



Sé Íntegro Sé Misionero Sé Innovador

Capa de transporte

Integrantes:

- Dany Haro Ortiz
- Franco Cabanillas
- Aldair Sanchez
- Enrique Matencio
- Mijail Palomino



Sé Íntegro Sé Misionero Sé Innovador

Protocolos de capa de transporte

Función de la capa de transporte

Es responsable de establecer una sesión de comunicación temporal entre dos aplicaciones y de transmitir datos entre ellas. El enlace entre las capas de aplicación y las capas inferiores que se encargan de la transmisión a través de la red.

Tareas:

Seguimiento de las conversaciones: realiza un seguimiento de cada conversación individual que fluye entre una aplicación de origen y una de destino.

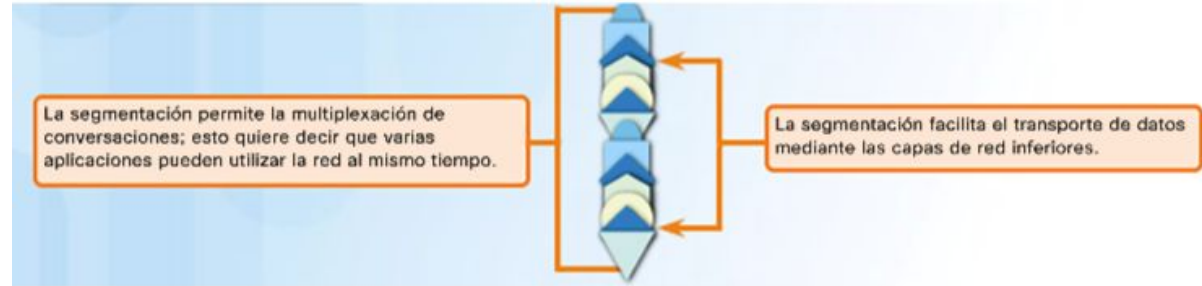
Segmentación: divide los datos en segmentos que son más fáciles de administrar y de transportar. El encabezado, que se utiliza para el rearmado, se utiliza para el seguimiento.

Identificación de la aplicación: garantiza que, aunque sean varias las aplicaciones que se ejecuten en un dispositivo, todas reciban los datos correctos a través de los números de puerto.



Multiplexación de conversaciones

La segmentación de los datos en partes más pequeñas permite que se multiplexen muchas comunicaciones distintas en la misma red.



Confiabilidad de la capa de transporte

El TCP/IP proporciona dos protocolos de capa de transporte:

Protocolo de control de transmisión(TCP):

Confiable y asegura que todos los datos lleguen al destino. (Mayor tamaño y demora).

Protocolo de datagramas de usuario(UDP):

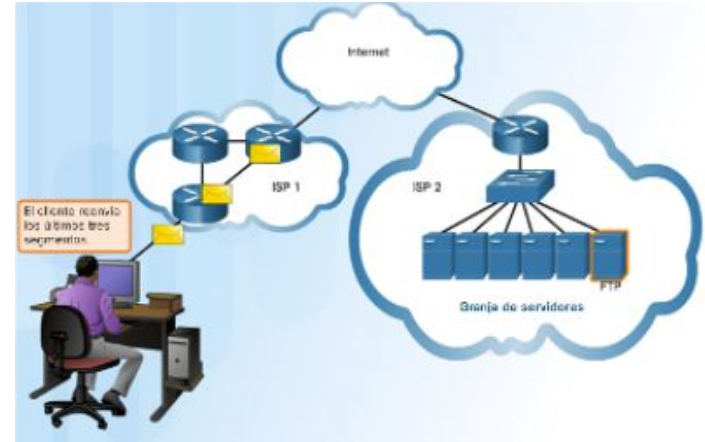
No proporciona confiabilidad, debido a que tiene menos campos.(Más rápido)

Transporte de datos TCP

El transporte del TCP es similar a enviar paquetes con seguimiento. Si se divide un pedido de envío en varios paquetes, el cliente puede revisar en línea el orden de la entrega.

Funciones:

- Numeración y seguimiento de segmentos de datos
- Reconocimiento de los datos recibidos
- Retransmisión de los datos sin reconocimiento después de un tiempo determinado



Transporte de datos UDP

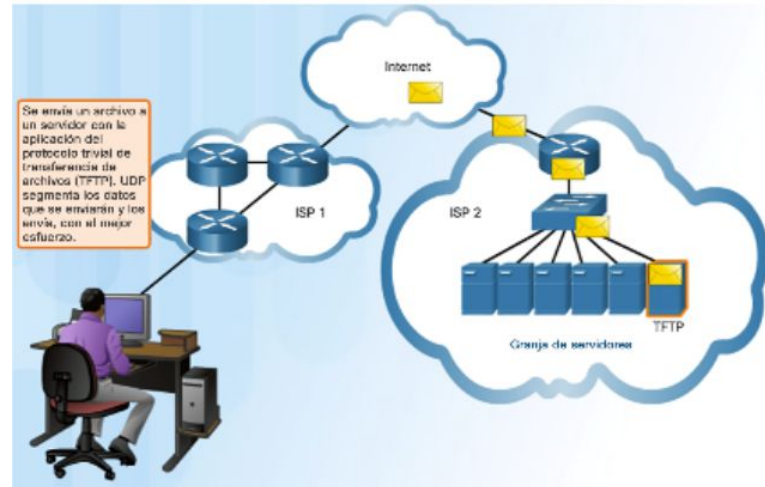
Utiliza UDP para menos sobrecarga y para reducir las posibles demoras.

Funciones:

Entrega de mejor esfuerzo (no confiable)

Ningún reconocimiento

Similar a una carta no certificada



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

UDP



Telefonía IP



Transmisión de
video en vivo

Propiedades de protocolo requeridas:

- Rápido
- Baja sobrecarga
- No requiere reconocimiento
- No reenvía los datos perdidos
- Entrega los datos a medida que llegan

Si uno o dos segmentos de una transmisión de video en vivo no llegan, si se interrumpe la transmisión, es posible que no sea perceptible para el usuario.

TCP



SMTP/POP
(correo electrónico)



HTTP

Propiedades de protocolo requeridas:

- Confiable
- Reconoce los datos
- Reenvía los datos perdidos
- Entrega los datos en orden secuencial

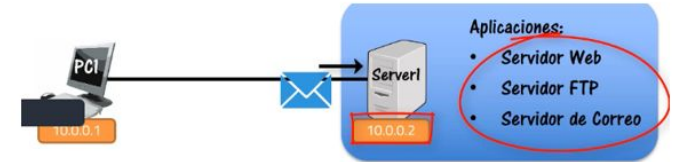
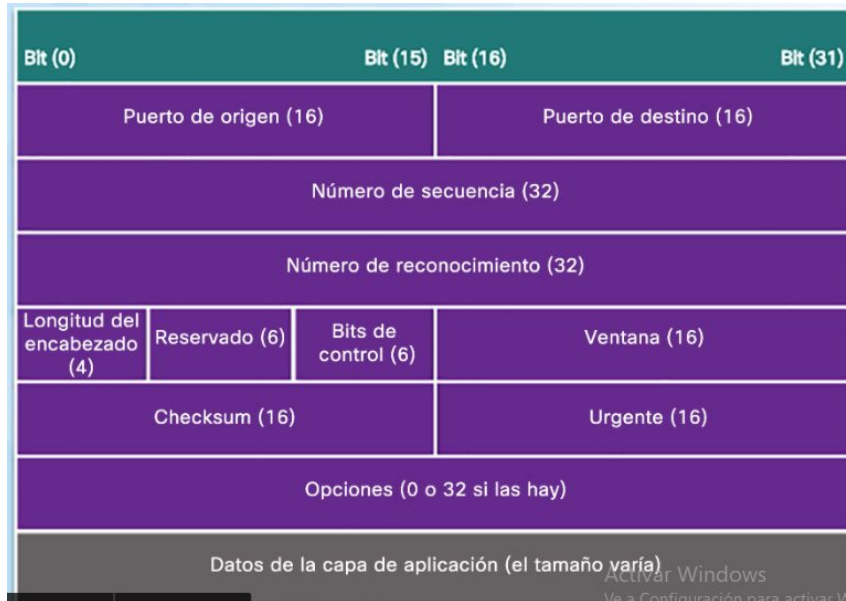
Las bases de datos, los navegadores web y los clientes de correo electrónico requieren que todos los datos que se envían lleguen a destino en su formato original.

Características de TCP

- Establecimiento de una sesión
 - Protocolo orientado a la conexión
 - Garantiza que la aplicación está lista para recibir datos
 - Negocia la cantidad de tráfico que se puede reenviar en un momento determinado
- Entrega confiable
 - Asegura que cada segmento que envía el origen llegue al destino
- Entrega en el mismo orden
 - La numeración y la secuencia de los segmentos garantiza el rearmado en el orden correcto
- Control de flujo
 - Regula la cantidad de datos que transmite la fuente

ENCABEZADO TCP

- El puerto origen y destino se usa para identificar la aplicación
- El número de secuencia se usa para el rearmada de datos
- Longitud del encabezado del segmento TCP
- Ventana indica la cantidad de bytes que se puede aceptar por vez



Usando el puerto de cada aplicación, cada aplicación tiene un puerto.



ENCABEZADO

TCP

Para saber a qué aplicación (servidor web, servidor FTP, servidor de correo) va destinado utilizamos un identificador en la cabecera, en la capa de transporte que es el puerto.

Nº de puertos y protocolos.

```
> Frame 160: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits) on interface \Device\NPF_{E63AED1E-895C-4B5C-95C1-2C48FABD6A58}, id 0
> Ethernet II, Src: LiteonTe_de:16:9b (98:22:ef:de:16:9b), Dst: AskeyCom_25:d1:30 (7c:db:98:25:d1:30)
> Internet Protocol Version 6, Src: 2001:1388:70c0:442:10e9:3a1:888f:985a, Dst: 2800:240:a:18f::1771
> Transmission Control Protocol, Src Port: 53825, Dst Port: 80, Seq: 1, Ack: 1, Len: 442
< Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.godaddy.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: es-ES,es;q=0.9,en;q=0.8\r\n
```

Nº DE PUERTO	PROTOCOLO	APLICACIÓN
7	TCP	Echo
7	UDP	Echo
20	TCP	File Transfer
21	TCP	FTP Control
23	TCP	Telnet
25	TCP	Simple Mail Transfer
53	TCP	Domain Name
53	UDP	Domain Name Server
66	UDP	DHCP Server
67	UDP	DHCP Client
69	UDP	Trivial File Transfer
80	TCP	HTTP
143	TCP	Internet Message Access Protocol (IMAP4)
161	UDP	SNMP
179	TCP	Border Gateway Protocol (BGP)
443	TCP	SSL
443	UDP	SSL
514	UDP	SYSLOG

RFC 1700

ENCABEZADO UDP

- UDP (Protocolo de datagramas de usuario)



- Permite el envío de datagramas sin establecer previamente una conexión.
- Información mínima en el encabezado
- No tiene confirmación – no confiable
- No permite el control de flujo
- No ordena
- No segmenta



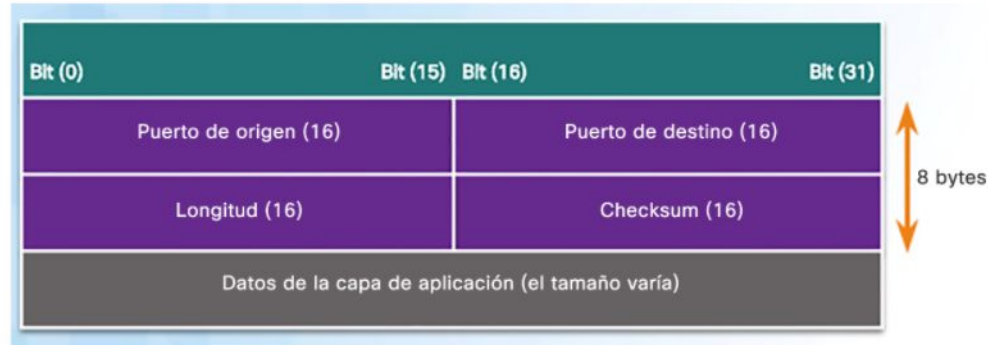
Conversación separadas multiples

El TCP y UDP administran múltiples conversaciones mediante los identificadores únicos que son los Puertos

PUERTO ORIGEN: puerto origen de la aplicación que es generado dinámicamente

PUERTO DESTINO: Servicio que se solicita

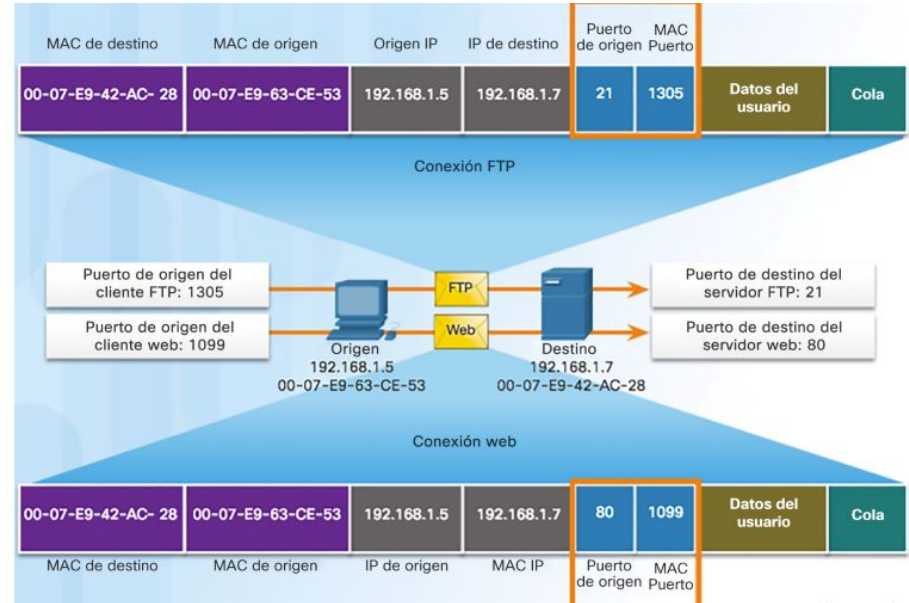
- UDP es un protocolo sin información de estado, sin seguimiento.



Pares de socket

Un socket queda definido por un par de direcciones IP local y remota, un protocolo de transporte y un par de números de puerto local y remoto.

- El puerto origen y destino se incluye en el segmento.
- Ip y número de puerto = socket
- El puerto origen funciona como dirección de retorno



Grupos de números de puerto

- Puertos conocidos (números del 0 al 1023): estos números se reservan para servicios y aplicaciones.
- Puertos registrados (números del 1024 al 49 151): IANA asigna estos números de puerto a una entidad que los solicite para utilizar con procesos o aplicaciones específicos.
- Puertos dinámicos o privados (números 49 152 a 65 535): en general, el sistema operativo del cliente los asigna dinámicamente y los utiliza para identificar la aplicación del cliente durante la comunicación.

NETSTAT: muestra un listado de las conexiones activas de una computadora

Información del estado de las conexiones

NETSTAT devuelve una serie de parámetros que indican el estado en que se encuentran las conexiones, son los siguientes:

LISTENING:	El puerto está abierto escuchando en espera de una conexión.
ESTABLISHED:	La conexión ha sido establecida.
CLOSE_WAIT:	La conexión sigue abierta, pero el otro extremo nos comunica que no se continuará enviando información.
TIME_WAIT:	La conexión ha sido cerrada, pero no se elimina de la tabla de conexión por si hay algo pendiente de recibir.
LAST_ACK:	La conexión se está cerrando.
CLOSED:	La conexión ha sido cerrada completamente.

UPeU | UNIVERSIDAD
PERUANA UNIÓN

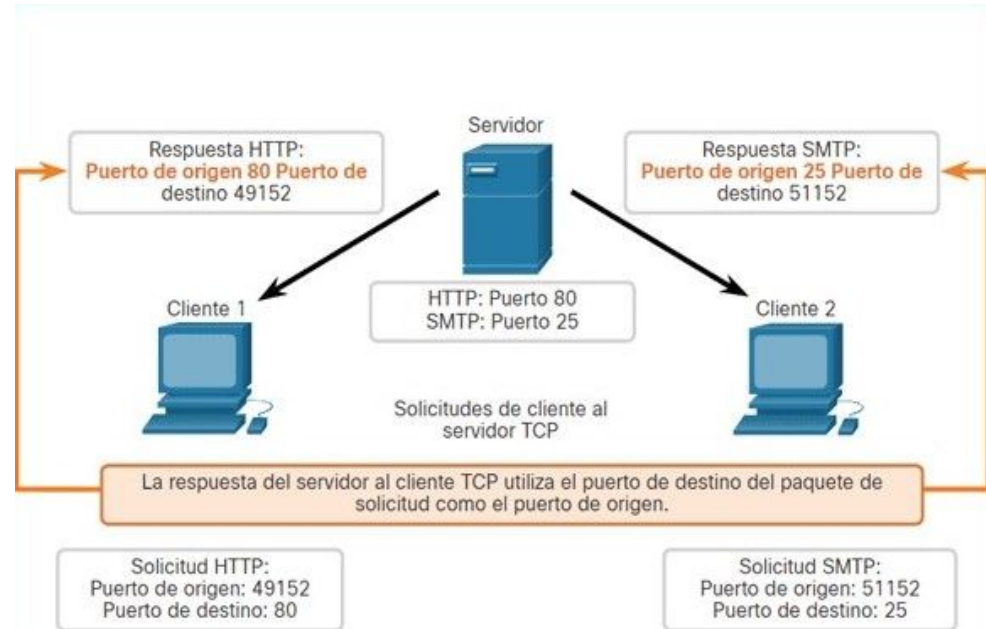
Sé Íntegro **Sé** Misionero **Sé** Innovador

TCP y UDP

Proceso de comunicación en TCP

Proceso del servidor TCP

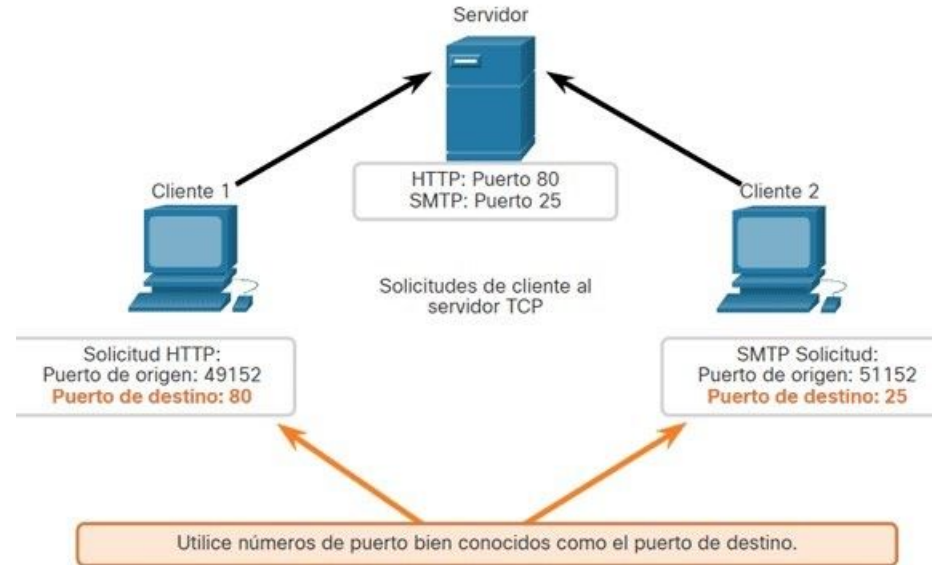
El cliente 1 solicita servicios web y el cliente 2 solicita servicio de correo electrónico utilizando puertos conocidos (es decir, servicios web es puerto 80, servicios de correo electrónico es puerto 25).



Proceso de comunicación en TCP

Proceso del servidor TCP

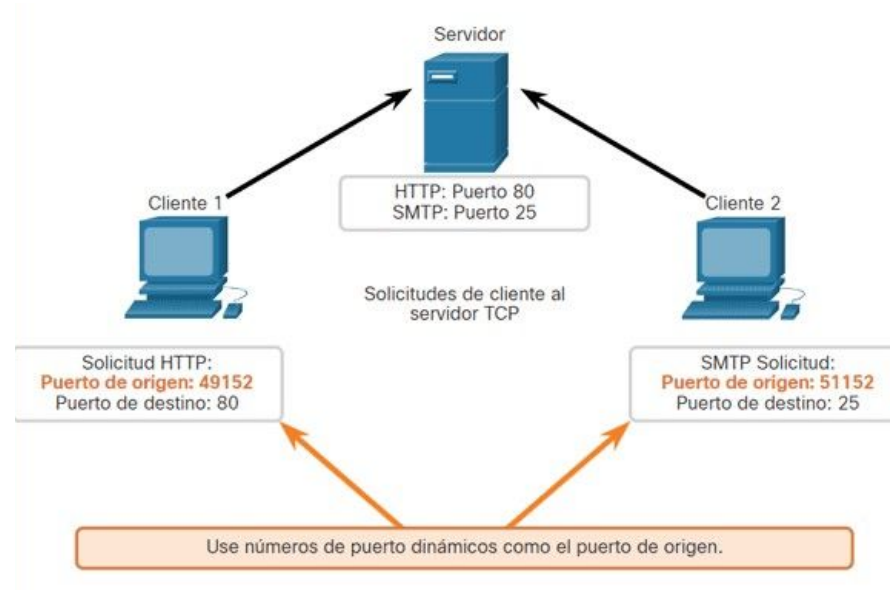
Las solicitudes generan dinámicamente un número de puerto de origen. En este caso, el Cliente 1 está utilizando el puerto de origen 49152 y el Cliente 2 está utilizando el puerto de origen 51152.



Proceso de comunicación en TCP

Proceso del servidor TCP

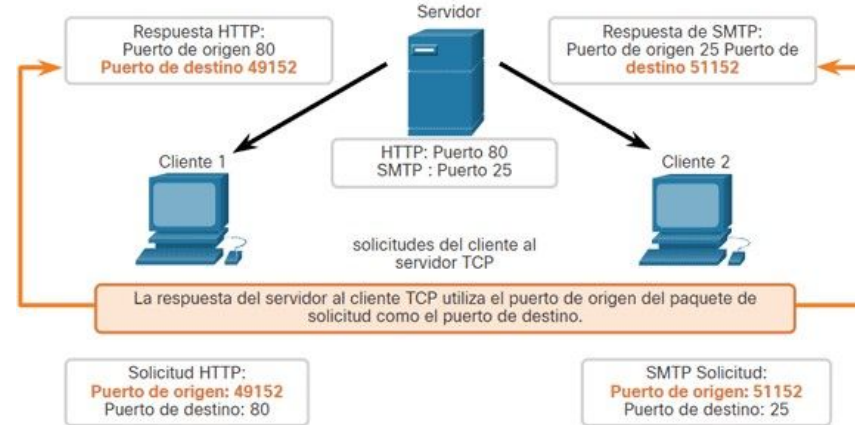
Cuando el servidor responde a las solicitudes del cliente, invierte el destino y los puertos de origen de la solicitud inicial.



Proceso de comunicación en TCP

Proceso del servidor TCP

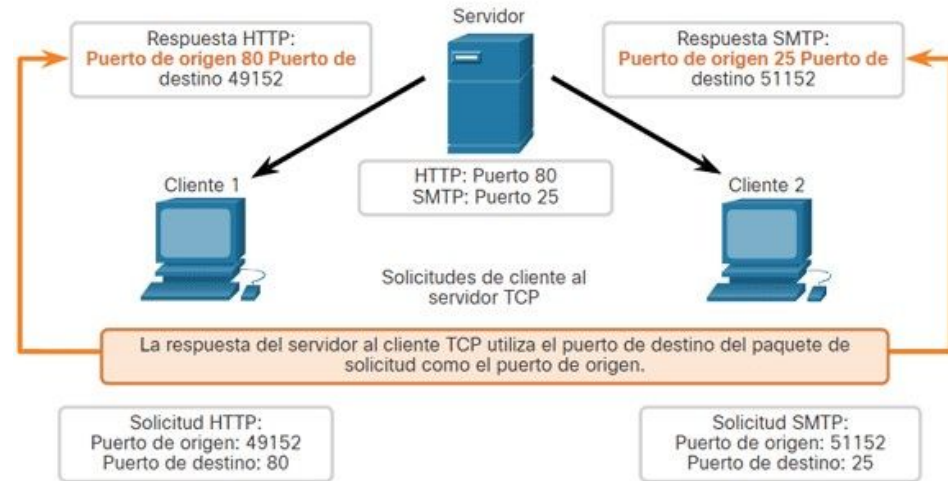
Observa que la respuesta del servidor a la solicitud web ahora tiene el puerto de destino 49152 y la respuesta de correo electrónico ahora tiene el puerto de destino 51152.



Proceso de comunicación en TCP

Proceso del servidor TCP

El puerto de origen en la respuesta del servidor es el puerto de destino original en las solicitudes iniciales.



Proceso de comunicación en TCP

Análisis del protocolo TCP de enlace de tres vías

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

Comunicación TCP

Protocolo TCP de enlace de tres vías: paso 1

Paso 1: el cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor

Protocolo TCP de enlace de tres vías (SYN)

No.	Time	Source	Destination
10	16.303490	10.1.1.1	192.168.254.254
11	16.304896	192.168.254.254	10.1.1.1
12	16.304925	10.1.1.1	192.168.254.254
13	16.305153	10.1.1.1	192.168.254.254
14	16.307875	192.168.254.254	10.1.1.1

Frame 10: 62 bytes on wire (496 bits), 62 bytes captured on interface 0

- Ethernet II, Src: vmware_be:62:88 (00:50:56:be:62:88), Dst: 02:00:00:00:00:00
- Internet Protocol Version 4, Src: 10.1.1.1, Destination: 192.168.254.254
- Transmission Control Protocol, Src Port: kiosk (1061), Dst Port: http (80)
 - Source port: kiosk (1061)
 - Destination port: http (80)

Un analizador de protocolos muestra la solicitud del cliente inicial para la sesión en la trama 10

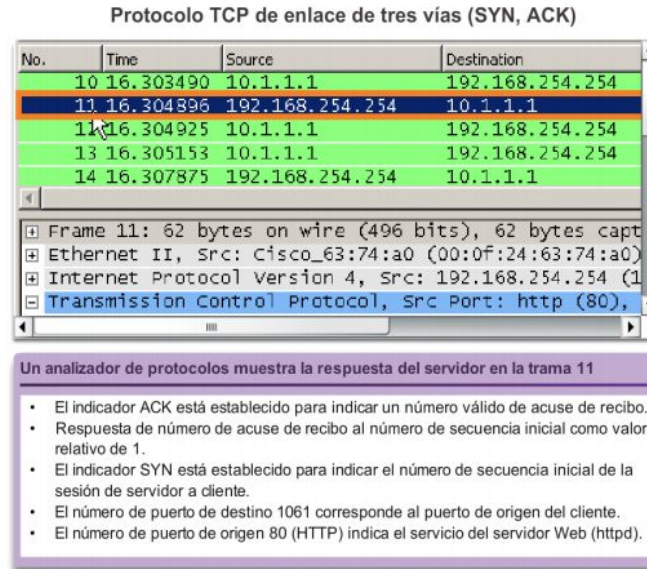
En el segmento TCP de esta trama se muestra lo siguiente:

- El indicador SYN está establecido para validar un número de secuencia inicial.
- El número de secuencia seleccionado aleatoriamente es válido (el valor relativo es 0).
- El puerto de origen aleatorio es 1061.

Comunicación TCP

Protocolo TCP de enlace de tres vías: paso 2

Paso 2: el servidor reconoce la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.



Comunicación TCP

Protocolo TCP de enlace de tres vías: paso 3

Paso 3: el cliente de origen reconoce la sesión de comunicación de servidor a cliente.

Protocolo TCP de enlace de tres vías (ACK)

No.	Time	Source	Destination
10	16.303490	10.1.1.1	192.168.254.254
11	16.304896	192.168.254.254	10.1.1.1
12	16.304925	10.1.1.1	192.168.254.254
13	16.305153	10.1.1.1	192.168.254.254
14	16.307875	192.168.254.254	10.1.1.1

Frame 12: 54 bytes on wire (432 bits), 54 bytes captured on interface 0

Ethernet II, Src: Vmware_b8:62:88 (00:50:56:b8:62:88), Dst: 10.1.1.1 (01:00:00:00:00:00)

Internet Protocol Version 4, Src: 10.1.1.1, Dst: 192.168.254.254

Transmission Control Protocol, Src Port: 1061, Dst Port: 80, Seq: 1061, Len: 0

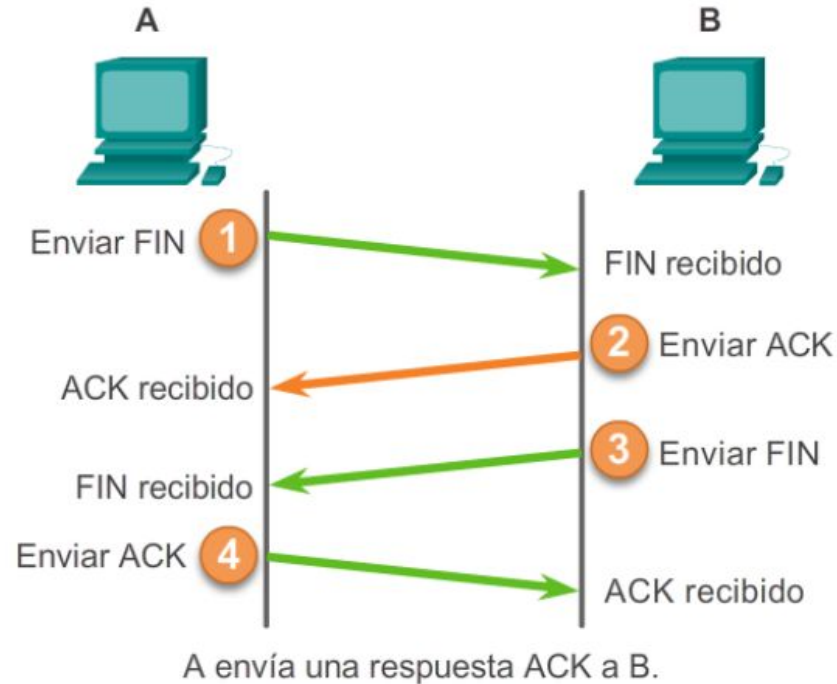
Un analizador de protocolos muestra la respuesta del cliente para la sesión en la trama 12

En el segmento TCP de esta trama se muestra lo siguiente:

- El indicador ACK está establecido para indicar un número válido de acuse de recibo.
- Respuesta de número de acuse de recibo al número de secuencia inicial como valor relativo de 1.
- El número de puerto de origen 1061 corresponde a
- El número de puerto de destino 80 (HTTP) indica el servicio del servidor Web (httpd).

Comunicación TCP

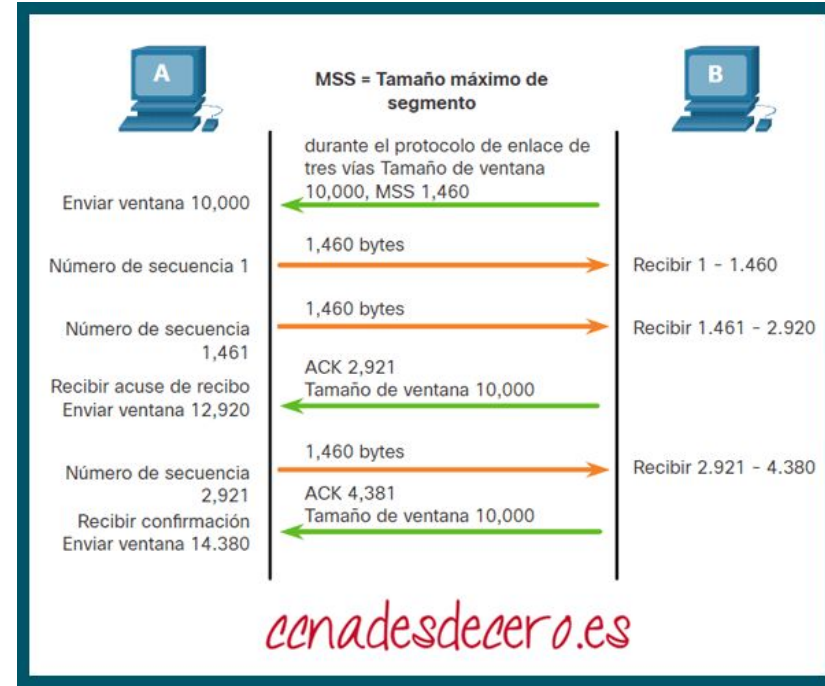
Terminación de sesión TCP



Confiabilidad y control de flujo

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

- El tamaño de la ventana se establece durante la realización del enlace de tres vías
- Por lo general, la PC B no esperará a los 10000 bytes antes de enviar el reconocimiento
- La PC A puede ajustar la ventana de envío a medida que recibe reconocimiento de PC B

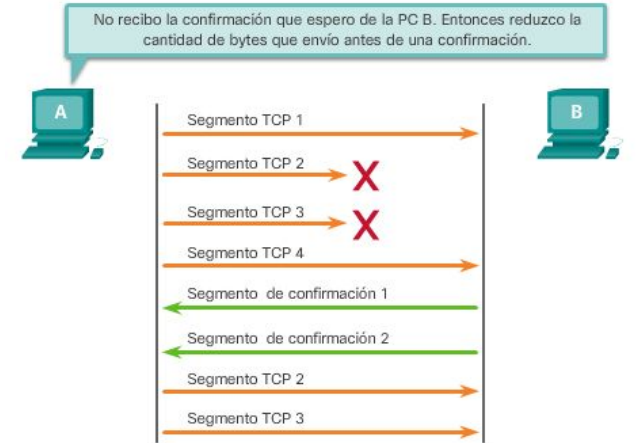


Confiabilidad y control de flujo

Control del flujo de TCP: prevención de congestiones

- La congestión causa la retransmisión de los segmentos TCP perdidos
- Ejemplo reduce la cantidad de bytes que envía antes de recibir un reconocimiento
- La retransmisión de los segmentos puede empeorar la congestión

Control de congestión de TCP



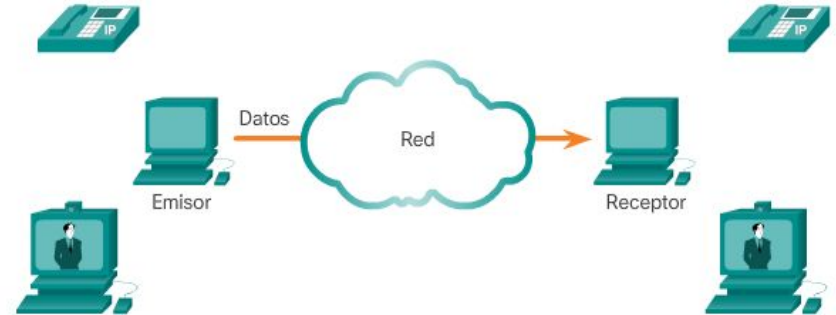
Los números de confirmación son para el próximo byte esperado y no para un segmento.
Los números de segmentos utilizados se simplifican con fines ilustrativos.

Proceso de comunicación en UDP

Comparación de baja sobrecarga y confiabilidad de UDP

- UDP no está orientado a la conexión
- Las funciones que no proporciona la capa de transporte se implementan aparte
- No ofrece retransmisión, secuencia ni control de flujo

Transporte de datos con baja sobrecarga de UDP



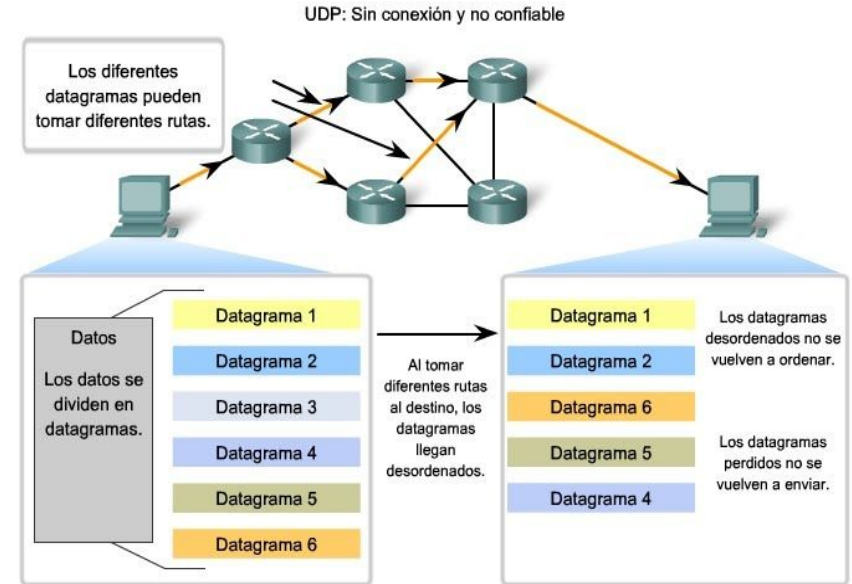
UDP no establece ninguna conexión antes de enviar datos.

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

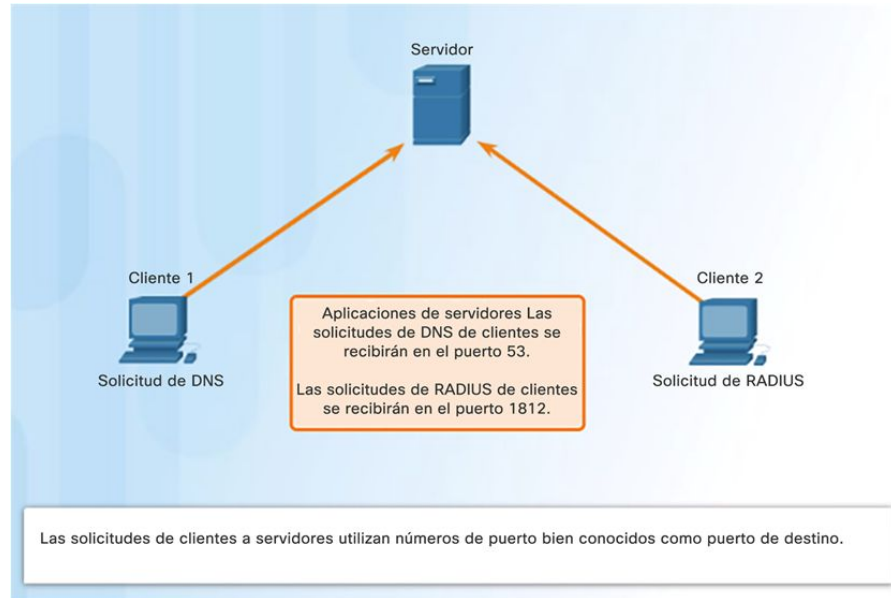
- Si es necesario, la aplicación debe identificar la secuencia correcta
- UDP simplemente vuelve a armar los datos en el orden en el que se recibieron
- UDP no realiza un seguimiento de los números de secuencia de la manera en que lo hace TCP



Proceso de comunicación en UDP

Procesos y solicitudes de servidores UDP

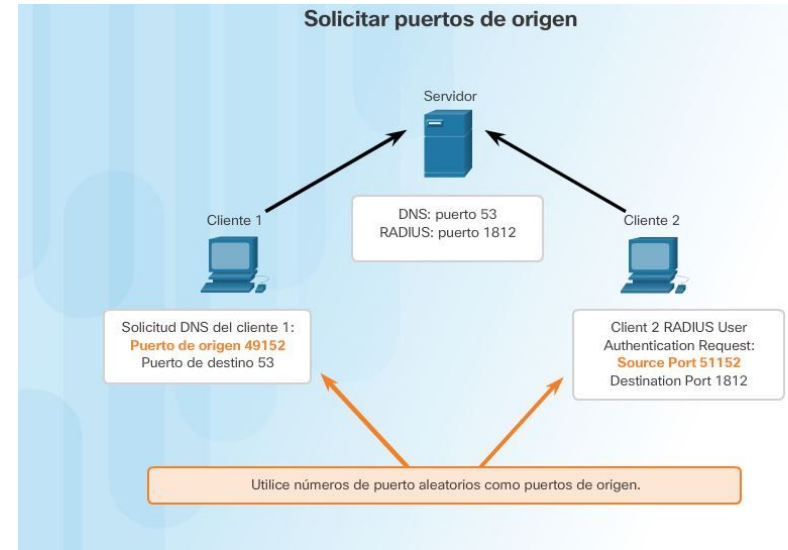
- El servidor del servicio de usuario de acceso telefónico de autenticación remota (RADIUS) que se muestra en la figura proporciona servicios de autenticación, autorización y auditoría para administrar el acceso de usuario.



Proceso de comunicación en UDP

Procesos de cliente UDP

- A las aplicaciones de servicios basadas en UDP se les asigna números de puertos conocidos o registrados
- Las Aplicaciones y los servicios UDP que se ejecutan en un servidor aceptan las solicitudes de cliente UDP
- Las solicitudes que se reciben en un puerto específico se envía a la aplicación adecuada según los números de puerto

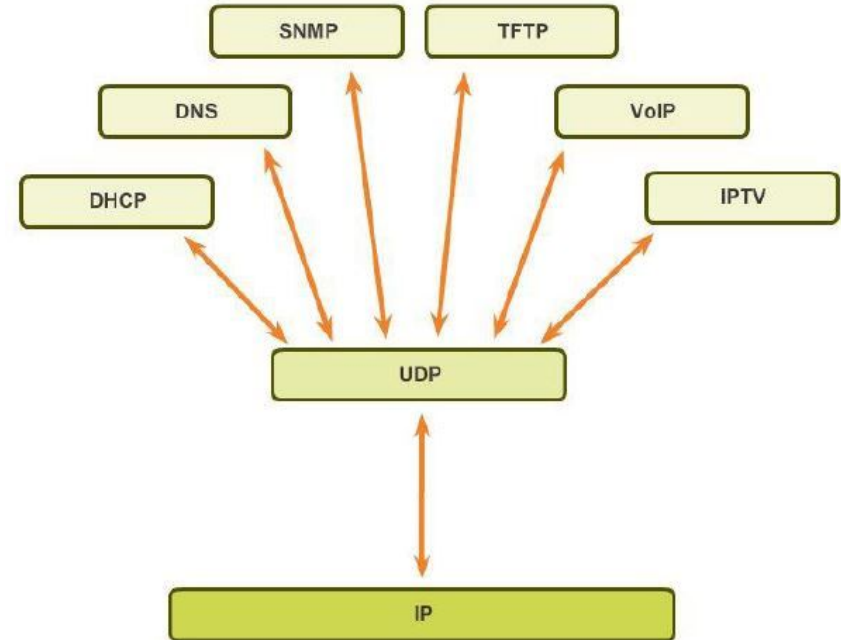


TCP o UDP

Aplicaciones que utilizan TCP

- TCP maneja todas las tareas relacionadas con la capa de transporte
- esto hace que la aplicación no tenga que administrar ninguna de dichas tareas
- Las aplicaciones simplemente pueden enviar el flujo de datos a la capa de transporte y utilizar los servicios de TCP
- Solicitudes y respuestas simples, Aplicaciones multimedia y video en vivo, aplicaciones que manejan la confiabilidad por su cuenta

Aplicaciones que utilizan UDP

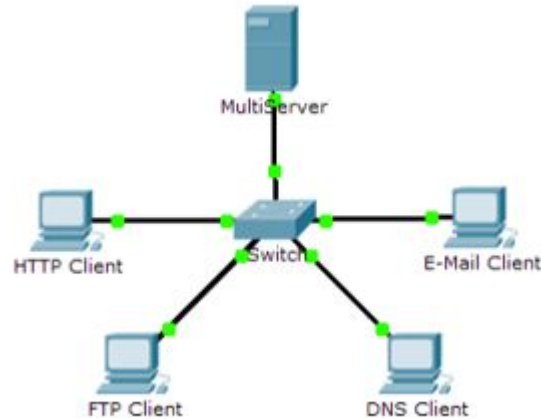




Sé Íntegro Sé Misionero Sé Innovador

9.3 Resumen del Capítulo

Packet Tracer: Comunicaciones TCP y UDP



Objetivos:

- Parte 1: Generar tráfico de red en modo de simulación.
- Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP.

Conclusión:

- Explicar la forma en que los protocolos y servicios de capa de transporte admiten comunicaciones a través de las redes de datos.
- Comparar el funcionamiento de los protocolos de capa de transporte en la admisión de la comunicación de extremo a extremo.

Sección 9.1

Nuevos términos y comandos

<ul style="list-style-type: none">• Número de puerto• Multiplexación	<ul style="list-style-type: none">• Protocolo de control de transmisión (TCP)• Protocolo de datagramas de usuario (UDP)	<ul style="list-style-type: none">• Orientado a la conexión• Con información de estado• Socket
---	--	--

Sección 9.2

Nuevos términos y comandos

- | | |
|--|---|
| <ul style="list-style-type: none">● Protocolo de enlace de tres vías● Número de puerto de secuencia inicial (ISN) | <ul style="list-style-type: none">● Acuse de recibo● Reconocimiento selectivo (SACK)● Tamaño de ventana |
|--|---|