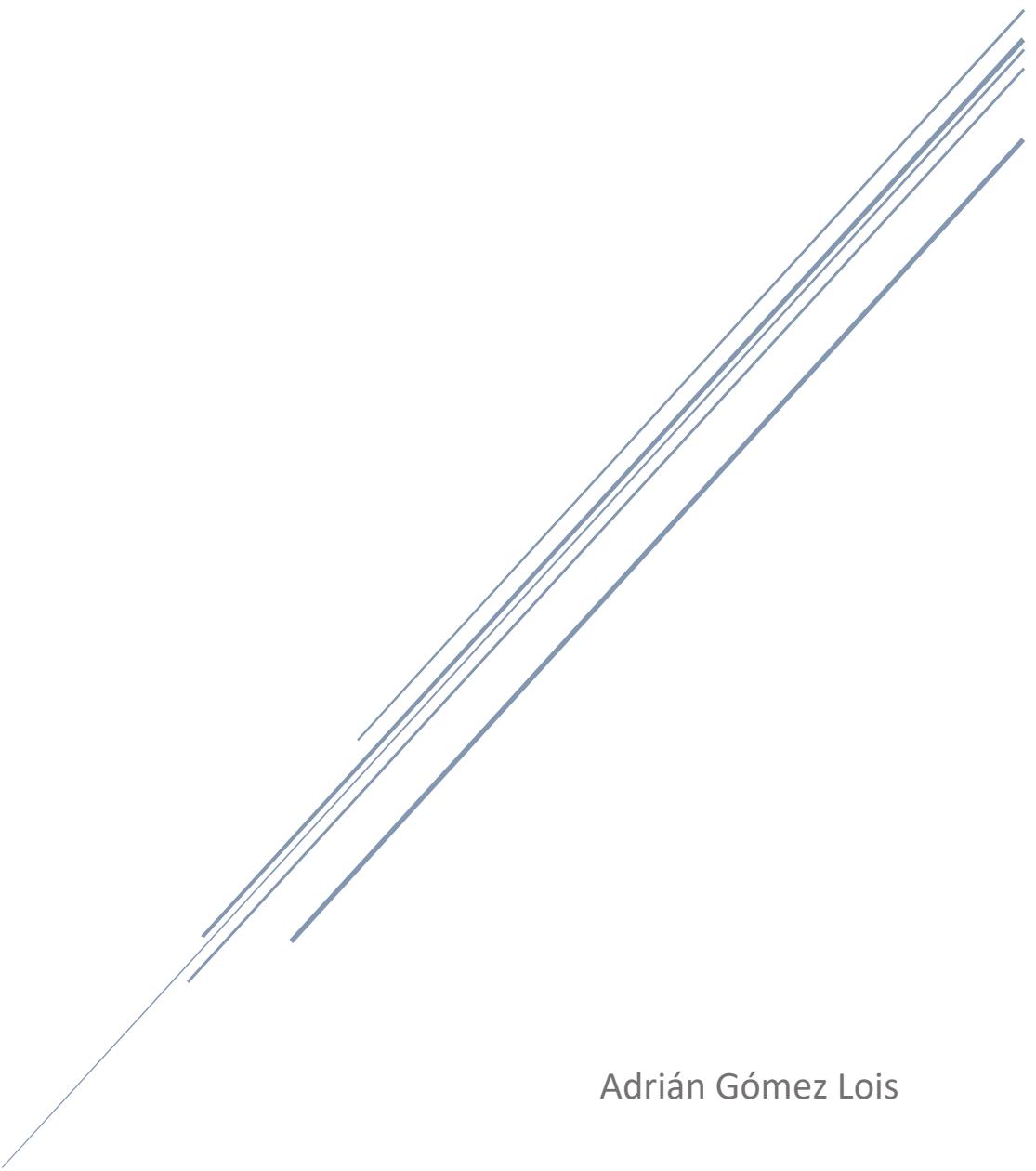


# DNS

## DOMAIN NAME SYSTEM (3º PARTE)



Adrián Gómez Lois

## Contenido

<b>1. Obxectivos .....</b>	3
<b>2. 1º Parte DNS .....</b>	4
2.1. Primeiras consultas DNS con nslookup .....	4
2.2. Administradores do DNS .....	5
2.3. Dominios TLD .....	6
2.4. Rexistro de dominios.....	8
2.5. Servidores de nomes.....	13
2.6. Resolución de direccións.....	17
2.7. Consulta a servidores DNS con nslookup, host e dig .....	19
<b>3. 2º Parte DNS .....</b>	30
3.1. Exercicio 1: Consultas DNS .....	30
3.2. Exercicio 2: Consultas DNS .....	33
3.3. Exercicio 3: Consultas DNS .....	38
<b>4. 3º Parte DNS .....</b>	42
4.1. Configuración e proba dun servidor DNS primario nun servidor Windows Server 2012	42
4.2. Configuración e proba dun servidor DNS secundario nun servidor Windows Server 2012. DNS Failover.....	50
4.3. Configuración e proba dun servidor DNS e DHCP nun Debian (modo texto) a través de Webmin.....	58
4.4. Configuración e proba dun servidor DNS maestro e escravo con Bind nun Ubuntu Server 16.04 .....	67
<b>5. Conclusións .....</b>	77

## 1. Obxectivos

Os obxectivos principais son coñecer como para que sirve e como funciona un sistema de nomes de dominio (DNS), que utilidades existen para explotalo no lado cliente/consultas, e como instalar e configurar un servidor primario é secundario no lado servidor.

Na primeira parte investigarase que organismos e de que quemodo xestionan os nomes de dominio.

Na segunda parte realizaranse consultas a nomes de dominio tanto en búsqueda directa como inversa mediante utilidades de comandos internos dos sistemas operativos empregados, Windows e Linux. Comprobando a súa utilización e manexo.

Na terceira parte montaranse diversos escenarios de rede, unha estructura cliente/servidor para o comprobar o proceso de resolución DNS. Tanto no lado de instalación de configuración do servidor, como no lado cliente para comprobar o funcionamento deste.

Usaranse como servidores: Windows Server 2012, Debian+Webmin, Ubuntu Server.

Como clientes: Ubuntu server, Windows XP e Windows 7.

Donde finalmente veráse unha parte interesante donde dous sistemas Windows XP e 7 traballando sobre o mesmo protocolo (DNS) non funcionan exactamente igual como clientes, debido a novos protocolos propietarios de Microsoft que surxiron a partires de Windows XP en adiante.

## 2. 1º Parte DNS

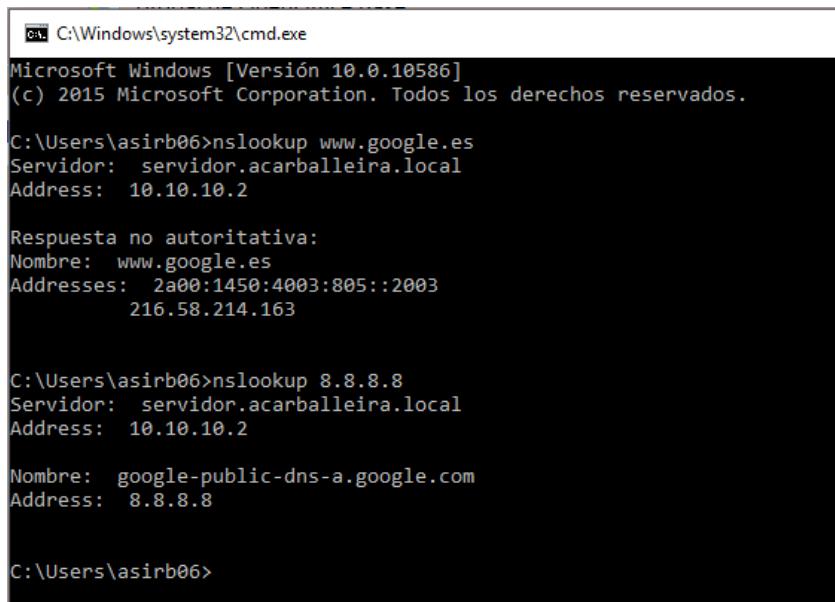
### 2.1. Primeiras consultas DNS con nslookup

a. O comando nslookup permite realizar preguntas ao servidor DNS que estea configurado no equipo e amosa por pantalla información da resposta obtida. Abre un terminal no teu propio equipo ou nunha máquina virtual cliente do contorno de prácticas e realiza unha consulta DNS directa e outra inversa utilizando o comando nslookup. Por exemplo:

```
nslookup www.google.es
```

```
nslookup 8.8.8.8
```

b. Observa os resultados.



The screenshot shows a Windows command prompt window titled 'C:\Windows\system32\cmd.exe'. It displays the following output from the nslookup command:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.10586]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.

C:\Users\asirb06>nslookup www.google.es
Servidor: servidor.acarballeira.local
Address: 10.10.10.2

Respuesta no autoritativa:
Nombre: www.google.es
Addresses: 2a00:1450:4003:805::2003
           216.58.214.163

C:\Users\asirb06>nslookup 8.8.8.8
Servidor: servidor.acarballeira.local
Address: 10.10.10.2

Nombre: google-public-dns-a.google.com
Address: 8.8.8.8

C:\Users\asirb06>
```

Que servidor está utilizando o equipo?

10.10.10.2 (servidor.acarballeira.local)

Cal é a resposta do servidor DNS en cada caso? Que información adicional proporciona o comando? Realiza capturas de pantalla.

No caso de consultar o nome, mástrase o nome e a dirección IP que estamos usando para facer a consulta, o segundo bloque amósanos o nome e a dirección IPv6 e IPv4 da consulta realizada.

Como información adicional a resposta no caso da consulta por nome vemos que é non autoritativa, quere decir que non é propietario do dominio que estamos buscando.

No caso de consultar a IP, móstrase no mesmo caso que o anterior, o segundo bloque indícanos o nome do servidor DNS consultado seguido da IP asignada a este.

## 2.2. Administradores do DNS

a. Procura información en Internet sobre os seguintes organismos:

**ICANN** (*Internet Corporation for Assigned Names and Numbers*): Entidade sin fines de lucro responsable da coordinación global de sistemas de identificadores únicos de Internet y do seu funcionamiento estable e seguro. Preserva a estabilidade de Internet por medio de procesos basados en consenso. Coordina a administración de elementos técnicos DNS para garantir a resolución única de nomes, de modo que os usuarios podan encontrar todas as direccións sin ser repetidas. A ICANN delega diversas tarefas a IANA.

**Internic** (*Internet Network Information Center*): Foi o principal organismo gubernamental de Internet responsable dos nomes de dominio DNS e as direccións IP, as asignacións foron hasta o 18 de setembro de 1998, cando este papel foi asumido pola ICANN.

**IANA** (*Internet Assigned Numbers Authority*): Entidade que supervisa a asignación global de direccións IP, sistemas autónomos, servidores raíz de nomes de dominio DNS e outros recursos relativos os protocolos de Internet. Actualmente e un departamento operado pola ICANN.

**IAB** (*Internet Architecture Board*): E un comité da IETF (*Internet Engineering Task Force*) e un organismo asesor ISOC (*Internet Society*), responsables das normas de Internet e a designación de RFC (*Request for comments*).

**Red.es**: Entre diversas tarefas ten encomendada a xestión de rexistros dos nomes de dominio baixo o código ".es", dacordo ca política da Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI). Dentro do marco da xestión do ".es" impulsase a presenza dixital de Internet os cidadans, empresas e as administracións públicas.

## 2.3. Dominios TLD

a. Accede á web da IANA para obter máis información sobre os dominios TLD: <http://www.iana.org/domains/root/db>

b. Consulta no RFC2606 a finalidade dos dominios reservados: <http://www.rfc-es.org/rfc/rfc2606-es.txt>

c. Investiga sobre o dominio “gal”:

i. Que tipo de dominio é? Quen o administra? Cal é a súa finalidade?

.gal e o tipo de dominio xenérico, administrador pola asociación puntoGAL, xestionar e coordinar a asignación de código “.gal” según a que tipo de entidades se traten e con que fines.

d. Realiza un esquema cos diferentes tipos de dominios TLD.

**ccTLD** (Country Code TLD): dominios de nivel superior xeográficos.

**gTLD** (Generic TLD): Dominios de primer nivel

[https://es.wikipedia.org/wiki/Dominio\\_de\\_nivel\\_superior](https://es.wikipedia.org/wiki/Dominio_de_nivel_superior)

Dentro dos gTLD están:

**sTLD**: Patrocinados por fundacións independentes.

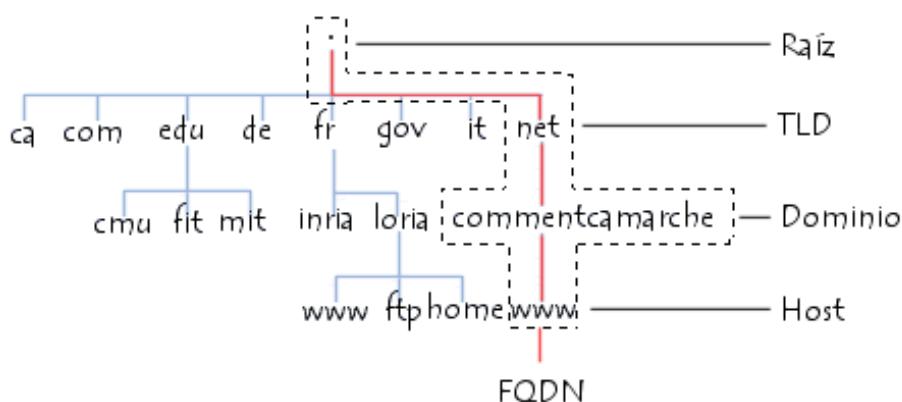
**uTLD**: Non patrocinados.

**ITLD** (International TLD): Trátase de dominios lingüísticos que están destinados a fomentar o uso dunha lingua

Despois estarían outros TLDs:

**arpa** (“*in-addr.arpa*” e “*ip6.arpa*”), úsanse para resolución inversa de direccións IP.

**Dominios reservados**: “test”, “example”, “invalid” e “localhost” están reservados para utilizarse en probas privadas, exemplos de documentación, etc.



e. Procura varios exemplos de dominios de cada tipo indicando a organización que xestiona cada un e a finalidade para a que se creou ese tipo de dominio. Inclúe polo menos os seguintes dominios: “.com”, “.es”, “.gal”, “.coop”, “.arpa” e os dominios reservados.

“.com”: Generic, VeriSign Global Registry Services, dedicado a usos comerciais ainda que hoxe en día úsase de forma xenérica.

“.es”: Country-code, xestionado por Red.es, dedica a usos dentro de websites con contido en castelán (España).

“.gal”: Generic, xestionado por Asociación puntoGAL, dedica a usos de contidos en galego ou administracións públicas de Galicia.

“.coop”: Sponsored, xestionado por DotCooperation LLC, dedicado a sociedades cooperativas.

“.arpa”: Infraestructura, xestionado por Internet Architecture Board (IAB), .

“.info”: Generic, xestionado por Afiliias Limited, dedicado a servizos de información de todo tipo.

“.net”: Generic, xestionado por VeriSign Global Registry Services, no seu inicio pensouse para usos de empresas relacionadas con tecnoloxías en redes, pero hoxe en día úsase de forma xenérica.

“.org”: Generic, xestionado por Public Interest Registry (PIR), dedicado a Organizacións sin ánimo de lucro.

“.int”: Sponsored, xestionado por Internet Assigned Numbers Authority (IANA), dedicados a organismos internacionais.

“.mil”: Sponsored, xestionado por DoD Network Information Center, dedicados a organismos de carácter militar.

“.edu”: Sponsored, xestionado por EDUCAUSE, dedicado a universidades ou entidades relacionadas coa educación.

“.gov”: Sponsored, xestionado por General Services Administration Attn: QTDC, 2E08 (.gov Domain Registration), dedicado a usos polo goberno de Estados Unidos e dedicado exclusivamente a organizacións gubernamentais de ese país.

“.biz”: Generic-restricted, xestionado por Neustar, Inc, dedicado xenéricamente a empresas.

#### Reservados:

“.test”: Recoméndase para o uso de probas de código novo ou actual relacionado con DNS.

“.example”: Recoméndase para o uso de documentación ou exemplos.

“.invalid”: Está pensado para úsallo na construcción “online” de nomes de dominio que estamos seguros non son válidos.

“.localhost”: Tradicionalmente de manera estática nas implementacións DNS de máquinas como asociado a un rexistro A que apunta a dirección IP de loopback, e está reservado para tal uso.

## 2.4. Rexistro de dominios

### a. Axentes rexistradores

i. Consulta a web da ICANN e trata de respostar ás seguintes preguntas:

1. Cales son as normas de rexistro de dominios gTLD?

As normas varían según a súa natureza do gTLD, e necesario comunicarse cun rexistrador acreditado da ICANN.

2. Cales son as normas de rexistro de dominios ccTLD?

Teñen que corresponder a un país, territorio ou outra ubicación xeográfica, as regras varían significativamente e resérvanse unha cantidade de ccTLD según os cidadans do país correspondente. Algúns rexistradores acreditados ofrecen servizos de rexistro ccTLD, sin embargo a ICANN non acredita a rexistradores nin establece políticas de rexistro para os ccTLD. Unha lista de todos os ccTLD e os seus administradores designados e a seguinte: <http://www.iana.org/domains/root/db>

3. Se hai problemas cun axente rexistrador, hai que informar á ICANN?

A ICANN non resolve este tipo de cuestiós e reclamos de clientes particulares, e un organismo de coordinación técnica. Terá que ser o propio cliente que se teñan que poner en contacto co axente rexistrador en cuestión, ainda así, si seguimos insistindo como cortesía a ICANN enviará a petición o rexistrador.

4. Obtén unha lista de axentes rexistradores acreditados.

<https://www.icann.org/registrar-reports/accreditation-qualified-list.html>

5. Consulta a web de Red.es e obtén unha lista de axentes rexistradores acreditados para o dominio “es”.

<http://www.dominios.es/dominios/es/agentes-registradores/todos-los-agentes-registradores>

6. Que axentes rexistradores galegos coñeces? Obtén unha lista de axentes rexistradores acreditados para o dominio “gal”.

dinahosting.com

## b. Rexistrando un dominio

i. Eixe un nome de dominio para unha organización, real ou ficticia. Comproba que o dominio non está xa rexistrado. Realiza unha comparativa de precios e servizos ofrecidos entre 3 axentes rexistradores, e argumenta a elección dun deles. Realiza capturas de pantalla.

Facendo un test co dominio “adrianglois.com” decido escoller neste caso 1&1 xa que durante o primeiro ano o coste e de 0,99€ e despois de unhos 10€. Polo que he a opción máis barata.

### c. Whois

i. Eixe 2 ou 3 nomes de dominio xa rexistrados e procura información sobre eles a través dalgún servizo Whois, como por exemplo:

1. <http://www.whois.net>
2. <http://www.iana.org/whois>
3. <http://whois.domaintools.com>
4. <http://www.internic.net/whois.html>



*Resultados correspondientes a: TUSUBTITULO.COM*  
Consulta original: tusubtitulo.com

Información de contacto		
<b>Contacto del registrario</b>	<b>Contacto administrativo</b>	<b>Contacto técnico</b>
Nombre: Tus Subtítulos De Series Organización Tus Subtítulos De Series Dirección postal: 6100 Center Drive Suite 1190, Los Angeles CA 90045 US Teléfono: +1.7574166575 Interno: Fax: Interno: Correo electrónico:tusubtitulo.com@dns-protect.net	Nombre: Tus Subtítulos De Series Organización C/O InMotion Hosting, Inc Dirección postal: 6100 Center Drive Suite 1190, Los Angeles CA 90045 US Teléfono: +1.7574166575 Interno: Fax: Interno: Correo electrónico:tusubtitulo.com@dns-protect.net	Nombre: Domain Administrator Organización C/O InMotion Hosting, Inc Dirección postal: 6100 Center Drive Suite 1190, Los Angeles CA 90045 US Teléfono: +1.7574166575 Interno: Fax: Interno: Correo electrónico:dns-admin@inmotionhosting.com

<b>Registrador</b>  Servidor de WHOIS: whois.tucows.com URL: http://tucowsdomains.com Registrador: TUCOWS, INC. ID de la IANA: 69	<b>Estado</b>  Estado del dominio: ok https://icann.org/epp#ok
--	--

 **ICANN WHOIS**

zonasystem.com **Búsqueda**

*Resultados correspondientes a: ZONASYSTEM.COM*  
Consulta original: zonasystem.com

<b>Información de contacto</b>		
<b>Contacto del registrario</b>	<b>Contacto administrativo</b>	<b>Contacto técnico</b>
Nombre: WHOIS AGENT Organización WHOIS PRIVACY PROTECTION SERVICE, INC. Dirección postal: PO BOX 639, KIRKLAND WA 98083 US Teléfono: +1.4252740657 Interno: Fax: +1.4259744730 Interno: Correo electrónico: QLCRXTCBVG@WHOISPRIVACYPROTECT.COM	Nombre: WHOIS AGENT Organización WHOIS PRIVACY PROTECTION SERVICE, INC. Dirección postal: PO BOX 639, KIRKLAND WA 98083 US Teléfono: +1.4252740657 Interno: Fax: +1.4259744730 Interno: Correo electrónico: QLCRXTCBVG@WHOISPRIVACYPROTECT.COM	Nombre: WHOIS AGENT Organización WHOIS PRIVACY PROTECTION SERVICE, INC. Dirección postal: PO BOX 639, KIRKLAND WA 98083 US Teléfono: +1.4252740657 Interno: Fax: +1.4259744730 Interno: Correo electrónico: QLCRXTCBVG@WHOISPRIVACYPROTECT.COM

 **ICANN WHOIS**

foromtb.com **Búsqueda**

*Resultados correspondientes a: FOROMTB.COM*  
Consulta original: foromtb.com

<b>Información de contacto</b>		
<b>Contacto del registrario</b>	<b>Contacto administrativo</b>	<b>Contacto técnico</b>
Nombre: Luis Romeral Gallego Organización DDM Dirección postal: Avda Errípagana 15, Burlada Navarra 31600 ES Teléfono: +34.620329575 Interno: Fax: Interno: Correo electrónico: luis.romeral@gmail.com	Nombre: Luis Romeral Gallego Organización DDM Dirección postal: Avda Errípagana 15, Burlada Navarra 31600 ES Teléfono: +34.620329575 Interno: Fax: Interno: Correo electrónico: luis.romeral@gmail.com	Nombre: Luis Romeral Gallego Organización DDM Dirección postal: Avda Errípagana 15, Burlada Navarra 31600 ES Teléfono: +34.620329575 Interno: Fax: Interno: Correo electrónico: luis.romeral@gmail.com

<b>Registrador</b>	<b>Estado</b>
Servidor de WHOIS: whois.godaddy.com URL: http://www.godaddy.com Registrador: GoDaddy.com, LLC ID de la IANA: 146 Correo electrónico para informar casos de uso indebido: abuse@godaddy.com Teléfono para informar casos de uso indebido: +1.4806242505	Estado del dominio: clientTransferProhibited <a href="http://www.icann.org/epp#clientTransferProhibited">http://www.icann.org/epp#clientTransferProhibited</a> Estado del dominio: clientUpdateProhibited <a href="http://www.icann.org/epp#clientUpdateProhibited">http://www.icann.org/epp#clientUpdateProhibited</a> Estado del dominio: clientRenewProhibited <a href="http://www.icann.org/epp#clientRenewProhibited">http://www.icann.org/epp#clientRenewProhibited</a> Estado del dominio: clientDeleteProhibited <a href="http://www.icann.org/epp#clientDeleteProhibited">http://www.icann.org/epp#clientDeleteProhibited</a>

**Para os dominios elixidos trata de averiguar a seguinte información:**

- Quen é o rexistrador do dominio (registrant)?

**tusubtitulo.com:** “Tus Subtitulos De Series”

**zonasystem.com:** Neste caso non se podería ver xa que este dominio ten un WHOIS PRIVACY (“WHOIS PRIVACY PROTECTION SERVICE, INC.”).

**foromtb.com:** “Luis Romeral Gallego”

- Quen é o axente rexistrador (registrar)?

**tusubtitulo.com:** “TUCOWS, INC.”

**zonasystem.com:** “ENOM, INC.”

**foromtb.com:** “GoDaddy.com, LLC”

- Cando expira o rexistro do dominio?

**tusubtitulo.com:** “Registration Expiration Date: 2017-07-03”

**zonasystem.com:** “Fecha de vencimiento de la registración: 2017-10-04”

**foromtb.com:** “Fecha de vencimiento de la registración: 2024-06-14”

#### d. Ciberocupación

- i. Investiga o significado do termo “Ciberocupación”.

**Ciberocupación:** É a acción de registrar un nome de dominio, con propósito de extorsionar o candidato que lle interesa para que o compre ou ben simplemente desviar o tráfico web hacia esa dirección de dominio.

## 2.5. Servidores de nomes

### a. Servidores caché

- i. Procura en Internet un listado que amose os servidores DNS caché dos principais proveedores de servizos de internet (ISP) que operan en España (Movistar, R, Vodafone, etc.).

<http://www.adslayuda.com/dns.html>

- ii. Averigua tamén cales son os servidores DNS caché que Google ofrece aos usuarios de Internet. Que ventaxas e inconvenientes ten configurar estes servidores no teu equipo?

**IPv4:** 8.8.8.8 e 8.8.4.4

**IPv6:** 2001:4860:4860::8888 e 2001:4860:4860::8844

**Ventaxas:** Ten a gran parte de websites globais indexadas na súa caché, tamén son más eficientes e rápidos.

**Desventaxas:** Non vexo ningunha a priori, quizás que poden saber que webs visitamos, o igual que o noso ISP no caso de ter as DNS configuradas por defecto do proveedor de servicios.

- iii. Investiga sobre o proxecto <http://www.opendns.org/>. Cal é a finalidade e as características principais do proxecto?

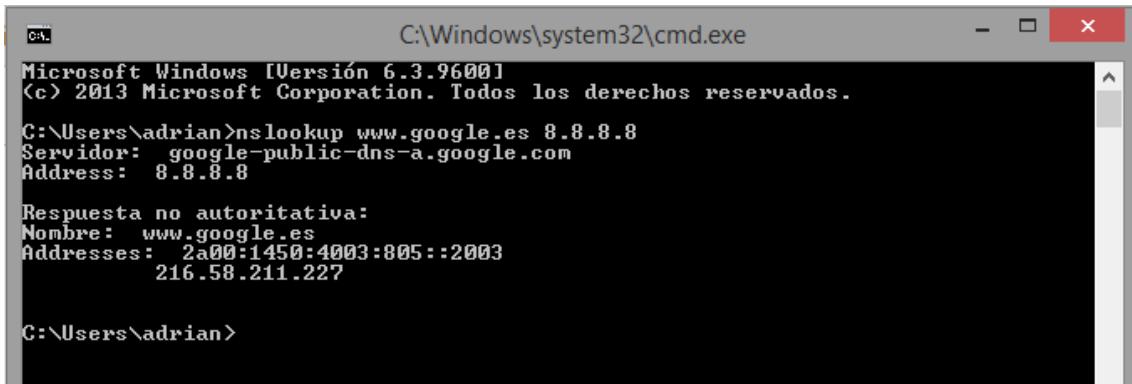
E un proxecto de servidores DNS raíz que é unha alternativa os DNS da ICANN. Proporciona unha lista dos seus TLDs.

### b. Consultas a servidores

- i. Abre un terminal no teu propio equipo ou nunha máquina virtual cliente do contorno de prácticas. Realiza as operación que se indican, respondendo ás preguntas e ilustrándolas con capturas de pantalla:

1. Executa o comando nslookup www.google.es 8.8.8.8 para preguntar ao servidor DNS 8.8.8.8 polo nome de dominio www.google.es. Observa que a resposta é non autorizada. Que significa?

Entendendo a sintaxis da ferramenta nslookup, queremos obter a dirección IP do nome de dominio “www.google.es” facendo a consulta a IP do servidor “8.8.8.8”. O ter unha resposta non autoritativa significa que o servidor 8.8.8.8 non ten autoridade sobre a ese nome polo que non ten configurado dito nome de dominio.



The screenshot shows a Windows Command Prompt window titled 'C:\Windows\system32\cmd.exe'. The window displays the following output:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Users\adrian>nslookup www.google.es 8.8.8.8
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

Respueta no autoritativa:
Nombre: www.google.es
Addresses: 2a00:1450:4003:805::2003
216.58.211.227

C:\Users\adrian>
```

2. Executa o comando nslookup www.google.es ns1.google.com para facer a mesma pregunta ao servidor ns1.google.com. Observa que a resposta é autorizada. Que significa?

Neste caso o preguntarle o servidor “ns1.google.com” polo nome de dominio [www.google.es](http://www.google.es) este respondenos de forma autoritativa xa que ns1.google.com si ten autoridade sobre o nome de dominio www.google.es.

```
C:\Users\adrian>nslookup www.google.es ns1.google.com
Servidor:  ns1.google.com
Address:  216.239.32.10

Nombre:  www.google.es
Addresses:  2a00:1450:4002:800::2003
           172.217.23.67

C:\Users\adrian>
```

3. Executa os comandos nslookup www.edu.xunta.es ns1.google.com e nslookup www.edu.xunta.es 8.8.8.8. Observa a diferencia nas respostas. Que significa? Que diferencia hai entre o servidor 8.8.8.8 e ns1.google.com?

Neste caso estamos preguntáolle o servidor “ns1.google.com” polo nome de dominio “www.edu.xunta.es” obtemos unha resposta rechazada, sin embargo no seguinte caso preguntamos polo mesmo nome de dominio pero ao servidor “8.8.8.8” e este danos unha resposta non autoritativa xa que non o ten na súa zona de autoridade pero este si pregunta a outros servidores de nivel superior de forma recursiva ata encontrar un servidor autoritativo para coñecer a súa dirección IP e obter unha resposta.

```
C:\Users\adrian>nslookup www.edu.xunta.es ns1.google.com
Servidor:  ns1.google.com
Address:  216.239.32.10

*** ns1.google.com no encuentra www.edu.xunta.es: Query refused

C:\Users\adrian>nslookup www.edu.xunta.es 8.8.8.8
Servidor:  google-public-dns-a.google.com
Address:  8.8.8.8

Respuesta no autoritativa:
Nombre:  www.edu.xunta.es
Address:  85.91.64.102

C:\Users\adrian>
```

### c. Servidores raíz

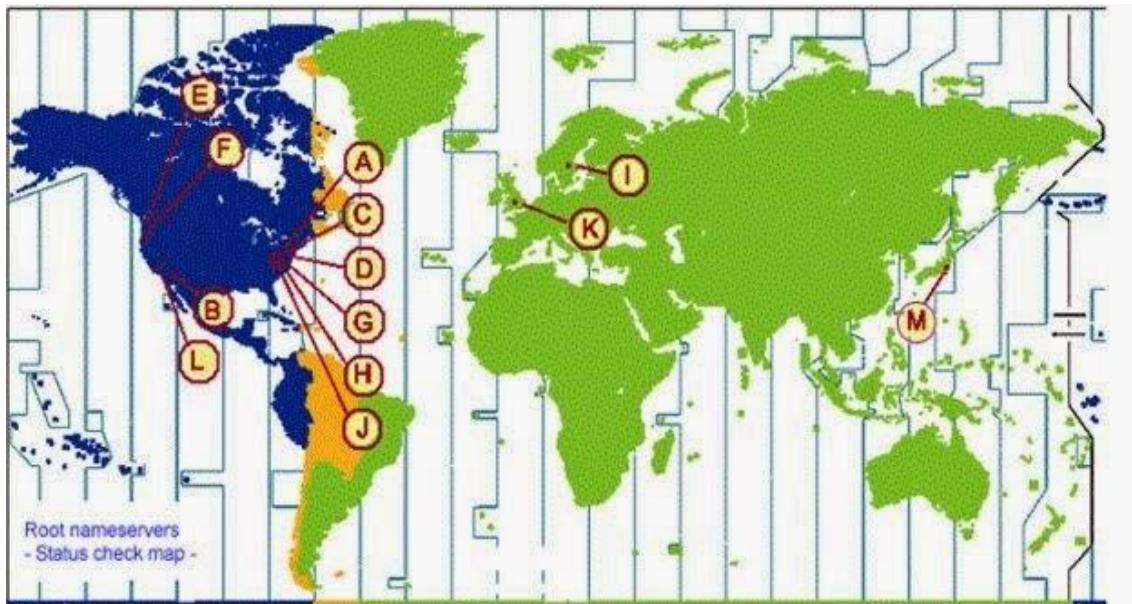
- i. Explora as seguintes webs para ampliar información sobre os servidores raíz, como se nomean, onde se ubican, que organizacións os administran, o seu estado actual, o software que utilizan, etc.

1. <http://root-servers.org>
2. <http://public-root.com>
3. <http://www.iana.org/domains/root>

## ii. Realiza un esquema cos 13 servidores principais e ilústralo cun mapa.

Esta é unha lista das súas direccións IPv4, IPv6 e o seus administradores: <https://www.iana.org/domains/root/servers>

Os 13 servidores están replicados (instancias) entre eles por diversas parte do mundo. Os principais nomeanse polas letras do abecedario, da "A" a "M".



As instancias destes refléxanse no seguinte esquema.



### iii. Hints file

1. Procura e descarga o Hints File, o ficheiro de suxerencias que contén unha copia da información que todos os servidores DNS deben coñecer. Ábreo cun editor de texto e examina o seu contido.

<ftp://rs.internic.net/domain/named.root>  
<https://www.internic.net/domain/named.root>

#### iv. Root Zone

1. Procura e descarga o arquivo da zona raíz (root.zone), e ábreo cun editor de texto. Este arquivo é unha copia do ficheiro de zona que conteñen todos os servidores DNS raíz. En él están reflexados todos os dominios de primeiro nivel (TLD). Para cada un deles existe un ou varios rexistros de recursos do tipo NS, que indican os servidores de nomes autorizados nos que se delega a xestión dese TLD. Procura no arquivo os rexistros NS correspondentes a un dominio dado, por exemplo o “gal”, e compara os seus valores coa información obtida sobre o dominio na web da IANA (<http://www.iana.org/domains/root/db>).

<ftp://rs.internic.net/domain/root.zone>  
<https://www.internic.net/domain/root.zone>  
<http://www.iana.org/domains/root/db/gal.h>

## 2.6. Resolución de direcciones

a. Nun cliente Linux executa o seguinte comando:

```
dig @8.8.8.8 www.edu.xunta.es +trace
```

b. Con este comando envíámosslle unha consulta recursiva ao servidor 8.8.8.8 preguntando polo nome de dominio “www.edu.xunta.es”. Coa opción +trace indicámosslle que amose todo o rastro do proceso de resolución. Observa e comenta a saída do comando e ilústralo cunha captura de pantalla.

De forma recursiva o servidor 8.8.8.8 realiza unha consulta os root servers por si coñecen o dominio .es a súa vez estes outros envíanse consultas entre eles ata encontrar o dominio xunta o cal ten autoridade para sobre “www.edu.xunta.es”, responstando finalmente a consulta.

```
agl_US32-16.4_SERI_dns2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
admin@ns1:~$ dig @8.8.8.8 www.edu.xunta.es +trace
; <>> DiG 9.10.3-P4-Ubuntu <>> @8.8.8.8 www.edu.xunta.es +trace
; (1 server found)
; global options: +cmd
;                                          185140  IN      NS      a.root-servers.net.
;                                          185140  IN      NS      b.root-servers.net.
;                                          185140  IN      NS      c.root-servers.net.
;                                          185140  IN      NS      d.root-servers.net.
;                                          185140  IN      NS      e.root-servers.net.
;                                          185140  IN      NS      f.root-servers.net.
;                                          185140  IN      NS      g.root-servers.net.
;                                          185140  IN      NS      h.root-servers.net.
;                                          185140  IN      NS      i.root-servers.net.
;                                          185140  IN      NS      j.root-servers.net.
;                                          185140  IN      NS      k.root-servers.net.
;                                          185140  IN      NS      l.root-servers.net.
;                                          185140  IN      NS      m.root-servers.net.
;                                          185140  IN      RRSIG   NS 8 0 158400 201611209170000 20161126160000 39291 .
fJKOM1hLMK1l2PZ2ZP9o5t6jb53MMzxDUyvug08C6D016aZ7sI15V.mSwa QafPU10QcgA16aJCA5NvBy2dte022EWBR1r4TuONIrpb
6g7F10XZPnGNd cdScIglv1uB91q2fwqENQqabSHs1GuJtDoWD6c2EitMCwj3bnL9M9DMvX ovq8KN4VuwiCNX4yMgRXRMZYURPYA+
BbprGEEed2f IT2w9VLTxZT1YXM9R xpsdWdP0OB5CwY.bsXrCueZhBQ2exrahUx5nkwcjdQ+PPV9.jU1w96FQbac
Cn/Lu9EV5xemWh+/>pPr40ULLaRb21tGcooDyahz6so fkYtiQ==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 14 ms

es.          172800  IN      NS      g.nic.es.
es.          172800  IN      NS      sns-pb.isc.org.
es.          172800  IN      NS      ns-ext.nic.cl.
es.          172800  IN      NS      f.nic.es.
es.          172800  IN      NS      a.nic.es.
es.          172800  IN      NS      ns3.nic.fr.
es.          172800  IN      NS      ns1.cesca.es.
es.          86400   IN      DS      44290 8 2 562EF35E7065588A7178A4BD0155C8527F029C82AA
455DD359C84908 B2A7FE17
es.          86400   IN      DS      44290 8 1 7711F564D55B41C8CE7DFAF4DD323C5B271F86CD
es.          86400   IN      RRSIG   DS 8 1 86400 20161210170000 20161127160000 39291 . G
vPMo5iV5iY0ieNaCp558mQPADYajS3Zk2EKpS4.jQ+P2ATyKAsy24Wzz 12ogbsFoaCqTRvQX1z2CTUkzs4VnaVhtq13c7uc1YFLG
9+c2gABkb2Rtu Ti5z2IYntC1q+XtUzpgzLQ3.GcuabpFF3LJE2U7edr9FrhLcJiDkYU P2Z+qzayymunZqn2dcXmA5GKaHaA1r
d5q5jm23txal/ePNJt9U4i1s8d4 4+DgAgqKoYa8vCrD4wI48cW4J4.FRNFBHwU0DHEYcpgrho3bqdw307qB1/ qUBgFmD9.jzEWruuJ
L/B1bMmkpf74NrHs/fKrI3FLHjGYw0?G6pdY2Bz adjuMyQ=-
;; Received 851 bytes from 202.12.27.33#53(ns.root-servers.net) in 34 ms

xunta.es.     86400   IN      NS      ns2.xunta.es.
xunta.es.     86400   IN      NS      ns1.xunta.es.
arsop9k8ot1utqucd.jpgaurgiu37691c.es. 86400 IN NSEC3 1 1 5 BB0A6E12362AD41F ARSSRJDNQITLNG0MT4I30I2IF
NMGB8DGU NS SOA RRSIG DNSKEY NSEC3PARAM
arsop9k8ot1utqucd.jpgaurgiu37691c.es. 86400 IN RRSIG NSEC3 8 2 86400 20161208222631 20161124230217 10
798 es. Q6el1CPhn7thuUcQs/bwEORINL10vp21Pg3hS4nwLaHDMS5BkLR5SaKSu rzBusq/H0ygUaUbSu+jyyqe6RtpTLgZaMY
SudjBTQr+NOjW01Xwb9c0 2Mtyk5pBtReU6gvvgg/uLxeMHLk2BYtQa3UhMr6Mps0/BNv0Ly.juTYbGfk TNA=
719nhm1o9iq1uhf jnugtg0qk9r57drn9.es. 86400 IN NSEC3 1 1 5 BB0A6E12362AD41F 71GANHTN7PM6EPNSV8A5A8SE2
A2BDQNC MS DS RRSIG
719nhm1o9iq1uhf jnugtg0qk9r57drn9.es. 86400 IN RRSIG NSEC3 8 2 86400 20161209063043 20161124230217 10
798 es. eAr8kz/Tg9w1QD2/gNV08UQ4p11o0KB42Ea4uNeu35wJuEDMaxcqB3 7TwGTQJxaJZDgHJS7lim5TzNcbnuMrDGbGR
u4y7b1JLdRhssr1dSuFQn p8Btf8aiix.EzrK9PiWRwTiRNuWPidbxR1rI3Ja5i30z1iIavvAvId 07M=
;; Received 612 bytes from 192.5.4.1#53(sns-pb.isc.org) in 55 ms

www.edu.xunta.es. 28800  IN      A      85.91.64.102
xunta.es.        28800  IN      NS      ns2.xunta.es.
xunta.es.        28800  IN      NS      ns1.xunta.es.
;; Received 129 bytes from 85.91.64.172#53(ns1.xunta.es) in 119 ms

admin@ns1:~$
```

c. Proba a executar de novo o comando cambiando o nome de dominio a resolver e o servidor DNS ao que se lle pregunta. Observa e comenta os resultados.

Probando co servidor DNS público dun ISP de Movistar e preguntando polo nome de dominio “www.zonasytem.com”, ocorre o mesmo, sendo as consultas recursivas ata conseguir unha resposta.

```

; <>> DiG 9.10.3-P4-Ubuntu <>> @80.58.61.254 www.zonasystem.com +trace
; (1 server found)
;; global options: +cmd
                250557 IN      NS      f.root-servers.net.
                250557 IN      NS      l.root-servers.net.
                250557 IN      NS      h.root-servers.net.
                250557 IN      NS      b.root-servers.net.
                250557 IN      NS      d.root-servers.net.
                250557 IN      NS      e.root-servers.net.
                250557 IN      NS      m.root-servers.net.
                250557 IN      NS      g.root-servers.net.
                250557 IN      NS      a.root-servers.net.
                250557 IN      NS      k.root-servers.net.
                250557 IN      NS      c.root-servers.net.
                250557 IN      NS      j.root-servers.net.
                250557 IN      NS      i.root-servers.net.
;; Received 587 bytes from 80.58.61.254#53(80.58.61.254) in 18 ms

com.                      172800 IN      NS      c.gtld-servers.net.
com.                      172800 IN      NS      i.gtld-servers.net.
com.                      172800 IN      NS      m.gtld-servers.net.
com.                      172800 IN      NS      j.gtld-servers.net.
com.                      172800 IN      NS      e.gtld-servers.net.
com.                      172800 IN      NS      g.gtld-servers.net.
com.                      172800 IN      NS      l.gtld-servers.net.
com.                      172800 IN      NS      1.gtld-servers.net.
com.                      172800 IN      NS      d.gtld-servers.net.
com.                      172800 IN      NS      a.gtld-servers.net.
com.                      172800 IN      NS      f.gtld-servers.net.
com.                      172800 IN      NS      k.gtld-servers.net.
com.                      172800 IN      NS      b.gtld-servers.net.
com.                      172800 IN      NS      h.gtld-servers.net.
com.                      86400  IN      DS      30909 8 2 E2D3C916F6DEEAC73294E826FB5885044A833FC54
59588P4A9184CF C41A5766
com.                      86400  IN      RRSIG   DS 8 1 86400 20161210170000 20161127160000 39291 . Z
6VJa2NG3S93wgkzYKPaNu9u2NL48o7kyJW2BrcSY2qkIYfApM7jAnjk? c4psUkdTwdsFngrUZYu5M1uIptrBuqCNM12hrfKg+S2
UmtpbPTgY0I Y9iBmDpIRCj21owSryhXuHuQx?auxOxT3W2uRFFX/5zrqWCMAN5mYC 2MuTsfe9X0tfr.jkntPrFKBaBQ/X7xy
xHLxp18022Axw1lbdvE0Kd7URw D-nPrQhQC1V9bd3KFu0w7Drmp193Nf ih7gUrda3ZQX3Xv17Pw0avvNb+ y CotMipvpQomf vUq
6rea13jdTtaUk9wPITEJQpghx3ekp0LLXhxLrfI zrrowQ==
;; Received 870 bytes from 193.0.14.129#53(k.root-servers.net) in 85 ms

zonasystem.com.          172800 IN      NS      dns1.name-services.com.
zonasystem.com.          172800 IN      NS      dns2.name-services.com.
zonasystem.com.          172800 IN      NS      dns3.name-services.com.
zonasystem.com.          172800 IN      NS      dns4.name-services.com.
zonasystem.com.          172800 IN      NS      dns5.name-services.com.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0Q1GIN43N1ARRC90SM6QPQR81H5M9A NS SOA
RRSIG DNSKEY NSEC3PARAM
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 8 2 86400 20161204054708 20161127043708 6
404 com. suwJf2pApG7mc5J+qkBFRYzYyz2NbbAbLN9dAMHIodDiJuB1WXk7suMG r1Hjdduvb8M95yBKwFDATqUbNNHEH2Gwz6
X8UA2VZ/YE22BrX3BYr1Tk 1AVQA02EBy4Hbh811xgUK7zfqtUD+y+8pObmq36MdUTb3y4eU/c0rUEJ Szc=
UPAR084LQQCKGCJRQUEO189NPPH7629Q.com. 86400 IN NSEC3 1 1 0 - UPB00L6BGA4AM1UQU9R32SD90LEE7A29 NS DS
RRSIG
UPAR084LQQCKGCJRQUEO189NPPH7629Q.com. 86400 IN RRSIG NSEC3 8 2 86400 20161201053105 20161124042105 6
404 com. Yh+ImJtrEgB3dhej+xDk+aYq8UDxEh5yUFWQpFKSbhmajbPRomUhmg GL2EBCKkus8BqauLzd0p8V1DyQl25WIGba
3mSgn8cpull0kxs0YKAg5X QaT08GWBSR34s3CTzm1hvTnQ1NxMoKigFEosdH6IsIV9Gp9b+ZQ1lewY k3Q=
;; Received 861 bytes from 192.41.162.30#53(1.gtld-servers.net) in 181 ms

www.zonasystem.com.     1800   IN      CNAME   ghs.google.com.
;; Received 72 bytes from 162.88.60.23#53(dns2.name-services.com) in 41 ms

uadmin@ns1:~$
```

## 2.7. Consulta a servidores DNS con nslookup, host e dig

As ferramentas nslookup, host e dig permiten configurar o tipo de consulta que se quere realizar a un servidor DNS. Utilizarémolas para comprobar o funcionamento do servizo DNS, obter información e verificar o funcionamiento dos servidores.

O comando nslookup atópase dispoñible tanto en Windows como en Linux, host e dig só en Linux. Consulta en Internet ou na axuda do sistema as opcións de configuración destes comandos e realiza as accións que se indican a continuación.

### a. Nslookup

- Obtén a dirección IP de “www.edu.xunta.es”.

```
C:\Users\adrian>nslookup
Servidor predeterminado: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

> www.edu.xunta.es
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
Nombre: www.edu.xunta.es
Address: 85.91.64.102

>
```

- Accede a nslookup en modo interactivo. Configura o servidor 8.8.8.8 como servidor ao que se realizarán as preguntas e consulta os servidores DNS autorizados para o dominio “www.edu.xunta.es”.

```
C:\Users\adrian>nslookup
Servidor predeterminado: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

> server 8.8.8.8
Servidor predeterminado: google-public-dns-a.google.com
Address: 8.8.8.8

> set query=NS
> edu.xunta.es
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

xunta.es
    primary name server = ns1.xunta.es
    responsible mail addr = sistemas.xunta.es
    serial    = 2016110901
    refresh   = 10800 <3 hours>
    retry     = 1800 <30 mins>
    expire    = 1814400 <21 days>
    default TTL = 1800 <30 mins>

> correos.es
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

Respuesta no autoritativa:
correos.es      nameserver = ns2.correos.es
correos.es      nameserver = artemis.ttd.net
correos.es      nameserver = ns1.correos.es
> -
```

**iii. Consulta os servidores de correo autorizados para o dominio “www.edu.xunta.es” (RR=MX).**

```
> set query=MX
> edu.xunta.es
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

Respuesta no autoritativa:
edu.xunta.es      MX preference = 5, mail exchanger = smtp.edu.xunta.es
> correos.es
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

Respuesta no autoritativa:
correos.es        MX preference = 5, mail exchanger = mx.cep.correos.es
>
```

**iv. Consulta os servidores DNS autorizados para o dominio raíz. (Utiliza un punto “.” como nome de dominio).**

```
> set query=NS
> .
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

Respuesta no autoritativa:
<root> nameserver = d.root-servers.net
<root> nameserver = e.root-servers.net
<root> nameserver = a.root-servers.net
<root> nameserver = k.root-servers.net
<root> nameserver = f.root-servers.net
<root> nameserver = j.root-servers.net
<root> nameserver = c.root-servers.net
<root> nameserver = g.root-servers.net
<root> nameserver = l.root-servers.net
<root> nameserver = h.root-servers.net
<root> nameserver = m.root-servers.net
<root> nameserver = i.root-servers.net
<root> nameserver = b.root-servers.net
```

**v. Configura os servidores autorizados para o dominio “com”.**

Configuraremos un root server dos anteriores para realizar a consulta a os gTLDs (operadores de rexistro) “com.”

```
> com.
Servidor: d.root-servers.net
Address: 199.7.91.13

Nombre: com
Served by:
- e.gtld-servers.net
    192.12.94.30
    com
- k.gtld-servers.net
    192.52.178.30
    com
- l.gtld-servers.net
    192.41.162.30
    com
- b.gtld-servers.net
    192.33.14.30
    2001:503:231d::2:30
    com
- c.gtld-servers.net
    192.26.92.30
```

**vi.** Configura un deles como servidor DNS que responderá as consultas.

Configuramos un root servidor

```
> server 192.12.94.30
in-addr.arpa    nameserver = f.in-addr-servers.arpa
in-addr.arpa    nameserver = d.in-addr-servers.arpa
in-addr.arpa    nameserver = c.in-addr-servers.arpa
in-addr.arpa    nameserver = a.in-addr-servers.arpa
in-addr.arpa    nameserver = b.in-addr-servers.arpa
in-addr.arpa    nameserver = e.in-addr-servers.arpa
a.in-addr-servers.arpa   internet address = 199.212.0.73
b.in-addr-servers.arpa   internet address = 199.253.183.183
c.in-addr-servers.arpa   internet address = 196.216.169.10
d.in-addr-servers.arpa   internet address = 200.10.60.53
e.in-addr-servers.arpa   internet address = 203.119.86.101
f.in-addr-servers.arpa   internet address = 193.0.9.1
a.in-addr-servers.arpa   AAAA IPv6 address = 2001:500:13::73
b.in-addr-servers.arpa   AAAA IPv6 address = 2001:500:87::87
c.in-addr-servers.arpa   AAAA IPv6 address = 2001:43f8:110::10
d.in-addr-servers.arpa   AAAA IPv6 address = 2001:13c7:7010::53
e.in-addr-servers.arpa   AAAA IPv6 address = 2001:dd8:6::101
f.in-addr-servers.arpa   AAAA IPv6 address = 2001:67c:e0::1
Servidor predeterminado: [192.12.94.30]
Address: 192.12.94.30
```

**vii.** Pregunta polo dominio “iesleliadoura.com”. Observa que o servidor responde coa lista de servidores autorizados para o dominio “iesleliadoura.com”.

```
> iesleliadoura.com
Servidor: [192.12.94.30]
Address: 192.12.94.30
Nombre: iesleliadoura.com
Served by:
- ns.dinahosting.com
  82.98.128.132
  iesleliadoura.com
- ns2.dinahosting.com
  82.98.128.196
  iesleliadoura.com
- ns3.dinahosting.com
  72.29.96.10
  iesleliadoura.com
- ns4.dinahosting.com
  93.89.82.218
  iesleliadoura.com
```

**viii.** Pregunta polo dominio “iesleliadoura.es”. Que significa o resultado?.

```
> iesleliadoura.es
Servidor: [192.12.94.30]
Address: 192.12.94.30
Nombre: iesleliadoura.es
Served by:
- g.root-servers.net

- h.root-servers.net

- i.root-servers.net

- j.root-servers.net

- k.root-servers.net

- l.root-servers.net

- m.root-servers.net

- a.root-servers.net

- b.root-servers.net

- c.root-servers.net

> -
```

**ix.** Continúa experimentando co comando nslookup. Por exemplo, obtén os servidores autorizados para outros dominios, obtén os rexistros SOA dos seus ficheiros de zona, consulta o número de serie, etc.

set debug > muestra información avanzada.

```
> set debug
> sergas.es
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

-----
Got answer:
HEADER:
    opcode = QUERY, id = 11, rcode = REFUSED
    header flags: response, want recursion, recursion avail.
    questions = 0, answers = 0, authority records = 0, additional = 0

-----
Got answer:
HEADER:
    opcode = QUERY, id = 12, rcode = REFUSED
    header flags: response, want recursion, recursion avail.
    questions = 0, answers = 0, authority records = 0, additional = 0

-----
Got answer:
HEADER:
    opcode = QUERY, id = 13, rcode = REFUSED
    header flags: response, want recursion, recursion avail.
    questions = 1, answers = 0, authority records = 0, additional = 0

    QUESTIONS:
        sergas.es, type = A, class = ANY

-----
Got answer:
HEADER:
    opcode = QUERY, id = 14, rcode = REFUSED
    header flags: response, want recursion, recursion avail.
    questions = 1, answers = 0, authority records = 0, additional = 0

    QUESTIONS:
        sergas.es, type = AAAA, class = ANY

*** 250.red-80-58-61.staticip.rima-tde.net no encuentra sergas.es: Query refused
> -
```

set d2 > muestra información aún más avanzada.

```
> set d2
> sergas.es
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

SendRequest(), len 27
HEADER:
    opcode = QUERY, id = 15, rcode = NOERROR
    header flags: query, want recursion
    questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
    sergas.es, type = A, class = ANY
-----

Got answer (27 bytes):
HEADER:
    opcode = QUERY, id = 15, rcode = REFUSED
    header flags: response, want recursion, recursion avail.
    questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
    sergas.es, type = A, class = ANY
-----

SendRequest(), len 27
HEADER:
    opcode = QUERY, id = 16, rcode = NOERROR
    header flags: query, want recursion
    questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
    sergas.es, type = AAAA, class = ANY
-----

Got answer (12 bytes):
HEADER:
    opcode = QUERY, id = 16, rcode = REFUSED
    header flags: response, want recursion, recursion avail.
    questions = 0, answers = 0, authority records = 0, additional = 0
-----

SendRequest(), len 27
HEADER:
    opcode = QUERY, id = 17, rcode = NOERROR
    header flags: query, want recursion
    questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
    sergas.es, type = A, class = ANY
-----

Got answer (27 bytes):
HEADER:
    opcode = QUERY, id = 17, rcode = REFUSED
    header flags: response, want recursion, recursion avail.
    questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
    sergas.es, type = A, class = ANY
-----

SendRequest(), len 27
HEADER:
    opcode = QUERY, id = 18, rcode = NOERROR
    header flags: query, want recursion
    questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
    sergas.es, type = AAAA, class = ANY
-----

Got answer (27 bytes):
HEADER:
    opcode = QUERY, id = 18, rcode = REFUSED
    header flags: response, want recursion, recursion avail.
    questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
    sergas.es, type = AAAA, class = ANY
```

```
C:\>nslookup
Servidor predeterminado: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

> flickr.com
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
Nombre: flickr.com
Address: 69.147.76.173

> set type=ns
> flickr.com
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
flickr.com      nameserver = ns5.yahoo.com
flickr.com      nameserver = ns3.yahoo.com
flickr.com      nameserver = ns2.yahoo.com
flickr.com      nameserver = ns4.yahoo.com
flickr.com      nameserver = ns1.yahoo.com
> server ns1.yahoo.com
Servidor predeterminado: ns1.yahoo.com
Addresses: 2001:4998:130::1001
68.180.131.16

> ls -s flickr.com
ls: connect: No error
*** No se puede hacer una lista del dominio flickr.com: Unspecified error
El servidor DNS rechazó la transferencia de la zona flickr.com a su equipo. Si es
incorrecto, compruebe la configuración de seguridad de la zona de transferencia
para flickr.com en el servidor DNS en la dirección IP 2001:4998:130::1001.

> ls -a flickr.com
ls: connect: No error
*** No se puede hacer una lista del dominio flickr.com: Unspecified error
El servidor DNS rechazó la transferencia de la zona flickr.com a su equipo. Si es
incorrecto, compruebe la configuración de seguridad de la zona de transferencia
para flickr.com en el servidor DNS en la dirección IP 2001:4998:130::1001.

>
```

Facendo outras consultas co propio servidor ns1.yahoo.com configurado como servidor DNS, de forma que as preguntas os dominios internos podan ser respondidas con “ls [-argumento] [dominio]” síguese sin obter resposta, o cual sería o normal, por seguridade, tamén os servidores ns1.yahoo.com e demais non están autorizados a responder xa que que tampouco actúan como reenviadores.

```
> set type=ns
> flickr.com
Servidor: servidor.acarballeira.local
Address: 10.10.10.2

Respuesta no autoritativa:
flickr.com      nameserver = ns3.yahoo.com
flickr.com      nameserver = ns2.yahoo.com
flickr.com      nameserver = ns5.yahoo.com
flickr.com      nameserver = ns1.yahoo.com
flickr.com      nameserver = ns4.yahoo.com

ns3.yahoo.com  internet address = 203.84.221.53
ns2.yahoo.com  internet address = 68.142.255.16
ns5.yahoo.com  internet address = 119.160.247.124
ns1.yahoo.com  internet address = 68.180.131.16
ns4.yahoo.com  internet address = 98.138.11.157
> server ns1.yahoo.com
Servidor predeterminado: ns1.yahoo.com
Addresses: 2001:4998:130::1001
68.180.131.16

> ls -s ns1.yahoo.com
ls: connect: No error
*** No se puede hacer una lista del dominio ns1.yahoo.com: Unspecified error
El servidor DNS rechazó la transferencia de la zona ns1.yahoo.com a su equipo. Si es
incorrecto, compruebe la configuración de seguridad de la zona de transferencia
para ns1.yahoo.com en el servidor DNS en la dirección IP 2001:4998:130::1001.

> ls -s flickr.com
ls: connect: No error
*** No se puede hacer una lista del dominio flickr.com: Unspecified error
El servidor DNS rechazó la transferencia de la zona flickr.com a su equipo. Si es
incorrecto, compruebe la configuración de seguridad de la zona de transferencia
para flickr.com en el servidor DNS en la dirección IP 2001:4998:130::1001.

> ls -a flickr.com
ls: connect: No error
*** No se puede hacer una lista del dominio flickr.com: Unspecified error
El servidor DNS rechazó la transferencia de la zona flickr.com a su equipo. Si es
incorrecto, compruebe la configuración de seguridad de la zona de transferencia
para flickr.com en el servidor DNS en la dirección IP 2001:4998:130::1001.

>
```

**b. host**

- i. Realiza unha consulta directa dun nome de dominio usando o servidor DNS configurado no sistema.

```
uadmin@ns1:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#      DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.100.2
nameserver 80.58.61.250
nameserver 80.58.61.254
uadmin@ns1:~$ host www.zonasystem.com
www.zonasystem.com is an alias for ghs.google.com.
ghs.google.com is an alias for ghs.l.google.com.
ghs.l.google.com has address 216.58.210.179
ghs.l.google.com has IPv6 address 2a00:1450:4003:804::2013
uadmin@ns1:~$
```

- ii. Realiza unha consulta inversa dunha dirección IP usando o servidor DNS configurado no sistema.

```
uadmin@ns1:~$ host 216.58.210.179
179.210.58.216.in-addr.arpa domain name pointer mad06s10-in-f19.1e100.net.
179.210.58.216.in-addr.arpa domain name pointer mad06s10-in-f179.1e100.net.
uadmin@ns1:~$ host 81.47.192.13
13.192.47.81.in-addr.arpa domain name pointer 13.red-81-47-192.staticip.rima-tde.net.
uadmin@ns1:~$ host 8.8.8.8
8.8.8.8.in-addr.arpa domain name pointer google-public-dns-a.google.com.
uadmin@ns1:~$
```

- iii. Realiza unha nova consulta, directa ou inversa, utilizando un servidor DNS concreto, por exemplo 8.8.4.4.

```
uadmin@ns1:~$ host www.zonasystem.com 8.8.4.4
Using domain server:
Name: 8.8.4.4
Address: 8.8.4.4#53
Aliases:

www.zonasystem.com is an alias for ghs.google.com.
ghs.google.com is an alias for ghs.l.google.com.
ghs.l.google.com has address 216.58.210.179
ghs.l.google.com has IPv6 address 2a00:1450:4003:804::2013
uadmin@ns1:~$ host www.zonasystem.com ns1.google.com
Using domain server:
Name: ns1.google.com
Address: 216.239.32.10#53
Aliases:

Host www.zonasystem.com not found: 5(REFUSED)
uadmin@ns1:~$ _
```

#### iv. Consulta os servidores DNS autorizados (rexistro NS) para un domino concreto.

```
uadmin@ns1:~$ host -t NS lavozdegalicia.es 8.8.4.4
Using domain server:
Name: 8.8.4.4
Address: 8.8.4.4#53
Aliases:

lavozdegalicia.es name server dns1.lavoz.es.
lavozdegalicia.es name server dns2.lavoz.es.
uadmin@ns1:~$ host -a lavozdegalicia.es 8.8.4.4
Trying "lavozdegalicia.es"
Using domain server:
Name: 8.8.4.4
Address: 8.8.4.4#53
Aliases:

;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 56751
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;lavozdegalicia.es.      IN      ANY

;; ANSWER SECTION:
lavozdegalicia.es.    2522    IN      SOA     dns1.lavoz.es. root.mail.lavoz.es. 1611031230 16384
2048 1048576 2560
lavozdegalicia.es.    86362   IN      NS      dns1.lavoz.es.
lavozdegalicia.es.    86362   IN      NS      dns2.lavoz.es.
lavozdegalicia.es.    86362   IN      MX      10 a.mx.lavozdegalicia.es.
lavozdegalicia.es.    86362   IN      MX      20 b.mx.lavozdegalicia.es.
lavozdegalicia.es.    86362   IN      TXT    "v=spf1 a mx include:spf.acumbamail.com ~all"
lavozdegalicia.es.    86362   IN      A       77.27.236.100

Received 236 bytes from 8.8.4.4#53 in 14 ms
uadmin@ns1:~$ _
```

#### v. Consulta o rexistro SOA dun dominio concreto. Que valor ten o número de serie e que significa?.

O número de serie representa a versión do ficheiro de zona correspondiente e aumenta cada vez que o ficheiro cambia. Isto é de utilidade os servidores secundarios e así comprobar se a copia que eles teñen está actualizada ou non.

```
uadmin@ns1:~$ host -C lavozdegalicia.es
Nameserver 82.98.137.203:
    lavozdegalicia.es has SOA record dns1.lavoz.es. root.mail.lavoz.es. 1611031230 16384 2048 10
48576 2560
Nameserver 77.27.236.84:
    lavozdegalicia.es has SOA record dns1.lavoz.es. root.mail.lavoz.es. 1611031225 16384 2048 10
48576 2560
uadmin@ns1:~$ _
```

#### vi. Continúa explorando as posibilidades do comando host.

```
uadmin@ns1:~$ host -t MX lavozdegalicia.es
lavozdegalicia.es mail is handled by 10 a.mx.lavozdegalicia.es.
lavozdegalicia.es mail is handled by 20 b.mx.lavozdegalicia.es.
uadmin@ns1:~$ host -a lavozdegalicia.es
Trying "lavozdegalicia.es"
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 43920
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;lavozdegalicia.es.      IN      ANY

;; ANSWER SECTION:
lavozdegalicia.es.    85754   IN      MX      20 b.mx.lavozdegalicia.es.
lavozdegalicia.es.    85754   IN      MX      10 a.mx.lavozdegalicia.es.
lavozdegalicia.es.    31161   IN      A       77.27.236.100
lavozdegalicia.es.    2368    IN      SOA    dns1.lavoz.es. root.mail.lavoz.es. 1611031225 16384
2048 1048576 2560
lavozdegalicia.es.    81994   IN      NS      dns1.lavoz.es.
lavozdegalicia.es.    81994   IN      NS      dns2.lavoz.es.

;; AUTHORITY SECTION:
lavozdegalicia.es.    81994   IN      NS      dns1.lavoz.es.
lavozdegalicia.es.    81994   IN      NS      dns2.lavoz.es.

;; ADDITIONAL SECTION:
dns1.lavoz.es.        82179   IN      A       77.27.236.84
dns2.lavoz.es.        76147   IN      A       82.98.137.203

Received 240 bytes from 192.168.100.2#53 in 22 ms
uadmin@ns1:~$ host -t SOA lavozdegalicia.es
lavozdegalicia.es has SOA record dns1.lavoz.es. root.mail.lavoz.es. 1611031225 16384 2048 1048576 25
60
uadmin@ns1:~$
```

### c. Dig

i. Obtén información sobre un nome de dominio, por exemplo “www.edu.xunta.es”. Observa toda a información que proporciona o comando dig: organiza os datos amosados en seccións que se corresponden cos campos principais da cabeceira das mensaxes DNS.

(*Header, Question, Answer, Authority e Additional*) e amosa os rexistros de recursos recibidos nun formato similar ao dos ficheiros de zona. As liñas que comezan por punto e coma “;” son comentarios introducidos polo comando dig.

```
uadmin@ns1:~$ dig www.edu.xunta.es

; <>> DiG 9.10.3-P4-Ubuntu <>> www.edu.xunta.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57564
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.edu.xunta.es.           IN      A

;; ANSWER SECTION:
www.edu.xunta.es.      17137    IN      A      85.91.64.102

;; Query time: 45 msec
;; SERVER: 192.168.100.2#53(192.168.100.2)
;; WHEN: Mon Nov 28 13:27:52 CET 2016
;; MSG SIZE rcvd: 61

uadmin@ns1:~$ _
```

ii. Realiza unha consulta inversa e obtén o nome asociado a unha dirección IP.

```
uadmin@ns1:~$ dig -x 85.91.64.102

; <>> DiG 9.10.3-P4-Ubuntu <>> -x 85.91.64.102
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61307
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;102.64.91.85.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
102.64.91.85.in-addr.arpa. 28799 IN      PTR      www.edu.xunta.es.

;; Query time: 220 msec
;; SERVER: 192.168.100.2#53(192.168.100.2)
;; WHEN: Mon Nov 28 13:32:50 CET 2016
;; MSG SIZE rcvd: 84

uadmin@ns1:~$ _
```

```
uadmin@ns1:~$ dig -x 85.91.64.102 +short
www.edu.xunta.es.
uadmin@ns1:~$ _
```

**iii.** Realiza unha consulta a un servidor DNS distinto ao configurado no sistema.

```
uadmin@ns1:~$ dig @8.8.4.4 www.edu.xunta.es
; <>> DiG 9.10.3-P4-Ubuntu <>> @8.8.4.4 www.edu.xunta.es
; (1 server found)
; global options: +cmd
; Got answer:
;-->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34194
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; QUESTION SECTION:
;www.edu.xunta.es.           IN      A

; ANSWER SECTION:
www.edu.xunta.es.    19972   IN      A      85.91.64.102

; Query time: 14 msec
; SERVER: 8.8.4.4#53(8.8.4.4)
; WHEN: Mon Nov 28 13:36:44 CET 2016
; MSG SIZE rcvd: 61

uadmin@ns1:~$ dig @8.8.4.4 www.edu.xunta.es +short
85.91.64.102
uadmin@ns1:~$ _
```

**iv.** Consulta polos servidores autorizados para un nome de dominio.

```
uadmin@ns1:~$ dig sergas.es soa
; <>> DiG 9.10.3-P4-Ubuntu <>> sergas.es soa
; global options: +cmd
; Got answer:
;-->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10540
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; QUESTION SECTION:
;sergas.es.           IN      SOA

; ANSWER SECTION:
sergas.es.        86176   IN      SOA     ns1.sergas.es. soporte\comunicaciones.sergas.es. 20
16100401 43200 900 2419200 43200

; AUTHORITY SECTION:
sergas.es.        86176   IN      NS      ns1.sergas.es.
sergas.es.        86176   IN      NS      ns3.sergas.es.
sergas.es.        86176   IN      NS      ns2.sergas.es.
sergas.es.        86176   IN      NS      artemis.ttd.net.
sergas.es.        86176   IN      NS      ns4.sergas.es.

; Query time: 0 msec
; SERVER: 192.168.100.2#53(192.168.100.2)
; WHEN: Mon Nov 28 14:00:10 CET 2016
; MSG SIZE rcvd: 198

uadmin@ns1:~$ _
```

**v.** Pregunta por todos os rexistros de recursos dun dominio concreto.

```
uadmin@ns1:~$ dig sergas.es any
; <>> DiG 9.10.3-P4-Ubuntu <>> sergas.es any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62164
;; flags: qr rd ra; QUERY: 1, ANSWER: 12, AUTHORITY: 5, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sergas.es.           IN      ANY

;; ANSWER SECTION:
sergas.es.          86399   IN      SPF     "v=spf1 mx ip4:217.124.244.71 ip4:217.124.244.72 ip4
:217.124.244.99 ~all"
sergas.es.          86399   IN      TXT     "v=spf1 mx ip4:217.124.244.71 ip4:217.124.244.72 ip4
:217.124.244.99 ~all"
sergas.es.          86399   IN      MX      10 mail01.sergas.es.
sergas.es.          86399   IN      MX      10 mail02.sergas.es.
sergas.es.          86399   IN      MX      20 mail04.sergas.es.
sergas.es.          86399   IN      A       217.124.244.30
sergas.es.          86399   IN      NS      ns2.sergas.es.
sergas.es.          86399   IN      NS      artemis.ttd.net.
sergas.es.          86399   IN      NS      ns4.sergas.es.

sergas.es.          86399   IN      NS      ns3.sergas.es.
sergas.es.          86399   IN      NS      ns1.sergas.es.
sergas.es.          86399   IN      SOA    ns1.sergas.es. soporte\comunicaciones.sergas.es. 20
16100401 43200 900 2419200 43200

;; AUTHORITY SECTION:
sergas.es.          86399   IN      NS      ns4.sergas.es.
sergas.es.          86399   IN      NS      ns1.sergas.es.
sergas.es.          86399   IN      NS      ns3.sergas.es.
sergas.es.          86399   IN      NS      artemis.ttd.net.
sergas.es.          86399   IN      NS      ns2.sergas.es.

;; Query time: 87 msec
;; SERVER: 192.168.100.2#53(192.168.100.2)
;; WHEN: Mon Nov 28 13:56:27 CET 2016
;; MSG SIZE rcvd: 521

uadmin@ns1:~$ _
```

**vi.** Continúa explorando as posibilidades do comando *dig*.

Consultar varios nomes de dominios a partir dun arquivo de texto.

```
uadmin@ns1:~$ cat consultaDNS.txt
www.edu.xunta.es
www.lavozdegalicia.es
www.elpais.com
uadmin@ns1:~$ dig -f consultaDNS.txt +short
85.91.64.102
akavoz-1413069856.eu-west-1.elb.amazonaws.com.
52.31.125.224
52.211.30.7
52.208.168.47
elpais.es.edgesuite.net.
a1749.g.akamai.net.
84.53.132.241
84.53.132.249
uadmin@ns1:~$ _
```

Realizar consultas concatenadas preguntando por diferentes types.

```
uadmin@ns1:~$ dig edu.xunta.es mx lavozdegalicia.es ns +short
5 smtp.edu.xunta.es.
dns1.lavoz.es.
dns2.lavoz.es.
uadmin@ns1:~$ _
```

### 3. 2º Parte DNS

#### 3.1. Exercicio 1: Consultas DNS

1. Mediante máquinas virtuais e empregando o SW Wireshark utiliza os comandos dig e nslookup (ou host) para:

- a) Obter os nomes dos servidores autorizados para o dominio “es”.

```
C:\Windows\system32\cmd.exe - nslookup
C:\Users\wadmin>nslookup
Servidor predeterminado: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

> set type=NS
> es.
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
es      nameserver = ns3.nic.fr
es      nameserver = g.nic.es
es      nameserver = f.nic.es
es      nameserver = ns1.cesca.es
es      nameserver = a.nic.es
es      nameserver = sns-pb.isc.org
es      nameserver = ns-ext.nic.cl

ns1.cesca.es    internet address = 84.88.0.3
ns1.cesca.es    AAAA IPv6 address = 2001:40b0:1:1122:ce5c:a000:0:3
>
```

	66 18.401117	10.0.0.22	80.58.61.250	DNS	62 Standard query 0x0002 NS es
	67 18.426411	80.58.61.250	10.0.0.22	DNS	261 Standard query response 0x0002 NS es

```
.... .0. .... .... = Authoritative: Server is not an authority for domain
.... .0. .... .... = Truncated: Message is not truncated
.... ...1 .... .... = Recursion desired: Do query recursively
.... .... 1.... .... = Recursion available: Server can do recursive queries
.... .... .0. .... = Z: reserved (0)
.... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
.... .... ...0 .... = Non-authenticated data: Unacceptable
.... .... .... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 7
Authority RRs: 0
Additional RRs: 2
Queries
  ▾ es: type NS, class IN
    Name: es
    [Name Length: 2]
    [Label Count: 1]
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
  ▾ Answers
    ▷ es: type NS, class IN, ns ns3.nic.fr
    ▷ es: type NS, class IN, ns g.nic.es
    ▷ es: type NS, class IN, ns f.nic.es
    ▷ es: type NS, class IN, ns ns1.cesca.es
    ▷ es: type NS, class IN, ns a.nic.es
    ▷ es: type NS, class IN, ns sns-pb.isc.org
    ▷ es: type NS, class IN, ns ns-ext.nic.cl
  ▾ Additional records
    ▷ ns1.cesca.es: type A, class IN, addr 84.88.0.3
    ▷ ns1.cesca.es: type AAAA, class IN, addr 2001:40b0:1:1122:ce5c:a000:0:3
```

b) Nome e IP do servidor de correo electrónico para o dominio "xunta.gal".

```
C:\Users\wadmin>nslookup
Servidor predeterminado: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

> set type=MX
> xunta.gal
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
xunta.gal      MX preference = 10, mail exchanger = mail.xunta.es
>
```

144 137.153288 10.0.0.22 80.58.61.250 DNS 69 Standard query 0x0002 MX xunta.gal
145 137.184120 80.58.61.250 10.0.0.22 DNS 98 Standard query response 0x0002 MX xunta.gal MX 10 mail.xunta.es
197 220.211804 10.0.0.22 80.58.61.250 DNS 85 Standard query 0x0001 PTR 250.61.58.80.in-addr.arpa
198 220.223699 80.58.61.250 10.0.0.22 DNS 137 Standard query response 0x0001 PTR 250.61.58.80.in-addr.arpa PTR 250.red-80-58-61.staticip.rima-tde.net

Ethernet II, Src: AskeyCom\_ce01:2b (fc:04:e6:ce:01:2b), Dst: PcsSyste\_ad:ba:5b (08:00:27:ad:ba:5b)
Internet Protocol Version 4, Src: 80.58.61.250, Dst: 10.0.0.22
Use Datagram Protocol, Src Port: 53, Dst Port: 63524
Domain Name System (response)
[Request In: 144]
[Time: 0.030852000 seconds]
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
xunta.gal: type MX, class IN
 Name: xunta.gal
 [Name Length: 9]
 [Label Count: 2]
 Type: MX (Mail eXchange) (15)
 Class: IN (0x0001)
Answers
xunta.gal: type MX, class IN, preference 10, mx mail.xunta.es
 Name: xunta.gal
 Type: MX (Mail eXchange) (15)
 Class: IN (0x0001)
 Time to live: 28800
 Data length: 17
 Preference: 10
 Mail Exchange: mail.xunta.es

0000 00 00 27 ad ba 5b fc b4 e6 ce 01 2b 08 00 45 00 ..'.[... ...+E.
0010 00 54 bb fb 40 00 f7 11 2f 53 50 3a 3d fa 0a 00 ..T..@... /Sp=...
0020 00 16 00 35 f8 24 00 40 95 7a 00 02 81 80 00 01 ..5.\$@.z....
0030 00 01 00 00 00 05 78 75 6e 74 61 03 67 61 6c .....x.unta.gal
0040 00 00 0f 00 01 c8 0c 00 0f 00 01 00 00 70 80 00 ..... ....p..
0050 11 00 0a 04 6d 61 69 6c 05 78 75 6e 74 61 02 65 ...mail.xunta.e
0060 73 06 ..

- c) Obtén unha resposta autorizada sobre a dirección IP correspondente ao nome "www.cifpcarballeira.es".

```

C:\Windows\system32\cmd.exe - nslookup
C:\Users\wadmin>nslookup
Servidor predeterminado: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250
> exit

C:\Users\wadmin>nslookup
Servidor predeterminado: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250
> cifpcarballeira.es
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250
Respuesta no autoritativa:
Nombre: cifpcarballeira.es
Addresses: 2001:8d8:1001:115d:af97:6985:fdce:2821
          217.160.230.126
> set type=ns
> cifpcarballeira.es
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250
Respuesta no autoritativa:
cifpcarballeira.es nameserver = ns-es.iandi-dns.biz
cifpcarballeira.es nameserver = ns-es.iandi-dns.org
cifpcarballeira.es nameserver = ns-es.iandi-dns.es
cifpcarballeira.es nameserver = ns-es.iandi-dns.com
cifpcarballeira.es nameserver = ns-es.iandi-dns.net
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250
Respuesta no autoritativa:
cifpcarballeira.es nameserver = ns-es.iandi-dns.biz
cifpcarballeira.es nameserver = ns-es.iandi-dns.org
cifpcarballeira.es nameserver = ns-es.iandi-dns.com
cifpcarballeira.es nameserver = ns-es.iandi-dns.net
ns-es.iandi-dns.biz      internet address = 217.160.81.5
ns-es.iandi-dns.biz      AAAA IPv6 address = 2001:8d8:fe:53:0:d9a0:5105:100
ns-es.iandi-dns.org     internet address = 2001:8d8:fe:53:0:d9a0:5305:100
ns-es.iandi-dns.com     internet address = 217.160.82.5
ns-es.iandi-dns.com     AAAA IPv6 address = 2001:8d8:fe:52:0:d9a0:5205:100
ns-es.iandi-dns.es      internet address = 217.160.80.5
ns-es.iandi-dns.es      AAAA IPv6 address = 2001:8d8:fe:53:0:d9a0:5005:100
> -
  
```

```

C:\Windows\system32\cmd.exe - nslookup
C:\Users\wadmin>nslookup
Servidor predeterminado: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250
> server 217.160.80.5
Servidor predeterminado: ns-es.iandi-dns.es
Address: 217.160.80.5
> cifpcarballeira.es
Servidor: ns-es.iandi-dns.es
Address: 217.160.80.5
Nombre: cifpcarballeira.es
Addresses: 2001:8d8:1001:115d:af97:6985:fdce:2821
          217.160.230.126
>
  
```

No.	Time	Source	Destination	Protocol	Length	Info
3	0.957714	10.0.0.22	80.58.61.250	DNS	85	Standard query 0x3619 A teredo.ipv6.microsoft.com
4	0.969182	80.58.61.250	10.0.0.22	DNS	187	Standard query response 0x3619 No such name A teredo.ipv6.microsoft.com

**Frame 4: 187 bytes on wire (1496 bits), 187 bytes captured (1496 bits) on interface 0**

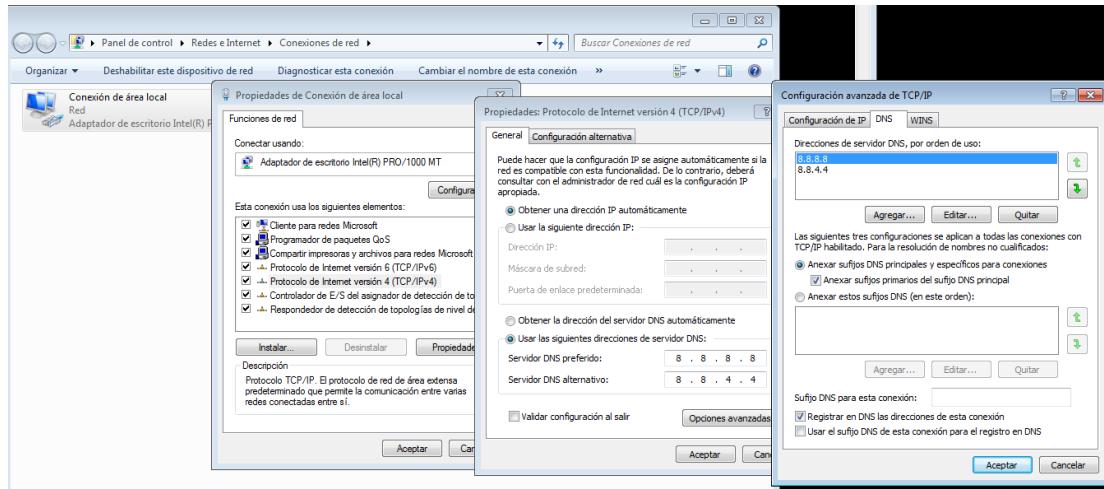
- ① Ethernet II, Src: AskynetCom\_ce:01:2b (fc:b4:e6:ce:01:2b), Dst: PcsSysteme\_ad:ba:5b (08:00:27:ad:ba:5b)
- ② Internet Protocol Version 4, Src: 80.58.61.250, Dst: 10.0.0.22
- ③ User Datagram Protocol, Src Port: 53, Dst Port: 51641
- ④ Domain Name System (request)
  - Request In: 31
    - [Time: 0.011468000 seconds]
    - Transaction ID: 0x3619
    - Flags: 0x0183 Standard query response, No such name
    - Questions: 1
    - Answer RRs: 1
    - Authority RRs: 1
    - Additional RRs: 0
  - Queries
  - Answers
  - Authoritative nameservers
    - nsatc.net: type SOA, class IN, mname admin.nsatc.net
      - Name: nsatc.net
      - Type: SOA (Start of a zone of Authority) (6)
      - Class: IN (0x0001)
      - Time to live: 80
      - Data length: 41
      - Primary name server: admin.nsatc.net
      - Responsible authority's mailbox: dns.level3.net
      - Serial Number: 1477308682
      - Refresh Interval: 10800 (3 hours)
      - Retry Interval: 2700 (45 minutes)
      - Expire limit: 3600000 (41 days, 16 hours)
      - Minimum TTL: 900 (15 minutes)

### 3.2. Exercicio 2: Consultas DNS

**2.** Arranca unha MV cliente Windows. Realiza as seguintes operacións ilustrándoas con capturas de pantalla:

a) Configura os servidores caché de Google como servidores DNS principal e secundario.

Engadir os DNS primario é secundario con posibilidade de engadir máis servidores DNS de forma gráfica en Windows.



Engadir os DNS desde consola de comandos de Windows con “netsh”.

b) Utiliza o comando nslookup para averiguar a dirección IP do nome DNS “www.edu.xunta.es”.

```
C:\Windows\system32>nslookup www.edu.xunta.es
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

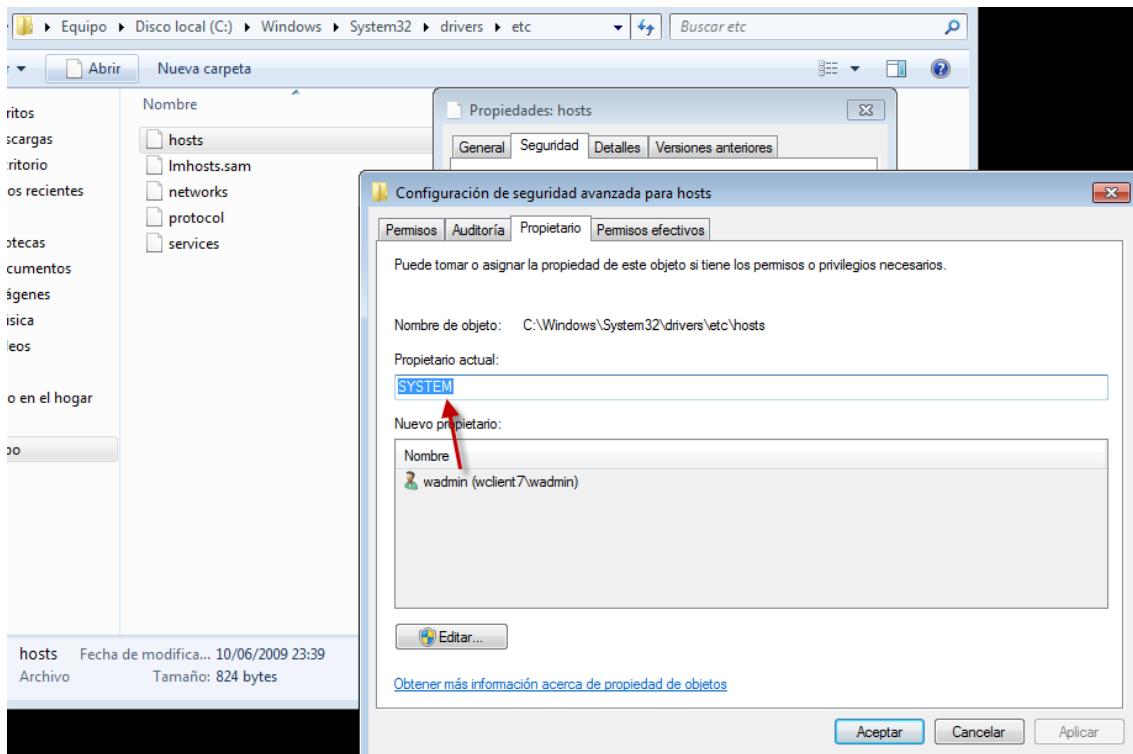
Respueta no autoritativa:
Nombre: www.edu.xunta.es
Address: 85.91.64.102

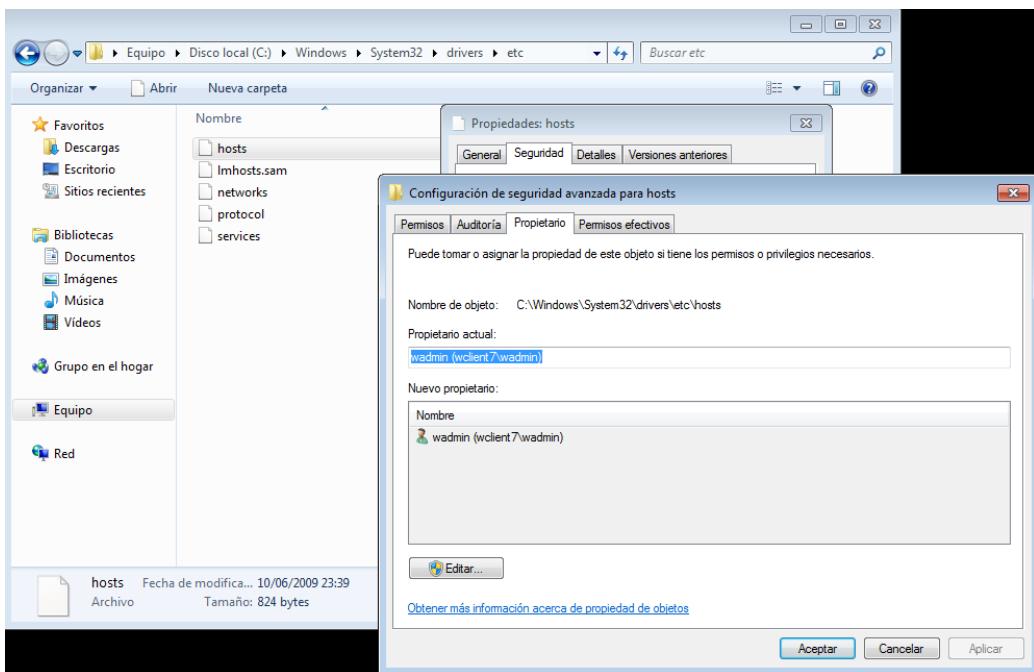
C:\Windows\system32>
```

c) Engade unha entrada no ficheiro hosts onde se relacione a IP do apartado anterior co nome “www.xunta.gal”.

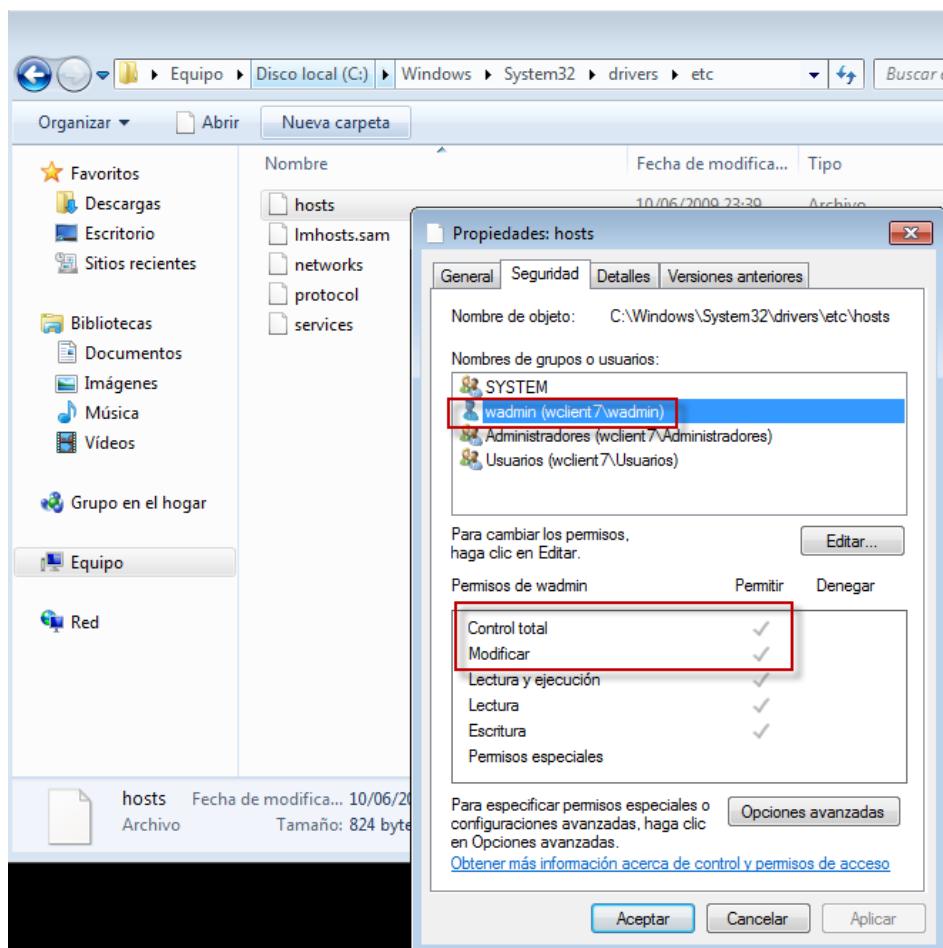
Para poder editar o ficheiro hosts de forma más rápida e no caso de que o queiramos editar en repitadas ocasións, existe unha forma en Windows para poder facelo se modificamos os permisos NTFS do ficheiro con certos privilexios.

Aínda que nos demos control total para o noso usuario isto non vai funcionar, xa que teríamos que poñer o noso usuario actual que pertenecerá por defecto o grupo administradores do equipo local, establecelo como Propietario do ficheiro hosts xa que por defecto o propietario deste, e por seguridade, é o usuario SYSTEM.

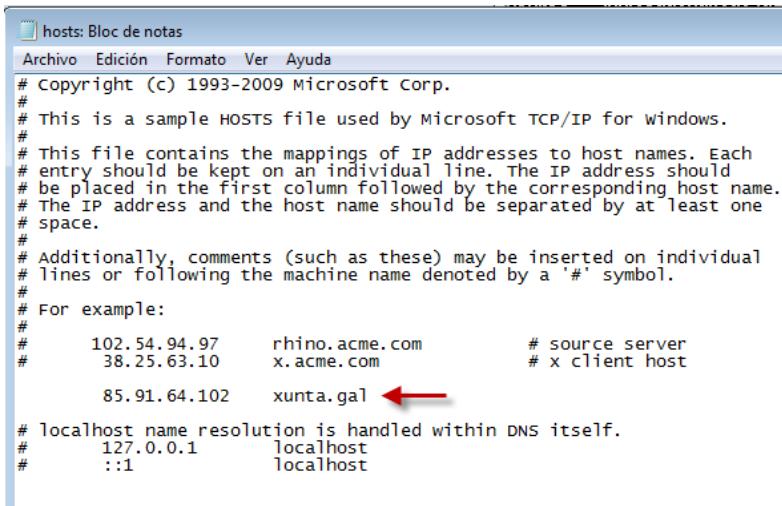




Unha vez somos propietarios do ficheiro este permítenos modificar o noso antoxo os permisos para o usuario que queiramos, polo que engadimos o usuario actual explícitamente e a este otorgámoslle control total sobre este ficheiro.



Agora poderemos editar o ficheiro e gardalo no mesmo directorio actual por defecto "%systemroot%\System32\drivers\etc\hosts" sin máis complicacións



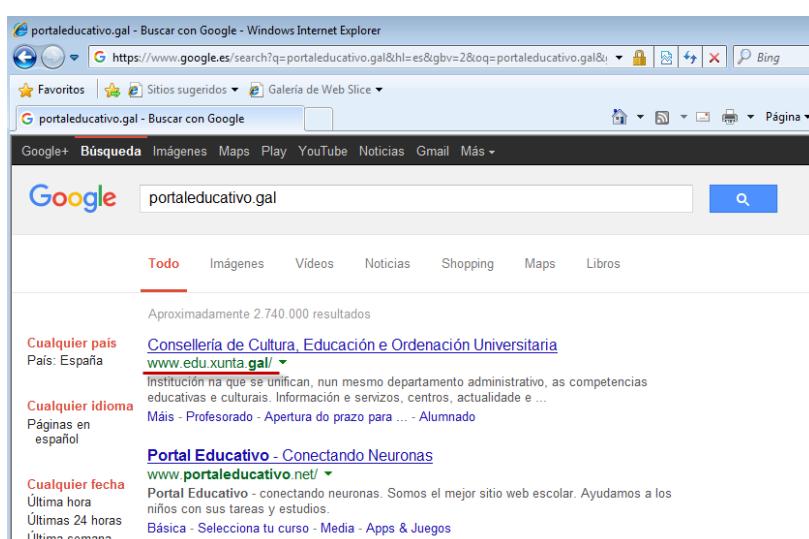
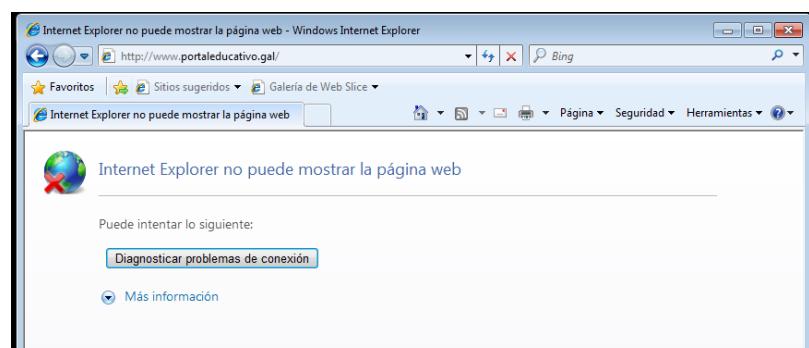
```

hosts: Bloc de notas
Archivo Edición Formato Ver Ayuda
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host
#
#      85.91.64.102      xunta.gal          ← Red arrow here
#
# Localhost name resolution is handled within DNS itself.
#      127.0.0.1      localhost
#      ::1            localhost

```

- d) Comproba que podes usar o nome “www.portaleducativo.gal” para acceder ao portal “www.edu.xunta.gal”.

A website indicada estaba caída... aínda que me imaxino que nun pasado esto sería unha redirección DNS, como se mostra na búsqueda directamente en Google por ese dominio.



e) Visualiza a caché do cliente DNS da máquina Windows.

Mostrando a caché vemos como non existe o nome de dominio [www.portaleducativo.gal](http://www.portaleducativo.gal).



```
C:\Windows\system32\cmd.exe
C:\>ipconfig /displaydns
Configuración IP de Windows

xunta.gal
-----
Nombre de registro . . . : xunta.gal
Tipo de registro . . . : 1
Período de vida . . . : 86400
Longitud de datos . . . : 4
Sección . . . : respuesta
Un registro <host> . . . : 85.91.64.102

xunta.gal
-----
No hay registros de tipo AAAA

www.portaleducativo.gal
-----
No existe el nombre.

www.edu.xunta.gal
-----
Nombre de registro . . . : www.edu.xunta.gal
Tipo de registro . . . : 1
Período de vida . . . : 18546
Longitud de datos . . . : 4
Sección . . . : respuesta
Un registro <host> . . . : 85.91.64.110

102.64.91.85.in-addr.arpa
-----
Nombre de registro . . . : 102.64.91.85.in-addr.arpa.
Tipo de registro . . . : 12
Período de vida . . . : 86400
Longitud de datos . . . : 4
Sección . . . : respuesta
Registro PTR . . . . . : xunta.gal
```

### 3.3. Exercicio 3: Consultas DNS

3. Nunha máquina cliente Linux, captura empregando o Wireshark o tráfico xerado pola execución do comando **dig @8.8.8.8 www.edu.xunta.es +trace**. Garda o ficheiro de captura (pcap) e resposta as seguintes preguntas:

- a) Engade unha captura de pantalla da saída do comando e describe de forma xeral o proceso de resolución de consulta levado a cabo.

Faese unha consulta a dirección IP do servidor caché público de Google “8.8.8.8”, e pregúntaselle polo nome de dominio “[www.edu.xunta.es](http://www.edu.xunta.es)”.

Este o non coñeceder a dirección IP a resolver do nome de dominio reenvíalle a petición algúun servidor que teña autoridade sobre o dominio raíz “.” os root servers. Os root servers non saben a dirección IP deste dominio sin embargo si sabén quen ten autoridade sobre o dominio “es.” polo que un deles neste caso o “f.root-servers.net.” reenvialle a petición desde ccTLD algúun servidor autorizado, o servidor “a.nic.es.” respondelle decindo que ten autoridade sobre o dominio “xunta.es”, polo que a consulta final e derivada a un servidor autorizado da zona DNS de xunta.es. conseguindo finalmente a resposta a resolución do nome de dominio “edu.xunta.es.”

```
Aplicativos Lugares Sistema
• uadmin@uclient1610: ~
Ficheiro Editar Ver Buscar Terminal Axuda
uadmin@uclient1610:~$ dig @8.8.8.8 www.edu.xunta.es +trace

; <>> DiG 9.10.3-P4-Ubuntu <>> @8.8.8.8 www.edu.xunta.es +trace
; (1 server found)
;; global options: +cmd
.          215943  IN      NS      a.root-servers.net.
.          215943  IN      NS      b.root-servers.net.
.          215943  IN      NS      c.root-servers.net.
.          215943  IN      NS      d.root-servers.net.
.          215943  IN      NS      e.root-servers.net.
.          215943  IN      NS      f.root-servers.net.
.          215943  IN      NS      g.root-servers.net.
.          215943  IN      NS      h.root-servers.net.
.          215943  IN      NS      i.root-servers.net.
.          215943  IN      NS      j.root-servers.net.
.          215943  IN      NS      k.root-servers.net.
.          215943  IN      NS      l.root-servers.net.
.          215943  IN      NS      m.root-servers.net.
.          215943  IN      RRSIG   NS 8 0 518400 20161216050000 201
61203040000 39291 . CVR+03t+LUTSulTyodM940Dtlc6QnhEkr/zn/VTYF+1TTfv7s8E1w3dL tiw
ls05w2yuzss3vwpYZCV/Q1y6sRSUI+19ee3ZSkZxp3sFoYwYQai80 UcocHoi9GWgp+UCPiU33EBWR7n
Dj75ZAhZgGjbb4NC7kjoivyb8ViCm4 /HDK+Pbt1/XDK9WqBCgE1l0a4qfNcozZoF/I/VJMt1CFCYu+f
LHaZ7BS ooAefw7fz3Rhqfh1IloMwhNr+iAuMfIYg5GDqvNcM8PceogA21cVY76b iQp061dZCTuLWXN
qISZlfn2EUwMXv3xnG7Ti5ka0biLLPRaD6l9jbDPK nH+7qw==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 12 ms

es.          172800  IN      NS      sns-pb.isc.org.
es.          172800  IN      NS      f.nic.es.
es.          172800  IN      NS      g.nic.es.
es.          172800  IN      NS      a.nic.es.
es.          172800  IN      NS      ns3.nic.fr.
es.          172800  IN      NS      ns-ext.nic.cl.
es.          172800  IN      NS      ns1.cesca.es.
es.          86400   IN      DS      44290 8 1 771F564D55B41C8CE7DFA
F4DD323C5B271F86CD
es.          86400   IN      DS      44290 8 2 562EF35E7065588A7178A4
BD0155C8527F029C82AA455DD359C84908 B2A7FE17
es.          86400   IN      RRSIG   DS 8 1 86400 20161216170000 2016
1203160000 39291 . XvkFL8nAxizL9pCRhqJ5F3LT/+SVBiGUpNjRGWwnT93bRsy9uFzIw3tA Q0NI
QKVdjjsYELAY2Qqx0kSxGR92+ICtzrahyWAxnc2UhnsLYgo7Mwmws ZSMH0Ls2tIg7Spa2DD74HFgefBF
k0GAsEStPgW14ZE6eq8fxKZ5JNHqz eh90eKaUvrlMfJPUd2GnmEwjfEO//ZyE8R7Bye+cbjJ9AnIJT
ImcaHD h0MVcvd6z+5AuMaWSoPgsZbjswu82Fu2v61eEl0q8AEFn0eAS50VDOIZ aapQxLb2S+HRhhjm
q4a1auwvMXxBkLe4IarB4bqhQltWEUHJpKFkhGH1 vg3ZRA==
```

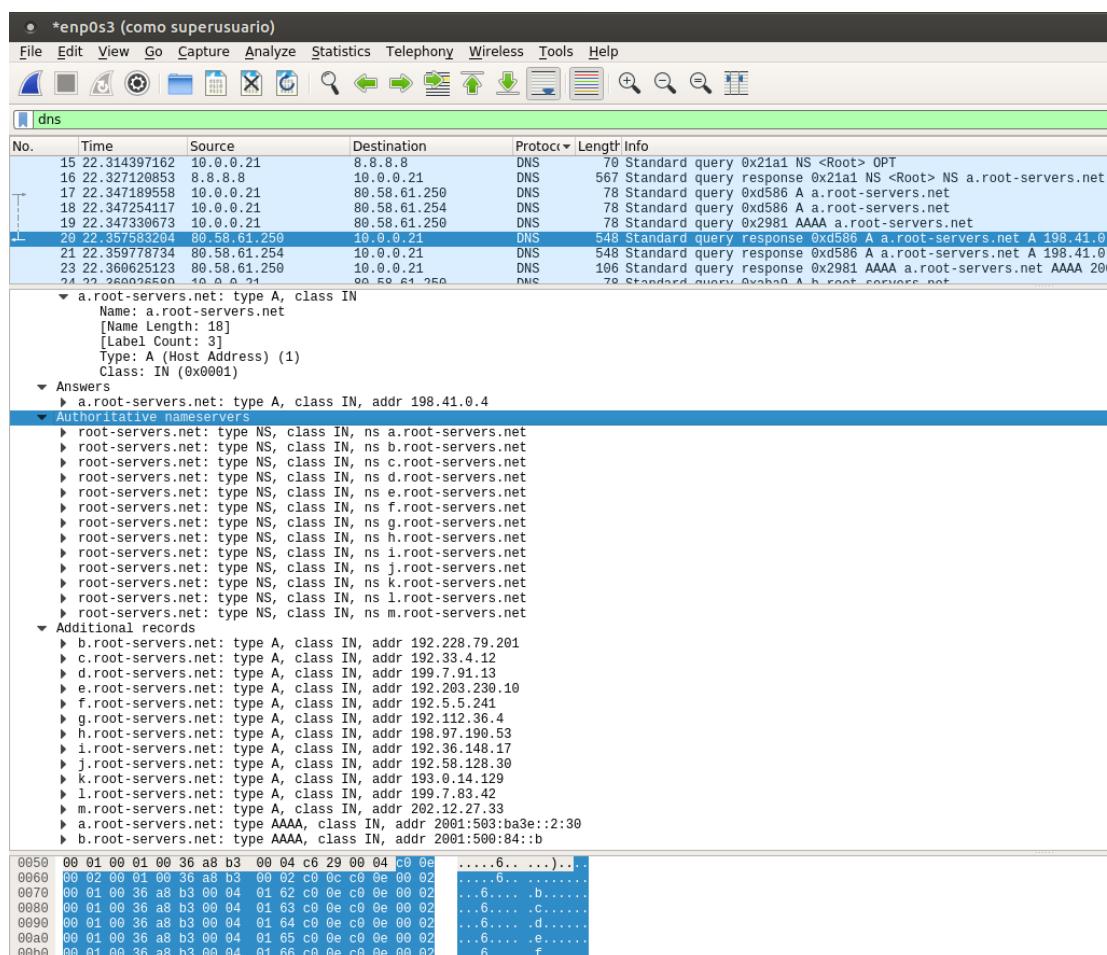
```
; Received 851 bytes from 192.5.5.241#53(f.root-servers.net) in 14 ms

xunta.es.          86400   IN      NS      ns2.xunta.es.
xunta.es.          86400   IN      NS      ns1.xunta.es.
arsop9k8ot1utgucdjpgaurgiv3769lc.es. 86400 IN NSEC3 1 1 5 BB0A6E12362AD41F ARSSR
JDNQITLNG0MT4I30I2IFNMG8D6V NS SOA RRSIG DNSKEY NSEC3PARAM
arsop9k8ot1utgucdjpgaurgiv3769lc.es. 86400 IN RRSIG NSEC3 8 2 86400 201612082226
31 20161124230217 10798 es. Q6el/CPhn7thyUcQs/bwEORINLloVp21Pg3hS4nwlaHDM58kLR5S
aksU rzBvsq/H0ggUAUBdSuj+yqye6RtPTLgZaMYSuJjBTQr+NOJW0IXwb9c0 ZMtyk5pBtReU6gvgg/
uLxeMHLkZBYtQa3UhWr6Mps0/8NvNyjUTYbGfk TNA=
719hn109iqluhfjnugtg0qk9r57drn9.es. 86400 IN NSEC3 1 1 5 BB0A6E12362AD41F 71GAN
HTN7PM6EPNSV8A5A8SE2A2BDQNC NS DS RRSIG
719hn109iqluhfjnugtg0qk9r57drn9.es. 86400 IN RRSIG NSEC3 8 2 86400 201612090630
43 20161124230217 10798 es. eAr8k/zTg9wr1QD2/gNVQ8UQ4pl1o0KB42Ea4uUNeu35vJuEDMax
cqB3 7TwGTQJxaJZDqHJS7lim5TzNcbnuMrDGbGRu4y7b1JLdRhssr1dSuFqn p8BFTf8aiixEzrk9Pi
CWRvTiRNWBPinPdbxR1rI3JA5130z1iIavvAIVid 07M=
;; Received 612 bytes from 194.69.254.1#53(a.nic.es) in 12 ms

www.edu.xunta.es. 28800   IN      A       85.91.64.102
xunta.es.         28800   IN      NS      ns1.xunta.es.
xunta.es.         28800   IN      NS      ns2.xunta.es.
;; Received 129 bytes from 85.91.64.172#53(ns1.xunta.es) in 28 ms

uadmin@uclient1610:~$ █
```

- b) Localiza e visualiza o paquete que inclúe unha resposta cos nomes dos servidores raíz. Engade unha captura de pantalla.



c) Localiza e visualiza a resposta DNS que contén a dirección IPv6 do servidor “h.root-servers.net”. Engade unha captura de pantalla.

No.	Time	Source	Destination	Protocol	Length	Info
47	23.856562210	80.58.61.250	10.0.0.21	DNS	106	Standard query response 0xd2c0 AAAA g.root-servers.net AAAA 2001:500:12::d0
48	23.858394245	80.58.61.250	10.0.0.21	DNS	536	Standard query response 0x314e A g.root-servers.net A 192.112.36.4 NS a.root-servers.net
49	23.858631619	10.0.0.21	80.58.61.250	DNS	78	Standard query 0xc4cf A h.root-servers.net
50	23.858689245	10.0.0.21	80.58.61.250	DNS	78	Standard query 0xf40f AAAA h.root-servers.net
51	23.904752772	80.58.61.250	10.0.0.21	DNS	94	Standard query response 0xc4cf A h.root-servers.net A 198.97.190.53
52	23.921504816	80.58.61.250	10.0.0.21	DNS	548	Standard query response 0xf40f AAAA h.root-servers.net AAAA 2001:500:1::53
53	23.921859042	10.0.0.21	80.58.61.250	DNS	78	Standard query 0xb952 A 1.root-servers.net
54	23.921917421	10.0.0.21	80.58.61.250	DNS	78	Standard query 0x1265 AAAA 1.root-servers.net

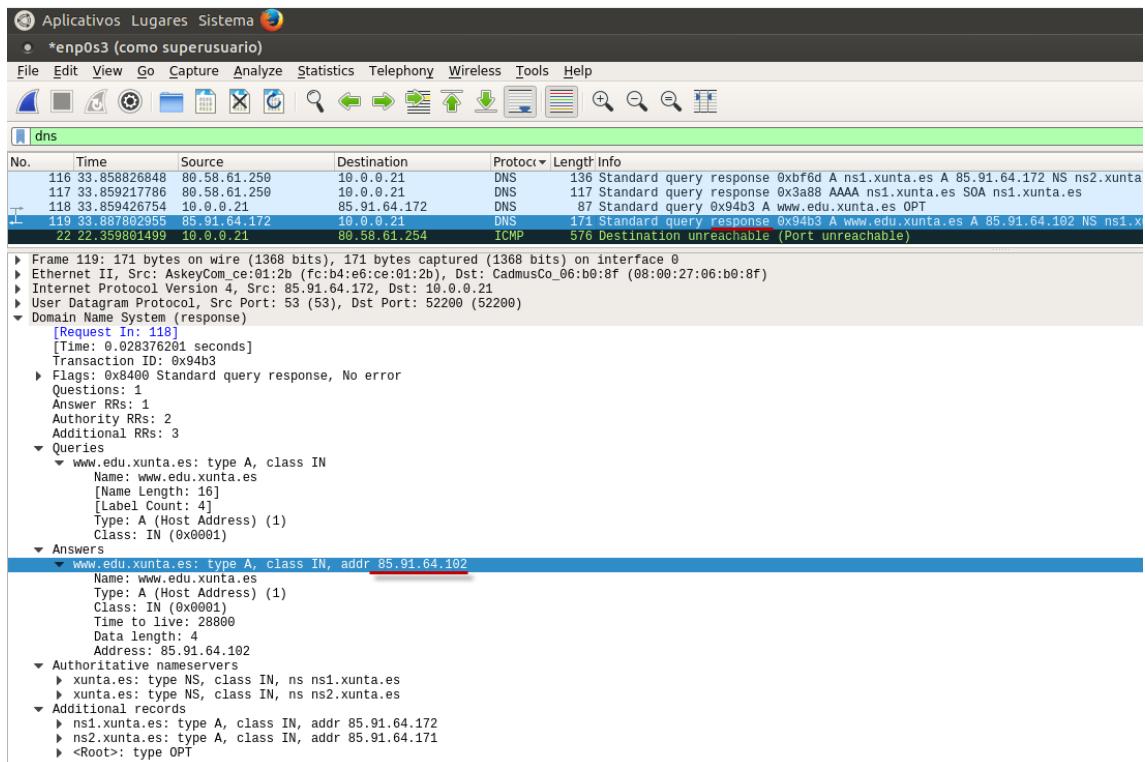
Frame 52: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface 0  
 ▶ Ethernet II, Src: AskeyCom\_ce:01:2b (fc:b4:e6:ce:01:2b), Dst: CadmusCo\_06:b0:8f (08:00:27:06:b0:8f)  
 ▶ Internet Protocol Version 4, Src: 80.58.61.250, Dst: 10.0.0.21  
 ▶ User Datagram Protocol, Src Port: 53 (53), Dst Port: 33558 (33558)  
 ▶ Domain Name System (response)  
 [Request In: 50]  
 [Time: 0.062915571 seconds]  
 Transaction ID: 0xf40f  
 ▶ Flags: 0x8100 Standard query response, No error  
 Questions: 1  
 Answer RRs: 1  
 Authority RRs: 13  
 Additional RRs: 14  
 ▶ Queries  
 ▶ h.root-servers.net: type AAAA, class IN  
 Name: h.root-servers.net  
 [Name Length: 18]  
 [Label Count: 3]  
 Type: AAAA (IPv6 Address) (28)  
 Class: IN (0x0001)  
 ▶ Answers  
 ▶ h.root-servers.net: type AAAA, class IN, addr 2001:500:1::53  
 Name: h.root-servers.net  
 Type: AAAA (IPv6 Address) (28)  
 Class: IN (0x0001)  
 Time to live: 3600000  
 Data length: 16  
 AAAA Address: 2001:500:1::53  
 ▶ Authoritative nameservers  
 ▶ Additional records

d) Localiza e visualiza a resposta DNS que contén os servidores autorizados para o nome “www.edu.xunta.es”. Engade unha captura de pantalla.

No.	Time	Source	Destination	Protocol	Length	Info
104	32.789258915	10.0.0.21	80.58.61.250	DNS	72	Standard query 0x16e2 A ns1.cesca.es
105	32.789348224	10.0.0.21	80.58.61.250	DNS	72	Standard query 0xb9df AAAA ns1.cesca.es
106	32.800604819	80.58.61.250	10.0.0.21	DNS	88	Standard query response 0x16e2 A ns1.cesca.es A 84.88.0.3
107	32.802724747	80.58.61.250	10.0.0.21	DNS	238	Standard query response 0x8daf AAAA ns1.cesca.es AAAA 2001:500:1::53
108	33.823572915	10.0.0.21	194.69.254.1	DNS	87	Standard query 0xf3c3 A www.edu.xunta.es OPT
109	33.835808535	194.69.254.1	10.0.0.21	DNS	654	Standard query response 0xf3c3 A www.edu.xunta.es NS ns2.xunta.es
110	33.836124577	10.0.0.21	80.58.61.250	DNS	72	Standard query 0xa833 A ns2.xunta.es
111	33.836168208	10.0.0.21	80.58.61.250	DNS	72	Standard query 0x0ccb AAAA ns2.xunta.es

Frame 109: 654 bytes on wire (5232 bits), 654 bytes captured (5232 bits) on interface 0  
 ▶ Ethernet II, Src: AskeyCom\_ce:01:2b (fc:b4:e6:ce:01:2b), Dst: CadmusCo\_06:b0:8f (08:00:27:06:b0:8f)  
 ▶ Internet Protocol Version 4, Src: 194.69.254.1, Dst: 10.0.0.21  
 ▶ User Datagram Protocol, Src Port: 53 (53), Dst Port: 35411 (35411)  
 ▶ Domain Name System (response)  
 [Request In: 108]  
 [Time: 0.012235620 seconds]  
 Transaction ID: 0xf3c3  
 ▶ Flags: 0x8000 Standard query response, No error  
 Questions: 1  
 Answer RRs: 0  
 Authority RRs: 6  
 Additional RRs: 3  
 ▶ Queries  
 ▶ www.edu.xunta.es: type A, class IN  
 Name: www.edu.xunta.es  
 [Name Length: 16]  
 [Label Count: 4]  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)  
 ▶ Authoritative nameservers  
 ▶ xunta.es: type NS, class IN, ns ns2.xunta.es ← Red arrow points here  
 ▶ xunta.es: type NS, class IN, ns ns1.xunta.es  
 ▶ arsop9k8ot1utgucdjipgaurgiv37691c.es: type NSEC3, class IN  
 ▶ arsop9k8ot1utgucdjipgaurgiv37691c.es: type RRSIG, class IN  
 ▶ 719hn109iqluhfjngtq0k9r57drn9.es: type NSEC3, class IN  
 ▶ 719hn109iqluhfjngtq0k9r57drn9.es: type RRSIG, class IN  
 ▶ Additional records  
 ▶ ns1.xunta.es: type A, class IN, addr 85.91.64.172  
 ▶ ns2.xunta.es: type A, class IN, addr 85.91.64.171  
 ▶ <Root>: type OPT

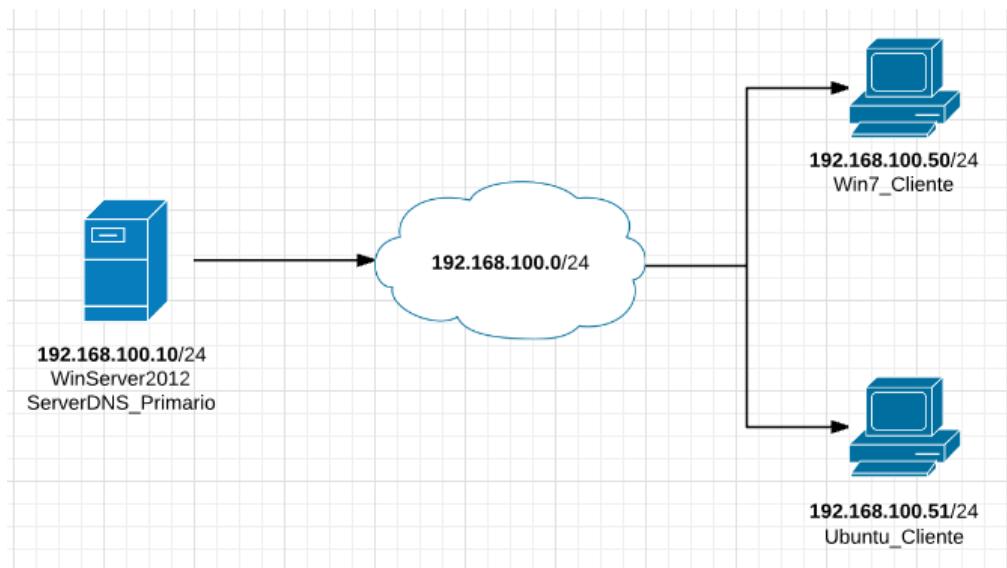
- e) Localiza e visualiza a resposta DNS que contén finalmente a IPv4 correspondente a "www.edu.xunta.es".



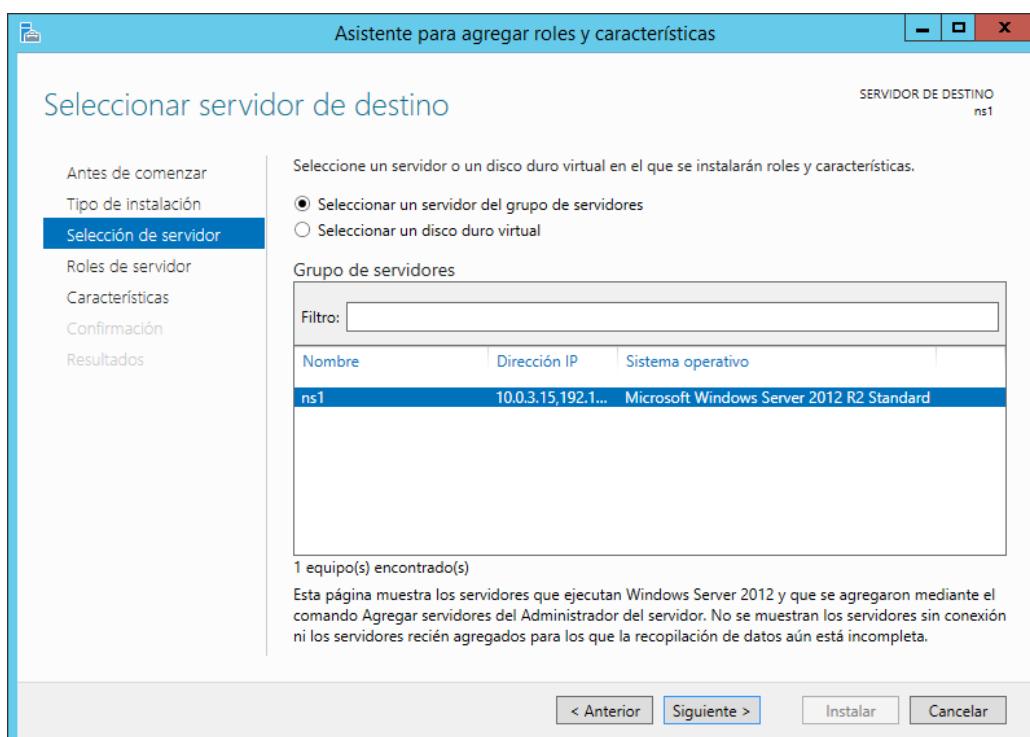
## 4. 3º Parte DNS

### 4.1. Configuración e proba dun servidor DNS primario nun servidor Windows Server 2012

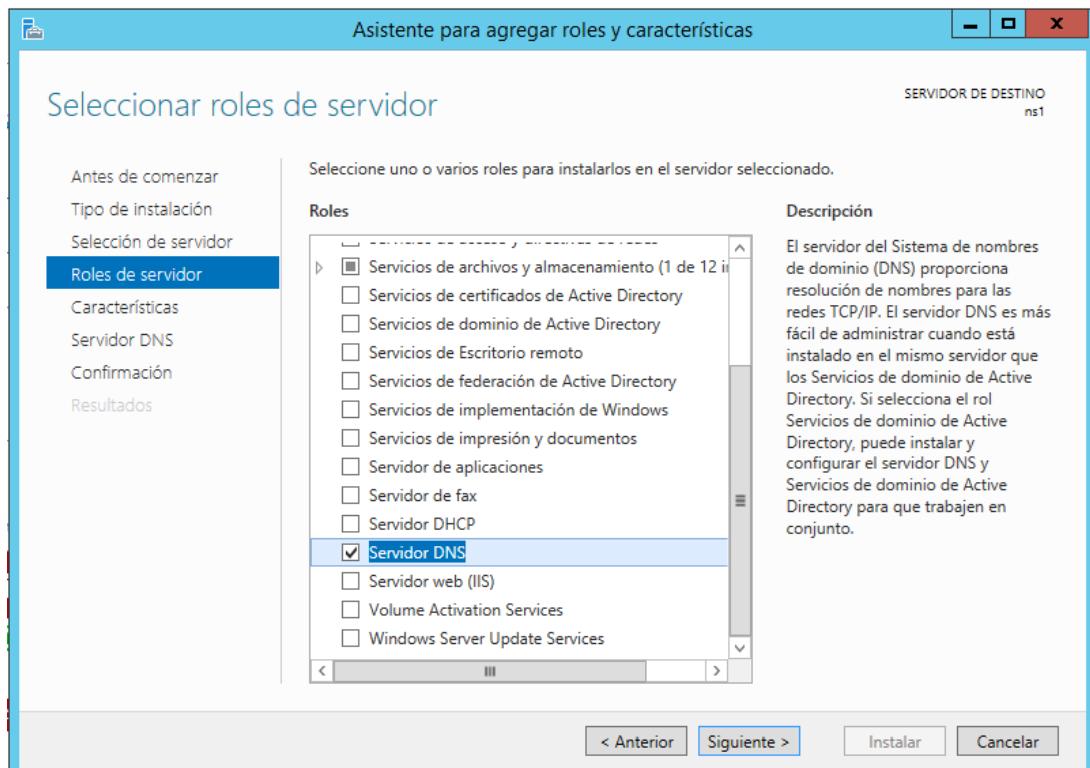
Esta tarefa realizare a partir do seguinte esquema de rede.



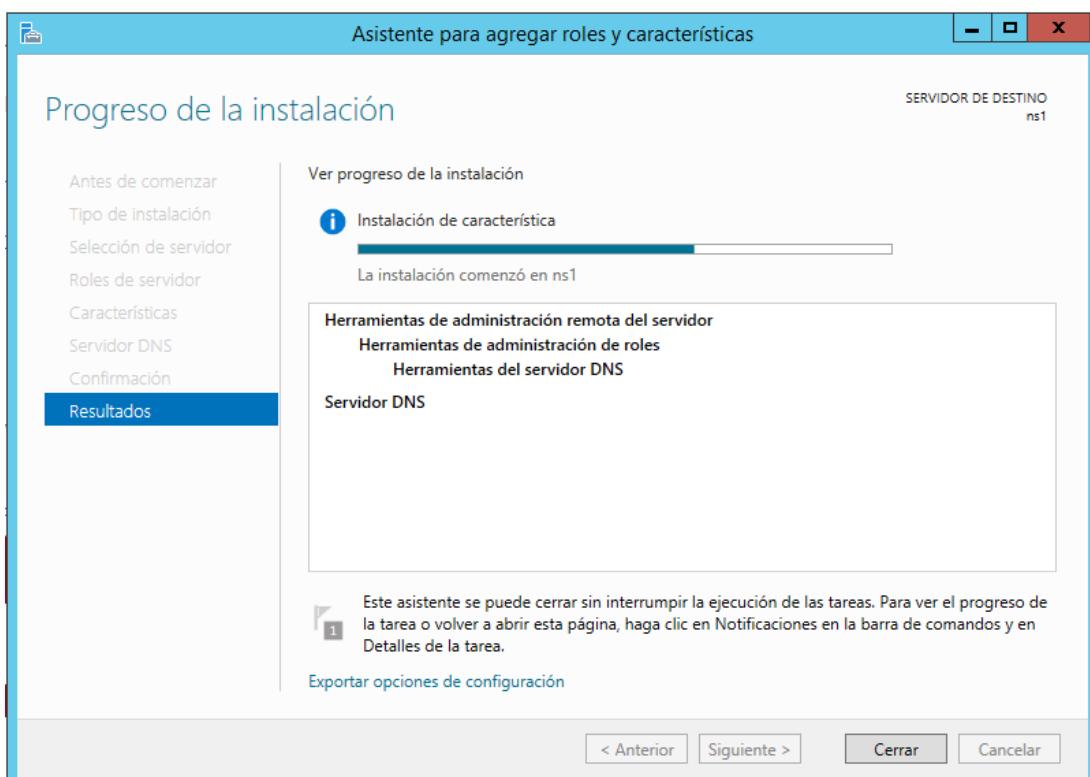
Unha vez configurados os adaptadores de rede é cambiado os nomes de todos os equipos, no equipo Windows Server 2012 agregaremos un novo rol.



O rol seleccionado será o de “servidor DNS”, este agregará automáticamente características adicionais (dependencias) para o seu correcto funcionamento.

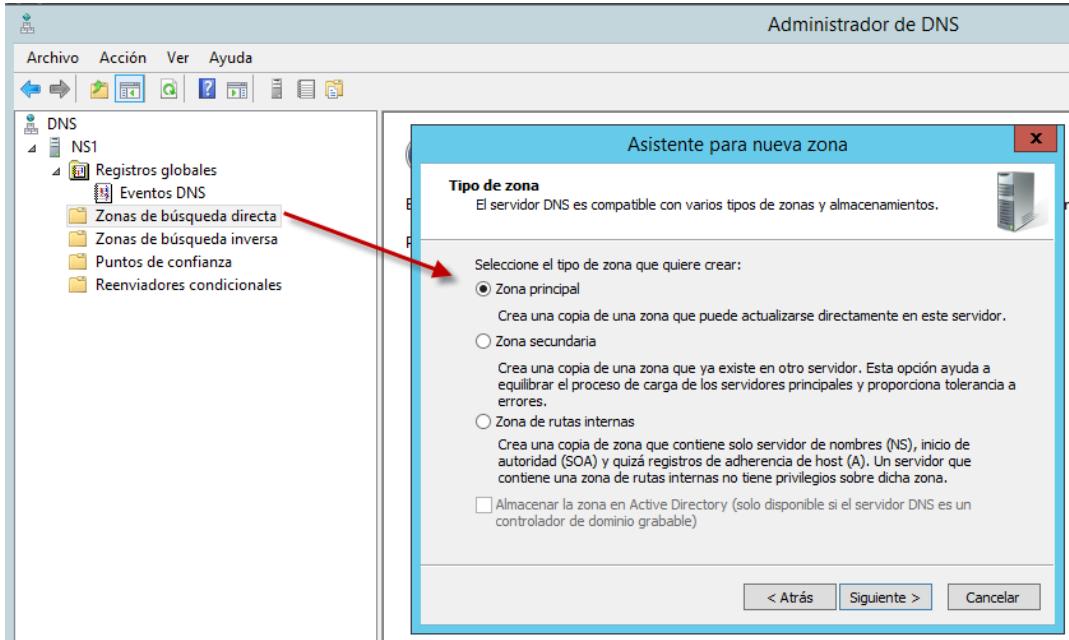


Instalamos o rol de servidor DNS.

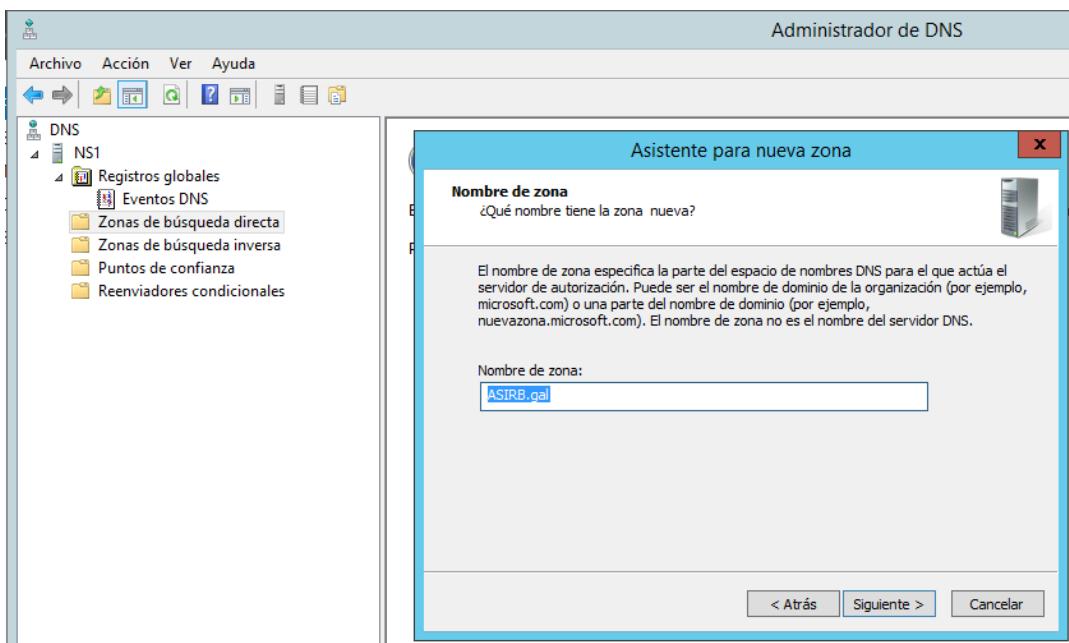


Unha vez termine a instalación abrimos a consola de administración de DNS (dnsmgmt.msc).

Nas “Zonas de búsqueda directa” crearemos unha nova “zona principal” para o servidor ns1.

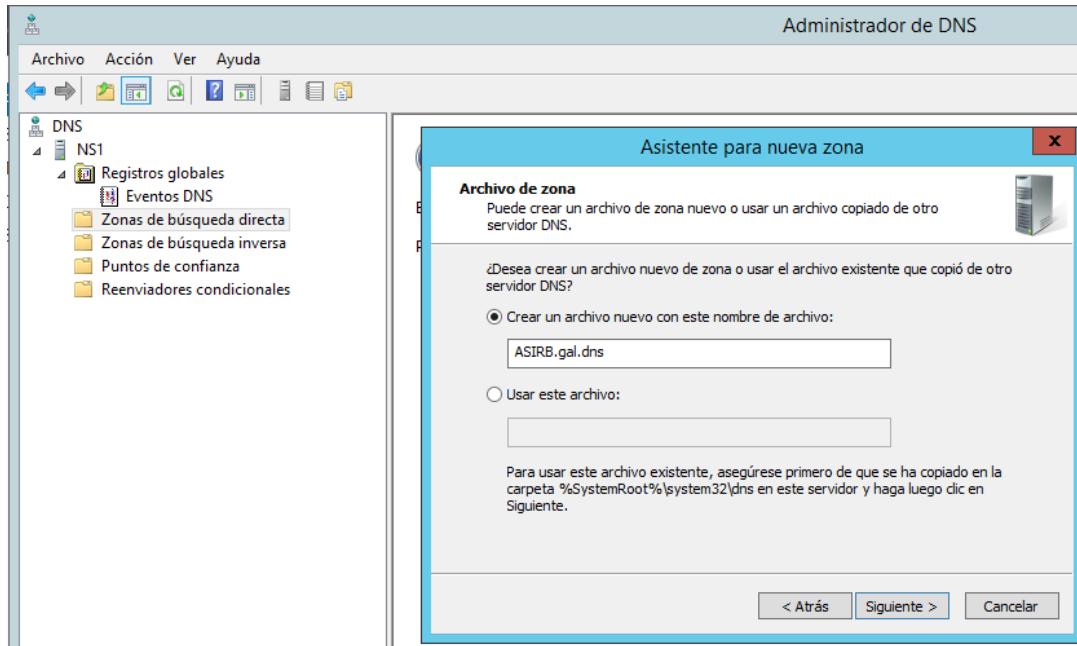


Establecemos un nome de zona “ASIRB.GAL”.

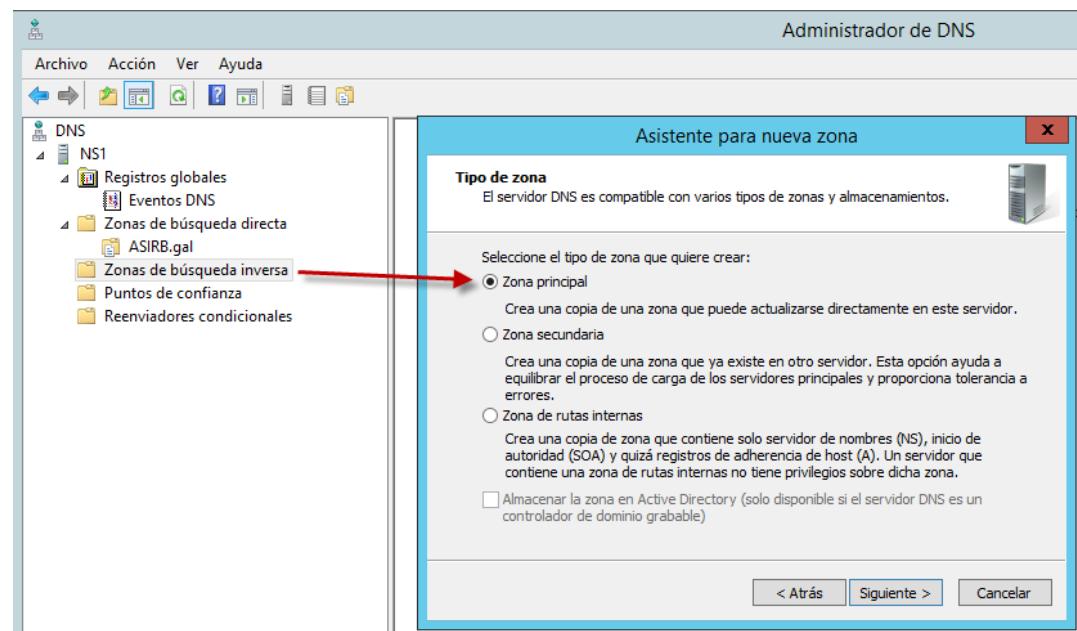


O ser unha zona nova e non ter a intención de querer cargar unha zona xa existente ou configurada previamente, este arquivo xenerarase no momento co nome por defecto “ASIRB.gal.dns” ubicado en “%systemroot%\system32\dns”. Pasará o mesmo cando se xenera a zona de búsqueda inversa, como veremos máis adiante.

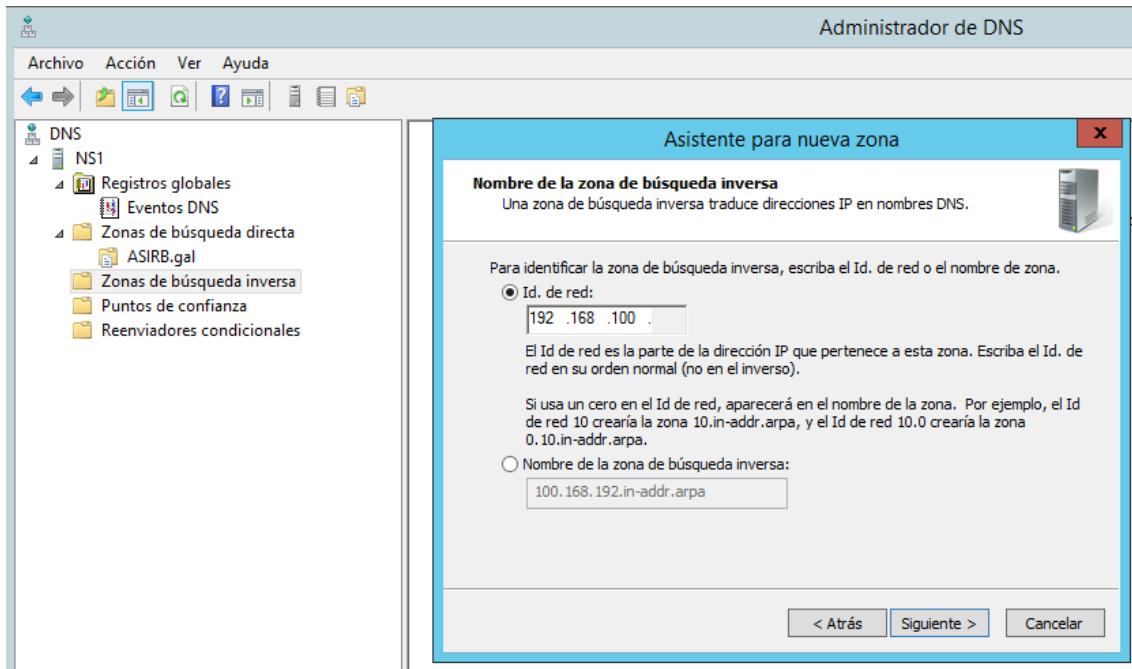
**NOTA:** Na segunda parte desta tarefa mostrarse en detalle estos ficheiros (pax.18).



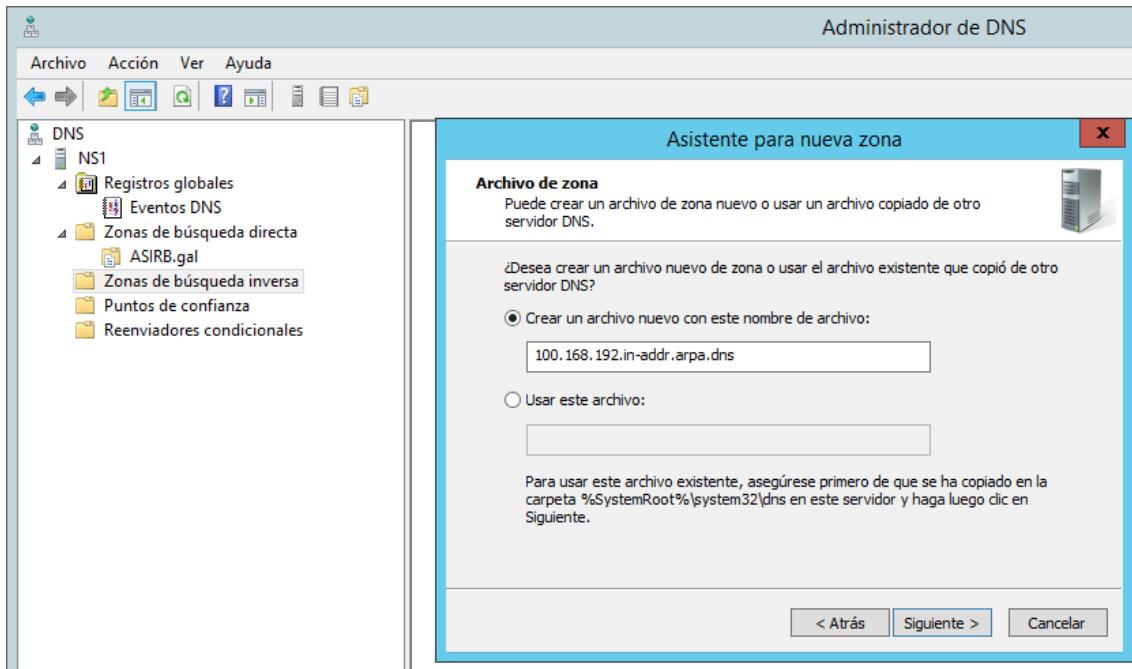
Creamos unha nova zona nas “Zonas de búsqueda inversa” o tipo de zona será principal para o servidor ns1.



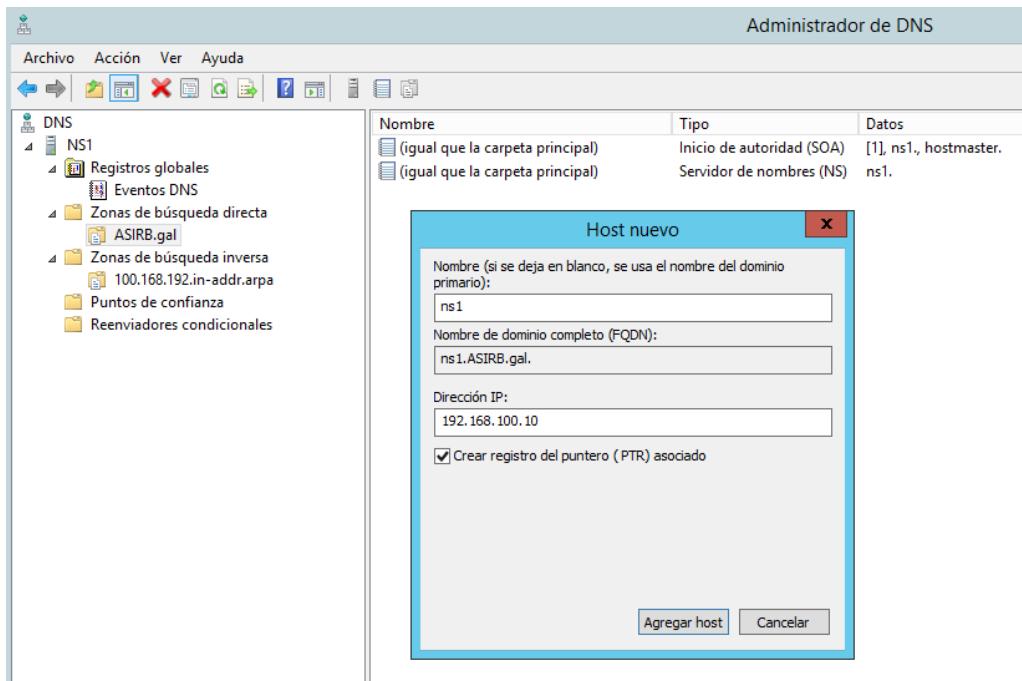
Neste caso en vez o nome de zona teremos que indentificar o Id. de rede o cal por defecto creará a zona inversa: "100.168.192.in-addr.arpa".



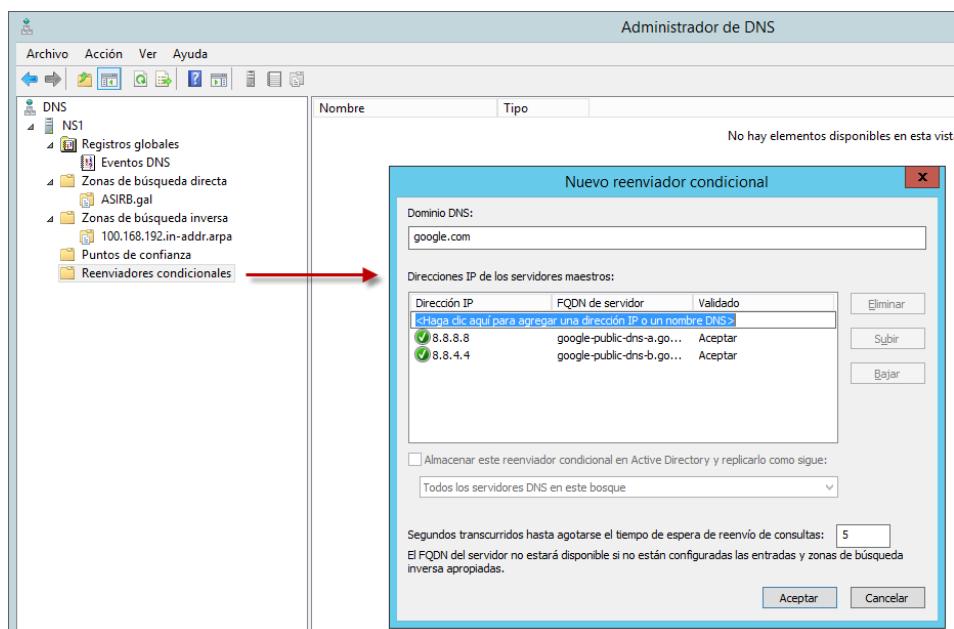
Crearase o arquivo de zona DNS, por defecto co mesmo nome mantendo así orden e coherencia. Este arquivo comentarasé más adiente.



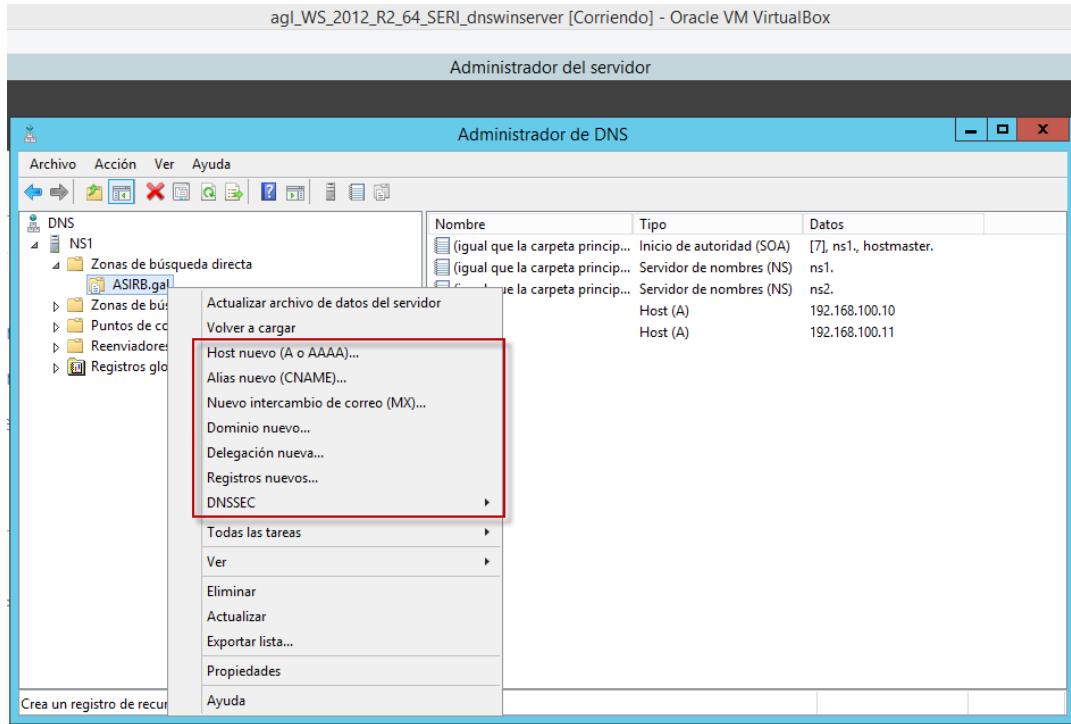
Unha vez creadas as zonas DNS directa e inversa, creamos un novo rexistro de recurso tipo A (host) para o servidor primario ns1, establecendo a súa dirección IP e marcando o checkbox para que se cree automáticamente un RR PTR asociado. O cal crearase na zona de búsqueda inversa.



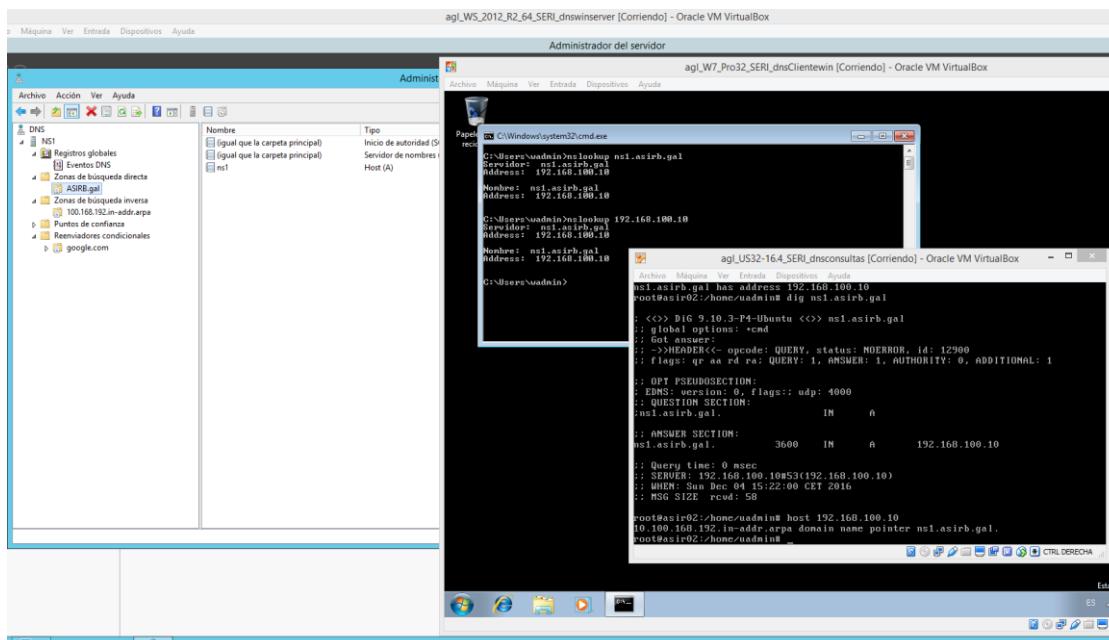
Por último podemos engadir un par de servidores caché para consultas externas do dominio asirb.gal. De modo que si algún equipo da rede interna tenta resolver un nome de dominio externo o servidor DNS (ns1) reenviará as peticións a estes reenviadores os cales farán o proceso habitual para a resolución do dominio inicialmente solicitado. Neste caso engadimos na zona de “Reenviadores condicionales” os servidores caché de Google (8.8.8.8, 8.8.4.4).



Dentro das zonas DNS creadas podemos crear máis tipos de recursos de rexistro (RR). A parte dos host (A ou AAAA), CNAME, MX, outros tipos de RR como poden ser: TXT, SRV, etc. No apartado DNSSEC, temos a posibilidade xenerar unha firma, tipo de RR RRSIG. No e obxectivo desta práctica crear este tipo de rexistros, pero suelen ser moi comúns e normalmente de fácil creación.

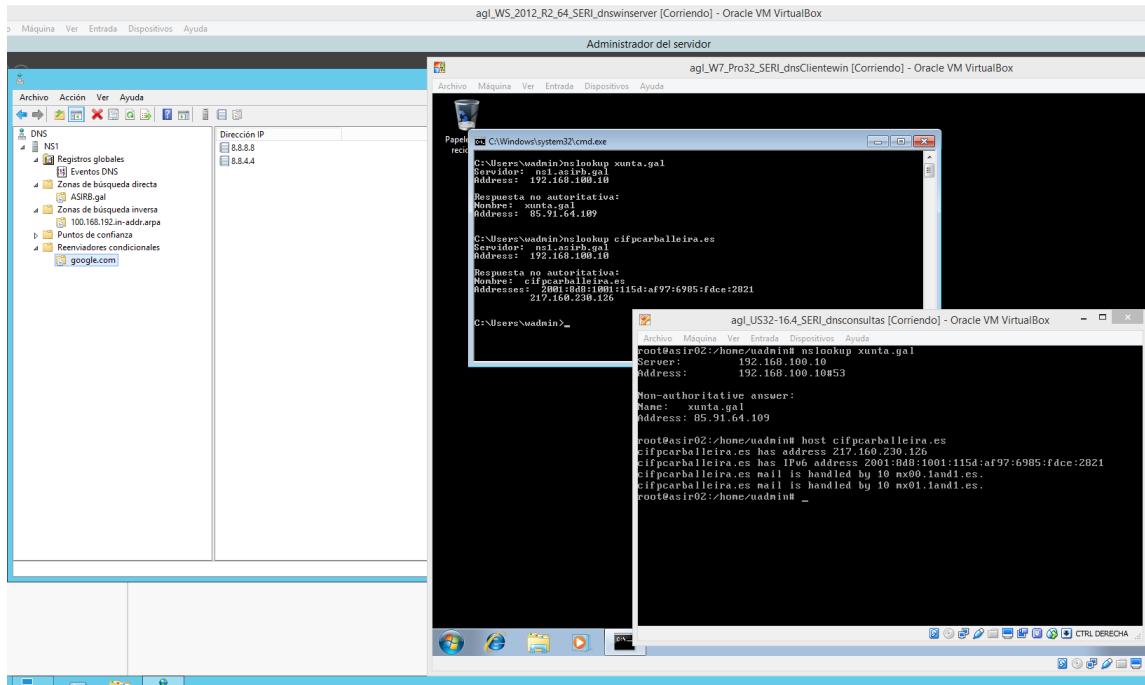


Finalmente comprobamos con dous equipos clientes, tanto un Ubuntu como un Windows que estes poden resolver consultas directas e inversas dirixidas dentro da misma rede o propio servidor DNS.



Probamos tamén a función dos reenviadores configurados nas resolucións de nomes a dominios externos.

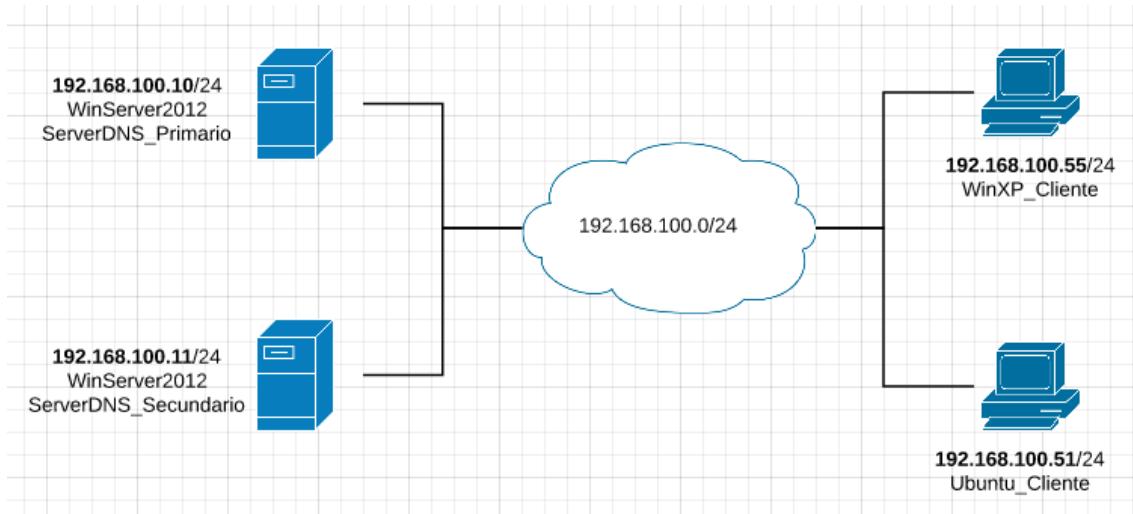
Vemos que funcionan correctamente, e que o servidor DNS (ns1) reenviará as peticións a estos servidores caché, unha vez o servidor DNS (ns1) obteña a resolución de nome este enviaralle a resposta de consulta os clientes.



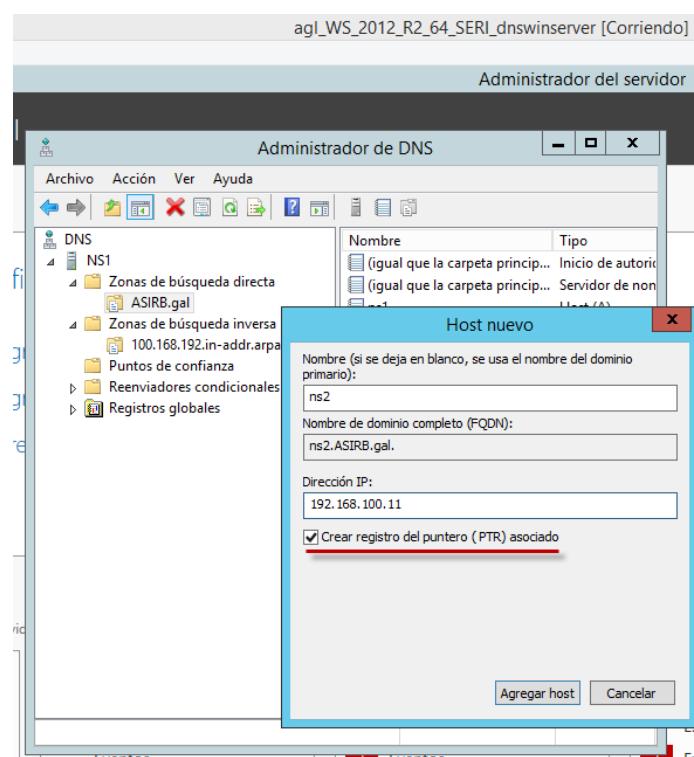
## 4.2. Configuración e proba dun servidor DNS secundario nun servidor Windows Server 2012. DNS Failover.

Continuando o apartado anterior complementaremos esta tarefa engadindo e configurando un servidor DNS escravo ou secundario, para garantir redundancia e disponibilidade, esto coñécese como un servidor DNS Failover.

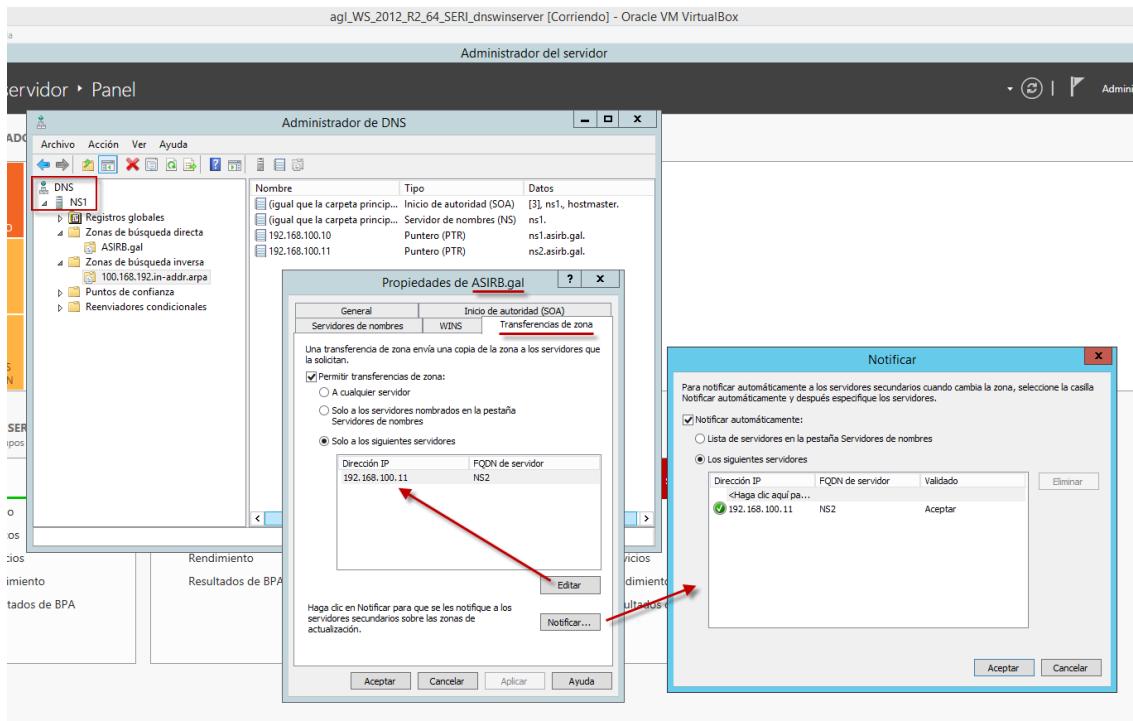
O esquema de rede utilizado para este apartado sería o seguinte:



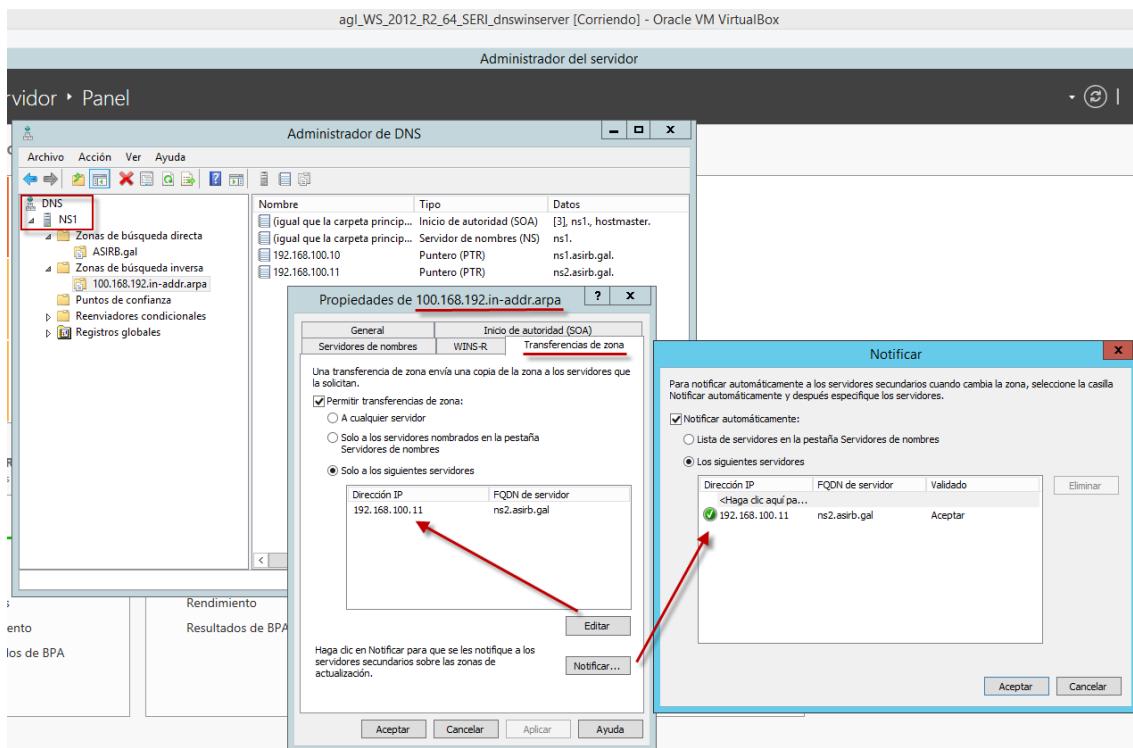
Primeiramente tendo configurado as zonas DNS de búsqueda directa e inversa no servidor primario, neste engadiremos un novo RR tipo A (host) establecendo como nome ns2 e a dirección IP asociado a ese equipo. Marcaremos o checkbox para que automáticamente se nos cree un RR PTR deste host para a zona de búsquedas inversa.



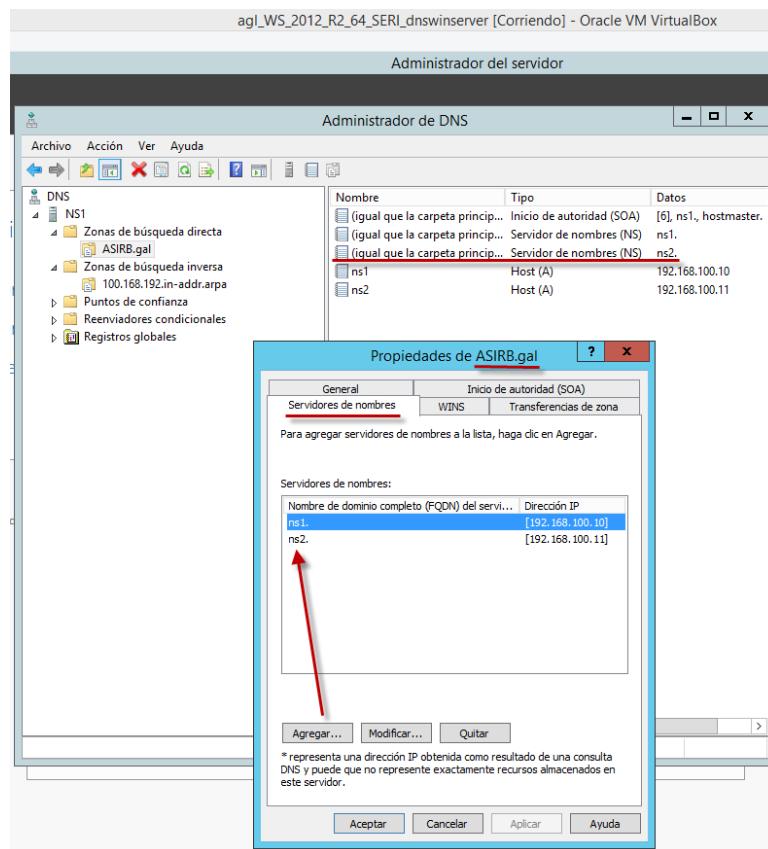
Nas propiedades da zona de búsqueda directa, neste caso ASIRB.gal, iremos o apartado de “Transferencia de zona” e indicarémoslle que transfira a configuración desta zona DNS os servidores indicados, que neste caso será a dirección IP do servidor ns2 (que será o servidor secundario).



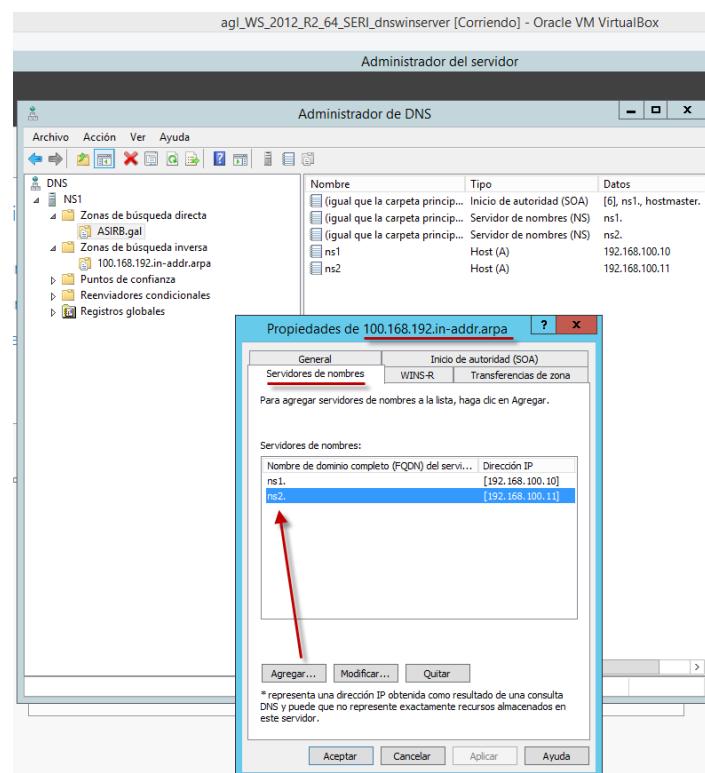
Faremos o mesmo para o apartado da zona DNS de búsqueda inversa.



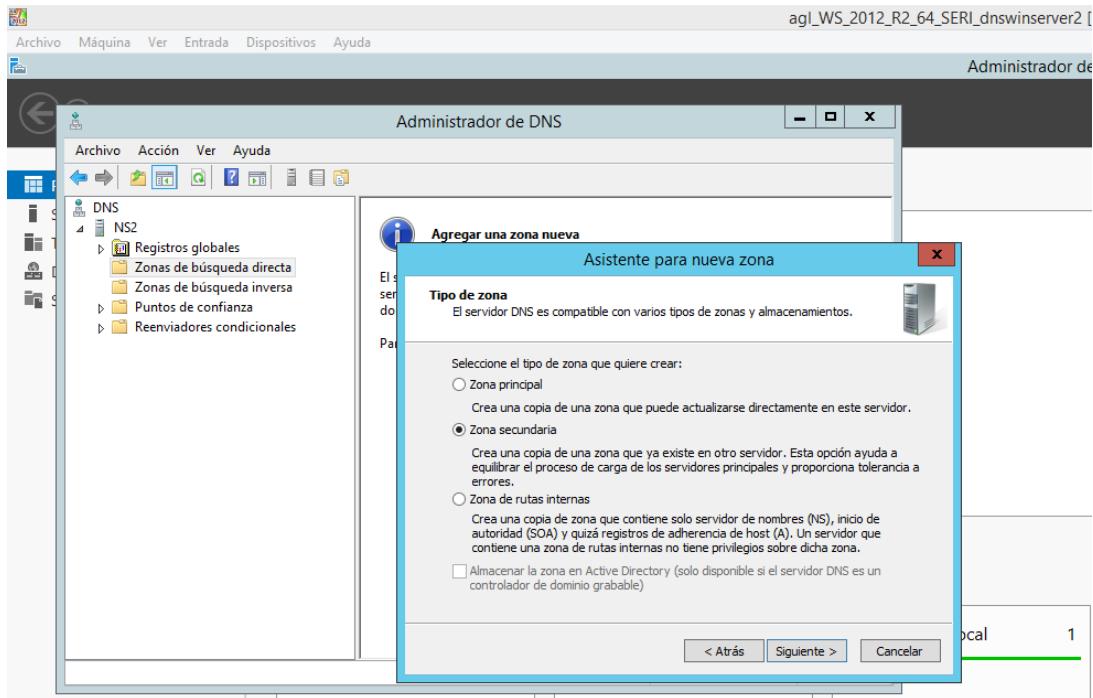
Segundo nas propiedades de zona agregaremos o servidor secundario tamén como servidor de nomes ns2. coa dirección IP correspondente.



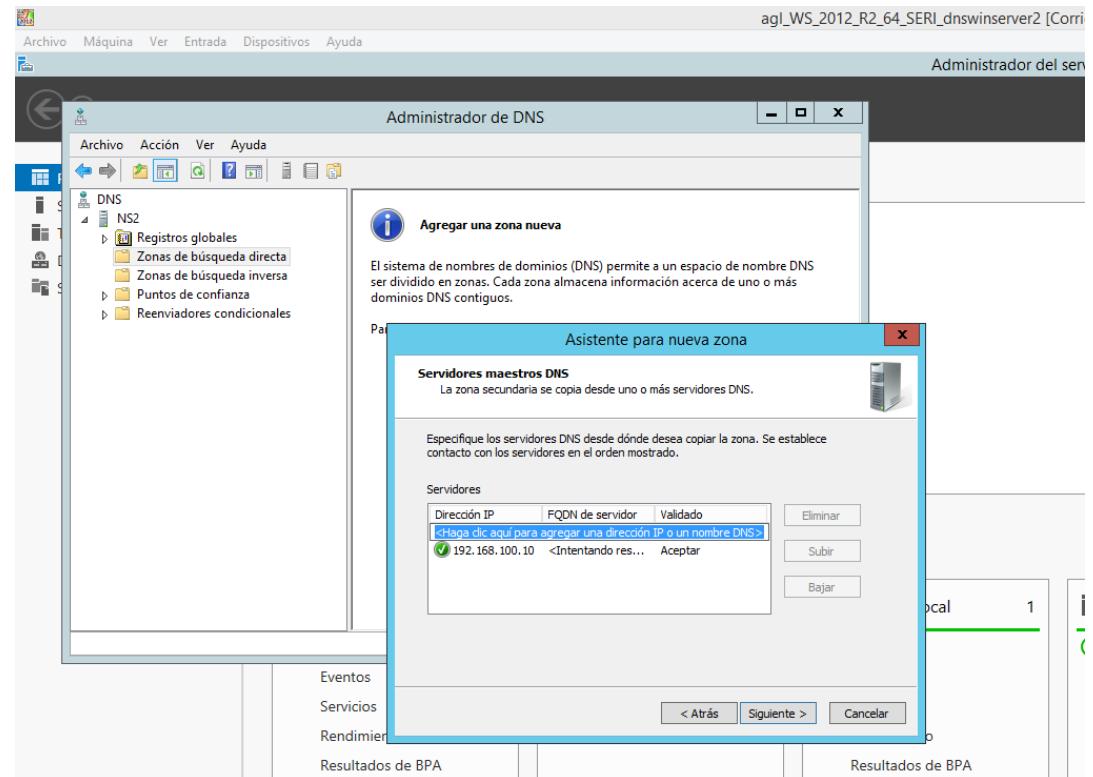
Faremos o mesmo para a zona de búsqueda inversa.



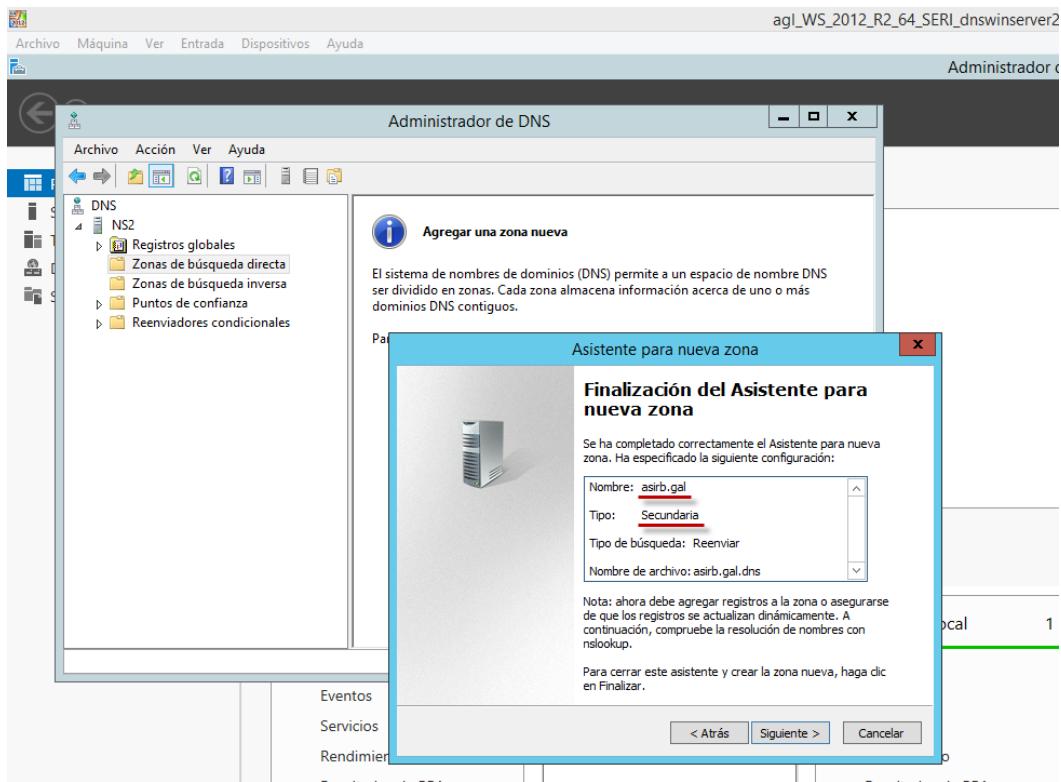
Agora no servidor secundario, xa configurado dentro da rede e instalado o servidor DNS. Na zona DNS de búsqueda directa agregaremos unha nova zona pero esta vez será unha zona secundaria a cal creará unha copia da zona DNS ca mesma configuración ca do servidor primario.



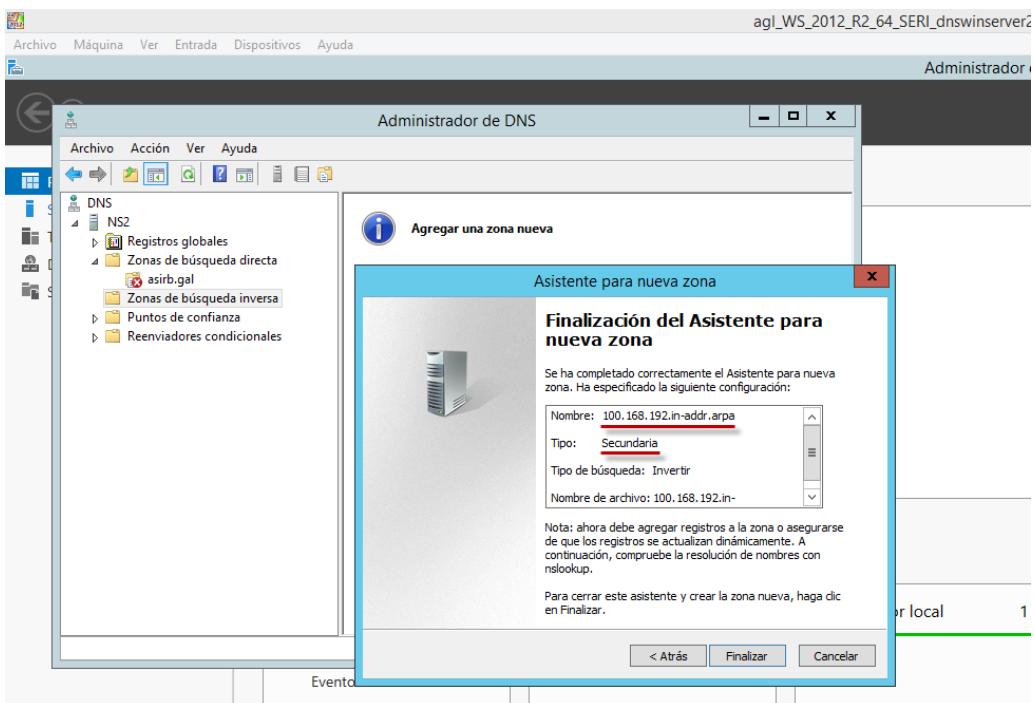
No mesmo asistente agregaremos a dirección IP do servidor primario o cal queremos transferir a zona DNS de búsqueda directa.



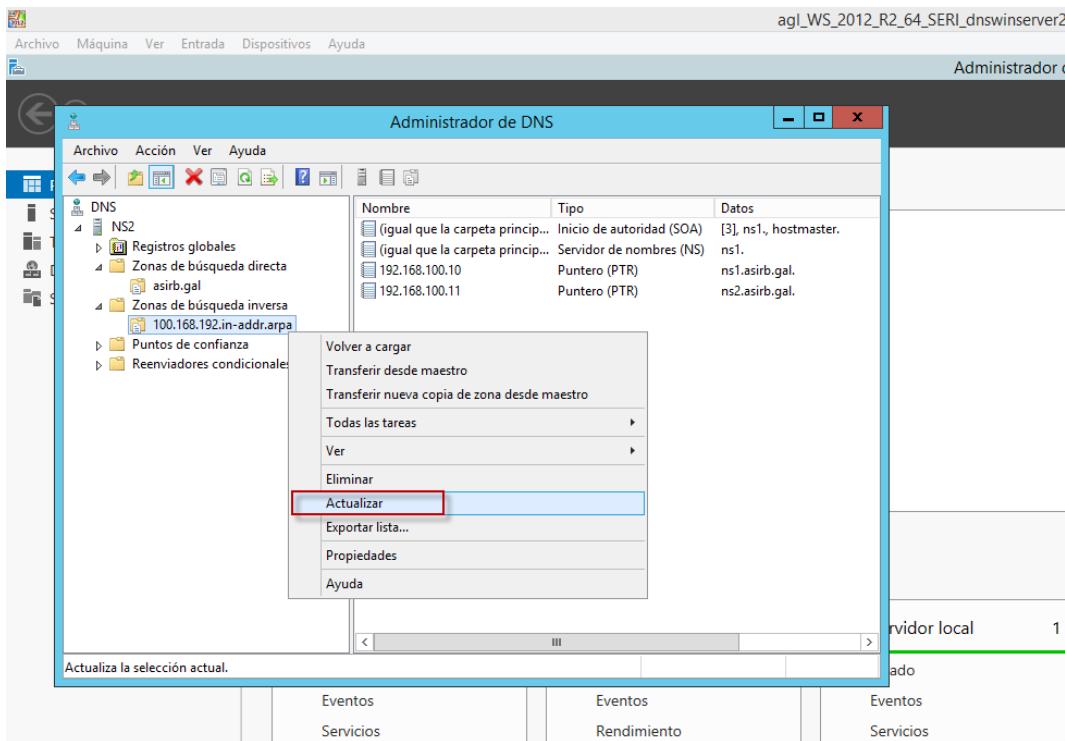
Vemos que o nome da zona será o mesmo (este nome foi indicado previamente no mesmo asistente para a creación da zona DNS), e será un tipo de zona secundaria.



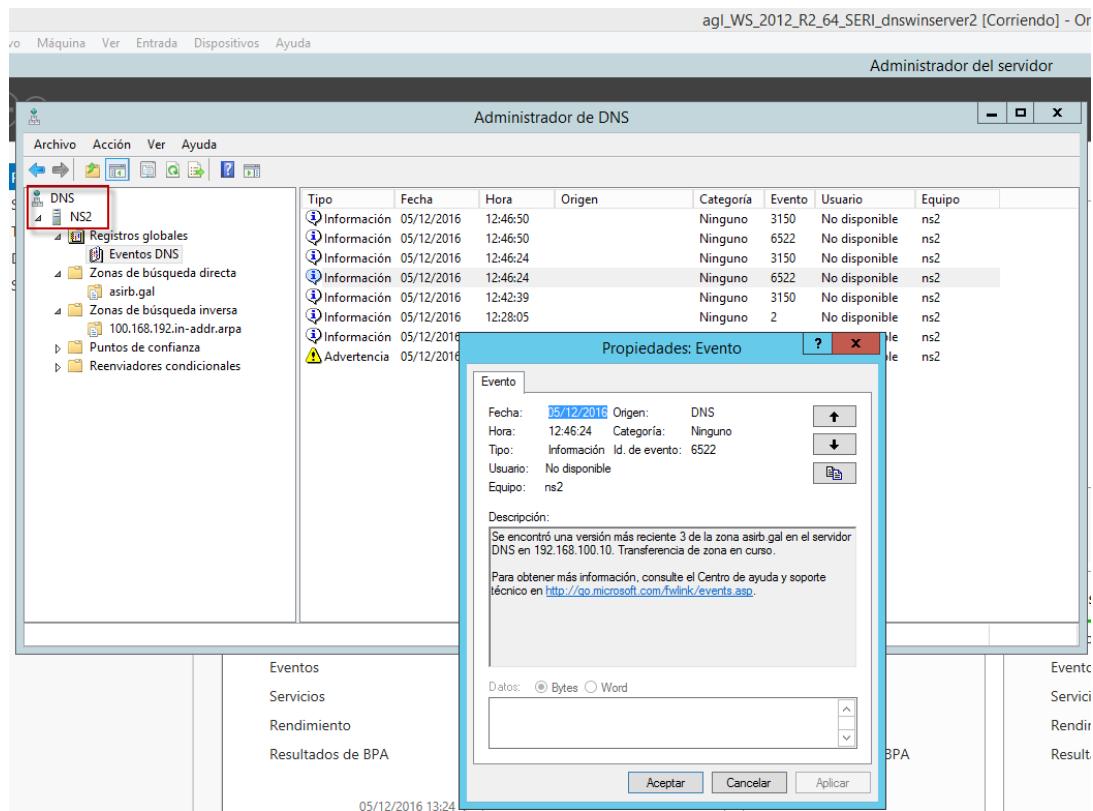
Faremos o mesmo proceso para a zona DNS de búsqueda inversa.



Actualizamos cada una das zonas DNS creadas no servidor secundario, esto sumará un incremento o número de serie dos ficheiros de configuración de cada zona.



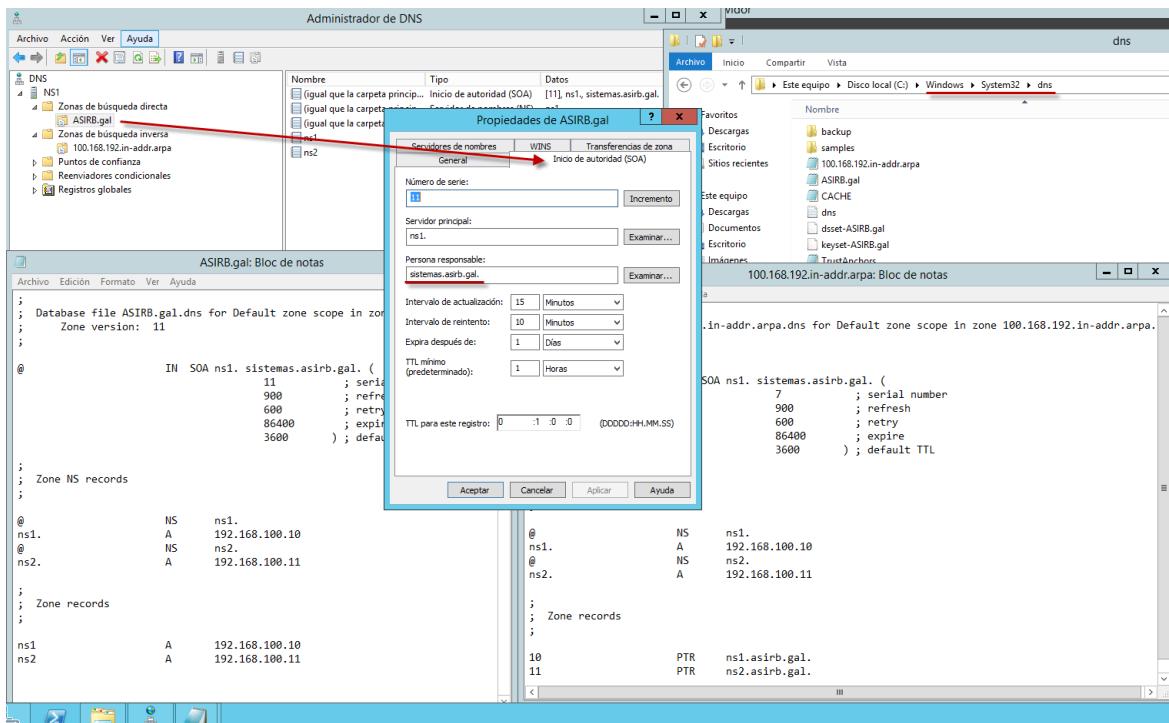
No visor de eventos DNS, pódese observar como xa se creou un rexistro da transferencia de zona do servidor primario o secundario.



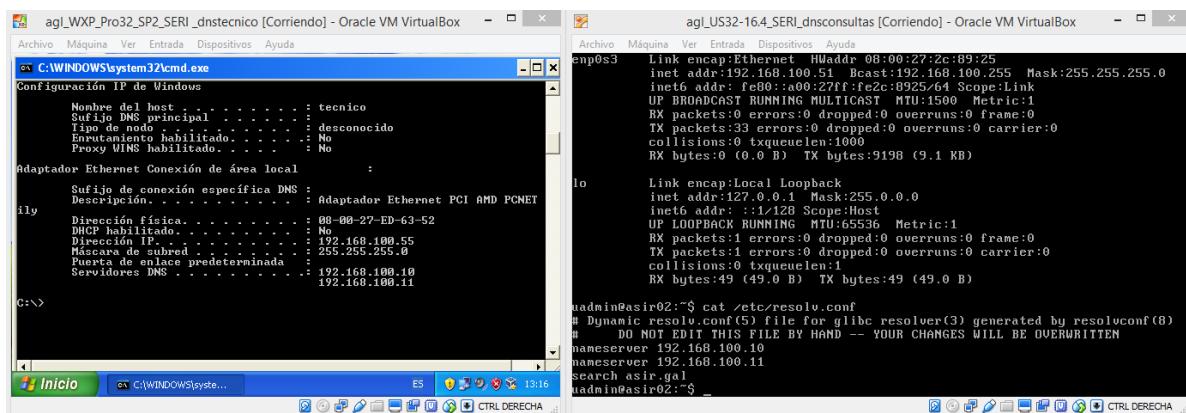
Como xa se comentara neste apartado móstranse a configuración dos ficheiros de zona DNS seguindo a sintaxis normativa do “RFC 1035”. Ficheiros almacenados e creados de forma automática por cada zona DNS no path “%systemroot%\Windows\System32\dns”.

Revisando a zona de inicio de autoridade (SOA) vemos o número de incrementos que foi modificado o ficheiro, conocido como “Número de serie” da zona DNS en cuestión, e número polo cal o servidor secundario pode comprobar si existe algún cambio e de ser así transferir este novo ficheiro do servidor primario o servidor secundario.

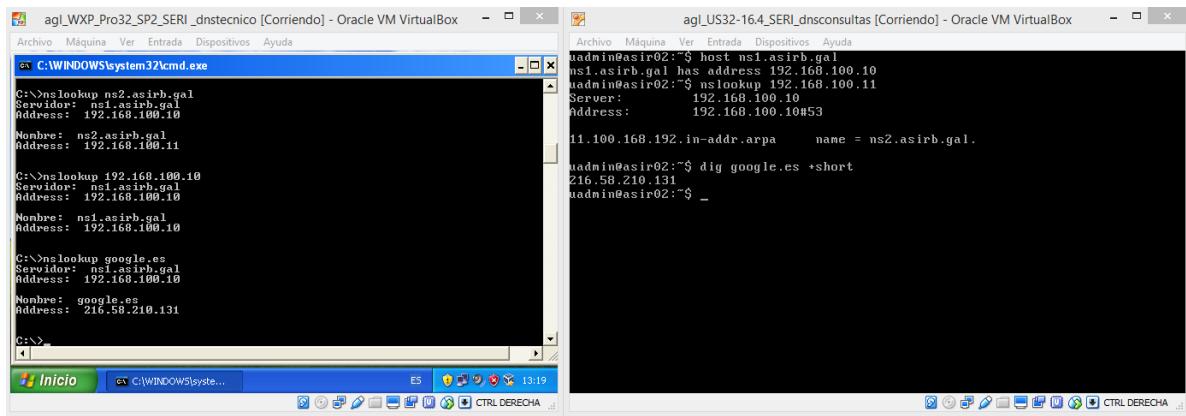
Podemos ver tamen o servidor principal (ns1), e a persoa responsable, por defecto marcada como “hostmaster” pero que a moficiaremos por “sistemas.asirb.gal” que sería traducido polo sistema DNS a: [sistemas@asirb.gal](mailto:sistemas@asirb.gal). Faremos o mesmo para a zona inversa.



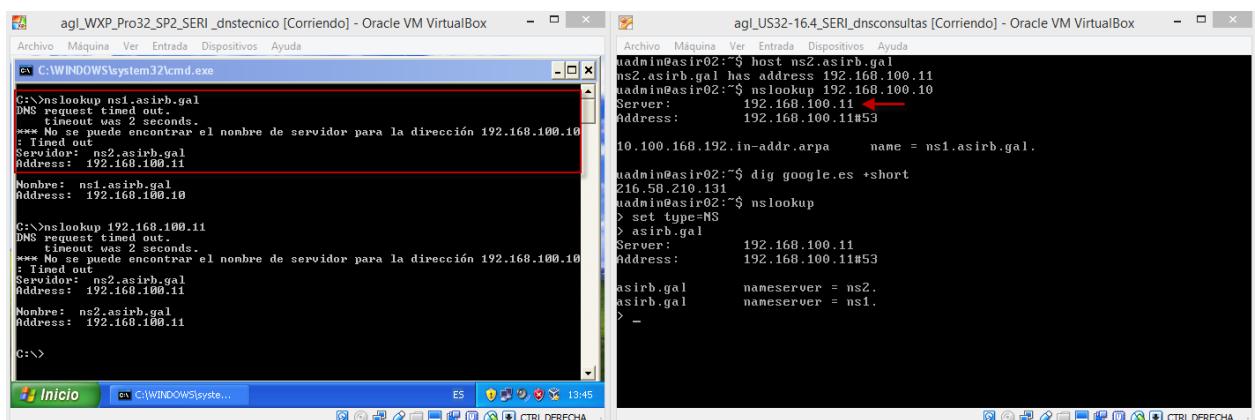
Para comprobar o funcionamiento deste servidor DNS Failover, usaremos unha máquina en Windows XP e outra en Ubuntu Server. Móstrase a configuración de rede.



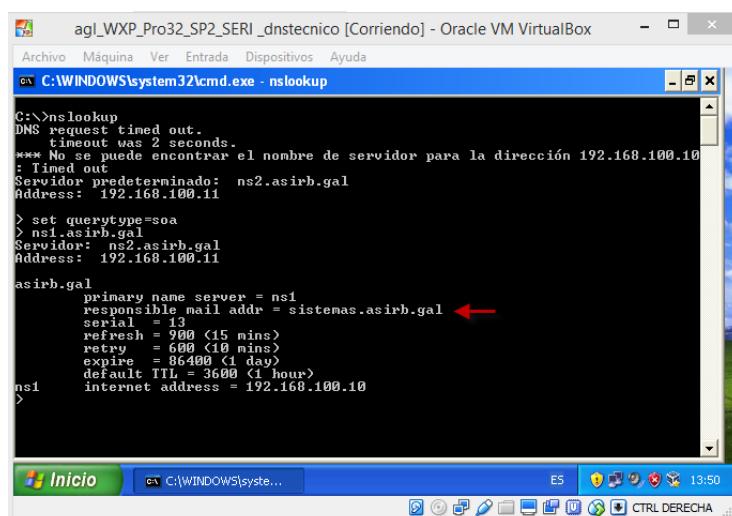
Facendo unha consulta directa e inversa ao propio servidor, vemos como nos contesta o servidor primario ns1.



Parando o servidor do servidor DNS primario ns1 ou simplemente apagando dito servidor, simulando unha caída do sistema primario. Agora debería contestar o servidor secundario ns2. O cal como se poden ver nas capturas de pantalla funciona correctamente, e no caso de Windows XP avísanos de que o servidor ns1 está caído e que agora o sistema traballará co DNS alternativo configurado que será o ns2.

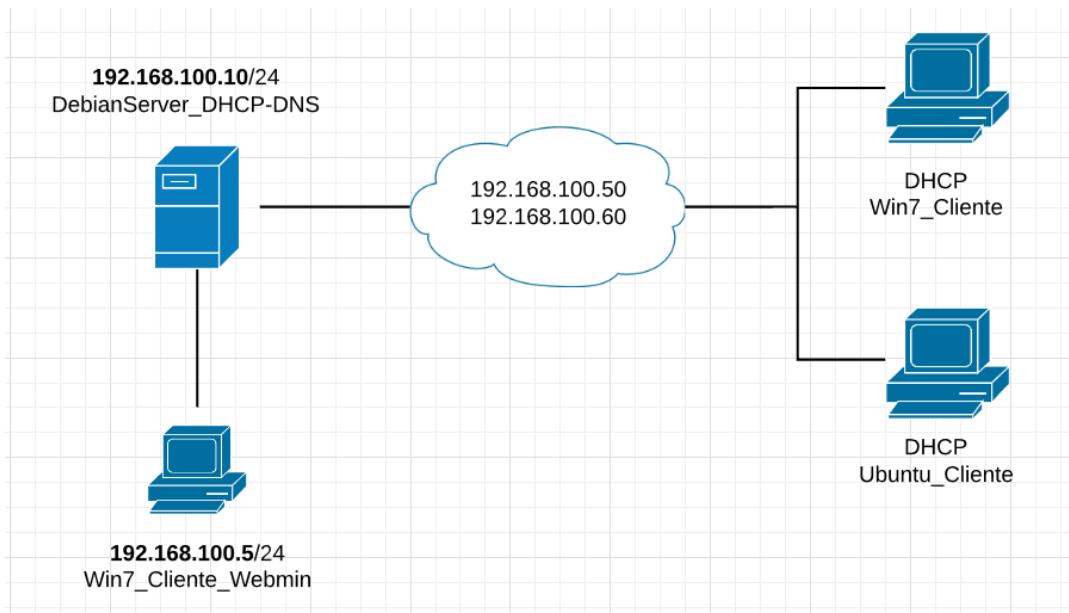


Por último podemos facer unha consulta SOA para ver a dirección email do responsable "sistemas.asirb.gal", que previaneté habíamos configurado no inicio de autoridade das zonas DNS.



#### 4.3. Configuración e proba dun servidor DNS e DHCP nun Debian (modo texto) a través de Webmin

Na seguinte tarefa montarase un servidor DNS en Webmin instalado nun sistema Debian, os clientes serán un Windows 7 e un Ubuntu server os cales obterán a configuración de rede TCP/IP a través dun servidor DHCP montado e xestionado tamén a través de Webmin. Seguiremos o seguinte esquema rede:



Primeiro instalamos Webmin, esto podémolo facer de diferentes formas, neste caso obtouse por engadir as direccións dos repositorios oficiais no arquivo local de listas de repositorios do sistema Debian.

```
# deb cdrom:[Debian GNU/Linux 8.2.0 _Jessie_ - Official i386 DVD Binary-1 20150901] jessie main  
#deb cdrom:[Debian GNU/Linux 8.2.0 _Jessie_ - Official i386 DVD Binary-1 20150901] jessie-updates main contrib  
  
deb http://ftp.es.debian.org/debian/ jessie main  
deb-src http://ftp.es.debian.org/debian/ jessie main  
  
deb http://security.debian.org/ jessie/updates main contrib  
deb-src http://security.debian.org/ jessie/updates main contrib  
  
# jessie-updates, previously known as 'volatile'  
deb http://ftp.es.debian.org/debian/ jessie-updates main contrib  
deb-src http://ftp.es.debian.org/debian/ jessie-updates main contrib  
  
deb http://download.webmin.com/download/repository sarge contrib  
deb http://webmin.mirror.somersettechsolutions.co.uk/repository sarge contrib
```

Descargamos e engadimos a chave pública “jcameron-key.asc” o sistema.

```
root@debian:~# wget http://www.webmin.com/jcameron-key.asc
--2016-12-04 16:47:11-- http://www.webmin.com/jcameron-key.asc
Resolvendo www.webmin.com (www.webmin.com)... 216.34.181.97
Conectando con www.webmin.com (www.webmin.com) 216.34.181.97:80... conectado.
Petición HTTP enviada, aguardando unha resposta... 200 OK
Lonxitude: 1320 (1,3K) [text/plain]
Gardando en: «jcameron-key.asc»

jcameron-key.asc    100%[=====] 1,29K --.-KB/s en 0s

2016-12-04 16:47:12 (103 MB/s) - gardouse «jcameron-key.asc» [1320/1320]

root@debian:~# apt-key add jcameron-key.asc
OK
```

Actualizamos os repositorios: “`sudo apt-get update`”.

Instalamos Webmin: “`sudo apt-get install webmin`”.

Unha vez instalado Webmin no sistema Debian, accedemos a súa interfaz web a través doutro equipo un Windows 7 con browser Mozilla Firefox e a través da dirección: “[https://IP\\_Servidor\\_Debian:10000](https://IP_Servidor_Debian:10000)”.

Instalamos o servidor DHCP (isc-dhcp-server), accedemos o panel de configuración e creamos unha novo ámbito, o scope de direccións para este caso será de 10 direccións libres para asignación os hosts conectados que soliciten unha configuración IP.

Nas opcións de cliente dentro da subrede creada, estableceremos unha porta de enlace que será o propio servidor Debian (ainda este de momento non fará de router), e a parte interesante é que engadiremos tamén o servidor DNS, que tamén será o sistema Debian quen faga de servidor DNS. Engadimos tamén o servidor de búsquedas DNS directamente a "asirb.gal".

The screenshot shows the 'Client Options' module in Webmin, specifically for subnet 192.168.100.0. The 'DNS domains to search' field is set to 'asirb.gal'. The 'DNS servers' field is set to '192.168.100.10'. Both fields are highlighted with red boxes.

Si accedemos os clientes veremos que automáticamente configurouse unha IP e un servidor DNS no sistema Ubuntu.

```

agl_US32-16.4_SERI_dnsconsultas [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
uadmin@asir02:~$ ifconfig -a
enp0s3      Link encap:Ethernet HWaddr 08:00:27:2c:89:25
             inet addr:192.168.100.50 Bcast:192.168.100.255 Mask:255.255.255.0
             inet6 addr: fe80::a00:27ff:fe2c:8925/64 Scope:Link
               UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
               RX packets:1428 errors:0 dropped:0 overruns:0 frame:0
               TX packets:157 errors:0 dropped:0 overruns:0 carrier:0
               collisions:0 txqueuelen:1000
               RX bytes:174365 (174.3 KB) TX bytes:23573 (23.5 KB)

lo          Link encap:Local Loopback
             inet addr:127.0.0.1 Mask:255.0.0.0
             inet6 addr: ::1/128 Scope:Host
               UP LOOPBACK RUNNING MTU:65536 Metric:1
               RX packets:32 errors:0 dropped:0 overruns:0 frame:0
               TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
               collisions:0 txqueuelen:1
               RX bytes:1638 (1.6 KB) TX bytes:1638 (1.6 KB)

uadmin@asir02:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.100.10 ←
search example.org
uadmin@asir02:~$ 

```

E tamén ocorre o mesmo para o sistema Windows cliente.

Podemos ver as concesións de dirección IP no servidor Debian a través do entorno gráfico de Webmin.

Webmin 1.820 on ns1debia... +

https://192.168.100.10:10000 | C | Buscar

Login: root

Module Index

DHCP Leases

Display mode : DHCP leases | Subnets and usage

11 IP addresses available, 2 allocated (18 %)

Select all. | Invert selection.

IP Address	Ethernet	Hostname	Start Date
192.168.100.50	08:00:27:2c:89:25	asir02	2016/12/02 00:10:08
192.168.100.51	08:00:27:53:d3:20	technico	2016/12/02 00:15:10

Select all. | Invert selection.

[Delete Selected Leases](#)

[List all active and expired leases](#)

[Return to network and host list](#)

▶ Webmin  
▶ System  
▼ Servers  
Apache Webserver  
BIND DNS Server  
DHCP Server  
MySQL Database Server  
Procmail Mail Filter  
ProFTPD Server  
Read User Mail  
Samba Windows File Sharing  
SSH Server  
▶ Others

Instalamos o servidor DNS Bind en Webmin.

Unha vez instalado empezaremos a configuralo creando unha zona DNS maestra.

The screenshot shows the 'BIND DNS Server' module in Webmin. On the left, there's a sidebar with various server modules like Apache, MySQL, and DNS. The main area is titled 'Global Server Options' and contains several icons for managing DNS. Below that is the 'Existing DNS Zones' section, which lists several zones: 'Root zone', '0', '127', '255', and 'localhost'. At the top of this section, there are links for creating different types of zones: 'Create master zone...', 'Create slave zone...', 'Create stub zone...', 'Create forward zone...', 'Create delegation zone...', and 'Create zones from batch file...'. A red box highlights the 'Create master zone...' link.

Esta zona DNS maestra levará o nome habitual empregado nestas tarefas, “`asirb.gal`”. o nome do servidor maestro Debian (`ns1debian`) e o email do responsable de zona “[sistemas@asirb.gal](mailto:sistemas@asirb.gal)”, o resto de parámetros podémolos deixar como están por defecto.

The screenshot shows the 'Create Master Zone' configuration page. It has a 'New master zone options' section. Under 'Zone type', 'Forward (Names to Addresses)' is selected. The 'Domain name / Network' field is filled with 'ASIRB gal'. Under 'Master server', 'ns1debian' is listed with the checkbox 'Add NS record for master server?' checked. The 'Email address' field is set to 'sistemas@asirb.gal'. There are sections for 'Use zone template?' (set to 'No'), 'Add reverses for template addresses?' (set to 'Yes'), and various time-related settings like 'Refresh time' (10800 seconds), 'Expiry time' (604800 seconds), 'Transfer retry time' (3600 seconds), and 'Negative cache time' (38400 seconds). A 'Create' button is at the bottom.

Entrando nas opcións de configuración da zona maestra, engadiremos un novo rexistro e un servidor de nomes.

The screenshot shows the 'Edit Master Zone' interface for the 'ASIRB.gal' zone. On the left, there's a sidebar with various server modules like Apache Webserver, BIND DNS Server, and MySQL Database Server. The main area displays icons for different record types: Address (1), Name Server (1), Name Alias (0), Mail Server (0), Host Information (0), Text (0), Sender Permitted From (0), Well Known Service (0), Responsible Person (0), Reverse Address (0), Service Address (0), Public Key (0), SSL Certificate (0), IPv6 Address (0), All Record Types (2), Record Generators, Edit Records File, Edit Zone Parameters, Edit Zone Options, Find Free IPs, Lookup WHOIS Information, and Setup DNSSEC Key. The 'Address (1)' icon is highlighted with a red box.

O servidor de nomes será “ns1debian”. Co dominio “asirb.gal.”.

The screenshot shows the 'Name Server Records' interface for the 'ASIRB.gal' zone. It includes fields for 'Zone Name' (ASIRB.gal) and 'Name Server' (ns1debian). Below this, a table lists existing records: one entry for 'ns1debian' with 'Default' TTL and 'ns1debian.' as the name. A red box highlights this entry.

Name	TTL	Name Server
ns1debian	Default	ns1debian.

Engadiremos tamén un RR tipo A host. (ns1debian.asirb.gal > 192.168.100.10)

The screenshot shows the 'Address Records' interface for the 'ASIRB.gal' zone. It includes fields for 'Name' (ns1debian.asirb.gal) and 'Address' (192.168.100.10). Below this, a table lists existing records: one entry for 'ns1debian.asirb.gal' with 'Default' TTL and '192.168.100.10' as the address. A red box highlights this entry.

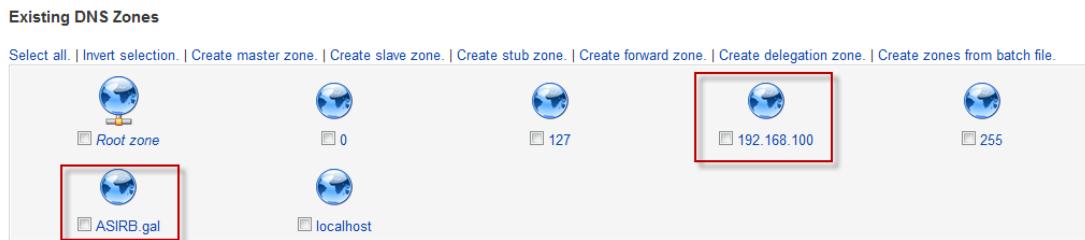
Name	TTL	Address
ns1debian.asirb.gal	Default	192.168.100.10

Agora crearemos unha nova zona DNS pero para as búsquedas inversas, para iso faremos os mesmos pasos que no caso anterior pero cambiando o dato do nome da zona por un máis coherente e ordenado. (192.168.100)

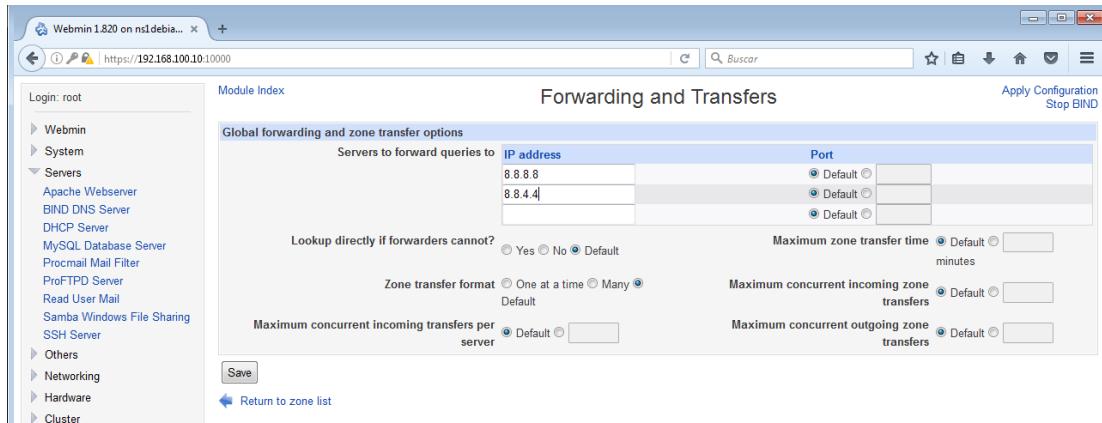
Crearemos para esta zona DNS inversa un servidor de nomes para as resolución inversas. (100.168.192.in-addr.arpa. > ns1debian)

Crearemos despois un RR para que a dirección IP (192.168.100.10) do servidor a apunte o nome "ns1debian.asirb.gal".

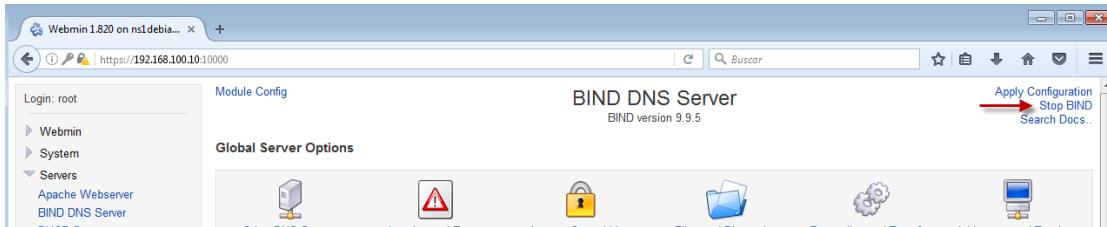
Como vemos temos as dúas zonas creadas no panel principal de configuración de Webmin do servidor DNS.



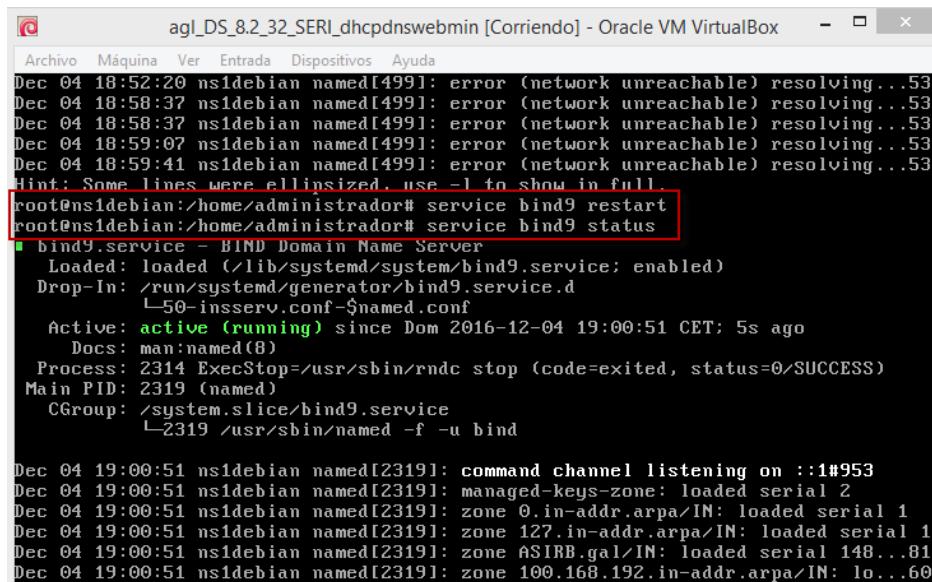
Como paso final complementario, engadiremos un par de servidores caché, servidores os cales si algún dos clientes preguntan por determinado nome ou dirección IP que o servidor non coñeña ou non teña configurado este reenviaralle a consulta a este servidores caché. Neste exemplo estableceranse os de Google (8.8.8.8 e 8.8.4.4).



Para actualizar tódolos cambios reinicizaremos o servizo dende o panel de Webmin.



Ou tamén temos a opción de irnos o servidor Debian e reinícialo dende o propio servidor por terminal (tty).



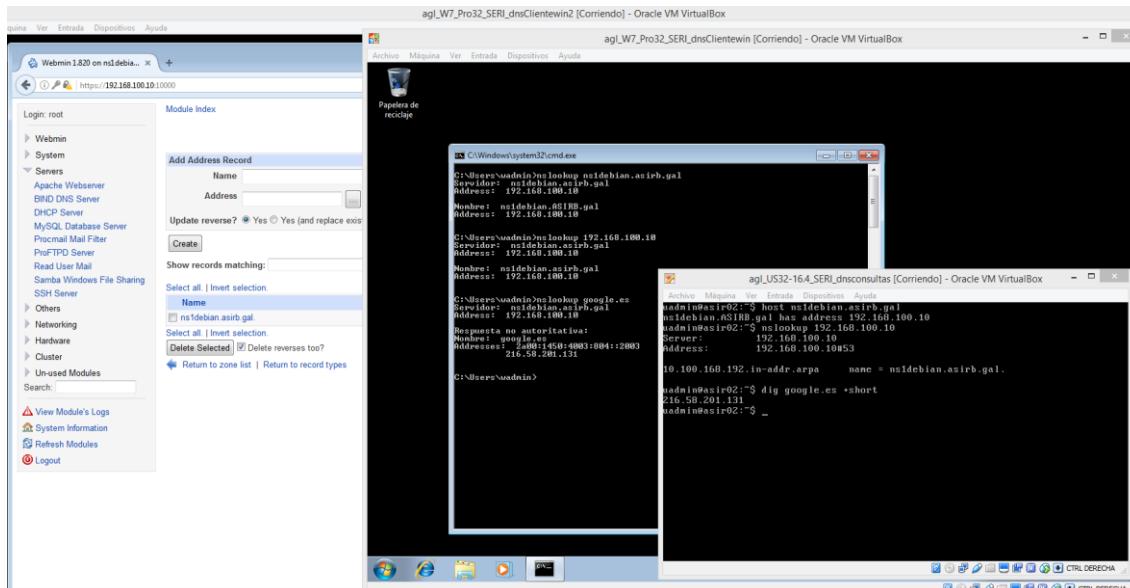
```

agl_DS_8.2_32_SERI_dhcpdnswebmin [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Dec 04 18:52:20 ns1debian named[4991]: error (network unreachable) resolving...53
Dec 04 18:58:37 ns1debian named[4991]: error (network unreachable) resolving...53
Dec 04 18:58:37 ns1debian named[4991]: error (network unreachable) resolving...53
Dec 04 18:59:07 ns1debian named[4991]: error (network unreachable) resolving...53
Dec 04 18:59:41 ns1debian named[4991]: error (network unreachable) resolving...53
Hint: Some lines were ellipsized. use -l to show in full.
root@ns1debian:/home/administrador# service bind9 restart
root@ns1debian:/home/administrador# service bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled)
   Drop-In: /run/systemd/generator/bind9.service.d
             └─50-insserv.conf-$named.conf
     Active: active (running) since Dom 2016-12-04 19:00:51 CET; 5s ago
       Docs: man:named(8)
   Process: 2314 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 2319 (named)
    CGroup: /system.slice/bind9.service
            └─2319 /usr/sbin/named -f -u bind

Dec 04 19:00:51 ns1debian named[2319]: command channel listening on ::1#953
Dec 04 19:00:51 ns1debian named[2319]: managed-keys-zone: loaded serial 2
Dec 04 19:00:51 ns1debian named[2319]: zone 0.in-addr.arpa/IN: loaded serial 1
Dec 04 19:00:51 ns1debian named[2319]: zone 127.in-addr.arpa/IN: loaded serial 1
Dec 04 19:00:51 ns1debian named[2319]: zone ASIRB.gal/IN: loaded serial 148...81
Dec 04 19:00:51 ns1debian named[2319]: zone 100.168.192.in-addr.arpa/IN: lo...60

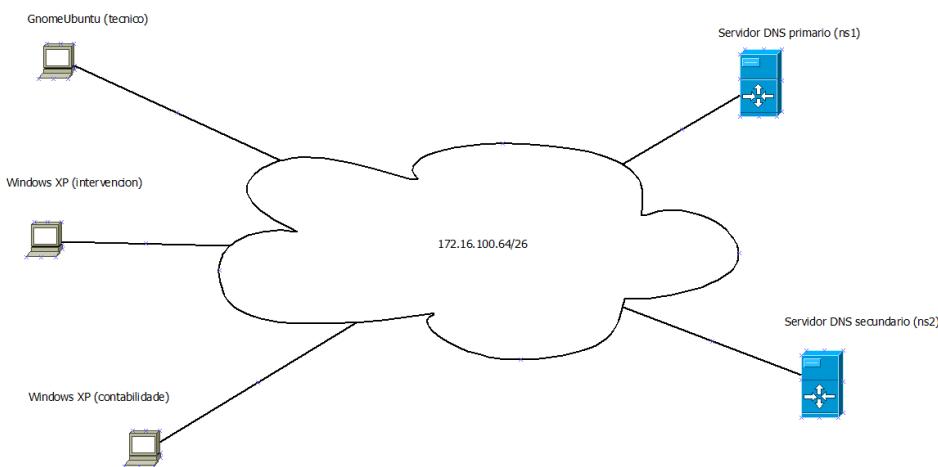
```

Probamos agora consultas os servidores DNS e consultas a un dominio externo. Vemos que tanto o cliente Windows como o cliente Ubuntu server obteñen as answers correctamente das requests enviadas o servidor DNS.



## 4.4. Configuración e proba dun servidor DNS maestro e escravo con Bind nun Ubuntu Server 16.04

Segundo o seguinte esquema de rede proposto, configurarase un servidor DNS Bind nunha contorna Ubuntu Server, con tres clientes Windows XP e outros Windows 7. Aínda que non foi solicitado na práctica estos cliente Windows 7, explicarase máis adiante da práctica por que se incluiron.



A configuración de rede e os nomes dos clientes Windows 7 e a seguinte.

Las capturas muestran la configuración IP y los servidores DNS para tres clientes Windows 7:

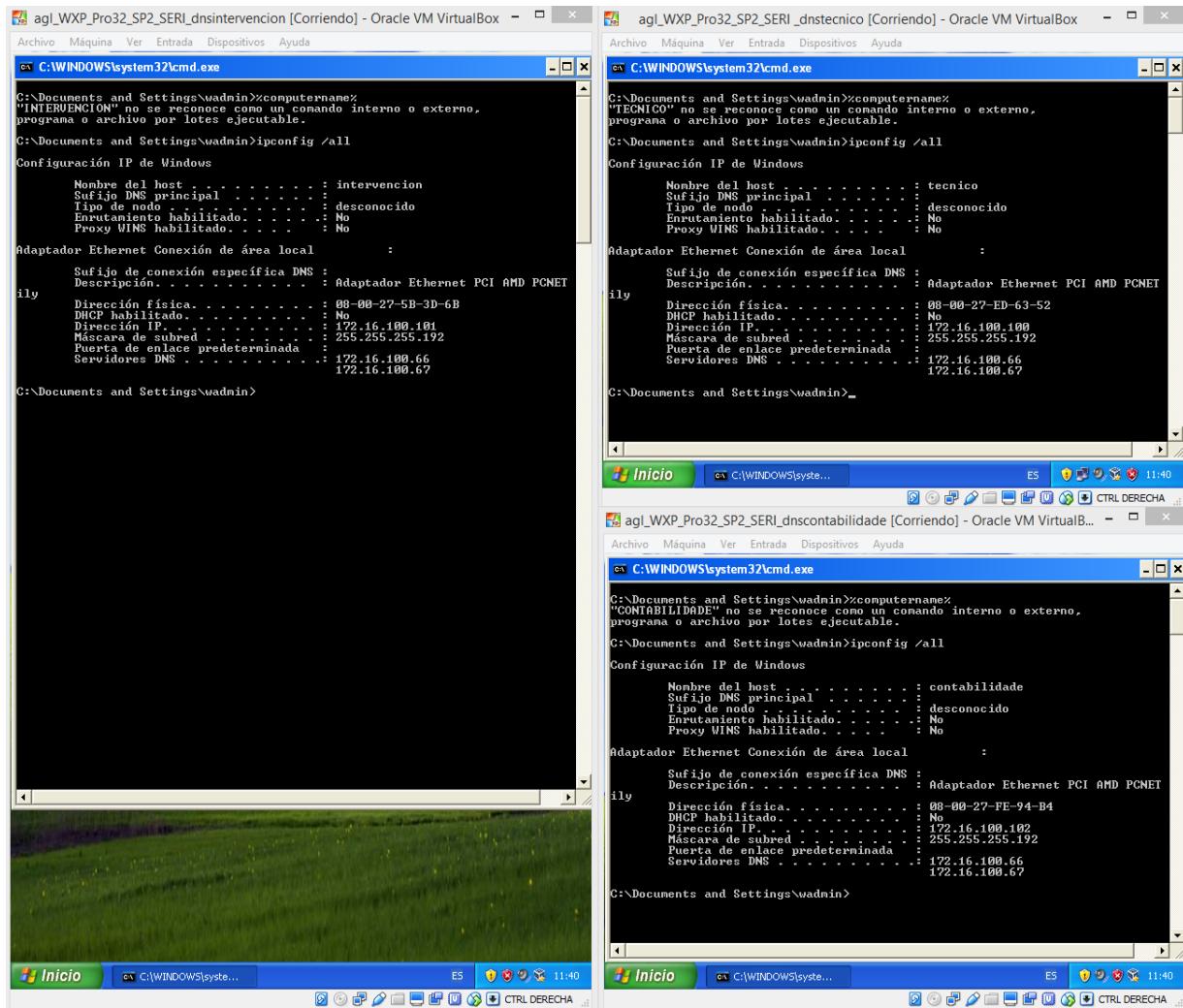
- Intervención:** Servidor DNS: 172.16.100.66 (indicado por un rojo).
- Contabilidad:** Servidor DNS: 172.16.100.66 (indicado por un rojo).
- Técnico:** Servidor DNS: 172.16.100.67 (indicado por un rojo).

```

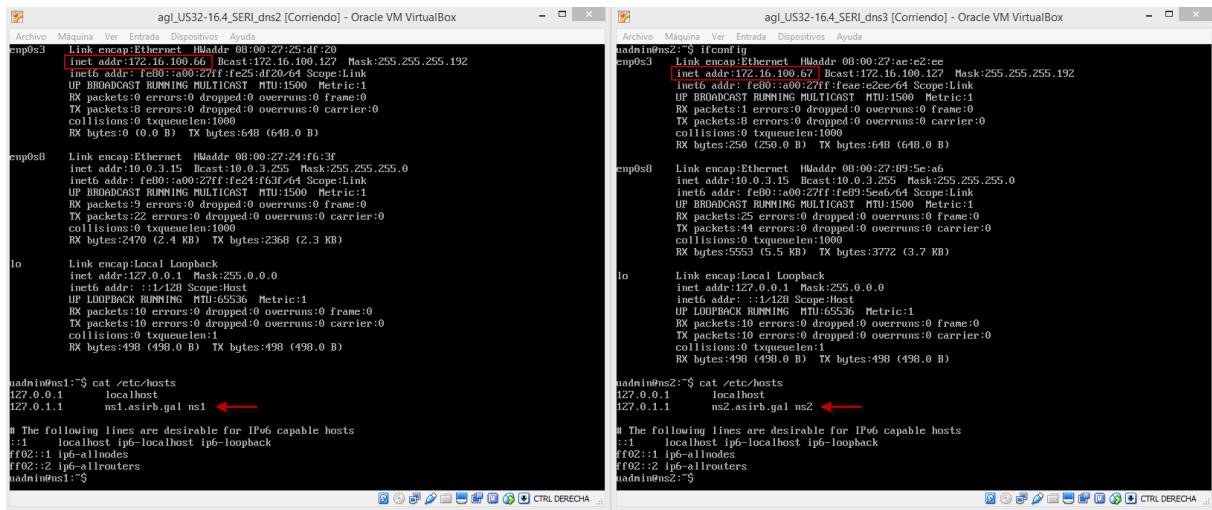
agl_W7_Pro32_SERI_dnsClientewin [Corriendo] - Oracle VM VirtualBox
C:\Users\wadmin>whoami
C:\Users\wadmin>ipconfig /all
Configuración IP de Windows
  Nombre de host . . . . . : intervencion
  Sufijo DNS principal . . . . . : híbrido
  Tipo de nodo . . . . . : híbrido
  Enrutamiento IP habilitado . . . . . : no
  Proxy WINS habilitado . . . . . : no
  Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión . . . . . : Adaptador de escritorio Intel(R) PRO/1000 MT
    Descripción . . . . . : Adaptador de escritorio Intel(R) PRO/1000 MT
    Dirección física . . . . . : 08-00-27-53-D3-20
    DHCP habilitado . . . . . : no
    Configuración automática habilitada . . . . . : sí
    Vinculo: dirección IPv6 local . . . . : fe80::592c:9d83:f8f6:26c7%11<Preferido>
    Dirección IPv4 . . . . . : 172.16.100.100<Preferido>
    Máscara de subred . . . . . : 255.255.255.192
    Puerta de enlace predeterminada . . . . . : 172.16.100.67
    ID de DHCPv6 . . . . . : 235405351
    DUID de cliente DHCPv6 . . . . . : 00-01-00-01-1E-AA-83-25-08-00-27-7C-84-38
    Servidores DNS . . . . . : 172.16.100.66
    NetBIOS sobre TCP/IP . . . . . : habilitado
  Adaptador de túnel isatap.8EFP0E4B-3BB4-49E9-A77E-C8E932531A4:
    Estado de los medios . . . . . : medios desconectados
    Sufijo DNS específico para la conexión . . . . . : medios desconectados
    Descripción . . . . . : Adaptador ISATAP de Microsoft
    Dirección física . . . . . : 00-00-00-00-00-00-E0
    DHCP habilitado . . . . . : no
    Configuración automática habilitada . . . . . : sí
  C:\Users\wadmin>_
  
agl_W7_Pro32_SERI_dnsClientewin2 [Corriendo] - Oracle VM VirtualBox
C:\Users\wadmin>whoami
C:\Users\wadmin>ipconfig /all
Configuración IP de Windows
  Nombre de host . . . . . : intervencion
  Sufijo DNS principal . . . . . : híbrido
  Tipo de nodo . . . . . : híbrido
  Enrutamiento IP habilitado . . . . . : no
  Proxy WINS habilitado . . . . . : no
  Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión . . . . . : Adaptador de escritorio Intel(R) PRO/1000 MT
    Descripción . . . . . : Adaptador de escritorio Intel(R) PRO/1000 MT
    Dirección física . . . . . : 08-00-27-59-E4-95
    DHCP habilitado . . . . . : no
    Configuración automática habilitada . . . . . : sí
    Vinculo: dirección IPv6 local . . . . : fe80::442d:23e1:ce35:a4eb%11<Preferido>
    Dirección IPv4 . . . . . : 172.16.100.104<Preferido>
    Máscara de subred . . . . . : 255.255.255.192
    Puerta de enlace predeterminada . . . . . : 172.16.100.67
    ID de DHCPv6 . . . . . : 235405351
    DUID de cliente DHCPv6 . . . . . : 00-01-00-01-1E-AA-83-25-08-00-27-7C-84-38
    Servidores DNS . . . . . : 172.16.100.66
    NetBIOS sobre TCP/IP . . . . . : habilitado
  Adaptador de túnel isatap.8EFP0E4B-3BB4-49E9-A77E-C8E932531A4:
    Dirección IPv4 . . . . . : 172.16.100.104<Preferido>
    Máscara de subred . . . . . : 255.255.255.192
    Puerta de enlace predeterminada . . . . . : 172.16.100.67
    ID de DHCPv6 . . . . . : 235405351
    DUID de cliente DHCPv6 . . . . . : 00-01-00-01-1E-AA-83-25-08-00-27-7C-84-38
    Servidores DNS . . . . . : 172.16.100.66
    NetBIOS sobre TCP/IP . . . . . : habilitado
  C:\Users\wadmin>_
  
agl_W7_Pro32_SERI_dnsconsultas [Corriendo] - Oracle VM VirtualBox
C:\Users\wadmin>whoami
C:\Users\wadmin>ipconfig /all
Configuración IP de Windows
  Nombre de host . . . . . : contabilidad
  Sufijo DNS principal . . . . . : híbrido
  Tipo de nodo . . . . . : híbrido
  Enrutamiento IP habilitado . . . . . : no
  Proxy WINS habilitado . . . . . : no
  Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión . . . . . : Adaptador de escritorio Intel(R) PRO/1000 MT
    Descripción . . . . . : Adaptador de escritorio Intel(R) PRO/1000 MT
    Dirección física . . . . . : 08-00-27-AD-BB-5B
    DHCP habilitado . . . . . : no
    Configuración automática habilitada . . . . . : sí
    Vinculo: dirección IPv6 local . . . . : fe80::ad01:d05b:9e0e:830a%11<Preferido>
    Dirección IPv4 . . . . . : 172.16.100.102<Preferido>
    Máscara de subred . . . . . : 255.255.255.192
    Puerta de enlace predeterminada . . . . . : 172.16.100.67
    ID de DHCPv6 . . . . . : 235405351
    DUID de cliente DHCPv6 . . . . . : 00-01-00-01-1E-AA-83-25-08-00-27-7C-84-38
    Servidores DNS . . . . . : 172.16.100.67
    NetBIOS sobre TCP/IP . . . . . : habilitado
  Adaptador de túnel isatap.8EFP0E4B-3BB4-49E9-A77E-C8E932531A4:
    Dirección IPv4 . . . . . : 172.16.100.102<Preferido>
    Máscara de subred . . . . . : 255.255.255.192
    Puerta de enlace predeterminada . . . . . : 172.16.100.67
    ID de DHCPv6 . . . . . : 235405351
    DUID de cliente DHCPv6 . . . . . : 00-01-00-01-1E-AA-83-25-08-00-27-7C-84-38
    Servidores DNS . . . . . : 172.16.100.67
    NetBIOS sobre TCP/IP . . . . . : habilitado
  C:\Users\wadmin>_

```

A configuración de rede e os nomes dos clientes Windows XP e a seguinte. Tanto a dos clientes de Windows 7 como as do Windows XP, son a mesma configuración usada para o mesmo escenario, pero cando están activos as máquina virtuais dos equipos Windows XP as de Windows 7 están apagadas e viceversa. Esto fixose para comprobar a decisión do servidor alternativo DNS de Windows, xa que non funciona da mesma maneira con clientes Windows XP que con Windows 7 ou versións de Windows posteriores.



Configuraremos as interfaces de rede e os nomes dos equipos (en “/etc/hostname” e “/etc/hosts”) dos que serán os servidores DNS tanto o maestro (primario) como o escravo (secundario).



No servidor DNS maestro instalamos DNS Bind. Os ficheiros de configuración de Bind por defecto son instalados no directorio /etc/default/bind9.

Neste directorio encontraremos varios arquivos o principal para Bind será o “named.conf”, arquivo que únicamente contén o mapeo doutros arquivos principais de configuración.

```

GNU nano 2.5.3          Ficheiro: named.conf

// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

No arquivo “/etc/default/bind9” está básicamente a configuración do tipo de opcións que queremos establecer no servidor DNS, por exemplo aquí poderemos establecer a operabilidade soamente forzando a IPv4.

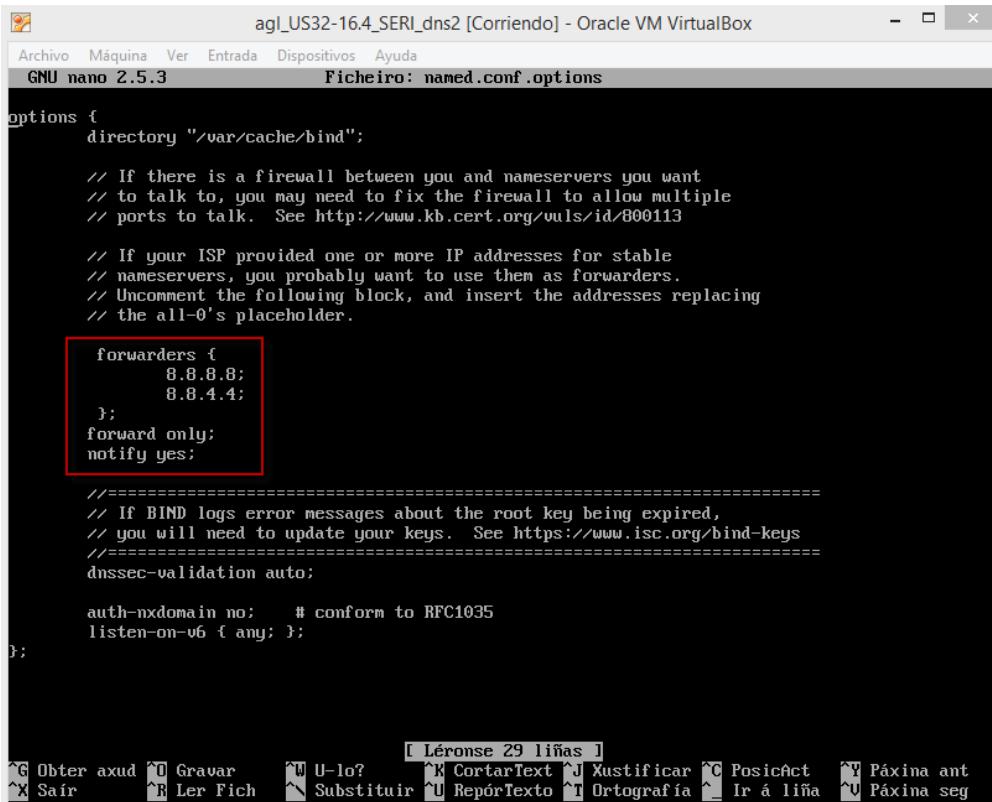
```

GNU nano 2.5.3          Ficheiro: /etc/default/bind9

# run resolvconf?
RESOLVCONF=no

# startup options for the server
OPTIONS="-u bind -4" ←
```

No arquivo “/etc/default/bind9/named.conf.options” podemos definir diversos parámetros, algúns deles son donde estableceremos o directorio caché, os reenviadores, notificación dalgún cambio, etc.



```

GNU nano 2.5.3          Ficheiro: named.conf.options

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
    forward only;
    notify yes;

    //========================================================================
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //================================================================
    dnssec-validation auto;

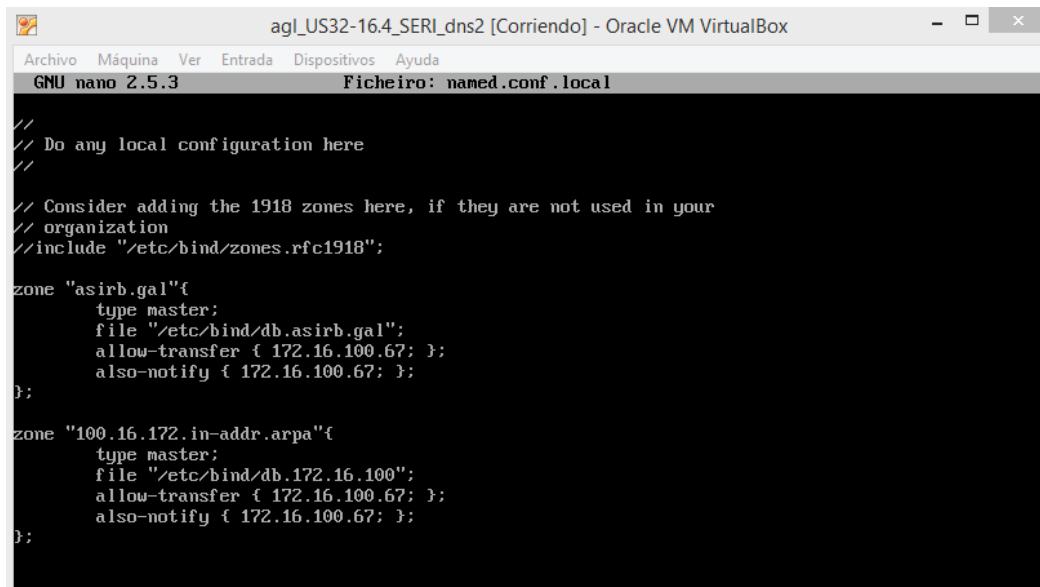
    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };

};

[ Léronse 29 liñas ]

```

No arquivo “/etc/default/bind9/named.conf.local” definiremos as zonas DNS tanto de búsqueda directa como inversa. Estableceremos tamén o tipo de servidor que será (maestro ou escravo), estableceremos o arquivo da configuración de zona, no caso de ter algún servidor escravo (como será este caso) decímoslle que transfira o ficheiro de zona e que avise dalgún cambio en dito ficheiro ao servidor escravo indicado (172.16.100.67).



```

GNU nano 2.5.3          Ficheiro: named.conf.local

// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "asirb.gal"{
    type master;
    file "/etc/bind/db.asirb.gal";
    allow-transfer { 172.16.100.67; };
    also-notify { 172.16.100.67; };
};

zone "100.16.172.in-addr.arpa"{
    type master;
    file "/etc/bind/db.172.16.100";
    allow-transfer { 172.16.100.67; };
    also-notify { 172.16.100.67; };
};

```

Agora definiremos os ficheiros de configuración de zona, seguindo o mesmo patrón que algún arquivo de exemplo que xa nos facilita o servidor, farese unha copia e editarase (neste caso /etc/default/bind9/db.asirb.gal).

Establecemos o SOA, dominio e email responsable. Despois definiremos os RR A e NS. Hai que ter en conta que o @ sería traducido polo dominio “asirb.gal” ou incluso se non se pon nada tamén se interpretaría así.

```

agl_US32-16.4_SERI_dns2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 2.5.3 Ficheiro: db.asirb.gal

;
; BD data file for asirb.gal
;
$TTL    604800
@       IN      SOA     asirb.gal. webmaster.asirb.gal. (
                            2           ; Serial
                            604800      ; Refresh
                            86400       ; Retry
                            2419200     ; Expire
                            604800 )    ; Negative Cache TTL
;
@       IN      NS      ns1.asirb.gal.
ns2    IN      A       172.16.100.67
@       IN      NS      ns2.asirb.gal.
ns1    IN      A       172.16.100.66

```

Faremos o mesmo co anterior pero esta vez con un arquivo para a zona de búsquedas inversa, donde establecerase os RR NS e PTR, donde 66 e 67 será a parte do último octeto da dirección IP asociada a cada máquina e que resolverá co nome de dominio asignado no arquivo.

```

agl_US32-16.4_SERI_dns2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 2.5.3 Ficheiro: db.172.16.100

;
; BIND reverse data file db.172.16.100
;
$TTL    604800
@       IN      SOA     100.16.172.in-addr.arpa. webmaster.asirb.gal. (
                            1           ; Serial
                            604800      ; Refresh
                            86400       ; Retry
                            2419200     ; Expire
                            604800 )    ; Negative Cache TTL
;
@       IN      NS      ns1.asirb.gal.
66     IN      PTR     ns1.asirb.gal.
@       IN      NS      ns2.asirb.gal.
67     IN      PTR     ns2.asirb.gal.

```

A continuación **configurarase o servidor DNS escravo**, unha vez instalado DNS Bind neste servidor simplemente crearemos as zonas DNS para as búsquedas directas e inversas no arquivo “/etc/default/bind9/named.conf.local”, coa diferencia de que os parámetros para cada zona serán distintos o dos establecidos no servidor maestro, neste caso definirase o tipo de servidor como slave, os ficheiros de configuración de zona DNS serán referenciados soamente co mesmo nome que teñen no servidor maestro, e por último estableceremos quen vai ser o servidor maestro polo cal solicitaralle futuras actualización dos arquivos de zona DNS.

```
agl_US32-16.4_SERI_dns3 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 2.5.3 Ficheiro: named.conf.local

// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "asirb.gal"{
    type slave;
    file "db.asirb.gal";
    mastersf 172.16.100.66; };
zone "100.16.172.in-addr.arpa"{
    type slave;
    file "db.172.16.100";
    mastersf 172.16.100.66; };

```

Os reenviadores tamén están **configurados** manualmente (`/etc/default/bind9/named.conf.options`) no **servidor escravo**.

Para comprobar que todo está correcto podémolo facer co comando “named-checkconf” o cal comproba posibles errores no ficheiro /etc/bind/named.conf.local. E tamén co comando “named-checkzone” indicando o nome de zona e a ruta absoluta, o cal comproba posibles errores nos ficheiros de configuración creados para as zonas DNS.

Reiniciamos o servizo: "sudo service bind9 restart"

Ver o estado do servizo para posibles comprobacións de correcto ou mal funcionamiento:

”sudo service bind9 status“

```

agl_US32-16_4_SERI_dns2 [Corriendo] - Oracle VM VirtualBox - x
Administrator:~$ sudo bind9 restart
Administrator:~$ sudo service bind9 status
bind9.service
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Drop-In: /run/systemd/generator/bind9.service.d
             └─50-insserv.conf-shamed.conf
     Active: active (running) since Dom 2016-12-04 21:43:07 CET; 7s ago
       Docs: man:named(8)
   Process: 1564 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
    Main PID: 1572 (named)
      Tasks: 1
     Memory: 8.3M
        CPU: 17ms
       CGroup: /system.slice/bind9.service
                  └─1572 /usr/sbin/named -f -u bind

Dec 04 21:43:08 ns1 named[1572]: zone 0.in-addr.arpa/IN: loaded serial 1
Dec 04 21:43:08 ns1 named[1572]: zone 127.in-addr.arpa/IN: loaded serial 1
Dec 04 21:43:08 ns1 named[1572]: zone 100.16.172.in-addr.arpa/IN: loaded serial 1
Dec 04 21:43:08 ns1 named[1572]: zone 100.16.172.in-addr.arpa/IN: loaded serial 1
Dec 04 21:43:08 ns1 named[1572]: zone asirb.gal/IN: loaded serial 1
Dec 04 21:43:08 ns1 named[1572]: zone localhost/IN: loaded serial 2
Dec 04 21:43:08 ns1 named[1572]: all zones loaded
Dec 04 21:43:08 ns1 named[1572]: running
Dec 04 21:43:08 ns1 named[1572]: sending notifies (serial 2)
Dec 04 21:43:08 ns1 named[1572]: zone asirb.gal/IN: sending notifies (serial 1)
Administrator:~$ sudo bind9 named-checkconf
Administrator:~$ sudo bind9 named-checkzone db.asirb.gal /etc/bind/db.asirb.gal
zone db.asirb.gal/IN: loaded serial 2
OK
Administrator:~$ sudo bind9 named-checkzone db.172.16.100 /etc/bind/db.172.16.100
zone db.172.16.100/IN: loaded serial 1
OK
Administrator:~$ sudo bind9

```

Tanto no servidor maestro como no servidor escravo podemos comprobar que os arquivos de configuración das zonas DNS transferíronse correctamente visualizando o log de sistema, por exemplo: "tail -n 50 /var/log/syslog".

Podemos comprobar no servidor escravo se os arquivos están sendo usados e polo tanto foron correctamente transferidos e revisar en que punto de actualización están respeto os arquivos de zona DNS do servidor maestro, comprobando o número de serie incremental de modificación de cada un dos arquivos, pero para esto temos que encontrar e abrir os arquivos. Por defecto está definido no arquivo de configuración de bind "/etc/default/bind9/named.conf.options" a ruta caché. Polo que consultamos dita ruta no servidor escravo: "ls /var/cache/bind".

```

agl_US32-14_SERI_dns2 [Corriendo] - Oracle VM VirtualBox
Agente de sistema
Archivo Máquina Ver Entrada Dispositivos Ayuda
Dec 4 21:43:08 ns1 named[1572]: GeoIP NetSpeed (type 10) DB not available
Dec 4 21:43:08 ns1 named[1572]: using default UDP/IPv4 port range: [32768, 69999]
Dec 4 21:43:08 ns1 named[1572]: using default UDP/IPv6 port range: [32768, 69999]
Dec 4 21:43:08 ns1 named[1572]: listening on IPv4 interfaces port 53
Dec 4 21:43:08 ns1 named[1572]: listening on IPv6 interfaces port 53
Dec 4 21:43:08 ns1 named[1572]: listening on IPv4 interface ep0s3, 172.16.100.66#53
Dec 4 21:43:08 ns1 named[1572]: listening on IPv4 interface ep0s8, 10.0.3.15#53
Dec 4 21:43:08 ns1 named[1572]: generating session key for dynamic DNS
Dec 4 21:43:08 ns1 named[1572]: sizing zone task pool based on 7 zones
Dec 4 21:43:08 ns1 named[1572]: using built-in root key for view _default
Dec 4 21:43:08 ns1 named[1572]: set up managed keys zone for view _default, file 'managed-keys.bind'
Dec 4 21:43:08 ns1 named[1572]: configuring command channel from '/etc/bind/rndc.key'
Dec 4 21:43:08 ns1 named[1572]: command channel listening on 127.0.0.1#953
Dec 4 21:43:08 ns1 named[1572]: configuring command channel from '/etc/bind/rndc.key'
Dec 4 21:43:08 ns1 named[1572]: command channel listening on :1#953
Dec 4 21:43:08 ns1 named[1572]: managed-keys-zone: journal file is out of date: removing journal file
Dec 4 21:43:08 ns1 named[1572]: managed-keys-zone: loaded serial 20
Dec 4 21:43:08 ns1 named[1572]: zone 0.in-addr.arpa/IN: loaded serial 1
Dec 4 21:43:08 ns1 named[1572]: zone 127.in-addr.arpa/IN: loaded serial 1
Dec 4 21:43:08 ns1 named[1572]: zone 100.16.172.in-addr.arpa/IN: loaded serial 1
Dec 4 21:43:08 ns1 named[1572]: zone 255.in-addr.arpa/IN: loaded serial 1
Dec 4 21:43:08 ns1 named[1572]: zone asirb.gal/IN: loaded serial 2
Dec 4 21:43:08 ns1 named[1572]: zone localhost/IN: loaded serial 2
Dec 4 21:43:08 ns1 named[1572]: zone zones loaded
Dec 4 21:43:08 ns1 named[1572]: running
Dec 4 21:43:08 ns1 named[1572]: zone asirb.gal/IN: sending notifies (serial 2)
Dec 4 21:43:08 ns1 named[1572]: zone 100.16.172.in-addr.arpa/IN: sending notifies (serial 1)
Dec 4 21:43:08 ns1 named[1572]: client 172.16.100.67#32806: received notify for zone 'asirb.gal'
Dec 4 21:43:08 ns1 named[1572]: client 172.16.100.67#51811 (100.16.172.in-addr.arpa): transfer of '100.16.172.in-addr.arpa/IN': AXFR started (serial 1)
Dec 4 21:43:08 ns1 named[1572]: client 172.16.100.67#51811 (100.16.172.in-addr.arpa): transfer of '100.16.172.in-addr.arpa/IN': AXFR ended
Dec 4 21:43:08 ns1 named[1572]: client 172.16.100.67#3156: received notify for zone '100.16.172.in-addr.arpa'
admin@ns1:~$ /etc/bind$
```

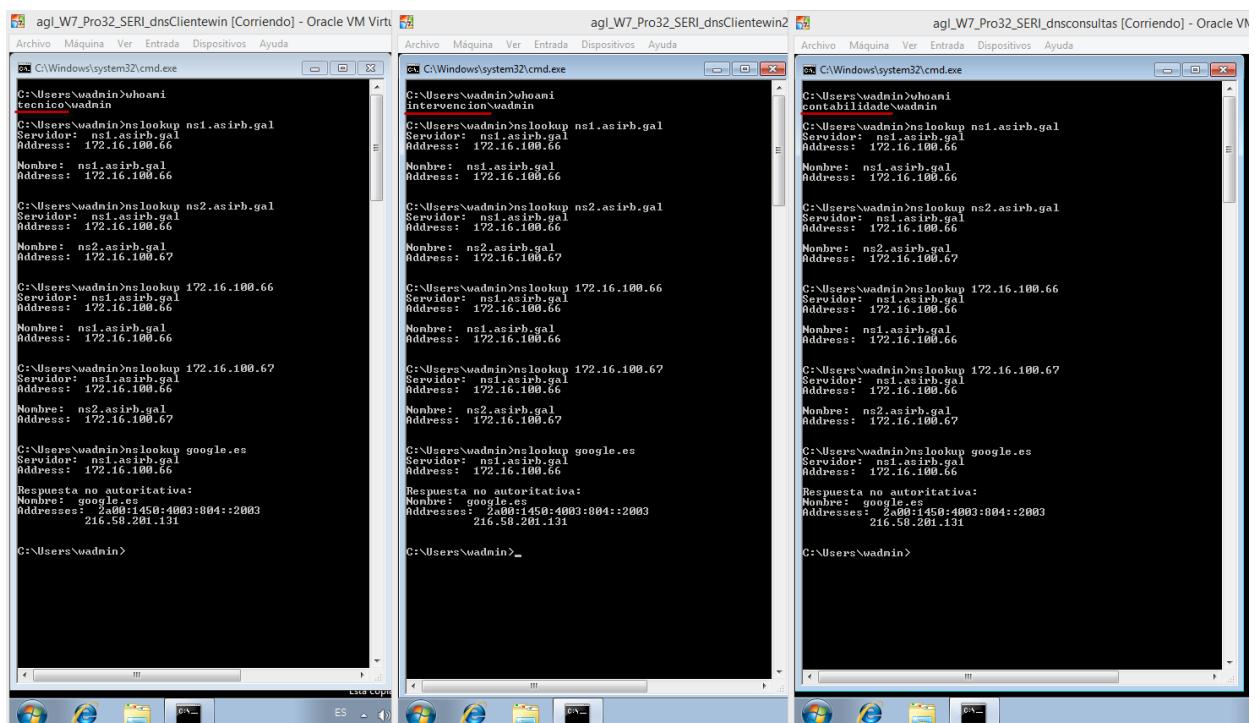
  

```

agl_US32-16_SERI_dns3 [Corriendo] - Oracle VM VirtualBox
Agente de sistema
Archivo Máquina Ver Entrada Dispositivos Ayuda
Dec 4 21:43:58 ns2 named[1460]: automatic empty zone: B.E.F.IP6.ARPA
Dec 4 21:43:58 ns2 named[1460]: automatic empty zone: B.B.D.0.1.0.0.1.P6.ARPA
Dec 4 21:43:58 ns2 named[1460]: automatic empty zone: E.M.T.Y.S112.ARPA
Dec 4 21:43:58 ns2 named[1460]: configuring command channel from '/etc/bind/rndc.key'
Dec 4 21:43:58 ns2 named[1460]: command channel listening on 127.0.0.1#953
Dec 4 21:43:58 ns2 named[1460]: configuring command channel from '/etc/bind/rndc.key'
Dec 4 21:43:58 ns2 named[1460]: command channel listening on ::1#953
Dec 4 21:43:58 ns2 named[1460]: managed-keys-zone: journal file is out of date: removing journal file
Dec 4 21:43:58 ns2 named[1460]: managed-keys-zone: loaded serial 16
Dec 4 21:43:58 ns2 named[1460]: zone 0.in-addr.arpa/IN: loaded serial 1
Dec 4 21:43:58 ns2 named[1460]: zone 127.in-addr.arpa/IN: loaded serial 1
Dec 4 21:43:58 ns2 named[1460]: zone 255.in-addr.arpa/IN: loaded serial 1
Dec 4 21:43:58 ns2 named[1460]: zone asirb.gal/IN: loaded serial 2
Dec 4 21:43:58 ns2 named[1460]: zone localhost/IN: loaded serial 2
Dec 4 21:43:58 ns2 named[1460]: all zones loaded
Dec 4 21:43:58 ns2 named[1460]: zone asirb.gal/IN: running
Dec 4 21:43:58 ns2 named[1460]: zone asirb.gal/IN: sending notifies (serial 2)
Dec 4 21:43:58 ns2 named[1460]: zone 100.16.172.in-addr.arpa/IN: transfer started.
Dec 4 21:43:58 ns2 named[1460]: transfer of '100.16.172.in-addr.arpa/IN' from 172.16.100.66#53: connected using 172.16.100.67#51811
Dec 4 21:43:58 ns2 named[1460]: transfer of '100.16.172.in-addr.arpa/IN': transferred serial 1
Dec 4 21:43:58 ns2 named[1460]: transfer of '100.16.172.in-addr.arpa/IN' from 172.16.100.66#53: Transfer status: success
Dec 4 21:43:58 ns2 named[1460]: transfer of '100.16.172.in-addr.arpa/IN' from 172.16.100.66#53: Transfer completed: 1 message, 0 records, 202 bytes, 000 seconds (20200 bytes/sec)
Dec 4 21:43:58 ns2 named[1460]: network unreachable resolving '._DNSEK.V.IN': 2001:a63::35#53
Dec 4 21:43:58 ns2 named[1460]: network unreachable resolving '._DNSEV.V.IN': 2001:500:84::#53
Dec 4 21:43:58 ns2 named[1460]: network unreachable resolving 'E.ROOT-SERVERS.NET._AAAA.V.IN': 2001:7f1:a1:#53
Dec 4 21:43:58 ns2 named[1460]: network unreachable resolving 'G.ROOT-SERVERS.NET._AAAA.V.IN': 2001:7f1:a1:#53
Dec 4 21:43:58 ns2 named[1460]: network unreachable resolving '._DNSEK.V.IN': 2001:7fd:#1#53
Dec 4 21:43:58 ns2 named[1460]: network unreachable resolving '._DNSEV.V.IN': 2001:7fd:#1#53
Dec 4 21:43:58 ns2 named[1460]: network unreachable resolving 'E.ROOT-SERVERS.NET._AAAA.V.IN': 2001:7f1:a1:#53
Dec 4 21:43:58 ns2 named[1460]: network unreachable resolving 'G.ROOT-SERVERS.NET._AAAA.V.IN': 2001:7f1:a1:#53
admin@ns2:~$ /etc/bind$
```

Por último comprobarase o correcto funcionamiento dos servidores DNS anteriores instalados e configurados.

Empezaremos con tres clientes Windows 7, os cales vemos que o servidor maestro funciona correctamente, este servidor está configurado para os clientes Windows 7 como "servidor preferido". Compróbase o funcionamento dos reenviadouros a consultas de dominios externos.



Agora vamos simular unha caída do servidor apagando a máquina ns1.asirb.gal correspondente o servidor DNS maestro.

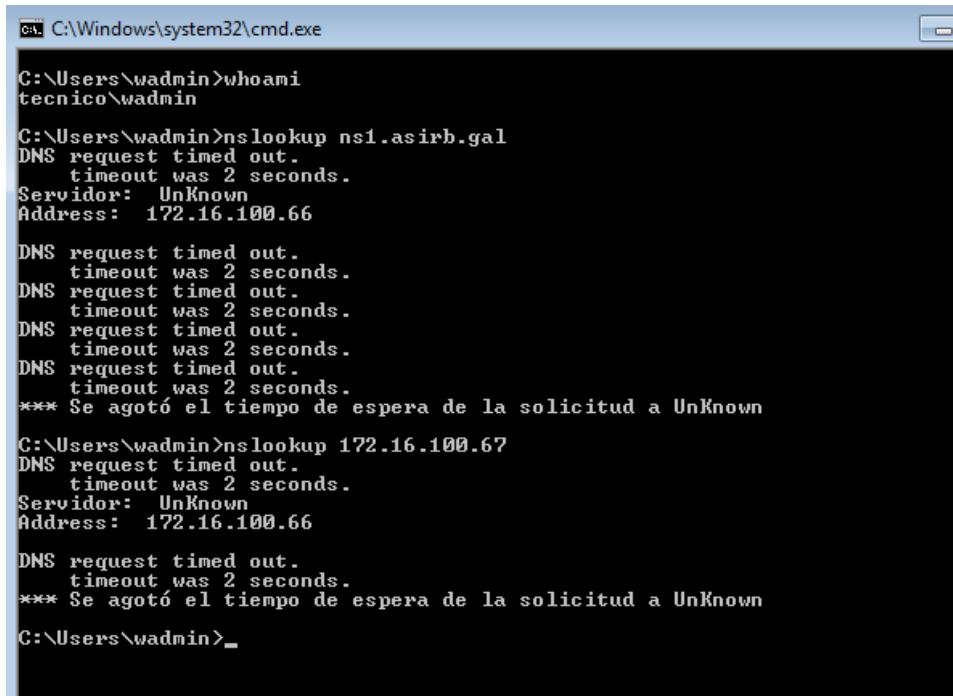
Vemos que un dos clientes Windows 7 tenta resolver os nomes de dominio solicitados a través do primeiro servidor, e decir, na configuración de Windows 7 como servidor preferido (servidor maestro) aínda que se da de conta de que este non está operativo por que non lle está respondendo, Windows 7 non é capaz de establecer o seu segundo servidor alternativo configurado (servidor escravo).

Investigando este tema, cheguei a conclusión que esto ocurre por como funcionan certos protocolos propietarios de Microsoft e como operan estos mecanismos dentro de este tipo de sistema. Poderíamos pensar que se debe a un tempo de espera, en moitos sitios fálase de esperar 15 minutos xa que é o tempo de refresco por defecto do servidor DNS tanto Bind como un rol servidor DNS en Windows. Tamén falábbase de que Windows 7 pese a que teña dous servidores DNS configurados este establecerá por defecto sempre o servidor que lle conteste no arribo do sistema, teríamos que reiniciar o equipo para que se actualize o cambio e vaciar a caché DNS do cliente (ipconfig /flushdns).

Pero ninguna das opcións anteriores, e outras más que pueden comprobar persoalmente funcionan así.

Deixo unha referencia a un artículo que más ou menos explica un poco este caso.

<http://blogs.msmvps.com/acefekay/2009/11/29/dns-wins-netbios-amp-the-client-side-resolver-browser-service-disabling-netbios-direct-hosted-smb-directsmb-if-one-dc-is-down-does-a-client-logon-to-another-dc-and-dns-forwarders-algorithm>



The screenshot shows a Windows Command Prompt window titled 'C:\Windows\system32\cmd.exe'. The user is running under the account 'wadmin' in the 'tecnico' group. The command 'whoami' is run first, followed by 'nslookup ns1.asirb.gal'. This command fails because the server is timed out, with a timeout of 2 seconds. It then attempts to resolve the IP address 172.16.100.67, which also times out. Both attempts result in a 'Servidor: UnKnown' response and an 'Address: 172.16.100.66' output. Finally, another 'nslookup' command is run for the IP address 172.16.100.67, which again times out and results in a 'Servidor: UnKnown' response.

```
C:\Users\wadmin>whoami
wadmin
C:\Users\wadmin>nslookup ns1.asirb.gal
DNS request timed out.
    timeout was 2 seconds.
Servidor: UnKnown
Address: 172.16.100.66

DNS request timed out.
    timeout was 2 seconds.
*** Se agotó el tiempo de espera de la solicitud a UnKnown

C:\Users\wadmin>nslookup 172.16.100.67
DNS request timed out.
    timeout was 2 seconds.
Servidor: UnKnown
Address: 172.16.100.66

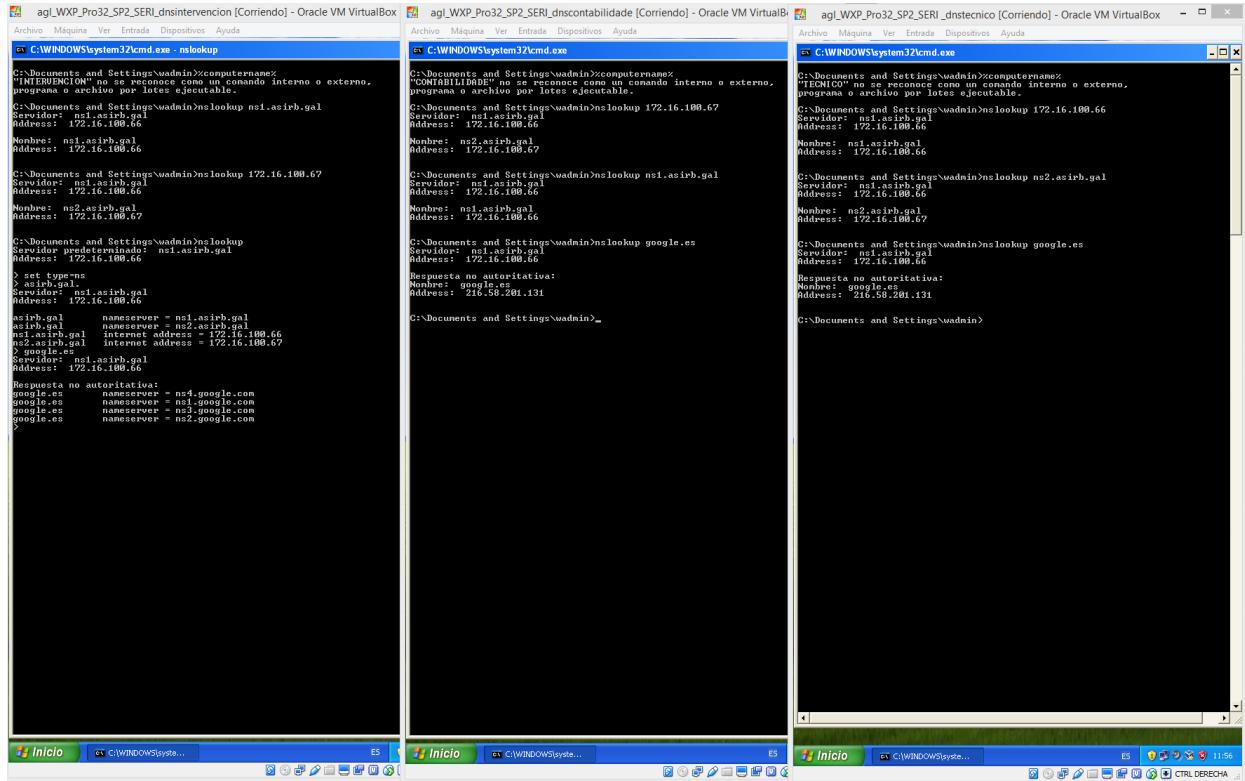
DNS request timed out.
    timeout was 2 seconds.
*** Se agotó el tiempo de espera de la solicitud a UnKnown

C:\Users\wadmin>
```

Sin embargo, facendo as probas de resolución DNS nos equipos clientes Windows XP, vemos que esto xa funciona doutro modo.

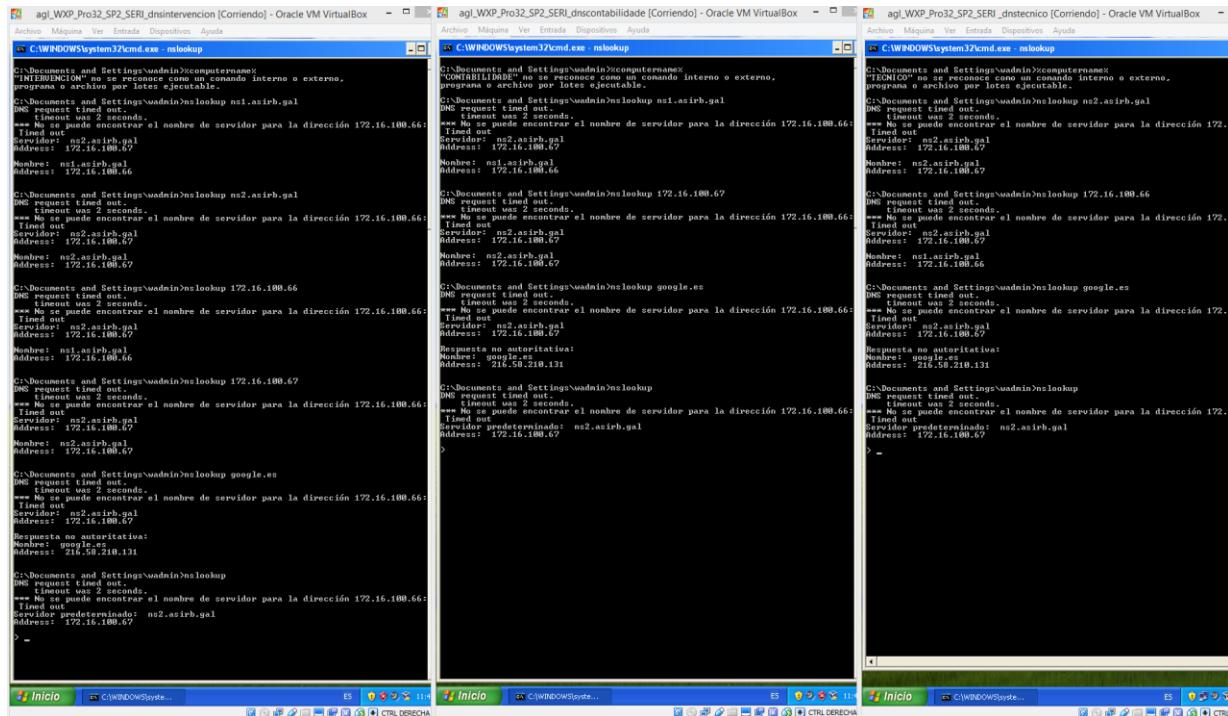
A comprobación de consultas ao servidor maestro ou preferido configurado para Windows XP e funciona correctamente.

Vemos tamén como os reenviadores están funcionando e facendo resolucións de consultas de nomes externos.



Cando se simula a caída do servidor maestro, vemos a comprobación de consultas do servidor escravo ou alternativo para configurado en Windows XP e vemos que funciona correctamente.

Despois dun pequeno intervalo de tempo este dase de conta de que o servidor maestro non está dispoñible, polo que entra en funcionamento o seguinte servidor alternativo que será o servidor escravo, vemos que se mostra unha mensaxe de advertencia donde se indica que non puido encontrar o servidor preferido establecido (que sería o servidor maestro).



## 5. Conclusóns

Despois de todo o feito ata agora podemos chegar a conclusión de que o protocolo de resolución de nomes DNS é vital para o funcionamento de todo Internet, e un protocolo pilar na comunicación xa e resulta sorprendente como co so 13 servidores root (pese que haiga varias réplicas de cada un deles) todo o mundo está comunicado a través da resolución de nomes en direccións IP e viceversa.

As utilidades de comandos internos nslookup, host e dig, sendo dig o más pontente e extenso na súa detallada información. Son utilidades que nos dan moita información para coñecer non so as direccións IP de certos nomes e viceversa, se non que tamén podemos tentar coñecer de que forma e que nomenclaturas internas úsanse determinadas organizacións, xa sexa consultando a SOA, os NS autorizados para unha zona DNS, email responsables de zona, que servidores dependen de que dominios e teñen autoridade sobre determinados TLDs, ver a caché de servidores corporativos, realizando preguntas internas a ese servidor por determinados nomes de dominio e esperando a súa resposta se é ou non autoritativa, sabendo así si nesa organización visitaron ou non certos nomes de dominio (DNS Snooping) etc.

As prácticas desenvoltas, podemos ver como tanto unha configuración dun servidor DNS primario (master) e secundario (slave) a idea e básicamente a mesma, tanto para sistemas Windows como para contornas Linux, xa que non se trata do sistema que opere o DNS se non que DNS é un protocolo estándar.

Tanto en Webmin como en Windows Server a instalación e configuración de zonas foi sinxela, si se complicou un pouco máis nunha contorna Ubuntu Server en formato terminal pero analizando os ficheiro e comprendendo a lóxica de funcionamento concluíronse as prácticas realizas correctamente.

Xa que o importante nestes casos non é saber onde está determinando ficheiro ou si un comando interno chamábase dunha forma ou outra, o importante é ter o concepto de funcionamiento claro, en base a eso aplícalo a calquera sistema, o como aplícalo para un determinado sistema xa e algo que podemos votar man dalgún libro ou buscando na rede de Internet.