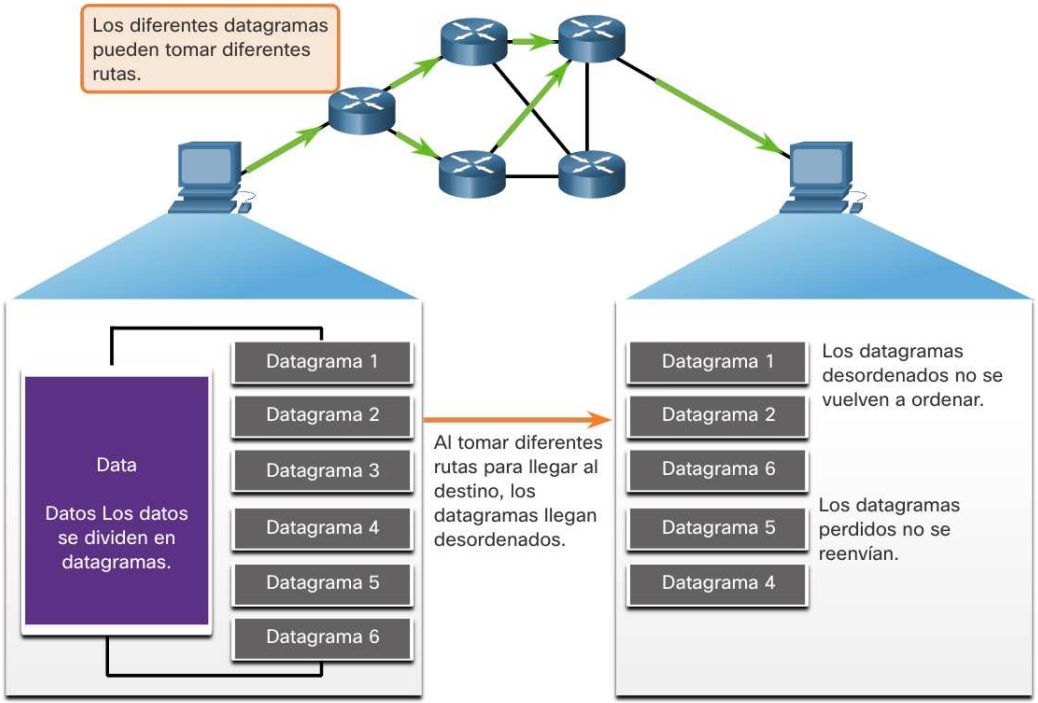
UDP baja sobrecarga versus confiabilidad

UDP no establece una conexión. UDP proporciona un transporte de datos de baja sobrecarga porque tiene un encabezado de datagrama pequeño y no tiene tráfico de administración de red.



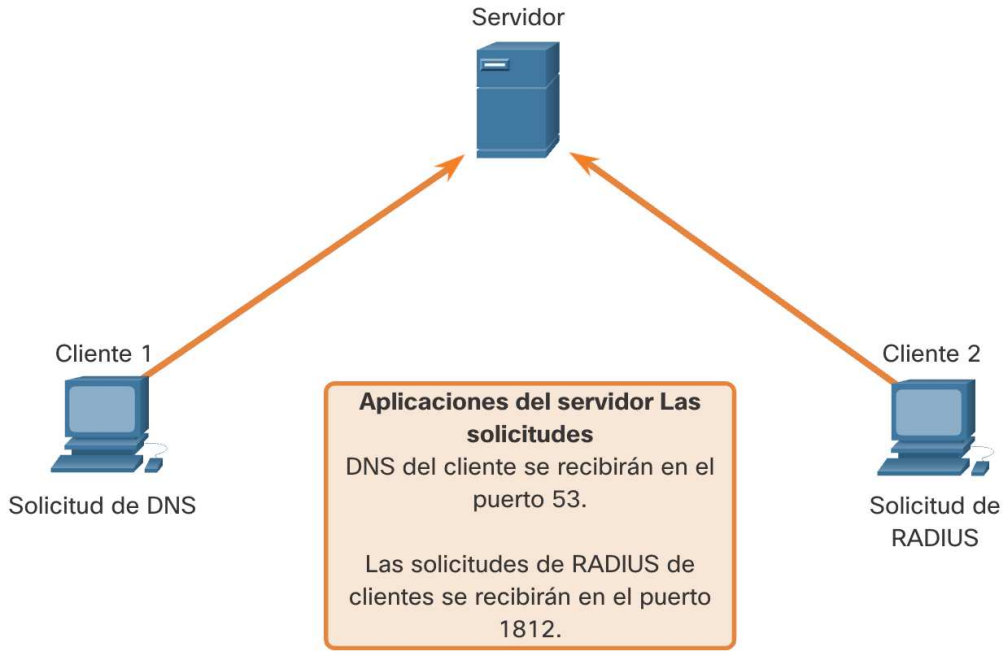
Reensamblaje del datagramas UDP

- UDP no rastrea los números de secuencia como lo hace TCP.
- UDP no tiene forma de reordenar los datagramas en su orden de transmisión.
- UDP simplemente vuelve a ensamblar los datos en el orden en que se recibieron y los reenvía a la aplicación.



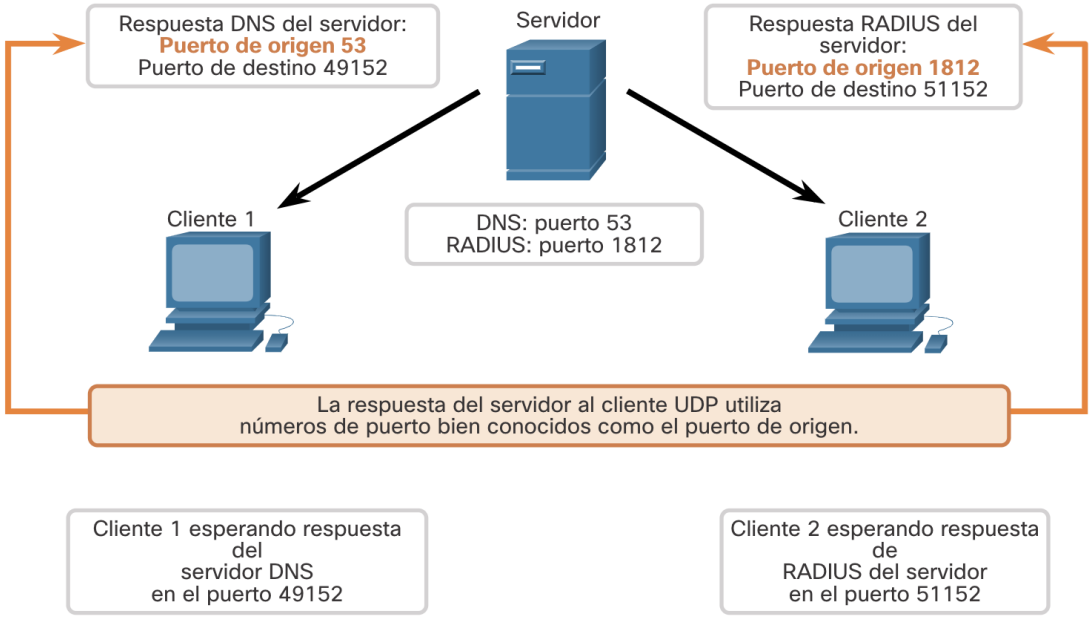
Procesos y solicitudes del servidor UDP

- Las aplicaciones de servidor basadas en UDP se les asignan números de puerto bien conocidos o registrados.
- UDP recibe un datagrama destinado a uno de estos puertos, reenvía los datos de la aplicación a la aplicación adecuada en función de su número de puerto.



Procesos del cliente UDP

- El proceso del cliente UDP selecciona dinámicamente un número de puerto del rango de números de puerto y lo usa como el puerto de origen.
- El puerto de destino suele ser el número de puerto registrado o conocido asignado al proceso del servidor.
- Una vez que un cliente ha seleccionado los puertos de origen y destino, se utiliza el mismo par de puertos en el encabezado de todos los datagramas de la transacción.



14.8 Práctica del módulo y cuestionario

Packet Tracer – Comunicaciones TCP y UDP (14.8.1)

En este Packet Tracer, hará lo siguiente:

- Genere tráfico de red en modo de simulación.
- Examine la funcionalidad de los protocolos TCP y UDP.

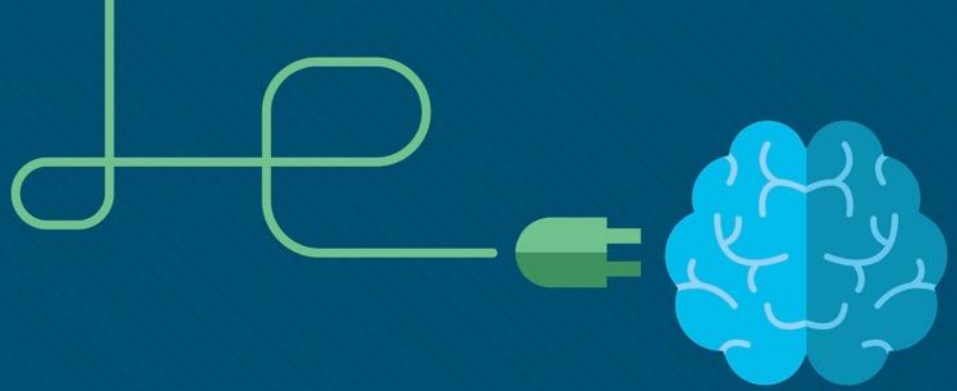
¿Qué aprendió en este módulo?

- La capa de transporte es el enlace entre la capa de aplicación y las capas inferiores que son responsables de la transmisión de la red.
- La capa de transporte incluye TCP y UDP.
- TCP establece sesiones, garantiza la confiabilidad, proporciona entregas y admite el control de flujo.
- UDP es un protocolo simple que proporciona las funciones básicas de la capa de transporte.
- UDP reconstruye los datos en el orden en que se reciben, los segmentos perdidos no se reenvían, no se establece la sesión y UPD no informa al remitente de la disponibilidad de recursos.
- Los protocolos de la capa de transporte TCP y UDP usan números de puerto para administrar múltiples conversaciones simultáneas.
- Cada proceso de aplicación que se ejecuta en un servidor está configurado para usar un número de puerto.

¿Qué aprendió en este módulo? (Cont.)

- El número de puerto lo asigna automáticamente o lo configura manualmente un administrador del sistema.
- Para que el destinatario entienda el mensaje original, se deben recibir todos los datos y los datos de estos segmentos deben volver a ensamblarse en el orden original.
- Los números de secuencia se asignan en el encabezado de cada paquete.
- El control de flujo ayuda a mantener la confiabilidad de la transmisión TCP ajustando la tasa de flujo de datos entre el origen y el destino.
- Una fuente podría estar transmitiendo 1460 bytes de datos dentro de cada segmento de TCP. Este es el MSS típico que puede recibir un dispositivo de destino.
- El proceso por el que el destino envía reconocimientos a medida que procesa los bytes recibidos y el ajuste continuo de la ventana de envío de la fuente se conoce como ventanas deslizantes.
- Para evitar y controlar la congestión, TCP emplea varios mecanismos de manejo de la congestión.


CISCO



Módulo 15: Capa de Aplicación

Introduction to Networks v7.0
(ITN)

Objetivos

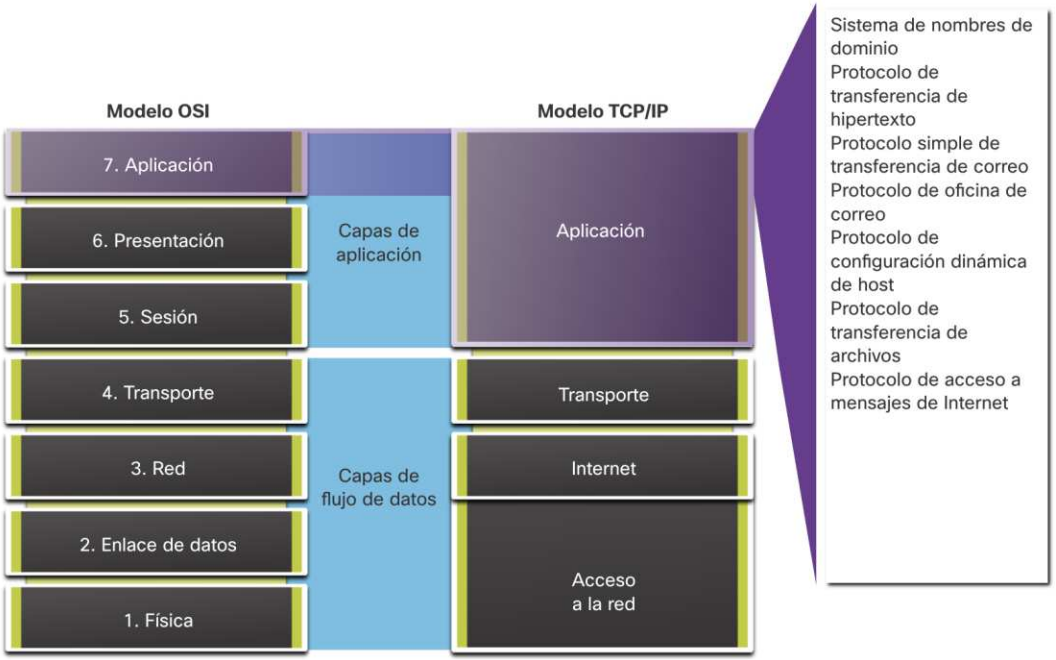
- **Título**: Capa de Aplicación
- **Objetivos**: Explicar el funcionamiento de los protocolos de la capa de aplicación

Tema	Objetivo
Aplicación, presentación y sesión	Explicar cómo las funciones de la capa de aplicación, la capa de presentación y la capa de sesión trabajan en conjunto para proporcionar servicios de red a las aplicaciones del usuario final.
Peer-to-Peer	Explicar cómo funcionan las aplicaciones de usuario final en una red peer-to-peer.
Protocolos web y de correo electrónico	Explicar como operan los protocolos web y de corre electrónico
Servicios de direccionamiento IP	Explicar como funcionan DNS y DHCP
Servicios de transferencia de archivos	Explicar como operan los protocolos de transferencia de archivos

15.1 Aplicación, Presentación y Sesión

Capa de aplicación

- Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) definen funciones de la capa de aplicación TCP/IP.
- La capa de aplicación proporciona la interfaz entre las aplicaciones utilizadas para comunicarse y la red subyacente a través de la cual se transmiten los mensajes.
- Algunos de los protocolos de capa de aplicación más conocidos incluyen HTTP, FTP, TFTP, IMAP y DNS.



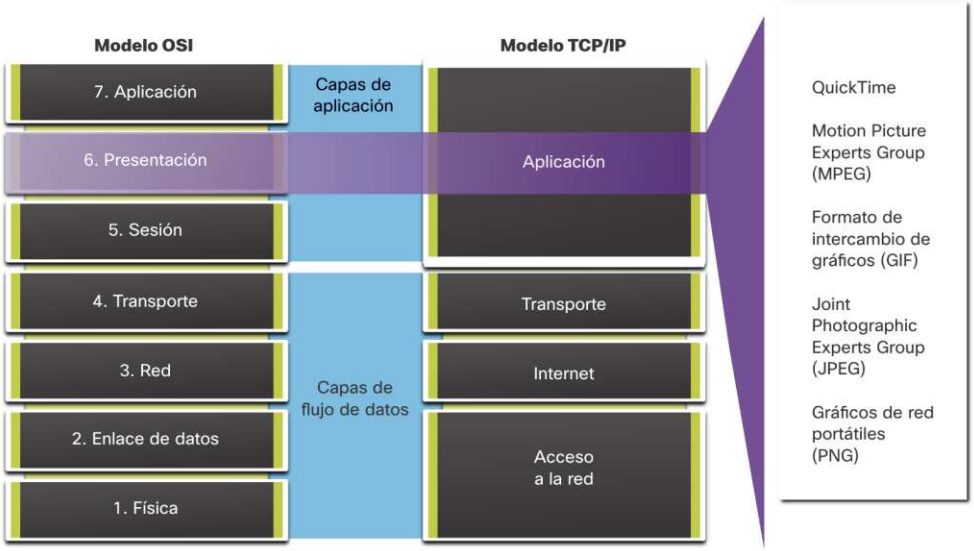
Capas de presentación y de sesión

La capa de presentación tiene tres funciones principales:

- Formatear o presentar los datos en el dispositivo de origen en un formato compatible para que el dispositivo de destino los reciba
- Comprimir datos de una manera que el dispositivo de destino pueda descomprimir
- Cifrar datos para transmitirlos y descifrarlos al recibirlos

La capa de sesión es responsible de:

- Crear y mantener los diálogos entre aplicaciones de origen y destino.
- Manejar el intercambio de información para iniciar diálogos, mantenerlos activos y reiniciar sesiones interrumpidas o inactivas durante un largo período de tiempo.



Protocolos de capa de aplicación TCP/IP (act 15.1.4)

- Los protocolos de aplicación TCP/IP especifican el formato y la información de control necesaria para muchas funciones comunes de comunicación de Internet.
- Los protocolos de la capa de aplicación son utilizados tanto por los dispositivos de origen como por los de destino durante una sesión de comunicación.
- Para que las comunicaciones sean exitosas, los protocolos de la capa de aplicación que se implementan en el host de origen y destino deben ser compatibles.

Sistema de nombres
DNS - Domain Name System (o Service)
- TCP, UDP cliente 53
- Traduce los nombres de dominio, como cisco.com, a direcciones IP.

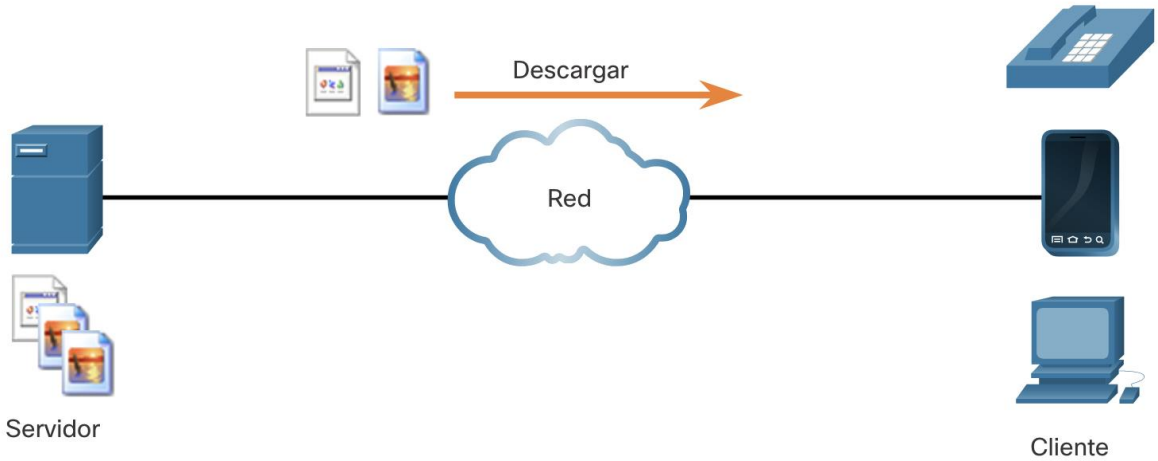
Configuración de host
DHCP - Dynamic Host Configuration Protocol
- UDP cliente 68, servidor 67
- Asigna dinámicamente direcciones IP para reutilizarlas cuando ya no se necesiten

Web
HTTP - Hypertext Transfer Protocol
- TCP 80, 8080
- Un conjunto de reglas para intercambiar texto, imágenes gráficas, sonido, video y otros archivos multimedia en el World Wide Web

15.2 Peer-to-Peer

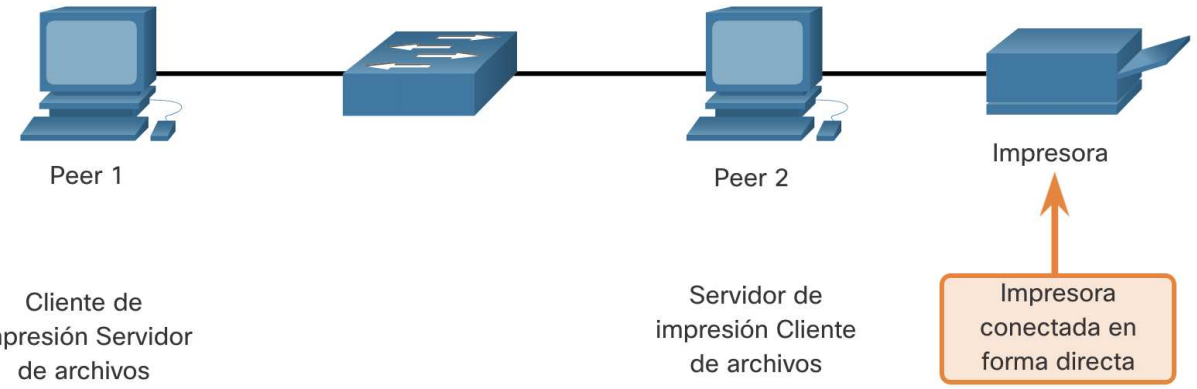
Modelo cliente-servidor

- Se considera que los procesos de cliente y servidor están en la capa de aplicación.
- En el modelo cliente/servidor, el dispositivo que solicita la información se denomina cliente y el dispositivo que responde a la solicitud se denomina servidor.
- Los protocolos de la capa de aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores.



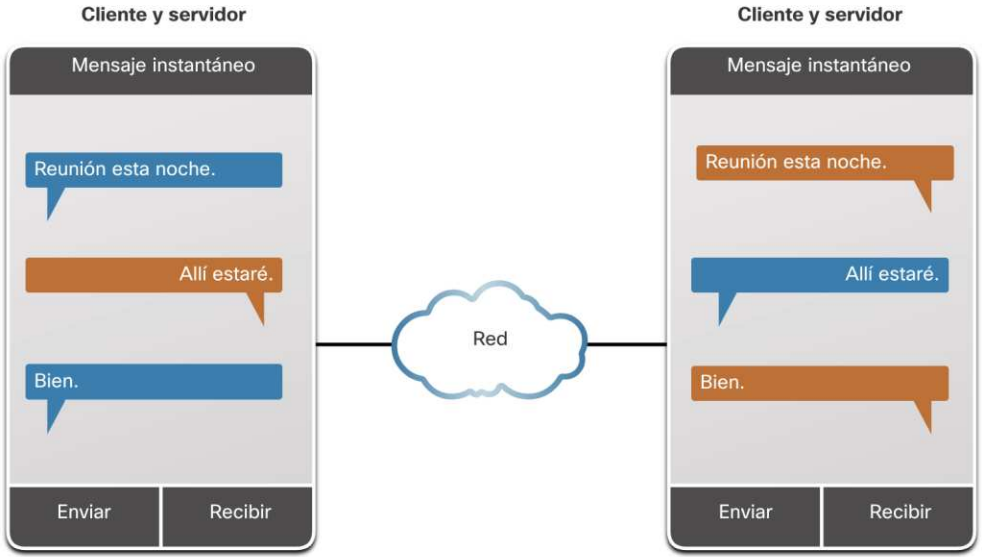
Redes Peer-to-Peer

- En una red peer-to-peer (P2P), dos o más computadoras están conectadas a través de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor dedicado.
- Cada dispositivo final conectado (conocido como par) puede funcionar como servidor y como cliente.
- Una computadora puede asumir el rol de servidor para una transacción mientras simultáneamente sirve como cliente para otra. Los roles de cliente y servidor se establecen por solicitud.



Applicaciones Peer-to-Peer

- Una aplicación P2P permite que un dispositivo actúe como cliente y servidor dentro de la misma comunicación.
- Algunas aplicaciones P2P utilizan un sistema híbrido en el que cada par accede a un servidor de índices para obtener la ubicación de un recurso almacenado en otro par.

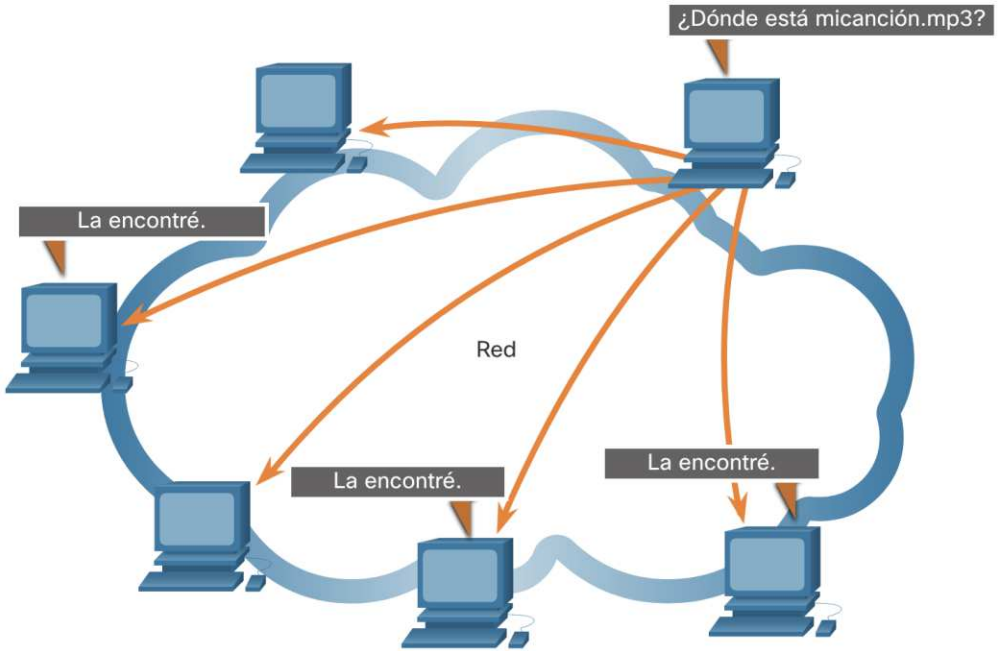


Aplicaciones P2P comunes

Con las aplicaciones P2P, cada computadora de la red que ejecuta la aplicación puede actuar como cliente o servidor para las otras computadoras de la red que también ejecutan la aplicación.

Las redes P2P comunes incluyen las siguientes:

- BitTorrent
- Direct Connect
- eDonkey
- Freenet



15.3 Protocolos web y de correo electrónico

Protoclo de transferencia de hypertexto y lenguaje de marcada de hypertexto

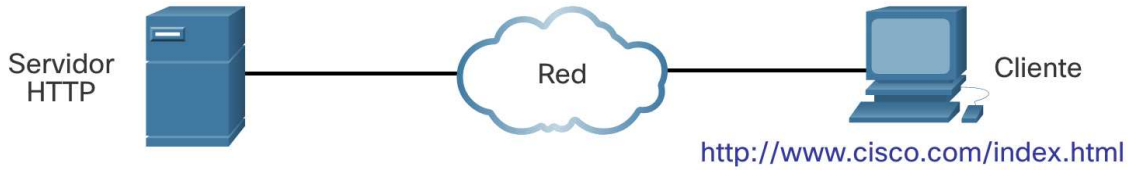
Cuando se escribe una dirección web o un un localizador uniforme de recursos (URL) en un navegador web, este establece una conexión con el servicio web. El servicio web se está ejecutando en el servidor que utiliza el protocolo HTTP.

Para comprender mejor cómo interactúan el navegador web y el servidor web, examine cómo se abre una página web en un navegador.

Paso 1

El navegador interpreta las tres partes de la URL:

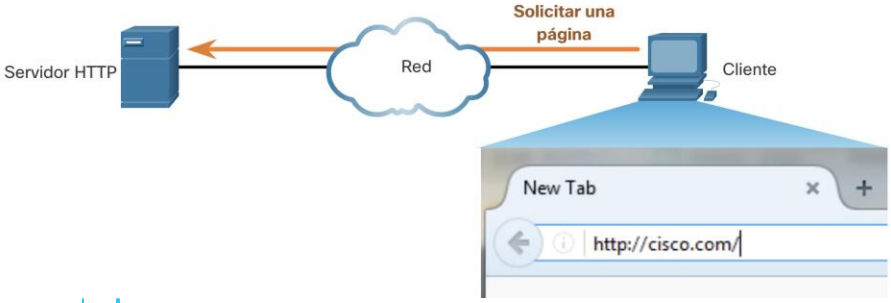
- http (el protocolo o esquema)
- www.cisco.com (el nombre del servidor)
- index.html (el nombre de archivo específico solicitado)



Protocolo de transferencia de hypertexto y lenguaje de marcada de hypertexto (Cont.)

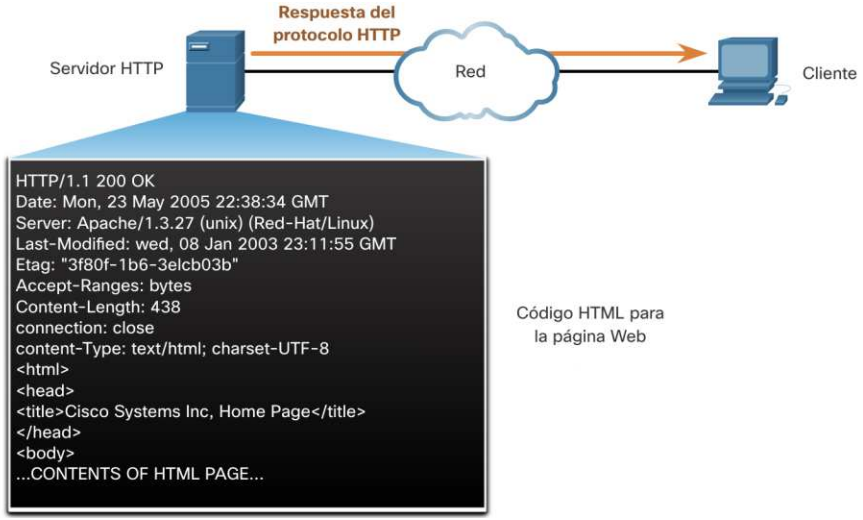
Paso 2

- Luego, el navegador verifica con un servidor de nombres para convertir www.cisco.com en una dirección IP numérica, que utiliza para conectarse al servidor.
- El cliente inicia una solicitud HTTP enviando una solicitud GET al servidor y solicita el archivo index.html.



Paso 3

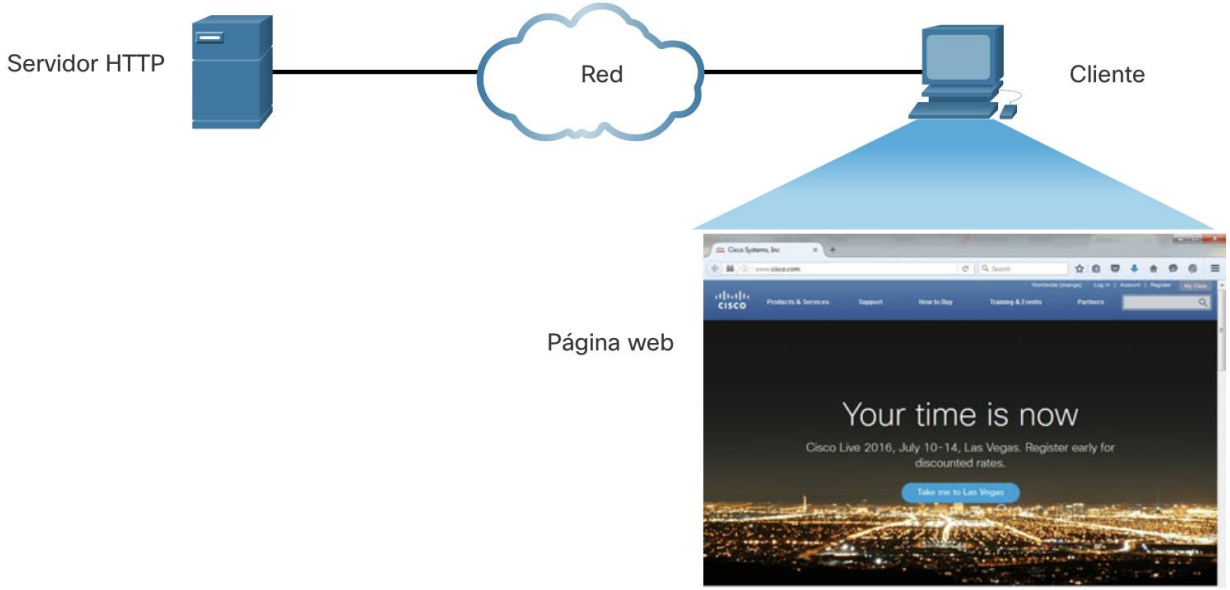
En respuesta a la solicitud, el servidor envía el código HTML de esta página web al navegador.



Protoclo de transferencia de hypertexto y lenguaje de marcada de hypertexto (Cont.) (Cont.)

Paso 4

El navegador interpreta el código HTML y formatea la página para la ventana del navegador.

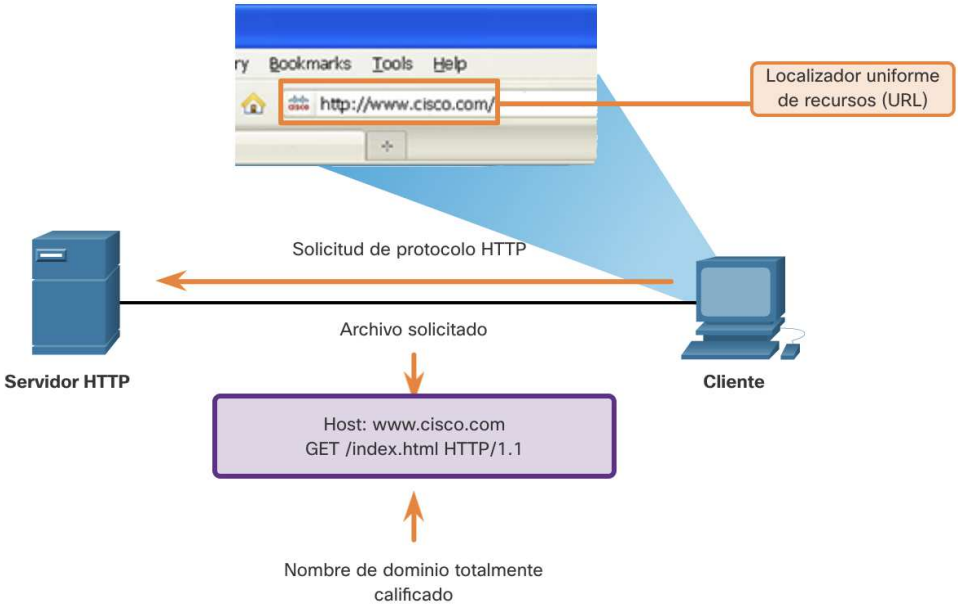


HTTP y HTTPS

HTTP es un protocolo de solicitud/respuesta que especifica los tipos de mensajes utilizados para esa comunicación.

Los tres tipos de mensajes comunes son GET, POST y PUT:

- GET: esta es una solicitud de datos del cliente. Un cliente (navegador web) envía el mensaje GET al servidor web para solicitar páginas HTML.
- POST: carga archivos de datos al servidor web, como datos de formularios.
- PUT: carga recursos o contenido en el servidor web, como una imagen.



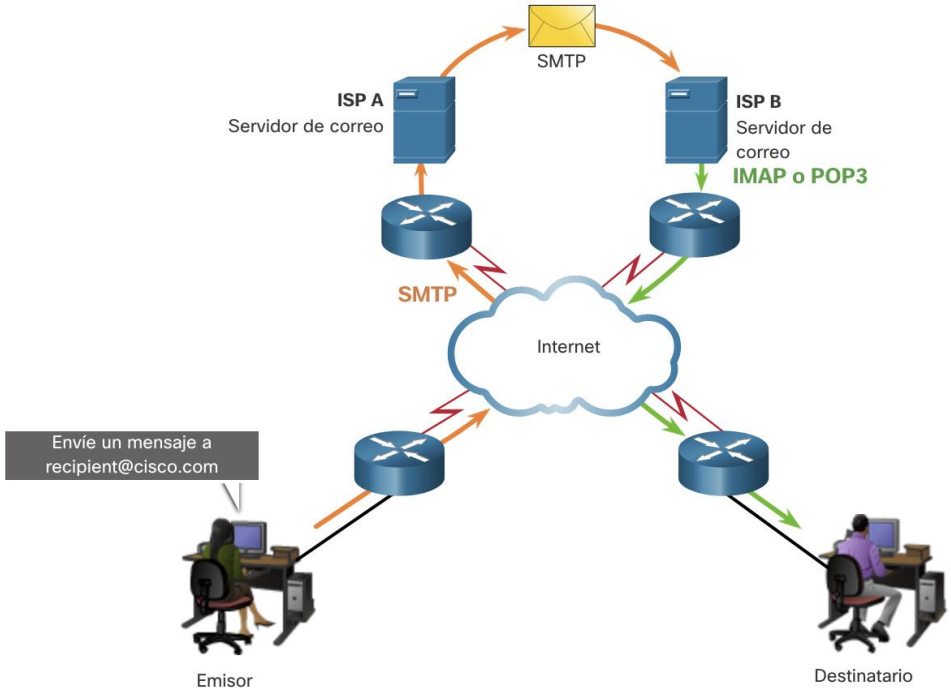
Nota: HTTP no es un protocolo seguro. Para comunicaciones seguras enviadas a través de Internet, se debe utilizar HTTPS.

Protocolos de correo electrónico

El correo electrónico es un método que se utiliza para enviar, guardar y recuperar mensajes electrónicos a través de la red. Los mensajes de correo electrónico se guardan en bases de datos en servidores de correo. Los clientes de email se comunican con los servidores de correo para enviar y recibir mensajes.

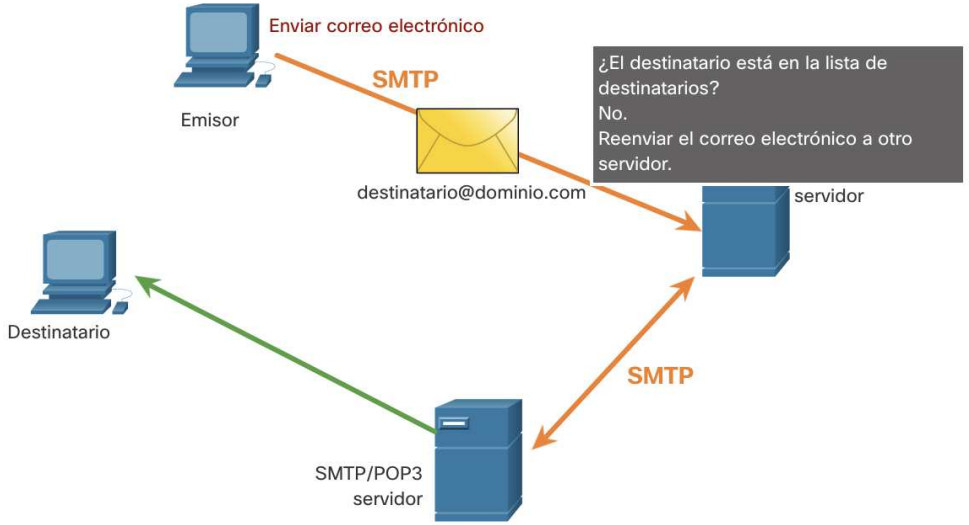
Los protocolos de correo electrónico utilizados para la operación son:

- Protocolo simple de transferencia de correo (SMTP): se utiliza para enviar correo.
- Protocolo de oficina postal (POP) e IMAP: se utiliza para que los clientes reciban correo.



SMTP, POP e IMAP

- Cuando un cliente envía un correo electrónico, el proceso SMTP del cliente se conecta con un proceso SMTP del servidor en el puerto conocido 25.
- Una vez realizada la conexión, el cliente intenta enviar el correo electrónico al servidor a través de la conexión.
- Cuando el servidor recibe el mensaje, coloca el mensaje en una cuenta local, si el destinatario es local, o reenvía el mensaje a otro servidor de correo para su entrega.
- Es posible que el servidor de correo electrónico de destino no esté en línea o que esté ocupado. Si es así, SMTP pone en cola los mensajes que se enviarán más tarde.

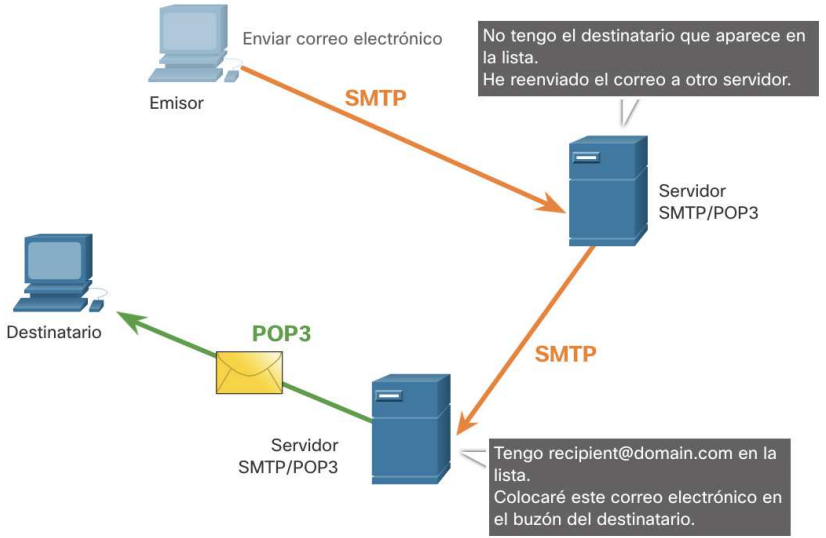


Nota: Los formatos de mensaje SMTP requieren un encabezado de mensaje (direcciones de correo electrónico del destinatario y del remitente) y un cuerpo del mensaje.

SMTP, POP e IMAP (Cont.)

Una aplicación utiliza POP para recuperar correos de un servidor. Cuando el correo se descarga del servidor al cliente mediante POP, los mensajes se eliminan del servidor.

- El servidor inicia el servicio POP escuchando pasivamente en el puerto TCP 110 las solicitudes de conexión del cliente.
- Cuando un cliente quiere hacer uso del servicio, envía una solicitud para establecer una conexión TCP con el servidor.
- Cuando se establece la conexión, el servidor POP envía un saludo.
- El cliente y el servidor POP luego intercambian comandos y respuestas hasta que la conexión se cierra o se cancela.

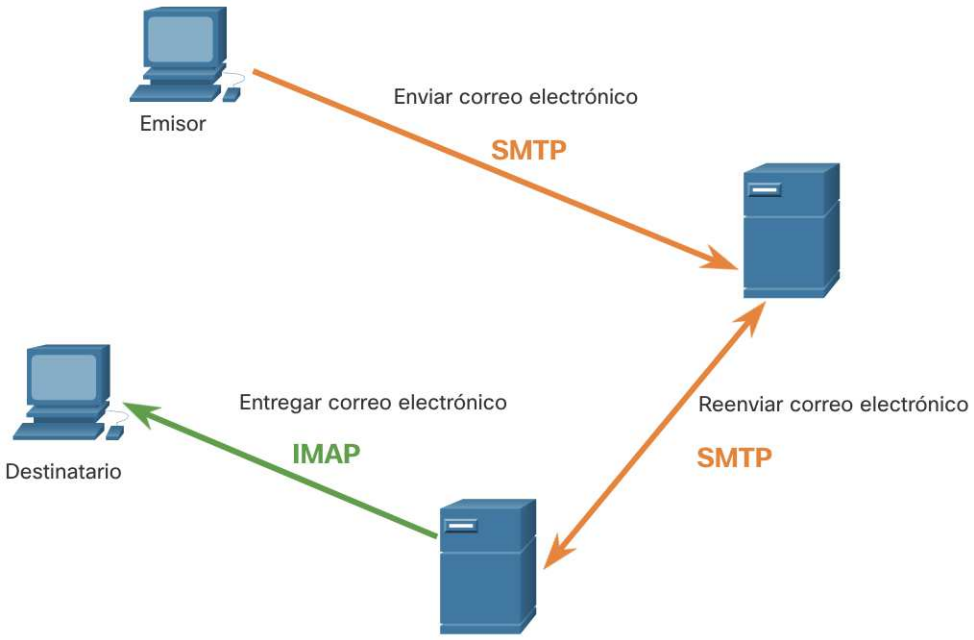


Nota: Dado que POP no almacena mensajes, no se recomienda para pequeñas empresas que necesitan una solución de copia de seguridad centralizada.

SMTP, POP e IMAP (Cont.)

IMAP es otro protocolo que describe un método para recuperar mensajes de correo electrónico.

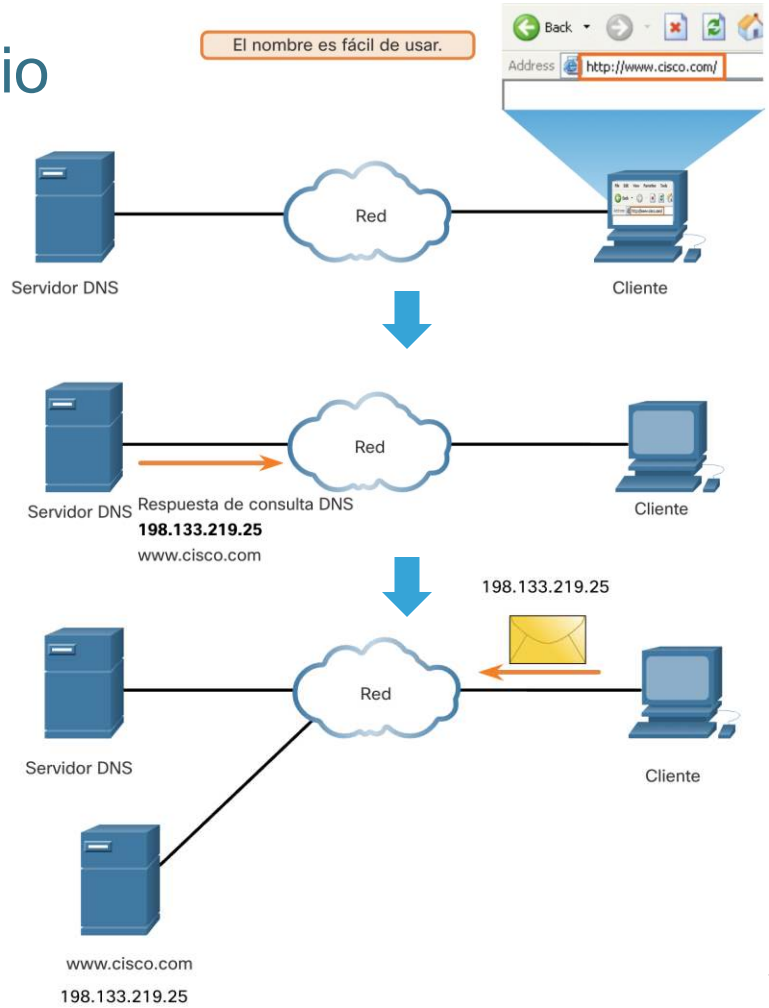
- A diferencia de POP, cuando un usuario se conecta a un servidor IMAP, las copias de los mensajes se descargan en la aplicación cliente. Los mensajes originales se guardan en el servidor hasta que se eliminan manualmente.
- Cuando un usuario decide eliminar un mensaje, el servidor sincroniza esa acción y elimina el mensaje del servidor.



15.4 Servicios de direccionamiento IP

Servicion de nombres de dominio

- Los nombres de dominio se crearon para convertir las direcciones IP numéricas en un nombre simple y reconocible.
- Los nombres de dominio totalmente calificados (FQDN), como http://www.cisco.com, son mucho más fáciles de recordar para las personas que 198.133.219.25.
- El protocolo DNS define un servicio automatizado que hace coincidir los nombres de los recursos con la dirección de red numérica requerida. Incluye el formato de consultas, respuestas y datos.



Formato de mensaje DNS

El servidor DNS almacena diferentes tipos de registros de recursos que se utilizan para resolver nombres. Estos registros contienen el nombre, la dirección y el tipo de registro.

Algunos de estos tipos de registros son los siguientes:

- **A** - una dirección IPv4 de terminal
- **NS** - un servidor de nombre autoritativo
- **AAAA** - una dirección IPv6 de terminal (pronunciada quad-A)
- **MX** - un registro de intercambio de correo

Cuando un cliente realiza una consulta, el proceso DNS del servidor primero busca en sus propios registros para resolver el nombre. Si no puede resolver el nombre utilizando sus registros almacenados, se pone en contacto con otros servidores para resolver el nombre.

Una vez que se encuentra una coincidencia y se devuelve al servidor solicitante original, el servidor almacena temporalmente la dirección numerada en caso de que se vuelva a solicitar el mismo nombre.

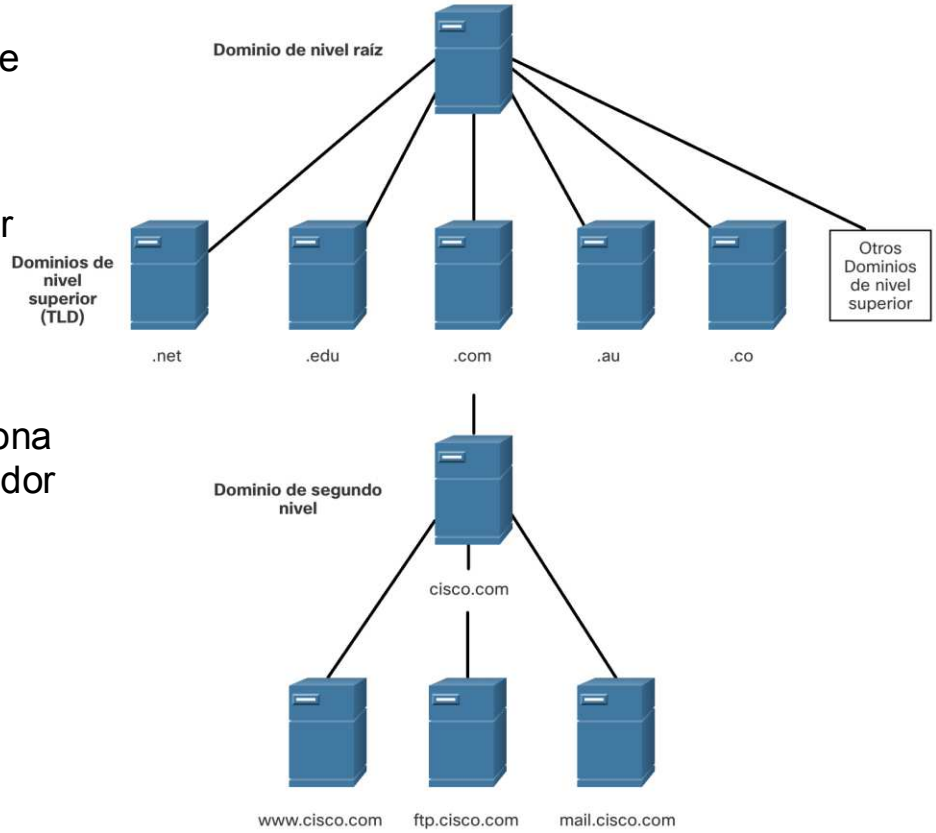
Formato de mensaje DNS (Cont.)

DNS usa el mismo formato de mensaje entre servidores, que consta de una pregunta, respuesta, autoridad e información adicional para todo tipo de consultas de clientes y respuestas de servidores, mensajes de error y transferencia de información de registros de recursos.

Sección de mensajes DNS	Descripción
Pregunta	La pregunta para el servidor de nombres
Respuesta	Registros de recursos que responden la pregunta
Autoridad	Registros de recursos que apuntan a una autoridad
Adicional	Registros de recursos que poseen información adicional

Jerarquía DNS

- DNS utiliza un sistema jerárquico para crear una base de datos para proporcionar resolución de nombres.
- Cada servidor DNS mantiene un archivo de base de datos específico y solo es responsable de administrar las asignaciones de nombre a IP para esa pequeña parte de la estructura completa del DNS.
- Cuando un servidor DNS recibe una solicitud de traducción de un nombre que no está dentro de su zona DNS, el servidor DNS reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para la traducción.
- Ejemplos de dominios de nivel superior:
  - **.com** - una empresa o industria
  - **.org** - una organización sin fines de lucro
  - **.au** - Australia



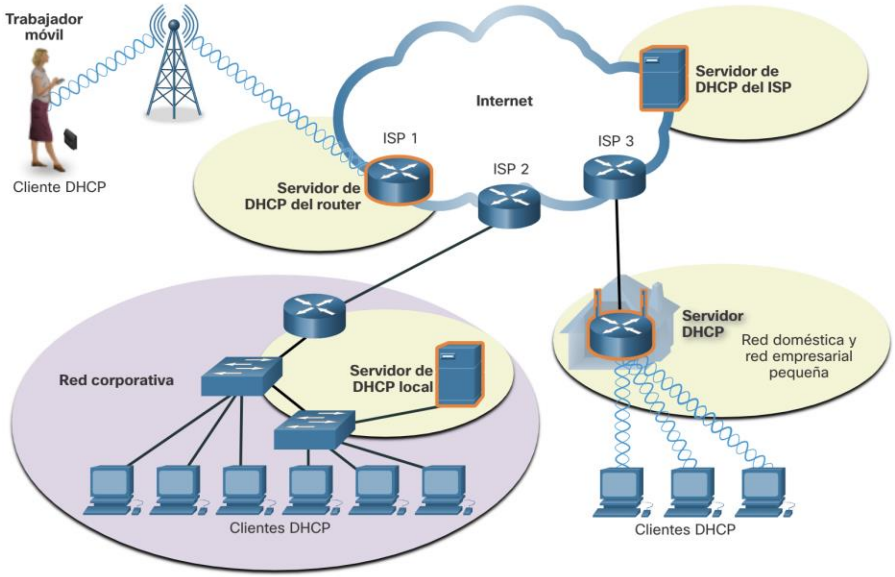
El comando nslookup

- Nslookup es una utilidad del sistema operativo de la computadora que permite a un usuario consultar manualmente los servidores DNS configurados en el dispositivo para resolver un nombre de host determinado.
- Esta utilidad también se puede utilizar para solucionar problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.
- Cuando se ejecuta el comando **nslookup**, se muestra el servidor DNS predeterminado configurado para su host.
- El nombre de un host o dominio se puede ingresar en el indicador de **nslookup.**

```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
>
```

Protocolo de configuración dinámica de host

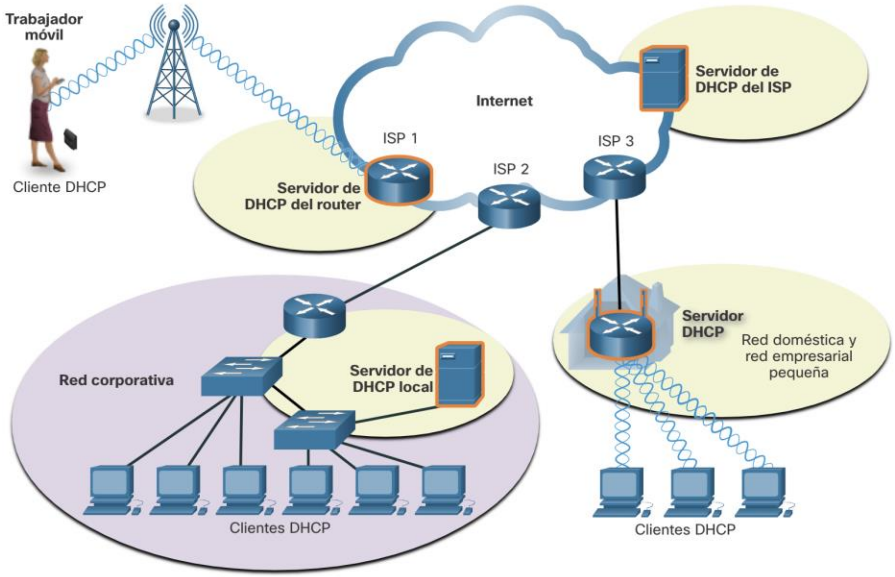
- El Protocolo de configuración dinámica de host (DHCP) para el servicio IPv4 automatiza la asignación de direcciones IPv4, máscaras de subred, puertas de enlace y otros parámetros de red IPv4.
- DHCP se considera direccionamiento dinámico en comparación con el direccionamiento estático. El direccionamiento estático consiste en ingresar manualmente la información de la dirección IP.



Nota: DHCP para IPv6 (DHCPv6) proporciona servicios similares para clientes IPv6. Sin embargo, DHCPv6 no proporciona una dirección de puerta de enlace predeterminada. Esto solo se puede obtener de forma dinámica a partir del mensaje de anuncio de enrutador del enrutador.

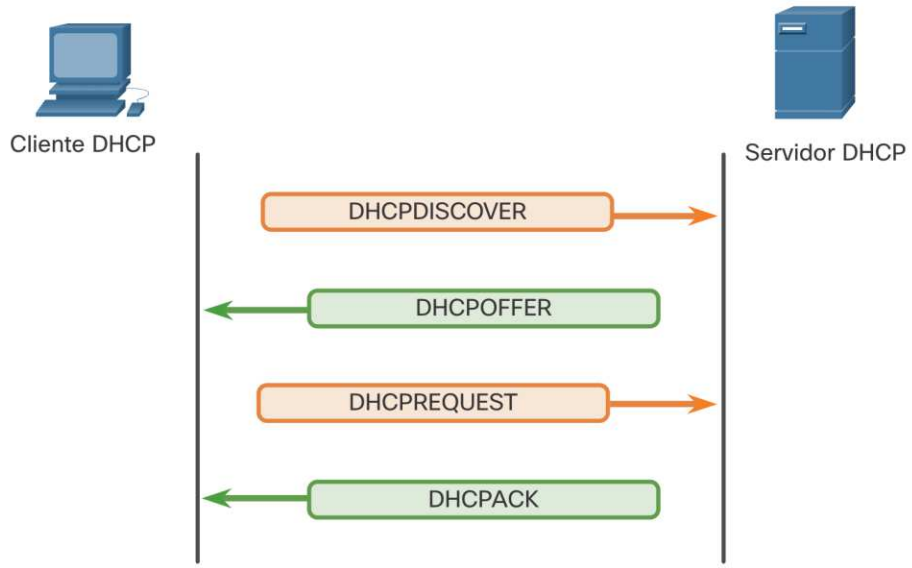
Protocolo de configuración dinámica de host

- Cuando un host se conecta a la red, se contacta con el servidor DHCP y se solicita una dirección. El servidor DHCP elige una dirección de un rango configurado de direcciones llamado grupo y la asigna (alquila) al host.
- Muchas redes utilizan tanto DHCP como direccionamiento estático. DHCP se utiliza para hosts de propósito general, como dispositivos de usuario final. El direccionamiento estático se utiliza para dispositivos de red, como enrutadores de puerta de enlace, conmutadores, servidores e impresoras.



Nota: DHCP para IPv6 (DHCPv6) proporciona servicios similares para clientes IPv6. Sin embargo, DHCPv6 no proporciona una dirección de puerta de enlace predeterminada. Esto solo se puede obtener de forma dinámica a partir del mensaje de anuncio de enrutador del enrutador.

Funcionamiento de DHCP



Note: DHCPv6 has a set of messages that is similar to those for DHCPv4. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

El proceso DHCP:

- Cuando un dispositivo IPv4 configurado con DHCP se conecta a la red, el cliente transmite un mensaje de descubrimiento (DHCPDISCOVER) para identificar cualquier servidor DHCP disponible en la red.
- Un servidor DHCP responde con un mensaje de oferta (DHCPOFFER), que ofrece una concesión al cliente. (Si un cliente recibe más de una oferta debido a múltiples servidores DHCP en la red, debe elegir uno).
- El cliente envía un mensaje de solicitud (DHCPREQUEST) que identifica el servidor explícito y la oferta de concesión que el cliente está aceptando.
- A continuación, el servidor devuelve un mensaje de confirmación (DHCPACK) que reconoce al cliente que la concesión se ha finalizado.
- Si la oferta ya no es válida, el servidor seleccionado responde con un mensaje de acuse de recibo negativo (DHCPNAK) y el proceso debe comenzar con un nuevo mensaje DHCPDISCOVER.

Lab – Observar la resolución de nombres DNS

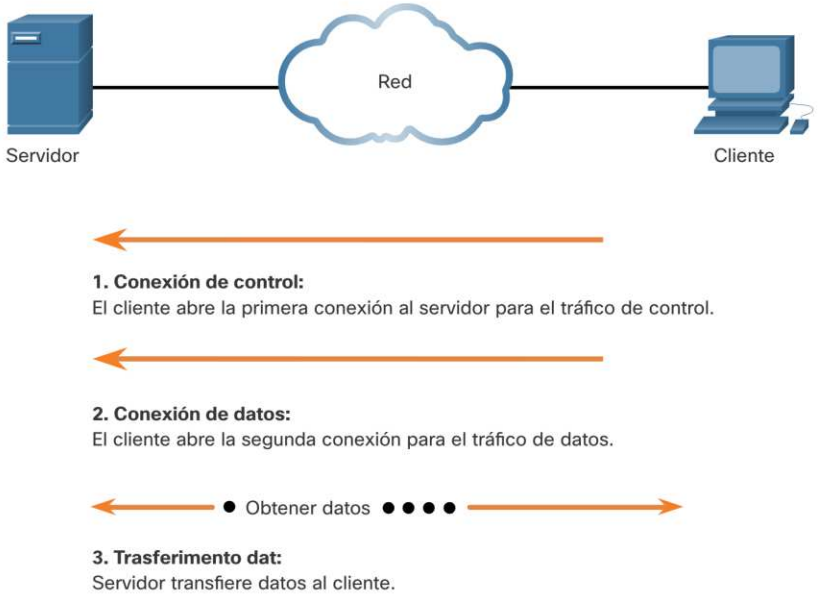
En este labo, completará los siguientes objetivos:

- Observe la conversión de DNS de una URL a una dirección IP
- Observe la búsqueda de DNS mediante el comando **nslookup** en un sitio web
- Observe la búsqueda de DNS mediante el comando **nslookup** en servidores de correo

15.5 Servicios de intercambio de archivos

Protocolo de transferencia de archivos

FTP fue desarrollado para permitir transferencias de datos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora que se utiliza para enviar y extraer datos de un servidor FTP.



Paso 1: el cliente establece la primera conexión con el servidor para controlar el tráfico mediante el puerto TCP 21. El tráfico consta de los comandos del cliente y las respuestas del servidor.

Paso 2: el cliente establece la segunda conexión con el servidor para la transferencia de datos real utilizando el puerto TCP 20. Esta conexión se crea cada vez que hay datos para transferir.

Paso 3: la transferencia de datos puede ocurrir en cualquier dirección. El cliente puede descargar (extraer) datos del servidor, o el cliente puede cargar (enviar) datos al servidor.

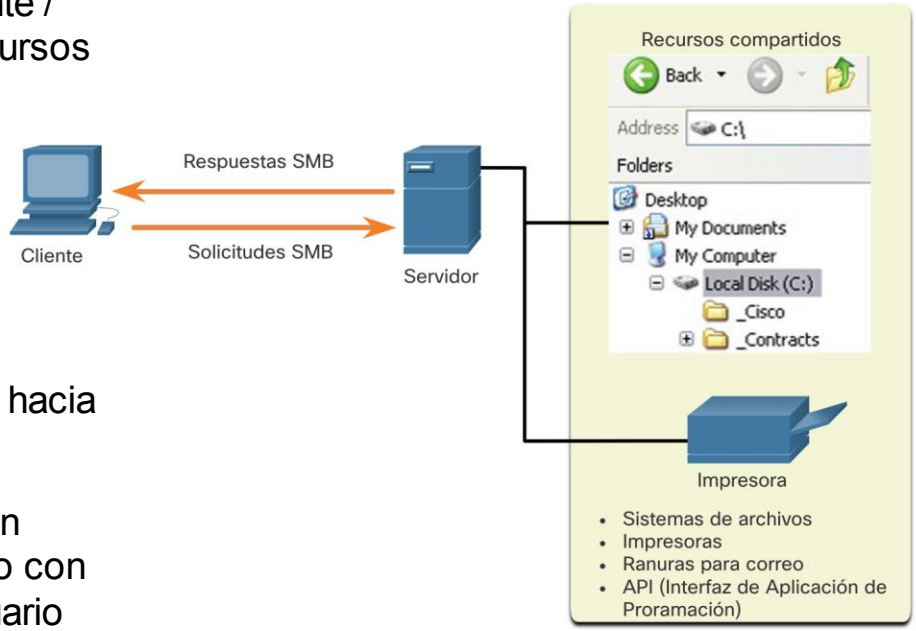
Bloque de mensajes de servidor

El bloque de mensajes del servidor (SMB) es un protocolo de intercambio de archivos de solicitud-respuesta cliente / servidor. Los servidores pueden poner sus propios recursos a disposición de los clientes de la red.

Tres funciones de los mensajes SMB:

- Iniciar, autenticar y finalizar sesiones
- Controlar el acceso a archivos e impresoras
- Permitir que una aplicación envíe o reciba mensajes hacia o desde otro dispositivo

A diferencia del intercambio de archivos compatible con FTP, los clientes establecen una conexión a largo plazo con los servidores. Una vez establecida la conexión, el usuario del cliente puede acceder a los recursos del servidor como si el recurso fuera local para el host del cliente.



15.6 Módulo de práctica y cuestionario

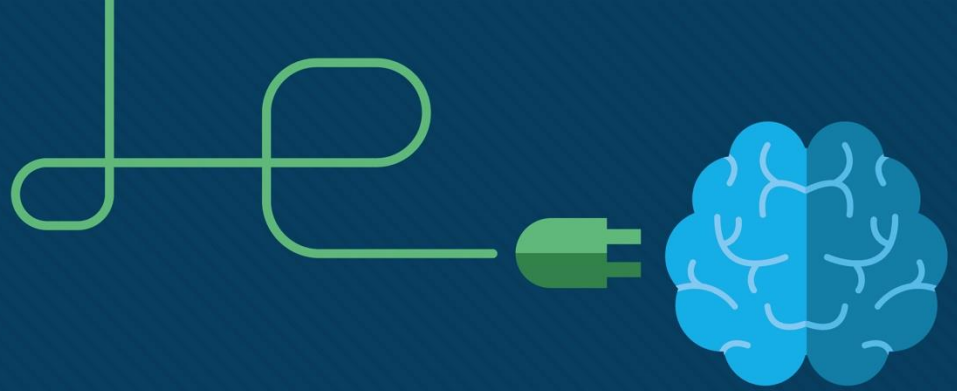
¿Qué aprendimos en este módulo?

- Los protocolos de la capa de aplicación se utilizan para intercambiar datos entre programas que se ejecutan en los hosts de origen y destino. La capa de presentación tiene tres funciones principales: formatear o presentar datos, comprimir datos y cifrar datos para transmitirlos y descifrarlos al recibirlos. La capa de sesión crea y mantiene diálogos entre las aplicaciones de origen y destino.
- En el modelo cliente/servidor, el dispositivo que solicita la información se denomina cliente y el dispositivo que responde a la solicitud se denomina servidor.
- En una red P2P, dos o más computadoras están conectadas a través de una red y pueden compartir recursos sin tener un servidor dedicado.
- Los tres tipos de mensajes HTTP comunes son GET, POST y PUT.
- El correo electrónico admite tres protocolos de funcionamiento independientes: SMTP, POP e IMAP.

¿Qué aprendimos en este módulo?

- El protocolo DNS hace coincidir los nombres de los recursos con la dirección de red numérica requerida.
- El servicio DHCP para IPv4 automatiza la asignación de direcciones IPv4, máscaras de subred, puertas de enlace y otros parámetros de red IPv4. Los mensajes DHCPv6 son SOLICITUDES, PUBLICIDAD, SOLICITUD DE INFORMACIÓN y RESPUESTA.
- Un cliente FTP es una aplicación que se ejecuta en una computadora que se utiliza para enviar y extraer datos de un servidor FTP.
- Tres funciones de los mensajes SMB: iniciar, autenticar y finalizar sesiones, controlar el acceso a archivos e impresoras y permitir que una aplicación envíe o reciba mensajes hacia o desde otro dispositivo.


CISCO



Módulo 16: Fundamentos de seguridad de red

Objetivos

Titulo: Fundementos de seguridad de red

Objetivo: Configure switches y routers con características de protección de dispositivos para mejorar la seguridad.

Tema	Objetivo
Vulnerabilidades y amenazas a la seguridad	Explicar por qué son necesarias las medidas básicas de seguridad en los dispositivos de red.
Ataques a la red	Identificar las vulnerabilidades de seguridad.
Mitigación de los ataques a la red	Identificar técnicas generales de mitigación.
Seguridad de los dispositivos	Configurar dispositivos de red con funciones de refuerzo de dispositivos para mitigar amenazas de seguridad.

16.1 Vulnerabilidades y amenazas a la seguridad de red

Tipos de amenazas

Los ataques a una red pueden ser devastadores y pueden resultar en pérdida de tiempo y dinero debido a daños o robo de información o activos importantes. Los intrusos pueden acceder a una red a través de vulnerabilidades de software, ataques de hardware o adivinando el nombre de usuario y la contraseña de alguien. Los intrusos que obtienen acceso modificando el software o explotando las vulnerabilidades del software se denominan actores de amenazas.

Una vez que el actor de la amenaza obtiene acceso a la red, pueden surgir cuatro tipos de amenazas:

- Robo de información
- Pérdida y manipulación de datos
- Robo de identidad
- Interrupción del servicio

Tipos de Vulnerabilidades

La vulnerabilidad es el grado de debilidad de una red o un dispositivo. Cierto grado de vulnerabilidad es inherente a routers, swtichs, computadoras de escritorio, servidores e incluso dispositivos de seguridad. Por lo general, los dispositivos de red atacados son los puntos finales, como servidores y computadoras de escritorio.

Hay tres vulnerabilidades o debilidades principales:

- **Las vulnerabilidades tecnológicas** pueden incluir debilidades del protocolo TCP/IP, debilidades del sistema operativo y debilidades del equipo de red.
- **Las vulnerabilidades de configuración** pueden incluir cuentas de usuario no seguras, cuentas del sistema con contraseñas fáciles de adivinar, servicios de Internet mal configurados, configuraciones predeterminadas no seguras y equipos de red mal configurados.
- **Las vulnerabilidades de la política** de seguridad pueden incluir la falta de una política de seguridad escrita, políticas, falta de continuidad de autenticación, controles de acceso lógico no aplicados, instalación y cambios de software y hardware que no siguen la política y un plan de recuperación ante desastres inexistente.

Estas tres fuentes de vulnerabilidades pueden dejar una red o un dispositivo expuesto a varios ataques, incluidos los ataques de código malicioso y los ataques a la red.

Seguridad física

Los recursos de la red pueden verse comprometidos físicamente, un actor de amenazas puede negar el uso de los recursos de la red. Las cuatro clases de amenazas físicas son las siguientes:

- **Amenazas de Hardware** - Esto incluye daños físicos a servidores, enrutadores, conmutadores, planta de cableado y estaciones de trabajo.
- **Amenazas del Entorno** - Esto incluye temperaturas extremas (demasiado calor o demasiado frío) o temperaturas extremas (demasiado húmedo o demasiado seco).
- **Amenazas Eléctricas** - Esto incluye picos de voltaje, voltaje de suministro insuficiente (caídas de voltaje), energía no condicionada (ruido) y pérdida total de energía.
- **Amenazas de Mantenimiento** - Esto incluye un manejo deficiente de los componentes eléctricos clave (descarga electrostática), falta de repuestos críticos, cableado deficiente y etiquetado deficiente.

Seguridad física (cont.)

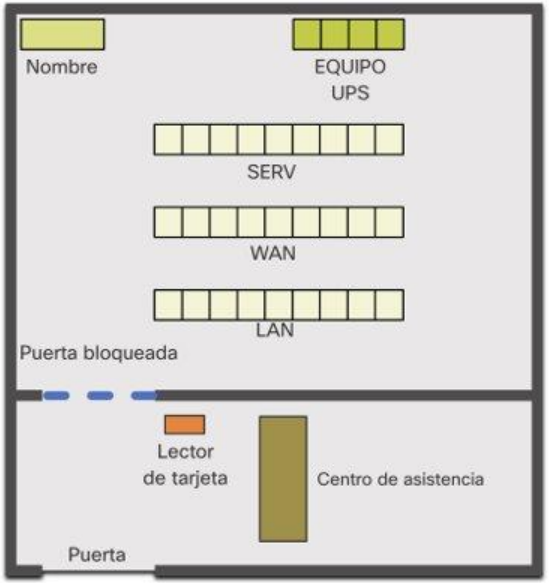
Se debe crear e implementar un buen plan de seguridad física para abordar estos problemas.

- Sala de informática segura.
- Implemente seguridad física para limitar el daño al equipo.

Paso 1. Mantenga los equipos bajo llave y evite el acceso no autorizado por puertas, techos, pisos elevados, ventanas, canales y conductos de ventilación.

Paso 2. Controle la entrada del armario con registros electrónicos.

Paso 3. Utilice cámaras de seguridad.



16.2 Ataques de red

Tipos de Malware(ver animación 16.2.1)

Malware es la abreviatura de software malicioso. Es un código o software diseñado específicamente para dañar, interrumpir, robar o infligir acciones “malas” o ilegítimas en datos, hosts o redes. Los siguientes son tipos de malware:

- **Virus:** un virus informático es un tipo de malware que se propaga insertando una copia de sí mismo en otro programa y convirtiéndose en parte de él. Se propaga de una computadora a otra, dejando infecciones a medida que viaja.
- **Gusanos:** los gusanos informáticos son similares a los virus en el sentido de que replican copias funcionales de sí mismos y pueden causar el mismo tipo de daño. A diferencia de los virus, que requieren la propagación de un archivo host infectado, los gusanos son un software independiente y no requieren un programa host o ayuda humana para propagarse.
- **Trojan Horses:** es un software dañino que parece legítimo. A diferencia de los virus y gusanos, los caballos de Troya no se reproducen infectando otros archivos. Se auto-replican. Los caballos de Troya deben propagarse a través de la interacción del usuario, como abrir un archivo adjunto de correo electrónico o descargar y ejecutar un archivo de Internet.

Ataques de reconocimiento (ver animación 16.2.2)

Además de los ataques de códigos maliciosos, también es posible que las redes sean víctimas de varios ataques de red. Los ataques de red se pueden clasificar en tres categorías principales:

- **Ataques de reconocimiento**: descubrimiento y mapeo de sistemas, servicios o vulnerabilidades.
- **Ataques de acceso**: la manipulación no autorizada de datos, acceso al sistema o privilegios de usuario.
- **Denegación de servicio**: desactivación o corrupción de redes, sistemas o servicios.

Para los ataques de reconocimiento, los actores de amenazas externos pueden usar herramientas de Internet, como las utilidades **nslookup** y **whois**, para determinar fácilmente el espacio de direcciones IP asignado a una corporación o entidad determinada. Una vez que se determina el espacio de direcciones IP, un actor de amenazas puede hacer **ping** a las direcciones IP disponibles públicamente para identificar las direcciones que están activas.

Ataques con acceso (ver animación 16.2.3)

Los ataques de acceso aprovechan las vulnerabilidades conocidas en los servicios de autenticación, servicios FTP y servicios web para acceder a cuentas web, bases de datos confidenciales y otra información sensible.

Los ataques de acceso se pueden clasificar en cuatro tipos:

- **Ataques de contraseña:** implementados mediante fuerza bruta, troyano y rastreadores de paquetes.
- **Explotación de confianza:** un actor de amenazas utiliza privilegios no autorizados para obtener acceso a un sistema, posiblemente comprometiendo al objetivo.
- **Redirección de puertos:** un actor de amenazas utiliza un sistema comprometido como base para ataques contra otros objetivos. Por ejemplo, un actor de amenazas que usa SSH (puerto 22) para conectarse a un host A comprometido. El host B confía en el host A y, por lo tanto, el actor de amenazas puede usar Telnet (puerto 23) para acceder a él.
- **Hombre en el medio:** el actor de la amenaza se coloca entre dos entidades legítimas para leer o modificar los datos que pasan entre las dos partes.

Atques de negación des servicio(ver animación 16.2.4)

Los ataques Denial of service (DoS) son la forma de ataque más común y una de las más difíciles de eliminar. Sin embargo, debido a su facilidad de implementación y al daño potencialmente significativo, los ataques DoS merecen una atención especial por parte de los administradores de seguridad.

- Los ataques DoS adoptan muchas formas. En última instancia, evitan que las personas autorizadas utilicen un servicio al consumir recursos del sistema. Para prevenir ataques DoS, es importante mantenerse al día con las últimas actualizaciones de seguridad para sistemas operativos y aplicaciones.
- Los ataques DoS son un riesgo importante porque interrumpen la comunicación y provocan una pérdida significativa de tiempo y dinero. Estos ataques son relativamente simples de realizar, incluso por un actor de amenazas inexperto.
- Un DDoS es similar a un ataque DoS, pero se origina en múltiples fuentes coordinadas. Por ejemplo, un actor de amenazas crea una red de hosts infectados, conocidos como zombies. Una red de zombis se llama botnet. El actor de amenazas utiliza un programa de comando y control (CnC) para instruir a la botnet de zombies para que lleve a cabo un ataque DDoS.

Lab – Investigación de amenazas de seguridad de red

En este laboratorio, completará los siguientes objetivos:

- Parte 1: Explore el sitio web de SANS
- Parte 2: Identificar las amenazas recientes a la seguridad de la red
- Parte 3: Detalle de una amenaza de seguridad de red específica

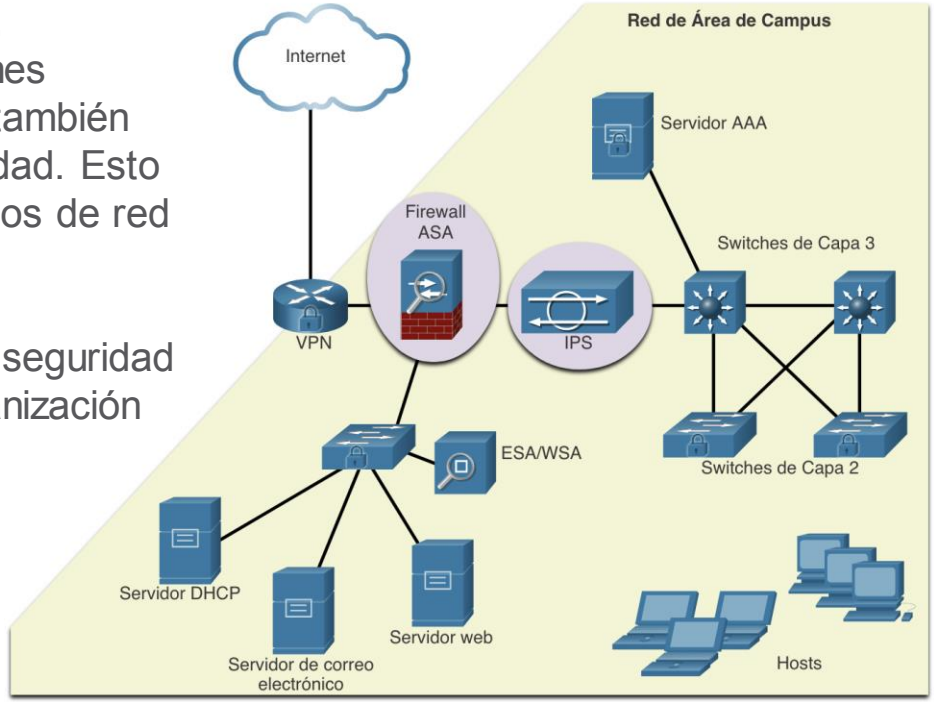
16.3 Mitigación de ataques de red

Enfoque de defensa en profundidad

Para mitigar los ataques a la red, primero debe proteger los dispositivos, incluidos enrutadores, conmutadores, servidores y hosts. La mayoría de las organizaciones emplean un enfoque de defensa en profundidad (también conocido como enfoque por capas) para la seguridad. Esto requiere una combinación de dispositivos y servicios de red que funcionen en conjunto.

Se implementan varios dispositivos y servicios de seguridad para proteger a los usuarios y activos de una organización contra las amenazas de TCP/IP:

- VPN
- Cortafuegos ASA
- IPS
- ESA / WSA
- Servidor AAA



Copias de seguridad

Hacer una copia de seguridad de las configuraciones y los datos del dispositivo es una de las formas más efectivas de protegerse contra la pérdida de datos.

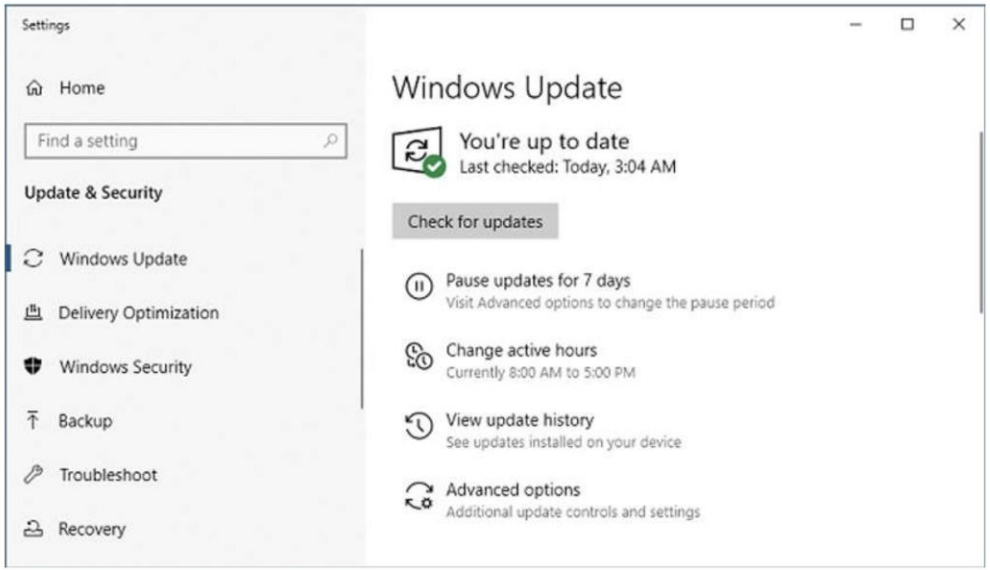
La tabla muestra las consideraciones sobre la copia de seguridad y sus descripciones.

Consideración	Descripción
Frecuencia	•Realice copias de seguridad de forma regular según se identifica en la política de seguridad. •Las copias de seguridad completas pueden llevar mucho tiempo, por lo tanto, realice copias de seguridad mensuales o semanales con copias de seguridad parciales frecuentes de los archivos modificados.
Almacenamiento	•Valide siempre las copias de seguridad para garantizar la integridad de los datos y valide los procedimientos de restauración de archivos.
Seguridad	•Las copias de seguridad deben transportarse a una ubicación de almacenamiento externa aprobada en una rotación diaria, semanal o mensual, según lo requiera la política de seguridad.
Validación	•Las copias de seguridad deben protegerse con contraseñas seguras. Se requiere la contraseña para restaurar los datos.

Mantengase actualizado

A medida que aparecen nuevo malware, las empresas deben mantenerse al día con las últimas versiones de software antivirus.

- La forma más eficaz de mitigar un ataque de gusano es descargar actualizaciones de seguridad del proveedor del sistema operativo y parchear todos los sistemas vulnerables.
- Una solución para la gestión de parches de seguridad críticos es asegurarse de que todos los sistemas finales descarguen automáticamente las actualizaciones.

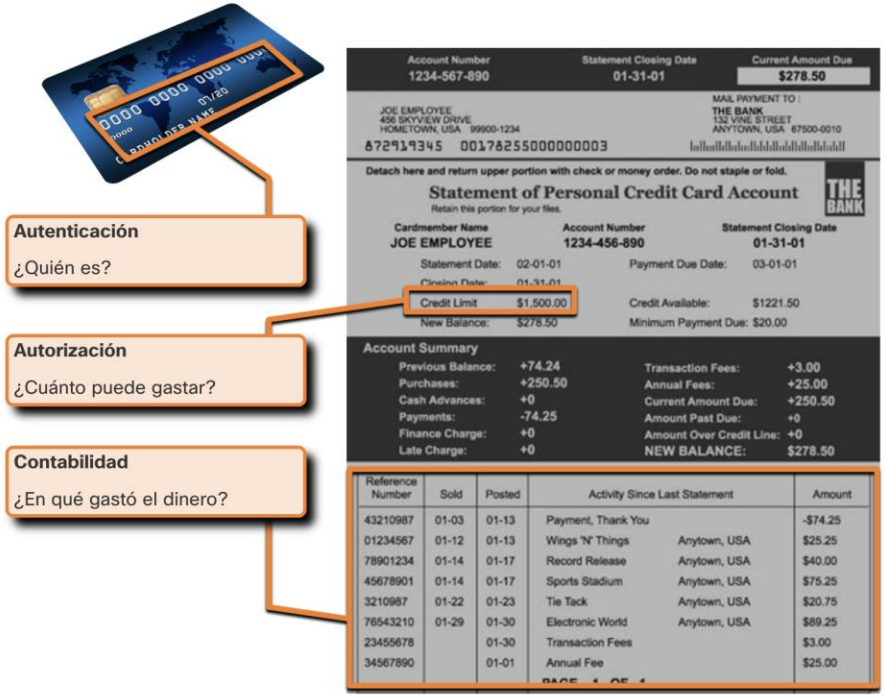


Autenticación, autorización y contabilidad AAA

Los servicios de seguridad de red de autenticación, autorización y contabilidad (AAA o "triple A") proporcionan el marco principal para configurar el control de acceso en los dispositivos de red.

AAA es una forma de controlar quién tiene permiso para acceder a una red (autenticarse), qué acciones realizan mientras acceden a la red (autorizar) y hacer un registro de lo que se hizo mientras están allí (contabilidad).

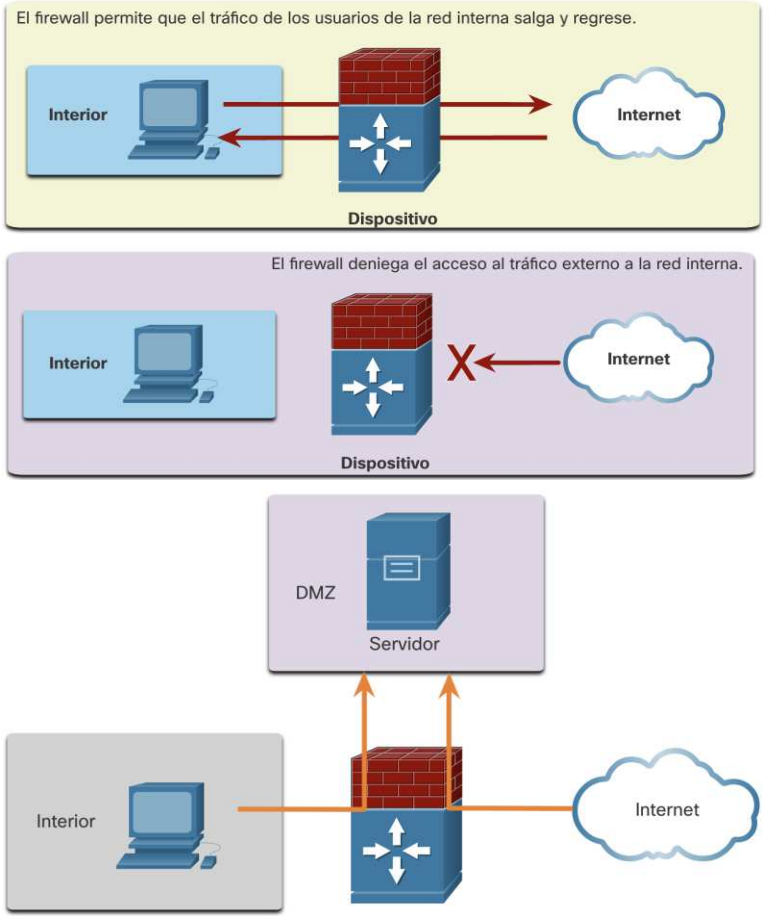
El concepto de AAA es similar al uso de una tarjeta de crédito. La tarjeta de crédito identifica quién puede usarla, cuánto puede gastar ese usuario y mantiene una cuenta de en qué artículos gastó el dinero el usuario.



Firewalls

Los firewalls de red residen entre dos o más redes, controlan el tráfico entre ellas y ayudan a prevenir el acceso no autorizado.

Un cortafuegos podría permitir a los usuarios externos un acceso controlado a servicios específicos. Por ejemplo, los servidores a los que pueden acceder los usuarios externos suelen estar ubicados en una red especial denominada zona desmilitarizada (DMZ). La DMZ permite que un administrador de red aplique políticas específicas para los hosts conectados a esa red.



Tipos de Firewalls

Los productos de cortafuegos vienen empaquetados en varias formas. Estos productos utilizan diferentes técnicas para determinar qué se permitirá o denegará el acceso a una red. Incluyen lo siguiente:

- **Filtrado de paquetes:** evita o permite el acceso basado en direcciones IP o MAC
- **Filtrado de aplicaciones:** impide o permite el acceso de tipos de aplicaciones específicos según los números de puerto.
- **Filtrado de URL:** evita o permite el acceso a sitios web basados en URL o palabras clave específicas.
- **Stateful packet inspection (SPI):** los paquetes entrantes deben ser respuestas legítimas a las solicitudes de los hosts internos. Los paquetes no solicitados se bloquean a menos que se permitan específicamente. SPI también puede incluir la capacidad de reconocer y filtrar tipos específicos de ataques, como denegación de servicio (DoS).

Seguridad de terminales

Un punto final, o host, es un sistema o dispositivo informático individual que actúa como cliente de red. Los puntos finales comunes son computadoras portátiles, computadoras de escritorio, servidores, teléfonos inteligentes y tabletas.

Asegurar los dispositivos de punto final es uno de los trabajos más desafiantes de un administrador de red porque involucra la naturaleza humana. Una empresa debe tener políticas bien documentadas y los empleados deben conocer estas reglas.

Los empleados deben recibir formación sobre el uso adecuado de la red. Las políticas a menudo incluyen el uso de software antivirus y prevención de intrusiones en el host. Las soluciones de seguridad de terminales más completas se basan en el control de acceso a la red.

16.4 Seguridad de los dispositivos

Cisco AutoSecure

En la mayoría de los casos, este nivel de seguridad predeterminado es inadecuado. Para los enrutadores Cisco, la función Cisco AutoSecure se puede utilizar para ayudar a proteger el sistema.

Además, hay algunos pasos simples que se deben seguir y que se aplican a la mayoría de los sistemas operativos:

- Los nombres de usuario y contraseñas predeterminados deben cambiarse inmediatamente.
- El acceso a los recursos del sistema debe restringirse solo a las personas que están autorizadas a utilizar esos recursos.
- Todos los servicios y aplicaciones innecesarios deben apagarse y desinstalarse cuando sea posible.
- A menudo, los dispositivos enviados por el fabricante han estado en un almacén durante un período de tiempo y no tienen instalados los parches más actualizados. Es importante actualizar cualquier software e instalar los parches de seguridad antes de la implementación.

Contraseñas

Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Estas son las pautas estándar a seguir:

- Utilice una contraseña de al menos ocho caracteres, preferiblemente 10 o más caracteres.
- Haga las contraseñas complejas. Incluya una combinación de letras mayúsculas y minúsculas, números, símbolos y espacios, si está permitido.
- Evite las contraseñas basadas en la repetición, palabras comunes del diccionario, secuencias de letras o números, nombres de usuario, nombres de familiares o mascotas, información biográfica, como fechas de nacimiento, números de identificación, nombres de antepasados u otra información fácilmente identificable.
- De manera deliberada, escribe mal una contraseña. Por ejemplo, Smith = Smyth = 5mYth o Security = 5ecur1ty.
- Cambie las contraseñas con frecuencia. Si una contraseña se ve comprometida sin saberlo, la ventana de oportunidad para que el actor de amenazas use la contraseña es limitada.
- No escriba las contraseñas y las deje en lugares obvios, como el escritorio o el monitor.

En los enrutadores Cisco, los espacios iniciales se ignoran para las contraseñas, pero los espacios después del primer carácter no. Por lo tanto, un método para crear una contraseña segura es usar la barra espaciadora y crear una frase compuesta de muchas palabras. Esto se llama frase de contraseña. Una frase de contraseña suele ser más fácil de recordar que una simple contraseña. También es más largo y más difícil de adivinar.

Seguridad de contraseña adicional

Hay varios pasos que se pueden tomar para ayudar a garantizar que las contraseñas permanezcan secretas en un enrutador y conmutador Cisco, incluidos los siguientes:

- Cifre todas las contraseñas de texto plano con el comando **service password-encryption**.
- Establezca una longitud mínima aceptable de contraseña con el comando **security passwords min-length**.
- Detenga los ataques de adivinación de contraseñas por fuerza bruta con el comando **login block-for # attempts # within #.**
- Deshabilite un acceso al modo EXEC privilegiado inactivo después de una cantidad de tiempo especificada con el commando **exec-timeout**.

```
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)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

Habilite SSH

Es posible configurar un dispositivo Cisco para que admita SSH mediante los siguientes pasos:

1. **Configurar un nombre de host de dispositivo único.** Un dispositivo debe tener un nombre de host único que no sea el predeterminado.
2. **Configurar el nombre de dominio de IP.** Configure mediante el comando del modo de configuración global **ip-domain name**.
3. **Generar una clave para cifrar el tráfico SSH**. SSH cifra el tráfico entre el origen y el destino. Sin embargo, para hacerlo, se debe generar una clave de autenticación única mediante el comando de configuración global **crypto key generate rsa general-keys modulus** *bits*. Los bits de módulo determinan el tamaño de la clave y se pueden configurar desde 360 bits hasta 2048 bits. Cuanto mayor sea el valor del bit, más segura será la clave. Sin embargo, los valores de bits más grandes también tardan más en cifrar y descifrar la información. La longitud mínima recomendada del módulo es de 1024 bits.
4. **Verificar o crear una entrada de base de datos local.** Cree una entrada de nombre de usuario de la base de datos local utilizando el comando de configuración global **username.**
5. **Autenticarse con la base de datos local.** Utilizar el comando de configuracion de linea **login local** para autenticar la linea vty contra una base de datos local.
6. **Habilitar las sesiones SSH entrantes de vty.** De forma predeterminada, no se permite ninguna sesión de entrada en las líneas vty. Puede especificar varios protocolos de entrada, incluidos Telnet y SSH, utilizando el comando **transport input [ssh | telnet]** .

Deshabilitar los servicios no utilizados

Los enrutadores y conmutadores de Cisco comienzan con una lista de servicios activos que pueden ser necesarios o no en su red. Deshabilite los servicios no utilizados para preservar los recursos del sistema, como los ciclos de la CPU y la RAM, y evite que los actores de amenazas exploten estos servicios.

- El tipo de servicios que están activados de forma predeterminada variará según la versión de IOS. Por ejemplo, IOS-XE normalmente solo tendrá abiertos los puertos HTTPS y DHCP. Puede verificar esto con el comando **show ip ports all**.
- Las versiones de IOS anteriores a IOS-XE utilizan el comando **show control-plane host open-ports**.

Packet Tracer – Configurar contraseñas seguras y SSH (act. 16.4.6)

En este Packet Tracer, configurará contraseñas y SSH:

- El administrador de la red le ha pedido que prepare RTA y SW1 para la implementación. Antes de que puedan conectarse a la red, deben habilitarse las medidas de seguridad.

Lab – Configurar dispositivos de red con SSH

En este lab, completará los siguientes objetivos:

- Parte 1: configurar los ajustes básicos del dispositivo
- Parte 2: configurar el enrutador para acceso SSH
- Parte 3: configurar el conmutador para acceso SSH
- Parte 4: SSH desde la CLI en el Switch

16.5 Prática del módulo y cuestionario

Packet Tracer – Dispositivos de red seguros (act. 16.5.1)

En esta actividad, configurará un enrutador y un conmutador según una lista de requisitos.

Lab – Dispositivos de red seguros (act. 16.5.2)

En este lab, completará los siguientes objetivos:

- Configurar los ajustes básicos del dispositivo
- Configurar medidas de seguridad básicas en el enrutador
- Configurar medidas de seguridad básicas en el conmutador

¿Qué aprendimos en este módulo?

- Una vez que el actor de la amenaza obtiene acceso a la red, pueden surgir cuatro tipos de amenazas: robo de información, pérdida y manipulación de datos, robo de identidad e interrupción del servicio.
- Hay tres vulnerabilidades o debilidades principales: tecnológica, de configuración y política de seguridad.
- Las cuatro clases de amenazas físicas son: hardware, medio ambientales, eléctricas y de mantenimiento.
- Malware es la abreviatura de software malicioso. Es un código o software diseñado específicamente para dañar, interrumpir, robar o infligir acciones "malas" o ilegítimas en datos, hosts o redes. Los virus, gusanos y caballos de Troya son tipos de malware.
- Los ataques a la red se pueden clasificar en tres categorías principales: reconocimiento, acceso y denegación de servicio.
- Para mitigar los ataques a la red, primero debe proteger los dispositivos, incluidos enrutadores, conmutadores, servidores y hosts. La mayoría de las organizaciones emplean un enfoque de seguridad de defensa en profundidad. Esto requiere una combinación de dispositivos y servicios de red que trabajen juntos.
- Se implementan varios dispositivos y servicios de seguridad para proteger a los usuarios y activos de una organización contra las amenazas de TCP / IP: VPN, firewall ASA, IPS, ESA / WSA y servidor AAA.

¿Qué aprendimos en este módulo? (Cont.)

- Los dispositivos de infraestructura deben tener copias de seguridad de los archivos de configuración e imágenes de IOS en un servidor de archivos FTP o similar. Si la computadora o el hardware de un enrutador falla, los datos o la configuración se pueden restaurar usando la copia de respaldo.
- La forma más eficaz de mitigar un ataque de gusano es descargar actualizaciones de seguridad del proveedor del sistema operativo y parchear todos los sistemas vulnerables. Para administrar parches de seguridad críticos, para asegurarse de que todos los sistemas finales descarguen automáticamente las actualizaciones.
- AAA es una forma de controlar quién tiene permiso para acceder a una red (autenticarse), qué pueden hacer mientras están allí (autorizar) y qué acciones realizan mientras acceden a la red (contabilidad).
- Los firewalls de red residen entre dos o más redes, controlan el tráfico entre ellas y ayudan a prevenir el acceso no autorizado.
- La protección de los dispositivos terminales es fundamental para la seguridad de la red. Una empresa debe tener políticas bien documentadas, que pueden incluir el uso de software antivirus y prevención de intrusiones en el host. Las soluciones de seguridad de terminales más completas se basan en el control de acceso a la red.

¿Qué aprendimos en este módulo? (Cont.)

- Para los enrutadores Cisco, la función Cisco AutoSecure se puede utilizar para ayudar a proteger el sistema. Para la mayoría de los sistemas operativos, los nombres de usuario y las contraseñas predeterminados deben cambiarse de inmediato, el acceso a los recursos del sistema debe restringirse solo a las personas que están autorizadas a usar esos recursos, y todos los servicios y aplicaciones innecesarios deben apagarse y desinstalarse cuando sea posible.
- Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Una frase de contraseña suele ser más fácil de recordar que una simple contraseña. También es más largo y más difícil de adivinar.
- Para enrutadores y conmutadores, cifre todas las contraseñas de texto sin formato, establezca una longitud mínima aceptable de contraseña, disuada de los ataques de adivinación de contraseña por fuerza bruta y desactive un acceso al modo EXEC privilegiado inactivo después de un período de tiempo específico.
- Configure los dispositivos adecuados para admitir SSH y desactive los servicios no utilizados.


CISCO