

DNS y DHCP

Sebastián Castro A.

CC50P-1

2006/2

Temario

- ◆ Introducción: ¿Qué es DNS?
- ◆ Nociones básicas sobre redes
- ◆ Estructura y conceptos del DNS
- ◆ Resolución de nombres: consultas DNS
- ◆ Servidores DNS

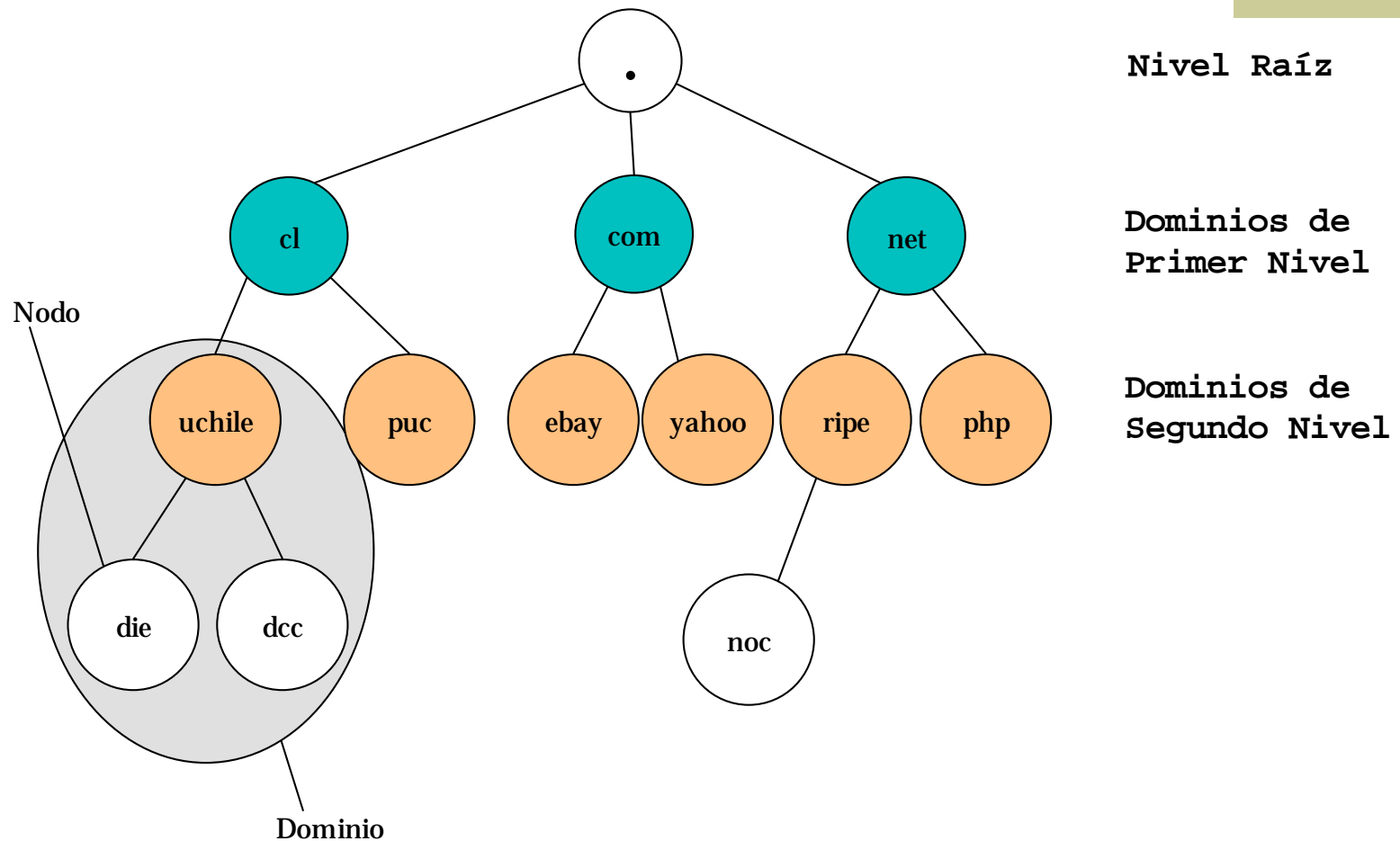
DNS

- ◆ Base de datos distribuida
- ◆ Redundante
- ◆ Sin administración central
- ◆ Traducción IP \longleftrightarrow nombre
- ◆ Delegación de Responsabilidad
- ◆ Cuatro funciones dentro del sistema
 - Servidores con autoridad (parte de la cadena de autoridad)
 - Primarios
 - Secundarios
 - Servidores sin autoridad (cache)
 - Cliente: stub resolver en el S.O.

Nociones de Redes

- ♦ IP provee TCP y UDP, entre otros
- ♦ Direcciones IPv4 son 4 octetos: 192.168.10.1
- ♦ Direcciones IPv6 son 128 bits (16 octetos).
- ♦ DNS usa principalmente UDP (eficiencia)
- ♦ TCP es usado en diversas circunstancias:
 - Transmisión de zonas (entre servidor maestro y esclavos)
 - Si la respuesta es demasiado grande
 - Originalmente más de 512 bytes.
 - En la actualidad depende del soporte a EDNS.
- ♦ Puerto 53 (tanto TCP como UDP)

Estructura



Estructura

- ♦ Organización jerárquica.
- ♦ En el tope se encuentra el nivel raíz (“.”)
- ♦ Como hijos, todos los TLD, separados en dos grandes categorías: gTLD o “generic Top Level Domain” y los ccTLD o “country code Top Level Domain”.
- ♦ Ejemplos de gTLD son .NET, .BIZ, .INFO
- ♦ Ejemplos de ccTLD son .DE, .CH, .TV, .DJ
- ♦ La administración de cada TLD está en manos de un NIC, que se encarga de los aspectos administrativos y técnicos asociados.

Estructura

- ◆ Cada subárbol de ésta jerarquía recibe el nombre de “dominio”.
- ◆ La información de cada dominio es descrita en “zonas”.
 - Las zonas pueden ser archivos de texto, una base de datos o cualquier otro soporte lógico de datos.
- ◆ Para asegurar la descentralización, el sistema promueve la “delegación de autoridad”, así un padre puede entregar la responsabilidad de un nodo hijo a otra organización.

Información

- ◆ Cada nodo del árbol puede tener información (descrita en una zona).
- ◆ La información se describe usando los RR (Resource Records).
- ◆ Los RR tiene la siguiente estructura: <Name, Class, Type, TTL, Rdata>
 - Name: Es el nombre del registro que se está definiendo. Puede ser de 255 bytes de largo máximo, puede tener 126 partes y cada parte no debe exceder los 63 bytes. Los caracteres válidos son A-Z, 0-9 y “-”.
 - Class: Puede ser IN (Internet), CH (Chaos) o HS (Hesiod). La más común es IN.
 - Type: Define el tipo de registro y puede ser A (address), MX (mail exchanger), SOA (start of authority), NS (name server), CNAME (canonical name), PTR (pointer), etc.
 - TTL: Define el tiempo en segundos en que éste registro puede ser recordado dentro de un caché.
 - Rdata: Describe el contenido del registro.

Información

◆ Ejemplos de RR's

■ SOA (Start of Authority)

- MNAME: nombre de dominio de origen
- RNAME: dirección de mail del responsable (con '.' en vez de '@')
- SERIAL: usado para identificar cambios y actualizaciones
- REFRESH: período de refrescos entre servidores autoritativos de una zona.
- RETRY: tiempo a esperar si un refresco falla.
- EXPIRE: tiempo de falla después del cual se considera el dominio inexistente.
- MINIMUM: TTL mínimo para todos los registros de la zona

Mensajes DNS

Mensaje DNS

Header
Question
Answer
Authority
Additional

Header Mensaje DNS

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ID															
QR	Opcode				AA	TC	RD	RA	Z			RCODE			
QDCOUNT															
ANCOUNT															
NSCOUNT															
ARCOUNT															

Consultas DNS

- ♦ El sistema está diseñado para generar/recibir consultas y darle respuestas.
- ♦ Las consultas tienen la estructura <Qname, Qclass, Qtype>.
- ♦ Las consultas pueden ser de dos tipos: iterativas (contéstame lo que sepas) o recursivas (búscame la respuesta).
- ♦ Desde el punto de vista del mensaje, van marcados con el flag QR, RD (si es recursiva), un ID, opcode QUERY, la consulta en la sección “QUERY” y el resto vacío.

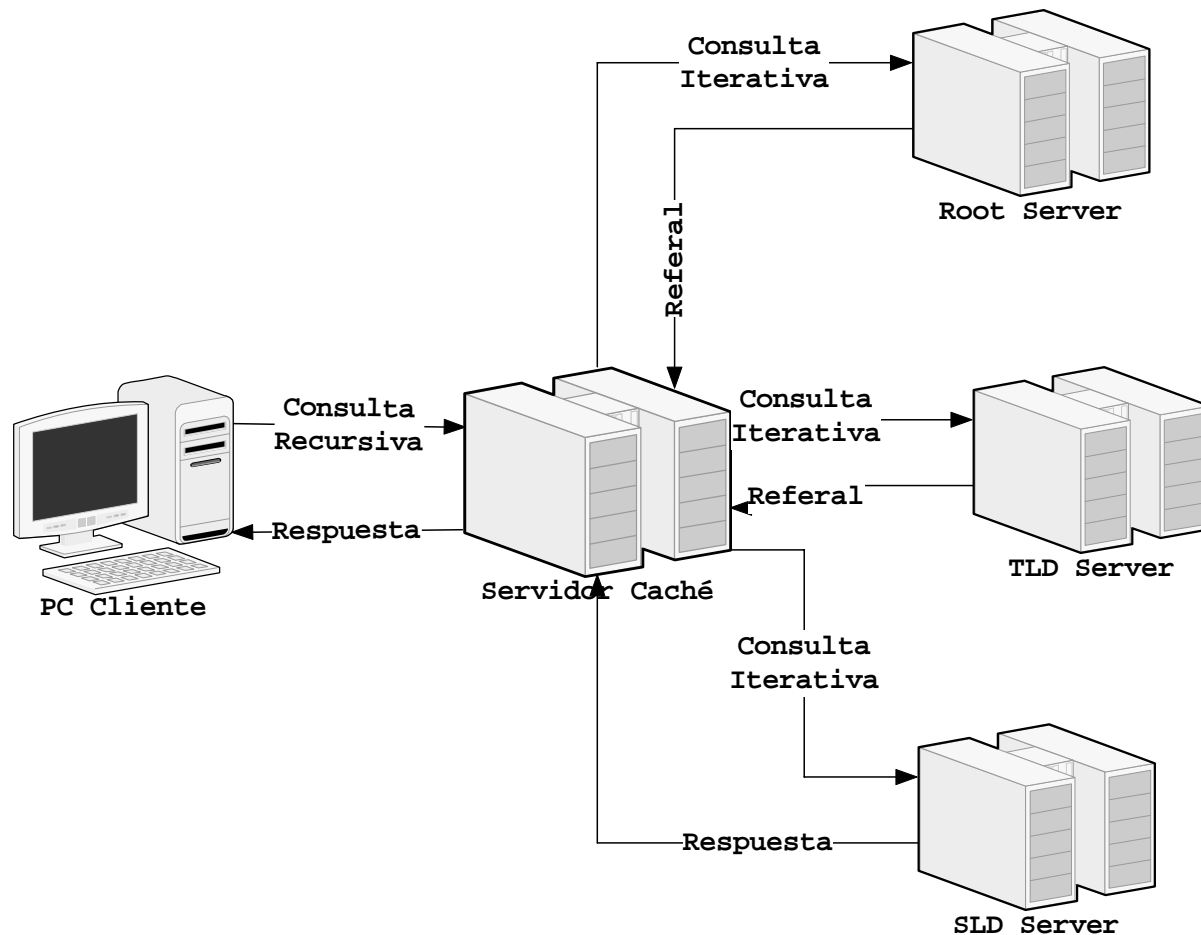
Respuestas DNS

- ♦ Las respuestas de DNS se producen contestando a las preguntas recibidas por el servidor.
- ♦ Vienen con el ID de la pregunta, opcode QUERY, QR=0, AA=1 (si la respuesta viene de un servidor autoritativo), RA=1 (si viene de un servidor caché), en la sección “Answer” o “Authority” la respuesta y en la sección “Additional” información extra de utilidad.
- ♦ Además incluyen el código de retorno de la consulta (RCODE), que puede ser:
 - NOERROR: No hubo error procesando la consulta.
 - NXDOMAIN: No existe ningún registro que calce con lo consultado.
 - SERVFAIL: Se ha producido un error contestando la consulta.
 - FORMERR: Mensaje con formato erroneo.
 - NOTIMPL: No se ha implementado el mecanismo para contestar lo preguntado.

Resolución DNS

- ◆ Sin DNS: Internet basada solamente en direcciones IP (e.g. 200.1.123.4 en vez de ns.nic.cl)
- ◆ Existe un sistema DNS configurado y funcionando
- ◆ Objetivo: traducir nombres a direcciones IP
- ◆ Otros usos
 - Resolución reversa (nombre -> IP)
 - Listas negras (herramientas antispam)
 - Información de contacto

Resolución (2)



Resolución (3)

1. Una aplicación hace una consulta al “Stub resolver” o librería resolver de su S.O.
2. Éste genera una consulta DNS recursiva, que es enviada al servidor caché configurado que corresponda (configurado en el S.O.)
3. El servidor caché envía construye una consulta iterativa y la envía a algún root server (registros NS para “.”)
4. Éstos contestan con una “referencia” al lugar donde encontrar la respuesta (generalmente los registros NS del TLD respectivo).
5. El servidor caché envía la misma pregunta, pero ahora a alguno de los servidores de nombre del TLD.
6. Éstos contestan con una “referencia” al lugar donde encontrar la respuesta (generalmente los registros NS del SLD respectivo)
7. El servidor caché envía la misma pregunta, a alguno de los registros NS entregados por el último servidor consultado.
8. El servidor debería entregar una respuesta definitiva a la pregunta y debería venir marcada con el bit AA. El caché toma la respuesta y guarda una copia (El tiempo que el caché guarda la copia depende del TTL).
9. El caché le envía la respuesta obtenida al cliente que hizo la consulta.

Resolución (4)

- ◆ ¿Qué pasa si n segundos después ($n < \text{TTL}$) algún otro cliente le envía la misma consulta al cache?
 - El caché entregará la respuesta que tiene memorizada. Esto dura mientras no se “agote” el TTL de los RR que venían en la respuesta.
 - Esto produce un fenómeno conocido como “propagación”, que consiste entre el tiempo transcurrido desde un cambio en un dominio hasta que todos los caché lo conocen.
 - Este tiempo varía y depende el TTL de la zona y del número de niveles de caché que existan.

Servidores de nombre

◆ Tipos

- Caché
- Primario
- Secundario
- Stealth

Servidores de nombre

◆ Algunas notas

- Alrededor del 80% de los servidores de nombre en el mundo utilizan BIND o algún derivado.
- Es conocida como la implementación por referencia del sistema DNS.
- Ningún TLD utiliza el DNS de Microsoft, y las autoridades así lo recomiendan (Draft BCP).
 - “Do not use Microsoft servers for DNS service; they behave oddly, scale poorly, and have very bad security problems. UNIX or Linux is recommended as the operating system of choice.”

Servidores de nombre

◆ Introducción

- Dentro de la estructura de DNS existen diferentes funciones.
 - Resolver: Cliente del DNS que busca información contenida en una zona usando protocolos de DNS.
 - Caché: Servidor de DNS que es capaz de recibir consultas de parte de los resolvers y averiguar las respuestas. Generalmente guarda una copia de lo recibido.
 - Servidor con autoridad: Un servidor que conoce el contenido de una zona a partir de una fuente local.

Servidores de nombre

◆ Introducción

■ Funciones

- Servidor primario: Servidor con autoridad donde la información de zona está configurada localmente. Conocido también como **maestro**.
- Servidor secundario: Servidor con autoridad que obtiene la información de una zona desde el servidor primario, utilizando un mecanismo llamado **transferencia de zona**. Es también conocido como **esclavo**, pues depende de un maestro.

Servidores de nombre

◆ Caché

- Toda infraestructura de red basada en protocolos de Internet (TCP/IP) necesita uno.
- También es llamado *resolver*.
- Se encarga de averiguar las respuestas a las preguntas que otros hacen.
- Guarda una copia de las respuestas que recibe: **caching**. La copia se recuerda durante la cantidad de segundos especificada en la respuesta: **TTL**.
- También se guarda copia de las consultas que no recibieron respuesta: **negative caching**.

Servidores de nombre

◆ Primario

- Se denomina *maestro* de una zona.
- DEBE entregar información con autoridad para una zona, sino cae en la categoría de **Lame Delegation**.
- La información de zona reside localmente en el servidor y es la copia maestra.
- La zona se puede almacenar en un archivo (BIND, NSD, MS DNS) o en una base de datos (PowerDNS, UltraDNS, ATLAS).

Servidores de nombre

■ Definición de la zona

@ es un
caracter
especial, que es
reemplazado
por el nombre
de la zona.

```
;$TTL 43200
@ IN SOA nicollette.nic.cl. root.nic.cl. (
    2001071814 ; Serial
    21600      ; Refresh
    7200       ; Retry
    2592000    ; Expire
    43200      ; TTL
)
; Incluimos solo un servidor de nombres
; IN NS nicollette.nic.cl.
;
spooler      IN A 10.0.46.51
hpcolor      IN A 10.0.46.63
impresora    IN A 10.0.46.62
```

Un
comentario,
empieza con
";"

Servidores de nombre

◆ Primario

■ Consideraciones generales

- Nunca usar un CNAME como NS (RFC 1912)
- Nunca usar un CNAME como MX (RFC 1034 y RFC 974)
- Elegir un número serial que sea siempre incremental. En particular se sugiere la norma YYYYMMDDHH
- El número serial no puede tener más de 10 dígitos, pues está representado por un entero de 32 bits.
- Su valor máximo es $2^{32}-1$ y es cíclico.

Servidores de nombre

◆ Primario

■ Recomendaciones

- No publicar en Internet direcciones IP privadas.
- Restringir el acceso a la zona sólo a los secundarios: seguridad a través de la obscuridad.
 - ◆ Asegurarse que los secundarios hacen lo mismo.
- Incremente el serial en cada cambio.
- El tiempo transcurrido entre el momento en que se hace un cambio en el primario hasta que todos lo conocen se conoce como **tiempo de propagación**.
 - ◆ Éste se puede disminuir habilitando los NOTIFY y disminuyendo el *refresh* y *TimeToLive* de la zona.

Servidores de nombre

◆ Secundario

- Se le denomina esclavo, pues depende de un maestro
- Mantiene una copia de una zona particular
- También entrega información con autoridad por el dominio.
- No reemplaza al primario o maestro, sino lo complementa.
- La copia se hace mediante una transferencia de zona

Servidores de nombre

♦ Secundario

■ Consideraciones generales

- Importancia de un secundario
 - ♦ Los secundarios apoyan y balancean carga con el primario, no actúan como *failover*. Derribar el mito del respaldo de los secundarios.
- Cómo elegir un secundario
 - ♦ Service Level Agreement: Que calidad de servicio necesito y me entregarán.
 - ♦ La elección de un secundario es equivalente a elegir un *business partner*.
- Responsabilidad por los secundarios:
 - ♦ ¿Debe realizar el primario verificaciones sobre sus secundarios?

Servidores de nombre

◆ Secundario

■ Recomendaciones

- Deben ser elegidos de modo de asegurar que al menos uno de los servidores con autoridad sea alcanzable.
 - ◆ Por lo mismo, es muy mala idea tener todos los servidores bajo en mismo enlace, en la misma sala o bajo la misma fuente de energía. El caso Microsoft es un vivo ejemplo.
- La desaparición de un dominio generalmente causa aumentos de tráfico.
- El estándar exige un mínimo de dos y recomienda un máximo de 5, salvo casos excepcionales.
- Es común acordar con una organización del mismo tamaño el intercambio de secundarios.

Servidores de nombre

◆ Stealth

- Aquellos servidores con autoridad, que no están listados en la delegación.
 - ◆ Generalmente se usan para mejorar el rendimiento local del servidor.
 - ◆ En otras ocasiones, se utiliza para ocultar al maestro, dejando a un secundario actuando como él.

Servidores de nombre

♦ Recomendaciones Finales

- Busque diversidad de plataforma
 - En lo posible también de software de DNS. BIND 8, BIND 9 y NSD son buenas alternativas.
- No mezcle las funciones de servidor con autoridad (primario/secundario) con un caché.
- Asegúrese que sus secundarios responden por su dominio.
- Después de un cambio, asegúrese que el primario contesta adecuadamente y que los secundarios se han sincronizado.
- En la configuración inicial, verifique que sus servidores son alcanzables y consultables.

DHCP

◆ BOOTP y DHCP

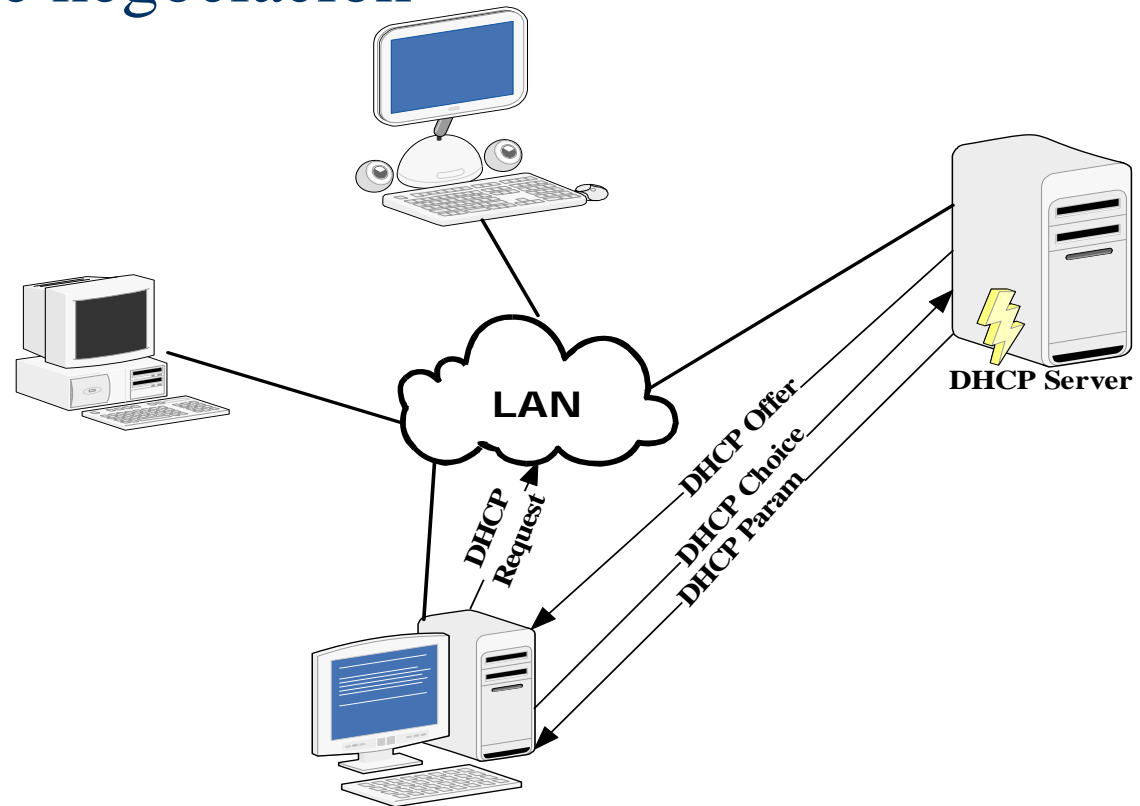
- BOOTP permite a estaciones sin disco cargar S.O y los parámetros necesarios para funcionar en red
- Asigna un IP predeterminado a una máquina

DHCP

- Extiende BOOTP
- Asignación dinámica de una dirección IP (y los parámetros necesarios)
 - Puede ser un mapeo variable o un mapeo fijo.
- Asignación temporal (leasing).
- Expiración de direcciones.
- Mejora la administración de la numeración.

DHCP

◆ Proceso de negociación



Integración DHCP/DNS

- ♦ DNS Dinámico.
- ♦ Generación fija de nombres en una zona
- ♦ Generación fija de reversos en una zona.

¿Que hacemos en el laboratorio?

◆ A nivel de DHCP

- Se activa un servidor de DHCP que asigna direcciones a partir de un pool.
- Se cambia la configuración del servidor, para que asigne una dirección fija a partir de la MAC Address de su computador.

◆ A nivel de DNS.

- Tenemos un resolver local
- Configuramos un primario
- Configuramos un secundario
 - Y activamos la transferencia de zona usando TSIG
- Verificamos el proceso de resolución de nombres internamente
- Probamos el uso de los reversos.