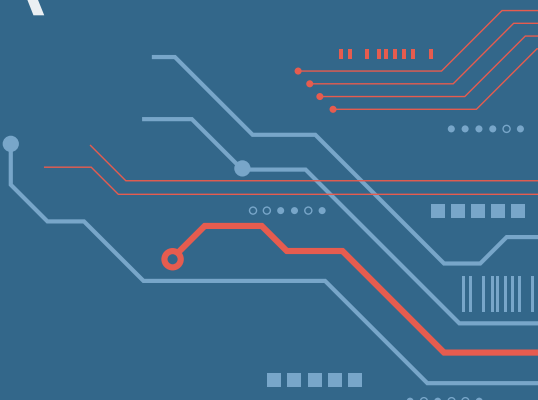


# REDES DE DATOS TUIA | FCEIA UNR

Docentes | 1C 2023

Juan Pablo Michelino  
Emiliano Pavicich  
Andrea León Cavallo  
Iván Pellejero  
Esteban Toribio

jpmich@fceia.unr.edu.ar  
pavicich@fceia.unr.edu.ar  
aleoncavallo@gmail.com  
ivan.pellejero97@gmail.com  
toribio@fceia.unr.edu.ar



# 08



# PROTOSCOLOS DE RED

8.1. DHCP: Dynamic Host Configuration Protocol.

8.2. DNS: Domain Name System.

8.3. NTP: Network Time Protocol.

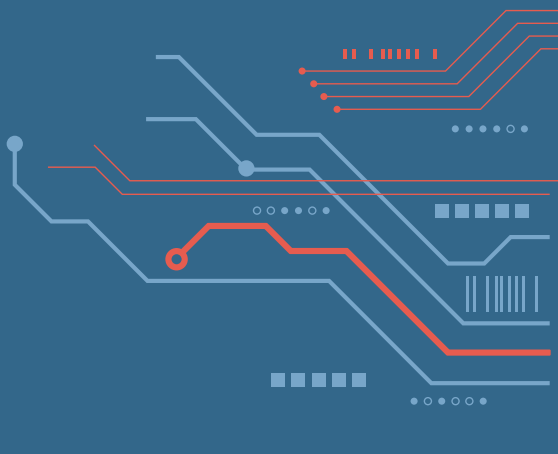
8.4. NAT: Network Address Translation.





# DHCP

Introducción, Mecanismo de asignación de direcciones, DHCP, Formato de mensaje, Tipo de mensajes, Asignación de nueva dirección, DHCP lease renewal process y Consideraciones para DHCP



# Introducción

## Situación:

- IP requiere la configuración de muchos parámetros dentro de la implementación del protocolo.
- IP puede ser utilizado en distintos tipos de hardware de red.

## Problema:

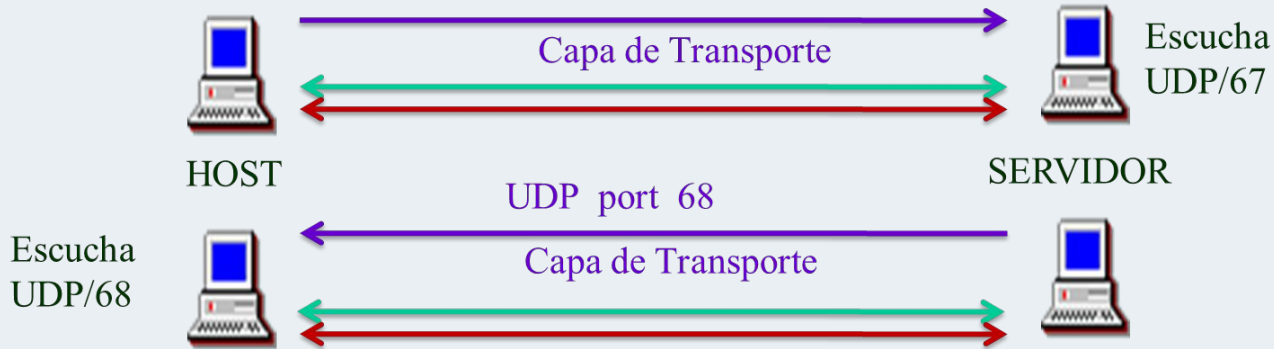
- Los valores para estos parámetros no pueden ser “adivinados” como así tampoco asumir valores por defecto.
- La utilización de un sistema distribuido de asignación de direcciones basado en un mecanismo de polling/defense para descubrir direcciones de red que se encuentran en uso, no puede garantizar la unicidad de las direcciones ya que los hosts pueden no siempre estar en posición de defender su dirección.

# Mecanismos de asignación de direcciones

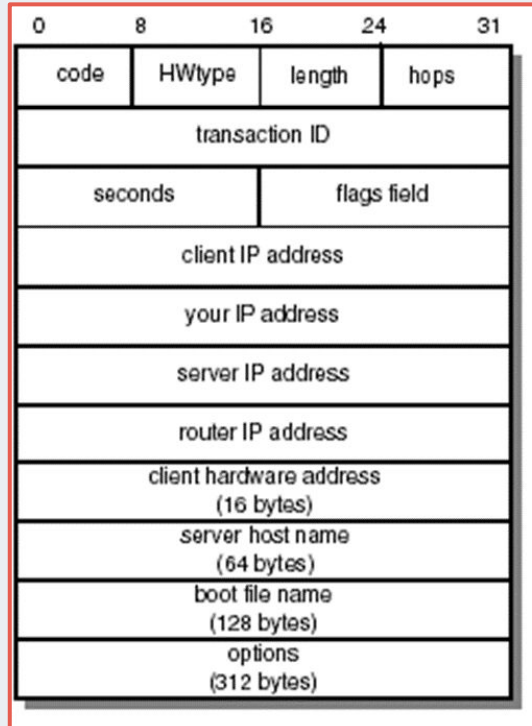
1. Automatic allocation (permanente).
2. Dynamic allocation (por un tiempo limitado - lease). Con esto permite el reuso de direcciones.
3. Manual allocation (asignada por el administrador)

# DHCP: Dynamic Host Configuration Protocol

- DHCP provee un marco de trabajo para pasar información de configuraciones a los hosts en una red TCP/IP.
- Basado y compatible con el protocolo BOOTP. Le agrega la capacidad de asignación automática de direcciones de red reutilizables y opciones de configuración adicionales.

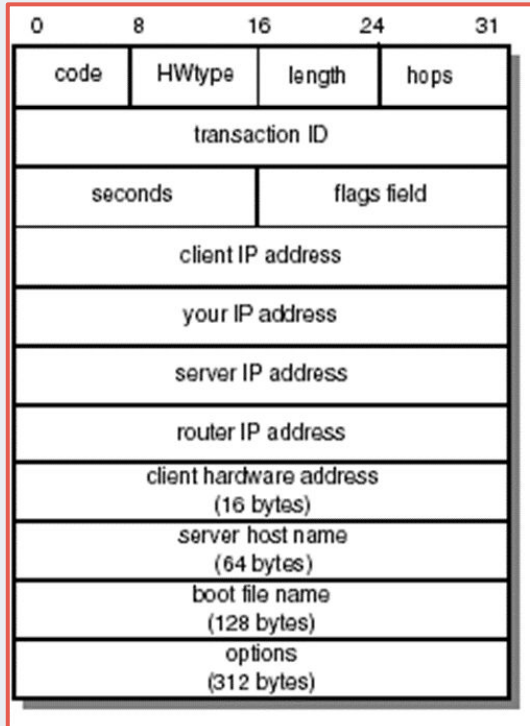


# Formato de mensaje DHCP



- **Code:** Indica request (1) o reply (2)
- **HWtype:** Tipo de hardware. Puede ser Ethernet (1), IEEE 802 (6) u otro.
- **Length:** Longitud de la dirección de Hardware en bytes. Ethernet y token-ring usan 6
- **Hops:** El cliente le asigna el número y es incrementado por routers que retransmiten el pedido a otro servidor. Se utiliza para identificar loops
- **Transaction ID:** Número aleatorio. Hace corresponder el pedido de booteo con la respuesta que se genera.
- **Seconds:** (cliente) Tiempo transcurrido en segundos desde que el cliente comenzó el proceso de booteo.

# Formato de mensaje DHCP



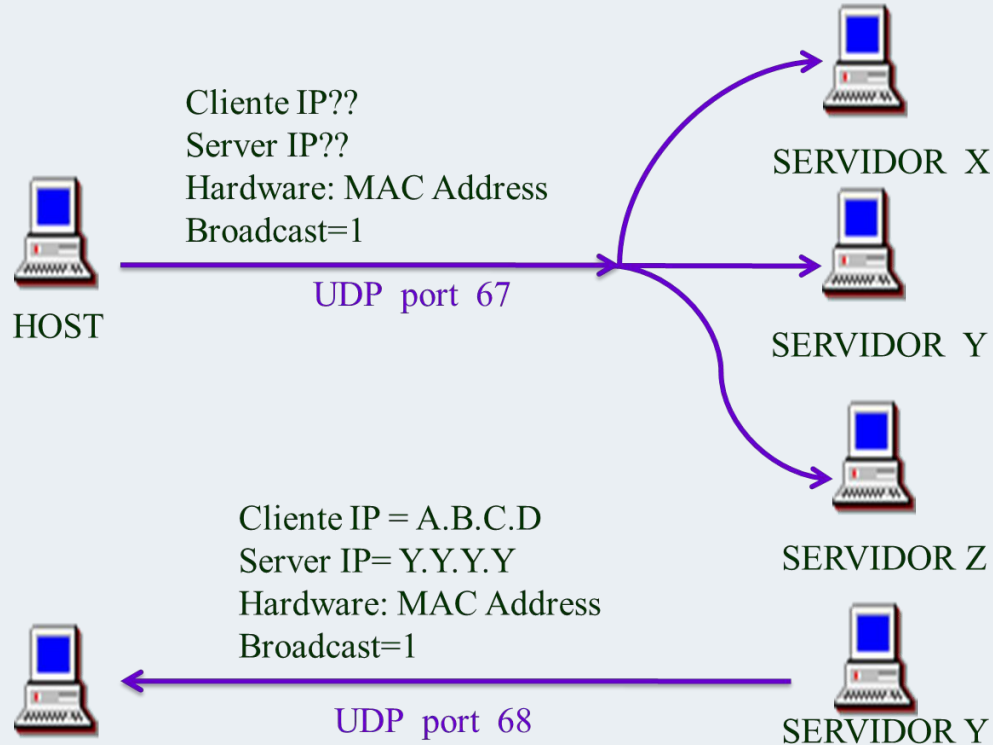
- **Flags field:** El bit más significativo es utilizado como bandera de broadcast.

Los servidores DHCP intentan enviar los mensajes directamente a un cliente utilizando unicast.

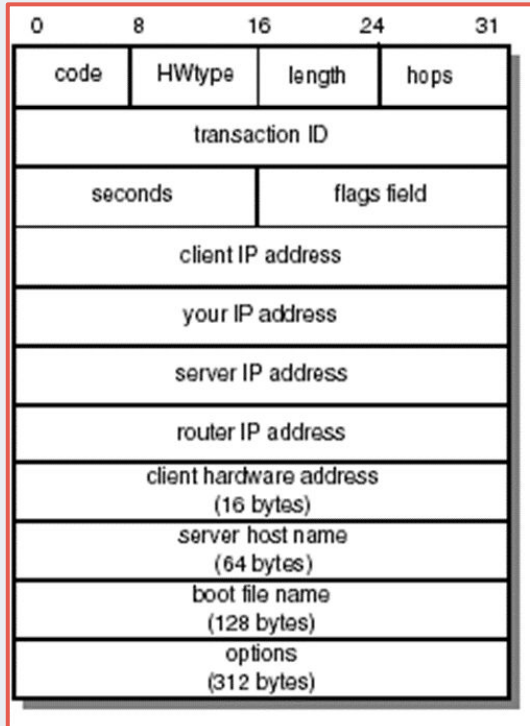
El bit más significativo de *flag field* debe ser configurado a uno para indicarle al servidor que la respuesta DHCP debe ser enviada como una IP y una MAC en forma de broadcast.



# Formato de mensaje DHCP

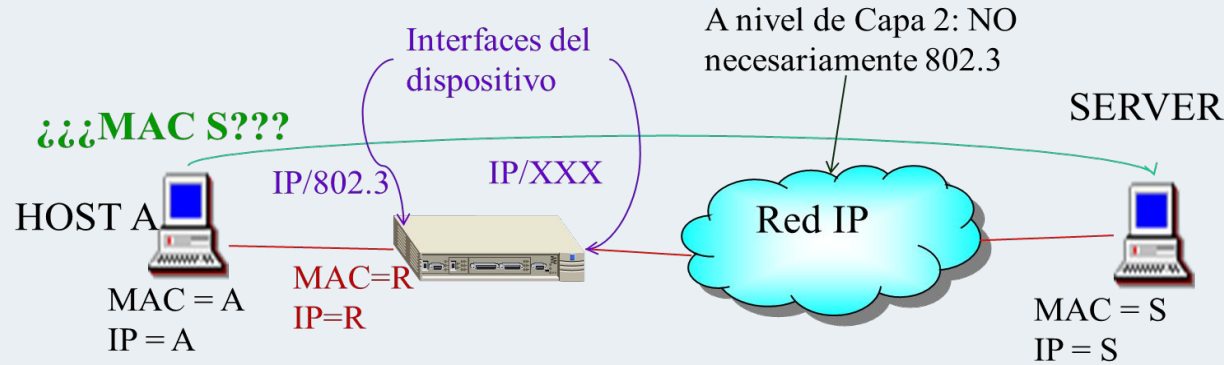


# Formato de mensaje DHCP



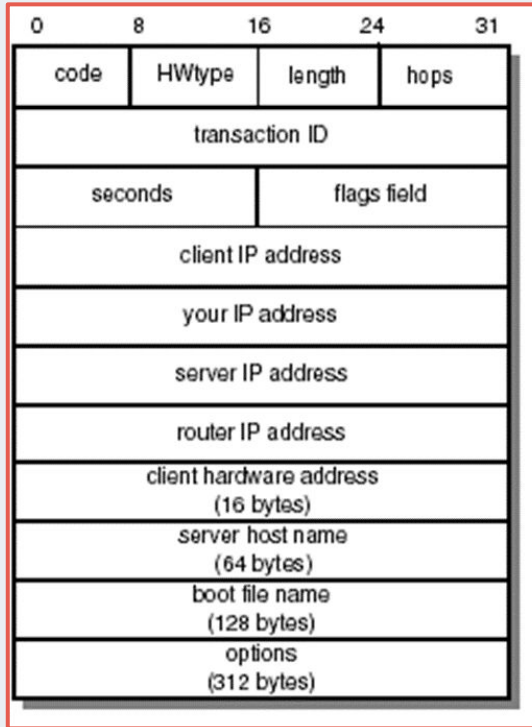
- **Client IP address:** 0.0.0.0. en caso que no se conozca
- **Your IP address:** Asignada por el servidor si el campo de dirección IP del cliente fue 0.0.0.0.
- **Server IP address**
- **Router IP address:** Dirección de un agente retransmisor BOOTP.

# Formato de mensaje DHCP



Los dispositivos de capa 3 (router, por ejemplo), en general, descarta todo aquello que llegue con dirección 0.0.0.0. Para que funcionen como **Agente Retransmisor**, debe entender el protocolo DHCP/BOOTP y asignarle su propia MAC, debe ser capaz de realizar BOOTP Forwarding (Utiliza HOP) y debe tener la dirección IP del servidor y poner su dirección IP=R

# Formato de mensaje DHCP



- **Client hardware address:** DHCP define una opción de identificador de cliente. Si no se utiliza el cliente es identificado por su MAC address.
- **Server host name:** (Opcional).
- **Boot file name:** (Cliente) nulo o se especifica un nombre genérico, como un router, indicando el tipo de archivo de booteo a utilizar.
- **Options:** Primeros 4 bytes contienen “*the magic cookie*” (99.130.83.99). El resto consiste de diversos parámetros. Por ejemplo T1, T2 y LT.

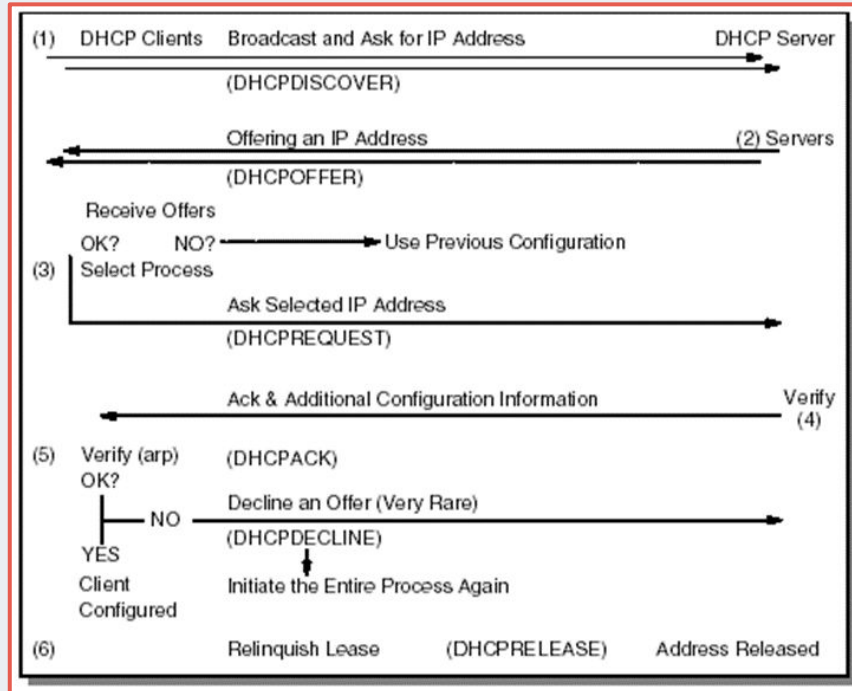
# Tipos de mensajes

- **DHCPDISCOVER** (Cliente a Servidor): Broadcast para encontrar servidores DHCP disponibles.
- **DHCPOFFER** (Servidor a Cliente): Respuesta a DHCPDISCOVER y ofrecimiento de dirección IP y otros parámetros.
- **DHCPREQUEST** (Cliente a Servidor):
  - Solicitud de uno de los parámetros ofrecidos y rechazo de los otros.
  - Verificación de una asignación previa de una dirección después de un cambio en el sistema o la red (reboot).
  - Solicitud de extensión del “arrendamiento” (lease) de una dirección.
- **DHCPACK** (Servidor a Cliente): Acuse positivo con parámetros y dirección IP.

# Tipos de mensajes

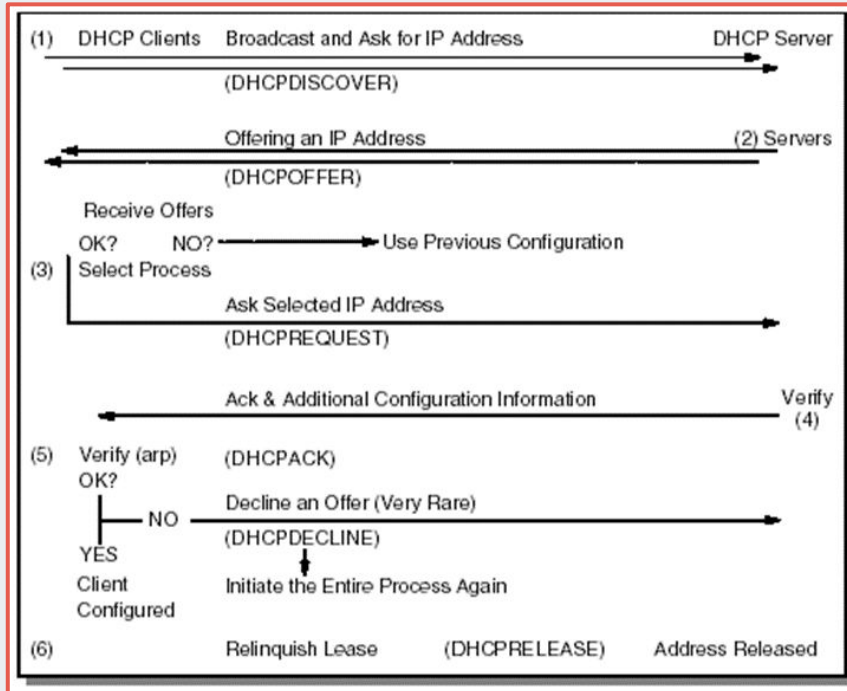
- **DHCPNACK** (Servidor a Cliente): Acuse negativo. Expiración del tiempo o dirección incorrecta.
- **DHCPDECLINE** (Cliente a Servidor): Dirección ofrecida en uso.
- **DHCPRELEASE** (Cliente a Servidor): Cancelar y liberar la dirección.
- **DHCPINFORM** (Cliente a Servidor): Solicitud de más parámetros de configuración al servidor DHCP por parte de un cliente que ya tiene una dirección IP (configurada manualmente, por ejemplo).

# Asignación de una nueva dirección



El cliente desconoce su dirección y se asume que el servidor DHCP posee un grupo de direcciones de red con las cuales puede satisfacer la solicitud. Cada servidor mantiene una base de datos con las direcciones asignadas.

# Asignación de una nueva dirección



1. El cliente envía un mensaje broadcast **DHCPDISCOVER** a su propia subnet (local physical subnet).

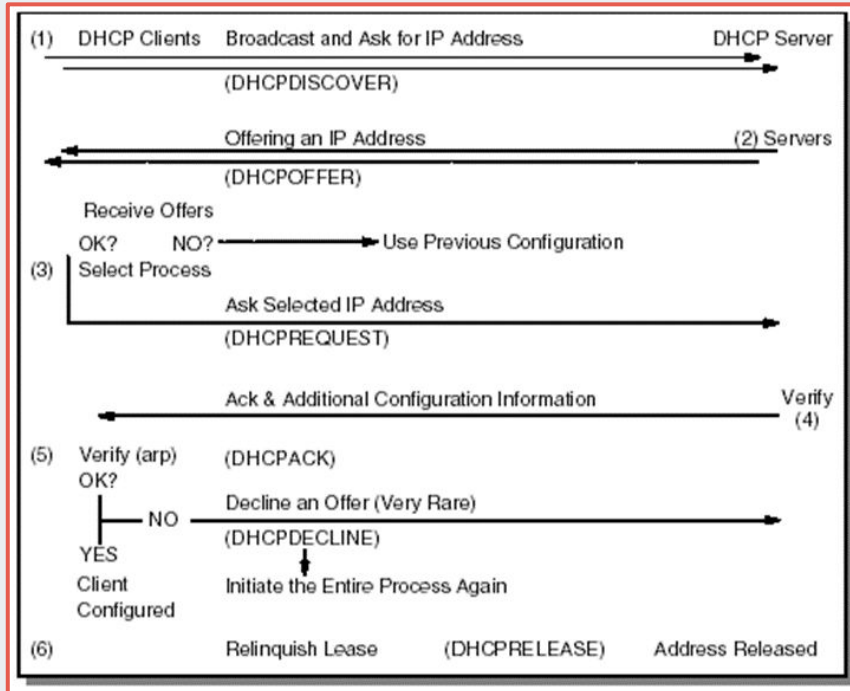
*El mensaje puede incluir algunas opciones como por ejemplo la sugerencia de una dirección IP determinada o el tiempo de asignación (lease duration).*

2. Cada servidor puede responder con un mensaje **DHCPOFFER** que incluya una dirección IP disponible y otras opciones de configuración.

*El servidor debe registrar el ofrecimiento de esta dirección para evitar asignarla nuevamente a otros clientes antes de que se haya terminado el proceso en cuestión.*



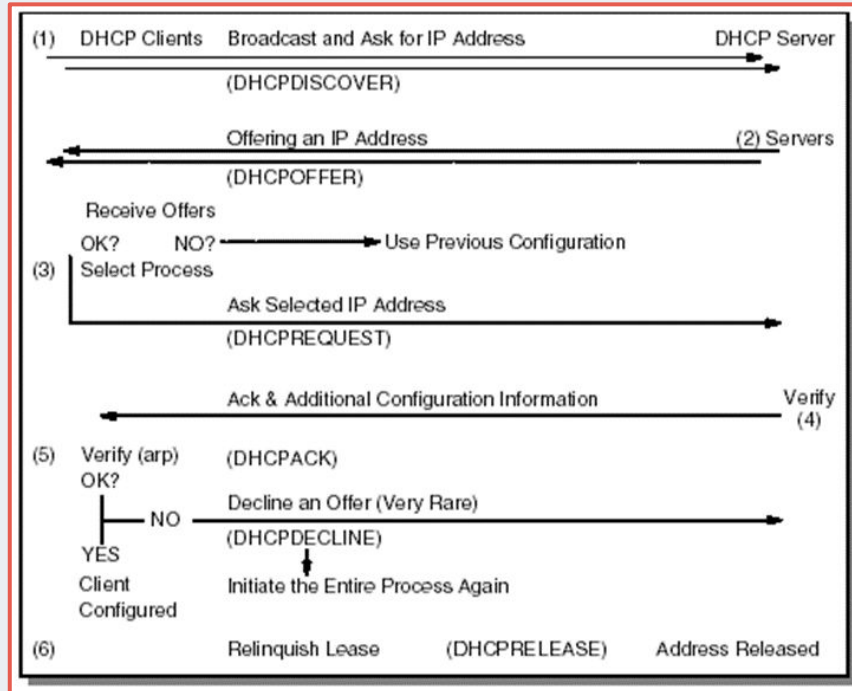
# Asignación de una nueva dirección



3. El cliente recibe uno o más mensajes **DHCPOFFER** de uno o más servidores. El cliente elige y envía un mensaje broadcast **DHCPREQUEST** que incluye la identificación del servidor de forma tal de indicar el mensaje y la correspondiente dirección IP que ha seleccionado.

*En el caso que no se reciba ningún DHCPOFFER, si el cliente tiene conocimiento de una dirección de red previamente asignada, este puede reutilizarla siempre y cuando el tiempo de asignación (lease) aún siga siendo válido y hasta que el mismo expire.*

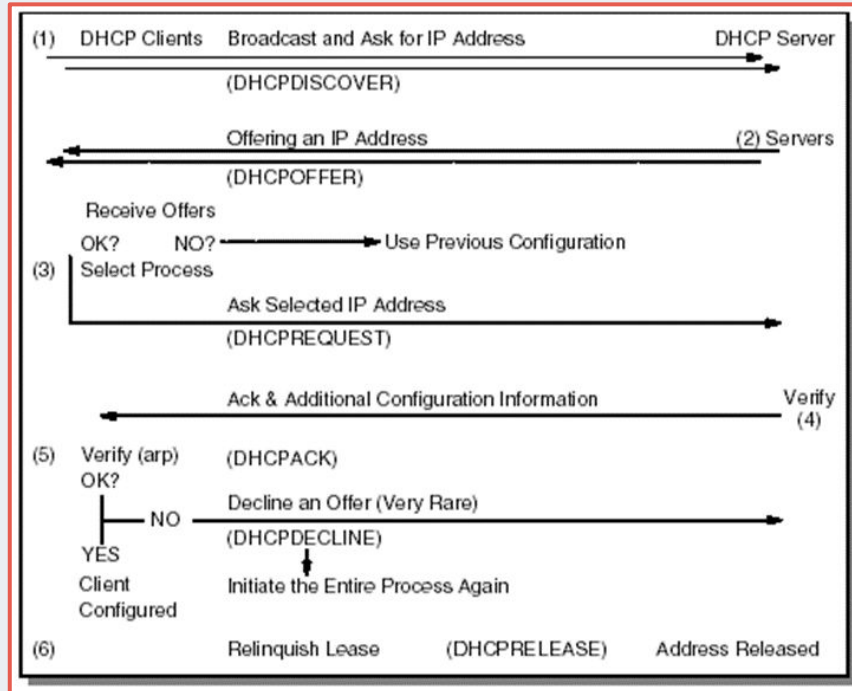
# Asignación de una nueva dirección



- Los servidores reciben el mensaje broadcast **DHCPREQUEST** del cliente. El servidor seleccionado registra la asignación y responde con un mensaje **DHCPACK** que contiene los parámetros de configuración requeridos por el cliente. Los no seleccionados, utilizan este broadcast como notificación de la declinación del cliente al ofrecimiento.

*La combinación de “client hardware” y “assigned network address” constituyen un identificador único para el cliente y son utilizados tanto por el cliente como por el servidor para identificar referencias al arrendamiento en cualquier mensaje DHCP. El campo “your IP address” en el mensaje DHCPACK se completa con la dirección de red seleccionada.*

# Asignación de una nueva dirección

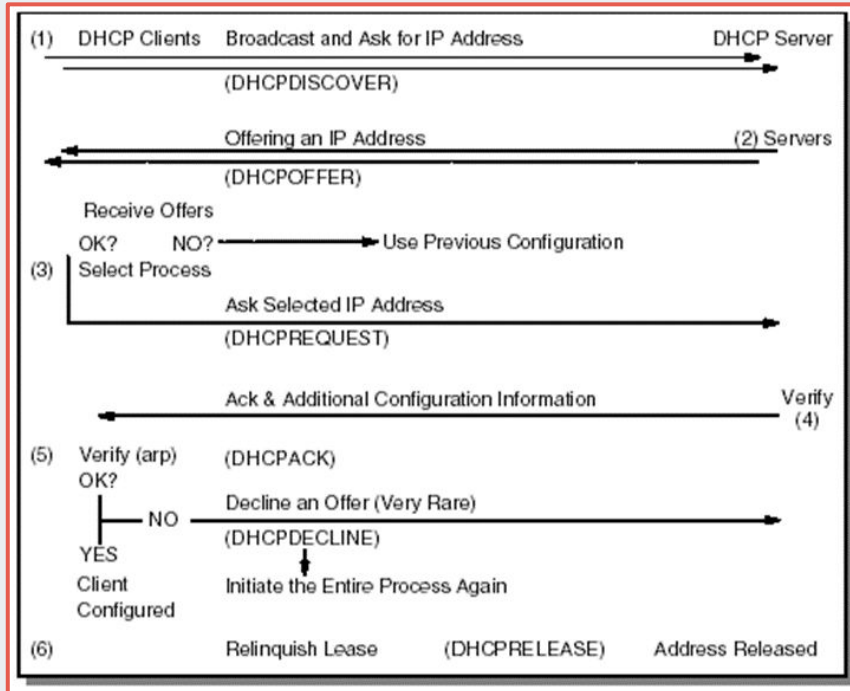


5.a. El cliente recibe el mensaje **DHCPACK** con los parámetros de configuración, realiza una verificación final (por ejemplo con las tabla ARP) y registra la duración y la cookie del arrendamiento.

*Si el cliente detecta un problema con los parámetros en el mensaje DHCPACK, envía un mensaje **DHCPDECLINE** al servidor, espera un mínimo de 10 segundos y reinicia el proceso de configuración.*

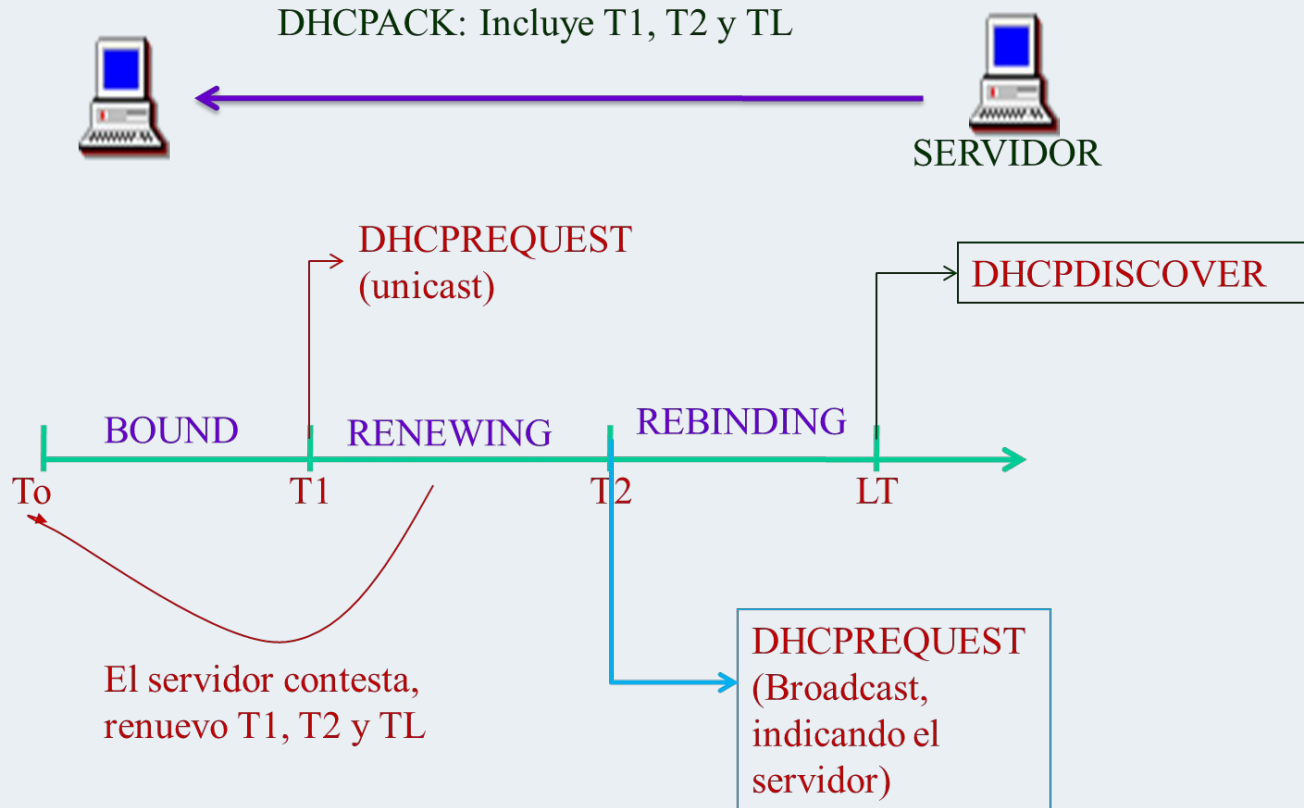
5.b. En caso de recibirse un mensaje de **DHCPDECLINE**, el server marca esa dirección como no disponible e informar al administrador de sistema. Si el cliente recibe un mensaje **DHCPNAK**, debe comenzar nuevamente el proceso de configuración.

# Asignación de una nueva dirección

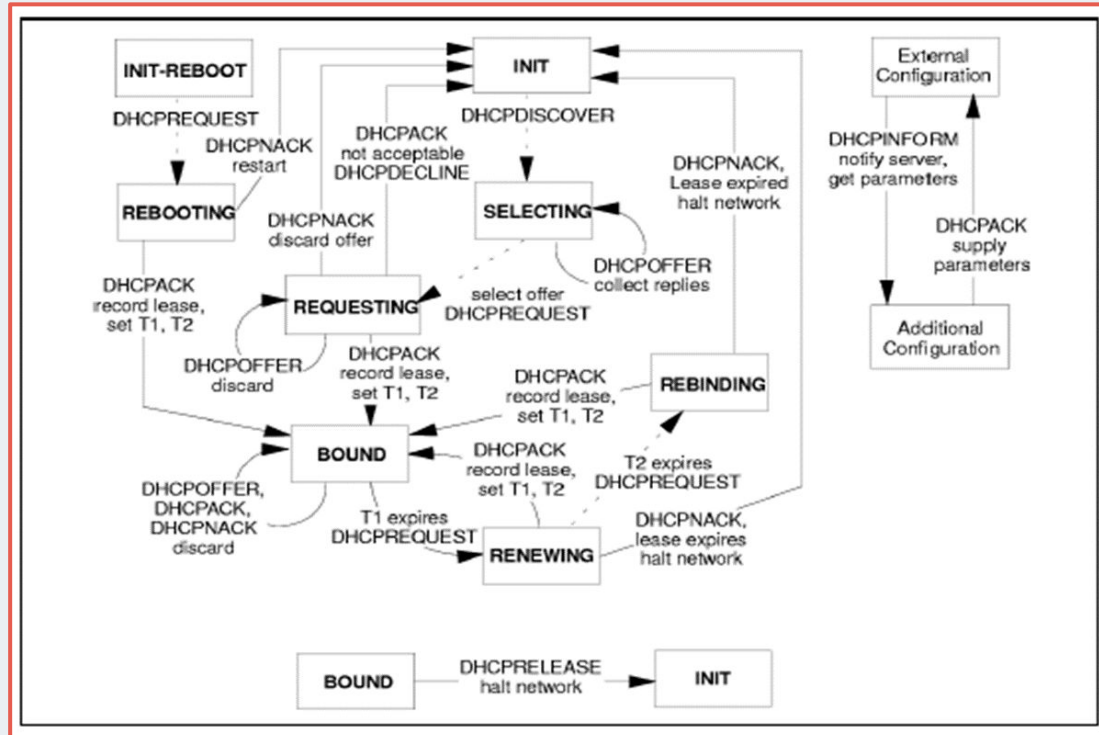


6. El cliente puede liberar la dirección IP mediante el envío de un mensaje **DHCPRELEASE** al servidor.

# DHCP lease renewal process



# DHCP lease renewal process



# Consideraciones para DHCP

## Aspectos positivos

- **Simplifica la tarea del administrador:** DHCP asigna en forma dinámica las direcciones IP y los parámetros de configuración liberando a los administradores de red de una pesada tarea manual.
- **Facilita la movilidad de los dispositivos:** La facilidad para un dispositivo de ser trasladado de una red a otra y automáticamente obtener parámetros de configuración válidos puede ser de gran utilidad en usuarios móviles.
- **Reciclado de direcciones IP:** Las direcciones IPs son asignadas únicamente cuando los clientes se encuentran activos, esto hace posible, mediante el uso de períodos de arrendamientos cortos y el hecho que los clientes móviles no necesitan tener asignada más de una dirección, reducir el número total de direcciones en la organización.
- **Interoperabilidad BOOTP/DHCP:** El formato del mensaje DHCP está basado en el de BOOTP, lo cual habilita a clientes BOOTP y DHCP a inter-operar. Cada mensaje DHCP contiene una opción de tipo de mensaje (51). Cualquier mensaje sin esta opción se asume como cliente BOOTP.

# Consideraciones para DHCP

## Aspectos negativos:

- **Inseguro:** DHCP utiliza UDP, el cual es inherentemente inseguro.
- **Clientes no autorizados:** Un cliente no autorizado podría conectarse a la red y obtener una dirección IP y parámetros de configuración válidos.

Para prevenir esto, es posible pre asignar direcciones IPs con direcciones MAC. Esto incrementa el trabajo del administrador y quita el beneficio del reciclado de direcciones.

- **Servidores no autorizados:** También pueden activarse servidores DHCP no autorizados, enviando información falsa a los clientes.



# Consideraciones para DHCP

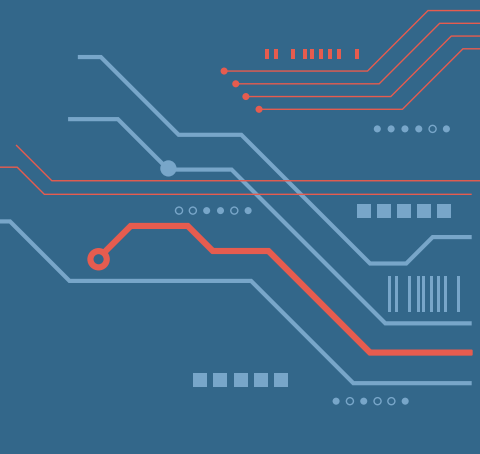
## Relación IP con DHCP Dinámica:

En un ambiente donde se está utilizando asignación dinámica de direcciones, por lo general no es posible predeterminedar la dirección IP de un cliente en un tiempo dado. En este caso, si se están utilizando servidores DNS estáticos, estos no poseerán vinculaciones válidas entre direcciones IP y nombres para los clientes. Si las entradas de estos clientes en el DNS son importantes, es posible utilizar DHCP manual para estos clientes y así poder relacionarlos correctamente en el servidor DNS.



# DNS

Acceso a recursos y aplicaciones; Problema y Solución; DNS;  
Espacio de nombres jerárquicos; Nombres; Administración  
jerárquica; Dominios de nivel superior; Administración de  
zonas; Resolución de nombres de dominio; Búsqueda DNS;  
Respuestas DNS; Operación del servidor DNS; Transporte;  
Registro; Formato de los registros de recursos; Formato del  
mensaje DNS; Sección de Consulta y Sección de Registros de  
Respuesta, Autoridad y recursos extras



# Acceso a recursos y aplicaciones

- Sistema de Nombres de Dominio se describe en la RFC 1034 y RFC 1035
- En los comienzos de Internet únicamente se utilizaban direcciones IP numéricas.
- Se incorporan nombres. Problema de mantenimiento del mapeo con las direcciones IP
- Inicialmente, la vinculación entre los nombres de host y las direcciones IP eran mantenidas por el NIC en un único archivo (HOSTS.TXT), el cual era descargado por todos los hosts mediante FTP. A esto se le denominaba *flat namespace*.

# Problema

- Vinculación de hostnames con direcciones IP
  - “foobar.cs.colorado.edu” con una dirección IP como 128.138.241.71
  - Crecimiento de cantidad de hosts

# Solución

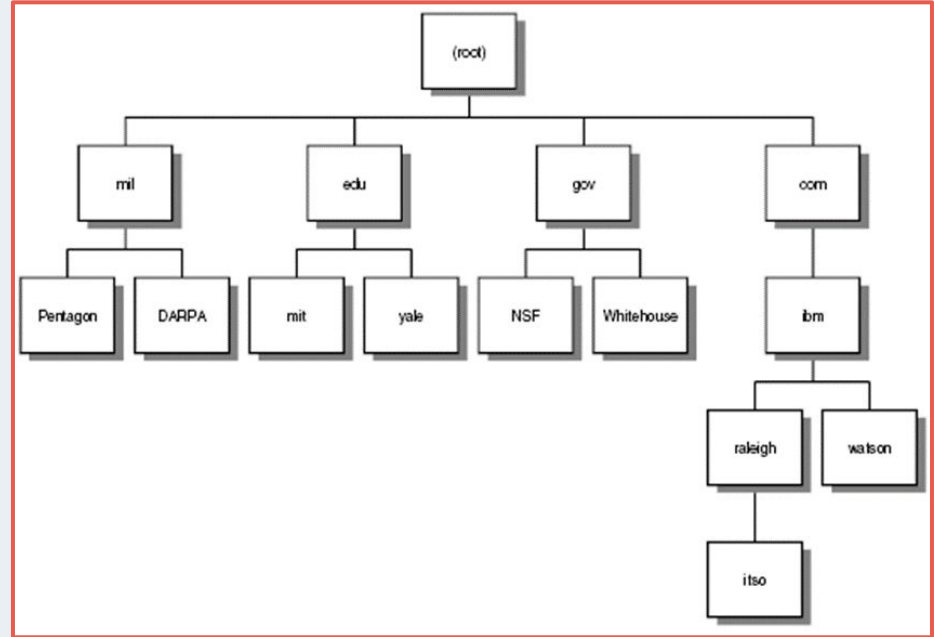
- Domain Name System (DNS)
  - Base de datos distribuida
  - Un “resolver” mapea nombres con direcciones IP utilizando servidores de nombres

# Domain Name System

- Un sistema DNS es, básicamente, una base de datos distribuida y jerárquica que almacena información asociada a los nombres de dominio en redes como lo es Internet.
- Esta base de datos está mantenida por miles de servidores DNS y cada uno de ellos es responsable de una “zona” en Internet.
- Como base de datos, el DNS es capaz de asociar distintos tipos de información a cada nombre, pero sus usos más comunes son:
  - La asignación de nombres de dominio a direcciones IP.
  - La localización de los servidores de correo electrónico de cada dominio.

# Espacio de nombres jerárquicos

Es una base de datos jerárquica porque los nombres de dominio son nodos que descienden de la raíz de la base de datos representada por el nodo raíz (".") al estilo de como funcionan los sistemas de ficheros en Unix.

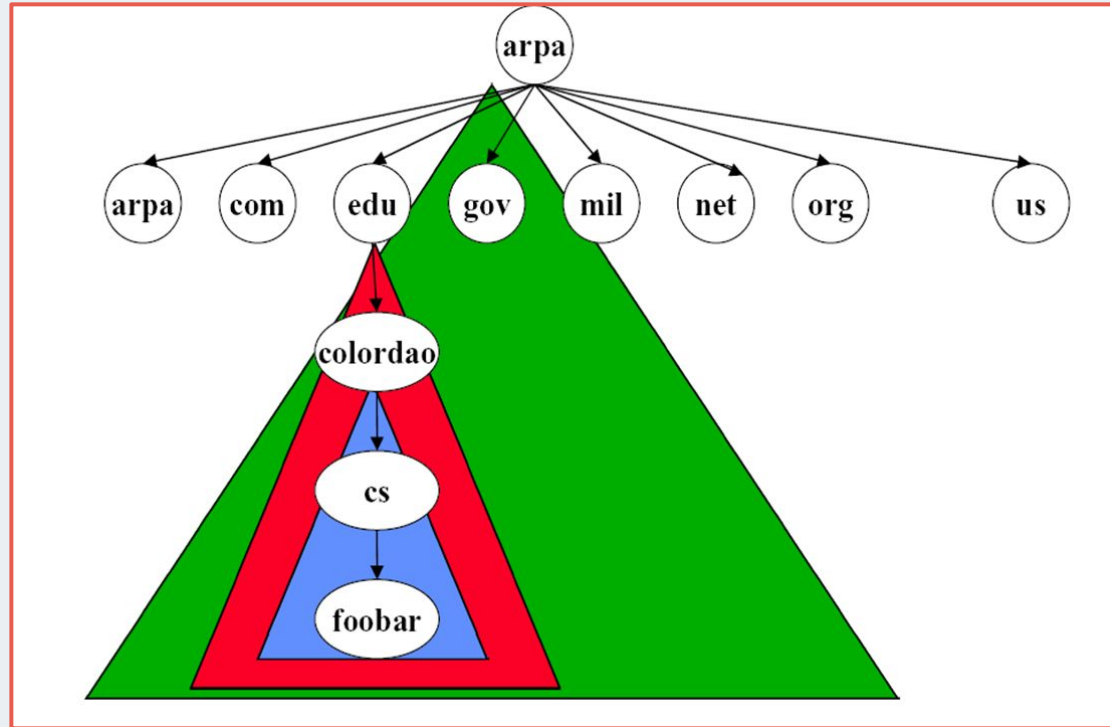


# Nombres

- El nombre de dominio específico de un host está compuesto de una secuencia de nombres, cada uno de los cuales puede tener hasta 63 caracteres de longitud, separados por puntos.
- Un dominio se dice que es un dominio de nombre absoluto (absolute domain name) o un nombre de dominio completamente calificado (FQDN: Fully Qualified Domain Name) si este termina con un punto.
  - “foobar.cs.colorado.edu.”
- La mayoría de los dominios genéricos (.com, .edu, etc) son internacionales, no obstante .gov y .mil son específicos de lo USA.



# Administración jerárquica

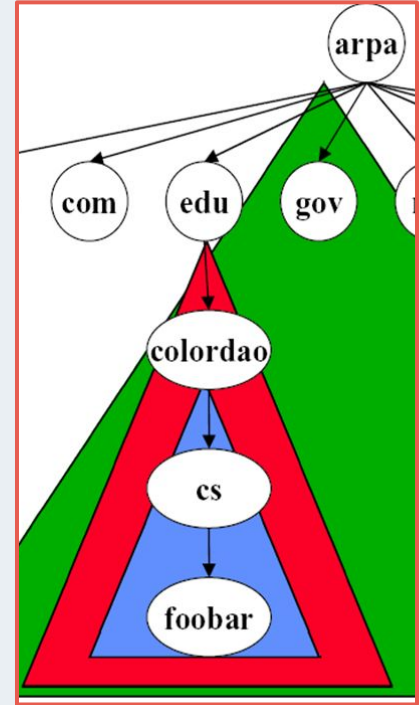


# Dominios de nivel superior

Domain Name	Meaning
com	Commercial organizations
edu	Educational institutions
gov	Government institutions
int	International organizations
mil	U.S. military
net	Major network support centers
org	Non-profit organizations
country code	ISO 2-letter identifier for country specific domains

# Administración de zonas

- Una zona es un “sub-árbol” del árbol DNS que es administrado en forma independiente.
- Los dominios de segundo nivel (“colorado.edu”) son usualmente zonas independientes.
- La mayoría de los sub-dominios (“cs.colorado.edu”) son independientes.
- Una zona debe proveer múltiples servidores de nombres. Estos servidores registran los miembros en el dominio.
- Usualmente es necesario un servidor de nombres primario y uno o más servidores de nombres secundarios, éstos últimos recopilan la información del servidor primario a través de una *transferencia de zona*.



# Resolución de nombres de dominio

- La resolución de nombre de dominio es un proceso del tipo cliente/servidor.
- La función del cliente (denominado *resolver*) es transparente para el usuario
  - Es llamada por las aplicaciones para resolver nombres simbólicos en direcciones IP o viceversa.
- El servidor de nombre de dominio, como su nombre lo indica, es la aplicación del servidor.

# Resolución de nombres de dominio

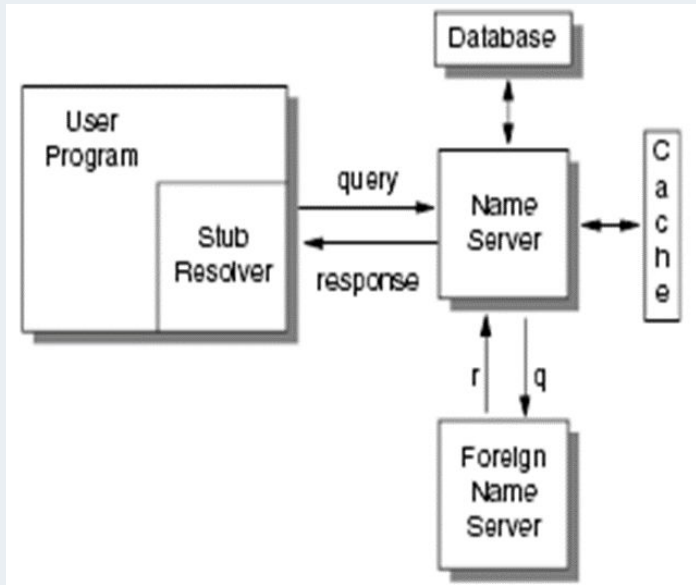
- Un programa de usuario realiza una llamada de sistema del tipo *gethostbyname()*.
  - Esta llamada particular es utilizada para preguntar por la dirección IP de un host mediante la entrega de un nombre.
- El “resolver” realiza una búsqueda en el servidor de nombres.
  - Full resolvers: Poseen en cache una base de nombres para consultar primero.
  - Stub resolvers: No poseen esta base en cahe.

# Resolución de nombres de dominio

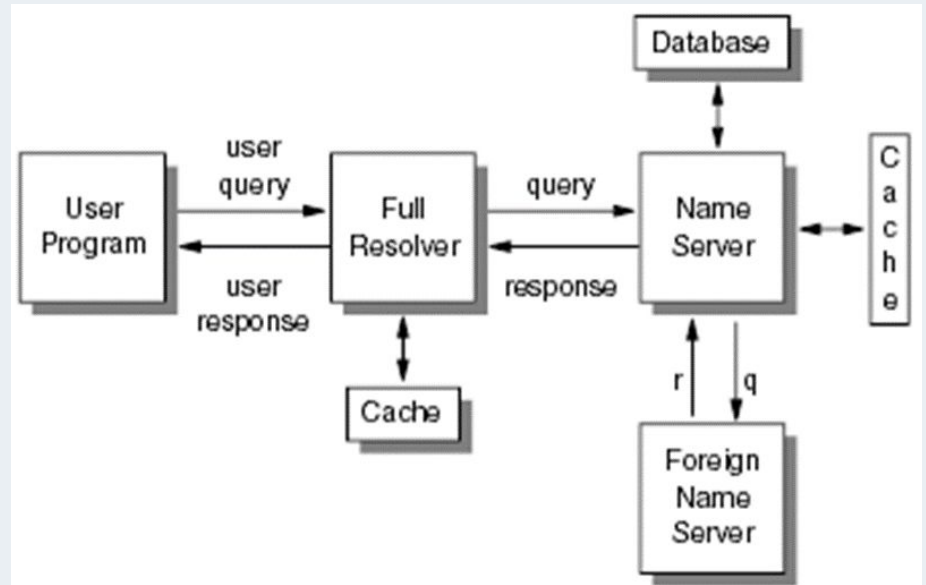
- El servidor de nombres verifica si la respuesta está en su base de datos local (authoritative) o en su cache, si es así, devuelve la respuesta al cliente.
  - En caso contrario, buscará otro/s servidor/es de nombres disponible(s), comenzando por el raíz (root) del árbol DNS o en lo más alto del árbol que le sea posible.
- Finalmente, el programa de usuario recibirá la correspondiente dirección IP (o el nombre de host, dependiendo del tipo de búsqueda) o un error si la búsqueda no arrojó ningún resultado.
- Los mensajes de búsqueda/respuesta son transportados en UDP/53 o TCP/53

# Resolución de nombres de dominio

Sub-resolver



Full-resolver



# Búsqueda DNS

Las búsquedas pueden ser de dos tipos:

- **Recursiva:** El propio servidor debe realizar la búsqueda completa.
- **Iterativa:** El servidor devuelve sólo la información que tiene disponible y una lista de servidores adicionales.

*Una bandera (un bit) en el mensaje de búsqueda especifica si el cliente desea o no una búsqueda recursiva. Un bit en el mensaje de respuesta indica si el servidor soporta búsquedas recursivas.*



# Respuestas DNS

- a) Sí la bandera de **búsqueda recursiva** no se encuentra configurada o el servidor no soporta consultas recursivas, este retornará sólo la información que posea en la caché y una lista de servidores DNS adicionales a ser contactados.
  
- b) Si la **búsqueda recursiva** se encuentra configurada en la solicitud y el servidor soporta dicho tipo de búsquedas, este realizará la solicitud a otro servidor de nombre:
  - i) Podrá ser un servidor de nombre con autoridad sobre el dominio en cuestión o uno de los servidores raíz.
  - ii) Si el segundo servidor no contesta con una respuesta autoritativa, el proceso se repite.
  - iii) Una vez obtenida la respuesta el servidor almacenará la misma en su caché. Este valor es almacenado por un tiempo máximo especificado en el campo de 32 bits TTL (entre 86,400 y 172,800 seg –1 y 2 días- es un valor típico)

# Operación del servidor DNS

- **Primario:** Un servidor DNS primario carga la información de zona de disco y tiene autoridad sobre la zona.
- **Secundario:** Un servidor DNS secundario tiene autoridad sobre la zona pero obtiene la información de zona de un servidor DNS primario mediante un proceso denominado *transferencia de zona* (zone transfer).
  - Para mantenerse sincronizado, el servidor secundario realiza consultas al primario en forma regular y ejecuta una transferencia de zona si el servidor primario ha sido actualizado.
- **Caching-only:** Es un servidor de nombres que no tiene autoridad sobre la zona y obtiene toda la información de los servidores primarios o secundarios.

# Operación del servidor DNS

- Un servidor de nombres puede operar para múltiples dominios, pudiendo funcionar como primario para alguno de ellos y como secundario para otros.
- Los servidores primarios y secundarios realizan todas las funciones de un servidor de sólo caché (caching only).

# Transporte

Los mensajes en DNS son transmitidos, tanto por datagramas UDP como vía conexiones TCP.

- **UDP/53:** Restringidos a 512 bytes de longitud, los mensajes más largos son truncados y el bit de truncado TC es activado en el encabezado.
- **TCP/53:** En este caso, el mensaje es precedido por un campo de 2 bytes indicando la longitud total del paquete.

# Registro

- La base de datos distribuidas de DNS se encuentra compuesta por registros de recursos (resource records - RRs), los cuales se encuentran divididos en clases en función del tipo de red.
- Los Registros de Recursos proveen un mapeo entre nombres de dominios y objetos de red.
- Los objetos de red más comunes son las direcciones de Internet de los hosts, sin embargo DNS está diseñado para acomodarse a un amplio rango de objetos diferentes.

# Formato de los registros de recursos

Name	TTL	Class	Type	RData
------	-----	-------	------	-------

**Name:** Nombre de Dominio a ser definido.

Las reglas para la composición de nombres en DNS es muy general:

- Una serie de etiquetas (labels) compuestas por caracteres alfanuméricos o guiones
- Cada etiqueta puede tener una longitud entre 1 y 63 caracteres
- Debe comenzar con un carácter alfabético.
- El uso de mayúsculas o minúsculas es indistinto en los nombres de dominio.

# Formato de los registros de recursos

Name	TTL	Class	Type	RData
------	-----	-------	------	-------

**TTL:** Tiempo, expresado en segundos, durante el cual un registro será válido en la caché de un servidor de nombres. Este se encuentra almacenado en el DNS como un valor, sin signo, de 32 bits. 86400 es un valor típico (1 día) para registros apuntando direcciones IPs.

# Formato de los registros de recursos

Name	TTL	Class	Type	RData
------	-----	-------	------	-------

**Class:** Identifica la familia de protocolos.

El más comúnmente utilizado es IN (Internet)



# Formato de los registros de recursos

Name	TTL	Class	Type	RData
------	-----	-------	------	-------

**Type:** Identifica el tipo de recurso dentro del registro.

# Formato de los registros de recursos

Tipo	Valor	Significado
A	1	Una dirección de host
CNAME	5	Nombre canónico. Especifica un alias para un host.
HINFO	13	CPU y OS del host. Es solo un campo de comentario.
MX	15	Servidor de mail de un dominio.
NS	2	El servidor autoritativo de un dominio.
PTR	12	Un puntero a otra parte del espacio de nombres de dominio.
SOA	6	El inicio de una zona de autoridad.
WKS	11	Well-known service. Especifica algún servicio que está siempre activo en éste host.

# Formato de los registros de recursos

Name	TTL	Class	Type	RData
------	-----	-------	------	-------

**Rdata:** Su valor depende del campo Type:

- **A:** Dirección IP de 32 bits
- **CNAME:** Un nombre de dominio
- **MX:** Un valor de preferencia de 16-bit preference value (valores bajos son preferidos) seguidos de un nombre de dominio
- **NS:** Un nombre de dominio
- **PTR:** Un nombre de dominio

# Formato del mensaje DNS

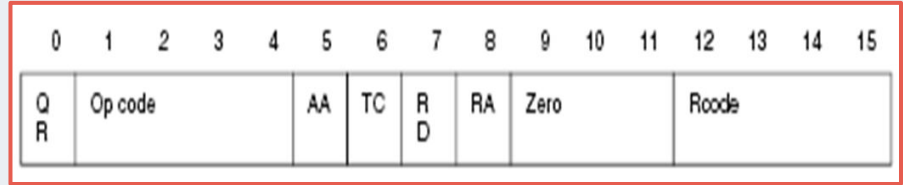
Identification	Flags
Number of questions	Number of answer RR's
Number of authority RR's	Number of additional RR's
Question	
Answers	
Authority	
Additional Information	

# Formato del mensaje DNS

**Identification:** Configurado por el cliente, devuelto por el servidor. Utilizado para que los clientes asocien consultas con respuestas.

## Banderas o Parámetros:

- **QR:** Identifica si es una consulta (0) o una respuesta (1)
- **Op Code:** Identifica el tipo de consulta (Standard, Inversa, Status, etc)
- **AA:** Bandera de respuesta autoritativa.
- **TC:** Bandera de respuesta truncada.
- **RD:** Bandera de recursión deseada.
- **RA:** Bandera de recursión disponible.
- **Zero:** Reservado para uso futuro.
- **RCode:** Código de respuesta (0-Sin error, 1-Error en formato, 2-Servidor no disponible, 3-Error de nombre, 4- No implementado, 5-Rechazado)



# Formato del mensaje DNS

**Questions:** nombre de host a resolver. Enviado en la consulta, devuelto en la respuesta.

**Answers:** Respuesta a las preguntas, únicamente en las respuestas. Es posible obtener múltiples respuestas por pregunta.

**Authority:** ¿Qué host es servidor de nombres con autoridad para esta búsqueda?

# Sección de Consulta

**length:** Un byte que indica la longitud de la siguiente etiqueta.

**label:** Un elemento del nombre de dominio.

**00:** Indica el final del nombre de dominio y representa la etiqueta nula para el dominio raíz.

**Type:** 2 bytes especificando el tipo de consulta.

**Class:** 2 bytes especificando la clase de la consulta.  
Para Internet IN.

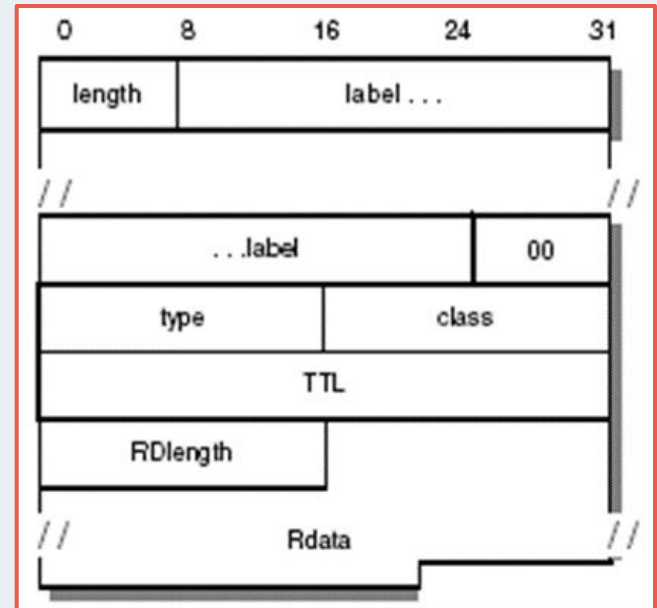


# Sección de Registros de Respuesta, Autoridad y recursos extras

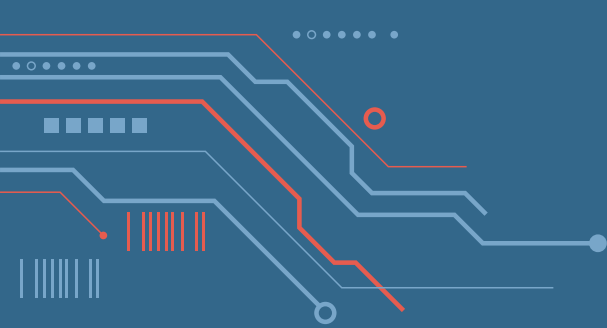
**TTL:** Tiempo de vida para el registro expresado en segundos mediante un valor de 32-bit.

**RDlength:** Campo de 16-bits indicando la longitud para el campo Rdata.

**Rdata:** Cadena de longitud variable.

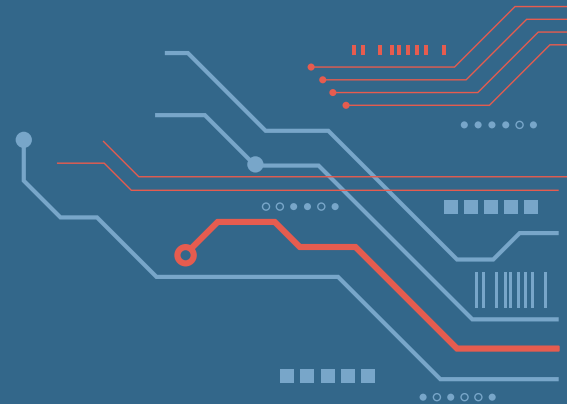






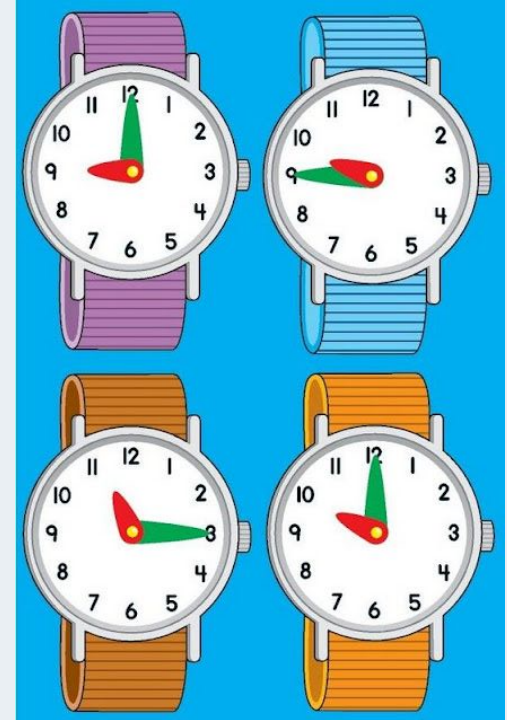
# NTP

Problema, Solución, UTC, NTP, Estratos de reloj, Intercambio de mensajes y Network Time Protocol.



# Problemática

- Cada host tiene un reloj
- Cada host registra (de forma local o remota) cuando ocurre cada evento.
- Tenemos que hacer un seguimiento de eventos entre dos o más hosts. ¿Qué pasa si los relojes no están sincronizados?



# Solución

- Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos.
- NTP trabaja de manera cliente/servidor y utiliza UDP como su capa de transporte, usando el puerto 123.
- Está diseñado para resistir los efectos de la latencia variable.
- La versión actual es la número 4 y está documentado en las RFC 778, RFC 891, RFC 956, RFC 958, RFC 1305, RFC 4330 y RFC 5905.

# Coordinated Universal Time (UTC)

- Es el estándar internacional para medir el tiempo.
- Es un sistema de tiempo de referencia que se utiliza como base para la medición de la hora en todo el mundo.

*Es una escala de tiempo atómica y se basa en la rotación de la Tierra en relación con el sol, pero es ajustada regularmente mediante la introducción de segundos intercalares para mantenerla en sincronía con la rotación de la Tierra.*



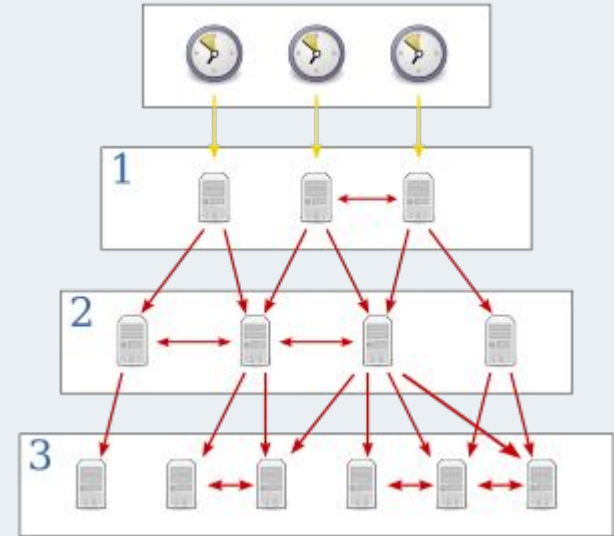
*El punto de hora 0 de UTC es conocido como el Meridiano de Greenwich y se encuentra en el Observatorio Real de Greenwich (Londres, Reino Unido).*

# Network Time Protocol (NTP)

- NTP utiliza el algoritmo de Marzullo con la escala de tiempo *Tiempo Universal Coordinado* (UTC).
- Puede mantenerse sincronizado con una diferencia máxima de 10 milisegundos a través de Internet y llegar a acercarse hasta 200 microsegundos o más en redes de área local.
- Es un sistema de jerarquía de estratos de reloj:
  - Los sistemas de estrato 1 están sincronizados con un reloj externo (reloj GPS o algún reloj atómico).
  - Los sistemas de estrato 2 derivan su tiempo de uno o más de los sistemas de estrato 1
  - y así consecutivamente.
- Las estampas de tiempo utilizadas por NTP consisten en un segundo de 32-bit y una parte fraccional de 32-bit.

# Estratos de reloj

- NTP tiene una estructura jerárquica denominada de estrato.
- Los niveles determinan la distancia desde el reloj de referencia (Estrato 0)
- Existe un máximo de 15 estratos, a medida que aumenta el número de estrato los dispositivos se vuelven menos precisos.
- Los servidores de un estrato pueden conectarse entre sí para mejorar la sincronización interna.
- Cada cliente puede consultar varios servidores del estrato superior.



# Estratos de reloj

## Estrato 0

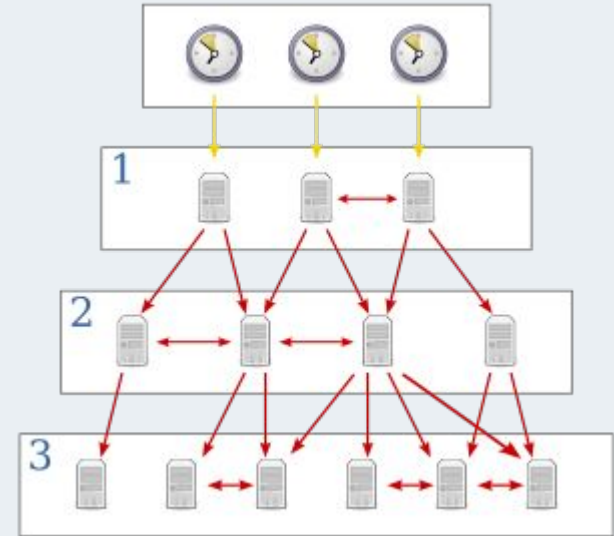
- Los dispositivos de este estrato se conocen como relojes de referencia.
- Tienen muy poco o ningún tiempo de retraso.
- Distribuyen UTC.

## Estrato 1

- Conectados directamente a un reloj de referencia, recibiendo la señal directamente la señal UTC.
- Se sincroniza en pocos microsegundos.

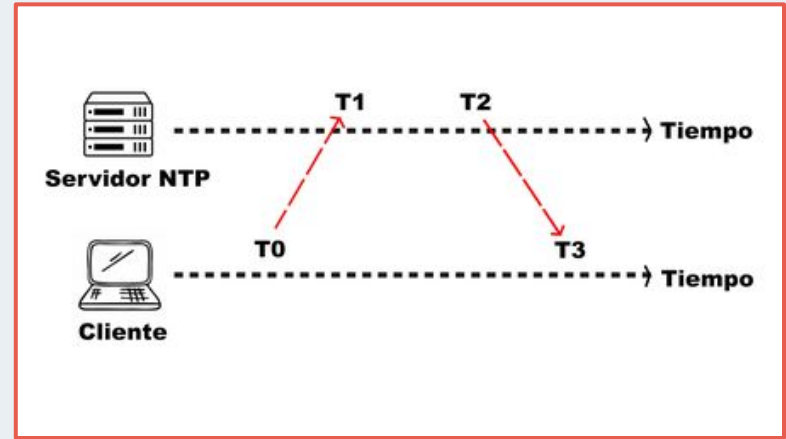
## Estrato 2

- Sincronizados con uno o más servidores del estrato 1.
- Actuarán como servidores para el estrato 3, y así sucesivamente.



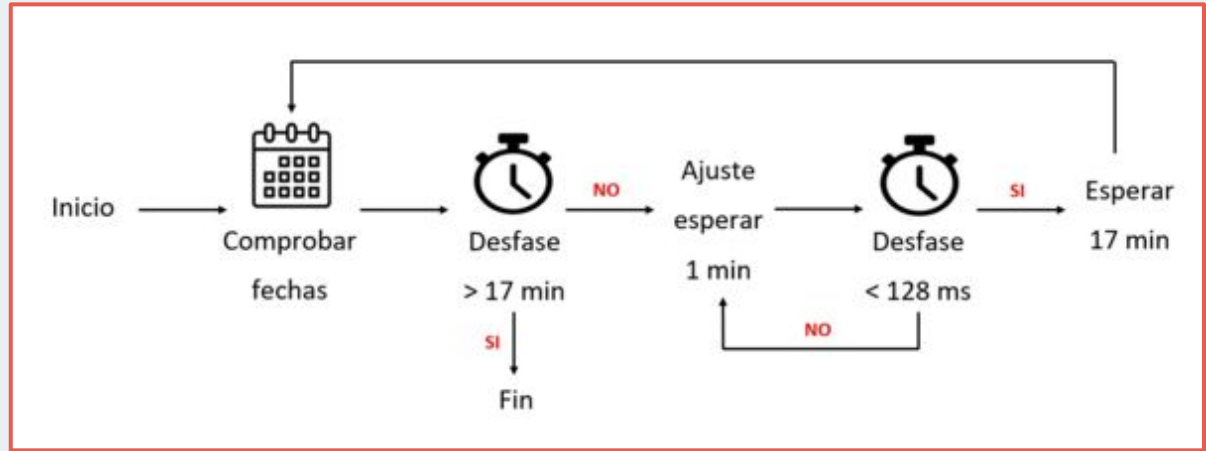
# Intercambio de mensajes

1. El cliente envía una petición de sincronización en el instante T0 para verificar si el tiempo de desfase entre servidor y cliente es mayor de 17 minutos.
2. El servidor la recibe en el instante T1:
  - a. Si el desfase es menor a 17 min, el servidor envía un mensaje en T2.
  - b. Si el desfase es mayor que 17min se terminará el proceso y no habrá sincronización.
3. En T3 el cliente recibirá el paquete. Cada minuto se realizará un ajuste del tiempo hasta aproximarse a 128ms del tiempo del servidor. A partir de un desfase mayor a 128ms, cada 17 minutos el desfase se va precisando.





# Intercambio de mensajes



El desfase ( $\theta$ ) entre ambos relojes se calcula mediante la siguiente fórmula:

$$\theta = \frac{(T1 - T0) + (T2 - T3)}{2}$$

# Network Time Security (NTS)

- Está especificado en la norma RFC 8915 y utiliza el puerto **TCP 4460** para el intercambio de claves de cifrado.
- Es un mecanismo de seguridad criptográfico para la sincronización de tiempo de red. Se proporciona una especificación completa para la aplicación de NTS al modo cliente-servidor del NTP (RFC 5905).

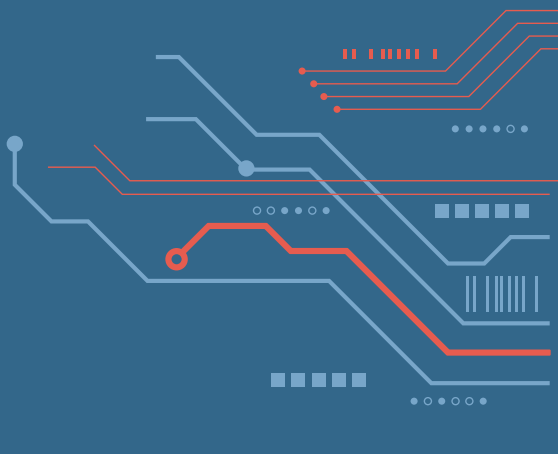
# Network Time Security (NTS)

- Los objetivos de NTS son:
  - Identidad: Se establece la identidad de las partes con las que se comunican mediante una clave pública.
  - Autenticación: Verificación criptográfica de los paquetes para asegurar que su origen está identificado y no han sido modificados en durante la transmisión.
  - Confidencialidad: Soporte para encriptar campos de extensión NTP.
  - Prevención de reproducción: Detección de los paquetes de sincronización de tiempo duplicados.
  - Consistencia de solicitud-respuesta: Verificación por parte del cliente de que un paquete de sincronización de tiempo recibido de parte del servidor corresponde con una solicitud del cliente previa.
  - Escalabilidad: El servidor puede servir a un gran número de clientes.
  - Rendimiento: El cifrado y la autenticación utilizados cuando se transfiere el tiempo deben ser mínimos.



# NAT

Problema, Solución, Funcionamiento, Formas  
de funcionamiento y Tipos de NAT



# Problema

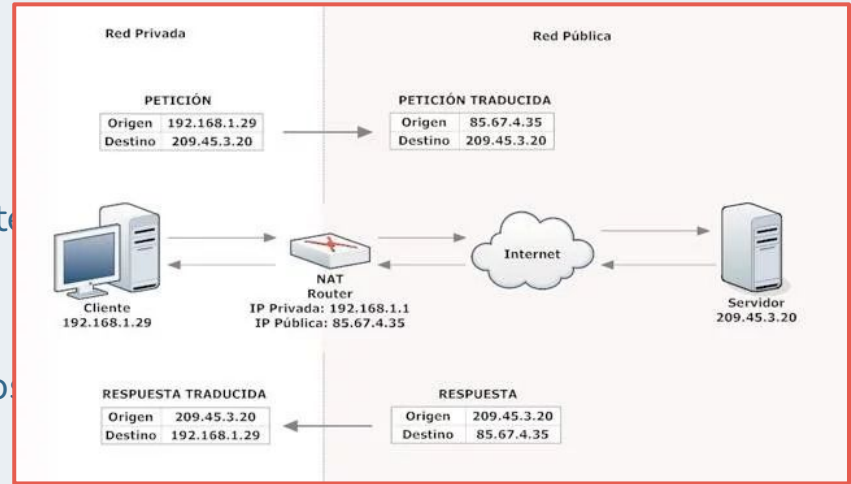
- Internet en sus inicios no fue pensado para ser una red tan extensa
- Se reservaron SOLO 32 bits para direcciones (**4.294.967.296** direcciones únicas)
- El número de máquinas conectadas a Internet aumentó exponencialmente y las direcciones IP se agotaban.

# Solución

- Network Address Translation (NAT): Un mecanismo utilizado por routers para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.
- Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.
- Es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.
- Su uso más común es permitir utilizar direcciones privadas para acceder a Internet.
- Se espera que con el advenimiento de IPv6 no sea necesario continuar con esta práctica.

# Funcionamiento

- El router de borde tiene una interface con una dirección privada y otra con una dirección pública.
- La dirección de origen en cada paquete se traduce de una dirección privada a una pública.
- El enrutador sigue la pista de los datos básicos de cada conexión activa (dirección de destino y el puerto).
- Cuando una respuesta llega al enrutador, este utiliza los datos de seguimiento de la conexión almacenados en la fase de salida para determinar la dirección privada de la red interna a la que remitir la respuesta.



# Formas de funcionamiento

- **NAT Estática (NAT 1:1):** Una dirección IP privada se traduce a una dirección IP pública, donde esa dirección pública es siempre la misma.
- **NAT Dinámica:** Una dirección IP privada se mapea a una IP pública basándose en una tabla de direcciones de IP registrada. El router mantendrá una tabla de direcciones IP registradas, y cuando una IP privada requiere acceso a Internet, el router elegirá una dirección IP de la tabla que no esté siendo usada por otra IP privada.
- **NAT de Sobrecarga:** Conocida también como PAT (Port Address Translation), NAPT (Network Address Port Translation), NAT de única dirección o NAT multiplexado a nivel de puerto.



# Tipos de NAT

**NAT de cono completo** (*Full-Cone NAT*): También llamada Port Address Traslator (PAT), mapea la dirección IP y puerto interno a una dirección y puerto público diferentes. Una vez establecido, cualquier host externo puede comunicarse con el host de la red privada enviando los paquetes a una dirección y puerto externo que haya sido mapeado.

**NAT de cono restringido** (*Restricted Cone NAT*): La IP y puerto externos de NAT son abiertos cuando el host de la red privada quiere comunicarse con una dirección IP específica fuera de su red. La NAT bloqueará todo tráfico que no venga de esa dirección IP específica.

**NAT de cono restringido de puertos** (*Port-Restricted Cone NAT*): También llamado *enmascaramiento*, NAT bloqueará todo el tráfico a menos que el host de la red privada haya enviado previamente tráfico a una IP y puerto específico, entonces solo en ese caso esa IP/puerto tendrán acceso a la red privada.

# Tipos de NAT

**NAT Simétrica** (*Symmetric NAT*). En este caso la traducción de dirección IP privada a dirección IP pública depende de la dirección IP de destino donde se quiere enviar el tráfico.

También existen otras denominaciones más genéricas:

- **Source NAT** (SNAT): Se traduce la dirección y puerto origen de los paquetes.
- **Destination NAT** (DNAT): Se traduce la dirección y puerto destino de los paquetes.

# RECURSOS BIBLIOGRÁFICOS

- Redes de Computadoras | Tannenbaum - Wetherall (2012) | 5ta Edición WordPress:
  - 7.1 DNS: El sistema de nombres de dominios
- IBM Redbooks | TCP/IP Tutorial and Technical Overview:
  - 3.7 Dynamic Host Configuration Protocol (DHCP)
  - 8.1 Domain Name System (DNS)
  - 21.4 Network Address Translation (NAT)
- Huawei | What is NTP?  
<https://support.huawei.com/enterprise/en/doc/EDOC1100206719>