

NIVEL DE APLICACIÓN



CONTENIDOS

- Introducción
- Protocolos de navegación web
- Protocolos de correo electrónico
- Protocolo de transferencia de ficheros
- Protocolo de resolución de nombres
- Protocolo de configuración dinámica de host

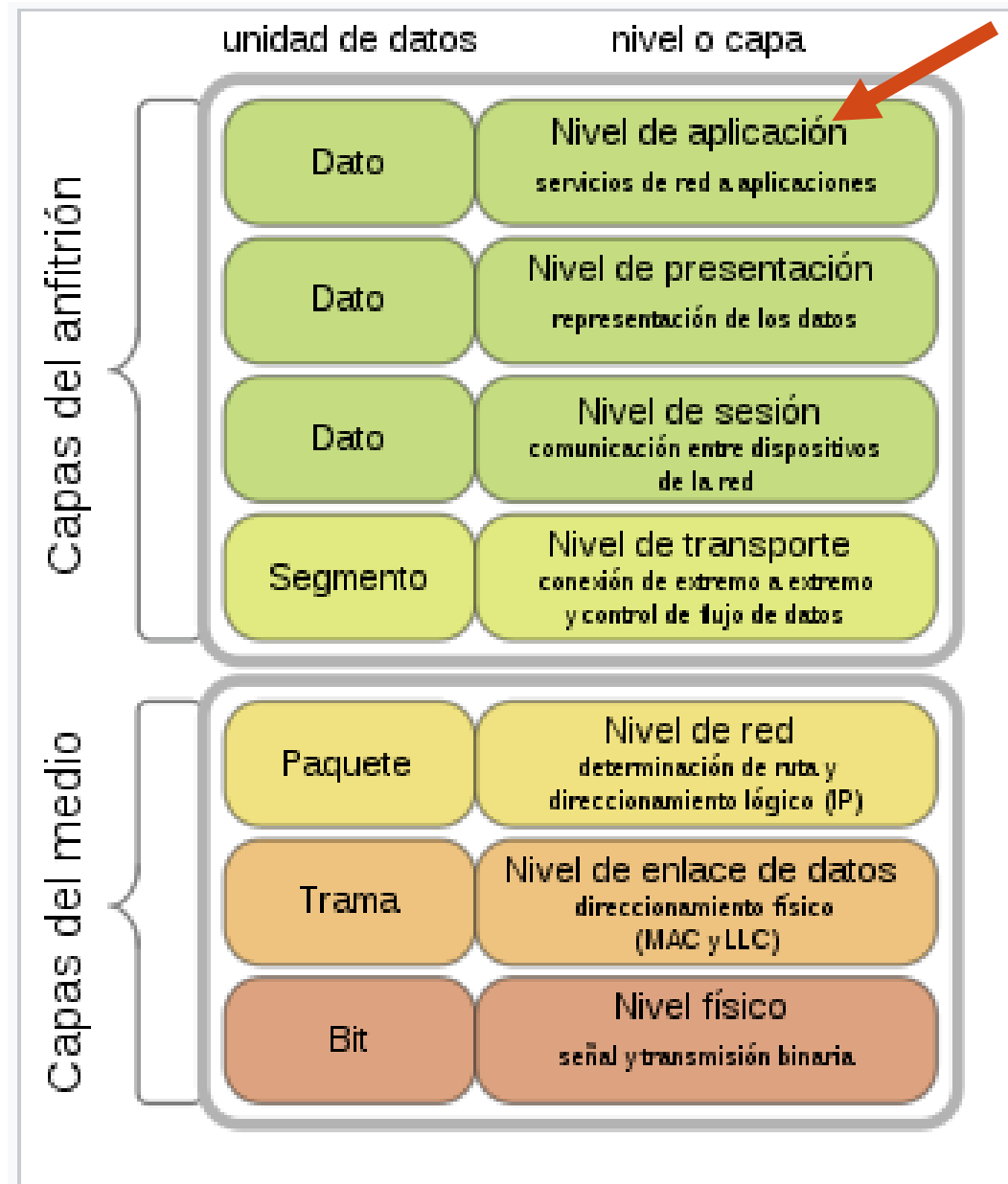


INTRODUCCIÓN

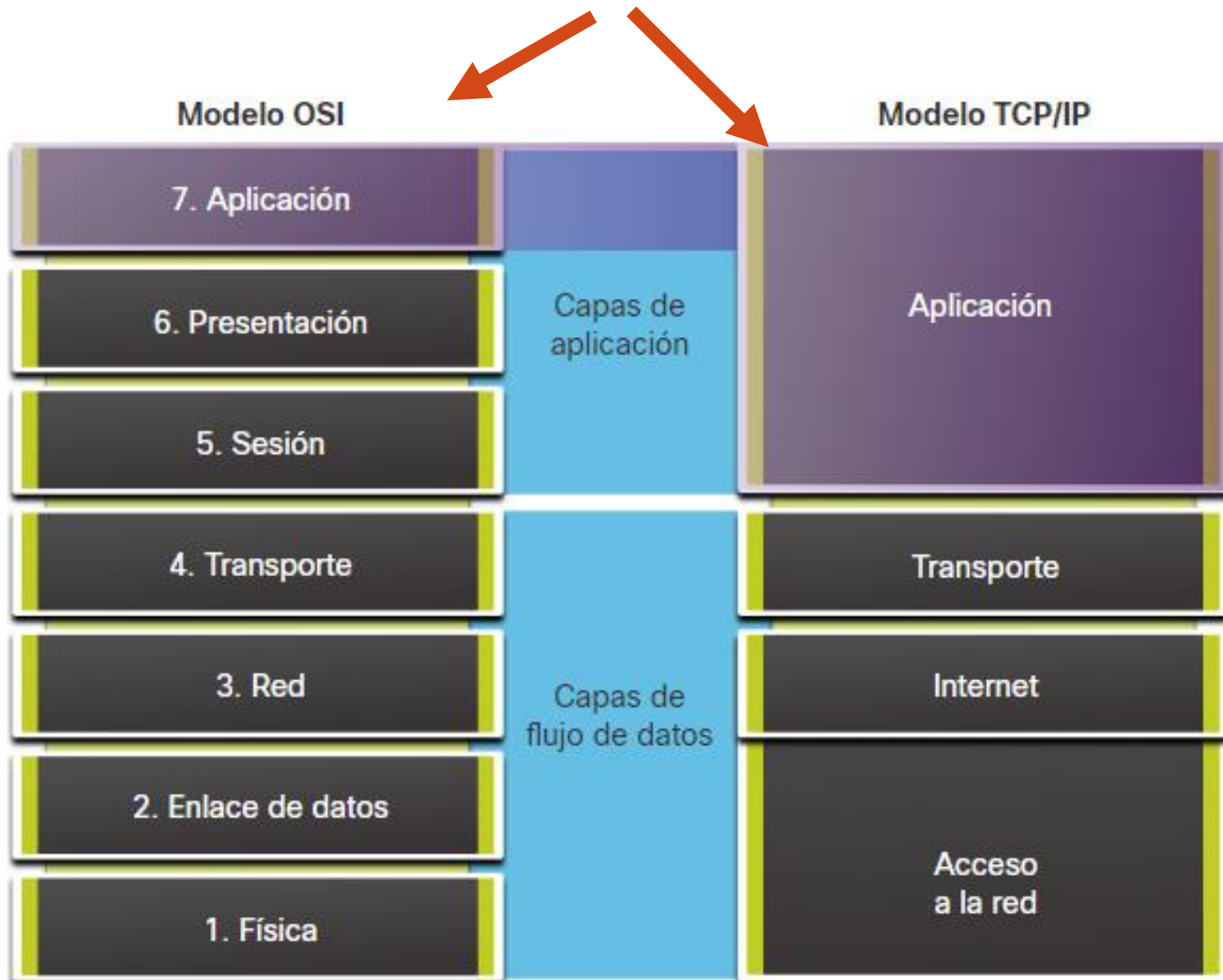


DONDE ESTAMOS

- Capa 7 del modelo OSI



DONDE ESTAMOS



CAPA DE PRESENTACIÓN Y SESIÓN

FUNCIONES DE LA CAPA DE PRESENTACIÓN

- 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.

EJEMPLO

Entre los formatos gráficos de imagen conocidos que se utilizan en redes, se incluyen los siguientes: formato de intercambio de gráficos (GIF), formato del Joint Photographic Experts Group (JPEG) y formato de gráficos de red portátiles (PNG).



CAPA DE PRESENTACIÓN Y SESIÓN

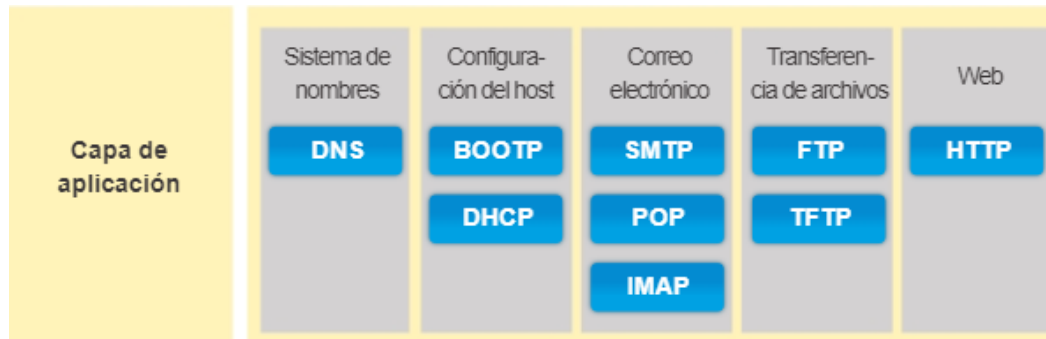
CAPA DE SESIÓN

- Crea y mantiene diálogos entre las aplicaciones de origen y destino.
- 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

- La función principal es la de proporcionar al usuario servicios de cualquier tipo.
- Principales servicios y sus protocolos asociados



Servicio de red	Protocolos
Resolución de nombres de dominio	DNS
Configuración dinámica de host	DHCP, BOOTP, APIPA...
Transferencia de ficheros	FTP, TFTP
Navegar por la web	HTTP, HTTPS
Correo electrónico	SMTP, POP3, IMAP4
Chat	IRC
Streaming	RTSP

SERVICIO VS PROTOCOLO

- ¿Es lo mismo servicio que protocolo?



SERVICIO VS PROTOCOLO

- ¿Es lo mismo servicio que protocolo?



NO

Servicio es una funcionalidad que se ofrece al usuario, mientras que protocolo es una implementación concreta para poder realizar esa funcionalidad.

Ejemplo: tenemos la funcionalidad de navegar por Internet de forma insegura con el protocolo HTTP o de forma segura con el protocolo HTTPS



SERVICIOS DE RED

- En este capítulo veremos de forma general algunos servicios de red como:
 - Asignación dinámica de direcciones DHCP
 - Resolución de nombres de dominio DNS
 - Transferencia de archivos FTP
 - Navegación web HTTP y HTTPS
 - Correo. SMTP y POP3/IMAP
 - Streaming. RSTP



PROTOSCOLOS DE NAVEGACIÓN WEB



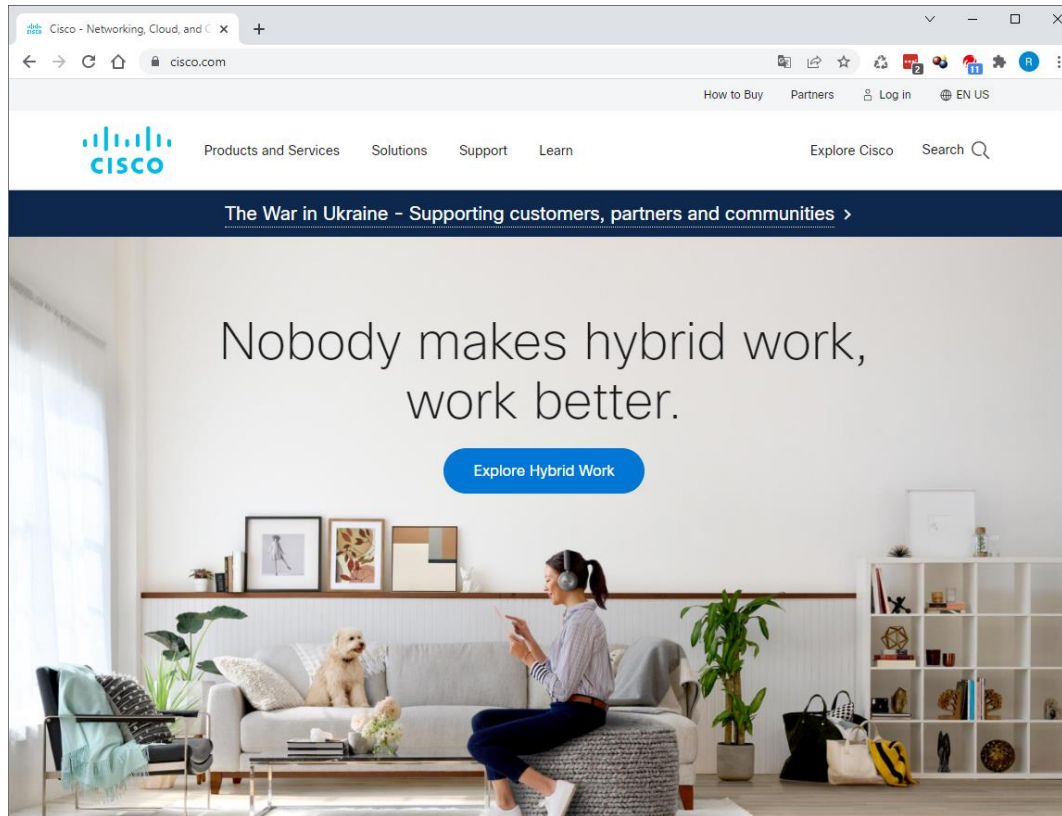
INTRODUCCIÓN

- Existen protocolos específicos de la capa de aplicación diseñados para usos comunes, como la navegación web y el correo electrónico.
- 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 se está ejecutando en el servidor que 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).



CÓMO FUNCIONA NAVEGADOR WEB

- ¿Qué sucede cuando escribimos en el navegador la URL: <http://www.cisco.com>



CÓMO FUNCIONA NAVEGADOR WEB

- ¿Qué sucede cuando escribimos en el navegador la URL:
<http://www.cisco.com>

Paso 1

Paso 2

Paso 3

Paso 4



CÓMO FUNCIONA NAVEGADOR WEB

- ¿Qué sucede cuando escribimos en el navegador la URL:
<http://www.cisco.com>

Paso 1

El explorador interpreta las tres partes del URL:

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

Paso 2

Paso 3

Paso 4



CÓMO FUNCIONA NAVEGADOR WEB

- ¿Qué sucede cuando escribimos en el navegador la URL:
<http://www.cisco.com>

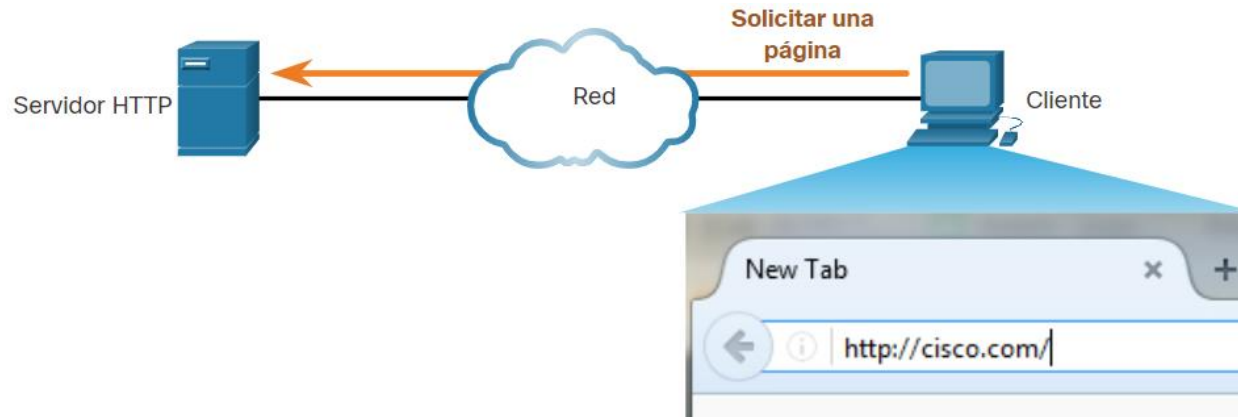
Paso 1

Paso 2

Paso 3

Paso 4

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`.



CÓMO FUNCIONA NAVEGADOR WEB

- ¿Qué sucede cuando escribimos en el navegador la URL:
<http://www.cisco.com>

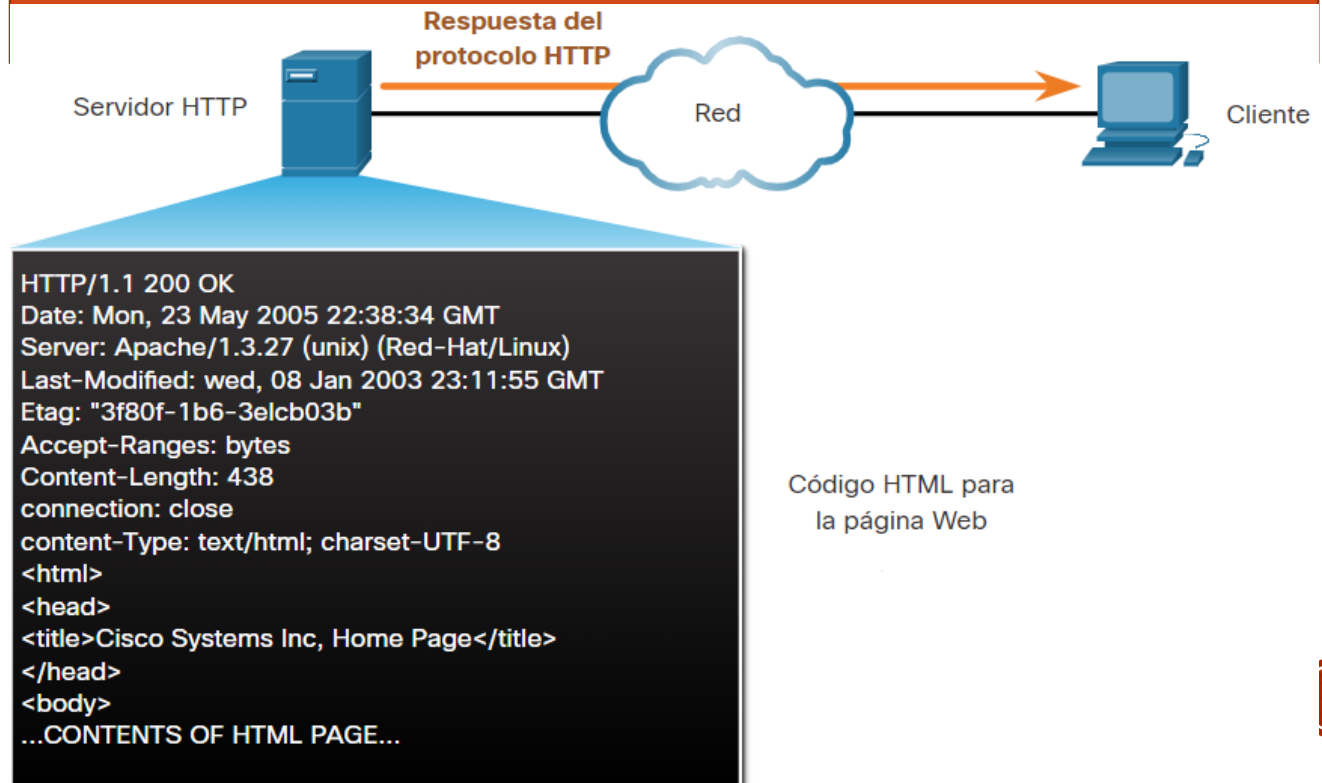
Paso 1

Paso 2

Paso 3

Paso 4

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



CÓMO FUNCIONA NAVEGADOR WEB

- ¿Qué sucede cuando escribimos en el navegador la URL:
<http://www.cisco.com>

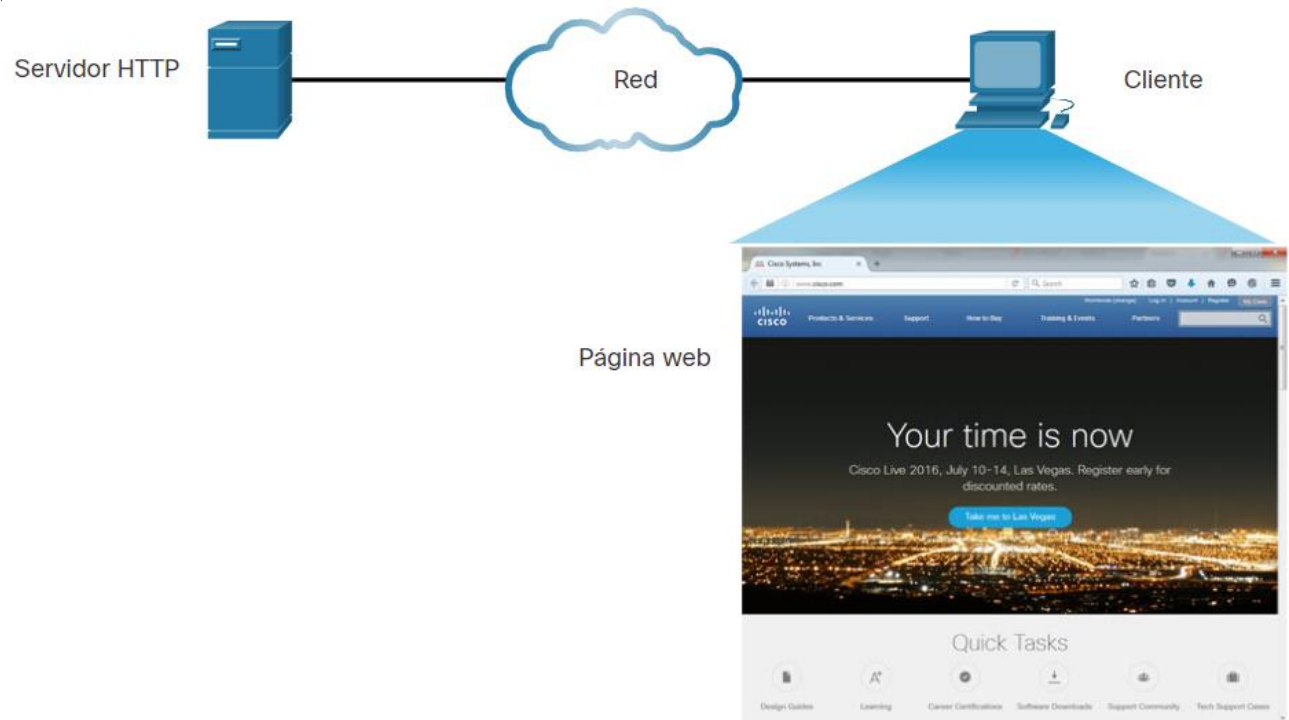
Paso 1

Paso 2

Paso 3

Paso 4

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

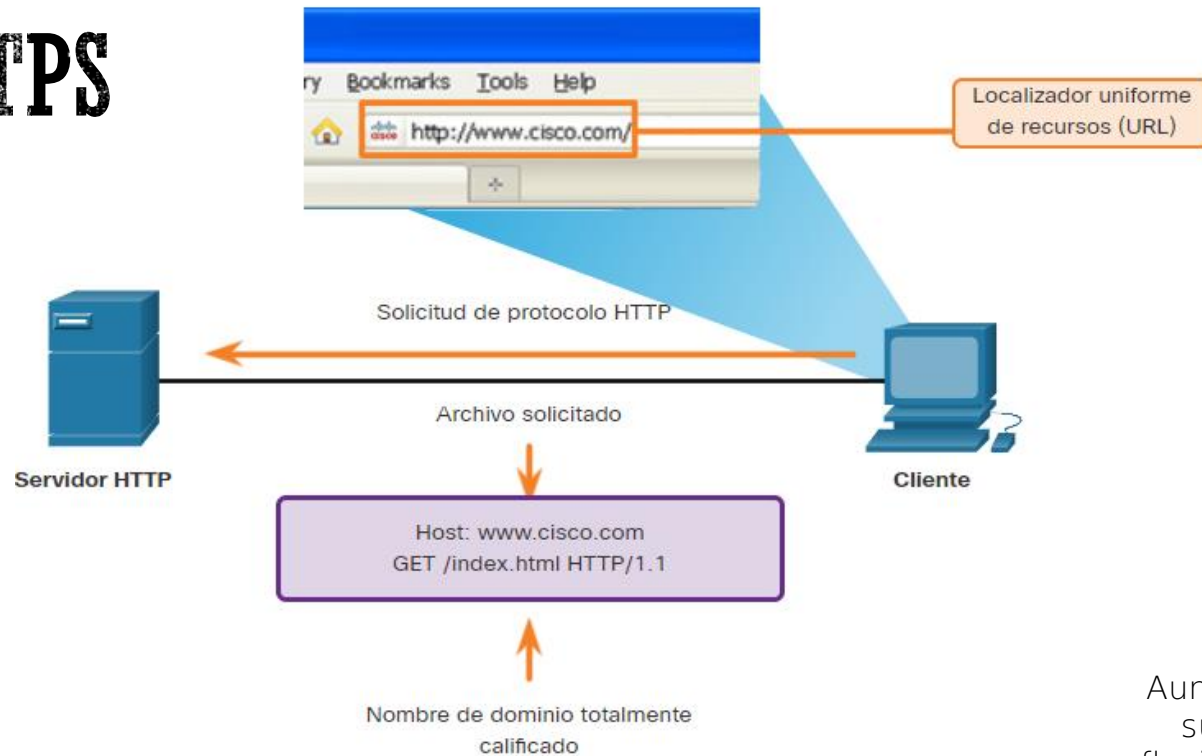


HTTP Y HTTPS

- El protocolo Hyper Text Transfer Protocol (HTTP) está diseñado para transferir páginas web desde un servidor hasta un cliente.
- Una página web está formada por varios tipos de archivos, principalmente un archivo HTML (Hypertext Markup Language) que contiene textos, hipervínculos, imágenes, formularios, tablas, vídeos, .. Además, suele tener archivos CSS (hoja de estilos) y Javascript
- El servidor web se mantiene a la espera de peticiones http, realizadas por el cliente que normalmente llamamos navegador. Después de una petición, si el recurso solicitado existe, el servidor responde enviando el archivo solicitado.
- El cliente es el encargado de interpretar las etiquetas HTML y los estilos CSS, es decir de mostrar el contenido con determinada apariencia de colores, posición, ancho, alto, etc.



HTTP Y HTTPS



Aunque HTTP es sumamente flexible, **no es un protocolo seguro.**

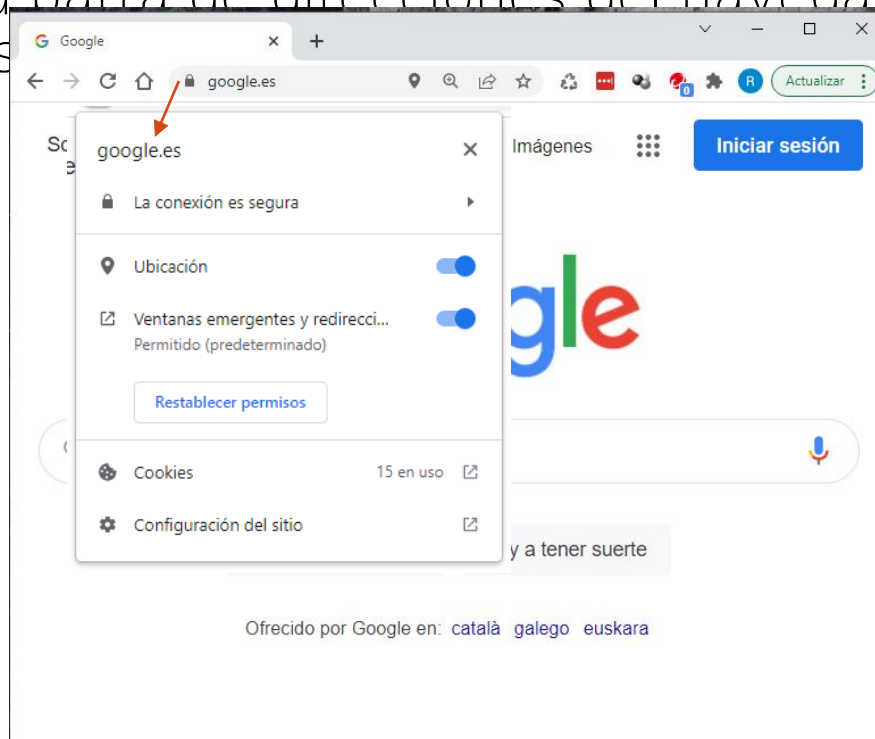
Los mensajes de solicitud envían información al servidor en texto sin formato que puede ser interceptado y leído. Las respuestas del servidor, generalmente páginas HTML, también están sin cifrar.

- 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.

- **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

- El protocolo que proporciona un servicio web seguro es HTTPS, para lo cual realiza un cifrado de todos los datos que intercambian cliente y servidor.
- En la barra de direcciones del navegador aparece expresamente https

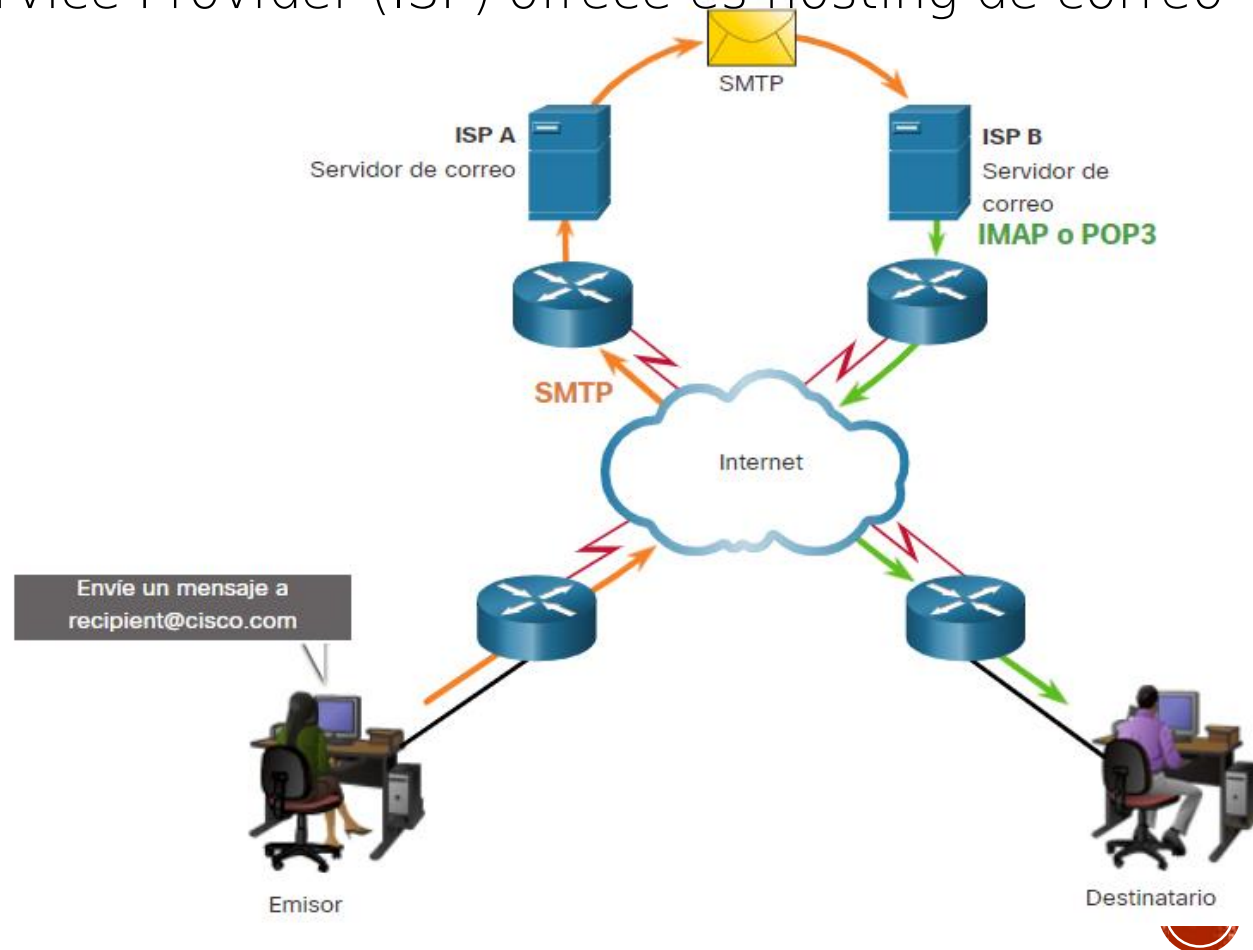


PROTOSCOLOS DE CORREO ELECTRÓNICO



INTRODUCCIÓN

- Uno de los principales servicios que un Proveedor de Servicios de Internet o Internet Service Provider (ISP) ofrece es hosting de correo electrónico
- Para ejecutar el correo electrónico en un PC o en otro terminal, se requieren varios servicios y aplicaciones.



INTRODUCCIÓN

- Un cliente de correo electrónico no se comunica directamente con otro cliente de correo electrónico cuando envía un correo electrónico.
- Los **clientes** de correo electrónico **se comunican con servidores de correo** para enviar y recibir correo electrónico.
- El **correo electrónico admite tres protocolos** diferentes para su funcionamiento

Simple Mail Transfer
Protocol(SMTP)

Post Office Protocol
(POP)

Internet Message
Access Protocol (IM
AP)



SMTP

- Es un protocolo para enviar mensajes desde un usuario a su servidor de correo y para el envío entre servidores.
- Protocolo orientado a la conexión y basado en texto.
- Utiliza como protocolo de transporte TCP

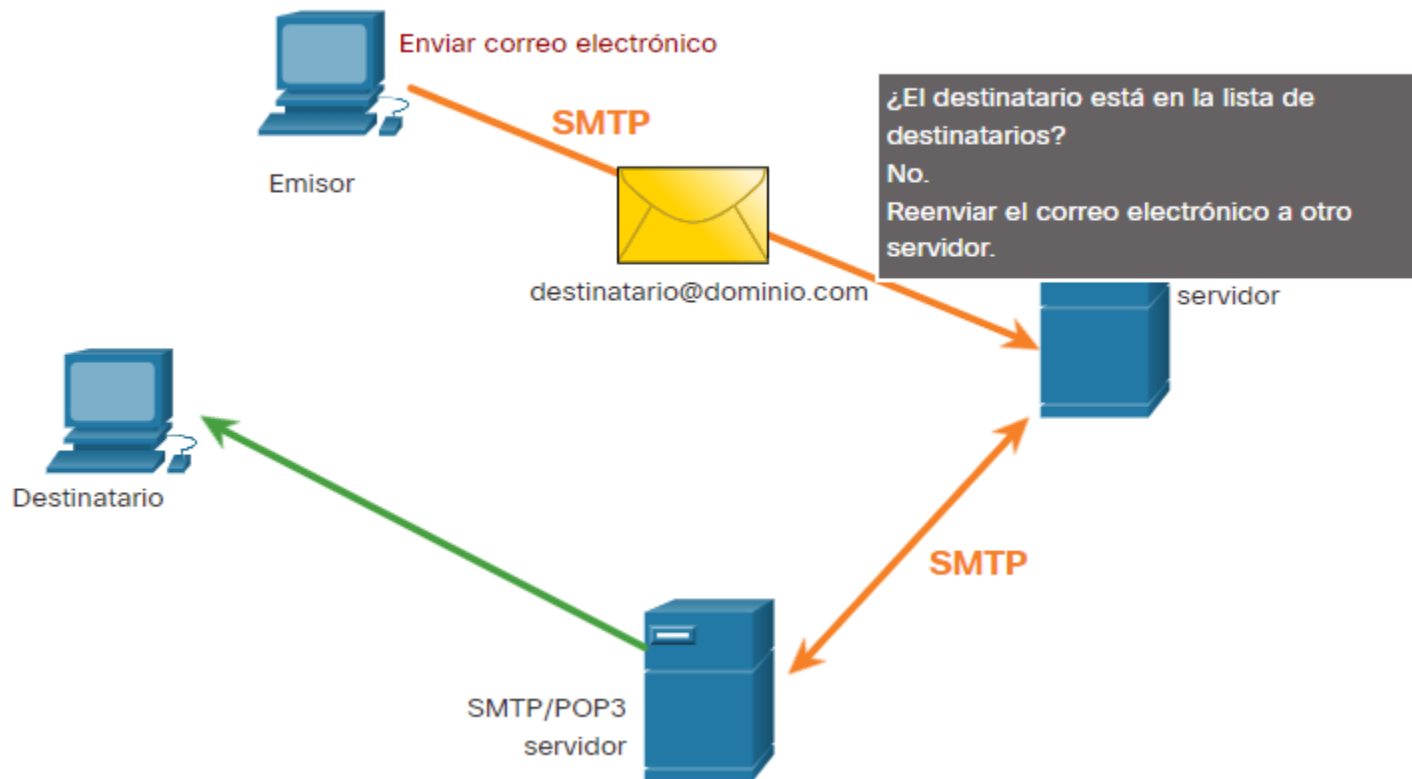


SMTP

- Los formatos de mensajes SMTP necesitan un encabezado y un cuerpo de mensaje. Mientras que el cuerpo del mensaje puede contener la cantidad de texto que se desee, el encabezado debe contar con una dirección de correo electrónico de destinatario correctamente formateada y una dirección de emisor.
- 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.
- 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.



SMTP

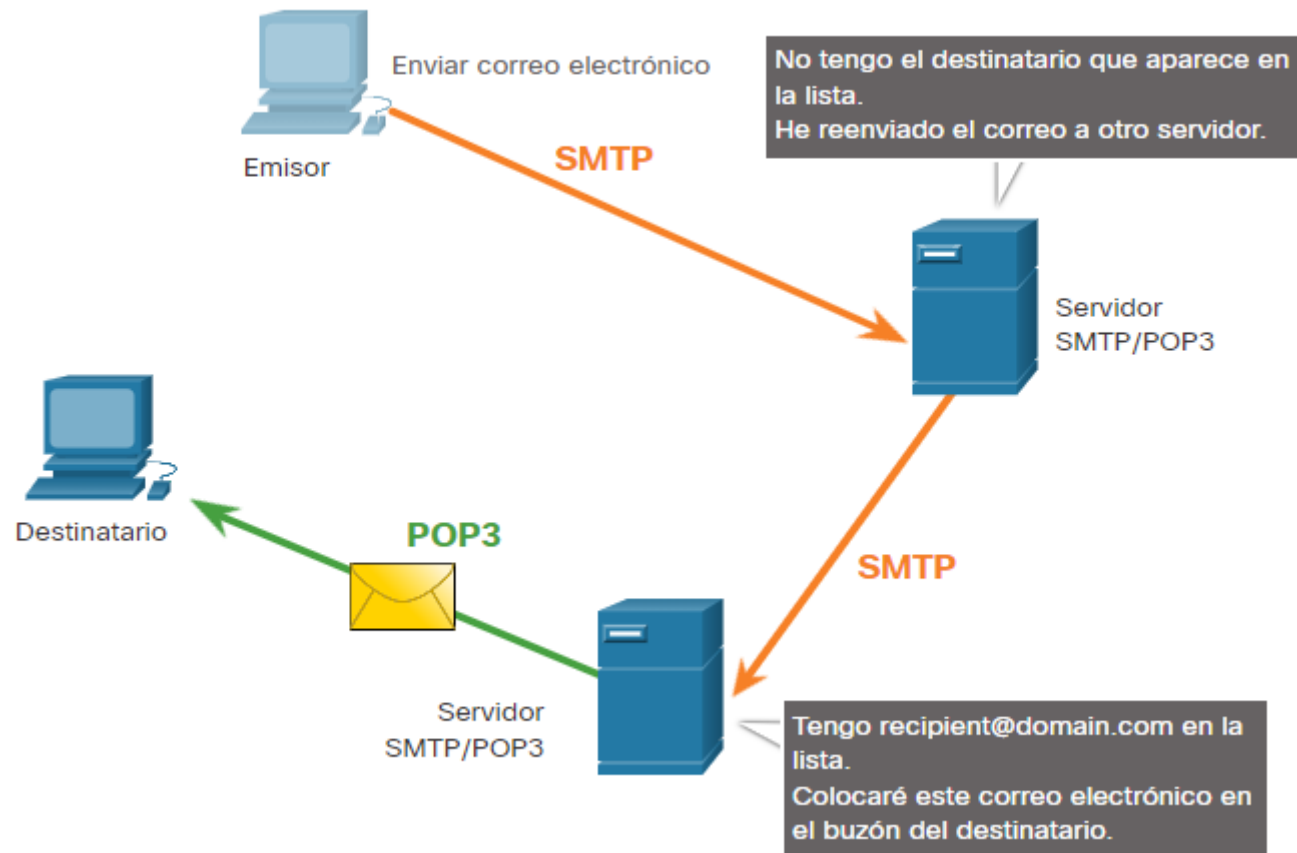


POP

- Es utilizado por una aplicación para recuperar correo electrónico de un servidor de correo.
- Es no orientado a conexión, por tanto utiliza UDP para el transporte
- 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, como se muestra en la figura. 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.



POP

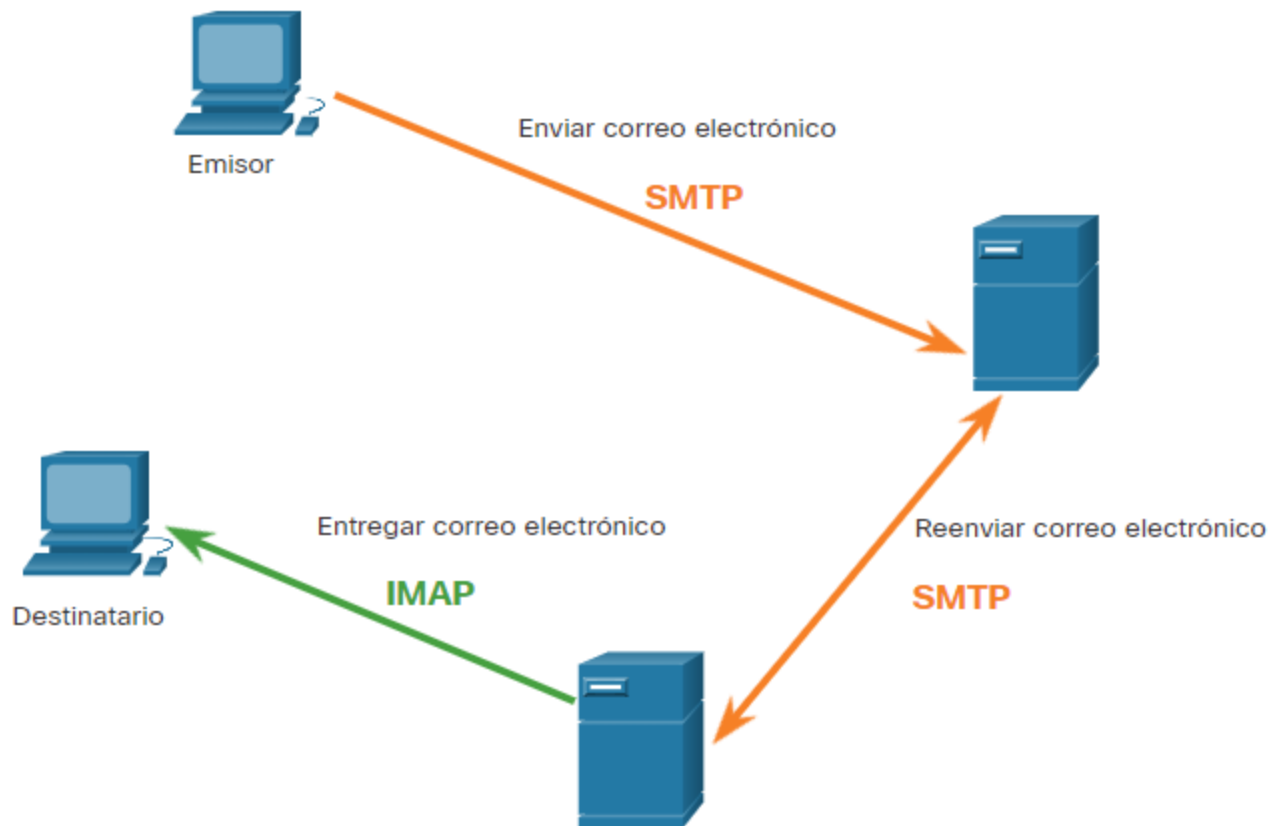


IMAP

- Es utilizado por una aplicación para recuperar correo electrónico de un servidor de correo.
- Es no orientado a conexión, por tanto utiliza UDP para el transporte
- 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. Los mensajes originales se mantienen en el servidor hasta que se eliminan manualmente.
- El almacenamiento de mensajes en el servidor permite su uso desde múltiples dispositivos y de forma simultánea.
- Permite la gestión de carpetas alojadas en el servidor



IMAP



PROTOCOLO DE TRANSFERENCIA DE FICHEROS



FTP

- File Transfer Protocol es un protocolo multiplataforma que sirve para transferir grandes bloques de datos por la red.
- Las páginas web “se suben” al servidor utilizando este protocolo
- Utiliza los puertos 20 y 21
 - Puerto 20: para el flujo de datos entre el cliente y servidor
 - Puerto 21: para el flujo de control
- Los sistemas operativos con soporte TCP/IP suelen conservar una versión primitiva del cliente FTP en línea de comandos

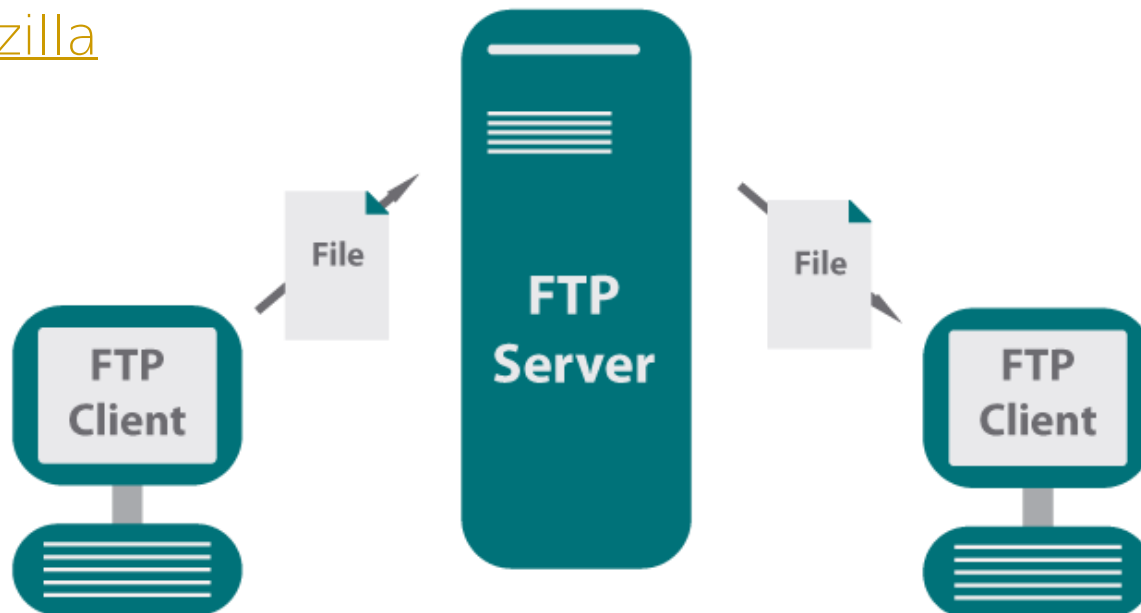
```
Símbolo del sistema - ftp ftp.rediris.es
Microsoft Windows [Versión 10.0.19044.1586]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ftp ftp.rediris.es
Conectado a ftp.rediris.es.
220- Bienvenido al servicio de replicas de RedIRIS.
220- Welcome to the RedIRIS mirror service.
220 Only anonymous FTP is allowed here
200 OK, UTF-8 enabled
Usuario (ftp.rediris.es:(none)):
230- RedIRIS - Red Académica y de Investigación Española
230- RedIRIS - Spanish National Research Network
230- ftp://ftp.rediris.es -- http://ftp.rediris.es
230 Anonymous user logged in
ftp>
```

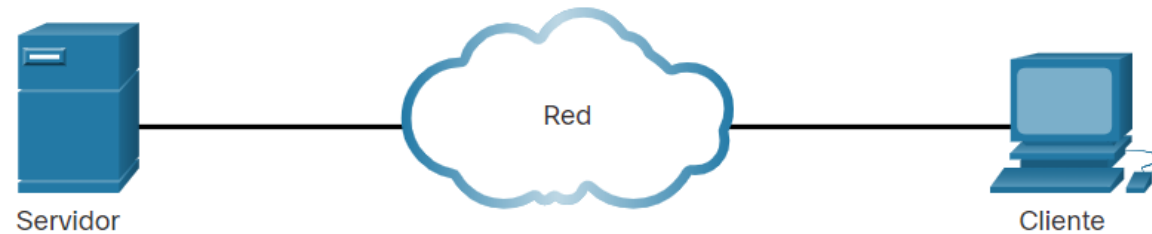


FTP

- Disponemos de distintos programas que podemos usar como clientes FTP.
- 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.
- Ejemplo: [Filezilla](#)



FUNCIONAMIENTO



1. Conexión de control:

El cliente abre la primera conexión al servidor para el tráfico de control.



2. Conexión de datos:

El cliente abre la segunda conexión para el tráfico de datos.



3. Traslamiento de datos:

Servidor transfiere datos al cliente.

- 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.



PROTOCOLO DE RESOLUCIÓN DE NOMBRES DE DOMINIO



INTRODUCCIÓN

- 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.
- Nos referimos principalmente a los servicios de DNS y DHCP. En este apartado trataremos el primero



DNS

- Domain Name System es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP (como Internet o una red privada). Este sistema almacena información sobre los nombres de dominio.
- Las **funciones básicas** son:
 - Conversión de nombres de dominio a direcciones IP
 - La localización de los servidores de correo dentro de cada dominio



QUÉ SON LOS NOMBRES DE DOMINIO

- En las redes, los dispositivos se etiquetan con direcciones IP numéricas para enviar y recibir datos a través de las redes. Los nombres de dominio se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible.
- 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.



CÓMO FUNCIONA

- Las comunicaciones del protocolo DNS utilizan un único formato llamado “mensaje”. Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Paso 1

Paso 2

Paso 3

Paso 4

Paso 5



CÓMO FUNCIONA

- Las comunicaciones del protocolo DNS utilizan un único formato llamado "mensaje". Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Paso 1

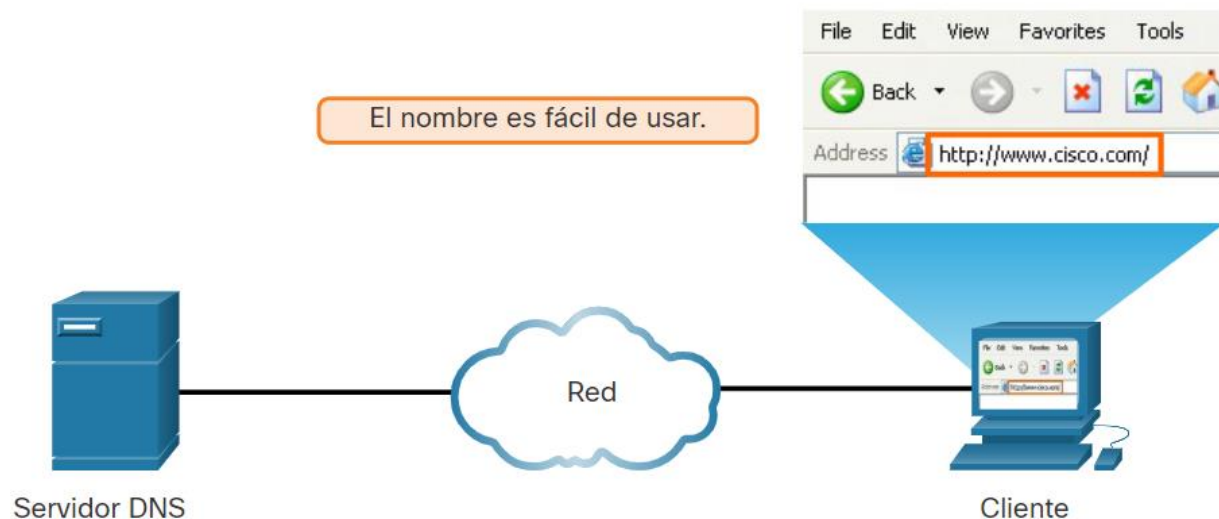
El usuario escribe un FQDN en un campo Dirección de aplicación del explorador.

Paso 2

Paso 3

Paso 4

Paso 5



CÓMO FUNCIONA

- Las comunicaciones del protocolo DNS utilizan un único formato llamado "mensaje". Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Paso 1

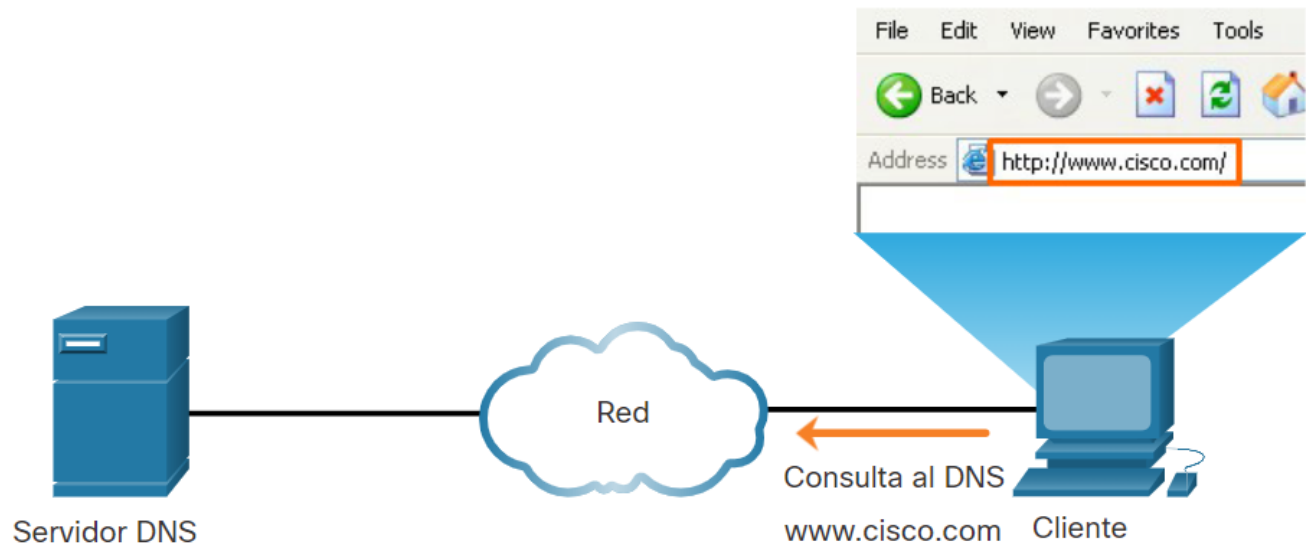
Se envía una consulta DNS al servidor DNS designado para el equipo cliente.

Paso 2

Paso 3

Paso 4

Paso 5



CÓMO FUNCIONA

- Las comunicaciones del protocolo DNS utilizan un único formato llamado "mensaje". Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Paso 1

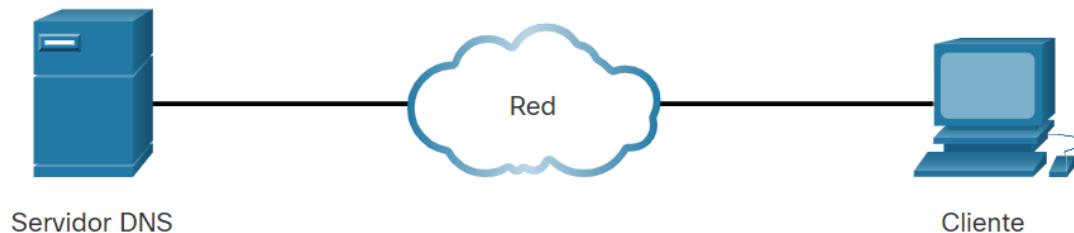
El servidor DNS coincide con el FQDN con su dirección IP.

Paso 2

Paso 3

Paso 4

Paso 5



FQDN	Dirección
www.cisco.com	198.133.219.25

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

Los dispositivos usan números.



CÓMO FUNCIONA

- Las comunicaciones del protocolo DNS utilizan un único formato llamado "mensaje". Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Paso 1

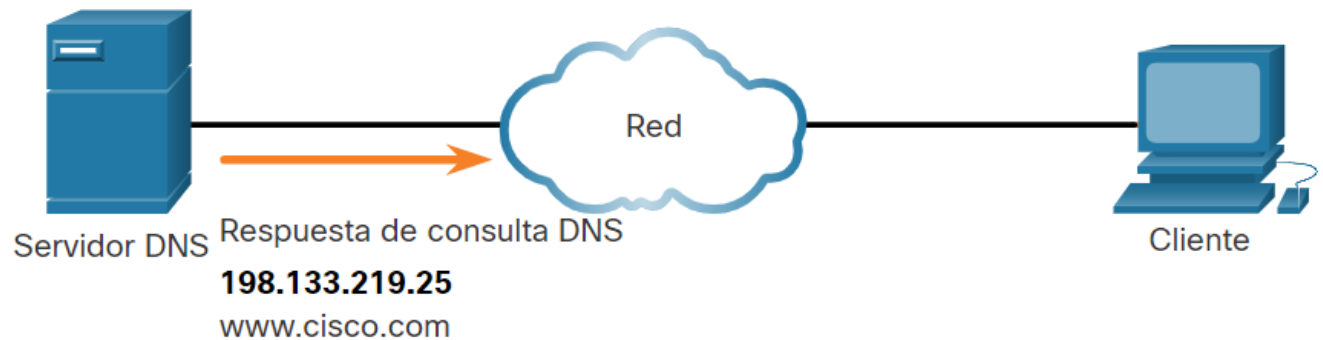
La respuesta de consulta DNS se envía de nuevo al cliente con la dirección IP del FQDN.

Paso 2

Paso 3

Paso 4

Paso 5



CÓMO FUNCIONA

- Las comunicaciones del protocolo DNS utilizan un único formato llamado "mensaje". Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Paso 1

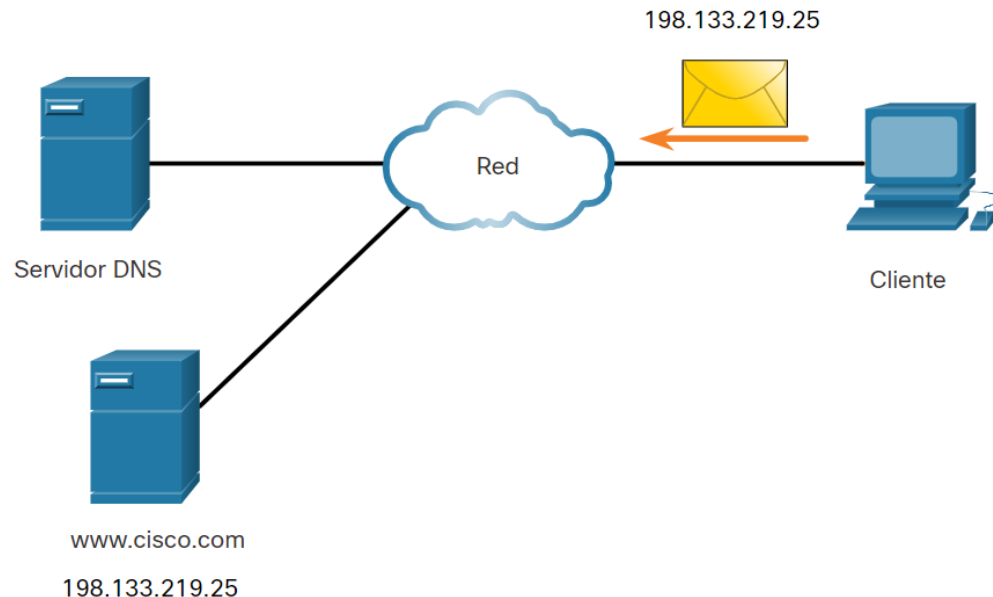
El equipo cliente utiliza la dirección IP para realizar solicitudes del servidor.

Paso 2

Paso 3

Paso 4

Paso 5



SERVIDOR DNS

- El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres.
- Estos registros contienen el nombre, la dirección y el tipo de registro. Algunos de estos **tipos de registros** son los siguientes:
 - **A** - una dirección IPv4 de terminal
 - **NS** - un servidor de nombre autoritativo
 - **AAAA** - una dirección IPv6
 - **MX** - un registro de intercambio de correo



PROCESO DNS

- 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.

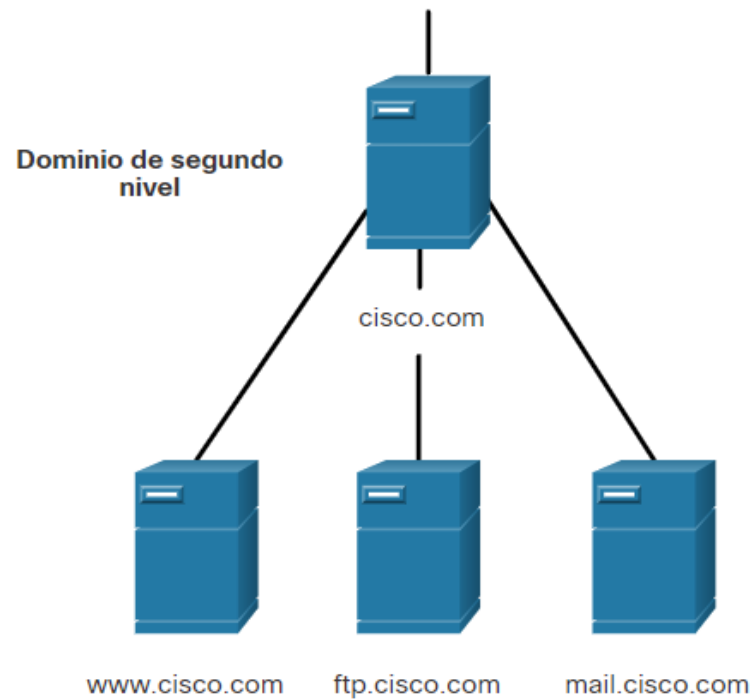
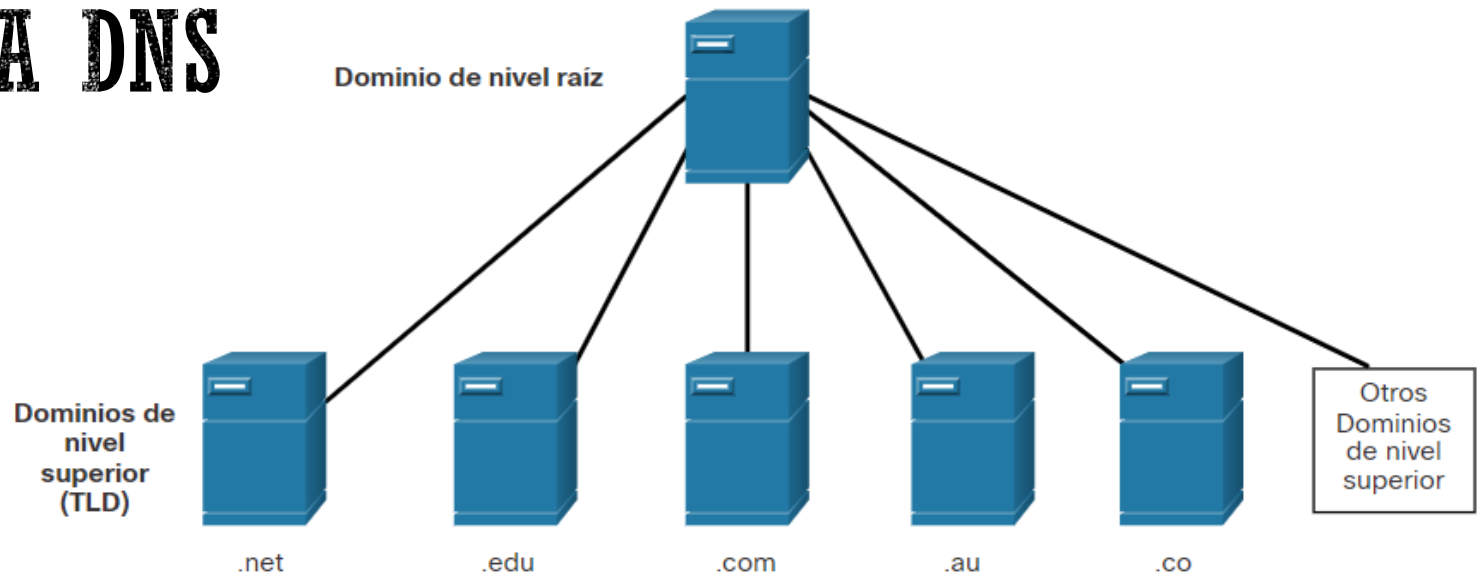


JERARQUÍA DNS

- El protocolo DNS utiliza un sistema jerárquico para crear una base de datos que proporcione la resolución de nombres. DNS utiliza nombres de dominio para formar la jerarquía.
- La estructura de nomenclatura se divide en zonas pequeñas y manejables.
- Cada servidor DNS mantiene un archivo de base de datos específico y sólo es responsable de administrar las asignaciones de nombre a IP para esa pequeña porción de toda la estructura DNS.
- Cuando un servidor DNS recibe una solicitud para una traducción de nombre que no se encuentra dentro de esa zona DNS, el servidor DNS reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para su traducción. DNS es escalable, porque la resolución de los nombres de hosts se distribuye entre varios servidores.
- Los diferentes dominios de primer nivel representan el tipo de organización o el país de origen. Algunos ejemplos de dominios de nivel superior son los siguientes:
 - .com - una empresa o industria
 - .org - una organización sin fines de lucro
 - .au - Australia
 - .co - Colombia



JERARQUÍA DNS



COMANDO 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 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
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
>
```



PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST



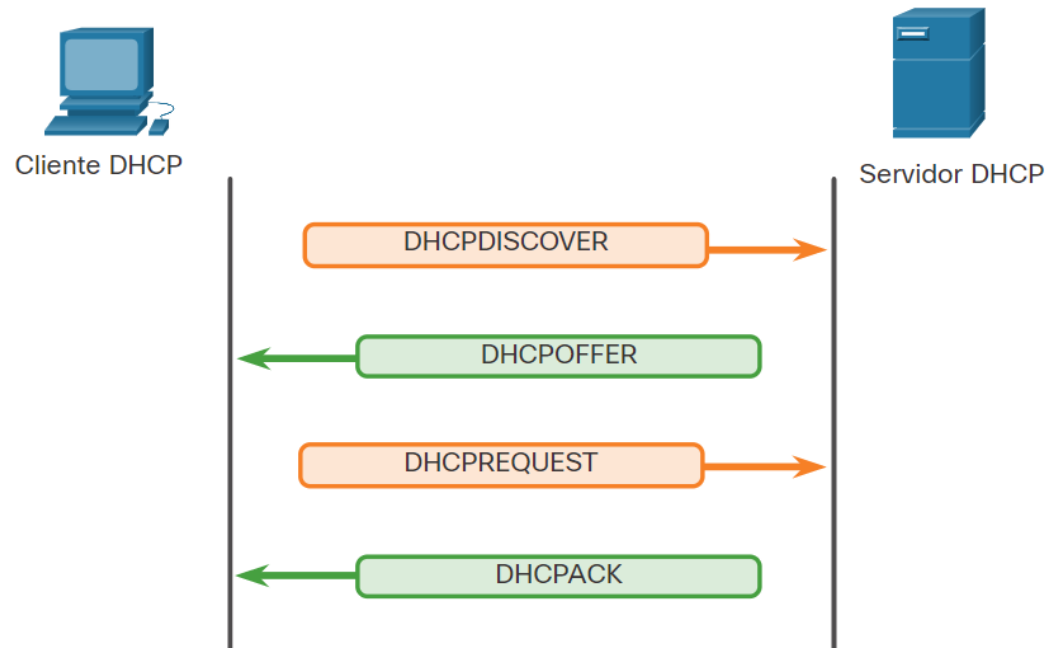
INTRODUCCIÓN

- Dynamic Host Configuration Protocol (DHCP) es un protocolo de la capa de aplicación cuya **función principal es asignar parámetros de la red de forma automática**, evitando que el administrador de la red lo tenga que configurar manualmente.
- Tiene muchas **ventajas**:
 - Ahorro de tiempo al administrador
 - Mejor servicio al usuario porque no depende de intervención externa
 - Permite cambiar un equipo de red sin tener que cambiar su configuración
 - Permite el ahorro de direcciones IP



FUNCIONAMIENTO

- 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.
- El 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



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

MONITORIZACIÓN DE RED



SNMP

- Protocolo simple de administración de red o SNMP (del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.
- Puede monitorizar equipos de diferentes fabricantes, sobre diferentes plataformas y ubicados en redes distintas



CONCEPTOS BÁSICOS

- SNMP se basa en los conceptos de Gestor y Agente
- Gestor: es un equipo que ejecuta un cliente SNMP
- Agente: es un equipo que ejecuta un servidor SNMP, y por tanto, es controlado por el Gestor
- El Gestor solicita información al Agente de forma periódica y además puede ordenar la ejecución de alguna tarea
- El Agente puede advertir al Gestor si se produce alguna situación inusual



BIBLIOGRAFÍA

- ❑ Capítulo 13. Nivel de aplicación
Planificación y Administración de Redes. Editorial Garceta 2ª Edición
- ❑ Módulo 15. Capa de aplicación
Curso CCNA 1 Introduction To Networks v7



NIVEL DE APLICACIÓN

