

Direccionamiento IPv6

Problemas de IPv4 Necesidad de IPv6

- IPv4 se está quedando sin direcciones. IPv6 es el sucesor de IPv4. IPv6 tiene un espacio de direcciones de 128 bits mucho más grande.
- El desarrollo de IPv6 también incluyó correcciones para limitaciones de IPv4 y otras mejoras.
- Con una población que accede a Internet cada vez mayor, un espacio de direcciones IPv4 limitado, los problemas de NAT y la Internet de todo, llegó el momento de comenzar la transición hacia IPv6.



Problemas con IPv4

Coexistencia de IPv4 e IPv6

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

El IETF creó diversos protocolos y herramientas para ayudar a los administradores de redes a migrar las redes a IPv6. Las técnicas de migración pueden dividirse en tres categorías:

- **Dual stack** -Los dispositivos ejecutan pilas de protocolos IPv4 e IPv6 de manera simultánea.
- **Tunneling** – Es un método para transportar un paquete IPv6 a través de una red IPv4. El paquete IPv6 se encapsula dentro de un paquete IPV4.
- **Translation** - Network Address Translation 64 (NAT64) permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT para IPv4.

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

Representación de direcciones IPv6 Formatos de direccionesIPv6

- Las direcciones IPv6 tienen 128 bits de longitud y están escritas en hexadecimal.
- Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas, y pueden escribirse en minúsculas o en mayúsculas.
- El formato preferido para escribir una dirección IPv6 es x: x: x: x: x: x: x: x, donde cada "x" consta de cuatro valores hexadecimales.
- En IPv6, un “hexteto” es el término no oficial que se utiliza 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

2001:0 db 8:0000:00 a3:abcd:0000:0000:1234

Representación de dirección IPv6

Regla 1 - Omitir el cero inicial

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

Ejemplos:

- 01ab se puede representar como 1ab
- 09f0 se puede representar como 9f0
- 0a00 se puede representar como a00
- 00ab se puede representar como ab

Nota: Esta regla solo es válida para los ceros iniciales, y NO para los ceros finales; de lo contrario, la dirección sería ambigua.

Tipo	Formato
Recomendado	2001:0db8:0000:1111:0000:0000:0200
Sin los ceros iniciales	2001:db8:0:1111:0:0:0:200

Representación de dirección IPv6

Regla 2 - Dos puntos

Los dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más segmentos de 16 bits (hextetos) que estén compuestas solo por ceros.

Por ejemplo:

- 2001:db8:cafe:1:0:0:0:1 (0s iniciales omitidos) podría representarse como 2001:db8:cafe:1::1

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

Tipo	Formato
Recomendado	2001:0db8:0000:1111:0000:0000:0000:0200
Comprimido	2001:db8:0:1111::200

Tipos de direcciones IPv6

Unicast, Multicast, Anycast

Existen tres categorías amplias de direcciones IPv6:

- **Unicast** – Identifica de manera única una interfaz de un dispositivo habilitado para IPv6.
- **Multicast** – Se usan para enviar un único paquete IPv6 a varios destinos.
- **Anycast** – Esta es cualquier dirección unicast de IPv6 que puede asignarse a varios dispositivos. Los paquetes enviados a una dirección de anycast se enrutan al dispositivo más cercano que tenga esa dirección.

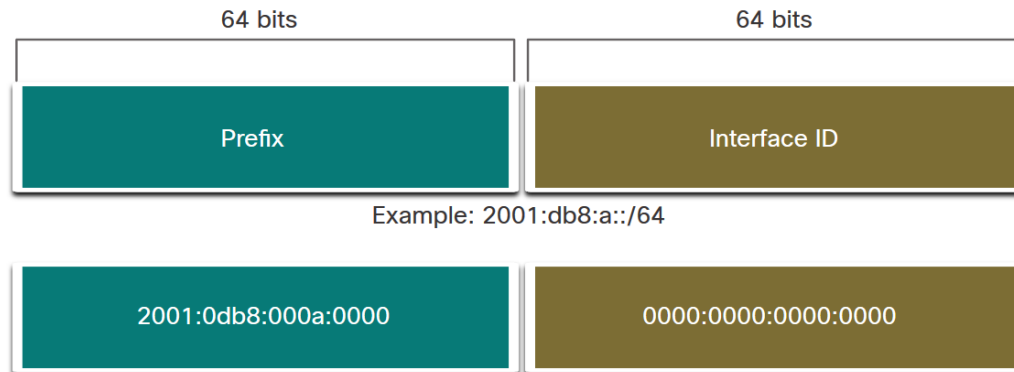
Nota: A diferencia de IPv4, IPv6 no tiene una dirección broadcast. Sin embargo, existe una dirección IPv6 de multicast de todos los nodos que brinda básicamente el mismo resultado.

Tipos de direcciones IPv6

Longitud de prefijo IPv6

La longitud del prefijo se representa en notación de barra diagonal y se usa para indicar la porción de red de una dirección IPv6.

La longitud de prefijo puede ir de 0 a 128. La longitud de prefijo IPv6 recomendada para LAN y la mayoría de los otros tipos de redes es / 64.



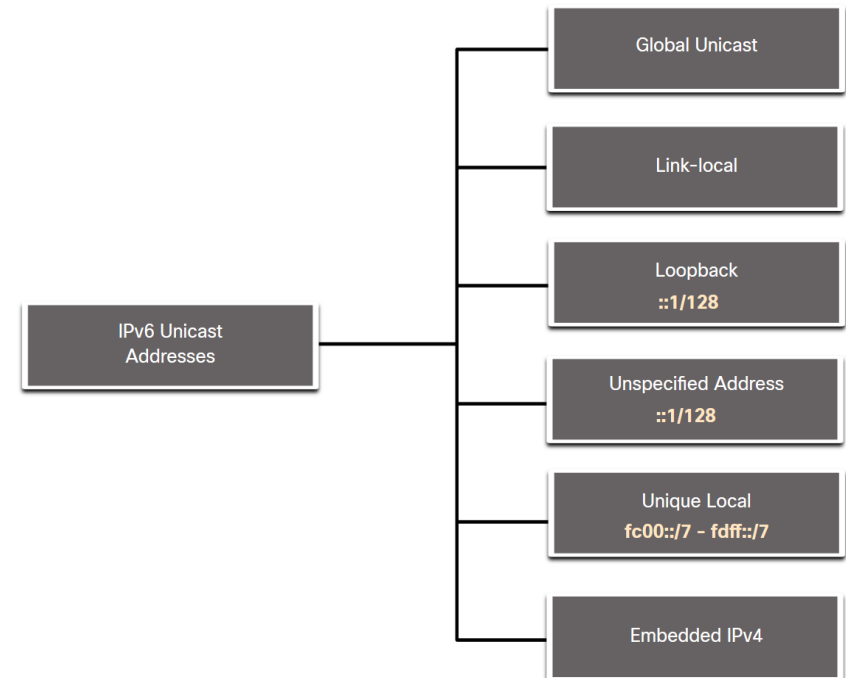
Nota: Se recomienda encarecidamente utilizar un ID de interfaz de 64 bits para la mayoría de las redes. Esto se debe a que la autoconfiguración de direcciones sin estado (SLAAC) utiliza 64 bits para el ID de la interfaz. También facilita la creación y administración de subredes.

Tipos de direcciones IPv6

Tipos de direcciones Unicast de IPv6

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

- **Global Unicast Address (GUA)** – Estas son similares a las direcciones IPv4 públicas. Estas son direcciones enrutables de Internet globalmente exclusivas.
- **Link-local Address (LLA)** - Se requiere para cada dispositivo con IPv6 y se usa para comunicarse con otros dispositivos en el mismo enlace local. Las LLAs no son enrutables y están confinadas a un único enlace.



Tipos de direcciones IPv6

Nota sobre la dirección local única

Las direcciones locales únicas de 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 una cantidad limitada de sitios.
- Se pueden utilizar direcciones locales únicas para dispositivos que nunca necesitarán acceder a otra red.
- Las direcciones locales únicas no se enrutan o traducen globalmente a una dirección IPv6 global.

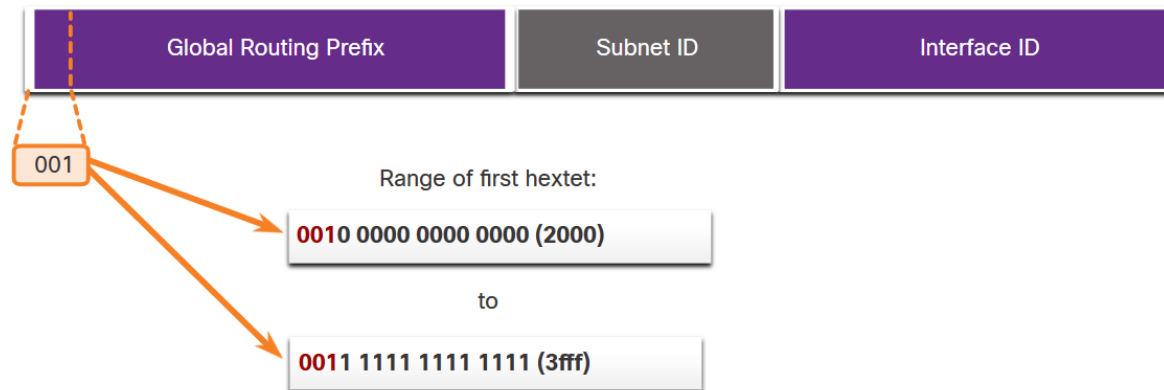
Nota: Muchos sitios utilizan la naturaleza privada de las direcciones RFC 1918 para intentar proteger u ocultar su red de posibles riesgos de seguridad. Este nunca fue el uso previsto de las ULAs.

Tipos de direcciones IPv6

IPv6 GUA

Las direcciones IPv6 unicast globales (GUA), son globalmente únicas y enrutables en Internet IPv6.

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



Tipos de direcciones IPv6

Estructura GUA de IPv6

Prefijo de enrutamiento global:

- El prefijo de enrutamiento global es la parte del prefijo, o red, de la dirección asignada por el proveedor, como un ISP, a un cliente o sitio. El prefijo de enrutamiento global variará en función de las políticas de ISP.

ID de subred

- El campo ID de subred es el área entre el Prefijo de enrutamiento global y la ID de interfaz. Las organizaciones utilizan la ID de subred para identificar subredes dentro de su ubicación.

ID de interfaz

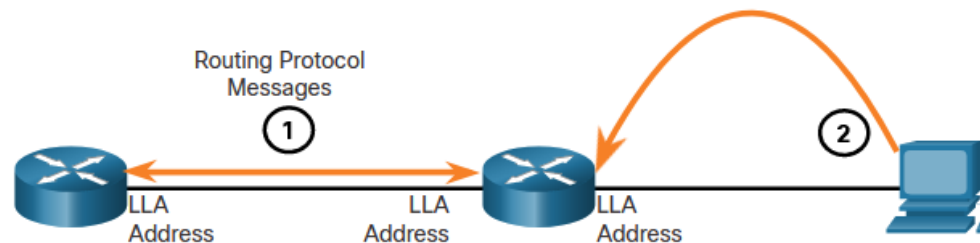
- La ID de interfaz IPv6 equivale a la porción de host de una dirección IPv4. Se recomienda encarecidamente que en la mayoría de los casos se utilicen subredes / 64, lo que crea una ID de interfaz de 64 bits.

Nota: IPv6 permite que las direcciones de host todo-0 y todo-1 se puedan asignar a un dispositivo. La dirección all-0s está reservada como una dirección de difusión ilimitada del router de subred, y debe asignarse solo a los routers.

Tipos de direcciones IPv6 LLA

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

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



1. Routers use the LLA of neighbor routers to send routing updates.
2. Hosts use the LLA of a local router as the default-gateway.

Configuración Estática de GUA y LLA

Configuración Estática de GUA en un Router

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

- El comando para configurar un GUA IPv6 en una interfaz es: **ipv6 address *ipv6-address/prefix-length***.
- El ejemplo muestra comandos para configurar un 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 de GUA en un host de Windows

- Configurar la dirección IPv6 en un host de forma manual es similar a configurar una dirección IPv4.
- El GUA o LLA de la interfaz del router se puede utilizar como el gateway predeterminado. La mejor práctica es utilizar la LLA.

Nota: Cuando se usa DHCPv6 o SLAAC, se especifica automáticamente la LLA del router local como dirección de gateway predeterminado.

Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

☐ Obtain an IPv6 address automatically

☒ Use the following IPv6 address:

IPv6 address: 2001:db8:acad:1::10

Subnet prefix length: 64

Default gateway: 2001:db8:acad:1::1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel

Configuración de GUA estática de una dirección Link-Local Unicast

Configurar la LLA manualmente permite crear una dirección reconocible y más fácil de recordar.

- Las LLAS se pueden configurar manualmente mediante el comando **ipv6 address ipv6-link-local-address link-local** .
- El ejemplo muestra comandos para configurar una 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: La misma LLA se puede configurar en cada enlace siempre que sea única en ese enlace. La práctica común es crear un LLA diferente en cada interfaz del router para facilitar la identificación del router y la interfaz específica.

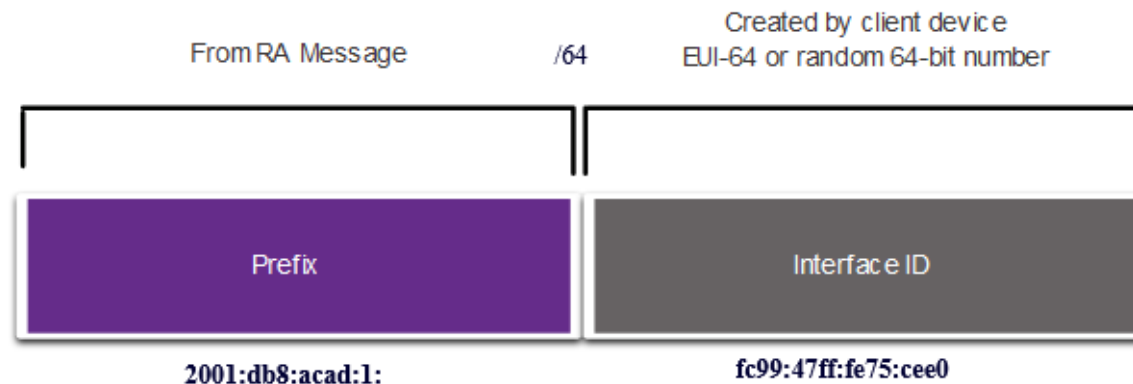
Mensajes RS y RA

Los dispositivos obtienen direcciones GUA dinámicamente a través de mensajes de Internet Control Message Protocol version 6 (ICMPv6).

- Los mensajes de solicitud de router (RS) son enviados por dispositivos host para descubrir routers IPv6
- Los routers envían mensajes de anuncio de router (RA) para informar a los hosts sobre cómo obtener un GUA IPv6 y proporcionar información útil de red, como:
 - Prefijo de red y longitud del prefijo
 - Dirección del gateway predeterminado
 - Direcciones DNS y nombre de dominio
- El RA puede proporcionar tres métodos para configurar un GUA IPv6:
 - SLAAC
 - SLAAC con servidor DHCPv6 stateless
 - Stateful DHCPv6 (no SLAAC)

Método 1: SLAAC

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



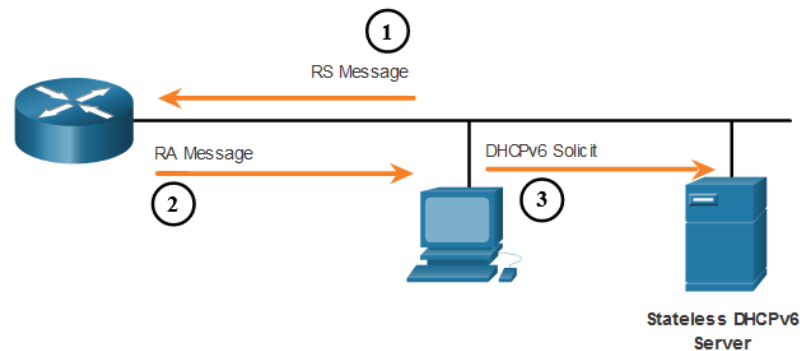
Direccionamiento dinámico para GUA IPv6

Método 2: SLAAC y DHCP sin estado

Una RA puede indicar a un dispositivo que use SLAAC y DHCPv6 stateless.

El mensaje RA sugiere que los dispositivos utilicen lo siguiente:

- SLAAC para crear su propio IPv6 GUA
- La dirección link-local del router, la dirección IPv6 de origen del RA para la dirección de gateway predeterminado
- Un servidor DHCPv6 stateless, que obtendrá otra información como la dirección del servidor DNS y el nombre de dominio



Direccionamiento dinámico para GUA IPv6

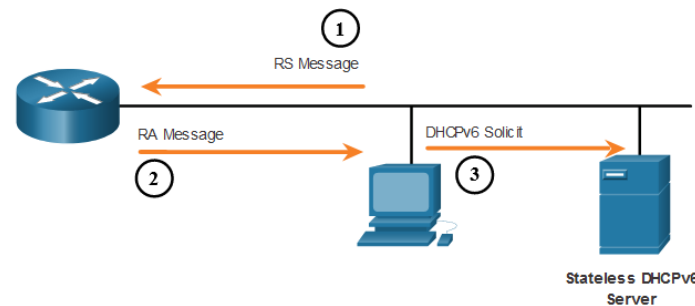
Método 3: DHCPv6 con estado

Un RA puede indicar a un dispositivo que use DHCPv6 Stateful solamente.

DHCPv6 Stateful es similar a DHCP para IPv4. Un dispositivo puede recibir automáticamente un GUA, la longitud de prefijo y las direcciones de los servidores DNS desde un servidor DHCPv6 Stateful.

El mensaje RA sugiere que los dispositivos utilicen lo siguiente:

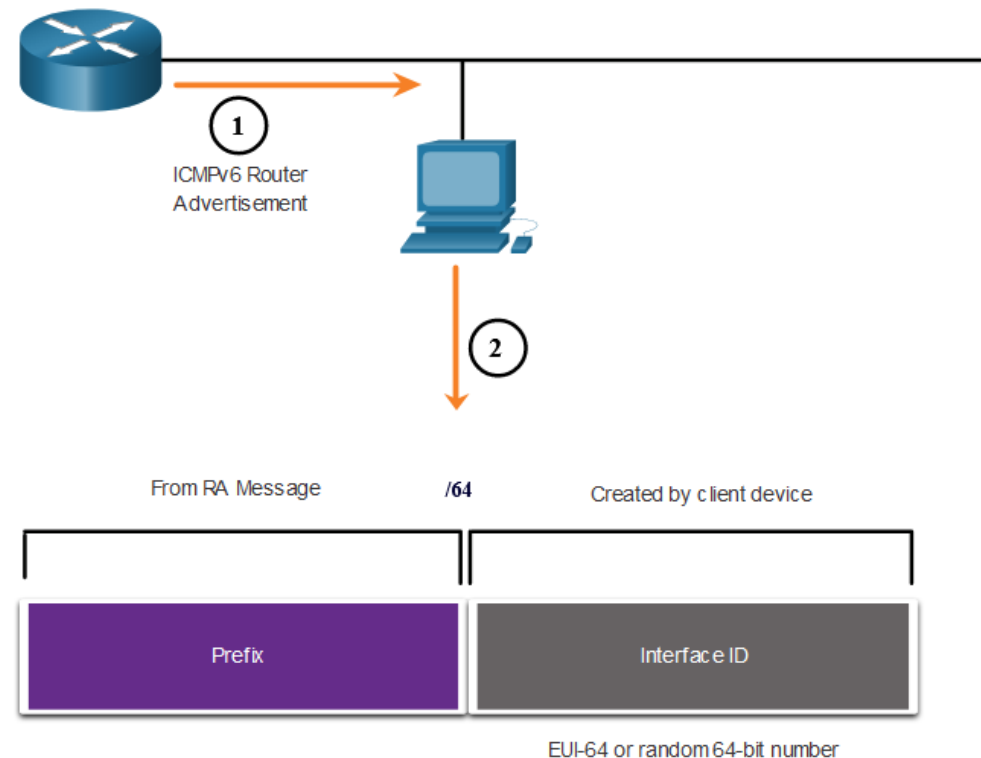
- La dirección LLA del router, que es la dirección IPv6 de origen del RA, para la dirección de gateway predeterminado
- Un servidor DHCPv6 Stateful, para obtener una GUA, otra información como la dirección del servidor DNS y el nombre de dominio



Direccionamiento dinámico para IPv6 GUAs

Proceso EUI-64 vs Generado aleatoriamente

- Cuando el mensaje RA es SLAAC o SLAAC con DHCPv6 stateless, el cliente debe generar su propia ID de interfaz.
- La ID de interfaz se puede crear utilizando el proceso EUI-64 o un número de 64 bits generado aleatoriamente.



Direccionamiento dinámico para GUA

IPv6 Proceso EUI-64

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

- Un valor de 16 bits de fffe (en hexadecimal) se inserta en el centro de la dirección MAC Ethernet de 48 bits del cliente.
- El 7ºbit de la dirección MAC del cliente se invierte del binario 0 al 1.
- Por ejemplo:

MAC de 48 bits	fc: 99:47:75:ce:e0
Id. de interfaz EUI-64	fe: 99:47:ff:fe:75:ce:e0

Direccionamiento dinámico para IPv6 GUAs ID de interfaz generados aleatoriamente

Según el sistema operativo, un dispositivo puede utilizar una ID de interfaz generada aleatoriamente en lugar de utilizar la dirección MAC y el proceso EUI-64.

A partir de Windows Vista, Windows utiliza una ID de interfaz generada aleatoriamente en lugar de una ID de interfaz creada mediante EUI-64.

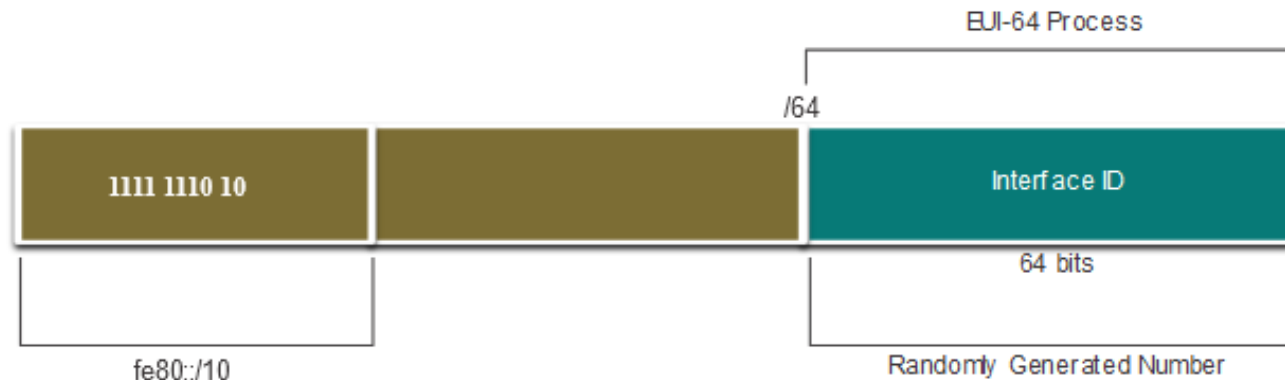
```
C:\> ipconfig
Windows IP Configuration
Conexión de área local del adaptador Ethernet:
Connection-specific DNS Suffix. :
IPv6 Address. . . . . : 2001:db8:acad: 1:50 a 5:8 a35:a5bb:66e1
Link-local IPv6 Address . . . . .: fe80: :50a 5:8 a35:a5bb:66e1
Default Gateway . . . . . : fe80::1
C:\>
```

Nota: Para garantizar la exclusividad de cualquier dirección unicast de IPv6, el cliente puede usar un proceso denominado "detección de direcciones duplicadas" (DAD) Es similar a una solicitud de ARP para su propia dirección. Si no se obtiene una respuesta, la dirección es única.

Direccionamiento dinámico para LLAs IPv6

LLAs Dinámicas

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



Direccionamiento dinámico para LLAS IPv6

LLAs Dinámicas en Windows

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

ID de interfaz generada mediante EUI-64

```
C:\> ipconfig
Windows IP Configuration
Conexión de área local del adaptador Ethernet:
Connection-specific DNS Suffix. :
IPv6 Address. . . . . : 2001:db8:acad:1:fc 99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc 99:47ff:fe75:cee0
Default Gateway . . . . . : fe80::1
C:\>
```

ID de interfaz de 64 bits generada aleatoriamente

```
C:\> ipconfig
Windows IP Configuration
Conexión de área local del adaptador Ethernet:
Connection-specific DNS Suffix. :
IPv6 Address. . . . . : 2001:db8:acad:1:50a 5:8 a35:a5bb:66e1
Link-local IPv6 Address . . . . . : fe80::50a 5:8 a35:a5bb:66e1
Default Gateway . . . . . : fe80::1
C:\>
```

Direccionamiento Dinámico para LLAs IPv6

LLAs Dinámicas en Routers Cisco

Los routers Cisco crean automáticamente un LLA IPv6 cada vez que se asigna una GUA a la interfaz. De manera predeterminada, los routers con Cisco IOS utilizan EUI-64 para generar la ID de interfaz para todas las direcciones LLAs en las interfaces IPv6.

Aquí hay 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
```

Verificar la configuración de direcciones IPv6

Los routers Cisco crean automáticamente un LLA IPv6 cada vez que se asigna una GUA a la interfaz. De manera predeterminada, los routers con Cisco IOS utilizan EUI-64 para generar la ID de interfaz para todas las direcciones LLAs en las interfaces IPv6.

Aquí hay 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
```

Direcciones Multicast de IPv6

Direcciones Multicast de IPv6 Asignadas

Las direcciones multicast de IPv6 tienen el prefijo FF00::/8. Existen dos tipos de direcciones multicast de IPv6:

- Dirección de red multicast conocida
- Dirección multicast de nodo solicitado

Nota: las direcciones multicast solo pueden ser direcciones de destino y no direcciones de origen.

Direcciones Multicast de IPv6

Direcciones Multicast de IPv6 conocidas

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

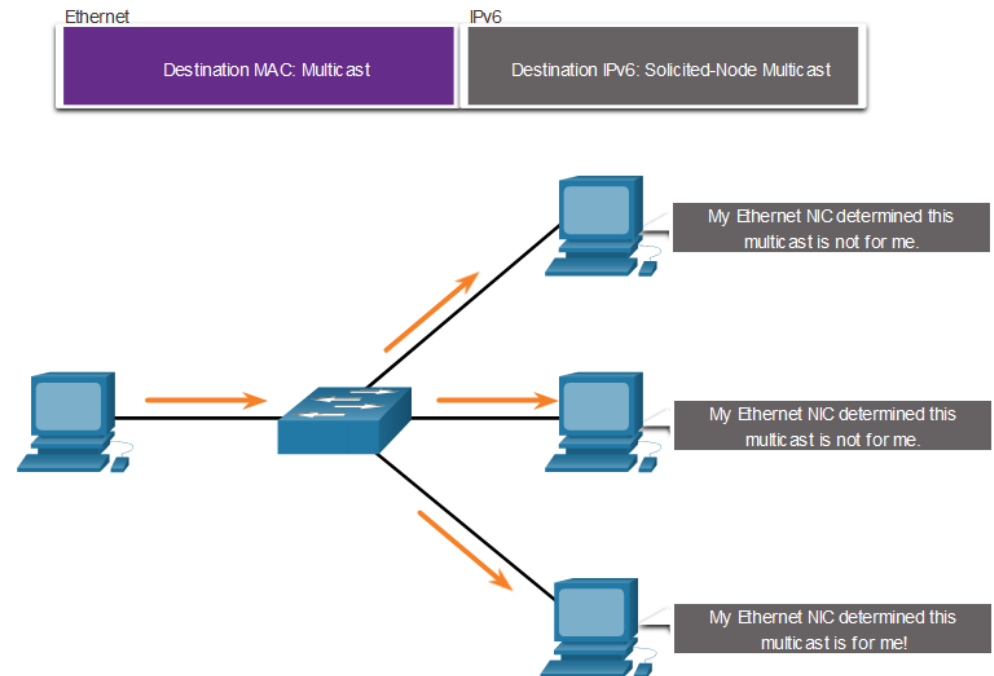
Hay dos grupos comunes de direcciones IPv6 multicast asignadas:

- **Grupo de multicast FF02::1 para todos los nodos** - Este es un grupo multicast al que se unen todos los dispositivos con IPv6 habilitado. Los paquetes que se envían a este grupo son recibidos y procesados por todas las interfaces IPv6 en el enlace o en la red.
- **ff02 :: 2 Grupo de multicast de todos los routers** - Este es un grupo multicast al que se unen todos los dispositivos con IPv6 habilitado. Un router comienza a formar parte de este grupo cuando se lo habilita como router IPv6 con el **comando de configuración global** ipv6 unicast-routing.

Direcciones multicast de IPv6

Direcciones multicast de IPv6 de nodo solicitado

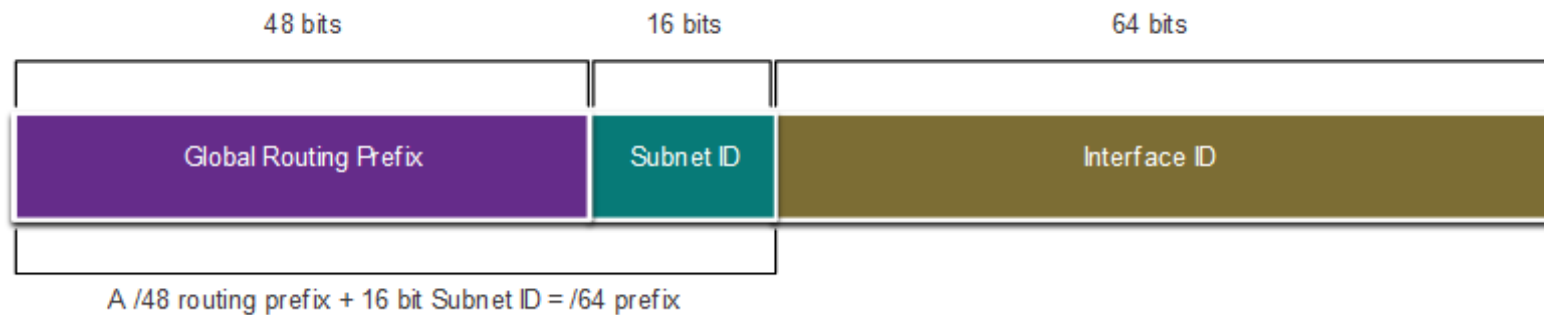
- Una dirección multicast de nodo solicitado es similar a una dirección multicast de todos los nodos.
- Una dirección multicast de nodo solicitado se asigna a una dirección especial de multicast de Ethernet.
- Esto permite que la NIC Ethernet filtre la trama al examinar la dirección MAC de destino sin enviarla al proceso de IPv6 para ver si el dispositivo es el objetivo previsto del paquete IPv6.



División de una red IPv6 en subredes
División en subredes mediante la ID de subred

IPv6 se diseñó teniendo en cuenta las subredes.

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



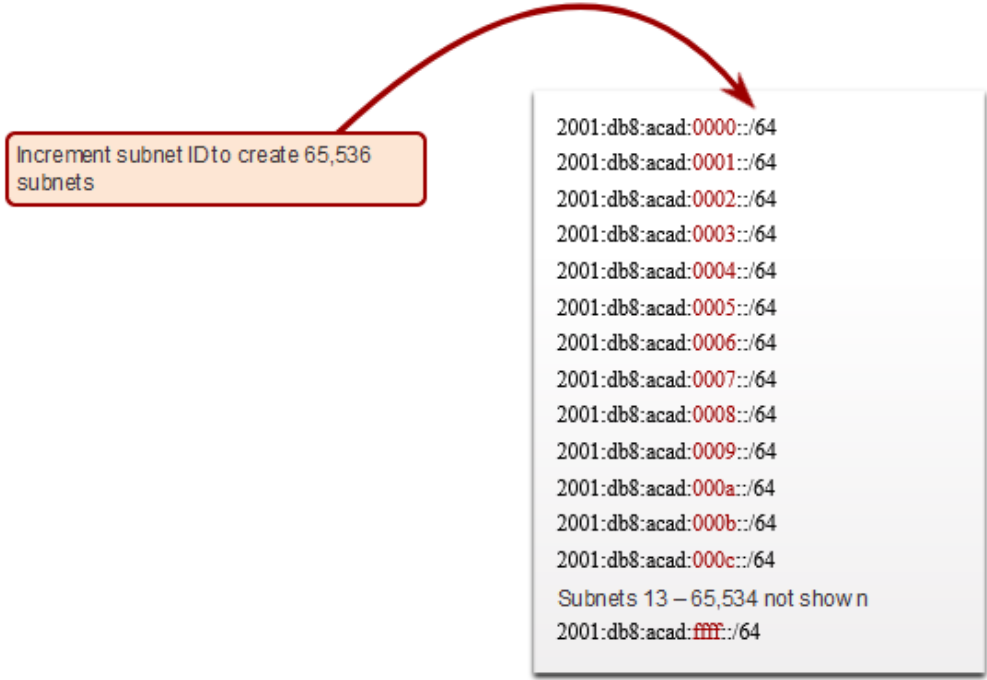
Subnetear una red IPv6

Ejemplo de subneteo 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 igual para todas las subredes.
- Solo se incrementa el hexteto de la ID de subred en sistema hexadecimal para cada subred.

Increment subnet ID to create 65,536 subnets

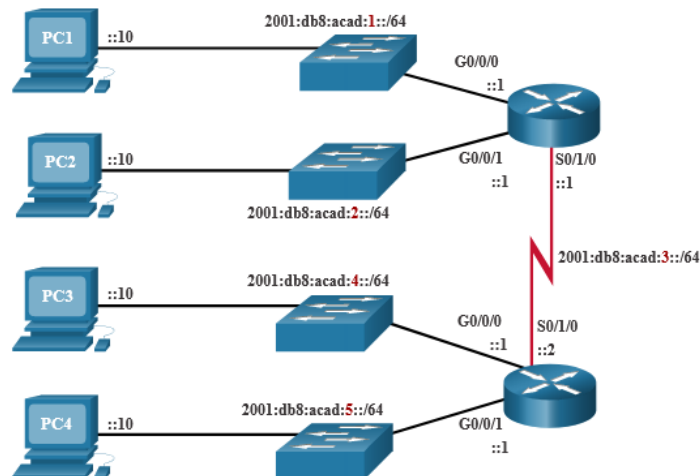


```
2001:db8:acad:0000::/64
2001:db8:acad:0001::/64
2001:db8:acad:0002::/64
2001:db8:acad:0003::/64
2001:db8:acad:0004::/64
2001:db8:acad:0005::/64
2001:db8:acad:0006::/64
2001:db8:acad:0007::/64
2001:db8:acad:0008::/64
2001:db8:acad:0009::/64
2001:db8:acad:000a::/64
2001:db8:acad:000b::/64
2001:db8:acad:000c::/64
Subnets 13 – 65,534 not shown
2001:db8:acad:ffff::/64
```


Subnetear una red IPv6 Asignación de subred IPv6

La topología de ejemplo requiere cinco subredes, una para cada LAN, así como para el enlace en serie entre R1 y R2.

Se asignaron las cinco subredes IPv6, con el campo ID de subred 0001 a 0005. Cada subred /64 proporcionará más direcciones de las que jamás se necesitarán.



5 subnets allocated from 65,536 available subnets

Address Block 2001:0db8:acad::/48

```
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
```

Subnetear una red IPv6

Router configurado con subredes IPv6

El ejemplo muestra que cada una de las interfaces del router 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
```

ICMP

Mensajes ICMP

Mensajes ICMPv4 e ICMPv6

- Internet Control Message Protocol (ICMP) proporciona información sobre problemas relacionados con el procesamiento de paquetes IP bajo ciertas condiciones.
- El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 es el protocolo de mensajería para IPv6 e incluye funcionalidad adicional.
- Los mensajes ICMP comunes a ICMPv4 e ICMPv6 incluyen:
 - Accesibilidad al host
 - Destino o servicio inaccesible
 - Tiempo superado

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

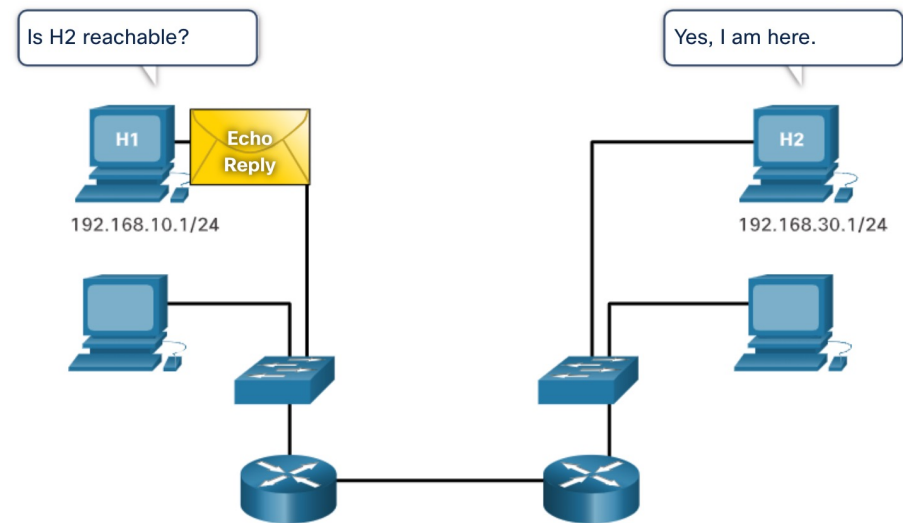
Mensajes ICMP

Accesibilidad del host

ICMP Echo Message se puede utilizar para probar la accesibilidad de un host en una red IP.

En el ejemplo:

- El host local envía una solicitud de eco ICMP a un host.
- Si el host se encuentra disponible, el host de destino responde con una respuesta de eco.



Mensajes ICMP

Destino o servicio inalcanzable

- Se puede utilizar un mensaje de destino inalcanzable ICMP para notificar al origen que un destino o servicio no es accesible.
- 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: red inalcanzable
- 1: host inalcanzable
- 2: protocolo inalcanzable
- 3: puerto inalcanzable

Algunos códigos de destino inalcanzables para ICMPv6 son los siguientes:

- 0 - No hay ruta para el destino
- 1 - La comunicación con el destino está prohibida administrativamente (por ejemplo, firewall)
- 2 — Más allá del alcance de la dirección de origen
- 3 - No se puede alcanzar la dirección
- 4 – Puerto inalcanzable

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

Mensajes ICMP

Tiempo excedido

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

```
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 **tracert**.

Mensajes ICMP

Mensajes ICMPv6

ICMPv6 tiene nuevas características y funcionalidad mejorada que no se encuentra en ICMPv4, incluyendo cuatro nuevos protocolos como parte del protocolo de detección de vecinos (ND o NDP).

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

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

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

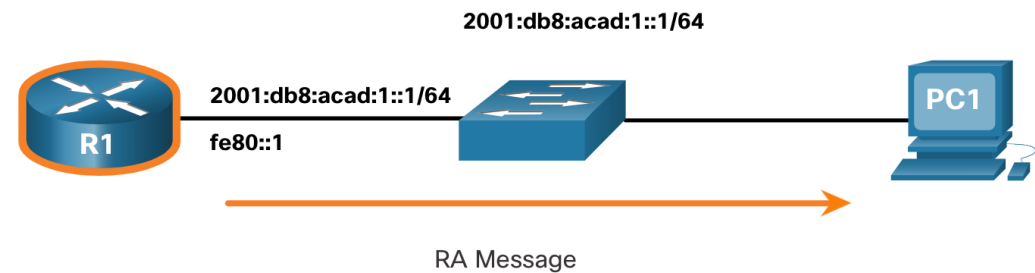
- Mensaje de solicitud de vecino (NS)
- Mensaje de anuncio de vecino (NA)

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

Mensajes ICMP

Mensajes ICMPv6 (cont.)

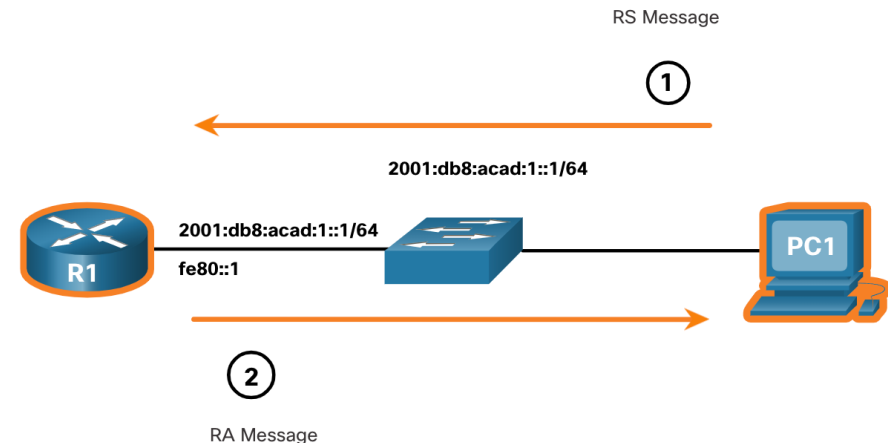
- Los routers habilitados para IPv6 envían mensajes de RA cada 200 segundos para proporcionar información de direccionamiento a los hosts habilitados para IPv6.
- El mensaje RA puede incluir información de direccionamiento para el host, como el prefijo, la longitud del prefijo, la dirección DNS y el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



Mensajes ICMP

Mensajes ICMPv6 (cont.)

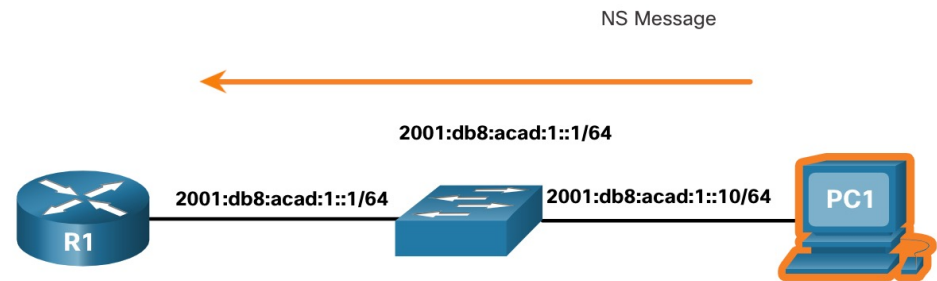
- Un router habilitado para IPv6 también enviará un mensaje RA en respuesta a un mensaje RS.
- En la figura, PC1 envía un mensaje RS para determinar cómo recibir dinámicamente su información de dirección IPv6.
 - R1 responde a la RS con un mensaje de RA.
 - PC1 envía un mensaje RS, «Hola, acabo de arrancar. ¿Hay un router IPv6 en la red? Necesito saber cómo obtener la información de mi dirección IPv6 de forma dinámica».
 - R1 responde con un mensaje de 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 enlace fe80::1 como su puerta de enlace predeterminada.»



Mensajes ICMP

Mensajes ICMPv6 (cont.)

- Un dispositivo asignado a una unidifusión IPv6 global o dirección unidifusión local de vínculo puede realizar la detección de direcciones duplicadas (DAD) para asegurarse de que la dirección IPv6 es única.
- Para verificar la unicidad de una dirección, el dispositivo enviará un mensaje NS con su propia dirección IPv6 como la dirección IPv6 objetivo.
- Si otro dispositivo en la red tiene esta dirección, responderá con un mensaje de NA notificando al dispositivo emisor que la dirección está en uso.

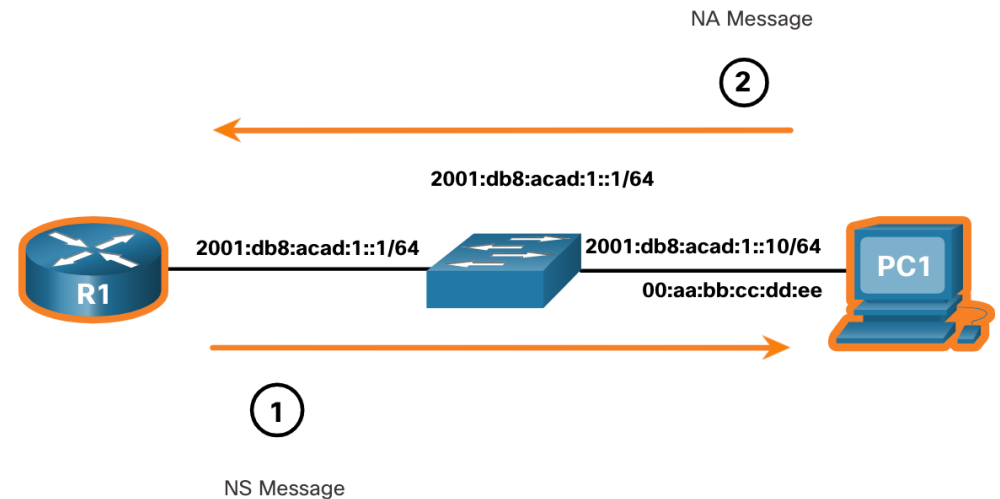


Nota: No se requiere DAD, pero RFC 4861 recomienda que DAD se realice en direcciones unicast.

Mensajes ICMP

Mensajes ICMPv6 (cont.)

- Para determinar la dirección MAC del destino, el dispositivo envía un mensaje de NS a la dirección de nodo solicitado.
- El mensaje incluye la dirección IPv6 conocida (objetivo). El dispositivo que se destinó a la dirección IPv6 responde con un mensaje NA que contiene la dirección MAC de Ethernet.
- En la figura, R1 envía un mensaje NS a 2001:db8:acad:1::10 pidiendo su dirección MAC.



Pruebas de Ping y Traceroute

Ping — Prueba de conectividad

- El comando **ping** es una utilidad de pruebas IPv4 e IPv6 que utiliza mensajes de solicitud de eco y respuesta de eco ICMP para probar la conectividad entre hosts y proporciona un resumen que incluye la tasa de éxito y el tiempo medio de ida y vuelta al destino.
- Si no se recibe una respuesta dentro del tiempo de espera, el comando ping proporciona un mensaje que indica que no se recibió una respuesta.
- Es común que el primer ping se agote 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
```

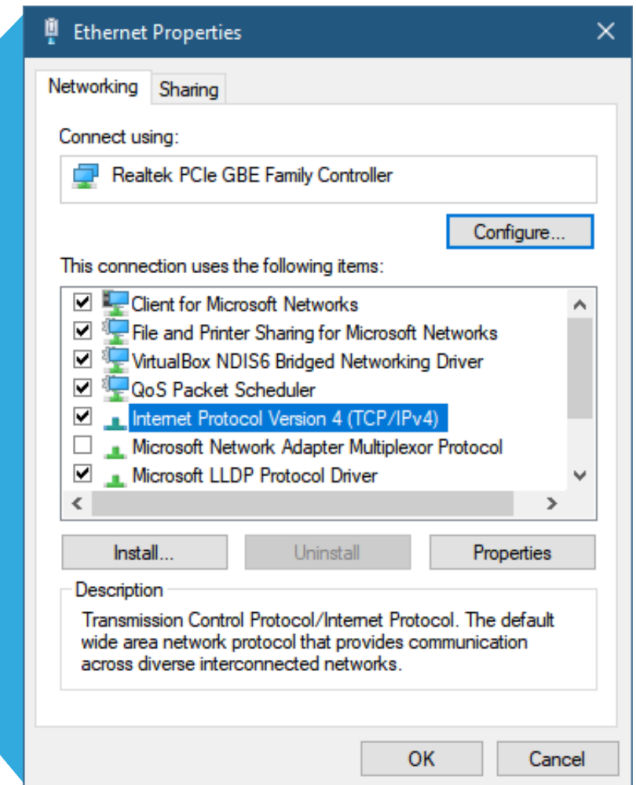
```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Pruebas de ping y Traceroute

Haga ping al Loopback

Ping se puede usar para probar la configuración interna de IPv4 o IPv6 en el host local. Para hacer esto, **haga ping** a la dirección de loopback local 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 funciona en el host.

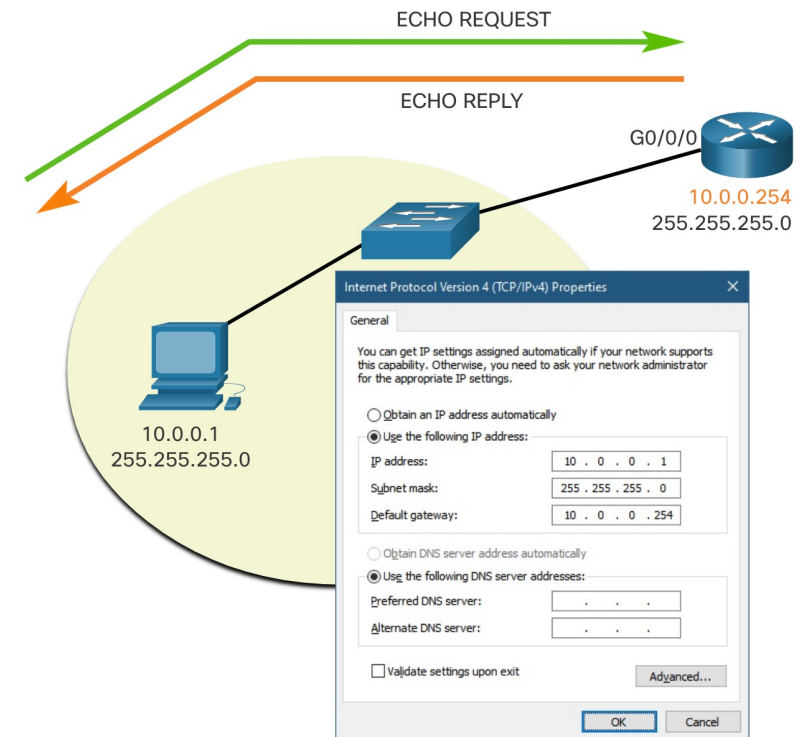


Hacer ping a la puerta de enlace predeterminada

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

La dirección de puerta de enlace predeterminada se usa con mayor frecuencia porque el router normalmente siempre está operativo.

- Un **ping** exitoso a la puerta de enlace predeterminada indica que el host y la interfaz del router que sirven como puerta de enlace predeterminada están operativos en la red local.
- Si la dirección de 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.



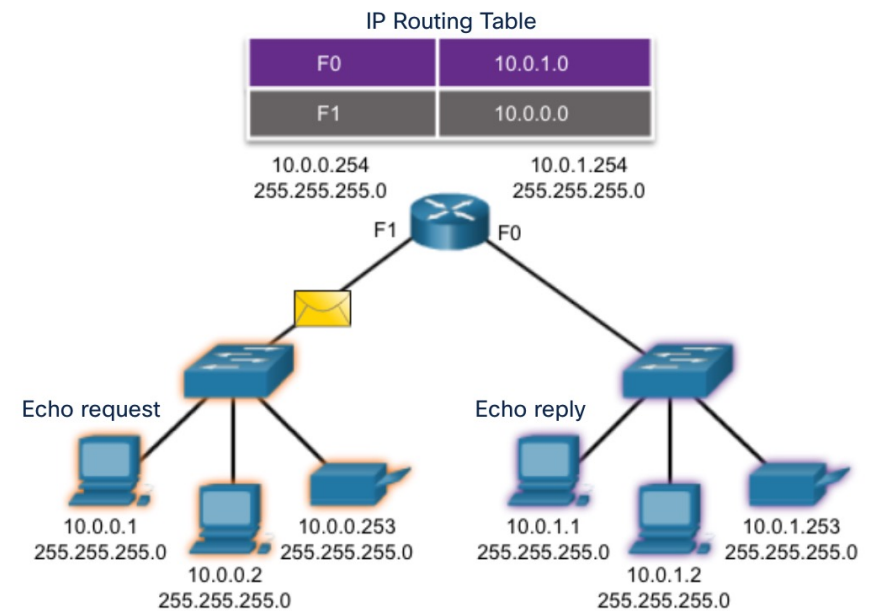
Pruebas de Ping y Traceroute

Hacer ping a un host remoto

También se puede utilizar el comando ping para probar la capacidad de un host local para comunicarse en una interconexión de redes.

Un host local puede hacer ping a un host de una red remota. Un **ping** exitoso a través de la red interna 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 – Pruebe el camino

- Traceroute (**tracert**) es una utilidad que se usa para probar la ruta entre dos hosts y proporcionar una lista de 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 del camino e indica si un salto no responde. Se utiliza un asterisco (*) para indicar un paquete perdido o sin respuesta.
- Esta información se puede usar para localizar un router problemático en la ruta o puede indicar que el router está configurado para no responder.

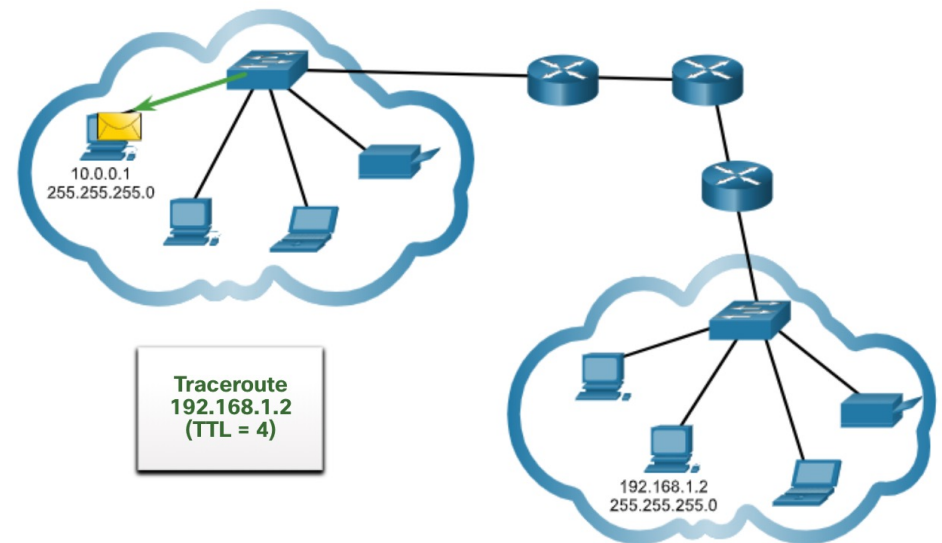
```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

 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 Límite de salto en IPv6 en los encabezados de Capa 3, junto con el mensaje Tiempo excedido ICMP.

Traceroute – Pruebe el camino (Cont.)

- El primer mensaje enviado desde traceroute tendrá un valor de campo TTL de 1. Esto hace que el TTL expire en el primer router. Este router responde con un mensaje ICMPv4 Tiempo excedido.
- A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. Esto proporciona el rastro con la dirección de cada salto a medida que los paquetes caducan más adelante en la ruta.
- El campo TTL sigue aumentando hasta que se alcanza el destino, o se incrementa a un máximo predefinido.



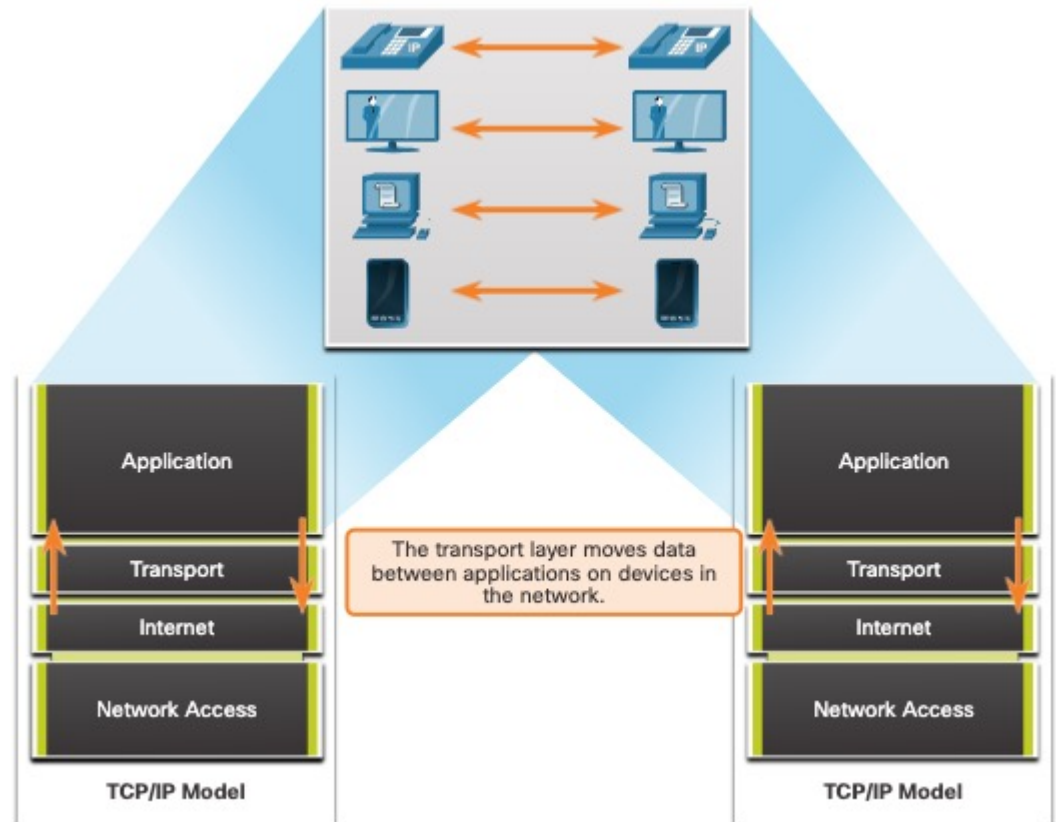
Capa de Transporte

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.
- Enlace entre la capas de aplicación y las capas inferiores que se encargan de la transmisión a través de la red.

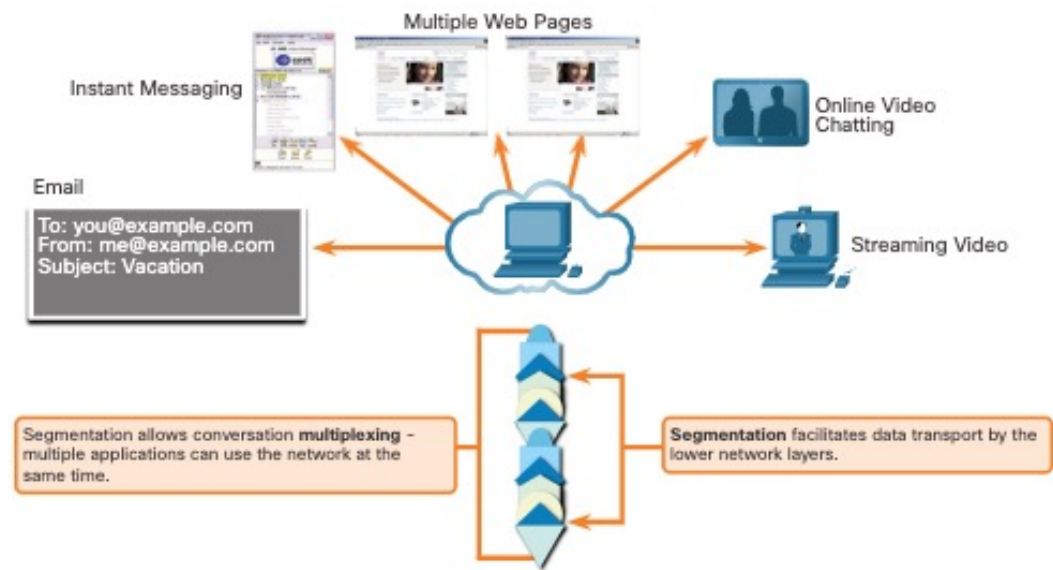


Transporte de datos

Tareas de la capa de transporte

La capa de transporte tiene las siguientes responsabilidades:

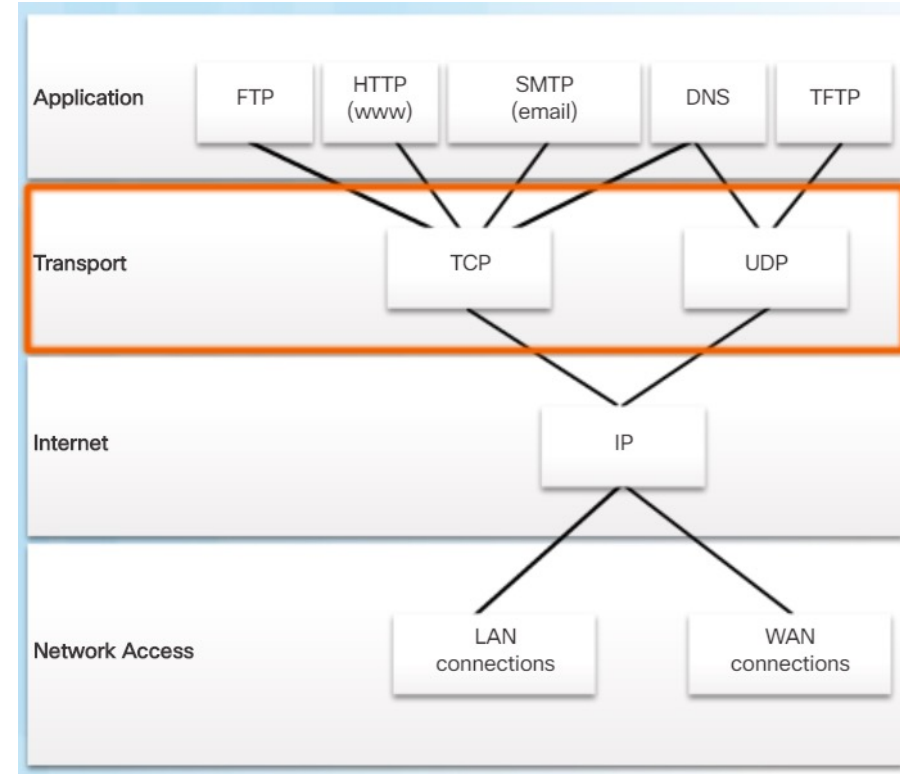
- Seguimiento de conversaciones individuales
- Segmentación de datos y rearmado de segmentos
- Agregar información de encabezado
- Identificar, separar y administrar múltiples conversaciones
- Utiliza segmentación y multiplexación para permitir que diferentes conversaciones de comunicación se intercalen en la misma red



Transporte de datos

Protocolos de la capa de transporte

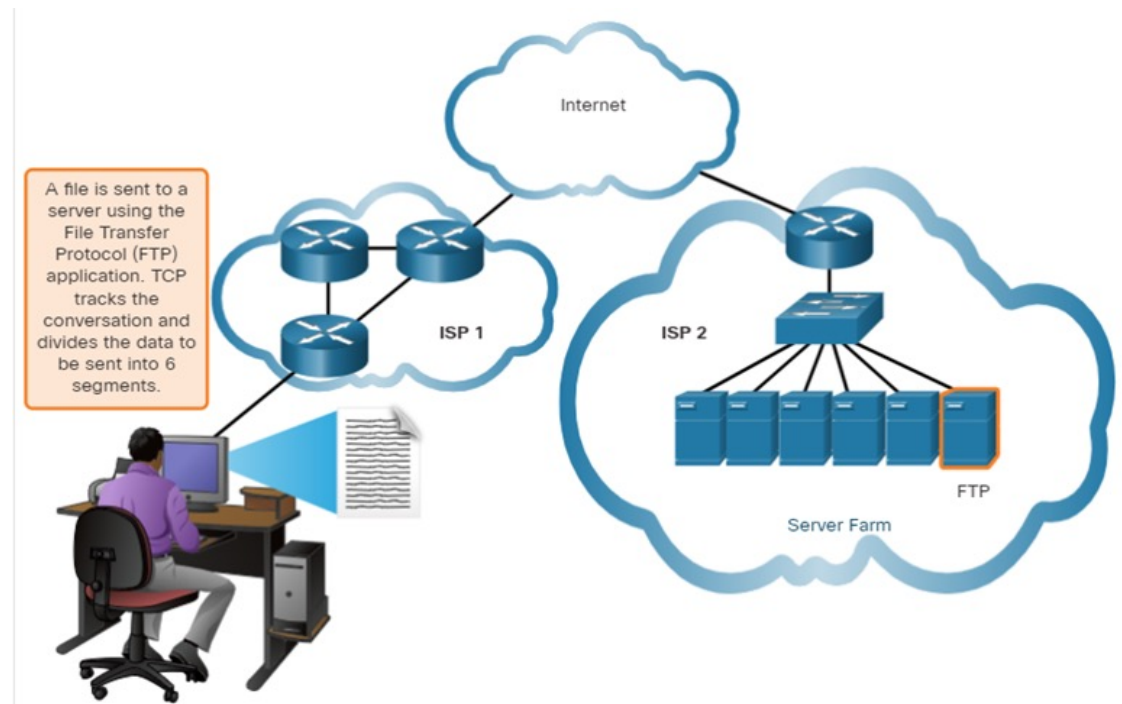
- IP no especifica la manera en que se lleva a cabo la entrega o el transporte de los paquetes.
- Los protocolos de capa de transporte especifican cómo transferir mensajes entre hosts y son responsables de administrar los requisitos de fiabilidad de una conversación.
- La capa de transporte incluye los protocolos TCP y UDP.



Transmission Control Protocol (Protocolo de control de transmisión)

TCP provee confiabilidad y control de flujo Operaciones básicas TCP:

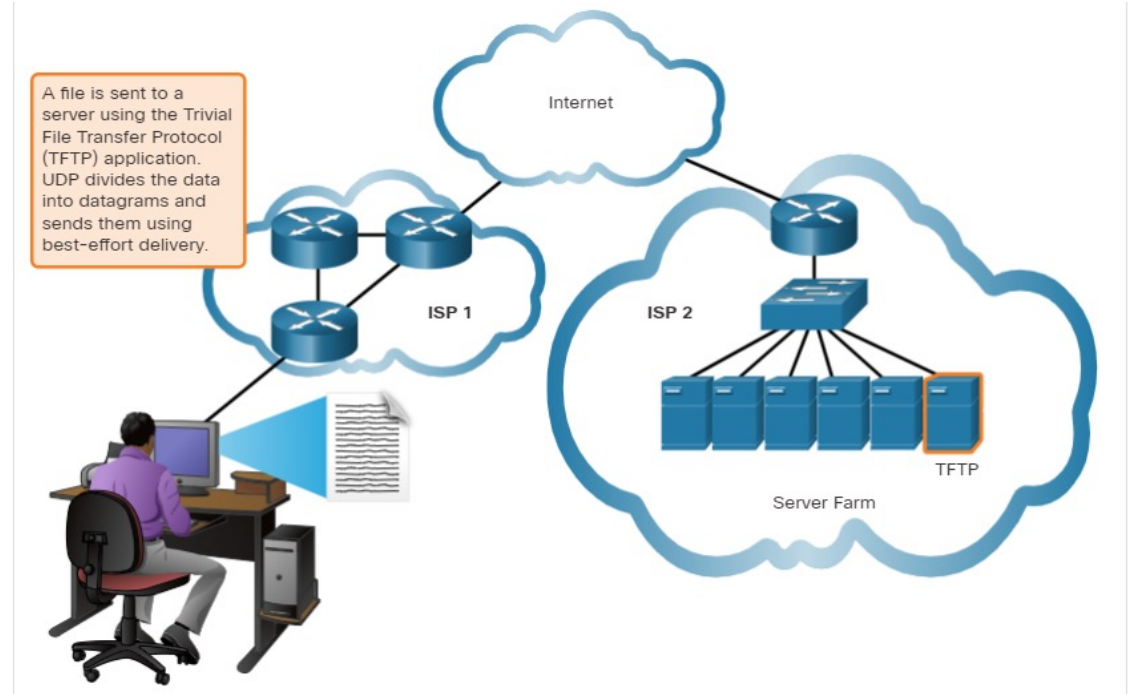
- Numere y rastree segmentos de datos transmitidos a un host específico desde una aplicación específica
- Confirmar datos recibidos
- Vuelva a transmitir cualquier información no reconocida después de un cierto período de tiempo
- Datos de secuencia que pueden llegar en un orden incorrecto
- Enviar datos a una velocidad eficiente que sea aceptable por el receptor



Protocolo de datagramas de usuario de datos (UDP)

El UDP proporciona las funciones básicas para entregar segmentos de datos entre las aplicaciones adecuadas, con muy poca sobrecarga y revisión de datos.

- UDP es un protocolo sin conexión.
- UDP también se conoce como un protocolo de entrega de mejor esfuerzo porque no hay reconocimiento de que los datos se reciben en el destino.



El protocolo de capa de transporte adecuado para la aplicación en cuestión

UDP también es utilizado por las aplicaciones de solicitud y respuesta donde los datos son mínimos, y la retransmisión se puede hacer rápidamente.

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

UDP



VoIP
(IP telephony)



DNS
(Domain Name Resolution)

Required protocol properties:

- Fast
- Low overhead
- Does not require acknowledgements
- Does not resend lost data
- Delivers data as it arrives

TCP



SMTP/IMAP
(Email)



HTTP/HTTPS
(World Wide Web)

Required protocol properties:

- Reliable
- Acknowledges data
- Resends lost data
- Delivers data in sequenced order

Descripción general de TCP

Características de TCP

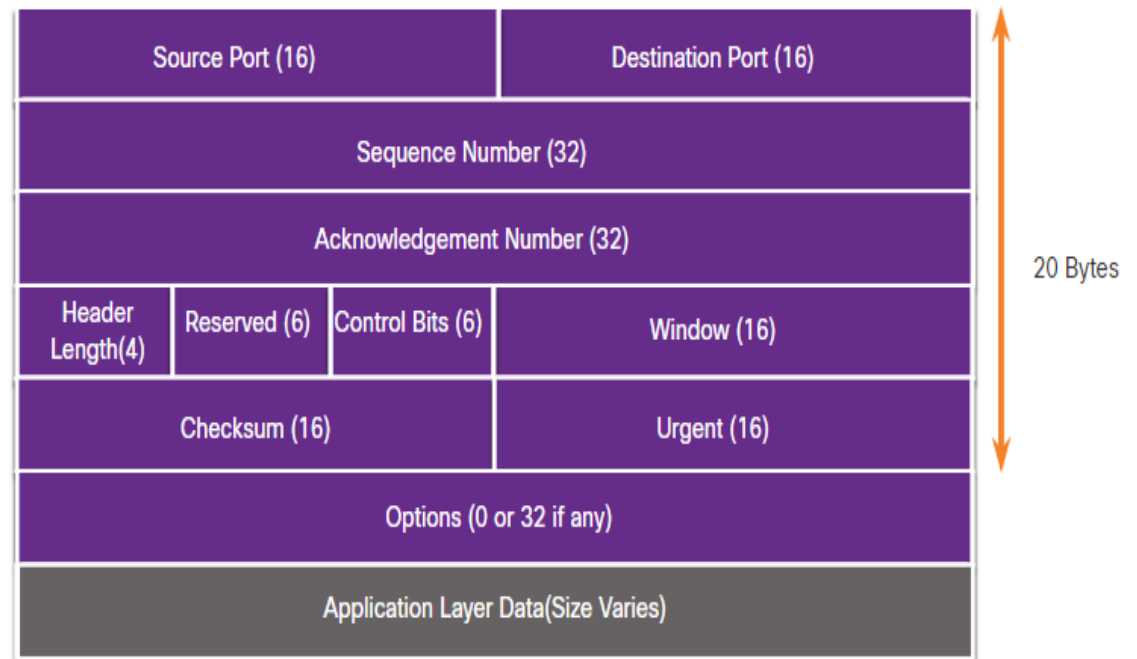
- **Establece una sesión** -TCP es un protocolo orientado a la conexión que negocia y establece una conexión permanente (o sesión) entre los dispositivos de origen y destino antes de reenviar cualquier tráfico.
- **Garantiza una entrega confiable**- Por muchas razones, es posible que un segmento se corrompa o se pierda por completo, ya que se transmite a través de la red. TCP asegura que cada segmento que envía la fuente llega al destino.
- **Proporciona entrega en el mismo pedido** - 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 (es decir, memoria y potencia de procesamiento). Cuando TCP advierte que estos recursos están sobrecargados, puede solicitar que la aplicación emisora reduzca la velocidad del flujo de datos.

Descripción general de TCP

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 se envió y qué información se reconoció.



Introducción a TCP

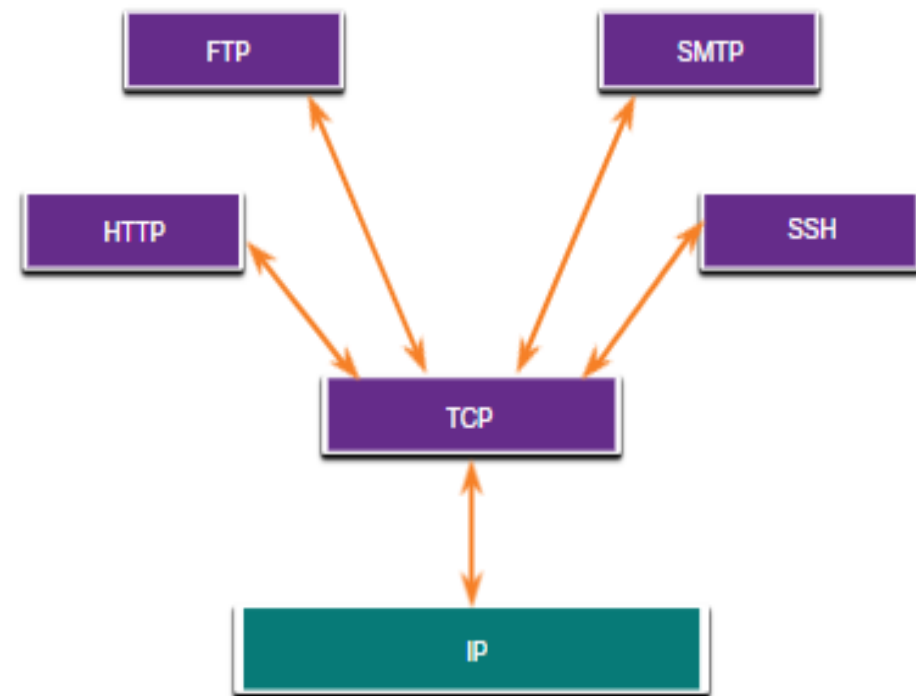
Campos de encabezado TCP

Campo de encabezado TCP	Descripción
Puerto de origen	Campo de 16 bits utilizado para identificar la aplicación de origen por número de puerto.
Puerto de destino	Campo de 16 bits utilizado para identificar la aplicación de destino por número de puerto.
Número de secuencia	Campo de 32 bits utilizado para reensamblar datos.
de 32 bits	Un campo de 32 bits utilizado para indicar que se han recibido datos y el siguiente byte esperado de la fuente.
Longitud del encabezado	Campo de 4 bits conocido como «desplazamiento de datos» que indica la longitud del encabezado del segmento TCP.
Reservado	Un campo de 6 bits que está reservado para uso futuro.
Bits de control	Un campo de 16 bits utilizado que incluye códigos de bit, o indicadores, que indican el propósito y la función del segmento TCP.
Tamaño de la ventana	Un campo de 16 bits utilizado para indicar el número de bytes que se pueden aceptar
Suma de comprobación	A 16-bit field used for error checking of the segment header and data.
Urgente	Campo de 16 bits utilizado para indicar si los datos contenidos son urgentes.

Descripción general de TCP

Aplicaciones que utilizan TCP

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.



Descripción general de UDP

Características UDP

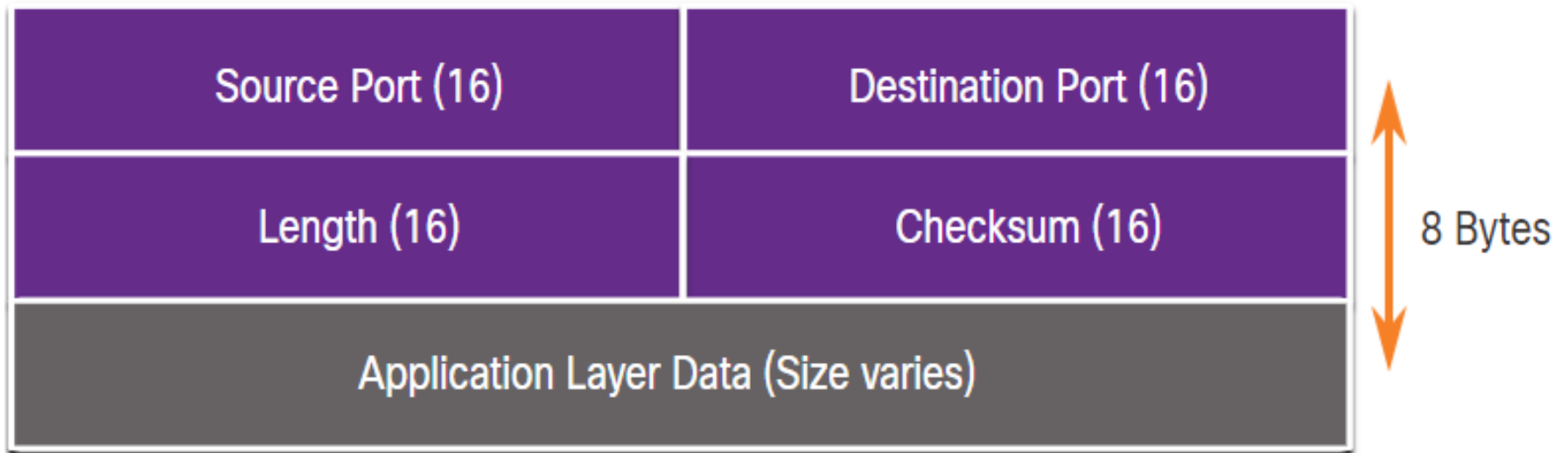
Las características UDP incluyen lo siguiente:

- Los datos se reconstruyen en el orden en que se recibieron.
- Los segmentos perdidos no se vuelven a enviar.
- No hay establecimiento de sesión.
- El envío no está informado sobre la disponibilidad de recursos.

Descripción general de UDP

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).



Visión General de UDP

Campos de Encabezado UDP

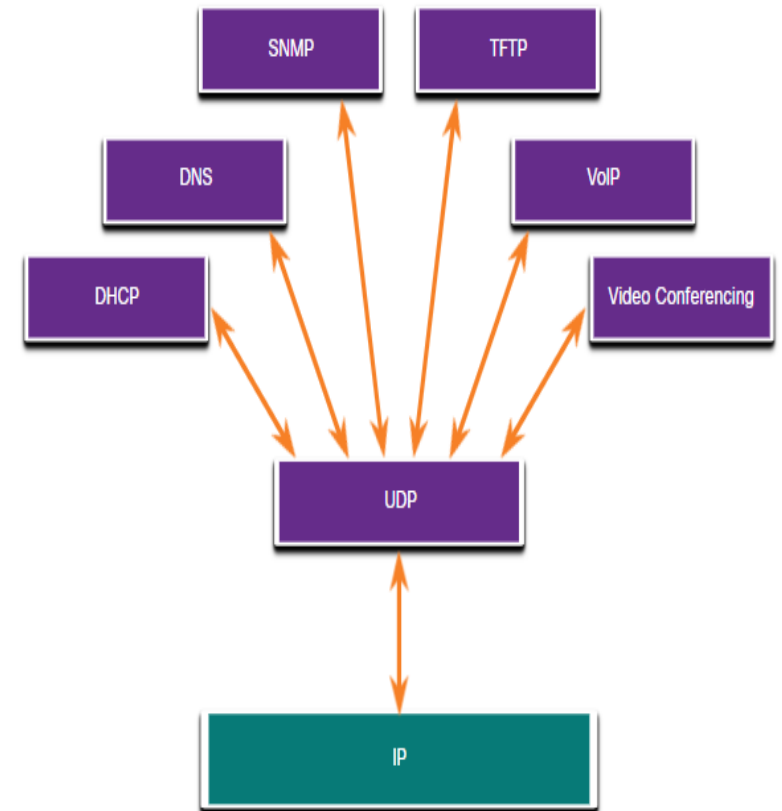
La tabla identifica y describe los cuatro campos de un encabezado UDP.

Campo de encabezado UDP	Descripción
Puerto de origen	Campo de 16 bits utilizado para identificar la aplicación de origen por número de puerto.
Puerto de destino	Campo de 16 bits utilizado 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 comprobación	Campo de 16 bits utilizado para la comprobación de errores del encabezado y los datos del datagrama.

Descripción general de UDP

Aplicaciones que utilizan TCP

- Aplicaciones de video y multimedia en vivo:- estas aplicaciones pueden tolerar cierta pérdida de datos, pero requieren poco o ningún retraso. Los ejemplos incluyen VoIP y la transmisión de video en vivo.
- Aplicaciones con solicitudes y respuestas simples: aplicaciones con transacciones simples en las que un host envía una solicitud y existe la posibilidad de que reciba una respuesta o no. 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 la aplicación puede manejarlos. Los ejemplos incluyen SNMP y TFTP.



Números de puerto Comunicaciones separadas múltiples

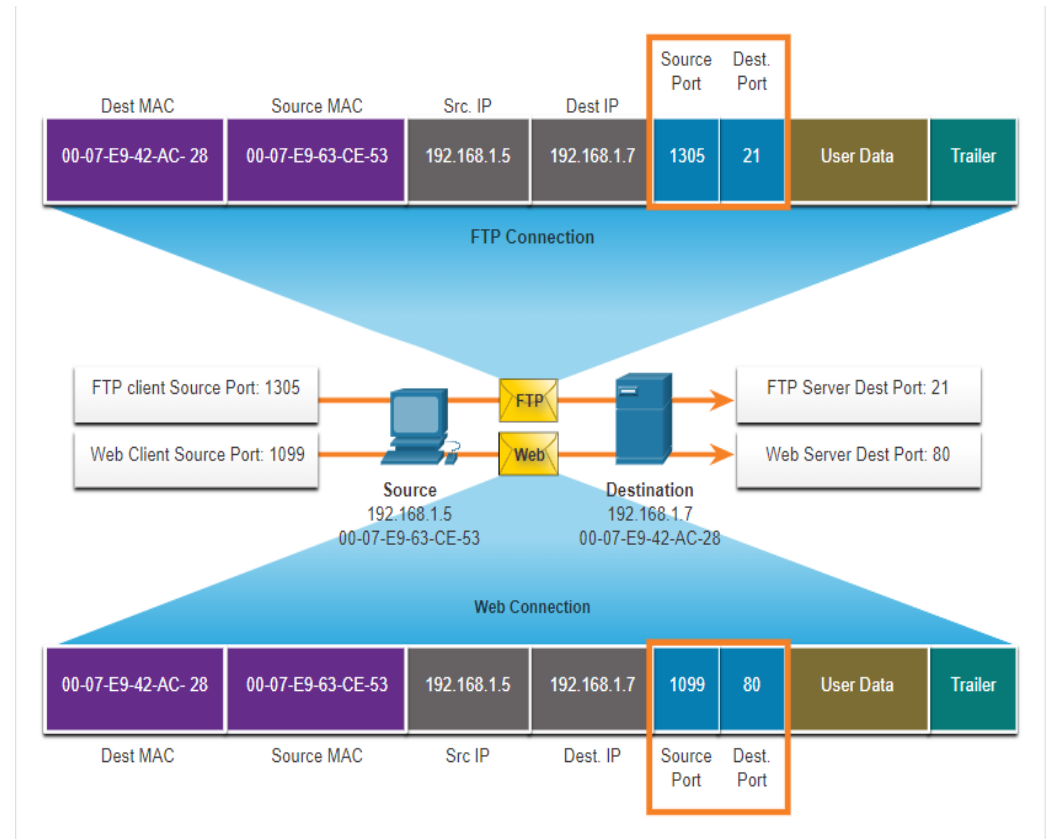
Los protocolos de capa de transporte TCP y UDP utilizan números de puerto para administrar múltiples conversaciones simultáneas.

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.



Números de puerto Pares de sockets

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



Números de puerto

Grupos de números de puerto

Grupo de puertos	Rango de números	Descripción
Puertos bien conocidos	0 to 1,023	<ul style="list-style-type: none">• Por lo general, se utilizan para aplicaciones como navegadores web, clientes de correo electrónico y clientes de acceso remoto.• Los puertos conocidos definidos para aplicaciones de servidor comunes permiten a los clientes identificar fácilmente el servicio asociado requerido.
Puertos registrados	1,024 to 49,151	<ul style="list-style-type: none">• Estos números de puerto son asignados a una entidad que los solicite para utilizar con procesos o aplicaciones específicos.• Principalmente, estos procesos son aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibiría un número de puerto conocido.• Por ejemplo, Cisco ha registrado el puerto 1812 para su proceso de autenticación del servidor RADIUS.
Puertos privados y/o Dinámicos.	49,152 to 65,535	<ul style="list-style-type: none">• Estos puertos también se conocen como <i>puertos efímeros</i>.• El sistema operativo del cliente suele asignar números de puerto dinámicamente cuando se inicia una conexión a un servicio.• Después, el puerto dinámico se utiliza para identificar la aplicación cliente durante la comunicación.

Números de puerto

Grupos de números de puerto (Cont.)

Números de puerto conocidos

Número de puerto	de Internet	Aplicación
20	TCP	Protocolo de transferencia de archivos (FTP) - Datos
21	TCP	Protocolo de transferencia de archivos (FTP) - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Protocolo simple de transferencia de correo (SMTP)
53	UDP, TCP	Servicio de nombres de dominio (DNS, Domain Name Service)
67	UDP	Protocolo de configuración dinámica de host (DHCP): servidor
68	UDP	Protocolo de configuración dinámica de host: cliente
69	UDP	Protocolo trivial de transferencia de archivos (TFTP)
80	TCP	Protocolo de transferencia de hipertexto (HTTP)
110	TCP	Protocolo de oficina de correos, versión 3 (POP3)
143	TCP	Protocolo de acceso a mensajes de Internet (IMAP)
161	UDP	Protocolo simple de administración de redes (SNMP)
443	TCP	Protocolo seguro de transferencia de hipertexto (HTTPS)

Números de puerto

El comando netstat

Las conexiones TCP no descritas pueden representar una importante amenaza a la seguridad. Netstat es una herramienta importante para verificar las conexiones.

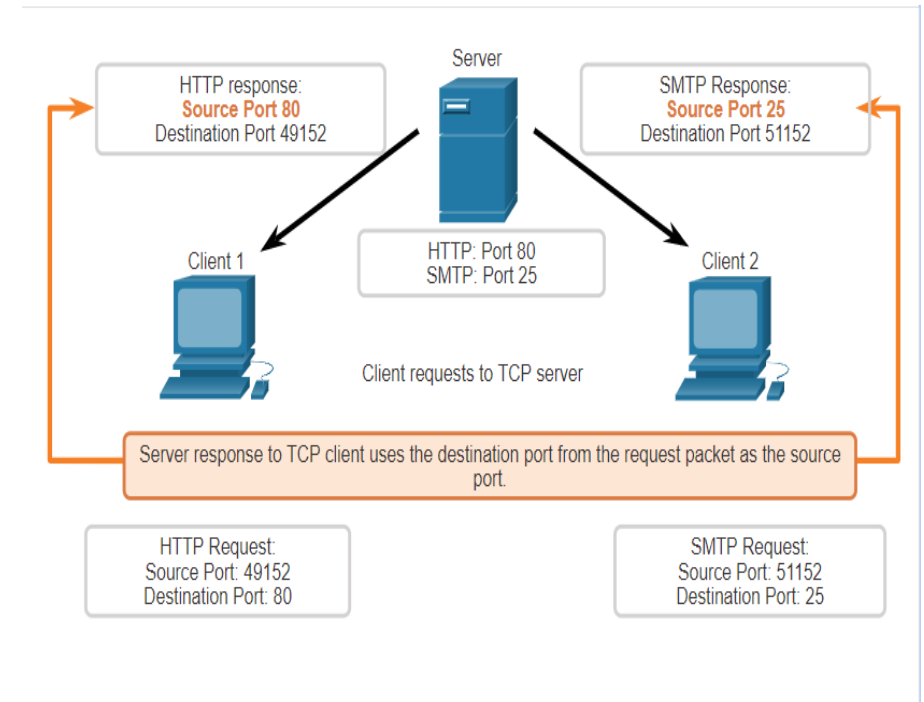
```
C:\> netstat
Active Connections
Proto Local Address Foreign Address State
TCP 192.168.1. 124:3126 192.168.0.2:netbios-ssn ESTABLECIDA
TCP 192.168.1. 124:3158 207.138.126.152:http ESTABLECIDA
TCP 192.168.1. 124:3159 207.138.126.169:http ESTABLECIDO
TCP 192.168.1. 124:3160 207.138.126.169:http ESTABLECIDA
TCP 192.168.1. 124:3161 sc.msn.com:http ESTABLECIDA
TCP 192.168.1. 124:3166 www.cisco.com:http ESTABLECIDA
```

Proceso de comunicación en TCP

Proceso del servidor TCP

Cada proceso de aplicación que se ejecuta en el servidor para utilizar un número de puerto.

- Un servidor individual no puede tener dos servicios asignados al mismo número de puerto dentro de los mismos servicios de la 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.
- Toda solicitud entrante de un cliente direccionada al socket correcto es aceptada y los datos se envían a la aplicación del servidor.



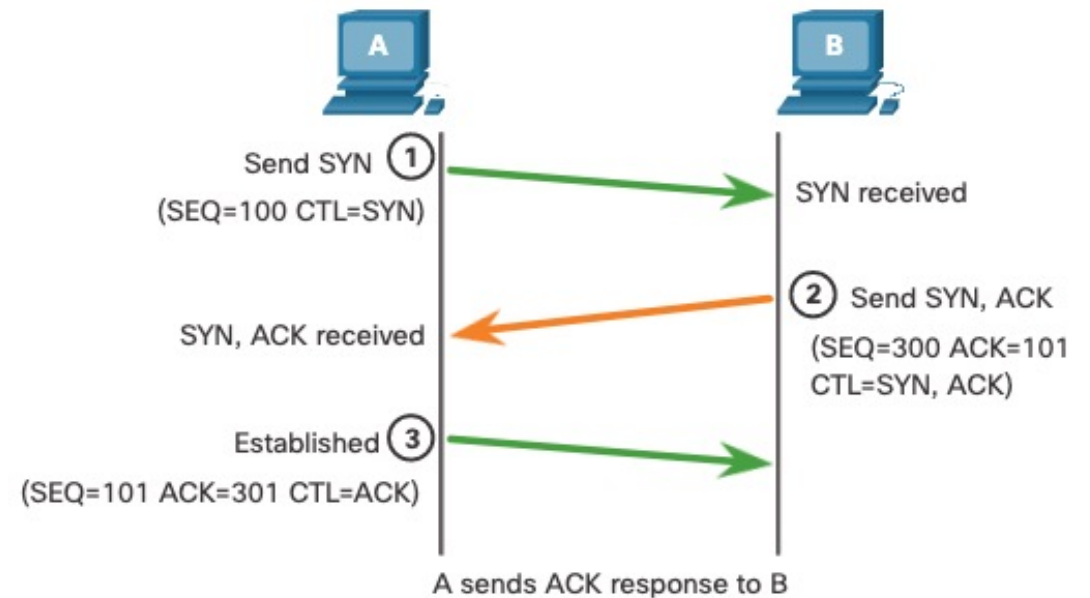
Proceso de comunicación en TCP

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 de origen reconoce la sesión de comunicación de servidor a cliente.



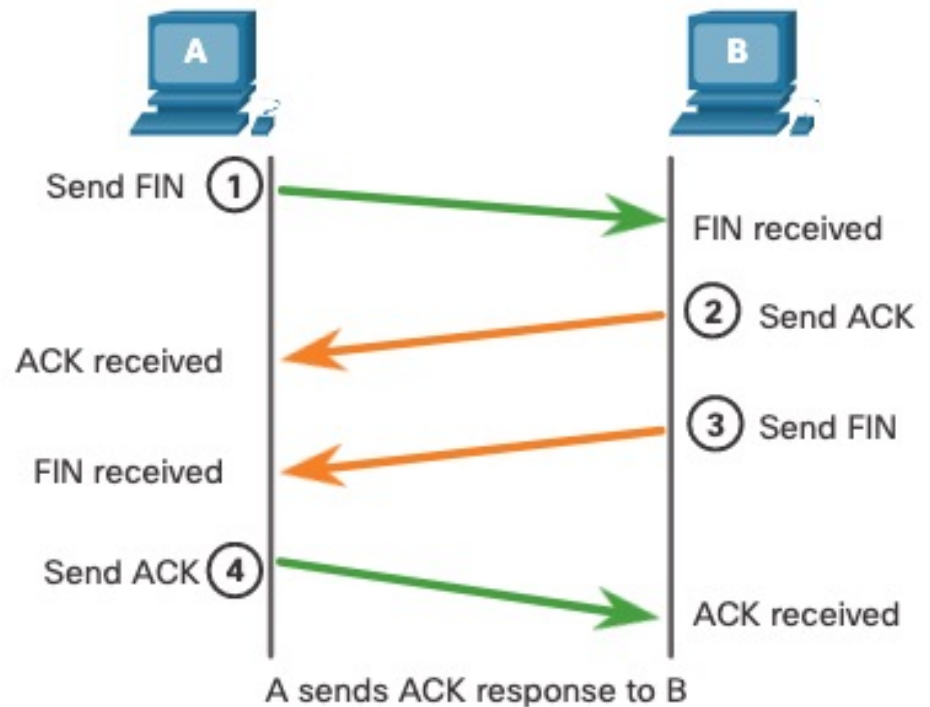
Proceso de comunicación en TCP
Finalización de la sesión TCP

Paso 1: Cuando el cliente no tiene más datos para enviar en la transmisión, envía un segmento con el indicador FIN establecido.

Paso 2: El servidor envía un ACK para confirmar el indicador FIN y finalizar 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 confirmar el FIN desde el servidor.



Proceso de comunicación en TCP

Análisis del protocolo TCP de enlace de tres vías

Funciones del enlace de tres vías:

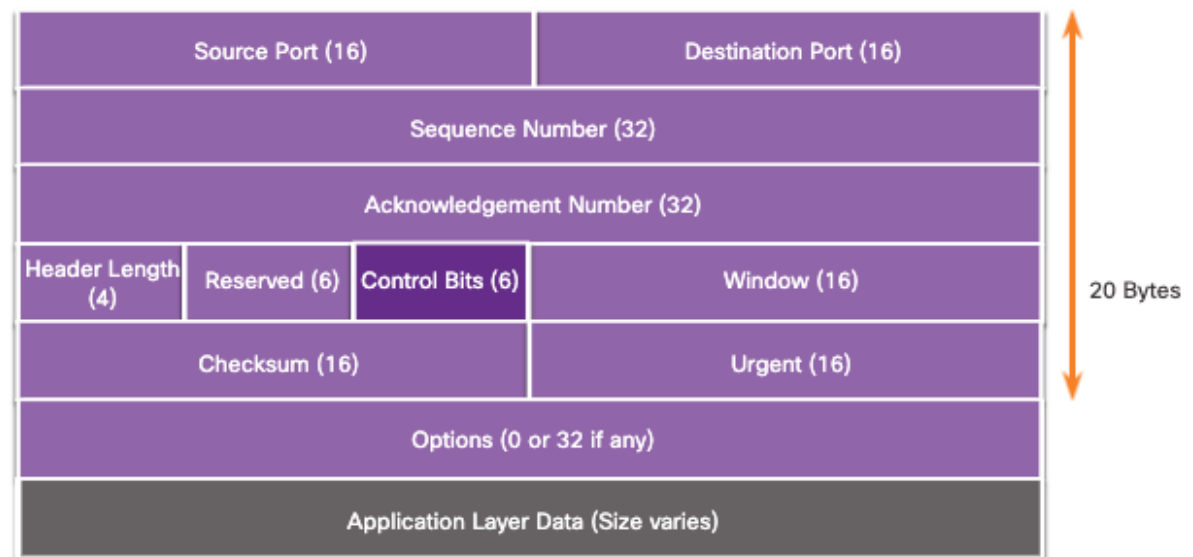
- Establece que el dispositivo de destino está presente en la red.
- Verifica que el dispositivo de destino tenga un servicio activo y acepte solicitudes en el número de puerto de destino que el cliente de origen desea utilizar.
- Informa al dispositivo de destino que el cliente de origen intenta establecer una sesión de comunicación en dicho número de puerto

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

Análisis de protocolo de enlace TCP de tres vías

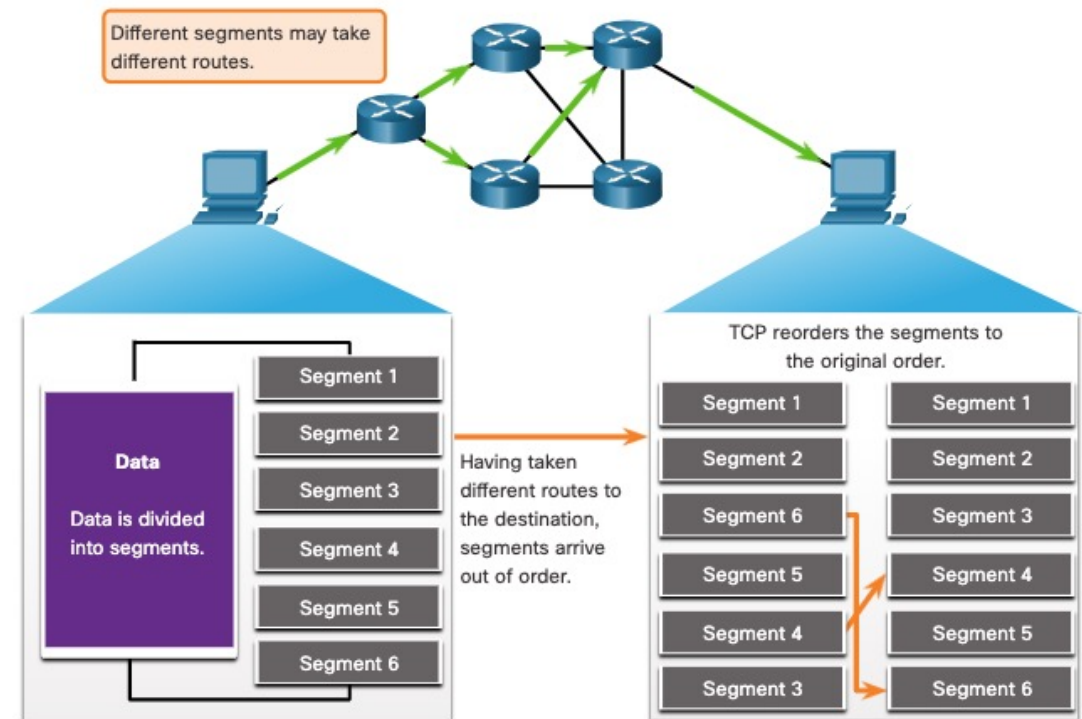
Los seis indicadores de bits de control son los siguientes:

- **URG** - Campo indicador urgente importante.
- **ACK** - Indicador de acuse de recibo utilizado en el establecimiento de la conexión y la terminación de la sesión.
- **PSH** - Función de empuje.
- **RST** - Restablecer una conexión cuando ocurre un error o se agota el tiempo de espera.
- **SYN** - Sincronizar números de secuencia utilizados en el establecimiento de conexión.
- **FIN** - No más datos del remitente y se utilizan en la terminación de la sesión.



Confiabilidad de TCP: Entrega garantizada y ordenada

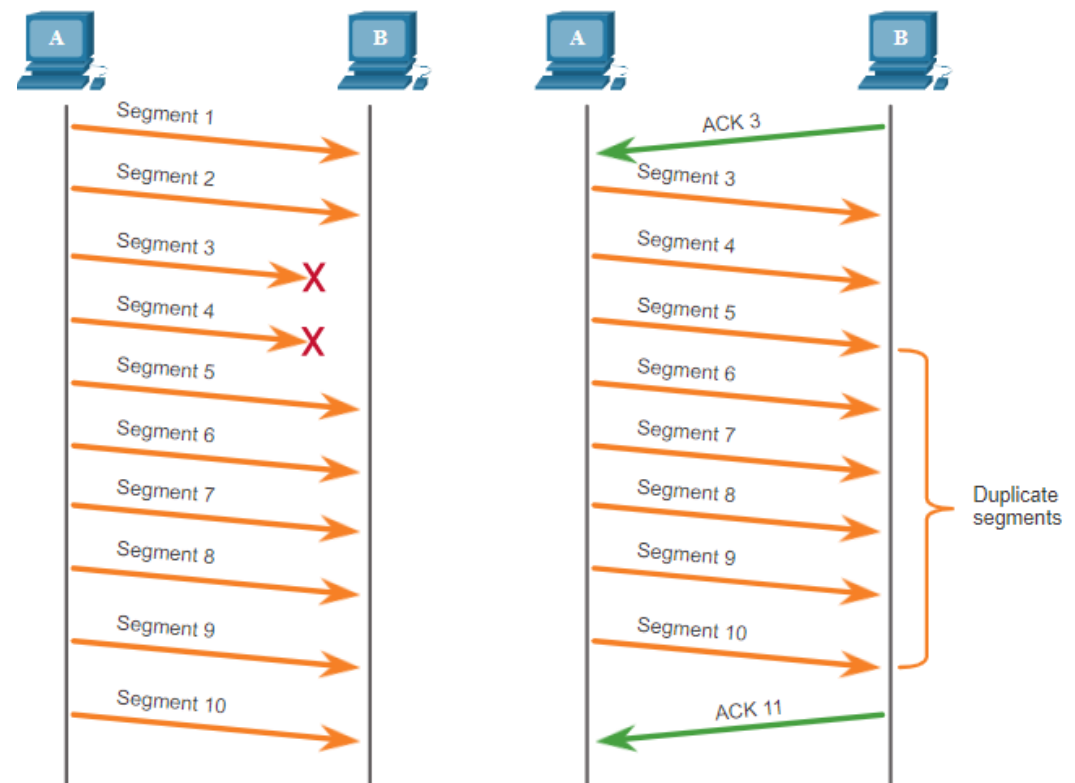
- TCP también puede ayudar a mantener el flujo de paquetes para que los dispositivos no se sobrecarguen.
- Algunas veces los segmentos TCP no llegan a su destino o lno llegan en orden.
- Todos los datos deben ser recibidos y los datos de estos segmentos deben ser reensamblados en el orden original.
- Para lograr esto, se asignan números de secuencia en el encabezado de cada paquete.



Confiabilidad TCP — Pérdida y retransmisión de datos

No importa cuán bien diseñada esté una red, ocasionalmente se produce la pérdida de datos.

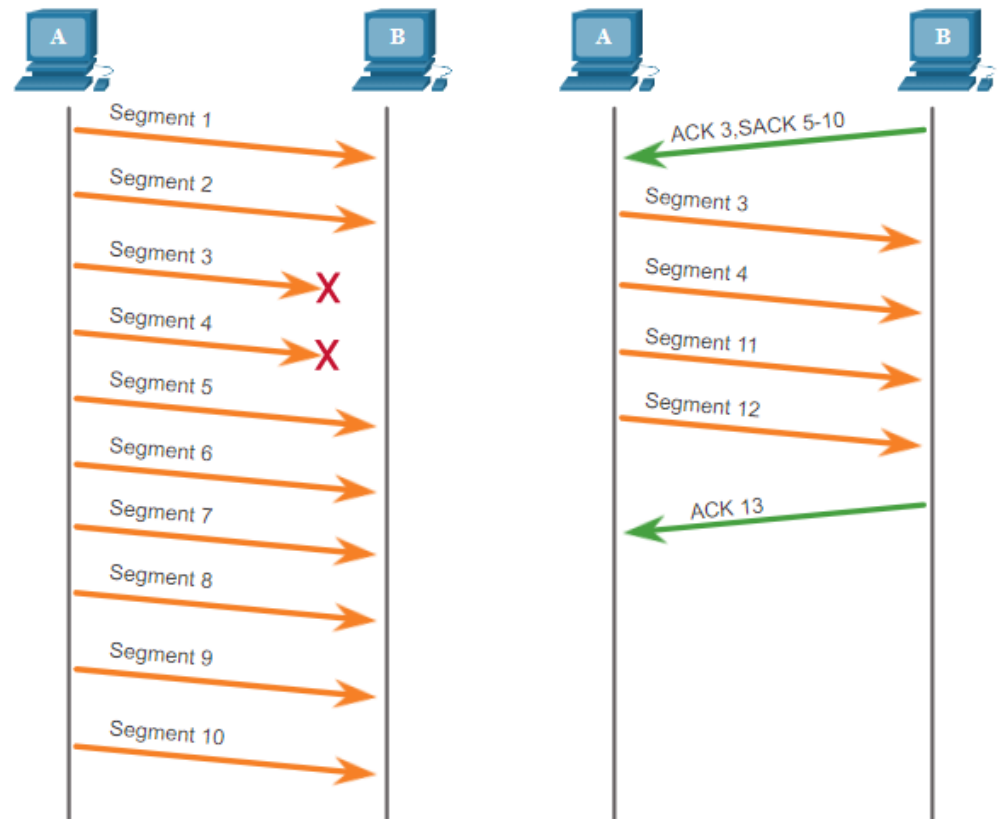
TCP proporciona métodos para administrar la pérdida de segmentos. Entre estos está un mecanismo para retransmitir segmentos para los datos sin reconocimiento.



Confiabilidad TCP — Pérdida y retransmisión de datos (Cont.)

Los sistemas operativos host actualmente suelen emplear una característica TCP opcional llamada reconocimiento selectivo (SACK), negociada durante el protocolo de enlace de tres vías.

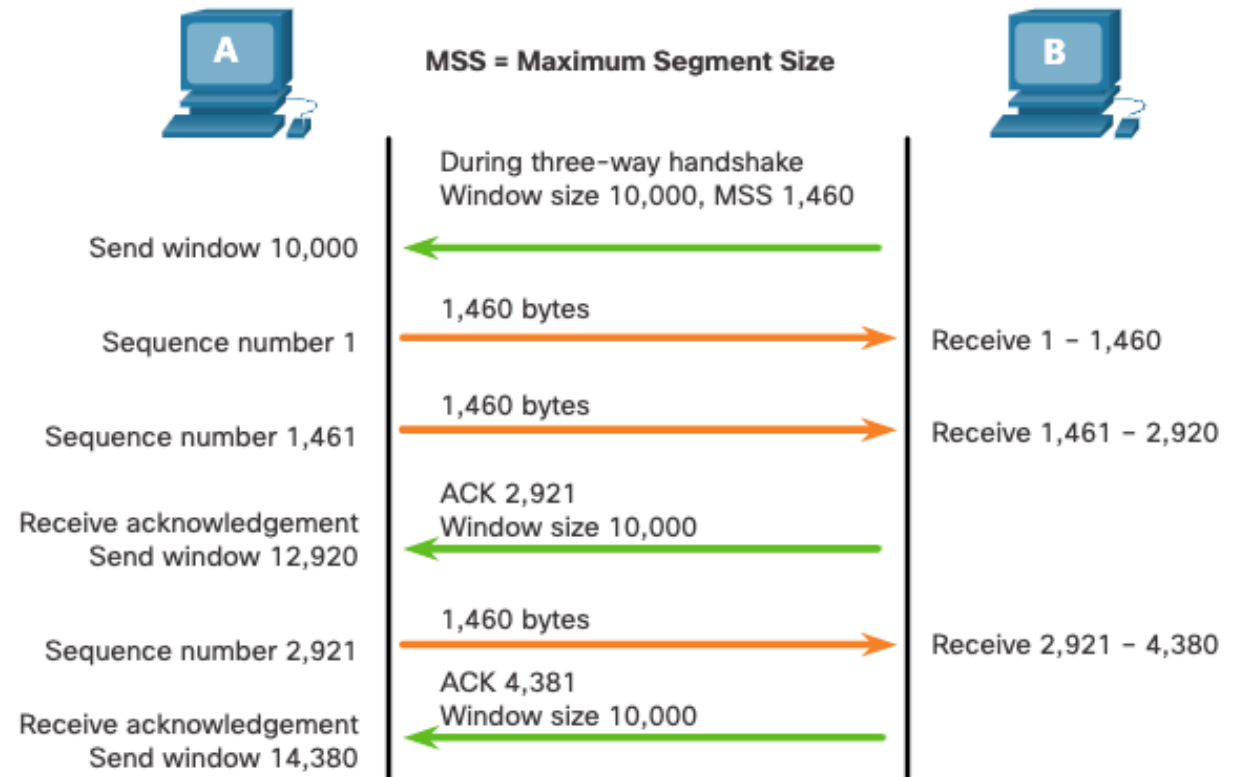
Si ambos hosts admiten SACK, el receptor puede reconocer explícitamente qué segmentos (bytes) se recibieron, incluidos los segmentos discontinuos.



Control del flujo de TCP: tamaño de la ventana y reconocimientos

El TCP también proporciona mecanismos de control de flujo.

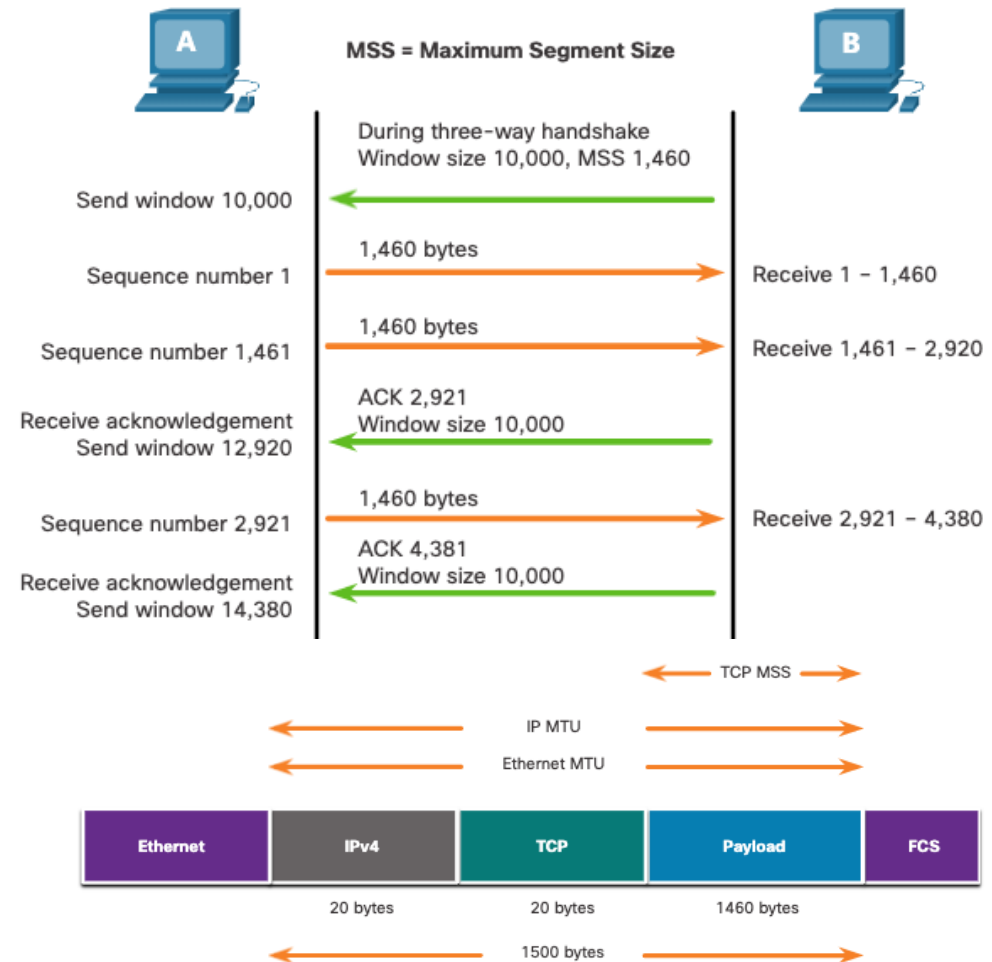
- El control de flujo es la cantidad de datos que el destino puede recibir y procesar de manera confiable.
- El control de flujo permite mantener la confiabilidad de la transmisión de TCP mediante el ajuste de la velocidad del flujo de datos entre el origen y el destino para una sesión dada.



TCP Control de flujo: tamaño máximo de segmento

Tamaño máximo de segmento (MSS) es la cantidad máxima de datos que puede recibir el dispositivo de destino.

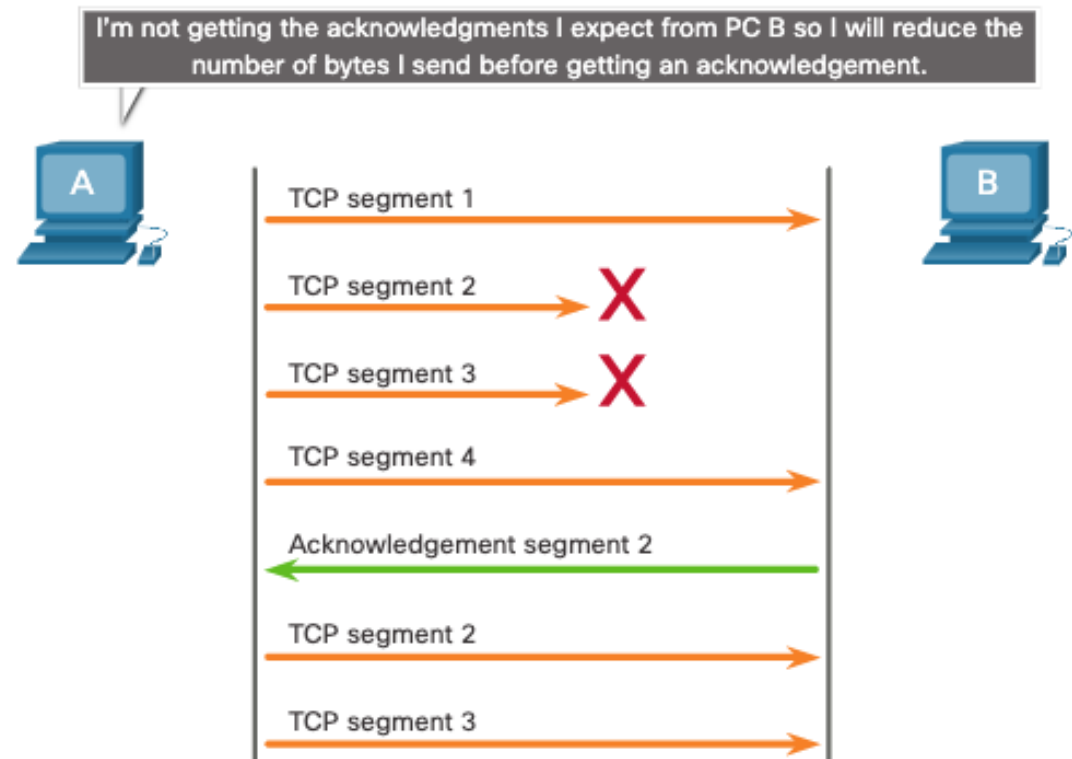
- Un MSS común es de 1.460 bytes cuando se usa IPv4.
- Un host determina el valor de su campo de MSS restando los encabezados IP y TCP de unidad máxima de transmisión (MTU) de Ethernet.
- 1500 menos 60 (20 bytes para el encabezado IPv4 y 20 bytes para el encabezado TCP) deja 1460 bytes.



Control del flujo de TCP: Prevención de congestiones

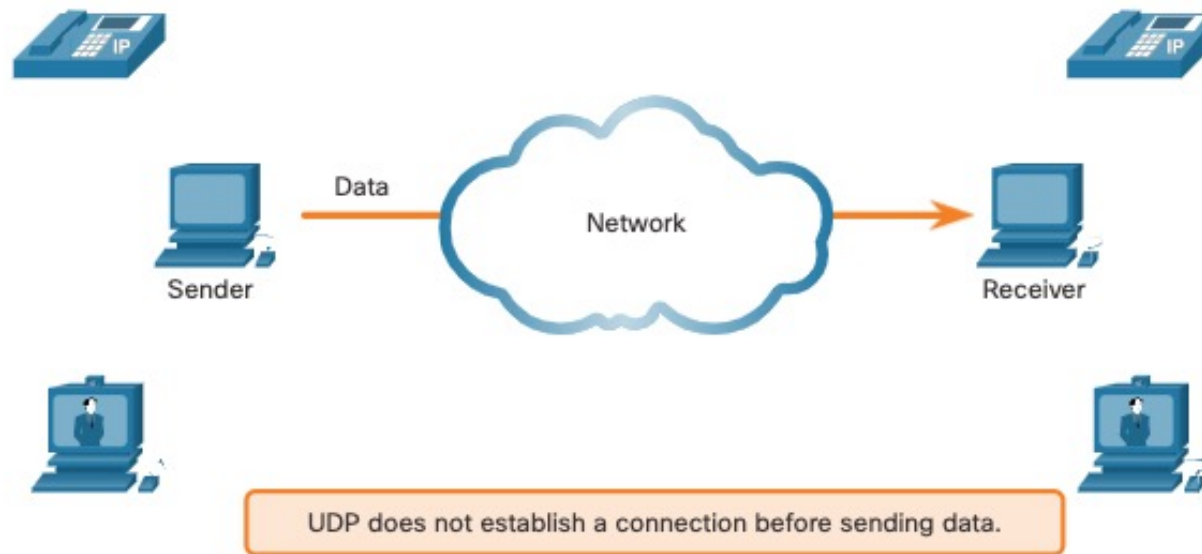
Cuando se produce congestión en una red, el router sobrecargado comienza a descartar paquetes.

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



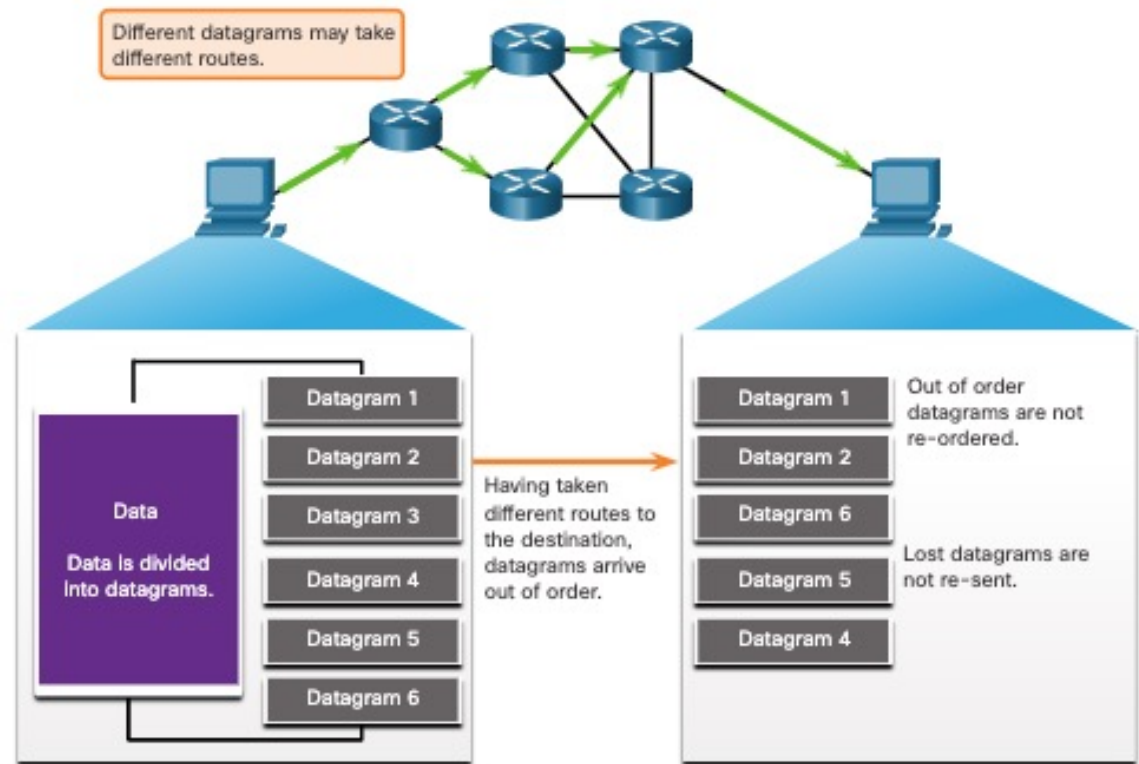
Comparación de baja sobrecarga y confiabilidad de UDP

UDP no establece ninguna conexión. UDP suministra transporte de datos con baja sobrecarga debido a que posee un encabezado de datagrama pequeño sin tráfico de administración de red.



Proceso de comunicación en UDP
Rearmado de datagramas UDP

- UDP no realiza un seguimiento de los números de secuencia de la manera en que lo hace TCP.
- UDP no puede reordenar los datagramas en el orden de la transmisión.
- UDP simplemente reensambla los datos en el orden en que se recibieron y los envía a la aplicación.

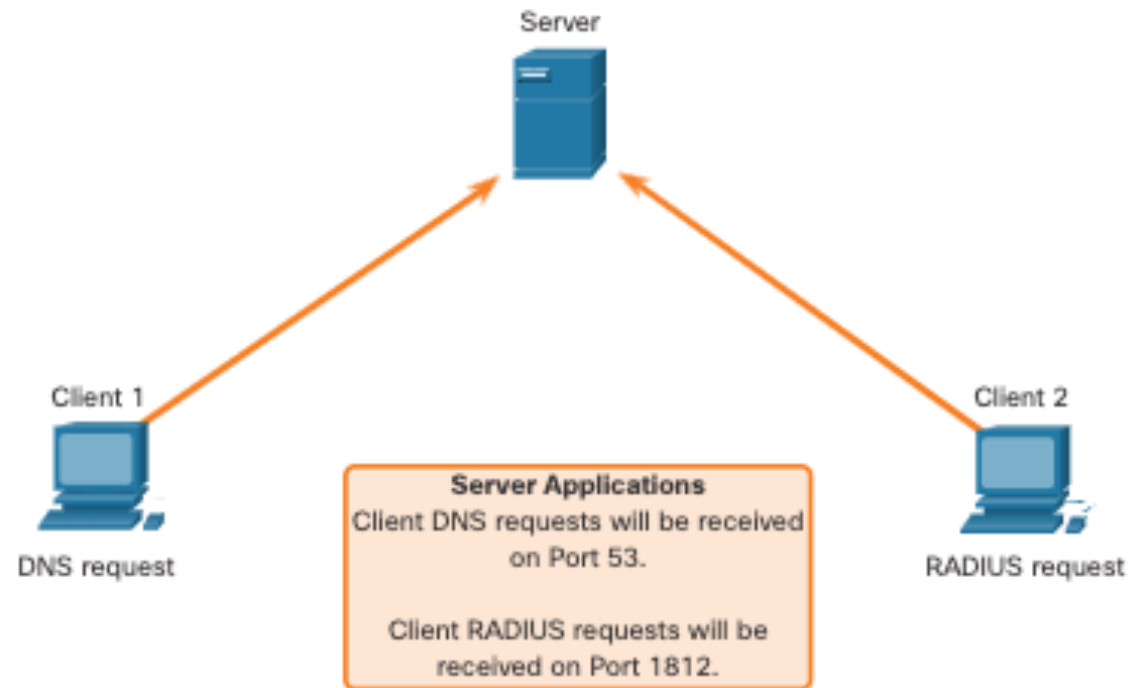


Proceso de comunicación en UDP

Procesos y solicitudes de servidores UDP

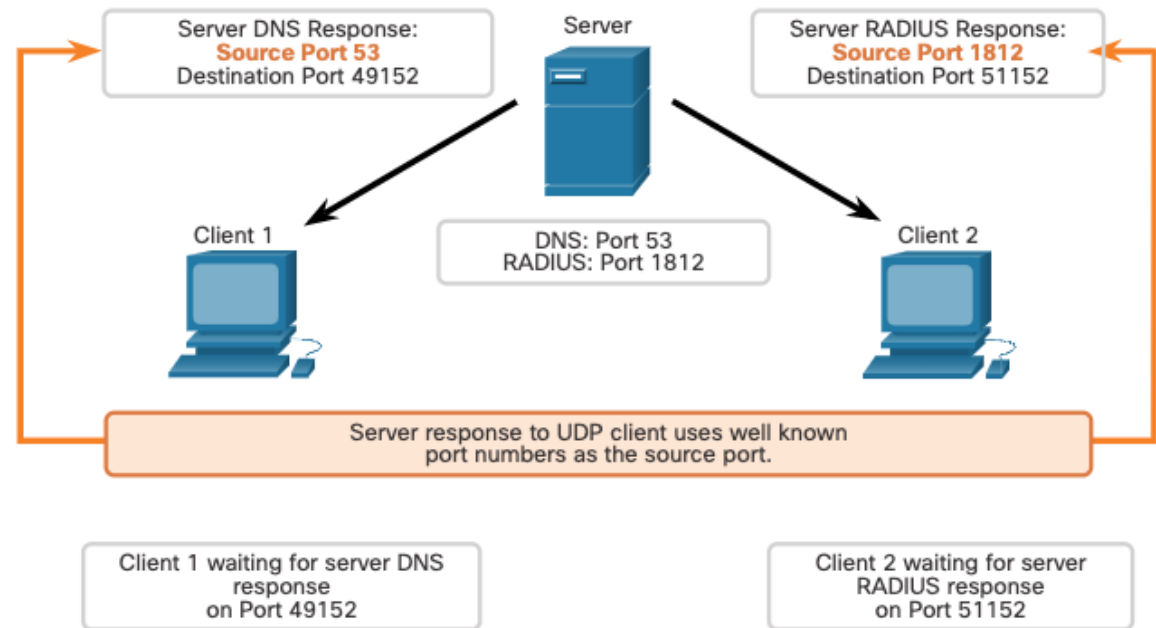
A las aplicaciones de servidor basadas en UDP se les asignan números de puerto conocidos o registrados.

UDP recibe un datagrama destinado a uno de esos puertos, envía los datos de aplicación a la aplicación adecuada en base a su número de puerto.



Proceso de comunicación en UDP Procesos de cliente UDP

- El proceso de cliente UDP selecciona dinámicamente un número de puerto del intervalo de números de puerto y lo utiliza como puerto de origen para la conversación.
- Por lo general, el puerto de destino es el número de puerto bien conocido o registrado que se asigna al proceso de servidor.
- Una vez que el cliente selecciona los puertos de origen y de destino, este mismo par de puertos se utiliza en el encabezado de todos los datagramas que se utilizan en la transacción.

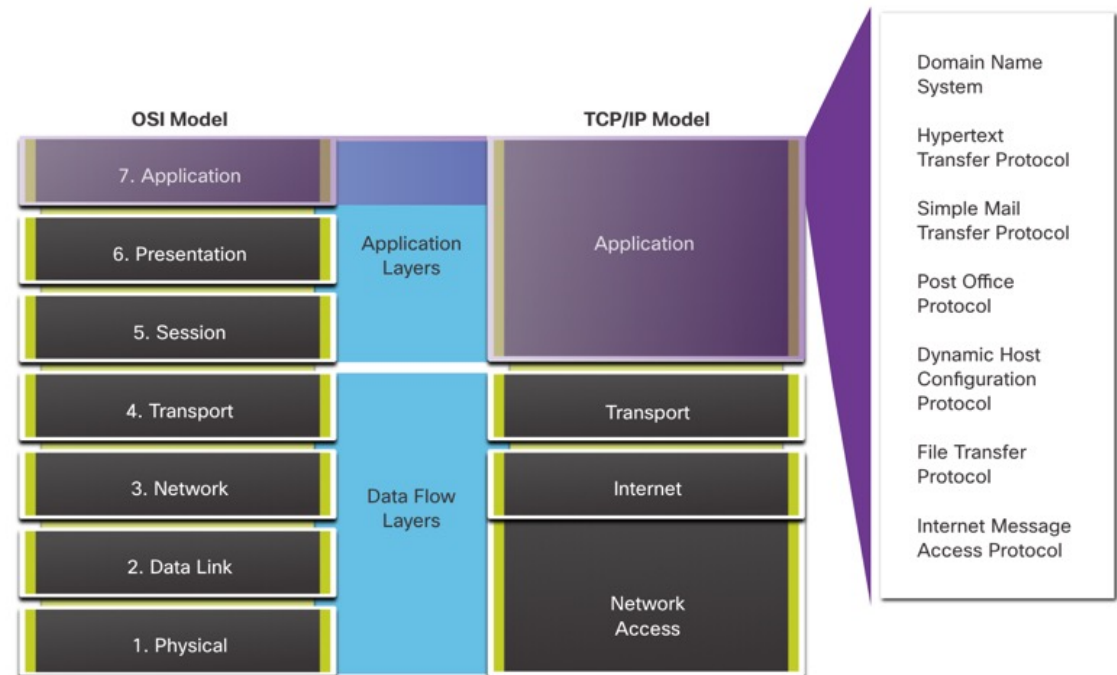


Capa de aplicación

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.



Aplicación, presentación y sesión

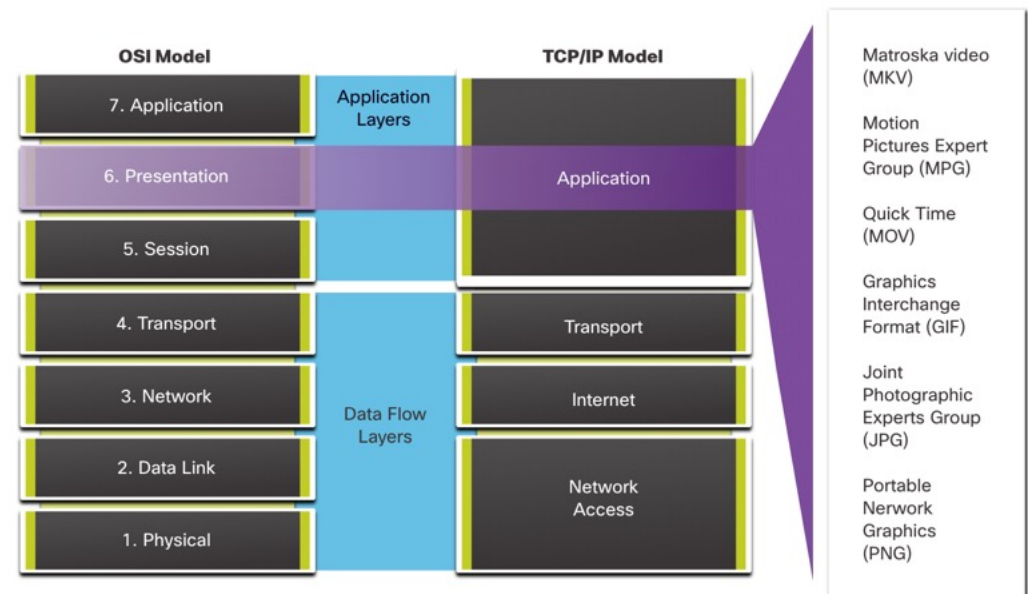
Capa de presentación y sesión

La capa de presentación tiene tres funciones principales:

- Dar formato a los datos del dispositivo de origen, o presentarlos, en una forma compatible para que lo reciba el dispositivo de destino.
- Comprimir los datos de forma tal que los pueda descomprimir el dispositivo de destino.
- Cifrar los datos para transmitirlos y descifrarlos al recibirlos.

Función de la capa de sesión:

- Crear y mantener diálogos entre las aplicaciones de origen y de destino.
- La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o que estuvieron inactivas durante un período prolongado.



Aplicación, presentación y sesión

Protocolos de capa de aplicación de TCP/IP

- Los protocolos de aplicación TCP/IP especifican el formato y la información de control necesarios para muchas funciones de comunicación comunes de Internet.
- Los protocolos de capa de aplicación son utilizados tanto por los dispositivos de origen como de destino durante una sesión de comunicación.
- Para que las comunicaciones se lleven a cabo correctamente, los protocolos de capa de aplicación que se implementaron en los hosts de origen y de destino deben ser compatibles.

Sistema de nombres

DNS - Sistema de nombres de dominio (o servicio)

- TCP, UDP cliente 53
- Traduce los nombres de dominio tales como cisco.com a direcciones IP

Configuración de host

DHCP (Protocolo de configuración dinámica de host)

- Cliente UDP 68, servidor 67
- Permite que las direcciones vuelvan a utilizarse cuando ya no son necesarias

Web

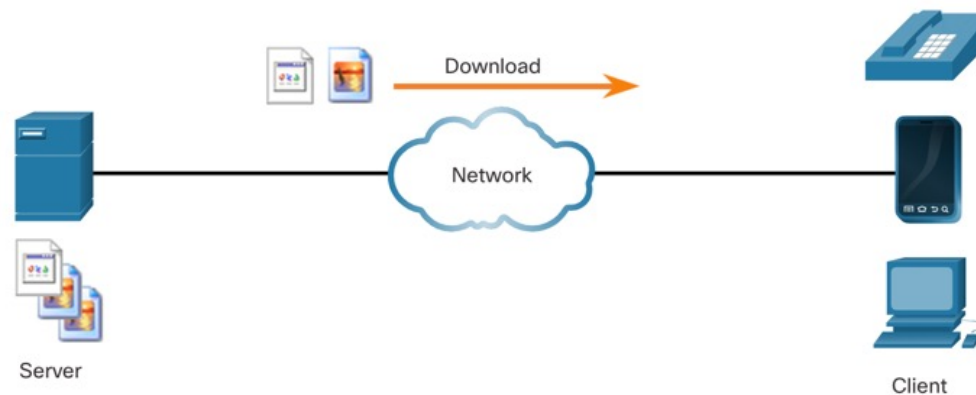
HTTP- Protocolo de transferencia de hipertexto

- TCP 80, 8080
- Un Conjunto de reglas para intercambiar texto, imágenes gráficas, sonido, video y otros archivos multimedia en la World Wide Web.

De Punto a Punto

Modelo cliente-servidor

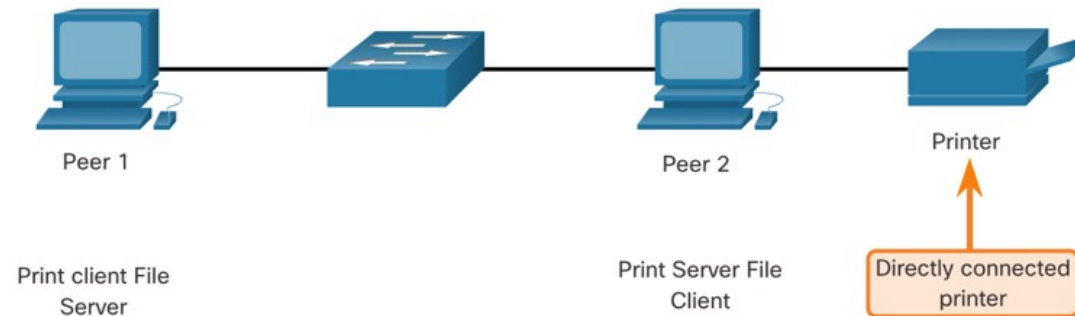
- Los procesos de cliente y servidor se consideran parte de la capa de aplicación.
- En el modelo cliente-servidor, el dispositivo que solicita información se denomina “cliente”, y el dispositivo que responde a la solicitud se denomina “servidor”.
- Los protocolos de la capa de aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores.



De Punto a Punto

Redes Punto a Punto

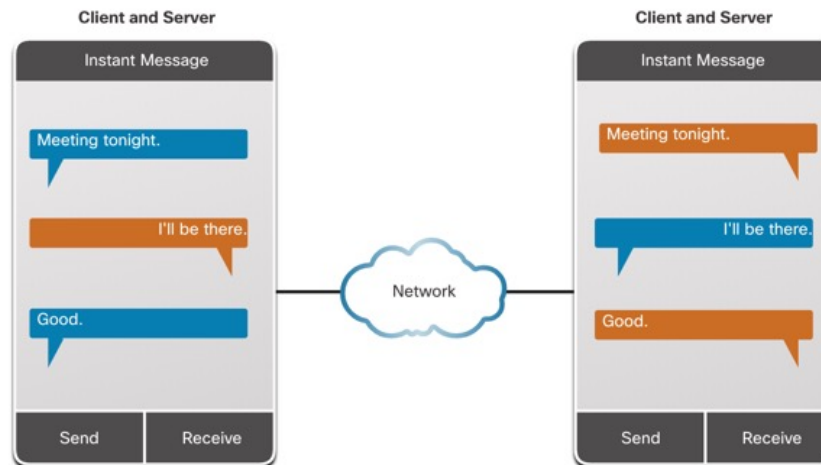
- En una red P2P, hay dos o más PC que están conectadas por medio de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor dedicado.
- Todo terminal conectado puede funcionar como servidor y como cliente.
- Un equipo puede asumir la función de servidor para una transacción mientras funciona en forma simultánea como cliente para otra transacción. Las funciones de cliente y servidor se establecen por solicitud.



De Punto a Punto

Aplicaciones punto a punto

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

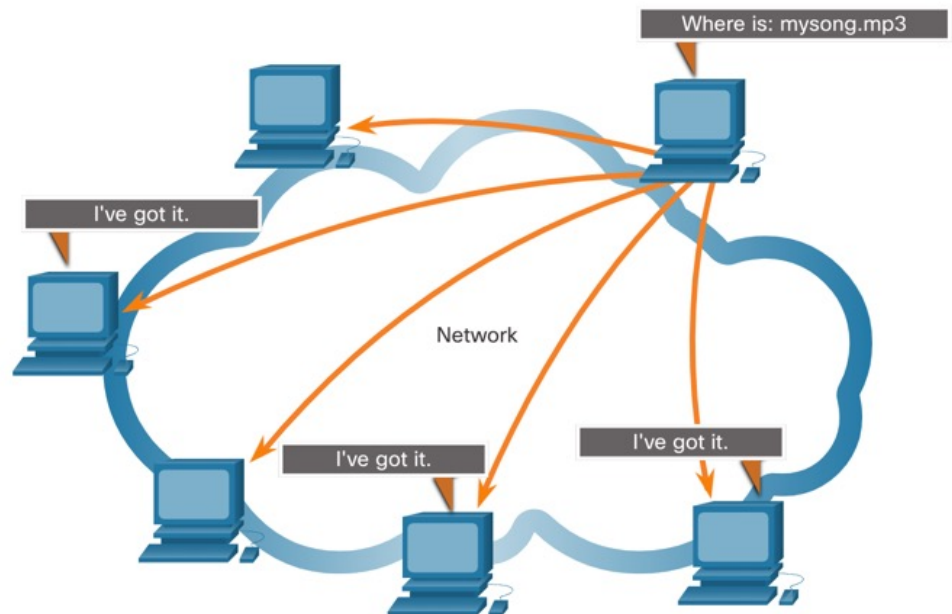


Aplicaciones P2P comunes punto a punto

Con las aplicaciones P2P, cada PC de la red que ejecuta la aplicación puede funcionar como cliente o como servidor para las otras PC en la red que ejecutan la aplicación.

Las redes P2P comunes incluyen las siguientes:

- BitTorrent
- Conexión directa
- eDonkey
- Freenet



Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto

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

Para comprender mejor cómo interactúa el navegador web con el servidor web, podemos analizar cómo se abre una página web en un navegador.

Paso 1

El explorador interpreta las tres partes del URL:

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

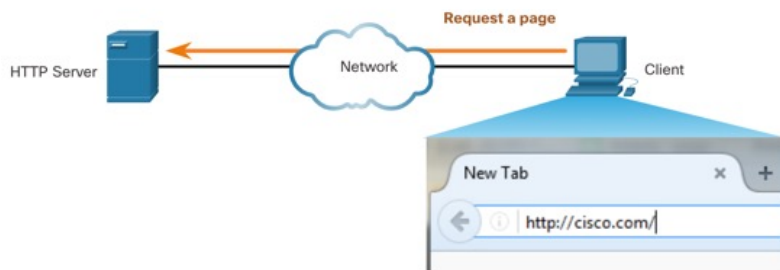


Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto

Paso 2

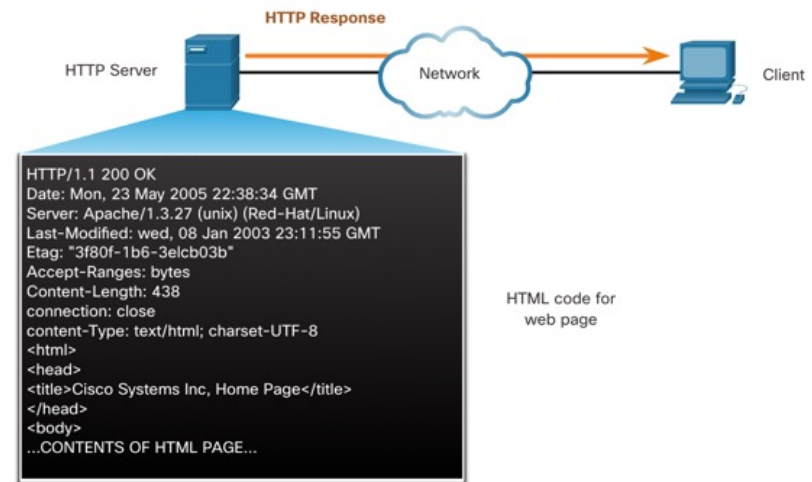
El navegador luego verifica con un Servidor de nombres de dominio (DNS) para convertir a www.cisco.com en una dirección numérica que utiliza para conectarse con el servidor.

El cliente inicia una solicitud HTTP a un servidor 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.

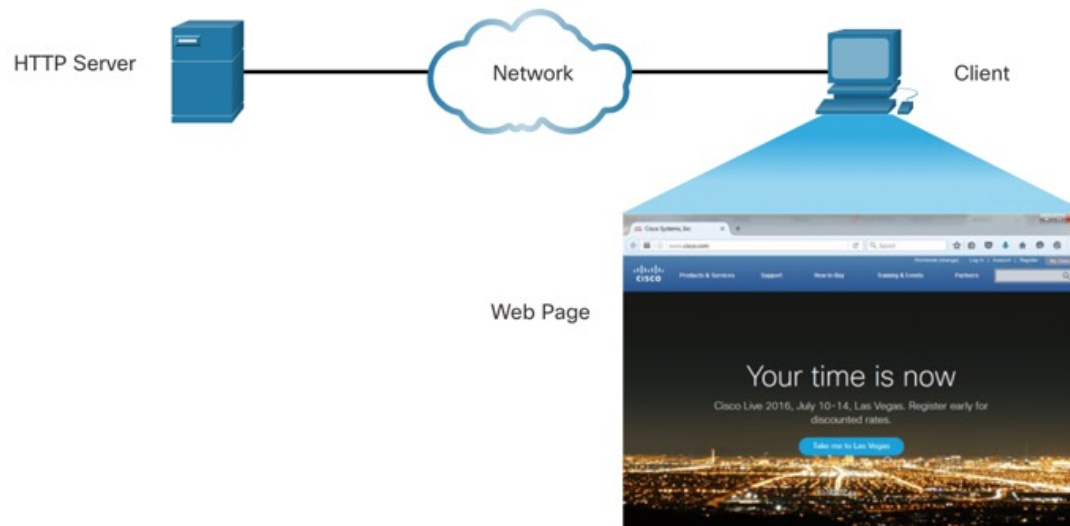


Protocolos web y de correo electrónico

Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto

Paso 4

El navegador descifra el código HTML y da formato a la página para que se pueda visualizar en la ventana del navegador.

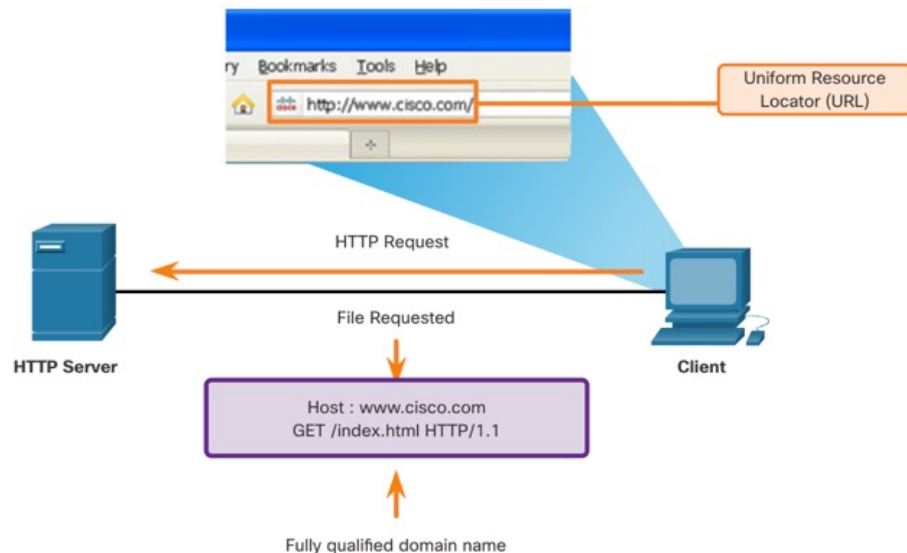


HTTP y HTTPS

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** - solicitud de datos por parte del cliente. Un cliente (navegador web) envía el mensaje GET al servidor web para solicitar las páginas HTML.
- **POST** carga archivos de datos, como los datos de formulario, al servidor web.
- **PUT** carga los recursos o el contenido, como por ejemplo una imagen, en el servidor web.



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

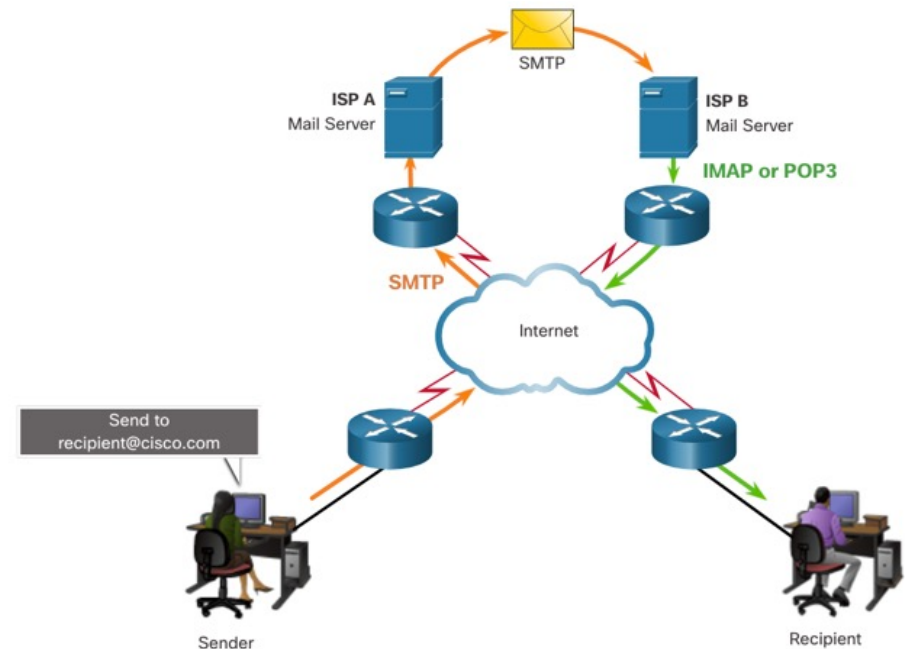
Protocolos web y de correo electrónico

Protocolos de correo electrónico

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

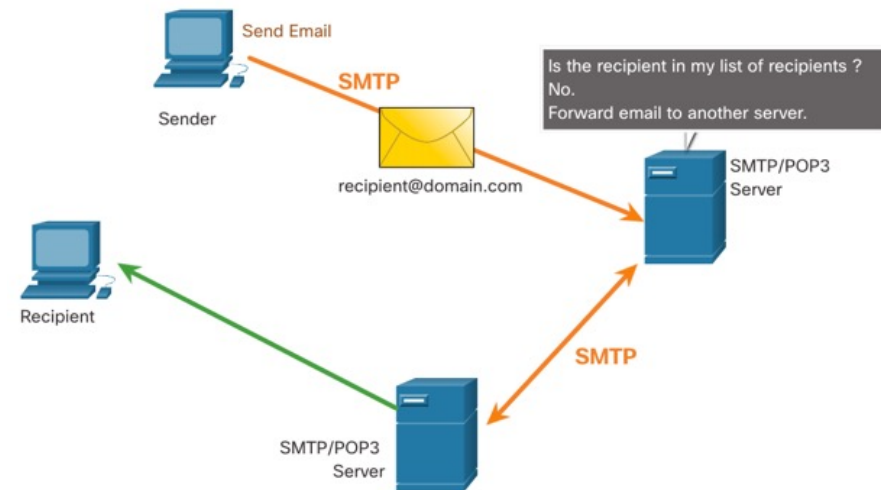
Los protocolos de correo electrónico utilizados para la operación son:

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



SMTP, POP e IMAP

- Cuando un cliente envía correo electrónico, el proceso SMTP del cliente se conecta a un proceso SMTP del servidor en el puerto bien conocido 25.
- Después de que se establece la conexión, el cliente intenta enviar el correo electrónico al servidor a través de esta.
- Una vez que el servidor recibe el mensaje, lo ubica en una cuenta local (si el destinatario es local) o lo reenvía a otro servidor de correo para su entrega.
- El servidor de correo electrónico de destino puede no estar en línea o puede estar ocupado. Si es así, SMTP pone en cola los mensajes que se enviarán más adelante.



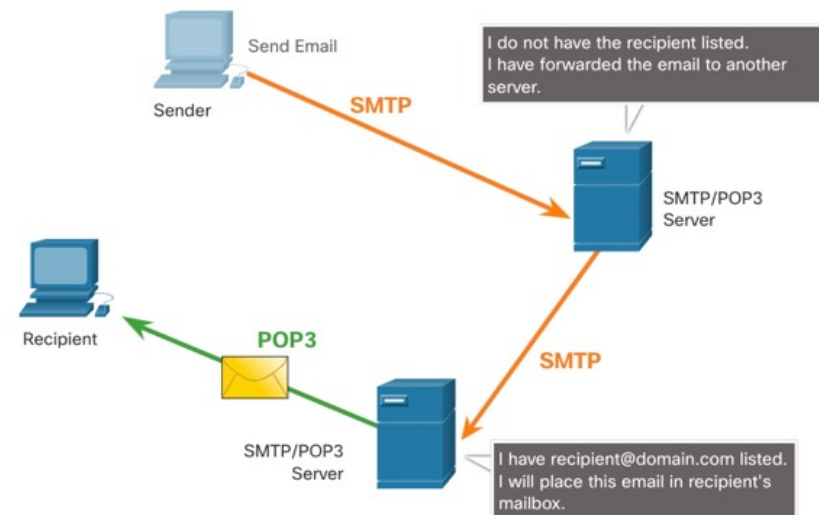
Nota: Los formatos de mensaje SMTP requieren un encabezado del mensaje (dirección de correo electrónico del destinatario y dirección de correo electrónico del remitente) y un cuerpo del mensaje.

Protocolos Web y Correo Electrónico

SMTP, POP e IMAP (Cont.)

POP es utilizado por una aplicación para recuperar correo electrónico de un servidor de correo. Cuando el correo se descarga del servidor al cliente mediante POP, los mensajes se eliminan en el servidor.

- El servidor comienza el servicio POP escuchando de manera pasiva en el puerto TCP 110 las solicitudes de conexión del cliente.
- Cuando un cliente desea utilizar el servicio, envía una solicitud para establecer una conexión TCP con el servidor.
- Una vez establecida la conexión, el servidor POP envía un saludo.
- A continuación, el cliente y el servidor POP intercambian comandos y respuestas hasta que la conexión se cierra o cancela.



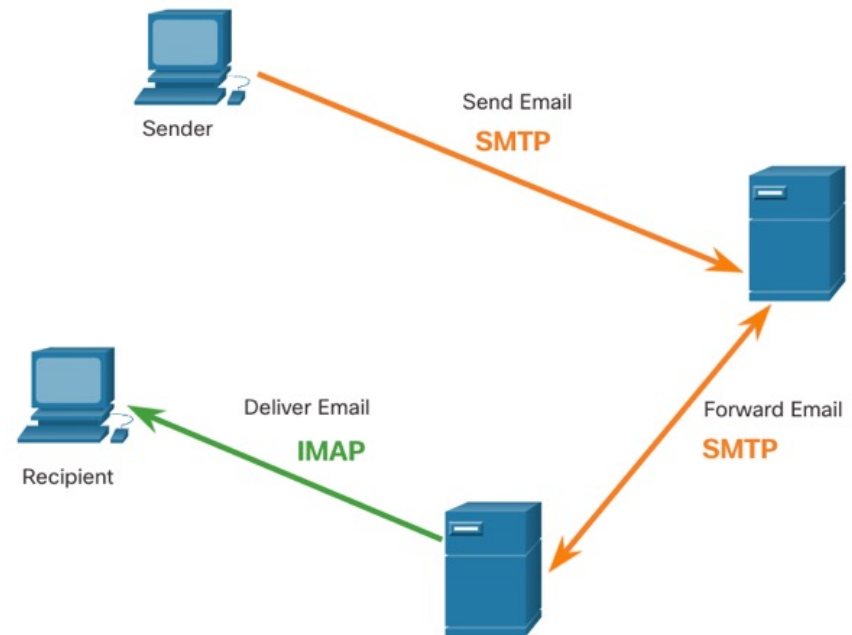
Nota: Dado que POP no almacena mensajes, no se recomienda para las pequeñas empresas que necesitan una solución de respaldo centralizada.

Protocolos web y de correo electrónico

SMTP, POP e IMAP (Cont.)

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

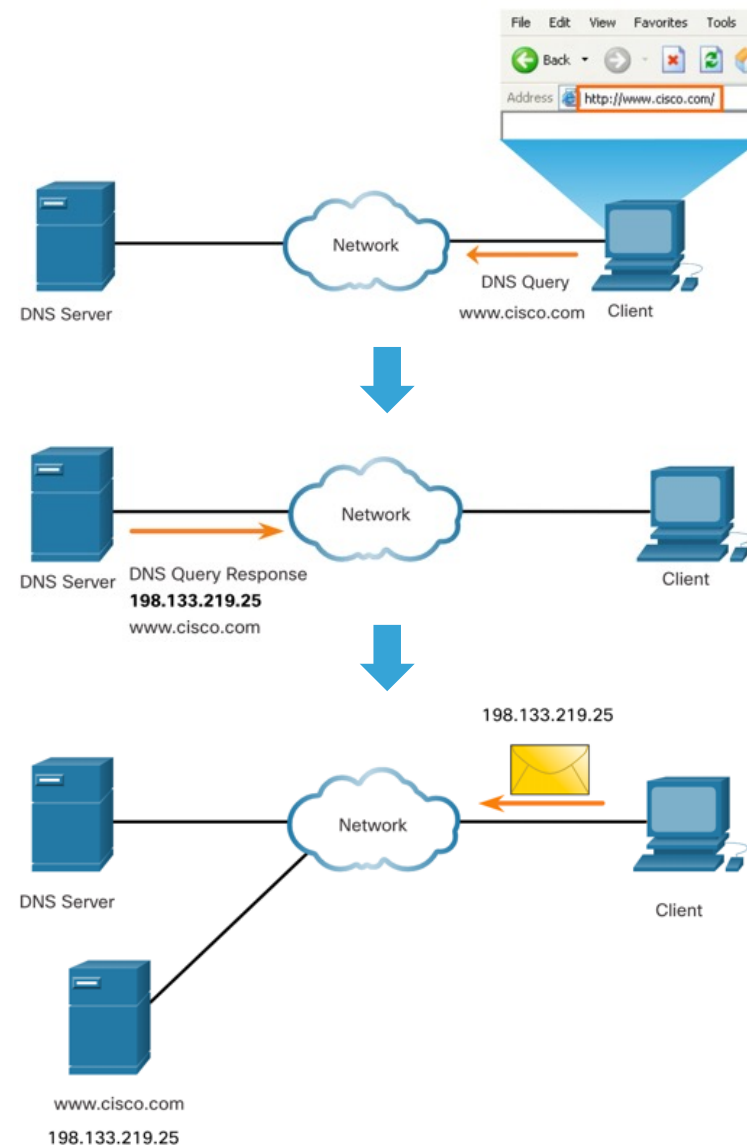
- A diferencia de POP, cuando un usuario se conecta a un servidor IMAP, se descargan copias de los mensajes a la aplicación cliente. Los mensajes originales se mantienen en el servidor hasta que se eliminen manualmente.
- Cuando un usuario decide eliminar un mensaje, el servidor sincroniza esa acción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



Servicios de direccionamiento IP

Servicio de nombres de dominio

- Los nombres de dominio se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible.
- Los nombres de dominio completos (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 coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye el formato de consultas, respuestas y datos.



Servicios de direccionamiento IP

Formato del mensaje DNS

El servidor DNS almacena diferentes tipos de registros de recursos utilizados 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**
- **MX: un registro de intercambio de correo**

Cuando un cliente realiza una consulta, el proceso DNS del servidor observa primero sus propios registros para resolver el nombre. Si no puede resolverlo con los registros almacenados, contacta a otros servidores para hacerlo.

Una vez que se encuentra una coincidencia y se la devuelve al servidor solicitante original, este almacena temporalmente la dirección numerada por si se vuelve a solicitar el mismo nombre.

Servicios de direccionamiento IP

Formato del mensaje DNS

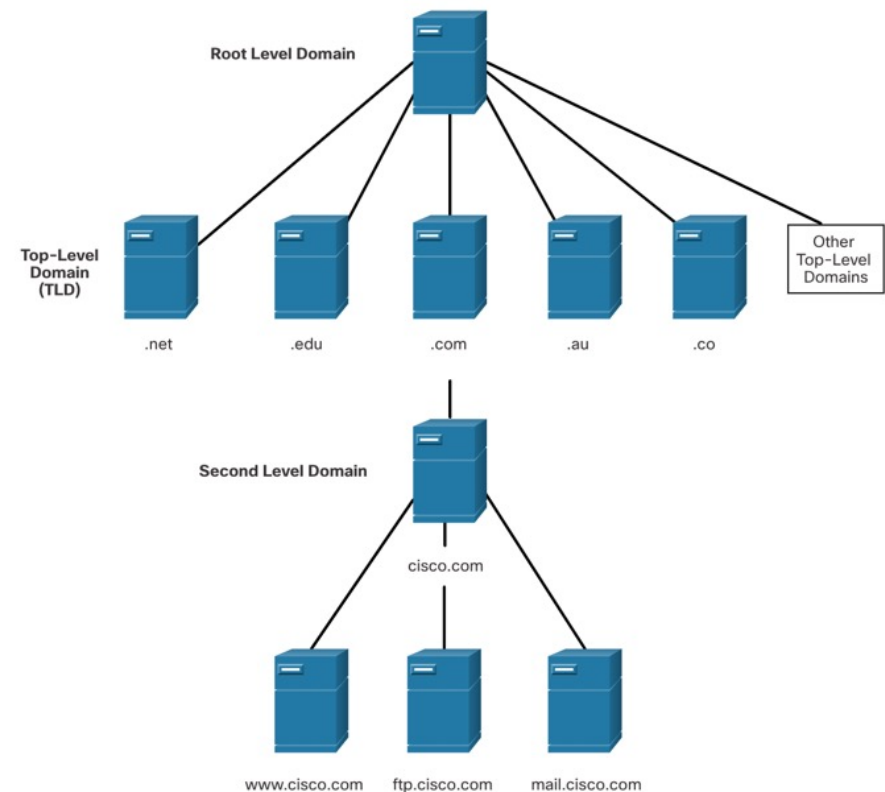
Este formato de mensaje que se ve en la figura se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, para los mensajes de error y para la transferencia de información de registro de recursos entre servidores.

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

Servicios de direccionamiento IP

Jerarquía DNS

- El protocolo DNS utiliza un sistema jerárquico para crear una base de datos que proporcione la resolución de nombres.
- Cada servidor DNS mantiene un archivo de base de datos específico y sólo es responsable de administrar las asignaciones de nombre a IP para esa pequeña porción de toda la estructura DNS.
- Cuando un servidor DNS recibe una solicitud para una traducción de nombre que no se encuentra dentro de esa zona DNS, el servidor DNS reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para su traducción.
- Algunos ejemplos de dominios de nivel superior son los siguientes:
 - **.com:** una empresa o industria
 - **.org** una organización sin fines de lucro
 - **.au** Australia



Servicios de direccionamiento IP

El comando nslookup

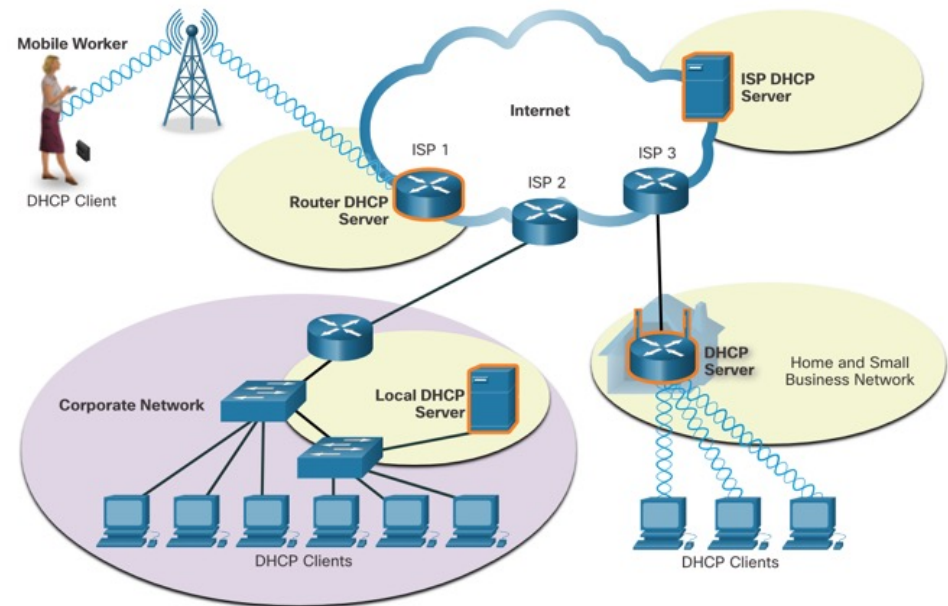
- Nslookup es una utilidad del sistema operativo de la computadora que permite al usuario consultar manualmente los servidores DNS configurados en el dispositivo para resolver un nombre de host dado.
- Esta utilidad también puede utilizarse para solucionar los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.
- En la figura 1, cuando se ejecuta el comando **nslookup**, se muestra el servidor DNS predeterminado configurado para su host.
- El nombre de un host o de un dominio se puede introducir en el símbolo del sistema 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
>
```

Servicios de direccionamiento IP

Protocolo de configuración dinámica de host

- El protocolo DHCP del servicio IPv4 automatiza la asignación de direcciones IPv4, máscaras de subred, gateways y otros parámetros de redes IPv4.
- DHCP se considera direccionamiento dinámico en comparación con direccionamiento estático. El direccionamiento estático está introduciendo manualmente la información de la dirección IP.
- Cuando un host se conecta a la red, se realiza el contacto con el servidor de DHCP y se solicita una dirección. El servidor de DHCP elige una dirección de un rango de direcciones configurado llamado grupo y la asigna (concede) al host.
- Muchas redes utilizan tanto el direccionamiento estático como DHCP. DHCP se utiliza para hosts de propósito general, tales como los dispositivos de usuario final. El direccionamiento estático se utiliza para los dispositivos de red, tales como gateways, switches, servidores e impresoras.



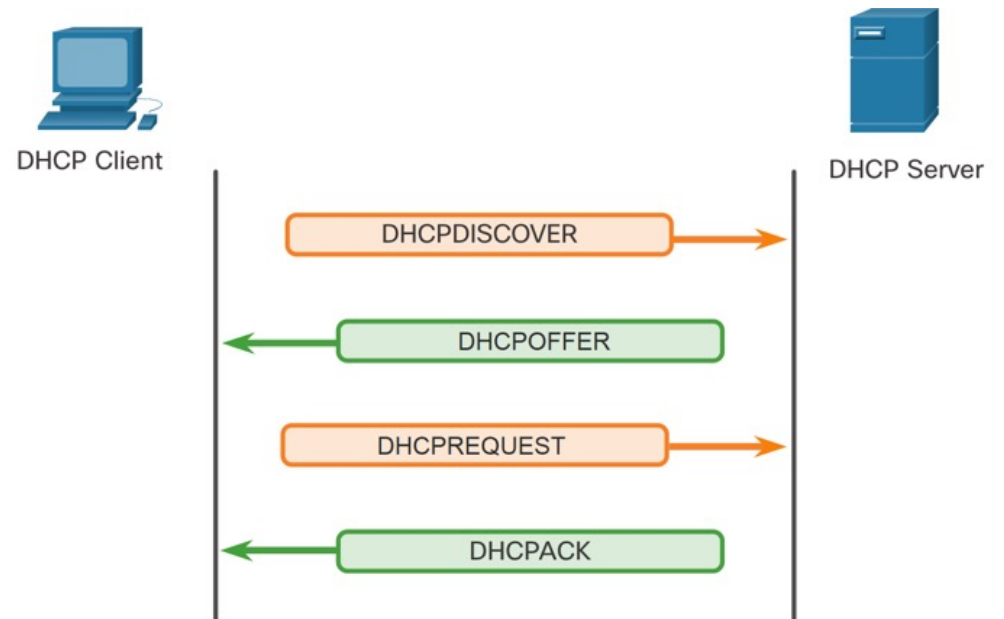
Nota: DHCPv6 (DHCP para IPv6) proporciona servicios similares para los clientes IPv6. Sin embargo, DHCPv6 no proporciona una dirección de puerta de enlace predeterminada. Esto sólo se puede obtener de forma dinámica a partir del anuncio de router del propio router.

Servicios de direccionamiento IP

Funcionamiento de DHCP

Proceso DHCP:

- Cuando un dispositivo configurado con DHCP e IPv4 se inicia o se conecta a la red, el cliente transmite un mensaje de detección de DHCP (DHCPDISCOVER) para identificar cualquier servidor de DHCP disponible en la red.
- Un servidor de DHCP responde con un mensaje de oferta de DHCP (DHCPOFFER), que ofrece una concesión al cliente. (Si un cliente recibe más de una oferta debido a varios servidores DHCP en la red, debe elegir una.)
- Por lo tanto, debe elegir entre ellos y enviar un mensaje de solicitud de DHCP (DHCPREQUEST) que identifique el servidor explícito y la oferta de concesión que el cliente acepta.
- A continuación, el servidor devuelve un mensaje de confirmación DHCP (DHCPACK) que reconoce al cliente que se ha finalizado la concesión.
- Si la oferta ya no es válida, el servidor seleccionado responde con un mensaje de reconocimiento negativo de DHCP (DHCPNAK) y el proceso debe comenzar con un nuevo mensaje de DHCPDISCOVER.

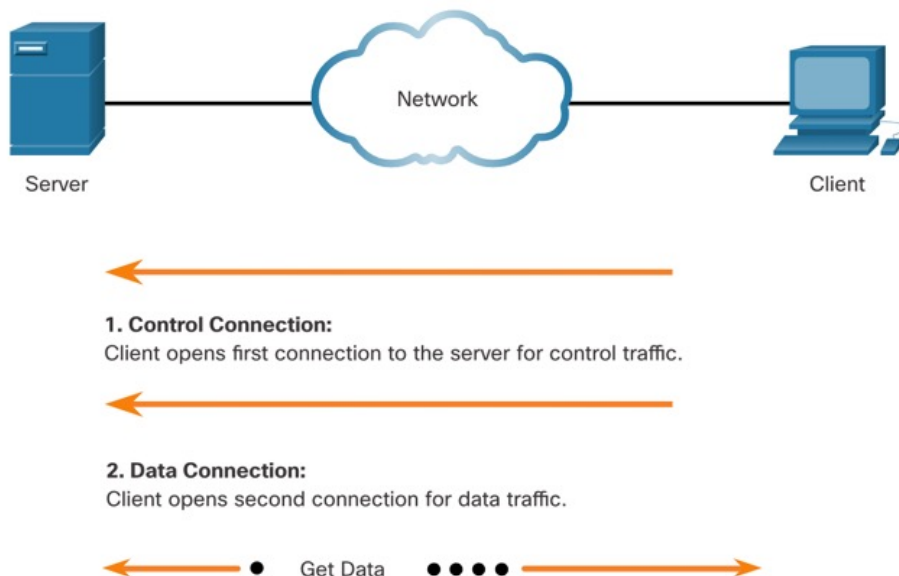


Nota: DHCPv6 tiene un conjunto de mensajes similares a los de DHCPv4. Los mensajes de DHCPv6 son SOLICIT, ADVERTISE, INFORMATION REQUEST y REPLY.

Servicios de uso compartido de archivos

Protocolo de transferencia de archivos

El protocolo FTP se desarrolló para permitir las transferencias de datos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora cliente y se utiliza para insertar y extraer datos en un servidor FTP.



Paso 1 El cliente establece la primera conexión al servidor para controlar el tráfico en el puerto TCP 21. El tráfico consiste en comandos de cliente y respuestas de servidor.

Paso 2: - el cliente establece la segunda conexión al 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 subir datos a él (insertarlos).

Servicios de uso compartido de archivos

Bloqueo de mensajes del servidor

El Bloque de mensajes del servidor (SMB, Server Message Block) es un protocolo cliente-servidor para compartir archivos: Los servidores pueden hacer que sus recursos estén disponibles en la red para que los usen los clientes.

Tres funciones de los mensajes SMB:

- Iniciar, autenticar y terminar sesiones
- Controlar el acceso a los archivos y a las impresoras
- Autorizar una aplicación para enviar o recibir mensajes para o de otro dispositivo

A diferencia del protocolo para compartir archivos admitido por FTP, los clientes establecen una conexión a largo plazo con los servidores. Después de establecer la conexión, el usuario del cliente puede acceder a los recursos en el servidor como si el recurso fuera local para el host del cliente.

