

3.0 Capitulo 3

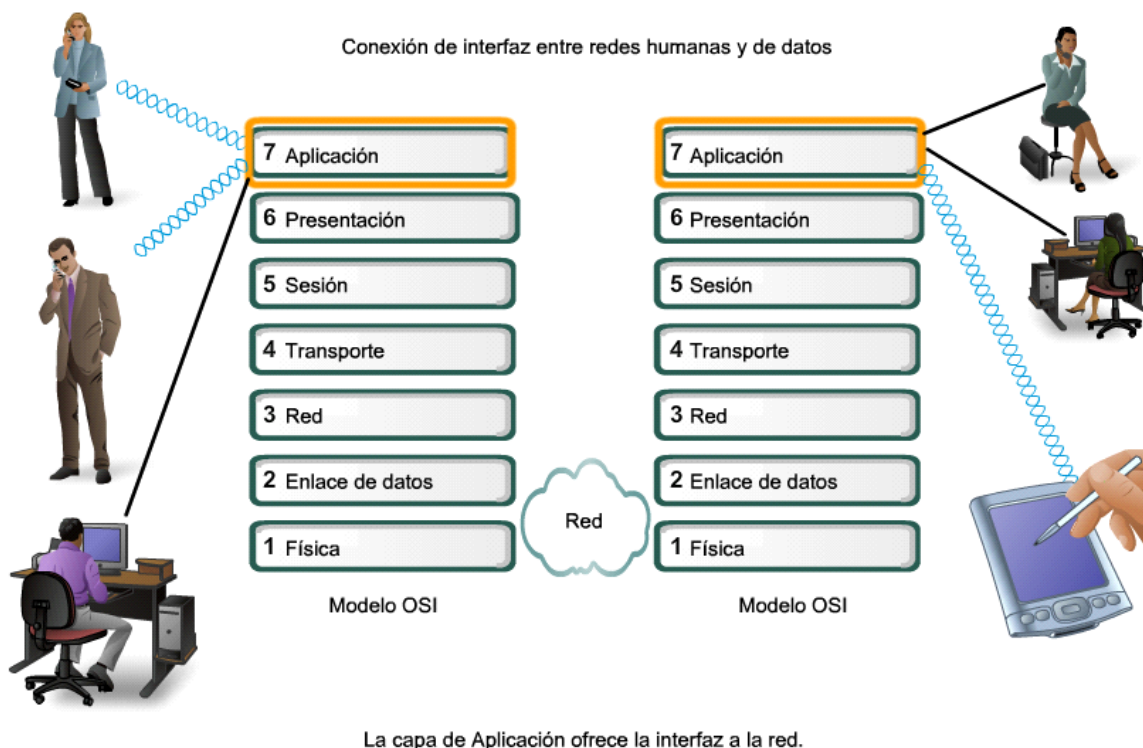
La capa de Aplicación

3.0.1 Introducción del capítulo

Componentes de la capa de aplicación: aplicaciones, servicios y protocolos.

Objetivos:

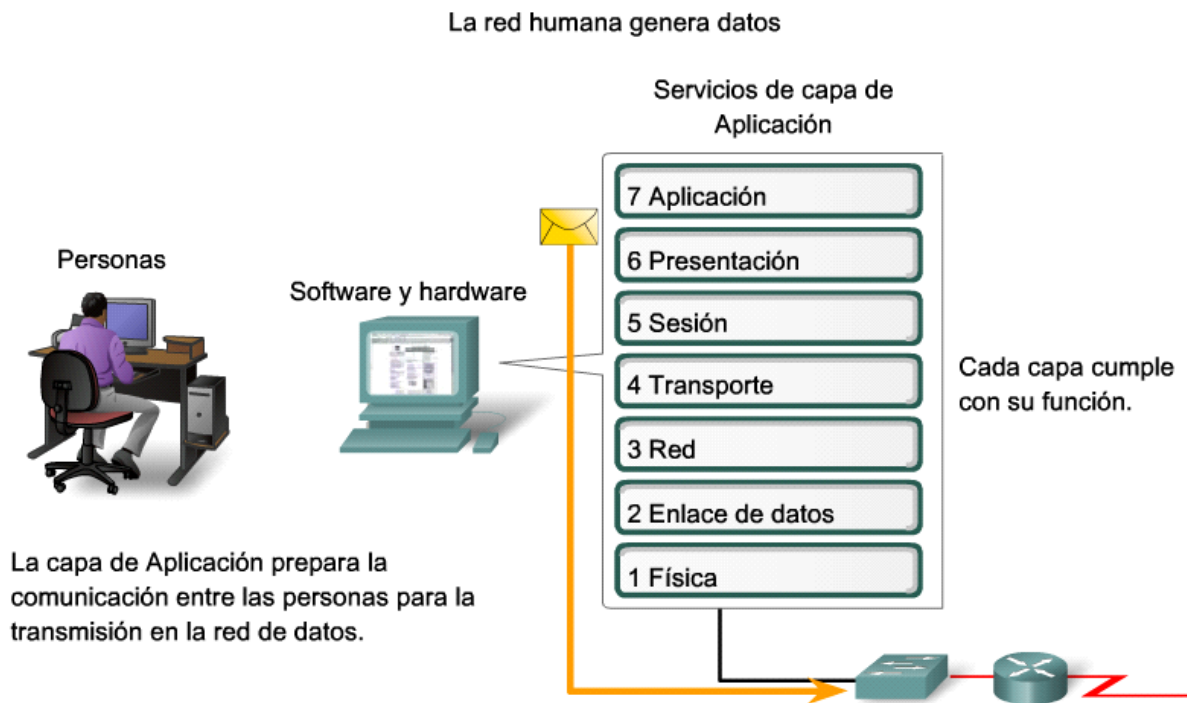
- Describir como las funciones de las últimas tres capas del modelo OSI proporcionan servicios de red al usuario final.
- Descripción del modo como la capa de aplicación de TCP/IP proporcionan los servicios que especifican las capas superiores del modelo OSI.
- Descripción del modo que el usuario utiliza la capa de aplicación para comunicarse a través de la red de información.
- Describir las funciones de algunas aplicaciones tales como HTTP, DNS, SMB, DHCP, SMTP/POP3, TELNET.
- Descripción de los procesos que se ejecutan en cada uno de los dispositivos terminales de datos para el intercambio de información.
- Explicación de como los protocolos que se ejecutan en una máquina pueden enviar o recibir información con dispositivos de red diferentes.
- Utilización de herramientas para el análisis del funcionamiento de aplicaciones diferentes.



3.1.1.1 Modelo OSI y modelo TCP/IP

La capa de aplicación le proporciona la interfaz al usuario para el ingreso a la red de datos. Los contenidos de las aplicaciones pasan por las diferentes capas en forma descendente hasta llegar al dispositivo de destino.

Los protocolos se utilizan para el intercambio de los datos entre los programas de aplicaciones que se ejecutan en los hosts de origen y destino.



3.1.1.2 El modelo OSI y el modelo TCP/IP

El modelo TCP/IP utiliza una sola capa para la representación funcional de las tres capas superiores del modelo OSI.

El protocolo TCP/IP se implementó antes de la aparición de las computadoras personales y de las aplicaciones gráficas. En consecuencia el protocolo TCP/IP implementa muy poco la funcionalidad de las tres capas superiores del modelo OSI.

La Capa de Presentación

Tiene tres funciones principales:

- Codificación y conversión de los datos procedentes del emisor para garantizar su interpretación en el dispositivo de destino. Códigos ASCII, EBCDIC, teclados de otros idiomas.
- Compresión de los datos para que puedan ser descomprimidos en el dispositivo de destino.
- Encriptación de los datos transmitidos y des-encriptación de los datos en el dispositivo de destino

Ejemplos de algunas aplicaciones:

Video:

- Quicktime: especificación de Apple Computer para audio y video.
- MPEG: grupo de expertos en películas, usado para la codificación y compresión de videos.

Imágenes gráficas:

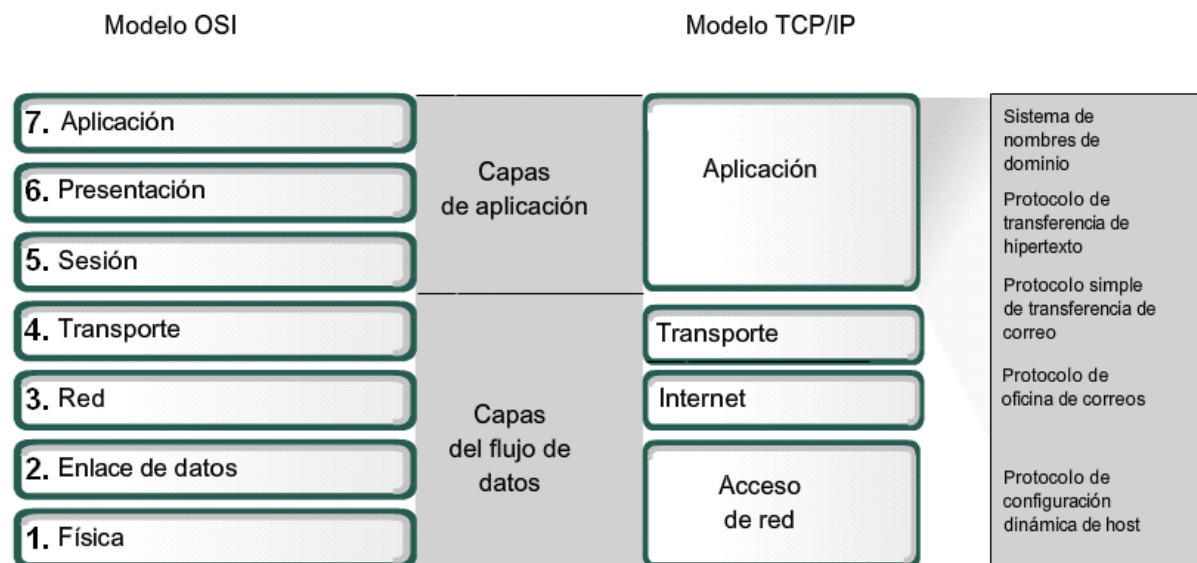
- GIF: formato de intercambio gráfico, codificación y compresión de imágenes gráficas.
- JPEG: grupo de expertos en fotografía, codificación y compresión de imágenes gráficas.
- TIFF: formato de codificación estándar para imágenes gráficas.

La Capa de Sesión

Maneja el dialogo entre los dos extremos para mantener activa la comunicación.

Control de acceso a la aplicación por medio de claves.

Reinicio de sesiones que fueron interrumpidas o permanecieron inactivas por un tiempo largo.



3.1.1.3 El modelo OSI y el modelo TCP/IP

El protocolo Servicio de Nombres de Dominio DNS se utiliza para la resolución de nombres de dominio con direcciones IP. Ofrece la dirección de un sitio Web.

El protocolo de transferencia de hipertexto HTTP se utiliza para la transferencia de archivos que forman las paginas Web de la WWW. Es una transferencia entre clientes y servidores.

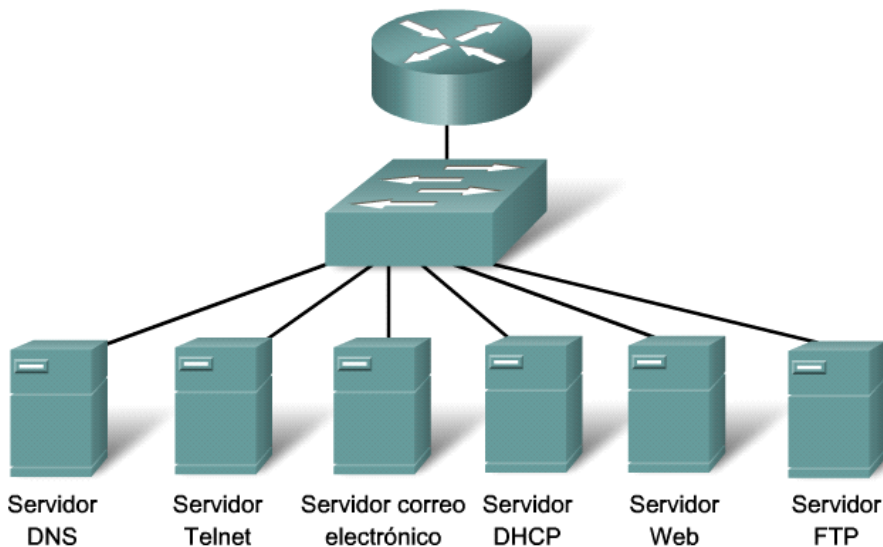
El servidor de correo electrónico, protocolos SMTP, IMAP, POP3.

El protocolo Telnet, permite la emulación de terminal para tener acceso remoto a servidores y a dispositivos de red, como si estuvieran registrados de forma local.

El protocolo de transferencia de archivos FTP se utiliza para la transferencia de archivos interactivos entre sistemas.

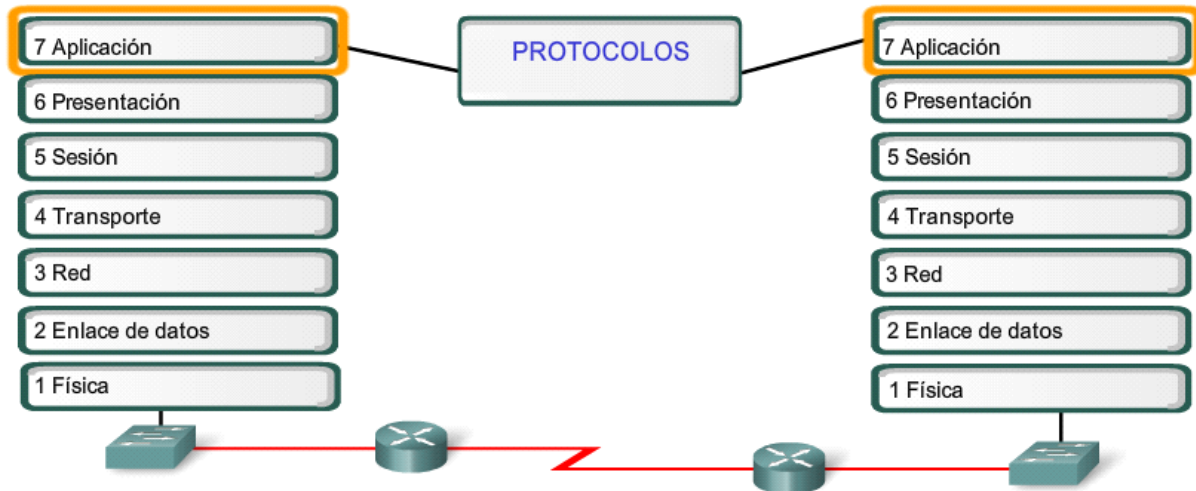
El protocolo DHCP asigna la dirección IP, la máscara y la puerta de acceso por defecto (gateway).

Asignación dinámica.



3.1.4 Funciones del protocolo de la Capa de Aplicación

Los protocolos establecen reglas consistentes para el intercambio de información entre capas pares. Los protocolos especifican las estructuras de los mensajes, los tipos de mensajes. Los tipos de mensajes pueden ser acuses de recibos, mensajes de error, transferencia de datos. Un protocolo puede especificar el proceso de establecimiento de la conexión ó desconexión entre dos dispositivos.



Los protocolos de capa de Aplicación proporcionan las reglas para la comunicación entre las aplicaciones.

Protocolos:

- Define los procesos en cada uno de los extremos de la comunicación
- Define los tipos de mensajes
- Define la sintaxis de los mensajes
- Define el significado de los campos de información
- Define la forma en que se envían los mensajes y la respuesta esperada
- Define la interacción con la próxima capa inferior

3.2.1 El modelo cliente-servidor

Un usuario puede no tener su información almacenada en sus equipos locales. Podría estar ubicada en un servidor. Es necesario el establecimiento de procedimientos de acceso a la información ubicada en otro equipo.

El modelo cliente-servidor

El dispositivo que solicita la información se denomina cliente.

El dispositivo que envía la información solicitada se denomina servidor.

En la mayoría de los casos es necesario el ingreso de una clave para el acceso a los recursos del servidor.

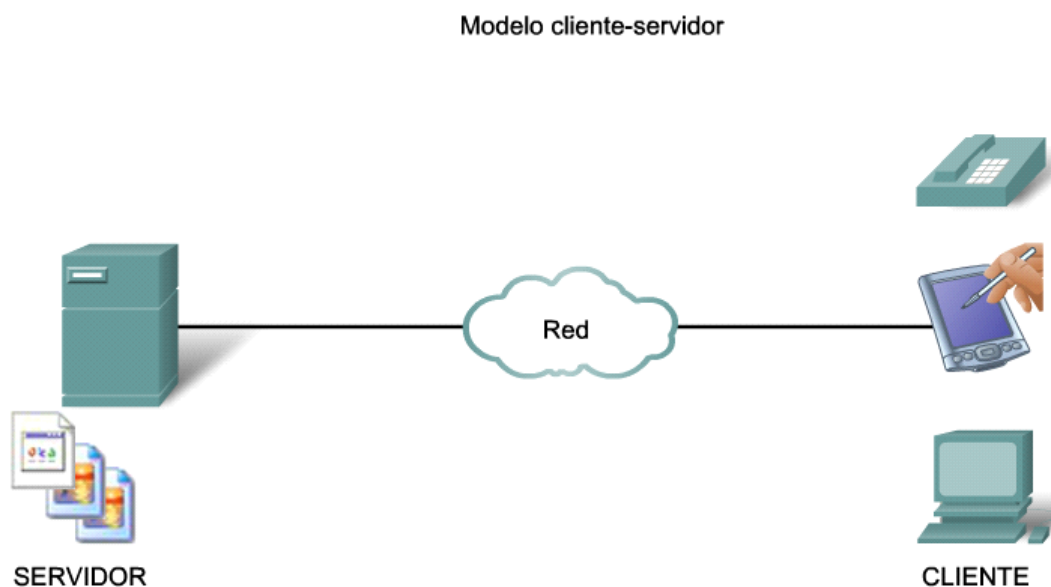
Los protocolos de la capa de aplicación describen los formatos de las solicitudes y respuestas entre el cliente y el servidor.

El correo electrónico es un servicio que funciona en la modalidad cliente-servidor.

El origen del flujo de los datos puede ser desde cualquiera de los dispositivos de un modelo cliente-servidor.

Carga: transferencia de datos desde un cliente hasta un servidor.

Descarga: transferencia de datos desde un servidor hacia un cliente.



3.2.2 Servidores

En general, un servidor contiene información para ser compartida con numerosos clientes. Ejemplos: páginas web, bases de datos, archivos de imágenes.

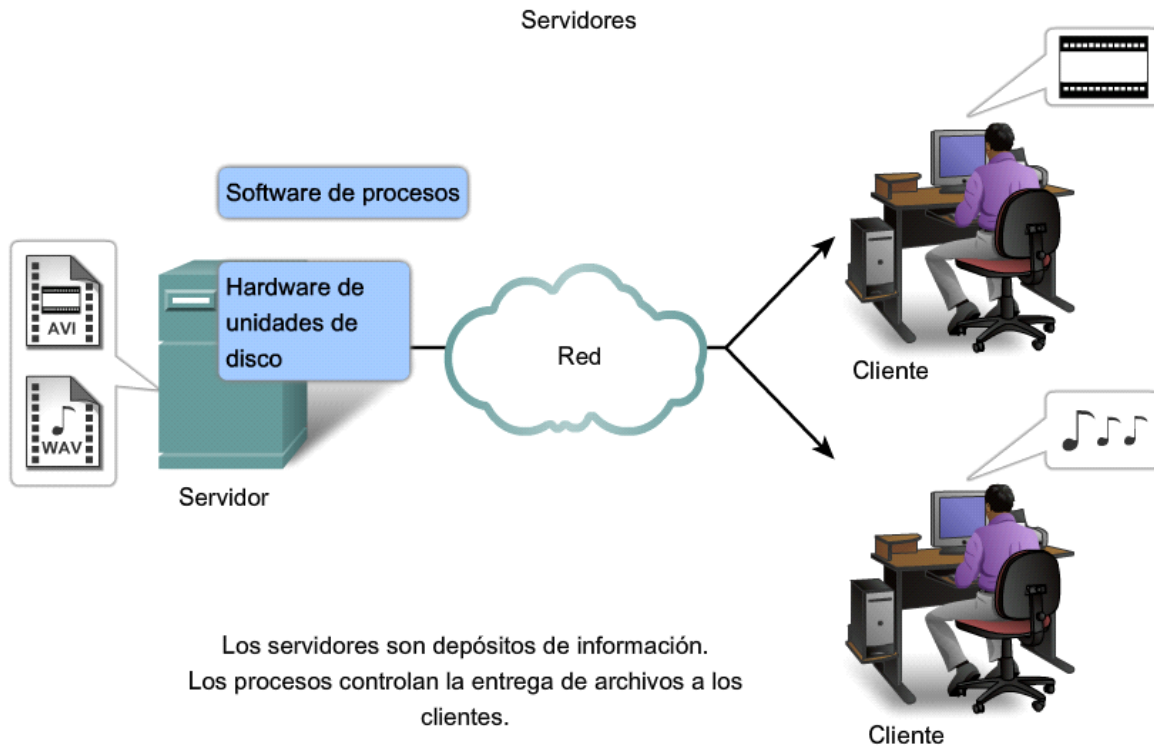
Las aplicaciones existentes en un servidor pueden tener controles de acceso por medio de claves. En este caso se tiene una lista centralizada de usuarios autorizados.

Una manera de acceso a los servidores es por medio del protocolo FTP, usualmente usado para la descarga de datos.

En un servidor usualmente funcionan procesos subyacentes(background) que no son prioritarios ni son controlados por el cliente.

Estos procesos son denominados demonios generalmente funcionan en un segundo plano.

Daemon: disk and execution monitor

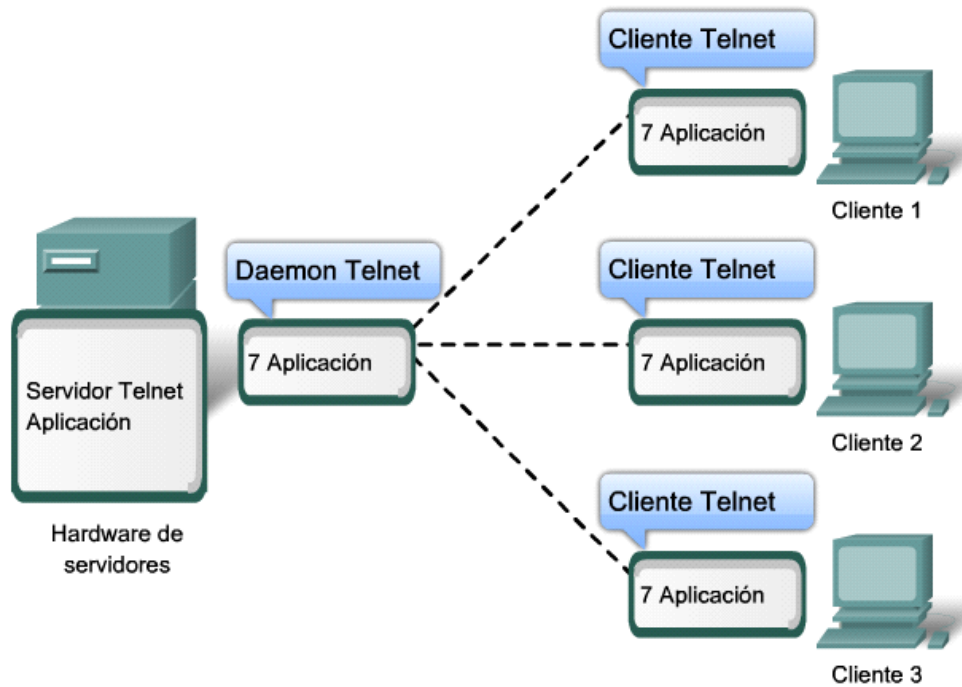


3.2.3 Servicios y protocolos de la capa de aplicación

Un usuario puede solicitar múltiples servicios a un servidor.

Un servidor puede tener múltiples clientes para el acceso a una determinada aplicación, como por ejemplo en el caso del protocolo Telnet.

Los procesos de servidores pueden admitir múltiples clientes.



3.3.1.1 Protocolos y servicios DNS

3.3.1.1 Protocolo y servicios de DNS.

La capa de transporte utiliza un esquema de direccionamiento llamado número de puerto.

El número de puerto identifica las aplicaciones y los servicios de la capa de aplicación que son el origen y el destino de los datos.

Los programas del servidor usualmente utilizan números de puertos predefinidos que usualmente son conocidos por los clientes.

Algunos de los números de puertos TCP y UDP asociados con los servicios son:

- Sistema de nombres de dominio (DNS): TCP/UDP puerto 53.
- Protocolo de transferencia de hipertexto (HTTP): TCP puerto 80.
- Protocolo simple de transferencia de correo (SMTP): TCP puerto 25.
- Protocolo de oficina de correos (POP) : TCP puerto 110.
- Telnet: TCP puerto 23.
- Protocolo de configuración dinámica de host (DHCP): UDP puertos 67 y 68.
- Protocolo de transferencia de archivos (FTP): TCP puertos 20 y 21.

DNS

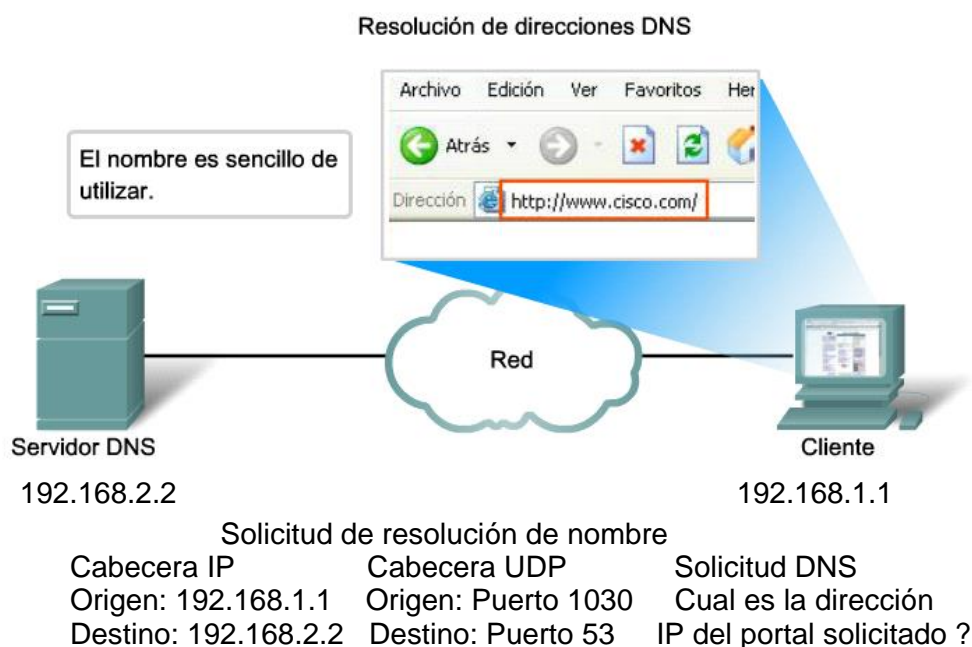
Convierte los nombres de dominio con una denominación sencilla y reconocible en direcciones numéricas IP.

El servidor puede cambiarse de ubicación con otra dirección numérica pero el nombre de dominio se mantiene.

DNS utiliza un conjunto de servidor distribuidos para la resolución del nombre de dominio con la dirección numérica.

Las comunicaciones del protocolo DNS utiliza un formato simple llamado mensaje, utilizado por los clientes para las consultas y por los servidores para las respuestas.

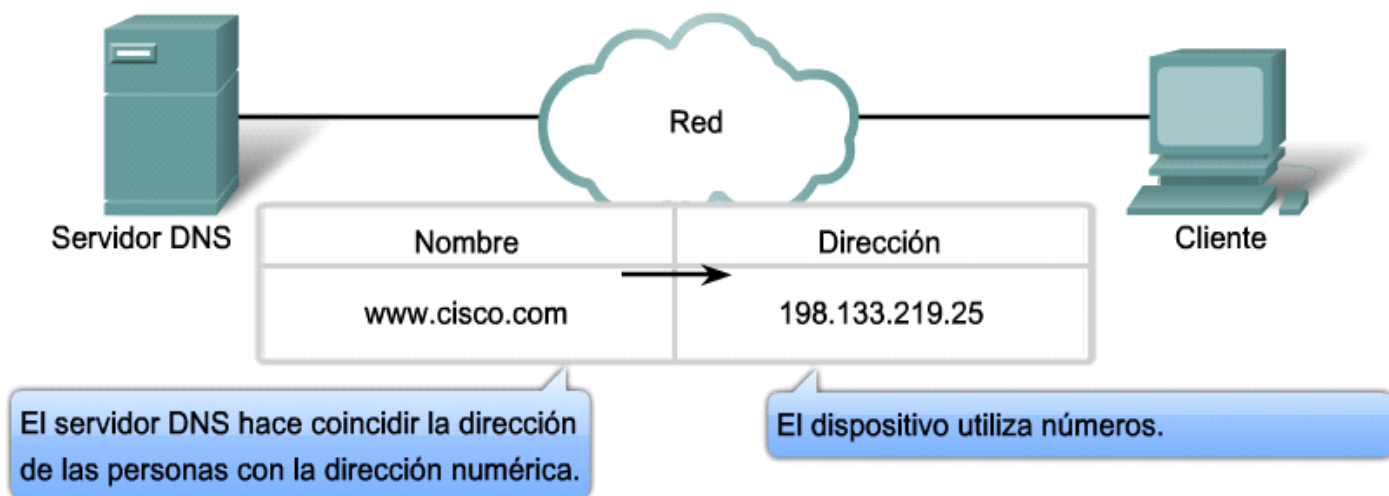
También ese formato lo utiliza para el intercambio de información entre servidores.



3.3.1.2 Protocolos y servicios DNS

Correspondencia entre el nombre de dominio y la dirección numérica IP.

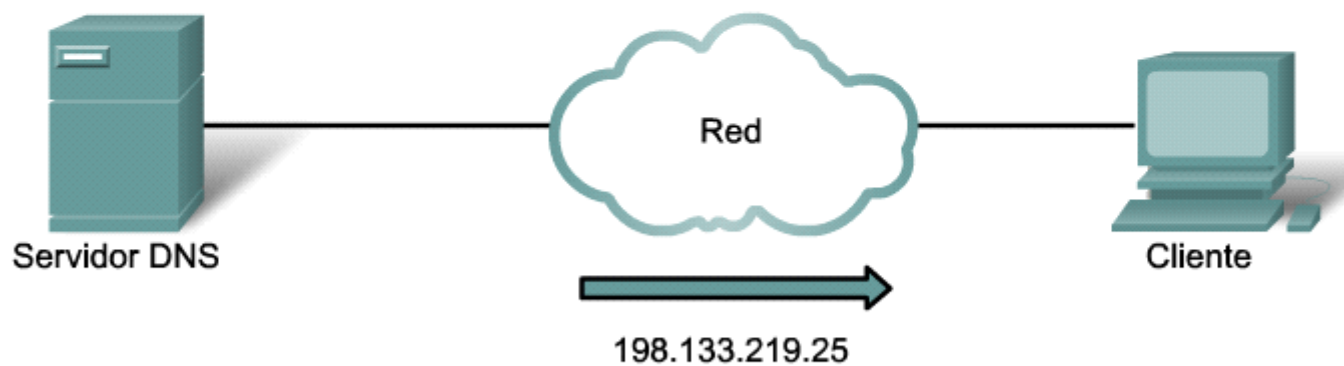
Resolución de direcciones DNS



3.3.1.3 Protocolos y servicios DNS

Respuesta del servidor

Resolución de direcciones DNS



El número se envía de regreso al cliente para su utilización en la realización de solicitudes del servidor.

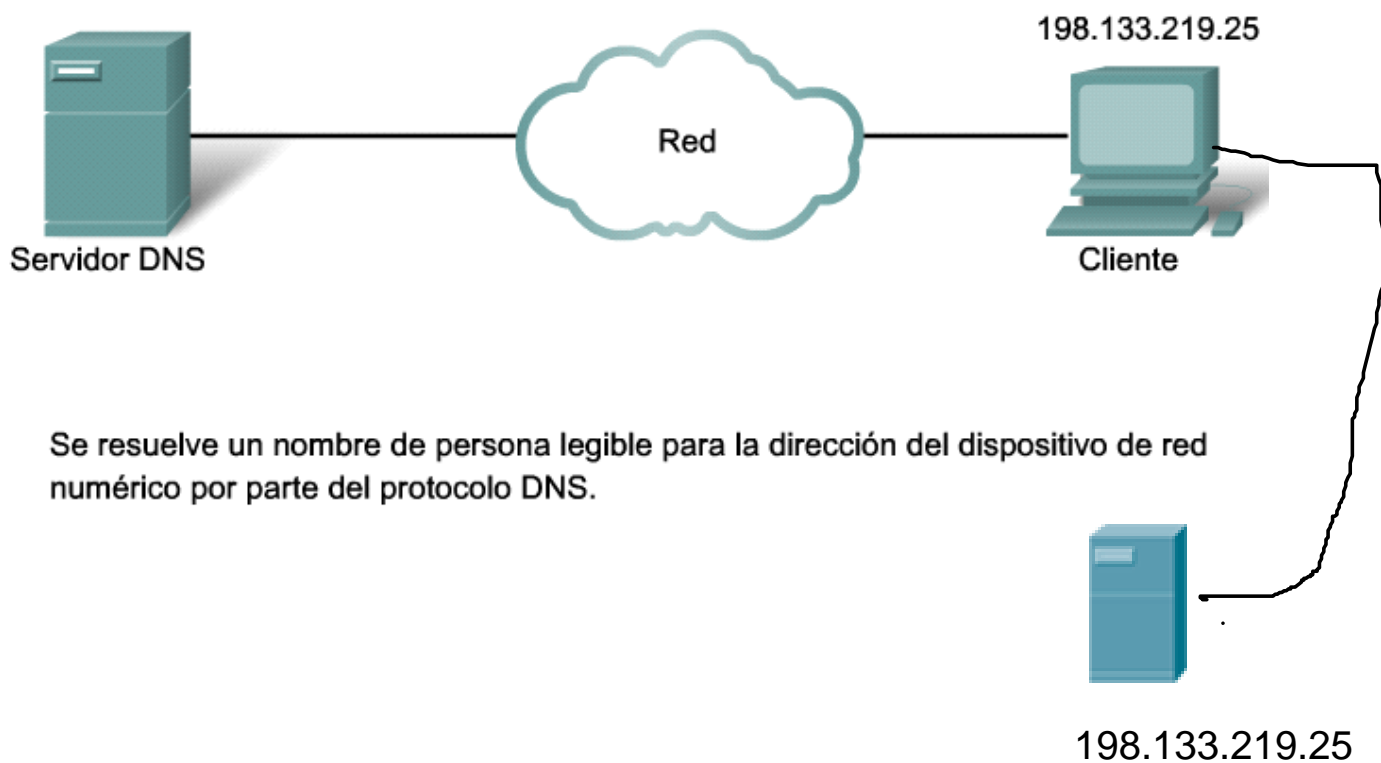
Respuesta de resolución de nombre

Cabecera IP	Cabecera UDP	Solicitud/respuesta DNS
Origen: 192.168.1.1	Origen: Puerto 1030	La dirección IP es
Destino: 192.168.2.2	Destino: Puerto 80	198.133.219.25

3.3.1.4 Protocolos y servicios DNS

Uso del número correspondiente a la dirección IP.

Resolución de direcciones DNS



Origen: 192.168.1.1	Origen: Puerto 1035
Destino: 198.133.219.25	Destino: Puerto 80 , SYN
Cabecera IP	Cabecera TCP

3.3.1.5 Protocolos y servicios DNS

El cliente DNS puede solicitar la resolución de nombres para diferentes aplicaciones de red que pueda estar utilizando.

Los equipos terminales de una misma red pueden acceder a diferentes DNS para la resolución de nombres.

Los proveedores de servicios de Internet pueden proporcionar servidores distribuidos para el servicio de DNS.

Cuando la aplicación del usuario solicita la conexión a un dispositivo servidor remoto por medio del nombre, el cliente DNS consulta uno de los servidores para resolver el nombre para una dirección numérica.

El servidor DNS traduce direcciones URL en direcciones binarias, lo cual le permite al cliente comunicarse con un servidor.

Algunas entidades disponen de uno o más servidores de DNS.

El comando `ipconfig /all` exhibe el listado de los servidores DNS en una red.

3.3.1.6 Protocolos y servicios DNS

Partes de un nombre de dominio

Un nombre de dominio consta de dos o más etiquetas separadas por puntos.

La longitud total de caracteres no debe exceder de 255.

A la etiqueta ubicada más hacia la derecha se le denomina dominio de nivel superior.

A la etiqueta contigua ubicada más a la izquierda se le denomina subdominio.

El subdominio expresa una dependencia relativa con respecto al dominio.

Ejemplo: www.berkeley.edu

Las etiquetas situadas más a la izquierda también se consideran subdominios con una descripción más exacta. Cada subdominio puede tener 127 niveles, con una longitud máxima de 63 caracteres en cada subdominio.

Ejemplo: www.unal.edu.co

En caso que hubiesen más etiquetas, la primera ubicada hacia la izquierda puede representar el nombre de un servidor.

Ejemplo: www.sia.unal.edu.co , www.virtual.unal.edu.co

El protocolo DNS está estructurado en un conjunto jerárquico de servidores. Cada dominio o subdominio tiene una ó más zonas de autoridad, que publican información acerca de los dominios y los nombres de servicios de cualquier dominio incluido.

Un servidor autoritativo contiene la información especificada en los campos de dominio ó subdominio.

Un servidor recursivo solicita información a otro servidor.

3.3.1.7 Protocolos y servicios DNS

El comando nslookup le permite a un cliente determinar el servidor DNS al cual está conectado.

```
C:\Documents and Settings\Cesar Lovera>nslookup
Servidor predeterminado: slnxdm4.unal.loc
Address: 168.176.5.148
```

Luego podemos escribir el nombre de dominio de un portal para conocer su dirección IP

```
C:\Documents and Settings\Cesar Lovera>nslookup
Servidor predeterminado: slnxdm4.unal.loc
Address: 168.176.5.148

> www.goodwill.com.tw
Servidor: slnxdm4.unal.loc
Address: 168.176.5.148

Respuesta no autoritativa:
Nombre: www.gwinstek.com.tw
Address: 59.120.26.35
Aliases: www.goodwill.com.tw

>
```

Con esta información es posible acceder al portal escribiendo directamente la dirección IP del portal de destino.

3.3.1.8 Protocolos y servicios de DNS

Si el servidor DNS no puede resolverlo, consulta a otros servidor DNS.

Esto ocasiona el consumo de ancho de banda en la red.

Si se encuentra la información solicitada, la respuesta se le devuelve al primer servidor. Este contenido queda almacenado temporalmente en el primer servidor para su re-utilización. Esto reduce el tráfico en la red.

El servicio de cliente en la DNS optimiza el rendimiento en la localización del destino solicitado.

Formato del mensaje DNS

DNS utiliza el mismo formato de mensaje para:

- **todos los tipos de consultas de clientes y respuestas de servidor**
- **mensajes de error**
- **la transferencia de información de registros de recursos entre servidores**

Encabezado

Pregunta

La pregunta para el servidor de nombres

Respuesta

Registros de recursos que responden la pregunta

Autoridad

Registros de recursos que apuntan a una autoridad

Adicional

Registros de recursos que poseen información adicional

3.3.1.9 Protocolos y servicios DNS

El servicio de cliente DNS mejora el rendimiento del protocolo por medio del almacenamiento de la información en la memoria temporal de la estación de trabajo. El comando `ipconfig /displaydns` exhibe las entradas vigentes.

```
informacion.quebuenacompra.com
-----
Nombre de registro . : informacion.quebuenacompra.com
Tipo de registro . . : 1
Período de vida . . . : 83006
Longitud de datos . . : 4
Sección . . . . . : respuesta
Un registro (host). . : 206.79.205.142

api.ipinfodb.com
-----
Nombre de registro . : api.ipinfodb.com
Tipo de registro . . : 1
Período de vida . . . : 357
Longitud de datos . . : 4
Sección . . . . . : respuesta
Un registro (host). . : 67.212.77.13

Nombre de registro . : api.ipinfodb.com
Tipo de registro . . : 1
Período de vida . . . : 357
Longitud de datos . . : 4
Sección . . . . . : respuesta
Un registro (host). . : 67.212.77.12

targetingservices.microsoft.com
-----
Nombre de registro . : targetingservices.microsoft.com
Tipo de registro . . : 1
Período de vida . . . : 1048
Longitud de datos . . : 4
Sección . . . . . : respuesta
Un registro (host). . : 65.55.56.119

s7.addthis.com
-----
Nombre de registro . : s7.addthis.com
Tipo de registro . . : 5
Período de vida . . . : 67
Longitud de datos . . : 8
Sección . . . . . : respuesta
Registro CNAME. . . : cs163.wac.edgecastcdn.net
```

3.3.1.10 Protocolos y servicios DNS

Algunas aplicaciones de clientes ejecutan un programa para la comunicación con el servidor. El cliente DNS se ejecuta por sí mismo, manualmente, cuando el usuario ingresa el nombre de la entidad con la cual desea conectarse.

Cuando se configura un dispositivo cliente, generalmente se configura una o más direcciones de servidores DNS.

La distribución jerárquica de los servidores está estructurado en la forma de un árbol invertido, con la raíz en la parte superior.

Los diferentes dominios de primer nivel representan algún tipo de organización o a los países. Ejemplo: .com, .org, .au, .co.

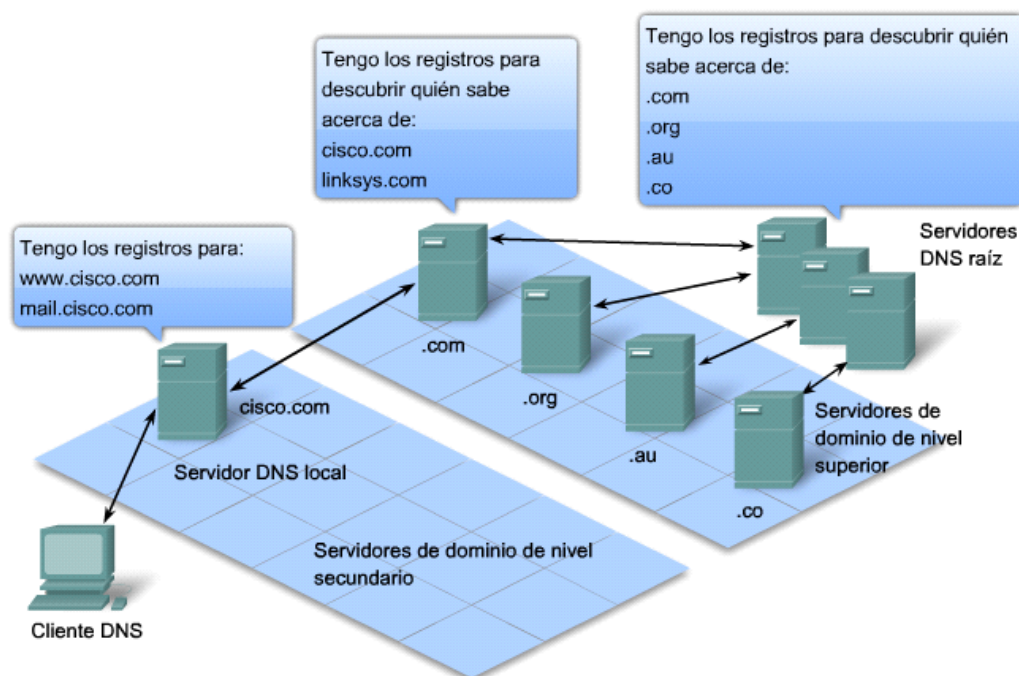
Usualmente los proveedores de servicios disponen de un conjunto de servidores DNS distribuidos para la resolución de nombres.

La búsqueda de la información se realiza desde los servidores de nivel superior hacia los servidores secundarios.

Cuando un servidor DNS no puede resolver la correspondencia entre un nombre y la dirección IP, el servidor envía la consulta a otros servidores.

El sistema de nombres de dominios utiliza un sistema jerárquico para la creación de una base de datos y proporcionar una resolución de nombres.

Si un servidor tiene registros de recursos que corresponden a su nivel en la jerarquía de dominios, se dice que es un servidor autoritativo para dichos registros.



Una jerarquía de servidores DNS contiene los registros de recursos que coordinan los nombres con las direcciones.

3.3.1.11 Protocolo DNS

Componentes de un sistema DNS

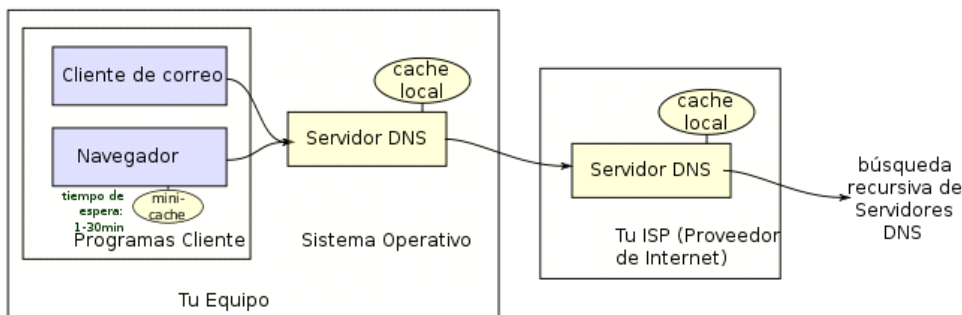
- Los clientes: un programa cliente DNS que se ejecuta en un host y genera peticiones de resolución de nombres a un servidor.
- Los servidores: contestan las peticiones a los clientes. Tienen la capacidad de enviar las peticiones a otros servidores en caso que no dispongan de la respuesta solicitada.
- Zonas de Autoridad: es una parte del espacio de los nombres de dominio sobre la cual es responsable un servidor DNS, que puede tener autoridad sobre varias zonas.
Ejemplo: direcciones .com, .net, .org ect.

3.3.1.12 Protocolo DNS

Funcionamiento del protocolo DNS

Los usuarios generalmente no se comunican directamente con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por ejemplo, navegadores, clientes de correo y otras aplicaciones que usan Internet). Al realizar una petición que requiere una búsqueda de DNS, la petición se envía al servidor DNS local del sistema operativo. El sistema operativo, antes de establecer alguna comunicación, comprueba si la respuesta se encuentra en la memoria temporal. En el caso de que no se encuentre, la petición se enviará a uno o más servidores DNS.

La mayoría de usuarios domésticos utilizan como servidor DNS el proporcionado por el proveedor de servicios de Internet. La dirección de estos servidores puede ser configurada de forma manual o automática mediante el protocolo DHCP. En otros casos, los administradores de red tienen configurados sus propios servidores DNS.



3.3.2.1 Servicio WWW y HTTP

El explorador web es una aplicación cliente que utilizan los equipos terminales para comunicarse con la World Wide Web y acceder a los recursos almacenados en un servidor web.

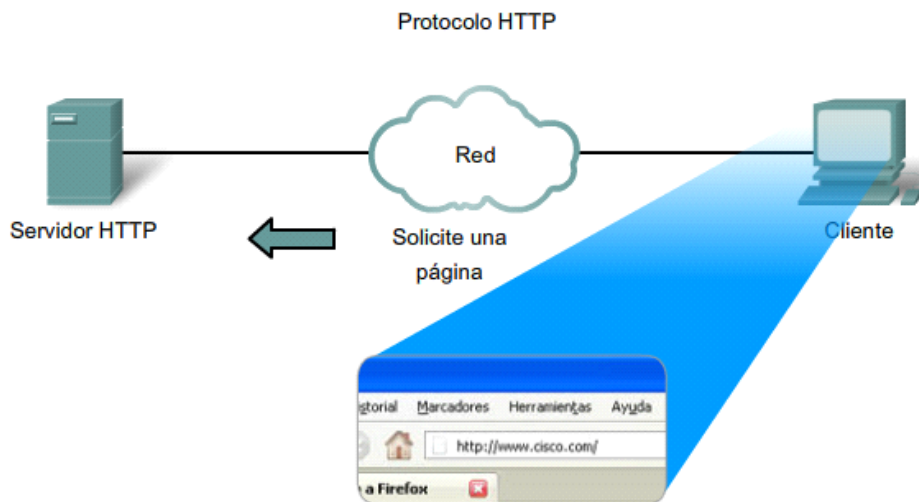
Para acceder al contenido, los clientes web realizan conexiones al servidor y solicitan los recursos deseados. El servidor responde con el recurso y el explorador interpreta el contenido recibido.

Los buscadores o exploradores pueden interpretar los datos recibidos los cuales vienen en un lenguaje. Uno de ellos es el HTML. Otros recursos se reciben en forma de complementos o plug-in.

El explorador interpreta las partes del mensaje recibido. Ejemplo

<http://www.empresa.com/index.htm>

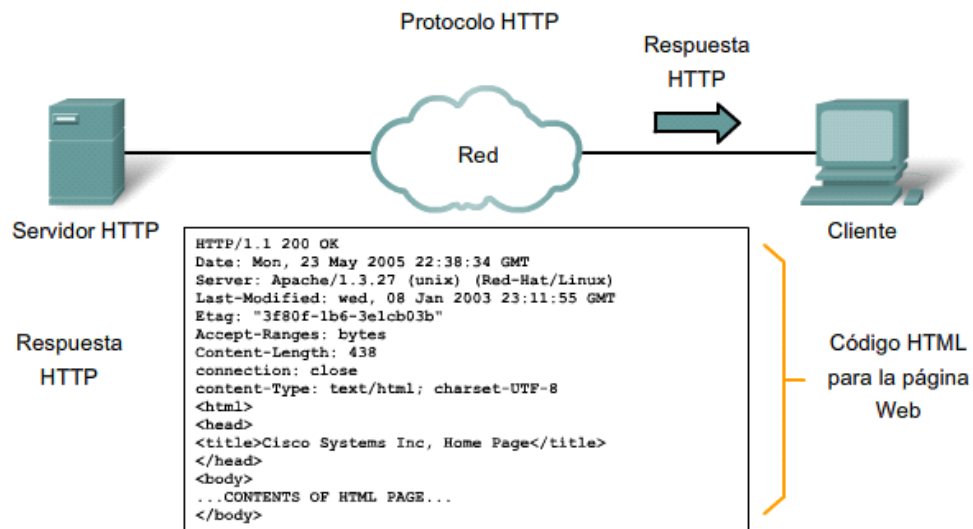
- Http: el nombre del protocolo
- www.empresa.com: el nombre del servidor.
- Index.htm : es el nombre del directorio o carpeta donde reside el recurso.



3.3.2.2 Servicio WWW y HTTP

El explorador envía una solicitud GET.

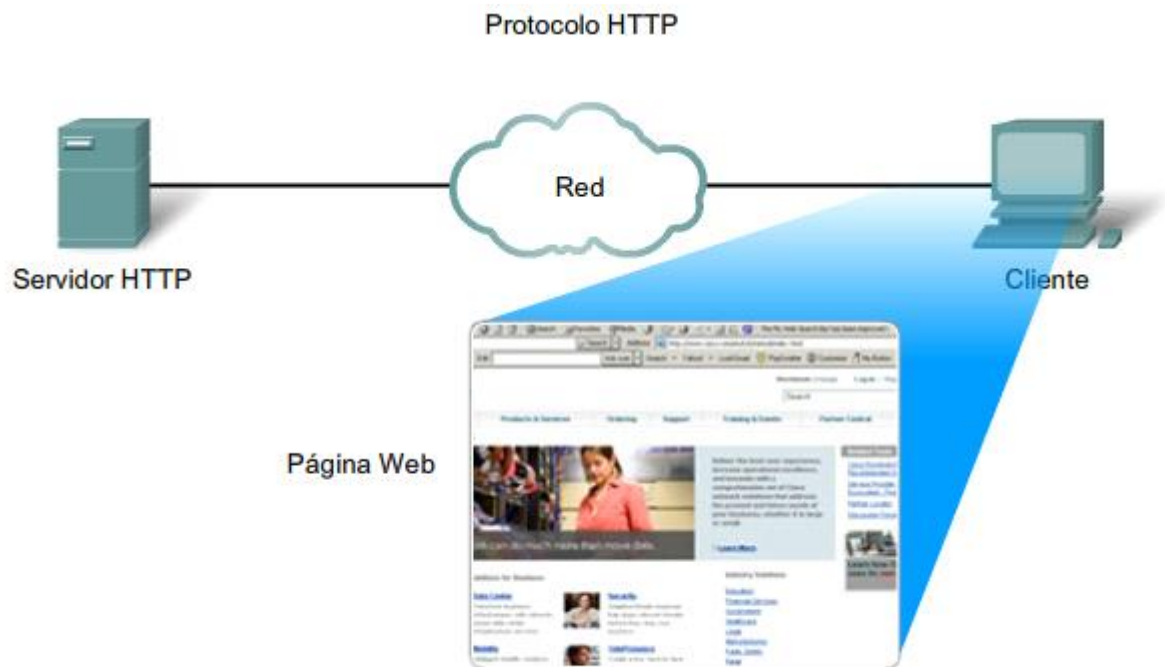
El servidor contesta con una secuencia de bits correspondiente al contenido en el servidor.



En respuesta a la solicitud, el servidor HTTP envía el código para una página Web.

3.3.2.3 Servicio WWW y HTTP

El cliente interpreta el contenido recibido y lo presenta al usuario.



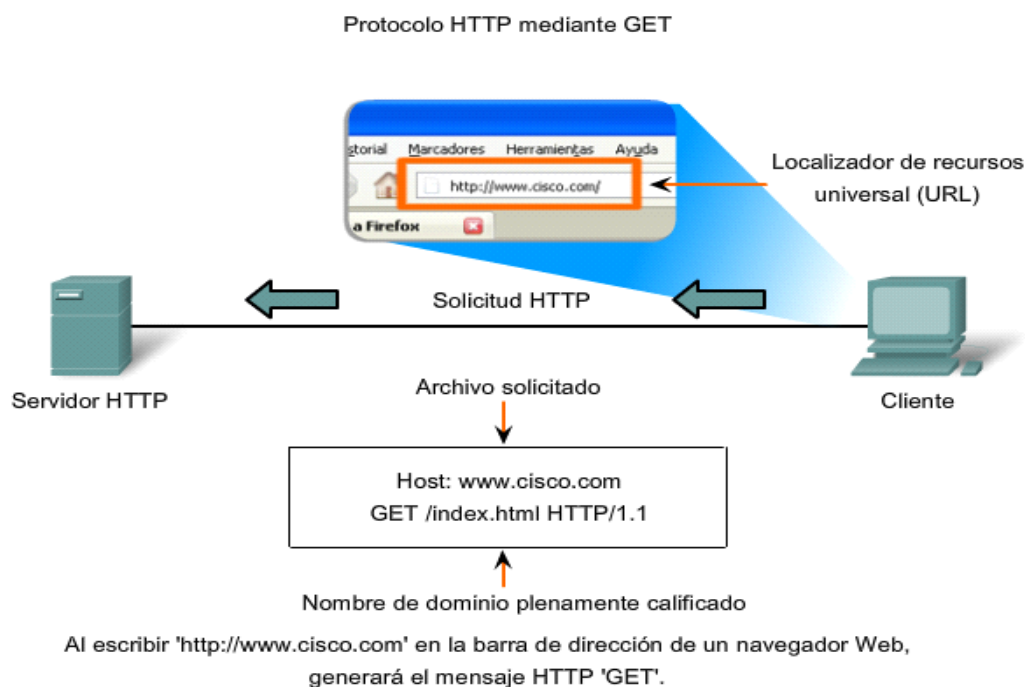
El navegador interpreta el código HTML y muestra una página Web.

3.3.2.4 Servicio WWW y HTTP

HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

Es muy común encontrar el prefijo "WWW" al comienzo de las direcciones web debido a la costumbre de nombrar a los host de Internet, los servidores, con los servicios que proporcionan. De esa forma, por ejemplo, el nombre de host para un servidor web normalmente es "WWW" y para un servidor FTP se suele usar "ftp".

HTTP especifica un protocolo de solicitud/respuesta. Cuando un cliente, generalmente un explorador Web, envía un mensaje de solicitud a un servidor, el protocolo HTTP define los tipos de mensajes que el cliente utiliza para solicitar la página Web y envía los tipos de mensajes que el servidor utiliza para responder.



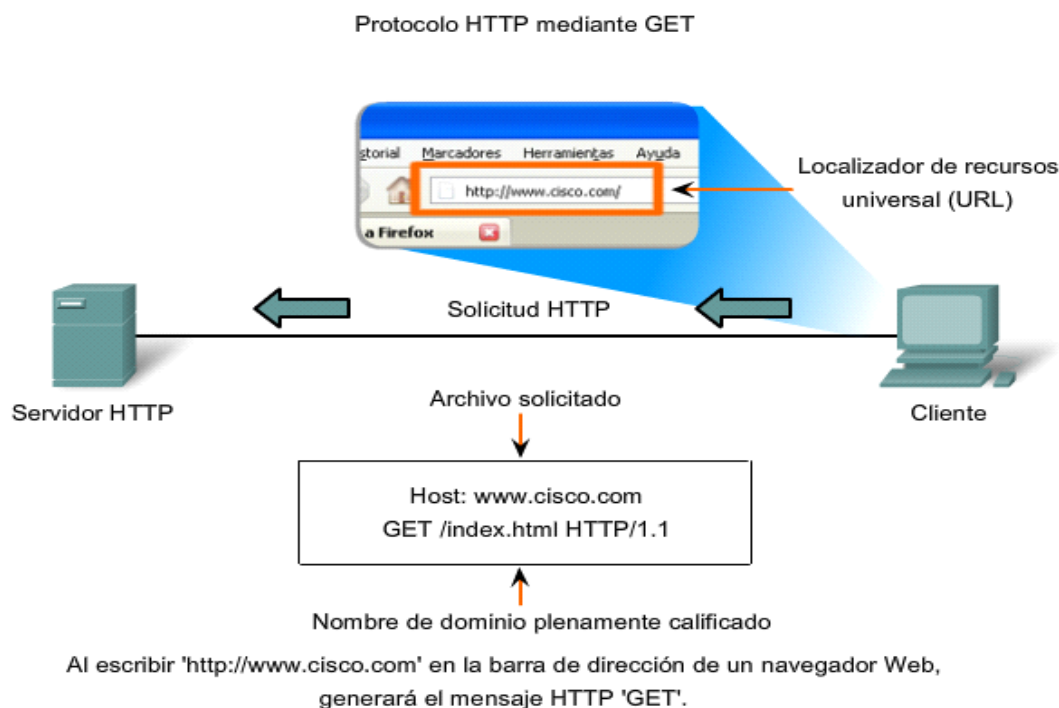
3.3.2.5 Servicio WWW y HTTP

Los tres tipos de mensajes comunes son GET, POST y PUT.

GET es una solicitud de datos por parte del cliente. Un explorador Web envía el mensaje GET para solicitar las páginas desde un servidor Web. Como se muestra en la figura, una vez que el servidor recibe la solicitud GET, responde con una línea de estado, como HTTP/1.1 200 OK, y un mensaje propio, el cuerpo del cual puede ser el archivo solicitado, un mensaje de error u otra información.

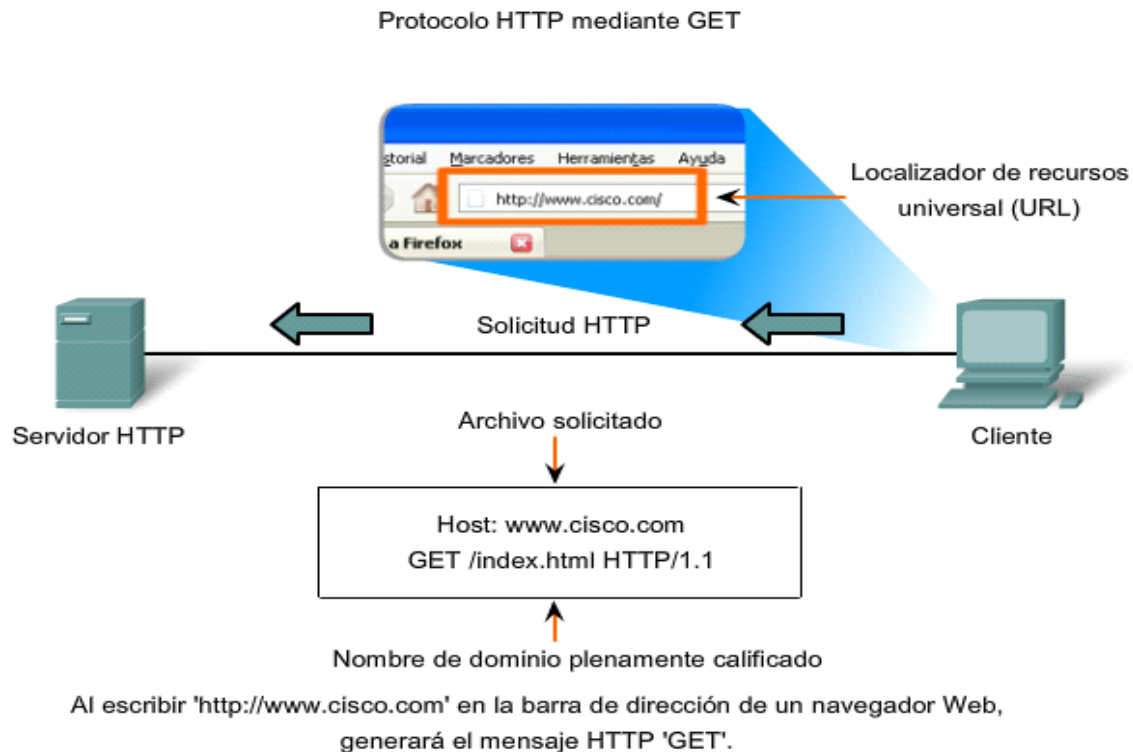
El comando POST permite el envío de los datos al servidor por ejemplo en un formulario. Estos datos son ocultos porque no son accesibles al cliente.

Permite transferir un archivo desde la maquina local hasta la maquina remota. El archivo_remoto es el nombre del archivo con el que desea que aparezca la transferencia, si no da este, lo transferirá con el mismo nombre del archivo_local.



3.3.2.6 Servicio WWW y HTTP

Para una comunicación segura a través de Internet, se utiliza el protocolo HTTP seguro (HTTPS) para acceder o subir información al servidor Web. HTTPS puede utilizar autenticación y encriptación para asegurar los datos cuando viajan entre el cliente y el servidor. HTTPS especifica reglas adicionales para pasar los datos entre la capa de aplicación y la capa de transporte.



3.3.2.7 Códigos de estado HTTP

En el proceso de acceso de un cliente a un servidor HTTP, el servidor puede emitir numerosos mensajes de estado o de servicio que están relacionados con el acceso a una aplicación. El primer dígito del código de respuesta indica una de las cinco clases de estados. Entre ellos se tiene

4xx: Errores del cliente.

HTTP 400 - Sintaxis incorrecta. La dirección URL tiene algún carácter erróneo.

HTTP 403 - Acceso denegado. La página solicitada existe. Podría tratarse de un contenido exclusivo para usuarios registrados.

HTTP 404 - No encontrado. La página que se está tratando de cargar no ha sido encontrada, carga a través de un enlace erróneo o la página existió anteriormente.

HTTP 406 - Código no interpretado por el navegador. La página devolvió un código no interpretable por el navegador.

3.3.2.8 Códigos de estado HTTP

5xx. Errores del servidor. Pueden generarse por un error en el código de la página web o dentro del propio servidor.

HTTP 500 - Error interno. la página web tiene algún error en el código, por lo que el servidor no puede generar el código HTML para devolver al usuario.

HTTP 504 - tiempo de espera para devolver la página web se ha agotado. Puede estar generado por un error en el propio servidor o porque la página web contiene algún código que nunca termina de ejecutarse.

HTTP 509 - Se ha superado el límite del ancho de banda disponible. Existe una limitación en el número de datos que el servidor puede devolver a los clientes.

Estos son algunos de los códigos de estado para el protocolo HTTP.

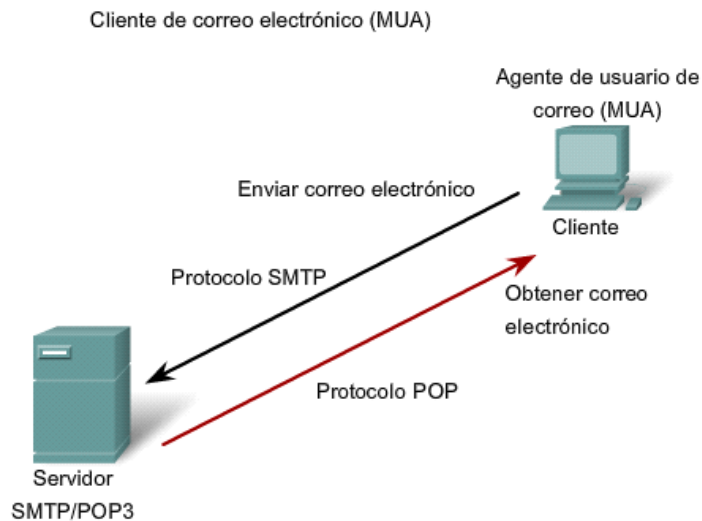
3.3.3.1 Servicios de correo electrónico y protocolos SMTP/POP3

Cuando el usuario accede a la aplicación del correo electrónico accede a una aplicación denominada agente de usuario de correo MUA en el cliente, el cual le permite la lectura o redacción del mensaje.

Los clientes envían mensajes de correo electrónico al servidor mediante el protocolo SMTP, puerto 25.

El servidor le envía el mensaje al cliente mediante el protocolo POP3, puerto 110.

El correo se entrega a un servidor donde funciona el MDA.



Los clientes envían correo electrónico a un servidor mediante SMTP y reciben correo electrónico mediante POP3.

3.3.3.2 Servicios de correo electrónico y protocolos SMTP/POP3

El servidor de correo electrónico utiliza dos procesos independientes: MTA y MDA.

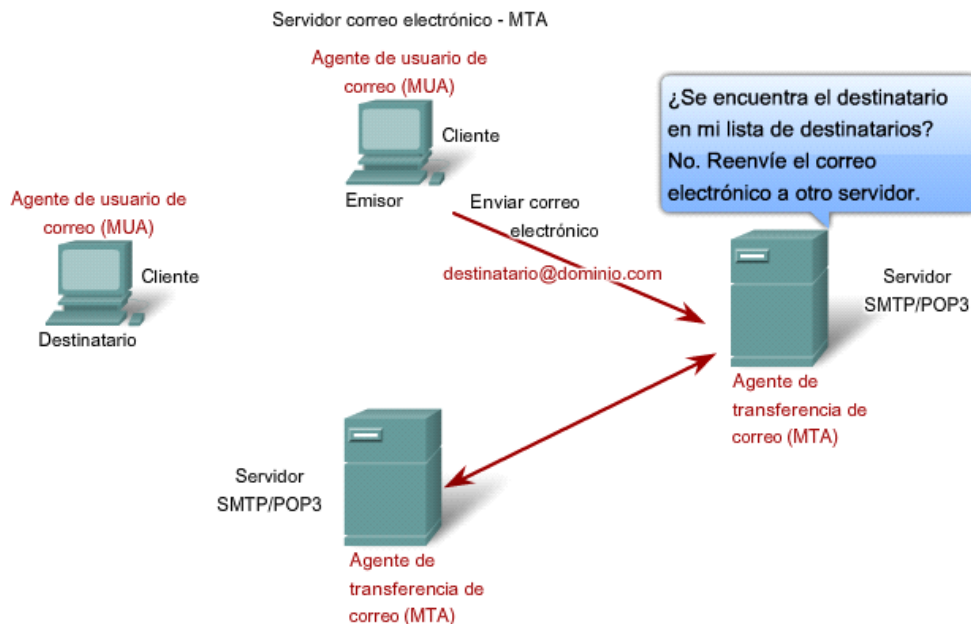
- MTA: el proceso Agente de Transferencia de Correo se utiliza para enviar correo electrónico. El MTA recibe los correos desde el MUA u otro MTA localizado en otro servidor de correo electrónico.

Durante la transferencia de mensajes entre dos servidores se presenta:

- El MTA que envía el correo es cliente del MTA receptor.
- El MTA que recibe el correo es servidor del MTA que envía el correo.

Si el correo electrónico es para un usuario cuyo buzón está en el servidor local, el correo se pasa al MDA.

Si el correo es para un usuario que no está en el servidor local, el MTA re-envía el correo electrónico al MTA en el servidor correspondiente.



El proceso de agente de transferencia de correo rige el manejo de correo electrónico entre servidores.

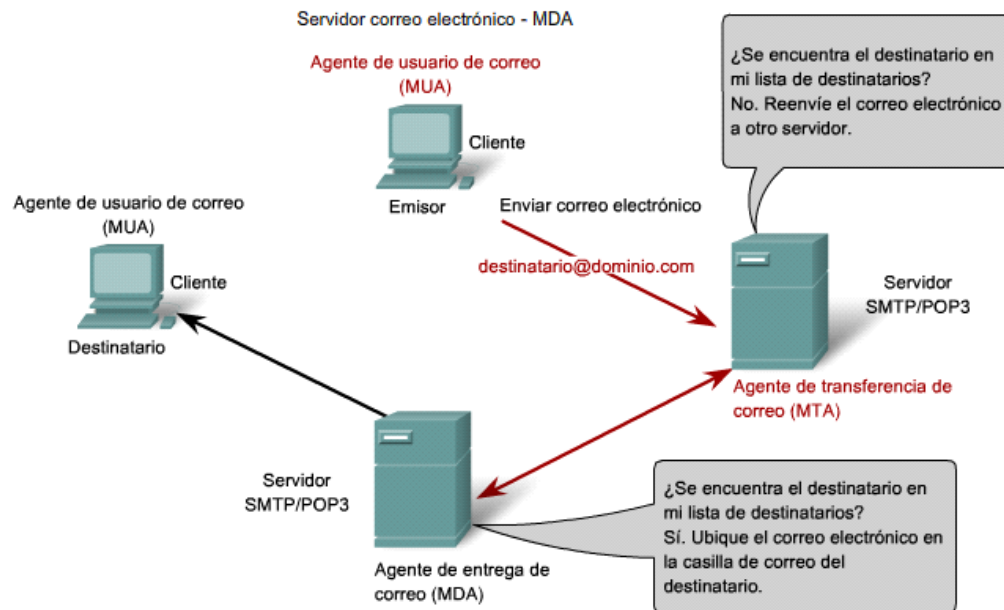
3.3.3.3 Servicios de correo electrónico y protocolos SMTP/POP3

Un servidor entrega el correo a un subscriptor por medio del MDA.

El MDA recibe y coloca en los buzones de los usuarios los correos electrónicos procedentes de los MTA.

El MDA puede resolver algunos casos como eliminación de virus, acuses de recibo, correo no deseado etc.

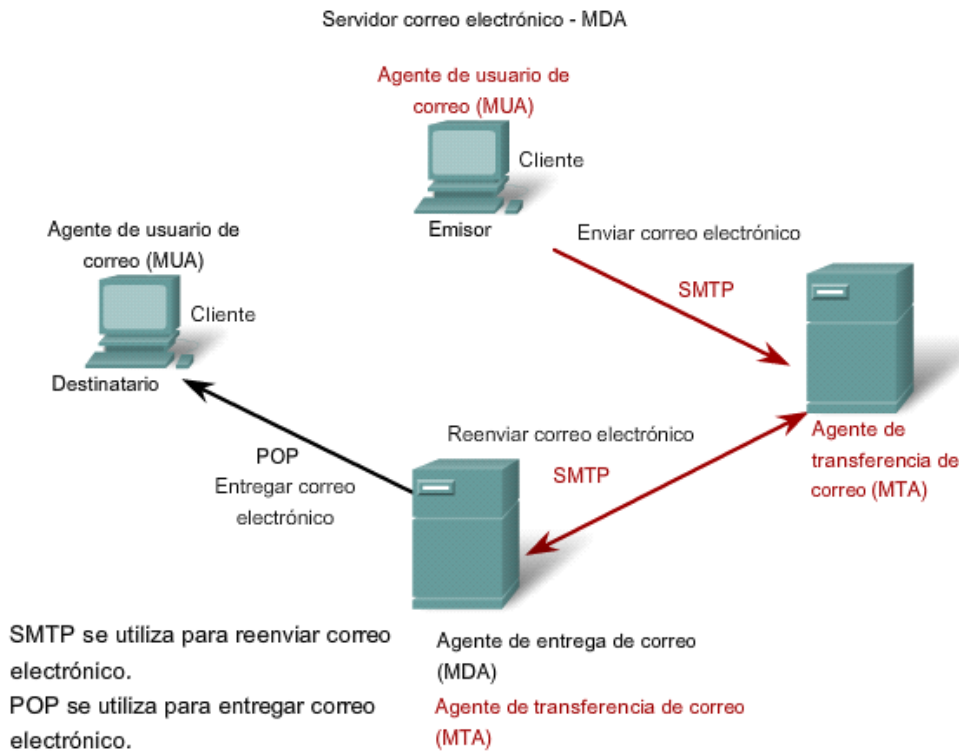
Las computadoras que no tengan el MUA instalado pueden conectarse a un servidor de correo por medio del protocolo HTTP para el envío y recepción de sus mensajes.



El proceso de agente de entrega de correo rige la entrega de correo electrónico entre servidores y clientes.

3.3.3.4 Servicios de correo electrónico y protocolos SMTP/POP3

POP3 es un protocolo de envío de correos desde el servidor hacia el cliente. El MDA detecta la conexión del cliente y procede a enviarle el correo electrónico. El MTA transporta el correo saliente desde el cliente hacia el servidor. El protocolo SMTP permite el intercambio de correos electrónico entre servidores con diferentes plataformas de correo electrónico y sistemas operativos. El proceso MTA se encarga de la transferencia de correos entre servidores.



3.3.3.5 Servicios de correo electrónico protocolo IMAP

Protocolo usado para la lectura de los mensajes de correo.

Es otra alternativa con relación al protocolo POP.

El protocolo IMAP

- Permite la lectura de los mensajes en línea, no es necesario descargarlo en el equipo cliente.
- Permite la configuración de carpetas en el servidor para la clasificación de los mensajes recibidos.
- Si se pierde la conexión con la red, no es posible la lectura de los mensajes recibidos.
- Es posible realizar algunas funciones en el servidor: eliminación, clasificación, respuesta al remitente, etc.
- Permite el acceso al correo desde cualquier dispositivo que tenga acceso a la red.
- Funcionamiento sincronizado independientemente desde donde acceda al servidor. Si un mensaje fue borrado desde un cliente, ese mensaje no vuelve a presentarse cuando se acceda desde otro cliente.
- Confidencialidad: el mensaje leído no queda almacenado en el cliente.

El envío del correo siempre se efectúa por medio del SMTP. Los clientes pueden ser POP3 o IMAP.

3.3.4 FTP

El FTP es una aplicación que permite la transferencia de archivos entre un cliente y un servidor.

Un cliente FTP es una aplicación que descarga archivos desde un servidor y carga archivos hacia un servidor.

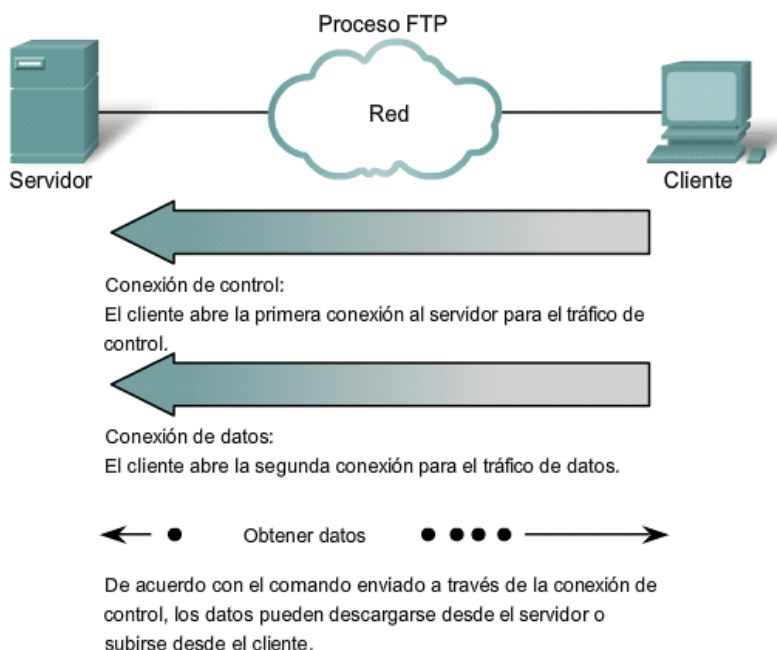
El FTP necesita dos conexiones para una transferencia de archivos en forma exitosa. Una conexión para comandos y respuestas. Otra conexión para la transferencia del archivo.

El cliente establece la primera conexión con el servidor TCP puerto 21. En esta conexión se ejecutan los comandos del cliente y las respuestas del servidor.

El cliente establece la segunda conexión con el servidor TCP puerto 20 para la transferencia del archivo. La transferencia puede ser bidireccional.

El cliente puede descargar (bajar) archivos desde el servidor.

El cliente puede cargar (subir) archivos hacia el servidor.



3.3.5.1 DHCP

El protocolo de configuración dinámica de host le permite a los dispositivos de red obtener asignaciones de direcciones IP y otras informaciones de un servidor DHCP. Este servicio automatiza la asignación dinámica de direcciones IP, máscaras de subred y puertas de entrada (gateways) en una red.

También proporciona las direcciones de los servidores DNS.

El servidor asigna la dirección IP por un tiempo determinado.

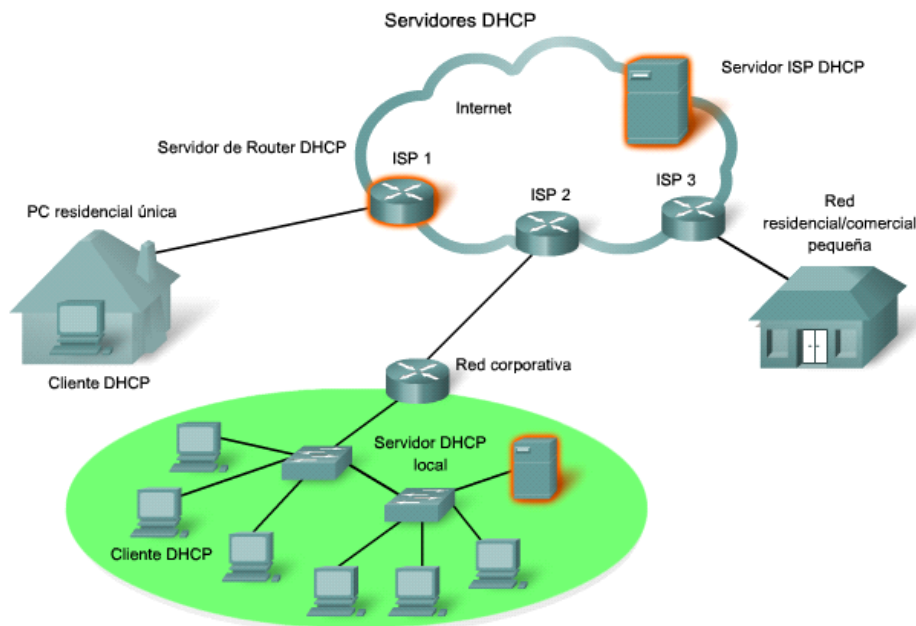
Este procedimiento es útil en las redes medianas o grandes donde existe movilidad con los equipos. Muchos usuarios se conectan con sus equipos portátiles donde el cliente DHCP se conecta al servidor DHCP y solicita la asignación de una dirección IP.

Las direcciones asignadas regresan al servidor cuando el host se desconecta de la red y para su posterior reasignación.

Para los clientes residenciales, el ISP dispone de un DHCP para la asignación de direcciones.

Este procedimiento implica un riesgo para una entidad en la cual cualquier equipo puede tener asignada una dirección IP de la empresa.

La asignación de direcciones IP por DHCP está dirigida hacia los hosts. Algunos dispositivos que cumplen determinadas funciones deben tener una dirección fija o estática como una impresora, un gateway ect.



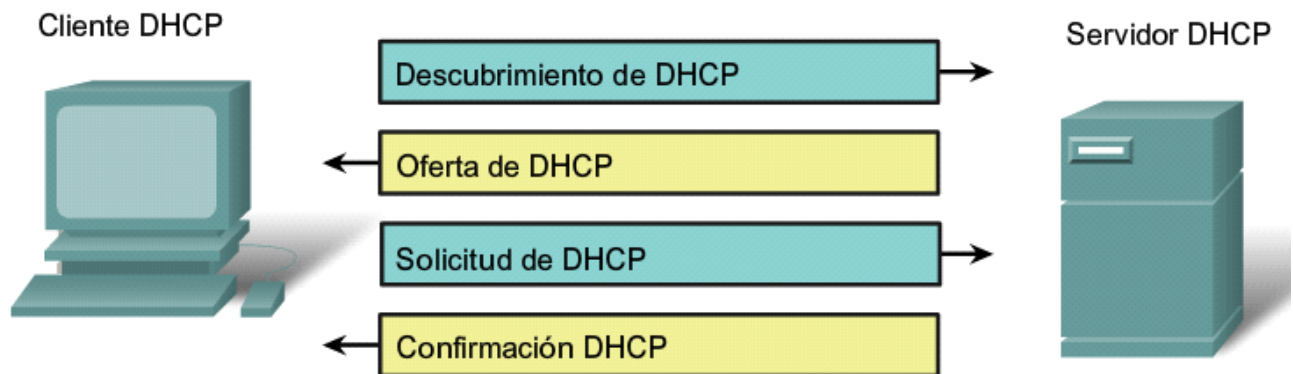
3.3.5.2 DHCP - Asignación de una dirección IP

Descubrimiento DHCP

Cuando el cliente enciende el equipo no tiene una dirección IP.

El equipo terminal del cliente envía un paquete DHCPDISCOVER con destino a la dirección de difusión 255.255.255.255 y con origen 0.0.0.0, dirigido al puerto 67.

El mensaje contiene un identificador de transacción, de manera que el cliente pueda relacionar la respuesta del servidor con su solicitud. El identificador del cliente usualmente es la dirección MAC.



Proceso de 4 Pasos

0.0.0.0 no existe en ninguna red.

El mensaje se envía a todos los dispositivos solicitando una dirección

.3.5.3 DHCP - Asignación de una dirección IP

Descubrimiento DHCP

En la gráfica inferior se presenta un ejemplo de una simulación de Descubrimiento de DHCP.

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 77			
ID: 0x20			0x0	0x0		
TTL: 128		PRO: 0x11	CHKSUM			
SRC IP: 0.0.0.0						
DST IP: 255.255.255.255						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

UDP

0	16	31	Bits
SRC PORT: 68		DEST PORT: 67	
LENGTH: 0x39		CHECKSUM: 0x0	
DATA (VARIABLE)			

DHCP

0	8	16	31	Bits
OP: 0x1	HW TYPE	HW LEN	HOPS	
TRANSACTION ID (4 BYTES)				
SECS		FLAGS		
CLIENT ADDRESS: 0.0.0.0				
"YOUR" CLIENT ADDRESS: 0.0.0.0				
SERVER ADDRESS: 0.0.0.0				
RELAY AGENT ADDRESS: 0.0.0.0				
CLIENT HARDWARE ADDRESS: 0002.17B4.D442				
SERVER HOSTNAME (64 BYTES)				
FILE (128 BYTES)				
OPTIONS (312 BYTES)				

3.3.5.4 DHCP - Asignación de una dirección IP

Oferta DHCP

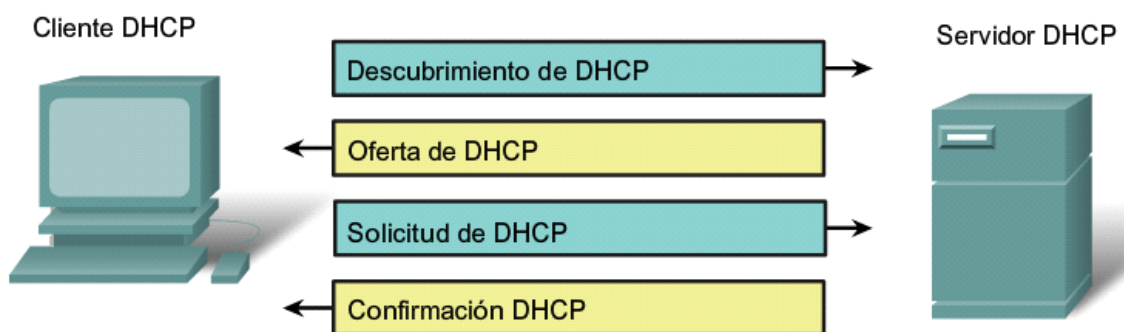
El servidor contesta con un paquete DHCPOFFER dirigido a la dirección de difusión 255.255.255.255 con el mismo identificador de transacción que el mensaje de descubrimiento. El servidor ofrece una dirección IP, una máscara de subred, una dirección de puerta de acceso predeterminada (gateway), una dirección del servidor DNS y el tiempo de concesión de acceso a la red o validez de la dirección IP.

Múltiples servidores DHCP pudieron haber contestado con el paquete DHCPOFFER.

El cliente contesta con un paquete DHCPREQUEST dirigido a la dirección de difusión 255.255.255.255, en la cual le solicita a uno de los servidores la asignación de la dirección IP.

Hasta este momento el cliente no tiene asignado la dirección IP. Se envía en el modo de difusión en caso que más de un servidor haya contestado.

El servidor contesta con un paquete DHCPACK dirigido a la dirección de difusión 255.255.255.255. La dirección IP asignada está contenida en este paquete.



3.3.5.5 DHCP - Asignación de una dirección IP

Oferta DHCP

En la gráfica inferior se exhibe un ejemplo de la respuesta de Oferta de DHCP de un servidor.

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 81			
ID: 0x36			0x0	0x0		
TTL: 128		PRO: 0x11	CHKSUM			
SRC IP: 192.168.1.241						
DST IP: 255.255.255.255						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

UDP

0	16	31	Bits
SRC PORT: 67		DEST PORT: 68	
LENGTH: 0x3d		CHECKSUM: 0x0	
DATA (VARIABLE)			

DHCP

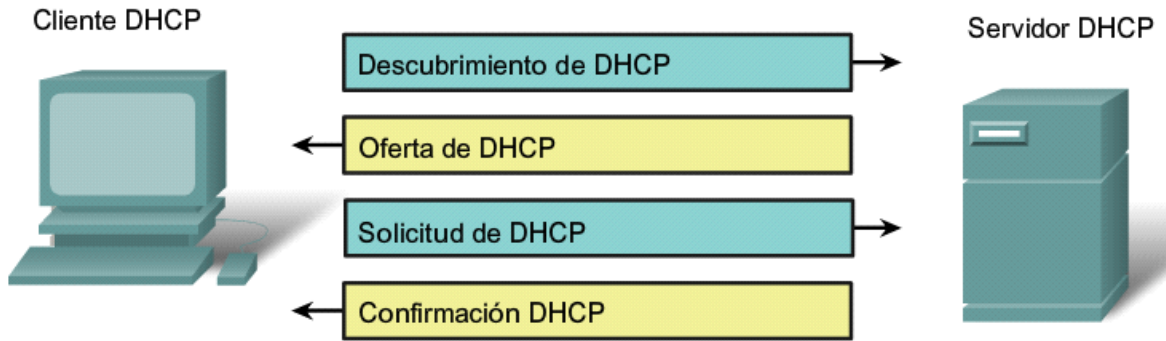
0	8	16	31	Bits
OP: 0x2	HW TYPE	HW LEN	HOPS	
TRANSACTION ID (4 BYTES)				
SECS		FLAGS		
CLIENT ADDRESS: 0.0.0.0				
"YOUR" CLIENT ADDRESS: 192.168.1.2				
SERVER ADDRESS: 192.168.1.241				
RELAY AGENT ADDRESS: 0.0.0.0				
CLIENT HARDWARE ADDRESS: 0002.17B4.D442				
SERVER HOSTNAME (64 BYTES)				
FILE (128 BYTES)				
OPTIONS (312 BYTES)				

.3.5.6 DHCP - Asignación de una dirección IP

Solicitud DHCP

El cliente contesta con un paquete DHCPREQUEST dirigido a la dirección de difusión 255.255.255.255, en la cual le solicita a uno de los servidores la asignación de la dirección IP. Hasta este momento el cliente no tiene asignado la dirección IP. Se envía en el modo de difusión en caso que más de un servidor haya contestado.

Este mensaje contiene los mismos parámetros que el mensaje de oferta de DHCP.



3.3.5.7 DHCP - Asignación de una dirección IP

Solicitud DHCP

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 77			
ID: 0x21			0x0	0x0		
TTL: 128		PRO: 0x11	CHKSUM			
SRC IP: 0.0.0.0						
DST IP: 255.255.255.255						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

UDP

0	16	31	Bits
SRC PORT: 68		DEST PORT: 67	
LENGTH: 0x39		CHECKSUM: 0x0	
DATA (VARIABLE)			

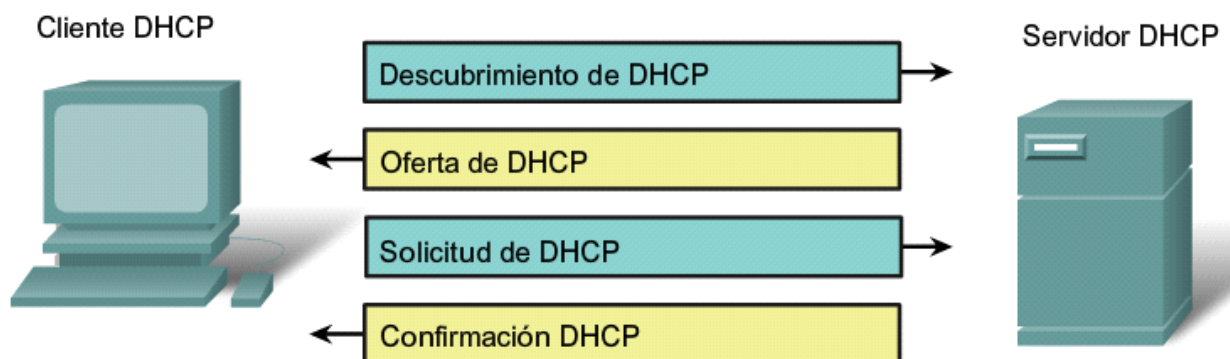
DHCP

0	8	16	31	Bits
OP: 0x1	HW TYPE	HW LEN	HOPS	
TRANSACTION ID (4 BYTES)				
SECS		FLAGS		
CLIENT ADDRESS: 0.0.0.0				
"YOUR" CLIENT ADDRESS: 192.168.1.2				
SERVER ADDRESS: 192.168.1.241				
RELAY AGENT ADDRESS: 0.0.0.0				
CLIENT HARDWARE ADDRESS: 0002.17B4.D442				
SERVER HOSTNAME (64 BYTES)				
FILE (128 BYTES)				
OPTIONS (312 BYTES)				

3.3.5.8 DHCP - Asignación de una dirección IP

Confirmación DHCP

El servidor contesta con un paquete DHCACK dirigido a la dirección de difusión 255.255.255.255. Este mensaje contiene el mismo conjunto de parámetros que han sido intercambiados en los mensaje anteriores.



3.3.5.9 DHCP - Asignación de una dirección IP

Confirmación DHCP

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 81			
ID: 0x37			0x0	0x0		
TTL: 128		PRO: 0x11	CHKSUM			
SRC IP: 192.168.1.241						
DST IP: 255.255.255.255						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

UDP

0	16	31	Bits
SRC PORT: 67		DEST PORT: 68	
LENGTH: 0x3d		CHECKSUM: 0x0	
DATA (VARIABLE)			

DHCP

0	8	16	31	Bits
OP: 0x2		HW TYPE	HW LEN	HOPS
TRANSACTION ID (4 BYTES)				
SECS		FLAGS		
CLIENT ADDRESS: 0.0.0.0				
"YOUR" CLIENT ADDRESS: 192.168.1.2				
SERVER ADDRESS: 192.168.1.241				
RELAY AGENT ADDRESS: 0.0.0.0				
CLIENT HARDWARE ADDRESS: 0002.17B4.D442				
SERVER HOSTNAME (64 BYTES)				
FILE (128 BYTES)				
OPTIONS (312 BYTES)				

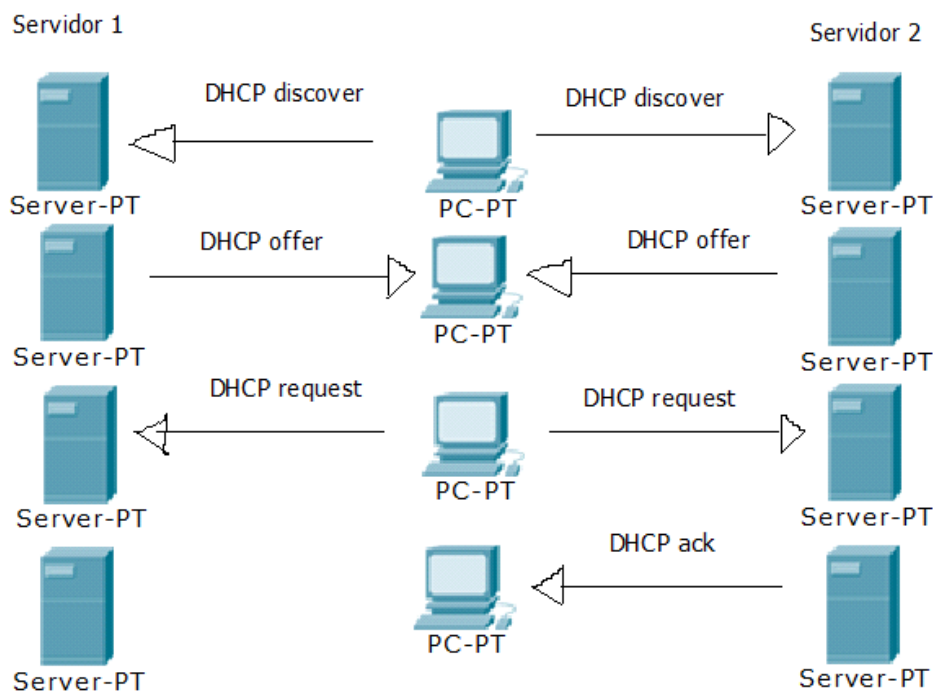
3.3.5.10 DHCP

Tabla de resumen del intercambio de direcciones

Source MAC addr	Dest MAC addr	Source IP addr	Dest IP addr	Packet Description
Client	Broadcast	0.0.0.0	255.255.255.255	DHCP Discover
DHCPsrvr	Broadcast	DHCPsrvr	255.255.255.255	DHCP Offer
Client	Broadcast	0.0.0.0	255.255.255.255	DHCP Request
DHCPsrvr	Broadcast	DHCPsrvr	255.255.255.255	DHCP ACK

El mensaje de difusión del cliente DHCPdiscover puede ser recibido por más de un servidor DHCP.

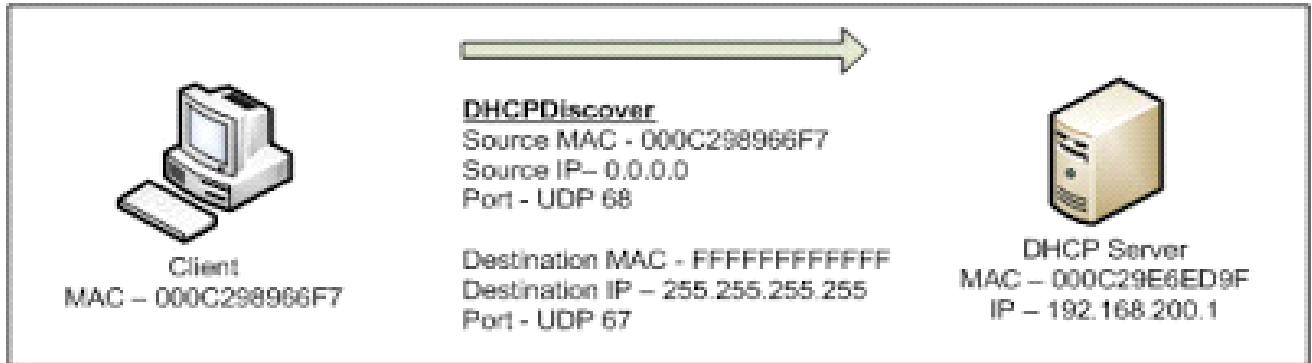
Dos o más servidores pueden contestar DHCPoffer al cliente con la oferta de direcciones. El cliente escoge la primera respuesta recibida.



3.3.5.11 Descubrimiento DHCP

DHCPDISCOVER

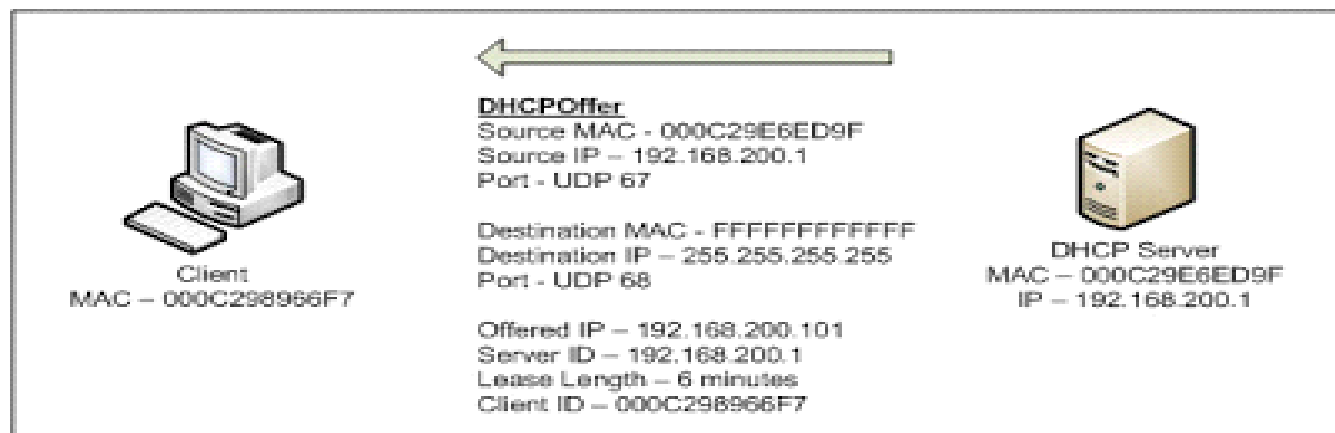
Es una solicitud DHCP realizada por un cliente de este protocolo para que el servidor DHCP de dicha red de computadoras le asigne una Dirección IP y otros Parámetros DHCP como la máscara de red o el nombre DNS.



3.3.5.12 Oferta DHCP

DHCPOFFER

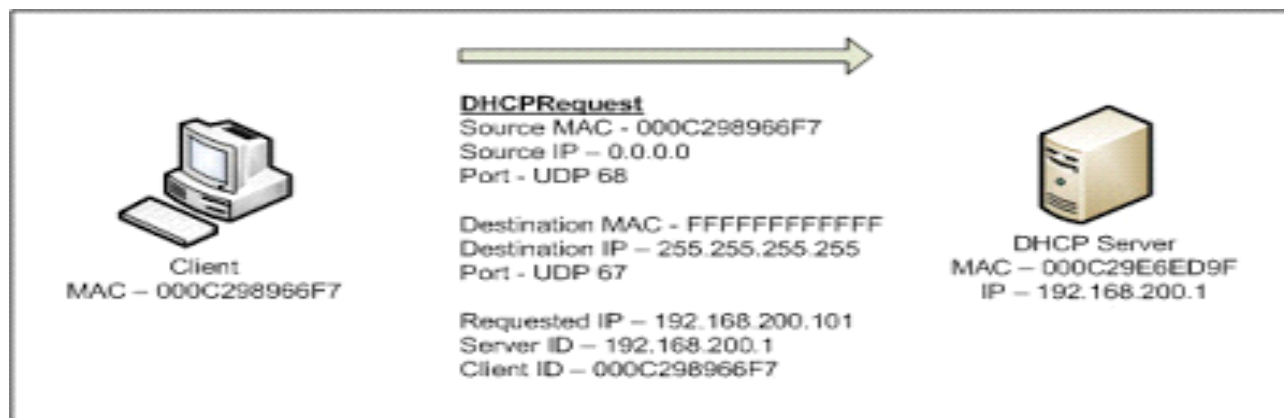
DHCP Offer es la respuesta del Servidor DHCP a un cliente DHCP ante su petición de la asignación de los Parámetros DHCP.



3.3.5.13 Solicitud DHCP

DHCPREQUEST

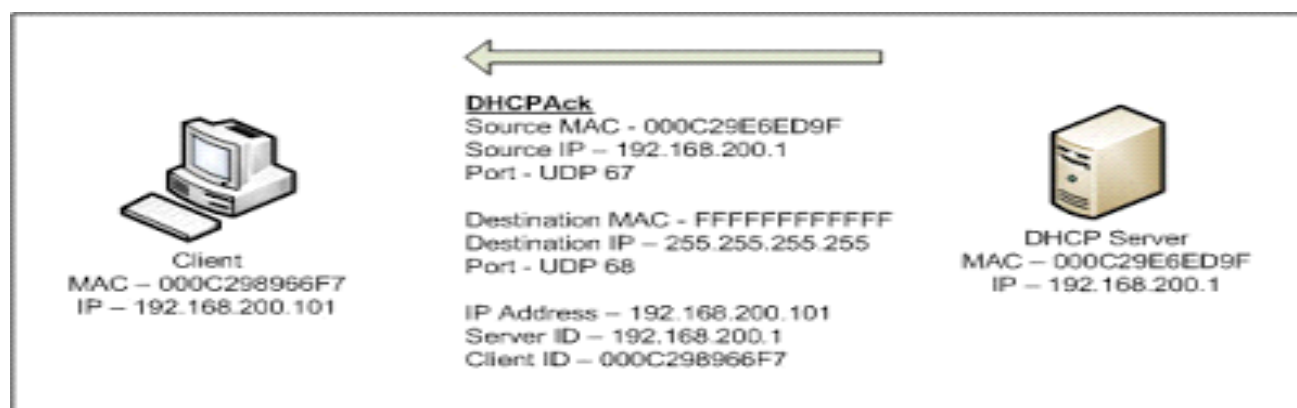
El cliente selecciona la configuración de los paquetes recibidos de DHCP Offer. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor.



3.3.5.14 Confirmación DHCP

DHCP ACKNOWLEDGE

Cuando el servidor DHCP recibe el mensaje DHCPREQUEST del cliente, se inicia la fase final del proceso de configuración. Esta fase implica el reconocimiento DHCPACK el envío de un paquete al cliente. Este paquete incluye el arrendamiento de duración y cualquier otra información de configuración que el cliente pueda tener solicitada. En este punto, la configuración TCP / IP proceso se ha completado.



3.3.5.15 DHCP

Concesión: El DHCP asigna las direcciones con una fecha de inicio y una fecha de vencimiento.

Si el cliente detecta que el vencimiento está próximo, inicia la renovación con la solicitud DHCPrequest.

Si el servidor detecta que la concesión va a vencer, envía un mensaje DHCPnack. Si no recibe una respuesta válida, el servidor recupera la dirección y le reasigna a otro cliente.

La concesión debe efectuarse de acuerdo al tipo de usuario y a la frecuencia de uso de los dispositivos clientes.

Un host pierde su dirección IP cuando se desconecta de la red.

Si un cliente ha tenido una dirección IP asignada por DHCP, al reiniciar el equipo puede volver a solicitar la misma dirección por medio de DHCPrequest, proceso limitado en el tiempo.

```
Adaptador de LAN inalámbrica Wi-Fi:
  Sufijo DNS específico para la conexión. . . : 
  Descripción . . . . . : Adaptador de red 802.11n Broadcom
  Dirección física. . . . . : 9C-2A-70-18-27-7B
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
  Vínculo: dirección IPv6 local. . . : fe80::5901:eae6:8d33:d37b%13<Preferido>
  Dirección IPv4. . . . . : 192.168.0.22<Preferido>
  Máscara de subred . . . . . : 255.255.255.0
  Concesión obtenida. . . . . : martes, 27 de agosto de 2013 7:33
  :22 p. m.
  La concesión expira . . . . . : domingo, 01 de septiembre de 2013
  :7:51:11 p. m.
  Puerta de enlace predeterminada . . . . . : 192.168.0.1
  Servidor DHCP . . . . . : 192.168.0.1
  IAID DHCPv6 . . . . . : 329001584
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-18-F0-9E-8C-E0-DB-55-
  DF-73-49
  Servidores DNS. . . . . : 200.75.51.132
  :200.75.51.133
  NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet Ethernet:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . : 
  Descripción . . . . . : Conexión de red Gigabit Intel(R)
  82579LM
  Dirección física. . . . . : E0-DB-55-DF-73-49
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí

Adaptador de túnel isatap.{6A6FF093-C41E-4A64-AFC1-CAA8945DA9C1}:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . : 
  Descripción . . . . . : Adaptador ISATAP de Microsoft
  Dirección física. . . . . : 00-00-00-00-00-00-00-E0
  DHCP habilitado . . . . . : no
  Configuración automática habilitada . . . : sí
```

3.3.6.1 Protocolos y servicios **Telnet**

Los primeros equipos terminales de datos usaban sistemas basados en textos y estaban conectadas directamente a una unidad central de procesamiento de datos.

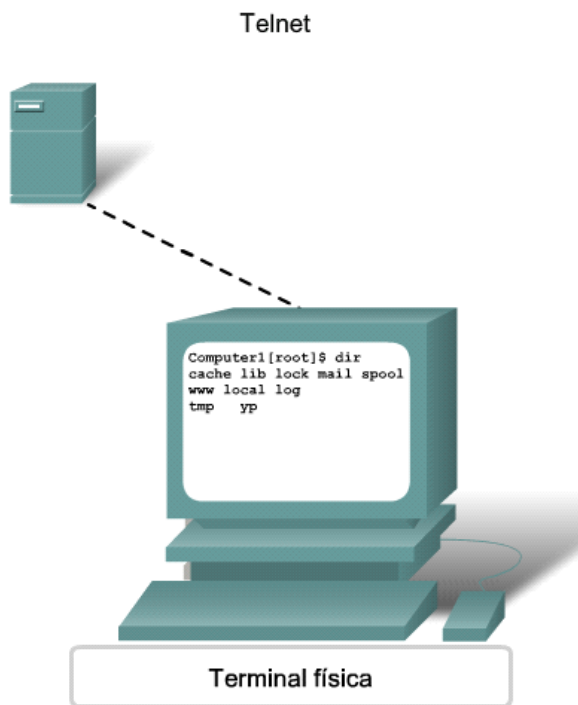
Telnet proporciona una facilidad para que un computador pueda emular a una terminal virtual y pueda conectarse remotamente a través de la red.

La mayoría de los sistemas operativos tienen instalado la aplicación Telnet que permite a los host conectarse con los servidores.

En algunos sistemas operativos, ciertos comandos pueden ser ejecutados desde una terminal conectada directamente a la unidad de procesamiento de datos o a través de Telnet.

Telnet permite el uso de claves de acceso a una aplicación pero la transferencia de los datos a través de la red no está encriptada.

En la actualidad se usa una aplicación alternativa SSH.



Permite conectarse remotamente a una unidad central de procesamiento.