



ITSQMET

INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

FORMANDO PROFESIONALES DE ÉLITE



FUNDAMENTOS DE REDES

CLASE 11

Ing. ANDRÉS PÉREZ





INTRODUCCIÓN A LA CLASE

1. Retroalimentación
2. Indicaciones generales
3. Objetivos de la clase



ITSQMET
INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

RETROALIMENTACIÓN

FORMANDO PROFESIONALES DE ÉLITE



Objetivos de la clase:

Establecer conceptos básicos sobre ICMP



ITSQMET
INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

ICMP

FORMANDO PROFESIONALES DE ÉLITE

© 2016 Cisco y/o sus filiales. Todos los derechos reservados.
Información confidencial de Cisco

Nº





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 inaccessible
 - Tiempo superado

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



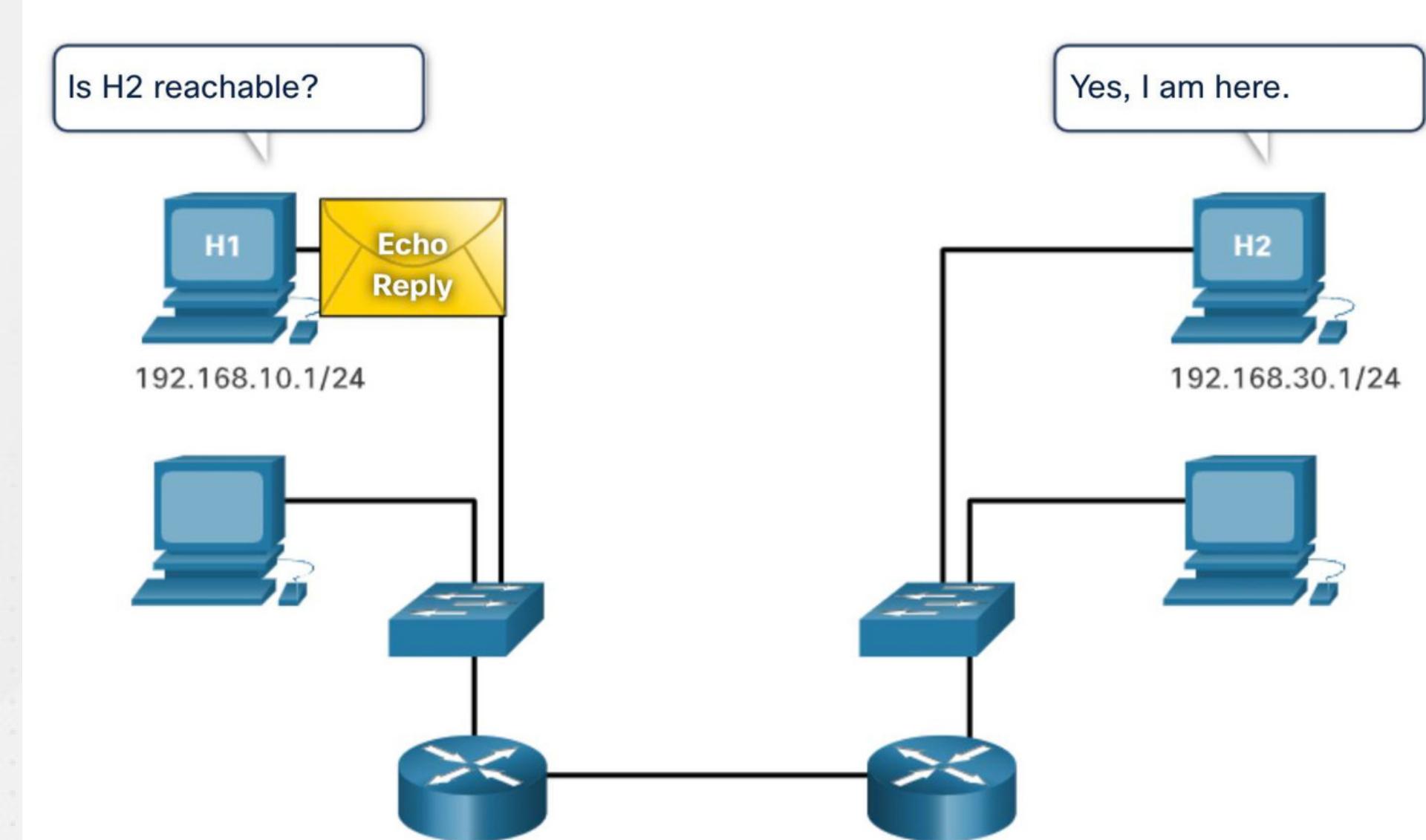
Mensajes ICMP

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.  
  
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 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:

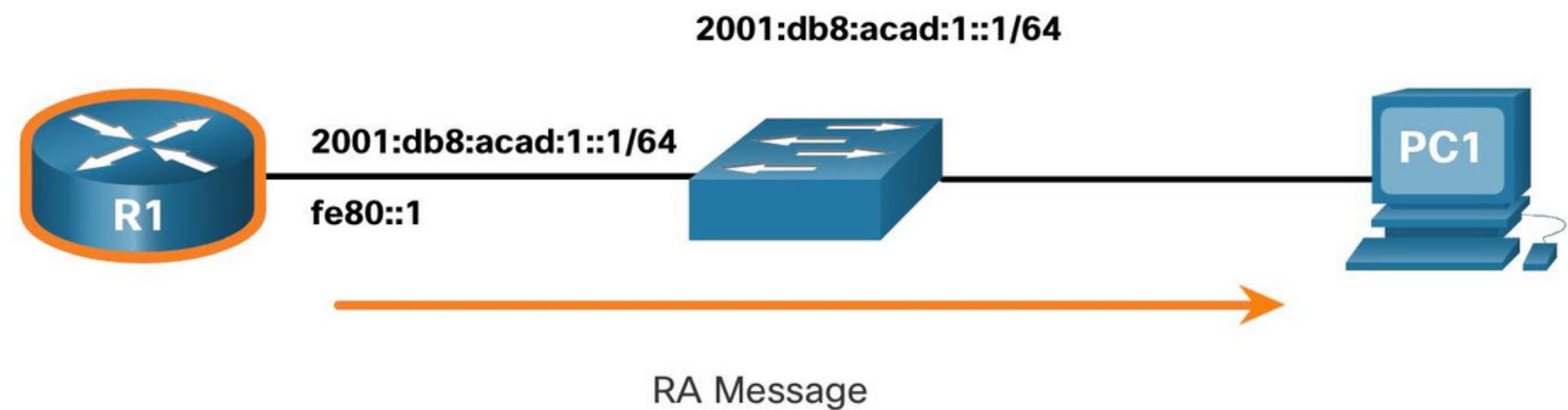
- Mensaje de solicitud de vecino (NS)
- Mensaje de anuncio de vecino (NA)

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.

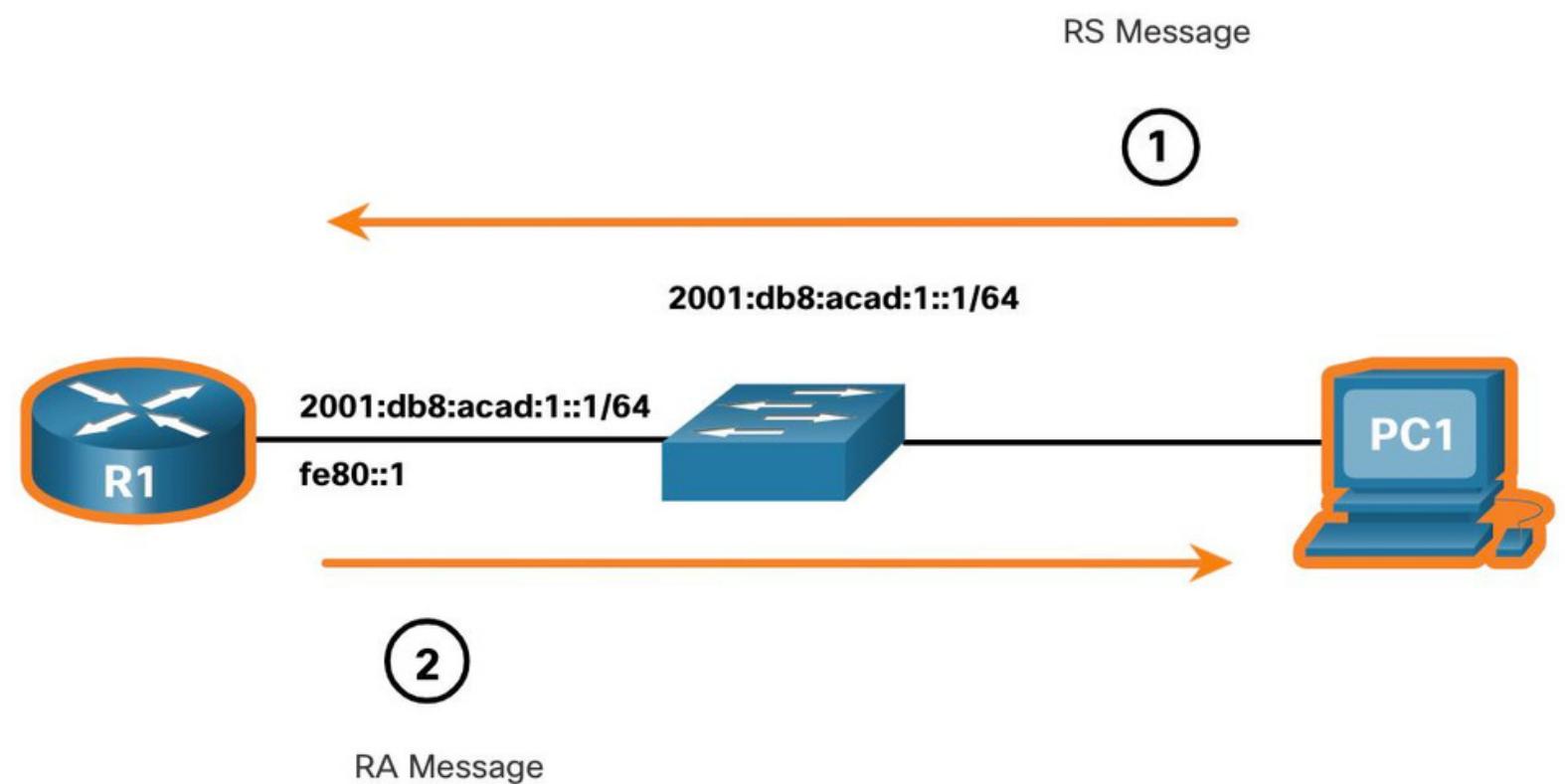




Mensajes ICMP

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. »

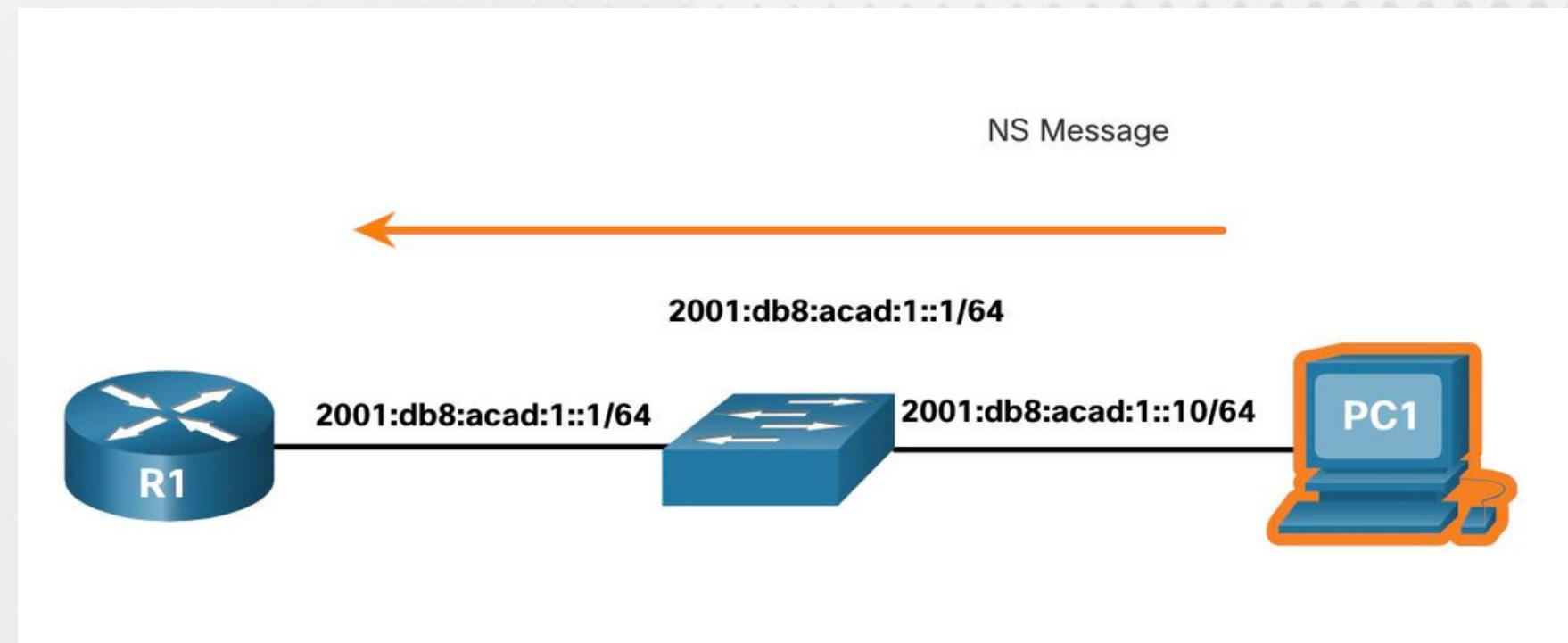




Mensajes ICMP

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.



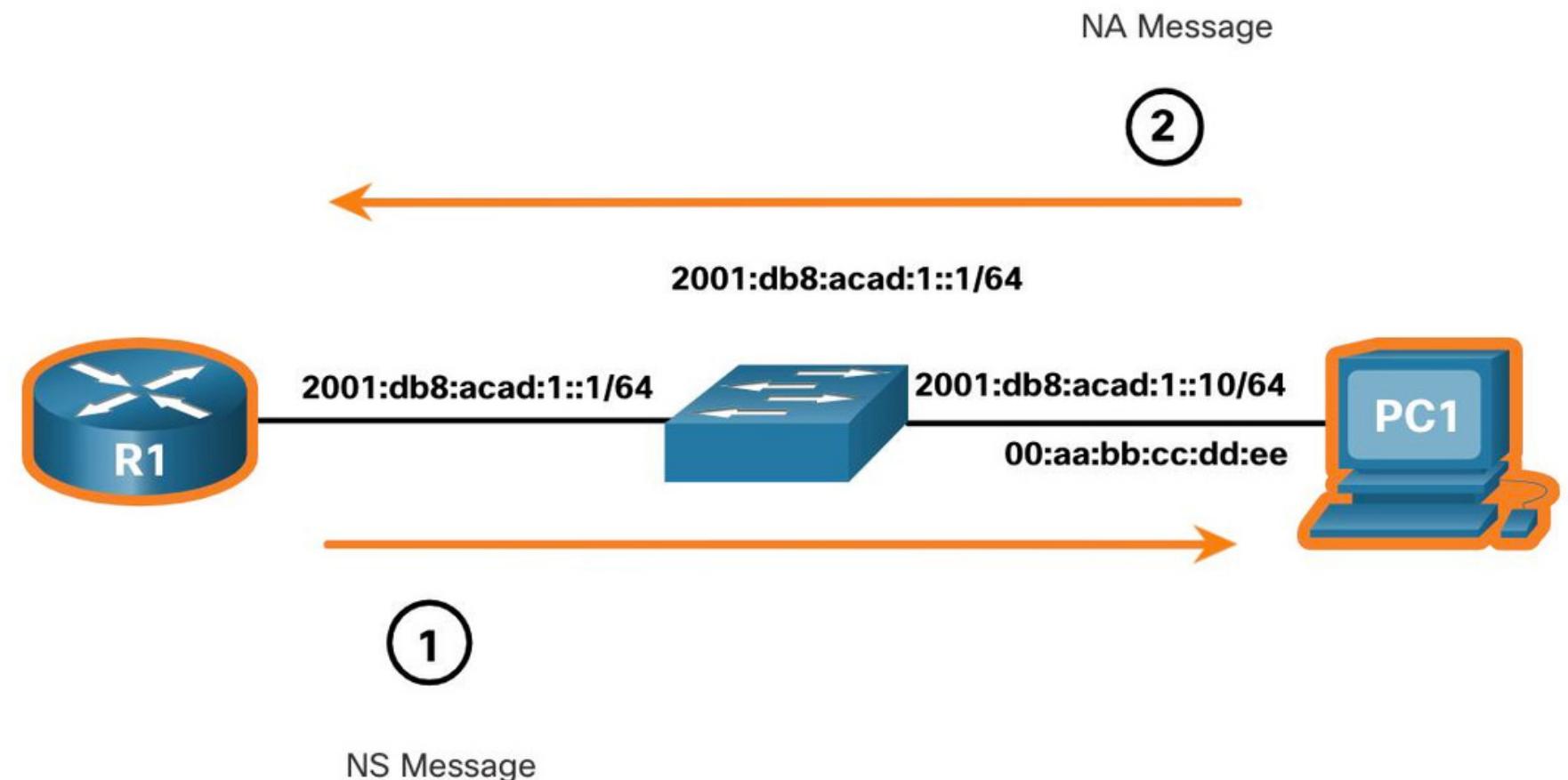
Nota: No se requiere DAD, pero RFC 4861 recomienda que DAD se realice en direcciones unicast.



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



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

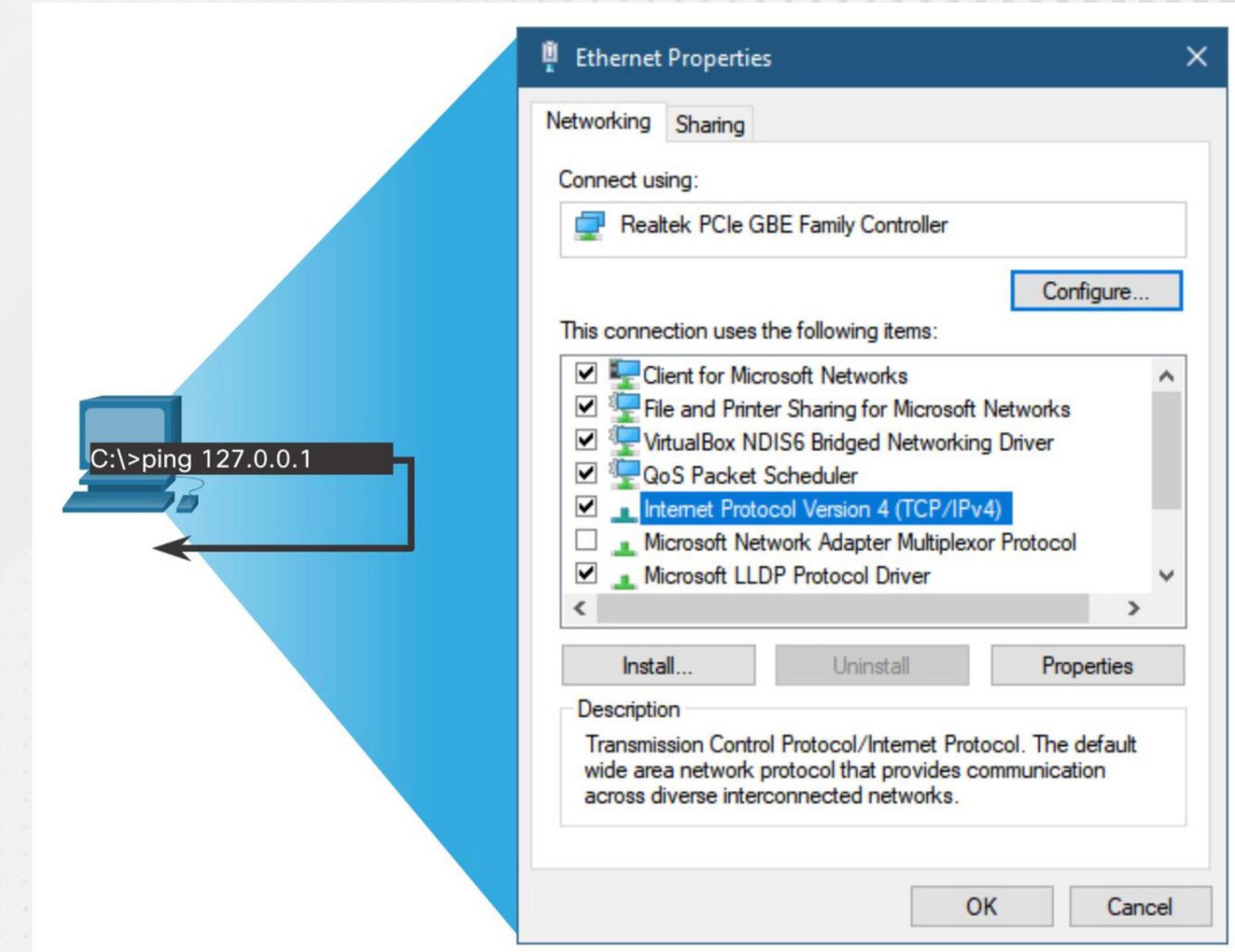


Pruebas de Ping y Traceroute

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 Pv4 (:: 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.



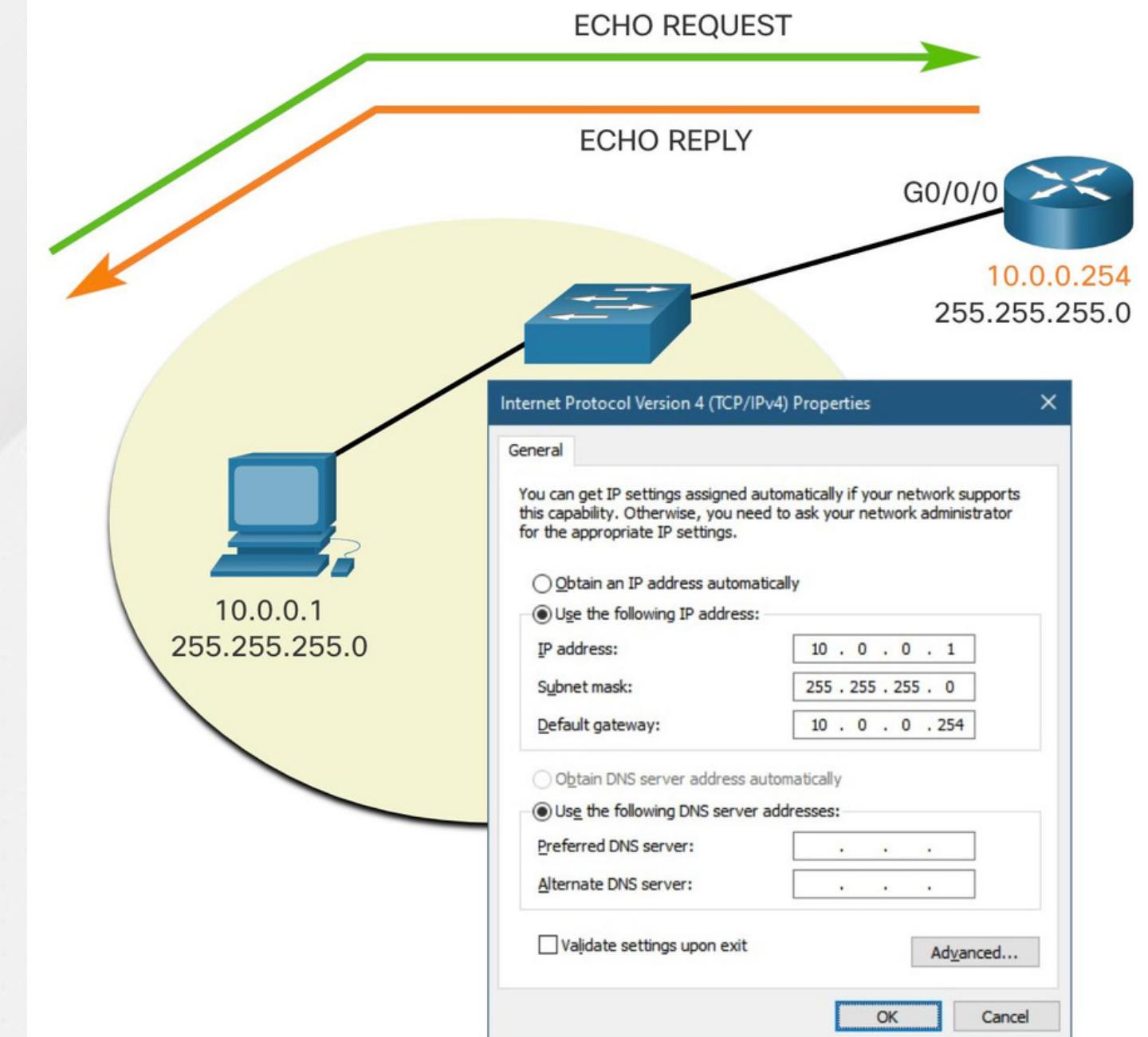


Hacer ping a la puerta de enlace predeterminada

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.





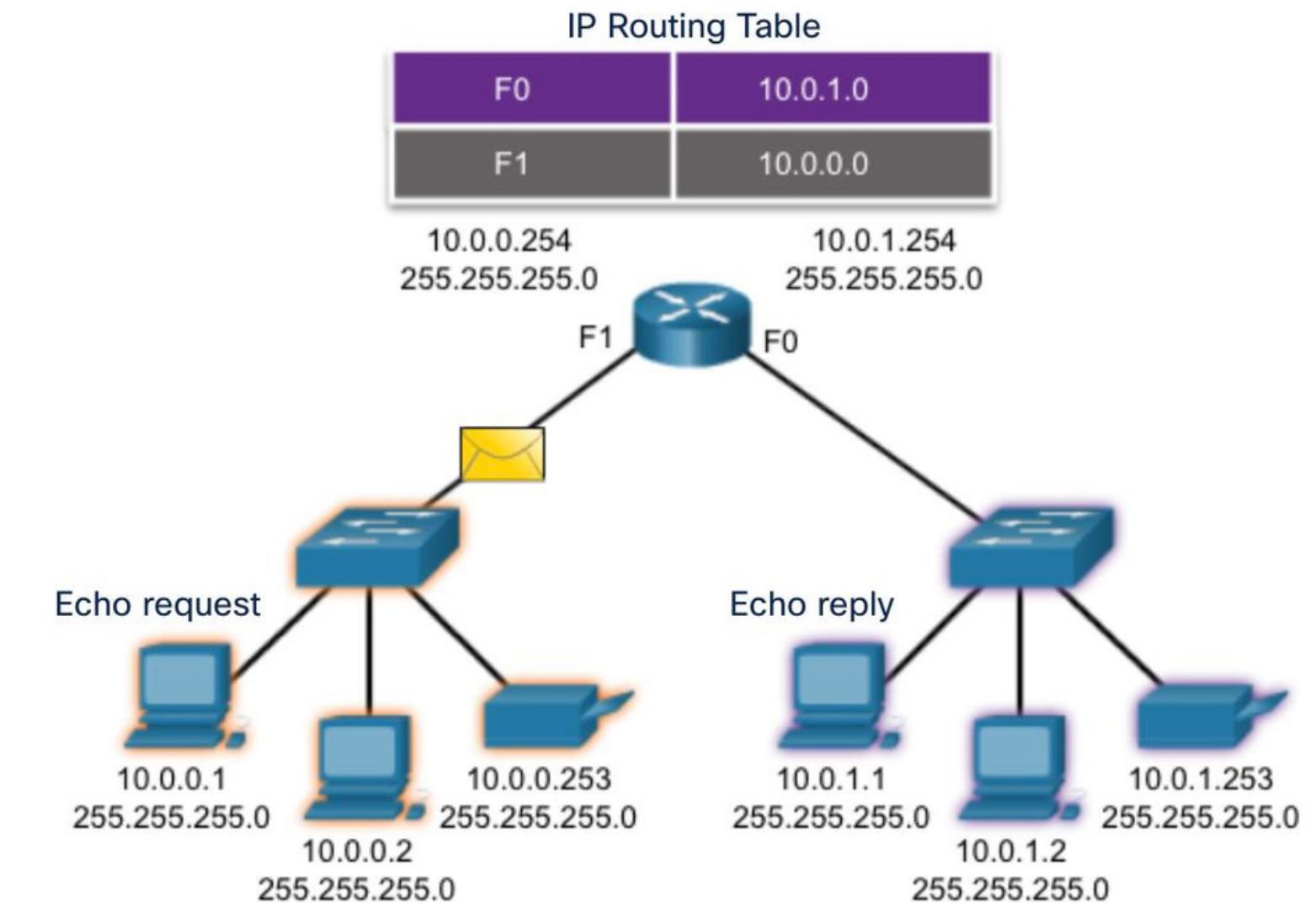
Pruebas de Ping y Traceroute

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.





Pruebas de Ping y Traceroute

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

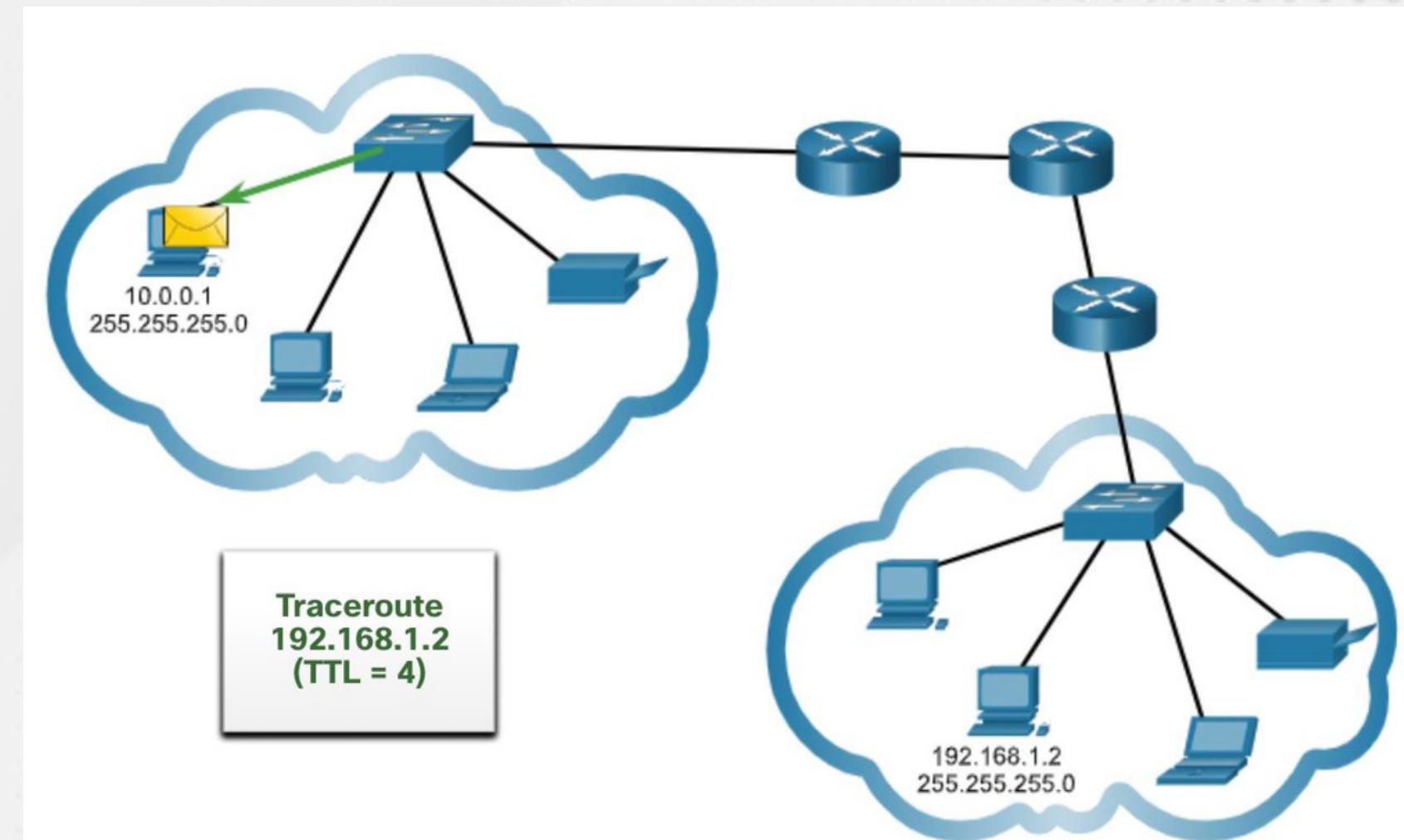
Nota: Traceroute utiliza una función del campo TTL en IPv4 y el campo Límite de salto en IPv6 en los encabezados de Capa 3, junto con el mensaje Tiempo excedido ICMP.



Pruebas de Ping y Traceroute

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.





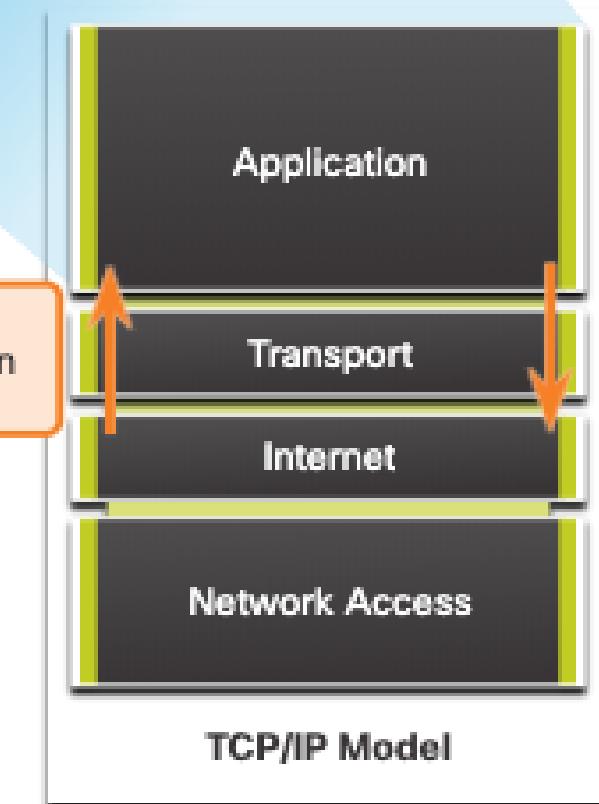
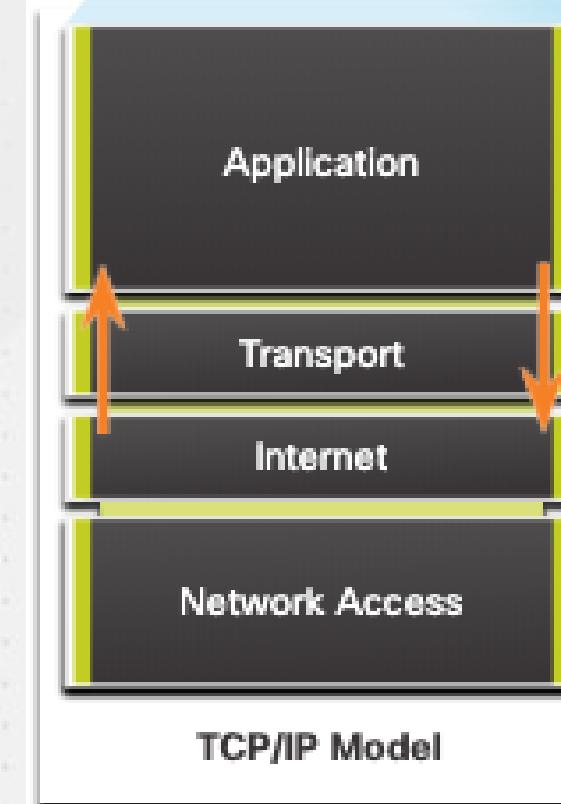
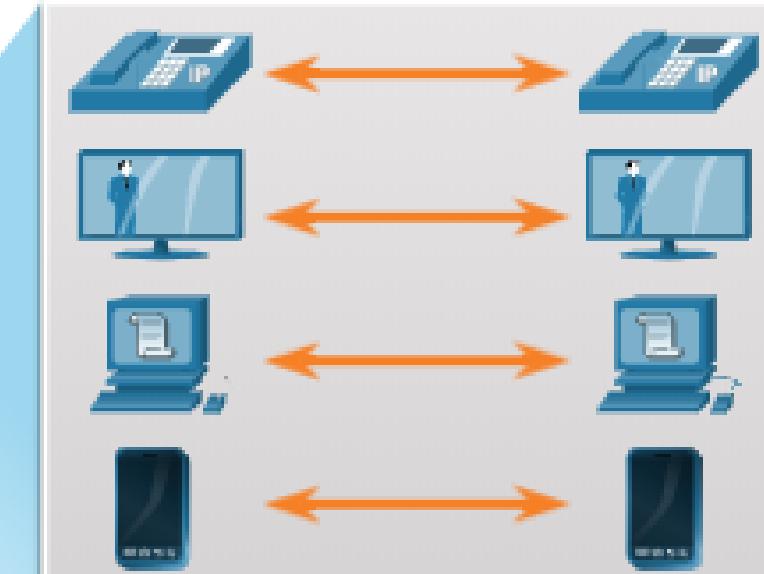
TRANSPORTE DE DATOS



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.



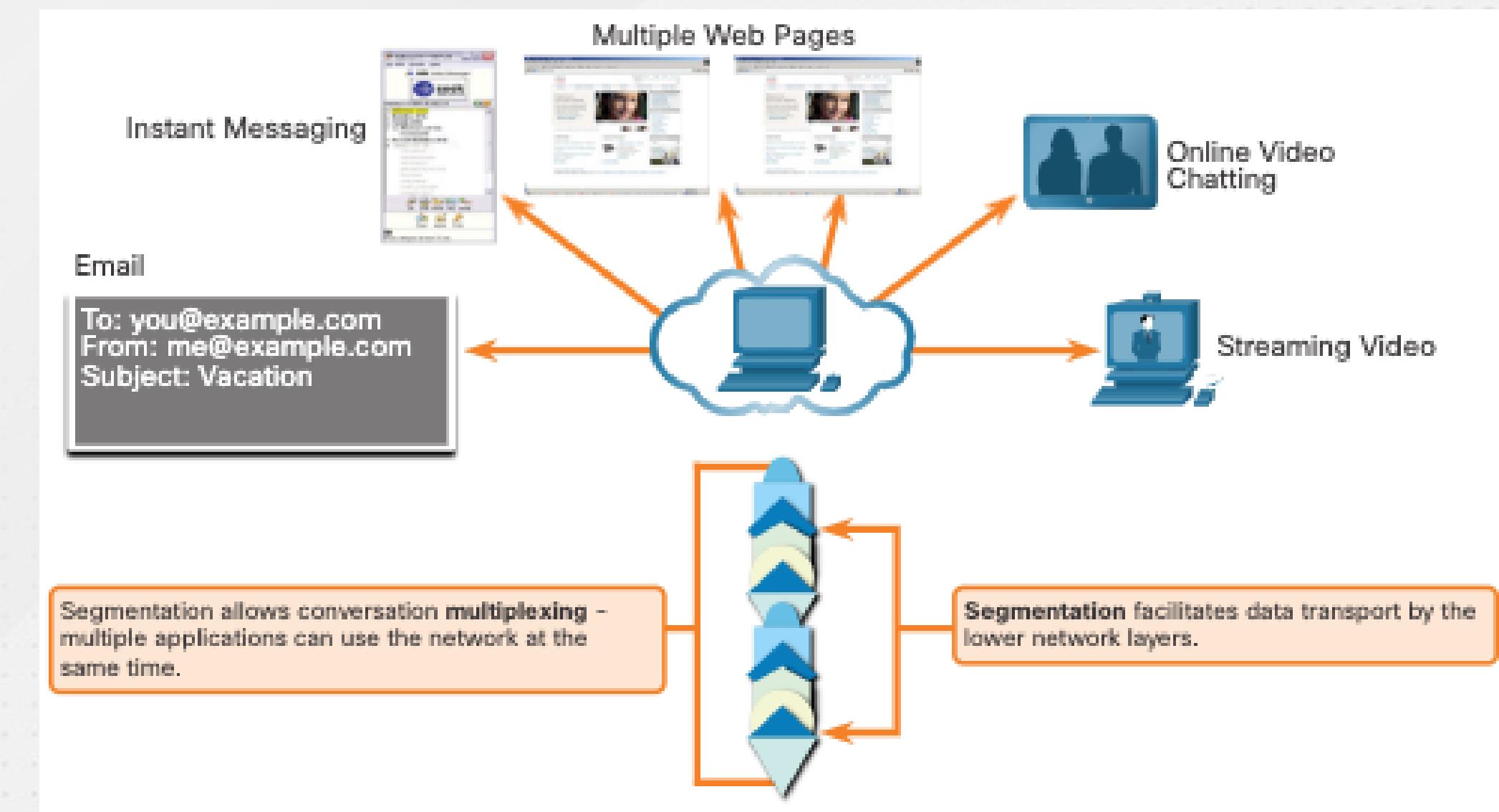


Transporte de datos

Tareas de la capa de transporte

La capa de transporte tiene las siguientes responsabilidades:

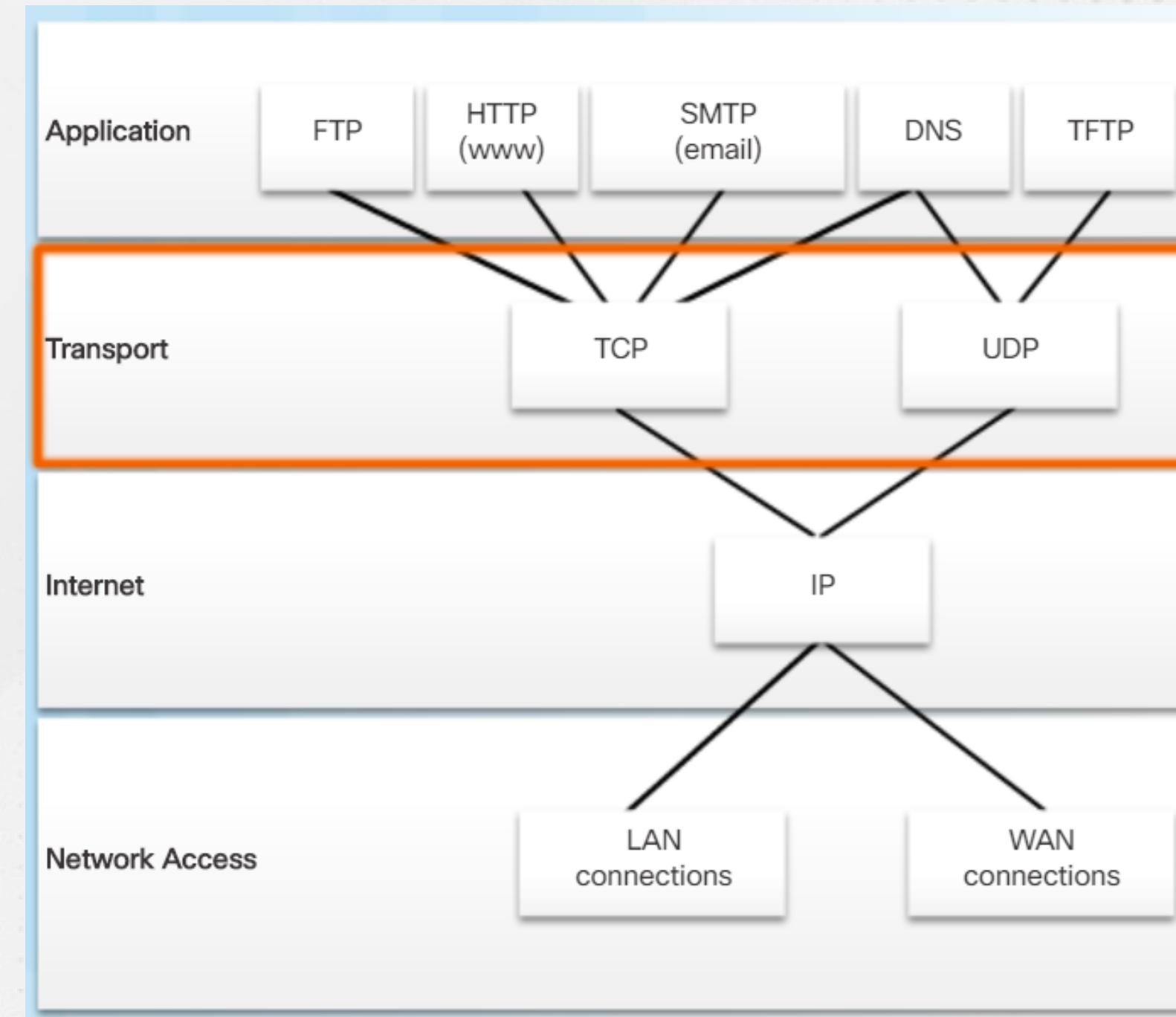
- Seguimiento de conversaciones individuales
- Segmentación de datos y rearmado de segmentos
- Agregar información de encabezado
- Identificar, separar y administrar múltiples conversaciones
- Utiliza segmentación y multiplexación para permitir que diferentes conversaciones de comunicación se intercalen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



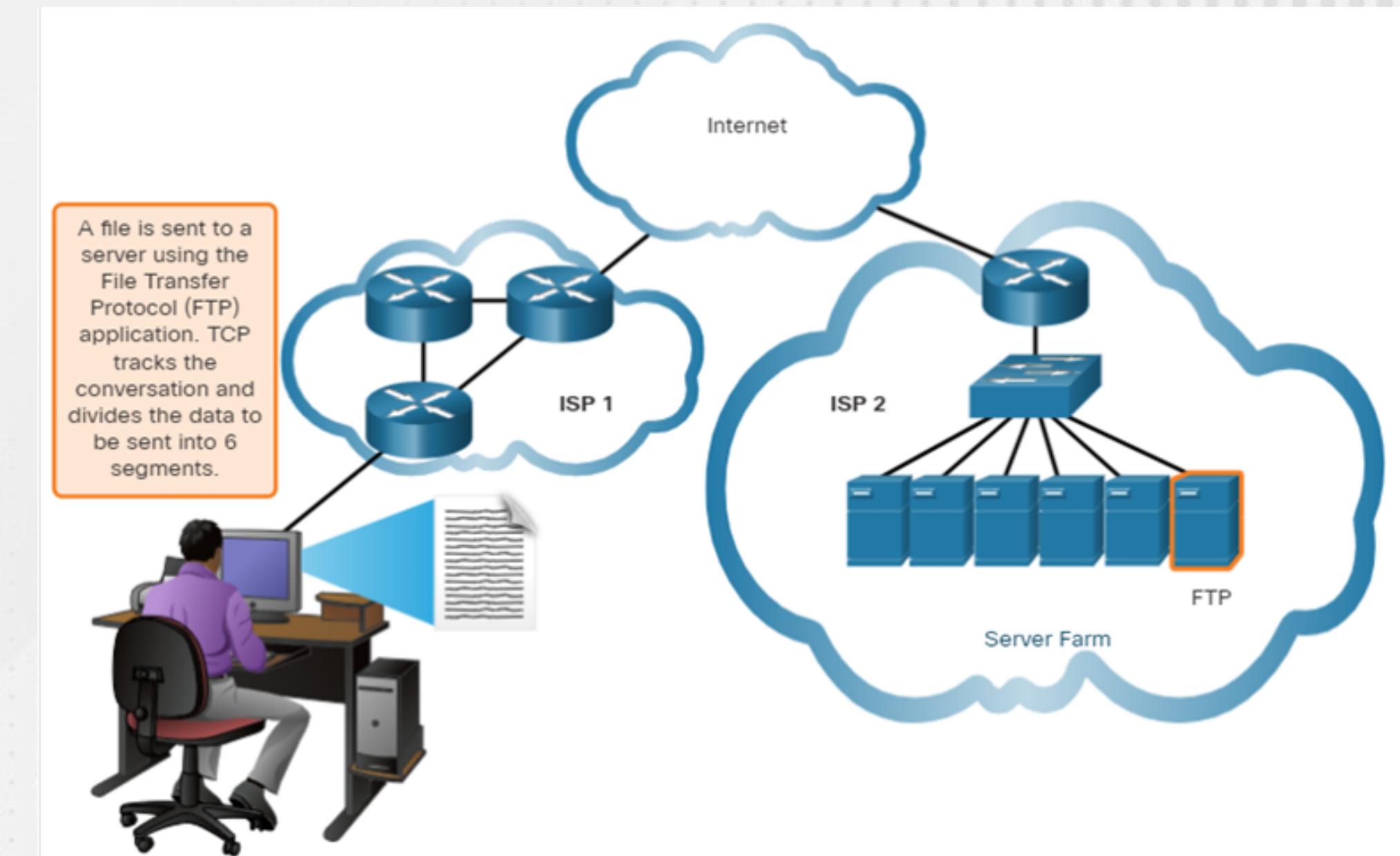


Transmission Control Protocol (Protocolo de control de transmisión)

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

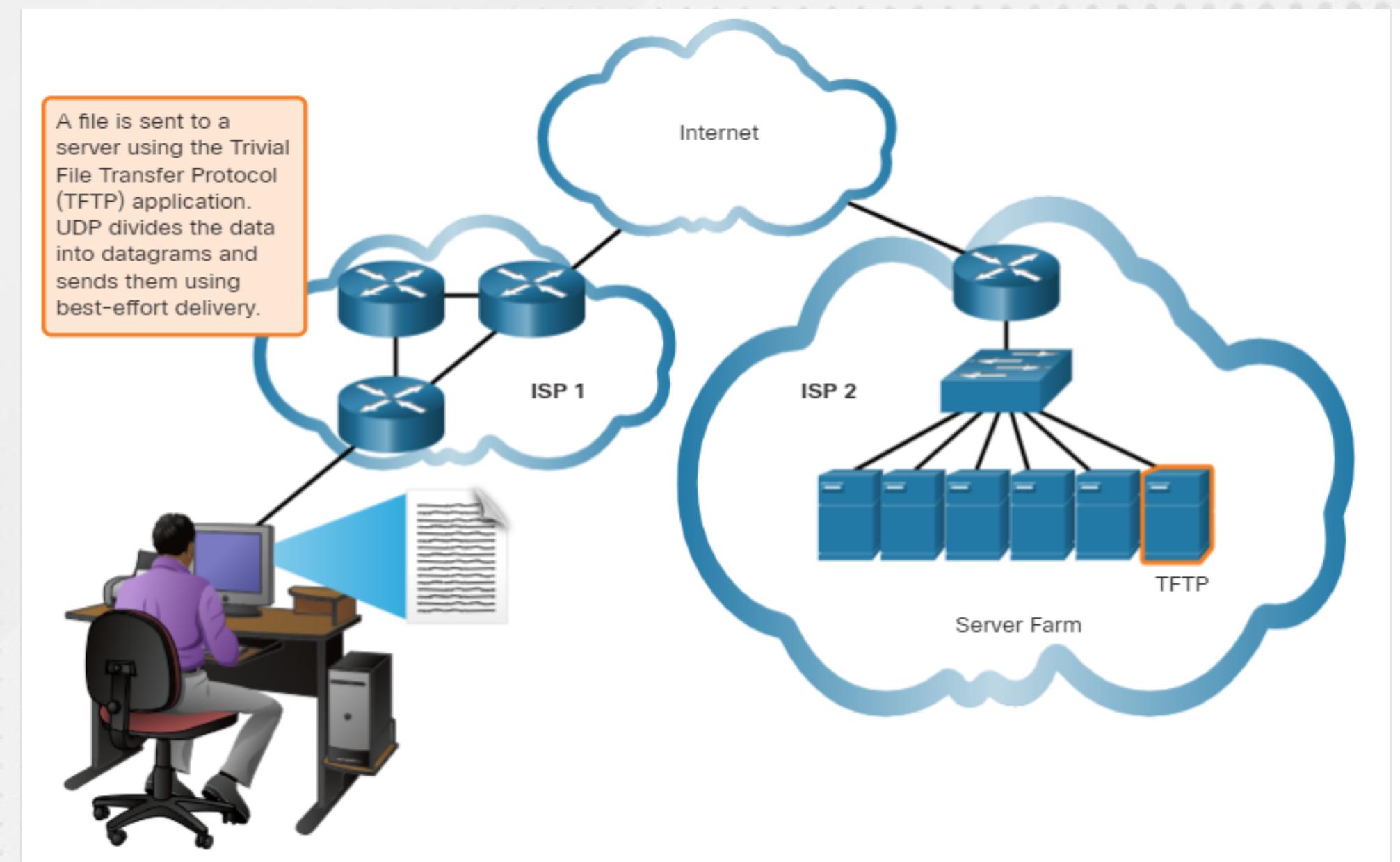




El UDP proporciona las funciones básicas para entregar segmentos de datos entre las aplicaciones adecuadas, con muy poca sobrecarga y revisión de datos.

- 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.

Protocolo de datagramas de usuario de datos (UDP)

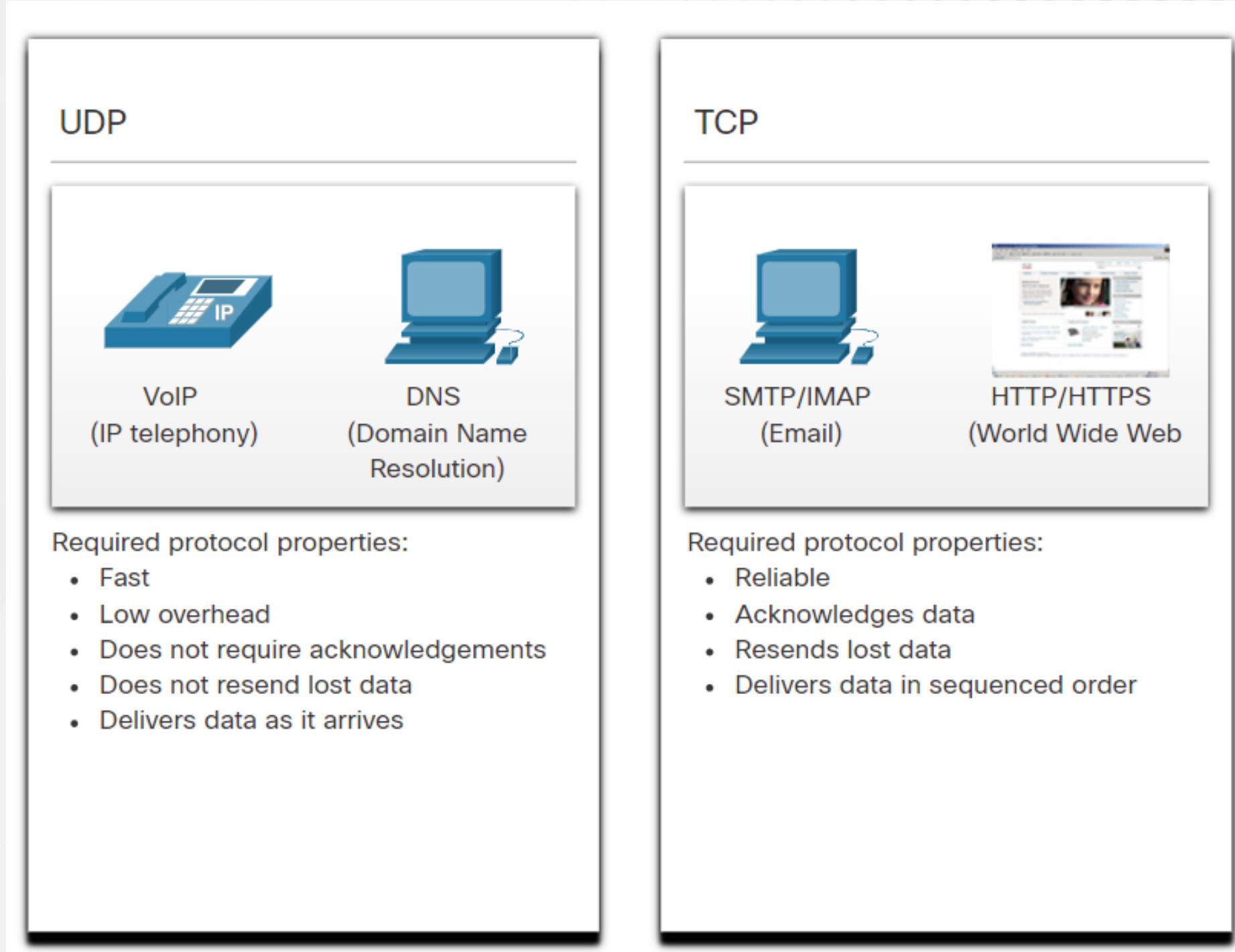




UDP también es utilizado por las aplicaciones de solicitud y respuesta donde los datos son mínimos, y la retransmisión se puede hacer rápidamente.

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

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





DESCRIPCIÓN GENERAL DE TCP



Descripción general de TCP Características de TCP

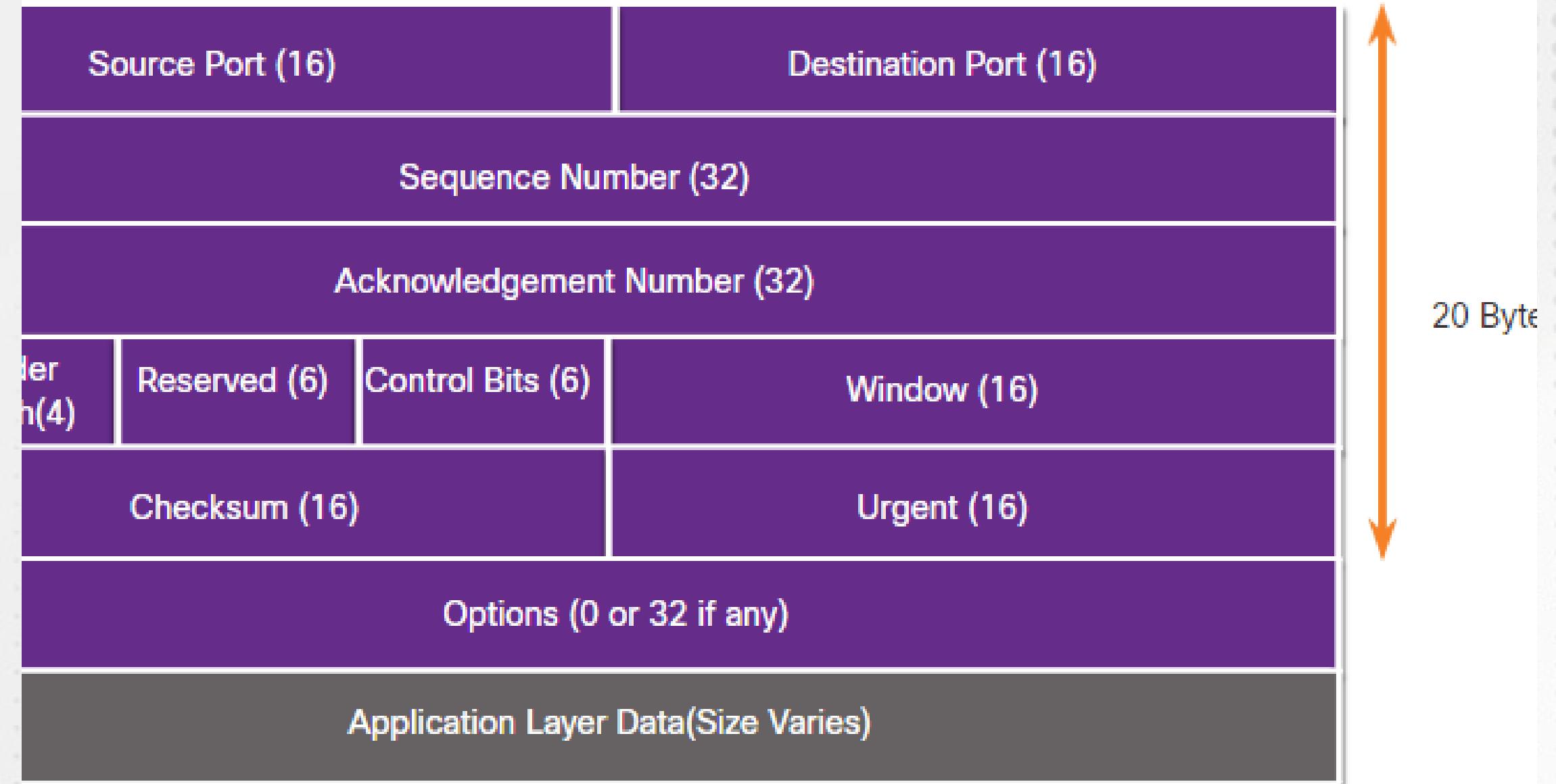
- **Establece una sesión** -TCP es un protocolo orientado a la conexión que negocia y establece una conexión permanente (o sesión) entre los dispositivos de origen y destino antes de reenviar cualquier tráfico.
- **Garantiza una entrega confiable**- Por muchas razones, es posible que un segmento se corrompa 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.



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.

Descripción general de TCP Encabezado TCP





Introducción a TCP

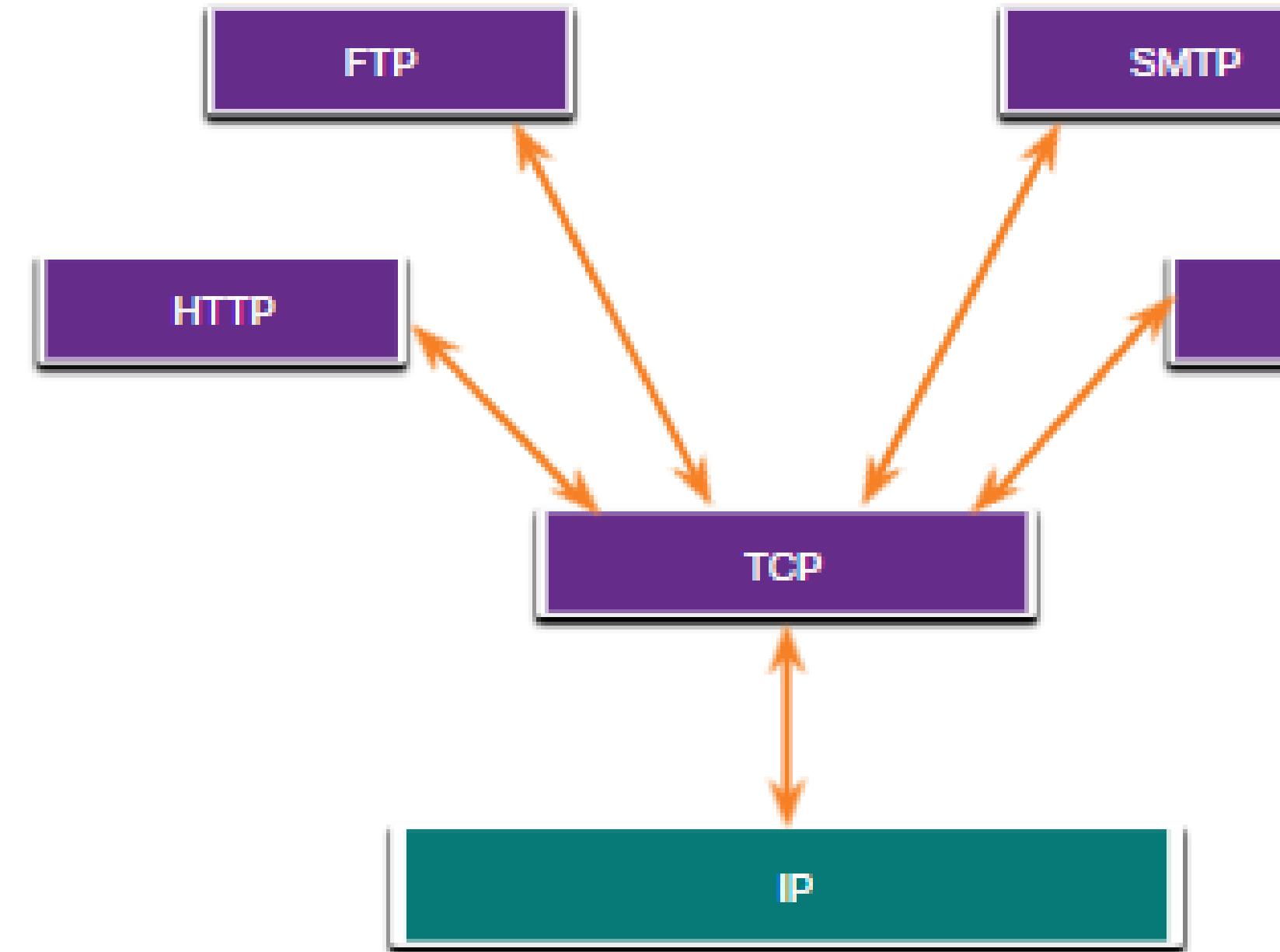
Campos de encabezado TCP

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 de 32 bits	Campo de 32 bits utilizado para reensamblar datos.
Longitud del encabezado	Un campo de 32 bits utilizado para indicar que se han recibido datos y el siguiente byte esperado de la fuente.
Reservado	Campo de 4 bits conocido como «desplazamiento de datos» que indica la longitud del encabezado del segmento TCP.
Bits de control	Un campo de 6 bits que está reservado para uso futuro.
Tamaño de la ventana	Un campo de 16 bits utilizado que incluye códigos de bit, o indicadores, que indican el propósito y la función del segmento TCP.
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.



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 TCP Aplicaciones que utilizan TCP





VISIÓN GENERAL DE UDP

FORMANDO PROFESIONALES DE ÉLITE

© 2016 Cisco y/o sus filiales. Todos los derechos reservados. Información <Nº>
confidencial de Cisco





Descripción general de UDP **Características UDP**

Las características UDP incluyen lo siguiente:

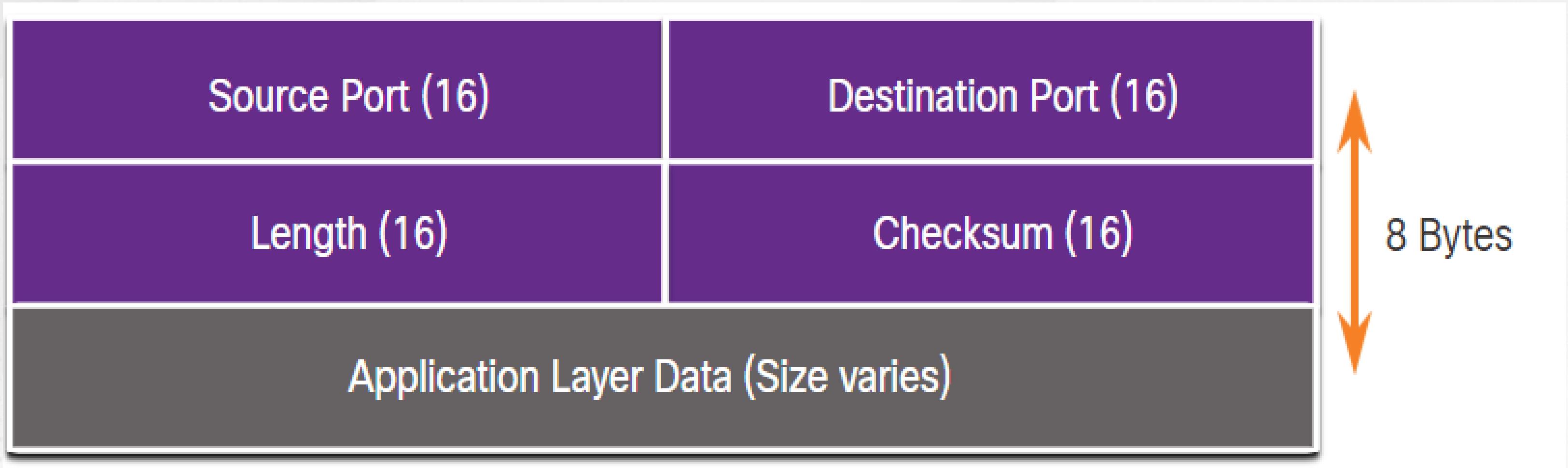
- Los datos se reconstruyen en el orden en que se recibieron.
- Los segmentos perdidos no se vuelven a enviar.
- No hay establecimiento de sesión.
- El envío no está informado sobre la disponibilidad de recursos.



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.

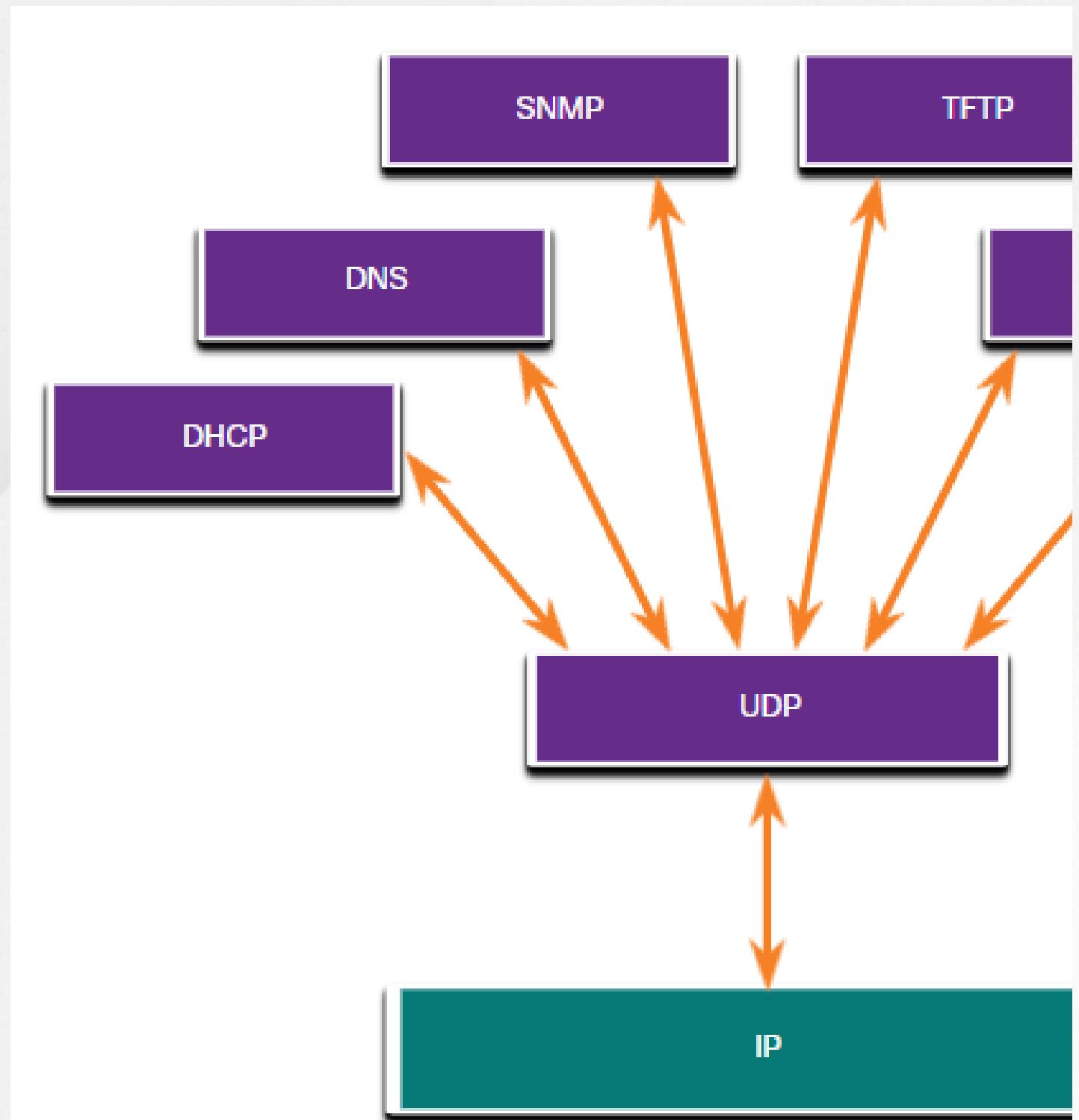
Campo de encabezado UDP	Descripción
Puerto de origen	Campo de 16 bits utilizado para identificar la aplicación de origen por número de puerto.
Puerto de destino	Campo de 16 bits utilizado para identificar la aplicación de destino por número de puerto.
Longitud	Campo de 16 bits que indica la longitud 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



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.

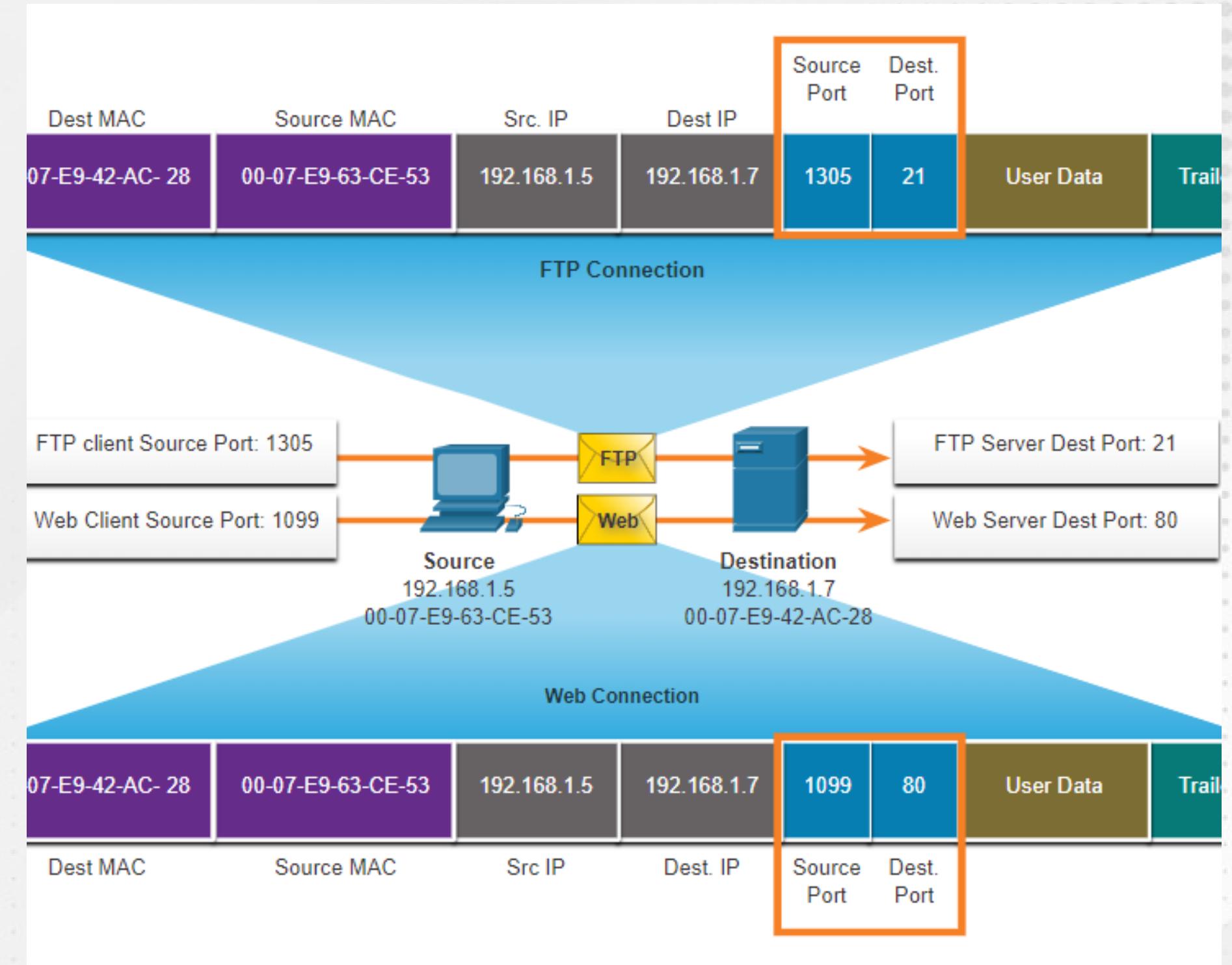
Source Port (16)

Destination Port (16)



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.)

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
```



ITSQMET

INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

PROCESO DE COMUNICACIÓN EN TCP

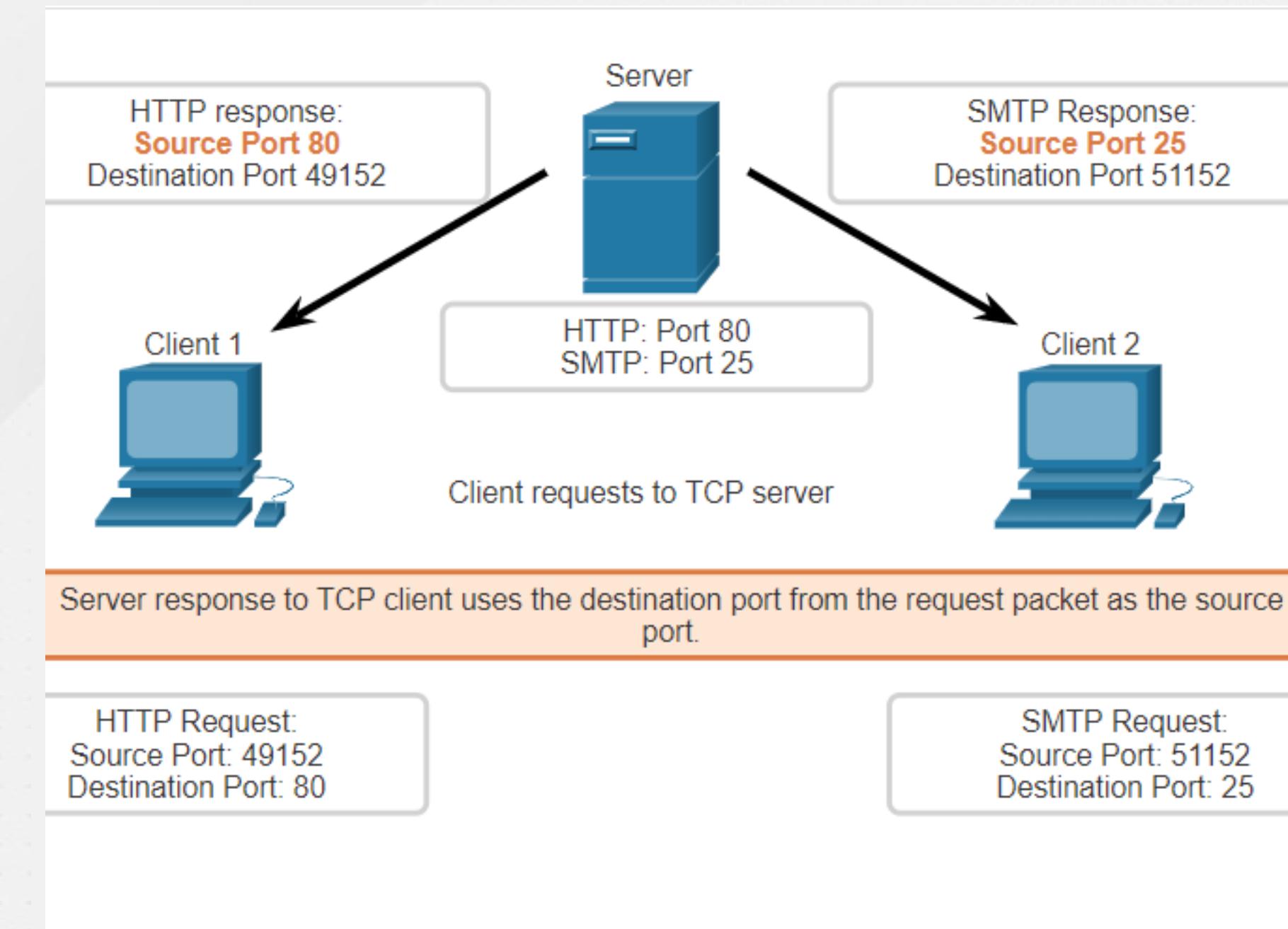
FORMANDO PROFESIONALES DE ÉLITE



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.





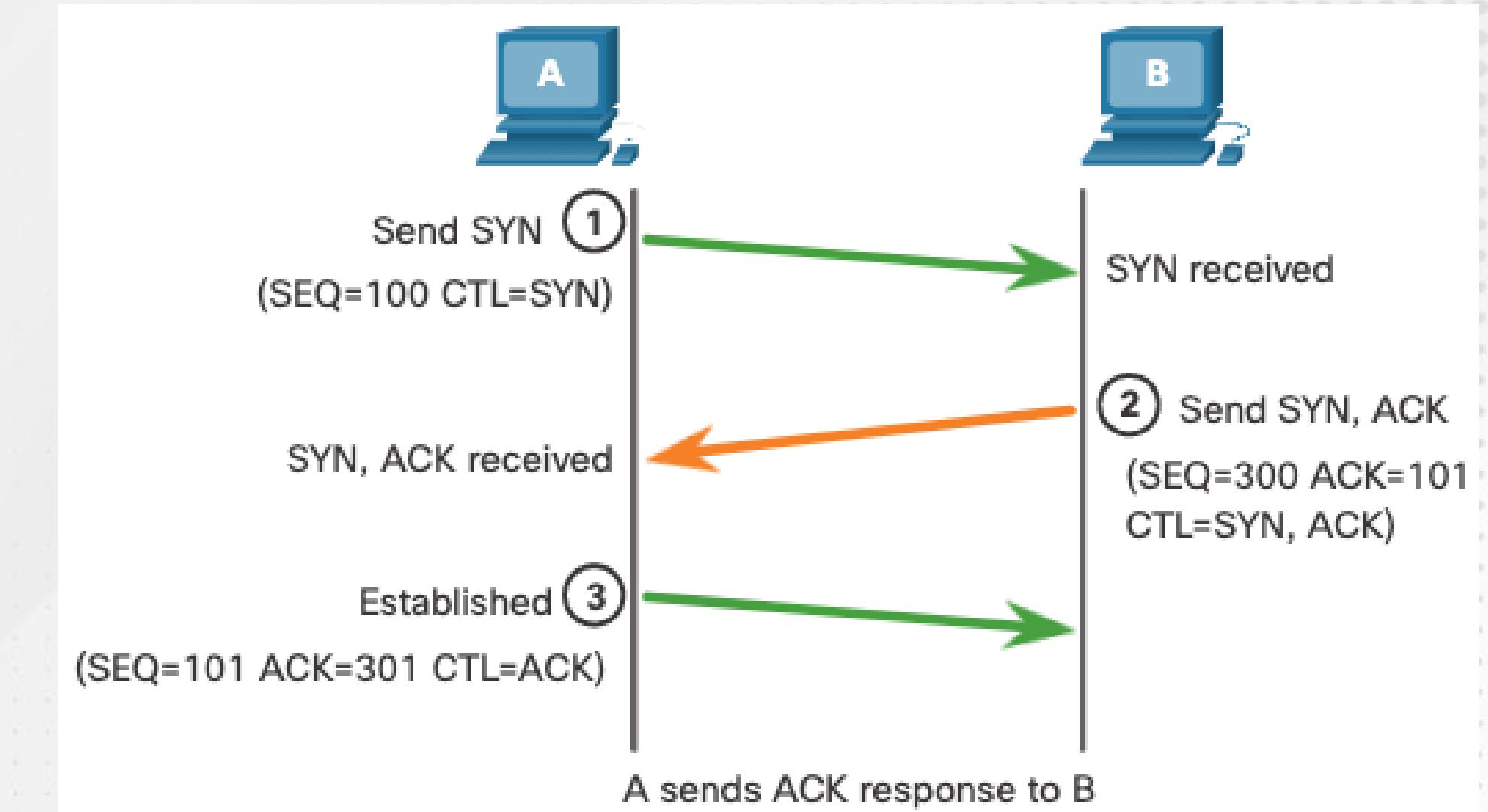
Proceso de comunicación en TCP

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

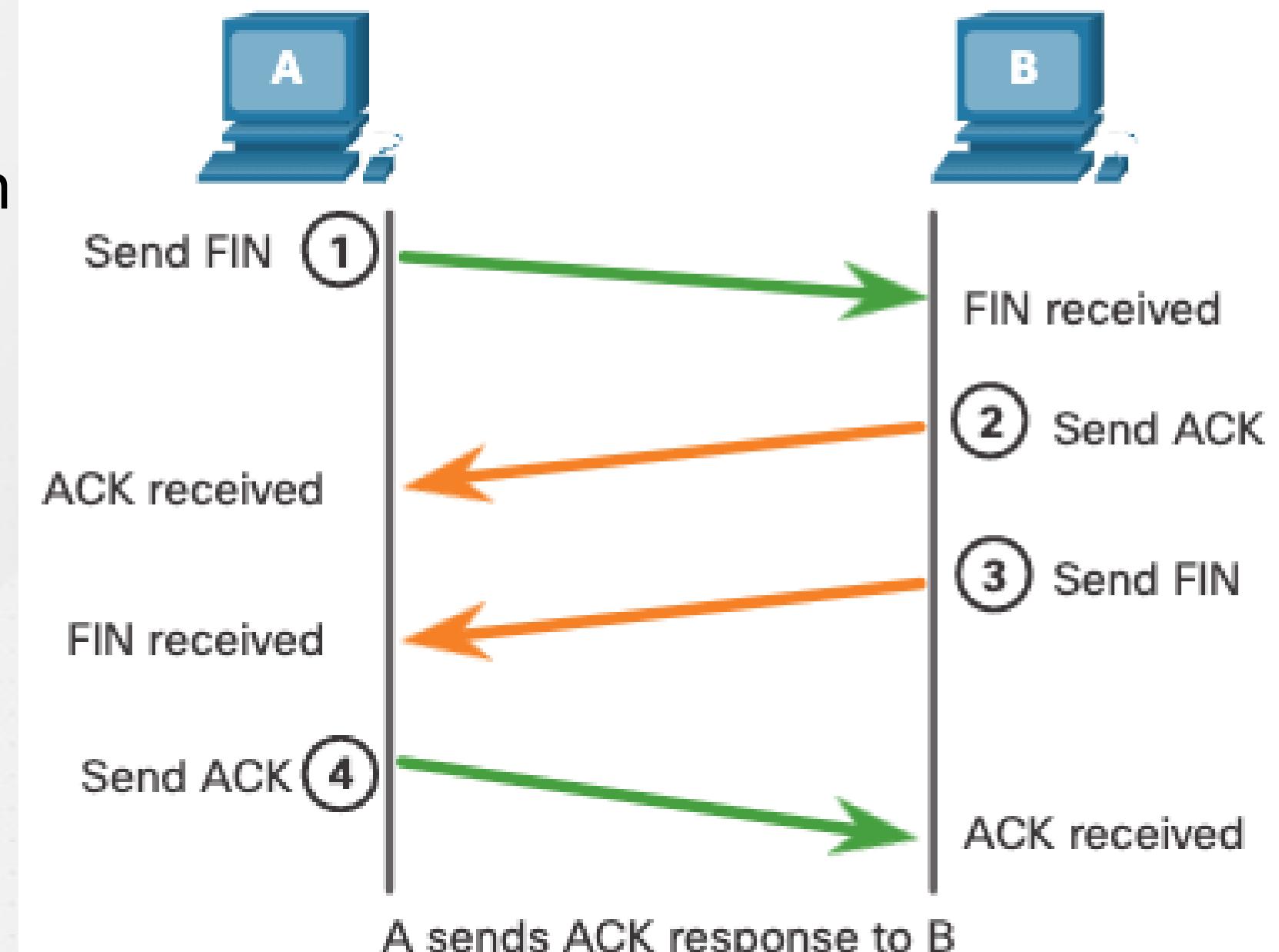
Finalización de la sesión TCP

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.





Funciones del enlace de tres vías:

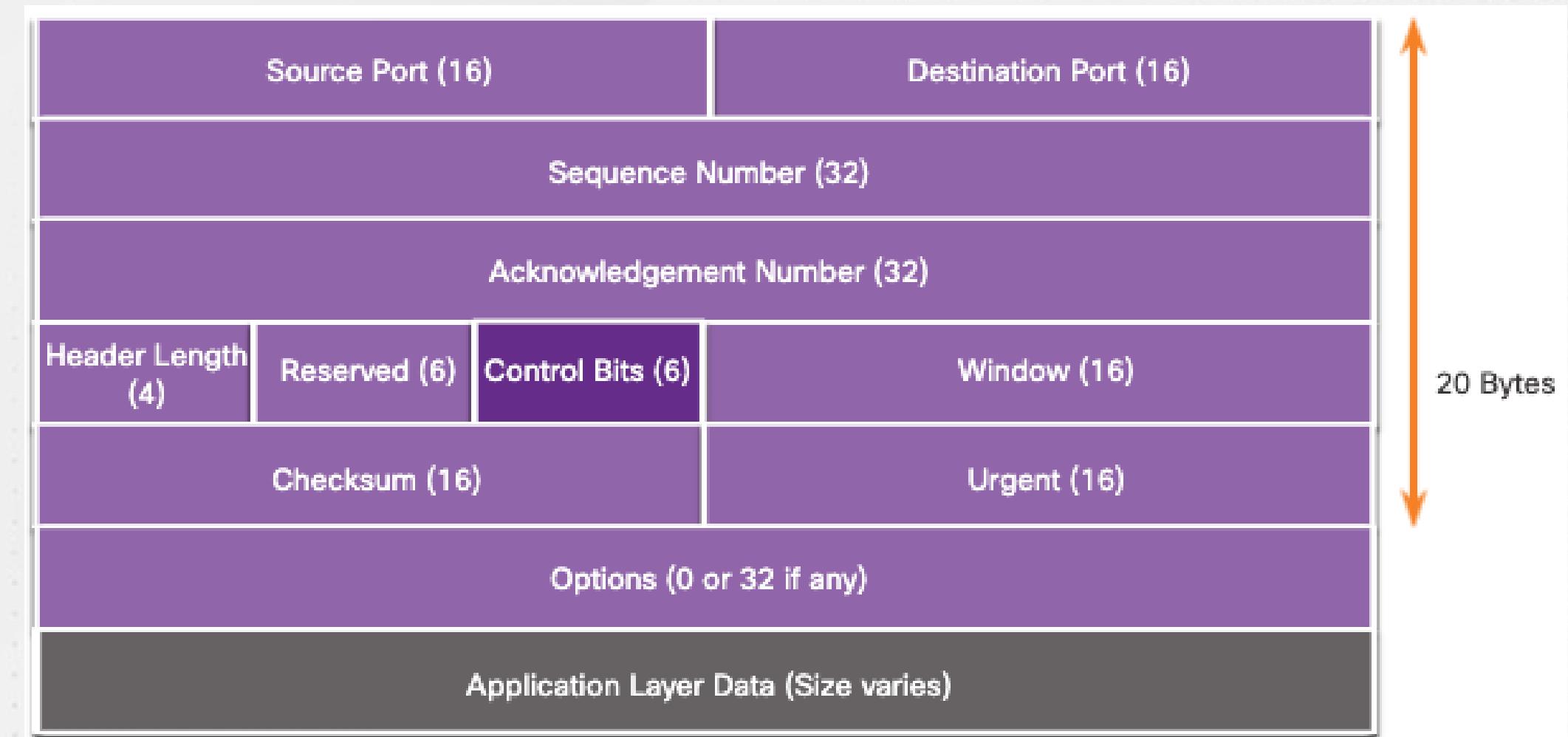
- Establece que el dispositivo de destino está presente en la red.
- Verifica que el dispositivo de destino tenga un servicio activo y acepte solicitudes en el número de puerto de destino que el cliente de origen desea utilizar.
- Informa al dispositivo de destino que el cliente de origen intenta establecer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



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.





ITSQMET

INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

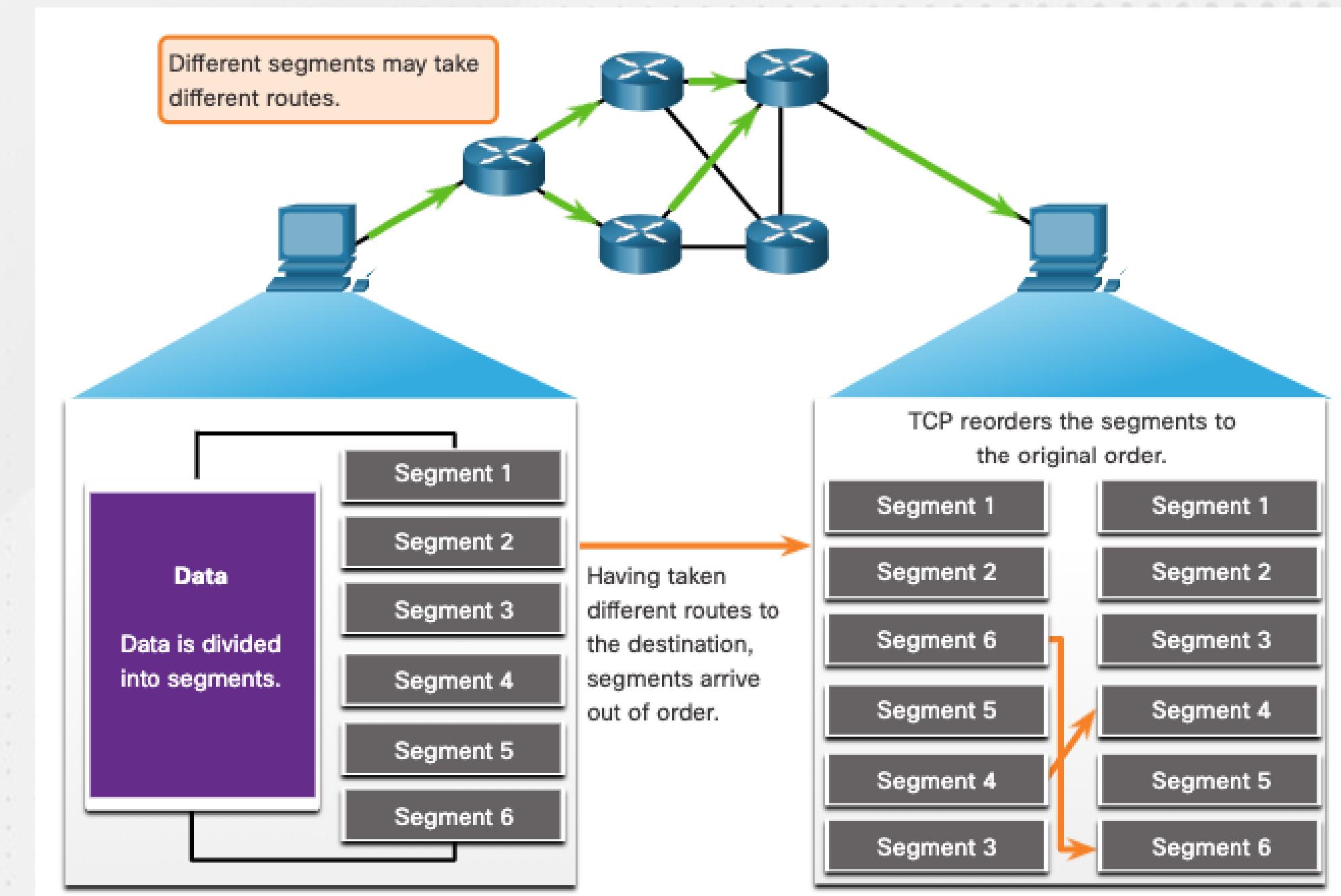
CONFIABILIDAD Y CONTROL DE FLUJO

FORMANDO PROFESIONALES DE ÉLITE



Confiabilidad y control del flujo 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 no 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.



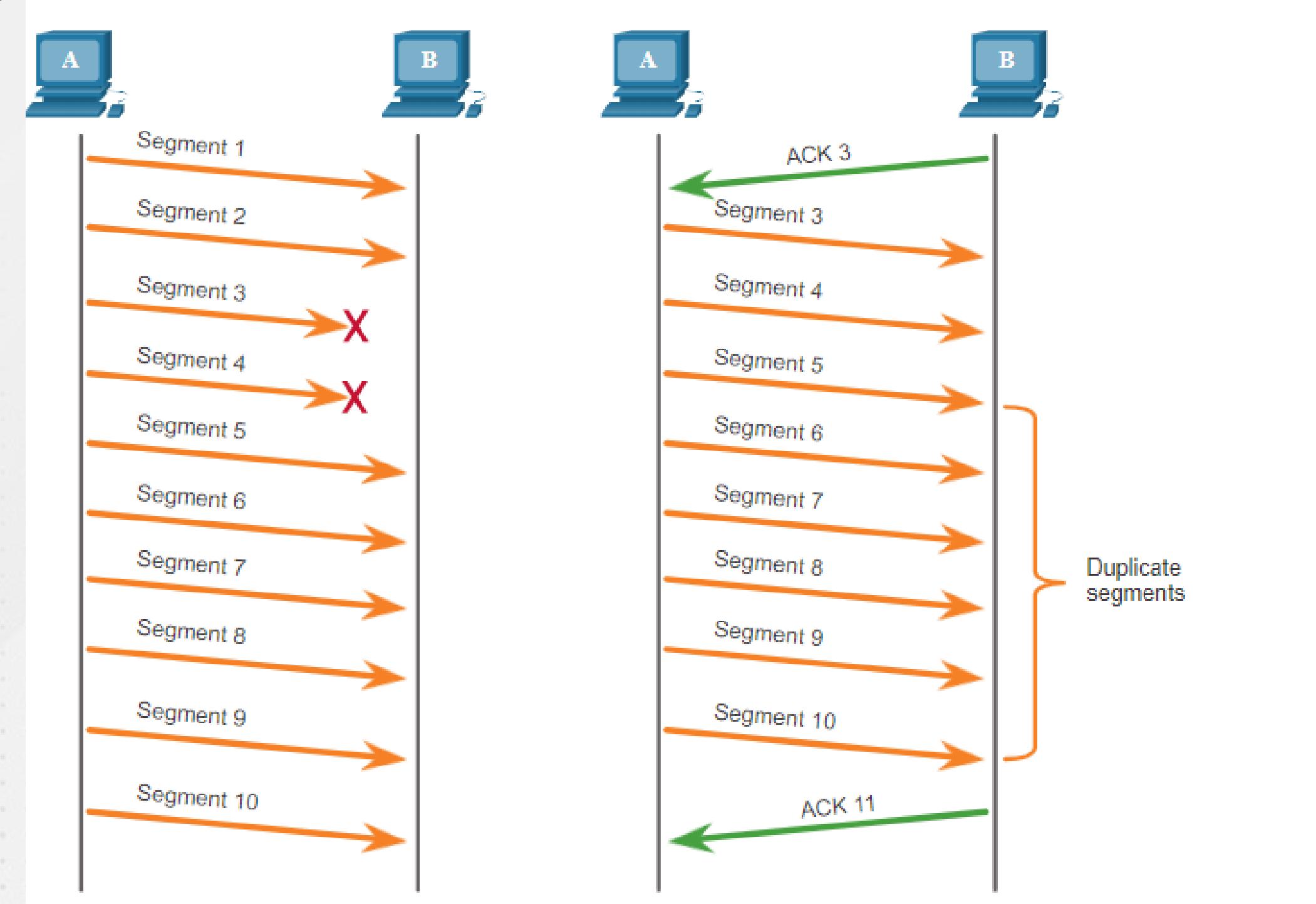


No importa cuán bien diseñada esté una red, ocasionalmente se produce la pérdida de datos.

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

Confiabilidad y control de flujo

Confiabilidad TCP — Pérdida y retransmisión de datos

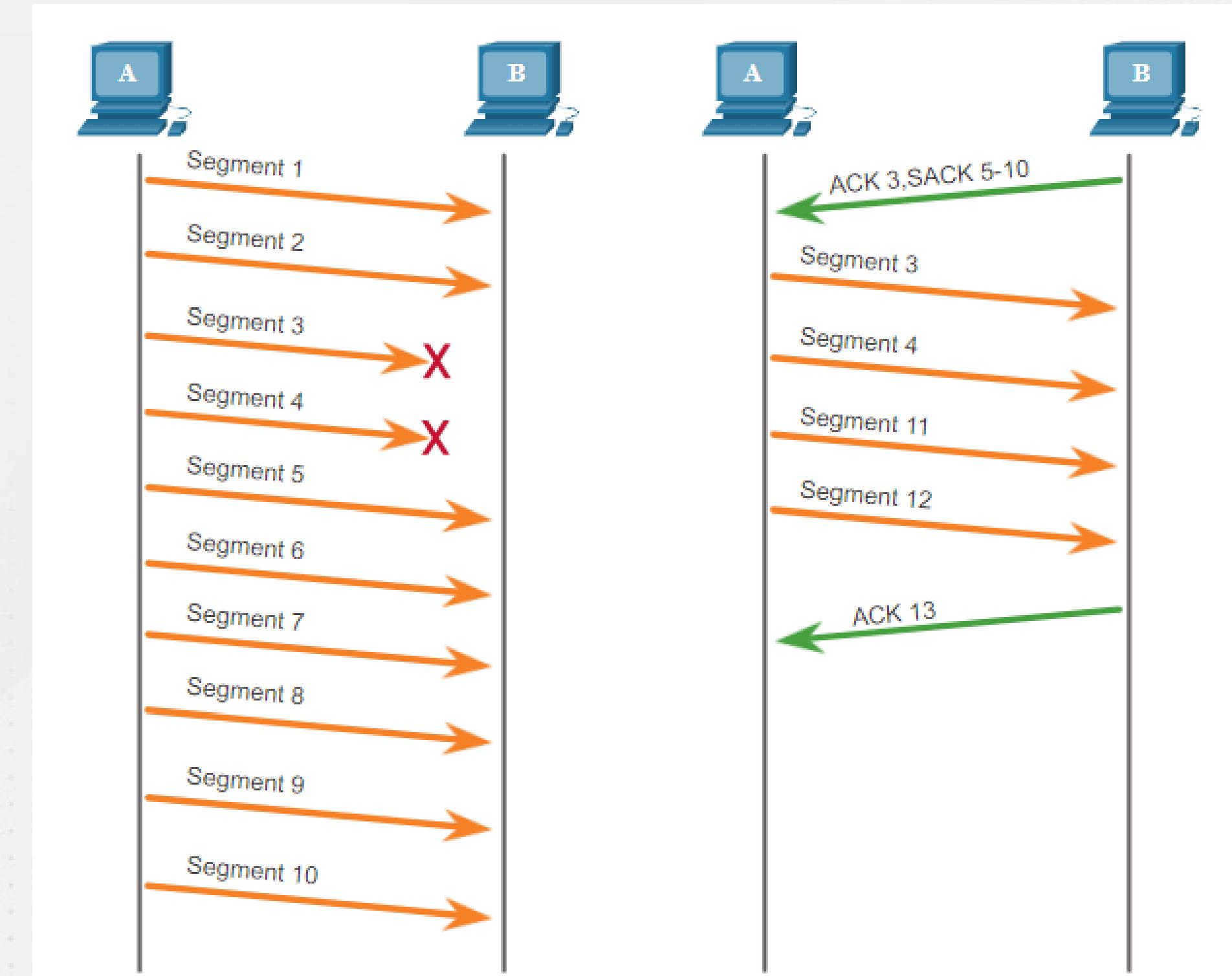




Confiabilidad TCP — Pérdida y retransmisión de datos

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.

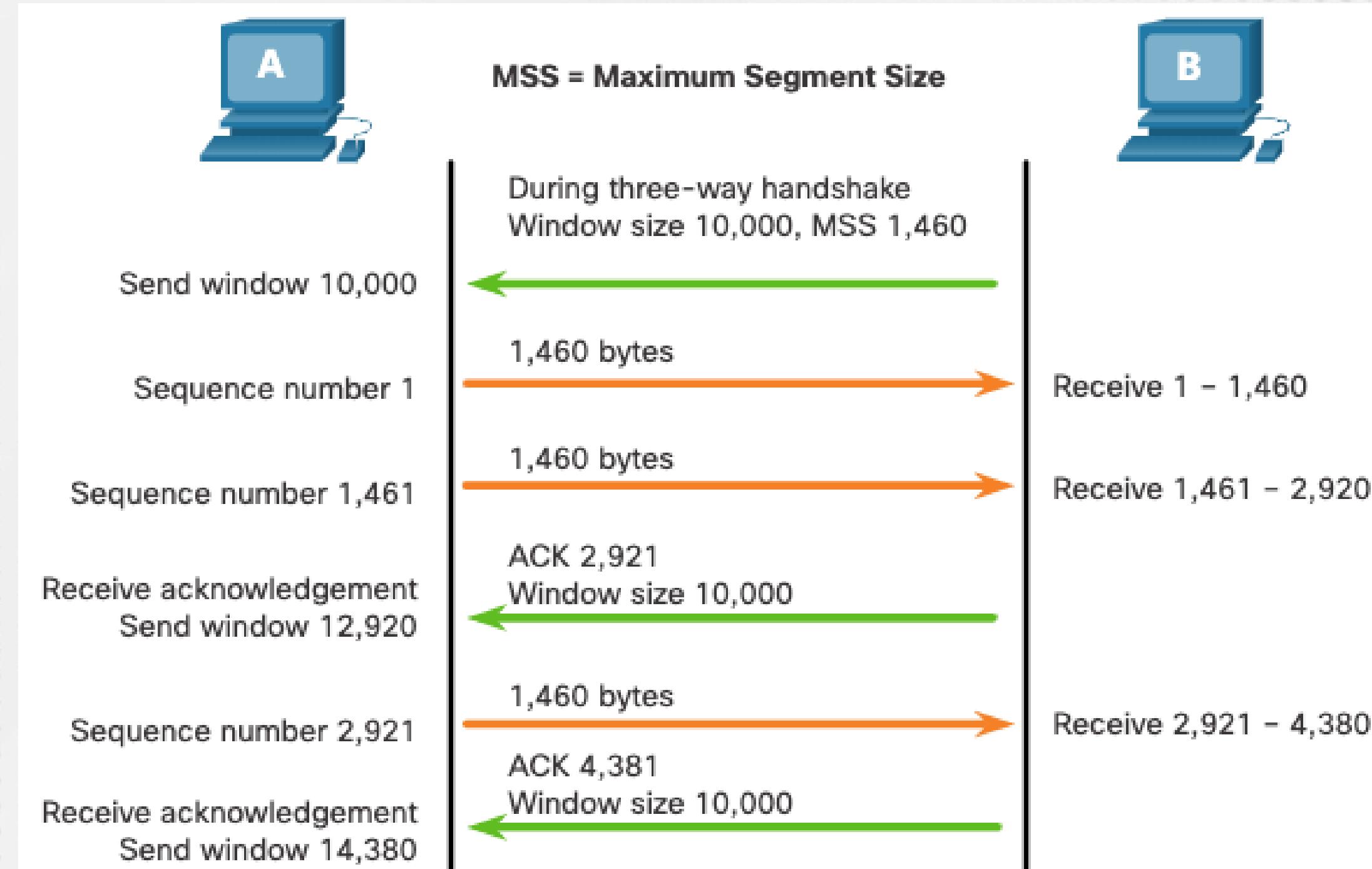


Control del flujo de TCP: tamaño de la ventana y reconocimientos



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.



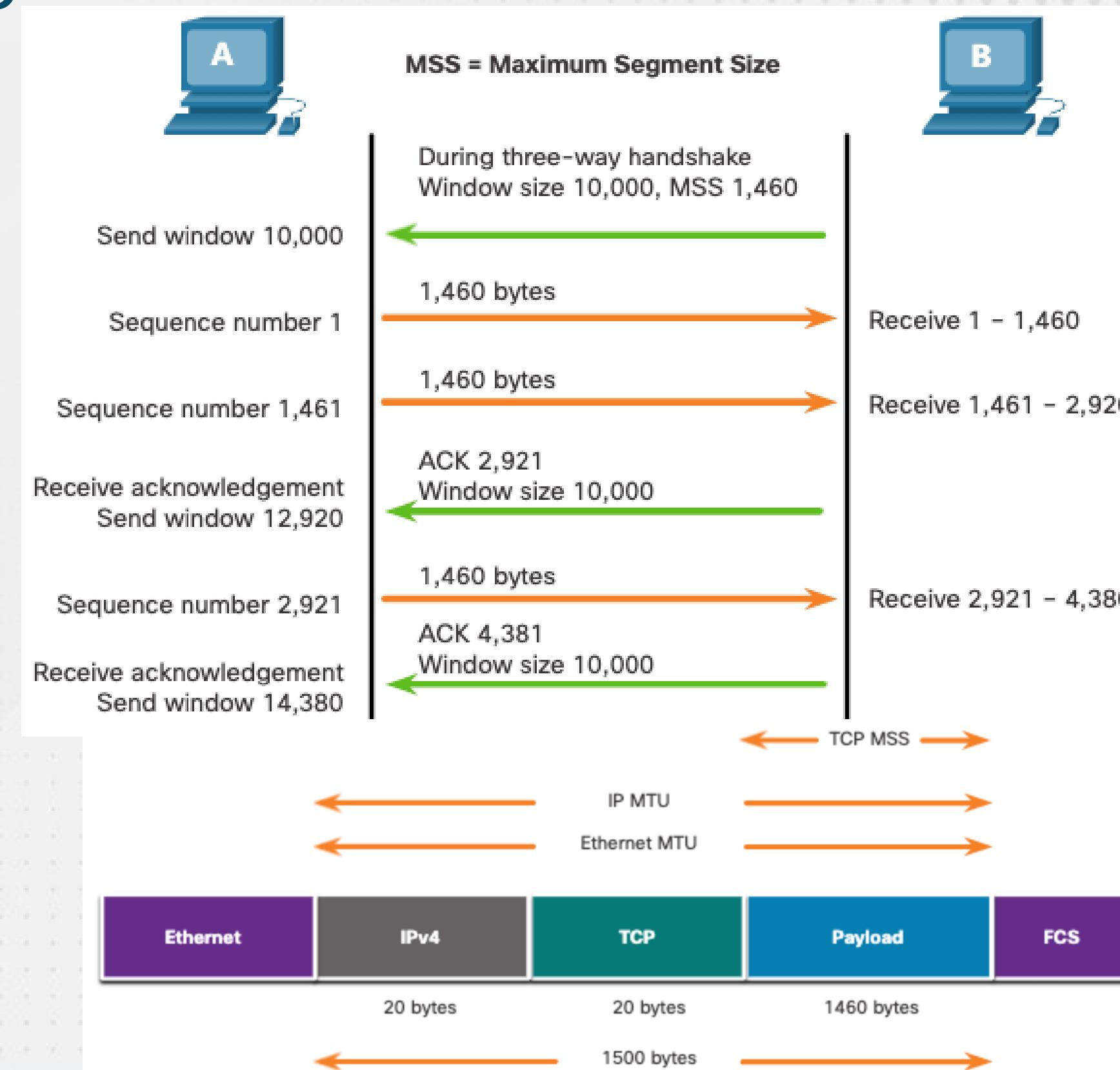


Tamaño máximo de segmento (MSS) es la cantidad máxima de datos que puede recibir el dispositivo de destino.

- 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.

Confiabilidad y control de flujo

TCP Control de flujo: tamaño máximo de segmento

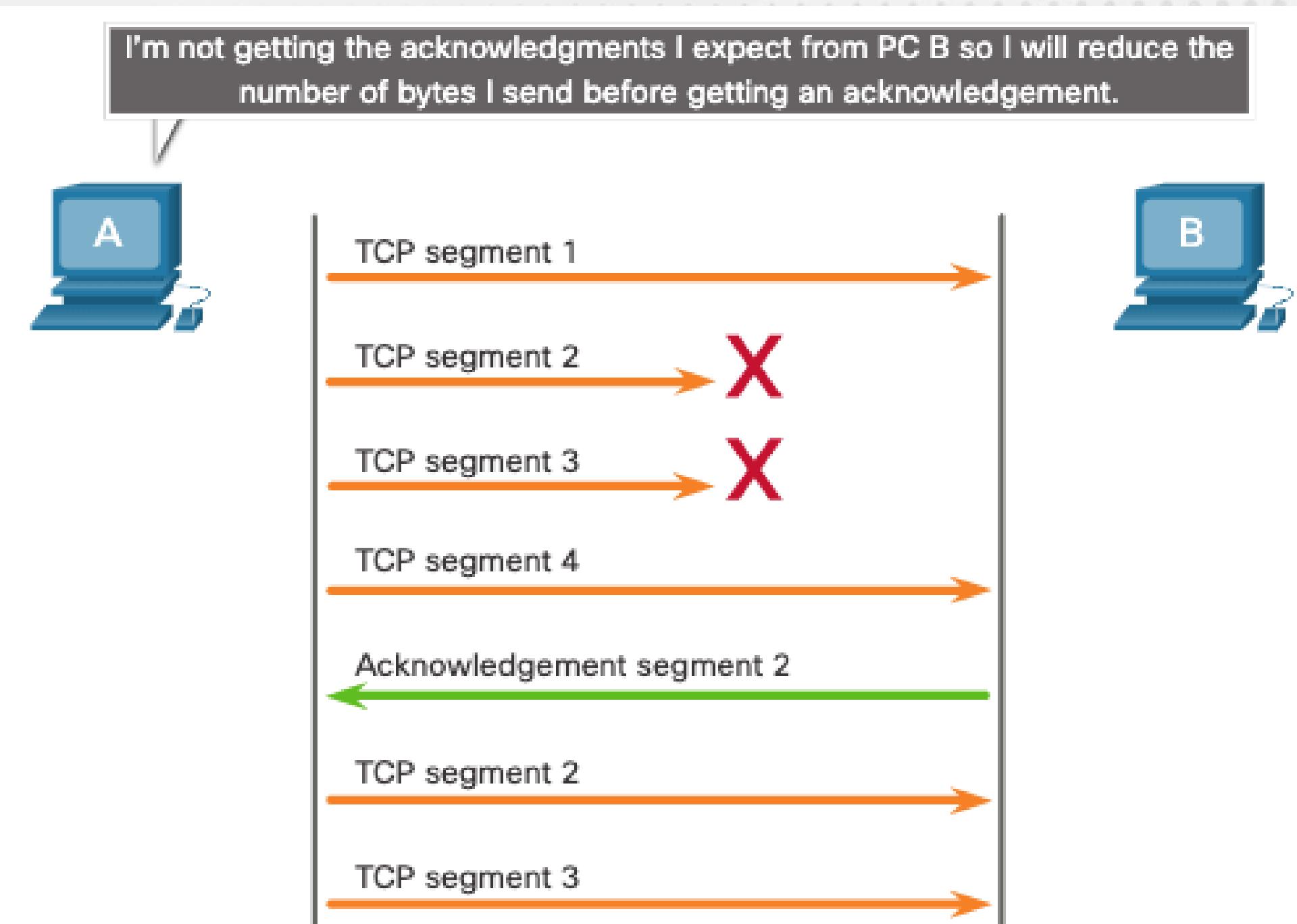




Confiabilidad y control de flujo Control del flujo de TCP: Prevención de congestiones

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.





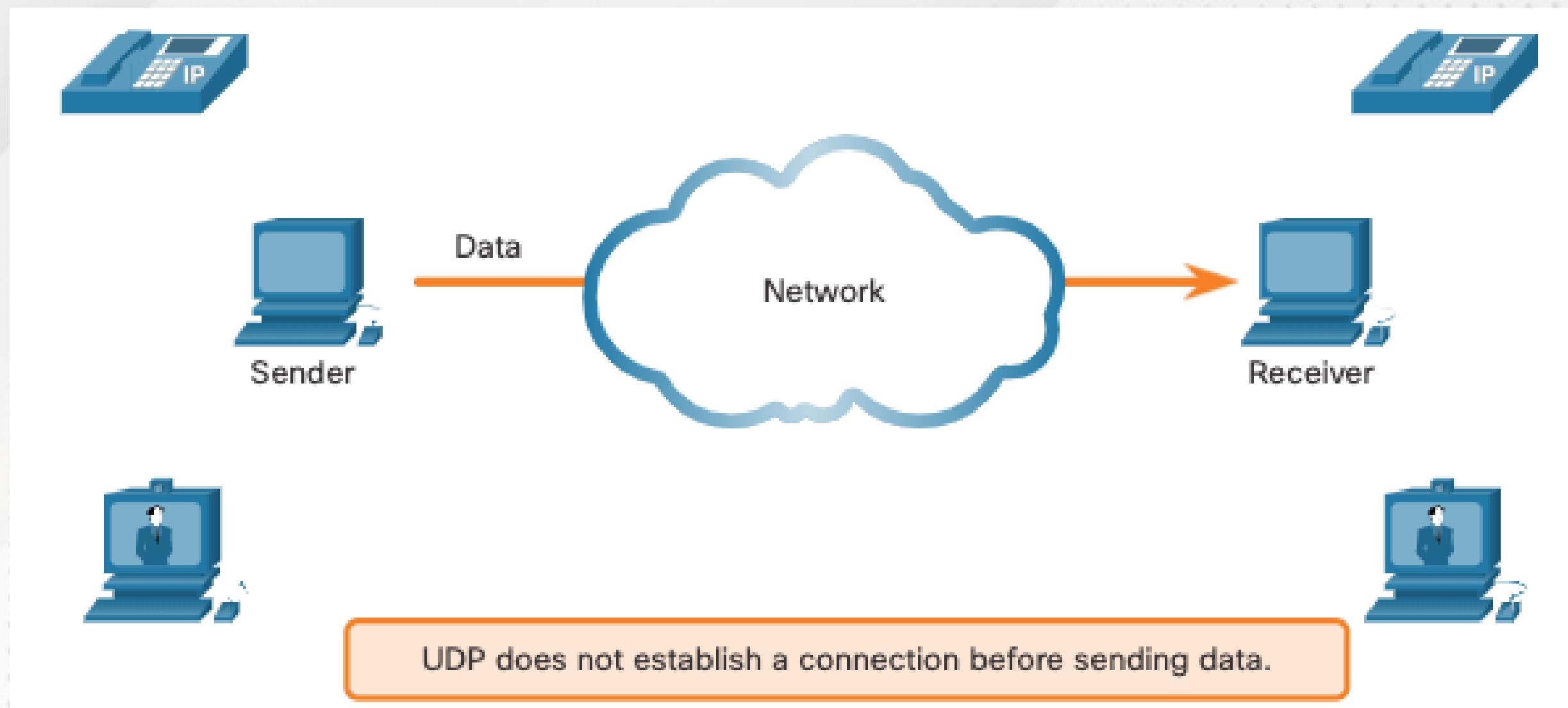
COMUNICACIÓN UDP

FORMANDO PROFESIONALES DE ÉLITE



Proceso de comunicación en UDP Comparación de baja sobrecarga y confiabilidad de UDP

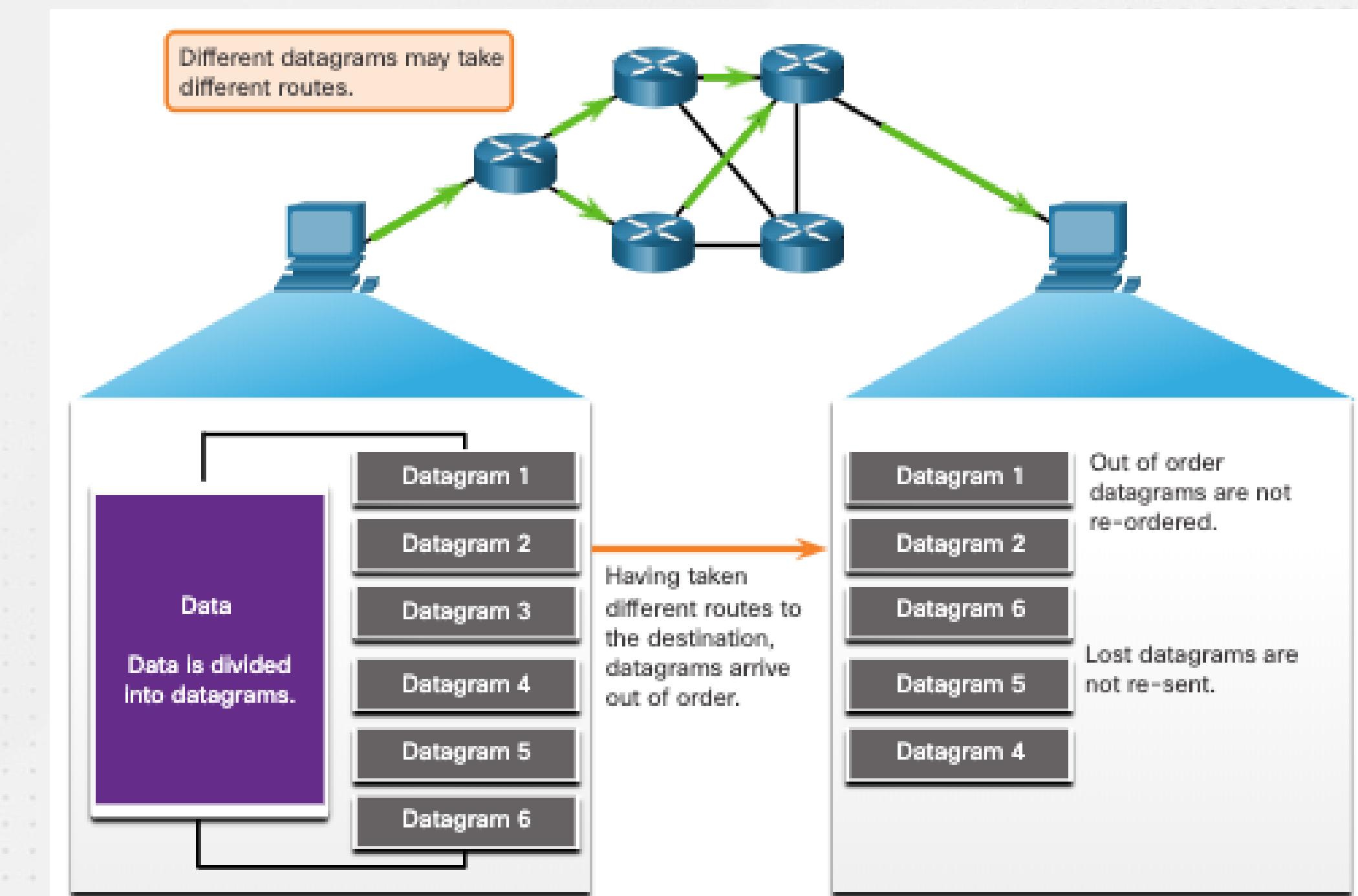
UDP no establece ninguna conexión. UDP suministra transporte de datos con baja sobrecarga debido a que posee un encabezado de datagrama pequeño sin tráfico de administración de red.





- 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 Rearmado de datagramas UDP



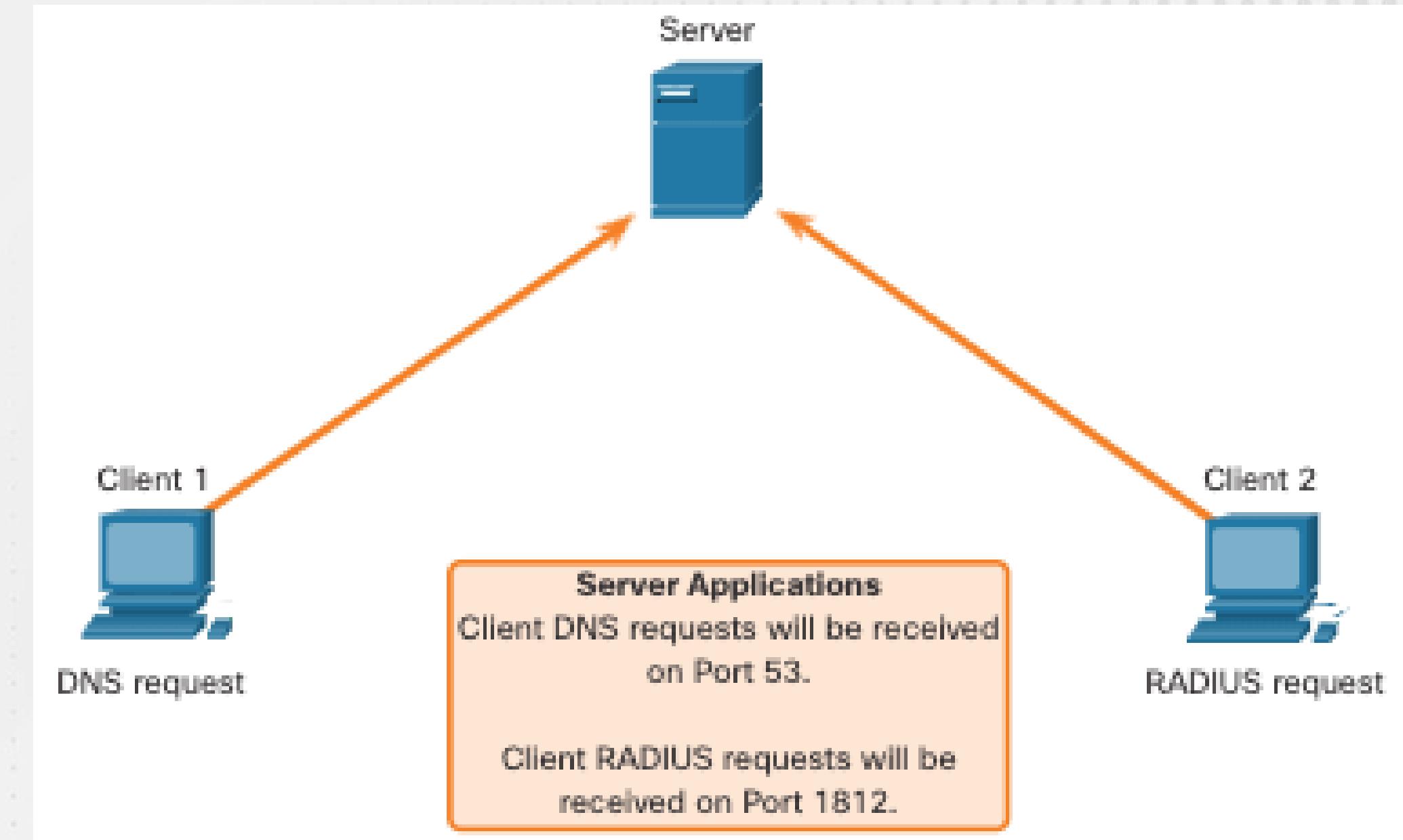


Proceso de comunicación en UDP

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.

