



# ITSQMET

INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

FORMANDO PROFESIONALES DE ÉLITE



# FUNDAMENTOS DE REDES

## CLASE 12

Ing. ANDRÉS PÉREZ





# INTRODUCCIÓN A LA CLASE

1. Retroalimentación
2. Indicaciones generales
3. Objetivos de la clase



**ITSQMET**  
INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

# RETROALIMENTACIÓN

FORMANDO PROFESIONALES DE ÉLITE



## Objetivos de la clase:

Establecer conceptos básicos sobre la capa de aplicación.



**ITSQMET**  
INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

# CAPA DE APLICACIÓN

FORMANDO PROFESIONALES DE ÉLITE

© 2016 Cisco y/o sus filiales. Todos los derechos reservados.  
Información confidencial de Cisco

Nº





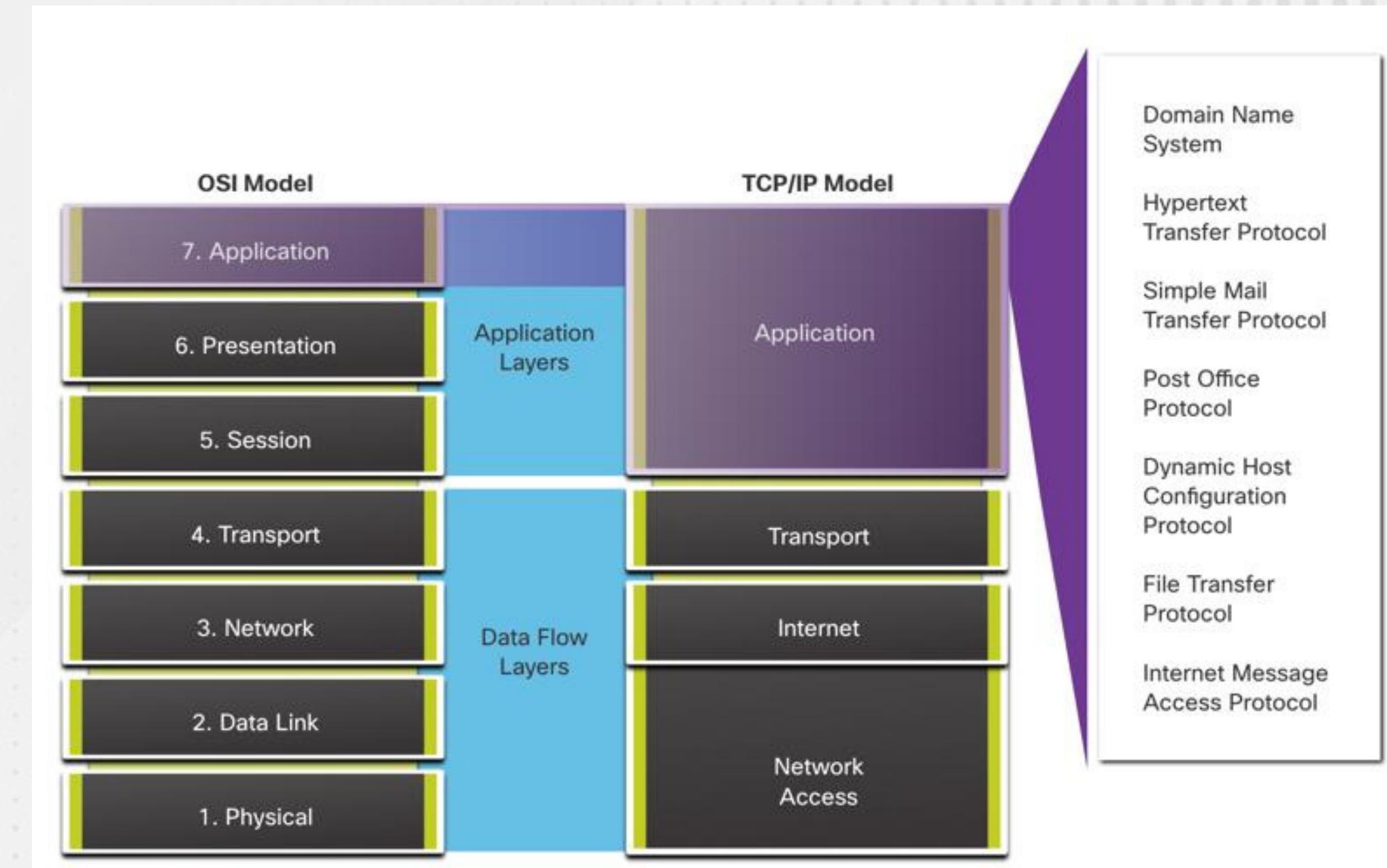
# SOLICITUD, PRESENTACIÓN Y SESIÓN



# Aplicación, presentación y sesión

## Capa de aplicación

- Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) definen funciones de la capa de aplicación TCP / IP.
- La capa de aplicación proporciona la interfaz entre las aplicaciones utilizadas para comunicarse y la red subyacente a través de la cual se transmiten los mensajes.
- Algunos de los protocolos de capa de aplicación más conocidos incluyen HTTP, FTP, TFTP, IMAP y DNS.





# Aplicación, presentación y sesión

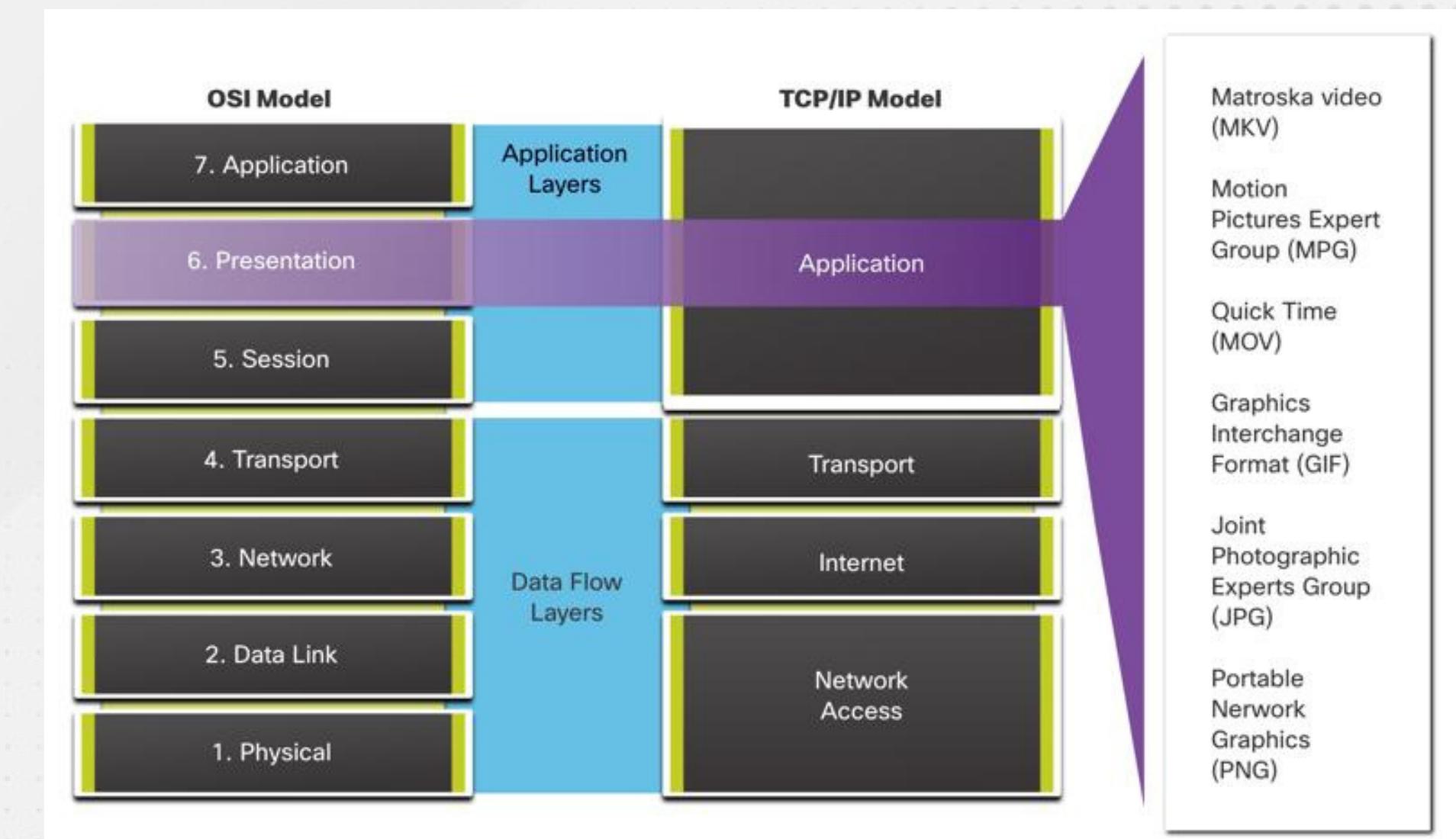
## Capa de presentación y sesión

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 recibirlas.

Función de la capa de sesión:

- Crear y mantener diálogos entre las aplicaciones de origen y de 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.





# Aplicación, presentación y sesión

## Protocolos de capa de aplicación de TCP/IP

- Los protocolos de aplicación TCP/IP especifican el formato y la información de control necesarios para muchas funciones de comunicación comunes de Internet.
- Los protocolos de capa de aplicación son utilizados tanto por los dispositivos de origen como de destino durante una sesión de comunicación.
- Para que las comunicaciones se lleven a cabo correctamente, los protocolos de capa de aplicación que se implementaron en los hosts de origen y de destino deben ser compatibles.

### Sistema de nombres

#### DNS - Sistema de nombres de dominio (o servicio)

- TCP, UDP cliente 53
- Traduce los nombres de dominio tales como cisco.com a direcciones IP

### Configuración de host

#### DHCP (Protocolo de configuración dinámica de host)

- Cliente UDP 68, servidor 67
- Permite que las direcciones vuelvan a utilizarse cuando ya no son necesarias

### Web

#### HTTP- Protocolo de transferencia de hipertexto

- TCP 80, 8080
- Un Conjunto de reglas para intercambiar texto, imágenes gráficas, sonido, video y otros archivos multimedia en la World Wide Web.



**ITSQMET**

INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

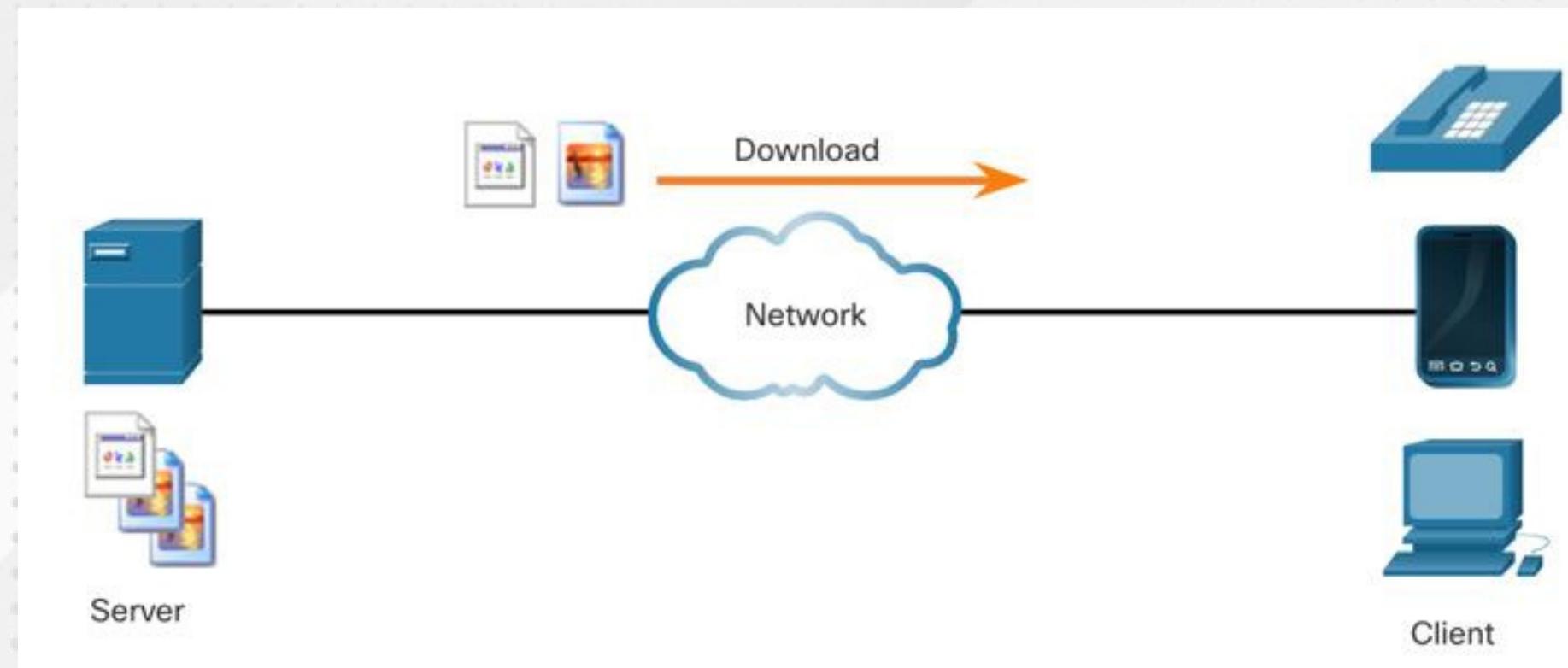
# DE PUNTO A PUNTO

FORMANDO PROFESIONALES DE ÉLITE



# De Punto a Punto Modelo cliente-servidor

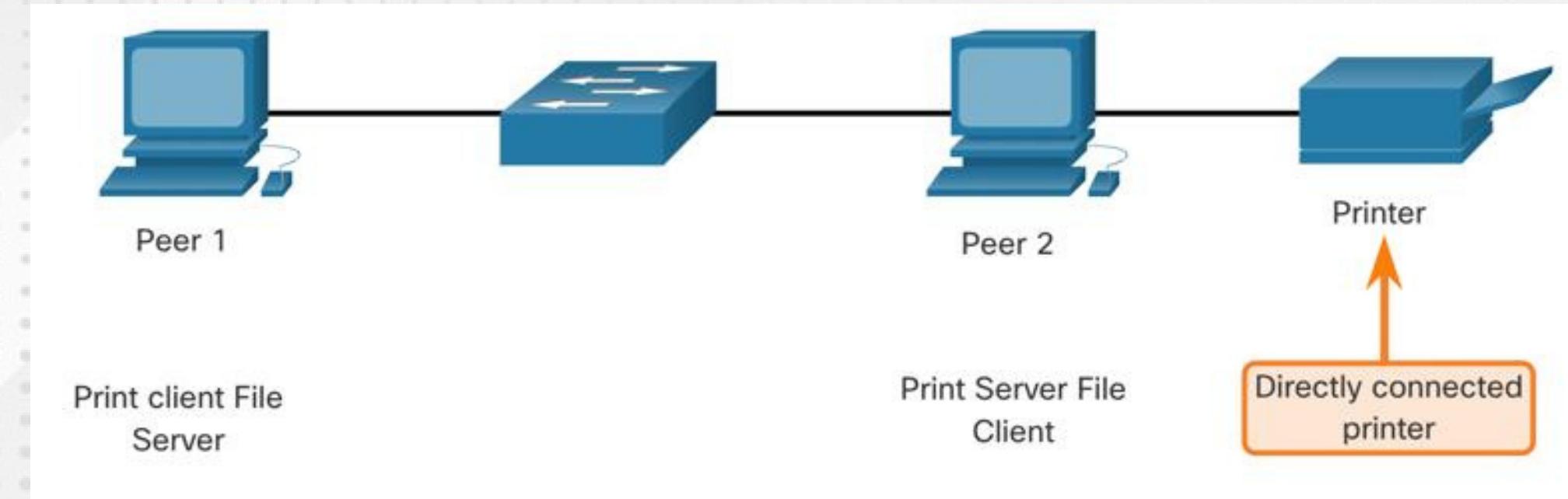
- Los procesos de cliente y servidor se consideran parte de la capa de aplicación.
- En el modelo cliente-servidor, el dispositivo que solicita información se denomina “cliente”, y el dispositivo que responde a la solicitud se denomina “servidor”.
- Los protocolos de la capa de aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores.





# De Punto a Punto Redes Punto a Punto

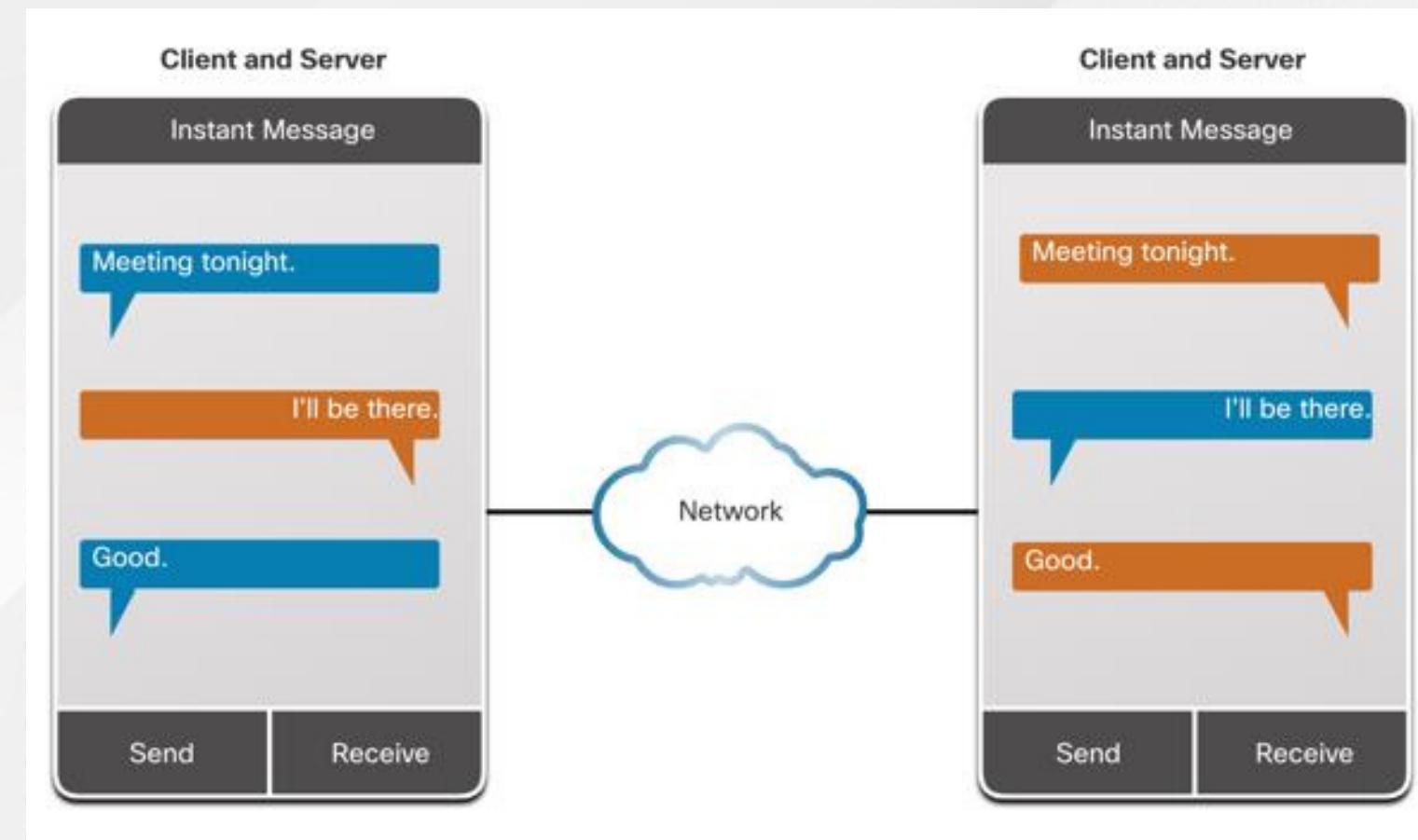
- En una red P2P, hay dos o más PC que están conectadas por medio de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor dedicado.
- Todo terminal conectado puede funcionar como servidor y como cliente.
- Un equipo puede asumir la función de servidor para una transacción mientras funciona en forma simultánea como cliente para otra transacción. Las funciones de cliente y servidor se establecen por solicitud.





# De Punto a Punto Aplicaciones punto a punto

- Una aplicación P2P permite que un dispositivo funcione como cliente y como servidor dentro de la misma comunicación.
- Algunas aplicaciones P2P utilizan un sistema híbrido en el que cada par accede a un servidor de índice para obtener la ubicación de un recurso almacenado en otro par.



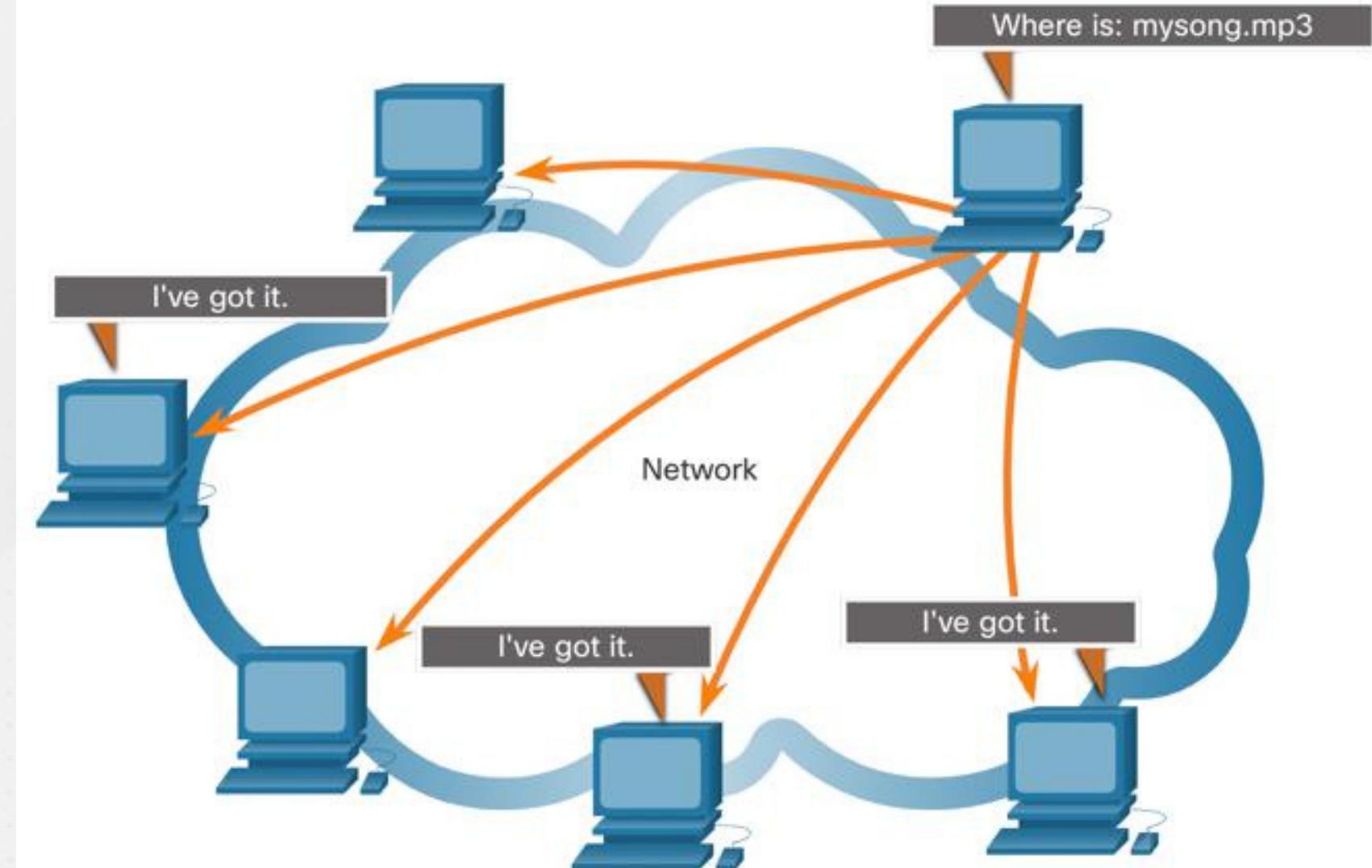


## Aplicaciones P2P comunes punto a punto

Con las aplicaciones P2P, cada PC de la red que ejecuta la aplicación puede funcionar como cliente o como servidor para las otras PC en la red que ejecutan la aplicación.

Las redes P2P comunes incluyen las siguientes:

- BitTorrent
- Conexión directa
- eDonkey
- Freenet





**ITSQMET**  
INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

# PROTOCOLOS WEB Y DE CORREO ELECTRÓNICO

FORMANDO PROFESIONALES DE ÉLITE



# Protocolos web y de correo electrónico

## Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto

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.  
Para comprender mejor cómo interactúa el navegador web con el servidor web, podemos analizar cómo se abre una página web en un navegador.

### Paso 1

El explorador interpreta las tres partes del URL:

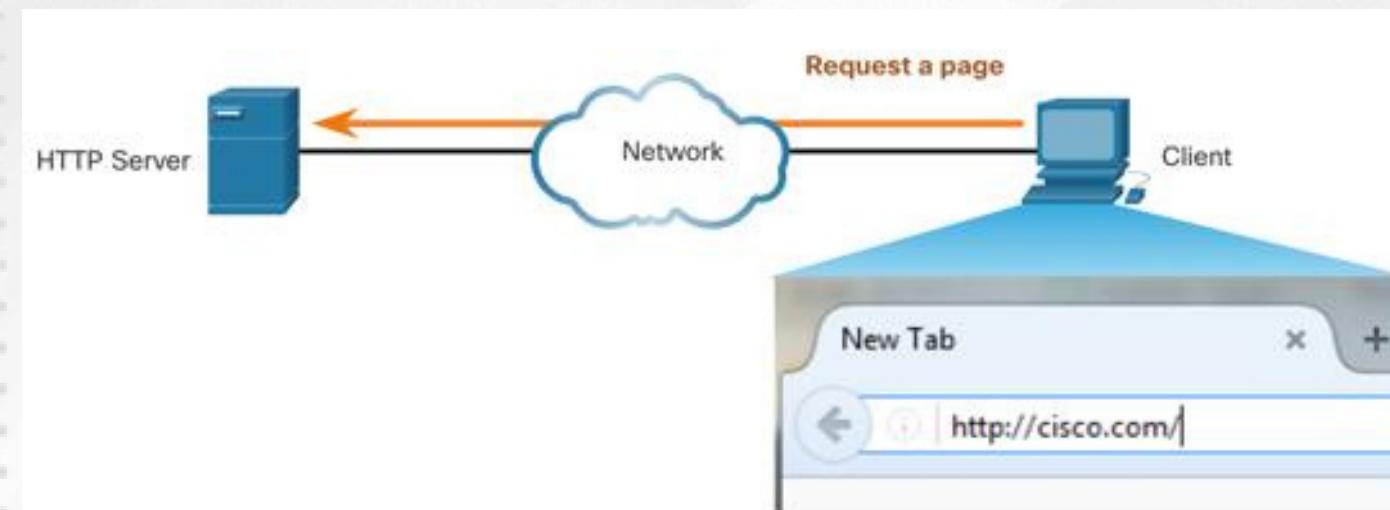
- http (el protocolo o esquema)
- www.cisco.com (el nombre del servidor)
- index.html (el nombre de archivo específico solicitado)



## Paso 2

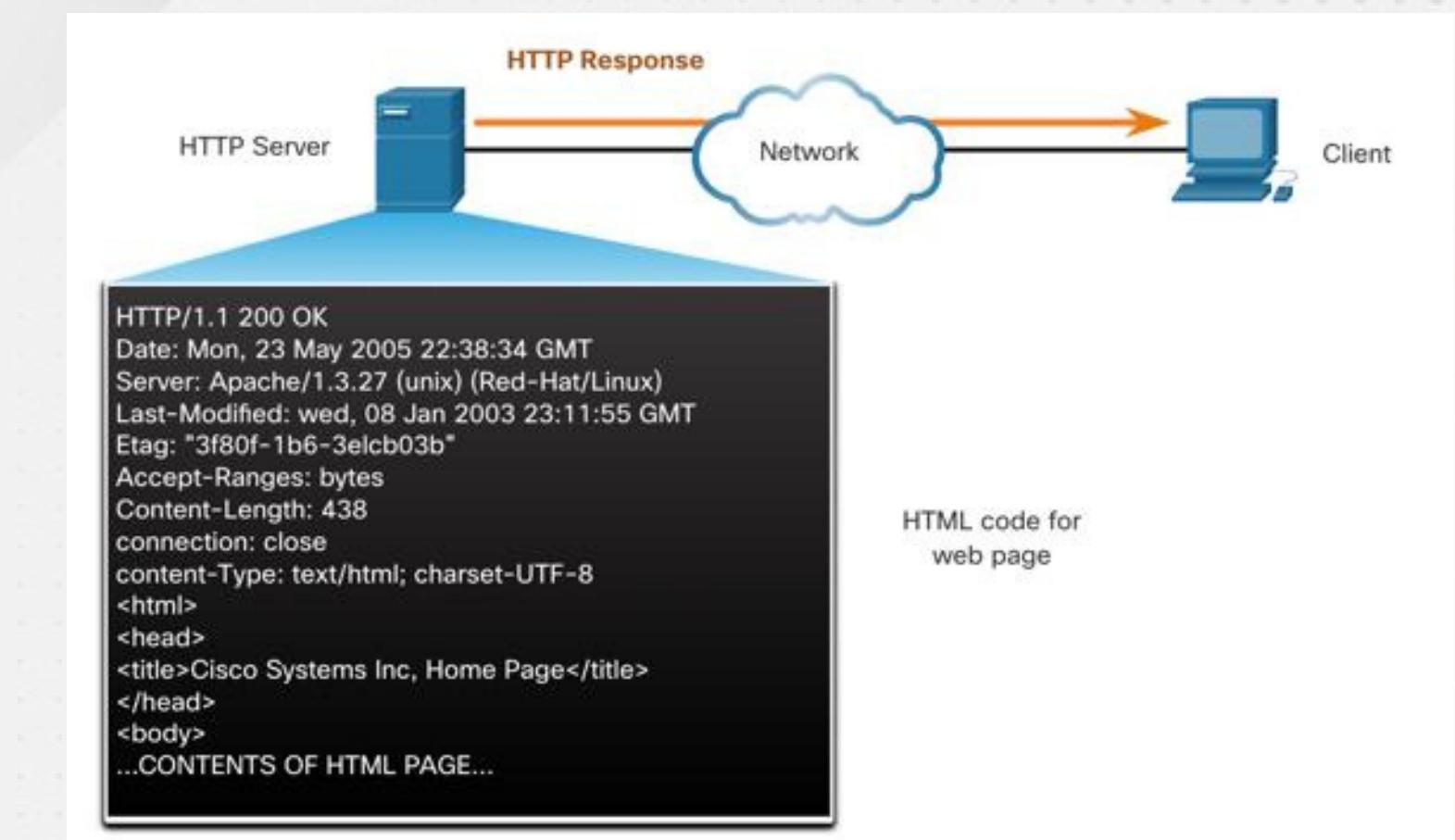
El navegador luego verifica con un Servidor de nombres de dominio (DNS) para convertir a [www.cisco.com](http://www.cisco.com) en una dirección numérica que utiliza para conectarse con el servidor.

El cliente inicia una solicitud HTTP a un servidor enviando una solicitud GET al servidor y solicita el archivo index.html.



## Paso 3

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



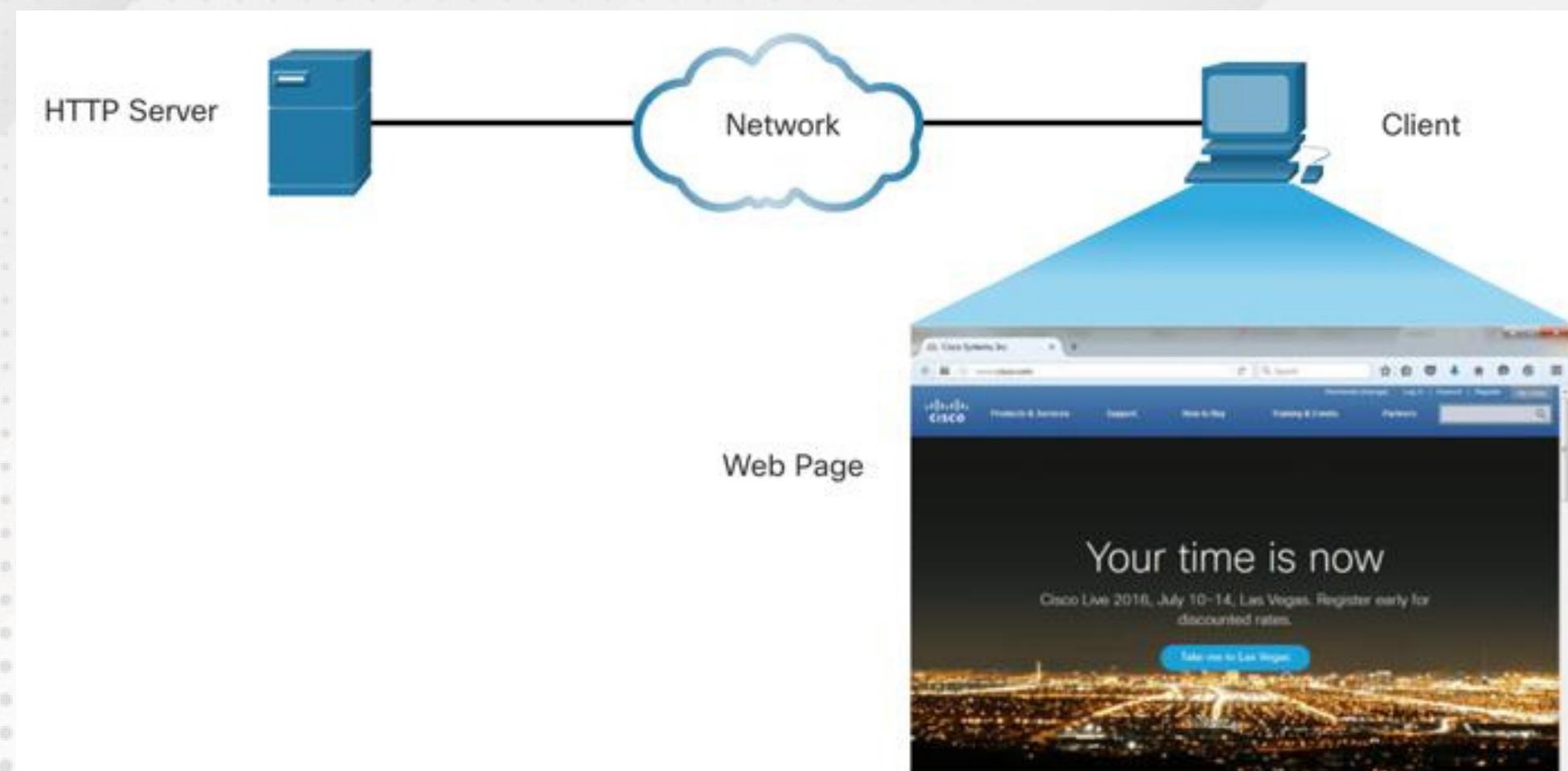


# Protocolos web y de correo electrónico

## Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto

### Paso 4

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



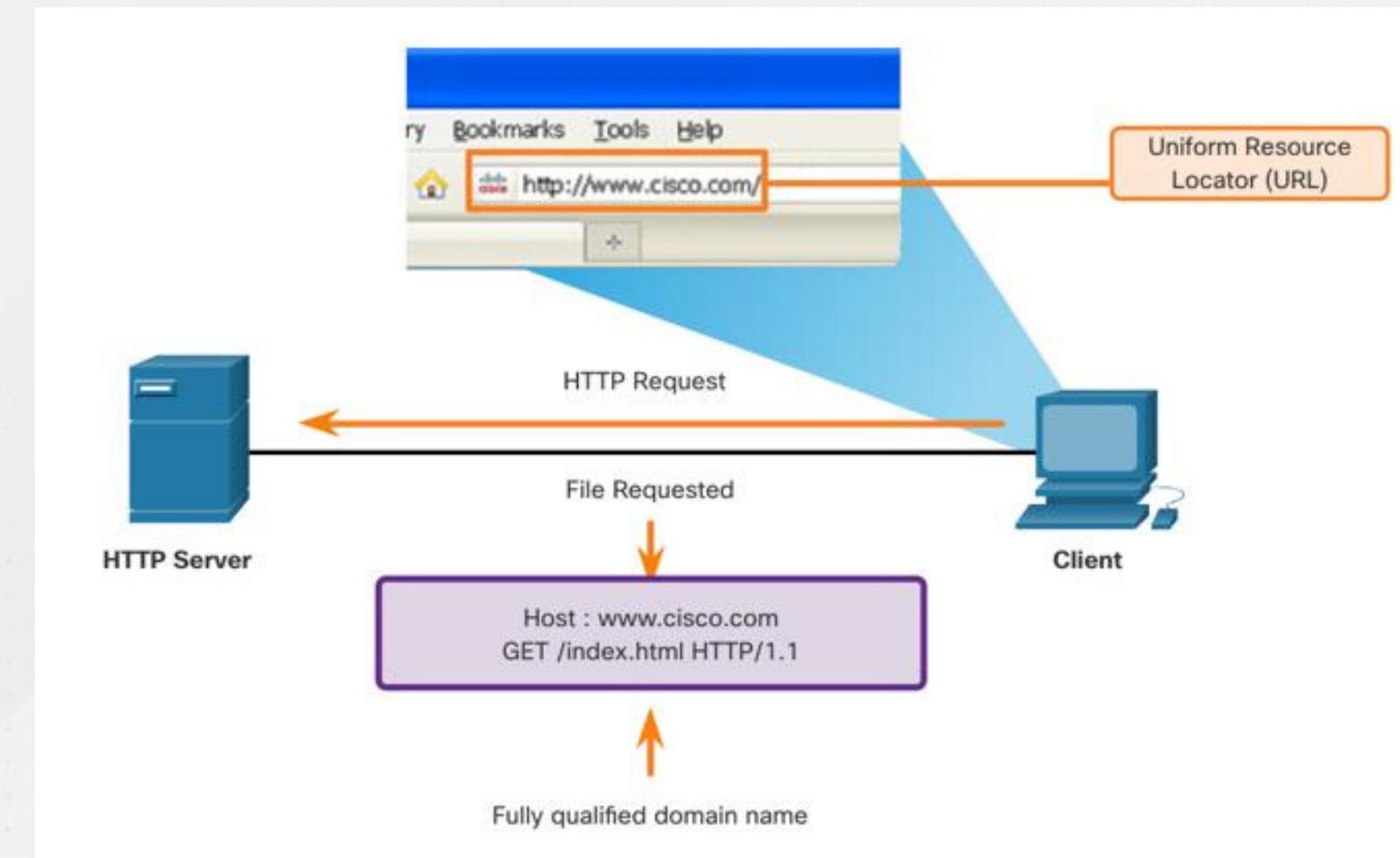


HTTP es un protocolo de solicitud/respuesta que especifica los tipos de mensajes utilizados para esa comunicación.

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.

# Protocolos web y de correo electrónico HTTP y HTTPS



**Nota:** HTTP no es un protocolo seguro. Para comunicaciones seguras enviadas a través de Internet, se debe utilizar HTTPS.



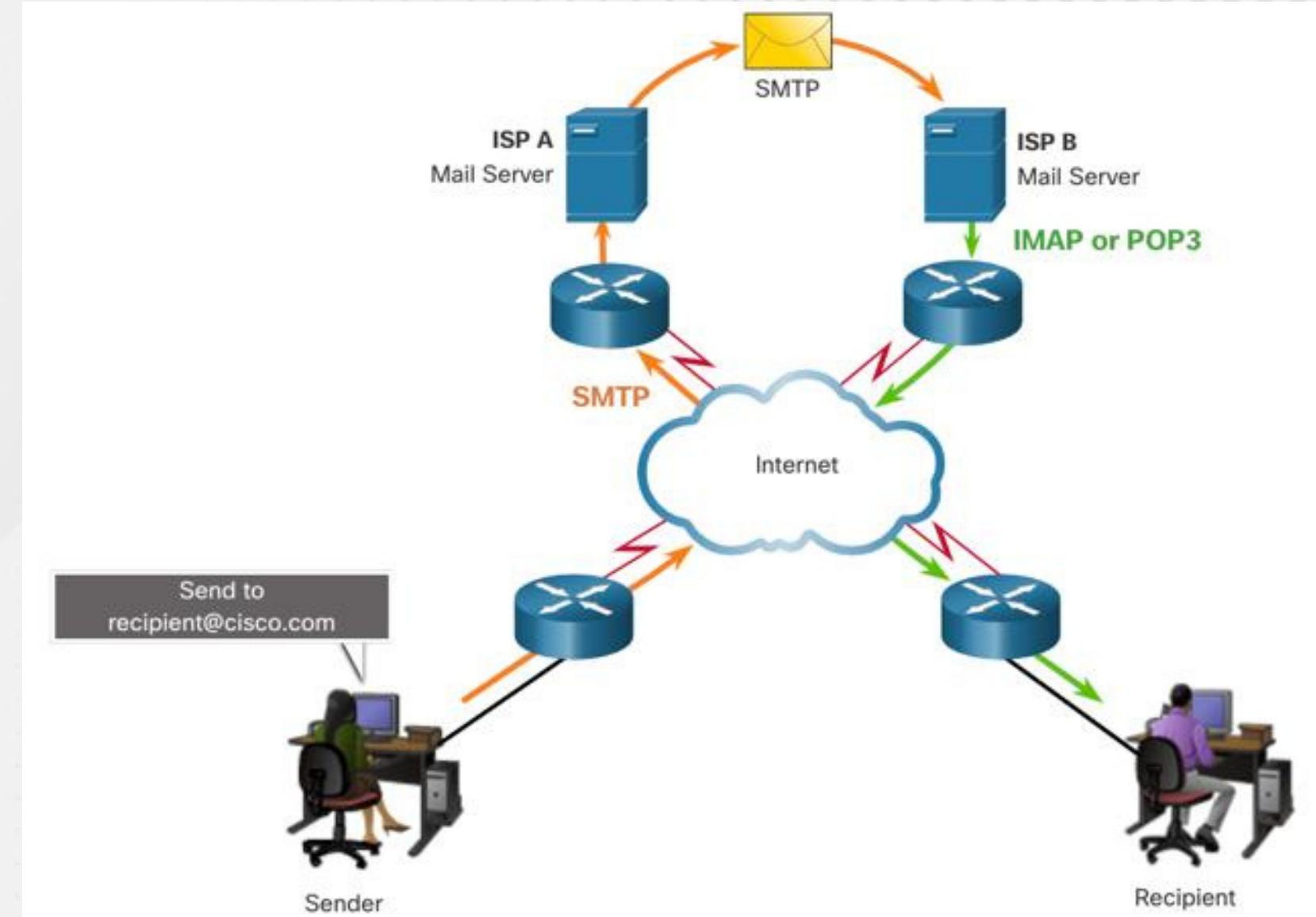
# Protocolos web y de correo electrónico

## Protocolos de correo electrónico

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. Los clientes de correo electrónico se comunican con servidores de correo para enviar y recibir correo electrónico.

Los protocolos de correo electrónico utilizados para la operación son:

- Protocolo simple de transferencia de correo (SMTP) para enviar correo electrónico.
- Protocolo de oficina de correos (POP) e IMAP: se utiliza para que los clientes reciban correo.

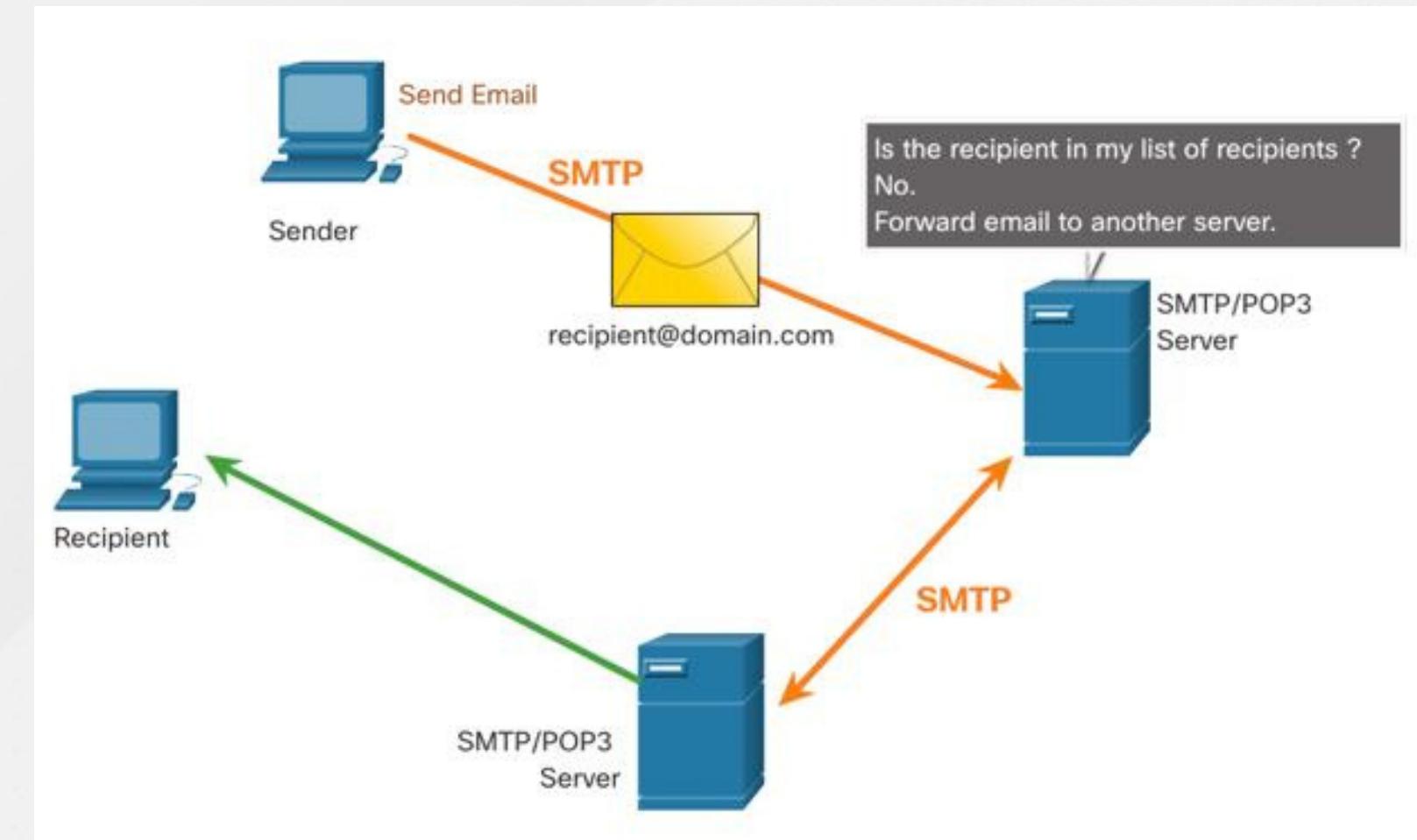




# Protocolos Web y Correo Electrónico SMTP, POP e IMAP

• 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.

- Despues 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 puede estar ocupado. Si es así, SMTP pone en cola los mensajes que se enviarán más adelante.



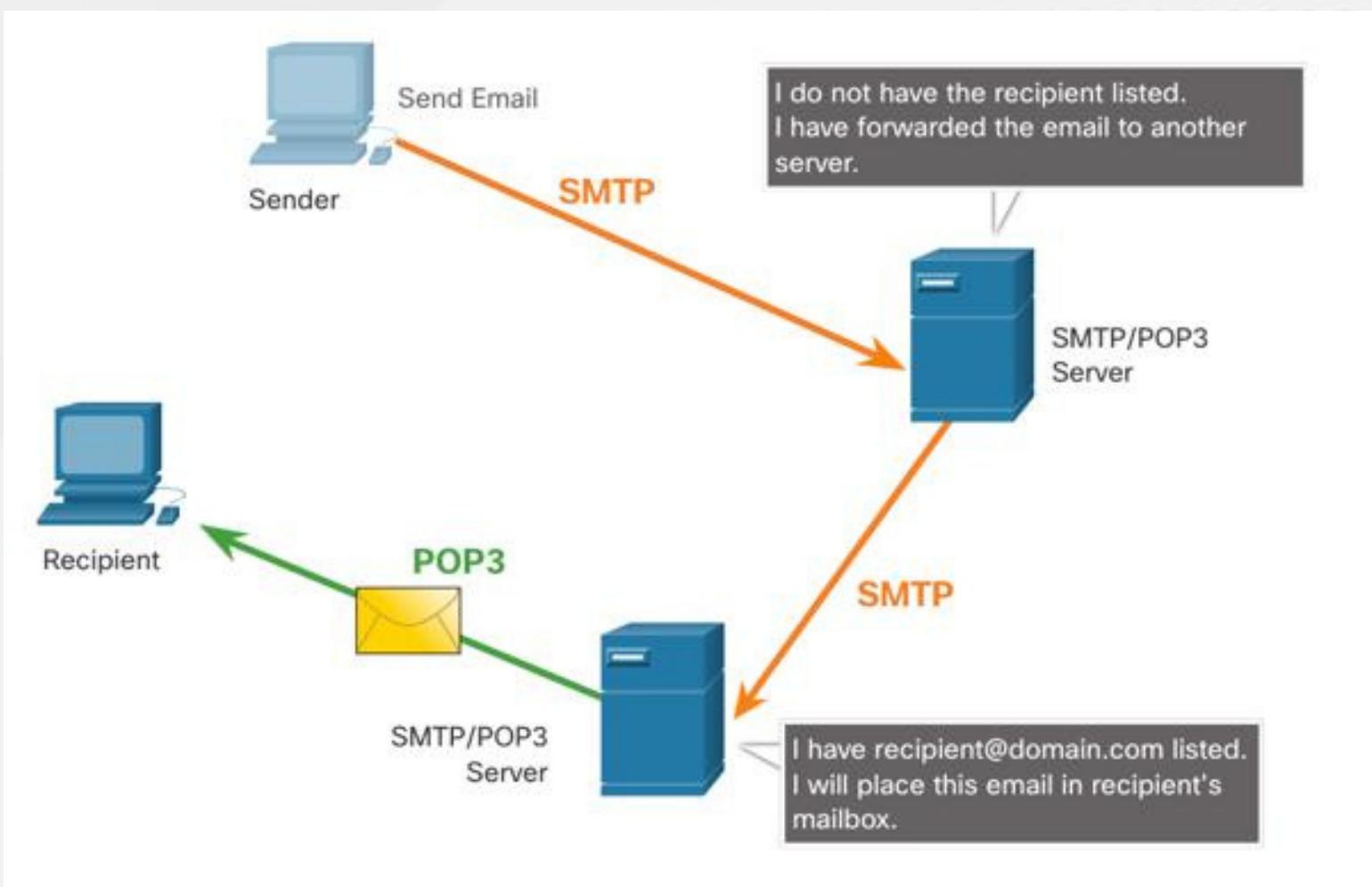
**Nota:** Los formatos de mensaje SMTP requieren un encabezado del mensaje (dirección de correo electrónico del destinatario y dirección de correo electrónico del remitente) y un cuerpo del mensaje.



# Protocolos Web y Correo Electrónico SMTP, POP e IMAP (Cont.)

POP es utilizado por una aplicación para recuperar correo electrónico de un servidor de correo. Cuando el correo se descarga del servidor al cliente mediante POP, los mensajes se eliminan en el servidor.

- 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.



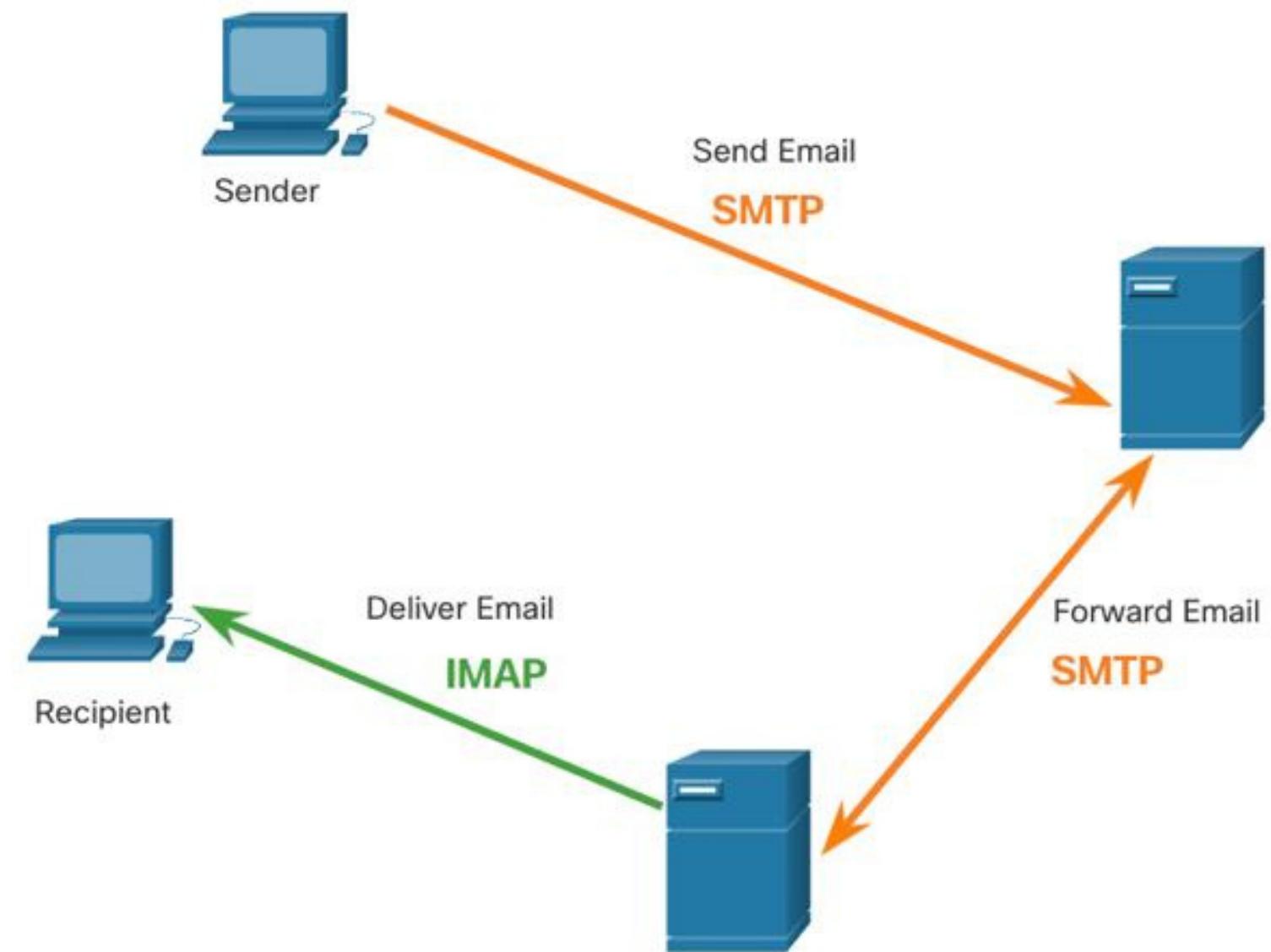
Nota: Dado que POP no almacena mensajes, no se recomienda para las pequeñas empresas que necesitan una solución de respaldo centralizada.



# Protocolos web y de correo electrónico SMTP, POP e IMAP (Cont.)

IMAP es otro protocolo que describe un método para recuperar mensajes de correo electrónico.

- A diferencia de POP, cuando un usuario se conecta a un servidor IMAP, se descargan copias de los mensajes a la aplicación cliente. Los mensajes originales se mantienen en el servidor hasta que se eliminan manualmente.
- Cuando un usuario decide eliminar un mensaje, el servidor sincroniza esa acción y elimina el mensaje del servidor.



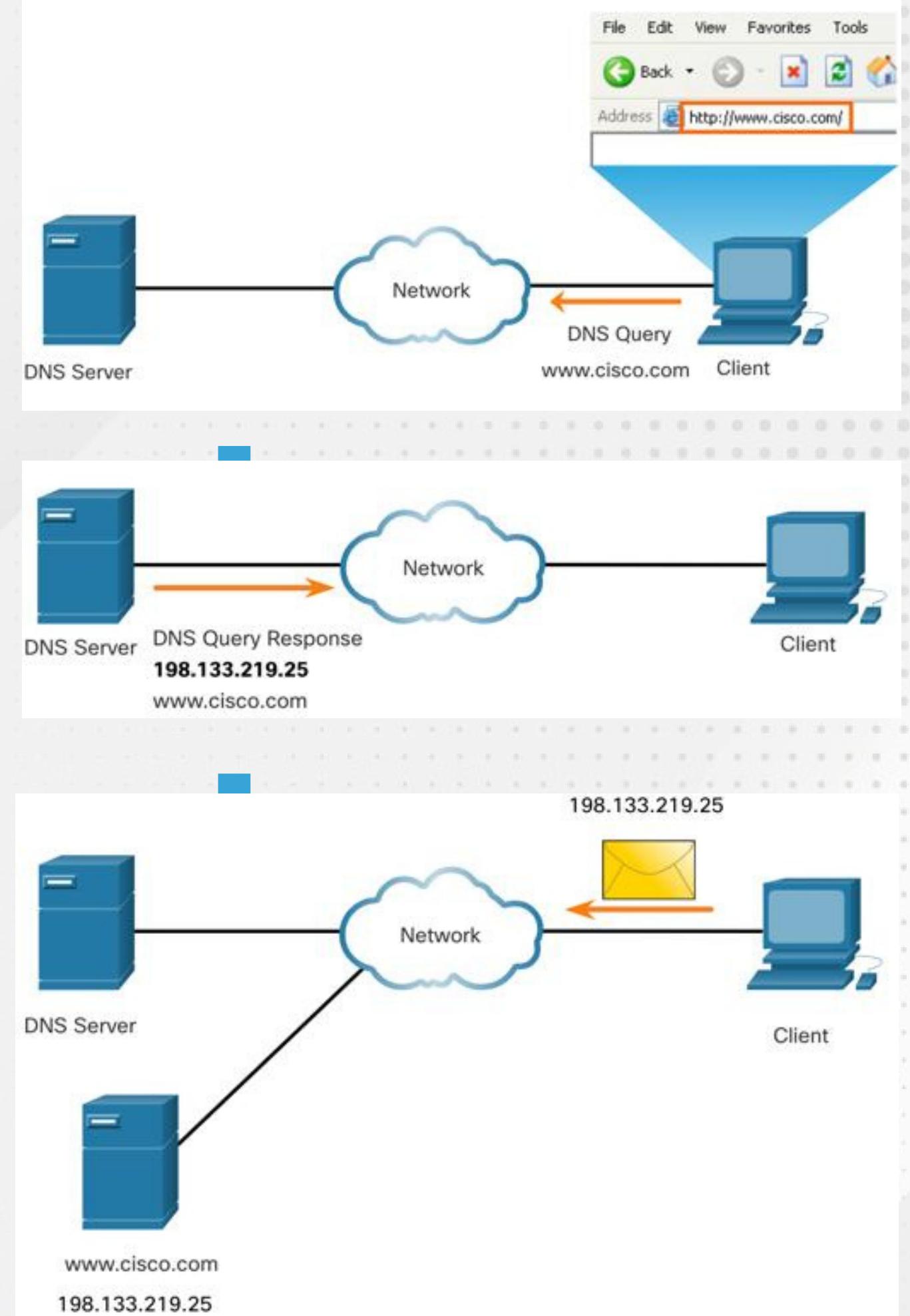


# SERVICIOS DE DIRECCIONAMIENTO IP



## Servicios de direccionamiento IP Servicio de nombres de dominio

- Los nombres de dominio se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible.
- Los nombres de dominio completos (FQDN), como <http://www.cisco.com>, son mucho más fáciles de recordar para las personas que 198.133.219.25.
- 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.





# Servicios de direccionamiento IP

## Formato del mensaje 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 de terminal
- MX: un registro de intercambio de correo

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.



# Servicios de direccionamiento IP

## Formato del mensaje DNS

Este formato de mensaje que se ve en la figura se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, para los mensajes de error y para la transferencia de información de registro de recursos entre servidores.

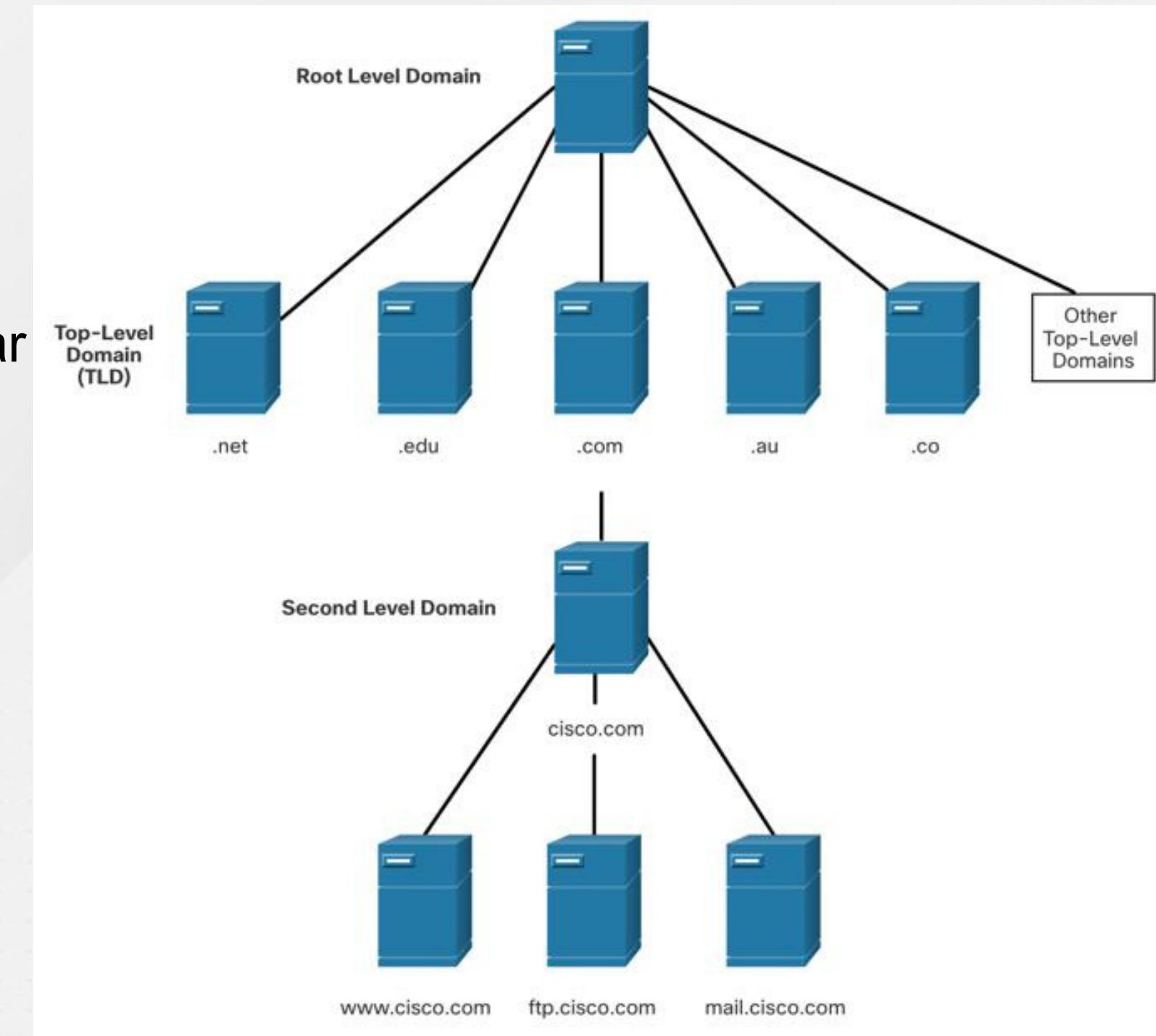
Sección de mensajes DNS	Descripción
Pregunta	La pregunta para el servidor de nombres
Respuesta	Registros de recursos que responden la pregunta
Autoridad	Registros de recursos que apuntan a una autoridad
Adicional	Registros de recursos que poseen información adicional



# Servicios de direccionamiento IP

## Jerarquía DNS

- El protocolo DNS utiliza un sistema jerárquico para crear una base de datos que proporcione la resolución de nombres.
- 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.
- Algunos ejemplos de dominios de nivel superior son los siguientes:
  - **.com**: una empresa o industria
  - **.org**: una organización sin fines de lucro
  - **.au** Australia





# Servicios de direccionamiento IP

## El comando nslookup

- Nslookup es una utilidad del sistema operativo de la computadora que permite al usuario consultar manualmente los servidores DNS configurados en el dispositivo 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.
- En la figura 1, cuando se ejecuta el comando **nslookup**, se muestra el servidor DNS predeterminado configurado para su host.
- El nombre de un host o de un dominio se puede introducir en el símbolo del sistema de **nslookup**.

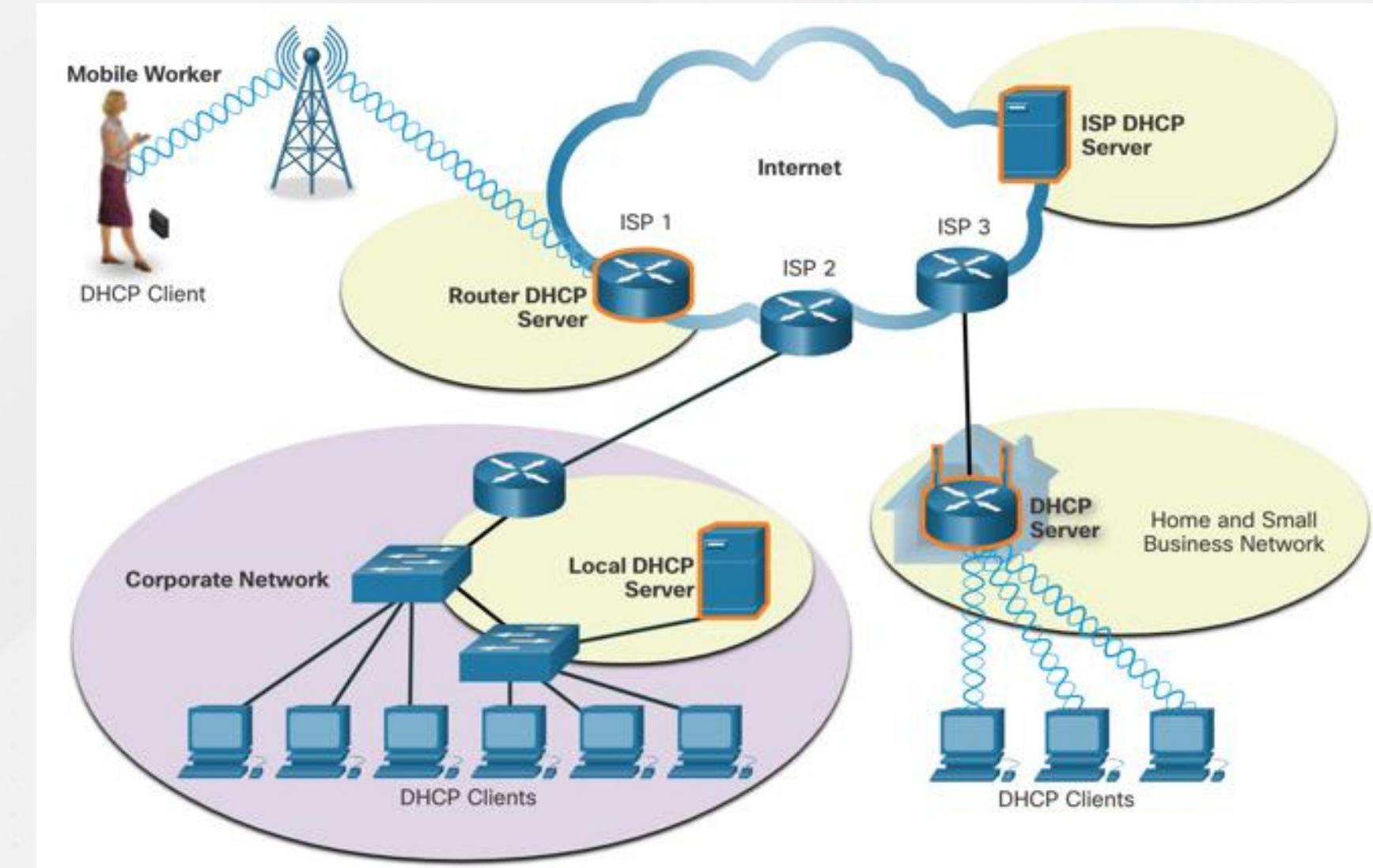
```
C:\Users> nslookup
Default Server: dns-sj.cisco.com
Address: 171.70.168.183
> www.cisco.com
Server: dns-sj.cisco.com
Address: 171.70.168.183
Name: origin-www.cisco.com
Addresses: 2001:420:1101:1::a
173.37.145.84
Aliases: www.cisco.com
> cisco.netacad.net
Server: dns-sj.cisco.com
Address: 171.70.168.183
Name: cisco.netacad.net
Address: 72.163.6.223
>
```



# Servicios de direccionamiento IP

## 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.
- DHCP se considera direccionamiento dinámico en comparación con direccionamiento estático. El direccionamiento estático está introduciendo manualmente la información de la dirección IP.
- 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.
- 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.



**Nota:** DHCPv6 (DHCP para IPv6) proporciona servicios similares para los clientes IPv6. Sin embargo, DHCPv6 no proporciona una dirección de puerta de enlace predeterminada. Esto sólo se puede obtener de forma dinámica a partir del anuncio de router del propio router.

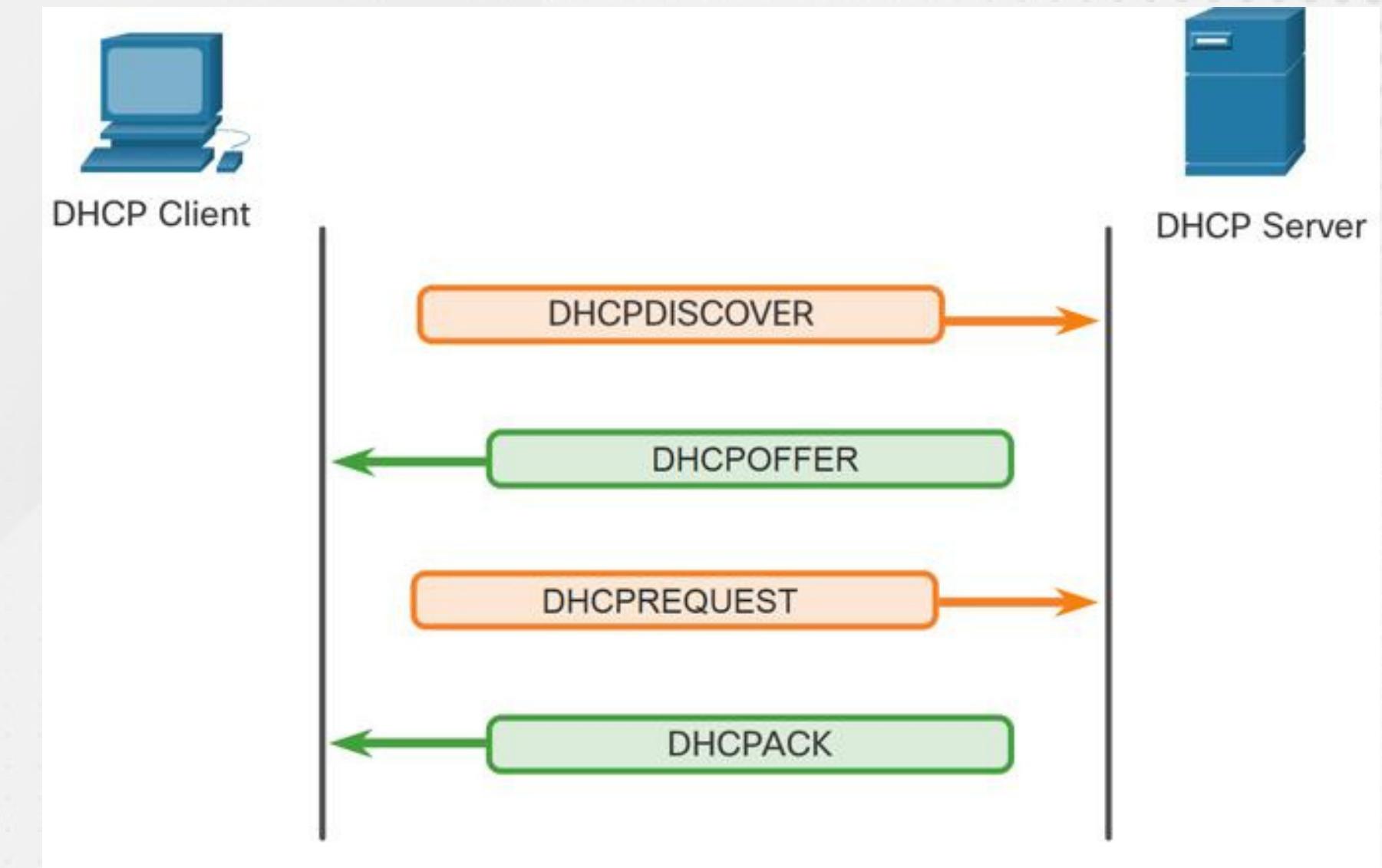


# Servicios de direccionamiento IP

## Funcionamiento de DHCP

### Proceso 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.
- Un servidor de DHCP responde con un mensaje de oferta de DHCP (DHCPOFFER), que ofrece una concesión al cliente.(Si un cliente recibe más de una oferta debido a varios servidores DHCP en la red, debe elegir una.)
- 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.
- A continuación, el servidor devuelve un mensaje de confirmación DHCP (DHCPACK) que reconoce al cliente que se ha finalizado la concesión.
- Si la oferta ya no es válida, el servidor seleccionado responde con un mensaje de reconocimiento negativo de DHCP (DHCPNAK) y el proceso debe comenzar con un nuevo mensaje de DHCPDISCOVER.



**Nota:** DHCPv6 tiene un conjunto de mensajes similares a los de DHCPv4. Los mensajes de DHCPv6 son SOLICIT, ADVERTISE, INFORMATION REQUEST y REPLY.



# DISPOSITIVOS DE UNA RED PEQUEÑA



# Dispositivos de una red pequeña Topologías de redes pequeñas

- La mayoría de las empresas son pequeñas, la mayoría de las redes comerciales también son pequeñas.
- Un diseño de red pequeño suele ser simple.
- Las redes pequeñas suelen tener una única conexión WAN proporcionada por DSL, cable o una conexión Ethernet.
- Las redes grandes requieren un departamento de TI para mantener, proteger y solucionar problemas de dispositivos de red y proteger los datos de la organización. Las redes pequeñas son administradas por un técnico local de TI o por un profesional contratado.



# Dispositivos de una red pequeña Selección de dispositivos para redes pequeñas

Al igual que las redes grandes, las redes pequeñas requieren planificación y diseño para cumplir con los requisitos del usuario. La planificación asegura que se consideren debidamente todos los requisitos, factores de costo y opciones de implementación. Una de las primeras consideraciones de diseño es el tipo de dispositivos intermedios que se utilizarán para admitir la red.

Los factores que deben tenerse en cuenta al seleccionar dispositivos de red incluyen:

- Costo
- Velocidad y tipos de puertos e interfaces
- Capacidad de expansión
- Características y servicios de los sistemas operativos



# Dispositivos de una red pequeña Asignación de direcciones IP para redes pequeñas

Al implementar una red, cree un esquema de direccionamiento IP y úselo. Todos los hosts y dispositivos dentro de una red interna deben tener una dirección única. Entre los dispositivos que se incluirán en el esquema de direccionamiento IP se incluyen los siguientes:

- Dispositivos de usuario final: número y tipo de conexiones (es decir, por cable, inalámbrico, acceso remoto)
- Servidores y dispositivos periféricos (por ejemplo, impresoras y cámaras de seguridad)
- Dispositivos intermedios, incluidos switches y puntos de acceso.

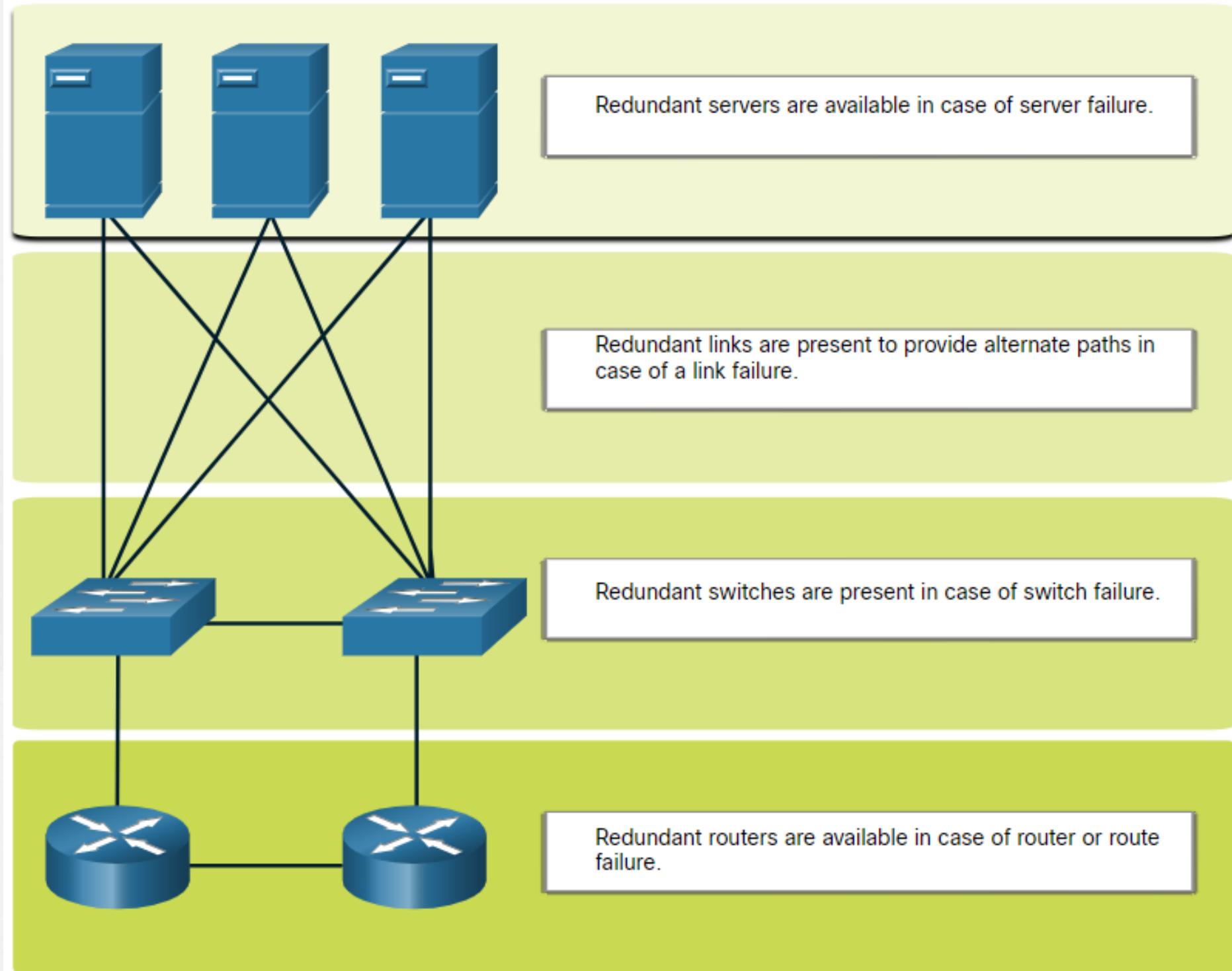
Se recomienda planificar, documentar y mantener un esquema de direccionamiento IP basado en el tipo de dispositivo. El uso de un esquema de direccionamiento IP planificado facilita la identificación de un tipo de dispositivo y la solución de problemas.



# Dispositivos de una red pequeña Redundancia en redes pequeñas

Para mantener un alto grado de confiabilidad, se requiere, *redundancia* en el diseño de red. La redundancia ayuda a eliminar puntos de error únicos.

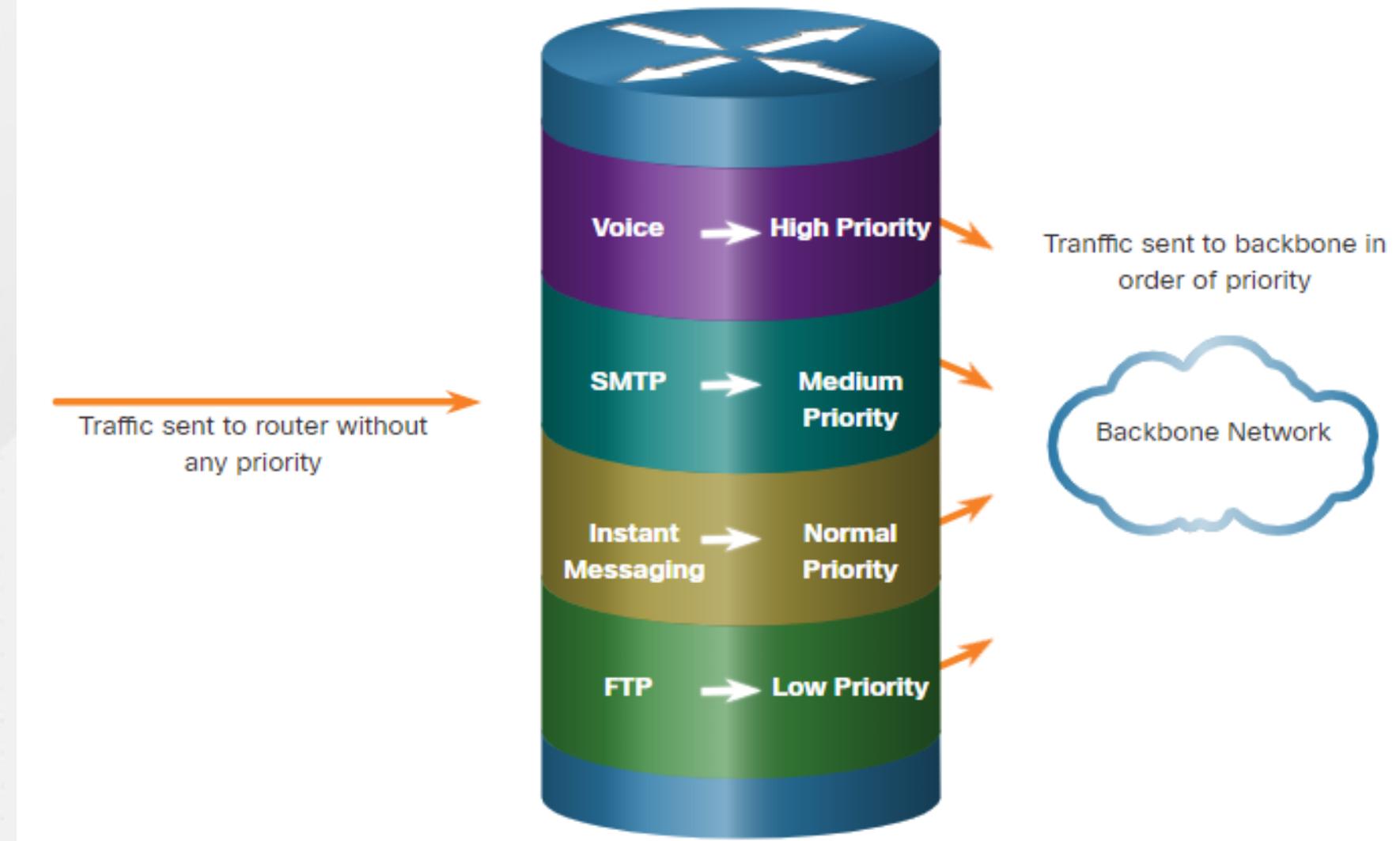
La redundancia se puede lograr instalando equipos duplicados. También se puede lograr mediante el suministro de enlaces de red duplicados para áreas críticas.





# Dispositivos de una red pequeña Administración de tráfico

- El objetivo de un buen diseño de red es mejorar la productividad de los empleados y minimizar el tiempo de inactividad de la red.
- Los routers y switches en una red pequeña se deben configurar para admitir el tráfico en tiempo real, como voz y vídeo, de forma independiente del tráfico de otros datos. Un buen diseño de red implementará la calidad de servicio (QoS).
- Hay cuatro colas de prioridad. La cola de prioridad alta siempre se vacía primero.





# APLICACIONES Y PROTOCOLOS DE REDES PEQUEÑAS



## Aplicaciones y protocolos de redes pequeñas Aplicaciones comunes

Después de configurarlo, la red aún necesita ciertos tipos de aplicaciones y protocolos para funcionar. La utilidad de las redes depende de las aplicaciones que se encuentren en ellas.

Existen dos formas de procesos o programas de software que proporcionan acceso a la red:

- **Aplicaciones de red:** aplicaciones que implementan protocolos de capa de aplicación y pueden comunicarse directamente con las capas inferiores de la pila de protocolos..
- **Servicios de capa de aplicación:** para aplicaciones que no son compatibles con la red, los programas que interactúan con la red y preparan los datos para su transferencia.



# Aplicaciones y protocolos de redes pequeñas

## Protocolos comunes

Los protocolos de red admiten los servicios y aplicaciones que usan los empleados en una red pequeña.

- Los administradores de red suelen requerir acceso a los dispositivos y servidores de red. Las dos soluciones de acceso remoto más comunes son Telnet y Secure Shell (SSH).
  - Protocolo de transferencia de hipertexto (HTTP) y Protocolo de transferencia de hipertexto seguro (HTTP) se utilizan entre clientes web y servidores web.
  - El Protocolo simple de transferencia de correo (SMTP) se utiliza para enviar correos electrónicos, los clientes utilizan el Protocolo de oficina postal (POP3) o el Protocolo de acceso a correo de Internet (IMAP) para recuperar el correo electrónico.
  - El Protocolo de transferencia de archivos (FTP) y el Protocolo de transferencia de archivos de seguridad (SFTP) se utilizan para descargar y cargar archivos entre un cliente y un servidor FTP.
  - Los clientes utilizan el Protocolo de configuración dinámica de host (DHCP) para adquirir una configuración IP de un servidor DHCP.
  - El Servicio de nombres de dominio (DNS) resuelve los nombres de dominio en direcciones IP.
- Nota:** Un servidor podría proporcionar varios servicios de red. Por ejemplo, un servidor podría ser un servidor de correo electrónico, FTP y SSH.



## Aplicaciones y protocolos de redes pequeñas **Protocolos comunes (Cont.)**

Estos protocolos de red comprenden el conjunto de herramientas fundamental de un profesional de la red, que define:

- Los procesos en cualquier extremo de una sesión de comunicación
- Tipos de mensajes
- La sintaxis de los mensajes
- El significado de los campos informativos
- Cómo se envían los mensajes y la respuesta esperada
- Interacción con la capa inferior siguiente

Muchas empresas han establecido una política de uso de versiones seguras (por ejemplo, SSH, SFTP y HTTPS) de estos protocolos siempre que sea posible.



# Aplicaciones y protocolos de redes pequeñas

## Aplicaciones de voz y video

- Las empresas actuales utilizan cada vez más la telefonía IP y los medios de transmisión para comunicarse con los clientes y socios comerciales, además de permitir que sus empleados trabajen de forma remota.
- El administrador de red debe asegurarse de que se instalen los equipos adecuados en la red y que se configuren los dispositivos de red para asegurar la entrega según las prioridades.
- Los factores que un administrador de una red pequeña debe tener en cuenta al admitir aplicaciones en tiempo real:
  - **Infraestructura:** ¿Tiene la capacidad y la capacidad para admitir aplicaciones en tiempo real?
  - **VoIP:** VoIP suele ser menos costoso que la telefonía IP, pero a costa de la calidad y las características.
  - **Telefonía IP** - Esto emplea servidores dedicados de control de llamadas y señalización.
  - **Aplicaciones en tiempo real:** la red debe admitir mecanismos de calidad de servicio (QoS) para minimizar los problemas de latencia. Protocolo de transporte en tiempo real (RTP) y Protocolo de control de transporte en tiempo real (RTCP) y dos protocolos que admiten aplicaciones en tiempo real.



# CREENCIAS HACIA REDES MÁS GRANDES

FORMANDO PROFESIONALES DE ÉLITE



# Crecimiento hacia redes más grandes

## Crecimiento de redes pequeñas

El crecimiento es un proceso natural para muchas pequeñas empresas, y sus redes deben crecer en consecuencia. Idealmente, el administrador de la red tiene suficiente tiempo de espera para tomar decisiones inteligentes sobre el crecimiento de la red en alineación con el crecimiento de la empresa.

Para extender una red, se requieren varios elementos:

- **Documentación de la red**- Topologías física y lógica.
- **Inventario de dispositivos** - Lista de dispositivos que utilizan o conforman la red.
- **Presupuesto** - Presupuesto de TI detallado, incluido el presupuesto de adquisición de equipos para el año fiscal.
- Análisis de tráfico: **se deben registrar los protocolos, las aplicaciones, los servicios y sus respectivos requisitos de tráfico.**

Estos elementos se utilizan para fundamentar la toma de decisiones que acompaña el escalamiento de una red pequeña.



# Crecimiento hacia redes más grandes Análisis de protocolos

Es importante comprender el tipo de tráfico que cruza la red, así como el flujo de tráfico actual. Hay varias herramientas de administración de red que se pueden utilizar para este propósito.

Para determinar los patrones de flujo de tráfico, es importante hacer lo siguiente:

- Capturar tráfico en horas de uso pico para obtener una buena representación de los diferentes tipos de tráfico.
- Realice la captura en diferentes segmentos de red y dispositivos, ya que parte del tráfico será local para un segmento en particular.
- La información recopilada por el analizador de protocolos se evalúa de acuerdo con el origen y el destino del tráfico, y con el tipo de tráfico que se envía.
- Este análisis puede utilizarse para tomar decisiones acerca de cómo administrar el tráfico de manera más eficiente.



## Crecimiento hacia redes más grandes **Uso de la red por parte de los empleados**

Muchos sistemas operativos proporcionan herramientas integradas para mostrar dicha información sobre la utilización de la red. Estas herramientas se pueden utilizar para capturar una «instantánea» de información como la siguiente:

- Os y versión del SO
- Utilización de CPU
- Utilización de RAM
- Utilización de unidades
- Aplicaciones que no utilizan la red
- Aplicaciones de red

Documentar instantáneas para los empleados en una red pequeña durante un período de tiempo es muy útil para identificar los requisitos de protocolo en evolución y los flujos de tráfico asociados.



**ITSQMET**  
INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

# VERIFICAR LA CONECTIVIDAD

FORMANDO PROFESIONALES DE ÉLITE

© 2016 Cisco y/o sus filiados. Todos los derechos reservados. Información – N°  
confidencial de Cisco

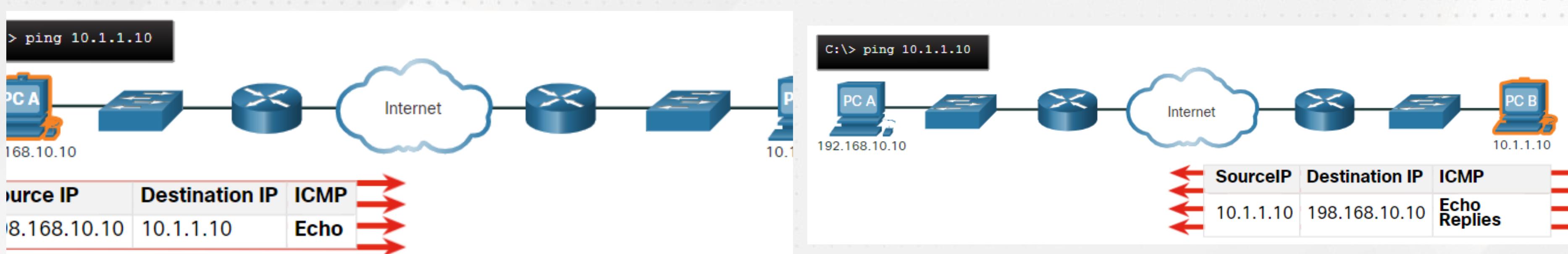




## Verificar la conectividad Verificar la conectividad con Ping

Si su red es pequeña y nueva, o si está escalando una red existente, siempre querrá poder verificar que sus componentes estén correctamente conectados entre sí y a Internet.

- El comando ping, disponible en la mayoría de los sistemas operativos, es la forma más eficaz de probar rápidamente la conectividad de Capa 3 entre una dirección IP de origen y destino.
- El comando ping utiliza los mensajes de eco del Protocolo de mensajes de control de Internet (ICMP) (ICMP tipo 8) y respuesta de eco (ICMP tipo 0).





## Verificar la conectividad **Verificar la conectividad con Ping (Cont.)**

En un host de Windows 10, el comando ping envía cuatro mensajes de eco ICMP consecutivos y espera cuatro respuestas de eco ICMP consecutivas desde el destino. El ping de IOS envía cinco mensajes de eco ICMP y muestra un indicador para cada respuesta de eco ICMP recibida.

Los indicadores de ping de IOS son los siguientes:



# Verificar la conectividad

## Verificar la conectividad con Ping (Cont.)

Elemento	Descripción
!	<ul style="list-style-type: none"><li>El signo de exclamación indica que se ha recibido correctamente un mensaje de respuesta de eco.</li><li>Valida una conexión de Capa 3 entre el origen y el destino.</li></ul>
.	<ul style="list-style-type: none"><li>Un punto significa que el tiempo expiró en espera de un mensaje de respuesta de eco.</li><li>Esto indica que ocurrió un problema de conectividad en algún lugar a lo largo del camino.</li></ul>
U	<ul style="list-style-type: none"><li><b>U mayúscula</b> indica que un router a lo largo de la ruta respondió con un mensaje de error ICMP tipo 3 "destino inalcanzable".</li><li>Las posibles razones incluyen que el router no conoce la dirección a la red de destino o que no pudo encontrar el host en la red de destino.</li></ul>

**Nota:** Otras posibles respuestas ping incluyen Q, M,? , o &. Sin embargo, el significado de estos están fuera de alcance para este módulo.



# Verificar conectividad Ping extendido

Cisco IOS ofrece un modo "extendido" del comando **ping**.

El ping extendido se ingresa en modo EXEC privilegiado escribiendo **ping** sin una dirección IP de destino. A continuación, se le darán varias indicaciones para personalizar el pingextendido.

**Note:** Al presionar **Enter** se aceptan los valores predeterminados indicados. El comando **ping ipv6** se usa para pings extendidos IPv6.

```
R1# ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 192.168.10.1
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

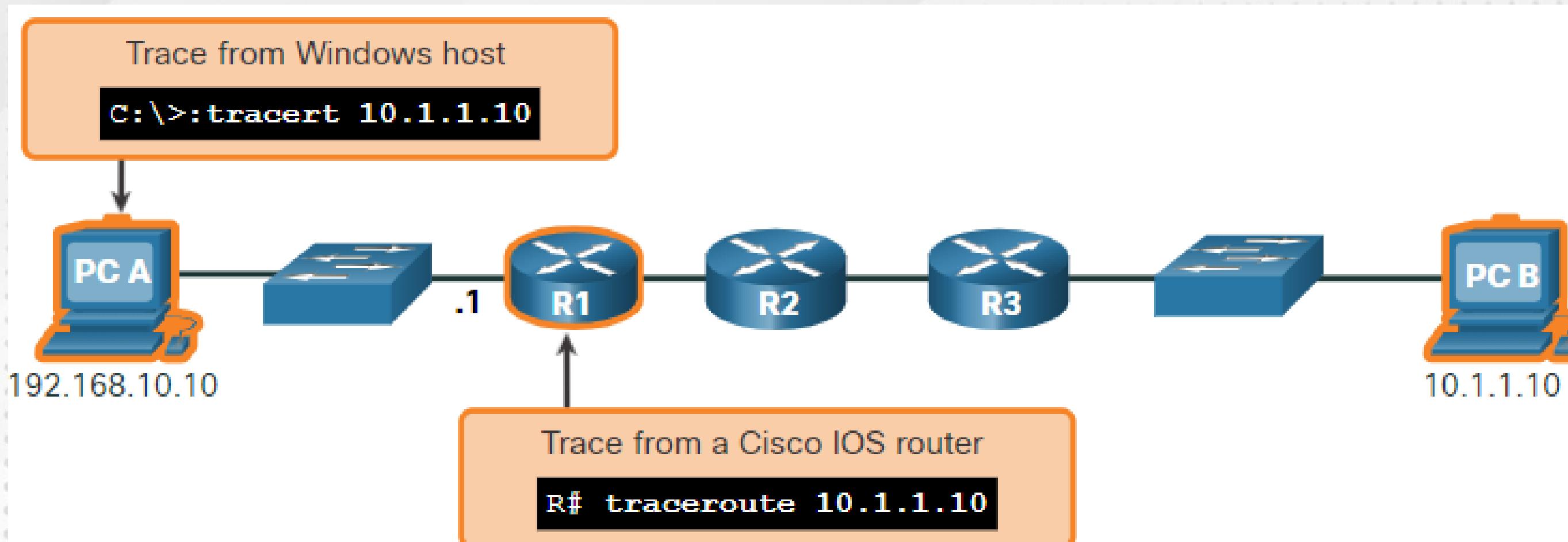


# Verificar conectividad

## Verificar conectividad con Traceroute

El comando ping es útil para determinar rápidamente si hay un problema de conectividad de Capa 3. Sin embargo, no identifica dónde se encuentra el problema a lo largo de la ruta.

- Traceroute puede ayudar a localizar áreas problemáticas de la Capa 3 en una red. Un rastreo proporciona una lista de saltos cuando un paquete se enruta a través de una red.
- La sintaxis del comando trace varía entre sistemas operativos.





## Verificar la conectividad Verificar la conectividad con Traceroute (Cont.)

- El siguiente es un ejemplo de salida de comando **tracert** en un host de Windows 10.  
**Nota:** Utilice **Ctrl-C** para interrumpir un **tracert** en Windows.
- La única respuesta exitosa fue desde el gateway de R1. Las solicitudes de seguimiento al siguiente salto se agotaron como indica el asterisco (\*), lo que significa que el router de salto siguiente no respondió o que existe un error en la ruta de red. En este ejemplo parece haber un problema entre R1 y R2.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.1.10 over a maximum of 30 hops:
  1    2 ms      2 ms      2 ms  192.168.10.1
  2    *          *          *      Request timed out.
  3    *          *          *      Request timed out.
  4    *          *          *      Request timed out.

^C
C:\Users\PC-A>
```



# Verificar la conectividad Verificar la conectividad con Traceroute (Cont.)

Los siguientes son los resultados de ejemplo del comando traceroute de R1:

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
 1 209.165.200.226 1 msec 0 msec 1 msec
 2 209.165.200.230 1 msec 0 msec 1 msec
 3 10.1.1.10 1 msec 0 msec
R1#
```

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
 1 209.165.200.226 1 msec 0 msec 1 msec
 2 209.165.200.230 1 msec 0 msec 1 msec
 3 * * *
 4 * * *
 5 *
```

- A la izquierda, el seguimiento validó que podía llegar con éxito al PC B.
- A la derecha, el host 10.1.1.10 no estaba disponible y el resultado muestra asteriscos donde se agotó el tiempo de espera de las respuestas. Los tiempos de espera indican un posible problema de red.
- Utilice **Ctrl-Shift-6** para interrumpir un **traceroute** en Cisco IOS.

**Nota:** La implementación de Windows de traceroute (tracert) envía solicitudes de eco ICMP. Cisco IOS y Linux utilizan UDP con un número de puerto no válido. El destino final devolverá un mensaje de puerto ICMP inalcanzable.



## Verificar conectividad Traceroute extendido

Al igual que el comando **ping extendido**, también hay un comando **traceroute** extendido. Permite al administrador ajustar los parámetros relacionados con la operación de comando.

El comando **tracert** de Windows permite la entrada de varios parámetros a través de opciones en la línea de comando. Sin embargo, no se guía como el comando extendido traceroute IOS. El siguiente resultado muestra las opciones disponibles para el comando **tracert** de Windows:

```
C:\Users\PC-A> tracert /?
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
                [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d           Do not resolve addresses to hostnames.
    -h maximum_hops Maximum number of hops to search for target.
    -j host-list  Loose source route along host-list (IPv4-only).
    -w timeout   Wait timeout milliseconds for each reply.
    -R           Trace round-trip path (IPv6-only).
    -S srcaddr   Source address to use (IPv6-only).
    -4           Force using IPv4.
    -6           Force using IPv6.

C:\Users\PC-A>
```



# Verificar conectividad Traceroute extendido (Cont.)

- La opción **traceroute** extendido del IOS de Cisco permite al usuario crear un tipo especial de seguimiento ajustando los parámetros relacionados con la operación de comando.
- Traceroute extendido se ingresa en modo EXEC privilegiado escribiendo **traceroute** sin una dirección IP de destino. IOS lo guiará en las opciones de comando presentando varios indicadores relacionados con la configuración de todos los parámetros diferentes.
- **Nota:** Al presionar **Enter** se aceptan los valores predeterminados indicados.

```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.1.10
Ingress traceroute [n]:
Source address: 192.168.10.1
DSCP Value [0]:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 1 msec 1 msec
  2 209.165.200.230 0 msec 1 msec 0 msec
  3 *
          10.1.1.10 2 msec 2 msec
R1#
```



## Verifique la conectividad Línea base de red

- Una de las herramientas más efectivas para controlar y resolver problemas relacionados con el rendimiento de la red es establecer una línea de base de red.
- Un método para iniciar una línea de base es copiar y pegar en un archivo de texto los resultados de los comandos ping, trace u otros comandos relevantes. Estos archivos de texto se pueden marcar con la fecha y guardarse en un archivo para su posterior recuperación y comparación.
- Entre los elementos que se deben tener en cuenta, se encuentran los mensajes de error y los tiempos de respuesta de host a host.
- Las redes corporativas deben tener líneas de base extensas; más extensas de lo que podemos describir en este curso. Existen herramientas de software a nivel profesional para almacenar y mantener información de línea de base.



# COMANDOS DE HOST Y DE IOS

FORMANDO PROFESIONALES DE ÉLITE

© 2016 Cisco y/o sus filiales. Todos los derechos reservados. Información dNº  
confidencial de Cisco





# Comandos de host e IOS Configuración IP en un host de Windows

En Windows 10, puede acceder a los detalles de la dirección IP desde el **Centro de redes y recursos compartidos** para ver rápidamente las cuatro configuraciones importantes: dirección, máscara, router y DNS. O puede ejecutar el comando **ipconfig** en la línea de comandos de una computadora con Windows.

- Utilice el comando **ipconfig /all** para ver la dirección MAC junto con varios detalles relacionados con la asignación de direcciones de capa 3 del dispositivo.
- Si un host está configurado como cliente DHCP, la configuración de la dirección IP se puede renovar mediante los comandos **ipconfig /release** e **ipconfig /renew**.
- El servicio del cliente DNS en PC con Windows también optimiza el rendimiento de la resolución de nombres DNS al almacenar en la memoria los nombres resueltos previamente. El comando **ipconfig /displaydns** muestra todas las entradas DNS en caché en un sistema de computación Windows.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
  IPv4 Address . . . . . : 192.168.10.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.10.1
(Output omitted)
```



# Comandos de host e IOS Configuración IP en un host Linux

- La verificación de la configuración IP usando la GUI en una máquina Linux variará dependiendo de la distribución Linux y la interfaz de escritorio.
- En la línea de comandos, utilice el comando **ifconfig** para mostrar el estado de las interfaces activas actualmente y su configuración IP.
- El comando **IP address** de Linux se utiliza para mostrar direcciones y sus propiedades. También se puede usar para agregar o eliminar direcciones IP.

**Nota:** El resultado mostrado puede variar dependiendo de la distribución de Linux.

```
[analyst@sec0ps ~]$ ifconfig
enp0s3    Link encap:Ethernet HWaddr 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15 Bcast:10.0.2.255 Mask: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:1855455014 (1.8 GB) TX bytes:13140139 (13.1 MB)
lo        flags=73 mtu 65536
          inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 prefixlen 128 scopeid 0x10
                  loop txqueuelen 1000 (Local Loopback)
                  RX packets 0 bytes 0 (0.0 B)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 0 bytes 0 (0.0 B)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



# Comandos de host e IOS Configuración IP en un host macOS

- En la GUI de un host Mac, abra **Preferencias de red > Avanzadas** para obtener la información de direcciones IP.
- El comando **ifconfig** también se puede utilizar para verificar la configuración IP de la interfaz en la línea de comandos.
- Otros comandos útiles de macOS para verificar la configuración de IP del host incluyen **networksetup -listallnetworkservices** y **networksetup -getinfo < network service >**.

```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$ 
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
MacBook-Air:~ Admin$
```



# Comandos de host y de IOS

## El comando arp

El comando **arp** se ejecuta desde el símbolo del sistema de Windows, Linux o Mac. El comando enumera todos los dispositivos actualmente en la caché ARP del host.

- El comando **arp -a** muestra los vínculos entre la dirección IP y la dirección MAC. El caché ARP solo muestra información de dispositivos a los que se ha accedido recientemente.
- Para asegurar que la caché ARP esté cargada, haga, **ping** a un dispositivo de manera tal que tenga una entrada en la tabla ARP.
- La memoria caché se puede borrar mediante el comando **netsh interface ip delete arpcache** en caso de que el administrador de la red quiera repoblar la memoria caché con información actualizada.

**Nota:** Es posible que necesite acceso de administrador en el host para poder utilizar el comando **netsh interface ip delete arpcache**.



# Comandos Host y de IOS

## Repasso de comandos show comunes

Comando	Descripción
show running-config	Verifica la configuración y configuración actuales
show interfaces	Verifica el estado de la interfaz y muestra cualquier mensaje de error
show ip interface	Verifica la información de la capa 3 de una interfaz
show arp	Verifica la lista de hosts conocidos en las LAN Ethernet locales
show ip route	Verifica la información de enrutamiento de la capa 3
show protocols	Verifica qué protocolos están operativos
show version	Verifica la memoria, las interfaces y las licencias del dispositivo



# Comandos de host y de IOS El comando show cdp neighbors

El CDP brinda la siguiente información acerca de cada dispositivo vecino de CDP:

- **Identificadores de dispositivos** - El nombre de host configurado de un switch, router u otro dispositivo
- Lista de direcciones: **hasta una dirección de capa de red para cada protocolo admitido.**
- Identificador de puerto: **el nombre del puerto local y remoto en forma de una cadena de caracteres ASCII, como por ejemplo, FastEthernet 0/0.**
- **Lista de capacidades** si un dispositivo específico es un switch de capa 2 o un switch de capa 3
- **Plataforma** - La plataforma de hardware del dispositivo.

El comando **show cdp neighbors detail** muestra las direcciones IP de los dispositivos vecinos.

```
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID      Local Intrfce     Holdtme   Capability Platform Port ID
S3            Gig 0/0/1          122        S I       WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```



# Comandos de host y de IOS El comando **show ip interface brief**

Uno de los comandos más utilizados es el comando **show ip interface brief**. Este comando proporciona un resultado más abreviado que el comando **show ip interface**. Proporciona un resumen de la información clave para todas las interfaces de red de un router.

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0/0 209.165.200.225 YES manual up            up
GigabitEthernet0/0/1 192.168.10.1   YES manual up            up
Serial0/1/0          unassigned     NO  unset  down           down
Serial0/1/1          unassigned     NO  unset  down           down
GigabitEthernet0      unassigned     YES unset administratively down down
R1#
```

```
S1# show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
Vlan1              192.168.254.250 YES manual up            up
FastEthernet0/1     unassigned     YES unset  down           down
FastEthernet0/2     unassigned     YES unset  up             up
FastEthernet0/3     unassigned     YES unset  up             up
```



# METODOLOGÍAS PARA LA SOLUCIÓN DE PROBLEMAS



# Metodologías de solución de problemas Enfoques para la solución de problemas básicos

Paso	Descripción
<b>Paso 1. Identificar del problema</b>	<ul style="list-style-type: none"><li>• El primer paso en el proceso de solución de problemas.</li><li>• Aunque las herramientas se pueden utilizar en este paso, una conversación con el usuario a menudo es muy útil.</li></ul>
<b>Paso 2. Establecer una teoría de causas probables</b>	<ul style="list-style-type: none"><li>• Después de identificar el problema, intente establecer una teoría de causas probables.</li><li>• Este paso generalmente permite ver más causas probables del problema.</li></ul>
<b>Paso 3: Poner a prueba la teoría para determinar la causa</b>	<ul style="list-style-type: none"><li>• Según las causas probables, pruebe sus teorías para determinar cuál es la causa del problema.</li><li>• Un técnico puede aplicar una solución rápida para probar y ver si resuelve el problema.</li><li>• Si una solución rápida no corrige el problema, es posible que deba investigar el problema más a fondo para establecer la causa exacta.</li></ul>
<b>Paso 4. Establecer un plan de acción e implementar la solución</b>	Una vez que haya determinado la causa exacta del problema, establezca un plan de acción para solucionar el problema e implementar la solución.
<b>Paso 5. Verificar la solución e implementar medidas preventivas</b>	<ul style="list-style-type: none"><li>• Después de que haya corregido el problema, verifique la funcionalidad completa.</li><li>• Si corresponde, implementar medidas preventivas.</li></ul>
<b>Paso 6. Registrar hallazgos, acciones y resultados</b>	<ul style="list-style-type: none"><li>• El último paso del proceso de solución de problemas consiste en registrar los hallazgos, las acciones y los resultados.</li><li>• Esto es muy importante para referencia futura.</li></ul>



## Metodologías de solución de problemas ¿Solucionar o escalar?

- En algunas situaciones, quizás no sea posible solucionar el problema de inmediato. Un problema debería escalarse cuando requiere la decisión del gerente, cierta experiencia específica, o el nivel de acceso a la red no está disponible para el técnico que debe solucionar el problema.
- Una política de la empresa debe indicar claramente cuándo y cómo un técnico debe escalar un problema.



# Solución de problemas Metodologías

## El comando debug

- El comando de IOS **debug** le permite al administrador mostrar el proceso del SO, el protocolo, el mecanismo y los mensajes de eventos en tiempo real para su análisis.
- Todos los comandos **debug** se introducen en el modo EXEC privilegiado. Cisco IOS permite limitar el resultado de **debug** para incluir solo la característica o la subcaracterística relevante. Use los comandos **debug** solo para solucionar problemas específicos.
  - Para acceder a una breve descripción de todas las opciones del comando de depuración, utilice el comando **debug ?** en modo EXEC con privilegios, en la línea de comandos.
  - Para desactivar una característica de depuración específica, agregue la palabra clave **no** delante del comando **debug**:
  - Alternativamente, puede ingresar la forma **undebug** del comando en modo EXEC privilegiado:
  - Para desactivar todos los comandos debug activos de inmediato, utilice el comando **undebug all**:
- Tenga cuidado al usar algunos comandos de **debug** ya que pueden generar una cantidad sustancial de salida y utilizar una gran parte de los recursos del sistema. El router podría estar tan ocupado mostrando mensajes de **debug** que no tendría suficiente potencia de procesamiento para realizar sus funciones de red, o incluso escuchar comandos para desactivar la depuración.



## Métodos de solución de problemas El comando terminal monitor

- **debug** y algunos otros mensajes de salida de IOS no se muestran automáticamente en las conexiones remotas. Esto se debe a que se impide que los mensajes de registro se muestren en líneas vty.
- Para mostrar los mensajes de registro en una terminal (consola virtual), utilice el comando modo EXEC privilegiado **terminal monitor**. Para detener los mensajes de registro en una terminal, utilice el comando modo EXEC privilegiado **terminal no monitor**.

```
R2# telnet 209.165.200.225
Trying 209.165.200.225 ... Open
Authorized access only!
User Access Verification
Password:
R1> enable
Password:
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```

```
R1# terminal monitor
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1# no debug ip icmp
ICMP packet debugging is off
R1#
```



# ESCENARIOS PARA LA SOLUCIÓN DE PROBLEMAS



- Las interfaces de interconexión de Ethernet deben funcionar en el mismo modo dúplex para un mejor rendimiento de comunicación y para evitar la ineficiencia y la latencia en el enlace.
- La función de negociación automática Ethernet facilita la configuración, minimiza los problemas y maximiza el rendimiento de los enlaces entre dos enlaces Ethernet de interconexión. Los dispositivos conectados primero anuncian sus capacidades utilizadas y luego eligen el modo de mayor rendimiento soportado por ambos extremos.
- Surge una discordancia si uno de los dos dispositivos conectados funciona en modo dúplex completo y el otro funciona en modo semidúplex. Si bien la comunicación de datos se realizará a través de un enlace con una discordancia de dúplex, el rendimiento del enlace será muy deficiente.
- Los desajustes de dúplex suelen deberse a una interfaz mal configurada o, en raras ocasiones, a una negociación automática fallida. Las discordancias de dúplex pueden ser difíciles de resolver mientras se produce la comunicación entre dispositivos.



# Situaciones de solución de problemas Problemas de asignación de direcciones IP en dispositivos IOS

- Dos causas comunes de asignación incorrecta de IPv4 son los errores manuales de asignación o los problemas relacionados con DHCP.
- Los administradores de redes tienen que asignar a menudo las direcciones IP manualmente a los dispositivos como servidores y routers. Si se genera un error durante la asignación, es muy probable que ocurran problemas de comunicación con el dispositivo.
- En un dispositivo IOS, utilice los comandos **show ip interface** o **show ip interface brief** para comprobar qué direcciones IPv4 se asignan a las interfaces de red. Por ejemplo, ejecutar el comando **show ip interface brief** como se muestra validaría el estado de la interfaz en R1.

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0/0 209.165.200.225 YES manual up           up
GigabitEthernet0/0/1 192.168.10.1   YES manual up           up
Serial0/1/0          unassigned     NO  unset  down        down
Serial0/1/1          unassigned     NO  unset  down        down
GigabitEthernet0      unassigned     YES unset  administratively down down
R1#
```



Escenarios para la solución de problemas

## Problemas de asignación de direcciones IP en dispositivos finales

- En las máquinas con Windows, cuando el dispositivo no puede comunicarse con un servidor DHCP, Windows asigna automáticamente una dirección que pertenezca al rango 169.254.0.0/16. Esta función se denomina direccionamiento IP privado automático (APIPA).
- Una computadora con una dirección APIPA no podrá comunicarse con otros dispositivos en la red porque esos dispositivos probablemente no pertenecerán a la red 169.254.0.0/16.
  - **Nota:** Otros sistemas operativos, como Linux y OS X, no utilizan APIPA.
- Si el dispositivo no puede comunicarse con el servidor DHCP, el servidor no puede asignar una dirección IPv4 para la red específica y el dispositivo no podrá comunicarse.
- Para verificar las direcciones IP asignadas a una computadora con Windows, use el comando **ipconfig**.



# Situaciones posibles para la solución de problemas **Problemas con el gateway predeterminado**

- El gateway predeterminado para un dispositivo final es el dispositivo de red más cercano, que pertenece a la misma red que el dispositivo final, que puede reenviar el tráfico a otras redes. Si un dispositivo tiene una dirección de gateway predeterminado incorrecta o inexistente, no podrá comunicarse con los dispositivos de las redes remotas.
- Como sucede con los problemas de asignación de direcciones IPv4, los problemas del gateway predeterminado pueden estar relacionados con la configuración incorrecta (en el caso de la asignación manual) o problemas de DHCP (si está en uso la asignación automática).
- Utilice el comando **ipconfig** para verificar el gateway predeterminado en una computadora basada en Windows.
- En un router, utilice el comando **show ip route** para mostrar la tabla de enrutamiento y verificar que se ha establecido el gateway predeterminado, conocido como ruta predeterminada. Se usa esta ruta cuando la dirección de destino del paquete no coincide con ninguna otra ruta en la tabla de enrutamiento.



# Escenarios para la solución de problemas **Solución de problemas de DNS**

- Es común que los usuarios relacionen erróneamente el funcionamiento de un enlace de Internet con la disponibilidad del servicio DNS.
- Las direcciones del servidor DNS pueden asignarse manual o automáticamente a través de DHCP.
- Si bien es común que las empresas y las organizaciones administren sus propios servidores DNS, cualquier servidor DNS accesible puede utilizarse para solucionar nombres.
- Cisco ofrece OpenDNS que proporciona un servicio DNS seguro mediante el filtrado de phishing y algunos sitios de malware. Las direcciones OpenDNS son 208.67.222.222 y 208.67.220.220. Las funciones avanzadas, como el filtrado y la seguridad de contenido web, están disponibles para familias y empresas.
- Use el comando **ipconfig /all** como se muestra para verificar qué servidor DNS está usando la computadora con Windows.
- El comando **nslookup** es otra herramienta útil para la solución de problemas de DNS para PC. Con **nslookup** un usuario puede configurar manualmente las consultas de DNS y analizar la respuesta de DNS.