Planificación y Administración de Redes

T.7 La capa de aplicación

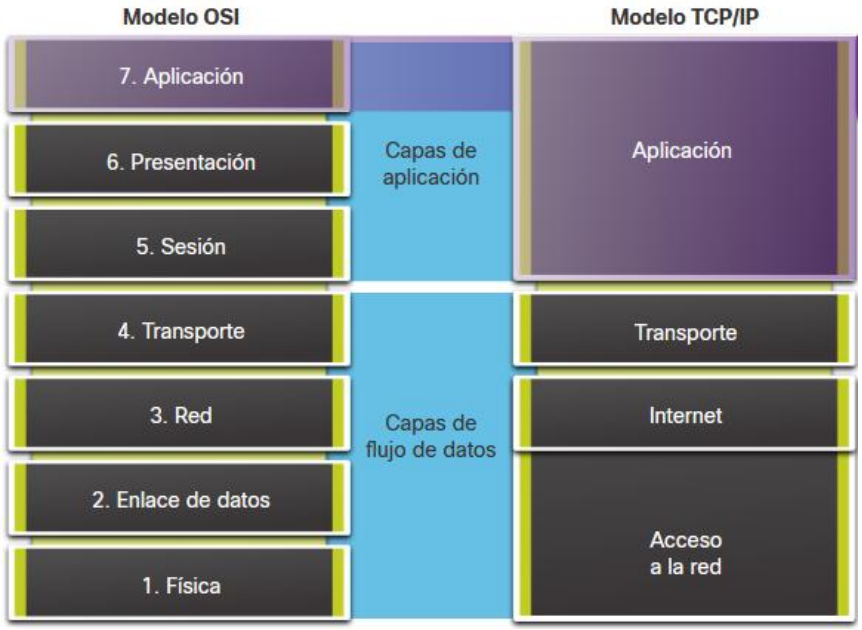
Índice

1. Capa de aplicación (15.1)
2. Protocolos Web (15.3.1 y 15.3.2)
3. Protocolos de email (15.3.3 y 15.3.4)
4. Servicios de direccionamiento IP (15.4)
5. Servicios de intercambio de archivos (15.5)

1 Capa de aplicación

Capa de aplicación

En los modelo OSI y TCP/IP, la **capa de aplicación es la más cercana al usuario final**. Es la capa que proporciona la interfaz entre las aplicaciones utilizadas para la comunicación y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino.



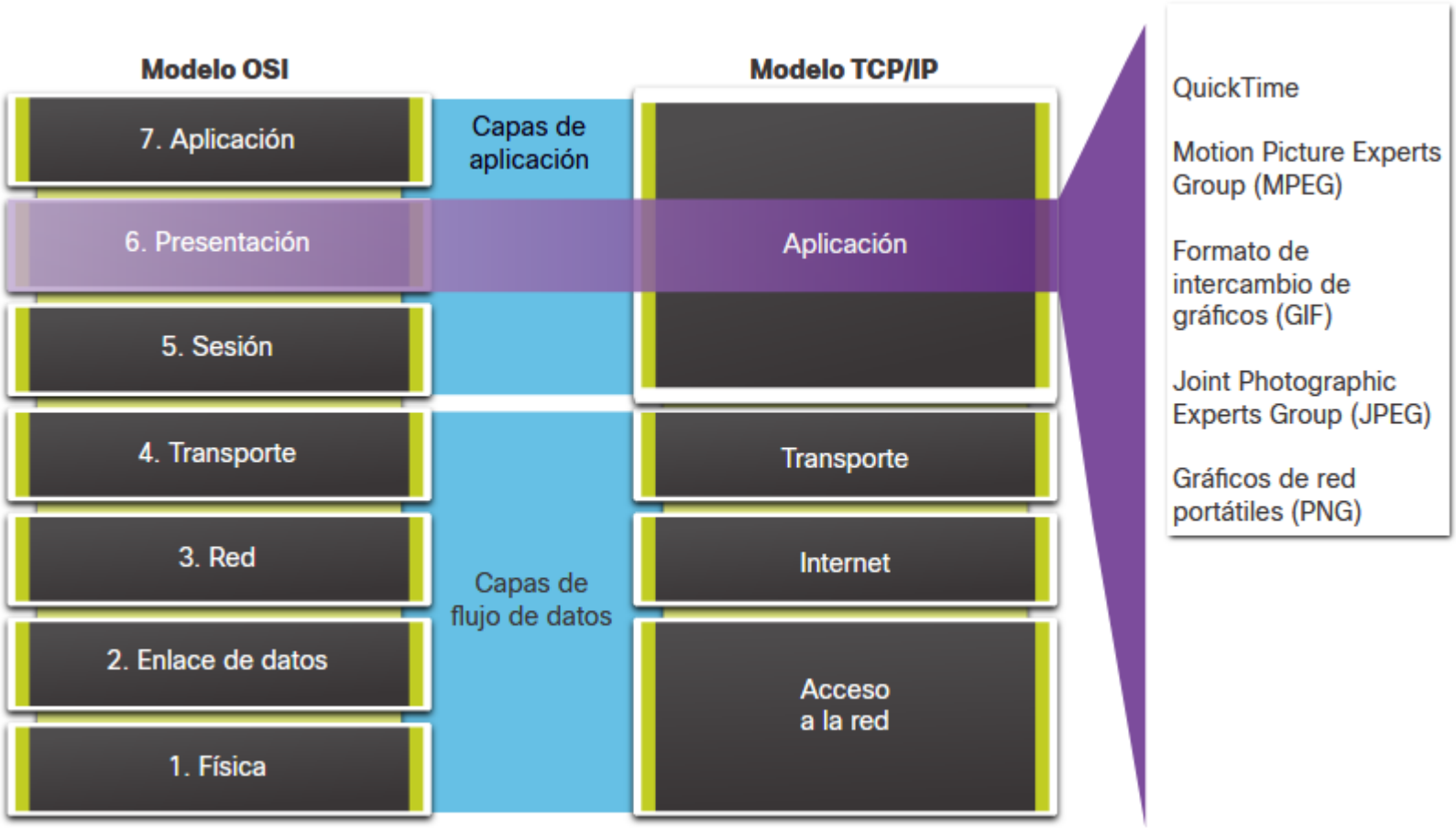
Capa de aplicación

La **capa de presentación** tiene tres funciones principales:

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

Las funciones de la **capa de sesión** crean y mantienen diálogos entre las aplicaciones de origen y destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o que estuvieron inactivas durante un período prolongado.

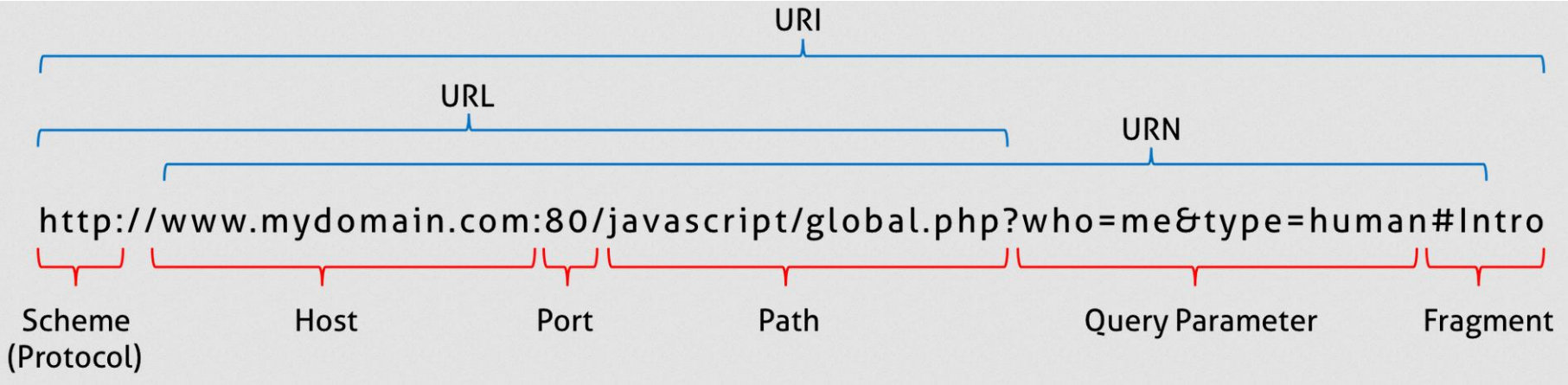
Capa de aplicación



2 Protocolos Web

HTTP y HTTPS

Cuando se escribe una dirección web o un localizador uniforme de recursos (URL) **en un navegador web, el navegador establece una conexión con el servicio web. El servicio web que se está ejecutando en el servidor está utilizando el protocolo HTTP.** Los nombres que la mayoría de las personas asocia con las direcciones web son URL e identificador uniforme de recursos (URI).



HTTP y HTTPS

Paso 1

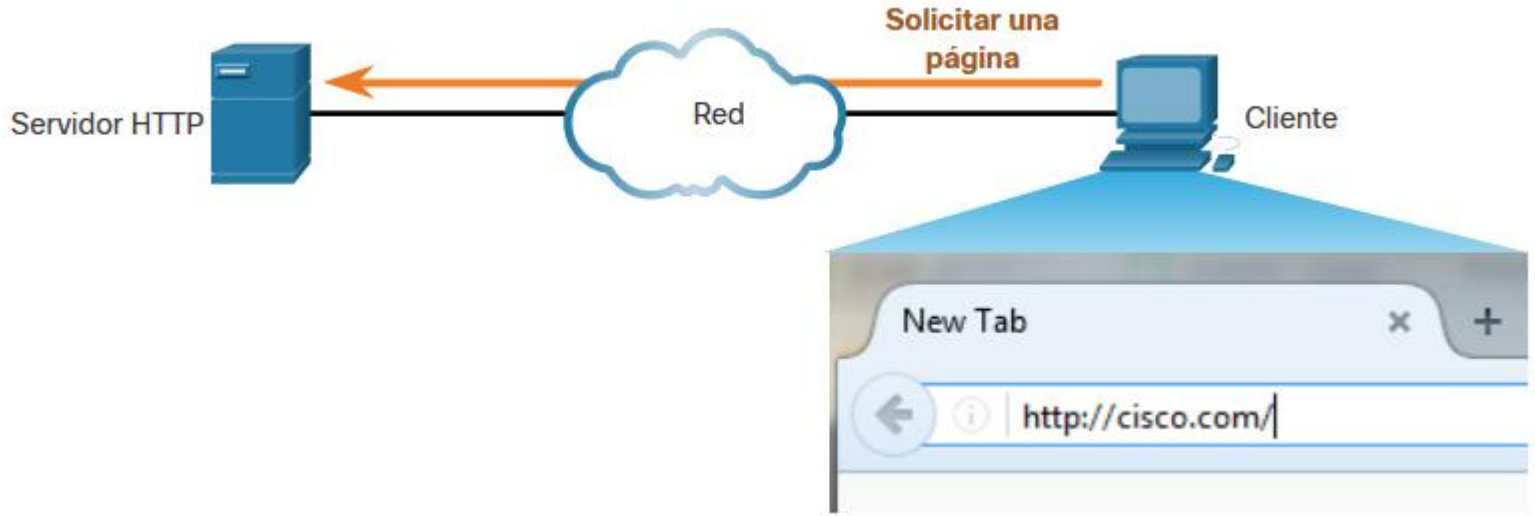
El navegador interpreta las tres partes de la URL:

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

HTTP y HTTPS

Paso 2

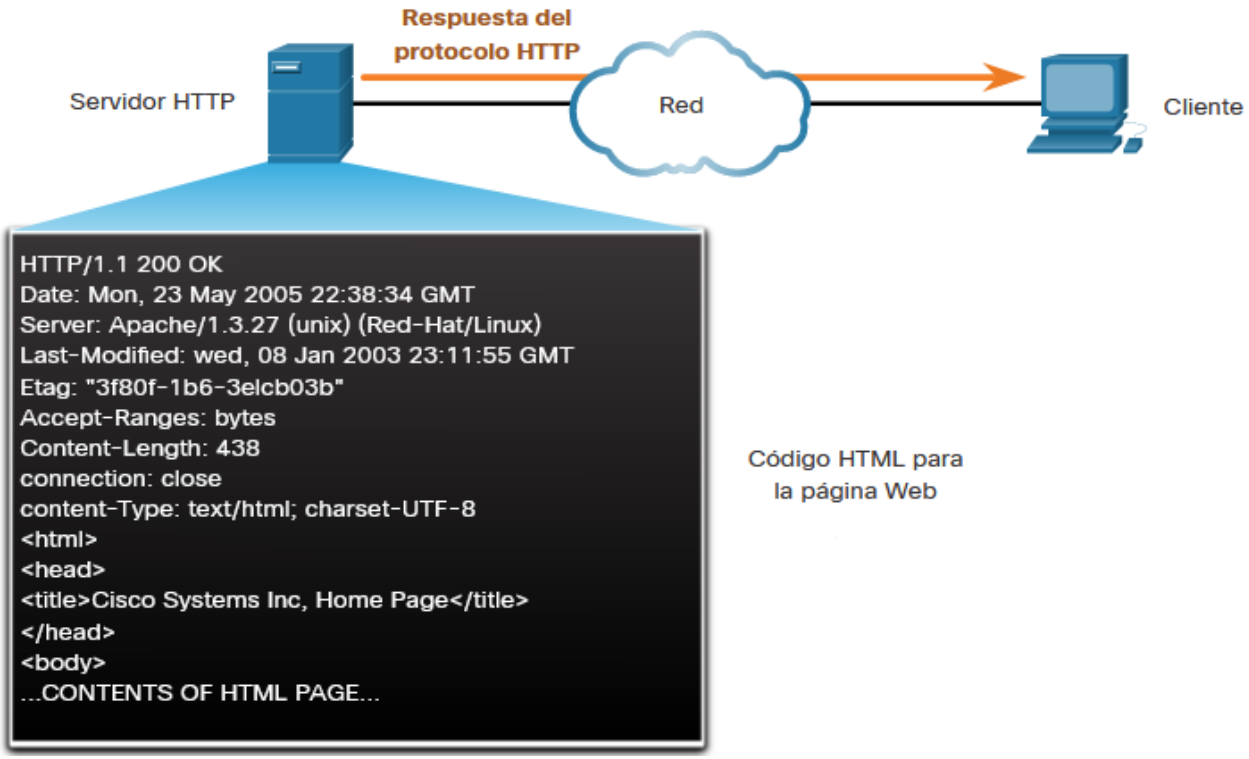
El navegador luego verifica con un Servidor de nombres de dominio (DNS) para convertir a www.cisco.com en una dirección numérica que utiliza para conectarse con el servidor. **El cliente inicia una solicitud HTTP a un servidor enviando una solicitud GET al servidor y solicita el archivo index.html.**



HTTP y HTTPS

Paso 3

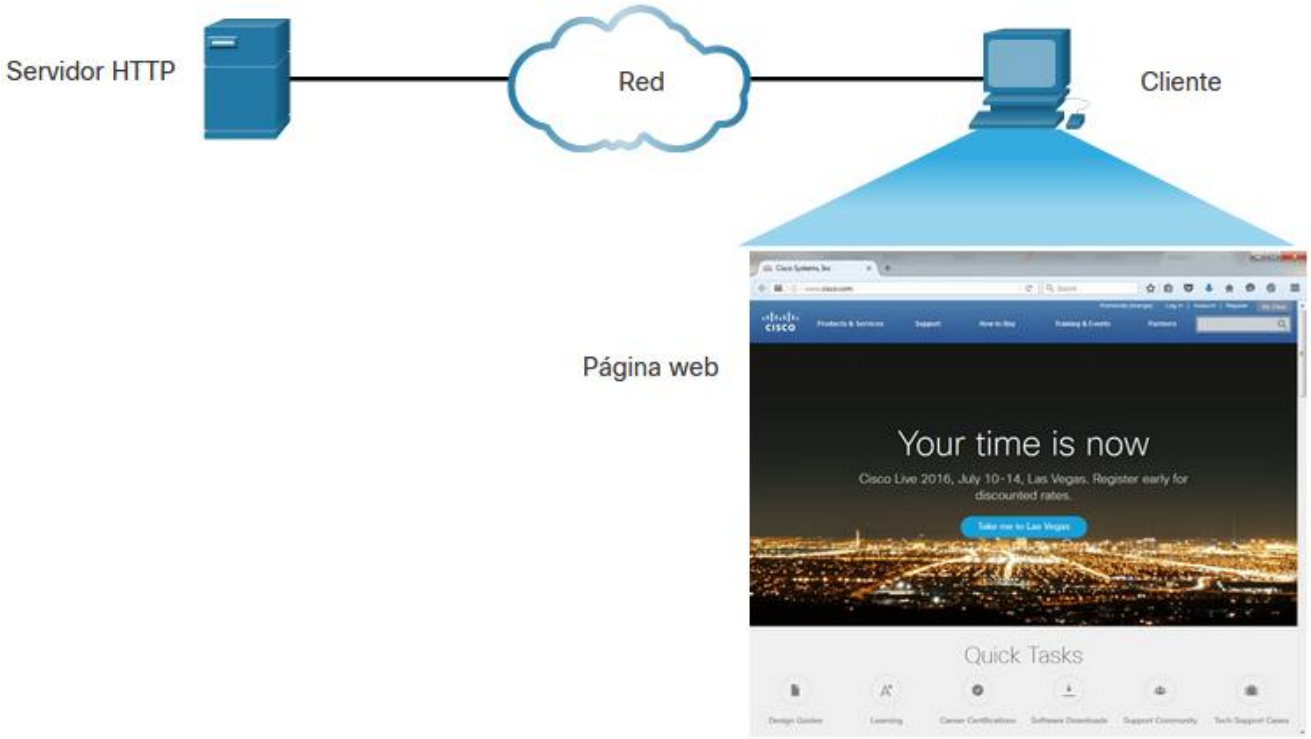
En respuesta a la solicitud, **el servidor envía el código HTML de esta página web al navegador.**



HTTP y HTTPS

Paso 4

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

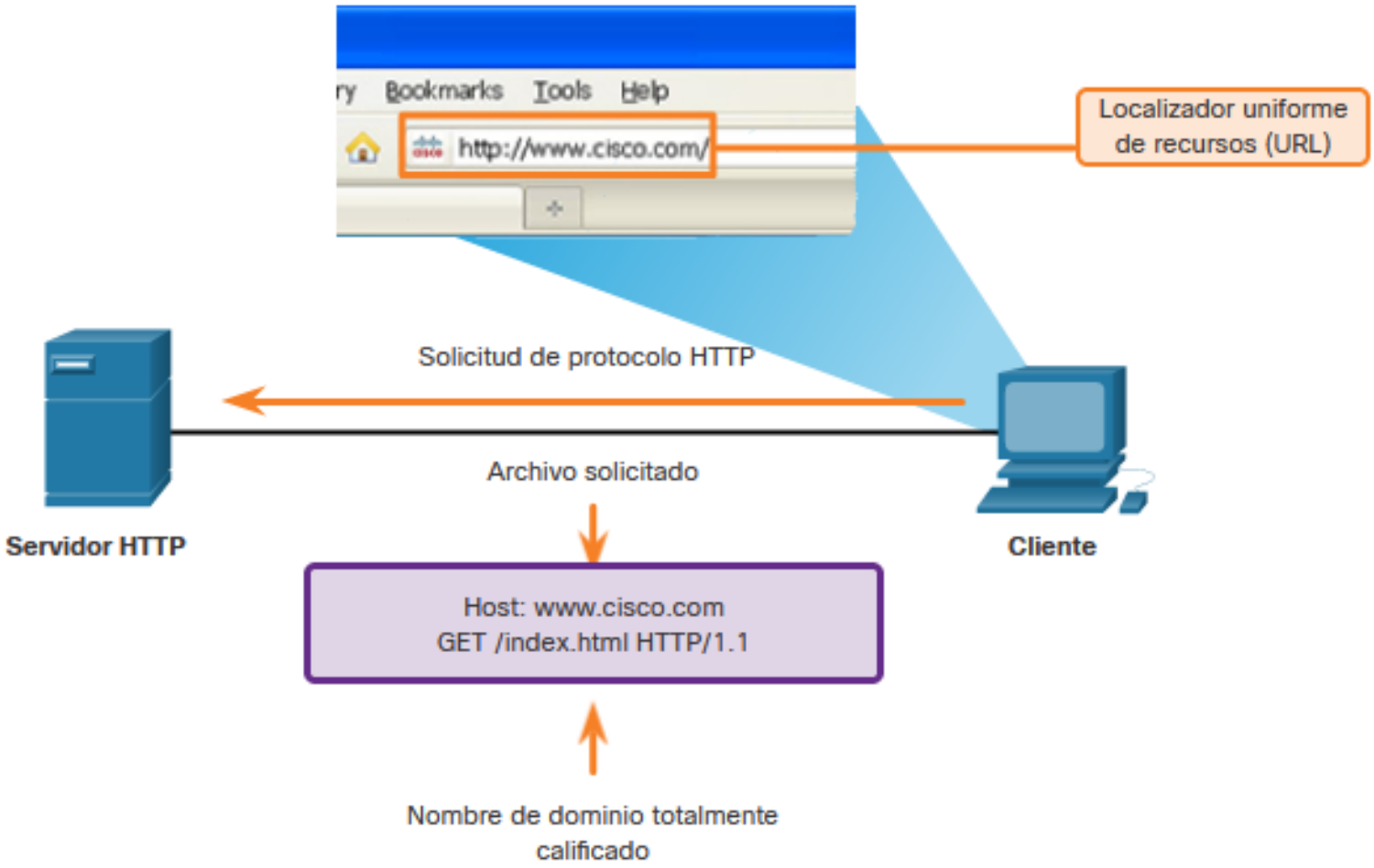


HTTP y HTTPS

HTTP es un protocolo de solicitud/respuesta. Cuando un cliente, por lo general un navegador web, envía una solicitud a un servidor web, HTTP especifica los tipos de mensaje que se utilizan para esa comunicación. Los tres tipos de mensajes comunes son GET, POST y PUT:

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

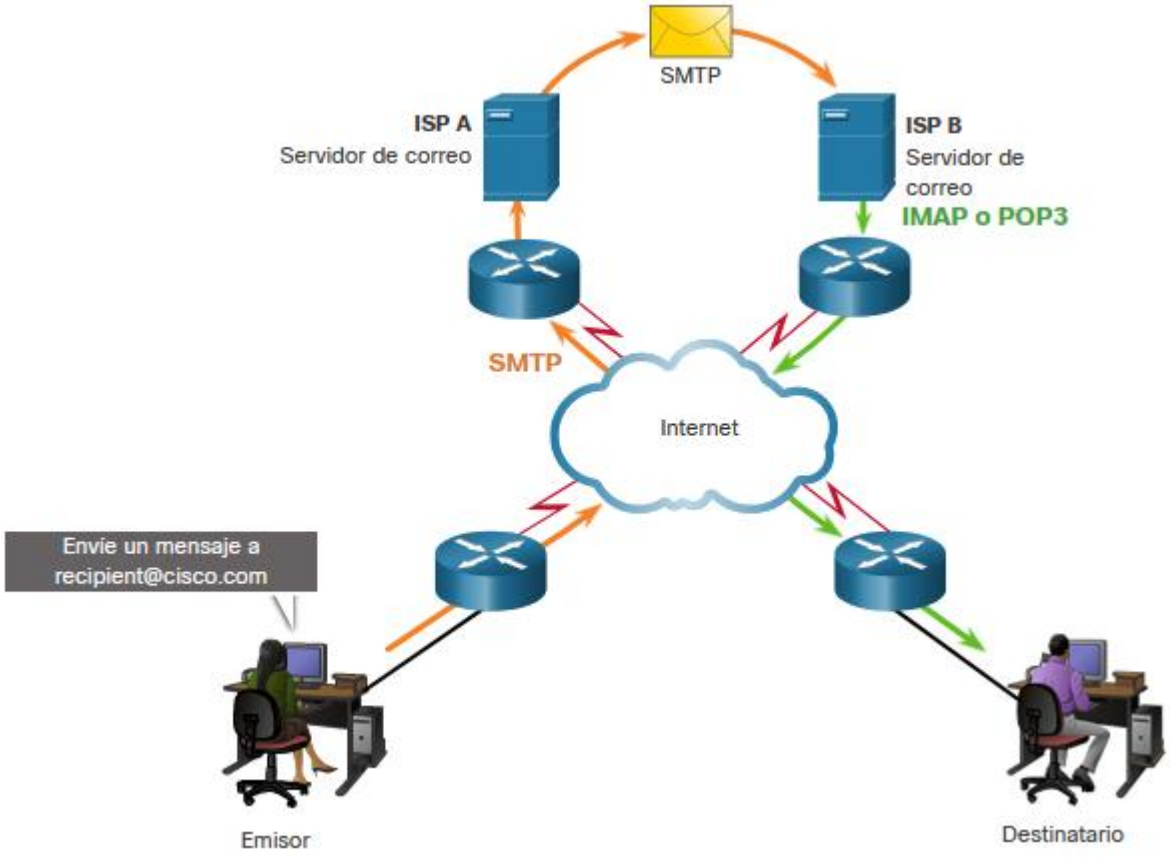
HTTP y HTTPS


ry Bookmarks Tools Help
http://www.cisco.com/
Localizador uniforme de recursos (URL)
Solicitud de protocolo HTTP
Archivo solicitado
Servidor HTTP
Cliente
Host: www.cisco.com
GET /index.html HTTP/1.1
Nombre de dominio totalmente calificado

3 Protocolos de correo electrónico

Protocolos de correo electrónico

Para ejecutar el correo electrónico en un PC o en otro terminal, se requieren varios servicios y aplicaciones. **El correo electrónico es un método de guardado y desvío que se utiliza para enviar, guardar y recuperar mensajes electrónicos a través de una red.** Los mensajes de correo electrónico se guardan en bases de datos en servidores de correo.



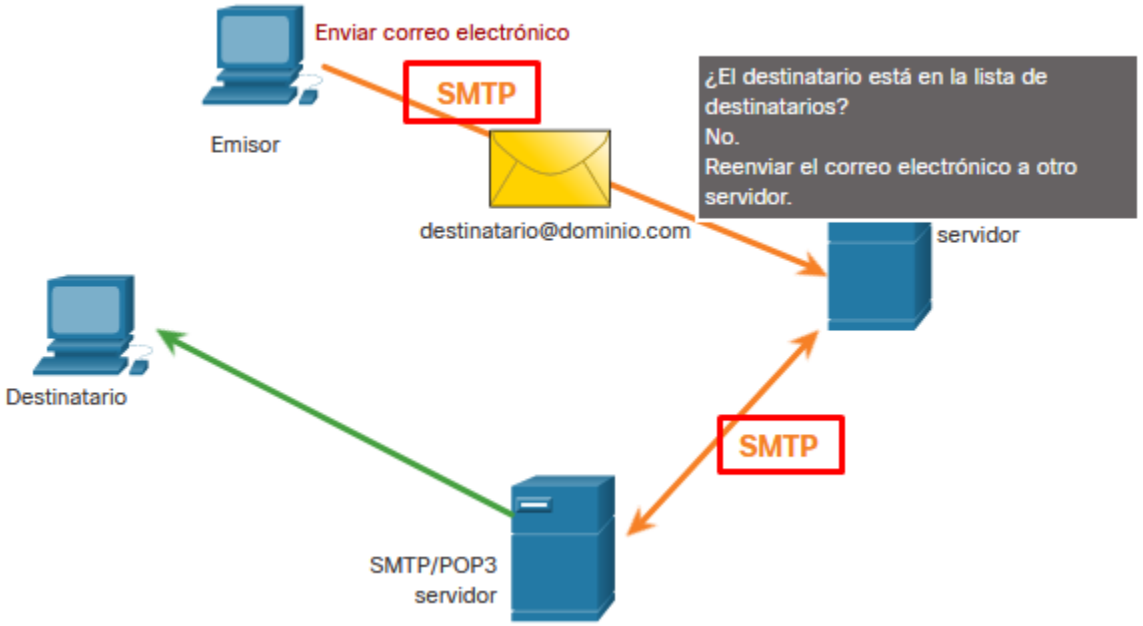
Protocolos de correo electrónico

Los clientes de correo electrónico se comunican con servidores de correo para enviar y recibir correo electrónico. Los servidores de correo se comunican con otros servidores de correo para transportar mensajes desde un dominio a otro. Un cliente de correo electrónico no se comunica directamente con otro cliente de correo electrónico cuando envía un correo electrónico. En cambio, ambos clientes dependen del servidor de correo para transportar los mensajes.

El correo electrónico admite tres protocolos diferentes para su funcionamiento: el protocolo simple de transferencia de correo (**SMTP**), el protocolo de oficina de correos (**POP**) e **IMAP**. El proceso de capa de aplicaciones que envía correo utiliza el SMTP. Un cliente recupera el correo electrónico mediante uno de los dos protocolos de capa de aplicaciones: el POP o el IMAP.

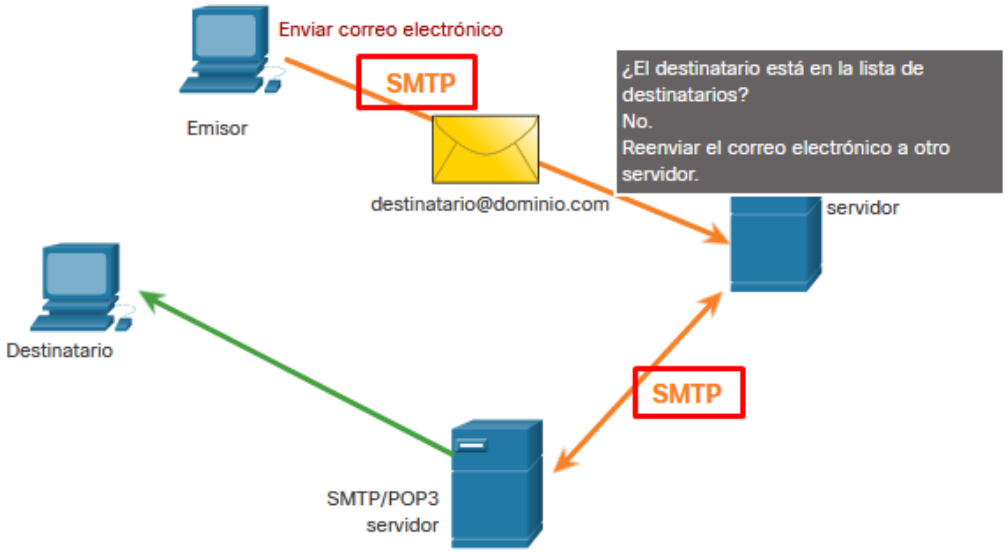
Protocolos de correo electrónico

Cuando un cliente envía correo electrónico, el proceso SMTP del cliente se conecta a un proceso **SMTP** del servidor en el **puerto** bien conocido **25**. Después de que se establece la conexión, el cliente intenta enviar el correo electrónico al servidor a través de esta. Una vez que el servidor recibe el mensaje, lo ubica en una cuenta local (si el destinatario es local) o lo reenvía a otro servidor de correo para su entrega.



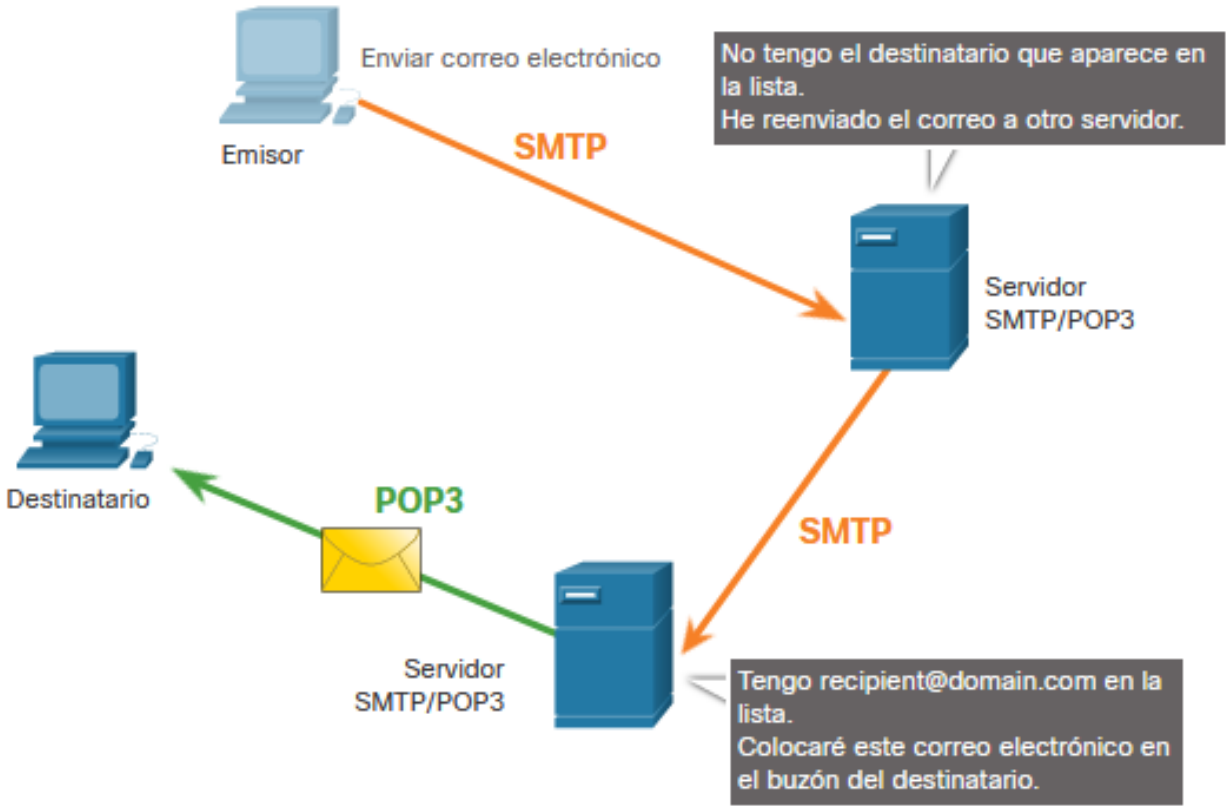
Protocolos de correo electrónico

El servidor de correo electrónico de destino puede no estar en línea, o estar muy ocupado, cuando se envían los mensajes. Por lo tanto, el SMTP pone los mensajes en cola para enviarlos posteriormente. El servidor verifica periódicamente la cola en busca de mensajes e intenta enviarlos nuevamente. Si el mensaje aún no se ha entregado después de un tiempo predeterminado de expiración, se devolverá al emisor como imposible de entregar.



Protocolos de correo electrónico

POP es utilizado por una aplicación para recuperar correo electrónico de un servidor de correo. Con POP, el correo se descarga desde el servidor al cliente y después se elimina en el servidor.



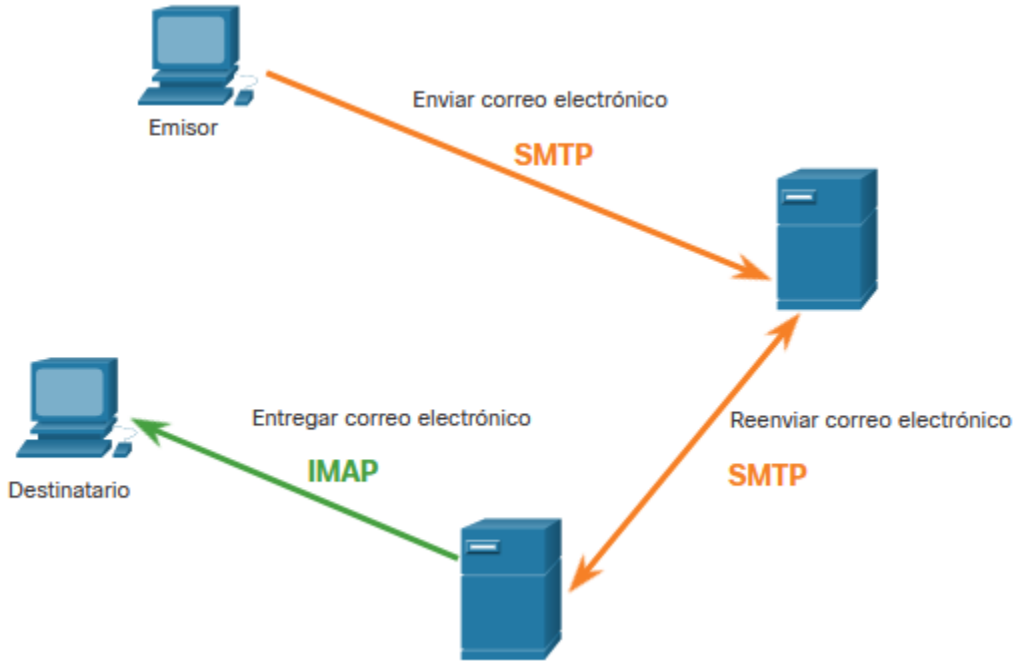
Protocolos de correo electrónico

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

Con POP, los mensajes de correo electrónico se descargan en el cliente y se eliminan del servidor, esto significa que no existe una ubicación centralizada donde se conserven los mensajes de correo electrónico. Como POP no almacena mensajes, no es una opción adecuada para una pequeña empresa que necesita una solución de respaldo centralizada. **POP3 es la versión más utilizada.**

Protocolos de correo electrónico

IMAP es otro protocolo que describe un método para recuperar mensajes de correo electrónico. A diferencia de POP, cuando el usuario se conecta a un servidor con capacidad IMAP, se **descargan copias de los mensajes a la aplicación cliente. Puerto 143.**



4 Servicios de direccionamiento IP

4.1 DNS

Servicio de nombres de dominios

Existen otros protocolos específicos de capa de aplicación diseñados para facilitar la obtención de direcciones para dispositivos de red. Estos servicios son esenciales porque llevaría mucho tiempo recordar direcciones IP en lugar de direcciones URL o configurar manualmente todos los dispositivos de una red mediana a grande.

Servicio de nombres de dominios

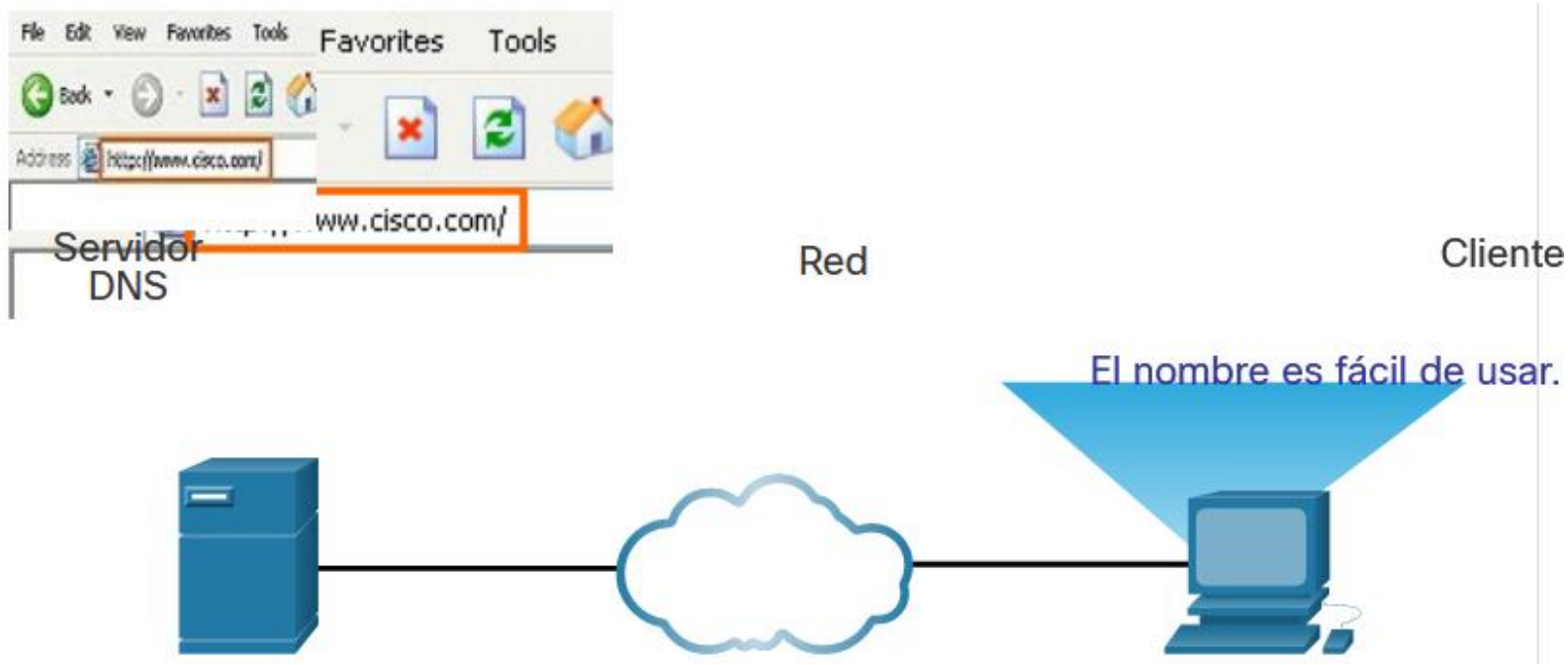
En Internet, los nombres de dominio, como http://www.cisco.com, son mucho más fáciles de recordar para las personas que 198.133.219.25, que es la dirección IP numérica real para este servidor. Si Cisco decide cambiar la dirección numérica de www.cisco.com, esto no afecta al usuario, porque el nombre de dominio se mantiene. Simplemente se une la nueva dirección al nombre de dominio existente y se mantiene la conectividad.

El **protocolo DNS define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada.** Incluye el formato de consultas, respuestas y datos.

Servicio de nombres de dominios

Paso 1

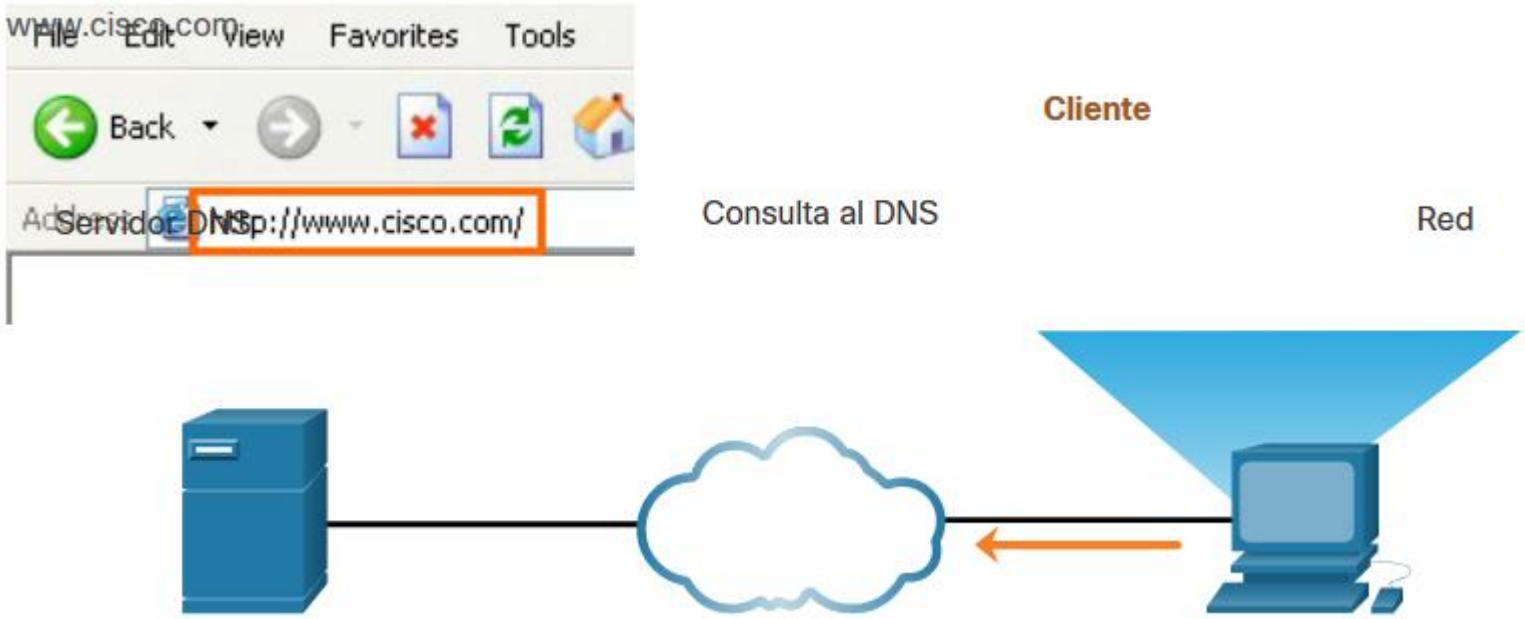
El usuario escribe un FQDN *Fully Qualified Domain Name*, es decir, un nombre de dominio completo, en un campo Dirección de aplicación del explorador.



Servicio de nombres de dominios

Paso 2

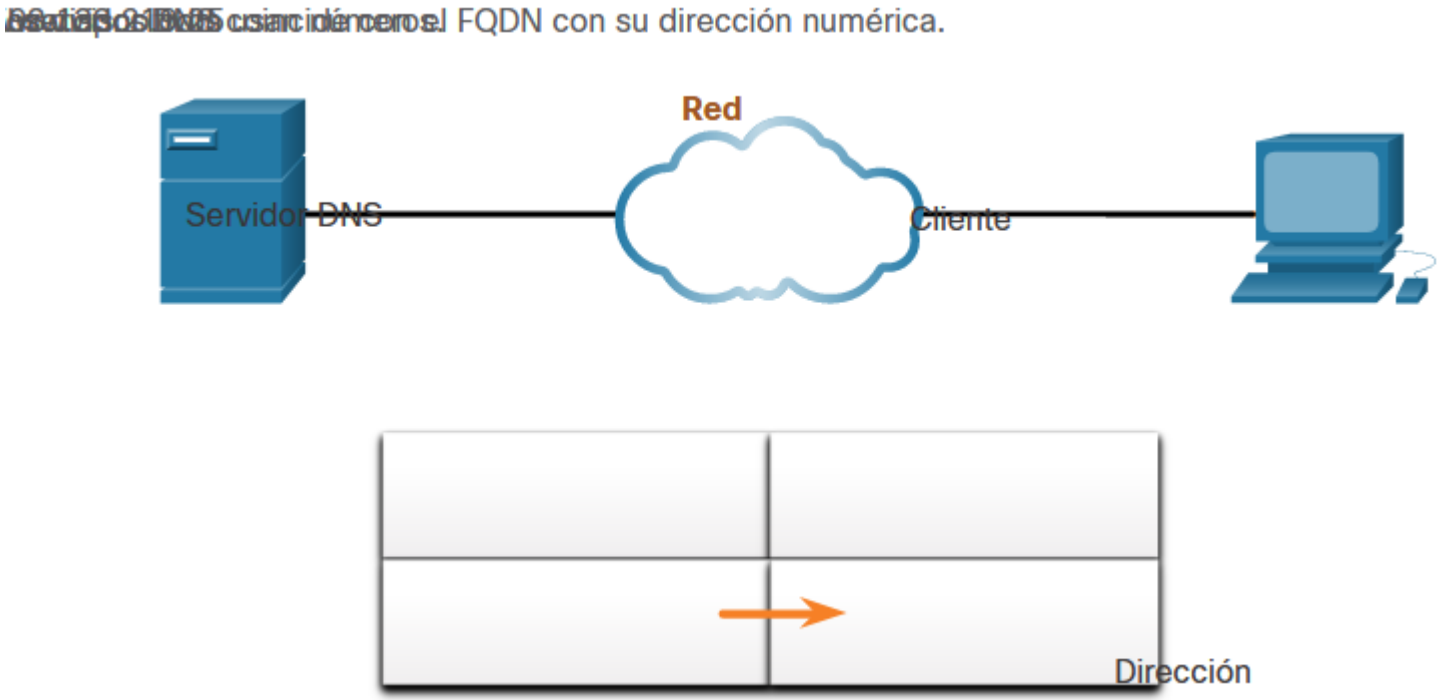
Se envía una consulta DNS al servidor DNS designado para el equipo cliente.



Servicio de nombres de dominios

Paso 3

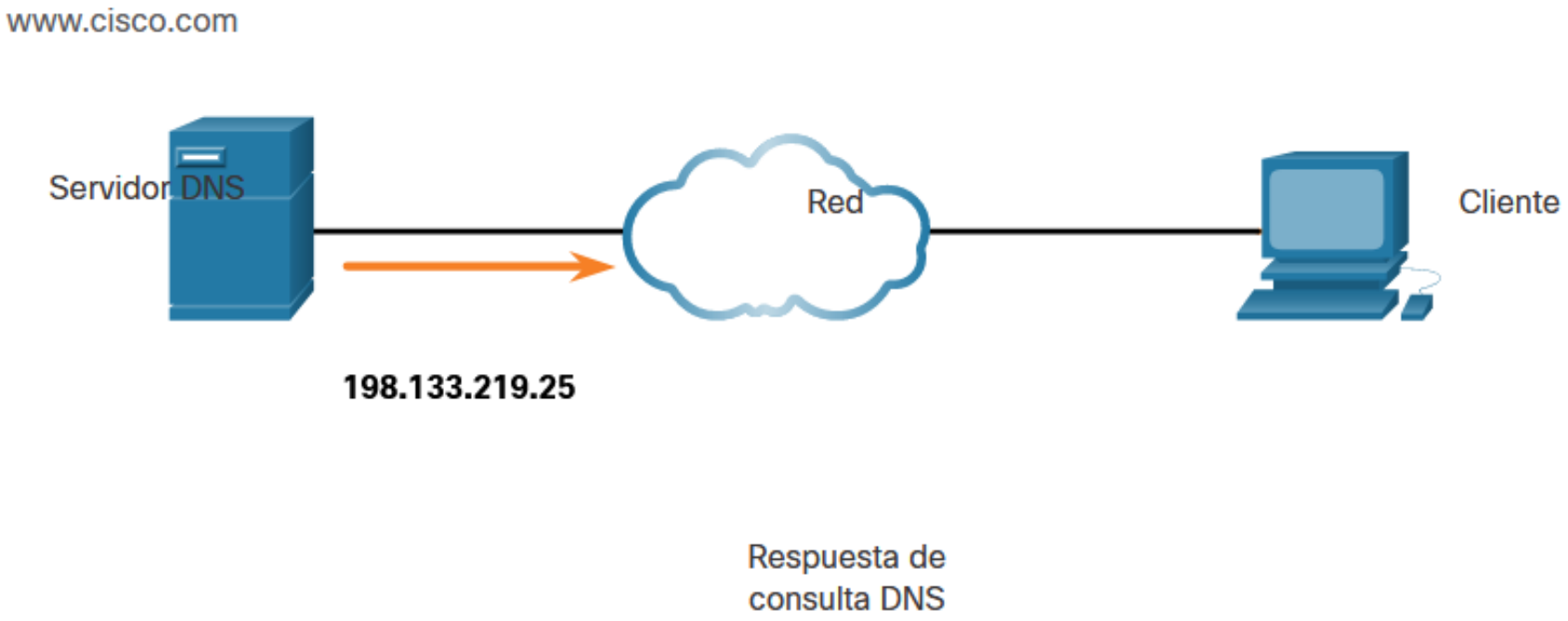
El servidor DNS coincide con el FQDN con su dirección IP.



Servicio de nombres de dominios

Paso 4

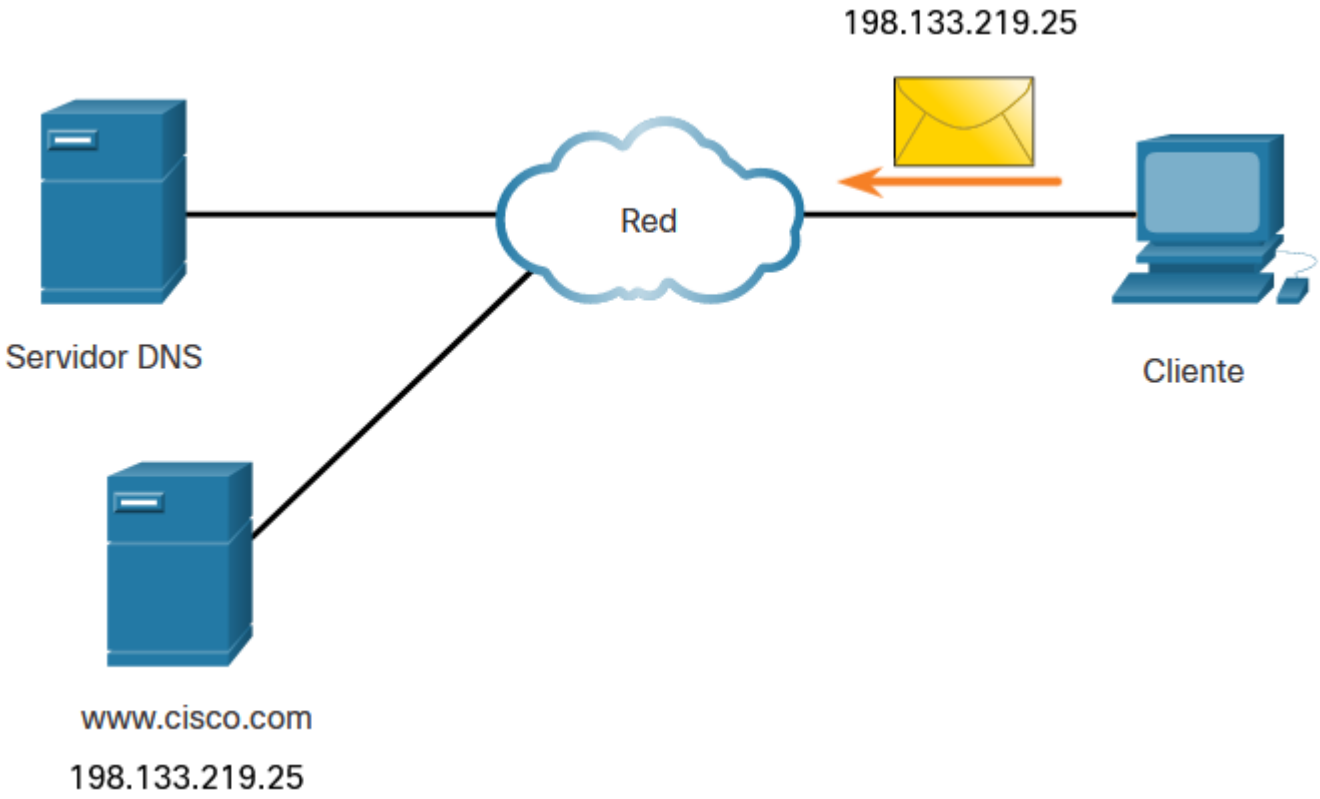
La respuesta de consulta DNS se envía de nuevo al cliente con la dirección IP del FQDN.



Servicio de nombres de dominios

Paso 5

El equipo cliente utiliza la dirección IP para realizar solicitudes del servidor.



Servicio de nombres de dominios

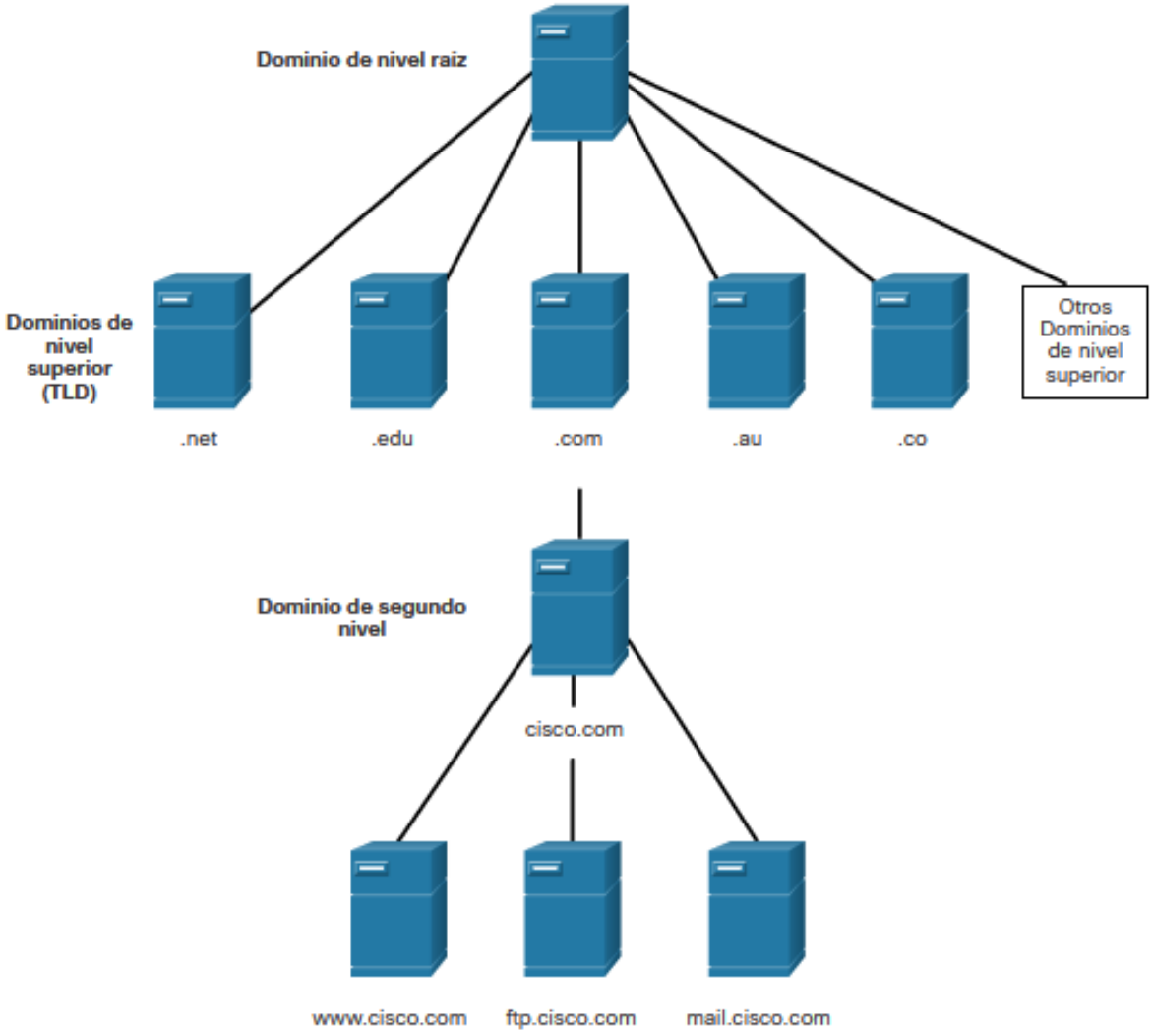
Cuando un cliente realiza una consulta, el proceso DNS del servidor observa primero sus propios registros para resolver el nombre. **Si no puede resolverlo** con los registros almacenados, **contacta a otros servidores para hacerlo**. Una vez que se encuentra una coincidencia y se la devuelve al servidor solicitante original, este almacena temporalmente la dirección numerada por si se vuelve a solicitar el mismo nombre.

El servicio del cliente DNS en los equipos Windows también almacena los nombres resueltos previamente en la memoria. El comando **ipconfig /displaydns** muestra todas las entradas de DNS en caché. **ipconfig /flushdns** elimina las entradas DNS en caché.

Jerarquía DNS

El protocolo DNS utiliza un **sistema jerárquico** para crear una base de datos que proporcione la resolución de nombres.

Los diferentes dominios de primer nivel representan el tipo de organización o el país de origen.



nslookup

Los sistemas operativos informáticos también cuentan con una herramienta llamada **nslookup** que permite que el usuario consulte de forma manual los servidores de nombres para resolver un nombre de host dado. Esta utilidad también puede utilizarse para solucionar los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.

```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
```

4.2 DHCP

Protocolo de configuración dinámica de host

El protocolo **DHCP** del servicio IPv4 **automatiza la asignación de direcciones IPv4, máscaras de subred, gateways y otros parámetros de redes IPv4.** Esto se denomina "**direccionamiento dinámico**". La **alternativa** al direccionamiento dinámico es el **direccionamiento estático**. Al utilizar el direccionamiento estático, el administrador de redes introduce manualmente la información de la dirección IP en los hosts.

Cuando un host se conecta a la red, se realiza el contacto con el servidor de DHCP y se solicita una dirección. **El servidor de DHCP elige una dirección de un rango de direcciones configurado llamado grupo y la asigna (concede) al host.**

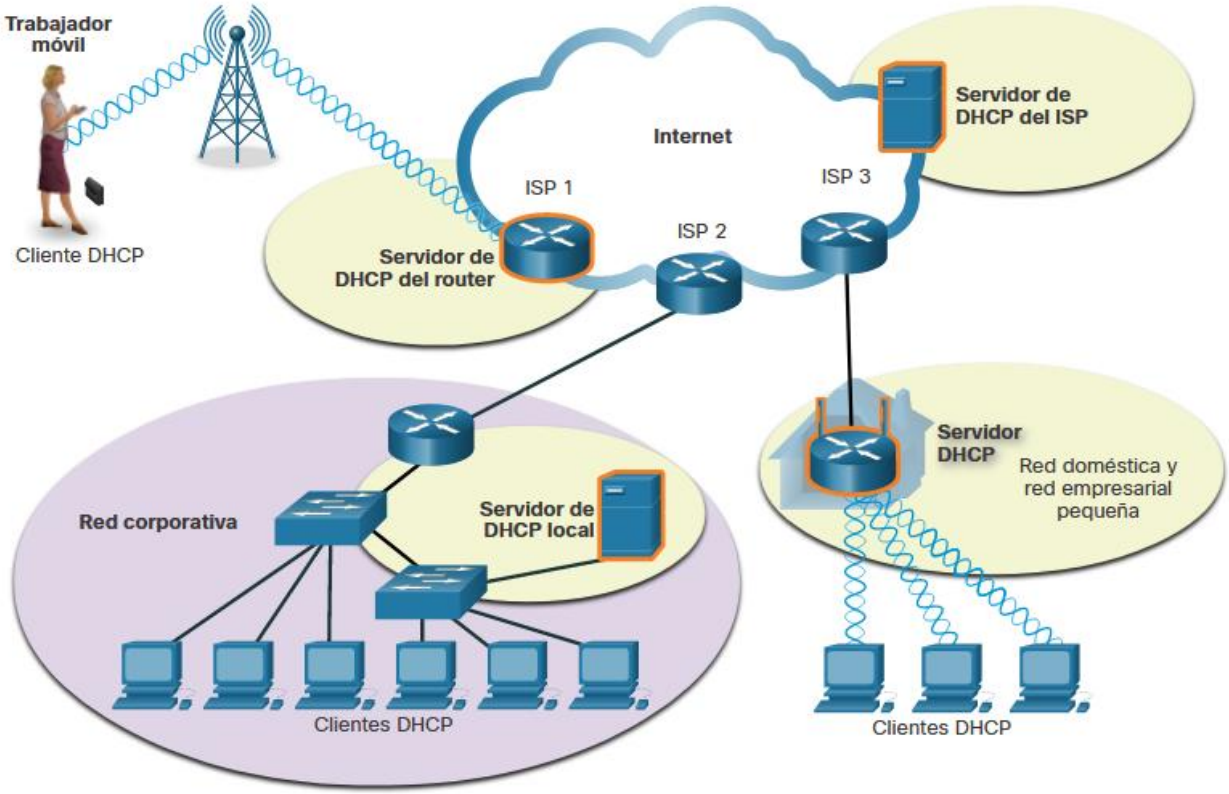
Protocolo de configuración dinámica de host

En **redes** más **grandes**, o donde los usuarios cambian con frecuencia, se prefiere asignar direcciones con **DHCP**.

DHCP puede asignar direcciones IP durante un período de tiempo configurable, denominado período de concesión. **Cuando caduca el período de concesión o el servidor DHCP recibe un mensaje DHCPRELASE, la dirección se devuelve al grupo DHCP para su reutilización.** Los usuarios pueden moverse libremente desde una ubicación a otra y volver a establecer con facilidad las conexiones de red por medio de DHCP.

Protocolo de configuración dinámica de host

En la mayoría de las **redes medianas a grandes, el servidor DHCP suele ser un servidor local** y dedicado con base en una PC. En las **redes domésticas, el servidor de DHCP** suele estar ubicado en el **router local** que conecta la red doméstica al ISP.

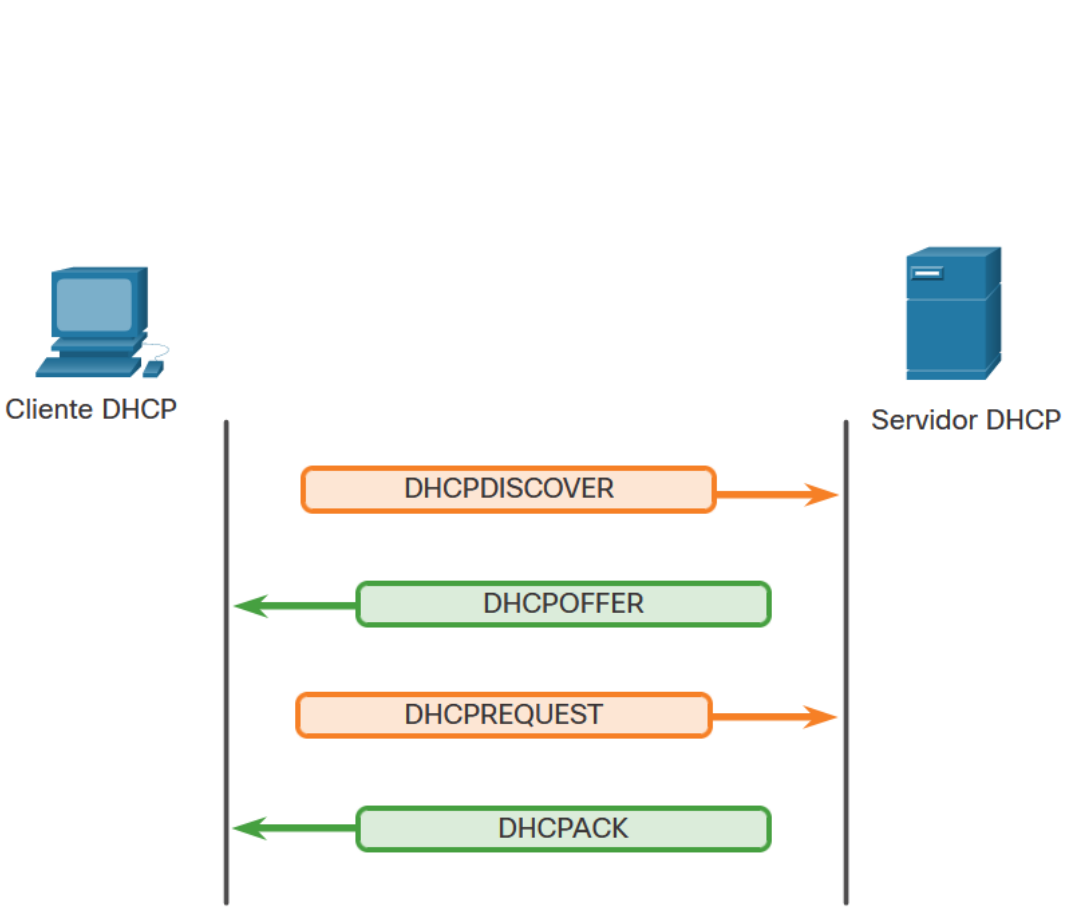


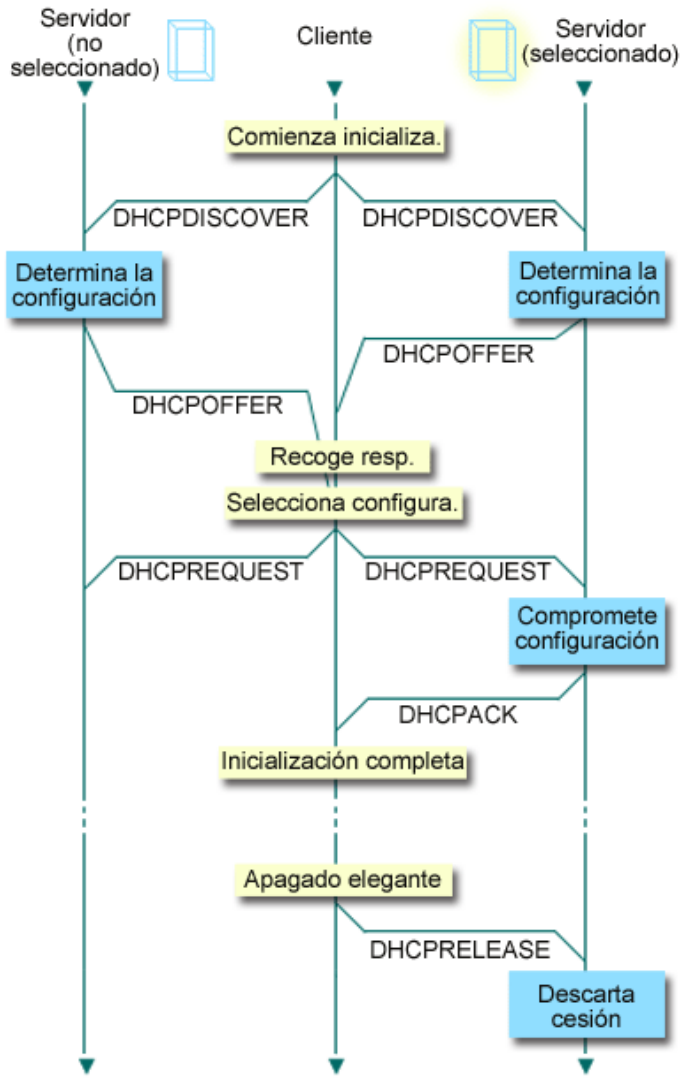
Protocolo de configuración dinámica de host

Muchas redes utilizan tanto el direccionamiento estático como DHCP. **DHCP** se utiliza para hosts de propósito general, tales como los dispositivos de **usuario final**. El **direccionamiento estático** se utiliza para los **dispositivos de red, tales como gateways, switches, servidores e impresoras.**

DHCPv6 (DHCP para IPv6) proporciona servicios similares para los clientes IPv6. Una diferencia importante es que DHCPv6 no brinda una dirección de gateway predeterminado. Esto sólo se puede obtener de forma dinámica a partir del anuncio de router del propio router (la dirección link-local del mensaje RA).

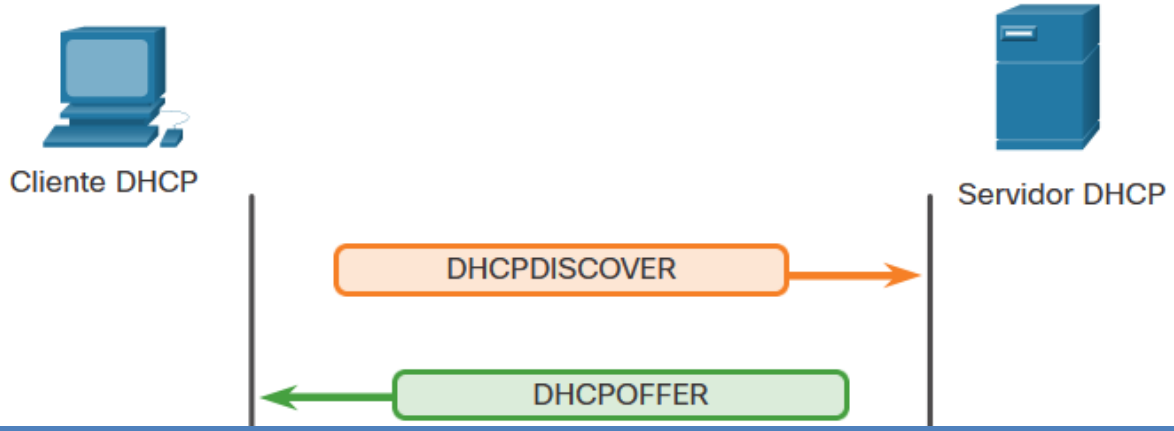
Funcionamiento de DHCP





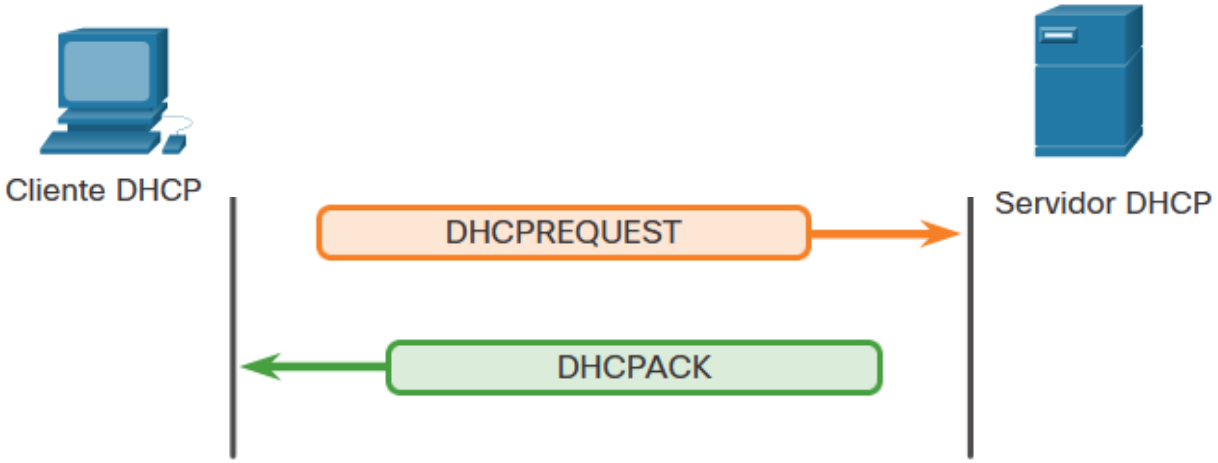
Funcionamiento de DHCP

Cuando un dispositivo configurado con DHCP e IPv4 se inicia o se conecta a la red, el cliente transmite un mensaje de detección de DHCP (**DHCPDISCOVER**) para identificar cualquier servidor de DHCP disponible en la red (**broadcast**). Un servidor de DHCP responde con un mensaje de oferta de DHCP (DHCPOFFER), que ofrece una concesión al cliente. El mensaje de oferta contiene **la dirección IPv4 y la máscara de subred que se deben asignar, la dirección IPv4 del servidor DNS y la dirección IPv4 del gateway predeterminado.** La **oferta de concesión** también incluye la duración de esta.



Funcionamiento de DHCP

El cliente puede recibir varios mensajes DHCPOFFER si hay más de un servidor de DHCP en la red local. Por lo tanto, debe elegir entre ellos y enviar un mensaje de solicitud de DHCP (DHCPREQUEST) que identifique el servidor explícito y la oferta de concesión que el cliente acepta. Este mensaje se difunde por toda la red para que todos los servidores DHCP sepan cuál es el servidor que se ha seleccionado. Un cliente también puede optar por solicitar una dirección previamente asignada por el servidor.



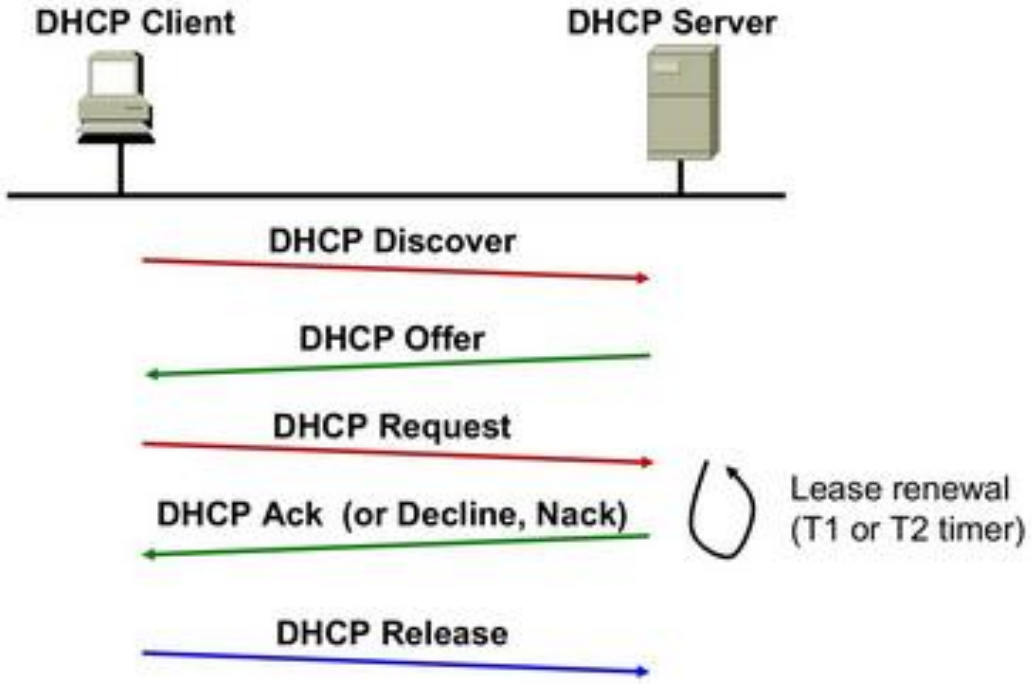
Funcionamiento de DHCP

Suponiendo que la dirección IPv4 solicitada por el cliente, u ofrecida por el servidor, aún está disponible, el servidor devuelve un mensaje de reconocimiento de DHCP (DHCPACK) que le informa al cliente que finalizó la concesión. Si la oferta ya no es válida, el servidor seleccionado responde con un mensaje de reconocimiento negativo de DHCP (DHCPNAK).

Si se devuelve un mensaje DHCPNAK, entonces el **proceso de selección debe volver a comenzar** con la transmisión de un nuevo mensaje DHCPDISCOVER. Una vez que el cliente tiene la concesión, se debe renovar mediante otro mensaje DHCPREQUEST antes de que expire.

Funcionamiento de DHCP

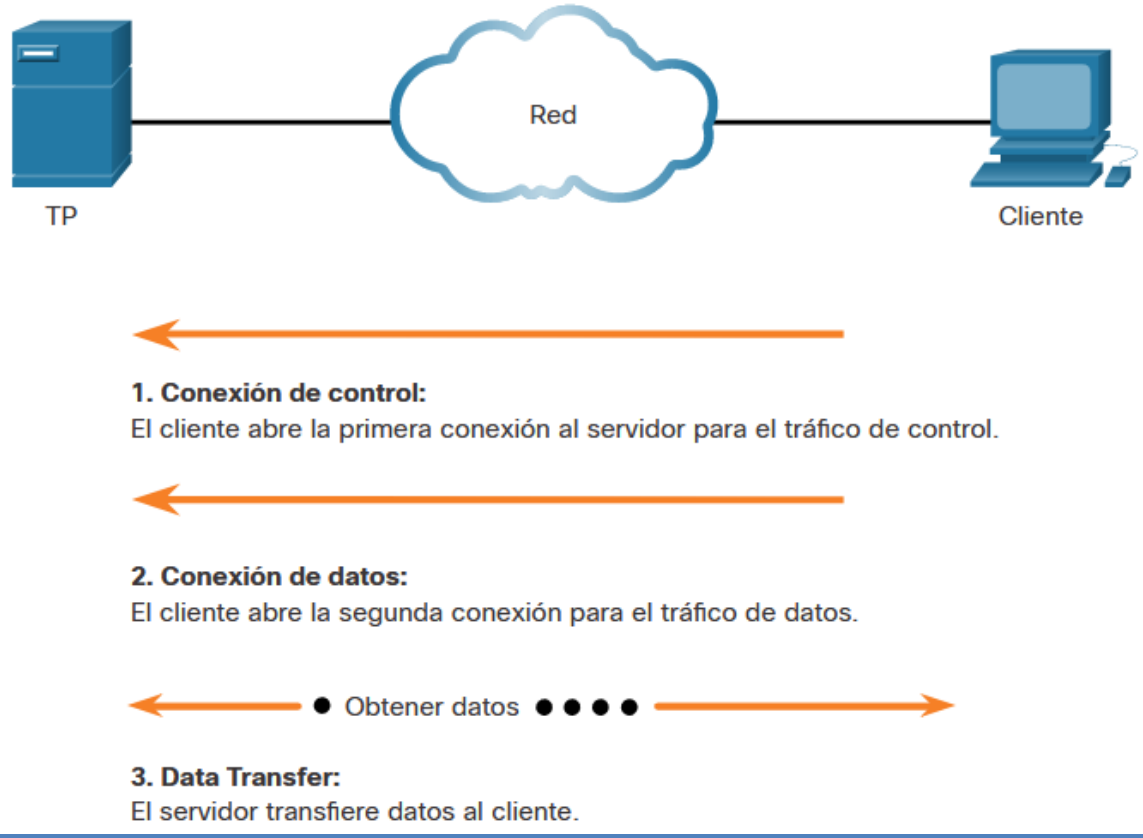
El servidor DHCP asegura que todas las direcciones IP sean únicas (no se puede asignar la misma dirección IP a dos dispositivos de red diferentes de forma simultánea). La mayoría de los proveedores de Internet utilizan DHCP para asignar direcciones a los clientes.



5 Servicios de intercambio de archivos

FTP

En el modelo cliente/servidor, el cliente puede cargar datos a un servidor y descargar datos desde un servidor, si ambos dispositivos utilizan un protocolo de transferencia de archivos (FTP). El protocolo FTP se desarrolló para permitir las transferencias de datos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora cliente y se utiliza para insertar y extraer datos en un servidor FTP.



FTP

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

El cliente establece la **segunda conexión** al servidor para la **transferencia de datos** propiamente dicha por medio del **puerto 20 de TCP**. Esta conexión se crea cada vez que hay datos para transferir.

La transferencia de datos se puede producir en ambas direcciones. El cliente puede descargar (extraer) datos del servidor o subir datos a él (insertarlos).

FTP

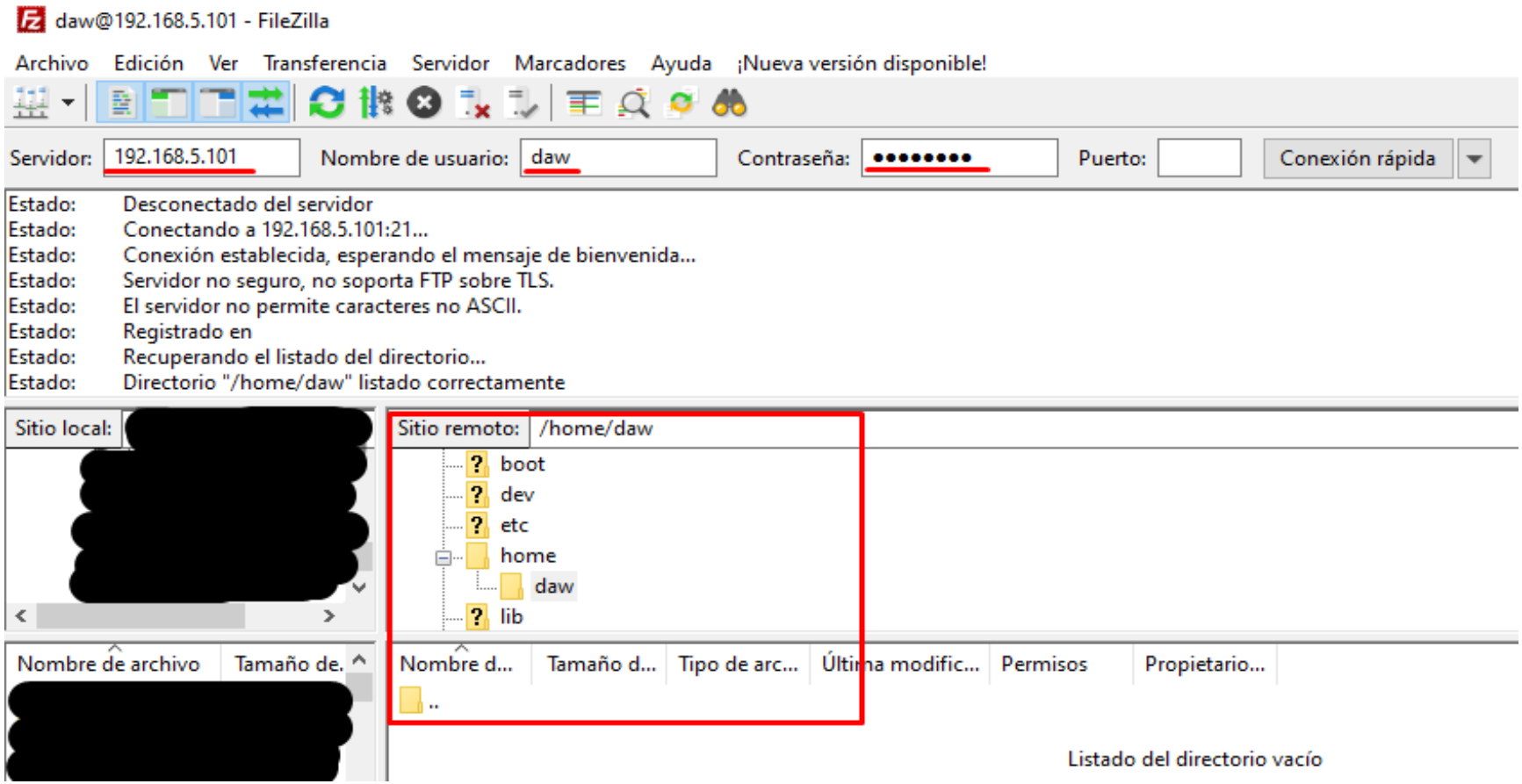
Servidor: vsftpd

```
daw@daw:~$ /sbin/ifcofig
-bash: /sbin/ifcofig: No such file or directory
daw@daw:~$ /sbin/ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fead:4434  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ad:44:34  txqueuelen 1000  (Ethernet)
        RX packets 32413  bytes 31743719 (31.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9841  bytes 617046 (617.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.5.101  netmask 255.255.255.0  broadcast 192.168.5.255
        inet6 fe80::a00:27ff:fe5a:dc63  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5a:dc:63  txqueuelen 1000  (Ethernet)
        RX packets 60  bytes 9742 (9.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3372 (3.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

FTP

Cliente: FileZilla,



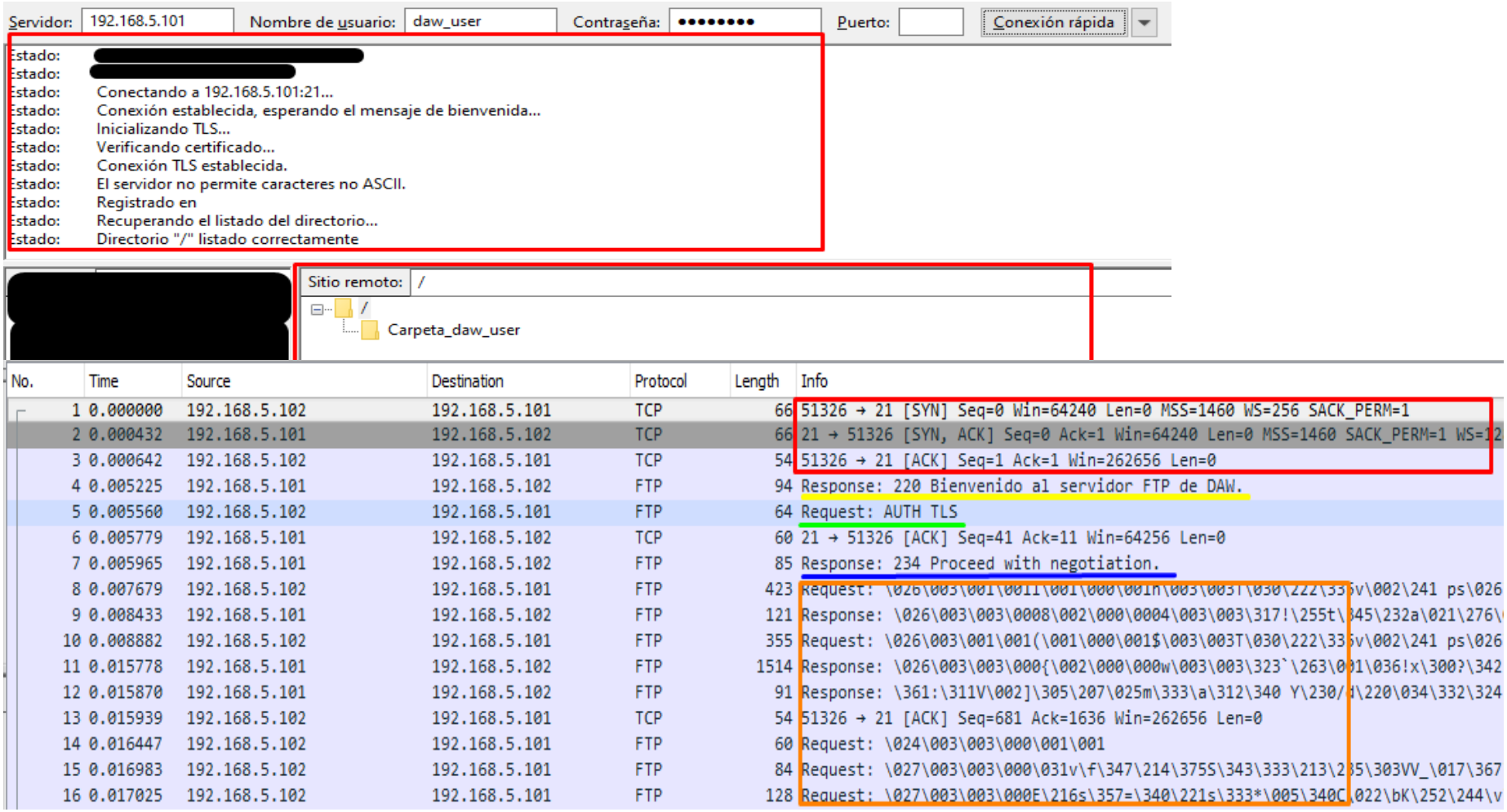
FTP

FTP es inseguro. Podemos capturar credenciales con Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.5.102	192.168.5.101	TCP	66	63651 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACI
2	0.000398	192.168.5.101	192.168.5.102	TCP	66	21 → 63651 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.000499	192.168.5.102	192.168.5.101	TCP	54	63651 → 21 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
4	0.004220	192.168.5.101	192.168.5.102	FTP	94	Response: 220 Bienvenido al servidor FTP de DAW.
5	0.004403	192.168.5.102	192.168.5.101	FTP	64	Request: AUTH TLS
6	0.004604	192.168.5.101	192.168.5.102	TCP	60	21 → 63651 [ACK] Seq=41 Ack=11 Win=64256 Len=0
7	0.004662	192.168.5.101	192.168.5.102	FTP	92	Response: 530 Please login with USER and PASS.
8	0.004746	192.168.5.102	192.168.5.101	FTP	64	Request: AUTH SSL
9	0.004960	192.168.5.101	192.168.5.102	FTP	92	Response: 530 Please login with USER and PASS.
10	0.016368	192.168.5.102	192.168.5.101	FTP	69	Request: USER daw user
11	0.016731	192.168.5.101	192.168.5.102	FTP	88	Response: 331 Please specify the password.
12	0.016875	192.168.5.102	192.168.5.101	FTP	69	Request: PASS password
13	0.060215	192.168.5.101	192.168.5.102	TCP	60	21 → 63651 [ACK] Seq=151 Ack=51 Win=64256 Len=0
14	0.085933	192.168.5.101	192.168.5.102	FTP	77	Response: 230 Login successful.
15	0.086079	192.168.5.102	192.168.5.101	FTP	60	Request: SYST
16	0.086259	192.168.5.101	192.168.5.102	TCP	60	21 → 63651 [ACK] Seq=174 Ack=57 Win=64256 Len=0
17	0.086314	192.168.5.101	192.168.5.102	FTP	73	Response: 215 UNIX Type: L8
18	0.086397	192.168.5.102	192.168.5.101	FTP	60	Request: FEAT
19	0.086631	192.168.5.101	192.168.5.102	FTP	69	Response: 211-Features:
20	0.086694	192.168.5.101	192.168.5.102	FTP	61	Response: EPRT

FTP

Hay que encriptar y utilizar FTPS



Gracias por la atenshion!