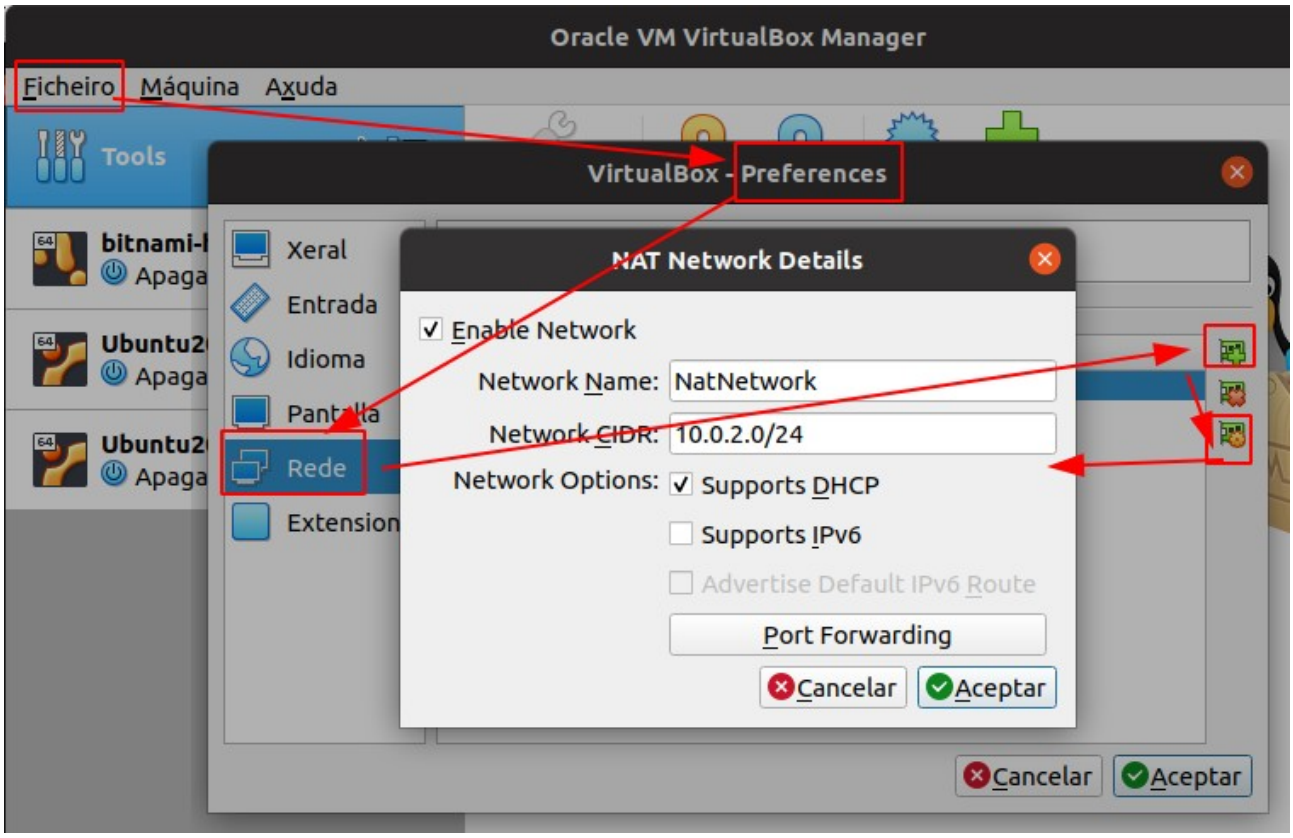
Sobre os distintos tipos de interfaces de rede de Virtual Box:
http://web.iesrodeira.com/mediawiki/index.php/Configuraci%C3%B3n_rede_VirtualBox

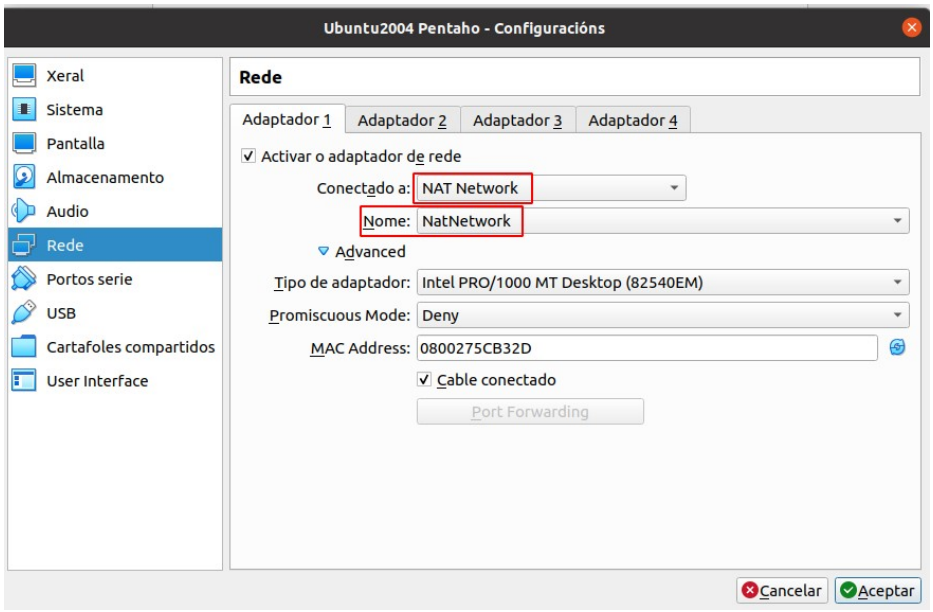
Interface de rede Nat Network

Para crear unha rede interna entre as máquinas virtuais, pero que teñan acceso a Internet, hai que configuralas cunha conexión de rede de tipo ***Nat Network***.

Previamente hai que defini-lo rango de IPs desa rede e darlle un nome que a identifique en Virtual Box para a súa asignación a máqinas virtuais. Por exemplo a "**10.0.2.0/24**" baixo o nome "**NatNetwork**"



De seguido só hai que indicar que o interface de rede que usan as máquinas virtuais é o que configuramos previamente como *Nat Network*.



Moi importante estas recomendacións para a exportación de máquinas virtuais.
Respecto á configuración das tarxetas de rede:

- Usar o modelo de tarxeta paravirtualizada, e se non o modelo Intel PRO/1000.
- Cando exportamos ou copiamos unha MV dunha máquina física a outra, é preferible cambiar antes as tarxetas de rede a modo NAT, xa que co modo ponte a tarxeta de rede queda enlazada a unha intefaz real da máquina host (eth0, wlan0, Conexión de área local, etc.). Cando logo importemos ou agreguemos a MV na máquina de destino, se esa interfaz non existe producirase un erro ó agregar a máquina.
    - Té-las tarxetas no modo NAT para evitar que queden "ligadas" coa tarxeta real do equipo anfitrión.
- Logo de importada a máquina virtual xa se pode cambia-lo interface novamente a bridge e se houbera problemas, usa-lo parámetro: ***--briggeadapter1 eth0***, co comando indicado para "liga-lo" interface virtual que se modifica, co interface real da nova máquina anfitriona (supoñenndo que, no caso do exemplo, este fose a 1ª tarxeta de rede, e que se indentifica por eth0).

Moi importante isto de que en modo bridge a máquina invitada queda "enlazada á interface real" e iso provoca un erro en caso de importación noutra máquina de destino.

Enderezos de rede privados

Os enderezos privados non se poden enrutar a través de Internet.

O RFC 1918 define uns rangos de enderezos IP privados, a utilizar en redes que requiran -ou non- un acceso limitado a Internet:

- rede 10.0.0.0**/8** (10.0.0.0 a 10.255.255.255)
- rede 172.16.0.0**/12** (172.16.0.0 a 172.31.255.255), usualmente convertida a 16 subredes dende 172.16.0.0/16 á 172.31.0.0**/16**
- rede 192.168.0.0**/16** (192.168.0.0 a 192.168.255.255), usualmente convertida en 256 subredes dende a 192.168.0.0/24 á 192.168.255.0**/24**

Na RFC 6598, a IANA reservou outro grupo de enderezos non enrutables globalmente, para que se utilicen en redes de proveedores de servizos (ISPs), coñecidos como "espazo de enderezo compartido":

- 100.64.0.0/10

Outros enderezos reservados

As **direccións de loopback (bucle)** están reservadas para que os host as utilicen para dirixi-lo tráfico cara a eles mesmos:

- 127.0.0.0/8 (da 127.0.0.0 á 127.255.255.255)

A dirección de loopback crea un método de acceso directo para as aplicacións e servizos TCP/IP que se executan no mesmo dispositivo para comunicarse entre si.

O RFC 3330 define un bloque chamado **direccións link-local** (tamén coñecidas como **APIPA: Automatic Private Internet Protocol Addressing - Direccionamiento Privado Automático do Protocolo de Internet**) que son asignadas polo sistema

operativo automaticamente en entornos de rede nos que non se dispón dunha configuración IP.

- 169.254.0.0/16 (da 169.254.0.0 á 169.254.255.255)

Pódense usar para obter unha configuración de rede cando o sistema está configurado para obter unha dirección dinamicamente e, ó iniciarse, este non atopa un servidor DHCP (Dynamic Host Configuration Protocol): o procedemento APIPA asigna unha dirección IP e a súa máscara de rede unicamente, e non configura ningún outro parámetro que configuraría un servidor DHCP, como poden ser unha ruta por omisión ou un servidor DNS. Isto significa que o sistema APIPA permite a funcionalidade básica para que o equipo funcione nun esquema de rede local, pero non proporcionará saída fóra da mesma, a Internet.

As **direccións test-net** resérvanse para o ensino e a aprendizaxe (a miúdo atópanse en uso cos nomes example.com ou example.net na documentación das RFC)

- 192.0.2.0/24 (da 192.2.0.0 á 192.2.0.255)

Portos TCP - UDP /IP

Un porto de rede é unha interface para comunicarse cun programa a través dunha rede.

Un porto adoita estar numerado. A implementación do protocolo no destino utilizará ese número para decidir a que programa entregará os datos recibidos. Esta asignación de portos permite a unha máquina establecer simultaneamente diversas conexións con máquinas distintas, xa que todos os paquetes que se reciben teñen a mesma dirección, pero van dirixidos a portos diferentes.

Os números de porto indícanse mediante unha palabra, 2 bytes (16 bits), polo que **existen 65535**. Aínda que podemos usar calquera deles para calquera protocolo, existe unha entidade, o *ICANN (Internet Corporation for Assigned Names and Number)* -anteriormente chamada *IANA*-, encargada da súa asignación. Creáronse tres categorías:

- Os **portos inferiores ó 1023 son portos reservados** para para servizos e aplicacións e **usados por "*protocolos ben coñecidos*"**. Se queremos usar un destes portos teremos que arrincar o servizo que os use tendo permisos de administrador, xa que só un superusuario ten os privilexios necesarios para abrilos.
    - Utilízanse comunmente para aplicacións como HTTP (servidor Web), protocolo de acceso a mensaxes da internet (IMAP) ou protocolo simple de transferencia de correo (SMTP) (servidor de correo electrónico) e Telnet. Ó definir estes portos ben coñecidos para as aplicacións dos servidores, as aplicacións cliente pódense programar para solicitar unha conexión a ese porto en particular e o servizo relacionado.
- Os comprendidos **entre 1024 (0400 en hexadecimal) e 49151 (BFFF en hexadecimal) son denominados "rexistrados" e poden ser usados por calquera aplicación. Existe unha lista publica na web do ICANN onde se pode ver que protocolo usa cada un deles**.
    - Estes números de porto asígnanse a procesos ou aplicacións do usuario. Principalmente, estes procesos son aplicacións individuais que o usuario elixe instalar en lugar de aplicacións comúns que recibiría un número de porto ben coñecido. Cando non se utilizan para un recurso do servidor, un cliente pode seleccionar estes portos de forma dinámica como o seu porto de orixe. Estes son os portos que as aplicacións de tipo servidor teñen que utilizar para aceptar conexións.
- Os comprendidos **entre os números 49152 (C000 en hexadecimal) e 65535 (FFFF en hexadecimal) son denominados dinámicos, privados ou efímeros**, porque **son os usados polo sistema operativo cando unha aplicación ten que conectarse a un servidor e por tanto necesita un porto por onde saír**.
    - Xeralmente asígnallos de forma dinámica ás aplicacións cliente cando o cliente inicia unha conexión a un servizo, para establece-la conexión do lado do cliente cara ó servidor. O porto dinámico adoita utilizarse para identificar a aplicación cliente durante a comunicación, mentres que o cliente utiliza o porto ben coñecido para identificar o

servizo que se solicita no servidor e conectarse ó devandito servizo. Cando unha aplicación actúa como cliente e necesita conectarse a un servidor se lle asigna un porto efímero; unha vez que a conexión terminou ese porto queda libre e pode ser reutilizado novamente por calquera outra aplicación. Estes portos asígnanse para conexións curtas, onde a reserva do porto é temporal e somentes existe durante o mantemento dunha canle de comunicación entre dúas computadoras.

- Non é común que un cliente se conecte a un servizo mediante un porto dinámico ou privado (aínda que algúns programas de intercambio de arquivos punto a punto o fan).

En Linux pódese ver unha lista de diferentes aplicaciónes e combinacións de porto/protocolo no arquivo `/etc/services` usando o comando cat:

```
$ cat /etc/services
```

Para enumerar tódolos portos abertos ou portos que se executan actualmente, incluídos TCP e UDP en Linux, úsase o comando `netstat`:

```
$ netstat -lntu
```

```
administrador@ubuntucesga:~$ sudo netstat -lntpu
[sudo] Contrasinal de administrador:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      527/systemd-resolve
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      713/cupsd
tcp6       0      0 ::1:631                 :::*                    LISTEN      713/cupsd
udp        0      0 0.0.0.0:631             0.0.0.0:*                           736/cups-browsed
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           567/avahi-daemon: r
udp        0      0 0.0.0.0:47101           0.0.0.0:*                           567/avahi-daemon: r
udp        0      0 127.0.0.53:53           0.0.0.0:*                           527/systemd-resolve
udp6       0      0 :::5353                 :::*                                567/avahi-daemon: r
udp6       0      0 :::48921                :::*                                567/avahi-daemon: r
```

`-l` : imprime só sockets de escoita

`-n` : amosa o número de porto

`-t` : amosa portos tcp

`-u` : amosa portos udp

`-p` : amosa o nome do programa que usa o porto

También pódese usa-lo comando `ss`, que permite examinar sockets nun sistema Linux.

```
$ ss -lntpu
```

```
administrador@ubuntucesga:~$ sudo ss -lntpu
Netid       State        Recv-Q       Send-Q             Local Address:Port             Peer Address:Port       Process
udp         UNCONN       0            0                        0.0.0.0:631                   0.0.0.0:*           users:(("cups-browsed",pid=736,fd=7))
udp         UNCONN       0            0                        0.0.0.0:5353                  0.0.0.0:*           users:(("avahi-daemon",pid=567,fd=12))
udp         UNCONN       0            0                        0.0.0.0:47101                 0.0.0.0:*           users:(("avahi-daemon",pid=567,fd=14))
udp         UNCONN       0            0                  127.0.0.53%lo:53                    0.0.0.0:*           users:(("systemd-resolve",pid=527,fd=12))
udp         UNCONN       0            0                           [::]:5353                     [::]:*           users:(("avahi-daemon",pid=567,fd=13))
udp         UNCONN       0            0                           [::]:48921                    [::]:*           users:(("avahi-daemon",pid=567,fd=15))
tcp         LISTEN       0            4096               127.0.0.53%lo:53                    0.0.0.0:*           users:(("systemd-resolve",pid=527,fd=13))
tcp         LISTEN       0            5                      127.0.0.1:631                   0.0.0.0:*           users:(("cupsd",pid=713,fd=7))
tcp         LISTEN       0            5                          [::1]:631                     [::]:*           users:(("cupsd",pid=713,fd=6))
administrador@ubuntucesga:~$
```