

Escenario completo 5.E - Solución

Sumario

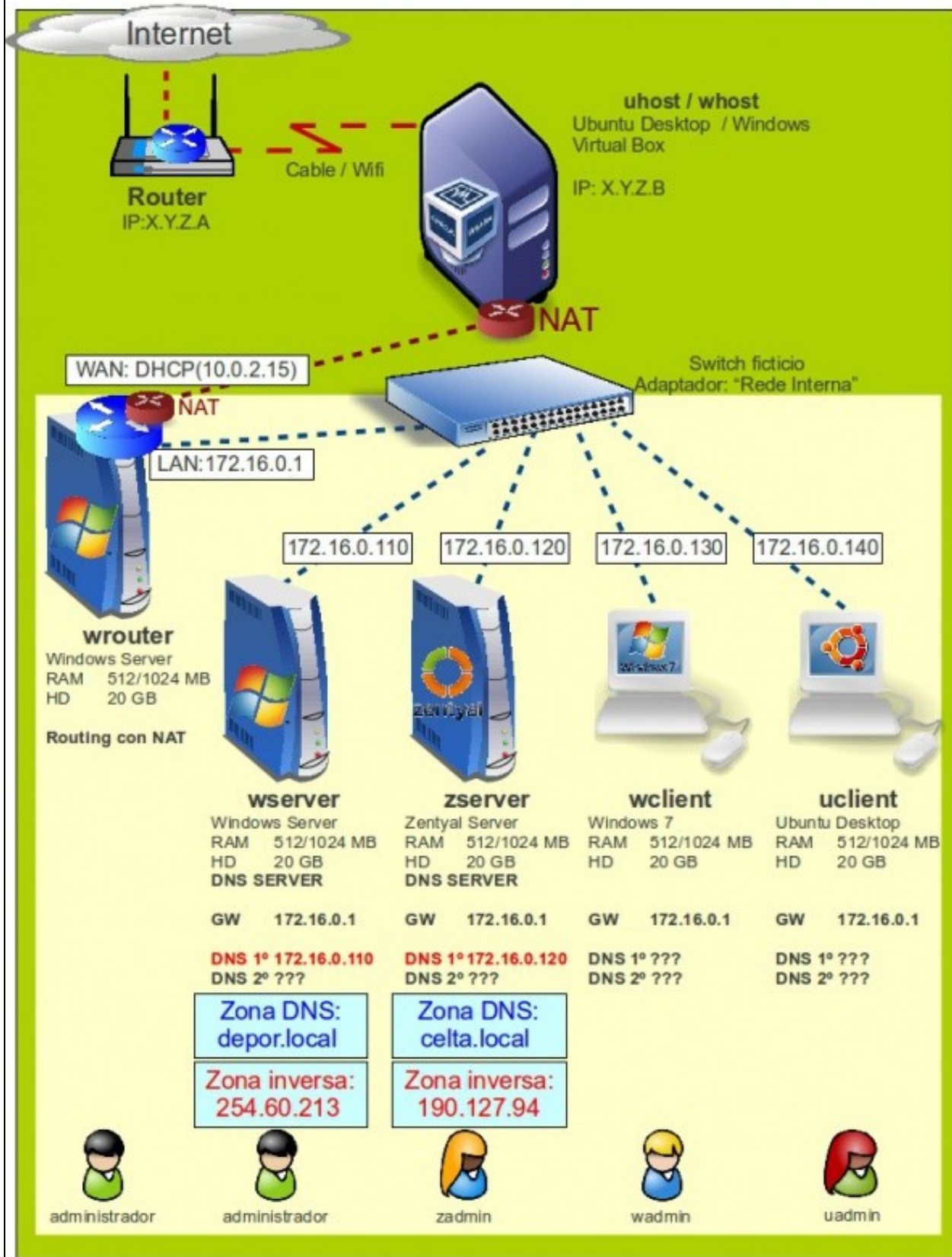
- 1 Introducción
- 2 Configuración básica servidores
- 3 Solución incorrecta: Configuración clientes DNS
- 4 Solución básica correcta: reenvío simple
 - ◆ 4.1 wserver como reenviador
 - ◆ 4.2 zserver como reenviador
- 5 Solución complexa correcta (Non recomendada): reenvío cruzado
- 6 Solución complexa non correcta: reenvío cruzado
- 7 Solución ideal: servidores secundarios

Introdución

- A continuación vaise aplicar o **principio de Pareto** á resolución do **Escenario completo 5.E**.
- Vanse ver distintas solucións:
 - ◆ Unha incorrecta que é a que se desexa evitar e é a primeira de todas.
 - ◆ A solución sinxela e recomendada para cando xurdan problemas detectalos máis facilmente.
 - ◆ Unhas solucións complexas e pouco recomendadas pola súa complexidade á hora de detectar problemas.
 - ◆ Unha solución ideal, que é usando servidores secundarios pero que non se viron no curso.
- Antes de continuar, o usuario debe distinguir claramente entre as partes servidor e cliente do servizo DNS:
 - ◆ **Servidor DNS**: é o que resolve (ben consultando nas zonas que xestiona ou ben preguntando a outros servidores DNS) nomes de dominio a IPs e viceversa (se hai zonas de busca inversa).
 - ◆ **Cliente DNS**: é o que pregunta á un ou varios servidores DNS por un nome de dominio para obter a súa IP (ou viceversa).
 - ◆ Aquí é importante facer notar que todo servidor DNS tamén é cliente DNS, pero a configuración cliente DNS dun servidor só afecta ás consultas que se inician desde el e non afecta para nada ao servidor DNS que nel estea instalado.

Configuración básica servidores

Escenario 5.E_1: Configuración básica de Servidores

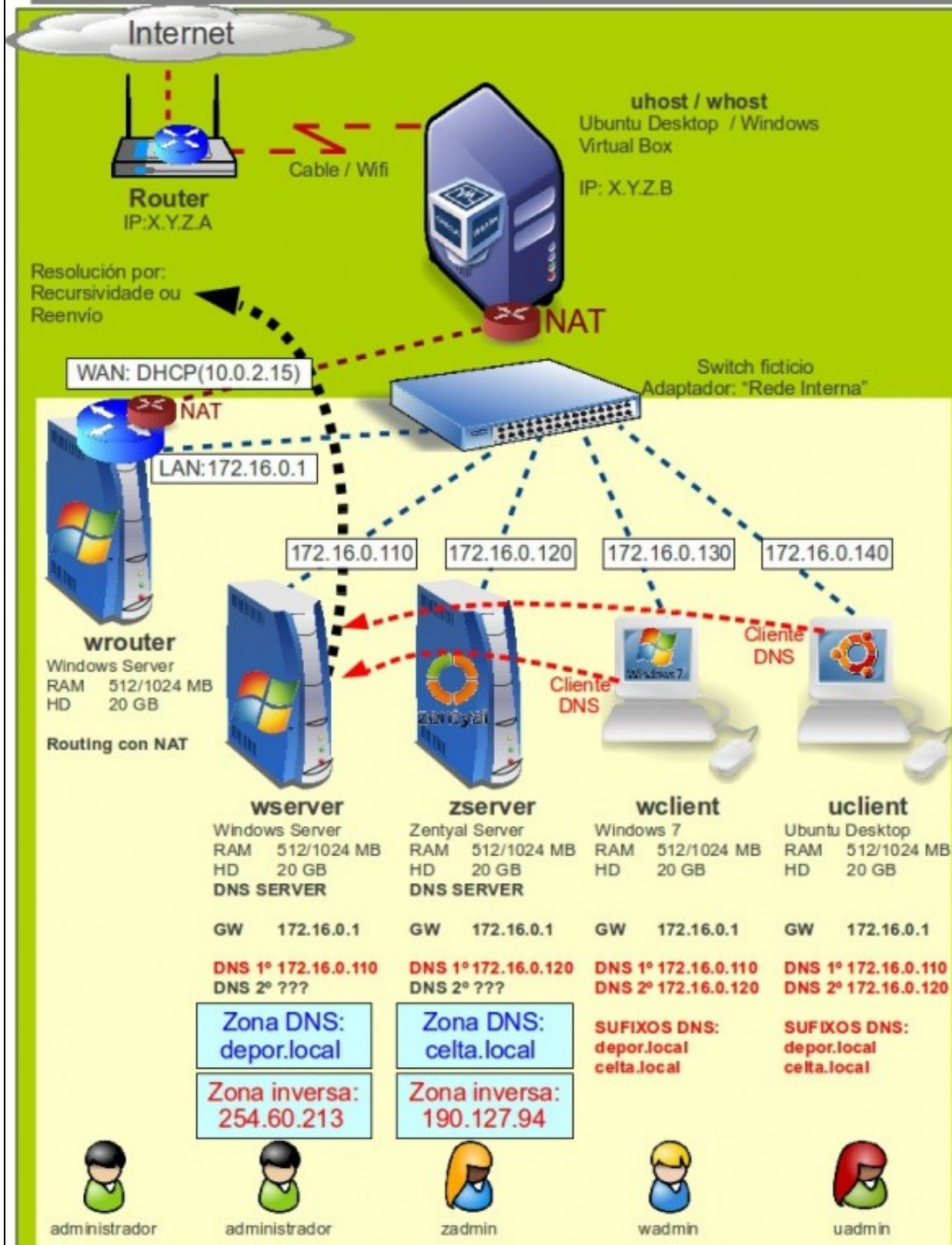


- O primeiro que se faría sería configurar os servidores:
- **wserver** crear as zonas:
 - ◆ de busca directa: depor.local
 - ◆ de busca inversa: aquí hai varias opcións que depende de como as cre o usuario, pero todas válidas:
 - ◇ Opción 1: 213
 - ◇ Opción 2: 60.213
 - ◇ Opción 3: 254.60.213
- **zserver** crear as zonas:
 - ◆ de busca directa: olimpia.local
 - ◆ de busca inversa xa a crea automaticamente Zentyal cando se dan os hosts de alta.
- Por agora non se fixo ningunha configuración do cliente DNS.

Solución incorrecta: Configuración clientes DNS

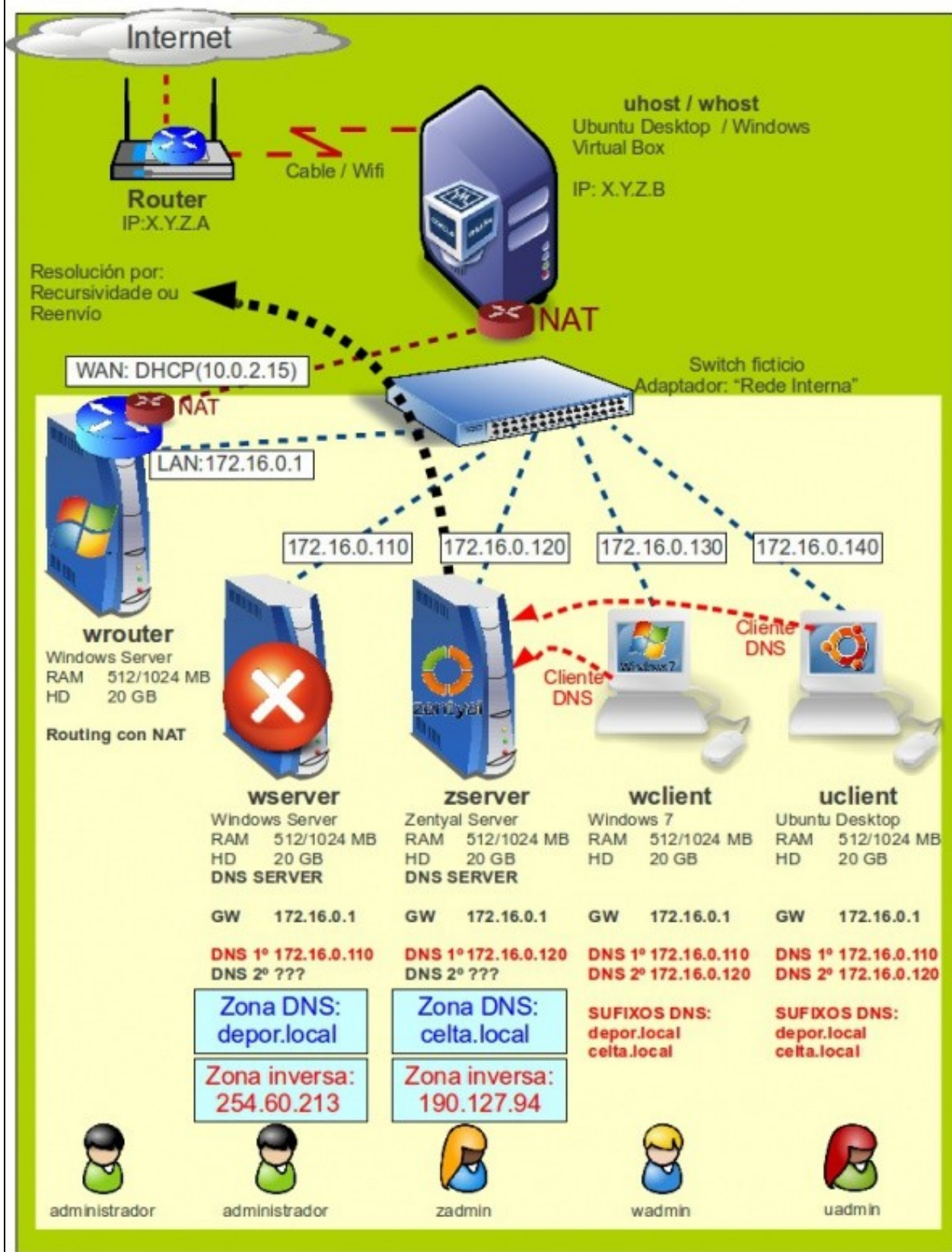
- Nestas imaxes vese como están configurados (cor vermello) os clientes DNS.

Escenario 5.E_2A: Solución Incorrecta: DNS de wserver ACCESIBLE celta.local INALCANZABLE.



- **Servidores:** cada un deles apuntaría a si mesmo.
- **wclient e ulclient:**
 - ◆ DNS primario: 172.16.0.110
 - ◆ DNS alternativo: 172.16.0.120
 - ◆ Para este caso tamén valería cambiando o primario polo alternativo.
 - ◆ Sufixos DNS: depor.local, celta.local
- Pero esta configuración de cliente DNS primario e alternativo ten problemas:
 - ◆ "celta.local" nunca será alcanzable mentres o servizo DNS de **wserver** estea accesible. Por que?.
 - ◇ Porque cando **uclient**, por exemplo, faga ping a **balaidos.celta.local**, este consultará ao servidor DNS primario, 172.16.0.110 neste caso. O servidor DNS **wserver** mira nas súas zonas de busca directa e non ten **celta.local**, co cal mira na súa cache e tampouco atopa nada. Finalmente **wserver** consulta ao exterior, ben reenviando ao ISP ou aos servidores raíz por recursividade. Pero fóra tampouco saben nada de **celta.local**. Co cal **wserver** vaille responder aos clientes que **balaidos.celta.local** non existe. E iso é co que se quedan os clientes, non van a consultar a un servidor alternativo, porque en boa lóxica teríalle que dicir o mesmo, que **balaidos.celta.local** non existe.
- Cando un cliente DNS fai uso do DNS alternativo?. Cando o servidor DNS primario non estea accesible:
- Razóns polas que un servidor DNS pode estar non accesible:
 - ◆ Cable de rede do servidor desconectado.
 - ◆ Servidor apagado.
 - ◆ Servizo DNS parado.
 - ◆ Firewall que non permite consultas DNS.
 - ◆ Servidor DNS miles de causas...
- A seguinte imaxe amosa que **wserver** non é accesible, por calquera das razóns anteriores.

Escenario 5.E_2B: Solución Incorrecta: DNS de wserver NON ACCESIBLE



- Neste caso, o mesmo cliente de antes **uclient**, pregunta por **balaidos.celta.local** ao servidor DNS primario, 172.16.0.110 e tras esperar un tempo non recibe ningunha resposta de **wserver**, nin positiva, nin negativa. É neste caso, entón, cando o cliente pasa a preguntar ao servidor DNS secundario/alternativo, 172.16.0.120.
- Neste caso **zserver** é consultado, si que xestiona **celta.local** e dentro ten un equipo **balaidos** co cal devólvelle a IP a **uclient**.
- **Problemas desta solución**
 - ♦ Se os 2 servidores están accesibles hai unha das zonas que non é accesible.
 - ♦ Se o servizo DNS de **wserver** non está accesible obtéñense resultados distintos a cando está accesible e iso non ten senso.

- **Conclusión**

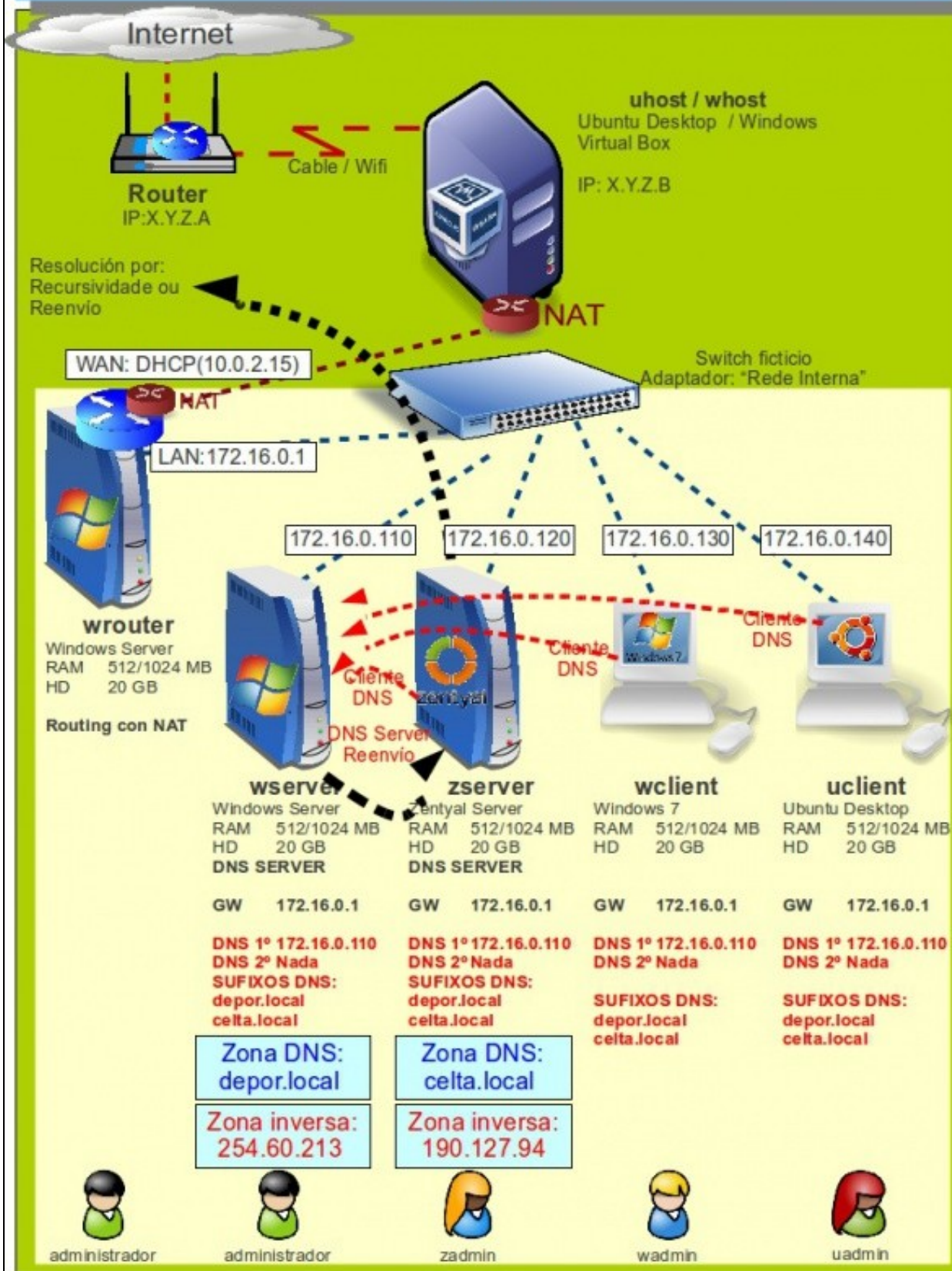
- ♦ Esta solución é a que se desexa evitar. Se a configuración cliente DNS apunta a servidores que non teñen a mesma información, ou que non xestionan as mesmas zonas, obtéñense resultados erráticos.

Solución básica correcta: reenvío simple

- A solución é moi simple:
 - ♦ Toda configuración cliente DNS apunta a un dos servidores.
 - ♦ O servidor elixido no paso anterior reenvía ao outro servidor.

wserver como reenviador

Escenario 5.E_3A: Solución Correcta 1: DNS wserver reenvía a DNS zserver



- **wclient e uclient:**

- ♦ Só configurar o DNS primario que apunte a 172.16.0.110

- **wserver:**

- ♦ **Servizo servidor DNS:** configuralo para que reenvíe ao servidor DNS 172.16.0.120
- ♦ **Cliente DNS:** só configurar o DNS primario apuntando a se mesmo. Engadir os sufixos DNS **depor.local** e **celta.local**.

- **zserver:**

- ♦ **Servizo servidor DNS:** non tocalo ou configuralo para que reenvíe aos servidores DNS do ISP.
- ♦ **Cliente DNS:** só configurar o DNS primario apuntando a **wserver** ou que apunte a se mesmo, todo depende se desde este servidor se van lanzar consultas sobre o dominio **depor.local**. Engadir os **sufixos DNS depor.local** e **celta.local**. O primeiro valerá a pena se se configura o cliente DNS para consultar a 172.16.0.120.
- ♦ Observar que se está a falar de que a configuración cliente DNS zserver apunte ou non a wserver, pero esta decisión só afecta para as preguntas que se inician dende zserver e non afecta para nada aos demais clientes da rede que estes só preguntan aos sevizos DNS dos servidores.

- **Resolución de problemas**

- ♦ Neste caso a configuración é moi sinxela para manexar mentalmente por calquera administrador.
- ♦ Os clientes non resolven nomes internos nin externos: entón o servizo DNS de **wserver** non está accesible.
- ♦ Os clientes resolven nomes internos, pero non externos: hai problemas en no servizo DNS de **zserver**.

- **Conclusión:**

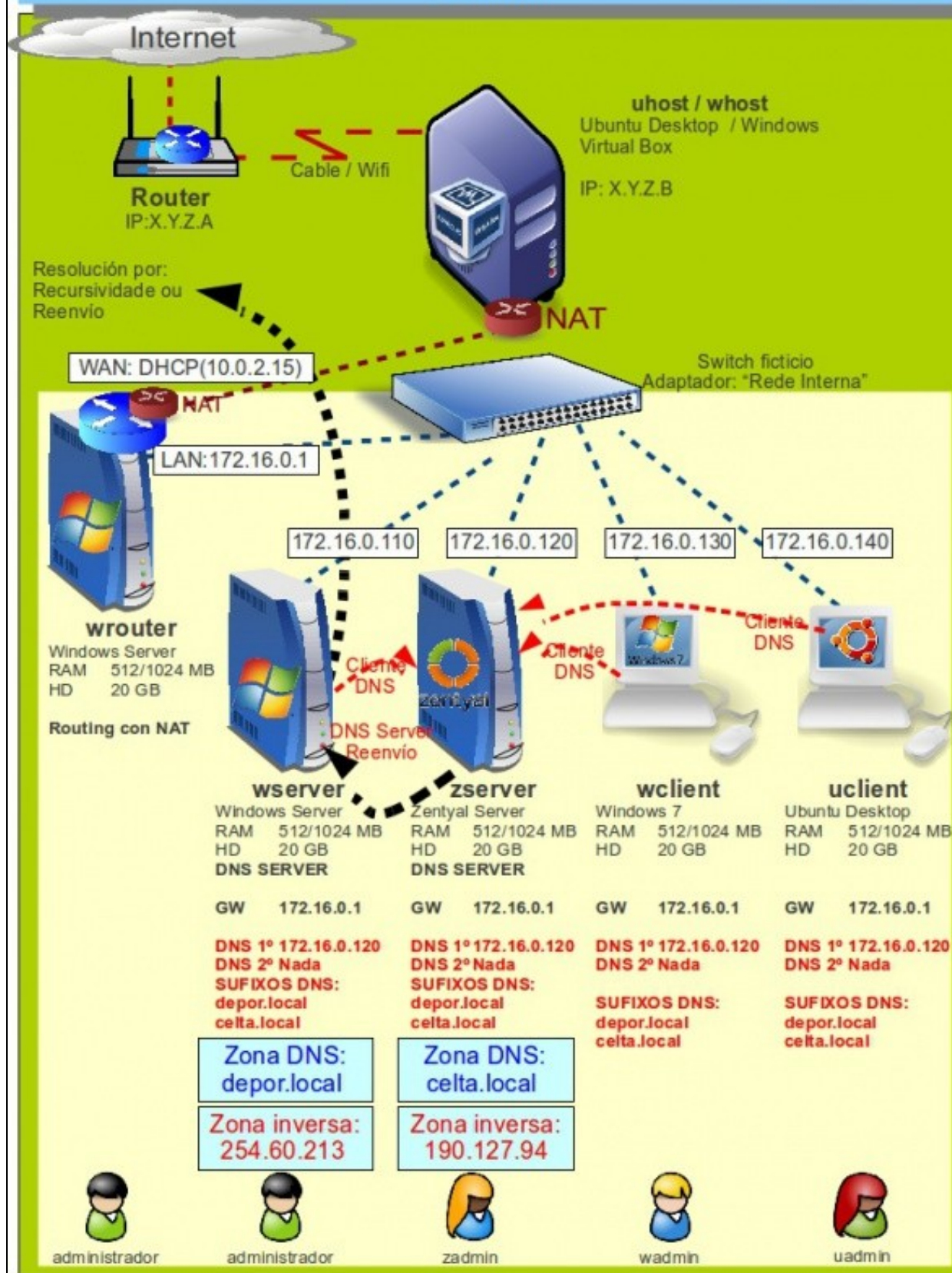
- ♦ Esta é a solución máis axeitada, cos servidores que se teñen, pois é moi sinxela na implantación e por tanto ante un fallo calquera de resolución DNS é fácil detectar onde está o problema.

- Agora xa só quedaría implantar a configuración deste escenario ou o da seguinte imaxe nas MVs.

zserver como reenviador

- Este escenario é o mesmo que o anterior, coa diferenza, de que quen actúa como reenviador é **zserver** e todo cliente DNS primario pregunta a 172.16.0.120.

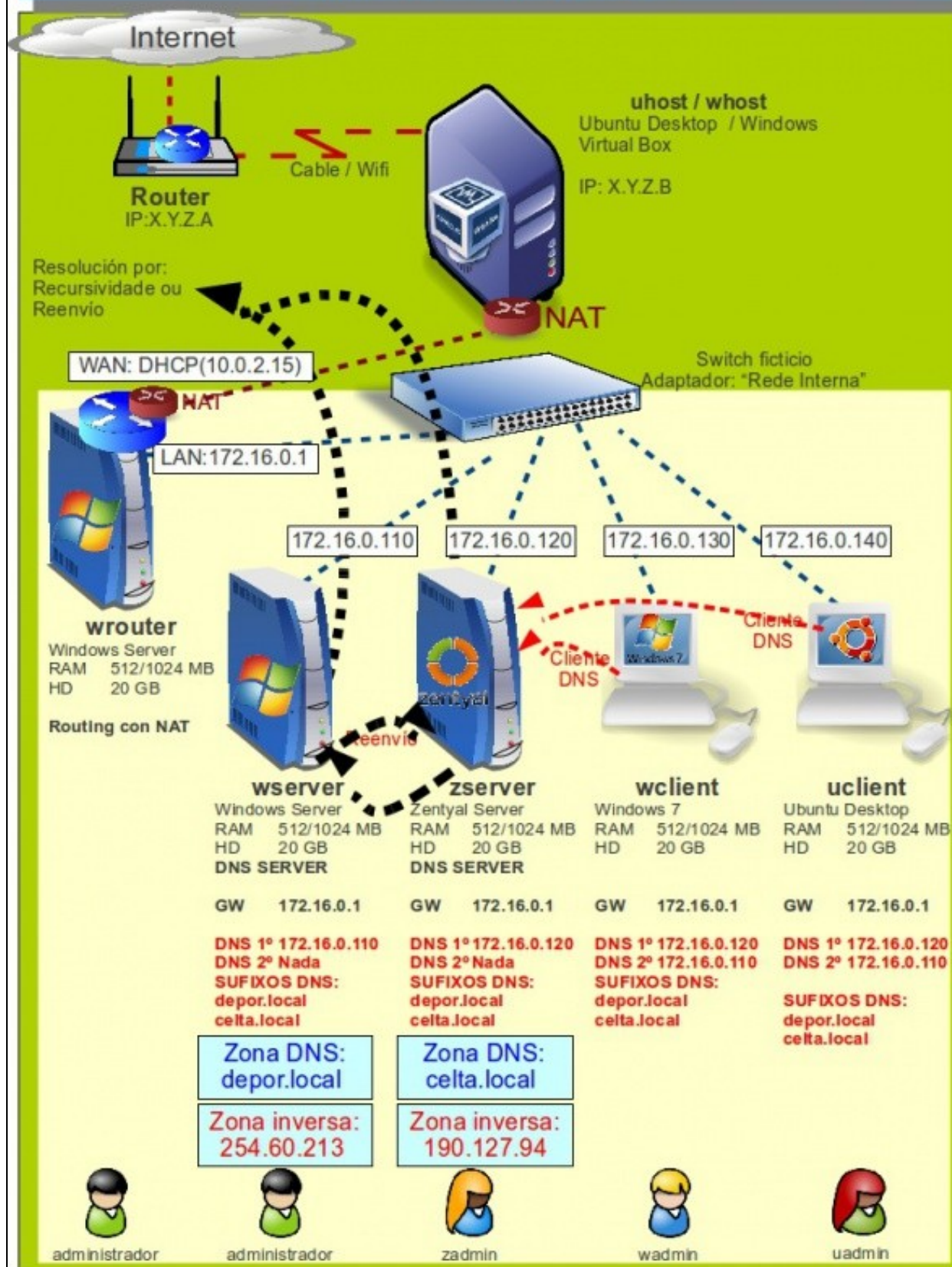
Escenario 5.E_3B: Solución Correcta 2: DNS zserver reenvía a DNS wserver



Solución complexa correcta (Non recomendada): reenvío cruzado

- A solución que se vai ver a continuación proporciona algo de redundancia para o acceso ao exterior. Está baseada na mistura da primeira e da segunda solucións anteriores.

Escenario 5.E_4A: Solución Compleja Correcta: zserver e wserver reenvío cruzado. zserver ACCESIBLE



- **wclient e uclient:**

- ♦ Servidor DNS primario: 172.16.0.120
- ♦ Servidor DNS secundario: 172.16.0.110
- ♦ Poderíanse cambiar os servidores anteriores de orde.

- **wserver e zserver:**

- ♦ Servizo DNS: configurar o reenviador de cada servidor para enviar ao servidor contrario.
- ♦ Cliente DNS: configurar cada servidor para que se consulte a si mesmo.

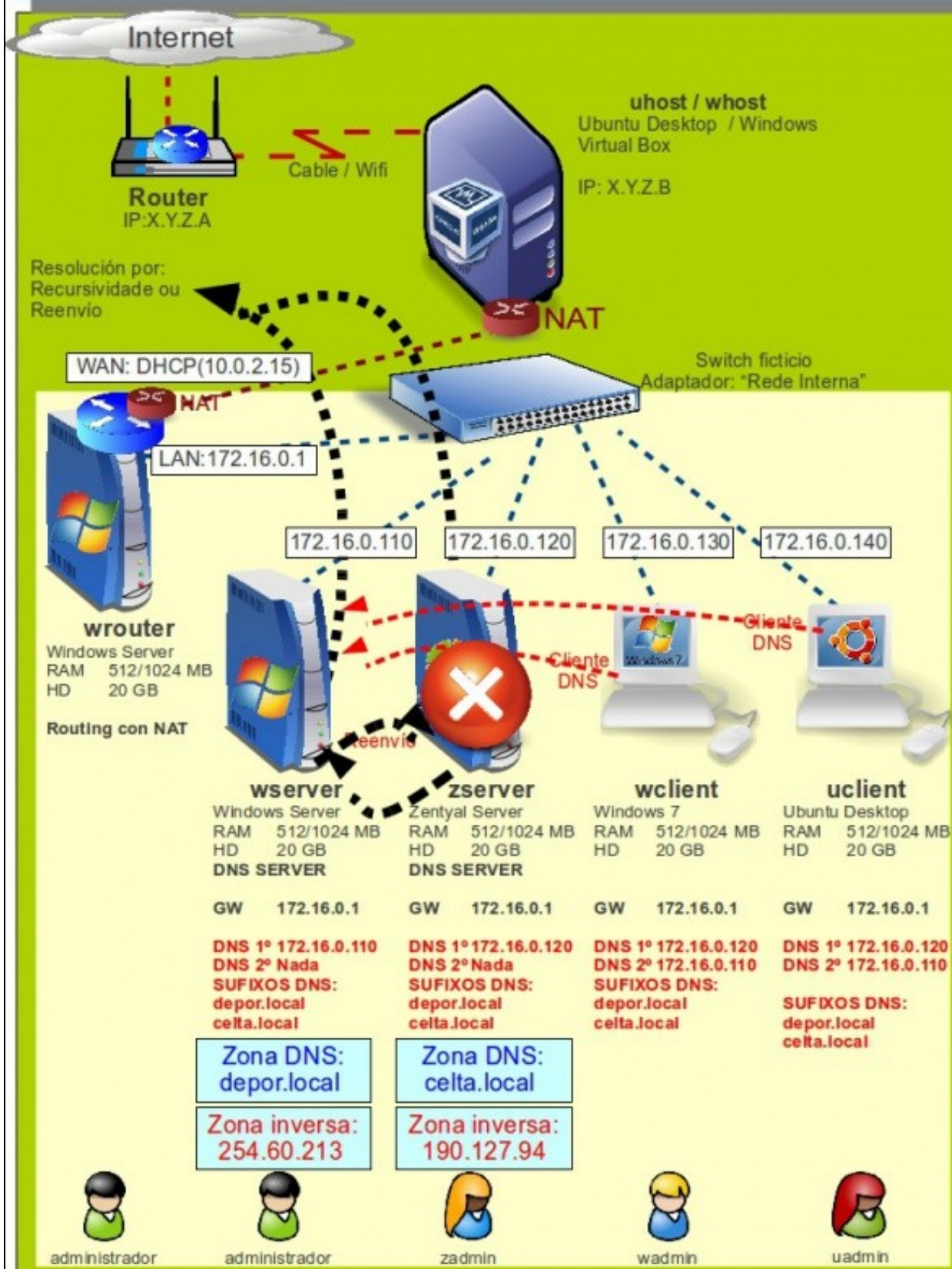
- **Problemas**

- ♦ Neste escenario hai un lazo nos servidores, que ante unha consulta de resolución dun nome externo, estes comézanse a pasar a pelota un ao outro, pero como, por defecto, cando se reenvía unha consulta o reenviador abre un temporizador para recibir unha resposta, se non a recibe ningunha resposta no tempo establecido pois reenvía ao seguinte reenviador (se hai) ou realiza a consulta por recursividade a través dos servidores raíz.

- **Vantaxes:**

A seguinte imaxe amosa unha vantaxe (que á par tamén é un inconveniente). Se fallase o servizo DNS do servidor 172.16.0.120 non estivera accesible, os clientes pasarían a preguntar ao servidor DNS secundario, co cal seguiría tendo a posibilidade de resolver nomes do exterior.

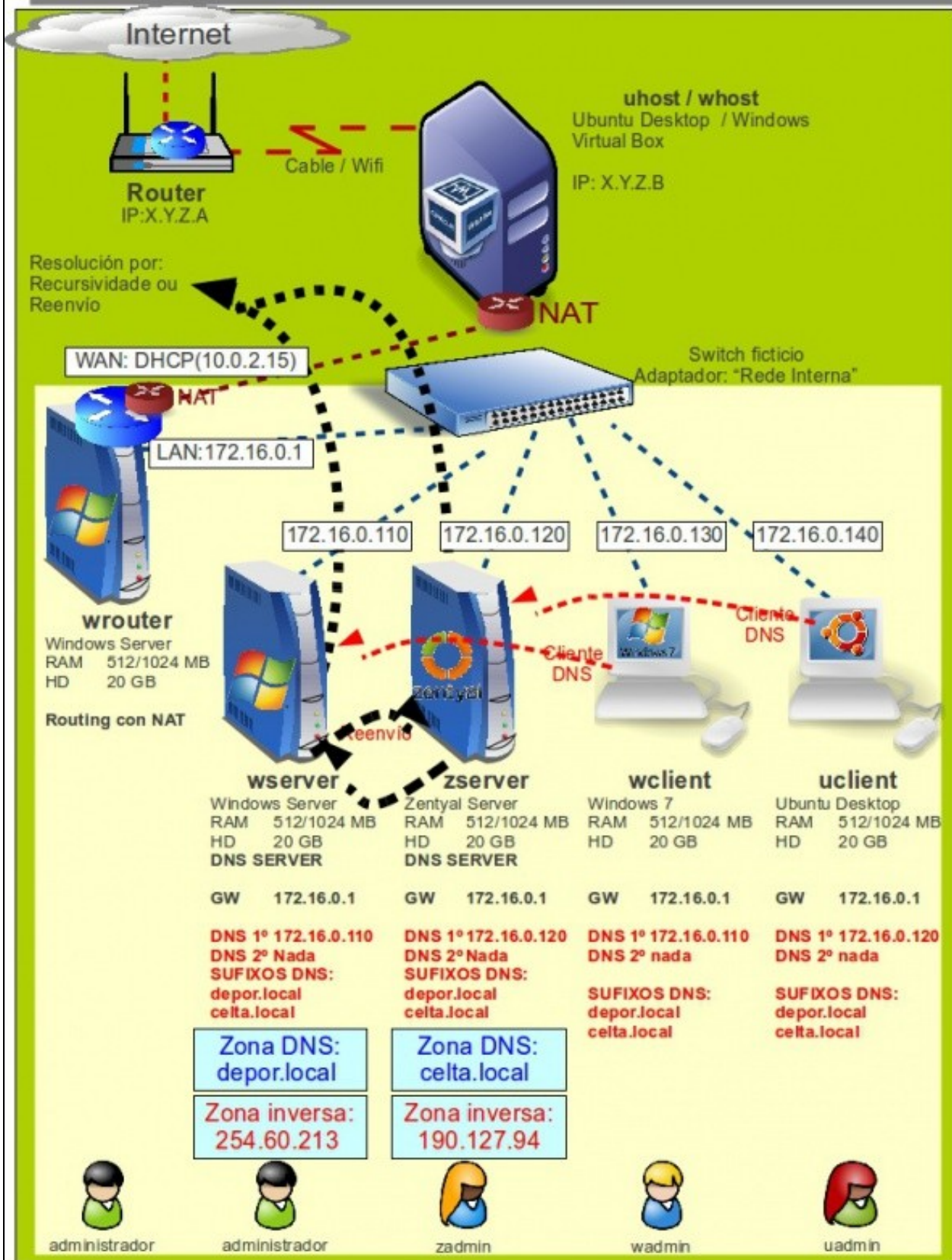
Escenario 5.E_4B: Solución Compleja Correcta: zserver e wserver reenvío cruzado. zserver NON ACCESIBLE



Solución complexa non correcta: reenvío cruzado

- Baseada na solución anterior, alguén podería pensar en balancear a carga entre os servidores, de xeito que uns clientes pregunten a un servidor e outros clientes a outros.

Escenario 5.E_5: Solución Compleja, que funciona, pero difícil detectar que sucede cando un Servidor DNS non está Accesible .

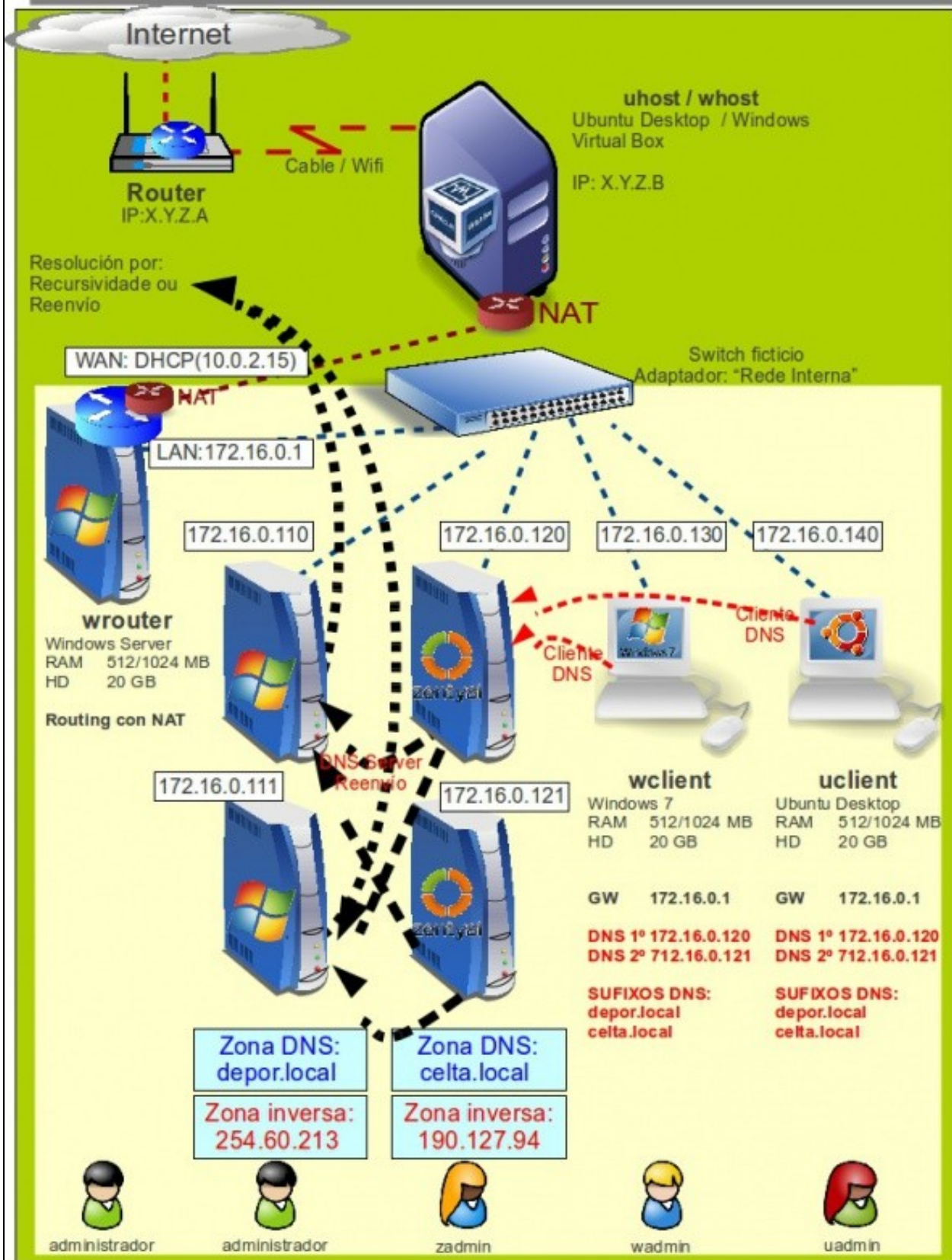


- Isto ten un problema, que se pasa pasado un tempo, os administradores teñen que estar moi áxiles. Por exemplo, se o servizo DNS de **zserver** non estivese accesible, habería clientes na rede que resolverían nomes DNS e outros non, coa cal, a reacción inicial é para volverse louco.
- **Conclusión:** cando algo falle é mellor que se vexan todos afectados para á hora diagnosticar o problema sexa moito máis rápido que se uns equipos teñen un problema e outros non.

Solución ideal: servidores secundarios

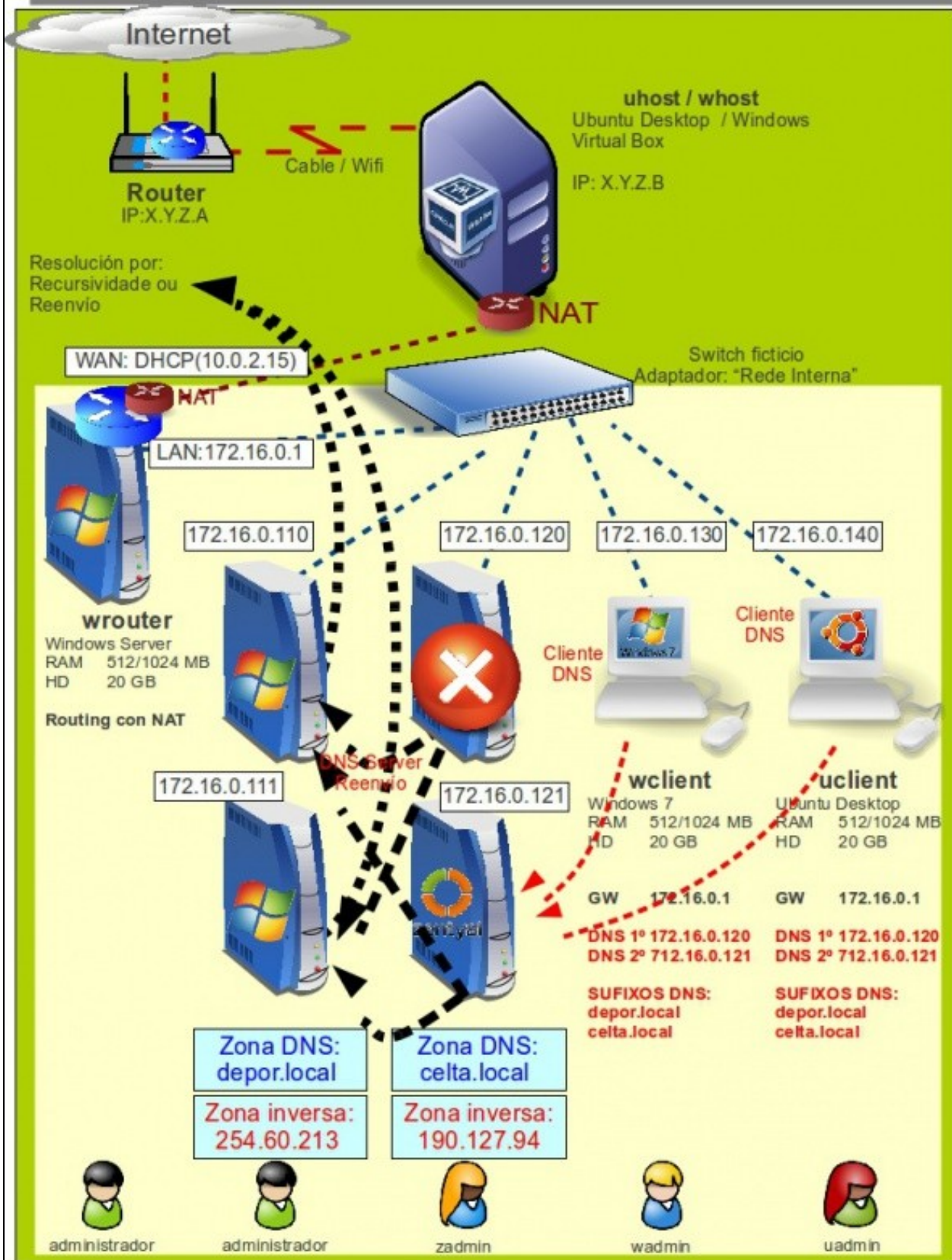
- Esta configuración non se viu no curso.
- Consiste en facer un servidor backup (secundario) de cada un dos servidores primarios.
- Un servidor secundario ten unha copia do servidor principal. E un servidor principal en Windows pode ter un servidor secundario en Linux e viceversa.
- Na seguinte imaxe, de cada servidor primario hai un servidor secundario.
- Agora escóllese que parella de servidores (Primario e secundario) vai actuar como reenviador á outra parella, neste caso escolleuse como servidores reenviadores 172.16.0.120 e 172.16.0.121 para reenviar aos outros 2 servidores: 172.16.0.110 e 172.16.0.111 . Podería ser ao revés.

Escenario 5.E_6A: Solución Ideal: Zonas Secundarias. Zserver - 1 ACCESIBLE



- Observar que agora todo cliente apunta a 2 servidores que conteñen a mesma información e xestionan as mesmas zonas. Neste caso, servidor DNS primario 172.16.0.120 e servidor DNS secundario 172.16.0.121.
- Que pasa en caso de que o servizo DNS do servidor primario non estea accesible?.

Escenario 5.E_6B: Solución Ideal: Zonas Secundarias. zserver - 1 NON ACCESIBLE



- Pois que os clientes preguntarán a un servidor secundario que ten a mesma información que o servidor primario.