

- 1. ¿Cuál es la funcionalidad del servicio de DHCP?**
- Asignar de forma automática las direcciones IP a los hosts conectados a la red.
- 2. Cuando se envían datos, debe de llevar la bandera PSH activada.**
- Verdadero
- 3. Defina el concepto de DMZ y cuál es su utilización.**
- DMZ o Zona Desmilitarizada por sus siglas en inglés, también conocido como Red Perimetral, es una red la cual separa la red interna de una entidad u organización y la red externa (Internet). Su utilización es para aislar la red interna de la organización de la red externa, haciendo que los dispositivos que están dentro de la DMZ puedan comunicarse con la red externa, pero impidiendo que la red externa acceda a cualquier dispositivo en la red interna.
- 4. Puerto utilizado por https.**
- 443
- 5. ¿Qué es un dominio de difusión?**
- Un dominio de difusión es por el cual se puede mandar un mensaje a todos los hosts conectados a una red.
- 6. Defina un socket.**
- Un socket es conformado por 2 direcciones IP y 2 puertos que permiten la comunicación entre hosts.
- 7. El protocolo UDP utiliza un buffer para entregar de forma ordenada los datos.**
- Falso
- 8. Cuál es el wildcard de la máscara /21.**
- 0.0.7.255
- 9. Describa la diferencia entre http y HTTPS.**
- La diferencia entre el http y el HTTPS es que el HTTPS tiene mayor seguridad, ya que impide que otros usuarios intercepten la información entre el cliente y el servidor.
- 10. Describa la principal función de la Capa 4.**
- Transmitir información entre procesos.
- 11. El protocolo DNS utiliza:**
- TCP y UDP
- 12. ¿Qué son los puertos dinámicos?**
- Los puertos dinámicos son aquellos a los cuales les podemos asignar cualquier protocolo.

Pregunta 13: UDP es un protocolo que: b. No orientado a la conexión

Pregunta 14: Los puertos Dinámicos son utilizados para identificar servicios bien conocidos

- Falso

Pregunta 15: TCP es un protocolo que: e. Orientado a la conexión

Pregunta 16: Los puertos que pueden ser utilizados por diferentes servicios de comunicación en la red, son utilizados por aplicaciones populares a. Registrados

Pregunta 18: ¿Qué es el protocolo three way handshake? ¿Cómo funciona?

- El protocolo three way handshake es un protocolo por medio del cual se establece conexión entre 2 hosts, funciona enviando un mensaje syn al receptor, este le devuelve un ack del syn recibido y le envía su propio syn, el emisor recibe ambos y le manda un receptor un mensaje ack.

Pregunta 19: Explique como se calcula el wildcard

- Se puede calcular sacando la inversa de una máscara de subred.

Pregunta 20: ICMP es un protocolo de capa (ingresar únicamente el número):

- Respuesta: 3

Pregunta 21: Desarrolle la diferencia entre IPv4 e IPv6

- La mayor diferencia entre el IPv4 y el IPv6 es que, el IPv6 acepta direcciones de ip de 128 bits, tiene soporte de configuración automática y no requiere de traducciones NAT.

Pregunta 22: Si quiero tener una red para conectar a 50 dispositivos, indique cual sería la máscara de red que optimiza el uso de direcciones

- 255.255.255.192
- /26

Pregunta 23: Los segmentos ACK d. Consumen un número de secuencia, siempre y cuando lleven datos (piggyback)

Pregunta 24: ¿Cómo se clasifican los puertos?

Respuesta: bien conocidos, registrados y dinámicos

Pregunta 25: ¿Qué es un ACK?

Respuesta: es un segmento el cual se envía como respuesta a un segmento syn

Pregunta 26: Son asignados aleatoriamente por los sistemas operativos para establecer conexiones: La respuesta seleccionada es correcta dinámicos. Los puertos dinámicos o privados son asignados por los sistemas operativos para establecer conexiones, generalmente en el rango de 49152-65535.

Pregunta 27: La explicación de las banderas de control está correcta. Se utilizan en el encabezado de los paquetes de protocolos como TCP para controlar el estado de la conexión y el flujo de datos.

Pregunta 28: La afirmación de que SCTP es un protocolo de capa 4 es verdadera. SCTP (Stream Control Transmission Protocol) es un protocolo de transporte, al igual que TCP y UDP, y opera en la capa 4 del modelo OSI.

Pregunta 29: La diferencia entre UDP y TCP está bien explicada. TCP es orientado a la conexión y asegura la entrega a través de acuses de recibo y retransmisiones, mientras que UDP es no orientado a la conexión y no garantiza la entrega.

Pregunta 30: Como se denomina el PDU de la capa de transporte La respuesta correcta es "Segmento". El PDU (Protocol Data Unit) de la capa de transporte se conoce como segmento en TCP y como datagrama en UDP.

Pregunta 31: El objetivo principal de la capa de enlace de datos no es proporcionar la transferencia de bits de una forma FIABLEE y EFICIENTE en una red adyacente, La respuesta seleccionada es correcta. La afirmación es falsa porque el objetivo principal de la capa de enlace de datos es proporcionar transferencia de datos de una manera confiable y eficiente, sí, pero no necesariamente en una red adyacente ya que también puede ser entre dispositivos directamente conectados.

Pregunta 32: La definición de puertos registrados está correcta. Son aquellos en el rango de 1024-49151 y están asignados por la IANA a servicios específicos. Son aquellos que son utilizados por puertos y aplicaciones conocidas si bien se pueden usar esos mismos puertos para otras aplicaciones se conoce que esas aplicaciones famosas / conocidas los utilizan

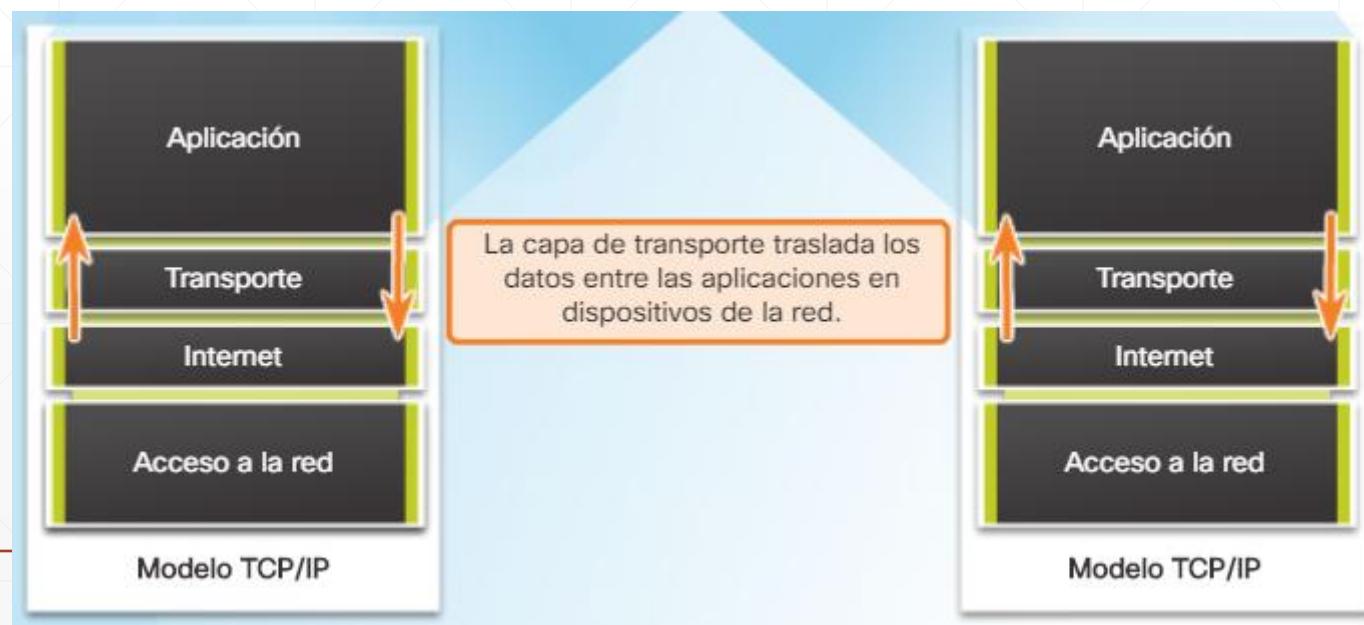
Pregunta 33: Que puertos utiliza el protocolo FTP: La respuesta a qué puertos utiliza el protocolo FTP es correcta. El puerto 20 se usa para la transferencia de datos y el puerto 21 se usa para el control de conexión. Los otros puertos listados no se utilizan para FTP: el puerto 80 es para HTTP, el 25 para SMTP (correo electrónico), y el 8080 es comúnmente un puerto alternativo para HTTP.

Capa 4 - Transporte

Redes I

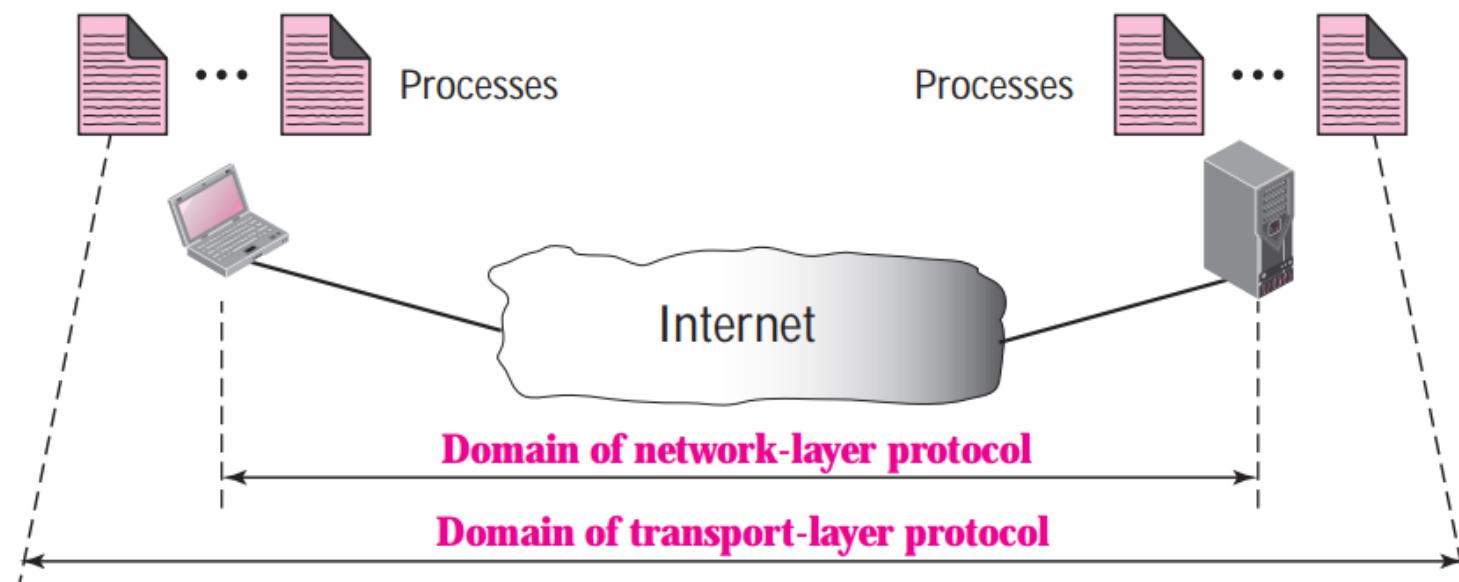
Función de la capa de transporte

- La capa de transporte es responsable de establecer una sesión de comunicación temporal entre dos aplicaciones y de transmitir datos entre ellas.
- Una aplicación genera datos que se envían desde una aplicación en un host de origen a una aplicación en un host de destino.



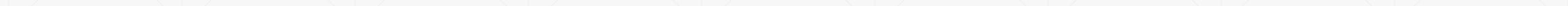
Process-to-process Communication

- La capa de red es la responsable de la comunicación a nivel host-to-host. Un protocolo de capa de red puede entregar un mensaje únicamente al host destino. Sin embargo esta es una entrega incompleta. El mensaje aun debe ser dirigido al proceso correcto.
- Un protocolo de capa de transporte es responsable de la entrega de un mensaje al proceso apropiado.



Responsabilidad de la capa de transporte

- Seguimiento de conversaciones individuales
- Segmentación de datos y rearmado de segmentos
- Identificación de las aplicaciones



Seguimiento de conversaciones individuales

- Cada conjunto de datos que fluye entre una aplicación de origen y una de destino se conoce como conversación.
 - Un host puede tener varias conversaciones en simultáneo a través de la red con otro host.
 - Es responsabilidad de la capa de transporte mantener y hacer un seguimiento de todas estas conversaciones.
-

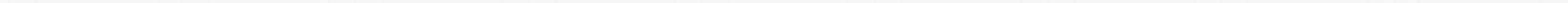
Segmentación de datos y rearmado de segmentos

- Se deben preparar los datos para el envío a través de los medios en partes manejables.
- Los protocolos de la capa de transporte tienen servicios que segmentan los datos de aplicación en bloques de un tamaño apropiado.
- Se agrega un encabezado a cada bloque de datos para el rearmado. Este encabezado se utiliza para hacer un seguimiento del flujo de datos.
- En el destino, la capa de transporte debe poder reconstruir las porciones de datos en un flujo de datos completo que sea útil para la capa de aplicación.



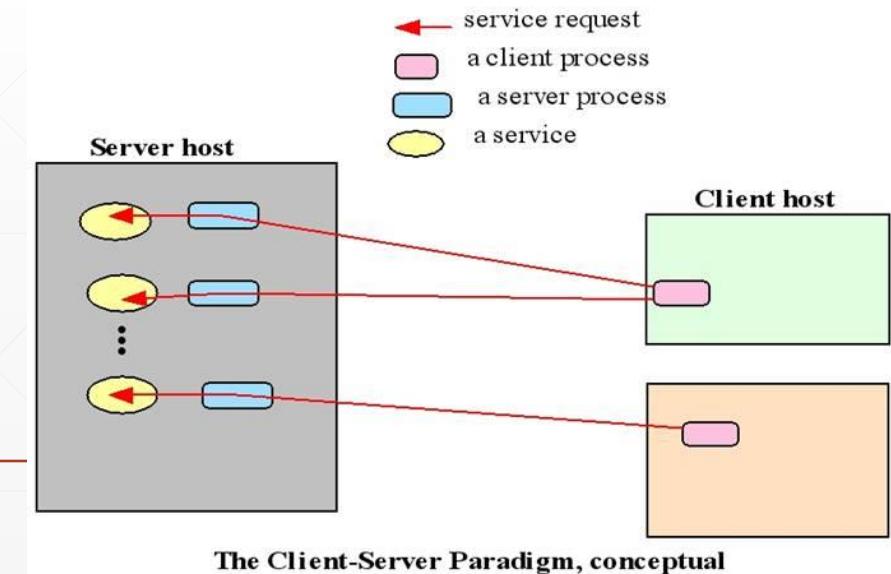
Identificación de las aplicaciones

- Para pasar flujos de datos a las aplicaciones adecuadas, la capa de transporte debe identificar la aplicación objetivo.
- La capa de transporte asigna un identificador a cada aplicación, llamado número de **puerto**.
- A todos los procesos de software que requieran acceso a la red se les asigna un número de puerto exclusivo para ese host.



Paradigma cliente-servidor

- Existen pocas maneras para lograr la comunicación proceso-a-proceso, la más común es a través del **paradigma cliente-servidor**.
- Un proceso en el host local, llamado **cliente**, necesita servicios de un proceso usualmente en un host remoto, llamado **servidor**.
- Ambos procesos (cliente y servidor) tienen el mismo nombre. Ejemplo: NTP
- Para establecer comunicación se debe definir:
 - Host local
 - Proceso local
 - Host remoto
 - Proceso remoto

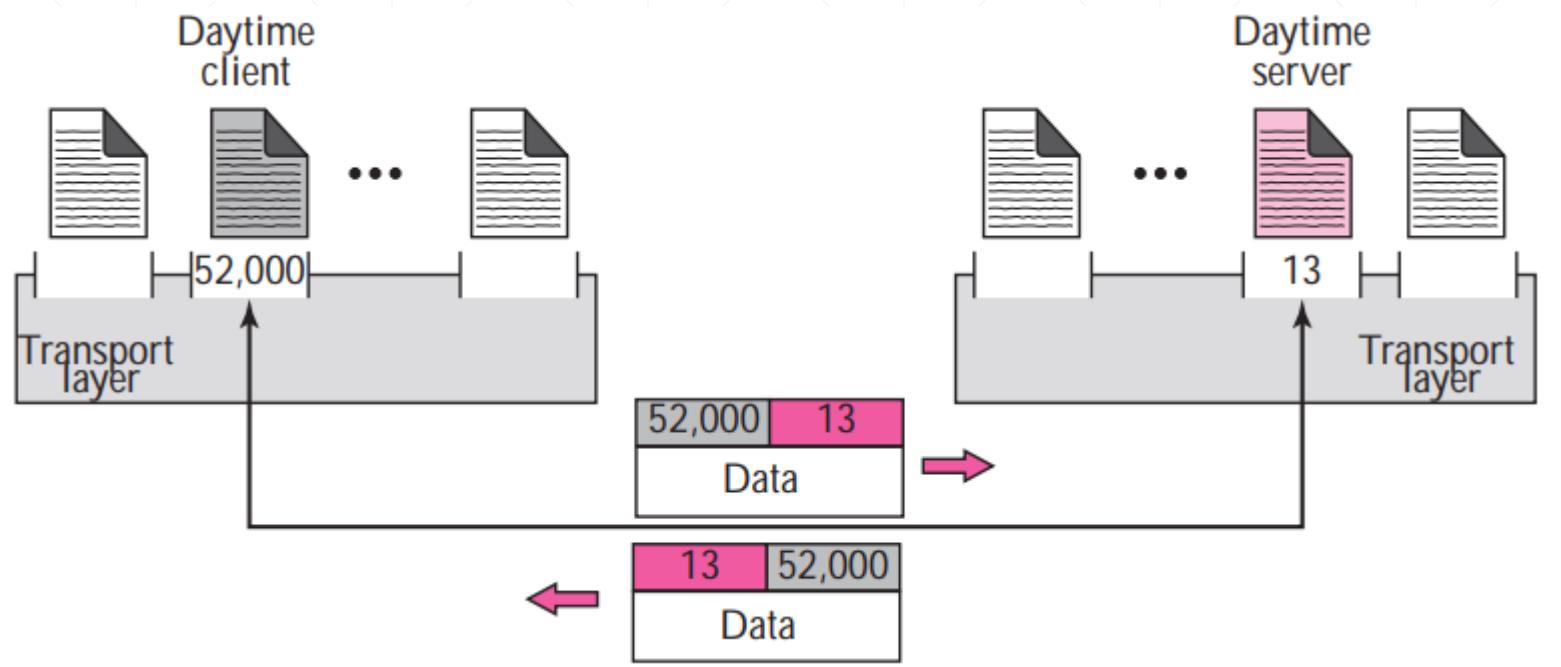


Números de puertos

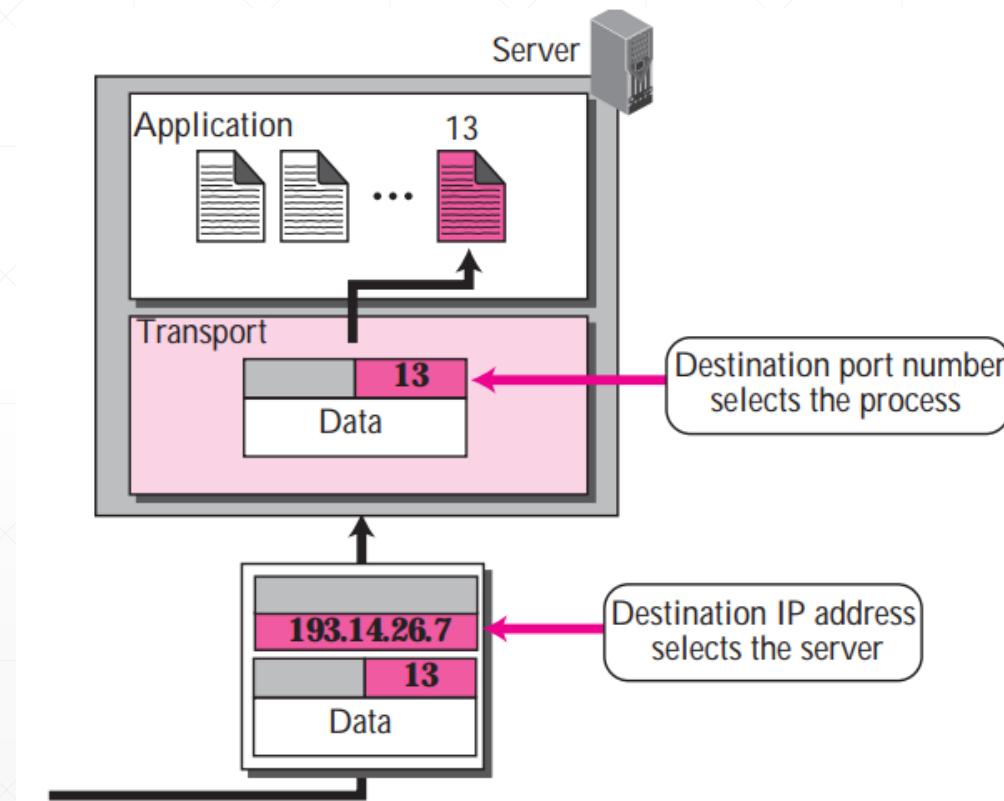
- El host local y el host remoto se definen utilizando direcciones IP.
- Para definir los procesos, se necesitan identificadores secundarios denominados **números de puerto**.
- En la suite del protocolo TCP/IP, los puertos son números enteros entre **0** y **65,535**.
- El proceso cliente se define a sí mismo con un número de puerto llamado **puerto efímero**. Un puerto efímero generalmente es un número aleatorio mayor a **1,024**.
- El proceso servidor también debe ser definido a través de un puerto. Pero este puerto no se asigna aleatoriamente.
- TCP/IP ha decidido utilizar puertos universales para servidores, llamados **puertos bien conocidos**.



Números de puerto

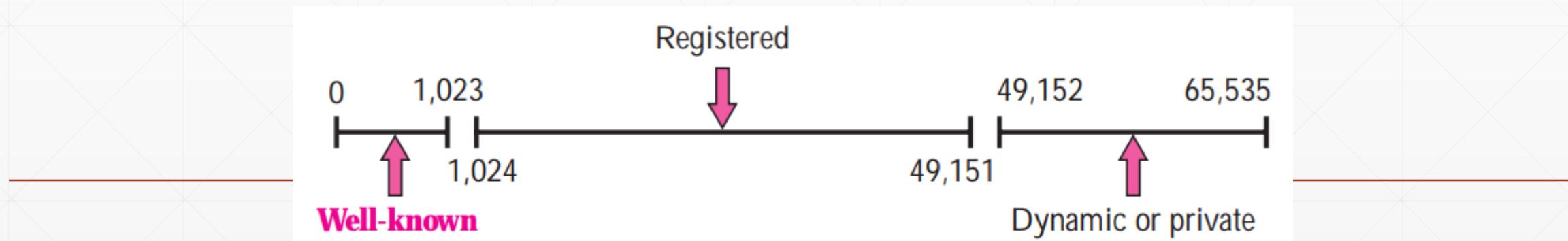


Direcciones IP vs números de puerto



Rangos de puertos de ICANN

- **Puertos bien conocidos:** rango del 0 al 1023 son asignados y controlados por ICANN.
- **Puertos registrados:** rango del 1024 al 49151 no son asignados ni controlados por ICANN. Solo deben de ser registrados en ICANN para evitar duplicados.
- **Puertos dinámicos:** rango del 49152 al 65535 no son ni controlados ni registrados. Son utilizados como puertos temporales o privados. Es recomendado que estos puertos sean asignados como puertos efímeros para las aplicaciones cliente.



Puertos bien conocidos

Tabla 145: Números de puertos bien conocidos (well-known ports) y aplicaciones TCP/IP

Puerto #	TCP / UDP	Keyword	Protocolo (abreviado)	Aplicación o nombre del protocolo / comentarios
7	TCP + UDP	echo	-----	Protocolo de eco (echo protocol)
9	TCP + UDP	discard	-----	Protocolo Discard
11	TCP + UDP	systat	-----	Protocolo Active users
13	TCP + UDP	daytime	-----	Protocolo Daytime
17	TCP + UDP	qotd	QOTD	Protocolo Quote of the day
19	TCP + UDP	chargen	-----	Protocolo Character Generator
20	TCP	ftp-data	FTP (DATA)	Protocolo ftp (puerto de datos x defecto)
21	TCP	ftp	FTP (CTRL)	Protocolo ftp (control y comandos)
23	TCP	telnet	-----	Protocolo telnet
25	TCP	smtp	SMTP	Protocolo SMTP
37	TCP + UDP	time	-----	Protocolo Time
43	TCP	nicname	-----	Protocolo Whois (también llamado Nicname)
53	TCP + UDP	domain	DNS	Servidor de Nombres de Dominio (Sistema de nombres de Dominio)
67	UDP	bootps	BOOTP / DHCP	Protocolo Bootstrap / Protocolo de configuración automática de hosts (servidor)
68	UDP	bootpc	BOOTP / DHCP	Protocolo Bootstrap / Protocolo de configuración automática de hosts (cliente)
69	UDP	tftp	TFTP	Protocolo para transferencia de archivos triviales (Trivial File Transfer Protocol)
70	TCP	gopher	-----	Protocolo Gopher
79	TCP	finger	-----	Protocolo Finger para información de usuarios
80	TCP	http	HTTP	Protocolo para Transferencia de Hipertextos (WWW)
110	TCP	pop3	POP	Protocolo de oficina de correos (Post Office Protocol version 3)
119	TCP	nntp	NNTP	Protocolo para transfereencias de noticias en red (Network News transfer Protocol)
123	UDP	ntp	NTP	Protocolo de tiempo (Network Time Protocol)
137	TCP + UDP	netbios-ns	-----	Protocolo NetBIOS (servicio de nombres)
138	UDP	netbios-dgm	-----	Protocolo NetBIOS (servicio de datagramas)
139	TCP	netbios-ssn	-----	Protocolo NetBIOS (servicio de sesiones)
143	TCP	imap	IMAP	Protocolo para acceso de mensajes en Internet (Internet Message Access Protocol)
161	UDP	snmp	SNMP	Protocolo Simple para administración de redes (Simple Network Management Protocol)
162	UDP	snmptrap	SNMP	Simple Network Management Protocol (trap)
179	TCP	bgp	BGP	Protocolo Border gateway
194	TCP	irc	IRC	Protocolo Internet Relay Chat
443	TCP	https	HTTP over SSL	Protocolo HTTP sobre capas seguras (Secure Sockets Layer)
500	UDP	isakmp	IKE	IPSec Internet Key Exchange
520	UDP	router	RIP	Protocolo Para información de rutas (Routing Information Protocol (RIP-1 and RIP-2))
521	UDP	ripng	RIPng	Protocolo Para información de rutas (neva generación)

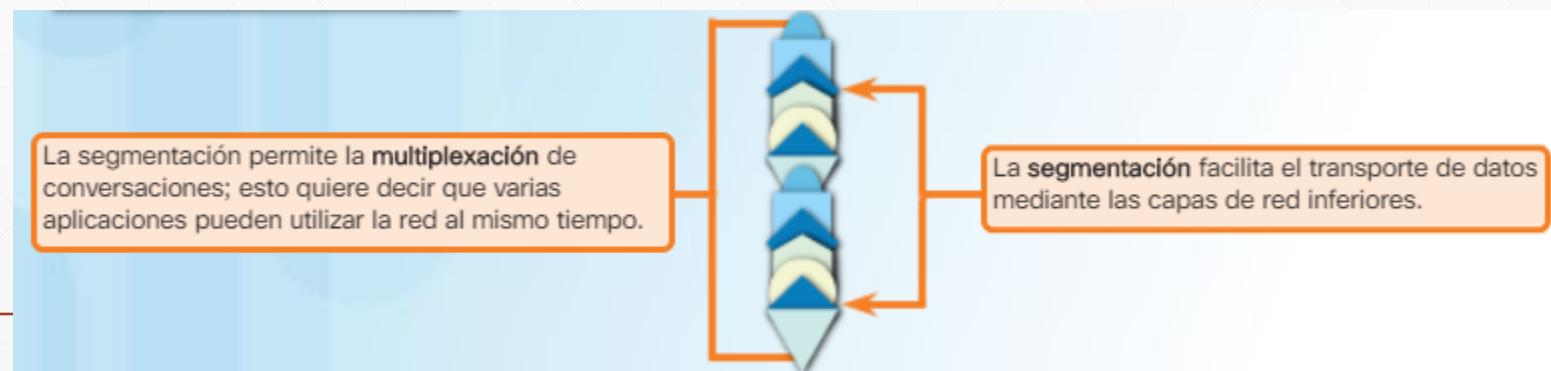
Puertos registrados

Tabla 146: Numeros comunes de puertos / aplicaciones registrados.

Puerto #	TCP / UDP	Keyword	Protocolo (abreviado)	Aplicación o nombre del protocolo / comentarios
1512	TCP + UDP	wins	WINS	Microsoft Windows Internet Naming Service
1701	UDP	l2tp	L2TP	Layer Two Tunneling Protocol
1723	TCP	pptp	PPTP	Point-To-Point Tunneling Protocol
2049	TCP + UDP	nfs	NFS	Network File System
6000 - 6063	TCP	x11	X11	X Window System

Multiplexación de conversaciones

- La segmentación de los datos en partes más pequeñas permite que se entrelacen (multiplexen) varias comunicaciones de distintos usuarios en la misma red.
- Para identificar cada segmento de datos, la capa de transporte agrega un encabezado que contiene datos binarios organizados en varios campos. Los valores de estos campos permiten que los distintos protocolos de la capa de transporte lleven a cabo variadas funciones de administración de la comunicación de datos.



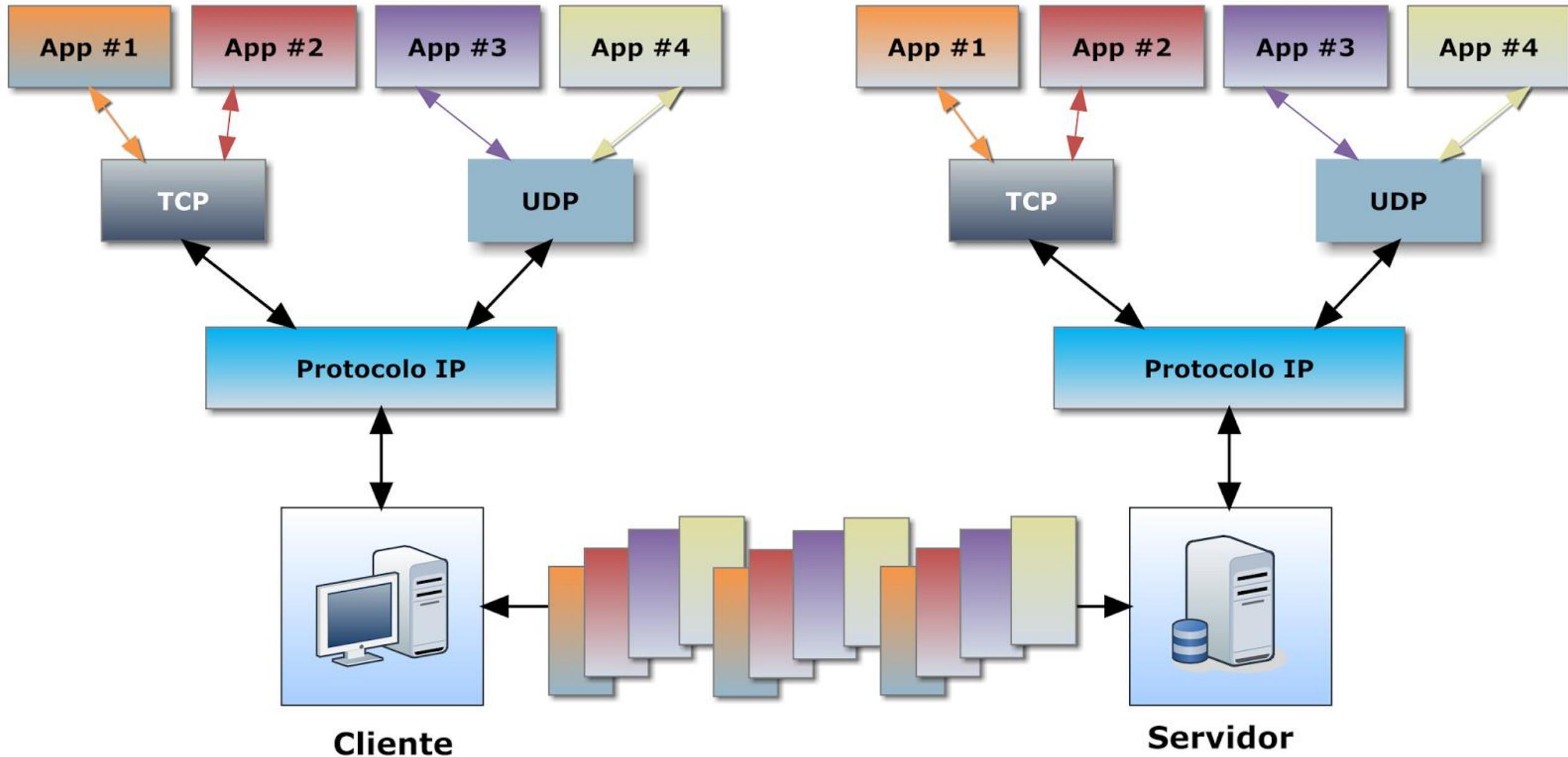


Figura 197: Multiplexación / demultiplexación de procesos en TCP/IP

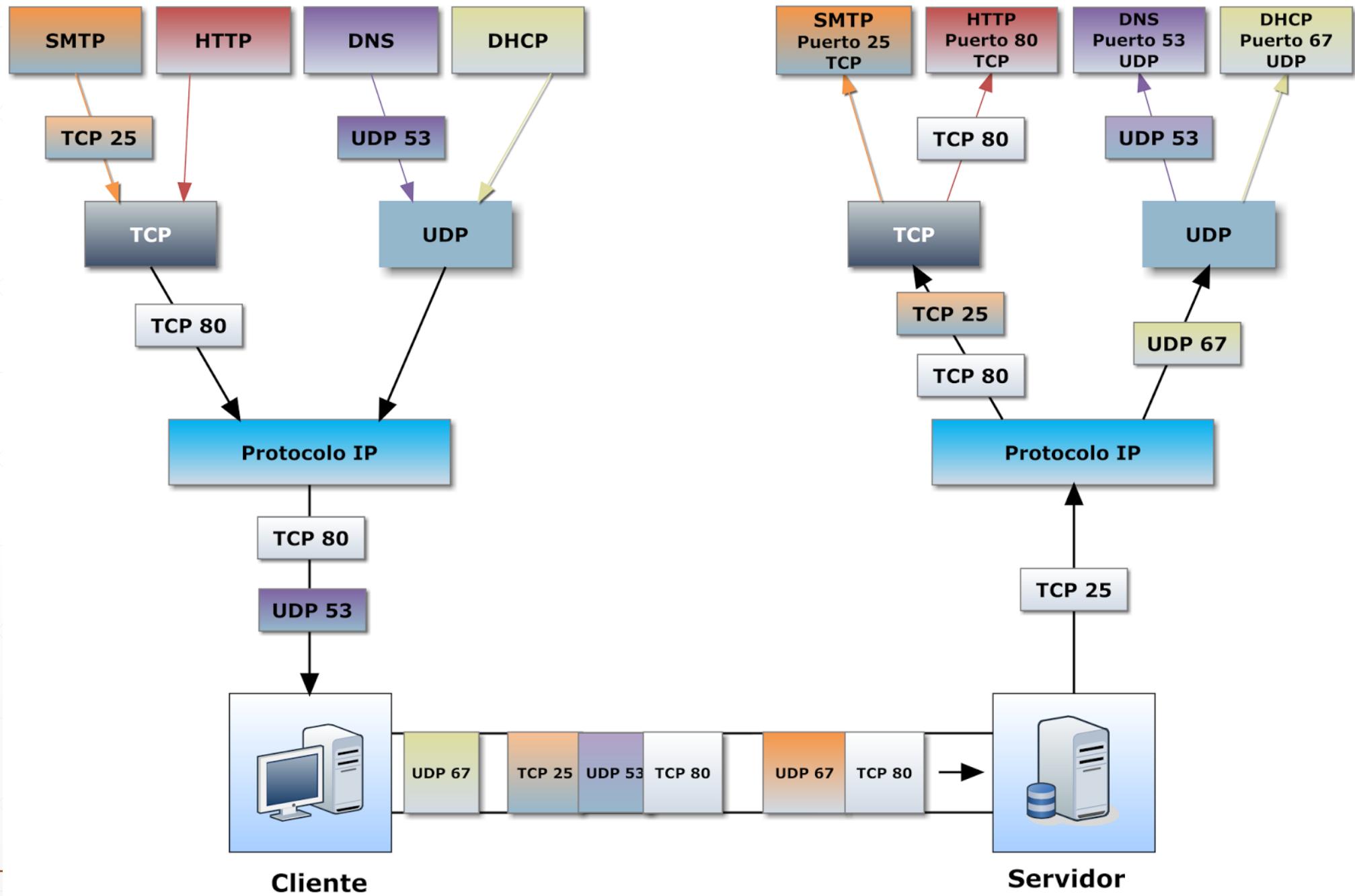
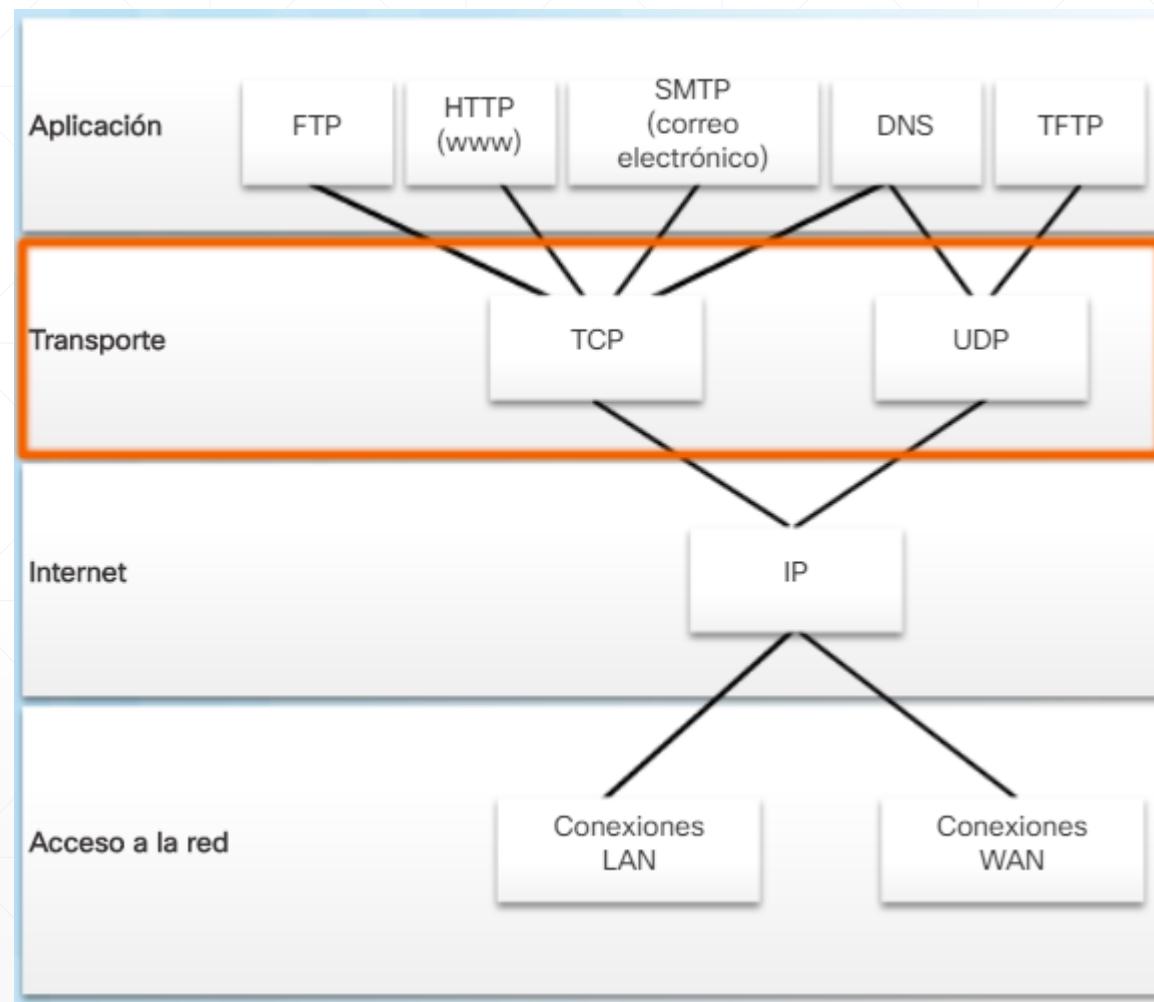


Figura 198: Multiplexación / demultiplexación de procesos en TCP/IP usando puertos TCP/UDP

Confiabilidad de la capa de transporte

- La capa de transporte también es responsable de administrar los requisitos de confiabilidad de las conversaciones. Las diferentes aplicaciones tienen diferentes requisitos de confiabilidad de transporte.
- TCP/IP proporciona dos protocolos de la capa de transporte:
 - TCP: Transmission Control Protocol
 - UDP: User Datagram Protocol
- TCP se considera un protocolo de la capa de transporte confiable y completo, ya que garantiza que todos los datos lleguen al destino. Sin embargo, esto requiere campos adicionales en el encabezado TCP que aumentan el tamaño del paquete y también la demora.
- En cambio, UDP es un protocolo de capa de transporte más simple, aunque no proporciona confiabilidad. Por lo tanto, tiene menos campos y es más rápido que TCP.

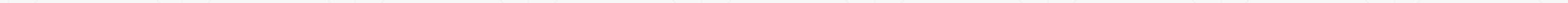




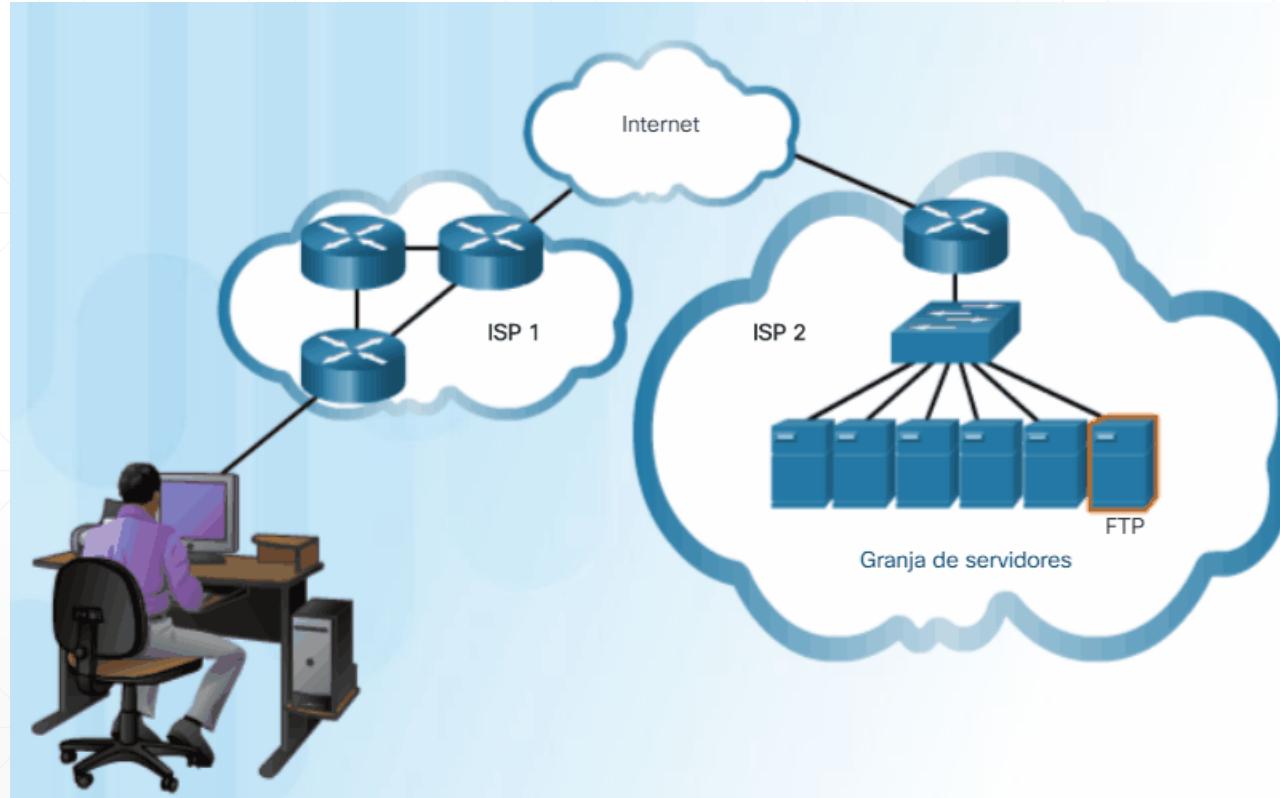
TCP

Con TCP, hay tres operaciones básicas de confiabilidad:

- Numeración y seguimiento de los segmentos de datos transmitidos a un host específico desde una aplicación específica
- Reconocimiento de los datos recibidos
- Retransmisión de los datos sin reconocimiento después de un tiempo determinado



TCP

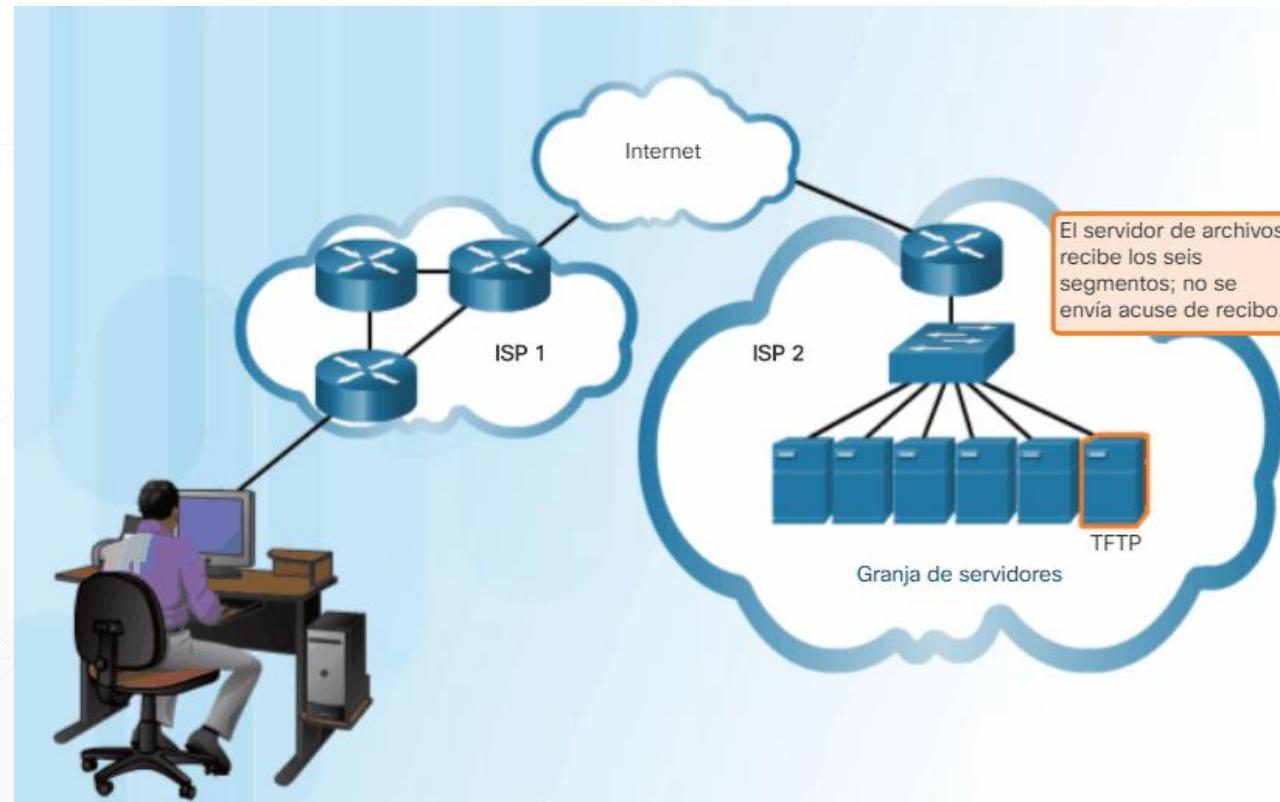


UDP

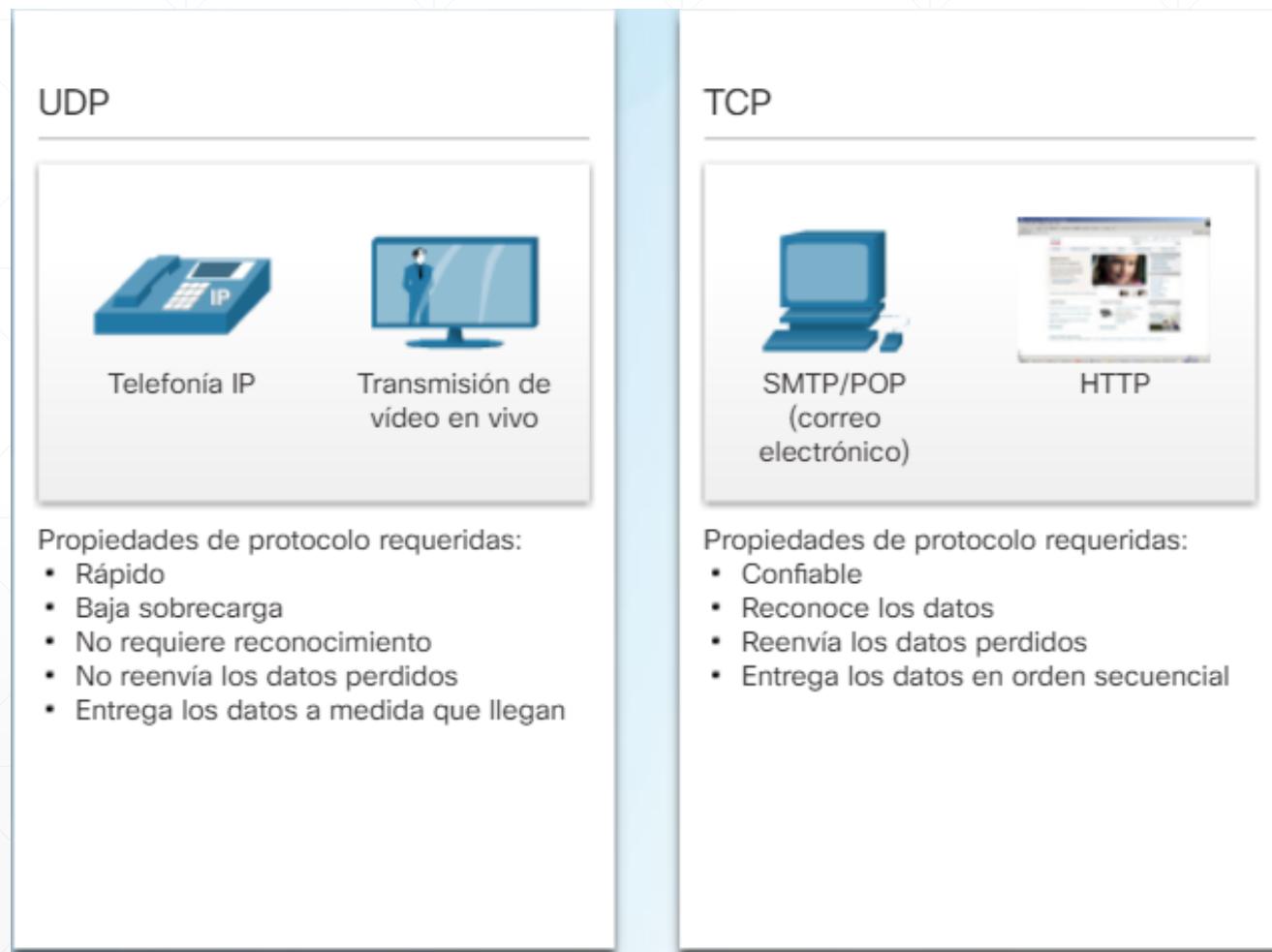
- Agregar sobrecarga para garantizar la confiabilidad para algunas aplicaciones podría reducir la utilidad a la aplicación e incluso ser perjudicial. En estos casos, UDP es un protocolo de transporte mejor.
- UDP proporciona las funciones básicas para entregar segmentos de datos entre las aplicaciones adecuadas, con muy poca sobrecarga y revisión de datos. UDP se conoce como un protocolo de entrega de **máximo esfuerzo**.
- En el contexto de redes, la entrega de máximo esfuerzo se denomina “**poco confiable**” porque no hay reconocimiento que indique que los datos se recibieron en el destino.



UDP



UDP vs TCP



Características TCP

Establecimiento de una sesión

- TCP es un protocolo orientado a la conexión.
 - Un protocolo orientado a la conexión es uno que negocia y establece una conexión (o sesión) permanente entre los dispositivos de origen y de destino antes de reenviar tráfico.
 - Mediante el establecimiento de sesión, los dispositivos negocian la cantidad de tráfico que se puede reenviar en un momento determinado, y los datos que se comunican entre ambos se pueden administrar detenidamente.
-

Características TCP

Entrega confiable

- En términos de redes, la confiabilidad significa asegurar que cada segmento que envía el origen llegue al destino. Por varias razones, es posible que un segmento se dañe o se pierda por completo a medida que se transmite en la red.

Entrega en el mismo orden

- Los datos pueden llegar en el orden equivocado, debido a que las redes pueden proporcionar varias rutas que pueden tener diferentes velocidades de transmisión.
- Al numerar y secuenciar los segmentos, TCP puede asegurar que estos se rearmen en el orden correcto.

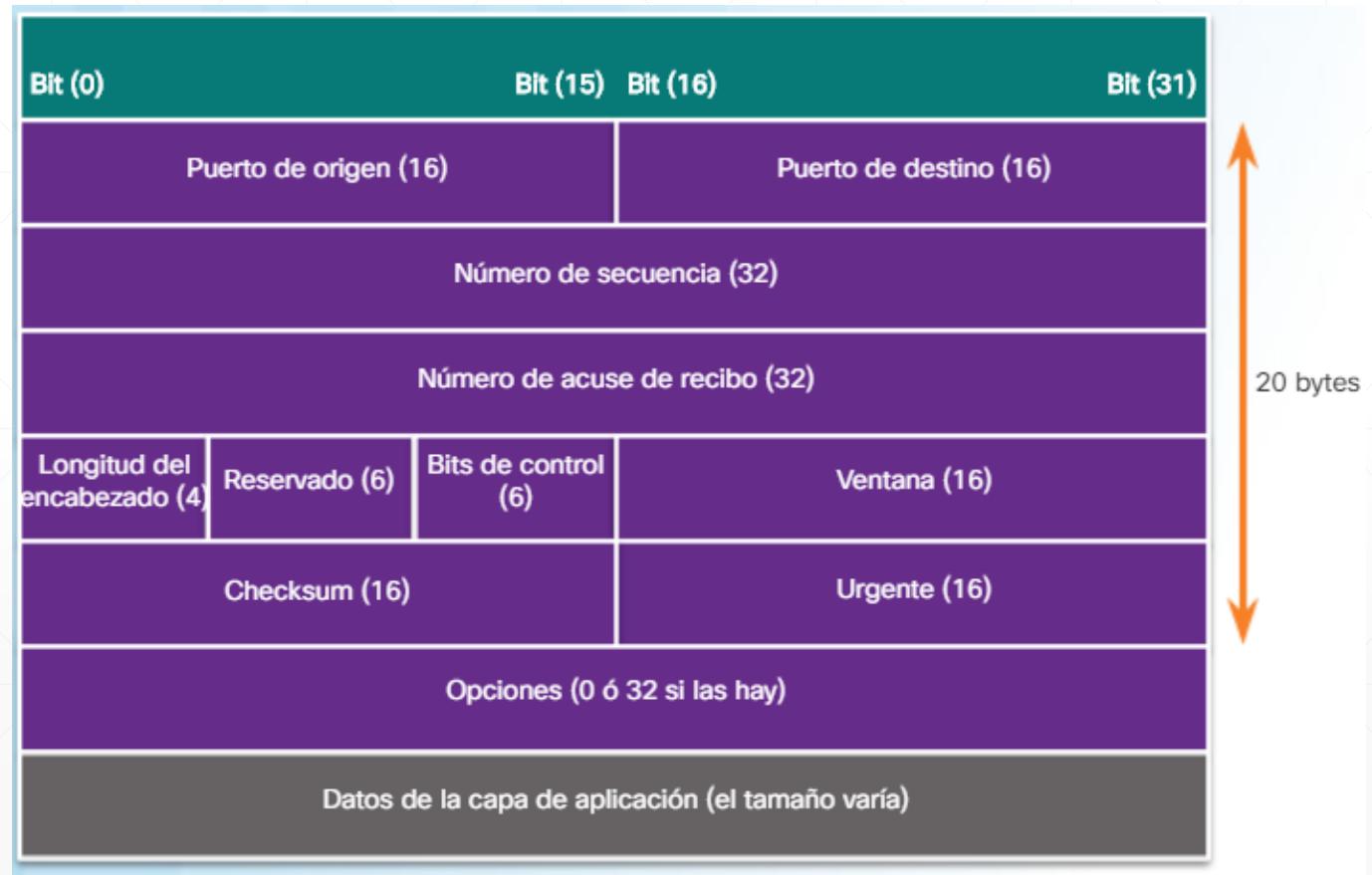


Características TCP

Control del flujo

- Los hosts de red tienen recursos limitados, como la memoria o la capacidad de procesamiento.
- Cuando TCP advierte que estos recursos están sobrecargados, puede solicitar que la aplicación emisora reduzca la velocidad del flujo de datos. Esto lo lleva a cabo TCP, que regula la cantidad de datos que transmite el origen.
- El control de flujo puede evitar la necesidad de retransmitir los datos cuando los recursos del host receptor están desbordados.

Segmento TCP



Encabezado TCP

- **Puerto de origen (16 bits) y puerto de destino (16 bits)** : se utilizan para identificar la aplicación.
- **Número de secuencia (32 bits)**: se utiliza para rearmar los datos.
- **Número de reconocimiento (32 bits)**: indica que los datos se han recibido y el siguiente byte esperado de la fuente.
- **Longitud del encabezado (4 bits)**: conocido como “desplazamiento de datos”. Indica la longitud del encabezado del segmento TCP.
- **Reservado (6 bits)**: este campo está reservado para el futuro.
- **Bits de control (6 bits)**: incluye códigos de bit, o marcadores, que indican el propósito y la función del segmento TCP.
- **Tamaño de la ventana (16 bits)**: indica la cantidad de bytes que se puedan aceptar por vez.
- **Checksum (16 bits)**: se utiliza para la verificación de errores en el encabezado y los datos del segmento.
- **Urgente (16 bits)**: indica si la información es urgente.



Bits de Control

URG: Urgent pointer is valid

ACK: Acknowledgment is valid

PSH: Request for push

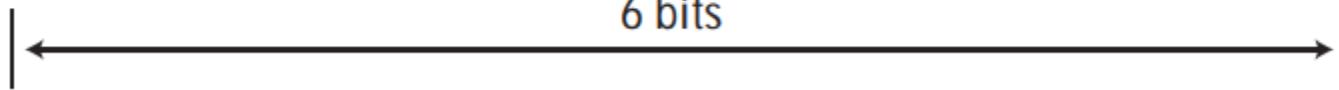
RST: Reset the connection

SYN: Synchronize sequence numbers

FIN: Terminate the connection



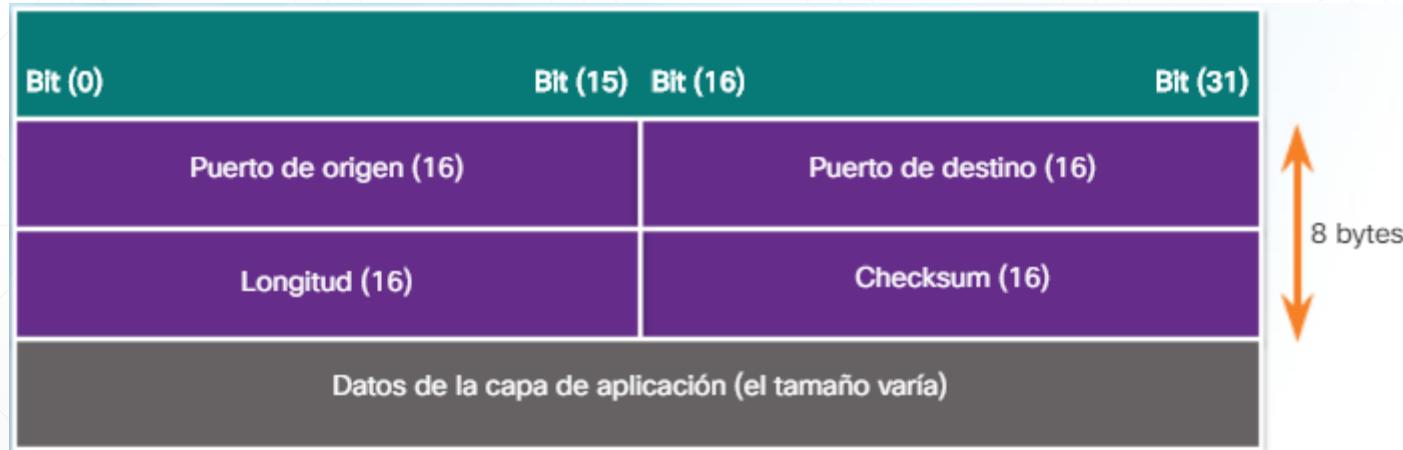
6 bits



Características UDP

- Los datos se construyen en el orden en que se recibieron.
 - Los segmentos perdidos no se vuelven a enviar.
 - No hay establecimiento de sesión.
 - No le informa al emisor sobre la disponibilidad de recursos.
-

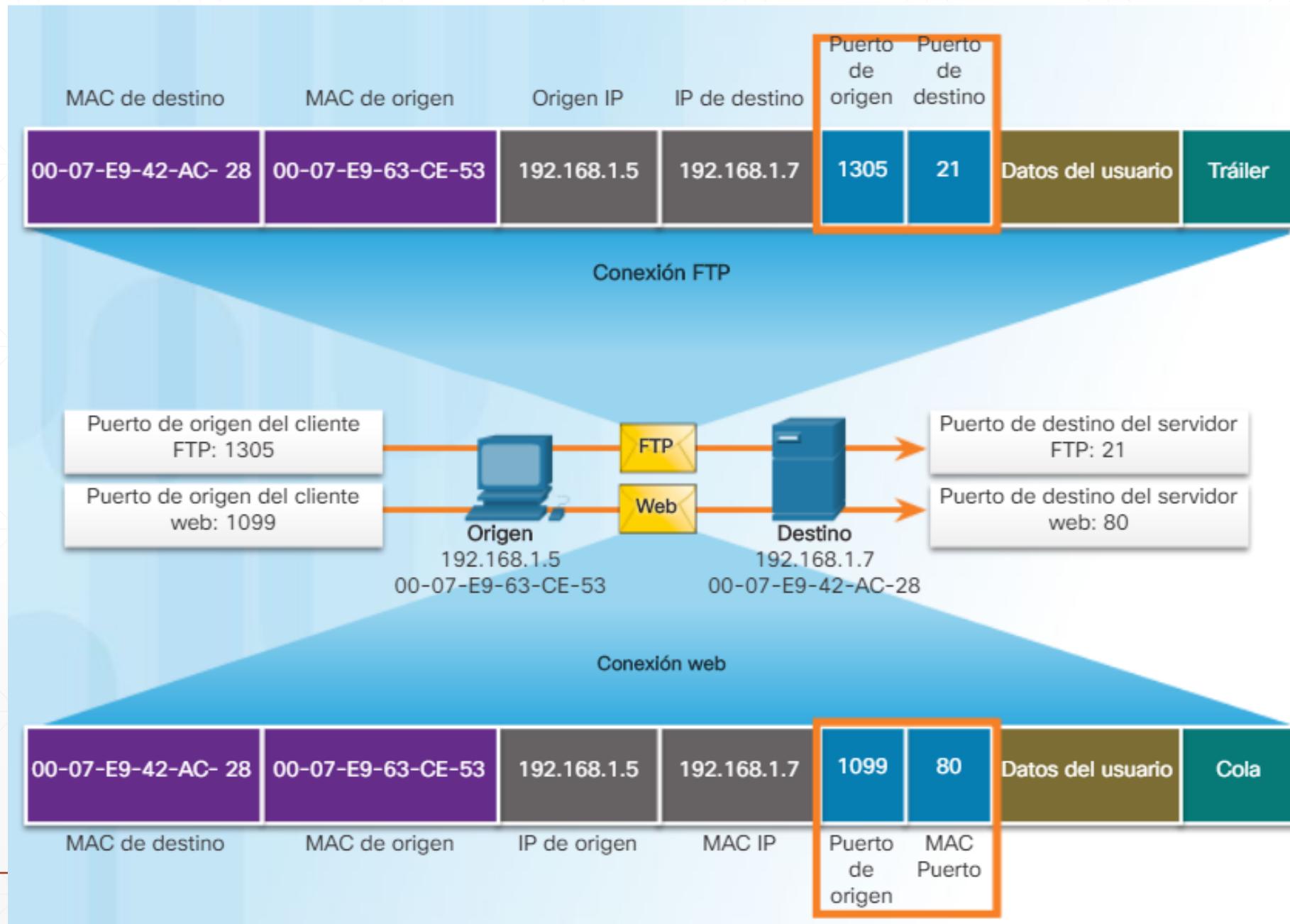
Datagrama UDP



Pares de sockets

- Los puertos de origen y de destino se colocan dentro del segmento. Los segmentos se encapsulan dentro de un paquete IP. El paquete IP contiene la dirección IP de origen y de destino.
- 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.
- El socket se utiliza para identificar el servidor y el servicio que solicita el cliente. Un socket de cliente puede ser parecido a esto, donde 1099 representa el número de puerto de origen: 192.168.1.5:1099
- El socket en un servidor web podría ser el siguiente: 192.168.1.7:80
- Juntos, estos dos sockets se combinan para formar un par de sockets: 192.168.1.5:1099, 192.168.1.7:80

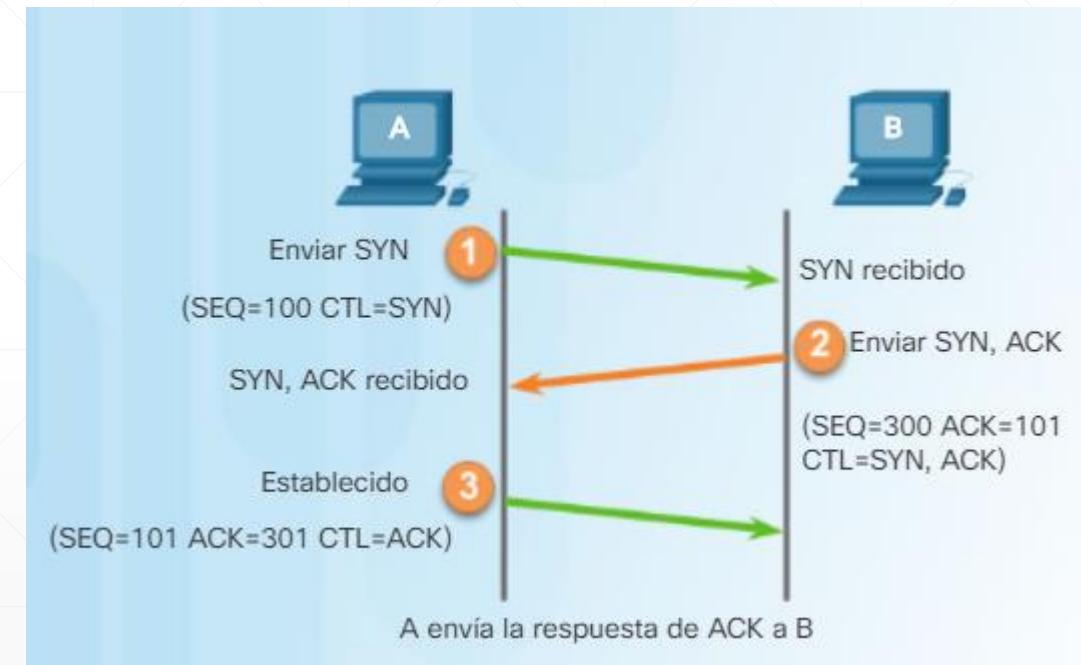




Establecimiento de conexiones (TCP three way handshake)

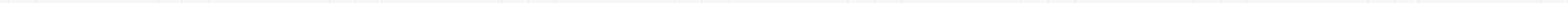
Una conexión TCP se establece en tres pasos:

- **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.



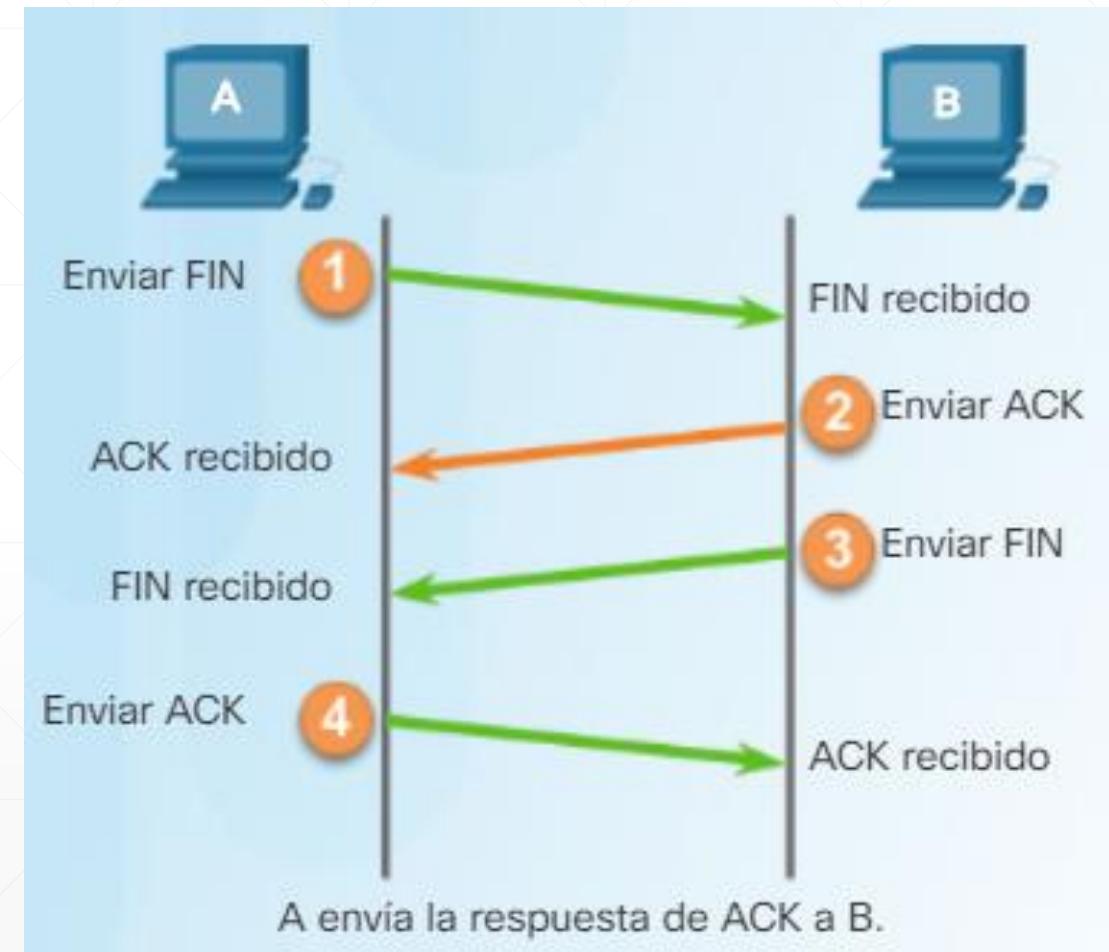
Finalización de la sesión TCP

- Para cerrar una conexión, se debe establecer el marcador de control de finalización (FIN) en el encabezado del segmento.
- Para finalizar todas las sesiones TCP de una vía, se utiliza un enlace de dos vías, que consta de un segmento FIN y un segmento de reconocimiento (ACK).
- Por lo tanto, para terminar una conversación simple admitida por TCP, se requieren cuatro intercambios para finalizar ambas sesiones.

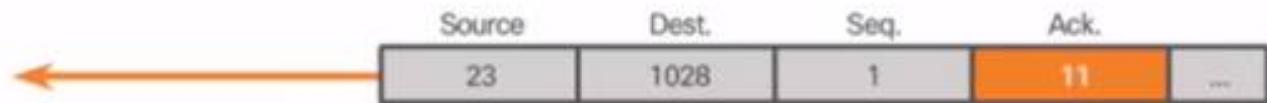
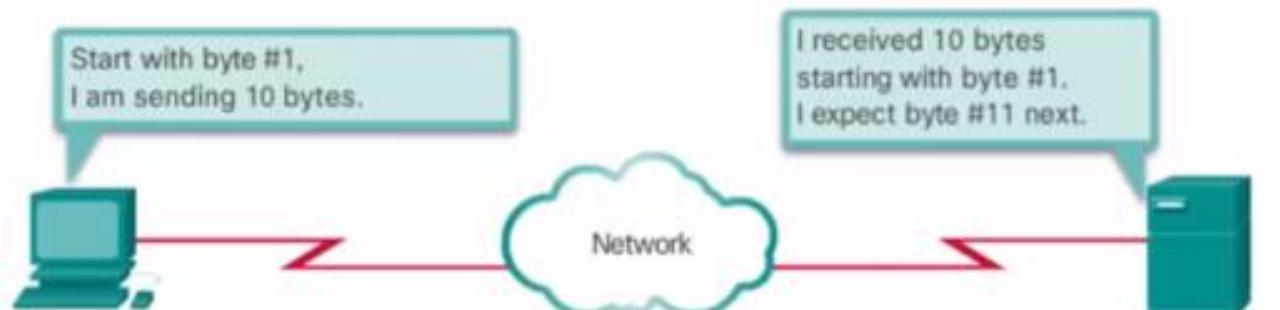
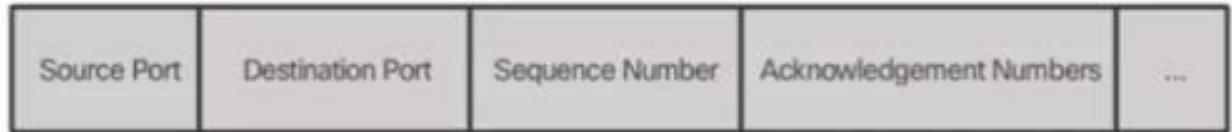


Finalización de la sesión TCP

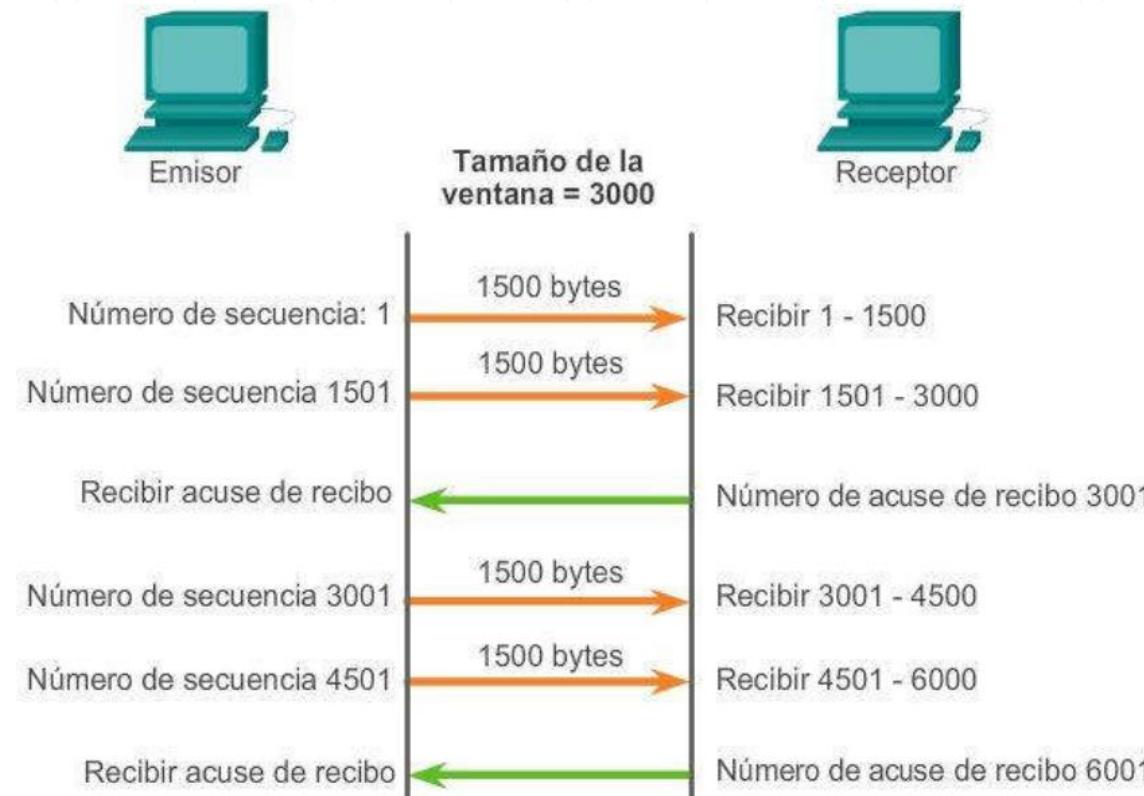
- **Paso 1:** cuando el cliente no tiene más datos para enviar en la transmisión, envía un segmento con el marcador FIN establecido.
- **Paso 2:** el servidor envía un ACK para reconocer el marcador FIN y terminar la sesión de cliente a servidor.
- **Paso 3:** el servidor envía un FIN al cliente para terminar la sesión de servidor a cliente.
- **Paso 4:** el cliente responde con un ACK para reconocer el recibo del FIN desde el servidor.



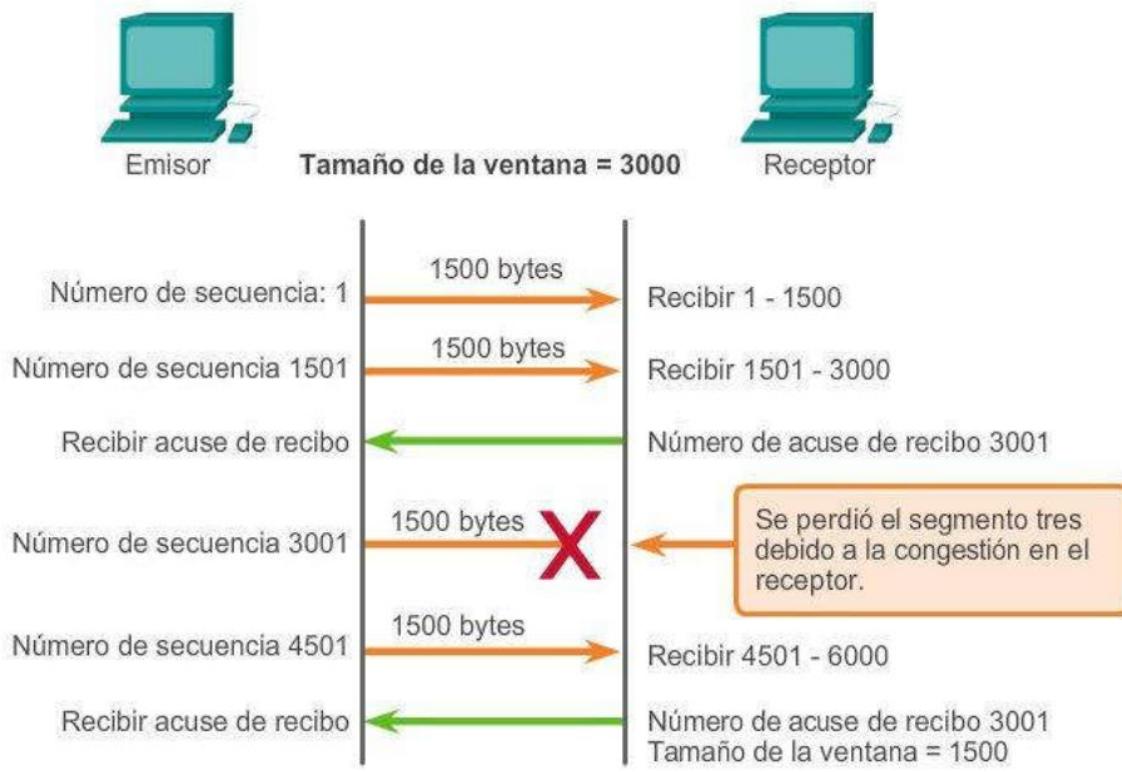
Window size



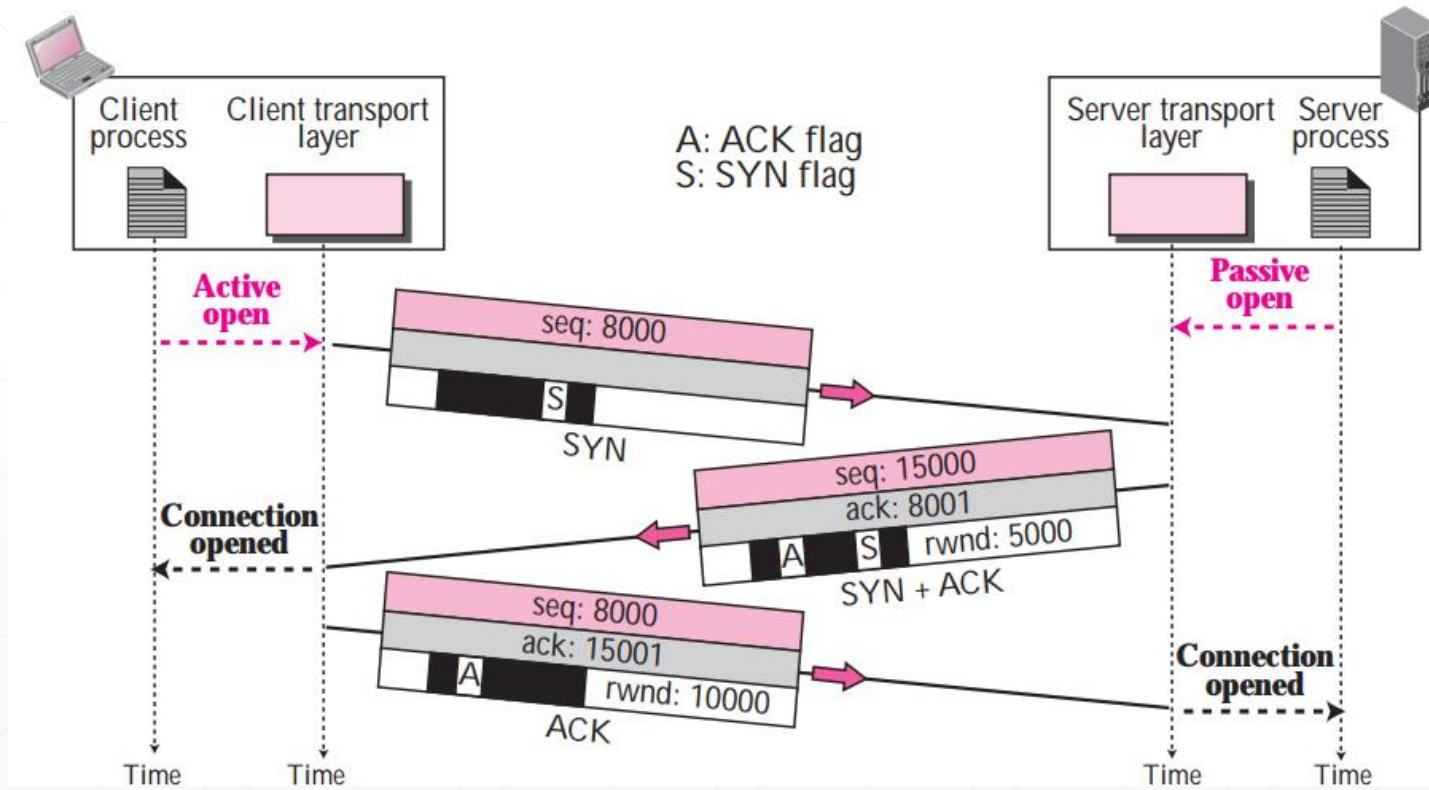
Acuse de recibido y tamaño de ventana TCP



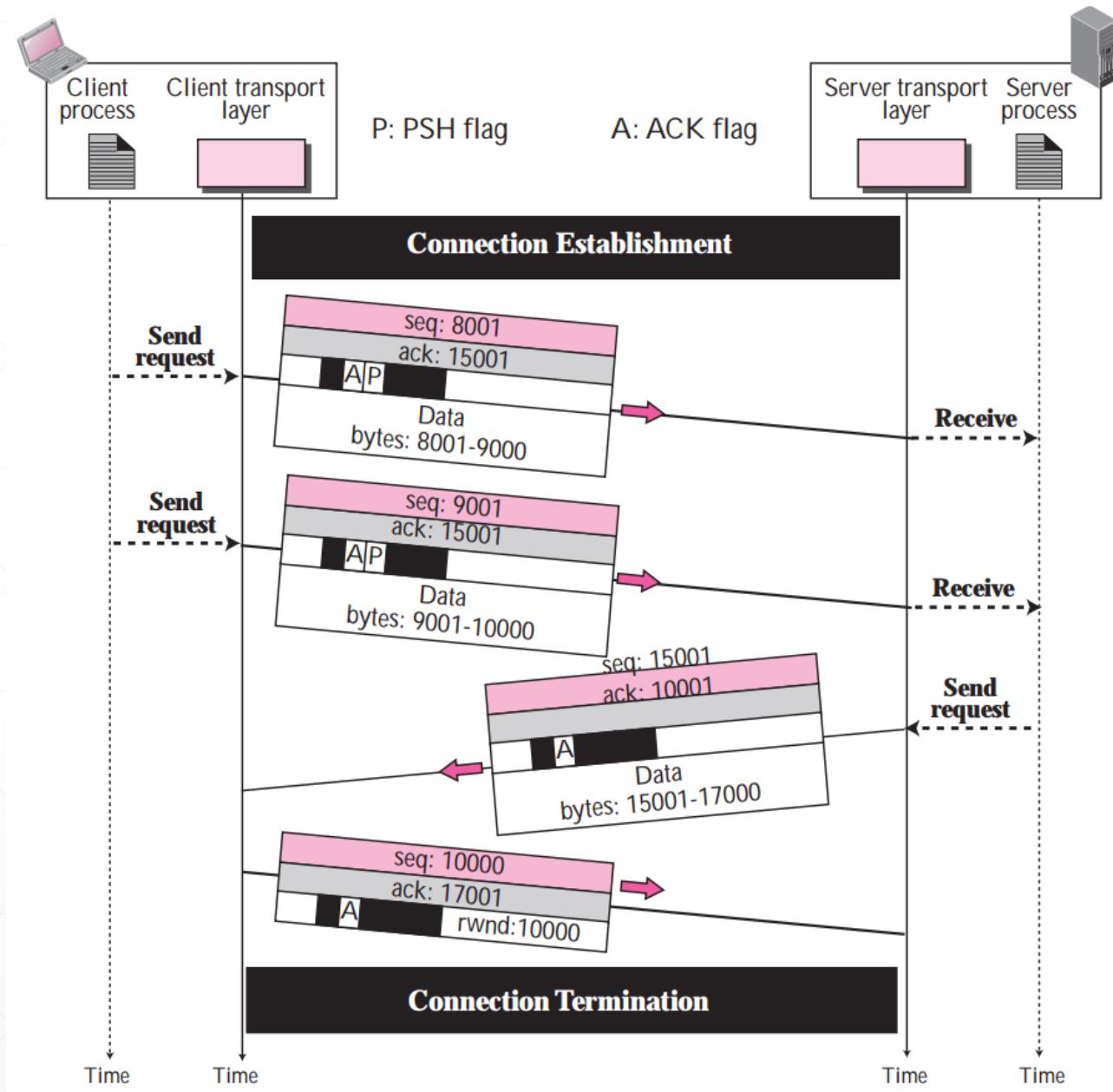
Congestión y control de flujo TCP



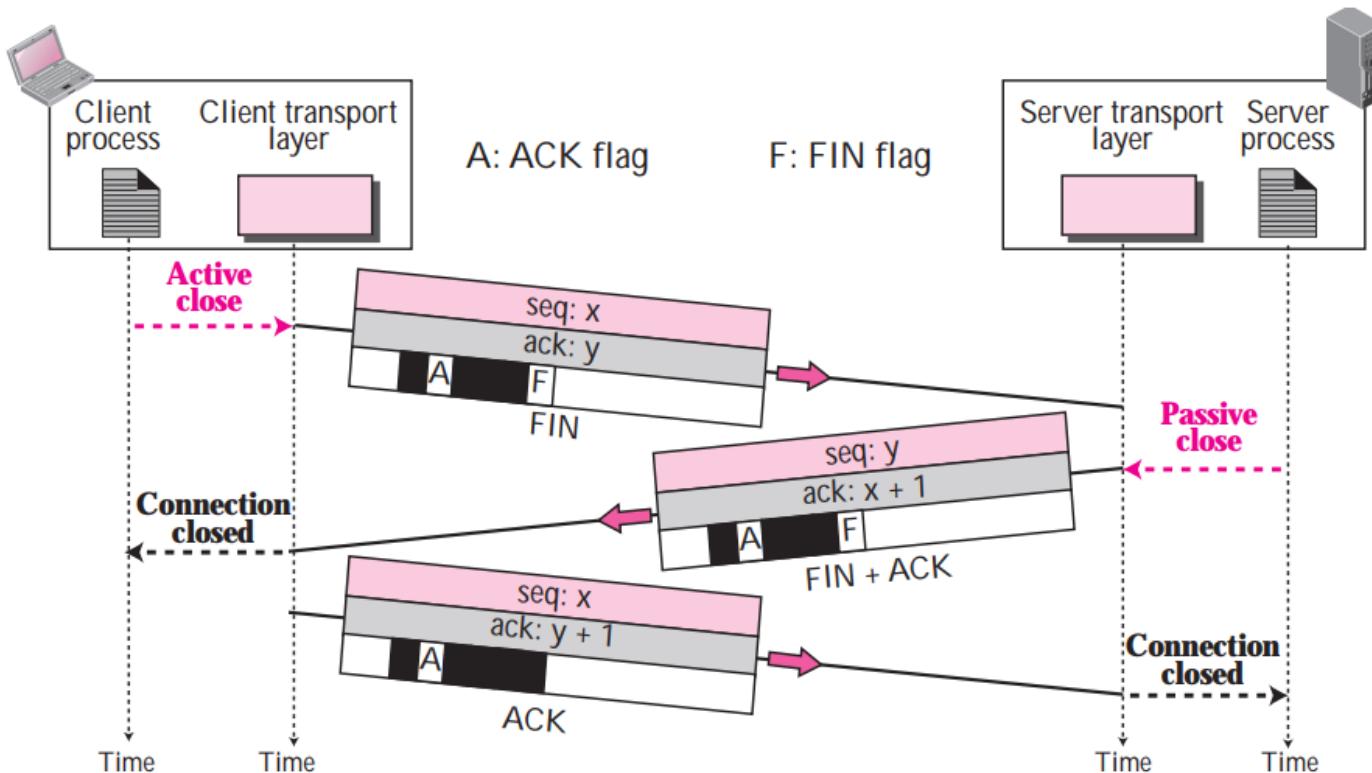
Connection establishment using three-way handshaking



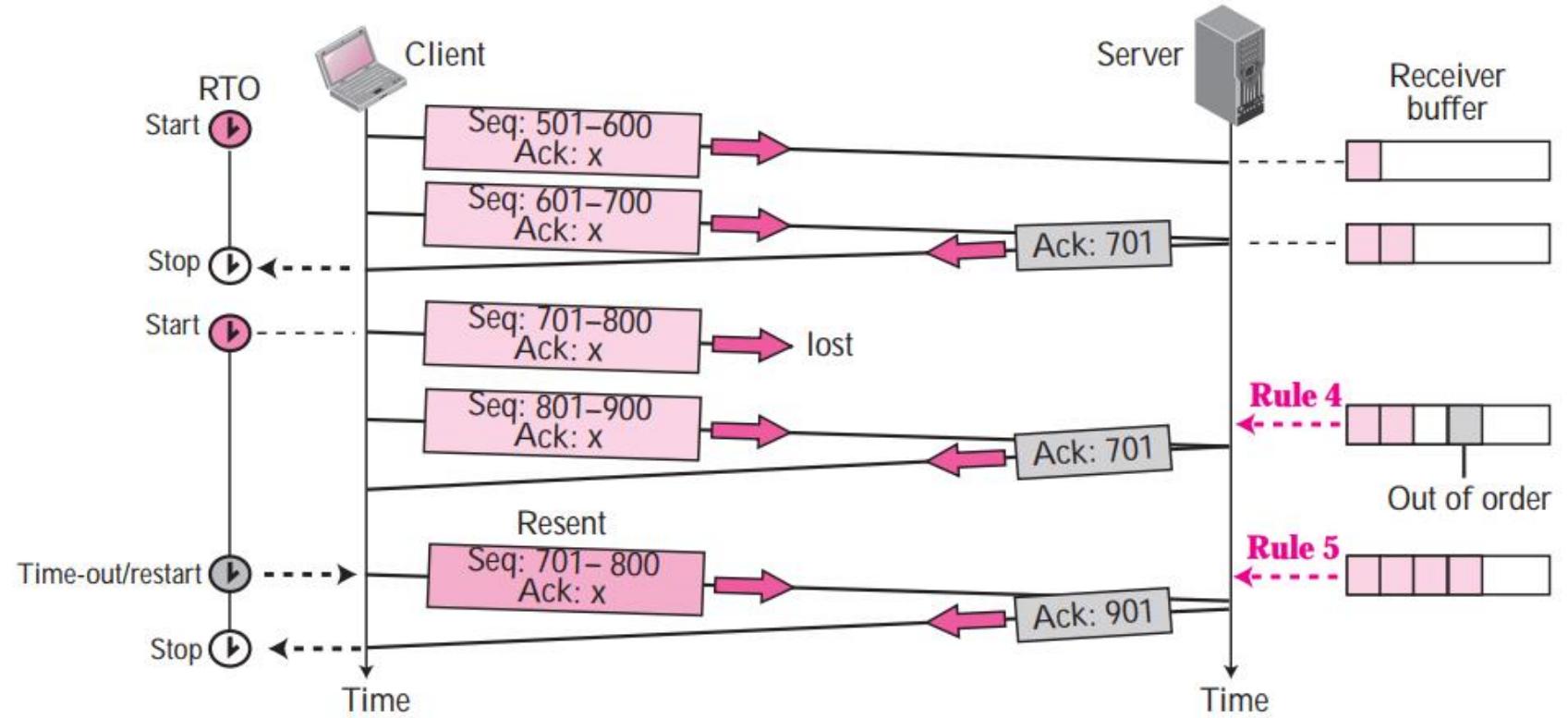
Data transfer



Connection termination using three-way handshaking



Lost packet





Capítulo 9: Capa de transporte



Introducción a Networks v6.0

Cisco | Networking Academy®
Mind Wide Open™



Capítulo 9: Secciones y objetivos

9.0 Introducción

9.1 División de una red IPv4 en subredes

- Describir el propósito de la capa de transporte en la administración del transporte de datos en la comunicación de extremo a extremo.
- Describir las características de los protocolos TCP y UDP, incluidos los números de puerto y sus usos.

9.2 Esquemas de direccionamiento

- Explicar la forma en que los procesos de establecimiento y finalización de sesión TCP promueven una comunicación confiable.
- Explicar la forma en que se transmiten y se reconocen las unidades de datos del protocolo TCP para garantizar la entrega.
- Describir los procesos de cliente UDP para establecer la comunicación con un servidor.
- Comparar UDP y TCP.

9.3 Resumen

9.1 Protocolos de capa de transporte





Protocolos de la capa de transporte

Transporte de datos

■ Función de la capa de transporte

- Es responsable de establecer una sesión de comunicación temporaria entre dos aplicaciones y de transmitir datos entre ellas.
- Proporciona compatibilidad con el flujo de datos orientado a la conexión, confiabilidad, control de flujo y multiplexión.

■ Tareas de la capa de transporte

- Realizar un seguimiento de conversaciones individuales.
- Segmentar datos y volver a armar segmentos.
- Identificar las aplicaciones.

■ Multiplexión de conversaciones

- Segmenta datos en fragmentos pequeños.
- Etiqueta fragmentos de datos según la conversación.

■ Confiabilidad de la capa de transporte

- Dos protocolos provistos: TCP y UDP.
- TCP aporta confiabilidad, UDP no.



Protocolos de la capa de transporte

Transporte de datos (continuación)

■ TCP

- Admite la confirmación de entrega de paquetes.
- Existen tres operaciones básicas que habilitan la confiabilidad con TCP:
 - La numeración y el seguimiento de los segmentos de datos transmitidos hacia un host específico desde una aplicación determinada
 - El acuse de recibo de datos
 - La retransmisión de cualquier dato sin acuse de recibo después de un período determinado

■ UDP

- UDP proporciona las funciones básicas para distribuir segmentos de datos entre las aplicaciones adecuadas, con muy poca sobrecarga y comprobación de datos.
 - Es ideal para aplicaciones que no requieren confiabilidad.
- ### ■ Protocolo de la capa de transporte correcto para la aplicación adecuada
- TCP es mejor para bases de datos, navegadores web, clientes de correo electrónico, etc.
 - UDP es mejor para transmisiones en vivo de audio o video, VoIP, etc.



Protocolos de la capa de transporte

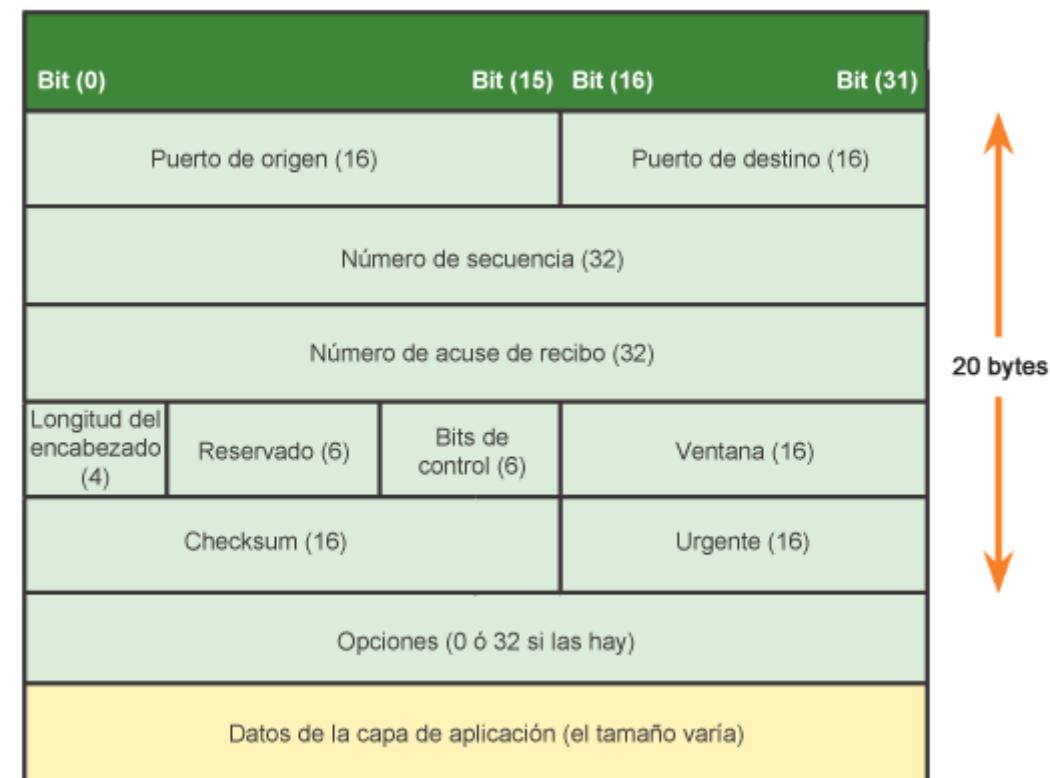
Descripción general de TCP y UDP

■ Características de TCP

- Establecimiento de una sesión
- Entrega confiable
- Entrega en el mismo orden
- Control de flujo

■ Encabezado TCP

- TCP es un protocolo con información de estado.
- TCP agrega 20 bytes de sobrecarga en el encabezado del segmento.





Protocolos de la capa de transporte

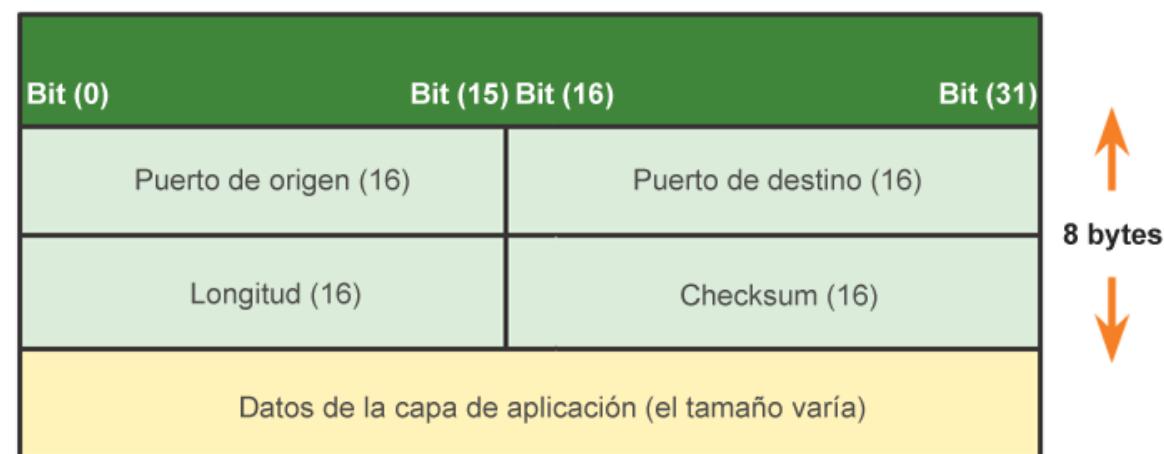
Descripción general de TCP y UDP (continuación)

■ Características de UDP

- Simple y rápido.

■ Encabezado UDP

- UDP es un protocolo sin información de estado.
- La aplicación debe manejar la confiabilidad.
- Las porciones de comunicación en UDP se denominan datagramas.
- UDP agrega solo 8 bytes de sobrecarga.





Protocolos de la capa de transporte

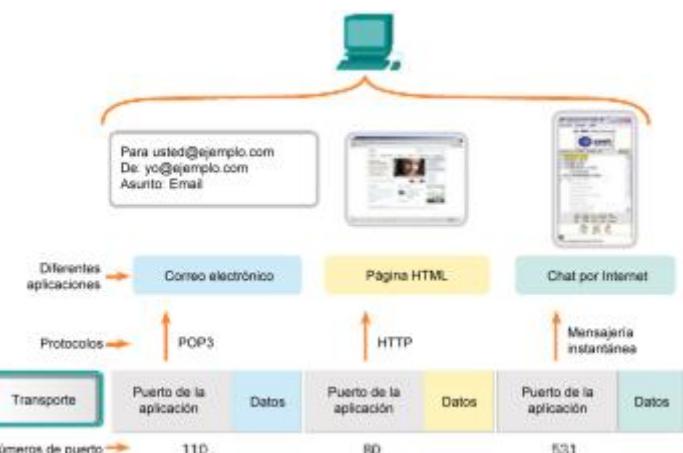
Descripción general de TCP y UDP (continuación)

■ Varias conversaciones por separado

- La capa de transporte separa y administra varias comunicaciones con diferentes requisitos de transporte.
- Diferentes aplicaciones envían y reciben datos en la red de manera simultánea.
- Los valores únicos de encabezado permiten que TCP y UDP administren estas distintas conversaciones simultáneas por medio de la identificación de estas aplicaciones.
- Estos identificadores únicos son números de puertos.

■ Números de puerto

- Suelen verse en pares: puerto de origen y puerto de destino.
- El emisor elige el puerto de origen en forma dinámica.
- El puerto de destino se utiliza para identificar una aplicación en el servidor (destino).





Protocolos de la capa de transporte

Descripción general de TCP y UDP (continuación)

■ Pares de sockets

- La combinación de la dirección IP de origen y el número de puerto de origen, o la dirección IP de destino y el número de puerto de destino, se conoce como “socket”.
- El socket se utiliza para identificar el servidor y el servicio que solicita el cliente.
- Se combinan dos sockets para formar un par de sockets: (192.168.1.5:1099, 192.168.1.7:80).
- Los sockets permiten que varios procesos que se ejecutan en un cliente y que varias conexiones a un proceso de servidor se distingan entre sí.

■ Grupos de números de puerto

- La IANA ha creado tres grupos de números de puerto:
- Puertos conocidos (0 a 1023)
- Puertos registrados (1024 a 49151)
- Puertos privados y/o dinámicos (49152 a 65535)

■ El comando netstat

- Netstat permite que un usuario vea las conexiones activas en un host.
- Netstat también muestra el proceso que está utilizando la conexión.

C:\> netstat				
Active Connections				
Proto	Local Address	Foreign Address	State	
TCP	kenpc:3126	192.168.0.2:netbios-ssn	ESTABLISHED	
TCP	kenpc:3158	207.138.126.152:http	ESTABLISHED	
TCP	kenpc:3159	207.138.126.159:http	ESTABLISHED	
TCP	kenpc:3160	207.138.126.169:http	ESTABLISHED	
TCP	kenpc:3161	sc.msn.com:http	ESTABLISHED	
TCP	kenpc:3166	www.cisco.com:http	ESTABLISHED	

9.2 TCP y UDP





Protocolos de la capa de transporte

Proceso de comunicación en TCP

■ Procesos del servidor TCP

- Cada proceso de aplicación que se ejecuta en el servidor utiliza un número de puerto.
- Un servidor individual no puede tener dos servicios asignados al mismo número de puerto dentro del mismo servicio de la capa de transporte.
- Una aplicación de servidor activa asignada a un puerto específico se considera abierta.
- Toda solicitud entrante de un cliente dirigida a un puerto abierto se acepta y se procesa en la aplicación de servidor conectada a dicho puerto.
- Pueden existir muchos puertos abiertos simultáneamente en un servidor, uno para cada aplicación de servidor activa.

■ Establecimiento de conexiones TCP

- Una conexión TCP se establece en tres pasos:
 - El cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor.
 - El servidor acusa recibo de la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.
 - El cliente de origen acusa recibo de la sesión de comunicación de servidor a cliente.



Protocolos de la capa de transporte

Proceso de comunicación en TCP (continuación)

■ Terminación de una sesión TCP

- El indicador TCP FIN se utiliza para terminar una conexión TCP.
 - Cuando el cliente no tiene más datos para enviar en la transmisión, envía un segmento con el indicador FIN establecido.
 - El servidor envía un ACK para acusar recibo del FIN para terminar la sesión de cliente a servidor.
 - El servidor envía un FIN al cliente para terminar la sesión de servidor a cliente.
 - El cliente responde con un ACK para dar acuse de recibo del FIN desde el servidor.
 - Una vez reconocidos todos los segmentos, la sesión se cierra.

■ Análisis del enlace de tres vías de TCP

- El 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

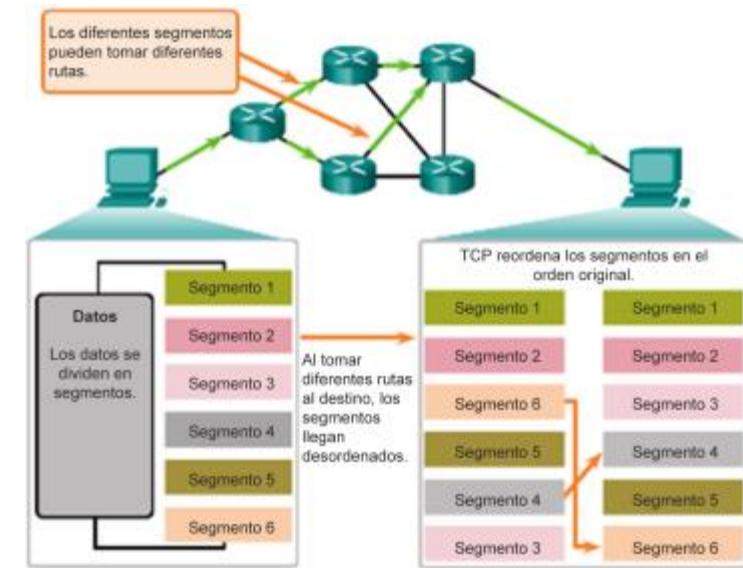


Protocolos de la capa de transporte

Confiabilidad y control de flujo

■ Confiabilidad de TCP: entrega ordenada

- Los segmentos TCP utilizan números de secuencia para identificar exclusivamente a cada segmento y dar acuse de recibo de ellos, hacer un seguimiento del orden de segmentos e indicar la forma en que se vuelven a armar y a reordenar los segmentos recibidos.
- Durante la configuración de la sesión TCP, se elige un número de secuencia inicial (ISN) al azar. Despues, el ISN se incrementa con el número de bytes transmitidos.
- El proceso de TCP receptor reúne los datos de los segmentos en el búfer hasta que se reciban y se vuelvan a armar todos los datos.
- Los segmentos que no se reciben en el orden correcto se conservan para su posterior procesamiento.
- Los datos se entregan a la capa de aplicación solo cuando se hayan recibido y vuelto a armar por completo.

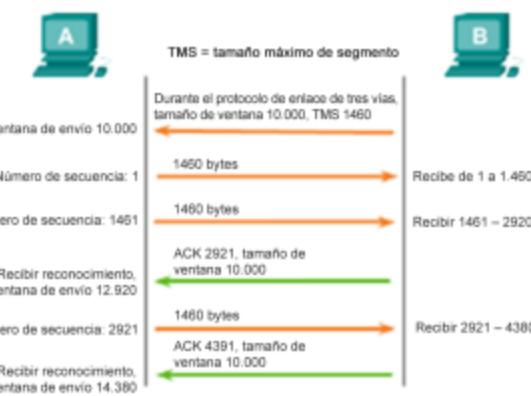




Protocolos de la capa de transporte

Confiabilidad y control de flujo (continuación)

- Control del flujo en TCP: Tamaño de la ventana y acuses de recibo
 - TCP también proporciona mecanismos para el control del flujo.
 - El control del flujo asegura que las terminales TCP puedan recibir y procesar datos de manera confiable.
 - TCP administra el control del flujo mediante el ajuste de la velocidad del flujo de datos entre el origen y el destino en una sesión determinada.
 - La función de control del flujo en TCP depende de un campo del encabezado TCP de 16 bits denominado Tamaño de ventana. El tamaño de ventana es la cantidad de bytes que el dispositivo de destino de una sesión TCP puede aceptar y procesar al mismo tiempo.
 - El origen y el destino TCP acuerdan el tamaño de ventana inicial cuando se establece la sesión TCP.
 - De ser necesario, los terminales TCP pueden ajustar el tamaño de ventana durante una sesión.

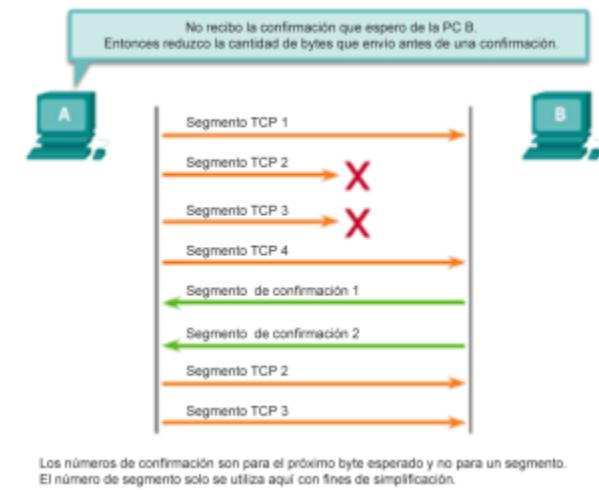




Protocolos de la capa de transporte

Confiabilidad y control de flujo (continuación)

- Control del flujo de TCP: prevención de congestiones
 - La congestión de red suele dar como resultado el descarte de paquetes.
 - Los segmentos TCP que no se entregan activan la retransmisión. La retransmisión de segmentos TCP puede empeorar la congestión.
 - El origen puede estimar un nivel determinado de congestión de red al observar la velocidad a la que se envían los segmentos TCP sin acusar recibo.
 - El origen puede reducir la cantidad de bytes que envía antes de recibir un acuse de recibo cuando se detecta la congestión.
 - El origen reduce la cantidad de bytes que envía sin acuse de recibo y no el tamaño de ventana, el cual lo determina el destino.
 - El destino suele desconocer la congestión de red y considera que no es necesario sugerir un nuevo tamaño de ventana.





Protocolos de la capa de transporte

Comunicación en UDP

- UDP: Baja sobrecarga vs. confiabilidad
 - UDP tiene mucha menos sobrecarga que TCP.
 - UDP no está orientado a la conexión y no proporciona los mecanismos sofisticados de retransmisión, secuenciación y control del flujo.
 - Las aplicaciones que ejecutan UDP aún pueden utilizar la confiabilidad, pero se debe implementar en la capa de aplicación.
 - Sin embargo, UDP no es inferior.
- Rearmado de datagramas UDP
 - UDP simplemente vuelve a armar los datos en el orden en el que se recibieron.
 - Si es necesario, la aplicación debe identificar la secuencia correcta.
- Procesos y solicitudes del servidor UDP
 - A las aplicaciones de servidor basadas en UDP se les asignan números de puerto conocidos o registrados.
 - Las solicitudes que se reciben en un puerto específico se reenvían a la aplicación adecuada según los números de puerto.



Protocolos de la capa de transporte

Comunicación en UDP (continuación)

■ Procesos de cliente UDP

- La comunicación entre cliente y servidor UDP también se inicia con una aplicación cliente.
- El proceso de cliente UDP selecciona de manera dinámica un número de puerto y lo utiliza como puerto de origen.
- Por lo general, el puerto de destino es el número de puerto conocido o registrado que se asigna al proceso de servidor.
- Se utiliza el mismo par de puertos de origen o destino en el encabezado de todos los datagramas usados en la transacción.
- En la devolución de datos del servidor al cliente, se invierten los números de puerto de origen y de destino en el encabezado del datagrama.



Protocolos de la capa de transporte

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.
- Aplicaciones que utilizan UDP
 - Aplicaciones multimedia y de video en vivo: pueden tolerar cierta pérdida de datos, pero requieren demoras breves o que no haya demoras. Los ejemplos incluyen VoIP y la transmisión de vídeo 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 en las que no se requiere control de flujo, detección de errores, acuses de recibo ni recuperación de errores, o en las que la aplicación pueda ocuparse de estas tareas.
Los ejemplos incluyen SNMP y TFTP.

9.3 Resumen





Resumen del capítulo

Resumen

- Implementar un esquema de direccionamiento IPv4 para permitir una conectividad completa en una red de pequeña o mediana empresa.
- Dado un conjunto de requisitos, implementar un esquema de direccionamiento VLSM para proporcionar conectividad a usuarios finales en una red pequeña o mediana.
- Explicar las consideraciones de diseño para implementar IPv6 en una red comercial.





JULIO ANTHONY ENGELS RUIZ COTO - 1284719

Hoja de trabajo Capa de transporte

Responda las siguientes preguntas.

1. ¿Cuál es el rango de puertos “Bien conocidos” para TCP y UDP?

R// los puertos “bien conocidos” van del 0 al 1023 son como números de teléfono que son especiales para ciertas aplicaciones de internet.

2. ¿A qué se refiere el concepto de “Confiabilidad de la capa de transporte” y cuáles son las tres operaciones básicas de TCP para lograrlo?

R// es como asegurarse de que una carta llegue a su destino sin daños y en orden el TCP lo hace mediante, revisando errores, asegurándose de no enviar demasiado rápido, ajustando él envío según el tráfico de la red.

3. Describa brevemente la función de la capa de transporte.

R// esta capa tiene como objetivo proporcionar comunicación de extremo a extremo entre dos dispositivos en una red, dicho esto se encarga de segmentar, secuenciar y asegurar la entrega de datos entre las aplicaciones de dos dispositivos.

4. Mencione 4 campos importantes del encabezado TCP de un segmento.

R// puerto de origen, puerto destino, numero de secuencia, (ACK)

5. Describa qué es un socket y cómo está compuesto.

R// el socket es un punto final de una conexión de red que se utiliza para enviar o recibir datos, este está compuesto por una dirección IP y un numero de puerto y juntos identifican un punto final específico en una red.

6. Describa la diferencia entre TCP y UDP.

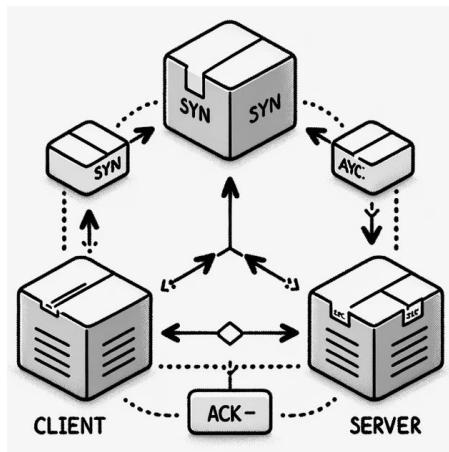
R// TCP, es un protocolo orientado a la conexión, confiable y orientado al flujo, asegura la entrega ordenada y sin errores de los datos.

UDP es un protocolo sin conexión y no garantiza la entrega de paquetes es más rápido y ligero que TCP, pero este es menos confiable.

7. ¿Cuál es el comando utilizado tanto en Windows como en Linux para verificar estado de las conexiones de red del sistema?

R// el comando es el “netstat”

8. Describa por medio de un diagrama el proceso de establecimiento de una conexión TCP a través de three-way handshake.



SYN: El cliente envía un paquete SYN (synchronize) al servidor solicitando la apertura de una conexión.

SYN-ACK: En respuesta al paquete SYN, el servidor envía un paquete SYN-ACK al cliente. Este

ACK: Finalmente, el cliente envía un paquete ACK (reconocimiento) al servidor, reconociendo el número de secuencia del servidor.

9. ¿Qué es y para qué se utiliza el “tamaño de la ventana” en el encabezado de un segmento TCP?

R// se refiere a la cantidad de bytes que un receptor está dispuesto a aceptar, se utiliza para el control de flujo, permitiendo al receptor decirle al emisor cuantos bytes está dispuesto a recibir antes de enviar un ACK.

10. ¿Qué diferencia un segmento de un datagrama?

R// un segmento es un paquete de datos de TCP, y un datagrama es un paquete de datos de UDP.

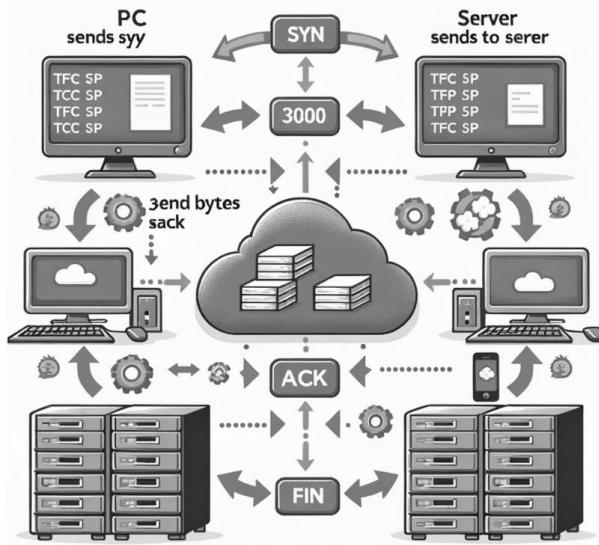
11. Explique el paradigma Cliente-Servidor

R// es un modelo de comunicación en el que un servidor proporciona recursos o servicios y los clientes acceden y utilizan esos recursos o servicios, el servidor espera solicitudes de los clientes las procesa y luego envía una respuesta.

12. ¿Qué es un puerto efímero?

R// es un puerto temporal utilizado para una sesión o conexión específica, estos puertos están en el rango de 1024 a 4951 y son asignados automáticamente por el sistema operativo.

13. Una PC necesita descargar un archivo de 12KB de un servidor FTP y el servidor tiene definida una ventana TCP de 3000 bytes. Detalle y haga un diagrama paso a paso de:



- a. El proceso de establecimiento de la conexión**
El cliente envía un segmento SYN al servidor para solicitar la conexión.
El servidor responde con un segmento SYN-ACK indica que esta dispuesto a establecer la conexión.
El cliente responde con un segmento ACK para que se confirme la conexión.
- b. El proceso de transferencia de los datos**
La ventana TCP de 3000 bytes enviara los primeros 3000 bytes del archivo
El cliente reciba esos 3000 bytes enviara un ACK al servidor
Este servidor enviara los siguientes 3000 bytes
Después de recibir esos 3000 bytes el cliente envía otro ACK al servidor
Y esto se repite hasta que se transfieran los 12KB completos, se requieren 4 ventanas para transferir el archivo.
- c. El proceso de finalización de la conexión**
Cuando el archivo se transferido completo el cliente enviara un segmento fin al servidor para indicar que se desea cerrar la conexión.
El servidor responderá con un segmento ACK para confirmar que ha recibido la solicitud de finalización.
El servidor enviara su propio segmento FIN al cliente.
Este cliente responderá con un ACK para confirmar que ha recibido el segmento FIN del servidor y se cerrara la conexión.



Capítulo 9: NAT para IPv4



Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™



Capítulo 9: Secciones y objetivos

- 9.1 Protocolos de capa de red
 - Explicar la forma en la que NAT proporciona escalabilidad de direcciones IPv4 en la red de una pequeña a mediana empresa.
- 9.2 Configuración de NAT
 - Configurar servicios NAT en el router perimetral para proporcionar la escalabilidad de las direcciones IPv4 en una red de una pequeña a mediana empresa.
- 9.3 Solucionar problemas en configuraciones de NAT
 - Solucionar problemas de NAT en la red de una pequeña a mediana empresa.

9.1 Funcionamiento de NAT

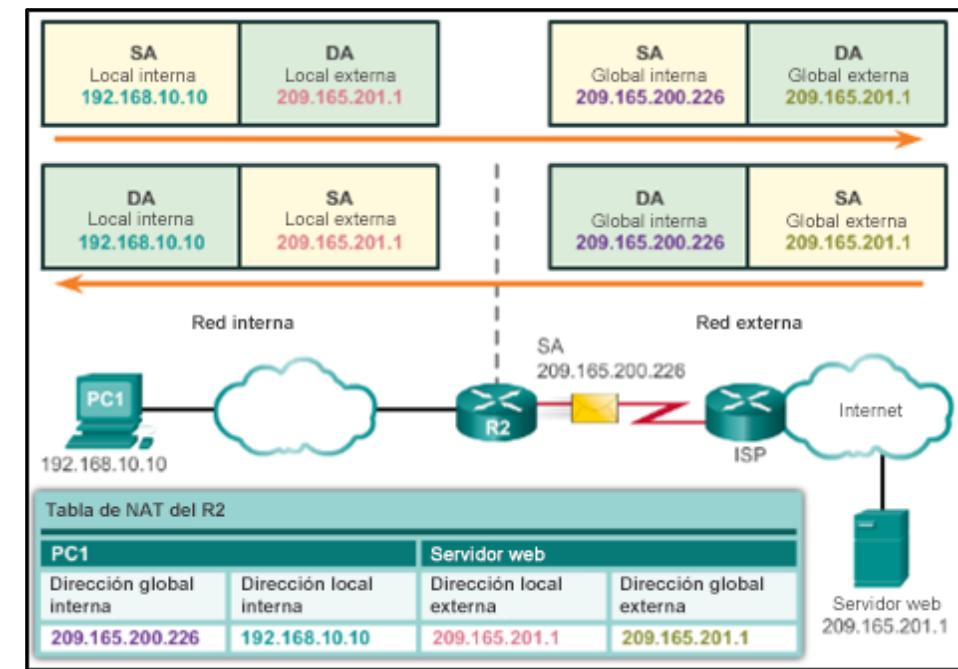




Funcionamiento de NAT

Características de NAT

- Espacio de direcciones IPv4 privadas
 - 10.0.0.0 /8, 172.16.0.0 /12 y 192.168.0.0 /16
- ¿Qué es NAT?
 - El proceso para traducir direcciones de red IPv4
 - Conserva las direcciones IPv4 públicas
 - Se configura en el router de frontera para la traducción
- Terminología de NAT
 - Dirección interna
 - Dirección local interna
 - Dirección global interna
 - Dirección externa
 - Dirección local externa
 - Dirección global externa





Funcionamiento de NAT

Tipos de NAT

NAT estática

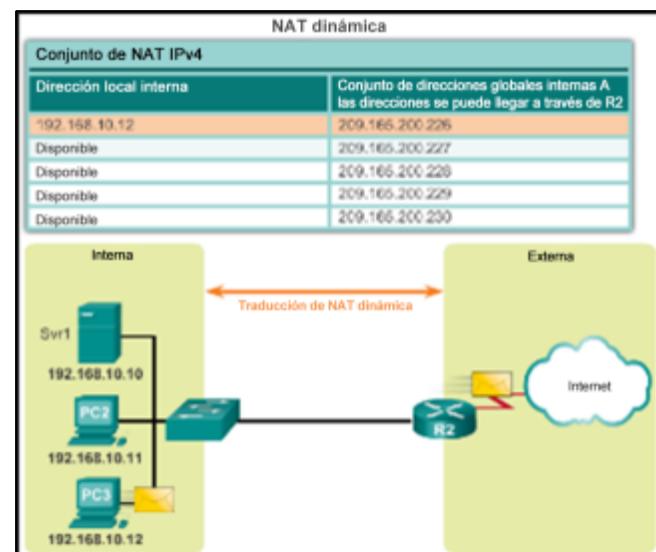
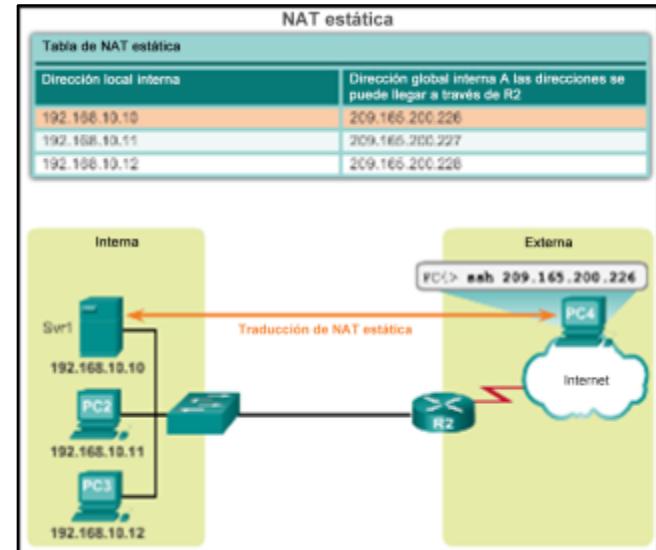
- Asignación uno a uno entre direcciones locales y globales.
- Es configurada por el administrador de red y se mantienen constantes.

NAT dinámica

- Utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada.
- Requiere que haya suficientes direcciones públicas para la cantidad total de sesiones de usuario simultáneas.

Traducción de la dirección del puerto (PAT)

- Asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública o a unas pocas direcciones.
- También se conoce como sobrecarga de NAT.
- Valida que los paquetes entrantes hayan sido solicitados.
- Utiliza números de puerto para reenviar los paquetes de respuesta al dispositivo interno correcto.





Funcionamiento de NAT

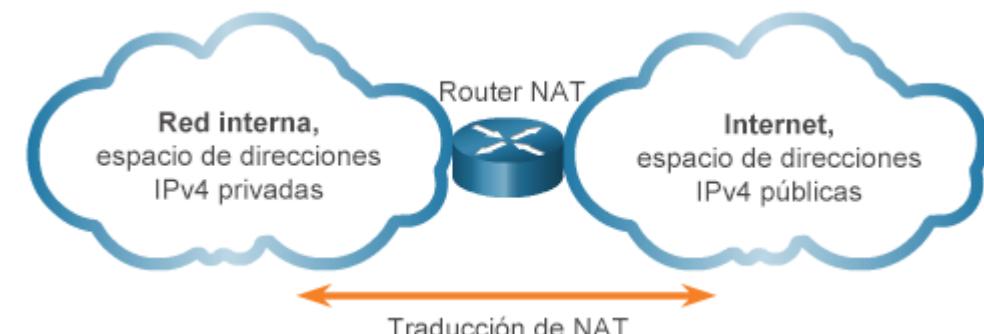
Ventajas de NAT

■ Ventajas de NAT

- Conserva el esquema de direccionamiento legalmente registrado.
- Aumenta la flexibilidad de las conexiones a la red pública.
- Proporciona coherencia a los esquemas de direccionamiento de red interna.
- Proporciona seguridad de red.

■ Desventajas de NAT

- Se deteriora el rendimiento.
- Se deteriora la funcionalidad de extremo a extremo.
- Se reduce el seguimiento IP de extremo a extremo.
- La tunelización se torna más complicada.
- Puede interrumpirse la inicialización de conexiones TCP.



9.2 Configuración de NAT





Configuración de NAT

Configuración de NAT estática

- Configuración de NAT estática

- Crear la asignación entre las direcciones locales internas y locales externas.

```
ip nat inside source static ip-local ip-global
```

- Definir qué interfaces pertenecen a la red interna y cuáles a la red externa.

```
ip nat inside
```

```
ip nat outside
```

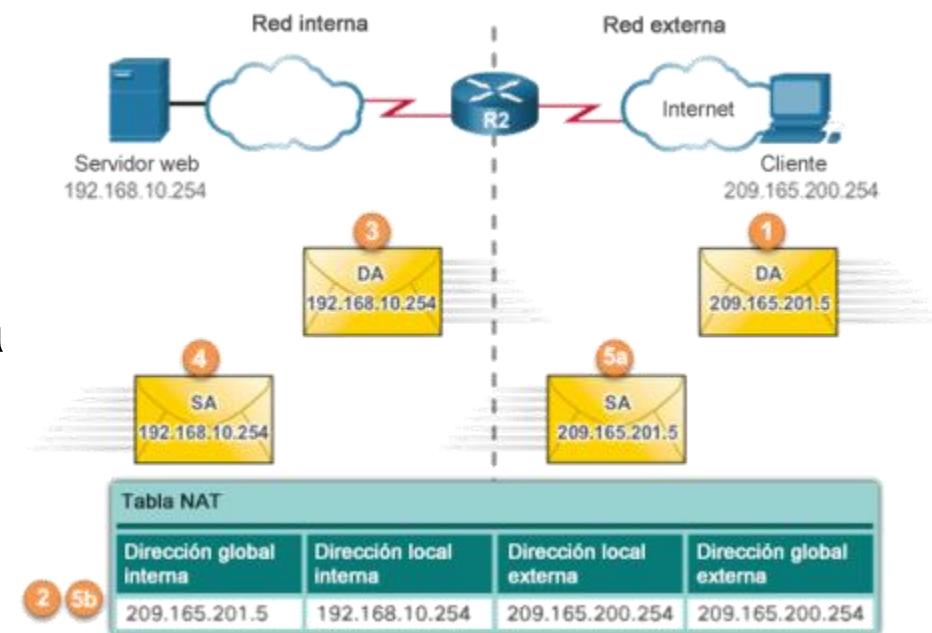
- Análisis de NAT estática

- Verificación de NAT estática

```
show ip nat translations
```

```
show ip nat statistics
```

```
clear ip nat statistics
```





Configuración de NAT

Configuración de NAT dinámica

■ Funcionamiento de NAT dinámica

- El conjunto de direcciones IPv4 públicas (conjunto de direcciones globales internas) se encuentra disponible para cualquier dispositivo en la red interna según el orden de llegada.
- Con NAT dinámica, una única dirección interna se traduce a una única dirección externa.
- El conjunto debe ser lo suficientemente grande como para admitir todos los dispositivos internos.
- Un dispositivo no puede comunicarse con ninguna red externa si no hay direcciones disponibles en el conjunto.



Configuración de NAT

Configuración de NAT dinámica (continuación)

- Configuración de NAT dinámica
 - Crear la asignación entre las direcciones locales internas y locales externas.

```
ip nat pool name ip-inicial ip-final {netmask máscara-de-red | prefix-length longitud-de-prefijo}
```

- Crear una ACL estándar para permitir la traducción de esas direcciones.

```
access-list número-de-lista-de-acceso permit origen  
[comodín-de-origen]
```

- Vincular la ACL al conjunto.

```
ip nat inside source list número-de-lista-de-acceso pool  
nombre
```

- Identificar las interfaces internas y externas.

```
ip nat inside
```

```
ip nat outside
```



Configuración de NAT

Configuración de NAT dinámica (continuación)

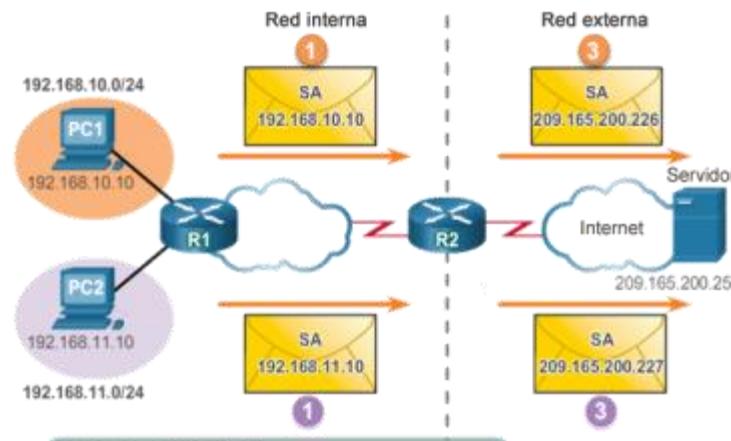
- Análisis de NAT dinámica
- Verificación de NAT dinámica

show ip nat translations

show ip nat translations verbose

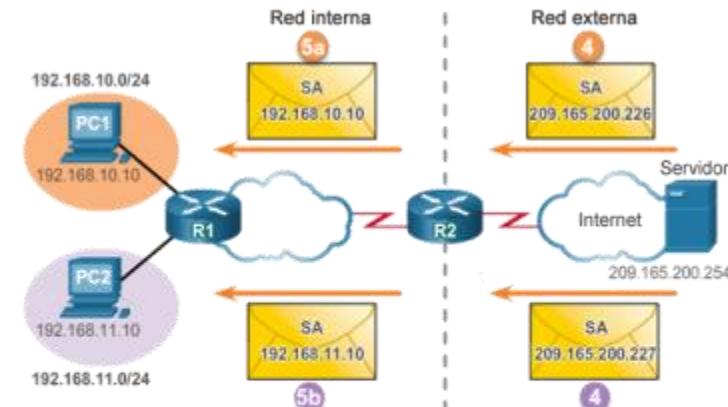
clear ip nat statistics

clear ip nat translations *



Conjunto de NAT IPv4

Conjunto de direcciones locales internas	Dirección global interna
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227



Conjunto de NAT IPv4

Conjunto de direcciones locales internas	Dirección global interna
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227



Configuración de NAT

Configuración de la Traducción de direcciones de puertos (PAT)

- Configuración de PAT: conjunto de direcciones
 - Crear la asignación entre las direcciones locales internas y locales externas.

```
ip nat pool name ip-inicial ip-final {netmask máscara-de-red |  
prefix-length longitud-de-prefijo}
```

- Crear una ACL estándar para permitir la traducción de esas direcciones.

```
access-list número-de-lista-de-acceso permit origen [comodín-  
de-origen]
```

- Vincular la ACL al conjunto.

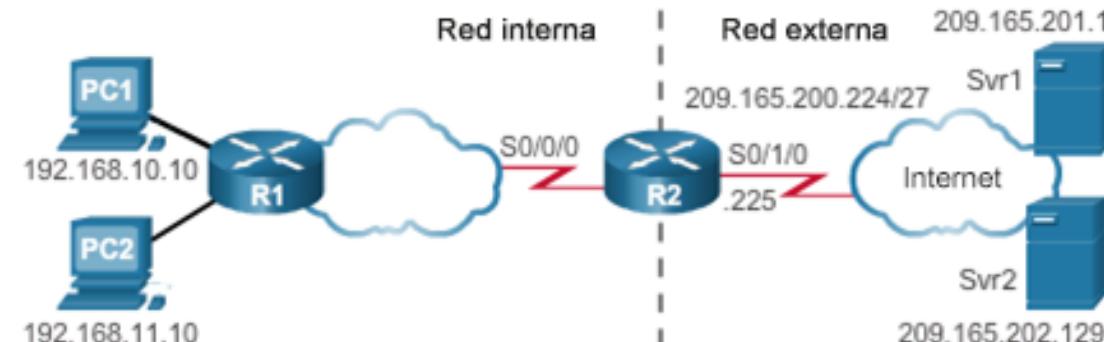
```
ip nat inside source list número-de-lista-de-acceso pool nombre
```

- Identificar las interfaces internas y externas.

```
ip nat inside
```

```
ip nat outside
```

Ejemplo de PAT con conjunto de direcciones





Configuración de NAT

Configuración de la Traducción de direcciones de puertos (PAT) (continuación)

- Configuración de PAT: dirección única

- Definir una ACL estándar para permitir la traducción de esas direcciones.

```
access-list número-de-lista-de-acceso permit origen [comodín-de-origen]
```

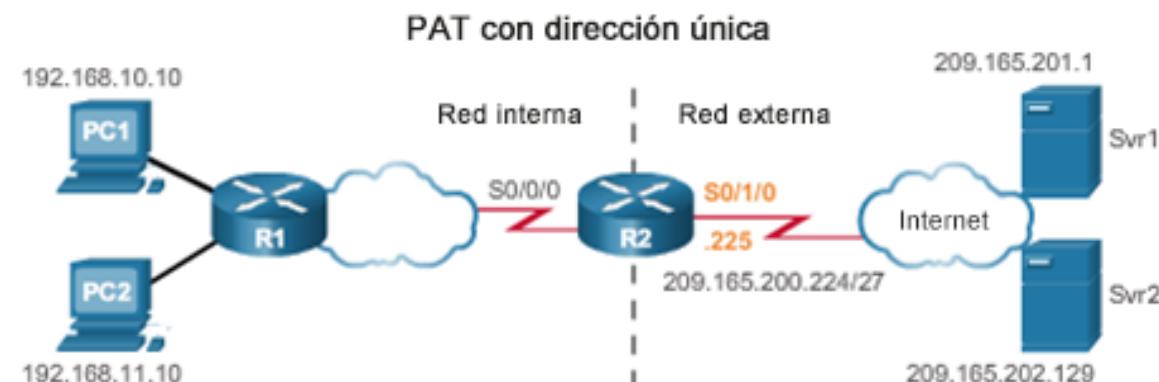
- Establecer la traducción de origen dinámica, especificar la ACL, la interfaz de salida y la opción de sobrecarga.

```
ip nat inside source list número-de-lista-de-acceso  
interface type nombre overload
```

- Identificar las interfaces internas y externas.

```
ip nat inside
```

```
ip nat outside
```





Configuración de NAT

Configuración de la Traducción de direcciones de puertos (PAT) (continuación)

- Análisis de PAT
- Verificación de una PAT

`show ip nat translations`

`show ip nat statistics`

`clear ip nat statistics`

Análisis de PAT de las computadoras a los servidores

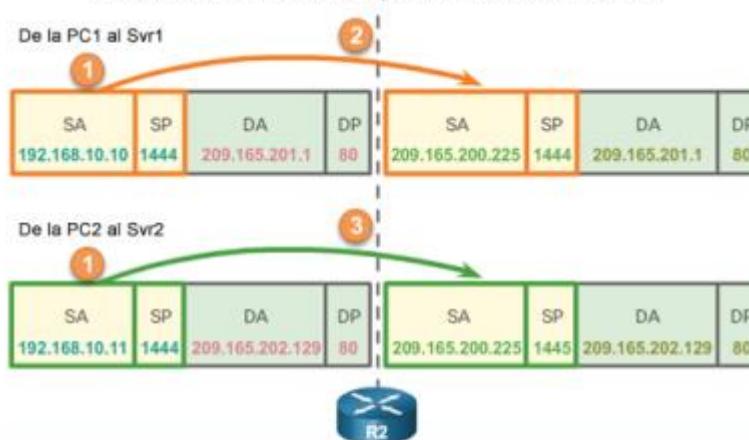


Tabla NAT

Dirección local interna	Dirección global interna	Dirección global externa	Dirección local externa
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

Análisis de PAT de los servidores a las computadoras

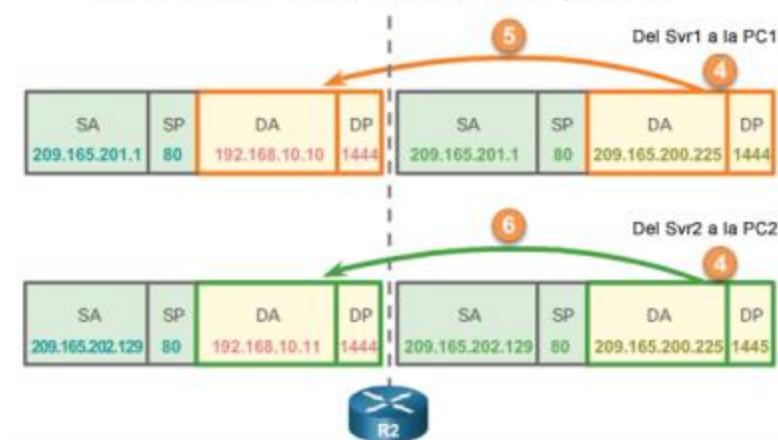


Tabla NAT

Dirección local interna	Dirección global interna	Dirección global externa	Dirección local externa
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

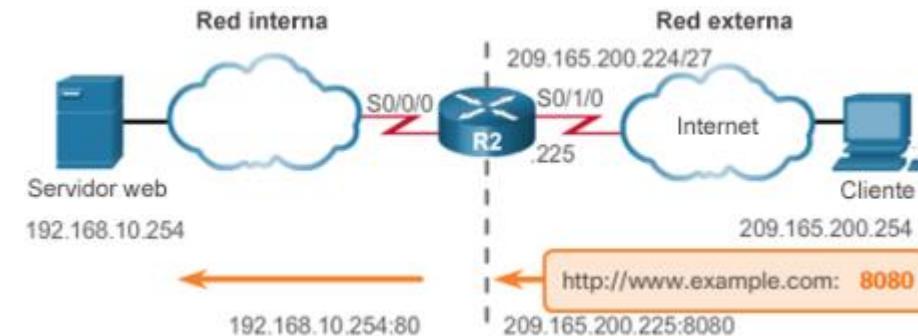
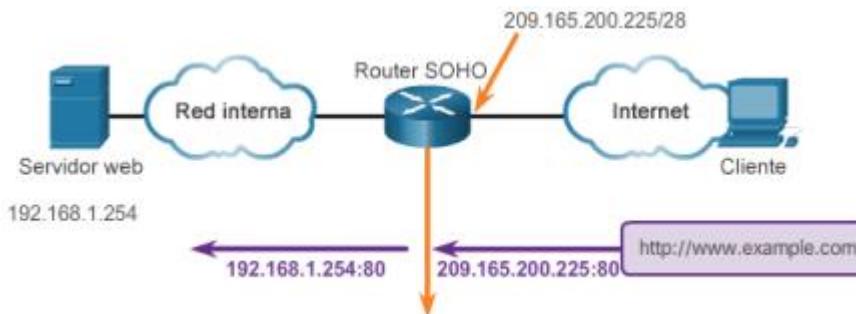


Configuración de NAT

Reenvío a puerto asignado

- Reenvío a puerto asignado
 - El reenvío a puerto asignado es el acto de reenviar un puerto de red de un nodo de red a otro.
 - Un paquete que se envía a la dirección IP pública y al puerto de un router se puede reenviar a una dirección IP privada y a un puerto en la red interna.
 - El reenvío a puerto asignado es útil en situaciones en las que los servidores tienen direcciones privadas a las que no se puede llegar desde las redes externas.
- Ejemplo de router inalámbrico
- Configuración de reenvío a puerto asignado con IOS

```
ip nat inside source [static {tcp | udp ip-local puerto-local ip-global puerto-global} [extendable]]
```





Configuración de NAT

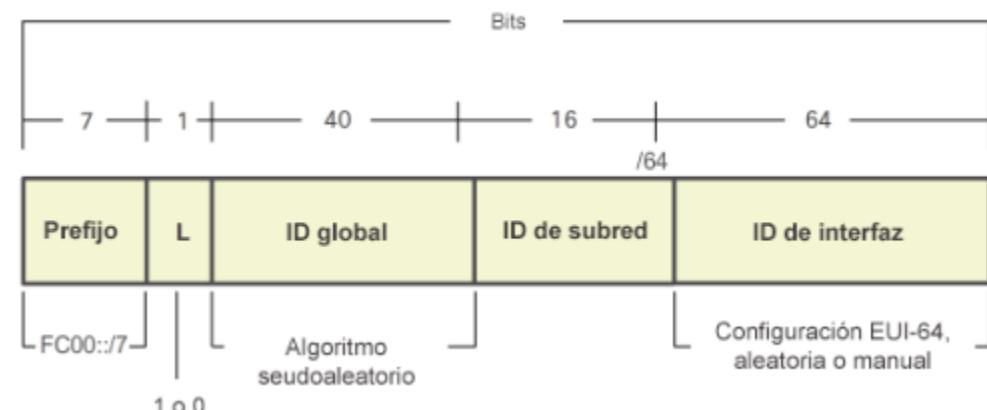
Configuración de NAT e IPv6

■ ¿NAT para IPv6?

- Con una dirección de 128 bits, IPv6 proporciona 340 sextillones de direcciones.
- El espacio de direcciones no presenta un problema para IPv6.
- Por diseño, IPv6 hace que sea innecesario el proceso de traducción NAT de direcciones IPv4 públicas a privadas; sin embargo, en IPv6 se implementa una forma de direcciones privadas, y se hace de un modo diferente que en el caso de IPv4.

■ Dirección IPv6 local única

- Las direcciones IPv6 locales únicas (ULA) están diseñadas para permitir las comunicaciones IPv6 dentro de un sitio local.
- Las ULA no están diseñadas para proporcionar espacio de direcciones IPv6 adicional.
- Las ULA tienen el prefijo FC00::/7, lo que deriva en un primer rango de hextetos de FC00 a FDFF.
- Las ULA también se conocen como direcciones IPv6 locales (que no se deben confundir con las direcciones IPv6 link-local).

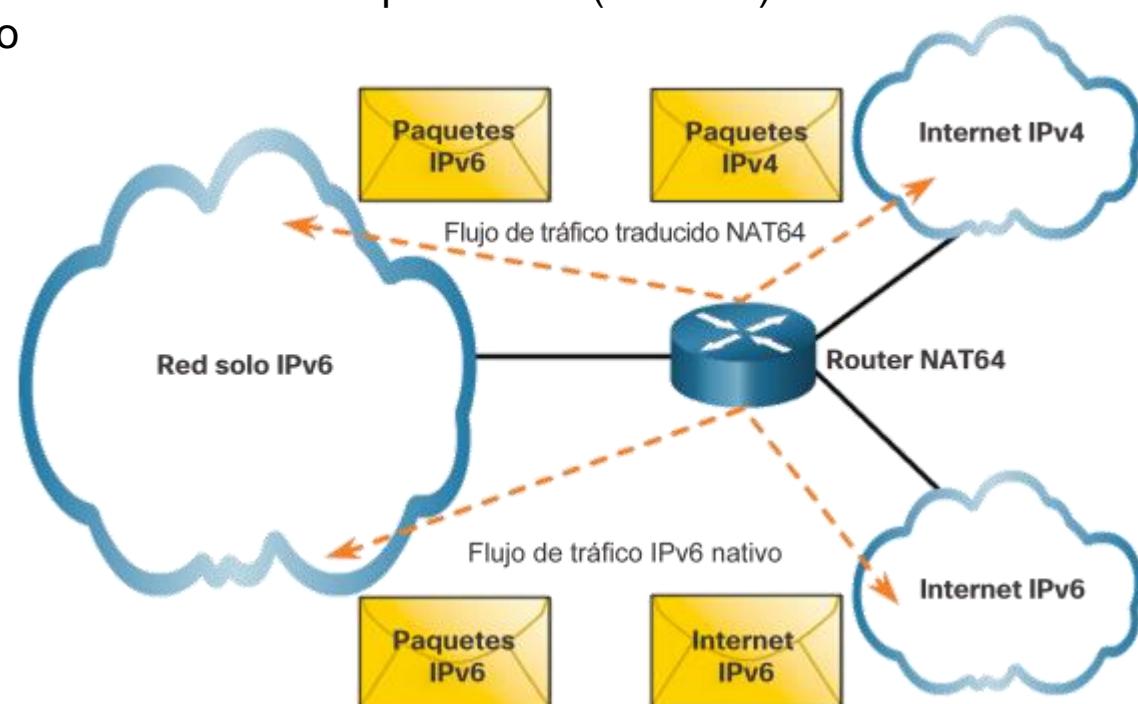




Configuración de NAT

Configuración de NAT e IPv6 (continuación)

- NAT para IPv6
 - IPv6 también utiliza NAT, pero en un contexto muy diferente.
 - En IPv6, NAT se utiliza para proporcionar una comunicación transparente entre IPv6 e IPv4.
 - El propósito de NAT64 no es ser una solución permanente; se implementa como un mecanismo de transición.
 - La Traducción de direcciones de red-Traducción de protocolos (NAT-PT) era otro mecanismo de transición basado en NAT para IPv6, pero el IETF lo dejó en desuso.
 - Ahora se recomienda utilizar NAT64.



9.3 Resolución de problemas de NAT





Solucionar problemas en NAT

Solucionar problemas en configuraciones de NAT

- Solución de problemas en NAT: comandos show

```
clear ip nat statistics
```

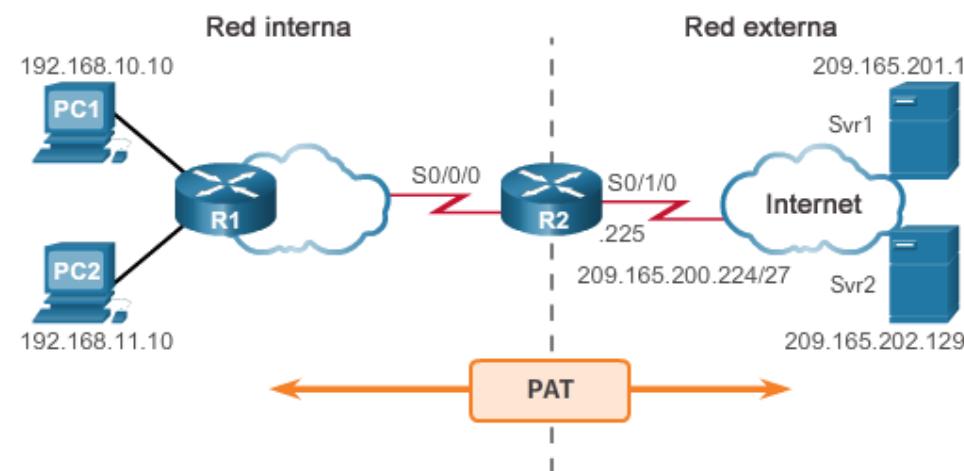
```
clear ip nat translations *
```

```
show ip nat statistics
```

```
show ip nat translations
```

- Solución de problemas en NAT: comandos debug

```
debug ip nat
```



9.4 Resumen del capítulo





Resumen del capítulo

Resumen

- Se explicó cómo se utiliza NAT para contribuir a mitigar el agotamiento del espacio de direcciones IPv4.
- NAT conserva el espacio de direcciones públicas y reduce la sobrecarga administrativa de forma considerable al administrar las adiciones, los movimientos y las modificaciones.
- NAT para IPv4, incluido lo siguiente:
 - Características, terminología y operaciones generales de NAT
 - Distintos tipos de NAT: NAT estática, NAT dinámica y NAT con sobrecarga.
 - Beneficios y desventajas de NAT.
- Configuración, verificación y análisis de NAT estática, NAT dinámica y NAT con sobrecarga.
- Cómo puede utilizarse el reenvío a puerto asignado para acceder a dispositivos internos desde Internet.
- Solución de problemas en NAT mediante los comandos **show** y **debug**.
- Cómo se utiliza NAT para IPv6 para traducir entre direcciones IPv6 y direcciones IPv4.

Cisco | Networking Academy®

Mind Wide Open™





Capítulo 10: Capa de aplicación



Introducción a Networks v6.0

Cisco | Networking Academy®
Mind Wide Open™



Capítulo 10: Secciones y objetivos

10.0 Introducción

10.1 Protocolos de capa de aplicación

- Explicar la forma en que las funciones de la capa de aplicación, de la capa de sesión y de la capa de presentación operan conjuntamente para proporcionar servicios de red a las aplicaciones de usuario final.
- Explicar la forma en que los protocolos de capa de aplicación comunes interactúan con las aplicaciones de usuario final.

10.2 Protocolos y servicios de capa de aplicación reconocidos

- Explicar la forma en que funcionan los protocolos web y de correo electrónico.
- Explicar la forma en que funcionan los protocolos de asignación de direcciones IP.
- Explicar la forma en que funcionan los protocolos de transferencia de archivos.

10.3 Resumen

10.1 Protocolos de capa de aplicación





Protocolos de la capa de aplicación

Aplicación, Presentación, Sesión

■ Capa de aplicación

- Es la más cercana al usuario final.
- Los protocolos de capa de aplicación permiten el intercambio de datos entre programas que se ejecutan en los hosts de origen y de destino.
- La capa de aplicación TCP/IP realiza las funciones de las tres capas superiores del modelo OSI.
- Los protocolos de capa de aplicación comunes incluyen HTTP, FTP, TFTP y DNS.

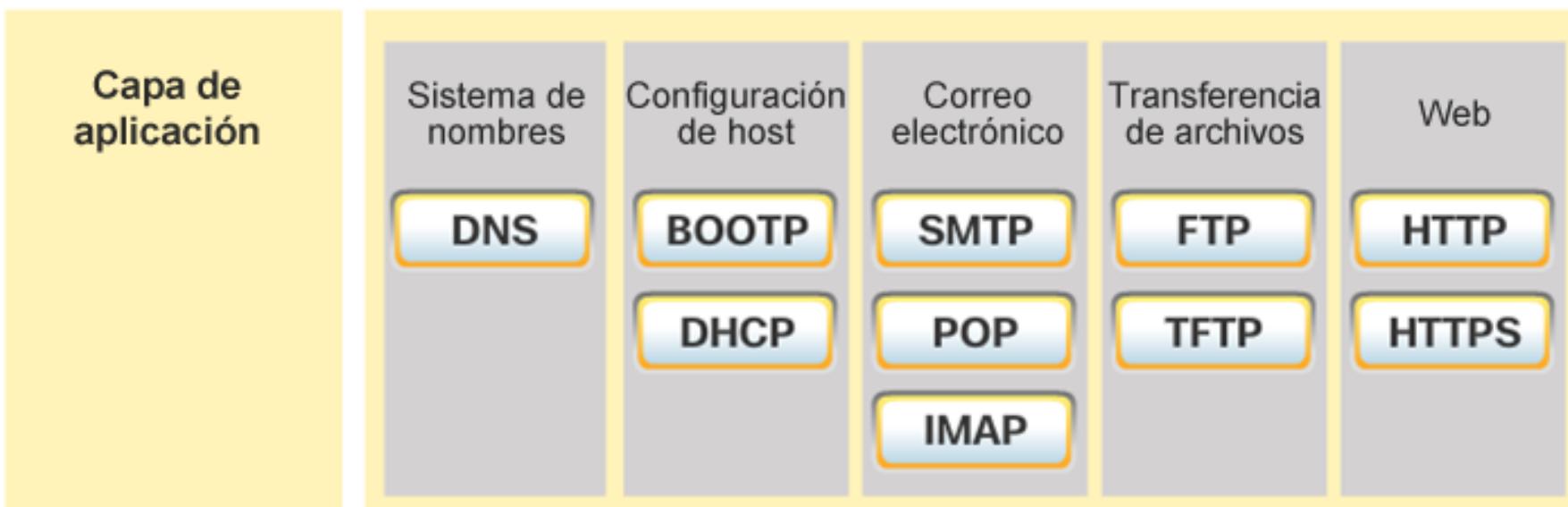
■ Capa de presentación y sesión

- Dar formato a los datos, comprimir y cifrar datos
- Los estándares comunes de video incluyen QuickTime y el Grupo de expertos en películas (MPEG).
- Los formatos de imágenes gráficas comunes son: GIF, JPEG y PNG.
- La capa de sesión crea y mantiene diálogos entre las aplicaciones de origen y de destino.
- La capa de sesión maneja el intercambio de información para iniciar diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o que estuvieron inactivas.



Protocolos de la capa de aplicación Aplicación, Presentación, Sesión (continuación)

- Protocolos de capa de aplicación de TCP/IP
 - Los protocolos de aplicación de TCP/IP especifican la información de control y el formato necesarios para funciones comunes de Internet.
 - Los protocolos de capa de aplicación se deben implementar tanto en los dispositivos de origen como en los de destino.
 - Los protocolos de capa de aplicación que se implementan en el host de origen y de destino deben ser compatibles para permitir la comunicación.





Protocolos de capa de aplicación

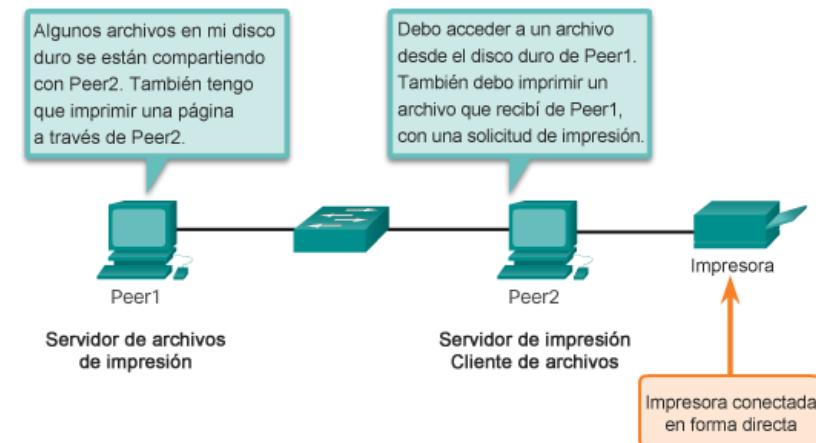
Cómo interactúan los protocolos de aplicación con las aplicaciones para usuarios finales

■ Modelo cliente-servidor

- Los clientes solicitan información y los servidores la proporcionan.
- Los procesos de cliente y servidor se consideran parte de la capa de aplicación.
- El contenido del intercambio de datos dependerá de la aplicación en uso.
- El correo electrónico es un ejemplo de una interacción de cliente y servidor.

■ Redes punto a punto

- A los datos se accede sin utilizar un servidor exclusivo.
- Se pueden conectar dos o más computadoras a una red P2P para compartir recursos.
- Toda terminal conectada (conocida como “punto”) puede funcionar como servidor y como cliente.
- Las funciones de cliente y servidor se establecen por solicitud.





Protocolos de capa de aplicación

Cómo interactúan los protocolos de aplicación con las aplicaciones para usuarios finales (continuación)

■ Aplicaciones punto a punto

- Algunas aplicaciones P2P utilizan un sistema híbrido, donde se descentraliza el uso compartido de recursos.
- Los índices que señalan las ubicaciones de recursos se almacenan en un directorio centralizado.
- En un sistema híbrido, cada punto accede a un servidor de índice para obtener la ubicación de un recurso almacenado en otro punto.

■ Aplicaciones P2P comunes

- Entre las redes P2P comunes se encuentran eDonkey, G2 y BitTorrent.
- Muchas aplicaciones P2P permiten que los usuarios compartan partes de varios archivos con otro usuario a la vez.
- Un archivo torrent pequeño contiene información sobre la ubicación de otros usuarios y de rastreadores.
- Los rastreadores son computadoras que hacen un seguimiento de los archivos que están alojados en los dispositivos de los usuarios.
- Esta tecnología se denomina BitTorrent. Existen muchos clientes BitTorrent, incluidos BitTorrent, uTorrent, Frostwire y qBittorrent.

10.2 Protocolos y servicios de capa de aplicación reconocidos





Protocolos y servicios de capa de aplicación reconocidos

Protocolos web y de correo electrónico

- Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto
 - Una dirección URL es una referencia a un servidor web.
 - Los nombres que la mayoría de las personas asocia con las direcciones web son URL y URI.
 - Las URL contienen el protocolo, el nombre del servidor y el nombre de archivo solicitado.
 - Con DNS, la porción del nombre del servidor de la URL se traduce entonces a la dirección IP asociada para que se pueda contactar al servidor.
- HTTP y HTTPS
 - El navegador envía una solicitud GET a la dirección IP del servidor y solicita el archivo index.html.
 - El servidor envía al cliente el archivo solicitado.
 - En la URL se especificó el archivo index.html, y contiene el código HTML para esta página web.
 - El navegador procesa el código HTML y da formato a la página para la ventana del navegador según el código del archivo.
 - HTTP no es seguro. Los mensajes se pueden interceptar.
 - HTTPS utiliza autenticación y cifrado para asegurar los datos.



Protocolos y servicios de capa de aplicación reconocidos

Protocolos web y de correo electrónico (continuación)

■ Protocolos de correo electrónico

- El correo electrónico es un método de almacenamiento y envío que se utiliza para enviar, almacenar y recuperar mensajes electrónicos.
- Los mensajes de correo electrónico se almacenan en servidores de correo.
- Los clientes de correo electrónico se comunican con servidores de correo para enviar y recibir mensajes de correo electrónico.
- Los servidores de correo se comunican con otros servidores de correo para transportar mensajes de un dominio a otro.
- El correo electrónico depende de tres protocolos separados para funcionar: SMTP, POP e IMAP.

■ Funcionamiento de SMTP

- Los formatos de mensajes SMTP necesitan un encabezado y un cuerpo del mensaje.
- El encabezado debe tener una dirección de correo electrónico de destinatario y de remitente con el formato correcto.
- Un cliente SMTP envía un correo electrónico al conectarse a un servidor SMTP en el puerto 25.
- El servidor recibe el mensaje y lo almacena en un buzón local o lo transmite a otro servidor de correo.
- Los usuarios utilizan clientes de correo electrónico para recuperar mensajes almacenados en el servidor.



Protocolos y servicios de capa de aplicación reconocidos

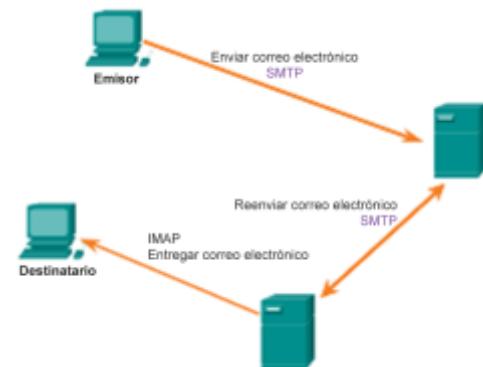
Protocolos web y de correo electrónico (continuación)

■ Funcionamiento de POP

- Los mensajes se descargan del servidor al cliente.
- Los clientes de correo electrónico dirigen las solicitudes POP a servidores de correo en el puerto TCP 110.
- POP permite que los mensajes de correo electrónico se descarguen en el dispositivo del cliente (computadora o teléfono) y se eliminen del servidor.
- Un mensaje descargado reside en el dispositivo que activó la descarga.

■ Protocolos IMAP

- IMAP es otro protocolo para recuperar mensajes de correo electrónico.
- Permite que los mensajes se muestren al usuario, en lugar de descargarlos.
- Los mensajes originales residen en el servidor hasta que el usuario los elimine manualmente.
- Los usuarios ven copias de los mensajes en su software de cliente de correo electrónico.
- Admiten jerarquía de carpetas para organizar y almacenar el correo.
- Cuando un usuario decide eliminar un mensaje, el servidor sincroniza esa acción y elimina el mensaje del servidor.





Protocolos y servicios de capa de aplicación reconocidos

Servicios de asignación de direcciones IP

■ Servicio de nombres de dominio

- Las direcciones IP no son fáciles de memorizar.
- Los nombres de dominio hacen que las direcciones de los servidores sean más fáciles de usar.
- Las computadoras aún necesitan la dirección numérica real para poder comunicarse.
- El protocolo DNS permite la traducción dinámica de un nombre de dominio a la dirección IP asociada.

■ Formato de mensaje DNS

- Los registros comunes de DNS son A, NS, AAAA y MX.
- Los servidores DNS buscan sus propios registros primero, y retransmiten la solicitud del cliente a otros servidores si no pueden resolverla.
- A continuación, la respuesta se reenvía al cliente.
- A menudo, el cliente almacena resoluciones de nombres anteriores. Utilice **ipconfig /displaydns** para enumerar entradas DNS en caché en Windows.

DNS utiliza el mismo formato de mensaje para:

- Todo tipo de consultas de clientes y respuestas del servidor
- Mensaje de error
- La transferencia de información sobre el registro de recursos de un servidor a otro

Encabezado	
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



Protocolos y servicios de capa de aplicación reconocidos

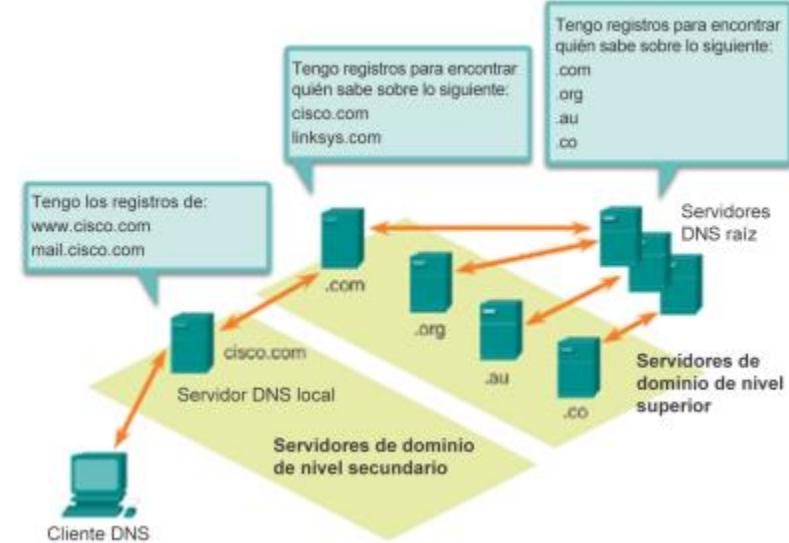
Servicios de asignación de direcciones IP (continuación)

■ Jerarquía DNS

- El protocolo DNS utiliza un sistema jerárquico.
- La estructura de denominación se divide en zonas pequeñas y manejables.
- Cada servidor DNS solo es responsable de administrar las asignaciones de nombre a IP correspondientes a una pequeña porción de toda la estructura DNS.
- Las solicitudes para zonas no almacenadas en un servidor DNS específico se reenvían a otros servidores para la traducción.
- Los dominios de nivel superior representan el tipo de dominio o el país de origen.
Algunos ejemplos de dominios de nivel superior son **.com**, **.org**, **.au** y **.co**.

■ El comando nslookup

- Utilice **nslookup** para realizar consultas DNS.
- Es útil para solucionar problemas de DNS.





Protocolos y servicios de capa de aplicación reconocidos

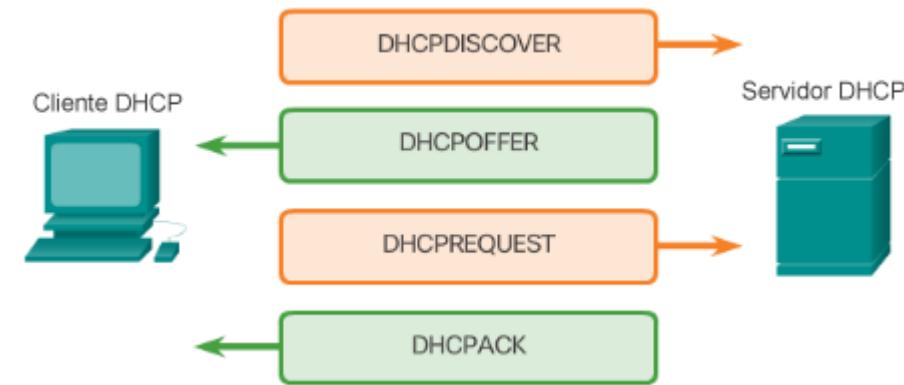
Servicios de asignación de direcciones IP (continuación)

■ Protocolo de configuración dinámica de host

- Las computadoras necesitan información sobre las IP de la red para comunicarse en una red.
- La información IP incluye las direcciones de los hosts y los gateways, la máscara y el servidor DNS.
- DHCP permite la distribución automatizada y escalable de la información de las IP.
- Las direcciones distribuidas mediante DHCP se conceden durante un tiempo establecido.
- Las direcciones se devuelven al pool para su reutilización cuando ya no se encuentran en uso.
- DHCP admite IPv4, y DHCPv6 admite IPv6.

■ Funcionamiento de DHCP

- El cliente transmite un mensaje DHCPDISCOVER.
- Un servidor DHCP responde con un mensaje DHCPOFFER.
- El cliente envía un mensaje DHCPREQUEST al servidor que desea usar (en el caso de haber varias ofertas).
- Un cliente también puede solicitar una dirección previamente asignada por el servidor.
- El servidor devuelve un mensaje DHCPACK para confirmar que ha finalizado la concesión.



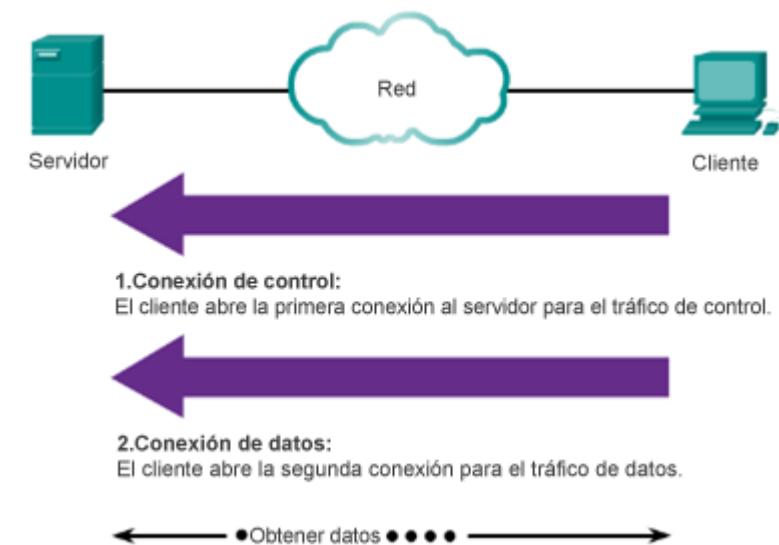


Protocolos y servicios de capa de aplicación reconocidos

Servicios de uso compartido de archivos

■ Protocolo de transferencia de archivos

- FTP se creó para permitir la transferencia de archivos en una red.
- Un cliente FTP es una aplicación que se ejecuta en un equipo cliente y que se utiliza para insertar y extraer datos en un servidor FTP.
- FTP requiere dos conexiones entre el cliente y el servidor: una para los comandos y las respuestas, y otra para la transferencia de archivos propiamente dicha.
- El cliente inicia y establece la primera conexión al servidor para controlar el tráfico en el puerto TCP 21.
- Entonces, el cliente establece la segunda conexión al servidor para la transferencia de datos propiamente dicha en el puerto TCP 20.
- El cliente puede descargar (extraer) datos del servidor o cargar (insertar) datos al servidor.



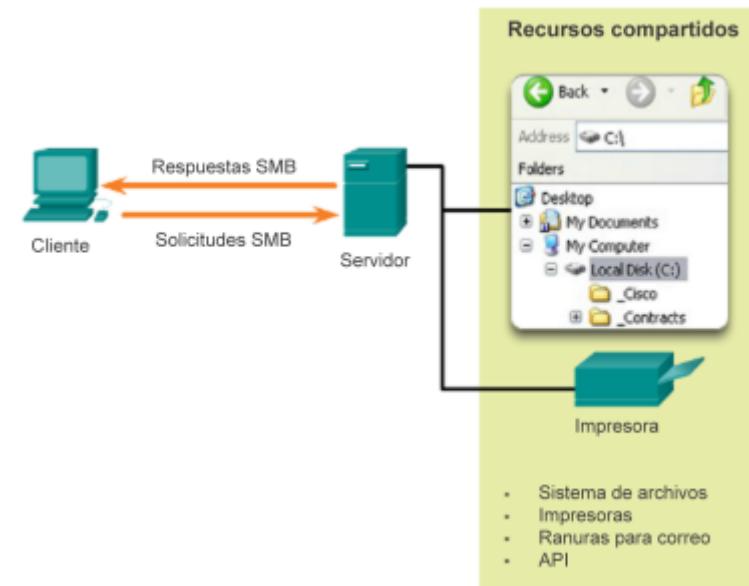


Protocolos y servicios de capa de aplicación reconocidos

Servicios de uso compartido de archivos (continuación)

■ Bloque de mensajes del servidor

- SMB es un protocolo de intercambio de archivos de cliente/servidor.
- Todos los mensajes SMB comparten un mismo formato.
- Los servicios de impresión y de intercambio de archivos de SMB se convirtieron en el pilar de las redes de Windows.
- Los productos de Microsoft ahora admiten protocolos TCP/IP para dar soporte directamente al uso compartido de recursos de SMB.
- 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.
- Los sistemas operativos Mac, LINUX y UNIX tienen su propia implementación de SMB.









8.1 DHCPv4



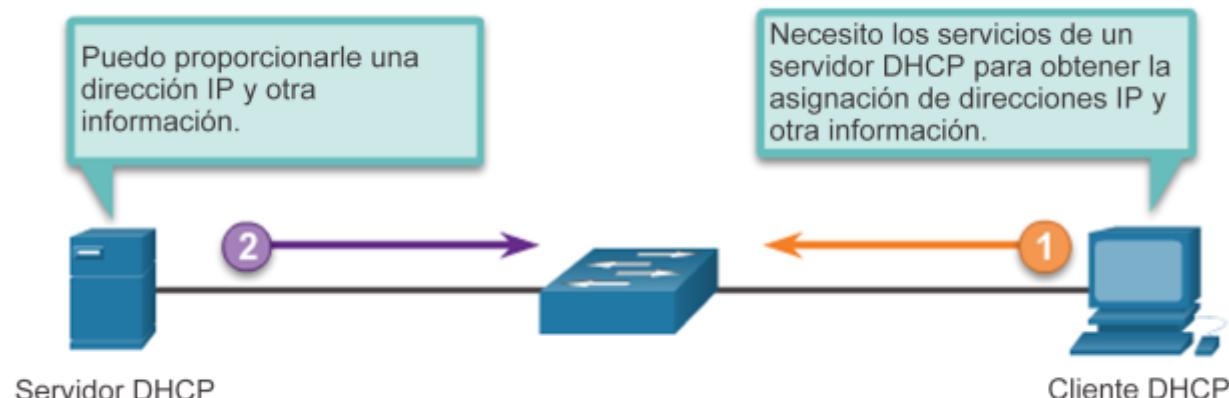
Cisco | Networking Academy®
Mind Wide Open™



Funcionamiento de DHCPv4

Introducción a DHCPv4

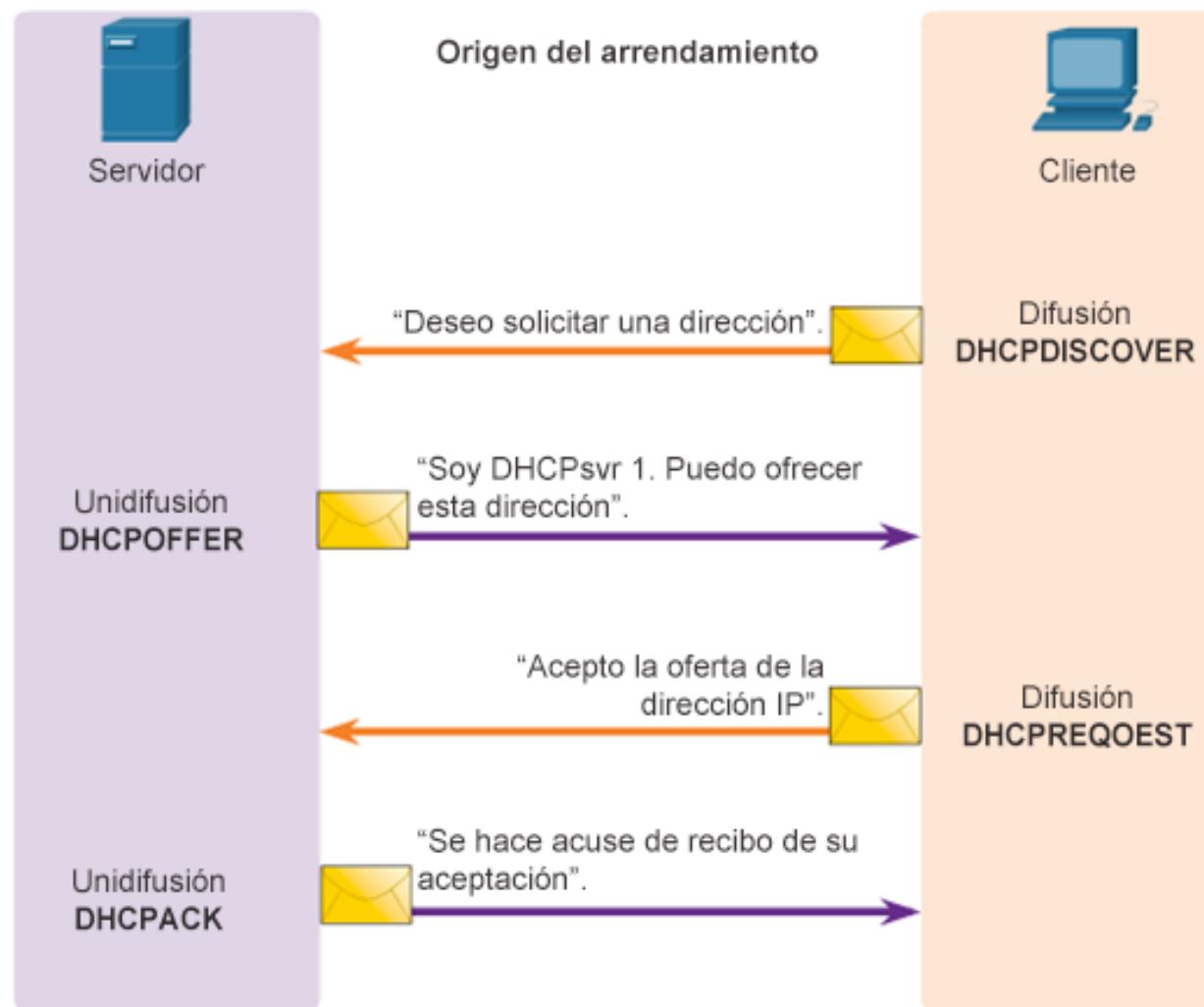
- DHCPv4:
 - Asigna direcciones IPv4 y otra información de configuración de red en forma dinámica.
 - Es una herramienta útil y que ahorra tiempo a los administradores de la red.
 - Asigna de manera dinámica, o arrienda, una dirección IPv4 de un conjunto de direcciones.
- Se puede configurar un router Cisco para proporcionar servicios DHCPv4.
- Los administradores configuran servidores DHCPv4 de modo que caduquen los arrendamientos. Entonces el cliente debe solicitar otra dirección, aunque generalmente se le vuelve a asignar la misma.





Funcionamiento de DHCPv4

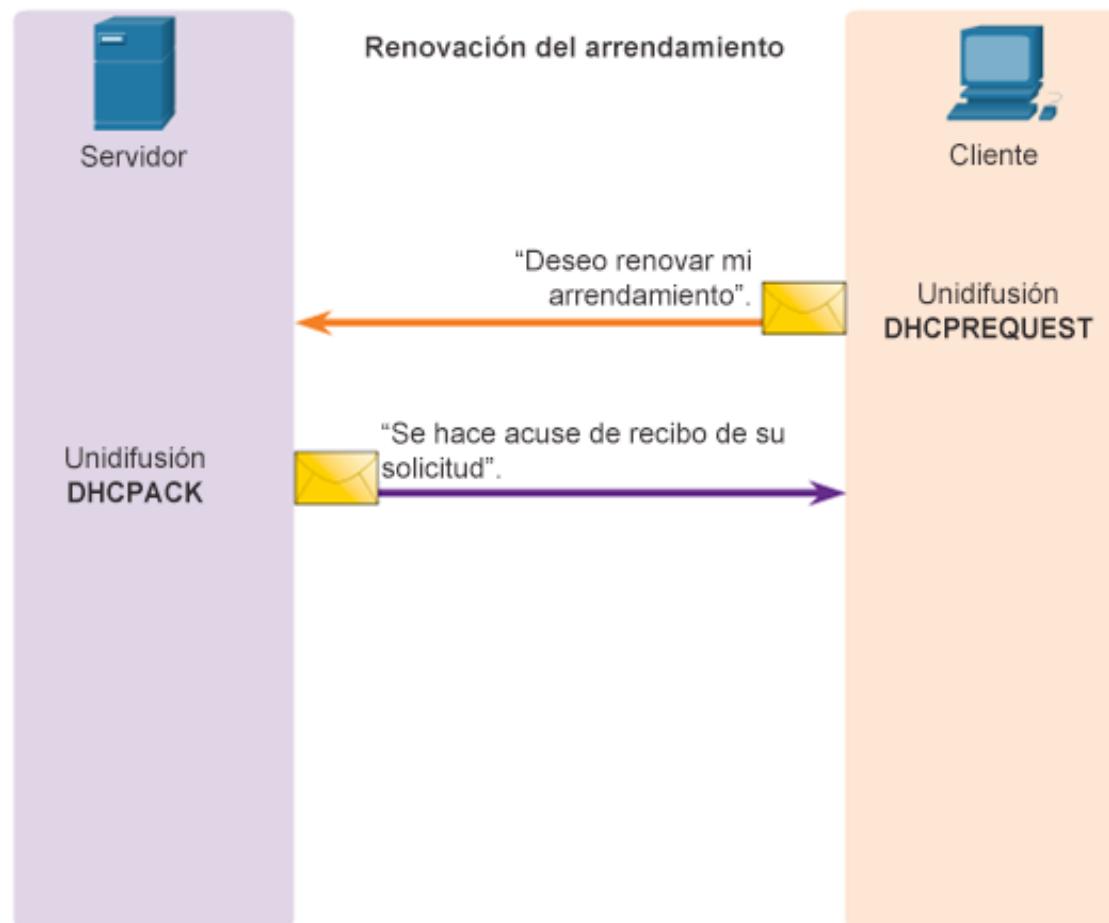
Funcionamiento de DHCPv4





Funcionamiento de DHCPv4

Funcionamiento de DHCPv4 (continuación)





Funcionamiento de DHCPv4

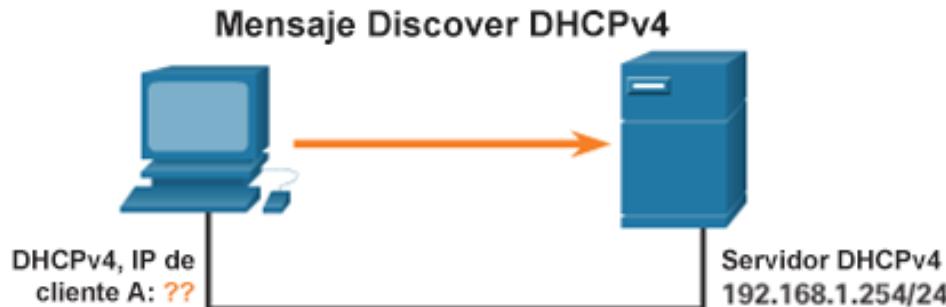
Formato de los mensajes de DHCPv4

8	16	24	32
Código OP (1)	Tipo de hardware (1)	Longitud de dirección de hardware (1)	Saltos (1)
Identificador de transacción			
Segundos: 2 bytes		Indicadores: 2 bytes	
Dirección IP del cliente (CIADDR): 4 bytes		Su dirección IP (YIADDR): 4 bytes	
Dirección IP del servidor (SIADDR): 4 bytes		Dirección IP del gateway (GIADDR): 4 bytes	
Dirección de hardware del cliente (CHADDR): 16 bytes		Nombre del servidor (SNAME): 64 bytes	
Nombre del archivo de arranque: 128 bytes		Opciones de DHCP: variable	



Funcionamiento de DHCPv4

Mensajes Discover y Offer de DHCPv4



Trama de Ethernet	IP	UDP	DHCPDISCOVER
DST MAC: FF:FF:FF:FF:FF:FF SRC MAC: MAC A	IP SRC: 0.0.0.0 IP DST: 255.255.255.255	UDP 67	CIADDR: 0.0.0.0 GIADDR: 0.0.0.0 Máscara: 0.0.0.0 CHADDR: MAC A

MAC: Dirección MAC
CIADDR: Dirección IP del cliente
GIADDR: Dirección IP de Gateway
CHADDR: Dirección de hardware del cliente

El cliente DHCP envía una difusión IP con un paquete DHCPDISCOVER. En este ejemplo, el servidor DHCP se encuentra en el mismo segmento y capta esta solicitud. El servidor advierte que el campo GIADDR está en blanco, de manera que el cliente está en el mismo segmento. El servidor también observa la dirección de hardware del cliente en el paquete de solicitud.



Funcionamiento de DHCPv4

Mensajes Discover y Offer de DHCPv4 (continuación)

Mensaje Offer DHCPv4



Trama de Ethernet	IP	UDP	Respuesta de DHCP
DST MAC: MAC A SRC MAC: MAC Serv	IP SRC: 192.168.1.254 IP DST: 192.168.1.10	UDP 68	CIADDR: 192.168.1.10 GIADDR: 0.0.0.0 Máscara: 255.255.255.0 CHADDR: MAC A

MAC: dirección de control de acceso a medios

CIADDR: Dirección IP del cliente

GIADDR: Dirección IP de Gateway

CHADDR: Dirección de hardware del cliente

El servidor DHCP recoge una dirección IP del grupo disponible para ese segmento, además de otros parámetros globales y de segmentos. El servidor DHCP los coloca en los campos correspondientes del paquete de DHCP. A continuación, el servidor DHCP usa la dirección de hardware de A (en CHADDR) a fin de armar la trama adecuada para devolver al



Configurar un servidor DHCPv4

Configurar un servidor DHCPv4 básico

Un router Cisco que ejecuta el software Cisco IOS puede configurarse para que actúe como servidor DHCPv4. Para configurar DHCP:

1. Excluya direcciones del conjunto.
2. Configure el nombre del conjunto de DHCP.
3. Defina el rango de direcciones y la máscara de subred. Utilice el comando **default-router** para el gateway predeterminado. Parámetros opcionales que pueden incluirse en el *conjunto*: *dns-server*, *domain-name*.

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

Para deshabilitar DHCP utilice el comando **no service dhcp**.



Configurar un servidor DHCPv4

Verificación de DHCPv4

- Comandos para verificar DHCP:

```
show running-config | section dhcp  
show ip dhcp binding  
show ip dhcp server statistics
```

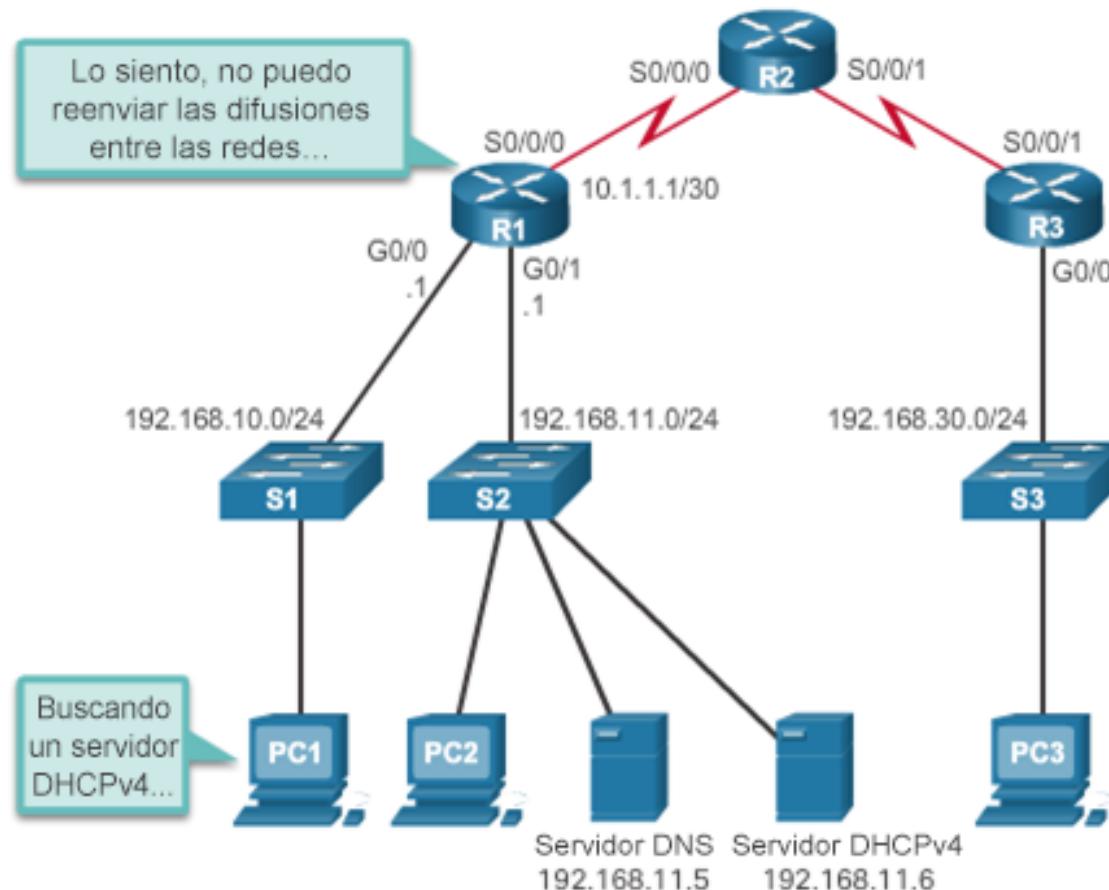
- En la PC, emita el comando **ipconfig /all**.

```
C:\> C:\WINDOWS\system32\cmd.exe  
WINS Proxy Enabled .....: No  
Ethernet Adapter Local Area Connection  
Connection-specific DNS Suffix.: example.com ←  
Description .....: SiS 900 PCI Fast Ethernet Adapter  
Physical Address.....: 00-E0-18-5B-DD-35  
Dhcp Enabled .....: Yes  
Autoconfiguration Enabled....: Yes  
IP Address .....: 192.168.10.10 ←  
Subnet Mask.....: 255.255.255.0 ←  
Default Gateway.....: 192.168.10.1 ←  
DHCP Server .. ....: 192.168.10.1  
Lease Obtained.....: Monday, May 27, 2013 1:06:22PM  
Lease Expires .....: Tuesday, May 28, 2013 1:06:22PM  
DNS Servers .....: 192.168.11.5 ←  
C:\>
```



Configurar un servidor DHCPv4 Retransmisión de DHCPv4

Problemas de DHCPv4





Configurar un servidor DHCPv4

Retransmisión de DHCPv4 (continuación)

- La dirección IP de ayuda permite habilitar un router para que reenvíe difusiones de DHCPv4 al servidor DHCPv4. Funciona como retransmisión.

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
<Output omitted>
```



Configurar un cliente DHCPv4

Configurar un router como cliente DHCP

Configuración de un router como cliente DHCP



```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
<output omitted>
```



Configurar un cliente DHCPv4

Configurar un router inalámbrico como cliente DHCPv4

Configuración del cliente DHCPv4 del router inalámbrico

Wireless-N
Broadband Router

Firmware Version: v0.91.3

Wireless-N Broadband Router WRT300N

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Host Name:

Domain Name:

Optional Settings (required by some internet service providers)

MTU: Size: 1500

Help...





Solucionar problemas en DHCPv4

Tareas para la solución de problemas

Tarea 1 de la resolución de problemas:	Resolver conflictos de dirección.
Tarea 2 de la resolución de problemas:	Verificar la conectividad física.
Tarea 3 de la resolución de problemas:	Probar con una dirección IPv4 estática.
Tarea 4 de la resolución de problemas:	Verificar la configuración de puertos del switch.
Tarea 5 de la resolución de problemas:	Probar desde la misma subred o VLAN.



Solución de problemas en DHCPv4

Verificar la configuración DHCPv4 de un router

Verificación de la retransmisión de DHCPv4 y de los servicios DHCPv4

```
R1# show running-config | section interface GigabitEthernet0/0
interface GigabitEthernet0/0
  ip address 192.168.10.1 255.255.255.0
  ip helper-address 192.168.11.6
  duplex auto
  speed auto
R1#
R1# show running-config | include no service dhcp
R1#
```



Solucionar problemas en DHCPv4

Depuración de DHCPv4

Verificación de DHCPv4 mediante los comandos `debug` del router

```
R1(config)# access-list 100 permit udp any any eq 67
R1(config)# access-list 100 permit udp any any eq 68
R1(config)# end
R1# debug ip packet 100
IP packet debugging is on for access list 100
*IP: s=0.0.0.0 (GigabitEthernet0/1), d=255.255.255.255, len 333,
rcvd 2
*IP: s=0.0.0.0 (GigabitEthernet0/1), d=255.255.255.255, len 333,
stop process pak for forus packet
*IP: s=192.168.11.1 (local), d=255.255.255.255
(GigabitEthernet0/1), len 328, sending broad/multicast

<output omitted>

R1# debug ip dhcp server events
DHCPD: returned 192.168.10.11 to address pool LAN-POOL-1
DHCPD: assigned IP address 192.168.10.12 to client
0100.0103.85e9.87.
DHCPD: checking for expired leases.
DHCPD: the lease for address 192.168.10.10 has expired.
DHCPD: returned 192.168.10.10 to address pool LAN-POOL-1
```

- En la ilustración, se muestra una ACL extendida que permite solamente paquetes con puertos de destino UDP de 67 o 68. Estos son los puertos típicos que utilizan los clientes y los servidores DHCPv4 al enviar mensajes DHCPv4. Se utiliza la ACL extendida con el comando `debug ippacket` para mostrar solo mensajes de DHCPv4.

8.2 DHCPv6

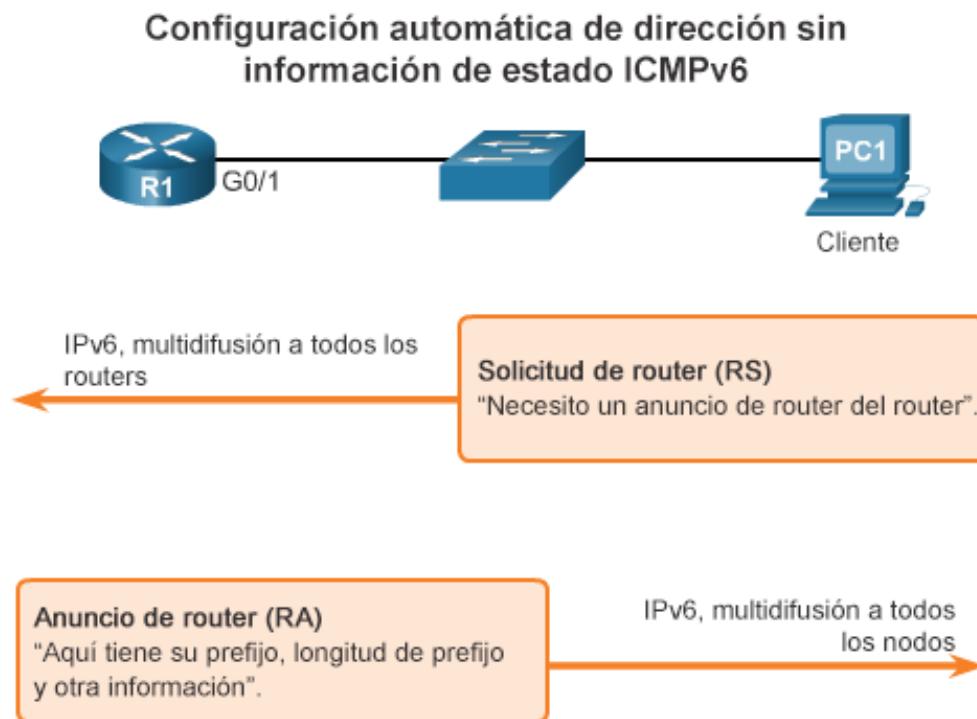




SLAAC y DHCPv6

Configuración automática de direcciones independiente del estado (SLAAC)

- SLAAC utiliza mensajes de solicitud y de anuncio de router ICMPv6 para proporcionar direccionamiento y otra información de configuración que normalmente proporcionaría un servidor DHCP:

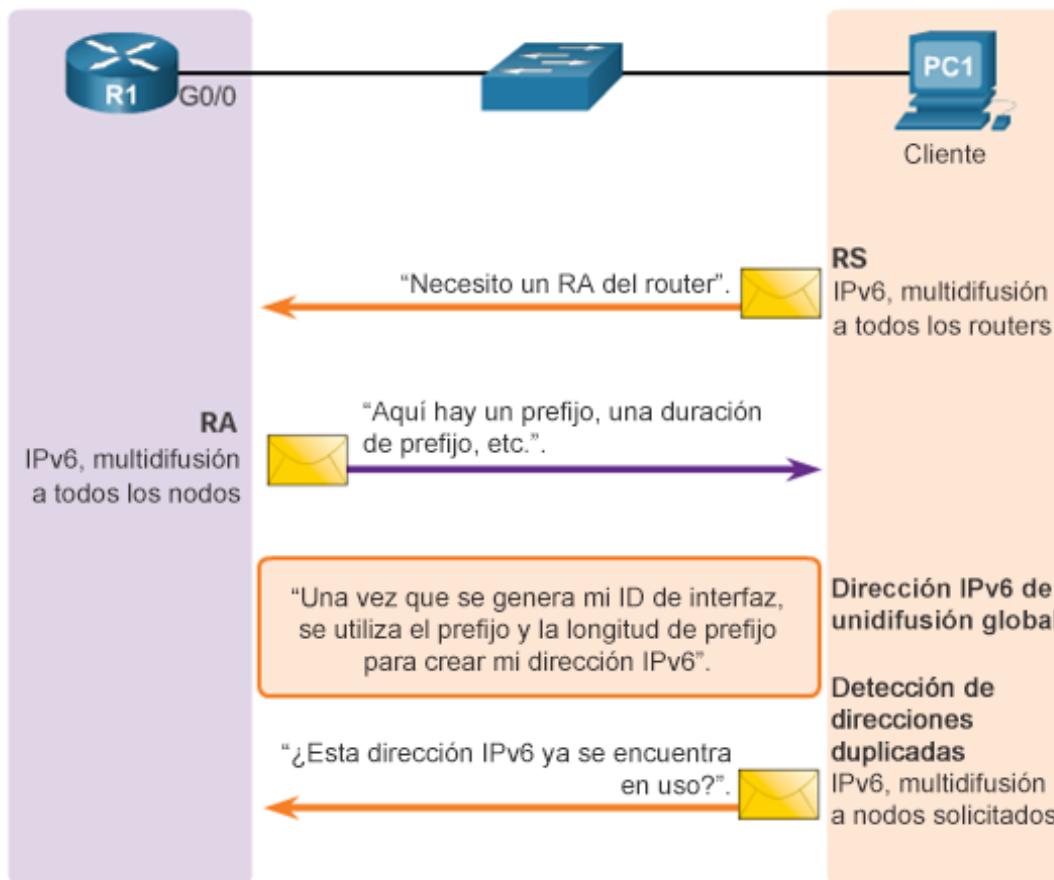




SLAAC y DHCPv6

Funcionamiento de SLAAC

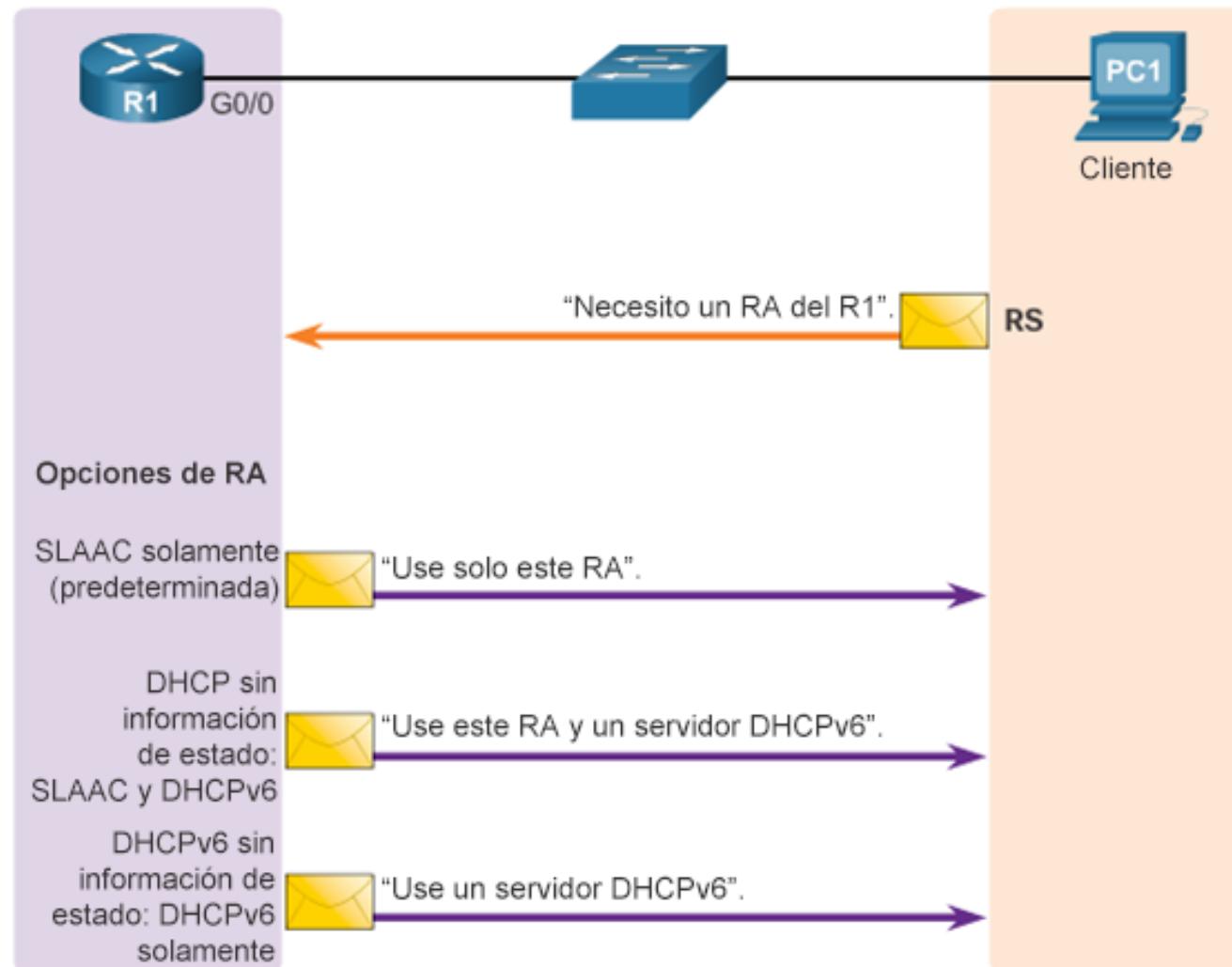
- Un router debe tener el routing IPv6 habilitado antes de poder enviar mensajes RA: Router(config)# **ipv6 unicast-routing**





SLAAC y DHCPv6

SLAAC y DHCPv6

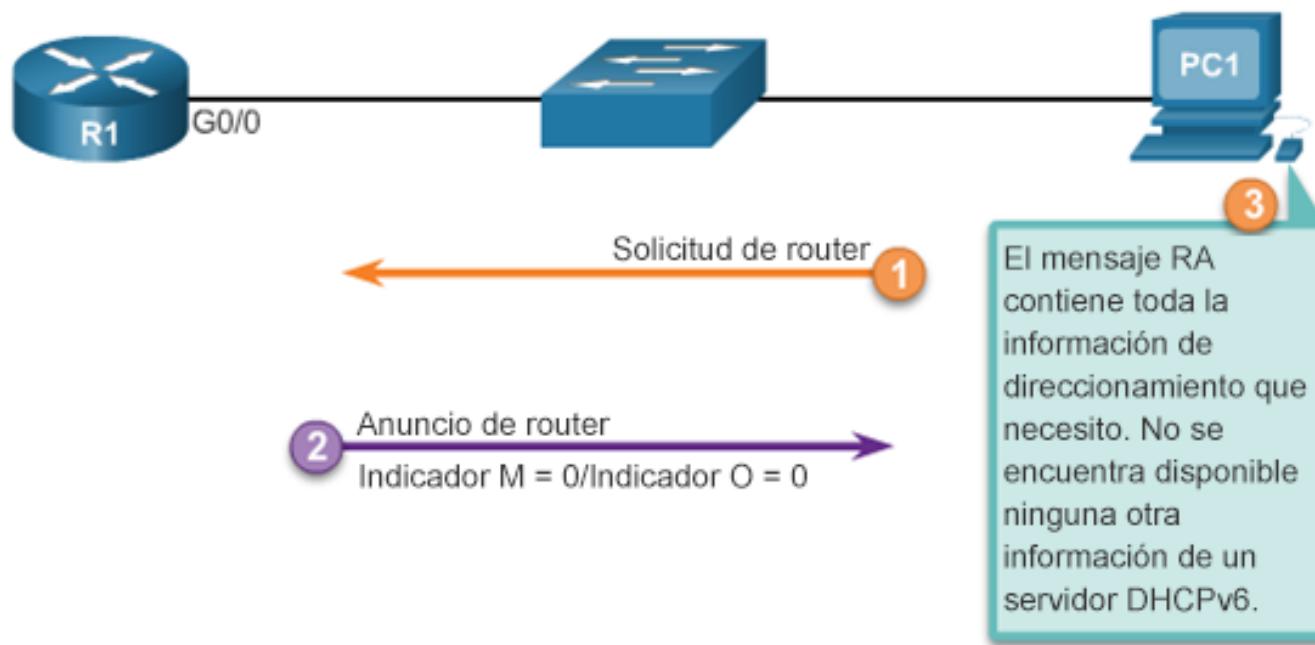




SLAAC y DHCPv6

Opción de SLAAC

- SLAAC es la opción predeterminada en los routers Cisco. Tanto el indicador M como el indicador O están establecidos en 0 en el RA, como se muestra en la ilustración.

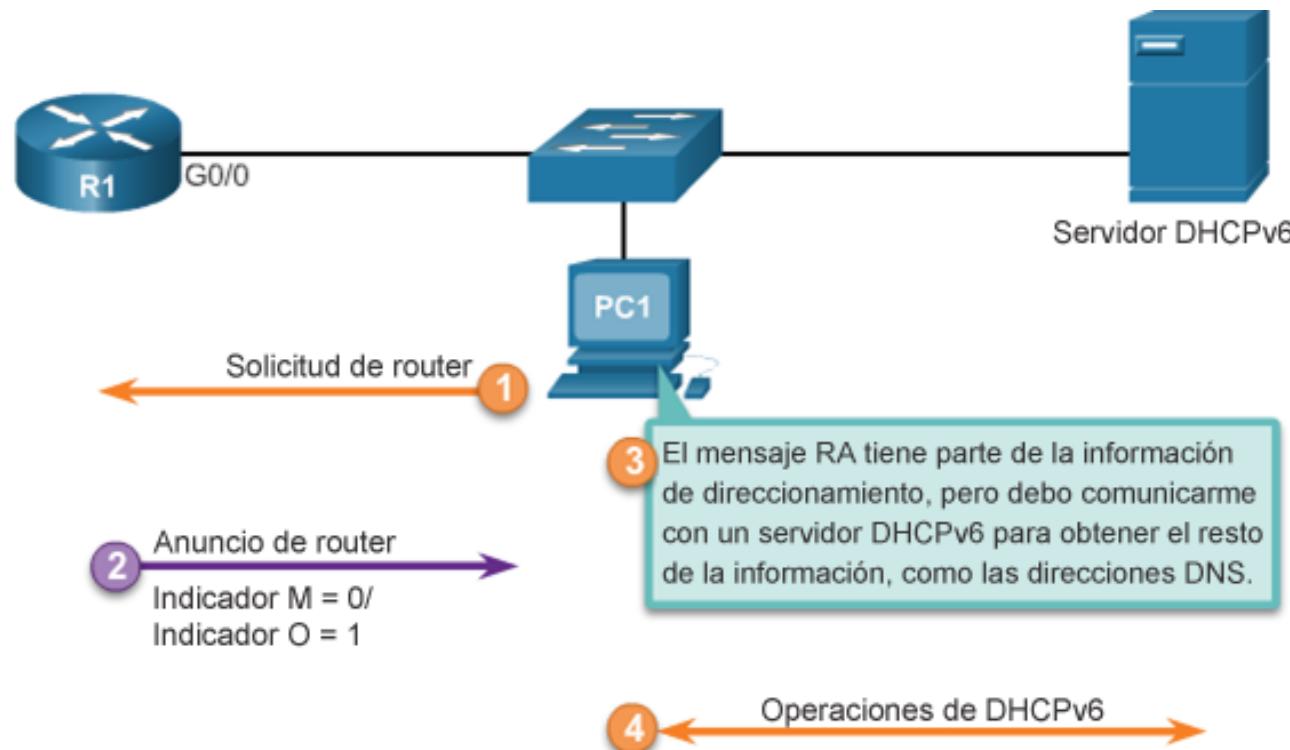




SLAAC y DHCPv6

Opción de DHCPv6 sin estado

- Para modificar el mensaje RA enviado en la interfaz de un router e indicar DHCPv6 sin estado, utilice el siguiente comando:
Router(config-if)# ipv6 nd other-config-flag

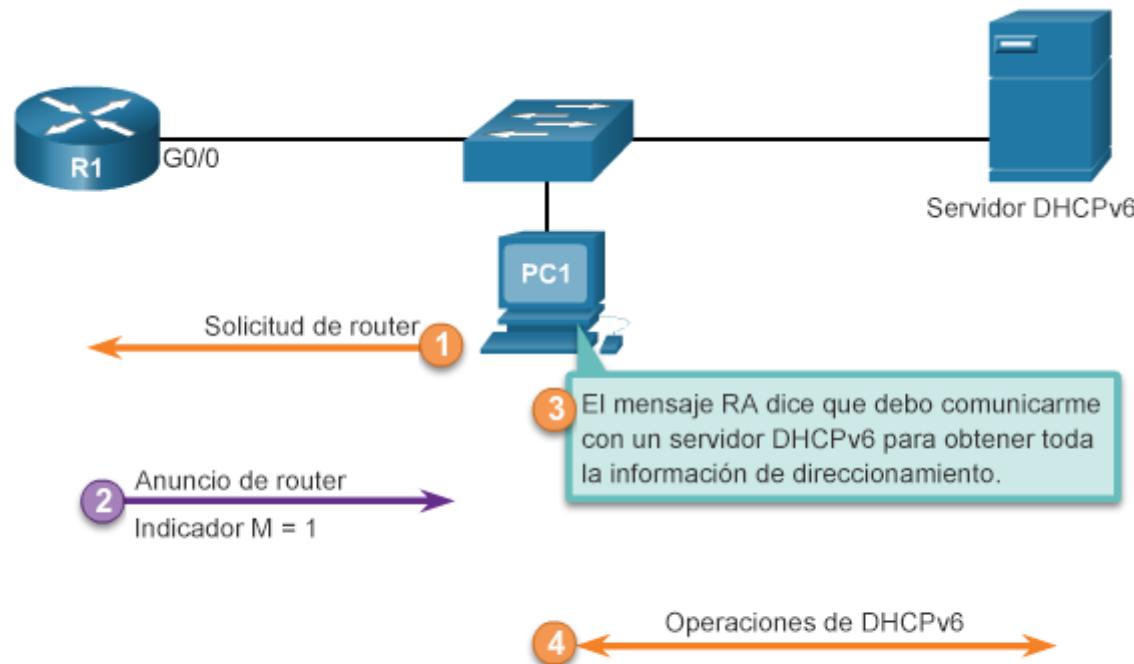




SLAAC y DHCPv6

Opción de DHCPv6 con estado

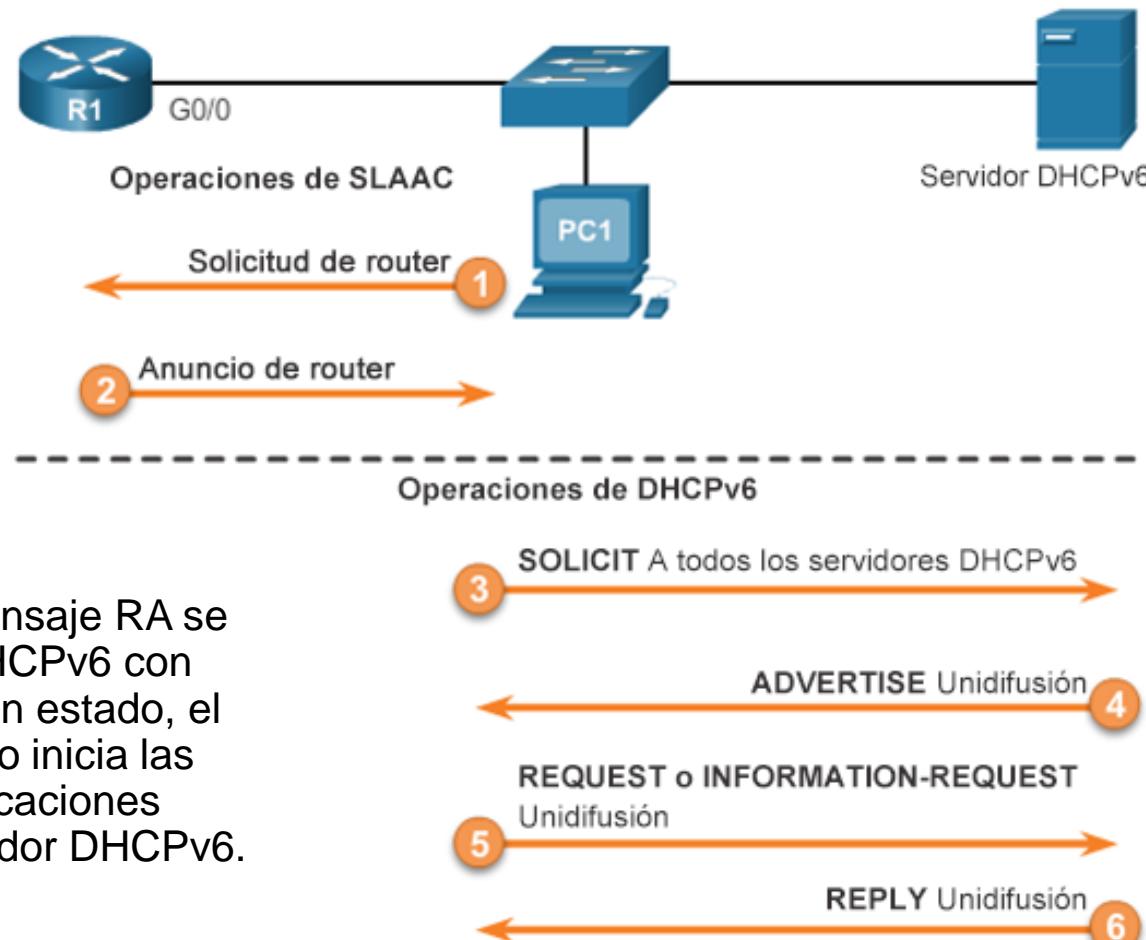
- Esta opción es la más similar a DHCPv4. En este caso, el mensaje RA le informa al cliente que no utilice la información contenida en el mensaje RA. Toda la información de direccionamiento y de configuración debe obtenerse de un servidor DHCPv6 con estado.
Router(config-if)# ipv6 nd managed-config-flag





SLAAC y DHCPv6

Operaciones de DHCPv6

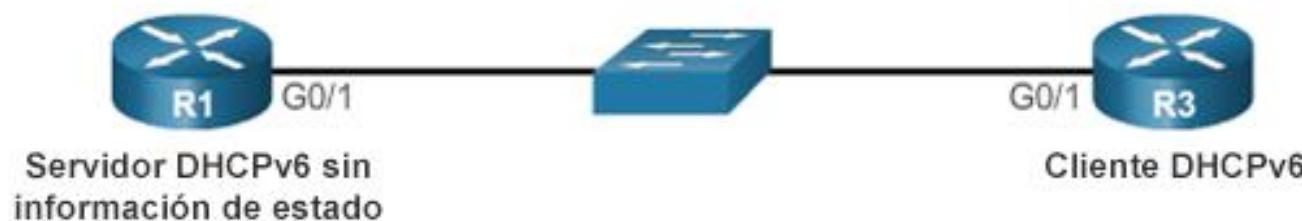


Si en el mensaje RA se indica DHCPv6 con estado o sin estado, el dispositivo inicia las comunicaciones cliente/servidor DHCPv6.



DHCPv6 sin estado

Configurar un router como servidor DHCPv6 sin estado

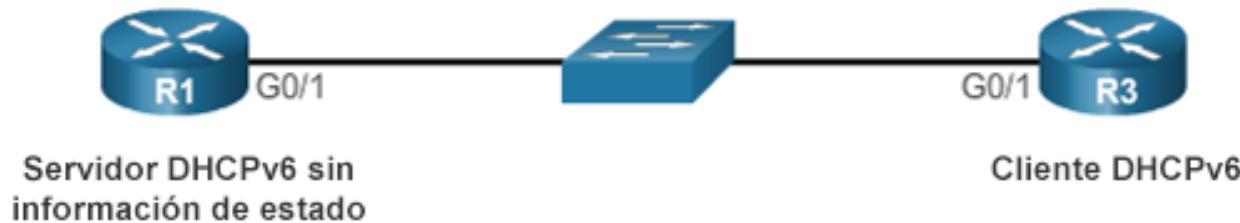


```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```



DHCPv6 sin estado

Configurar un router como cliente DHCPv6 sin estado



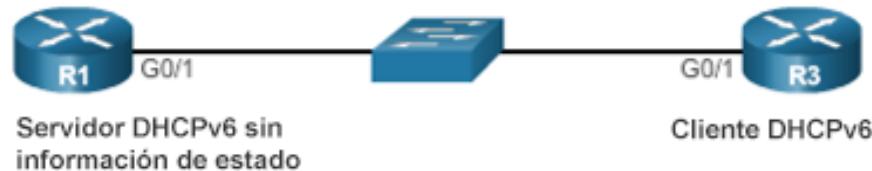
```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address autoconfig
R3(config-if)#

```



DHCPv6 sin estado

Verificación de DHCPv6 sin estado



```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATELESS
  DNS server: 2001:DB8:CAFE:AAAA::5
  Domain name: example.com
  Active clients: 0
R1#
```

Verifique el cliente DHCP sin estado usando los siguientes comandos:

- **show ipv6 interface**
- **debug ipv6 dhcp detail**



DHCPv6 con estado

Configurar un router como servidor DHCPv6 con estado

Paso 1. Habilitar el routing IPv6

```
Router(config)# ipv6 unicast-routing
```

Paso 2. Configurar un pool de DHCPv6

```
Router(config)# ipv6 dhcp pool pool-name
Router(config-dhcpv6) #
```

Paso 3. Configurar los parámetros del pool

```
Router(config-dhcpv6) # address prefix/length [lifetime
                      {valid-lifetime preferred-lifetime
                      | infinite}]
Router(config-dhcpv6) # dns-server dns-server-address
Router(config-dhcpv6) # domain-name domain-name
```

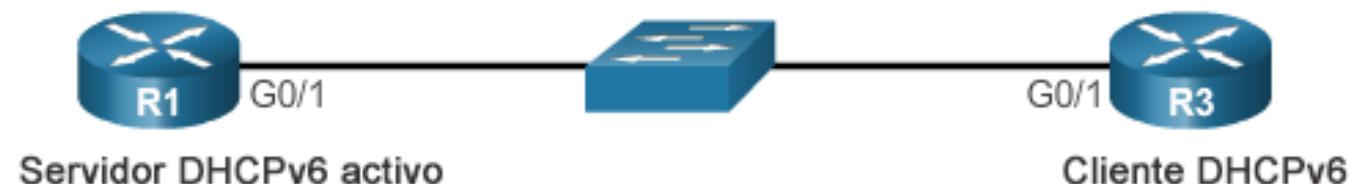
Paso 4. Configurar la interfaz DHCPv6

```
Router(config)# interface type number
Router(config-if)# ipv6 dhcp server pool-name
Router(config-if)# ipv6 nd managed-config-flag
```



DHCPv6 con estado

Configurar un router como servidor DHCPv6 con estado (continuación)

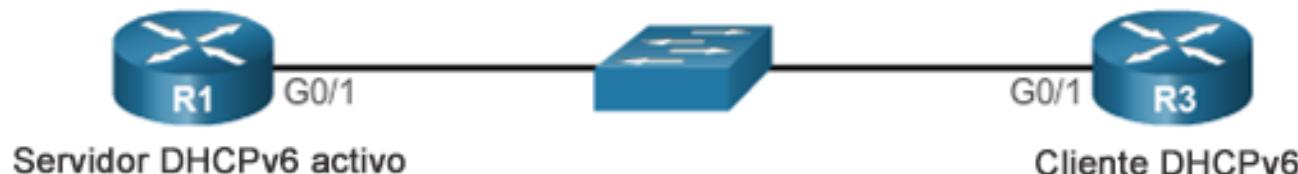


```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64
                  lifetime infinite
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
```



DHCPv6 con estado

Configurar un router como cliente DHCPv6 con estado

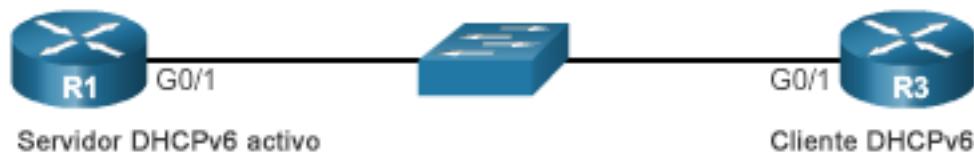


```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address dhcp
R3(config-if)#
```



Servidor DHCPv6 con estado

Verificación de DHCPv6 con estado



```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATEFUL
  Address allocation prefix: 2001:DB8:CAFE:1::/64 valid
  4294967295 preferred 4294967295 (1 in use, 0 conflicts)
  DNS server: 2001:DB8:CAFE:AAAA::5
  Domain name: example.com
  Active clients: 1
R1#
```

```
R1# show ipv6 dhcp binding
Client: FE80::32F7:DFF:FE25:2DE1
  DUID: 0003000130F70D252DE0
  Username : unassigned
  IA NA: IA ID 0x00040001, T1 43200, T2 69120
  Address: 2001:DB8:CAFE:1:5844:47B2:2603:C171
    preferred lifetime INFINITY, , valid lifetime
    INFINITY,
R1#
```



Servidor DHCPv6 con estado

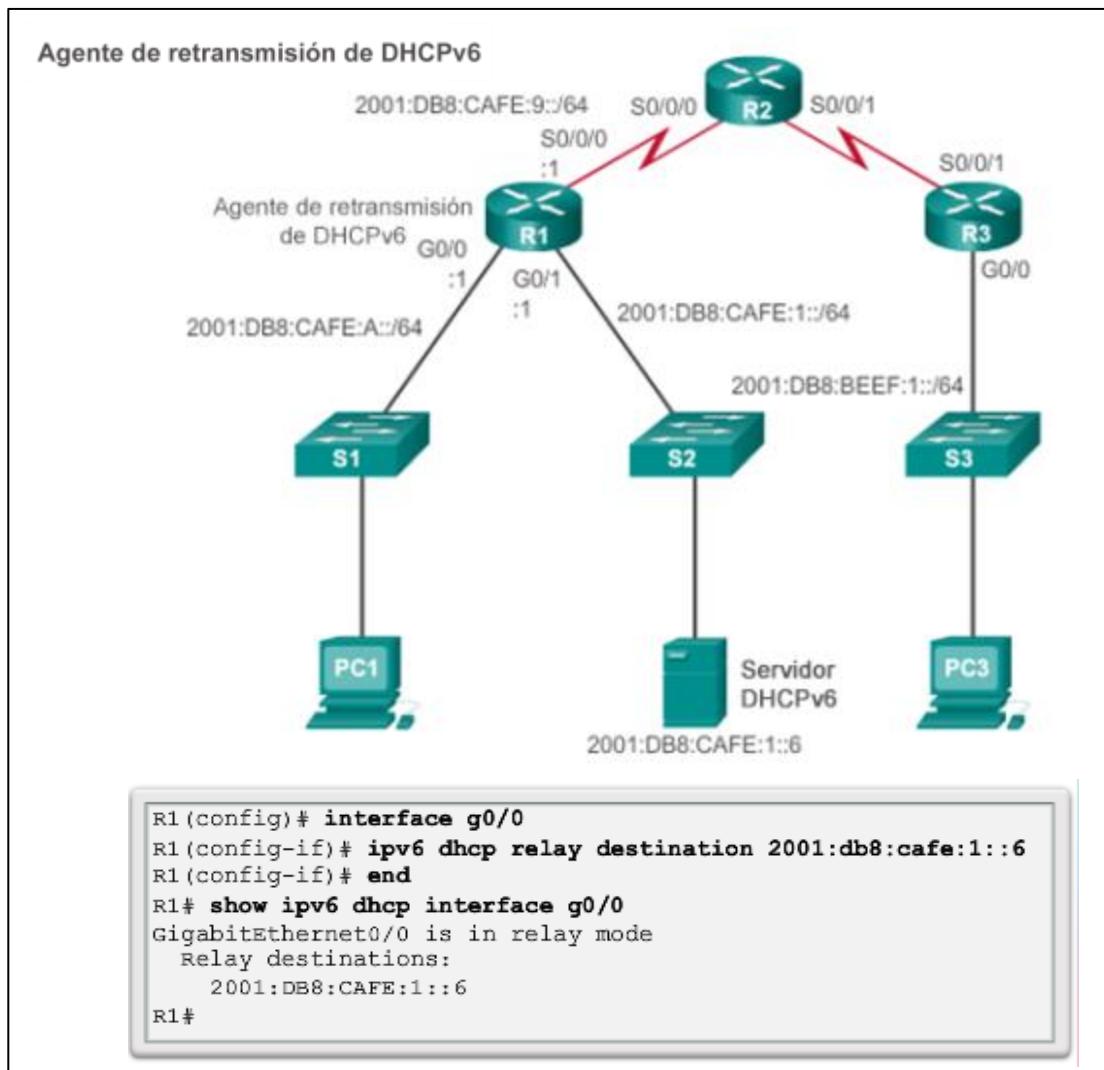
Verificación de DHCPv6 con estado (continuación)

```
R3# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
    FE80::32F7:DFF:FE25:2DE1
      No virtual link-local address(es):
      Global unicast address(es):
        2001:DB8:CAFE:1:5844:47B2:2603:C171, subnet is
        2001:DB8:CAFE:1:5844:47B2:2603:C171/128
        Joined group address(es):
          FF02::1
          FF02::1:FF03:C171
          FF02::1:FF25:2DE1
        MTU is 1500 bytes
        ICMP error messages limited to one every 100 milliseconds
        ICMP redirects are enabled
        ICMP unreachable are sent
        ND DAD is enabled, number of DAD attempts: 1
        ND reachable time is 30000 milliseconds (using 30000)
        ND NS retransmit interval is 1000 milliseconds
        Default router is FE80::D68C:B5FF:FECE:A0C1 on
          GigabitEthernet0/1
R3#
```



DHCPv6 con estado

Configurar un router como agente de retransmisión DHCPv6





Solucionar problemas en DHCPv6

Tareas para la solución de problemas

Tarea 1 de la resolución de problemas:	Resolver conflictos de dirección.
Tarea 2 de la resolución de problemas:	Verificar el método de asignación.
Tarea 3 de la resolución de problemas:	Probar con una dirección IPv6 estática.
Tarea 4 de la resolución de problemas:	Verificar la configuración de puertos del switch.
Tarea 5 de la resolución de problemas:	Probar desde la misma subred o VLAN.



Solución de problemas en DHCPv6

Verificar la configuración DHCPv6 de un router

Servicios DHCPv6 activos

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64 lifetime
infinite
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
```

Servicios DHCPv6 sin información de estado

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```



Solucionar problemas en DHCPv6

Depuración de DHCPv6

```
R1# debug ipv6 dhcp detail
    IPv6 DHCP debugging is on (detailed)
R1#
*Feb  3 21:27:41.123: IPv6 DHCP: Received SOLICIT from
FE80::32F7:DFF:FE25:2DE1 on GigabitEthernet0/1
*Feb  3 21:27:41.123: IPv6 DHCP: detailed packet contents
*Feb  3 21:27:41.123:     src FE80::32F7:DFF:FE25:2DE1
(GigabitEthernet0/1)
*Feb  3 21:27:41.127:     dst FF02::1:2
*Feb  3 21:27:41.127:     type SOLICIT(1), xid 13190645
*Feb  3 21:27:41.127:     option ELAPSED-TIME(8), len 2
*Feb  3 21:27:41.127:         elapsed-time 0
*Feb  3 21:27:41.127:     option CLIENTID(1), len 10
*Feb  3 21:27:41.127:         000
*Feb  3 21:27:41.127: IPv6 DHCP: Using interface pool IPV6-
STATEFUL
*Feb  3 21:27:41.127: IPv6 DHCP: Creating binding for
FE80::32F7:DFF:FE25:2DE1 in pool IPV6-STATEFUL
<output omitted>
```

8.3 Resumen





Resumen del capítulo

Resumen

- Explicar la forma en la que funciona DHCPv4 en la red de una pequeña o mediana empresa.
- Configurar un router como servidor DHCPv4.
- Configurar un router como cliente DHCPv4.
- Realizar la resolución de problemas de una configuración DHCP para IPv4 en una red conmutada.
- Explicar el funcionamiento de DHCPv6.
- Configurar DHCPv6 sin estado para una pequeña o mediana empresa.
- Configurar DHCPv6 con estado para una pequeña o mediana empresa.
- Realizar la resolución de problemas de una configuración DHCP para IPv6 en una red conmutada.

Cisco | Networking Academy®

Mind Wide Open™

