

Configuración da rede en XenServer: Interfaces, Ponte, Bonding, Rede Interna Privada

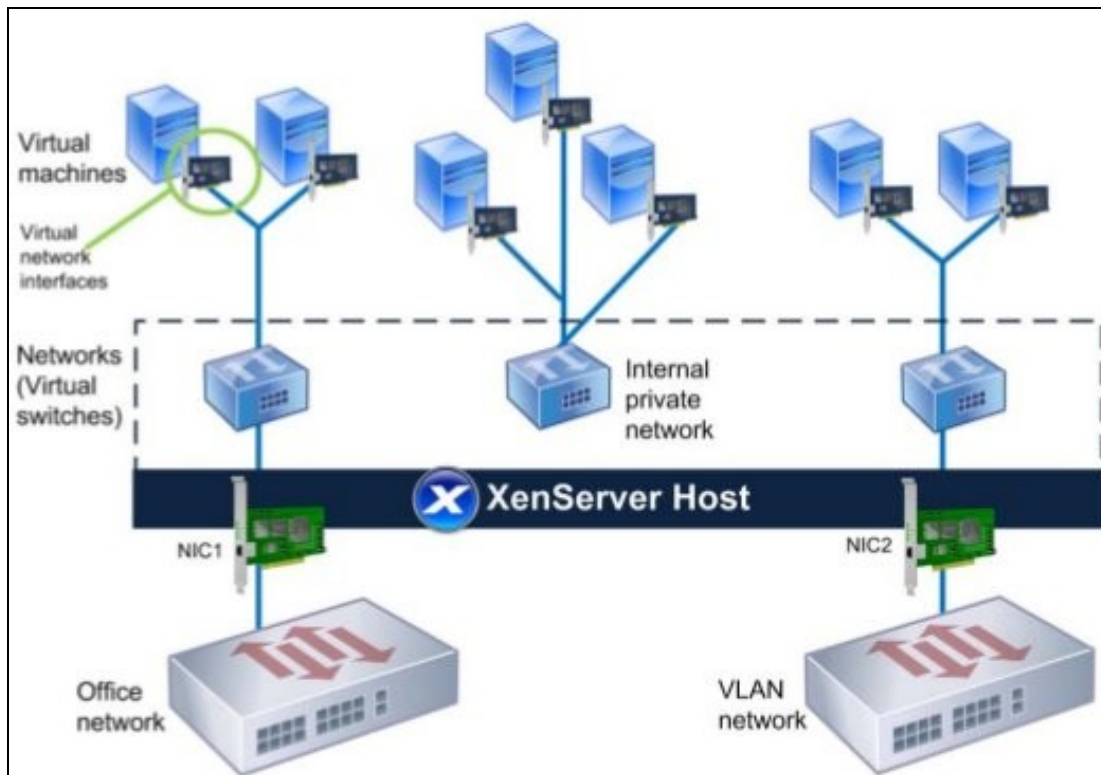
Sumario

- 1 Introducción
 - ◆ 1.1 Tipos de redes
 - ◆ 1.2 Tipos de tráfico: Interface de xestión, Tráfico MVs, Tráfico de Almacenamento
 - ◆ 1.3 Caso práctico sobre interfaces e redes
- 2 Agregación/Bonding
 - ◆ 2.1 Introducción
 - ◇ 2.1.1 Bonding activo-activo
 - ◇ 2.1.2 Bonding activo-pasivo
 - ◇ 2.1.3 Bonding LACP
 - ◆ 2.2 Caso práctico en XenServer
 - ◇ 2.2.1 Experimentación ante fallos
 - ◇ 2.2.2 Desfacer un bonding
- 3 Rede externa VLAN
- 4 Tráfico das MVs
- 5 Rede privada interna (solitaria)
 - ◆ 5.1 Caso práctico: Crear unha DMZ
 - ◇ 5.1.1 Script de configuración de iptables
- 6 Engadir un novo interface a un host
- 7 Tráfico de almacenamento
 - ◆ 7.1 Configuración da NAS
 - ◆ 7.2 Configuración de XenServer
- 8 Conclusión final sobre a xestión das redes en XEN

Introdución

- O que vén a continuación é unha parte extensa e con varias casuísticas.
- Búscase presentar ao usuario distintas formas de configurar a rede en XEN, para que cando se remate o seu estudio se poida analizar cal se adapta mellor aos seus intereses reais presentes e futuros.
- No caso do Bonding, vaise realizar nunha ocasión, para amosar o seu funcionamento, e logo non se vai usar máis neste material, pero o usuario poderá sacar conclusións de en que situacións o podería usar.
- Quen desexe afondar sobre este asunto pode consultar:
 - ◆ A guía dos administradores: http://docs.vmd.citrix.com/XenServer/6.2.0/1.0/en_gb/reference.html#networking.
 - ◆ Guía avanzada de deseño da rede en XenServer: http://support.citrix.com/servlet/KbServlet/download/27046-102-666250/XS-design-network_advanced.pdf
 - ◆ Deste último enlace foron tomadas as imaxes de deseño da rede en XS que se amosan a continuación.

Tipos de redes

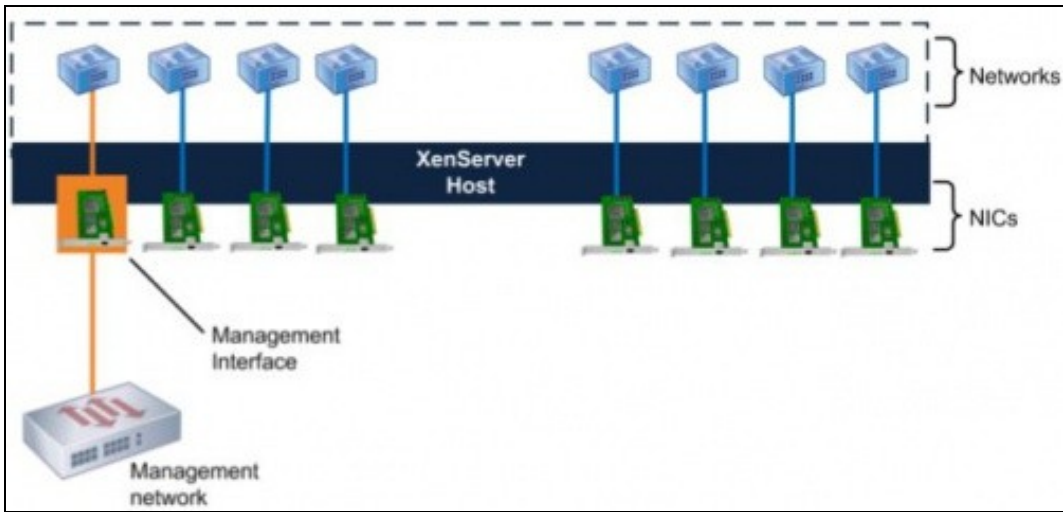


- Esta imaxe condensa a filosofía da xestión da rede de XenServer:
 - ◆ **Tarxetas físicas [NICs (Network Interface Card)]**, chamadas **PIF** (Physical Interface) serven para unir o host coa infraestrutura de rede da organización. Conéctanse aos switches xeralmente.
 - ◆ **Rede (Network) Externa**: Sobre cada NIC (PIF) XEN constrúe unha Rede/Switch que equivale a un Switch Virtual interno. Recibe o nome de **xenbrX** (XenBridge número X)
 - ◆ **VIF (Virtual Interface)**: as tarxetas de rede (virtuais) que se asocian a cada MV.

- - ◆ O nivel intermedio **Rede/Network/Switch Virtual/xenbr** actúa de intermediario entre a tarxeta real (**NIC/PIF**) e as tarxetas asociadas a cada MV (**VIFs**).
 - ◆ **VLAN**: outro tipo **Rede/Network/Switch Virtual/xenbr** chámase VLAN, e créase para que estea asociada a unha **VLAN** concreta do interface físico e non a toda a NIC.
 - ◆ **Rede privada virtual (solitaria)**: aquelas **Redes/Network/Switch Virtual/xenbr** que non están asociadas a ningún interface físico (NIC/PIF).
 - ◇ En similitude con VirtualBox equivale á configuración **Rede Interna** que se pode realizar nun adaptador de rede.
 - ◇ As redes privadas non permiten a Migración de MVs nun pool, para iso están:
 - ◆ Existe un cuarto tipo de redes chamado: **Cross-server Private** que permite a comunicación entre MVs de distintos hosts cuxas VIFs están asociadas a redes privadas. Este tipo non se vai ver neste curso.

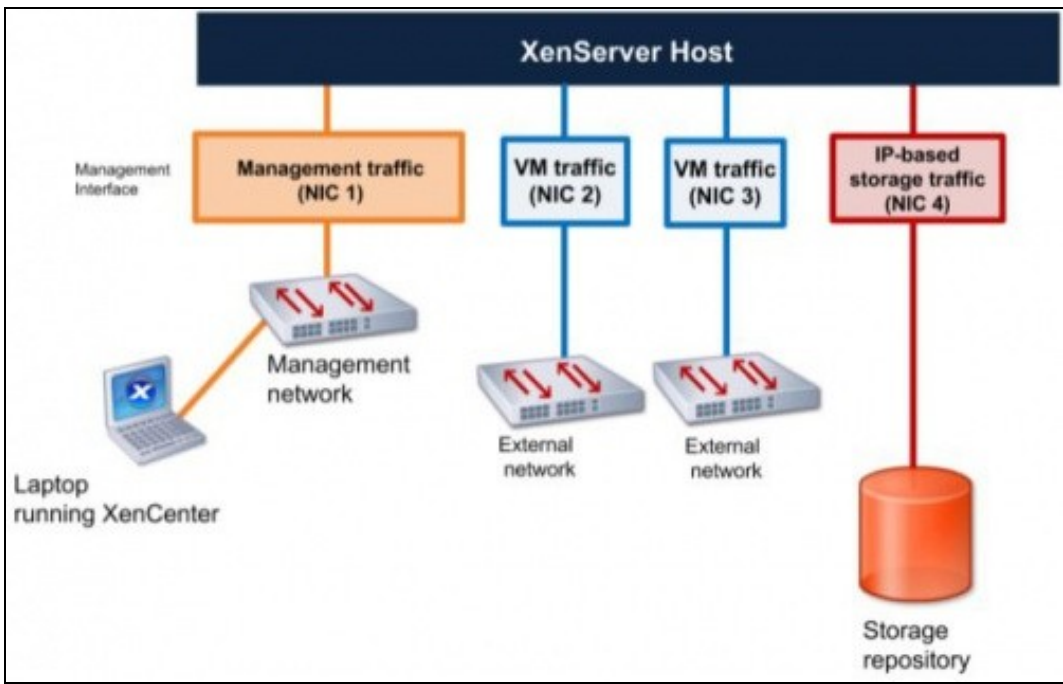
Tipos de tráfico: Interface de xestión, Tráfico MVs, Tráfico de Almacenamento

- A continuación preséntanse os tipos de tráfico que se poden ter en XEN: xestión, MVs e almacenamento.



• **Tráfico de xestión:**

- ◆ Refírese ao tráfico que se xera para administrar o host, migración de MVs, intercomunicación entre hosts nun Pool.
- ◆ Todo host debe ter un interface de xestión: **Management interface**.
- ◆ Se so hai un interface, este será o Management interface.
- ◆ Só pode haber un interface de xestión, aínda que este pode estar en Bonding.
- ◆ Debe ter unha **configuración IP**.
- ◆ Aconsellable ter unha rede física LAN para este tráfico, que non interfira co tráfico que xeran as MVs e o almacenamento.



- **Tráfico das MVs:**

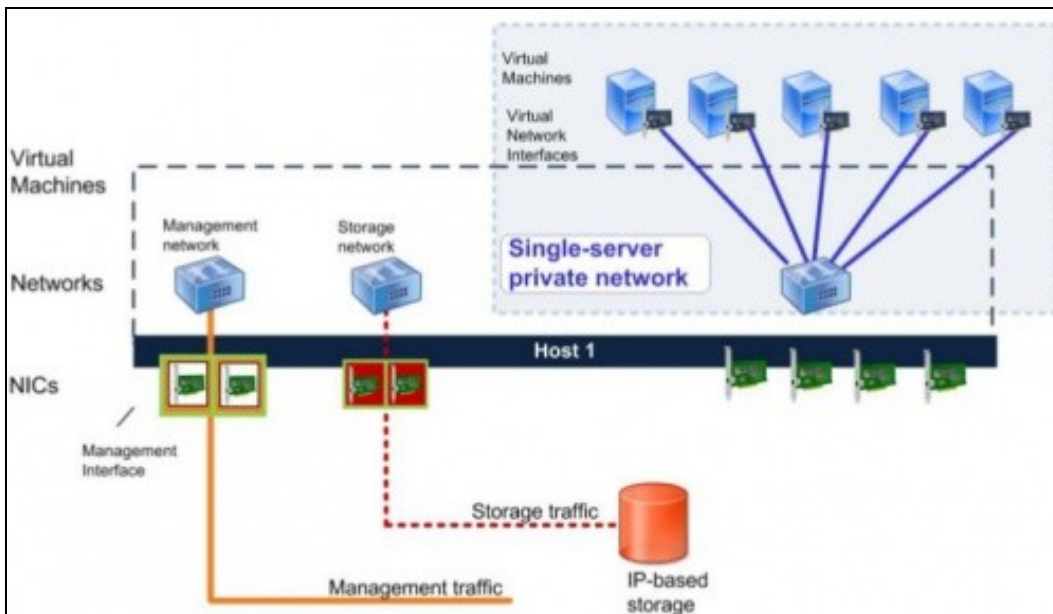
- ◆ Este tipo de tráfico sairá das MVs a través de algún NIC/PIF.
- ◆ Eses NICs/PIFs non precisan configuración IP, pois por aí só circula tráfico asociado ás VIFs das MVs. Isto é, tráfico das MVs.
- ◆ Pode haber varios NICs/PIFs para este tipo de tráfico, en función das necesidades e das posibilidades da organización.

- **Tráfico de almacenamento:**

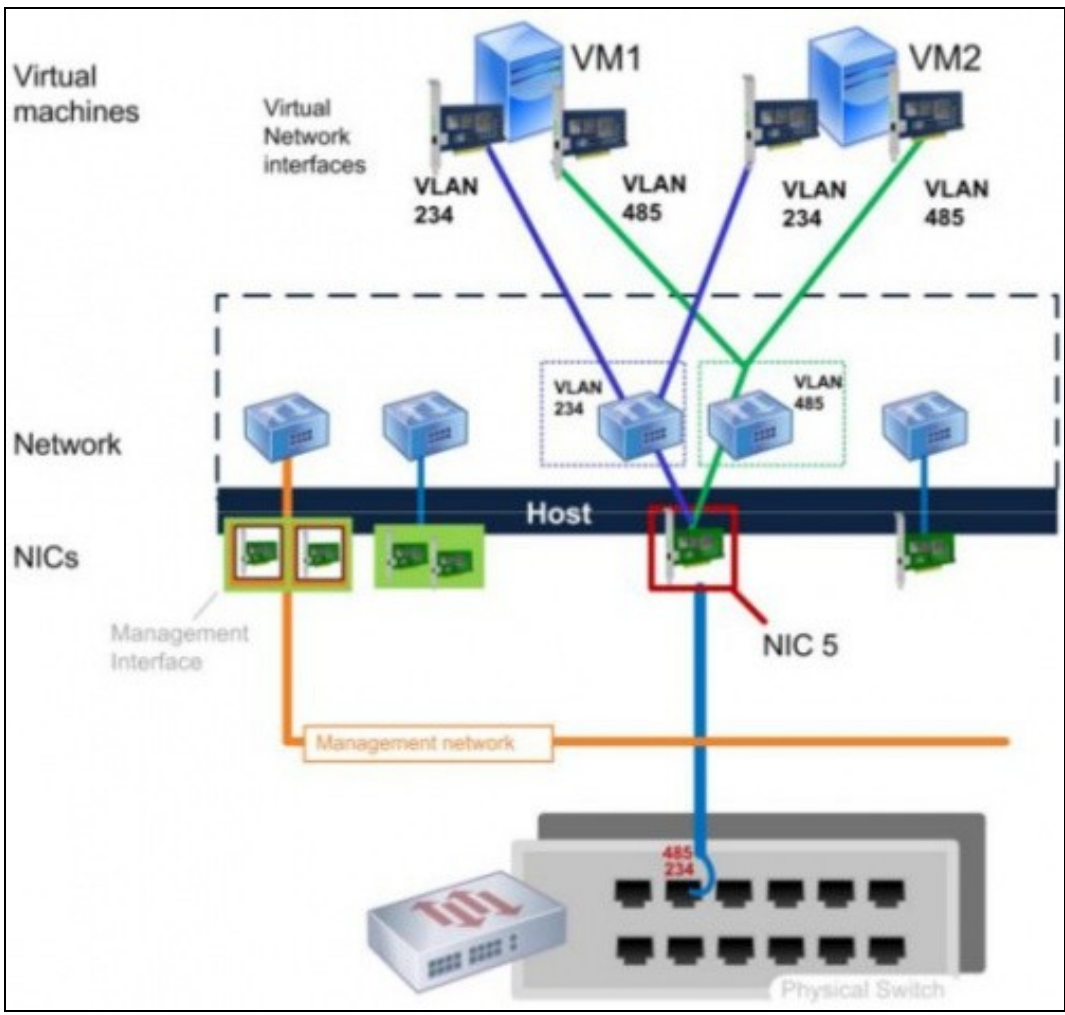
- ◆ É o tráfico que se orixina no host cando:
 - ◇ se almacenan externamente os discos das MVs,
 - ◇ os repositorios de Imaxes ISO, realización de copias de seguridade, etc.
- ◆ Este tipo de tráfico pode ser: NFS, SAMBA ou iSCSI.
- ◆ As NICs asociadas a este tipo de tráfico deben ter configuración IP, para poder comunicarse cos recursos externos de almacenamento.

- Neste dous últimos casos, se só hai unha NIC o tráfico das MVs e de almacenamento irán polo mesmo NIC que o de xestión.
- A configuración desexable sería ter, como mínimo, un NIC para cada tipo de tráfico. Isto é, dispor como mínimo de 3 NICs.

- Un pequeno resumo do visto:



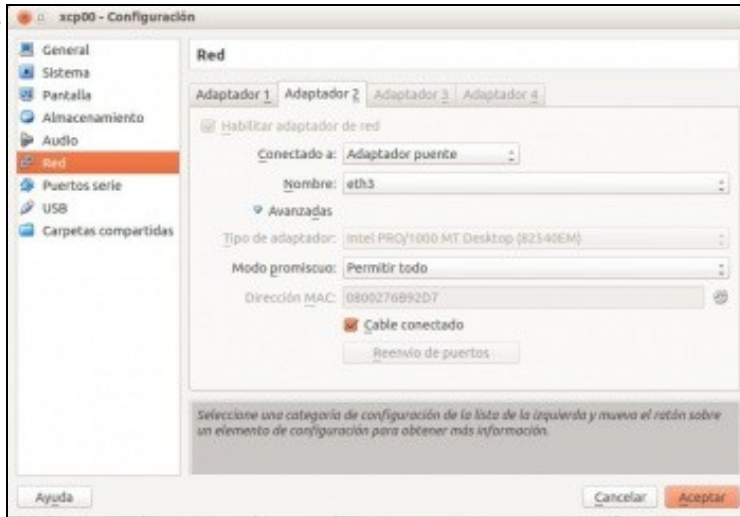
- Observar nesta imaxe como os tráficos de xestión (Management) e de almacenamento (Storage) están sobre NICs agregados nun Bonding.
- Tamén hai unha **Rede interna /switch virtual**, que ten vinculadas as **VIFs** de varias MVs e estas non teñen saída ao exterior, só se comunican entre elas.



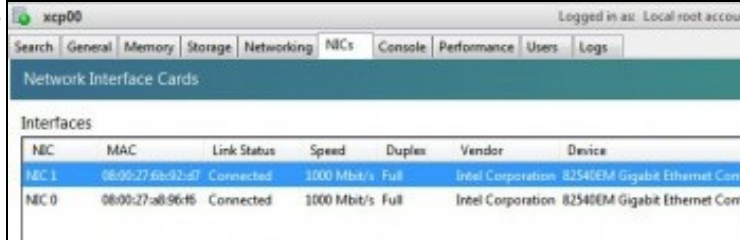
- Neste caso o tráfico de xestión está sobre NICs agregados nun Bonding.
 - O switch físico ten 2 VLANs (485, 234).
 - O host/servidor xen creou dúas **Redes Externas /Switches Virtuais** para cada unha das VLANs e sobre esa rede externa asignáronse VIFs (tarxetas de rede virtuais) ás MVs.
- A continuación vaise poñer en práctica o visto anteriormente: tipos de redes e tráfico.

Caso práctico sobre interfaces e redes

- Lembrar que o host **xen00** ten 2 NICs
- Interfaces e redes



Lembrar que xen00 instalárase con 2 NICs. Noutro caso engadir un segundo adaptador de rede en modo **Ponte/Promiscuo total**



Na lapela **NICs** de XenCenter pódense ver as 2 tarxetas de rede.

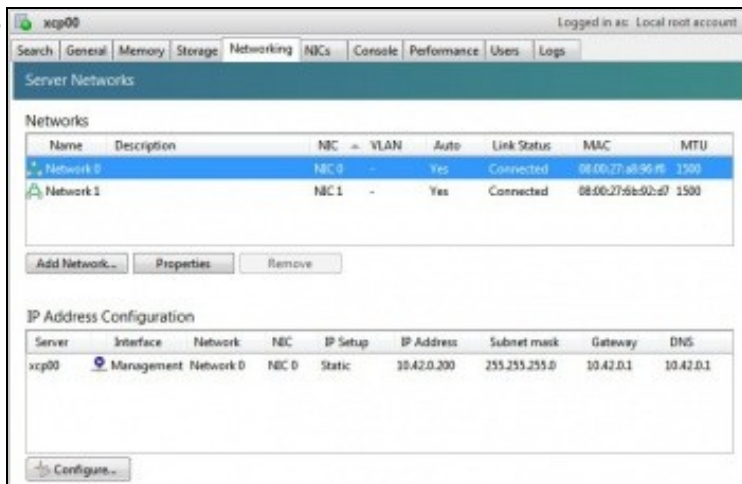
```

[root@xcp00 ~]# xe pif-list
uid ( RO)                : 78aca93c-11db-f2a8-717f-ec674596945d
  device ( RO)            : eth1
  currently-attached ( RO) : true
  VLAN ( RO)              : -1
  network-uuid ( RO)      : 78c7ce0b-ca07-ac27-7075-3444cd01e960

uid ( RO)                : be8132be-3306-dce1-9276-09e9abb837dd
  device ( RO)            : eth0
  currently-attached ( RO) : true
  VLAN ( RO)              : -1
  network-uuid ( RO)      : Bee98d45-22c1-066d-07a9-3ca3eb595594

```

No CLI xe: **xe pif-list** amosa os 2 NICs



A lapela de **Networking** (Redes/Switches Virtuais) amosa o nome das Redes (Network) e sobre que NIC están construídas esas redes. A configuración IP é asociada ás **Redes ou Switches Virtuais**, non ás tarxetas físicas de rede (NICs).

```
[root@xcp00 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:AB:96:F6
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:1975 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3028 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:500916 (496.9 KiB)  TX bytes:4666676 (4.4 MiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:6B:92:D7
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:5651 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5141720 (4.9 MiB)  TX bytes:0 (0.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1805 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1805 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5624803 (5.3 MiB)  TX bytes:5624803 (5.3 MiB)

xenbr0    Link encap:Ethernet  HWaddr 08:00:27:AB:96:F6
```

ifconfig amosa as tarxetas físicas (ethX) e as Redes (xenbrX)

```
[root@xcp00 ~]# ifconfig | grep Ethernet
eth0      Link encap:Ethernet  HWaddr 08:00:27:AB:96:F6
eth1      Link encap:Ethernet  HWaddr 08:00:27:6B:92:D7
xenbr0    Link encap:Ethernet  HWaddr 08:00:27:AB:96:F6
xenbr1    Link encap:Ethernet  HWaddr 08:00:27:6B:92:D7
[root@xcp00 ~]#
```

O mesmo pero filtrado

```
[root@xcp00 ~]# ifconfig xenbr0
xenbr0    Link encap:Ethernet  HWaddr 08:00:27:AB:96:F6
          inet addr:10.42.0.200  Bcast:10.42.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:1945 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2280 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:184828 (180.4 KiB)  TX bytes:8863826 (8.4 MiB)

[root@xcp00 ~]#
[root@xcp00 ~]# ifconfig xenbr1
xenbr1    Link encap:Ethernet  HWaddr 08:00:27:6B:92:D7
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4271 (4.1 KiB)  TX bytes:0 (0.0 b)
```

A configuración IP dunha Rede/Switch Virtual. Observar como só un deles ten IP e coincide coa de XenCenter.

```

[root@xcp00 ~]# xe pif-param-list uuid=be8132be-3306-dce1-9276-09e9abb837dd
uuid ( RO)
    device ( RO): eth0
    MAC ( RO): 08:00:27:a8:96:f6
    physical ( RO): true
    currently-attached ( RO): true
    MTU ( RO): 1500
    VLAN ( RO): -1
    bond-master-of ( RO):
    bond-slave-of ( RO): <not in database>
    tunnel-access-PIF-of ( RO):
    tunnel-transport-PIF-of ( RO):
    management ( RO): true
    network-uuid ( RO): 8ee98d45-22c1-066d-07a9-3ca3eb595594
    network-name-label ( RO): Network 0
    host-uuid ( RO): f175cc75-09b7-463d-94c7-a5eebcc82722
    host-name-label ( RO): xcp00
    IP-configuration-mode ( RO): Static
    IP ( RO): 10.42.0.200
    netmask ( RO): 255.255.255.0
    gateway ( RO): 10.42.0.1
    IPv6-configuration-mode ( RO): None
    IPv6 ( RO):
  
```

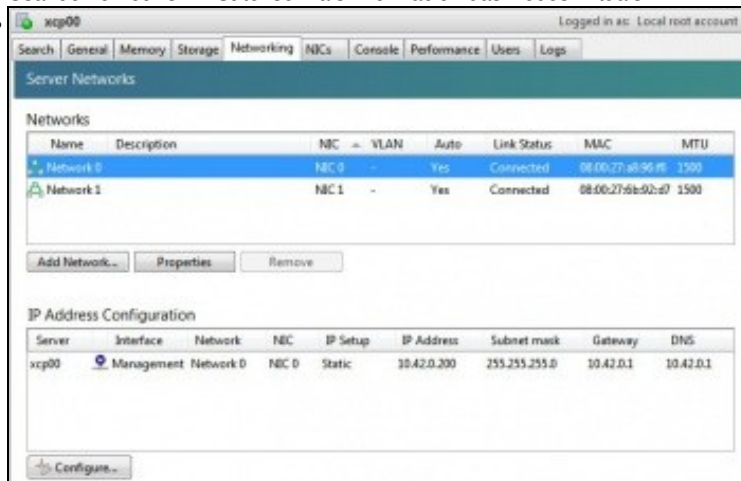
xe pif-param-list uuid=(UUID dunha tarxeta de rede) amosa os parámetros dunha NIC ...

```

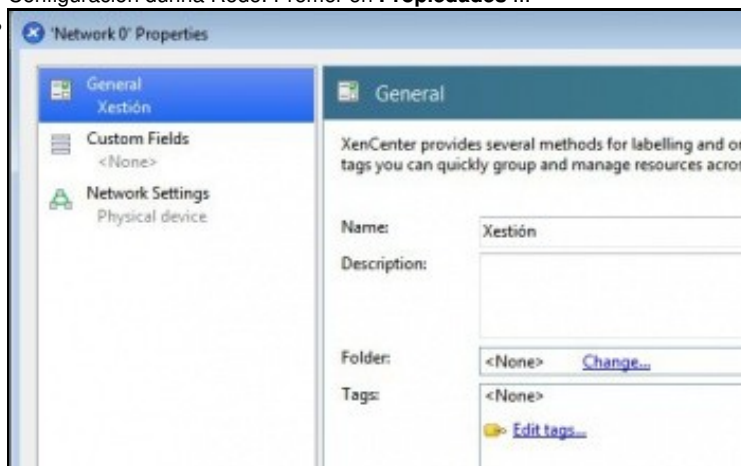
IP-configuration-mode ( RO): Static
IP ( RO): 10.42.0.200
netmask ( RO): 255.255.255.0
gateway ( RO): 10.42.0.1
IPv6-configuration-mode ( RO): None
IPv6 ( RO):
IPv6-gateway ( RO):
primary-address-type ( RO): IPv4
BMS ( RO): 10.42.0.1
io_read_kbs ( RO): 0.254
io_write_kbs ( RO): 0.159
carrier ( RO): true
vendor-id ( RO): 8086
vendor-name ( RO): Intel Corporation
device-id ( RO): 100e
device-name ( RO): 82540EM Gigabit Ethernet Controller
speed ( RO): 1000 Mbit/s
duplex ( RO): full
disallow-unplug ( RO): false
pci-bus-path ( RO): 0000:00:03.0
other-config ( MRM):
  
```

... máis parámetros.

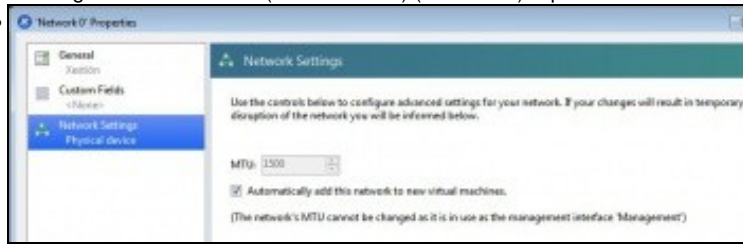
Usando xe network-list tense máis información das Redes virtuais.



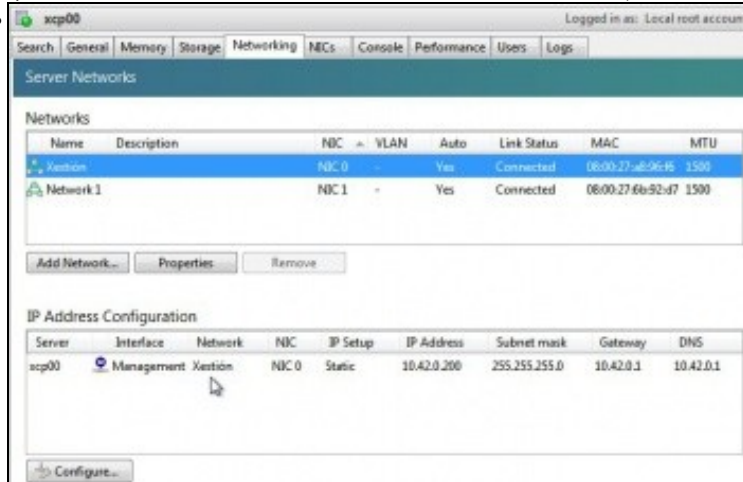
Configuración dunha Rede. Premer en **Propiedades** ...



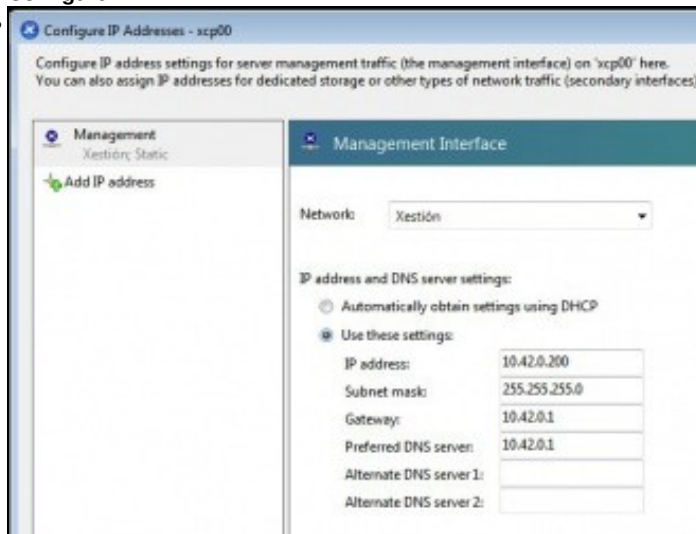
A configuración da Rede 0 (Switch Virtual) (Network 0). Aproveitamos e cambiámoslle o nome a **Xestión**.



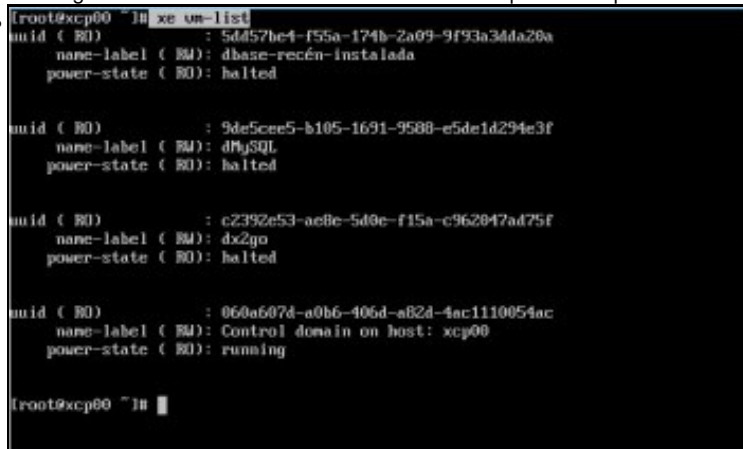
Pódese indicar se desexamos que as novas VIFs (Virtual Interfaces), que asignamos ás MVs, usen sempre esta Rede por defecto. Lembrar que as **Redes actúan de intermediarias dun PIF con varios VIFs** (isto é, entre unha tarxeta física e varias tarxetas de MVs).



Agora imos ver a configuración IP asociada á **Xestión**. (Se non aparece o nome correcto, Xestión, cambiar de lapela e volver). Premer en **Configure**.



A configuración IP do interface de xestión. Interface que non se pode borrar.



xe vm-list amosa as MVs.

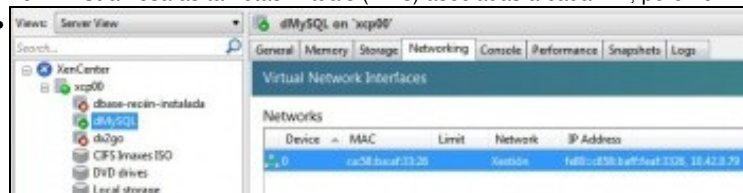
```
[root@xcp00 ~]# xe vif-list
uuid ( RO)           : 51a57837-8d2e-cc32-78d1-08e644f4ecfc
  um-uuid ( RO)      : 887f6952-4951-bb17-5d0b-489445929210
  device ( RO)       : 0
  network-uuid ( RO) : Bee98d45-22c1-066d-07a9-3ca3eb595594

uuid ( RO)           : e2be989a-815c-24c6-c1ac-c494b3d0638e
  um-uuid ( RO)      : fdac41bf-4dee-00ad-2c5d-4e4845b309af
  device ( RO)       : 0
  network-uuid ( RO) : Bee98d45-22c1-066d-07a9-3ca3eb595594

uuid ( RO)           : 2f78f1a2-3f1a-76c8-44b3-722e4ad72b0f
  um-uuid ( RO)      : 5dd57be4-f55a-174b-2a89-9f93a3da26a
  device ( RO)       : 0
  network-uuid ( RO) : Bee98d45-22c1-066d-07a9-3ca3eb595594

uuid ( RO)           : dd20aaac-9ffa-dc01-5f90-156723dcbe84
  um-uuid ( RO)      : c2392e53-ae8e-5d0e-f15a-c962047ad75f
  device ( RO)       : 0
  network-uuid ( RO) : Bee98d45-22c1-066d-07a9-3ca3eb595594
```

xe vif-list amosa as tarxetas virtuais (VIFs) asociadas a cada MV, pero non vemos con que Rede están asociadas.



Acendemos unha MV, ...

```
[root@xcp00 ~]# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:AB:96:F6
          UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
          RX packets:1715 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4785 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:261942 (255.8 KiB) TX bytes:5577812 (5.3 MiB)

eth1      Link encap:Ethernet HWaddr 08:00:27:6B:92:D7
          UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
          RX packets:6405 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5834888 (5.5 MiB) TX bytes:0 (0.0 b)

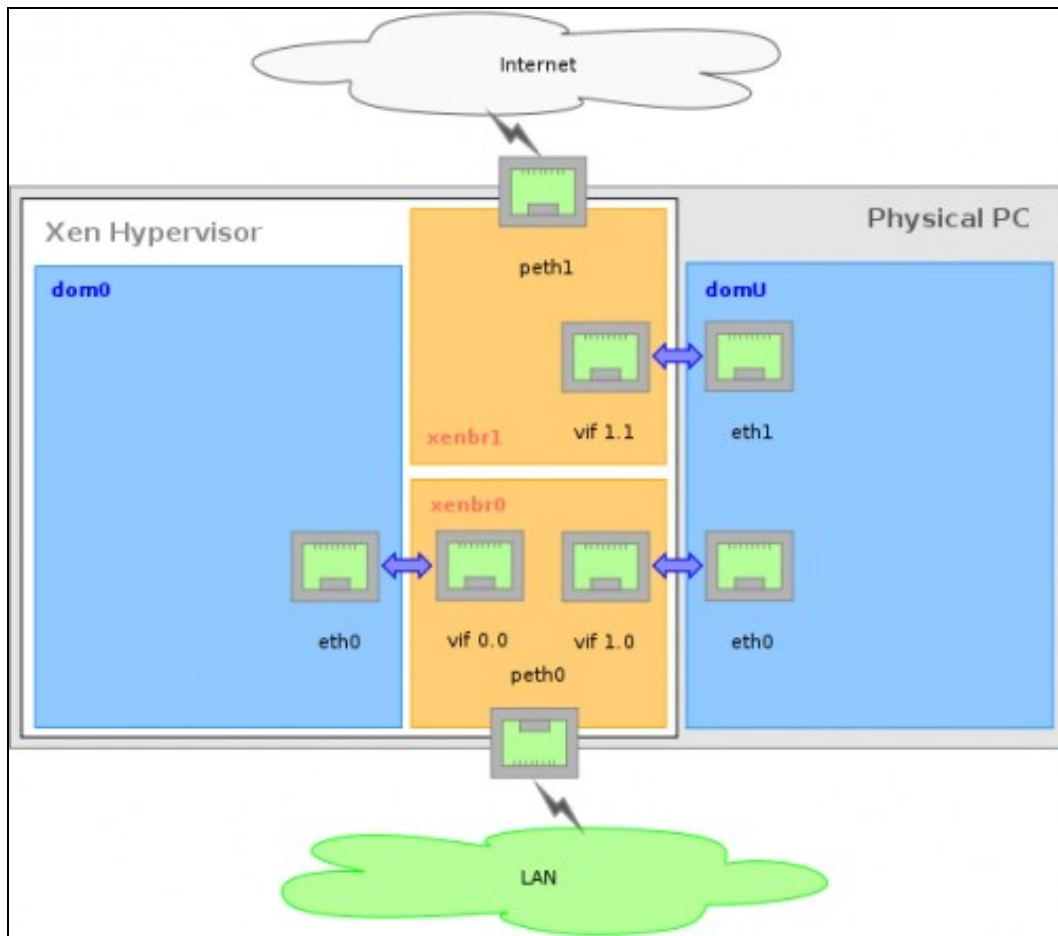
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:2784 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2784 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6284222 (5.9 MiB) TX bytes:6284222 (5.9 MiB)

vif1.0    Link encap:Ethernet HWaddr FE:FF:FF:FF:FF:FF
```

créase un novo interface (**vifx.y**, x=nº secuencial creado para cada MV que se acende (non depende da rede sobre a que está a vif). y=número secuencial que se asocia a cada VIF dunha MV).

```
[root@xcp00 ~]# ifconfig vif1.0
vif1.0    Link encap:Ethernet HWaddr FE:FF:FF:FF:FF:FF
          UP BROADCAST RUNNING NOARP PROMISC MTU:1500 Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:32
          RX bytes:1372 (1.3 KiB) TX bytes:8169 (7.9 KiB)
```

Información do interface virtual.



Esta imaxe amosa unha síntese do exposto enriba. Observar como a MV domU ten 2 VIFs sobre Redes (xenbrX) distintas e observar como se denominan os vifx.y.

Agregación/Bonding

Introdución

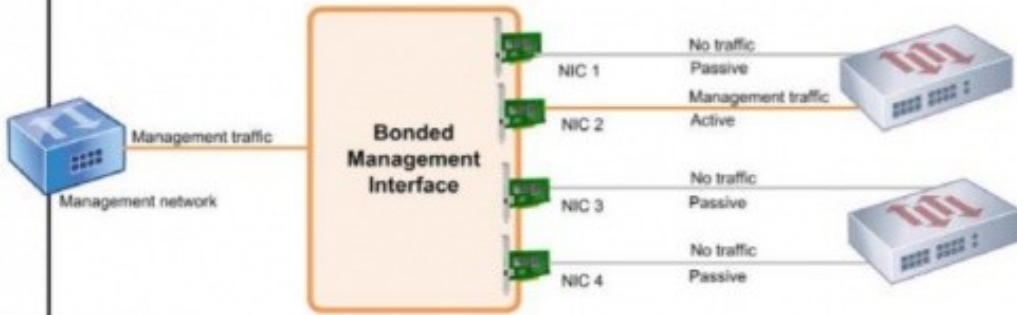
- Na parte V fíxose unha introdución ao Bonding e á súa implementación en FreeNAS: [Bonding. Multipath I/O \(MPIO\)](#)
- Nesta ocasión imos centrarnos nos modos de agregación / Bonding en XEN:
 - ◆ Pódense agregar 2,3 ou 4 NICs.
 - ◆ **Activo-Activo**: tódolos camiños están activos. Non precisa un switch 802.3ad. Isto é, non precisa que se realice bonding no switch.
 - ◆ **Activo-Pasivo**: un camiño activo e o outro de respaldo. Non precisa un switch 802.3ad.
 - ◆ **LACP (Con balanceo baseado en enderezos IPs Orixe/Destino)**: Precisa un switch 802.3ad. Neste caso o tráfico encamiñase por un NIC ou outro en función das IPs Orixe e Destino.
 - ◆ **LACP (Con balanceo baseado en enderezos MAC Orixe)**: Precisa un switch 802.3ad. Neste caso o tráfico encamiñase en función da MAC do VIF Asociada á MV.

- Estas imaxes resumen o explicado. Unha imaxe vale máis ca ...

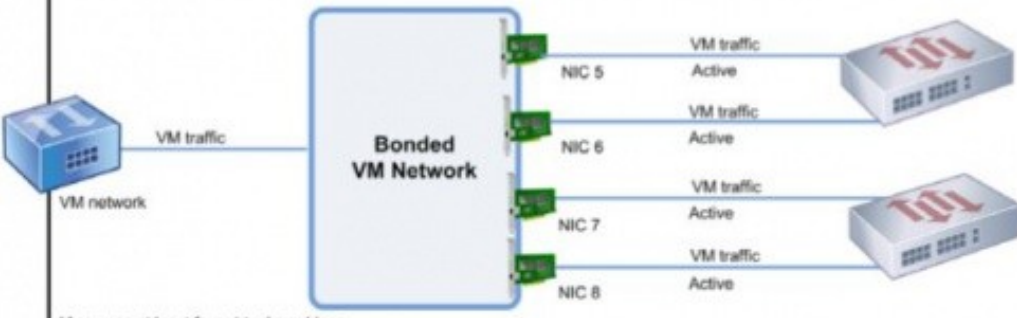
Bonding activo-activo

Active-active bonds (vSwitch network stack)

Management Interface Traffic

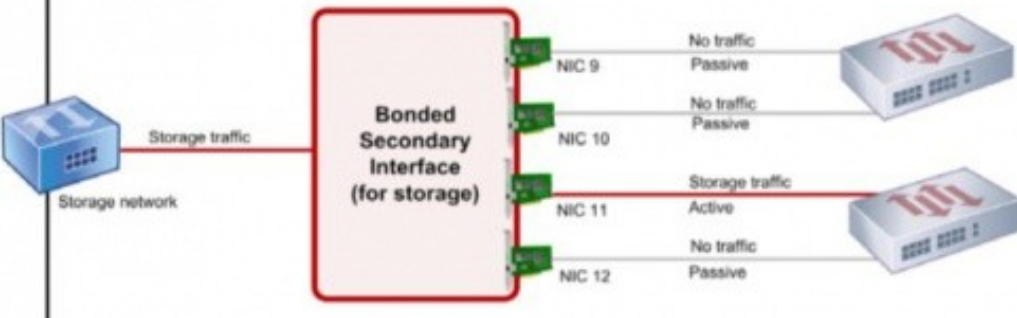


VM Network Traffic*



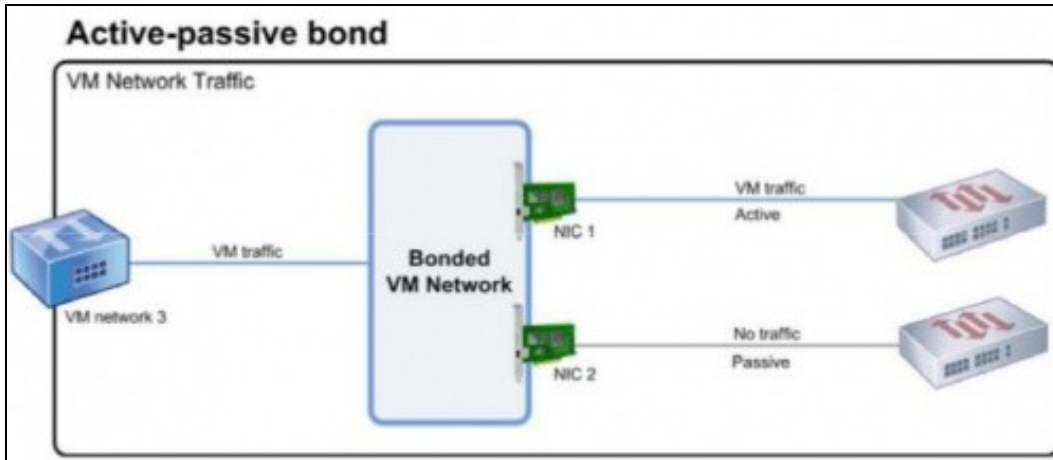
*Assumes at least four virtual machines

Storage Traffic



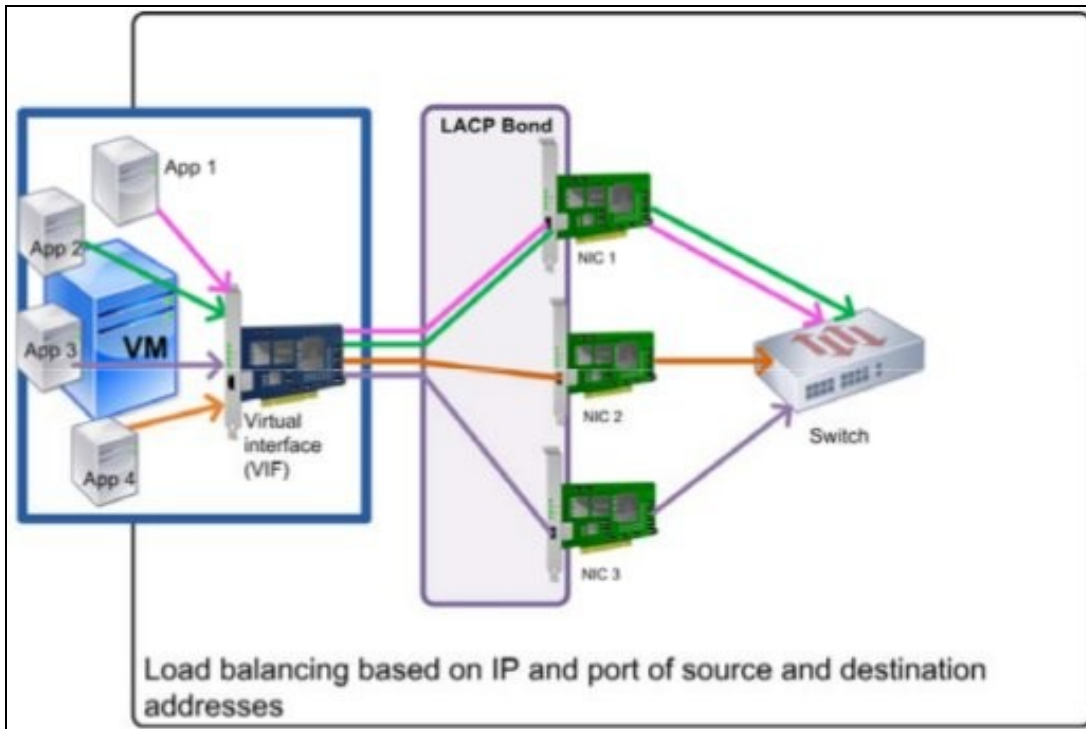
- Observar que se se fai bonding do interface de xestión, só vai haber un camiño activo en cada momento se só está conectado cun só Destino, como xa se viu na PARTE V.
- Se hai 4 ou máis MVs, no segundo caso, cada camiño vai estar activo.
- No terceiro caso, depende de cantos elementos de almacenamento externo teñamos. Neste exemplo só 1.

Bonding activo-pasivo



- Neste caso só un camiño estará activo en cada momento e outro estará de respaldo.

Bonding LACP

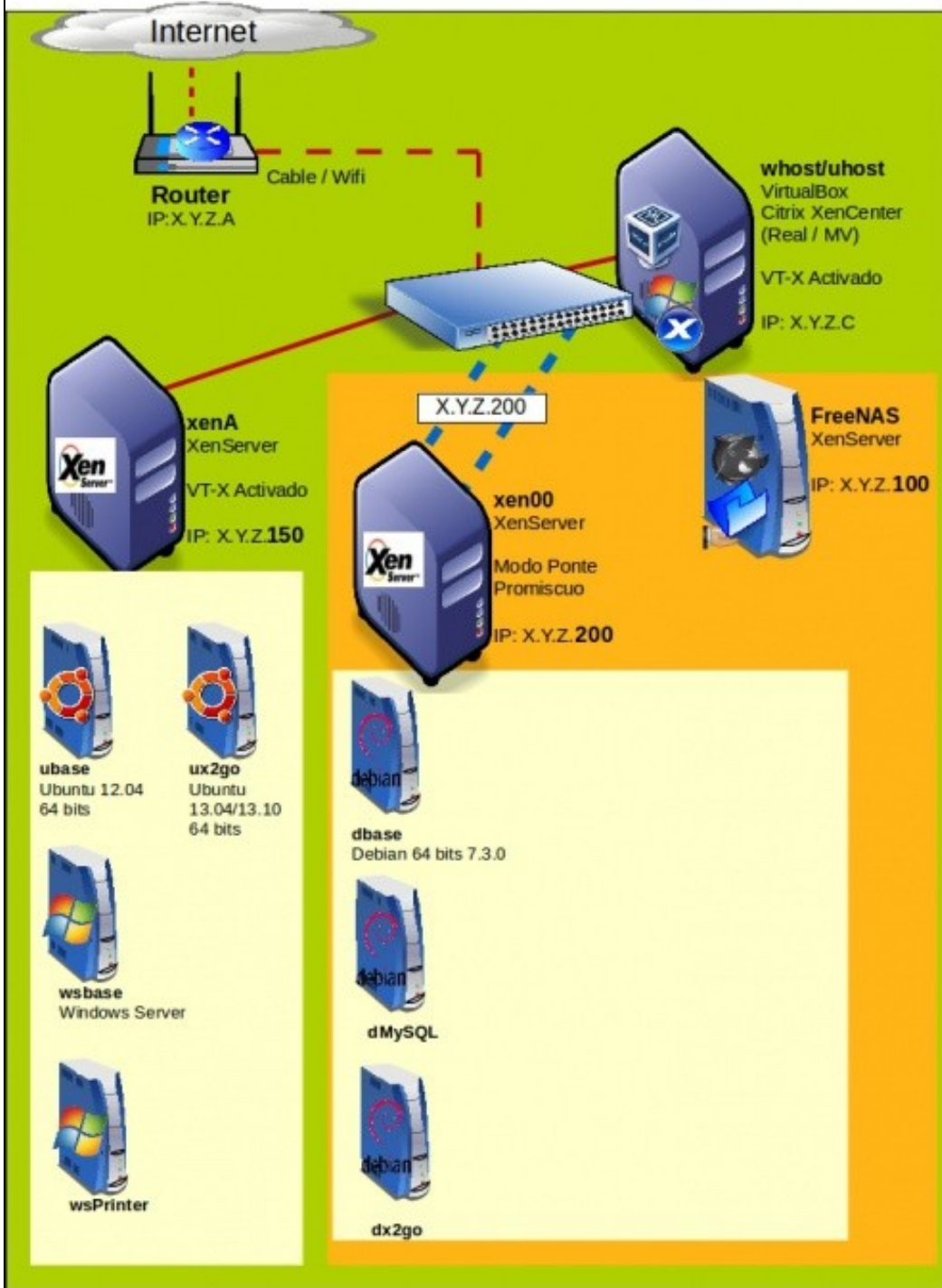


- Neste exemplo hai unha soa MV e un LACP sobre 3 NICs.
- Este é un exemplo de balanceo no que se ten en conta os enderezos IP Orixe e Destino.
- Se fose o caso de LACP baseado na MAC orixe, todo o tráfico desta MV sairía polo mesmo NIC físico. Se só houbera unha MV non habería balanceo.

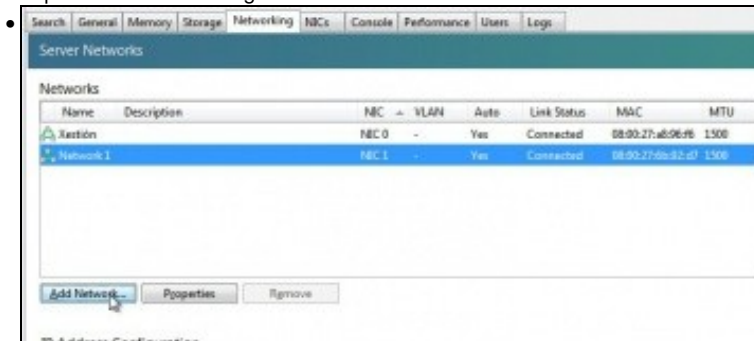
Caso práctico en XenServer

- Sobre o host **xen00**, vaise realizar un exemplo de Bonding.
- Como só hai 2 tarxetas, todo o tráfico (Xestión, MVs e Almacenamento) irá por este bonding.
- Ao rematar de practicar co Bonding, este desfarase.
- Deste xeito mírase o seu funcionamento e o usuario terá a posibilidade de estudar en que casos da súa situación real o podería usar.
- O Management Interface estará sobre un bonding.
- Lembrar que se creou o host xen00 con 2 NICs.

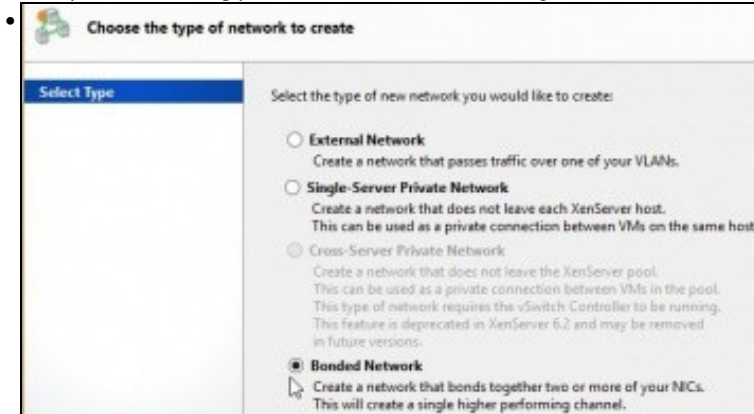
Escenario 6.A: Configuración de Rede: Bonding.



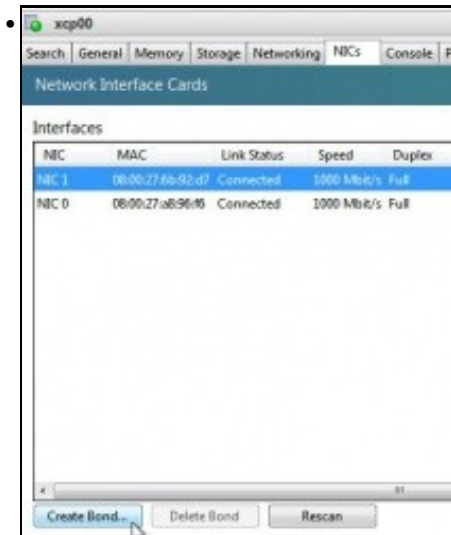
- Implantación de Bonding



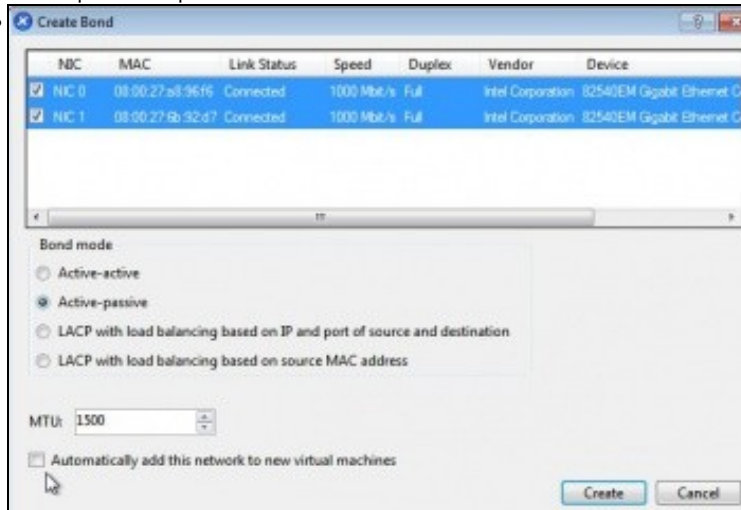
Na lapela **Networking** premer en **Add Network ...** e logo en, ...



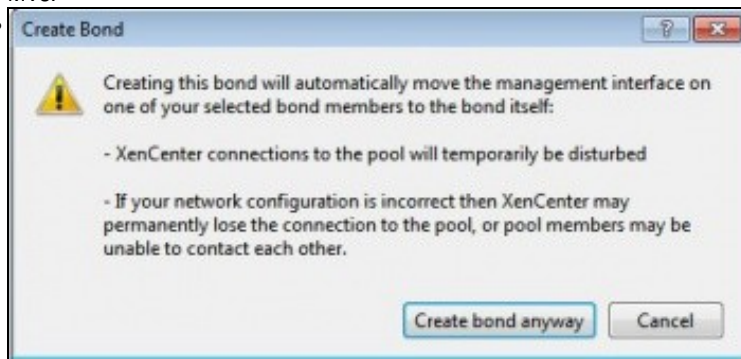
Bonded Network ou ben ...



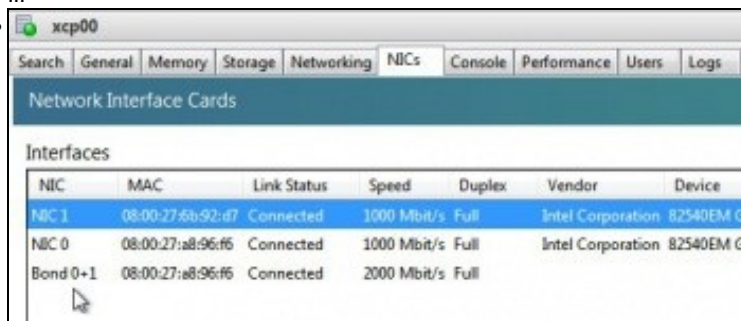
... na lapela **NICs** premer en **Create Bond...**



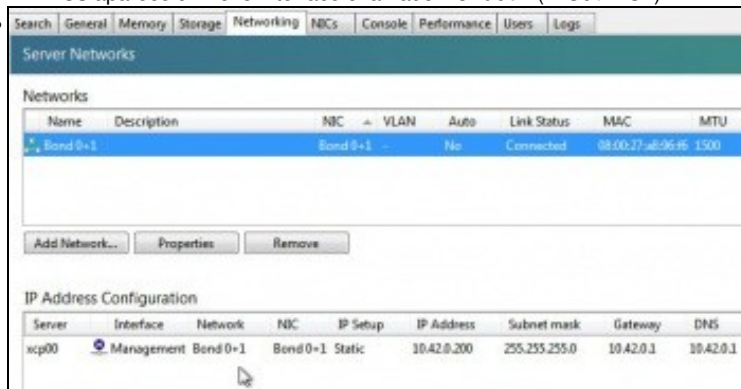
Marcar as tarxetas que participan no Bond. Neste exemplo vaise escoller o modo **Activo-Pasivo**, pois ao estar sobre VirtualBox o modo **Activo-Activo** recibe respostas duplicadas ás solicitudes de ping. Indicar se se desexa usar esta nova Rede/Switch Virtual para as novas MVs.



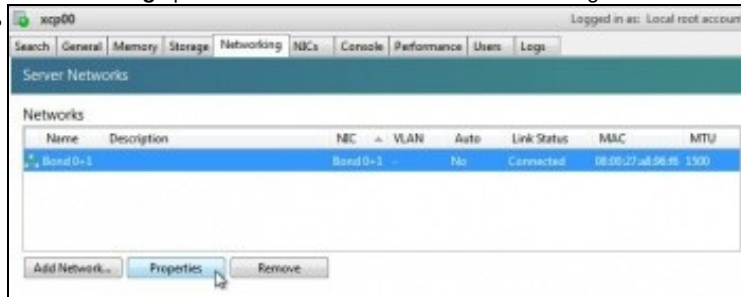
Aviso de que se vai mover o Management Interface á nova rede e que temporalmente se vai perder a conexión coa rede física. Crear o bond



En **NICs** aparece un novo interface chamado **Bond0+1** (NIC0+NIC1).



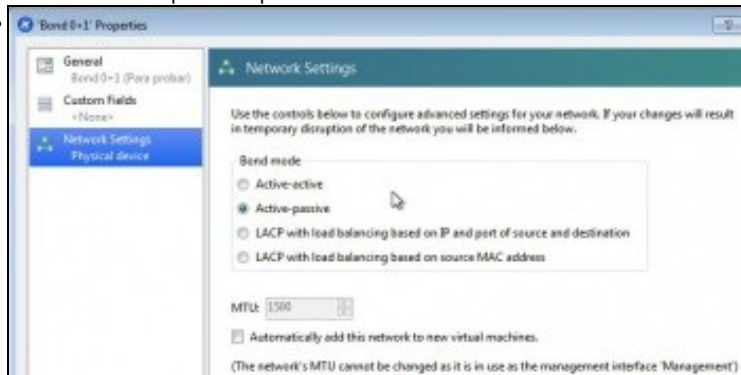
En **Networking** aparece a nova Rede/Switch Virtual e a configuración IP.



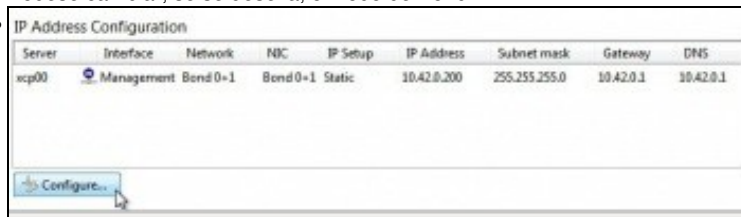
Ir a propiedades da nova Rede.



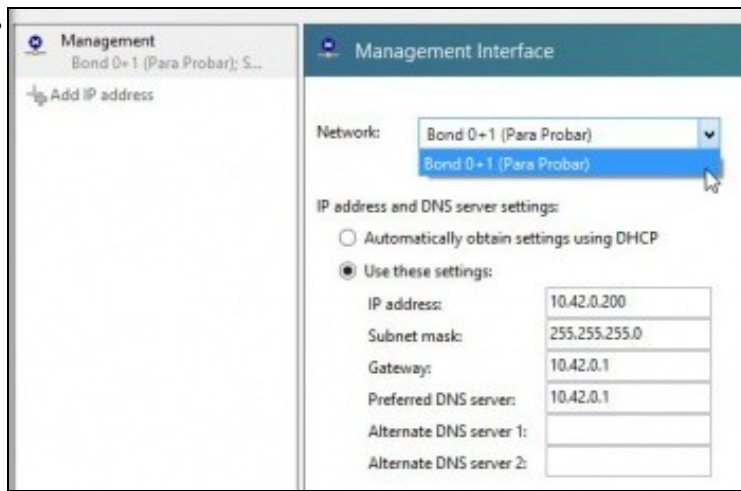
Cambiar o nome por exemplo da nova rede.



Pódese cambiar, se se desexa, o modo de Bond.



O novo nome xa aplicado á configuración IP. Se non aparece o novo nome, cambiar de lapela e volver. Iremos á configuración IP



Non hai máis Redes, nin xestión nin Network 1.



A configuración en xconsole ...



```

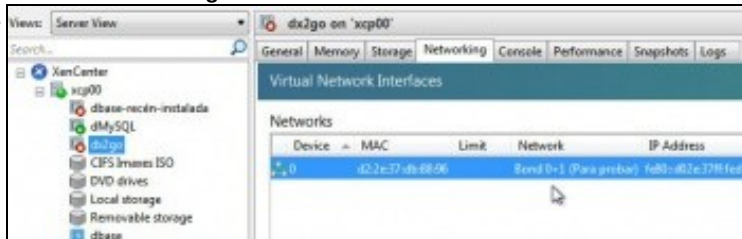
eth1    Link encap:Ethernet HWaddr 08:00:27:68:92:D7
        UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
        RX packets:11164 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2149 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:9784320 (9.3 MiB)  TX bytes:2062666 (1.9 MiB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:4631 errors:0 dropped:0 overruns:0 frame:0
        TX packets:4631 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:10032368 (10.3 MiB)  TX bytes:10032368 (10.3 MiB)

xapi0   Link encap:Ethernet HWaddr 08:00:27:AB:96:F6
        inet addr:10.42.0.200 Bcast:10.42.0.255  Mask:255.255.255.0
        UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
        RX packets:1496 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1244 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:168996 (165.0 KiB)  TX bytes:2013796 (1.9 MiB)

```

E na consola: **ifconfig**



Asignada a nova Rede a unha MV.

Experimentación ante fallos

- Experimentar con Bonding

```

root@xcp00 ~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=47 time=76.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=47 time=74.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=47 time=74.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=47 time=77.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=47 time=74.5 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=47 time=77.4 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=47 time=84.0 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=47 time=74.5 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=47 time=77.5 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=47 time=73.3 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=47 time=74.7 ms

```

Dende a consola de **xen00**, realizar **ping 8.8.8.8**.



Desconectar un dos cables de rede do host xen00. Logo volvelo conectar. Esperar e desconectar o outro.

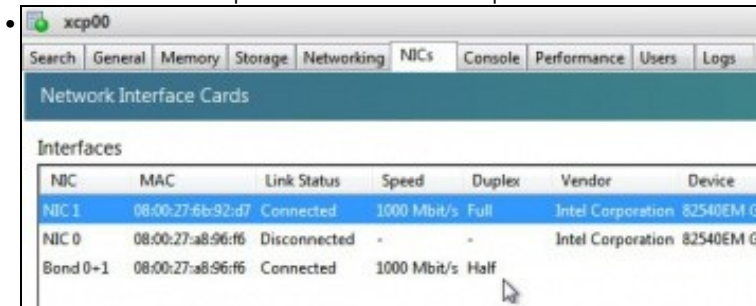
Lembrar que os dous adaptares estean sobre o mesmo interface de rede físico e en modo promíscuo (neste último caso para cando se fagan probas dende unha MV).

```
64 bytes from 8.8.8.8: icmp_seq=16 ttl=47 time=77.3 ns
64 bytes from 8.8.8.8: icmp_seq=17 ttl=47 time=77.6 ns
64 bytes from 8.8.8.8: icmp_seq=18 ttl=47 time=74.5 ns
64 bytes from 8.8.8.8: icmp_seq=19 ttl=47 time=73.5 ns
64 bytes from 8.8.8.8: icmp_seq=20 ttl=47 time=74.8 ns
^C
-- 8.8.8.8 ping statistics --
20 packets transmitted, 20 received, 0% packet loss, time 19186ms
rtt min/avg/max/mdev = 73.358/75.901/84.049/2.390 ms
[root@xcp00 ~]#
```

Dende o host xen00 non se perdeu un ping.

```
64 bytes from 10.42.0.200: icmp_req=30 ttl=64 time=0.669 ms
64 bytes from 10.42.0.200: icmp_req=31 ttl=64 time=0.340 ms
64 bytes from 10.42.0.200: icmp_req=32 ttl=64 time=1.86 ms
64 bytes from 10.42.0.200: icmp_req=34 ttl=64 time=0.482 ms
64 bytes from 10.42.0.200: icmp_req=35 ttl=64 time=0.872 ms
64 bytes from 10.42.0.200: icmp_req=36 ttl=64 time=1.05 ms
64 bytes from 10.42.0.200: icmp_req=37 ttl=64 time=0.940 ms
^C
--- 10.42.0.200 ping statistics ---
37 packets transmitted, 36 received, 2% packet loss, time 36029ms
rtt min/avg/max/mdev = 0.313/1.375/10.579/1.711 ms
administrador@base:~$
```

Dende o exterior si se perdeu un 2%. Neste exemplo.

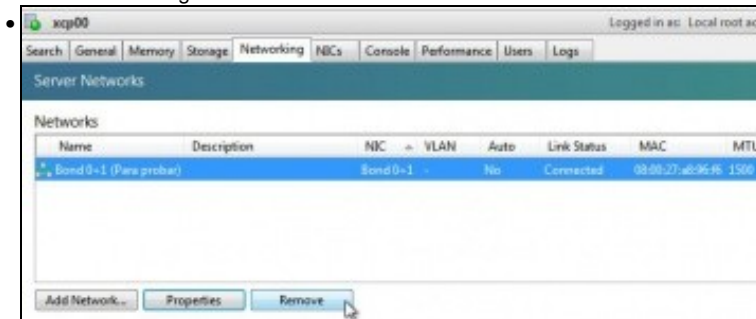


A lapela NICs, amosa que unha das NICs está caída e observar como no Bond indica **Half (Metade)**.

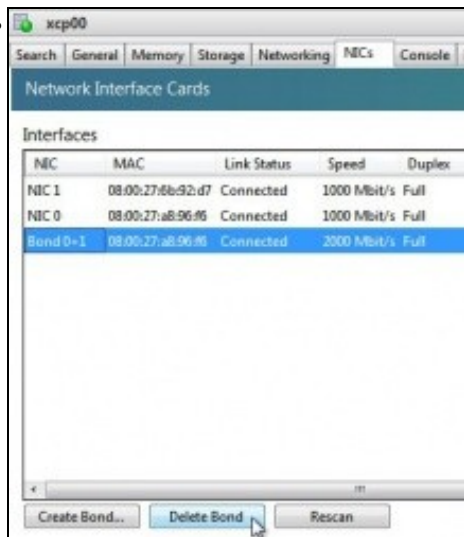
Desfacer un bonding

• Asegurarse de que as dúas NICs de xen00 están conectadas antes de desfacer o bonding.

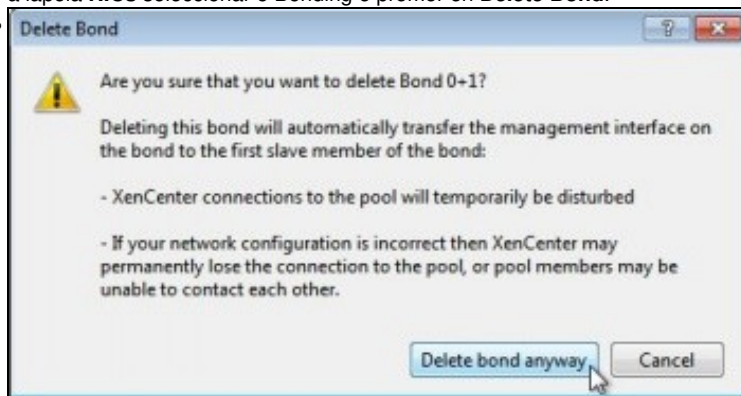
• Desfacer Bonding



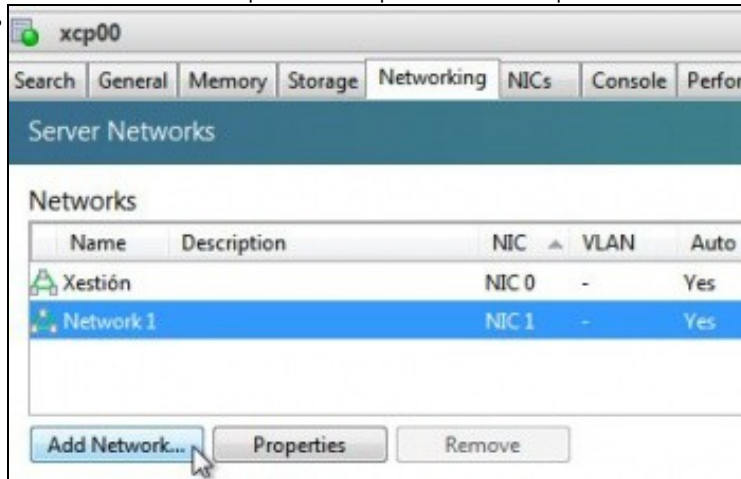
Ben dende **Networking** premer en **Remove** ou ben dende ...



a lapela **NICs** seleccionar o Bonding e premer en **Delete Bond**.



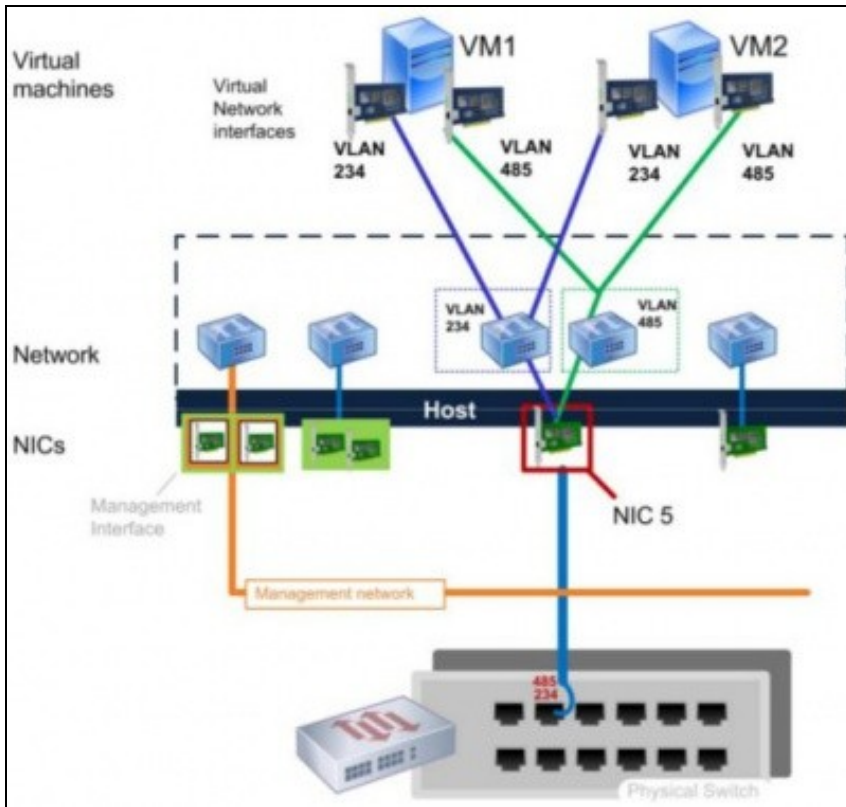
Eliminámo ... Aviso de que o host vai perder a conexión por un instante.



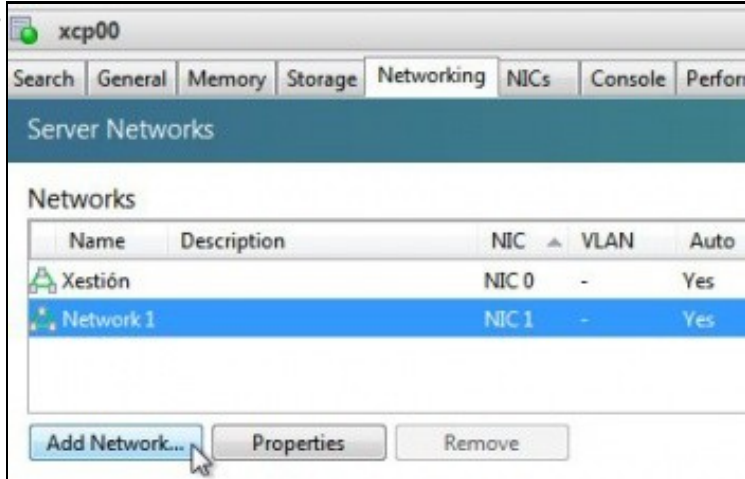
As Redes están configuradas como o estaban antes do Bonding.

Rede externa VLAN

- A modo de exemplo vaise amosar como se crearía unha Rede/Switch Virtual para unha VLAN sobre un interface.
- Algo parecido ao que se faría sobre o NIC5 da imaxe.



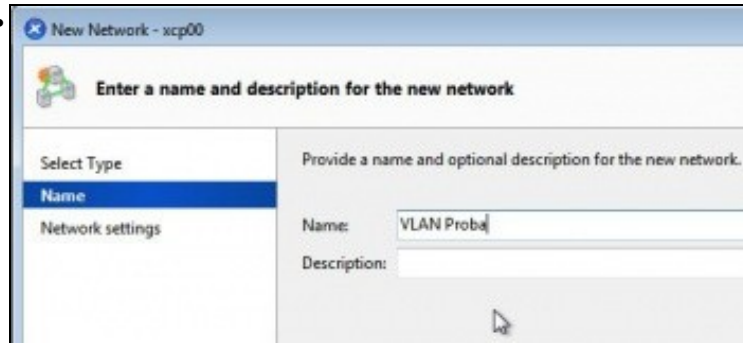
- Rede externa VLAN



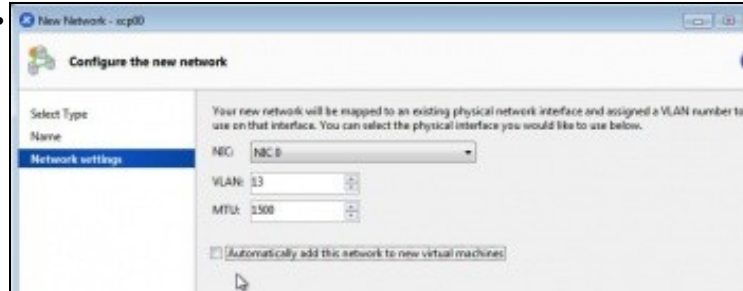
Premer en **Add Network**



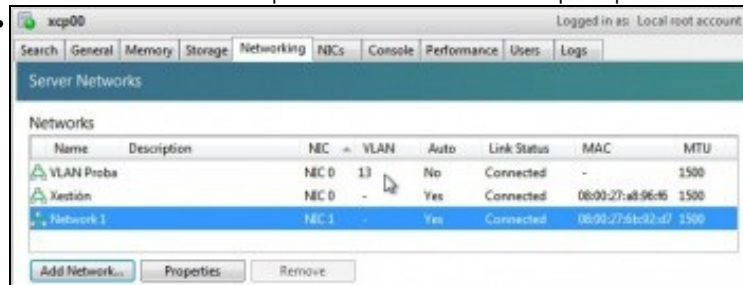
Seleccionar **External Network**.



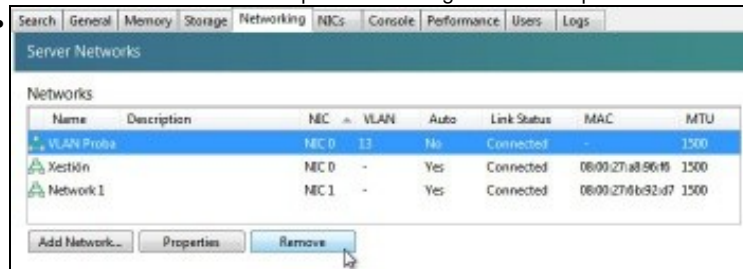
Poñer un nome ...



Seleccionar a NIC sobre a que se vai crear a nova rede e para que VLAN.



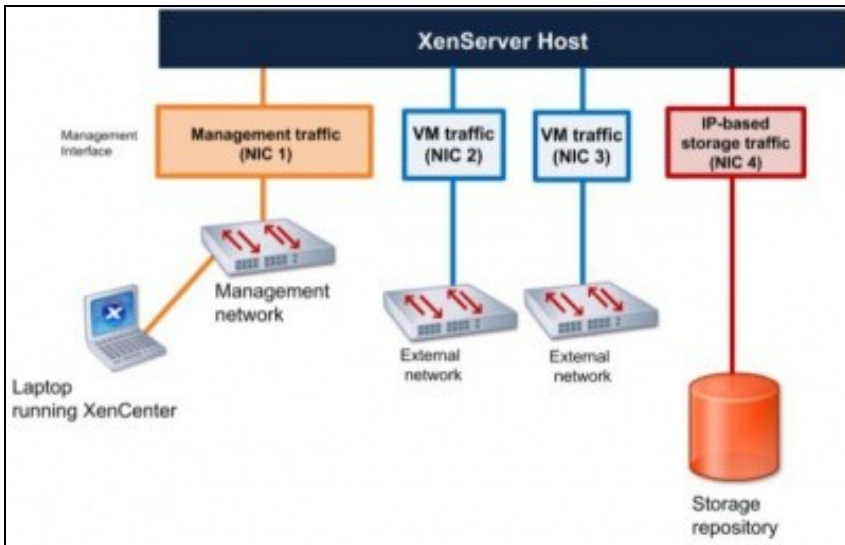
Esa nova rede non ten MAC e podería ser asignada a MVs que estarían conectadas á VLAN 13 da LAN Física.



Eliminamos esa Rede... **Remove**.

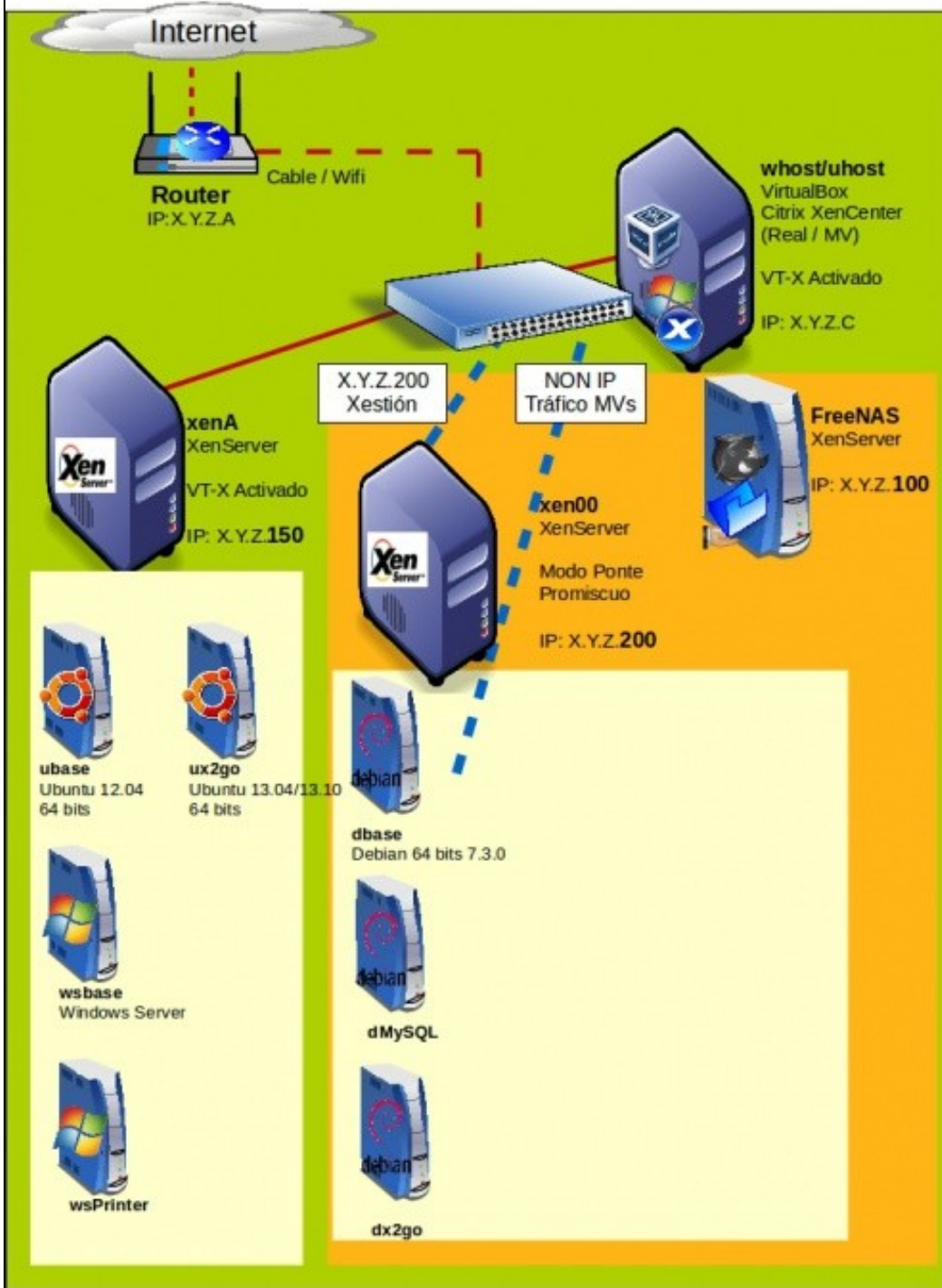
Tráfico das MVs

- Aproveitando que se dispón de 2 NICs, vanse usar para o seguinte tráfico:
 - ♦ **NIC0: Xestión**. E como non hai outra por agora, esta NIC tamén será usada para o tráfico de almacenamento.
 - ♦ **NIC1: Tráficos das MVs**. Non precisa ter configuración IP.
 - ◊ Na imaxe NIC1 sería o equivalente ás NIC2 e NIC3

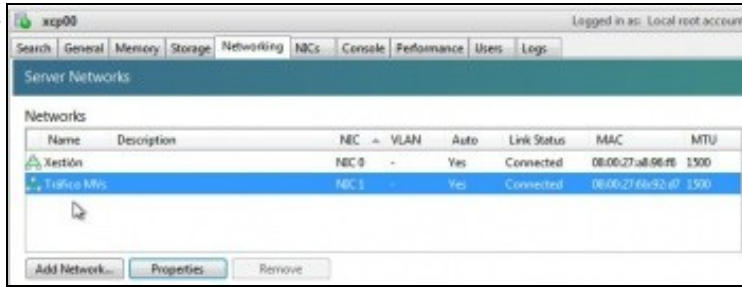


- A imaxe amosa o escenario que se vai poñer en práctica

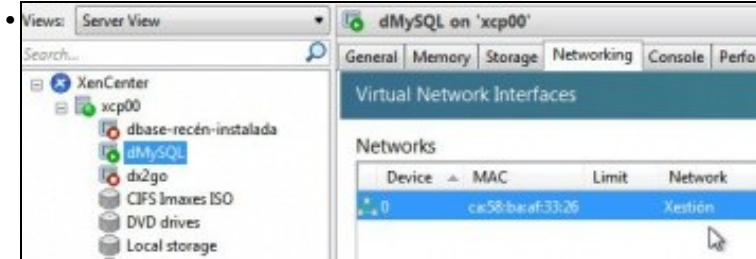
Escenario 6.B: Configuración de Rede: Tráfico MVs.



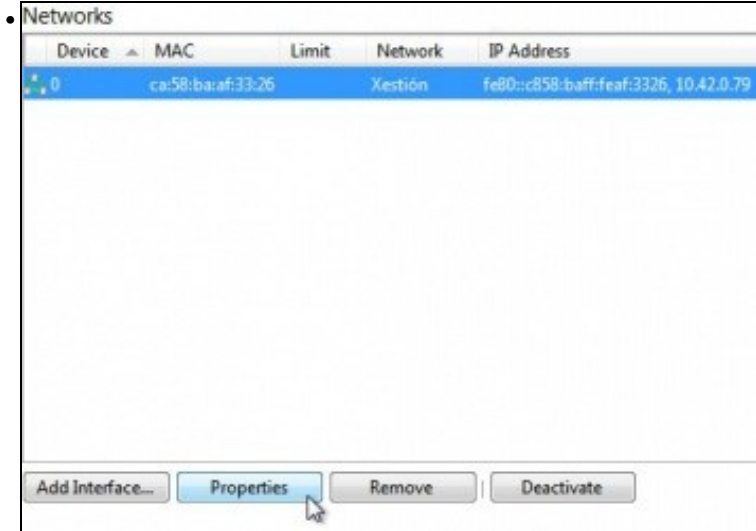
- Tráfico das MVs



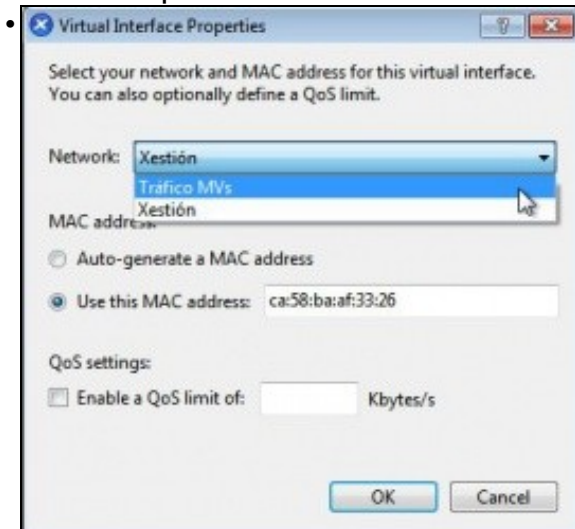
Cambiarlle o nome á rede **Network 1** por **Tráfico MVs**, así é máis fácil lembrarse á que está adicada cada Rede. Lembrarse de que o Adaptador de rede 2 de VirtualBox debe estar en modo promiscuo.



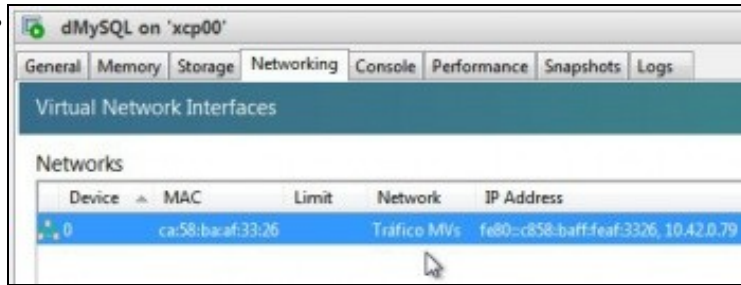
Ir á lapela **Networking** dunha MV ...



Por defecto esa VIF está sobre a **Rede Xestión** de escenarios anteriores. Premer en **Propiedades** e ...



Cambiar á Rede Tráfico VMs



Cambiada e ... A MAC da MV segue sendo a mesma, a IP tamén, etc.

```
root@dmysql:~# ifconfig eth0
eth0      Link encap:Ethernet HWaddr ca:58:ba:af:33:26
          inet addr:10.42.0.79 Bcast:10.42.0.255 Mask:255.255.255.0
          inet6 addr: fe80::c858:baff:feaf:3326/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7236 (7.0 KiB) TX bytes:3020 (2.9 KiB)
          Interrupt:9

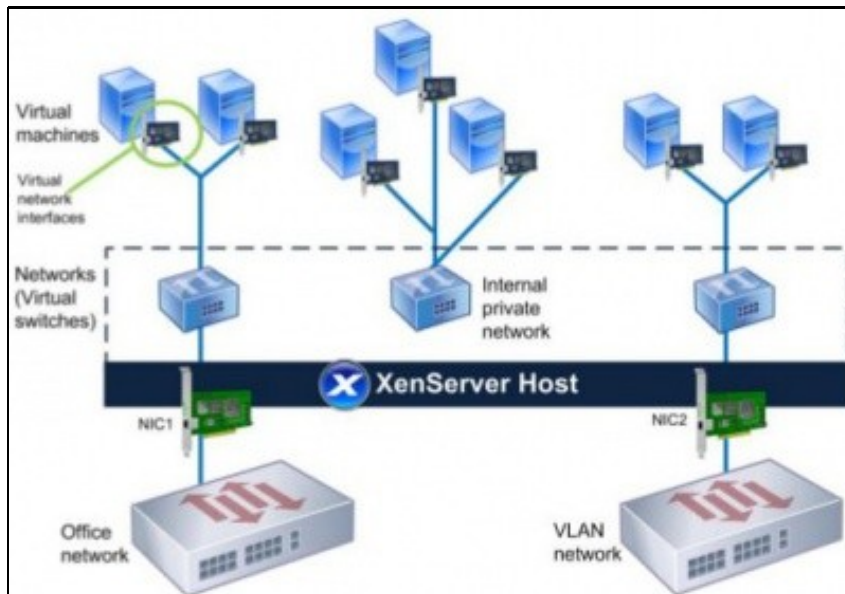
root@dmysql:~#
root@dmysql:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_req=1 ttl=47 time=76.5 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=47 time=78.6 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 76.553/77.616/78.600/1.099 ms
root@dmysql:~#
```

Revisión da configuración IP da MV: **ifconfig** e probar conectividade **ping 8.8.8.8**.

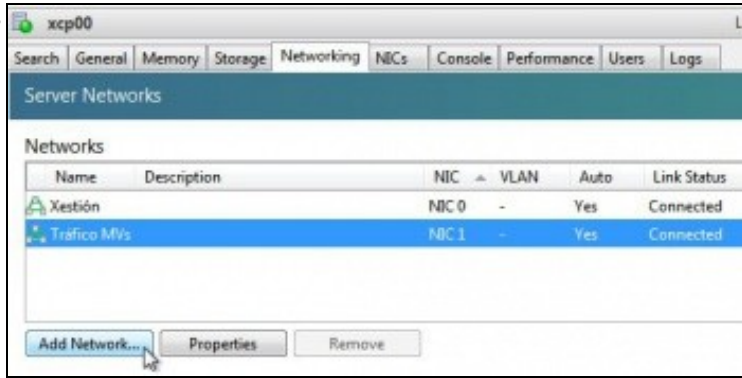
- Notar que en todo proceso á rede **Tráfico MVs** (NIC1) non ten asociada unha IP e non a necesita, só está para transmitir/recibir o tráfico que sae/entra da/na MV.

Rede privada interna (solitaria)

- Na imaxe sería o equivalente á rede Central



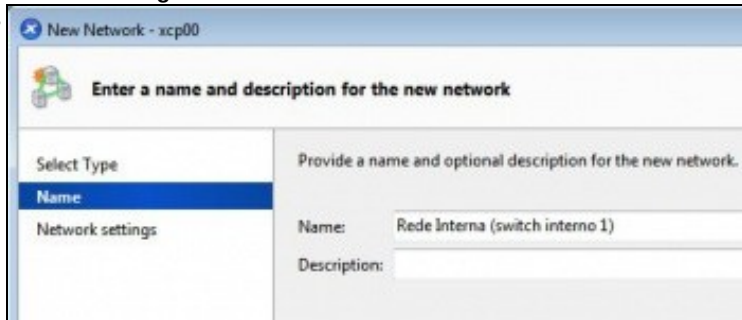
- Rede Privada Interna



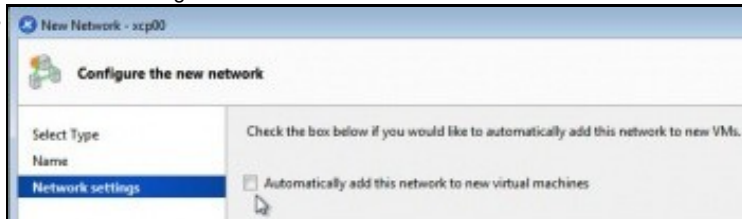
Engadir unha nova rede ...



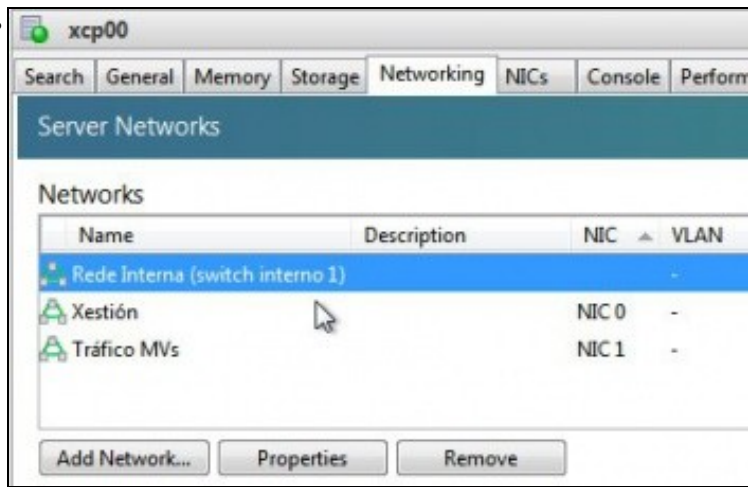
Seleccionar **Single-Server Private Network**



Poñer un nome significativo



Indicar se se desexa que esa nova rede se use por defecto para as novas MVs.



A nova rede non está sobre ningunha NIC.

```

[root@xcp00 ~]# xe network-list
uuid ( RO)                : 78c7ee0b-ea07-ac27-7075-3444cd01e960
  name-label ( RW)        : Pool-wide network associated with eth1
  name-description ( RW)  :
  bridge ( RO)           : xenbr1

uuid ( RO)                : 762b319c-c2dd-3eb5-dc2c-c16a2777a4fd
  name-label ( RW)        : Host internal management network
  name-description ( RW)  : Network on which guests will be assigned a private
link-local IP address which can be used to talk XenAPI
  bridge ( RO)           : xenapi

uuid ( RO)                : 8ee98d45-22c1-066d-07a9-3ca3eb595594
  name-label ( RW)        : Xestión
  name-description ( RW)  :
  bridge ( RO)           : xenbr0
  
```

xe network-list amosa as Redes/Switches Virtuais

```

[root@xcp00 ~]# xe network-param-list uuid=8ee98d45-22c1-066d-07a9-3ca3eb595594
uuid ( RO)                : 8ee98d45-22c1-066d-07a9-3ca3eb595594
  name-label ( RW)        : Xestión
  name-description ( RW)  :
  VIF-uuids ( SRW)       : 51a57837-6d2e-cc32-7bd1-80e644f4ecfc; e2be909a-0
15e-2dc6-clac-c494b3d0638e; 2f78f1a2-3f1a-76c8-d4b3-722e4ad72b0f; ca749b6e-01e6-
a6e7-35e3-aa2197e7c8e2; a7d020e5-4529-513d-1668-9f94b2201f33; 83246c69-17a5-de0d
-0100-bcfead5d408e; 7f90b552-49a8-d367-e4db-f421109aa0bd
  PIF-uuids ( SRW)       : bed132be-3306-dce1-9276-09e9abb837dd
  MTU ( RW)             : 1500
  bridge ( RO)          : xenbr0
  other-config ( MRW)   :
  blobs ( RO)           :
  tags ( SRW)           :
  default-locking-mode ( RW) : unlocked
  
```

Os parámetros da rede **Xestión**. Fixarse que está asociada a unha PIF (Physical InterFace).

```

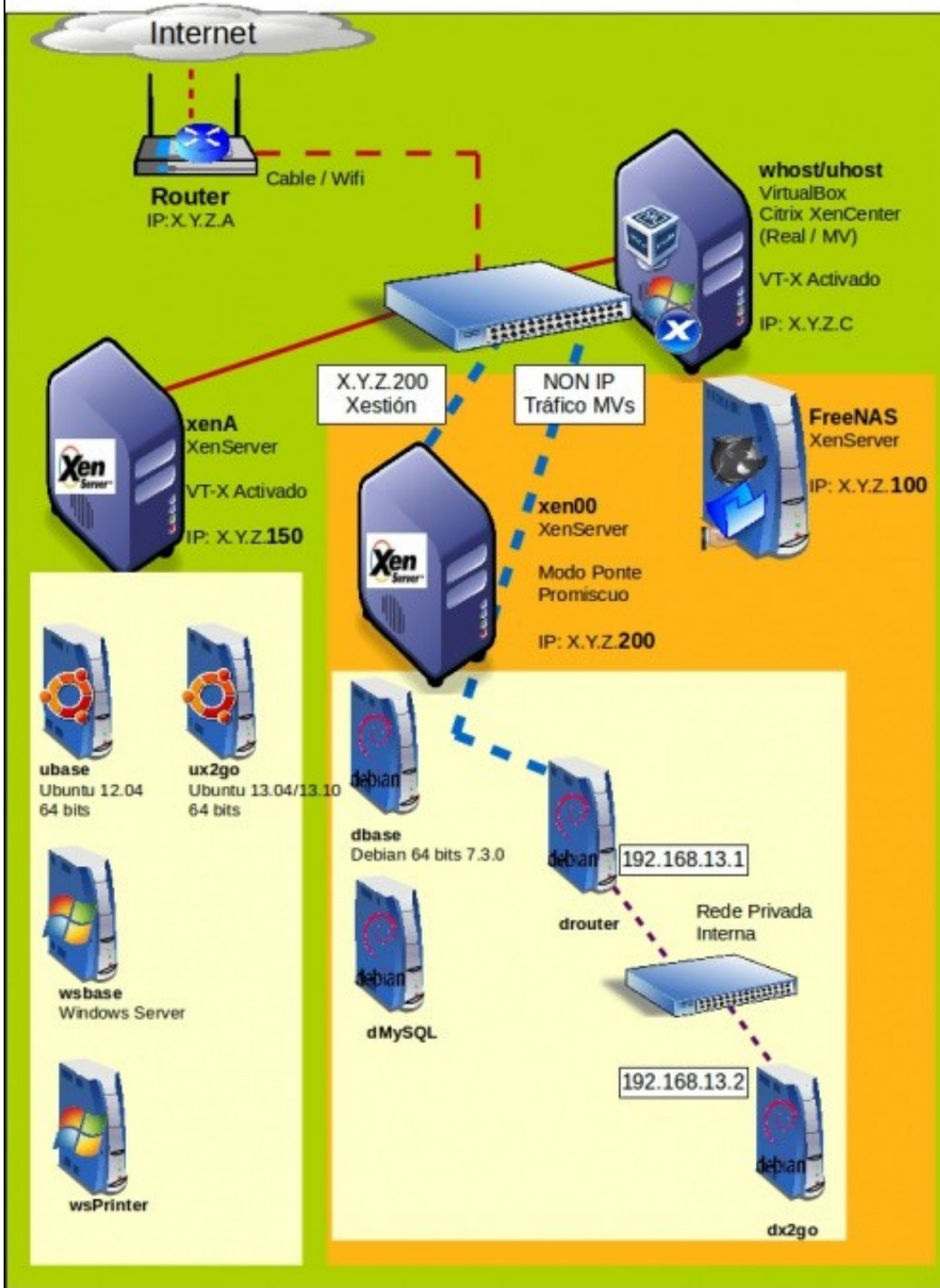
[root@xcp00 ~]# xe network-param-list uuid=9a5b259c-7abd-7f86-1032-cd516b8984ed
uuid ( RO)                : 9a5b259c-7abd-7f86-1032-cd516b8984ed
  name-label ( RW)        : Rede Interna (switch interno 1)
  name-description ( RW)  :
  VIF-uuids ( SRW)       : ee2cf8fa-66c1-bb21-1d78-c64d2a6480f9; 4517b4fe-c
d23-6c5c-3dcb-76a2b1a22e91
  PIF-uuids ( SRW)       :
  MTU ( RW)             : 1500
  bridge ( RO)          : xapi3
  other-config ( MRW)   : automatic: false
  blobs ( RO)           :
  tags ( SRW)           :
  default-locking-mode ( RW) : unlocked
  
```

Os parámetros da Rede Privada Interna. Fixarse que NON está asociada a unha PIF.

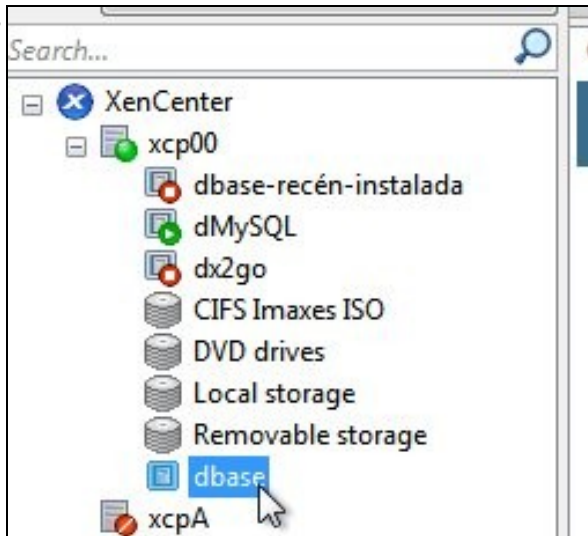
Caso práctico: Crear unha DMZ

- Neste exemplo vaise facer algo semellante ao escenario 2.F: [Escenario 2.F: Configuración dun router virtualizado con Debian](#).
- A imaxe amosa o escenario a implantar. Observar como **drouter** ten 2 VIFs: un na rede **Tráfico MVs** e o outro na **Rede privada interna**.
- Por outro lado o equipo **dx2go** ten unha VIF na **Rede privada interna**, co cal, se se desexa saír a internet, debe usar a equipo **drouter** como porta de enlace.
- Tamén se vai habilitar DNAT (NAT inverso) en **drouter** para que dende o exterior, conectándonos ao porto 2222 de **drouter**, nos reenvíe ao porto 22 de **dx2go**.

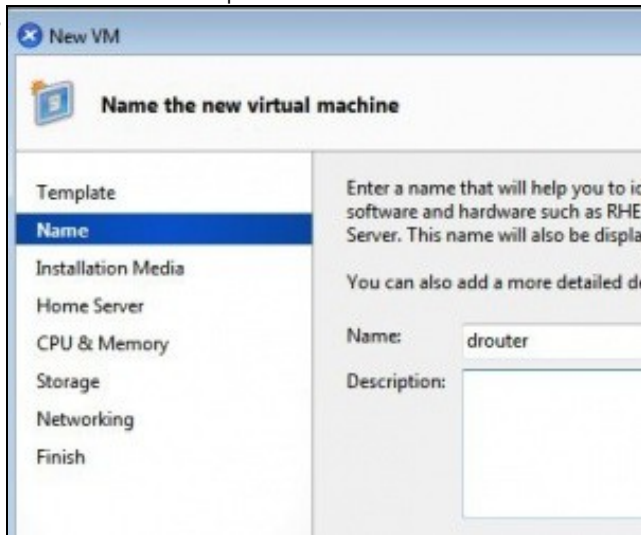
Escenario 6.C: Configuración de Rede: Rede interna Privada



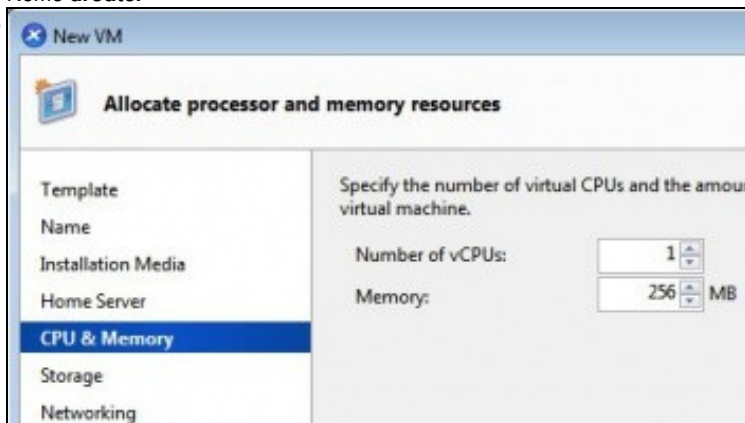
- Rede Privada Interna



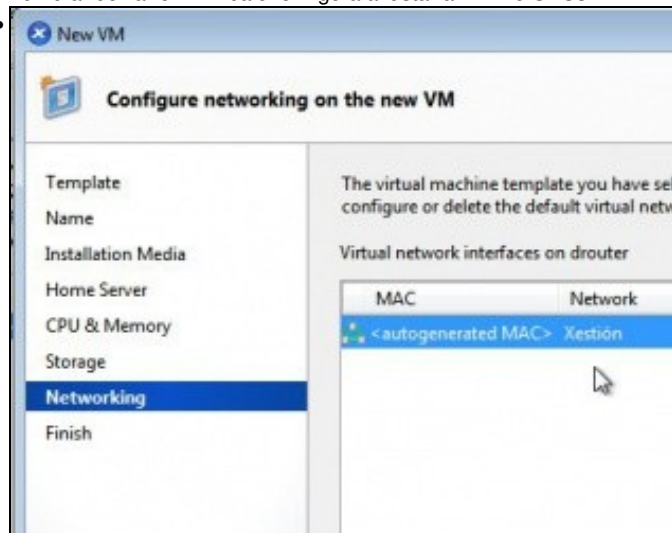
Crear unha nova MV a partir de **dbase**



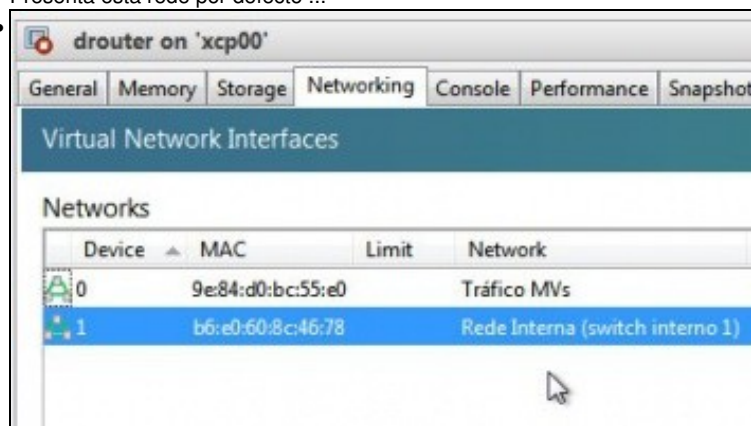
Nome **drouter**



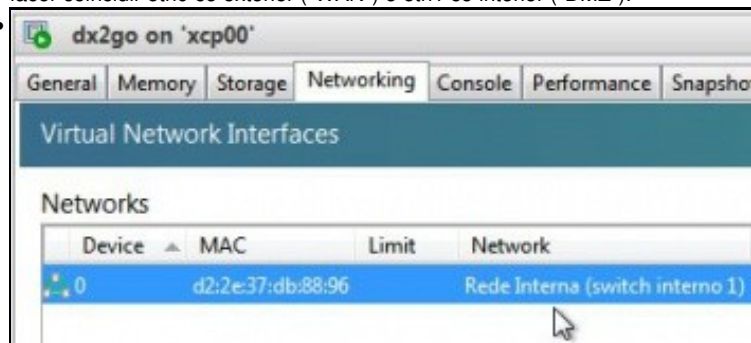
Lembrar deixar o DVD baleiro. Agora axustar a RAM e CPUs



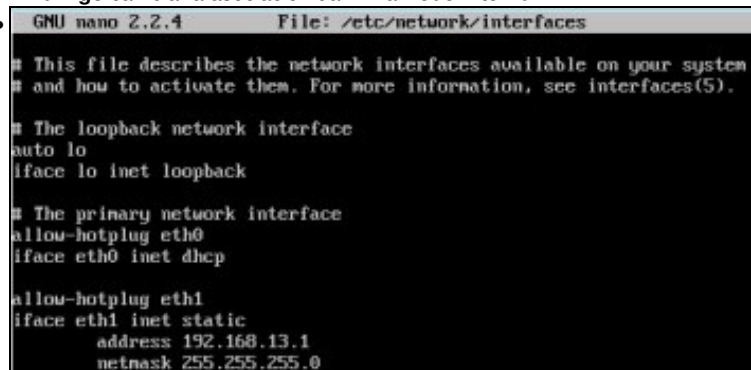
Presenta esta rede por defecto ...



Configurar a primeira VIF para que estea a asociada á rede: **Tráfico MVs** e engadir unha 2ª VIF e asociala á **Rede Interna**, nesa orde para facer coincidir eth0 co exterior ("WAN") e eth1 co interior ("DMZ").



En **dx2go** cambiar a asociación da VIF á **Rede Interna**



En **router** configurar eth1 como estático e coa IP do escenario: 192.168.13.1/24.

```
root@router:~# ifup eth1
root@router:~#
root@router:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 9e:84:d0:bc:55:e0
          inet addr:10.42.0.66  Bcast:10.42.0.255  Mask:255.255.255.0
          inet6 addr: fe80::9e84:d0ff:febc:55e0/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:206 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13364 (13.0 KiB)  TX bytes:4960 (4.8 KiB)
          Interrupt:7

eth1      Link encap:Ethernet  HWaddr b6:e0:60:8c:46:78
          inet addr:192.168.13.1  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::b6e0:60ff:fe8c:4678/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:900 (900.0 B)
          Interrupt:9

lo        Link encap:Local Loopback
```

Baixar (ifdown eth0) e levantar o interface (ifup eth0) ou reiniciar. Revisar a configuración IP: eth0 recibe unha IP por DHCP do exterior e eth1 ten a IP estática anterior. Se non hai un servidor DHCP débese configurar eth0 coa IP correspondente á configuración IP da rede LAN.

```
root@router:~# route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.13.0   0.0.0.0        255.255.255.0   U        0     0     0 eth1
10.42.0.0      0.0.0.0        255.255.255.0   U        0     0     0 eth0
0.0.0.0        10.42.0.1      0.0.0.0         UG       0     0     0 eth0
root@router:~#
```

A porta de enlace por defecto é o router da LAN real. Se non hai servidor DHCP configurar en eth0 **gateway IP que corresponda**.

```
GNU nano 2.2.4 File: /etc/network/interfaces

# This file describes the network interfaces available
# and how to activate them. For more information, see i

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
#NetworkManager
#iface eth0 inet dhcp

iface eth0 inet static
    address 192.168.13.2
    netmask 255.255.255.0
    gateway 192.168.13.1
```

Configurar en **dx2go** o interface de rede 192.168.13.2/24 e a porta de enlace 192.168.13.1.

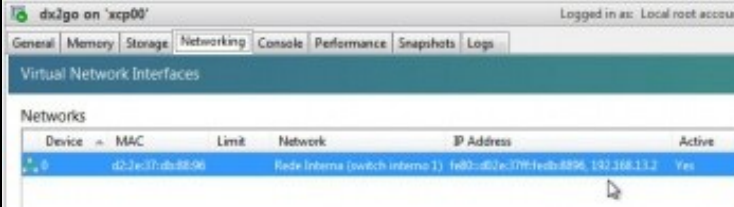
```
root@dx2go:~# ifup eth0
root@dx2go:~#
root@dx2go:~# ifconfig
eth0      Link encap:Ethernet  HWaddr d2:2e:37:db:88:96
          inet addr:192.168.13.2  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::d02e:37ff:fedb:8896/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28 (28.0 B)  TX bytes:8497 (8.2 KiB)
          Interrupt:8

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:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:560 (560.0 B)  TX bytes:560 (560.0 B)
```

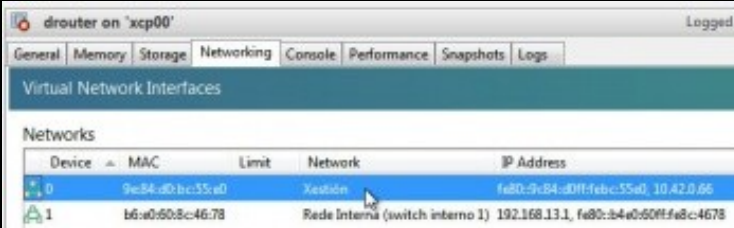
Levantar e subir o interface (ou reiniciar) e revisar a configuración IP.

```
root@dx2go:~# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.13.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
0.0.0.0 192.168.13.1 0.0.0.0 UG 0 0 0 eth0
root@dx2go:~#
```

A porta de enlace de **dx2go** é **drouter:192.168.13.1**.



Observar que as lapelas **Networking** de cada MV ...



... ten asignada/s as IPs correspondentes.

```
root@dx2go:~# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.13.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
0.0.0.0 192.168.13.1 0.0.0.0 UG 0 0 0 eth0
root@dx2go:~#
root@dx2go:~# ping 192.168.13.1
PING 192.168.13.1 (192.168.13.1) 56(84) bytes of data:
64 bytes from 192.168.13.1: icmp_req=1 ttl=64 time=6.78 ms
64 bytes from 192.168.13.1: icmp_req=2 ttl=64 time=8.25 ms
^C
--- 192.168.13.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 6.787/7.519/8.251/0.732 ms
root@dx2go:~#
root@dx2go:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1002ms
root@dx2go:~#
```

Dende **dx2go** facemos ping a **drouter** e funciona pero non funciona ao exterior. Hai que configurar o enrutamento en **drouter**. Pódese realizar o mesmo que se fixo no escenario 2.F anterior. Esta vez imos facelo cos ficheiros de configuración ...

```
root@drouter:~# nano /etc/init.d/iptables.sh
```

... a través de **iptables**]. Quen desexe afondar: <http://www.pello.info/filez/firewall/iptables.html>.

En **drouter** creamos o ficheiro **nano /etc/init.d/iptables.sh**.

```
GNU nano 2.2.4 File: /etc/init.d/iptables.sh
^Tbin/sh

#Habilitar enrutamento
echo 1 > /proc/sys/net/ipv4/ip_forward

#Borrar regras previas
iptables -F
iptables -t nat -F
iptables -Z
iptables -t nat -Z

#Habilitamos NAT (Sen ter en conta orixes e eth de saída)
iptables -t nat -A POSTROUTING -j MASQUERADE
#Permitir toda comunicación dende rede interna ao exterior
iptables -A FORWARD -s 192.168.13.0/24 -i eth1 -j ACCEPT
#Redireccionar porto 2222 a dx2go porto 22
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2222 -j DNAT --to 192.168.13.1:22
#Permitir conexións entrantes para tráfico previamente establecido
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

O seu contido está ao final deste apartado para ser copiado. **Coidado** ao pegar, pois pode que non pegue algúns retornos de carro. Por iso é bo revisar que o pegado coincida co script. Revisar liña a liña (son pouquiñas).

```
GNU nano 2.2.4 File: /etc/init.d/iptables.sh
Ctrl+Alt+Z
#Habilitar enrutamento
echo 1 > /proc/sys/net/ipv4/ip_forward

#Borrar regras previas
iptables -F
iptables -t nat -F
iptables -Z
iptables -t nat -Z

#Habilitamos NAT (Sea ter en conta orixes e eth de saída)
iptables -t nat -A POSTROUTING -j MASQUERADE
#Permitir toda comunicación dende rede interna ao exterior
iptables -A FORWARD -s 192.168.13.0/24 -i eth1 -j ACCEPT
#Redireccionar porta 2222 a dx2go porta 22
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2222 -j DNAT --to 192.168.0.22
#Permitir conexións entrantes para tráfico previamente establecido
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Asignamos o permiso de execución: **chmod +x /etc/init.d/iptables.sh**.

```
root@router:~# chmod +x /etc/init.d/iptables.sh
root@router:~#
root@router:~# update-rc.d iptables.sh defaults
update-rc.d: using dependency based boot sequencing
insserv: warning: script 'iptables.sh' missing LSB tags and overrides
```

Creamos enlaces nos niveles de execución. Podemos facelo manualmente, tamén podemos poñer unha chamada ao ficheiro en /etc/rc.local para que cando se inicie o equipo se execute o script coas directivas do FW. Pero imos facelo desta outra forma: **update-rc.d iptables.sh defaults**.

Para aprofundar máis **Niveis de execución**:http://es.wikipedia.org/wiki/Nivel_de_ejecuci%C3%B3n. Sobre **update-rc.d**:<http://www.tin.org/bin/man.cgi?section=8&topic=update-rc.d>.

A execución dá un aviso porque no script non usamos os estilos LSB (Linux Standard Base) para este script de inicio: <http://wiki.debian.org/LSBInitScripts>. Pero funciona igual.

Inciamos o servizo **service iptables.sh start** (Ou reiniciar o equipo).

```
root@dx2go:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1002ms

root@dx2go:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=46 time=113 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=46 time=81.6 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=46 time=97.9 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=46 time=86.1 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3014ms
rtt min/avg/max/mdev = 81.604/94.706/113.319/12.245 ms
root@dx2go:~#
```

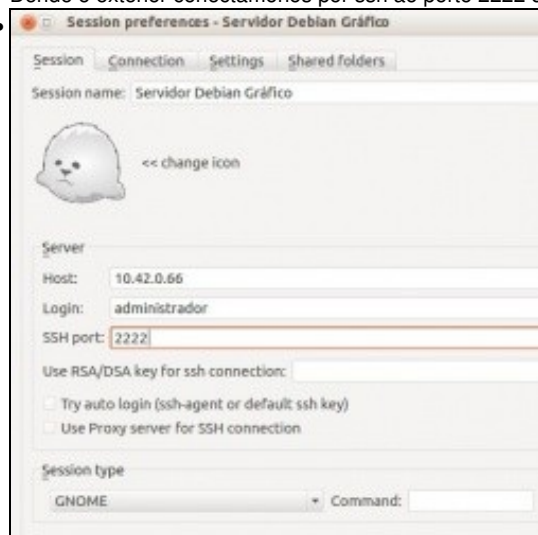
dx2go xa ten conexión co exterior.

```
administrador@base:~$ ssh root@10.42.0.66 -p 2222
The authenticity of host '[10.42.0.66]:2222 ([10.42.0.66]:2222)' can't be established.
RSA key fingerprint is 09:82:db:12:b0:9e:98:bb:ed:e5:d3:3c:c7:a7:35:5e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.42.0.66]:2222' (RSA) to the list of known hosts.
root@10.42.0.66's password:
Linux dx2go 2.6.32-5-and04 #1 SMP Mon Feb 25 00:26:11 UTC 2013 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat May 25 22:10:32 2013
root@dx2go:~#
```

Dende o exterior conectámonos por ssh ao porto 2222 da IP exterior de **router**. Vemos que realmente nos conectamos a **dx2go**.



O mesmo pero dende o cliente X2Go ...



Comprobamos cun **traceroute** os saltos ate o router da rede LAN de saída a internet. Obsérvase que se atravesa **router**.

Script de configuración de iptables

```
#!/bin/sh

#Habilitar enrutamento
echo 1 > /proc/sys/net/ipv4/ip_forward

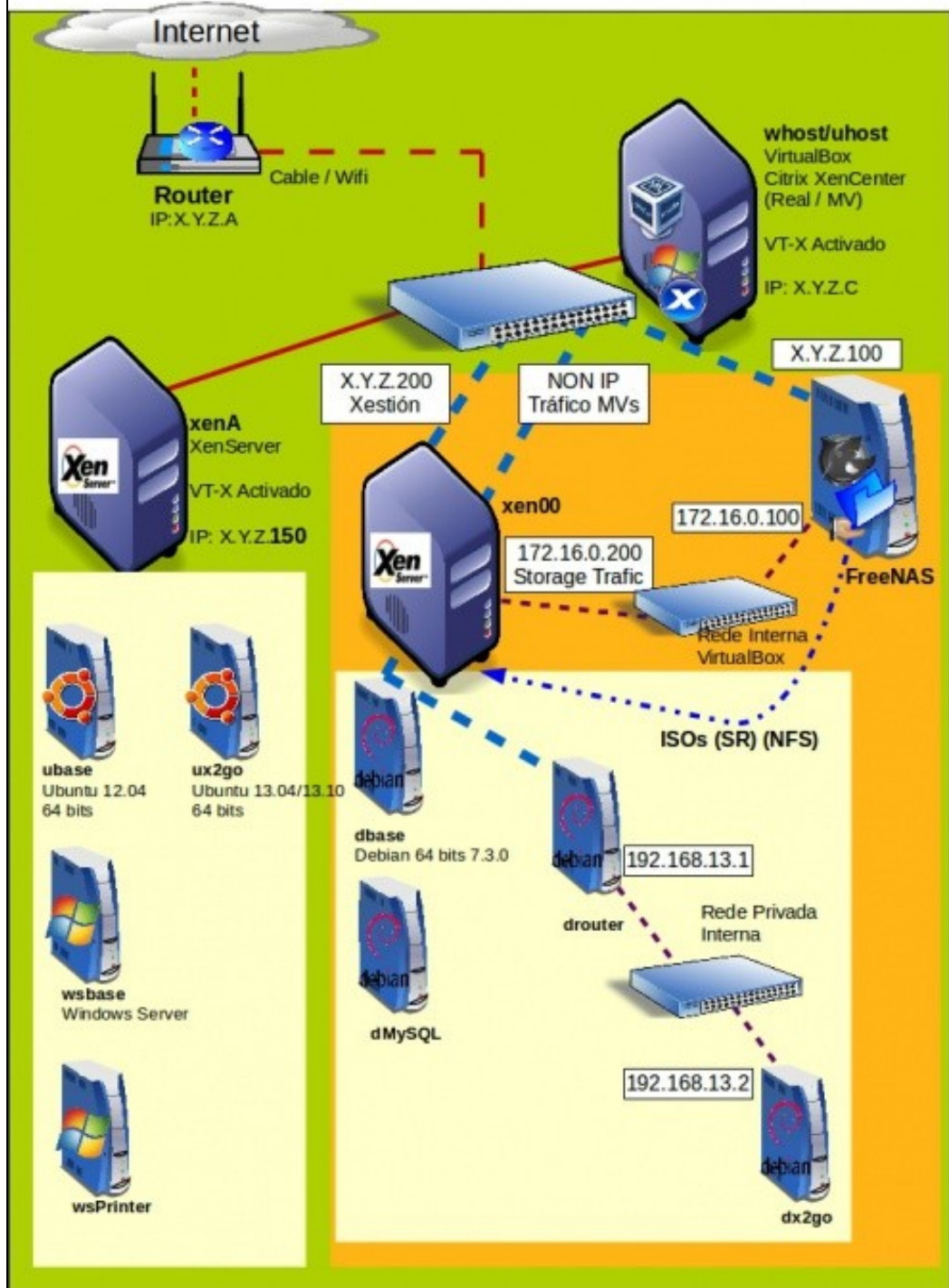
#Borrar regras previas
iptables -F
iptables -t nat -F
iptables -Z
iptables -t nat -Z

#Habilitamos NAT (Sen ter en conta orixes e eth de saída)
iptables -t nat -A POSTROUTING -j MASQUERADE
#Pemitir toda comunicacion dende rede interna ao exterior
iptables -A FORWARD -s 192.168.13.0/24 -i eth1 -j ACCEPT
#Redireccionar porto 2222 a dx2go porto 22
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2222 -j DNAT --to 192.168.13.2:22
#Permitir conexións entrantes para tráfico previamente establecido
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

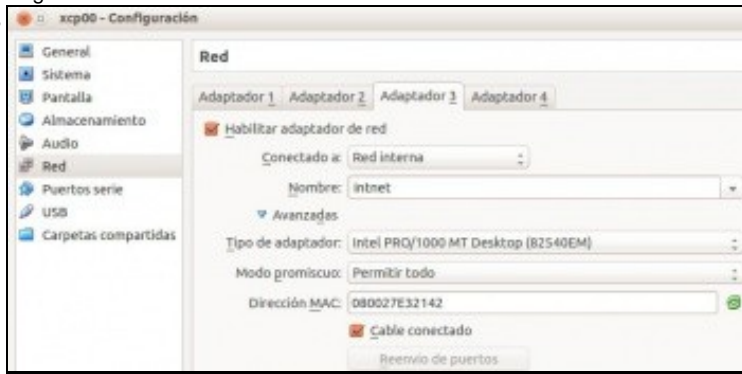
Engadir un novo interface a un host

- Vaise engadir un novo interface ao host (o terceiro), polo cal enviar/recibir o tráfico do almacenamento.
- Neste caso vaise engadir un adaptador de rede ao equipo xen00 en modo rede interna.
- Lembrar que a NAS xa tiña configurados dous adaptadores de rede.

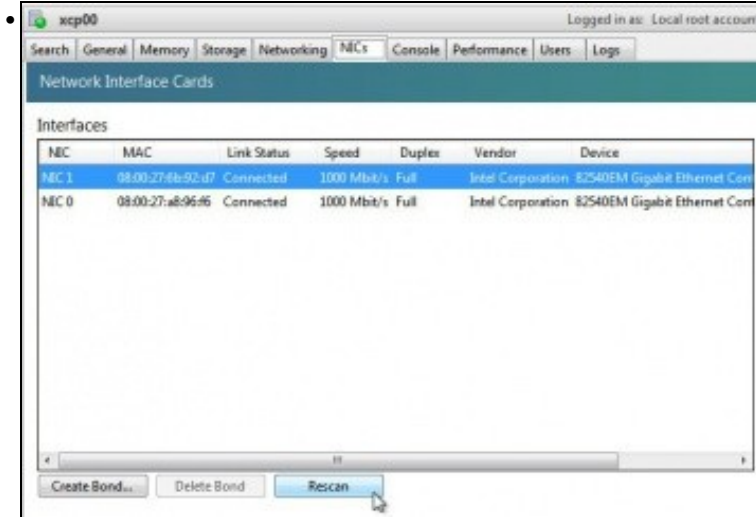
Escenario 6.D: Configuración de Red: Tráfico de almacenamiento



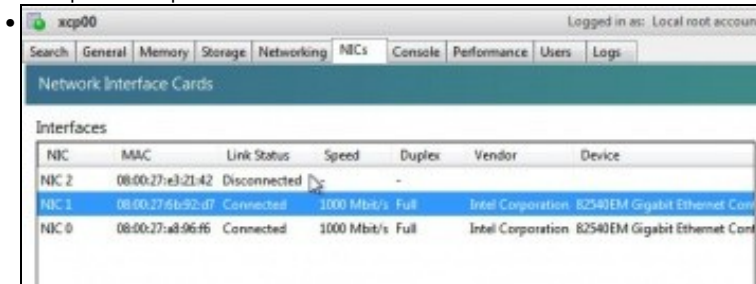
- Engadir NIC ao host



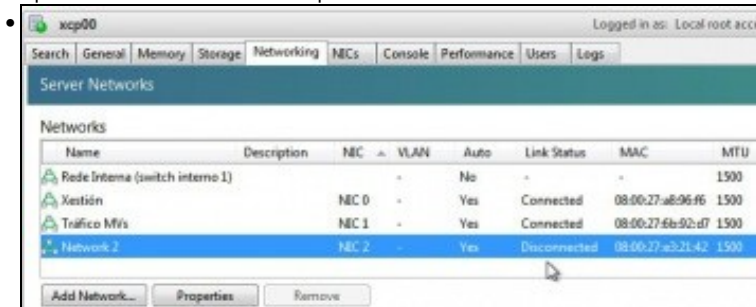
Engadir un novo interface en modo Rede Interna.



Na lapela **NICs** premer en **Rescan**.



Aparece un novo NIC e indica que está desconectado.



O mesmo pasa en **Networking**. Se reiniciamos o host xa o vai recoñecer no próximo inicio e conectar, ou ...

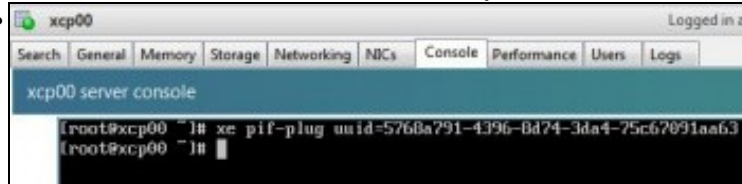
```
[root@xcp00 ~]# xe pif-list
uuid ( RO)                : 78aea93e-11db-f2a8-717f-ec674596945d
  device ( RO)            : eth1
  currently-attached ( RO) : true
  VLAN ( RO)              : -1
  network-uuid ( RO)      : 78c7ee0b-ea07-ac27-7075-3444cd01e960

uuid ( RO)                : 5768a791-4396-8d74-3da4-75c67091aa63
  device ( RO)            : eth2
  currently-attached ( RO) : false
  VLAN ( RO)              : -1
  network-uuid ( RO)      : 236e4acb-ea10-0b74-637a-0df13bdd3cea

uuid ( RO)                : be8132be-3306-dce1-9276-09e9abb837dd
  device ( RO)            : eth0
  currently-attached ( RO) : true
  VLAN ( RO)              : -1
  network-uuid ( RO)      : 8ee98d45-22c1-066d-07a9-3ca3eb595594

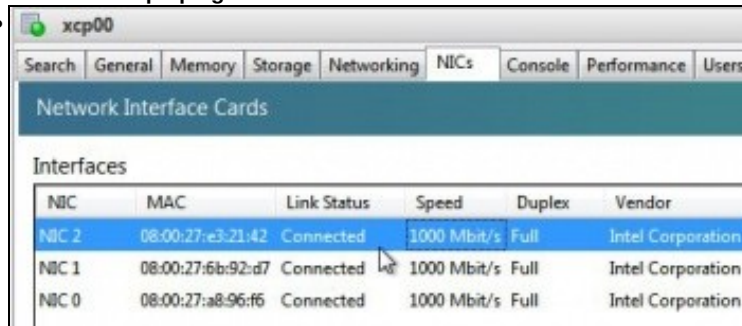
[root@xcp00 ~]#
```

Podemos mirar o uuid do PIF asociado a eth2: **xe pif-list** e ...



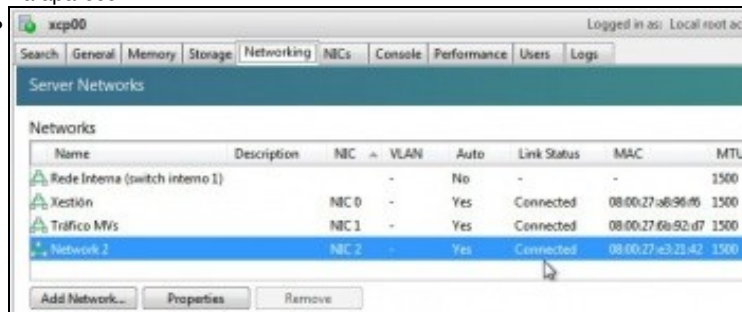
```
[root@xcp00 ~]# xe pif-plug uuid=5768a791-4396-8d74-3da4-75c67091aa63
[root@xcp00 ~]#
```

Conectalo: **xe pif-plug uuid=.....**



NIC	MAC	Link Status	Speed	Duplex	Vendor
NIC 2	08:00:27:e3:21:42	Connected	1000 Mbit/s	Full	Intel Corporation
NIC 1	08:00:27:6b:92:d7	Connected	1000 Mbit/s	Full	Intel Corporation
NIC 0	08:00:27:a8:96:f6	Connected	1000 Mbit/s	Full	Intel Corporation

Xa aparece ...



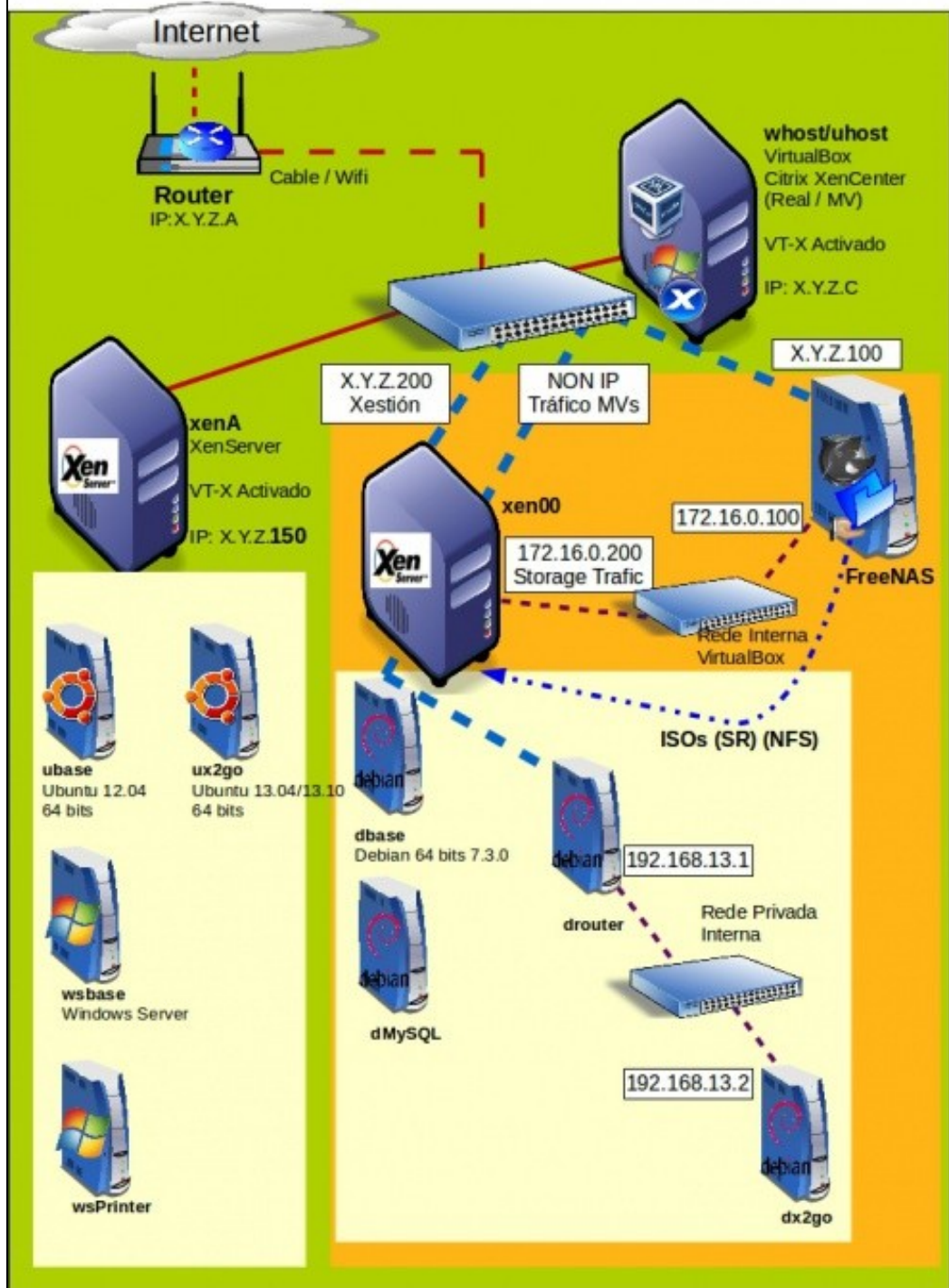
Name	Description	NIC	VLAN	Auto	Link Status	MAC	MTU
Rede Interna (switch interno 1)		-	-	No	-	-	1500
Xestión		NIC 0	-	Yes	Connected	08:00:27:a8:96:f6	1500
Tráfico MVs		NIC 1	-	Yes	Connected	08:00:27:6b:92:d7	1500
Network 2		NIC 2	-	Yes	Connected	08:00:27:e3:21:42	1500

conectado.

Tráfico de almacenamento

- Como se indicaba ao principio, pódese decidir que todo o tráfico do host co almacenamento externo, e viceversa, que se transmita a través dun NIC distinto ao de Xestión e o Tráfico das MVs.
- Na imaxe ese tráfico vaia enviar/recibir a través do novo NIC que acabamos de engadir, e ademais, vai por unha rede de comunicación distinta á do resto do tráfico.

Escenario 6.D: Configuración de Red: Tráfico de almacenamiento



Configuración da NAS

- Neste caso vaise conectar en XenServer ao repositorio de imaxes ISOs da NAS a través de NFS.
- Lembrar que a NAS xa ten dos escenarios anteriores un interface de rede en modo **Rede interna** e coa IP 172.16.0.100.
- Configurar permisos volume ISOs

Nombre	Usado	Disponible	Tamaño	Compression	Compression Ratio	Estado
xen	245.5 KIB (0%)	661.4 GIB	661.4 GIB	lz4	2.09x	HEALTHY
Backup	4.7 GIB (4%)	95.3 GIB	100.0 GIB	inherit	2.08x	HEALTHY
Homes	192.0 KIB (0%)	100.0 GIB	100.0 GIB	inherit	1.00x	HEALTHY
ISOs	192.0 KIB (0%)	50.0 GIB	50.0 GIB	inherit	1.00x	HEALTHY
NFS_VDis	192.0 KIB (0%)	200.0 GIB	200.0 GIB	inherit	1.00x	HEALTHY
xen/MySql_DDBB			100G			HEALTHY
xen/ISCSI_VDis			200G			HEALTHY

Seleccionar o volume ISOs.

Cambiar Permisos

Cambiar los permisos de /mnt/xen/ISOs a:

Propietario (usuario):

Propietario (grupo):

Modo:

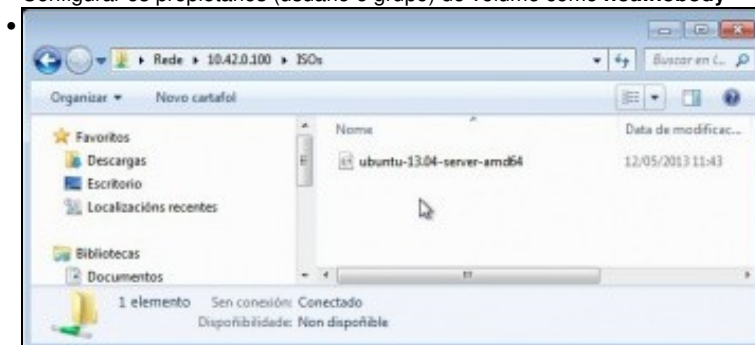
	Owner	Group	Other
Read	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Tipo de permiso ACL:

- Unix
- Windows

Establecer los permisos recursivamente

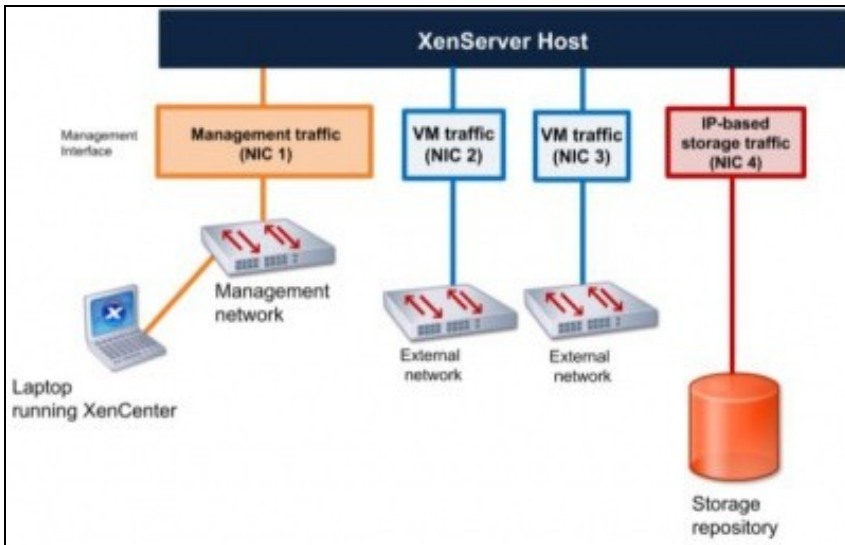
Configurar os propietarios (usuario e grupo) do volume como **noa:nobody**



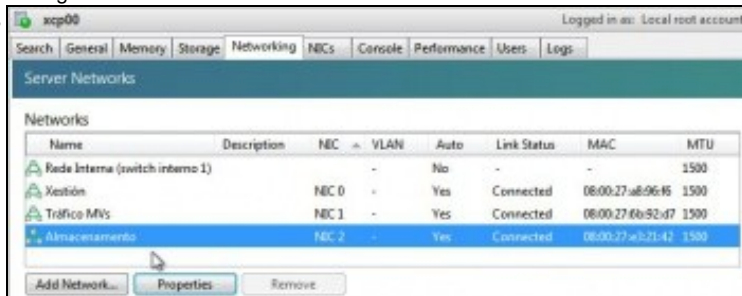
Dende calquera equipo conectarse ao recurso ISOs da NAS e copiar a el unha imaxe ISO. Neste caso foi por CIFS/SAMBA.

Configuración de XenServer

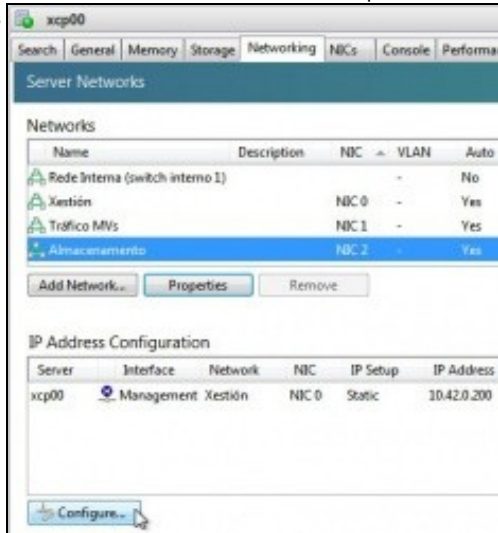
- Lembrar que a rede asociada ao tráfico do almacenamento debe ter unha IP.



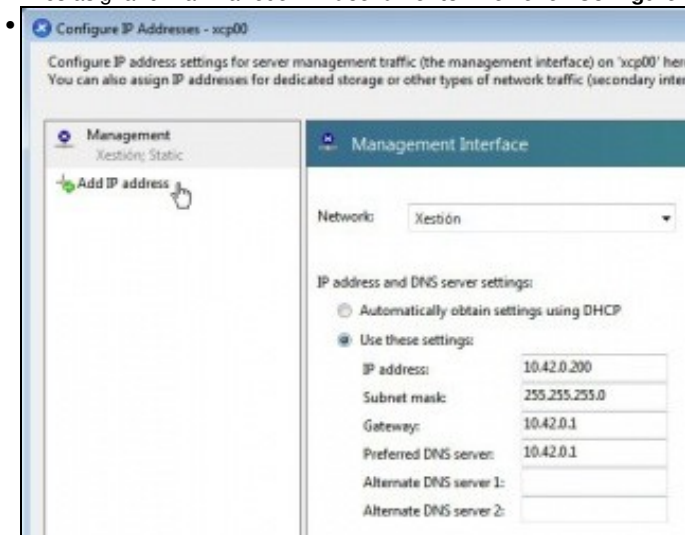
- Configurar rede armazenamento



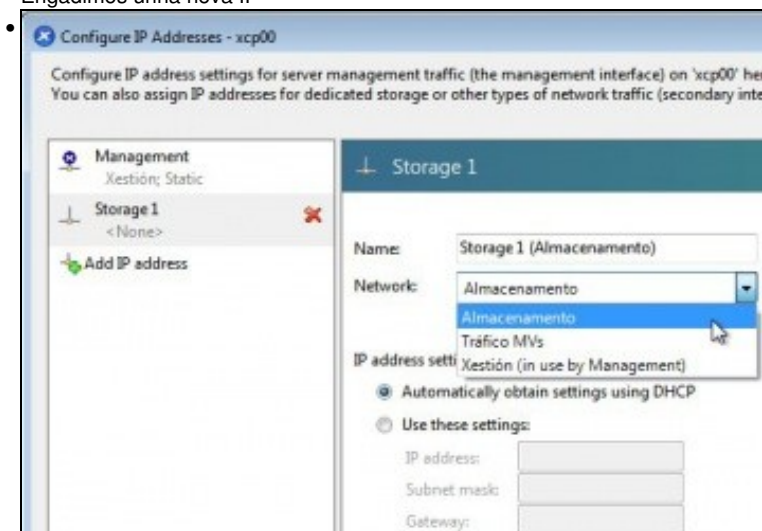
Renomear a rede á **Almacenamiento** para axudarnos a identificar cada Switch virtual.



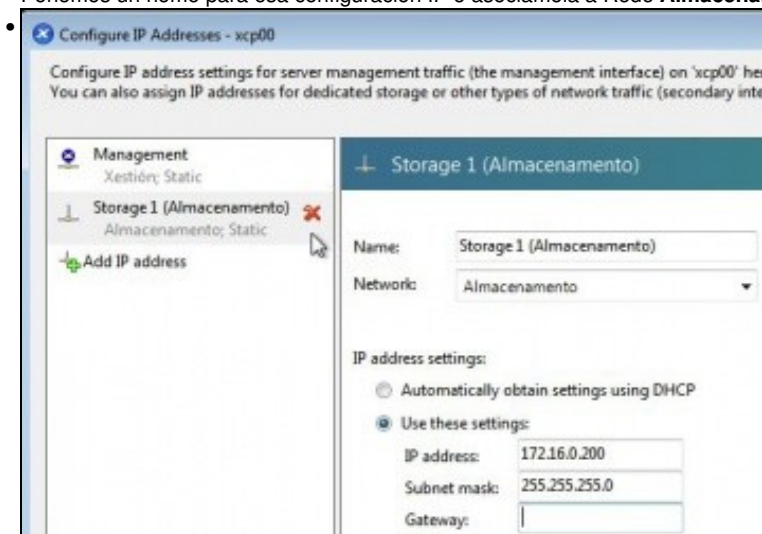
Imos asignar unha IP á rede **Almacenamento**. Premer en **Configure**.



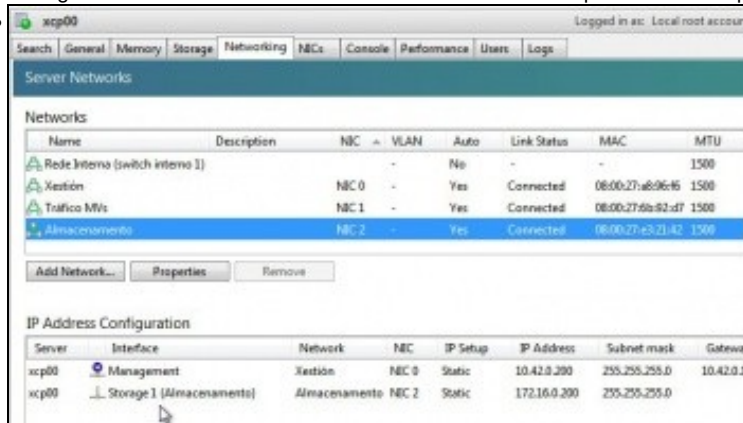
Engadimos unha nova IP



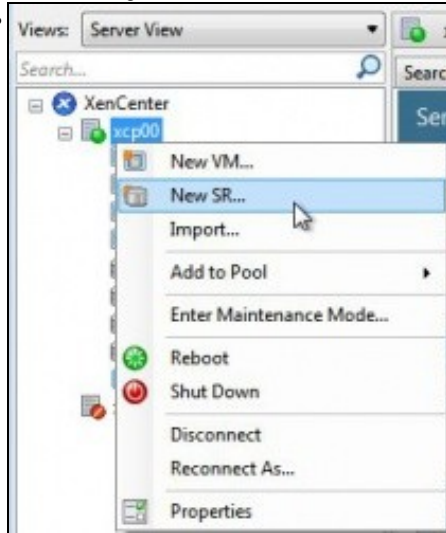
Poñemos un nome para esa configuración IP e asociámola á Rede **Almacenamento**.



Configuramos a IP 172.16.0.200/24. Neste caso non fai falla porta de enlace para chegar até o almacenamento.



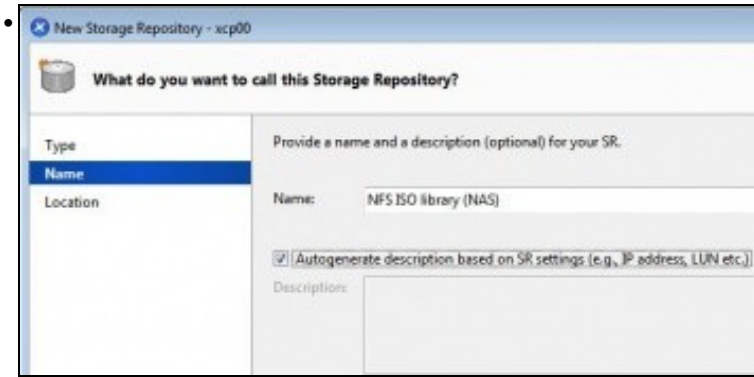
A nova configuración IP ...



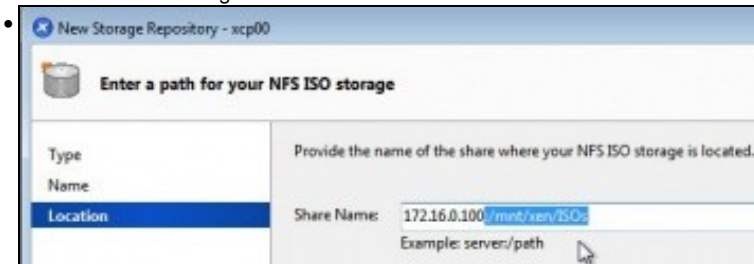
Agora creamos un novo Storage Resource ...



Seleccionamos NFS ISO



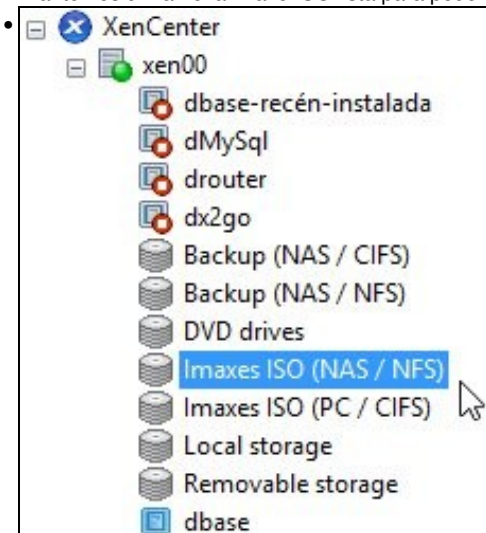
Poñemos un nome significativo.



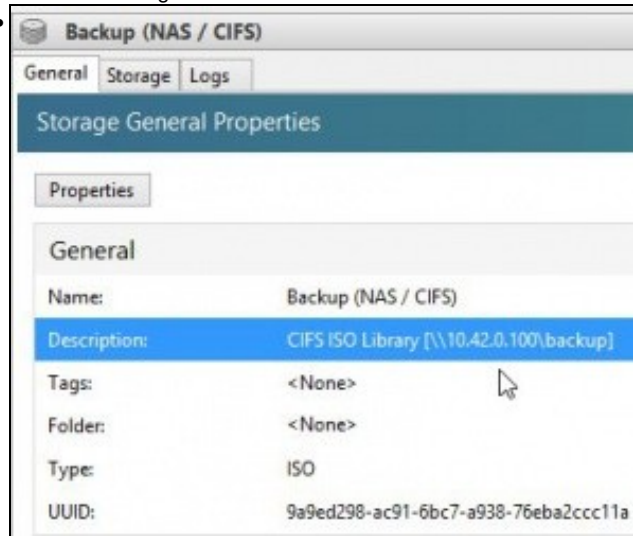
Indicamos a localización do repositorio. **172.16.0.100:/mnt/xen/ISOs**.



E aí temos unha nova imaxe ISO lista para poder ser usada nunha instalación dunha MV.



Para ter todo organizado renoméanse os nomes dos recursos de almacenamento asociados coas imaxes ISO.



Por outra banda se miramos calquera dos SR Backups (tanto CIFS como NFS) están conectados á NAS a través da **IP X.Y.Z.100**. Isto é, a través da rede **Xestión (NIC0)**.

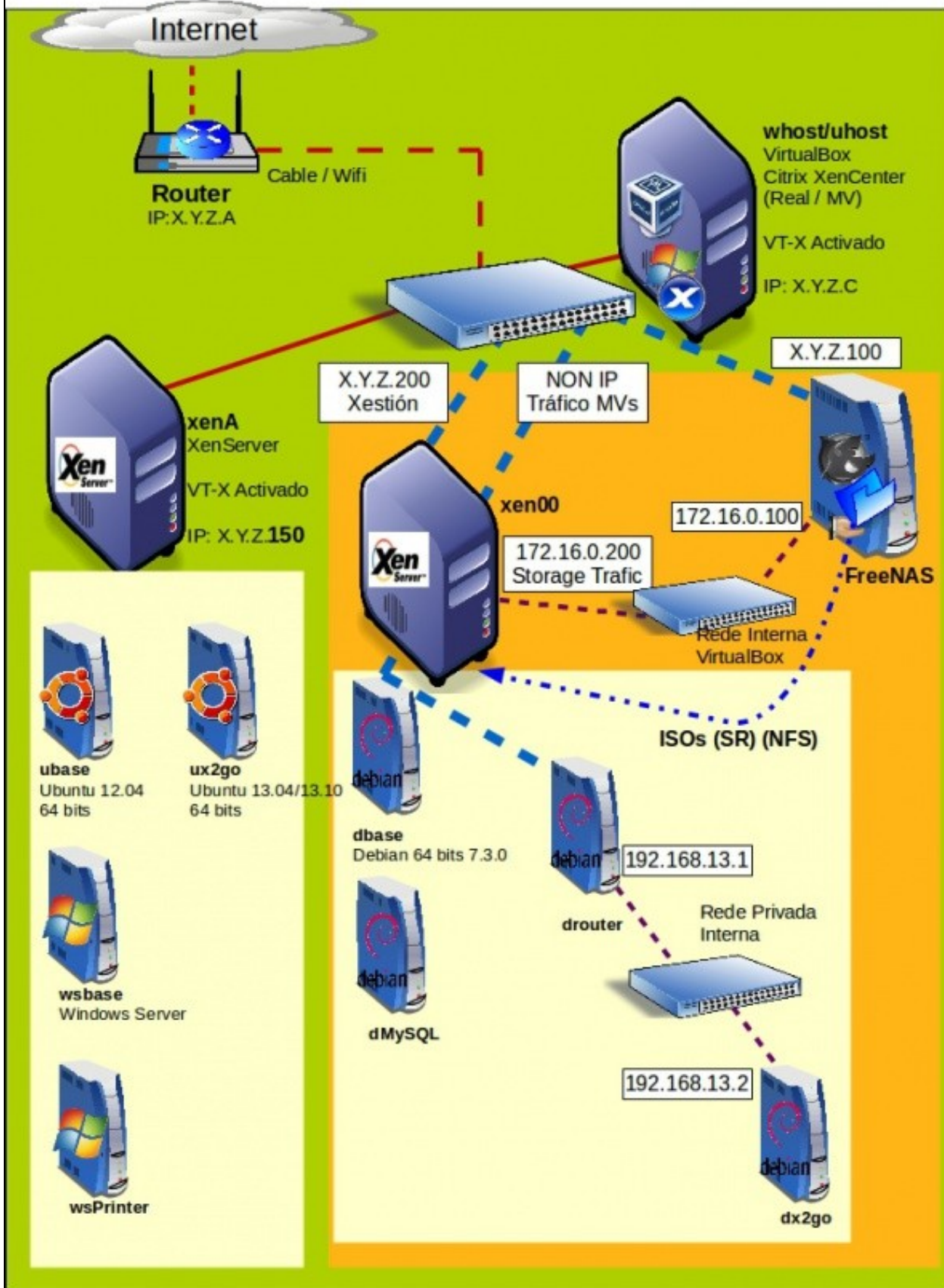
Agora sería o momento de desconectar estes dous SRs de Backup e conectalos de novo pero, a través do outro enlace da NAS: **172.16.0.100**, facendo uso en XenServer da Rede de **Almacenamento (NIC2)**.

Non o imos facer para logo ver o seu comportamento cando se produzan fallos no sistema.

Conclusión final sobre a xestión das redes en XEN

- O escenario 6.D é un resumo de todo o visto:

Escenario 6.D: Configuración de Red: Tráfico de almacenamiento



- Unha rede para o **tráfico de xestión**. Ten configuración IP: X.Y.Z.200
- Unha rede para o **tráfico das MVs**. *NON* ten configuración IP.
- Unha rede para o **tráfico do almacenamento**. Ten configuración IP: 172.16.0.200
- Unha **rede privada interna** que serve para comunicarse entre as MVs. *Non* ten configuración IP. Son as MVs as que teñen IP, non a rede.

- Nos seguintes apartados incorporaremos máis modos de almacenamento e veremos o que pasa cando se crea un Pool con 2 servidores sendo este o Mestre.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez (Maio-2013, Rev1: Feb 2014 - Rev2: Nov 2014)