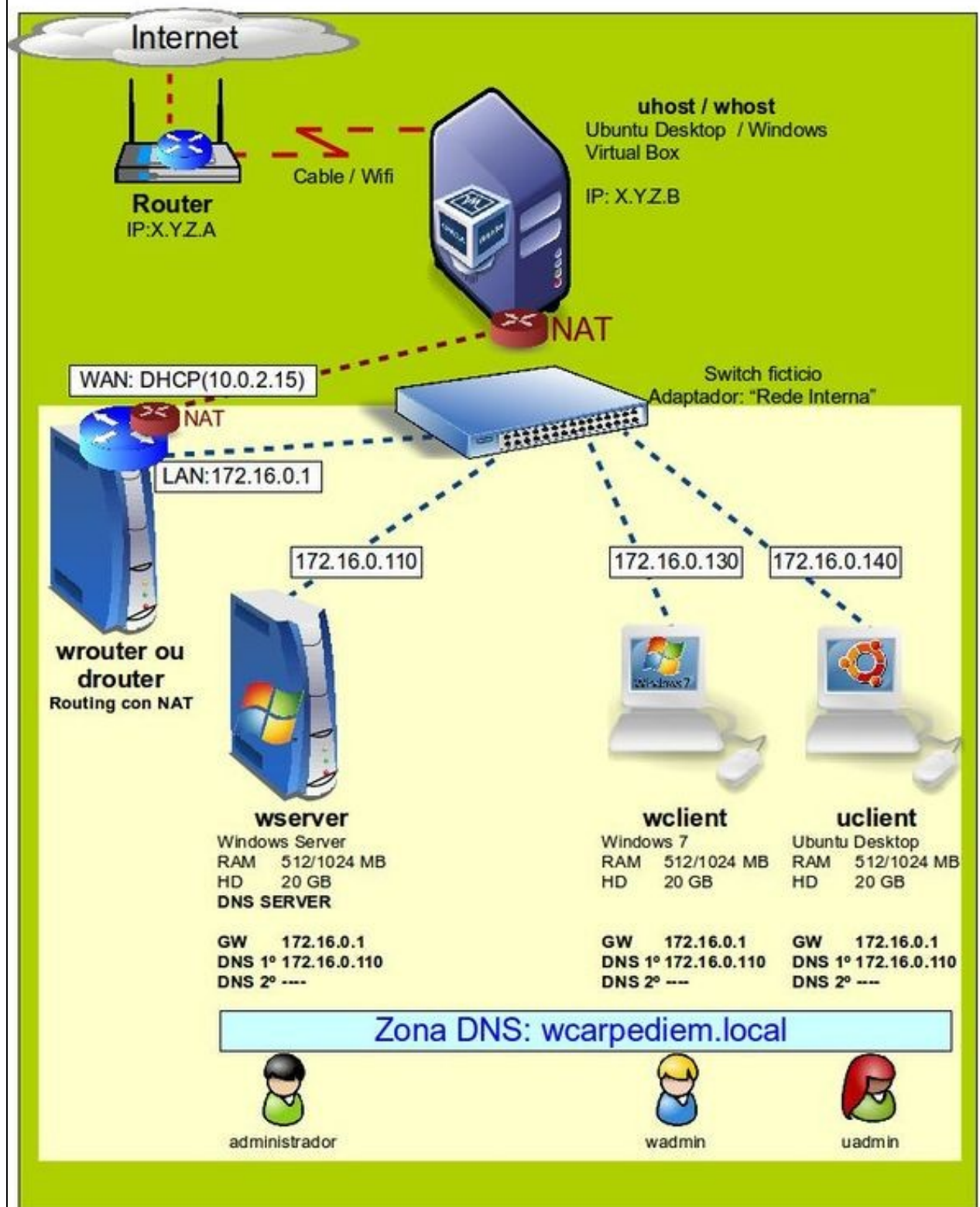


1 Windows: Instalação e configuração do servidor usando recursividade

Escenario 6.A: DNS: Servidor Windows. Recursividade (Servidores Raiz)



- Visto o escenario vaise instalar e configurar o servizo DNS no equipo **wserver**.
- Igual que na parte anterior do curso, a saída a Internet nas máquinas pódese facer usando a máquina *wrouter* ou *drouter* como router con NAT ou configurando as tarxetas das máquinas en modo de *rede NAT*.
- O servidor **wserver** terá configurada 2 zonas:
 - ♦ Zona de busca directa: **wcarpediem.local**

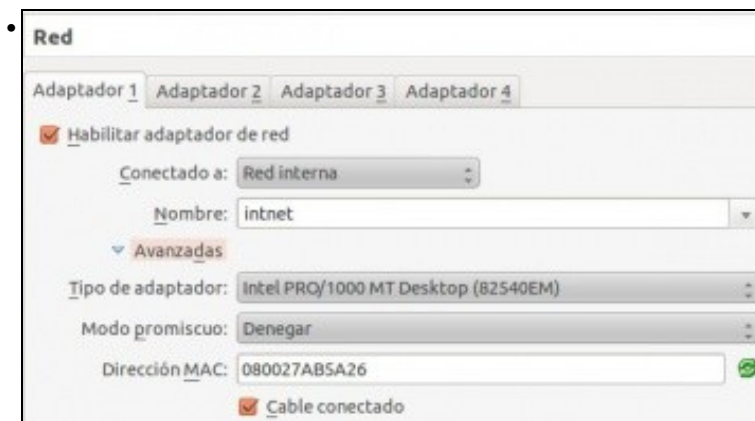
- ♦ Zona de busca inversa: **172.16.0.0**
- Ademais estará configurado para usar **recursividade**.
- Revisar os [Conceptos básicos de DNS](#) se non se ten claro algún dos parámetros anteriores.

1.1 Sumario

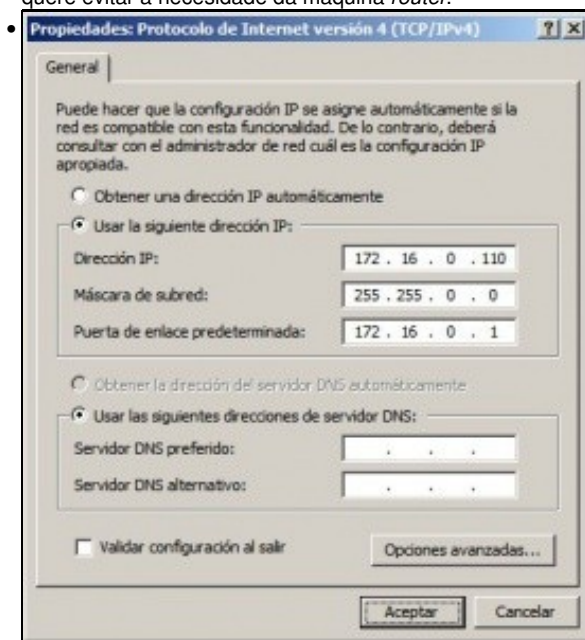
- 1 Configuración previa da MV wserver
- 2 Instalar o servizo DNS en wserver
- 3 Propiedades do servidor DNS
- 4 Configuración do cliente DNS de wserver
- 5 Configurar zona de busca directa: wcarpediem.local
- 6 Crear zona de busca inversa para 172.16.0.0
- 7 Creación de rexistros dentro das zonas
 - ♦ 7.1 Creación de rexistros con asociacións a IPs fóra da LAN
- 8 Para fondar máis sobre DNS en Windows

1.2 Configuración previa da MV wserver

- Facer unha instantánea de **wserver** coa MV apagada.



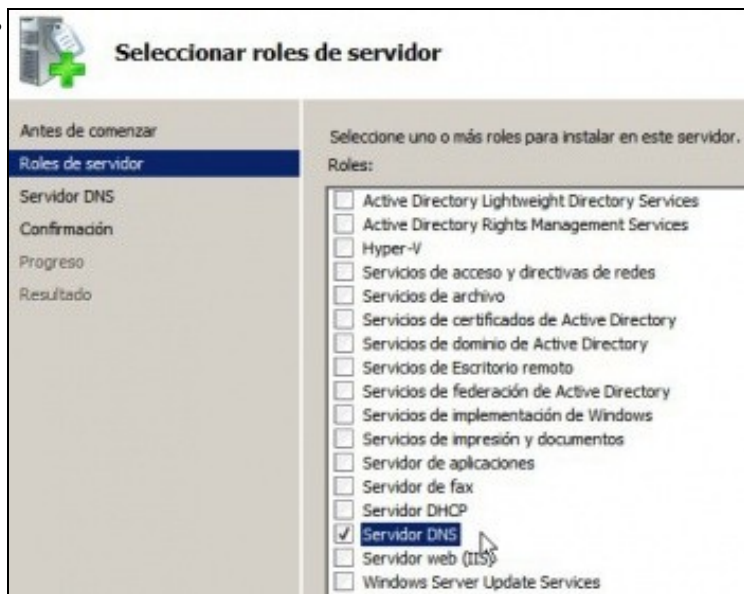
A MV **wserver** xa debera estar configurada do escenario anterior cun único adaptador en modo **Rede interna** ou en modo **Rede NAT** se se quere evitar a necesidade da máquina **router**.



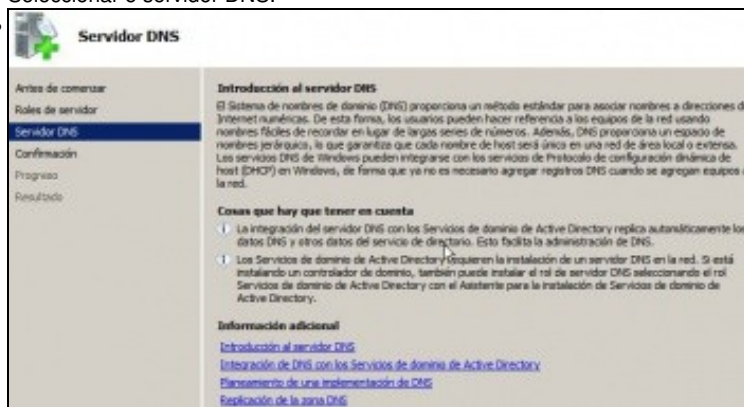
e coa configuración IP da imaxe.

1.3 Instalar o servizo DNS en wserver

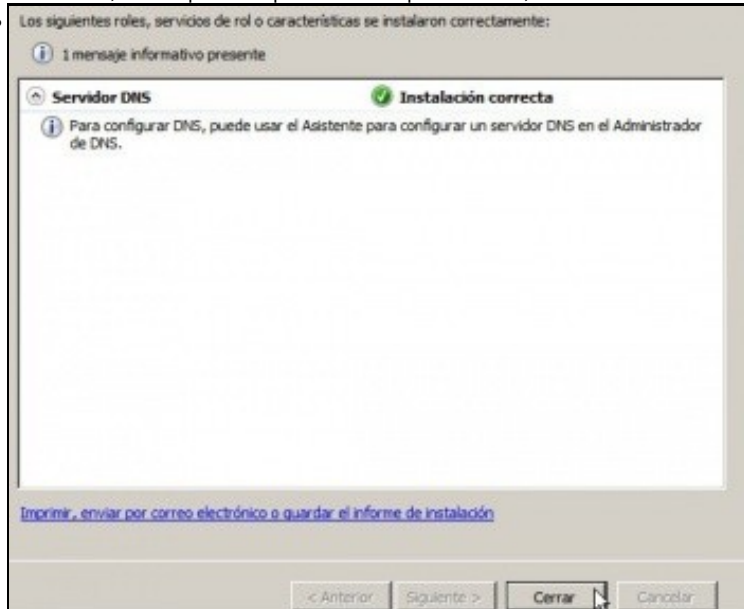
- Para instalar e configurar o servizo DNS, ir ao menú **Inicio->Ferramentas administrativas->Administrar o servidor** e premer en **Agregar roles** da categoría **Roles**.



Seleccionar o servidor DNS.



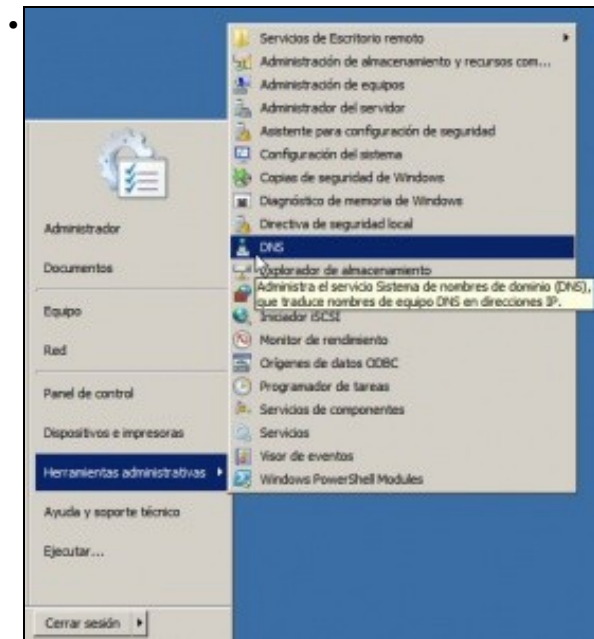
Pódese ler, aínda que sexa polo menos a primeira vez, a información de axuda.



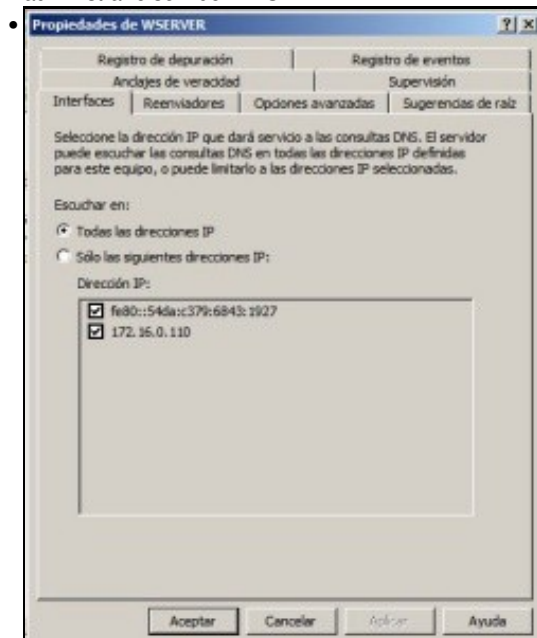
Comezar a instalar ... Se aparece algún asistente de configuración ... cancelalo.

1.4 Propiedades do servidor DNS

- Antes de configurar nada, nin de engadir ningunha zona, observar como está configurado o servidor DNS por defecto:



Ir ao menú Inicio->Ferramentas administrativas->DNS ou a Inicio->Ferramentas administrativas->Administrar o servidor, para administrar o servidor DNS.



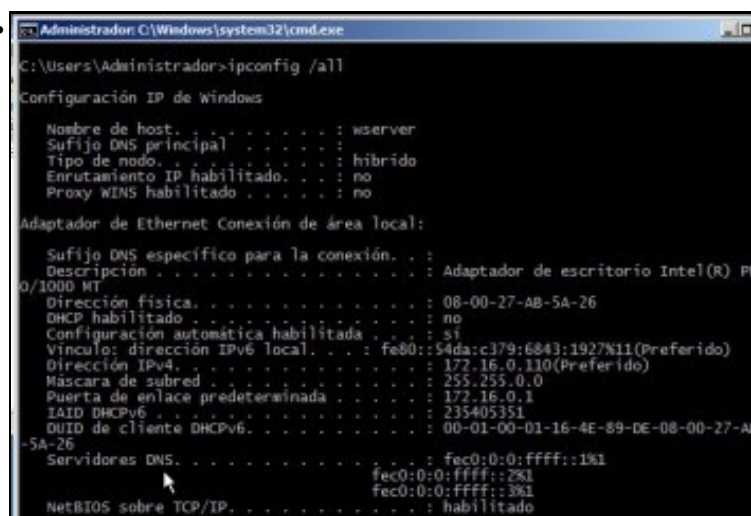
Premer co botón dereito sobre o servidor DNS **wserver**. Na lapela **Interfaces** poderíase indicar sobre que interfaces recibiría consultas DNS no caso de ter varios.



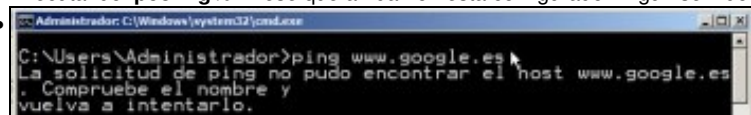
Na lapela **Suxerencias Raíz** pódense observar os enderezos IP dos servidores raíz, usados no proceso de recursividade.

1.5 Configuración do cliente DNS de wserver

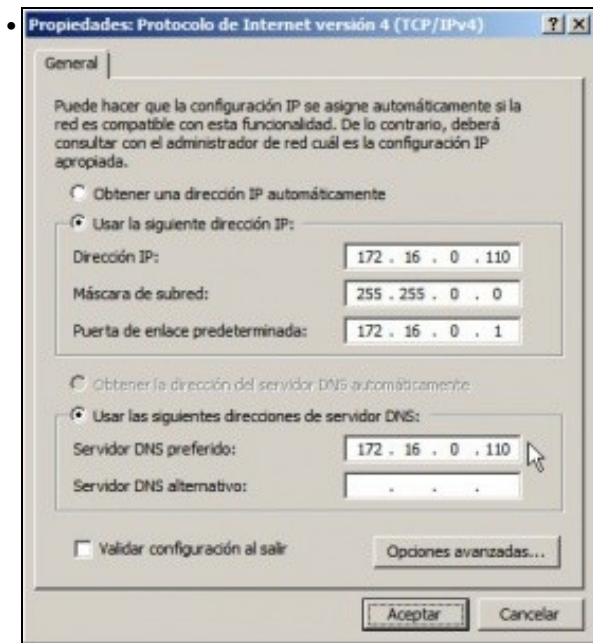
- Aínda que **wserver** sexa o servidor de DNS tamén é cliente, e haberá que configurar o cliente DNS para que pregunte ao servidor DNS que el mesmo ten instalado.



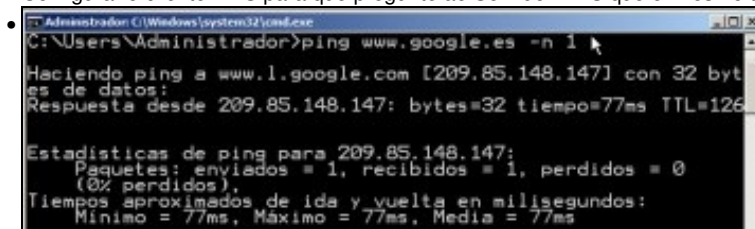
Executando **ipconfig /all** vese que aínda non está configurado ningún servidor DNS ao que preguntar para realizar resolucións de nomes.



Exemplo de como o **wserver**, aínda sendo servidor de DNS, non é quen de resolver un nome de dominio.



Configurar o cliente DNS para que pregunte ao Servidor DNS que el mesmo ten instalado.



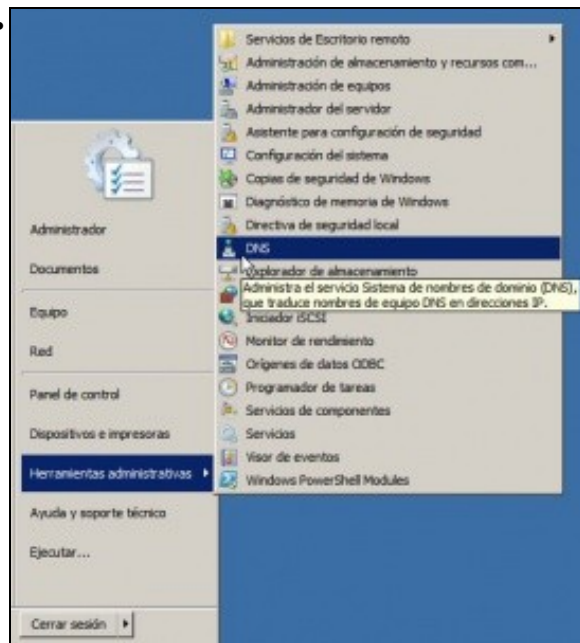
Ahora si que o propio servidor DNS, como cliente, xa é quen de facer resolucións DNS. Para iso o servidor DNS usa o proceso de recursividade a través dos servidores raíz anteriores.



Observar como agora xa se amosa cal é servidor de DNS ao que realizar as consultas DNS.

1.6 Configurar zona de busca directa: wcarpediem.local

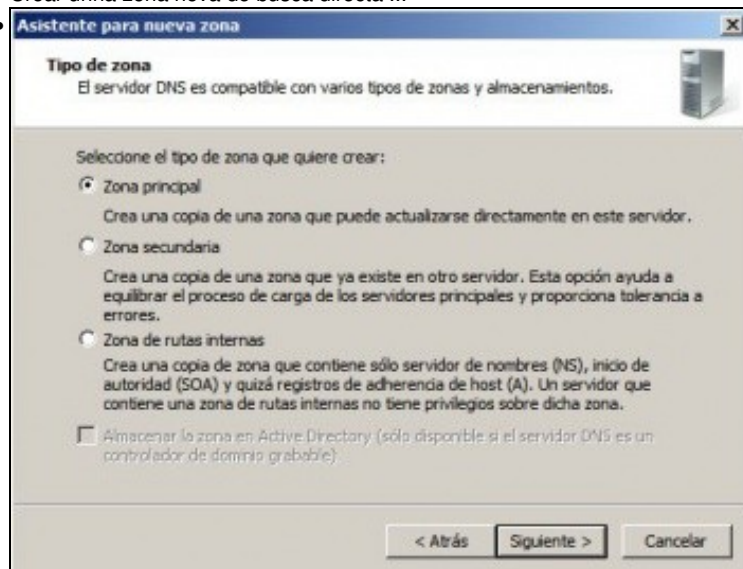
A continuación vaise crear a zona de busca directa para o dominio **wcarpediem.local**, isto é, dado un nome de dominio que nos diga a IP asociada.



Ir ao menú Inicio->Ferramentas administrativas->DNS ou a Inicio->Ferramentas administrativas->Administrar o servidor, para administrar o servidor DNS.



Crear unha zona nova de busca directa ...



Crear unha **zona principal**. Unha **zona secundaria** sería crear un zona de backup de outra xa existente e non é caso, nin se vai ver neste curso.

- Asistente para nueva zona**

Nombre de zona
¿Qué nombre tiene la zona nueva?

El nombre de zona especifica la parte del espacio de nombres DNS para el que actúa el servidor de autorización. Puede ser el nombre de dominio de la organización (por ejemplo, microsoft.com) o una parte del nombre de dominio (por ejemplo, nuevazona.microsoft.com). El nombre de zona no es el nombre del servidor DNS.

Nombre de zona:
wcarpediem.local

Indicar o nome da nova zona:wcarpediem.local

- Asistente para nueva zona**

Archivo de zona
Puede crear un archivo de zona nuevo o usar un archivo copiado de otro servidor DNS.

¿Desea crear un archivo nuevo de zona o usar el archivo existente que copió de otro servidor DNS?

☒ Crear un archivo nuevo con este nombre de archivo:
wcarpediem.local.dns

☐ Usar este archivo:

Para usar este archivo existente, asegúrese primero de que se ha copiado en la carpeta %SystemRoot%\system32\dns en este servidor y haga luego clic en Siguiente.

Indicar o nome do ficheiro onde se vai almacenar toda a información sobre esta zona. Como indica na imaxe ese ficheiro vai estar gardado en: **C:\windows\system32\dns**.

- Actualización dinámica**

Puede especificar si esta zona DNS aceptará actualizaciones seguras, no seguras o no dinámicas.

Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros de recursos con un servidor DNS cuando se produzcan cambios.

Seleccione el tipo de actualizaciones dinámicas que desea permitir:

☐ Permitir sólo actualizaciones dinámicas seguras (recomendado para Active Directory)
Esta opción sólo está disponible para las zonas que están integradas en Active Directory.

☐ Permitir todas las actualizaciones dinámicas (seguras y no seguras)
Se aceptan actualizaciones dinámicas de registros de recurso de todos los clientes.
⚠ Esta opción representa un serio peligro para la seguridad porque permite aceptar actualizaciones desde orígenes que no son de confianza.

☒ No admitir actualizaciones dinámicas
Esta zona no acepta actualizaciones dinámicas de registros de recurso. Tiene que actualizar sus registros manualmente.

Por agora non admitir actualizaci3ns dinámicas. Isto verase cando se vexa o servidor DHCP, nun apartado posterior.

• Finalización del Asistente para nueva zona

Se ha completado correctamente el Asistente para nueva zona. Ha especificado la siguiente configuración:

Nombre:	wcarpediem.local
Tipo:	Primaria estándar
Tipo de búsqueda:	Reenviar
Nombre de archivo:	wcarpediem.local.dns

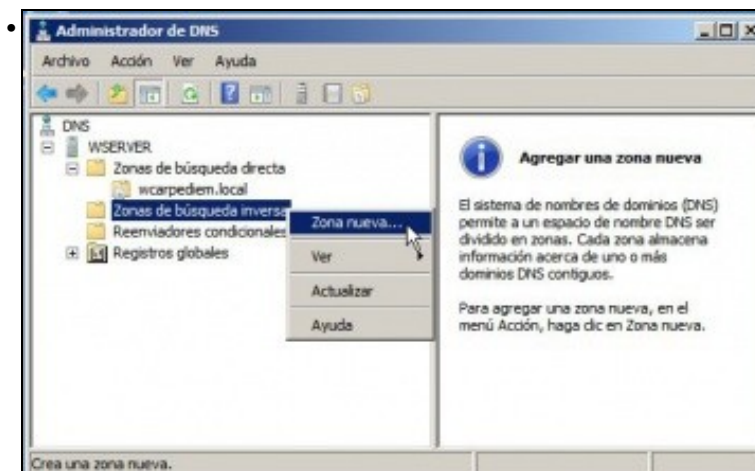
Nota: ahora debe agregar registros a la zona o asegurarse de que los registros se actualizan dinámicamente. A continuación, compruebe la resolución de nombres con nslookup.

Para cerrar este asistente y crear la zona nueva, haga clic en Finalizar.

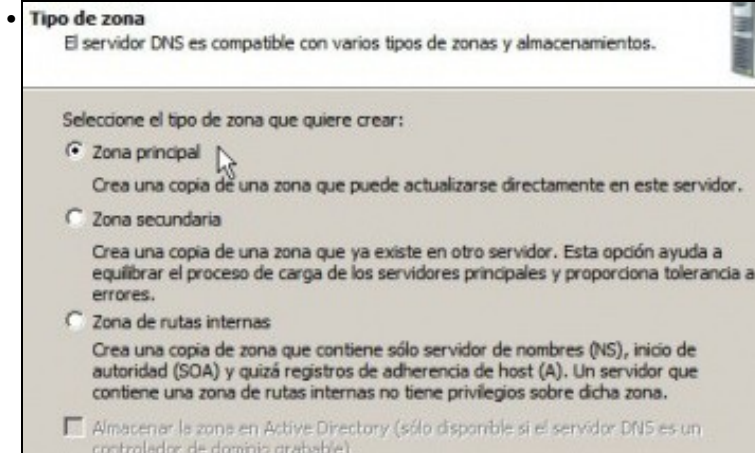
Resumo da zona a crear.

1.7 Crear zona de busca inversa para 172.16.0.0

A continuación vaise crear a zona de busca inversa para a rede **172.16.0.0**, isto é, dada unha IP que nos diga o nome do equipo do dominio asociado a esa IP.



Crear unha nova zona de busca inversa



Zona principal ...

- Nombre de la zona de búsqueda inversa**
 Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Elija si desea crear una zona de búsqueda inversa para direcciones IPv4 o direcciones IPv6.

☒ Zona de búsqueda inversa para IPv4
☐ Zona de búsqueda inversa para IPv6

Para resoluciones IPs da versión 4.

- Nombre de la zona de búsqueda inversa**
 Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Para identificar la zona de búsqueda inversa, escriba el Id. de red o el nombre de zona.

☒ Id. de red:

El Id de red es la parte de la dirección IP que pertenece a esta zona. Escriba el Id. de red en su orden normal (no en el inverso).

Si usa un cero en el Id de red, aparecerá en el nombre de la zona. Por ejemplo, el Id de red 10 crearía la zona 10.in-addr.arpa, y el Id de red 10.0 crearía la zona 0.10.in-addr.arpa.

☐ Nombre de la zona de búsqueda inversa:

Poñer o identificador da rede-IP.

- Archivo de zona**
 Puede crear un archivo de zona nuevo o usar un archivo copiado de otro servidor DNS.

¿Desea crear un archivo nuevo de zona o usar el archivo existente que copió de otro servidor DNS?

☒ Crear un archivo nuevo con este nombre de archivo:

☐ Usar este archivo:

Para usar este archivo existente, asegúrese primero de que se ha copiado en la carpeta %SystemRoot%\system32\dns en este servidor y haga luego clic en Siguiente.

Igual que no caso anterior, indicar o nome do ficheiro onde se vai almacenar toda a información relacionada con esta zona. Este ficheiro gárdase na mesma ruta que no caso anterior.

- Actualización dinámica**
 Puede especificar si esta zona DNS aceptará actualizaciones seguras, no seguras o no dinámicas.

Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros de recursos con un servidor DNS cuando se produzcan cambios.

Seleccione el tipo de actualizaciones dinámicas que desea permitir:

☐ Permitir sólo actualizaciones dinámicas seguras (recomendado para Active Directory)
 Esta opción sólo está disponible para las zonas que están integradas en Active Directory.

☐ Permitir todas las actualizaciones dinámicas (seguras y no seguras)
 Se aceptan actualizaciones dinámicas de registros de recurso de todos los clientes.
 ⚠ Esta opción representa un serio peligro para la seguridad porque permite aceptar actualizaciones desde orígenes que no son de confianza.

☒ No admitir actualizaciones dinámicas
 Esta zona no acepta actualizaciones dinámicas de registros de recurso. Tiene que actualizar sus registros manualmente.

Igual que antes non admitir actualización automáticas, xa se modificará cando se vexa DHCP.

- **Finalización del Asistente para nueva zona**

Se ha completado correctamente el Asistente para nueva zona. Ha especificado la siguiente configuración:

Nombre: 16.172.in-addr.arpa

Tipo: Primaria estándar

Tipo de búsqueda: Invertir

Nombre de archivo: 16.172.in-addr.arpa.dns

Nota: ahora debe agregar registros a la zona o asegurarse de que los registros se actualizan dinámicamente. A continuación, compruebe la resolución de nombres con nslookup.

Para cerrar este asistente y crear la zona nueva, haga clic en Finalizar.

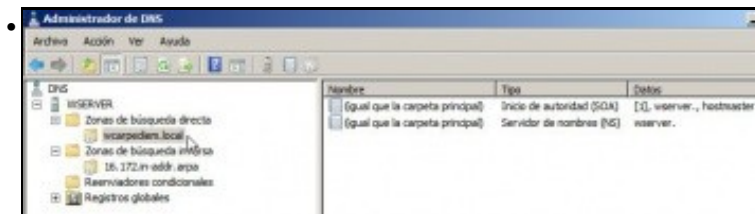
Resumo da zona a crear.



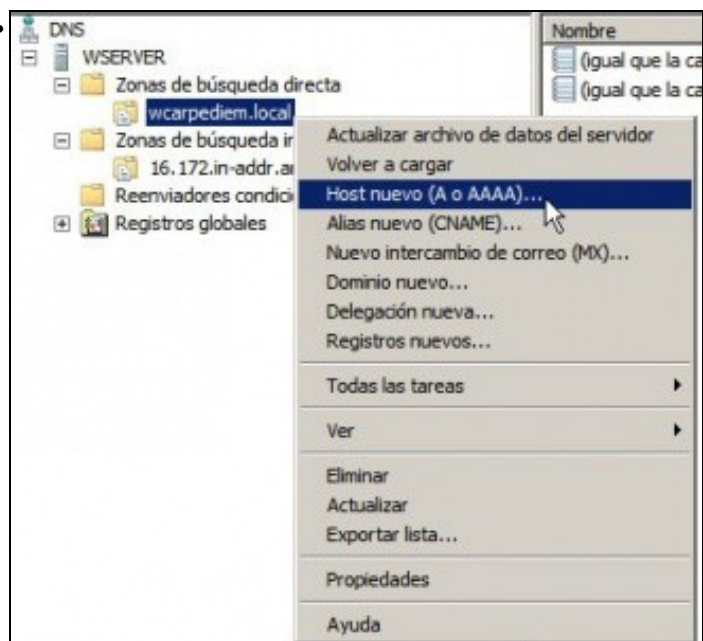
Esquema das zonas creadas.

1.8 Creación de rexistros dentro das zonas

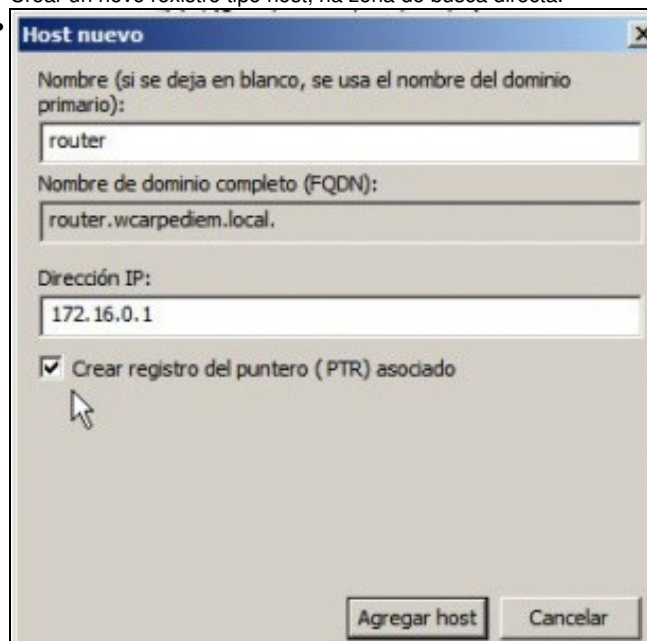
- Neste curso só se vai traballar cos rexistros tipo host (Coñecidos como A) e cos tipo PTR para a resolución inversa. Para afondar no coñecemento dos tipos de rexistro recoméndase: http://es.wikipedia.org/wiki/DNS#Tipos_de_registros_DNS.



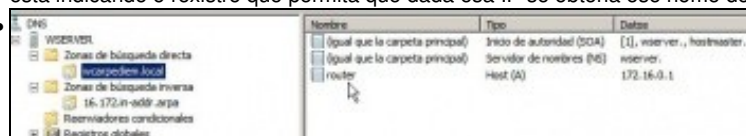
Observar que unha vez creadas as zonas hai uns rexistros creados por defecto.



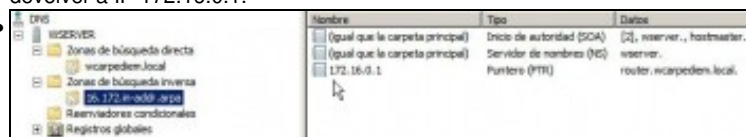
Crear un novo rexistro tipo host, na zona de busca directa.



Imos comezar creando un host calquera, por exemplo **router** que apunte á IP do router (172.16.0.1). O nome podería ser calquera outro. O importante é que dado ese nome imos obter unha IP. Ademais pregunta se desexamos que se cree na zona inversa asociada á IP que se está indicando o rexistro que permita que dada esa IP se obteña ese nome de dominio, neste caso: router.



Unha vez creado o rexistro, vese na zona de busca directa, que a partir de agora a quen pregunte por **router.wcarpediem.local** váiselle devolver a IP 172.16.0.1.



Pola contra, a quen pregunte por cal é o nome de dominio asociado a **172.16.0.1** váiselle devolver **router.wcarpediem.local**

```
Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>ping router.wcarpediem.local

Haciendo ping a router.wcarpediem.local [172.16.0.1] con 32
bytes de datos:
Respuesta desde 172.16.0.1: bytes=32 tiempo=1ms TTL=128
Respuesta desde 172.16.0.1: bytes=32 tiempo=1ms TTL=128
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 172.16.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

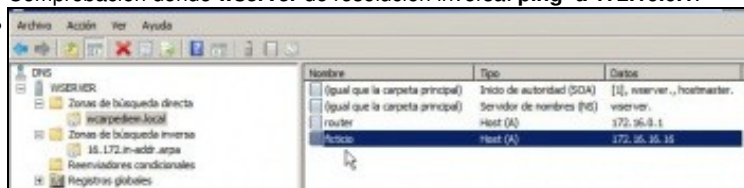
Comprobación desde **wserver** de resolución directa: **ping router.wcarpediem.local**.

```
Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>ping -a 172.16.0.1

Haciendo ping a router.wcarpediem.local [172.16.0.1] con 32
bytes de datos:
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.0.1: bytes=32 tiempo=1ms TTL=128
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.0.1: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 172.16.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Comprobación desde **wserver** de resolución inversa: **ping -a 172.16.0.1**.



Podese crear o que se desexe. Por exemplo un host chamado **ficticio** con IP que non ten ningún equipo da LAN: **172.16.16.16**. Crear tamén o rexistro de busca inversa (PTR).

```
Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>ping ficticio.wcarpediem.local -n 1

Haciendo ping a ficticio.wcarpediem.local [172.16.16.16] con
32 bytes de datos:
Respuesta desde 172.16.0.110: Host de destino inaccesible.

Estadísticas de ping para 172.16.16.16:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
        (0% perdidos),
```

Comprobar como o servidor DNS resolve ben: **ping ficticio.wcarpediem.local**, pero claro logo o ping non funciona porque non hai ningún equipo con IP 172.16.16.16, pero o que importa é que o servidor DNS fixo o seu traballo.

```
Seleccionar Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>ping -a 172.16.16.16 -n 1

Haciendo ping a ficticio.wcarpediem.local [172.16.16.16] con
32 bytes de datos:
Respuesta desde 172.16.0.110: Host de destino inaccesible.

Estadísticas de ping para 172.16.16.16:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
        (0% perdidos),
```

O mesmo coa resolución inversa: **ping -a 172.16.16.16**

```
Seleccionar Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>ping wserver -4 -n 1

Haciendo ping a wserver [172.16.0.110] con 32 bytes de datos
:
Respuesta desde 172.16.0.110: bytes=32 tiempo<1m TTL=128

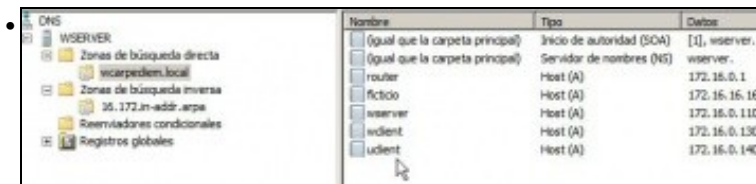
Estadísticas de ping para 172.16.0.110:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Pero que pasa co propio nome do servidor: **wserver**?. Se se pregunta polo nome a secas, faise a resolución correctamente, porque se está usando outro protocolo de Windows: **NetBIOS** sobre TCP/IP, e non TCP/IP puro e duro. O parámetro **-4** indica que se faga o ping usando a versión 4 do protocolo IP.

```
Seleccionar Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>ping wserver.wcarpediem.local -4 -n 1

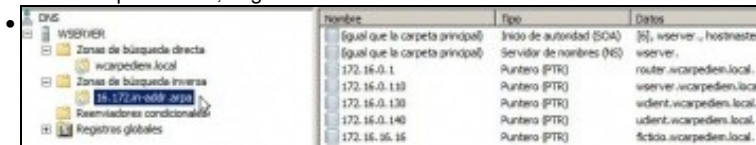
La solicitud de ping no pudo encontrar el host wserver.wcarpediem.local. Compruebe el nombre y vuelva a intentarlo.
```

Pero se se fai ping a **wserver.wcarpediem.local**, o cliente DNS de **wserver**, pregunta ao servidor DNS que el mesmo ten instalado, e na zona que xestiona non ten ningún host chamado **wserver**.

- 

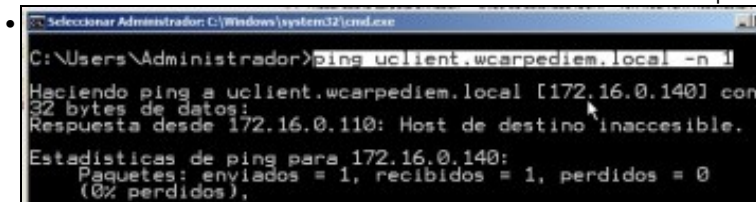
Nombre	Tipo	Datos
(igual que la carpeta principal)	Inicio de autoridad (SOA)	[1], wserver.,
(igual que la carpeta principal)	Servidor de nombres (NS)	wserver.
router	Host (A)	172.16.0.1
ficticio	Host (A)	172.16.16.16
wserver	Host (A)	172.16.0.110
uclient	Host (A)	172.16.0.130
uclient	Host (A)	172.16.0.140

Ben, pois procedamos a dar de alta na zona de busca directa (e na inversa) os rexistros asociados a **wserver**, **wclient** e **uclient** coas súas IPs correspondentes, segundo o escenario.

- 

Nombre	Tipo	Datos
(igual que la carpeta principal)	Inicio de autoridad (SOA)	[6], wserver., hostmaster
(igual que la carpeta principal)	Servidor de nombres (NS)	wserver.
172.16.0.1	Puntero (PTR)	router.wcarpediem.local
172.16.0.110	Puntero (PTR)	wserver.wcarpediem.local
172.16.0.130	Puntero (PTR)	uclient.wcarpediem.local
172.16.0.140	Puntero (PTR)	uclient.wcarpediem.local
172.16.16.16	Puntero (PTR)	ficticio.wcarpediem.local

Este é o resultado de crear os hosts na zona de busca directa anterior e que ao mesmo tempo creara o rexistro PTR asociado.

- 

```

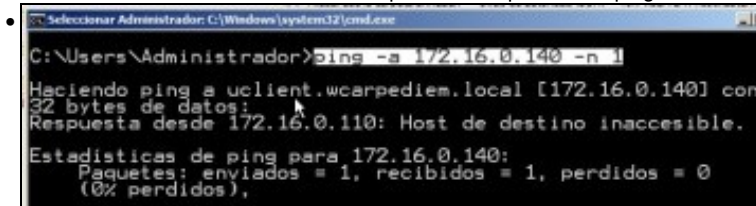
C:\Users\Administrador>ping uclient.wcarpediem.local -n 1

Haciendo ping a uclient.wcarpediem.local [172.16.0.140] con
32 bytes de datos:
Respuesta desde 172.16.0.110: Host de destino inaccesible.

Estadísticas de ping para 172.16.0.140:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 0
    (0% perdidos),

```

A estas alturas **uclient** aínda está apagado e non configurado, co cal se dende **wserver** se fai un ping a **uclient.wcarpediem.local** o servidor DNS resolverá correctamente pero non se pode facer ping ao cliente porque está apagado.

- 

```

C:\Users\Administrador>ping -a 172.16.0.140 -n 1

Haciendo ping a uclient.wcarpediem.local [172.16.0.140] con
32 bytes de datos:
Respuesta desde 172.16.0.110: Host de destino inaccesible.

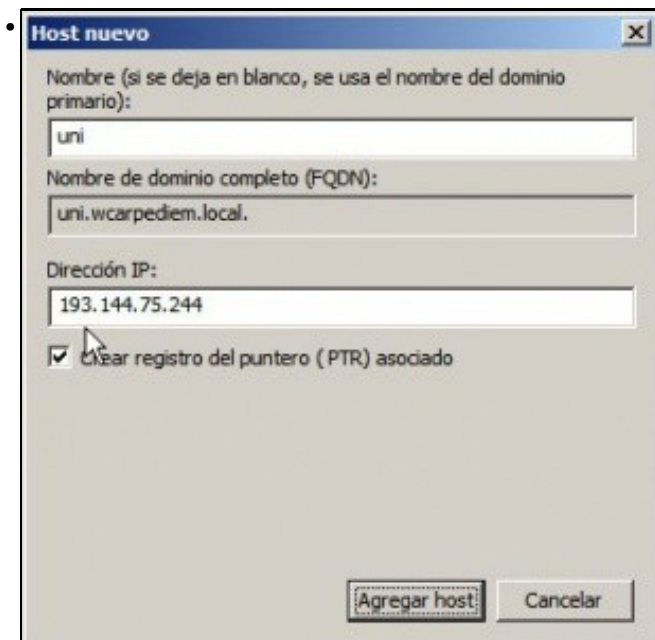
Estadísticas de ping para 172.16.0.140:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 0
    (0% perdidos),

```

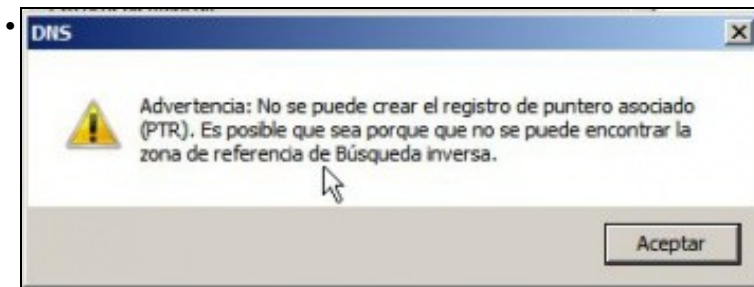
A resolución inversa tamén funciona correctamente.

1.8.1 Creación de rexistros con asociacións a IPs fóra da LAN

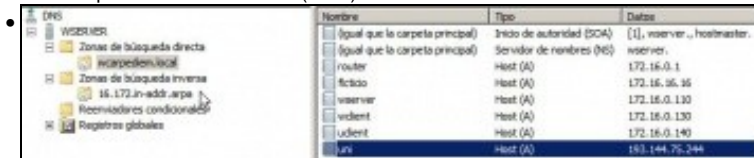
- Nesta ocasión vaise facer unha asociación dun nome de dominio de **wcarpediem.local** cunha IP dun servidor que non está na LAN. Neste caso facendo un **ping** a **www.usc.es** obtense a IP: 193.144.75.244

- 

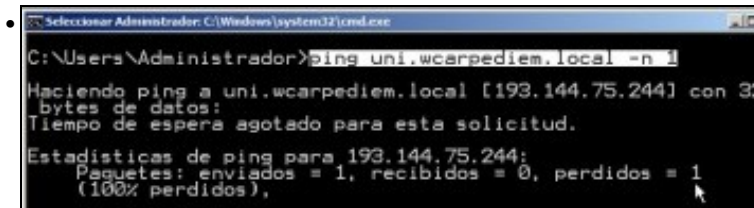
Crear un rexistro na zona de busca directa **wcarpediem.local** chamado **uni** e coa IP: 193.144.75.244.



Como non hai creada ningunha zona de busca inversa para a rede IP: 102.144.75.0, por iso nos dá un aviso de que non vai poder crear o rexistro para a busca inversa (PTR).



O rexistro creado na zona de busca directa.



Comprobar que o servidor resolve correctamente.



E nun navegador en **wserver** indicar a url: **uni.wcarpediem.local** e *voilà* aí está a páxina da Universidade. Pero ollo!!, isto é porque o servidor web da USC non está configurado para que haxa que poñerlle exactamente **www.usc.es** para que funcione. Recórdese tamén que para que este paso funcione correctamente debemos configurar o navegador para que non saia a internet a través do servidor proxy, porque senón sería o proxy o que resolvería o nome da URL.

1.9 Para fondar máis sobre DNS en Windows



PODES CONSULTAR...

Se desexas consultar como configurar en Windows zonas DNS secundarias, alias, balanceo de carga, etc, podes consultar:

- [Transparencias 14 a 40 do PDF sobre Servizos de Internet en Windows](#)

Para afondar no mesmo é preciso ter as nocións de táboas de enrutamento que se recollen en:

- [Transparencias 114 a 129 do PDF sobre modelo OSI / TCP-IP](#)

