Capitulo VII: Aplicaciones

7.1 Servicio DHCP

7.1.1 Protocolo de Configuración de Host Dinámica

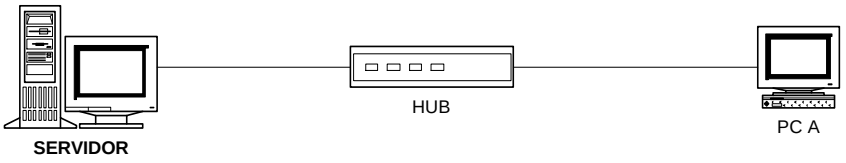
Muchas empresas cuentan con computadoras en red, compartiendo archivos e información importante. A causa de la gran cantidad de computadoras que pueden existir en una red, es que surge la necesidad de un mecanismo de asignación de direcciones IP de manera automática, para facilitar la administración de la red.

Por lo tanto el IETF, creo el Dynamic Host Confiuration Protocol (DHCP) cuyas características principales radican en permitir que una computadora pueda adquirir toda la información de configuración(dirección IP, mascara de subred, puerta de enlace, dirección de DNS) en un solo mensaje de configuración y además permite que una computadora pueda obtener una dirección IP en forma rápida y dinámica.

Para ello el administrador debe configurar un servidor proporcionándole a este un rango de direcciones IP a entregar. Una computadora nueva se conecta a la red y contacta al servidor DHCP para solicitar una dirección IP. El servidor selecciona una de las direcciones especificadas por el administrador de la red y se la entrega a la computadora cliente.

Registro de direcciones IP arrendadas

Direccion IP	Direccion MAC	Temporizacion
10.10.10.1	A	2 dias



Direccion IP del servidor: 10.10.10.254
Macara de subred: 255.0.0.0

Parametros DHCP

Rango de IP
from: 10.10.10.1
to: 10.10.10.254
Intervalo Exclusion: 10.10.10.254
Gateway: 10.10.10.254
DNS: 10.10.10.254

Direccion IP: 10.10.10.1
Mascara: 255.0.0.0
Gateway: 10.10.10.254
DNS: 10.10.10.254

Figura 3.1.1: Interacción de un servidor DHCP y un cliente

Por ejemplo, como se puede observar en la figura 3.1.1, tenemos una red con un servidor DHCP cuya dirección IP es la 10.10.10.254. Además, se puede observar que el administrador de la red configuro el rango de direcciones IP a entregar por el servidor en From: 10.10.10.1 – To: 10.10.10.254, la mascara de subred en 255.0.0.0, la puerta de enlace en 10.10.10.254, la dirección de DNS en 10.10.10.254 y el intervalo de exclusión 10.10.10.254. En el momento en que los dos clientes encienden sus computadoras, el servidor le otorga los parámetros de configuración como se muestra en la figura. El servidor DHCP utiliza la dirección MAC del cliente para identificar a quien le otorgo una dirección IP específica.

Un servidor DHCP no necesita conocer a priori la identidad de un cliente. Cualquier computadora conectada a la red del servidor DHCP puede obtener una dirección IP. El DHCP permite la autoconfiguración de la red, la cual esta sujeta a las restricciones impuestas por el administrador de la red. Una vez obtenido el IP comienza la autoconfiguración del TCP/IP.

7.1.2 Papel del administrador de la red

El administrador del servidor DHCP asigna al servidor un conjunto de direcciones IP. El administrador además puede realizar algunas restricciones de direcciones IP para reservarlas para uso futuro. El servidor DHCP arrienda una dirección a un cliente por un periodo de tiempo finito. Durante el periodo de arrendamiento, el servidor no alquilara la misma dirección a ningún otro cliente. Al final del periodo de arrendamiento el cliente debe renovarlo o dejar de usar la dirección entregada oportunamente.

El arrendamiento es configurable y depende de las necesidades de los clientes: que las direcciones se reciclen rápidamente (tiempo de arrendamiento finito) o que las direcciones sean permanentes(tiempo de arrendamiento infinito).

7.1.3 Diagrama de estados de adquisición de direcciones IP

El cliente DHCP debe pasar por seis estados, desde el momento de solicitud de la dirección IP, hasta la liberación de dicha dirección. El diagrama de estados en el cliente indica eventos y mensajes que ocasionan que un cliente cambie de estado. Para realizar las peticiones DHCP los clientes utilizan el puerto UDP 67.

Parar utilizar el DHCP un anfitrión debe volverse cliente y difundir un mensaje a todos los servidores de la red local. El anfitrión entonces reunirá los ofrecimientos de los servidores, seleccionara uno de ellos y verificara su aceptación por parte del servidor. El DHCP permite que el cliente termine el arrendamiento sin esperar que su tiempo expire. En el momento en que se renueven los arrendamientos se reiniciaran todas las temporizaciones.

Aplicaciones

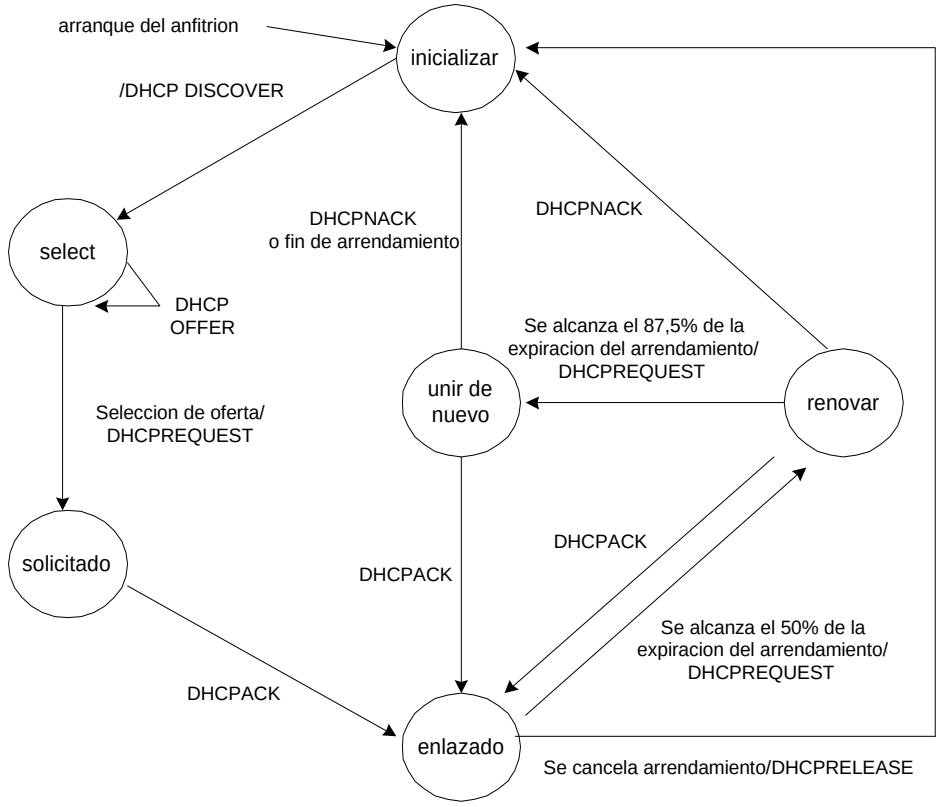


Figura 3.3.1: diagrama de estados del DHCP

7.1.4 Formato del mensaje DHCP

Significado de los campos:

- **Operación**: indica si el mensaje es una petición o una respuesta.
- **Tipo de Hardware**: indica que tipo de tecnología se utiliza en la capa de enlace de datos. Direcciones Ethernet se indica con un 1.
- **Longitud de la dirección de hardware**: longitud de la direcciones utilizadas en la capa de enlace de dato. Longitud de las direcciones MAC son de 48 bits.
- **Hops**: contador que se incrementa en el caso de que se tenga que atravesar varios enrutadores.
- **Id Transacción**: es un identificador que permite cotejar las respuestas con las solicitudes.

Aplicaciones

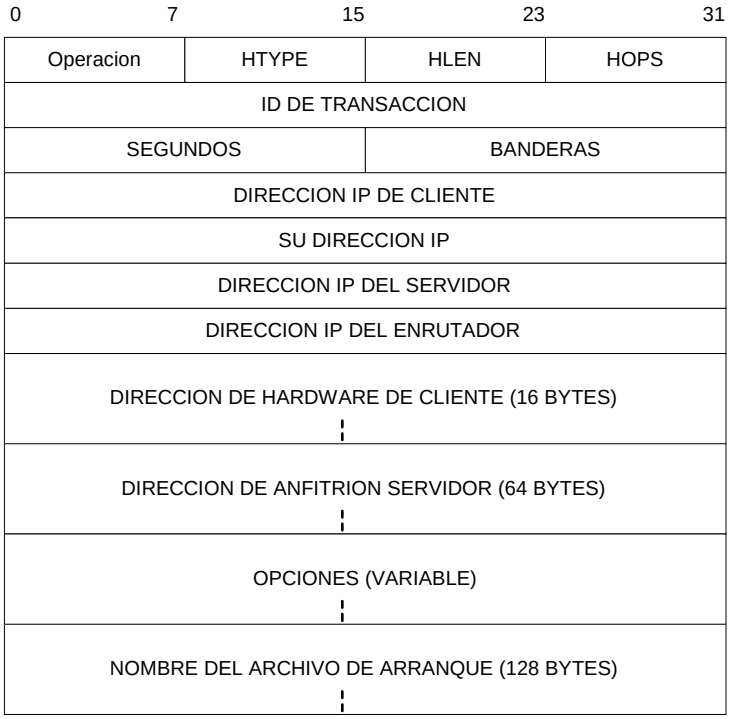


Figura 3.4.1: formato del mensaje DHCP

- **Segundos**: cantidad de tiempo que transcurrió desde que el cliente inicio el arranque del sistema operativo.
- **Banderas**: el formato del byte bandera es el siguiente: B0000000. Si el bit B esta en 1 significa que se realiza la difusión por hardware.
- **Dirección IP del cliente**: indica la dirección IP del cliente que emite el mensaje DHCP.
- **Su dirección IP**: es la dirección IP que le asigna el servidor DHCP
- **Dirección IP del servidor**: es la dirección IP del servidor que responde la solicitud de DHCP
- **Dirección IP del router**: es la dirección de puerta de enlace o gateway, para que el cliente sea capaz de alcanzar un enrutador y mediante este poder encaminar sus datos hacia otras redes.
- **Dirección de Hardware del cliente**: es la dirección física que utiliza el cliente en la capa de enlace de datos.
- **Nombre de anfitrión servidor**: nombre que identifica al servidor.
- **Nombre archivo arranque**: nombre del archivo de arranque. Este campo es utilizado por el protocolo BOOTP.

- **Opciones**: temporizaciones de arrendamiento y tipos de mensajes: 1. DHCP DISCOVER, 2. DHCP OFFER, 3. DHCP REQUEST, 4. DHCP DECLINE, 5. DHCP ACK, 6. DHCP NACK, 7. DHCP RELEASE.

7.2 Servicios NAT y PROXY

7.2.1 NAT - Traducción de la Dirección de Red(Network Address Translation)

La traducción de direcciones de red o NAT es una de las facilidades de seguridad más potentes. El servidor NAT se emplea para ocultar las direcciones de las redes privadas detrás de una sola dirección IP o de varias direcciones. Una versión de NAT denominada "IP Masquerading (mascarada IP)" ha gozado durante varios años de mucha popularidad entre los usuarios de Linux.

NAT puede implementarse de muchas formas pero, básicamente, crea un rango de direcciones privadas casi ilimitado para las redes internas que es "traducido" por el servidor NAT, de forma que las comunicaciones puedan transferirse a las redes públicas o entrar desde ellas sin revelar ninguna información sobre sistemas internos sensibles. Dado que se desconoce el rango de direcciones privado de la interfaz interna de los firewalls, es prácticamente imposible atacar directamente a un sistema en la red interna protegida por NAT.

7.2.1.1 Funcionamiento de NAT

La Traducción de la Dirección de Red (Network Address Translation, NAT) es un proceso que modifica las direcciones IP de los paquetes transmitidos desde/hacia la red de área local hacia/desde Internet u otras redes basadas en IP. Además el NAT para registrar y diferenciar los pedidos que realizan los clientes asigna a cada sesión o conexión que solicita un cliente un puerto TCP distinto por cada conexión.

7.2.1.1.1 Paquetes salientes

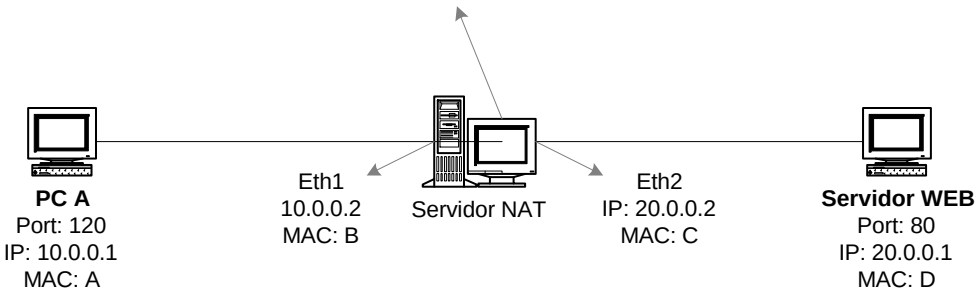
Los paquetes que pasan por el traductor de dirección saliendo de la LAN se cambian o traducen para que parezca que proceden del computador en el que se está ejecutando la NAT (ese computador está conectado directamente a Internet). Lo que realmente ocurre es que la dirección IP "origen" es cambiada en el encabezado del datagrama IP y sustituida por la dirección IP(pública) del computador "NAT".

El motor NAT también crea una tabla de registros que contiene información sobre cada paquete que ha pasado hacia Internet y almacena cual es el puerto TCP por el que esta saliendo la conexión del cliente. De esta forma, estableciendo una conexión TCP por cada pedido de los clientes, es posible que no se mezclen los pedidos y además lograr la identificación de las solicitudes de todos los clientes dentro de la LAN. Esto puede observarse en la figura siguiente.

Aplicaciones

Base de Datos Servidor NAT

Parametros Cliente de la LAN			Informacion WAN	
MAC Origen	IP Origen	Port Origen	IP Buscar	Puerto WAN
A	10.10.10.1	120	20.0.0.1	1001



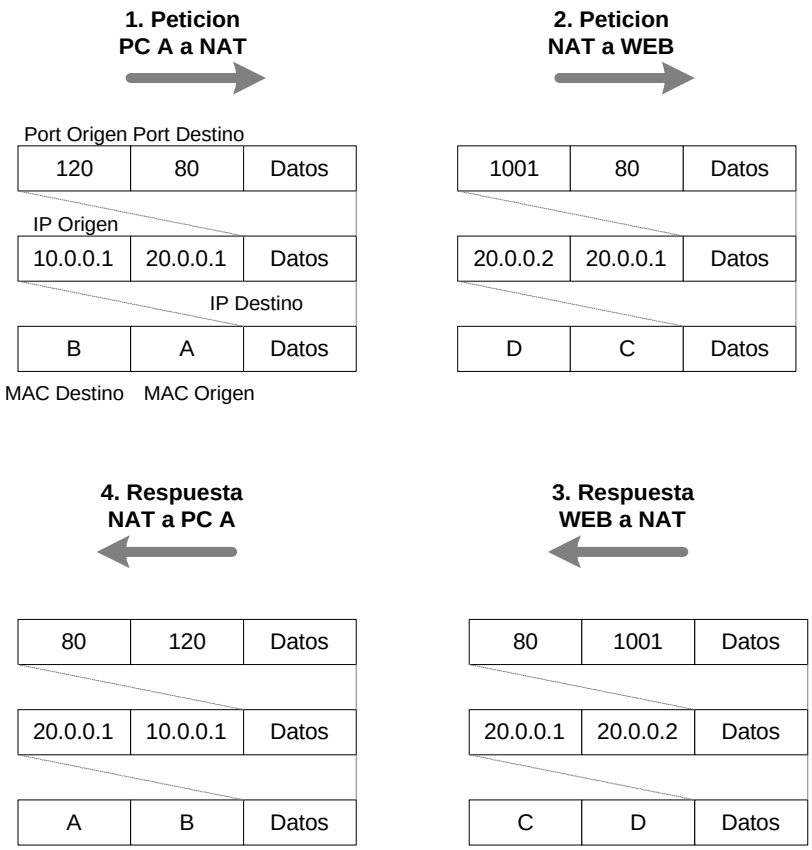


Figura 4.2.1: funcionamiento del servidor NAT

7.2.1.1.2 Paquetes entrantes

Los paquetes que pasan por NAT para entrar en la LAN se comparan con los registros almacenados por el motor NAT. Lo que el servicio NAT lee es el puerto de destino TCP que viene en el paquete, para buscar dicho puerto en cada fila de su tabla de registro. De esta manera determina cual es el cliente que solicito la información que esta llegando desde la Internet. Después, el puerto de destino y la dirección IP de "destino" se sustituyen(en base a los registros de la base de datos) nuevamente por el puerto de destino y la dirección IP específica de la clase privada interna, para que acceda al computador respectivo en la LAN.

Recuerde que originalmente el paquete llegó con la dirección IP pública del computador NAT como su dirección de "destino". El motor NAT tuvo que cambiar esa información para entregar el paquete al receptor correcto dentro de la red local. Una vez que el paquete fue entregado a su destino final, la entrada de solicitud es borrada de la base de datos del servidor NAT.

7.2.2 Vista de Conjunto Proxy

La finalidad principal de un servidor proxy es ahorrar ancho de banda en su conexión a Internet. Cuando los usuarios acceden a Internet a través de un proxy, el servidor proxy almacena los diferentes objetos solicitados que pasan por él (como páginas HTML, imágenes y otros tipos de ficheros) en su memoria caché(espacio físico en una unidad de almacenamiento, como puede ser un disco rígido). Cuando las páginas o imágenes son solicitadas nuevamente por el mismo usuario o por otra persona dentro de la LAN privada, el servidor proxy pone a disposición, desde su memoria caché, los elementos solicitados.

De esta forma se reduce la carga de la conexión a Internet y la operación completa es también más rápida que si se descargan nuevamente las imágenes desde Internet. Por otra parte, los objetos guardados en la memoria caché de un servidor proxy no están siempre actualizados. La definición del tiempo de vida (TTL ,Time-To-Live) de los documentos guardados es una cuestión muy delicada y debe definirse de forma equilibrada para evitar malentendidos que pueden surgir, por ejemplo, porque el día anterior leyó las noticias del diario. Las características de un servidor proxy son:

1. Permite ahorrar ancho de banda gracias al almacenamiento en cache de las paginas solicitadas

2. Utiliza por defecto el puerto TCP 3128

3. El tamaño de la memoria cache es establecido por el administrador de la red.

4. El tiempo de vida de las paginas almacenadas puede ser establecido por el administrador de la red.

5. Su funcionamiento es similar al del motor NAT, con la excepción fundamental de la memoria cache.

7.3 Servicio DNS

7.3.1 Nombres de dominio TCP/IP de Internet

El mecanismo que implementa una jerarquía de nombres de maquinas para las redes TCP/IP se conoce como Domain Name System(DNS). El DNS tiene dos aspectos conceptualmente independientes. Primero es **abstracto**, ya que especifica la sintaxis del nombre y las reglas para delegar la autoridad respecto a los nombres. Segundo, el DNS es **concreto**, ya que especifica la implementación de un sistema de computación distribuido que transforma eficientemente los nombres en direcciones.

El **sistema de nombres** de dominio se vale de un esquema de nombres **jerárquicos**, conocido como nombre de dominio. Un nombre de dominio consiste en una **secuencia de nombres separados** por un carácter delimitador: "**el punto**". De esta manera, el nombre de dominio

labredes.ubp.edu.ar

contiene cuatro etiquetas: labredes, ubp, edu y ar. Cualquier sufijo de una etiqueta en un nombre de dominio es llamado también dominio. En el ejemplo de arriba, el dominio de nivel inferior es "**labredes.ubp.edu.ar**" (el nombre de dominio para el laboratorio de redes de la universidad Blas Pascal), el segundo nivel de dominio es "**ubp.edu.ar**" (el nombre de dominio para la universidad de UBP), el tercer nivel del dominio es "**edu**" (el nombre de dominio para las instituciones educativas) y el ultimo dominio o el dominio superior es "**ar**" (nombre de dominio asignado a la Republica Argentina). Como se muestra en el ejemplo, los nombres de dominio están escritos con la etiqueta local primero y el dominio superior al último.

7.3.2 Nombres de dominio oficiales y no oficiales de Internet

En teoría, el estándar de nombres de dominio especifica un espacio de nombres jerárquico abstracto con valores arbitrarios para las etiquetas. Como el sistema de dominio dicta solo la forma de los nombres y no sus valores actuales, es posible, para cualquier grupo que constituya una instancia de sistema de dominio, seleccionar etiquetas para todas las partes de su jerarquía. Por ejemplo, una compañía privada puede establecer una jerarquía de dominios en la que las etiquetas de nivel superior especifiquen corporaciones y subsidiarias, el siguiente nivel divisiones corporativas y el nivel inferior los departamentos.

Sin embargo, la mayoría de los usuarios de tecnología de dominio sigue la jerarquía de etiqueta utilizada por el sistema de dominio oficial de Internet. Hay dos razones para ello. En primer lugar, el esquema de Internet es completo y flexible. Se puede adaptar a una amplia variedad de organizaciones y permite a cada grupo seleccionar entre una jerarquía de nombres asignados geográficamente o en función de la estructura organizativa. En segundo lugar, la mayor parte de las localidades sigue el esquema de Internet porque de esta manera puede conectar sus instalaciones TCP/IP a la red global de Internet sin cambiar nombres.

Conceptualmente, el nombre de nivel superior permite dos jerarquías de nombres completamente diferentes: el esquema geográfico y el organizacional. El geográfico divide el universo de maquinas por país. Las maquinas de Estados Unidos quedan bajo el dominio de nivel superior US, cuando otro país desea registrar maquinas en el sistema de nombres de dominio, la autoridad central asigna al país un nuevo dominio de nivel

Aplicaciones

superior con el estándar internacional del país identificado por dos letras como su etiqueta.

La autoridad para el dominio de US ha seleccionado dividirlo dentro de un dominio de segundo nivel por estado. Por ejemplo, el dominio para el Estado de Virginia es:

va.us

En cambio, la autoridad para el dominio de Argentina no ha seleccionado dividirlo dentro de un dominio de segundo nivel por estado, sino que parte directamente hacia la división por instituciones, comercio, instituciones educativas, etc…. Por ejemplo, el dominio para el Estado de Virginia es:

com.ar
net.ar
edu.ar

La autoridad de Internet ha seleccionado particionar su nivel superior en los dominios que se listan en la siguiente tabla.

Nombre de Dominio	***Significado***
COM	Organizaciones comerciales
EDU	Instituciones educativas
GOV	Instituciones gubernamentales
MIL	Grupos militares
NET	Centros mayores de soporte de red
ORG	Organizaciones diferentes a las anteriores
ARPA	Domino temporal de ARPANET (obsoleto)
INT	Organizaciones internacionales
Código del país	País en particular (según esquema geográfico)

Aun cuando los nombres se muestran en mayúsculas, el sistema de nombres de dominio es insensible a la distinción de mayúsculas y minúsculas, así pues, EDU es equivalente a edu.

Como alternativa para la jerarquía geográfica, el dominio de nivel superior también permite que las organizaciones se agrupen en función de su organización. Cuando una organización desea participar en el sistema de nombres de dominio, decide la forma en que desea que se registre y solicita su aprobación.

La autoridad central revisa la solicitud y asigna un subdominio a la organización bajo uno de los dominios de nivel superior existentes. Por ejemplo, es posible que una universidad se registre con un dominio de segundo nivel EDU (practica común) o que se registre según el estado o país en el que se localiza. De esta manera, algunas organizaciones han seleccionado la jerarquía geográfica, la mayoría prefiere registrarse con COM, EDU, MIL o GOV. Hay dos razones para ello.

En primer lugar, los nombres geográficos son mucho más difíciles de encontrar o adivinar. Por ejemplo, la Universidad de Blas Pascal se encuentra en Cordoba, Argentina. Mientras que un usuario puede adivinar fácilmente un nombre organizacional como purdue.edu, un nombre geográfico

resulta, con frecuencia, difícil de adivinar pues por lo general es una abreviatura como "cba.edu.ar" (indica que el estado es Cordoba, que es una universidad y esta en argentina).

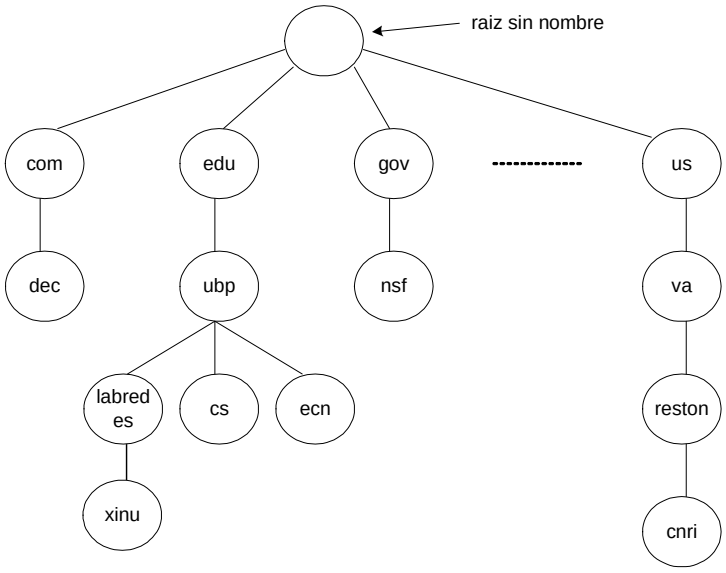


Figura 5.2.1: Una pequeña parte de la jerarquía de nombres de dominio de Internet. En la practica, el árbol es extenso y plano, la mayor parte de los anfitriones aparecen en el quinto nivel

Otro ejemplo puede ayudar a aclarar la relación entre la jerarquía de nombres y la autoridad para los nombres. Una maquina llamada "**xinu**" ubicada en el laboratorio de redes de la Universidad Blas Pascal tiene el nombre de dominio oficial:

xinu.labredes.ubp.edu.ar

El nombre de la maquina fue aprobado y registrado por el administrador de la red local en el Laboratorio de Redes. El administrador del laboratorio había obtenido previamente autorización para el subdominio labredes.ubp.edu.ar de una autoridad de la red universitaria, quien a su vez había obtenido permiso para administrar el subdominio ubp.edu.ar de la autoridad de Internet. La autoridad de Internet conserva el control del dominio edu.ar, de manera que nuevas universidades pueden añadirse solo con su permiso. En forma similar, el administrador de la red de la Universidad Blas Pascal conserva la autoridad para el subdominio ubp.edu.ar, de manera que los nuevos dominios de tercer nivel solo pueden ser añadidos con la autorización del administrador.

En la figura 5.2.1 se ilustra una pequeña parte de la jerarquía de nombres de dominio de Internet. Como se muestra en la figura, Digital Equipment Corporation, una organización comercial, esta registrada como dec.com, la universidad de Purdue esta registrada como purdue.edu y la National Science Foundation, una institución gubernamental esta registrada como nsf.gov. En contraste, la Corporation for National Research

Initiatives eligió registrarse bajo la jerarquía geográfica como cnri.reston.va.us.

7.3.3 Asociación de nombres de dominio en direcciones

Además de las reglas para la sintaxis del nombre y la delegación de autoridad, el esquema de nombres de dominio incluye un sistema distribuido, confiable y de propósito general para asociar nombres en direcciones. El sistema esta distribuido en el sentido técnico, esto significa que un conjunto de servidores, que opera en varias localidades de manera conjunta, resuelve el problema de la asociación de nombres en direcciones.

Es eficiente en el sentido de que la mayor parte de los nombres se pueden asociar localmente, solo unos pocos requieren trafico de red. Es de propósito general puesto que no se encuentra restringido a nombres de maquina. Por ultimo, es confiable ya que una sola falla de un maquina prevendrá al sistema para que opere correctamente.

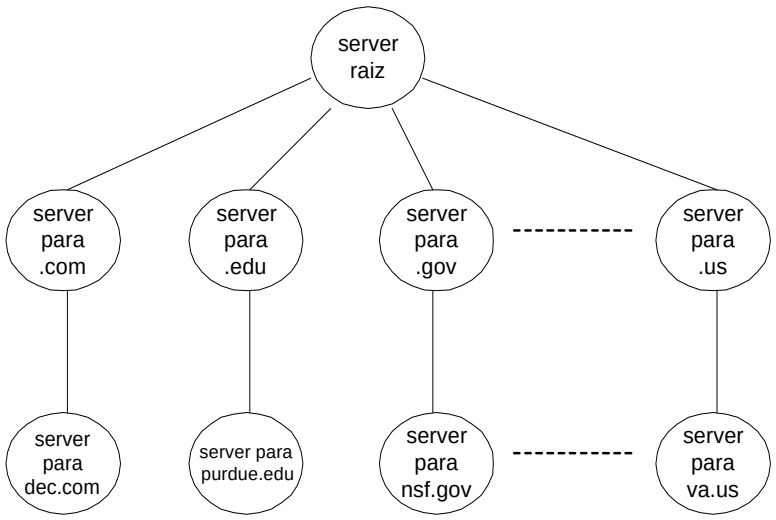


Figura 5.3.1: arreglo conceptual del servidor de nombres de dominio en un árbol que corresponde a la jerarquía de nombres. En teoría, cada servidor conoce la dirección de todos los servidores de bajo nivel para todos los subdominios dentro del dominio que maneja

El mecanismo de dominio para la asociación de nombres en direcciones consiste en sistemas independientes y cooperativos llamados servidores de nombres. Un servidor de nombres es un programa servidor que ofrece la asociación nombre a dirección, asociando los nombres de dominio en direcciones IP.

A menudo, el software servidor se ejecuta en un procesador dedicado y a la maquina se la conoce como **"servidor de nombres"**. El software cliente llamado, un **"resolvedor de nombres"** (**name resolver**), utiliza uno o mas servidores de nombres cuando traduce un nombre. La forma mas fácil de entender como trabaja un servidor de dominio es imaginándose como una estructura de árbol que corresponde a la jerarquía nombrada, como se muestra en la figura 5.3.1.

Aplicaciones

La **"raíz del árbol"** es un servidor que reconoce el dominio de nivel superior y sabe que servidor resuelve cada dominio. Teniendo un nombre por resolver, la raíz puede resolver el servidor correcto para ese nombre. En el siguiente nivel, un conjunto de servidores de nombres proporciona respuestas para un dominio de nivel superior (por ejemplo, edu).

Un servidor en este nivel sabe que servidor puede resolver cada uno de los subdominios bajo su dominio. En el tercer nivel del árbol, el servidor de nombres proporciona respuestas para el subdominio (por ejemplo, purdue bajo edu). El árbol conceptual continúa con un servidor en cada nivel para el que se ha definido un subdominio.

Los enlaces en el árbol conceptual no indican conexiones de red física. De hecho, muestran que otros servidores de nombres conoce y contacta un servidor dado. El servidor por si mismo puede localizarse en una localidad cualquiera dentro de una red IP. De esta manera, el árbol de servidores es una abstracción que emplea una red para comunicarse.

Si los servidores en el sistema de dominio trabajaran exactamente como lo sugiere nuestro modelo sencillo, la relación entre la conectividad y la autorización seria demasiado simple. Cuando la autoridad esta garantizada para un subdominio, la organización que lo solicita necesita establecer un servidor de nombres de dominio para este subdominio y enlazarlo dentro del árbol.

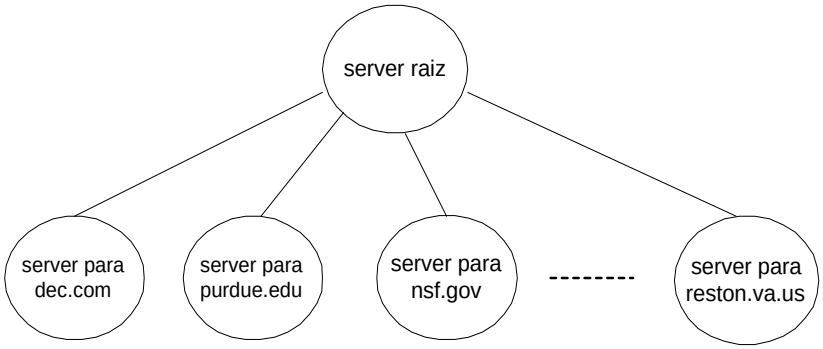


Figura 5.3.2: una organización realista de los servidores para la jerarquía de nombres de la figura 5.3.1. Dado que el árbol es extenso y plano, pocos servidores necesitan contactarse cuando se resuelve un nombre

En la práctica, la relación entre una jerarquía de nombres y el árbol de nombres no resulta tan sencilla como nuestro modelo lo plantea. El árbol de servidores tiene pocos niveles pues un solo servidor físico puede contener toda la información para partes extensas de una jerarquía de nombres. En particular, las organizaciones a menudo reúnen información de todos los subdominios desde un solo servidor. La figura 5.3.2 muestra una organización más realista de servidores para la jerarquía de nombres mostrada en la figura 5.3.1.

Un servidor raíz contiene información acerca de la raíz y de dominios de nivel superior y cada organización utiliza un solo servidor para sus nombres. Dado que el árbol de servidores es poco profundo, en la mayor parte de los casos dos servidores necesitan contactarse para resolver un nombre como xinu.cs.purdue.edu. El servidor raíz y el servidor para el dominio purdue.edu (esto quiere decir que el servidor raíz sabe que servidor maneja purdue.edu y toda la información de dominio reside en un servidor).

7.3.4 Resolución de nombres de dominio

Conceptualmente, la resolución de nombres de dominio procede de arriba hacia abajo, comenzando con el servidor de nombre raíz y siguiendo luego hacia los servidores localizados en las ramas del árbol. Hay dos formas de utilizar el sistema de nombres de dominio: contactar a un servidor de nombres cada vez que se necesite traducir un nombre o solicitar al sistema de servidores de nombres que realice la traducción completa de dominio.

En cada caso el software cliente forma una solicitud de nombres de dominio que contiene el nombre a resolver, una declaración sobre la clase del nombre, el tipo de respuesta deseada y un código que especifica si el servidor de nombres debe traducir el nombre completo. Se envía la solicitud a un servidor de nombres para su resolución.

Resolución Iterativa

Debe contactarse con el servidor Raíz porque ningún subdominio puede resolver el problema

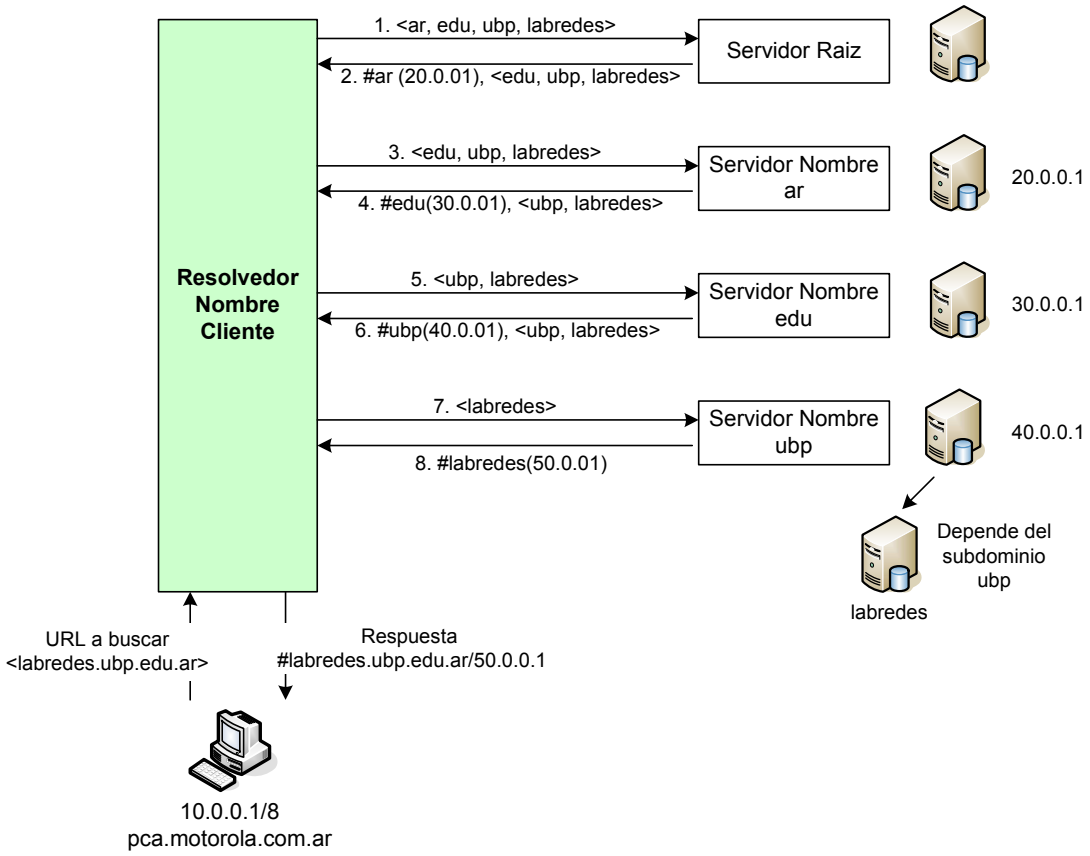


Figura 5.4.1: resolución de nombres iterativa

Aplicaciones

Resolución Recursiva

Debe contactarse con el servidor Raíz porque ningún subdominio puede resolver el problema

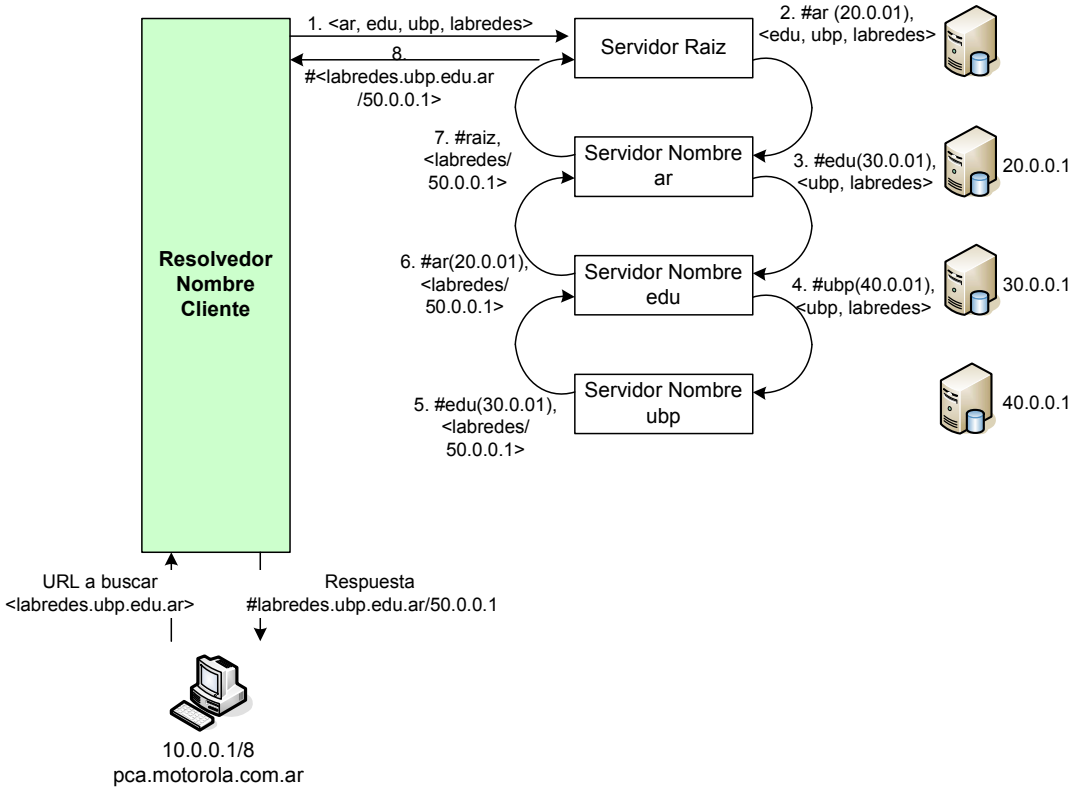


Figura 5.4.2: resolución de nombres recursiva

Cuando un servidor de nombres de dominio recibe una solicitud, verifica si el nombre señala un subdominio sobre el cual tenga autoridad. Si es así, traduce el nombre a una dirección de acuerdo con su base de datos y anexa una respuesta a la solicitud, antes de enviarla de regreso al cliente. Si el servidor de nombre no puede resolver el problema del nombre completamente, verifica que tipo de interacción especifico el cliente.

Si el cliente solicita una traducción completa (**recursiva**), el servidor se pone en contacto con un servidor de nombres de dominio que pueda resolver el problema del nombre y devuelve la respuesta al cliente. Si el cliente solicita una "**resolución no recursiva o iterativa**", el servidor de nombres no puede dar una respuesta, entonces se genera una replica que especifica el nombre del servidor que el cliente deberá contactar la próxima vez para resolver el problema del nombre.

Algunas de las preguntas mas frecuentes sobre el funcionamiento de los servidores de dominio son: ¿Cómo un cliente encuentra un servidor de nombres para comenzar la búsqueda? ¿Cómo encuentra un servidor de nombres a otros servidores de nombres que puedan responder a las solicitudes que el no puede responder?. Las respuestas son muy sencillas.

Un cliente debe saber como contactar al último servidor de nombre. Para asegurarse de que el servidor de nombres de dominio puede alcanzar a otros, el sistema de dominio requiere que cada servidor conozca la

dirección del ultimo servidor en la raíz o mejor dicho el servidor inmediatamente siguiente en el árbol de dominio. Además, un servidor podría conocer la dirección de un servidor para el dominio de un nivel inmediatamente superior (llamado padre).

Los servidores de nombres de dominio utilizan un puerto de protocolo bien conocido para toda comunicación, así, los clientes saben como comunicarse con un servidor una vez que conocen la dirección IP de la maquina que se conecta al servidor. En el proceso de resolución de nombres de dos etapas, la resolución comienza con el servidor de nombres local. Si el servidor local no puede resolver el nombre, la solicitud deberá enviarse hacia otro servidor en el sistema de dominio.

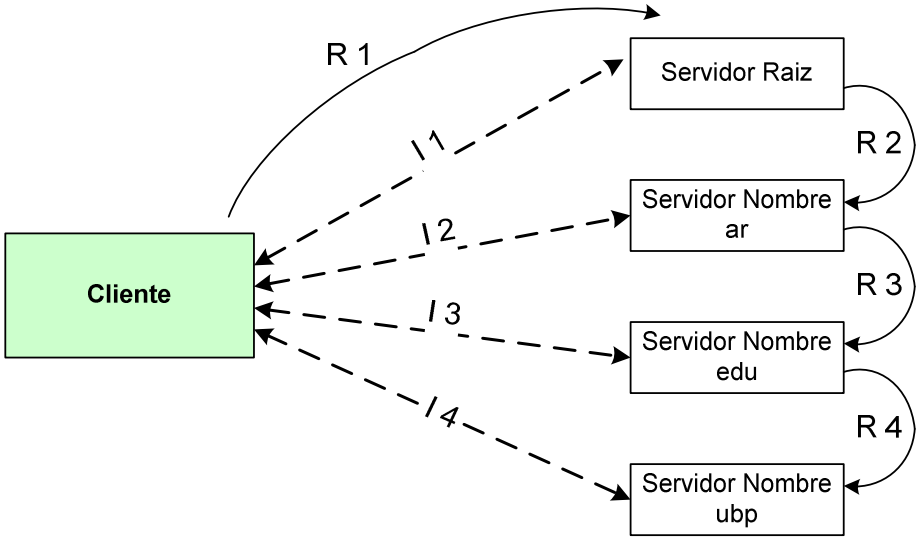


Figura 5.4.3: resumen de resolución de nombres iterativa (I) y recursiva (R)

7.3.5 Desempeño del cache: la clave de la eficiencia

El costo de una búsqueda para nombres no locales puede ser muy alto si se resuelve enviar cada solicitud hacia el servidor raíz. Incluso si las solicitudes pueden ir directamente hacia el servidor que tiene autoridad para el nombre, la búsqueda de nombres puede representar una pesada carga para una red de redes. Así, para mejorar el desempeño global de un sistema servidor de nombres, es necesario reducir los costos de búsqueda para nombres no locales.

Los servidores de nombres de Internet utilizan una memoria inmediata de nombres (**name caching**) para optimizar los costos de búsqueda. Cada servidor mantiene una memoria inmediata de los nombres resueltos utilizados más recientemente, así como un registro de donde fue obtenida la información para la asociación de nombres.

Cuando un cliente interroga a un servidor a fin de resolver el problema de un nombre, el servidor verifica primero si tiene autoridad para el nombre de acuerdo con el procedimiento estándar. Si no es así, el

servidor verifica su memoria inmediata para ver si el problema del nombre ser resolvió recientemente. Los servidores reportan la información almacenada en memora inmediata a los clientes, pero la marcan como una asignación no autorizada y entregan el nombre de dominio del servidor(S), desde el cual obtiene la asignación.

El servidor local también envía información adicional que le indica al cliente la asignación entre nombre y una dirección IP. De esta manera, los clientes reciben respuestas rápidamente, pero la información podría no estar actualizada. Si la eficiencia es importante, el cliente elegirá aceptar la respuesta no autorizada y continuar. Si la seguridad es importante, el cliente seleccionara contactar a la autoridad y verificar que la asignación entre el nombre y la dirección siga siendo valida.

Para mantener la memoria inmediata con información correcta, los servidores cronometran cada entrada y suprimen las entradas que excedan un tiempo razonable. Cuando el servidor es interrogado respecto a cierta información luego de que ha movido las entradas de información de la memoria inmediata, debe volver a la fuente autorizada y obtener la asignación de nuevo.

Cada vez que una autoridad responde a una solicitud, incluye un valor de Tiempo de Vida (TTL: time to live) en la respuesta, el cual especifica que tanto se garantiza la conservación de la asignación. Así, las autoridades pueden reducir la sobrecarga en la red especificando limites de tiempo largos para entradas en las que se esperan cambios pocos frecuentes, mientras que especifican limites de tiempo cortos para entradas en las que se esperan cambios con frecuencia.

Muchos sistemas operativos mejoran la eficiencia en la traducción de nombres ya que un anfitrión baja la base de datos completa de nombres y direcciones desde un servidor de nombres de dominio local en el arranque, con lo cual mantienen su propia memoria inmediata de nombres utilizados recientemente y utiliza el servidor local solo cuando los nombres no se encuentran o se comunican con este ultimo solo para realizar actualizaciones de su base de datos.

7.3.6 Formato de los mensajes del servidor de dominios

Supongamos que un usuario invoca a un programa de aplicación y proporciona el nombre de la maquina con la que la aplicación desea comunicarse. Antes de poder utilizar protocolos como el TCP o UDP para comunicarse con la máquina especificada, el programa de aplicación debe encontrar la dirección IP de la máquina. Debe pasar el nombre de dominio a la maquina local capaz de resolver el nombre y solicitar una dirección IP. El solucionador local verifica su memoria inmediata y devuelve la respuesta si hay alguna presente. Si el solucionador local no tiene una respuesta, elabora un mensaje y lo envía al servidor(es decir que se convierte en un cliente).

Aun cuando nuestro ejemplo solo comprende un nombre, el formato de mensaje permite a un cliente hacer varias solicitudes dentro de un solo mensaje. Cada uno consiste en un nombre de domino para el que el cliente busca una dirección IP, una especificación de la clase de solicitud (es decir una red de redes) y el tipo de objeto deseado (esto es, la dirección). El servidor responde devolviendo un mensaje similar que contiene respuestas a las solicitudes para las que el servidor tiene asignaciones. Si el servidor no puede responder a todas las preguntas, la respuesta contendrá información acerca de otro servidor de nombres que el cliente puede contactar para encontrar la respuesta.

Aplicaciones

Las respuestas también contienen información acerca de servidores que están autorizados para responder y las direcciones IP de tales servidores. La figura muestra el formato del mensaje, donde cada mensaje comienza con un encabezado fijo. El encabezado contiene el campo único IDENTIFICATION que el cliente utiliza para confrontar las repuestas solicitadas y el campo PARAMETER que especifica la operación solicitada y el código de respuesta. En la tabla se muestra la interpretación de los bits en el campo PARAMETERS.

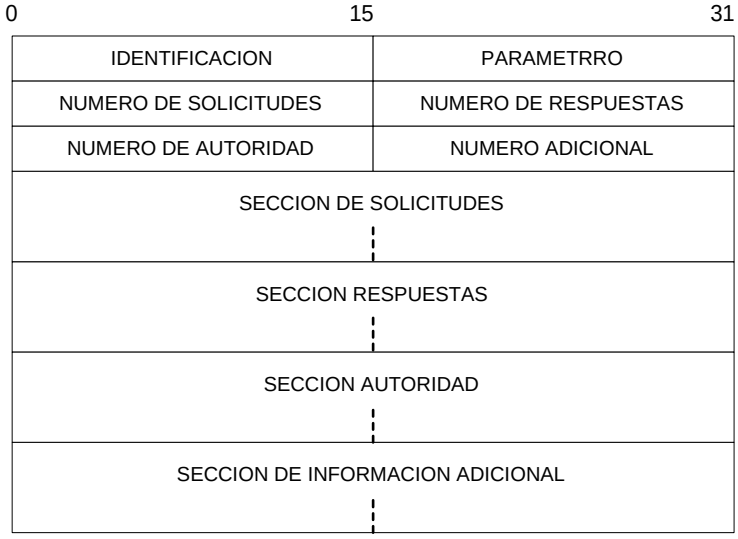


Figura 5.6.1: formato del mensaje de servidor de nombre de dominio

El campo NUMBER OF(Numero de) proporciona un conteo de las entradas en la sesión correspondiente que se presentan en el ultimo mensaje. Por ejemplo, el campo NUMBER OF QUESTIONS(Numero de solicitudes) proporciona el conteo de entradas que aparecen en la QUESTION SECTION(Sección Solicitudes) del mensaje.

QUESTION SECTION contiene las solicitudes para las que se desea una respuesta. El cliente llena solo la sección de solicitud, el servidor devuelve la solicitud y la respuesta en su replica. Cada solicitud consiste en un QUERY DOMAIN NAME(Solicitud del nombre de dominio) seguido por los campos QUERY TYPE(Tipo de solicitud) y QUERY CLASS(Clase de solicitud) como se muestra a continuación.

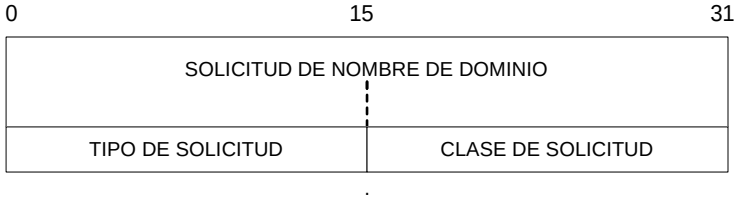


Figura 5.6.2: formato de entrada de información en QUESTION SECTION del mensaje de servidor de dominio

Aplicaciones

El campo QUERY TYPE codifica el tipo de solicitud (por ejemplo, si la solicitud se refiere a un nombre de maquina o a una dirección de correo). El campo QUERY CLASS permite que los nombres de dominio se utilicen para objetos arbitrarios debido a que los nombres oficiales de Internet son solo de una clase. El campo QUERY DOMAIN NAME puede contener un numero arbitrario de objetos. No se utilizan rellenos.

En un mensaje de servidor de nombres de dominio cada uno de los campos ANSWER SECTION(Sección de respuestas), AUTHORITY SECTION(Sección de autoridad) y ADDITIONAL INFORMATION SECTION(Sección de información adicional) consisten en un conjunto de registros de recursos que describen los nombres de dominios y las transformaciones. Cada registro de recurso describe un nombre. La figura muestra el formato. El campo RESOURCE DOMAIN NAME(Nombre de dominio del recurso) contiene el nombre de dominio al que este registro de recursos se refiere. El campo TYPE(Tipo) especifica el tipo de datos incluido en el registro de recurso, el campo CLASS(Clase) especifica la clase de datos.

El campo TIME TO LIVE(Tiempo de vida) contiene un entero que especifica el numero de segundos que la información en este registro de recursos se mantendrá en memoria inmediata. Este campo es utilizado por los clientes que han solicitado la asignación de un nombre y desean capturar el resultado. Los dos últimos campos contienen el resultado de la asignación, con el campo RESOURCE DATA LENGTH(Longitud de datos del recurso) especificando la cantidad de bytes que ocupa el campo RESOURCE DATA(Datos del recurso).

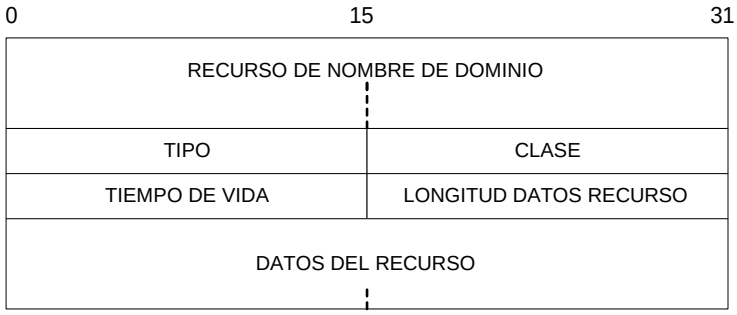


Figura 5.6.3: formato de un registro de recurso utilizado en la última sección de los mensajes devueltos por el servidor de nombre de dominio