Arquitectura y Administración de Redes

Capa de Transporte

Ms. Ing. Jorge Jara A.

UPAO
UNIVERSIDAD PRIVADA ANTENOR ORREGO

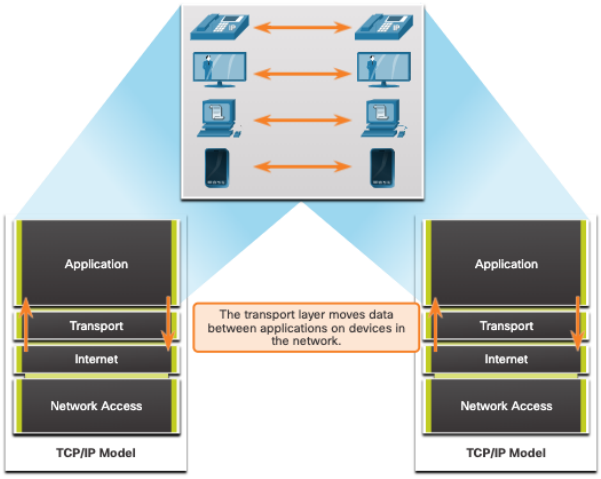
1.4.1 Transporte de datos

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.

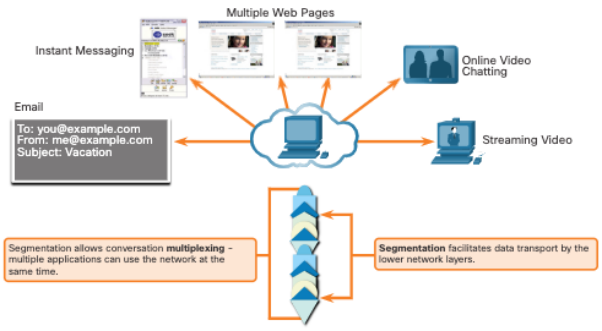


Transporte de datos

Tareas de la capa de transporte

La capa de transporte tiene las siguientes responsabilidades:

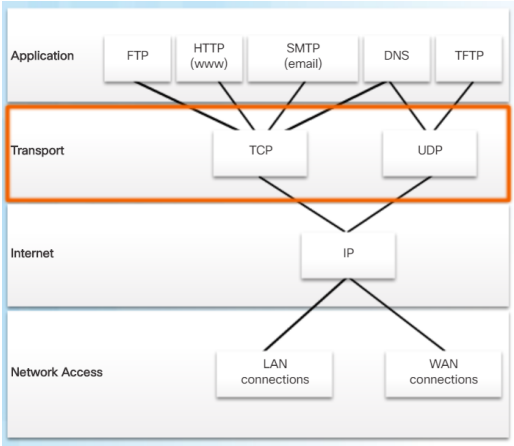
- Seguimiento de conversaciones individuales
- Segmentación de datos y rearmado de segmentos
- Agregar información de encabezado
- Identificar, separar y administrar múltiples conversaciones
- Utiliza segmentación y multiplexación para permitir que diferentes conversaciones de comunicación se intercalen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

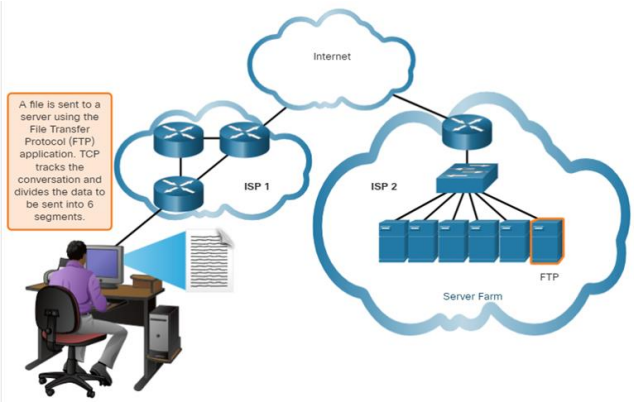


Transmission Control Protocol

(Protocolo de control de transmisión)

TCP provee confiabilidad y control de flujo Operaciones básicas TCP:

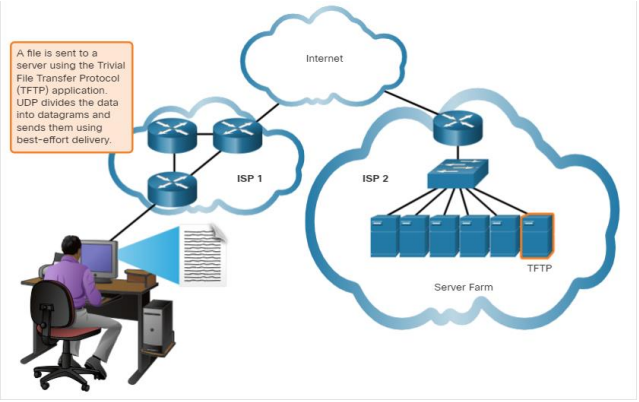
- Numere y rastree segmentos de datos transmitidos a un host específico desde una aplicación específica
- Confirmar datos recibidos
- Vuelva a transmitir cualquier información no reconocida después de un cierto período de tiempo
- Datos de secuencia que pueden llegar en un orden incorrecto
- Enviar datos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



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.

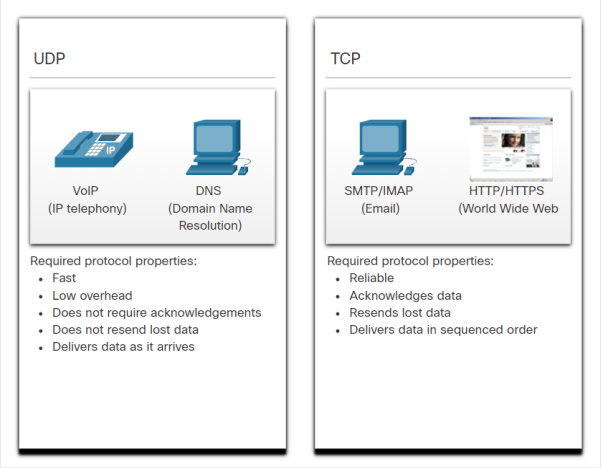


Transporte de datos

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.



14.2 Descripción general de TCP

Descripción general de TCP

Características de TCP

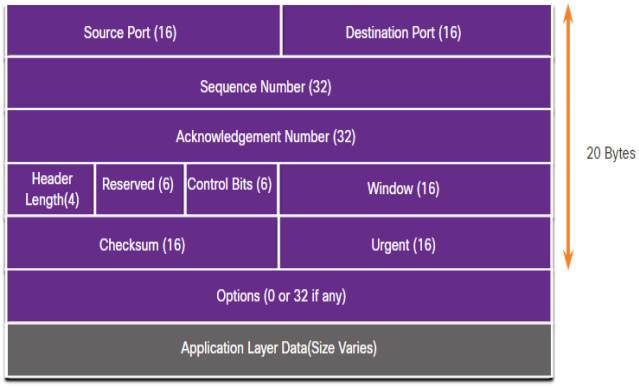
- **Establece una sesión** -TCP es un protocolo orientado a la conexión que negocia y establece una conexión permanente (o sesión) entre los dispositivos de origen y destino antes de reenviar cualquier tráfico.
- **Garantiza una entrega confiable**- Por muchas razones, es posible que un segmento se corrompa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

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

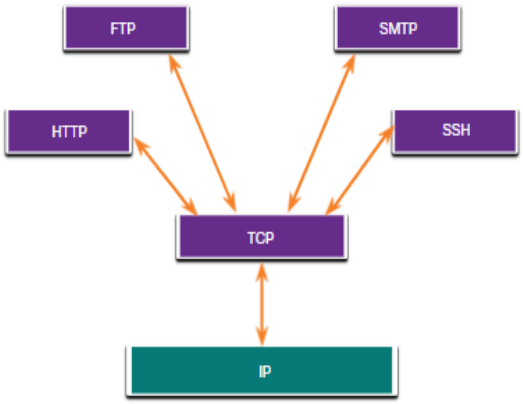
Campos de encabezado TCP

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.



14.3 Visión general de UDP

Descripción general de UDP

Características UDP

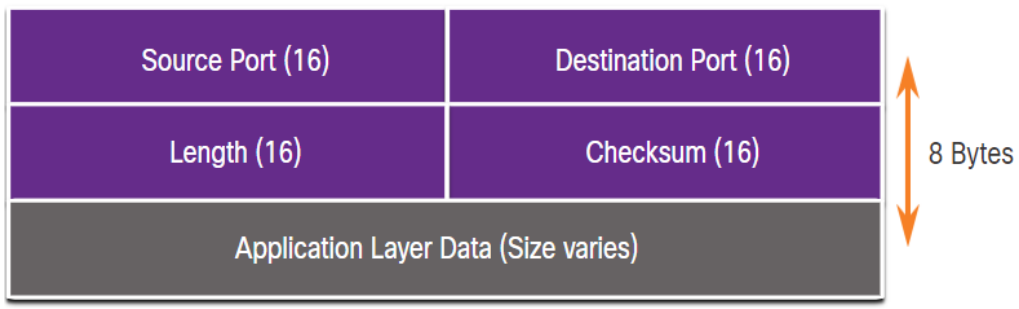
Las características UDP incluyen lo siguiente:

- 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

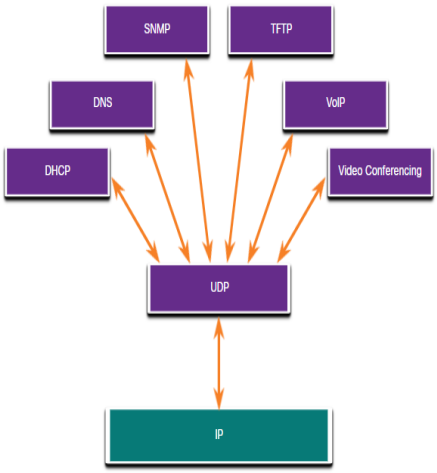
La tabla identifica y describe los cuatro campos de un encabezado UDP.

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 UDP

- 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.



14.4 Números de puerto

Números de puerto

Comunicaciones separadas múltiples

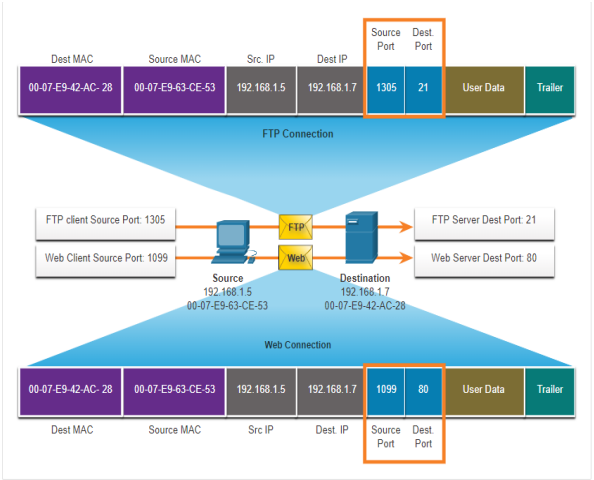
Los protocolos de capa de transporte TCP y UDP utilizan números de puerto para administrar múltiples conversaciones simultáneas.

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.

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**	•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**	•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**	•Estos puertos también se conocen como *puertos efímeros*. •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
```

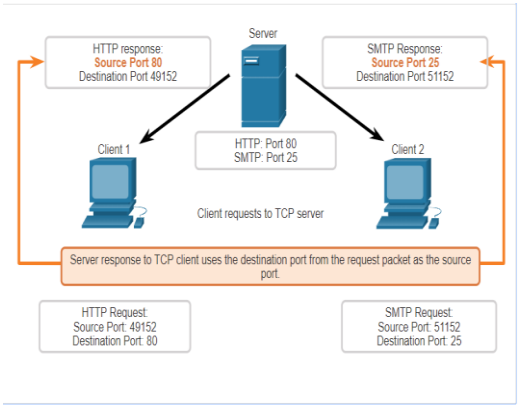
14.5 Proceso de comunicación en TCP

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.



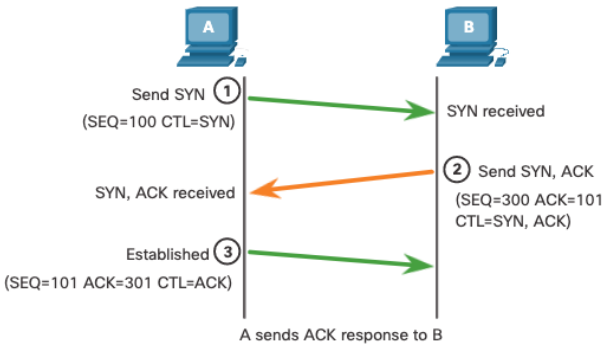
Proceso de comunicación en TCP

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

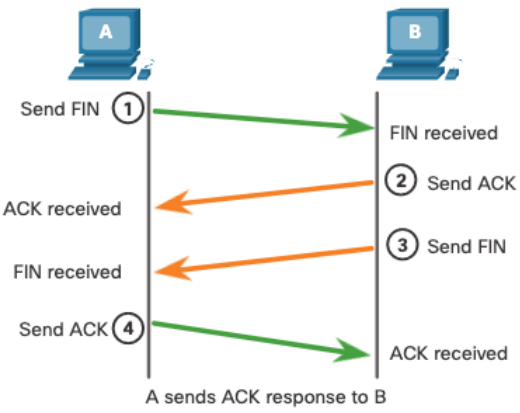
Finalización de la sesión TCP

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

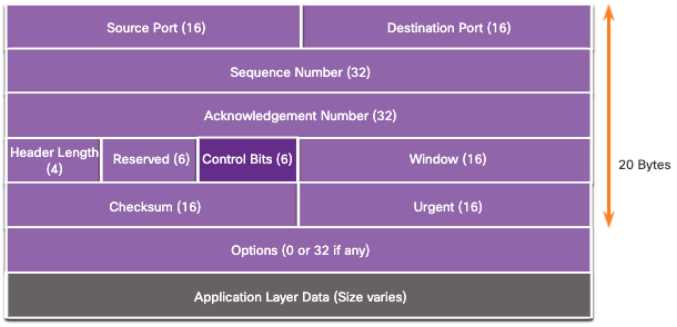
Una vez que se completa la comunicación, se cierran las sesiones y se finaliza la conexión. Los mecanismos de conexión y sesión habilitan la función de confiabilidad de TCP.

Proceso de comunicación en 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 session.

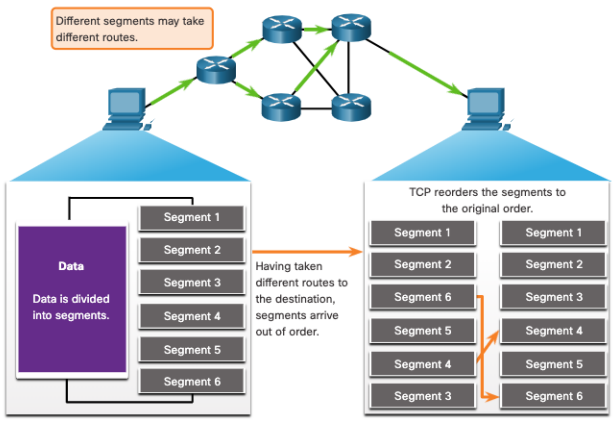


14.6 – Confiabilidad y control de flujo

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 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.

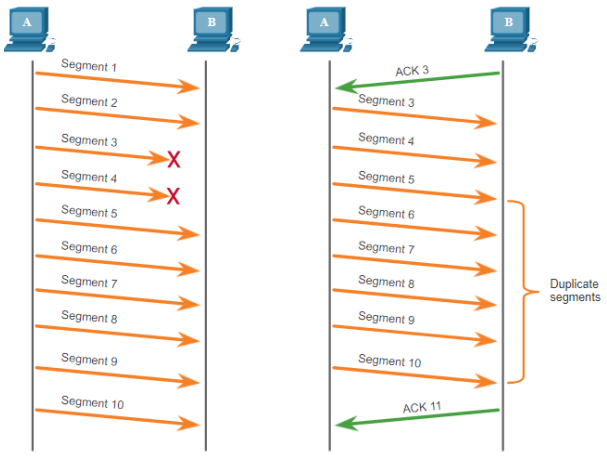


Confiabilidad y control de flujo

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.

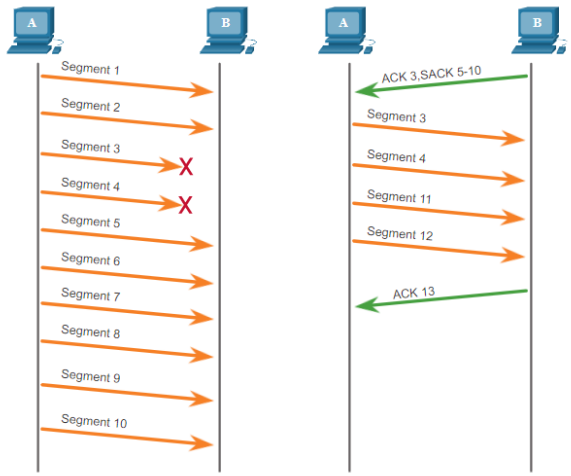


Confiabilidad y control de flujo

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.

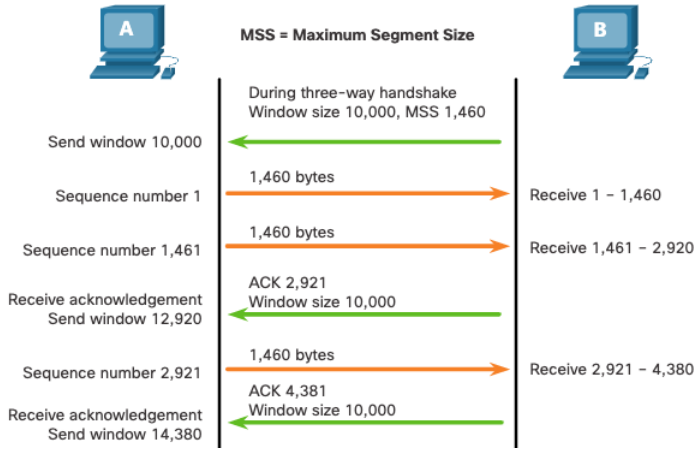


Confiabilidad y control de flujo

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.

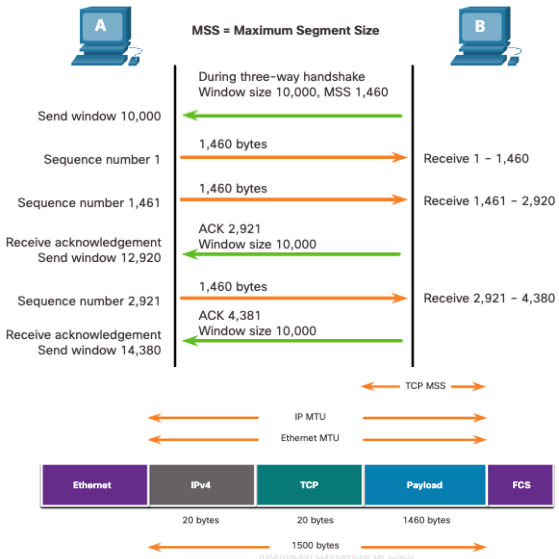


Confiabilidad y control de flujo

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.

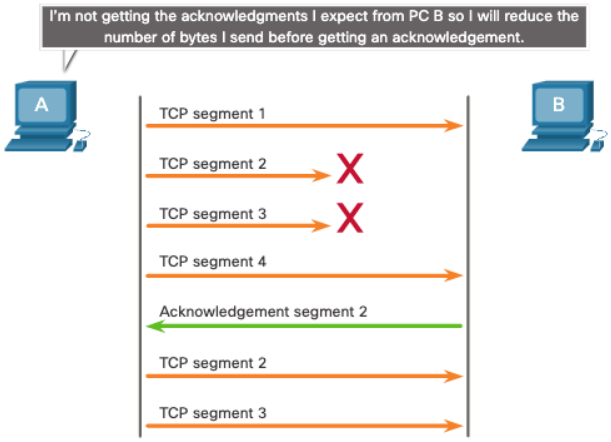


Confiabilidad y control de flujo

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.

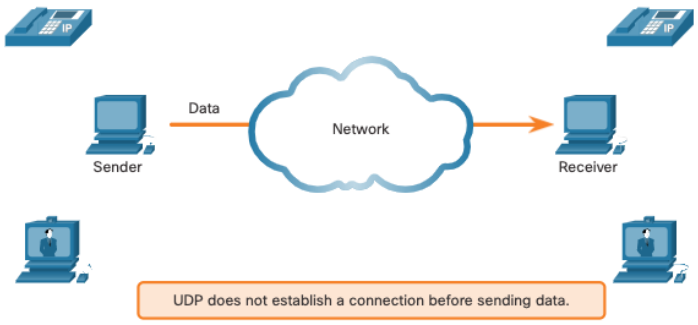


14.7 Comunicación UDP

Proceso de comunicación en UDP

Comparación de baja sobrecarga y confiabilidad de UDP

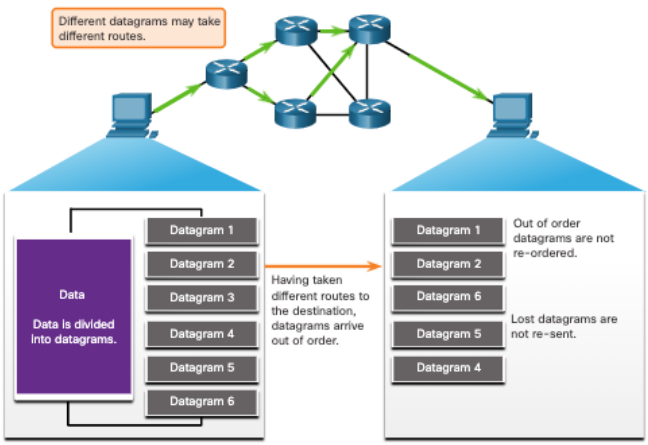
UDP no establece ninguna conexión. UDP suministra transporte de datos con baja sobrecarga debido a que posee un encabezado de datagrama pequeño sin tráfico de administración de red.



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.

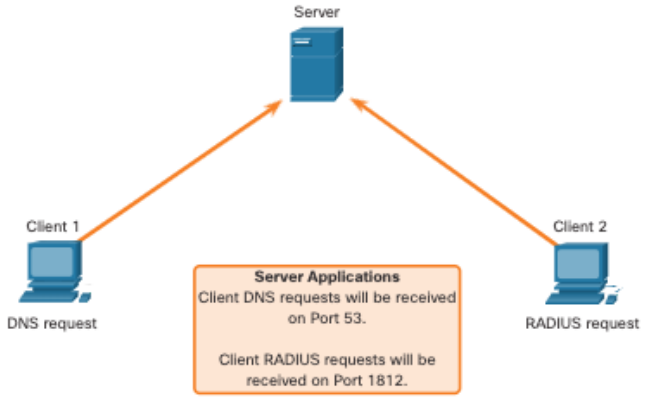


Proceso de comunicación en UDP

Procesos y solicitudes de servidores UDP

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

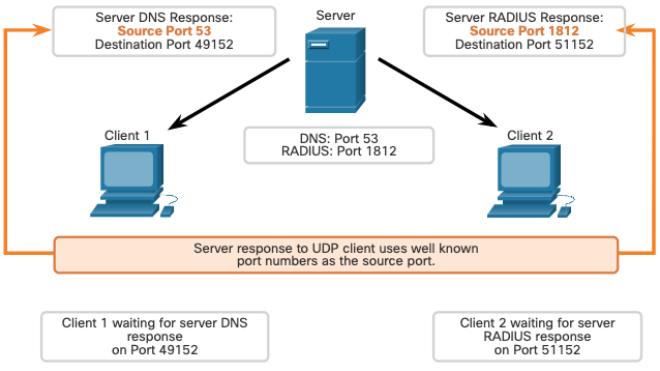
UDP recibe un datagrama destinado a uno de esos puertos, envía los datos de aplicación a la aplicación adecuada en base a su número de puerto.



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.




CISCO