UD1. Capa de aplicación

Índice

Introducción

Protocolos TCP/IP

Todas las aplicaciones finales que usamos se basan en otros protocolos. Los protocolos que use la aplicación estarán basados en otros de transporte como UDP y TCP y estos a su vez en protocolos de internet como IP, que son los que finalmente tienen acceso a la red.

Hay un modelo de referencia y una pila de protocolos. A cada capa (Internet, transporte y aplicación) se le asocia protocolos:

Arquitectura cliente/servidor

Generalmente se comportan de acuerdo a una estructura cliente-servidor. En ella existe un host que siempre está activo, el **servidor**, con **IP permanente**. Y este presta un servicio a las solicitudes de muchos otros hosts, que son sus clientes, con IP que puede ser dinámica y privada y no se comunican entre sí. Estos, por su parte, pueden estar activos de manera permanente o intermitente. Un servidor siempre está en funcionamiento, tiene IP permanente y normalmente pública. Se agrupan en granjas o clústeres, también denominados centros de datos, que permiten dar soporte a todas las peticiones de sus clientes sin ser desbordados.

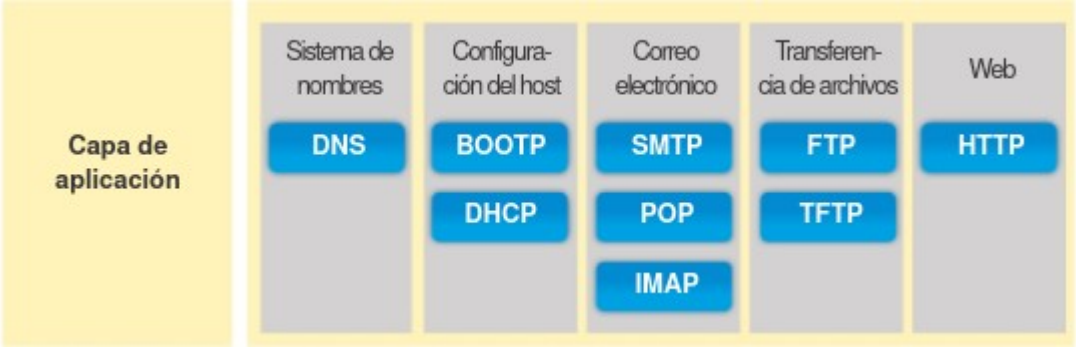
Los clientes funcionan intermitentemente, pueden tener IP dinámica y privada, se comunican con el servidor pero no se comunican entre sí.

Procesos cliente y servidor

El proceso cliente es el que inicia la comunicación, mientras que el proceso servidor es el que espera a ser contactado. Es por esto por lo que necesita tener una IP permanente y pública. Además, para recibir mensajes, un proceso debe tener un identificador, compuesto por una IP y un puerto.

Un proceso envía/recibe mensajes a/desde su socket. Para recibir mensajes un proceso debe tener un identificador (IP +puerto). Por ejemplo: servidor web www.iesrodeira.com con IP 128.119.245.12 y número de puerto 80.

La capa de Aplicación



Servicio de Nombres de Dominio (DNS)

Es un servicio (implementado en un servidor) que se encarga de traducir los nombres a direcciones IP.

Tiene una estructura jerárquica en dominios:

ParteLocal.dominioNivelN.(. . .).dominioNivel1

Donde Nivel1 es el dominio genérico.

La ICANN se encarga de delegar los nombres y números asignados.

Cuando un host quiere solicitar una determinada página a un servidor web introduce el nombre de dicho servidor web. El navegador extrae el nombre del host a partir del URL y lo pasa a la aplicación DNS. El cliente DNS envía una consulta con dicho nombre al servidor DNS, tras procesarlo, el servidor le responde con una dirección IP correspondiente, mediante el cual ya puede iniciar la conexión.

El ordenador original no resuelve todo el nombre del dominio. Este conecta con un servidor que será el encargado de conectar iterativamente con el resto de servidores.

De esta manera nos conectaríamos con los servidores “.”, los de dominio (Top-Level Domain, TDL), servidores Locales y servidores Autorizados y Zona.

Un host solicitaría la dirección de una URL (www.una.direccion.com) a su servidor local. Este envía la petición a un servidor raíz, el cual toma el sufijo (.com) y le responde al DNS local una lista de direcciones responsables de dicho dominio (los responsables del sufijo .com). Estos responsables son servidores TLD (top level domain) y a continuación se les envía una petición a estos. El servidor TLD examina el sufijo (direccion.com) y responde con la dirección del servidor DNS autorizado que puede dar la dirección del URL inicial. Después el servidor local consulta a dicho servidor DNS autorizado y este le responde con la dirección IP de la URL inicial (www.una.direccion.com).

Los servidores pueden dar una respuesta con autoridad, si tiene autoridad sobre la zona en la que se encuentra el nombre solicitado y devuelve la dirección IP. Una respuesta sin autoridad, cuando no tienen autoridad pero tienen la respuesta en caché. O bien puede no conocer la respuesta, lo que implicaría una consulta a un servidor superior.

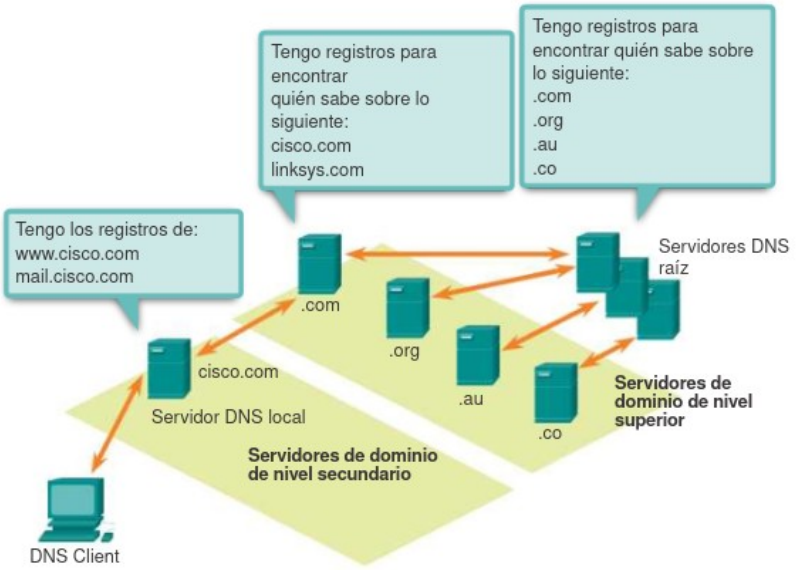
El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres. Estos registros contienen el nombre, la dirección y el tipo de registro.

Algunos de estos tipos de registros son:

- **A:** una dirección de dispositivo final
- **NS:** un servidor de nombre autoritativo
- **CNAME:** el nombre canónico (o el nombre de dominio completamente calificado) para un alias; se utiliza cuando varios servicios tienen una dirección de red única, pero cada servicio tiene su propia entrada en el DNS.
- **MX:** registro de intercambio de correos; asigna un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.

Cuando un cliente realiza una consulta, el proceso BIND 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.

La solicitud puede pasar a lo largo de cierta cantidad de servidores, lo cual puede tomar más tiempo y consumir banda ancha. Una vez que se encuentra una coincidencia y se la devuelve al servidor solicitante original, este almacena temporalmente en la memoria caché la dirección numerada que coincide con el nombre.



Si vuelve a solicitarse ese mismo nombre, el primer servidor puede regresar la dirección utilizando el valor almacenado en el caché de nombres. El almacenamiento en caché reduce el tráfico de la red de datos de consultas DNS y las cargas de trabajo de los servidores más altos de la jerarquía. El servicio del cliente DNS en los equipos Windows optimiza el rendimiento de la resolución de nombres DNS al almacenar también los nombres resueltos previamente en la memoria. El comando **ipconfig /displaydns** muestra todas las entradas DNS en caché en un sistema de computación Windows.

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

DHCP

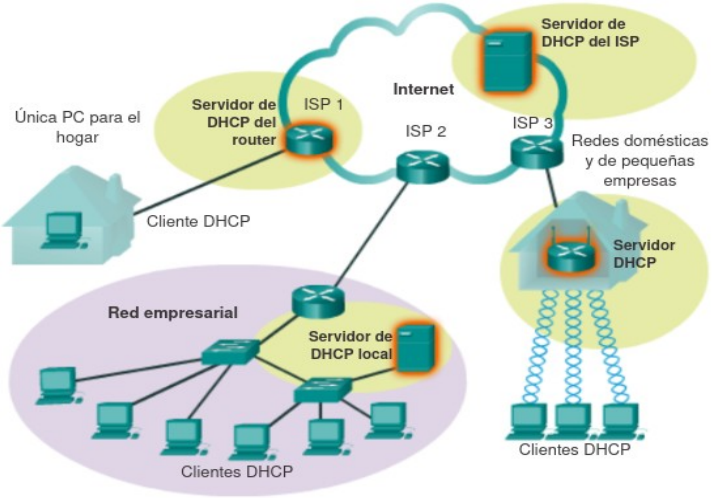
El servicio Protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) permite a los dispositivos de una red obtener direcciones IP y demás información de un servidor DHCP. Este servicio automatiza la asignación de direcciones IP, máscaras de subred, gateway y otros parámetros de redes IP. Esto se denomina “direccionamiento dinámico”. La alternativa al direccionamiento dinámico es el direccionamiento estático. Al utilizar el direccionamiento estático, el administrador de red introduce manualmente la información de la dirección IP en los hosts de red.

DHCP permite a un host obtener una dirección IP de forma dinámica cuando 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 “pool” y la asigna (concede) al host por un período establecido.

Las direcciones distribuidas por DHCP no se asignan de forma permanente a los hosts, sino que solo se conceden por un cierto período. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse.

Como lo muestra la figura, varios tipos de dispositivos pueden ser servidores de DHCP cuando ejecutan software de servicio de DHCP. En la mayoría de las redes medianas a grandes, el servidor de DHCP suele ser un servidor local dedicado con base en una PC. En las redes domésticas, el servidor de DHCP suele estar ubicado en el router local que conecta la red doméstica al ISP. Los hosts locales reciben la información de la dirección IP directamente del router local. El router local recibe una dirección IP del servidor de DHCP en el ISP.

DHCP puede representar un riesgo a la seguridad porque cualquier dispositivo conectado a la red puede recibir una dirección. Este riesgo hace que la seguridad física sea un factor determinante para el uso del direccionamiento dinámico o manual. Tanto el direccionamiento dinámico como el estático tienen un lugar en el diseño de red. Muchas redes utilizan tanto el direccionamiento estático como el DHCP. DHCP se utiliza para hosts de uso general, como los dispositivos para usuarios finales, mientras que el direccionamiento estático se utiliza para dispositivos de red, como gateways, switches, servidores e impresoras



cuando un dispositivo configurado con DHCP se inicia o se conecta a la red, el cliente transmite un mensaje de descubrimiento 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. El mensaje de oferta contiene la dirección IP y la máscara de subred que se deben asignar, la dirección IP del servidor DNS y la dirección IP del gateway predeterminado. La oferta de concesión también incluye la duración de esta.

El cliente puede recibir varios mensajes DHCPOFFER si hay más de un servidor de DHCP en la red local; por lo tanto, debe elegir entre ellos y enviar un mensaje de solicitud de DHCP (DHCPREQUEST) que identifique el servidor explícito y la oferta de concesión que el cliente acepta. Un cliente también puede optar por solicitar una dirección previamente asignada por el servidor.

Suponiendo que la dirección IP solicitada por el cliente, u ofrecida por el servidor, aún está disponible, el servidor devuelve un mensaje de acuse de recibo de DHCP (DHCPACK) que le informa al cliente que finalizó la concesión. Si la oferta ya no es válida, quizá debido a que hubo un tiempo de espera o a que otro cliente tomó la concesión, entonces el servidor seleccionado responde con un mensaje de acuse de recibo negativo de DHCP (DHCPNAK). Si se devuelve un mensaje DHCPNAK, entonces el proceso de selección debe volver a comenzar con la transmisión de un nuevo mensaje DHCPDISCOVER. Una vez que el cliente tiene la concesión, se debe renovar mediante otro mensaje DHCPREQUEST antes de que expire.

El servidor de DHCP asegura que todas las direcciones IP sean únicas (no se puede asignar la misma dirección IP a dos dispositivos de red diferentes de forma simultánea). Usar DHCP permite a los administradores de red volver a configurar fácilmente las direcciones IP del cliente sin tener que realizar cambios a los clientes en forma manual. La mayoría de los proveedores de Internet utilizan DHCP para asignar direcciones a los clientes que no necesitan una dirección estática.

Aunque normalmente se usan servidores DHCP aislados que permiten una gestión avanzada como por ejemplo integración con DNS, asignación de IP's asociadas a MAC's, Relays que permiten dar IP's en otros segmentos de red, etc. Cisco permite en sus routers que se habilite un servicio DHCP sencillo. Para ello tenemos que:

Definir y nombrar un pool de IP's

Establecer la red en la que daremos IP's

Decidir si queremos excluir ciertas direcciones (porque las vamos a asignar estaticamente)

Establecer la dirección IP del Gateway por defecto que enviaremos a los clientes

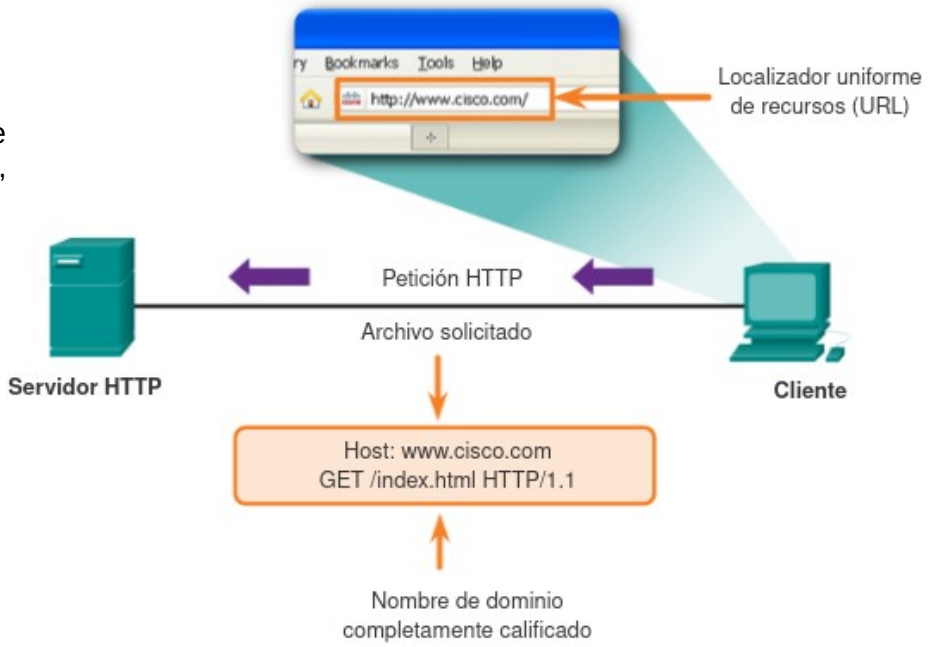
Establecer la dirección IP del servidor DNS que enviaremos a los clientes

- Creación del DHCP Pool llamado "DHCP-POOL-01"
  Router0(config)# ip dhcp pool DHCP-POOL-01
  Router0(dhcp-config)# default-router 172.16.0.1
  Router0(dhcp-config)# dns-server 172.16.0.1
  Router0(dhcp-config)# network 172.16.0.0 255.255.0.0
  Router0(dhcp-config)# exit

- Excluir direcciones IP del DHCP Pool
  Router0(config)# ip dhcp excluded-address 172.16.0.1 172.16.0.99
  Router0(config)# exit

Navegación Web

TCP al puerto 80: Inicio de conexión TCP, envío HTTP, cierre de conexión TCP.



El protocolo de transferencia de hipertexto, HTTP, es el protocolo de la capa de aplicación de la web y se encuentra en el corazón de la Web. Se implementa en dos programas, un cliente y un servidor.

Una página web es un fichero (HTML) formado por objetos, que pueden ser ficheros HTML, imágenes, applets y demás tipos de archivos. Cada objeto se direcciona con una URL. La mayoría de las páginas web tienen un archivo base HTML donde se referencian los objetos que están contenidos en esa web. Tiene su puerto bien definido, el 80.

El protocolo HTTP sigue un modelo cliente-servidor. El cliente es el que pide, recibe y muestra objetos web mediante el browser. El servidor es el que envía los objetos web en respuesta a peticiones.

HTTP es “stateless” → Cookies: El servidor no mantiene la información sobre las peticiones de los clientes. Esto puede implicar, por ejemplo, que cuando recibe dos peticiones idénticas del mismo cliente devuelve el objeto solicitado en lugar de devolver ningún tipo de error o mensaje informativo. Para identificar a los usuarios y su actividad se utilizan cookies, archivos que se almacenan en el sistema terminal del usuario y son gestionados por su navegador.

La conexión puede ser persistente o no persistente. En el primer caso se pueden enviar múltiples objetos sobre una única conexión TCP entre cliente y servidor, mientras que la no persistente crea nueva conexión para cada objeto a enviar. El persistente tiene un tiempo de transmisión total menor que el no persistente. Pero el no persistente permite gestionar mejor los recursos del servidor, pues no tiene que mantener el socket abierto durante toda la conexión, a cambio, al tener que establecer una conexión por objeto reduce su velocidad.

Hay dos tipos de mensajes HTTP: request y reponse. La petición de un elemento y su concesión. Cada uno de ellos tiene un formato específico, donde se indica la información concreta que se desea solicitar, o, en caso de ser desarrolladores de la página, mensajes de gestión. (GET,POST,HEAD,PUT,DELETE) Las respuestas se asemejan a las peticiones en cuanto a la indicación de un estado y cabecera, pero adicionalmente poseen el cuerpo de la entidad, donde se encuentra el objeto solicitado. La línea de estado indica un código de respuesta (200 OK, 301 moved permanently, 400 bad request, 505 HTTP version not supported).

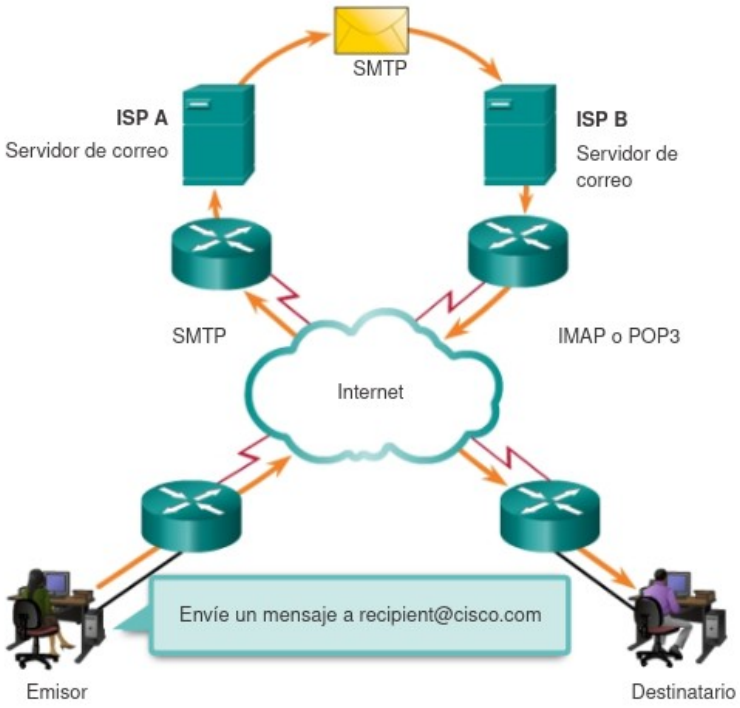
Correo electrónico

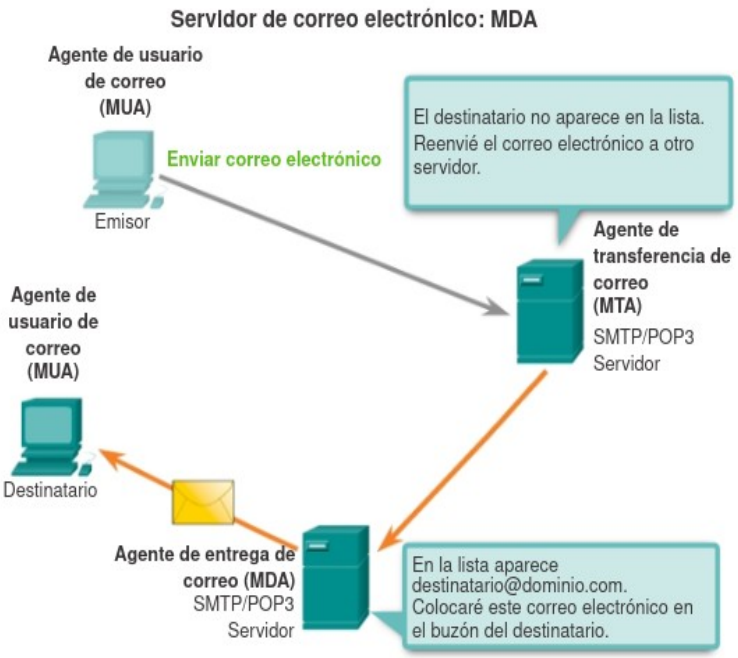
El usuario de origen utiliza su user agent para mandar el correo a su servidor de correo, se envía mediante SMTP o HTTP. El protocolo SMTP consiste en una conexión TCP con el servidor de correo destinatario mediante el puerto 25. El servidor de destino almacena el mensaje en la bandeja de entrada del usuario destino. El destinatario usará su agente de usuario arbitrariamente para leer el mensaje utilizando los protocolos POP3 (Post Office Protocol), IMAP (Internet Mail Access Protocol) o HTTP.

El principal problema de SMTP es que no requiere autenticación, lo que permite que cualquiera pueda enviar correo a cualquier persona o grupo de personas. Esta característica hace posible la existencia de correo basura o spam. Los servidores SMTP modernos intentan minimizar este comportamiento permitiendo que solo hosts conocidos accedan al servidos SMTP. Los servidores que no ponen tales restricciones se llaman open relay.

El protocolo de oficina de correos (POP) permite que una estación de trabajo pueda recuperar correos de un servidor de correo. Con POP, el correo se descarga desde el servidor al cliente y después se elimina 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.





El Protocolo de acceso a mensajes de Internet (IMAP, Internet Message Access Protocol) es otro protocolo que describe un método para recuperar mensajes de correo electrónico. Los usuarios pueden crear una jerarquía de archivos en el servidor para organizar y guardar el correo. Dicha estructura de archivos se duplica también en el cliente de correo electrónico. Cuando un usuario decide eliminar un mensaje, el servidor sincroniza esa acción y elimina el mensaje del servidor.