Guía A1 – Instalación y configuración

Contenido de la Guía

Objetivo general de la guía.

- Mostrar el procedimiento para configurar el equipo router1 de forma que dicho equipo provea los servicios DNS, DHCP, Router y Firewall a la nube híbrida de la EMPRESAY

Objetivos específicos.

- Instalar y configurar un servidor DNS con resolución externa utilizando los servidores NS de google y una zona directa para los equipos de la red híbrida.
- Instalar y configurar un servidor DHCP que envíe los parámetros IPv4 a los clientes de forma que se pueda navegar en Internet sin modificar los valores de la red IPv4 privada 192.168.50+Y.0
- Habilitar la función del kernel de Linux que permita en reenvío de paquetes IPv4.
- Instalar y configurar un firewall que permita la comunicación de los equipos de la red IPv4 local utilizando una dirección IPv4 con conexión a Internet

Nomenclatura de la guía:

En esta guía se ha utilizado el siguiente formato:

- Fuente courrier en negrita para los comandos que deben digitarse, por ejemplo:
  `root@front-end:~# ps aux |grep sshd`
- Texto con resaltado en amarillo, para la información que debe visualizar cuando realice algún procedimiento o comando. Puede contener color rojo dentro del fondo amarillo.
  ```
  root@front-end:~# mcedit /etc/resolv.conf
  search empresay.com.sv
  nameserver   192.168.2.1
  ```
- Las notas o consideraciones se destacan con: **Nota:**

La información aquí presentada ha sido creada por Víctor Cuchillac (padre), cualquier uso o referencia debe citarse al autor.

I. Indicaciones sobre la guía

1.1 Descripción del escenario global.

Usted y su equipo de trabajo han sido contratados para instalar y configurar en la EMPRESAY una nube híbrida formada por una nube privada con OpenNebula y una nube pública con equipos en AWS (Amazon)

Para realizar el macro proyecto se realizarán las siguientes tareas.

- Instalación y configuración de un Router con DNS y DHCP
- Instalación y configuración de un DataStore
- Instalación y configuración de un Frontend para el manejo de los hipervisores
- Instalación y configuración de un Hipervisor KVM
- Instalación de un Hipervisor XEN
- Instalación de un hipervisor ESXi
- Configuración de equipos en nube pública con AWS

En el siguiente cuadro se muestran los equipos que se tendrán al final del macro escenario,

Equipos que forman parte de la nube híbrida de la EMPRESAY				
No.	**Función**	**Servicios que ofrece**	**Tecnología**	**Nombre**
1	Infraestructura	DHCP (recomedado), DNS, Router y Firewall	Linux Alpine	router1
2	Red SAN	Target iSCSI con dos LUN,	FreeNAS 9.3	datastore1
3	Administrador nube	Controlar las MV de los hipervisores	Opennebula 4.12	frontend1
4	Hipervisor1	Virtualización	KVM + QEMU	hipervisor1
5	Hipervisor2	Virtualización	ESX + API	hipervisor2
6	Hipervisor3 (opcional)	Virtualización	XEN + virt-manager	*hipervisor3*
7	Nube pública	Virtualización	EC2 de AWS (Amazon)	ec2mv1
8	Equipos clientes	Se conectan a los servicios de las MV en los hipervisores	Windows, Linux y Android (opcional)	

Cuadro 1 – Detalle de equipos en la nube híbrida para la empresaY

Consideraciones para el macro escenario:

- El hipervidor3 es opcional y puede ser un equipo con el hipervisor: XEN o Hyper-V. Pero también podría utilizarse las tecnologías Open-VZ o VirtualBox para Nube.
- El equipo router1 se requiere para facilitar la implementación en el laboratorio y su existencia es clave en la implementación de la empresa, (este equipo podría ser sustituido si los estudiantes tuvieran sólidas competencias en la configuración de redes IP).
- El uso de un equipo Android es opcional y puede ser una MV con el sistema operativo 4.2 instalado. Su instalación facilita la comprensión de los servicios de las MV en una nube. Si se agrega se ganan puntos extras.

En la siguiente imagen se ilustra el diagrama de la red.

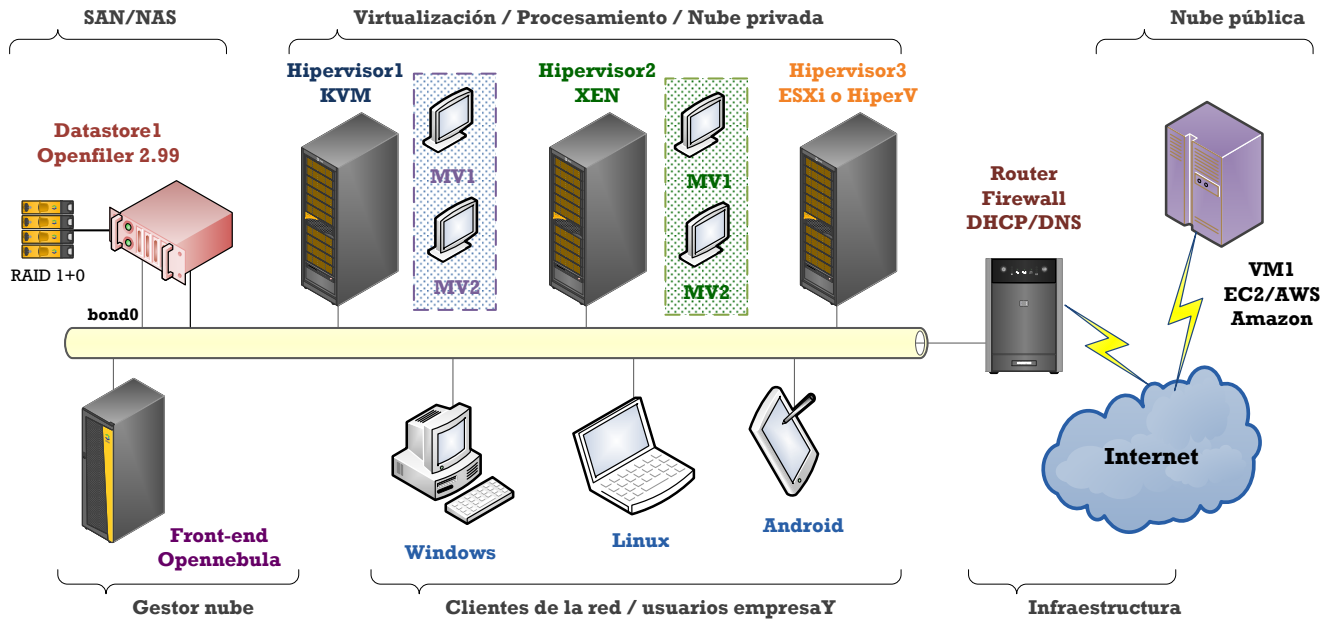


Figura No. 1 – Diagrama del escenario de la nube privada y pública de la empresaY.

A continuación se describen los servicios que desarrollarán cada equipo dentro del macro escenario.

Descripción de los servicios de los equipos de la EMPRESAY			
No.	**Nombre del host**	**Equipo**	**Función**
1	router1	Router con salida a Internet, Firewall	Encaminamiento de paquetes y salida a Internet por NAT
		Servidor DNS/DHCP	Resolución de nombres de los servidores privados y públicos, Asignar IPv4 a los clientes de la empresa
2	datastore1	Datastore con FreeNAS 9.X	Almacenar las VM de los hipervisores Almacenar archivos de datos
3	frontend1	Equipo con Opennebula 4.X	Administrar los hipervisores conectados
4	hipervisor1	Hipervisor con KVM	Ejecutar las MV: kvmMV1, kvmMV2
5	hipervisor2	Hipervisor con ESX	Ejecutar las MV: esxMV1, esxMV2
6	hipervisor3	Hipervisor con XEN	Ejecutar las DomU: xenMV1, xenMV2

Cuadro 2 – Detalle de equipos en la nube híbrida para la EMPRESAY

Para realizar este escenario existen dos opciones, siendo la primera la que se utilizará en los laboratorios

- La interconexión de dos o más computadoras
- Un equipo con suficiente capacidad de proceso (i7 con cuatro núcleos) y suficiente RAM (8 GB Mín 16 recomendado)

Nota: Para garantizar que no exista una dirección MAC, una IPv4, un host y un dominio duplicado en la red del laboratorio, se utilizará la siguiente nomenclatura:

- Y = representa el número del grupo de trabajo, y se utilizan dos dígitos
- X = representa el número del estudiante, se utilizan dos dígitos (cuando cada estudiante instala el equipo)

Ejemplos:	**Grupo 7 y estudiante 1**	**Grupo 05 y estudiante 2**	**Grupo 11 y estudiante 3**
MAC 02:**Y:X**:B0:00:02	02:**07:01:**B0:00:02	02:**05:02**:B0:00:02	02:**11:03**:B0:00:02
empresa**Y**.com.sv	empresa**07**.com.sv	empresa**05**.com.sv	empresa**11**.com.sv
192.168.**50+Y**.3	192.168.5**7**.3	192.168.5**5**.3	192.168.**61**.3

Direcciones Físicas para cada equipo

Para esta guía el escenario de red será el siguiente: (usted haga los cambios pertinentes en la red de su casa o en la red del laboratorio y sustituya Y por el número de grupo)

No.	Equipo	Dirección física	Descripción
1	router1	02:Y:X:B0:00:AA	Router con salida a Internet, firewall
		02:Y:X:B0:00:01	Linux Alpine, Servidor DNS/DHCP
2	datastore1	02:Y:X:B0:00:02	Datastore con FreeNAS 9.X
3	frontend1	02:Y:X:B0:00:03	Equipo con Opennebula 4.X
4	hipervisor1	02:Y:X:B0:00:04	Hipervisor con KVM
5	hipervisor2	02:Y:X:B0:00:05	Hipervisor con ESXi
6	hipervisor3	02:Y:X:B0:00:06	Hipervisor con XEN

Cuadro No. 3 – Asignaciones para direcciones físicas

Escenario IPv4 para la red

Para esta guía el escenario de red será el siguiente: (usted haga los cambios pertinentes en la red de su casa o en la red del laboratorio y sustituya Y por el número de grupo)

No.	Equipo	Dirección física	Descripción
1	router1	IP con salida a Internet	Linux Alpine
		192.168.50+Y.1	Linux Alpine,
2	datastore1	192.168.50+Y.2	Datastore con FreeNAS 9.X
3	frontend1	192.168.50+Y.3	Equipo con Opennebula 4.X
4	hipervisor1	192.168.50+Y.4	Hipervisor con KVM
5	hipervisor2	192.168.50+Y.5	Hipervisor con ESXi
6	hipervisor3	192.168.50+Y.6	Hipervisor con XEN

Cuadro No. 4 – Direcciones IPv4 de los equipos de la red

1.2 Consideraciones Previas

Recursos requeridos:

- Equipo o MV con dos tarjetas de red para la instalación y configuración del router1.
- Conexión a Internet.
- La imagen en formato ISO o el CD del sistema operativo Alphine Linux de 64 bits (enlace para descarga: http://alpinelinux.org/downloads). **Se utilizará esta distribución porque ocupa muy poco espacio de almacenamiento y RAM. Podría utilizarse cualquier sistema operativo Windows server o Linux con los servicios: DNS, DHCP, Router y Firewall si los recursos de los equipos en donde se ejecuten todos los equipos los permita**.
- Una computadora o máquina virtual para comprobar la configuración del router1. Se recomienda utilizar la versión TinyCore–6.4 (enlace para descarga: http://distro.ibiblio.org/tinycorelinux/6.x/x86/release/) **Se utilizará esta distribución porque ocupa muy poco espacio de almacenamiento y RAM y no necesita instalarse.**
- KiTTY para Windows.
- WinSCP o FileZilla para Windows.
- Notepad+++ para Windows (opcional)

Consideraciones:

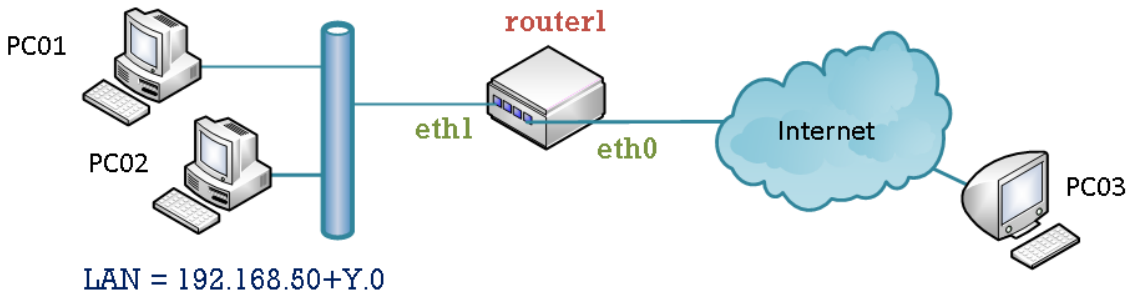
- Si utiliza máquinas virtuales se utilizará VirtualBox versión 5.X (De preferencia), y para cada equipo se utilizarán las direcciones físicas del cuadro 3
- Escriba en un papel todas las direcciones IPv4 de su red, utilice el valor de Y con el número de grupo asignado, por ejemplo: Y=grupo1 192.168.50+**Y**.1 = 192.168.168.51.1 (ver cuadro 4)
- La máquina virtual o equipo que se utilizará para el router1 debe tener dos interfaces de red.

1.3 Escenario de la guía

Se requiere que su equipo de trabajo instale y configure el equipo router1 utilizando la distribución Alpine Linux de 64 bits estable más reciente con los siguientes servicios:

- Servidor DHCP
  - Crear direcciones reservadas para los hipervisores y datastore1
  - Crear pool para clientes (estará desactivado después de las pruebas)
- Servidor DNS
  - Crear el dominio empresaY.com.sv
  - Agregar los registros A del datstore1 e hipervisores
- Router
  - La interfaz de salida será eth0 (dinámica o estática según sea el caso)
  - La interfaz para la LAN será eth1
- NAT y Firewall
  - Se debe permitir el tráfico de los equipos PC01 a Internet
  - Debe existir tráfico IP entre la red LAN y los equipos PC03 (red del laboratorio)

En la siguiente figura se ilustra el escenario de la guía



La computadora PC01 y PC02 será TinyCore 6.4
El equipo PC03 corresponde al equipo Windows 8.1 del laboratorio

II. Desarrollo de la guía.

2.1 Creación de la máquina virtual

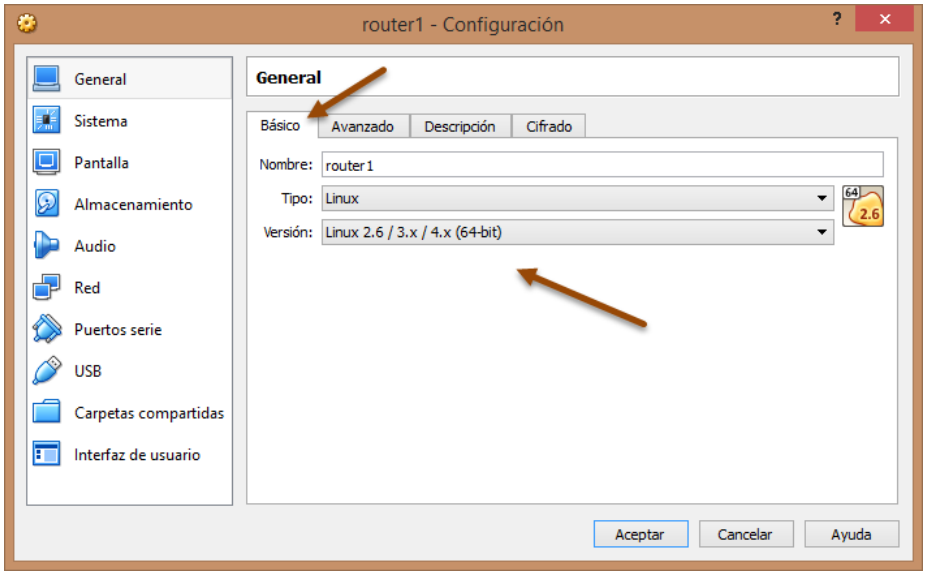
Si desea más información sobre Cómo crear una máquina virtual en VirtualBox, visite la siguiente dirección: http://wiki.alpinelinux.org/wiki/Install_Alpine_on_VirtualBox

Paso 1 – Crear máquina virtual para equipo router1

Cree una máquina virtual con las siguientes características (Linux/256MB/VDI/8GB)

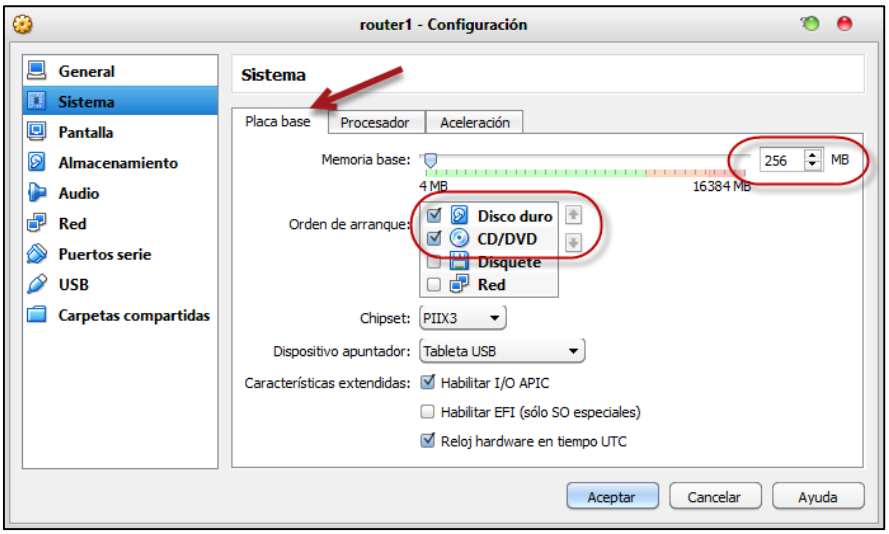
General / Ficha Básico:

- Tipo: Linux
- Versión: Linux 2.6 /3.X (64 bits)



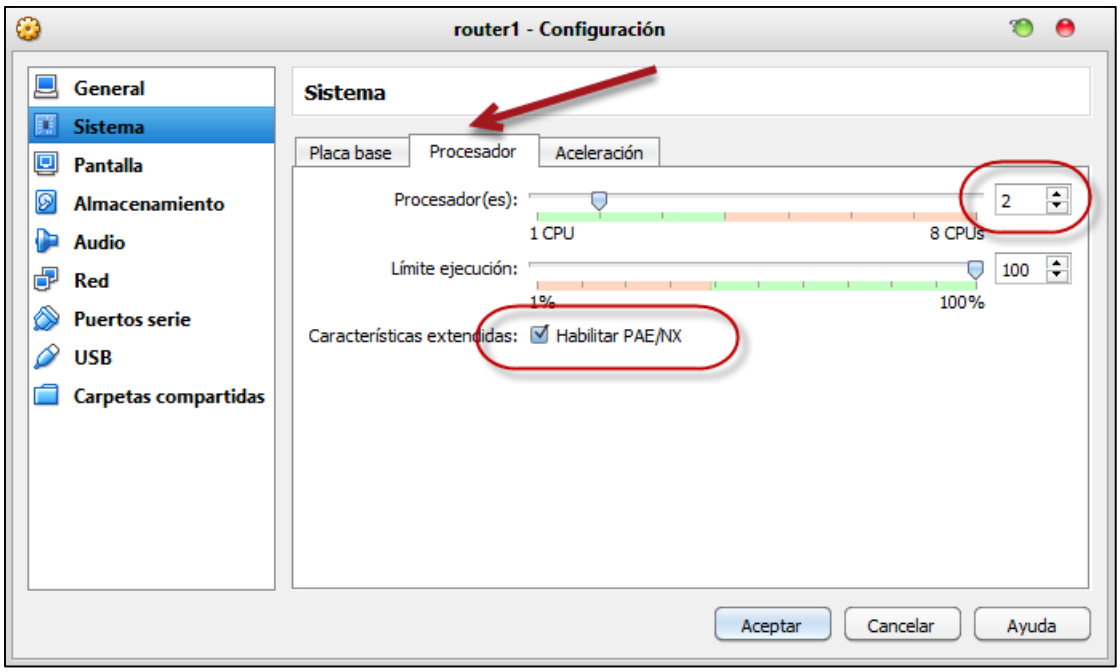
Sistema / Ficha Placa Base:

- RAM: 256 MB (o 512 MB si tiene más recursos)
- Orden de arranque: Disco Duro / CD/DVD (al inicio presione F12 para escoger orden de inicio)



Sistema / Ficha Procesador:

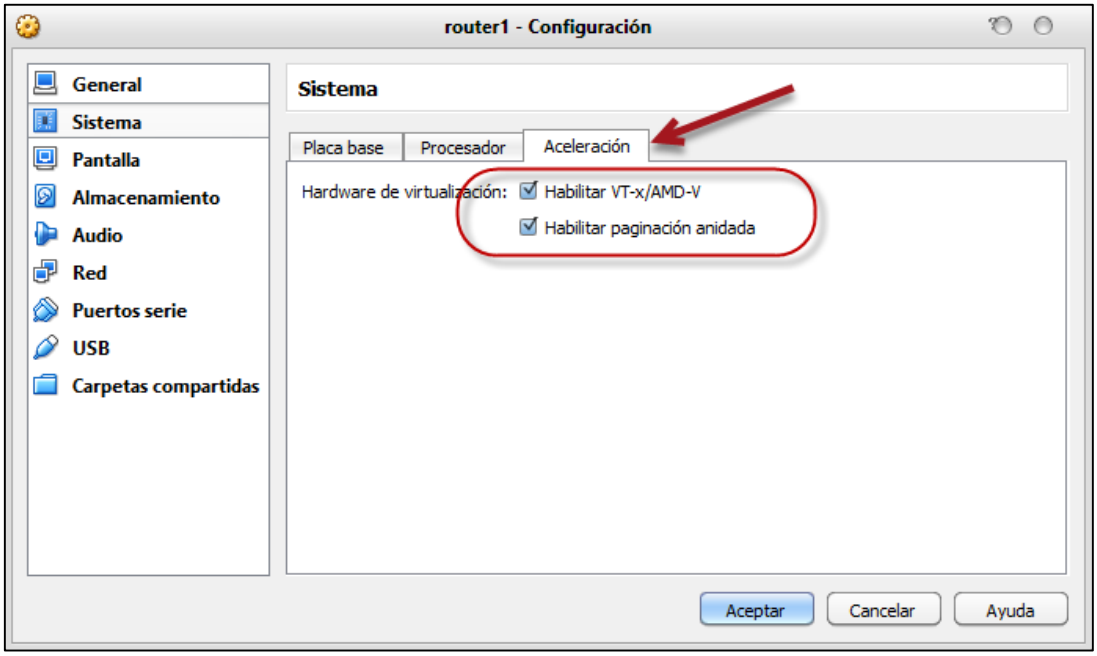
- Procesadores: 2 (recomendado), mínimo 1
- Habilitar el PAE



Sistema / Ficha Aceleración:

- Habilitar extensiones de virtualización.
- Habilitar paginación anidada.

`



Pantalla / Ficha Vídeo:

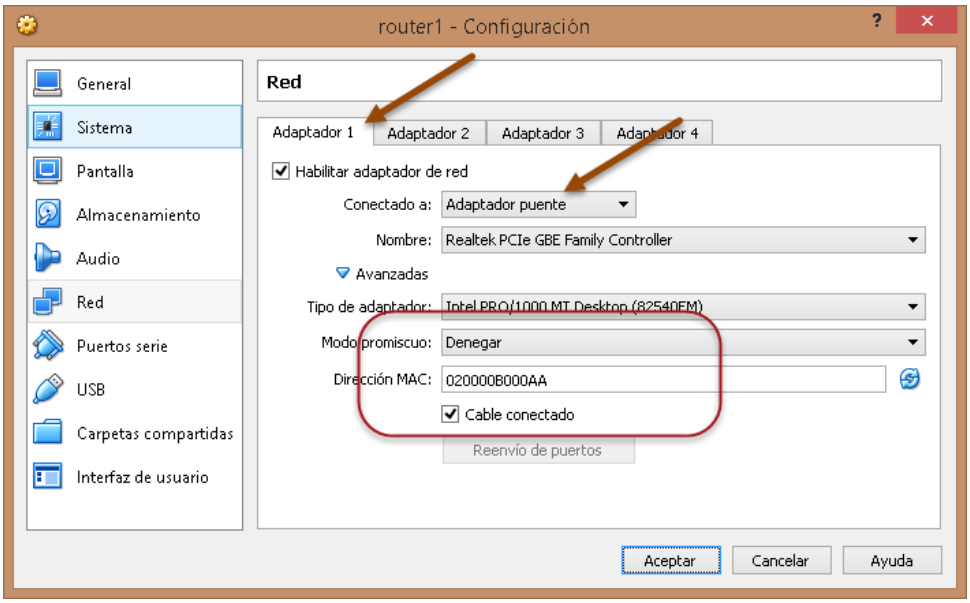
- Memoria Vídeo: 64 MB
- Monitores: 1.

Almacenamiento:

- CDROM tipo IDE con el archivo de Alpine Linux 3.2.3en formato ISO.
- Disco Duro tipo SATA de 4 GB con el nombre router1.vdi

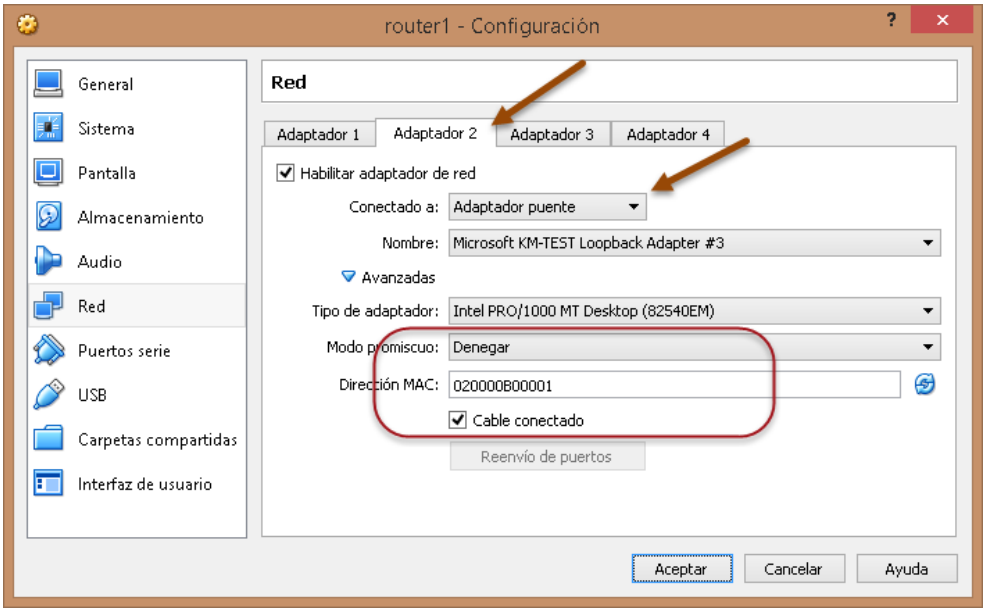
Red / Adaptador1: Esta será la interfaz eth0 y tendrá conexión a Internet.

- Conectado a: Adaptador puente (bridge)
- Nombre de la tarjeta real: Escoja su Ethernet, WIFI o VBoX Host Only.
- Dirección MAC: Defina MAC del cuadro No. 3



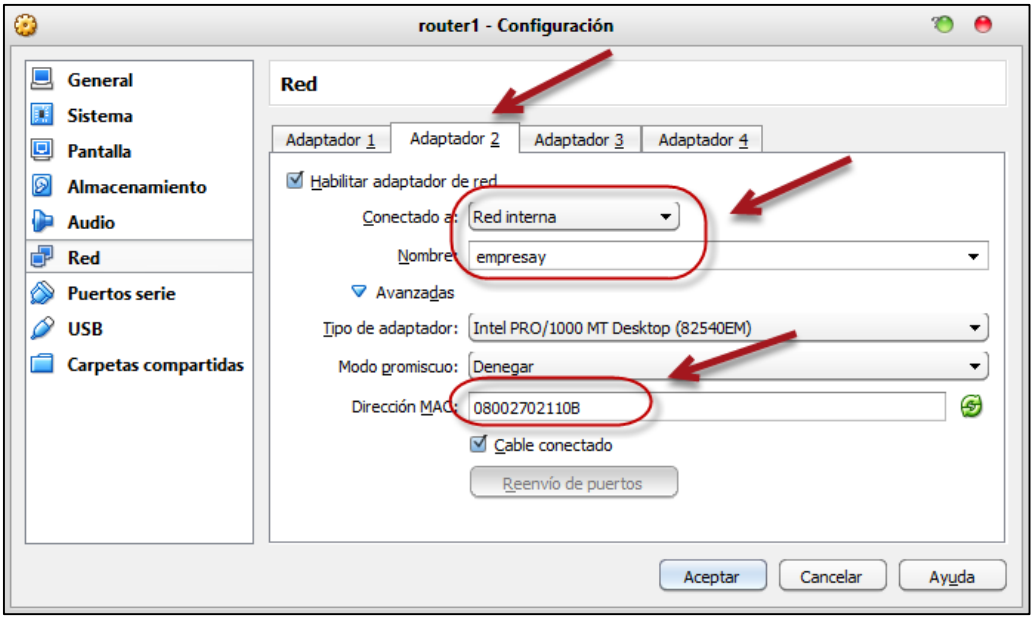
Red / Adaptador2: Opción para equipos en dos o más equipos del laboratorio.

- Conectado a: Adaptador puente
- Nombre de la red interna: Defina
- Dirección MAC: Defina una MAC que le permita identificar la eth1
-



Red / Adaptador2: Esta es una opción para un escenario que se instalará en una sola computadora

- Conectado a: Red Interna
- Nombre de la red interna: Defina "**empresay**", donde y es el número de su grupo {si es laptop}
- Dirección MAC: Defina una MAC que le permita identificar la eth1



Dé un clic en el botón Aceptar y encienda el equipo virtual.

Para el escenario de la nube privada será necesario que:

- La interfaz eth0 tenga salida a internet puede ser de forma estática o dinámicamente.
- La interfaz eth1 será la encargada de comunicarse con los hipervisores, datastore1 y demás equipos.

Nota: Para esta guía se ha utilizado las siguientes direcciones: (usted realice las propias modificaciones)

- IPv4 dinámica para eth0: 192.168.2.106 (puede ser 10.10.3.106, una con salida a Internet)
- IPV4 del GW: 192.168.2.1 (puede ser 10.10.3.254)
- IPv4 del DNS: 192.168.2.1 (puede ser 192.168.1.8)
- IPv4 para la eth1: 192.168.200.1 (192.168.20Y.1, donde Y represente el número del grupo)

Nota: Cuando estén configuradas las direcciones IPv4 del router1 se utilizara para la configuración y ejecución comandos en consola la herramienta KiTTY o PuTTY, tome en cuenta el juego de caracteres

Paso 2 – Comprobación de la conexión hacia Internet (opcional)

Debido a que en la instalación del **router1** se requiere una conexión a Internet, será necesario verificar que la salida hacia la dicha conexión exista. Se puede omitir si se está seguro que la red permitirá la salida a Internet

Presione la tecla “F12” cuando inicie la máquina virtual
Presione la tecla “c” para iniciar desde el CD-ROM virtual

Nota: Para ingresar al sistema el usuario root no tiene password

2.1 Asignación de direcciones IPv4

```
localhost:~# setup-interfaces

Available interfaces are: eth0 eth1.
Enter '?' for help on bridges, bonding and vlans.
```

2.2 Seleccione eth0

```
Which one do you want to initialize? (or '?' or 'done') [eth0] eth0
```

2.3 Seleccione dhcp

```
Ip address for eth0? (or 'dhcp', 'none', '?') [] dhcp
```

2.4 No Seleccione eth1

```
Available interfaces are: eth1.
Enter '?' for help on bridges, bonding and vlans.
Which one do you want to initialize? (or '?' or 'done') [eth1] done
```

2.5 No defina más opciones de red

```
Do you want to do any manual network configuration? [no] no
```

2.7 Reinicio del servicio de red

```
localhost:~# /etc/init.d/networking restart

 * Starting networking ...
 *   lo ...            [ ok ]
 *   eth0 ...          [ ok ]
```

2.7 Reinicio del servicio de red

```
localhost:~# setup-dns
DNS domain name? (e.g 'bar.com') [] empresay.com.sv
DNS nameserver(s)? [192.168.2.1 ] 192.168.2.1
```

2.8 Verifique que tenga una dirección IPv4 válida de la red

```
localhost:~# ifconfig

eth0      Link encap:Ethernet  HWaddr 08:00:27:02:11:0A
          inet addr:192.168.2.106  Bcast:0.0.0.0  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:196 errors:0 dropped:0 overruns:0 frame:0
          TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19246 (18.7 KiB)  TX bytes:16189 (15.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets: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:0 (0.0 B)  TX bytes:0 (0.0 B)
```

2.9 Verifique la dirección IPv4 del DNS

```
localhost:~# cat /etc/resolv.conf

nameserver 192.168.2.1
```

2.10 Verifique la dirección IPv4 del GW (Puede ser el ISP)

```
localhost:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.1     0.0.0.0         UG    202    0        0 eth0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

2.11 Compruebe hay comunicación con un servidor en Intenet

```
localhost:~# ping -c 3 cuchillac.net

PING cuchillac.net (50.87.152.212): 56 data bytes
64 bytes from 50.87.152.212: seq=0 ttl=51 time=127.155 ms
64 bytes from 50.87.152.212: seq=1 ttl=51 time=126.743 ms
64 bytes from 50.87.152.212: seq=2 ttl=51 time=125.114 ms

--- cuchillac.net ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 125.114/126.337/127.155 ms
```

Si en su red o en el laboratorio no se pudiera enviar paquetes ICMP utilice el siguiente comando:

```
localhost:~# nslookup cuchillac.net
nslookup: can't resolve '(null)': Name or service not known

Name:      cuchillac.net
Address 1: 50.87.152.212 50-87-152-212.unifiedlayer.com
```

Paso 3 – Solución de problemas (opcional)

Esta Sección es para utilizarse en caso de tener problemas de comunicación o configuración de red

3.1 Verifique que la eth0 sea IPv4 dinámica

```
localhost:~# cat /etc/network/interfaces
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
        hostname localhost
```

3.2 Verifique que la dirección IPv4 del DNS

```
localhost:~# cat /etc/resolv.conf
nameserver 192.168.2.1
```

Con los siguientes comandos se configurarán las opciones de red

- setup-interfaces = asignación de IPv4 o IPv6
- setup-dns = asignación de servidor DNS

3.3 Comandos a utilizar

```
localhost:~# setup-interfaces
Available interfaces are: eth0 eth1.
Enter '?' for help on bridges, bonding and vlans.
Which one do you want to initialize? (or '?' or 'done') [eth0] eth0
Ip address for eth0? (or 'dhcp', 'none', '?') [192.168.2.106] dhcp
Available interfaces are: eth1.
Enter '?' for help on bridges, bonding and vlans.
Which one do you want to initialize? (or '?' or 'done') [eth1] done
Do you want to do any manual network configuration? [no] no

localhost:~# setup-dns
DNS domain name? (e.g 'bar.com') [] empresay.com.sv
DNS nameserver(s)? [192.168.2.1 ] 192.168.2.1

localhost:~# /etc/init.d/networking restart
 * Stopping networking ...
 *   lo ...                 [ ok ]
 *   eth0 ...               [ ok ]
 * Starting networking ...
 *   lo ...                 [ ok ]
 *   eth0 ...               [ ok ]
```

Paso 4 – Instalación del sistema operativo

4.1 Ejecute script de instalación

```
localhost:~# setup-alpine
```

4.2 Seleccione la distribución de teclado

```
Available keyboard layouts:
be       croat    es       hu       la       pc       se       svwangbe
bg       cz       et       il       lt       pl       sg       tr
br       de       fi       is       mk       pt       sk       ua
by       dk       fr       it       nl       ro       slovene  uk
cf       dvorak   gr       jp       no       ru       sr       us
Select keyboard layout [none]: us
```

4.3 Digite si hay variante en el teclado (en esta guía yo utilizaré inglés)

```
Available variants: us-acentos us
Select variant []: us-acentos
 * rc-update: keymaps already installed in runlevel `boot'; skipping
```

4.4 Defina nombre del equipo

```
Enter system hostname (short form, e.g. 'foo') [localhost]: router1
```

4.5 Configure las interfaces de red

```
Available interfaces are: eth0 eth1.
Enter '?' for help on bridges, bonding and vlans.
```

4.6 Configure la interfaz eth0 (out / internet / exterior)

```
Which one do you want to initialize? (or '?' or 'done') [eth0] eth0
Ip address for eth0? (or 'dhcp', 'none', '?') [192.168.2.106] dhcp
```

4.7 Configure la interfaz eth1 (in / intranet / interna)

```
Available interfaces are: eth1.
Enter '?' for help on bridges, bonding and vlans.
Which one do you want to initialize? (or '?' or 'done') [eth1] eth1
Ip address for eth1? (or 'dhcp', 'none', '?') [dhcp] 192.168.50+Y.1
Netmask? [255.255.255.0] 255.255.255.0
Gateway? (or 'none') [none] Presione enter

Configuration for eth1:
  type=static
  address=192.168.50+Y.1
  netmask=255.255.255.0
  gateway=
Do you want to do any manual network configuration? [no] no
* WARNING: networking has already been started
```

Nota: Si la dirección de la eth0 es estática deberá definir el dominio DNS y la dirección IPv4 del NS

```
DNS domain name? (e.g 'bar.com') [] empresay.com.sv
DNS nameserver(s)? [192.168.2.1 ] 192.168.2.1
```

4.8 Definir la contraseña para el usuario root (123456)

```
Changing password for root
New password:  123456
Bad password: too weak
Retype password: 123456
Password for root changed by root
```

4.9 Definir zona horaria (America/El_Salvador)

```
Which timezone are you in? ('?' for list) [UTC] America/El_Salvador
 * WARNING: you are stopping a boot service
 * WARNING: you are stopping a boot service
 * Setting keymap ...                              [ ok ]
 * Starting busybox acpid ...                      [ ok ]
 * Starting busybox cron ...                       [ ok ]
```

4.10 Definir si existe proxy en la red (Para esta guía no hay)

```
HTTP/FTP proxy URL? (e.g. 'http://proxy:8080', or 'none') [none] none
```

4.11 Definir repositorio de descarga (se necesita conexión a Internet)

```
Available mirrors:
1) nl.alpinelinux.org
2) dl-2.alpinelinux.org
3) dl-3.alpinelinux.org
4) dl-4.alpinelinux.org
5) dl-5.alpinelinux.org
6) distrib-coffee.ipsl.jussieu.fr
7) mirror.yandex.ru
8) mirrors.gigenet.com
9) repos.lax-noc.com
10) mirror1.hs-esslingen.de

r) Add random from the above list
f) Detect and add fastest mirror from above list
e) Edit /etc/apk/repositores with text editor

Enter mirror number (1-10) or URL to add (or r/f/e/done) [f]: f
Finding fastest mirror...
  3.16 http://nl.alpinelinux.org/alpine/
  4.31 http://dl-2.alpinelinux.org/alpine/
  2.83 http://dl-3.alpinelinux.org/alpine/
  2.88 http://dl-4.alpinelinux.org/alpine/
  3.95 http://dl-5.alpinelinux.org/alpine/
. . .
. . .
```

Busca el repositorio con menor tiempo de descarga. Se debe esperar un momento hasta que se prueben los todos enlaces. Si tuviera problemas al seleccionarse el mejor repositorio, seleccione la opción No. 3 ó 4

4.12 Activar servidor ssh (openssh)

```
Which SSH server? ('openssh', 'dropbear' or 'none') [openssh] openssh
 * rc-update: sshd already installed in runlevel `default'; skipping
 * WARNING: sshd has already been started
```

El asistente creará las llaves privadas

4.13 Activar cliente NTP (openntpd)

```
Which NTP client to run? ('openntpd', 'chrony' or 'none') [chrony] chrony
 * service ntpd added to runlevel default
 * Caching service dependencies ...                          [ ok ]
 * Starting ntpd ...                                         [ ok ]
```

4.14 Definir disco de instalación (¡Se borrará todo!)

```
Available disks are:
  sda    (8.6 GB ATA      VBOX HARDDISK   )
  sr0    (0.1 GB VBOX     CD-ROM          )
Which disk(s) would you like to use? (or '?' for help or 'none') [none] sda

The following disk is selected:
  sda    (8.6 GB ATA      VBOX HARDDISK   )
```

4.15 Definir tipo de instalación (sys = sistema operativo)

```
How would you like to use it? ('sys', 'data' or '?' for help) [?] sys
WARNING: The following disk(s) will be erased:
  sda    (8.6 GB ATA      VBOX HARDDISK   )
[############################################################]

WARNING: Erase the above disk(s) and continue? [y/N]: y
Initializing partitions on /dev/sda...
Creating file systems...
Installing system on /dev/sda3:
/mnt/boot is device /dev/sda1
```

Espere un momento mientras se copian y descargan los archivos desde Internet, Si no

4.16 Reinicie el equipo.

```
Instalation is complete Please Reboot

Router1:~# reboot
```

Si desea consultar más información sobre la instalación en el disco, definiendo y creando las particiones de forma manual visite la siguiente dirección: http://wiki.alpinelinux.org/wiki/Install_to_disk

2.2 Instalación de herramientas (recomendado)

Paso 1 – Instalación de editores de texto para consola

1.1 Actualice el listado de paquetes del repositorio oficial

```
router1:~# apk update
WARNING: Ignoring /media/cdrom/apks/x86_64/APKINDEX.tar.gz: No such file or directory
fetch http://dl-2.alpinelinux.org/alpine/v2.7/main/x86_64/APKINDEX.tar.gz
main v2.7.2-10-g49ba8f1 [http://dl-2.alpinelinux.org/alpine/v2.7/main]
OK: 4216 distinct packages available
```

1.2 Instalar mc

```
router1:~# apk add mc

WARNING: Ignoring /media/cdrom/apks/x86_64/APKINDEX.tar.gz: No such file or directory
(1/7) Installing libffi (3.0.13-r0)
(2/7) Installing libiconv (1.12-r8)
(3/7) Installing libintl (0.18.3.1-r1)
. . .
(7/7) Installing mc (4.8.10-r0)
Executing busybox-1.21.1-r0.trigger
Executing uclibc-utils-0.9.33.2-r26.trigger
Executing glib-2.38.1-r0.trigger
OK: 172 MiB in 41 packages
```

1.3 Instalar nano

```
router1:~# apk add nano
WARNING: Ignoring /media/cdrom/apks/x86_64/APKINDEX.tar.gz: No such file or directory
(1/3) Installing ncurses-base (5.9-r1)
(2/3) Installing ncurses-widec-libs (5.9-r1)
(3/3) Installing nano (2.3.2-r0)
Executing busybox-1.21.1-r0.trigger
Executing uclibc-utils-0.9.33.2-r26.trigger
OK: 178 MiB in 66 packages
```

1.4 Edite el archivo /etc/hosts

Utilice el comando **mcedit** o nano para editar el archivo **/etc/hosts**, el archivo debe quedar como se muestra a continuación, recuerde que usted debe utilizar la red **192.168.50+Y.1** (donde Y es el número del grupo)

```
router1:~# mcedit /etc/hosts
127.0.0.1       localhost.localdomain           localhost
192.168.50+Y.1   router1.empresay.com.sv          router1
```

1.5 Instalar paquetes man

```
router1:~# apk add man
(1/4) Installing libstdc++ (4.9.2-r5)
(2/4) Installing groff (1.22.3-r0)
(3/4) Installing gawk (4.1.2-r0)
(4/4) Installing man (1.6g-r0)
Executing busybox-1.23.2-r0.trigger
OK: 302 MiB in 87 packages
```

Para cada paquete se digitará **apk add paquete-doc**

Paso 2 – Instalar la herramienta Web de monitoreo y configuración

2.1 Ejecute la herramienta de configuración ACF

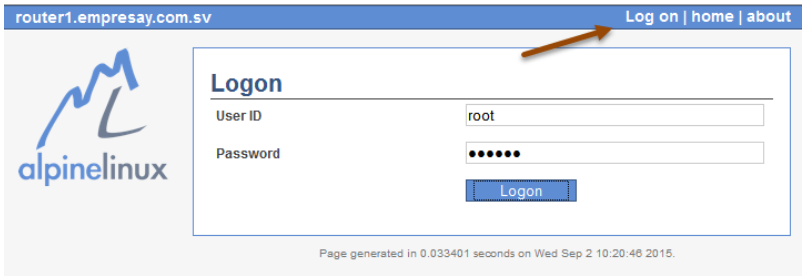
```
router1:/# setup-acf
(1/20) Installing libssl1.0 (1.0.1e-r5)
(2/20) Installing mini_httpd (1.19-r8)
Executing mini_httpd-1.19-r8.pre-install
(3/20) Installing acf-jquery (0.3.0-r0)
(4/20) Installing lua5.1-libs (5.1.5-r0)
(5/20) Installing lua-subprocess (0.0.20121211-r2)
(6/20) Installing acf-lib (0.6.1-r0)
(7/20) Installing acf-skins (0.5.1-r0)
(8/20) Installing haserl (0.9.32-r0)
(9/20) Installing lua5.1 (5.1.5-r0)
(10/20) Installing lua (5.1.5-r4)
(11/20) Installing lua-bitlib (26-r3)
(12/20) Installing lua5.1-posix (31-r1)
(13/20) Installing lua-posix (31-r1)
(14/20) Installing lua5.1-md5 (1.2-r1)
(15/20) Installing lua-md5 (1.2-r1)
(16/20) Installing lua-json4 (0.9.50-r0)
(17/20) Installing acf-core (0.17.1-r0)
(18/20) Installing acf-alpine-baselayout (0.11.0-r0)
(19/20) Installing acf-apk-tools (0.9.1-r0)
(20/20) Installing openssl (1.0.1e-r5)
Executing busybox-1.21.1-r0.trigger
Executing uclibc-utils-0.9.33.2-r26.trigger
OK: 176 MiB in 61 packages
Generating certificates for HTTPS...
Generating RSA private key, 2048 bit long modulus
.........................+++
.....................................................+++
e is 65537 (0x10001)
 * Caching service dependencies ...                    [ ok ]
 * Starting mini_httpd ...
bind: Address already in use
/usr/sbin/mini_httpd: started as root without requesting chroot(),warnin[ok]
```

2.2 Ingrese desde un navegador Web

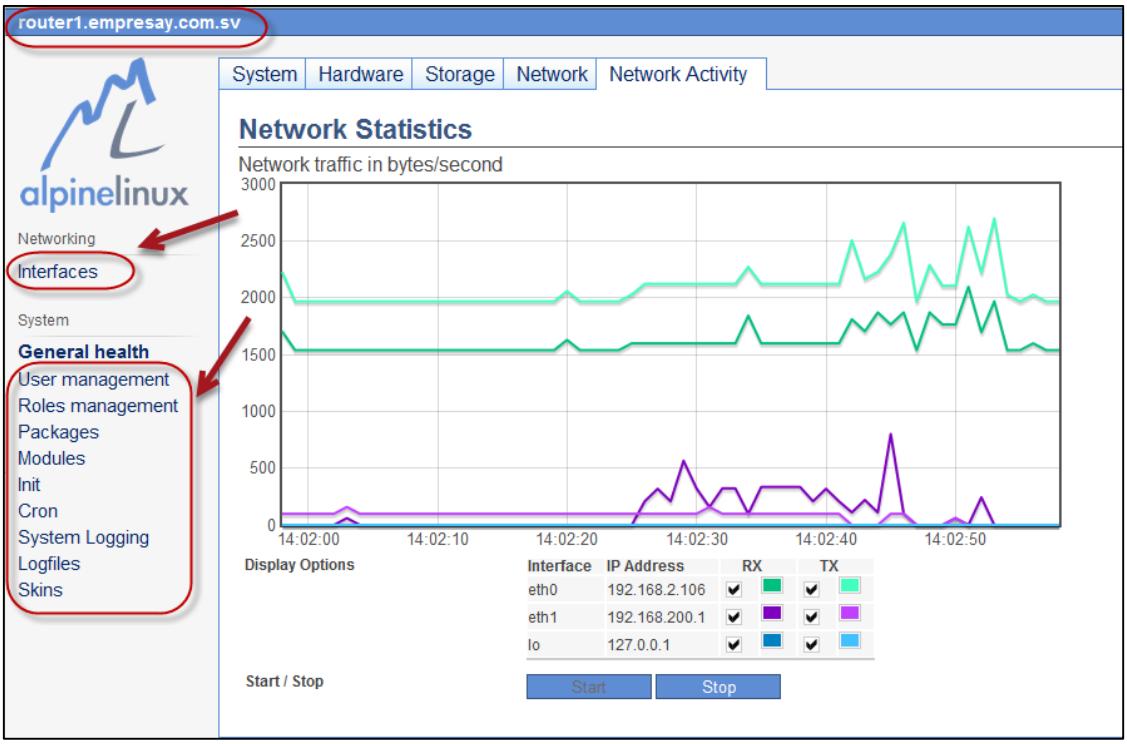
- Digite la URL https://192.168.50+Y.1 (IP de eth1) o la url: https://192.168.2.106 (IP de eth0)
- Acepte el certificado.

2.3 Dé un clic en el botón "Log on"

2.4 Ingrese las credenciales del usuario root



2.5 Tome un tiempo para ver los indicadores de RAM, Tráfico de red



2.3 Configuración del servidor DNS liviano (unbound)

Para el desarrollo de esta guía se ha seleccionado un servidor DNS que cumpla las siguientes consideraciones:

- Sea fácil de configurar. Editar pocos archivos y pocas opciones
- Consuma pocos recursos. Debido a que se utilizará un MV, en la vida real utilice **bind9** de **ISC**

El servidor seleccionado es **unbound** y en el siguiente enlace se puede obtener mayor información: http://wiki.alpinelinux.org/wiki/Setting_up_unbound_DNS_server

Tenga en cuenta lo siguiente

- Archivo de configuración: `/etc/unbound/unbound.conf`
- Archivo binario: `/etc/init.d/unbound start` (stop, restart)
- Herramienta de verificación : `unbound-checkconf`

Paso 1 – Instalar el servidor unbound (DNS)

1.1 Compruebe que tenga acceso a Internet

```
router1:/# apk add unbound
WARNING: Ignoring /media/cdrom/apks/x86_64/APKINDEX.tar.gz: No such file or directory
(1/5) Installing dnssec-root (20100715-r0)
(2/5) Installing expat (2.1.0-r0)
(3/5) Installing ldns (1.6.16-r0)
(4/5) Installing unbound-libs (1.4.21-r1)
(5/5) Installing unbound (1.4.21-r1)
Executing unbound-1.4.21-r1.pre-install
Executing busybox-1.21.1-r0.trigger
Executing uclibc-utils-0.9.33.2-r26.trigger
OK: 180 MiB in 71 packages
```

1.2 Saque copia del archivo de configuración

Ejecute los siguientes comandos:

```
router1:/# cd /etc/unbound/

router1:/etc/unbound# ls -l
total 28
-rw-r--r--    1 root     root          3048 Oct 28 10:34 root.hints
-rw-r--r--    1 root     root         23599 Oct 28 10:34 unbound.conf

router1:/etc/unbound# cp unbound.conf unbound.conf.ori

router1:/etc/unbound# ls -l
total 52
-rw-r--r--    1 root     root          3048 Oct 28 10:34 root.hints
-rw-r--r--    1 root     root         23599 Oct 28 10:34 unbound.conf
-rw-r--r--    1 root     root         23599 Dec 27 05:40 unbound.conf.ori
```

Paso 2 – Editar el archivo de configuración

Para definir la configuración del servidor DNS se puede realizar cualquiera de los siguientes métodos:

1. Editar el archivo **unbound.conf** directamente en el servidor usando el programa **mcedit** o **nano**
2. Copiar el archivo **unbound.conf** a Windows con **WinSCP** o **FIleZila**, editarlo con **Notepad++** o **Write** y enviarlo de nuevo al equipo router1 con **WinSCP** o **FileZilla**.

El archivo de configuración para esta práctica utilizará solo 4 secciones: "server:", "python:", "remote-control:", "forward-zone:" (con color azul)

Nota: Todas las instrucciones están en una sola línea, no omita los puntos y dos puntos, recuerde que "Y" representa el número de grupo. No digite **(línea anterior),** bórrela y una las dos líneas; ya que es parte de la línea previa

Nota: Para configurar el servidor DNS necesitará completar el cuadro No. 4 con los datos de su red (empresa**Y**)

```
router1:/etc/unbound# mcedit /etc/unbound/unbound.conf

server:
    verbosity: 1
    num-threads: 1
    interface: 0.0.0.0
    do-ip4: yes
    do-ip6: no
    do-udp: yes
    do-tcp: yes
    do-daemonize: yes
    access-control: 0.0.0.0/0 allow
    root-hints: /etc/unbound/root.hints

    local-zone: "localhost." static
    local-data: "localhost. 10800 IN NS localhost."
    local-data: "localhost. 10800 IN SOA localhost. nobody.invalid. 1 3600 1200
(línea anterior) 604800 10800"
    local-data: "localhost. 10800 IN A 127.0.0.1"

    local-zone: "127.in-addr.arpa." static
    local-data: "127.in-addr.arpa. 10800 IN SOA localhost. nobody.invalid. 2 3600
(línea anterior) 1200 604800 10800"
    local-data: "127.in-addr.arpa. 10800 IN NS localhost."
      local-data: "1.0.0.127.in-addr.arpa. 10800 IN PTR localhost."

    local-zone: "empresay.com.sv." static
    local-data: "empresay.com.sv.   86400       IN SOA  empresay.com.sv.
(línea anterior) admin.empresay.com.sv.  1 3600 1200 604800 86400"
    local-data: "empresay.com.sv.   86400       IN  NS  router1.empresay.com.sv."
    local-data: "router1.           IN  A   192.168.50+Y.1"
    local-data: "datastore1.        IN  A   192.168.50+Y.2"
    local-data: "frontend1.         IN  A   192.168.50+Y.3"
    local-data: "hipervisor1.       IN  A   192.168.50+Y.4"
    local-data: "hipervisor2.       IN  A   192.168.50+Y.5"
    local-data: "hipervisor3.       IN  A   192.168.50+Y.6"
    local-data: "www.               IN  A   192.168.50+Y.11"
    local-data: "datos.             IN  A   192.168.50+Y.12"
    local-data: "srvapp.            IN  A   192.168.50+Y.13"
    local-data: "mail.              IN  A   192.168.50+Y.14"
    local-data: "router1.empresay.com.sv.       IN  A   192.168.50+Y.1"
```

```
    local-data: "datastore1.empresay.com.sv.    IN  A   192.168.50+Y.2"
    local-data: "frontend1.empresay.com.sv.     IN  A   192.168.50+Y.3"
    local-data: "hipervisor1.empresay.com.sv.   IN  A   192.168.50+Y.4"
    local-data: "hipervisor2.empresay.com.sv.   IN  A   192.168.50+Y.5"
    local-data: "hipervisor3.empresay.com.sv.   IN  A   192.168.50+Y.6"
    local-data: "www.empresay.com.sv.           IN  A   192.168.50+Y.11"
    local-data: "datos.empresay.com.sv.         IN  A   192.168.50+Y.12"
    local-data: "srvapp.empresay.com.sv.        IN  A   192.168.50+Y.13"
    local-data: "mail.empresay.com.sv.          IN  A   192.168.50+Y.14"

    local-zone: "50+Y.168.192.in-addr.arpa." static
    local-data: "50+Y.168.192.in-addr.arpa.      10800 IN SOA empresay.com.sv.
(línea anterior) admin.empresay.com.sv. 1 3600 1200 604800 864000"
    local-data: "50+Y.168.192.in-addr.arpa.      10800 IN NS  router1."
    local-data: "1.50+Y.168.192.in-addr.arpa.  10800 IN PTR router1."
    local-data: "2.50+Y.168.192.in-addr.arpa.  10800 IN PTR datastore1."
    local-data: "3.50+Y.168.192.in-addr.arpa.  10800 IN PTR frontend1."
    local-data: "4.50+Y.168.192.in-addr.arpa.  10800 IN PTR hipervisor1."
    local-data: "5.50+Y.168.192.in-addr.arpa.  10800 IN PTR hipervisor2."
    local-data: "6.50+Y.168.192.in-addr.arpa.  10800 IN PTR hipervisor3."
    local-data: "11.50+Y.168.192.in-addr.arpa. 10800 IN PTR www."
    local-data: "12.50+Y.168.192.in-addr.arpa. 10800 IN PTR datos."
    local-data: "13.50+Y.168.192.in-addr.arpa. 10800 IN PTR srvapp."
    local-data: "14.50+Y.168.192.in-addr.arpa. 10800 IN PTR mail."
   local-data: "50+Y.168.192.in-addr.arpa.   10800 IN NS router1.empresay.com.sv."
   local-data: "1.50+Y.168.192.in-addr.arpa.  10800 IN PTR router1.empresay.com.sv."
   local-data: "2.50+Y.168.192.in-addr.arpa.  10800 IN PTR datastore1.empresay.com.sv."
   local-data: "3.50+Y.168.192.in-addr.arpa.  10800 IN PTR frontend1.empresay.com.sv."
   local-data: "4.50+Y.168.192.in-addr.arpa.  10800 IN PTR hipervisor1.empresay.com.sv."
   local-data: "5.50+Y.168.192.in-addr.arpa.  10800 IN PTR hipervisor2.empresay.com.sv."
   local-data: "6.50+Y.168.192.in-addr.arpa.  10800 IN PTR hipervisor3.empresay.com.sv."
    local-data: "11.50+Y.168.192.in-addr.arpa. 10800 IN PTR www.empresay.com.sv."
    local-data: "12.50+Y.168.192.in-addr.arpa. 10800 IN PTR datos.empresay.com.sv."
    local-data: "13.50+Y.168.192.in-addr.arpa. 10800 IN PTR srvapp.empresay.com.sv."
    local-data: "14.50+Y.168.192.in-addr.arpa. 10800 IN PTR mail.empresay.com.sv."

python:

remote-control:
    control-enable: no

forward-zone:
    name: "."
    forward-addr: 192.168.5.19
      forward-addr: 8.8.8.8
    forward-addr: 8.8.4.4
    forward-first: yes
```

Cuando se realicen las pruebas de la resolución de nombres será necesario que se prueben tanto los host como los FQDN. Como se expresó anteriormente este servicio es funcional para el escenario que se ha planteado, pero en un escenario real se deberá considerar instalar el servicio DNS **Bind9**

Paso 3 – Verificar funcionamiento del archivo de configuración

Ejecute el siguiente comando en el router1:

```
router1:/etc/unbound# unbound-checkconf

unbound-checkconf: no errors in /etc/unbound/unbound.conf
```

Si tiene errores por favor digite correctamente el archivo y tenga en cuenta lo siguiente:

- Mayúsculas y minúsculas son consideradas por separado.
- No omita el punto"." Al final del dominio.
- Si solo copia el contenido tendrá error porque debe sustituir la letra "Y" por el número de grupo.
- Si creó el archivo desde Windows y después lo envió al equipo router1, tenga en cuenta el salto de línea, lo mejor es crear el archivo desde Linux con el comando **touch unbound.conf**
- Si desea puede sustituir el valor del servidor DNS 8.8.8.8, por el servidor del ISP (por ejemplo 192.168.1.12)

Paso 4 – Ejecutar servidor DNS

4.1 Iniciar manualmente el servidor DNS

```
router1:~# /etc/init.d/unbound start
 * Starting unbound ...

[1388150724] unbound[1708:0] warning: increased limit(open files) from 1024 to 4140
[ ok ]
```

Nota: Puede utilizar las opciones: **stop, status, restart**.

4.2 Iniciar automáticamente el servidor DNS

Debido a que el servicio DNS debe quedar automáticamente ejecutándose cada vez que arranque el equipo virtual, será necesario agregarlo a la lista de procesos de inicio en el arranque

Si desea que el servicio se ejecute al inicio del sistema operativo digite el siguiente comando: **rc-update add unbound**

```
router1:/etc/unbound# rc-update add unbound

 * service unbound added to runlevel default
```

4.3 Comprobar que se ha agregado a lista de programas en el arranque

```
router1:/etc/unbound# rc-update show |grep unbound

              unbound |      default
```

Paso 5 – Realizar pruebas desde los clientes DNS

Puede utilizase un cliente Windows o un cliente Linux (TinyCorePlus 6.X)

5.1 Asigne una dirección IP en el rango de su red 192.168.50+Y.0

```
C:\> netsh interface ip set address "Conexión de área local" static 192.168.50+Y.101
255.255.255.0 192.168.50+Y.1 5
```

5.2 Asigne la dirección IP del DNS 192.168.50+Y.1

```
C:\> netsh interface ip set dns "Conexión de área local" static 192.168.50+Y.1
```

Verifique que tiene el DNS

```
C:\>ipconfig /all | find "Servidores DNS"
   Servidores DNS. . . . . . . . . . . . . : 192.168.2.1
```

5.3 Verifique que el servidor DNS muestre los datos de la zona directa e inversa

```
C:\>nslookup
Servidor predeterminado:  router1.empresay.com.sv
Address:  192.168.50+Y.1
>
```

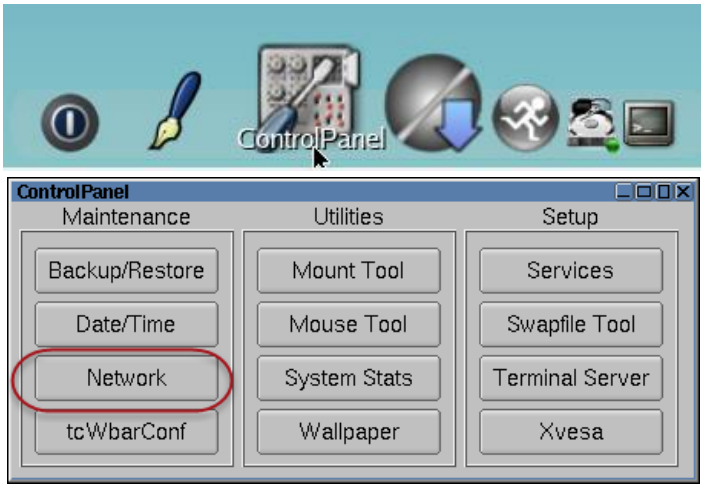
5.4 Consulte la base de datos

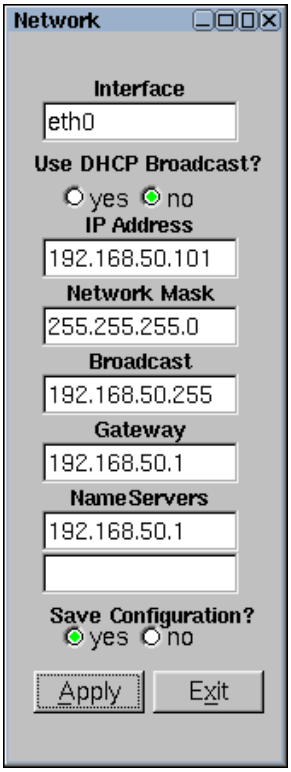
```
> datastore1.empresay.com.sv
Servidor:  router1.empresay.com.sv
Address:  192.168.50+Y.1
Nombre:  datastore1.empresay.com.sv
Address:  192.168.50+Y.2

> www.empresay.com.sv
Servidor: router1.empresay.com.sv
Address:  192.168.50+Y.1
Nombre:  www.empresay.com.sv
Address:  192.168.50+Y.11

> cuchillac.net
Servidor: router1.empresay.com.sv
Address:  192.168.50+Y.1
Respuesta no autoritativa:   <- Muy importante consulta a los fowarders
Nombre:  cuchillac.net
Address:  50.87.152.212

> 192.168.50+Y.14
Servidor: router1.empresay.com.sv
Address:  192.168.200.1
Nombre:  mail.empresay.com.sv
Address:  192.168.50+Y.14

> exit
```

Si utiliza el cliente TinyCorePlus 6.4

5.5 Configurar la dirección IPv4

1. Seleccione Control Panel
2. Dar clic en botón Network
3. Completar Panel pantalla de red
    3.1 Interface = eth0
    3.2 Usar DHCP = No
    3.3 IPv4 = 192.168.50+Y.101
    3.4 Máscara = 255.255.255.0
    3.5 Broadcast = 192.168.50+Y.255
    3.6 IP Gateway = 192.168.50+Y.1
    3.7 IP NS = 192.168.50+Y.1
4. Guardar configuración = Sí
5. Dar Clic en botón "**Apply**"c
6. Dar clic en botón "**Exit**"





5.6 Realizar consultas al servidor DNS

```
tc@box:$ nslookup datastore1.empresay.com.sv
Server:    192.168.50+Y.1
Address:   192.168.50+Y.1  router1.empresay.com.sv
Name:      datastore1.empresay.com.sv
Address:   192.168.50+Y.2  datastore1.empresay.com.sv

tc@box:$ nslookup www.empresay.com.sv
Server:    192.168.50+Y.1
Address:   192.168.50+Y.1  router1.empresay.com.sv
Name:      www.empresay.com.sv
Address:   192.168.50+Y.11  www.empresay.com.sv

tc@box:$ nslookup cuchillac.net
Server:    192.168.50+Y.1
Address:   192.168.50+Y.1  router1.empresay.com.sv
Name:      Cuchillac.net
Address:   50.87.153.222  50-87-153-222.unifiedlayer.com
```

Es importante que el servidor NS pueda resolver FQDN externos.

2.4 Configuración de un servidor DHCP (ISC)

Para esta guía se ha seleccionado el servidor DHCP ISC, el cual es muy robusto y cuya documentación es muy prolífica en Internet. Si desea más información del servidor DCHP ISC consulte el siguiente enlace: https://www.isc.org/downloads/dhcp/

Información opcional: http://syconet.wordpress.com/2013/03/19/instalacion-y-configuracion-de-un-servidor-dhcp-en-debian-6-squeeze/

Para configurar el servidor DHCP debe utilizar el cuadro No. 4 y considerar lo siguiente:

- Cree direcciones reservadas para los equipos según los cuadros No. 3 y No. 4
- Asigne la dirección 192.168.50+Y.1 como DNS local
- Las direcciones IPv4 que ofrecerá el servidor DHCP no deben entrar en conflicto con las direcciones IP de los equipos clientes. Cree un rango o scope desde la dirección 192.168.50+Y.101 a 192.168.50+Y.110

Los archivos que debe tomar en cuenta son:

- Archivo de configuración: **/etc/dhcp/dhcp.conf**
- Archivo binario: **/etc/init.d/dhcp**
- Archivo que guarda las IP asignadas: **/var/lib/dhcp.leases**

Archivo para ver la bitácora de eventos:

Paso 1 – Instalación del servidor

```
router1:~# apk add dhcp

WARNING: Ignoring /media/cdrom/apks/x86_64/APKINDEX.tar.gz: No such file or directory
(1/1) Installing dhcp (4.2.5_p1-r2)
Executing dhcp-4.2.5_p1-r2.pre-install
Executing busybox-1.21.1-r0.trigger
OK: 183 MiB in 72 packages
```

Paso 2 – Sacar copia del archivo de configuración

2.1 Ingrese al directorio del servidor dhcp

```
router1:~# cd /etc/dhcp/

router1:/etc/dhcp# ls
dhcpd.conf.example
```

2.2 Saque una copia del archivo

```
router1:/etc/dhcp# cp dhcpd.conf.example dhcpd.conf

router1:/etc/dhcp# ls -l
total 8
-rw-r--r--    1 root     root          3262 Dec 27 08:14 dhcpd.conf
-rw-r--r--    1 root     root          3262 Oct 27 16:42 dhcpd.conf.example
```

Paso 3 – Editar el archivo de configuración

Se recomienda descargar el archivo con WinSCP y editarlo con Notepad++

```
router1:~# mcedit /etc/dhcp/dhcpd.conf
```

```
# Configuración del servifor DHCP
# Opciones globales del servidor
ddns-update-style none;
option domain-name "empresay.com.sv";
option domain-name-servers 192.168.50+Y.1;
default-lease-time 7200;
max-lease-time 21600;
authoritative;
log-facility local7;

# Ámbitos (Scopes - Rangos)
subnet 192.168.50+Y.0 netmask 255.255.255.0 {
      range 192.168.50+Y.101 192.168.50+Y.110;
      option routers 192.168.50+Y.1;
}
#Para las direcciones reservadas utilice como plantilla los siguientes ejemplos
host datastore1{
   hardware ethernet 02:Y:X:B0:00:02;
   fixed-address 192.168.50+Y.2;
}
host frontend1{
   hardware ethernet 02:Y:X:B0:00:03;
   fixed-address 192.168.50+Y.3;
}
```

Paso 4 – Inicie el servicio DHCP

4.1 Inicie el servicio manualmente

```
router1:/etc/dhcp# /etc/init.d/dhcpd start
```

```
 * Caching service dependencies ...                [ ok ]
 * /var/run/dhcp: correcting owner
 * /var/lib/dhcp: correcting owner
 * /var/lib/dhcp/dhcpd.leases: creating file
 * /var/lib/dhcp/dhcpd.leases: correcting mode
 * Starting dhcpd ...                               [ ok ]
```

Nota: Puede utilizar las opciones: **stop, status, restart**. Recuerde que si utiliza las direcciones estáticas en los servidores no es necesario tener un servidor DHCP

4.2 Si desea iniciar el servidor durante el arranque (opcional)

```
router1:/etc/dhcp# rc-update add dhcpd
```

```
 * Service dhcpd added to runlevel default
```

Paso 5 – Verificar funcionamiento de servidor DHCP

5.1 Utilizando cliente Windows.

Para esta guía se asume que el nombre de la interfaz de red en Windows es LAN y que se poseen permisos de administrador.

Defina que la interfaz LAN utilizará una dirección IPv4 dinámica.

```
C:\>netsh interface ip set add LAN dhcp
```

Defina que la interfaz LAN utilizará la IPv4 del DNS de forma dinámica.

```
C:\>netsh interface ip set dns LAN dhcp
```

Verifique que el servidor DHCP ha asignado una IPv4 a la interfaz

```
C:\>ipconfig
```

```
Configuración IP de Windows
Adaptador de Ethernet LAN:
   Sufijo DNS específico para la conexión. . : empresay.com.sv
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.50+Y.101
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.50+Y.1
```

Para verificar que se haya enviado el la dirección IPv4 del DNS utilice el comando **`C:\>ipconfig /all`** y verifique la interfaz LAN

5.2 utilizando cliente Linux

Si utiliza TinyCore utilice la herramienta gráfica. Si utiliza otra versión de Linux el comando para solicitar una dirección IP en Linux es **`dhcliente eth0`**, el cual es ejecutado por el root y el archivo de configuración de la interfaz eth0 no debe tener una dirección IPv4 estática.

Problemas con el servidor DHCP.

Si tiene problemas en la asignación de direcciones IPv4 revise los siguientes puntos:

- Si el cliente DHCP obtiene una dirección APIPA (169.254.X.X), significa que el cliente envío la petición y ningún servidor DHCP le pudo asignar una IP
    - Verifique que haya conexión ICMP entre el servidor DHCP y el cliente.
    - Verifique la comunicación de las interfaces de Virtual Box o VMWare Workstation
    - Verifique el firewall del equipo Windows y el firewall del servidor DHCP.
- Si el cliente DHCP recibe una dirección de otro grupo (empresay), solo aplica al centro de cómputo 3.
    - Reinicie el cliente DHCP, no utilice los comandos `ipconfig /release`, `ipconfig /renew` porque estos utilizan la caché del cliente, para reiniciar el cliente DHCP, abra **`services`**`.msc` y reinicie el cliente DHCP.
    - Verifique que su cliente y servidor DHCP estén conectados entre ellos y no haya comunicación con otros servidores DHCP.

2.5 Habilitación de la función de reenvío de paquetes IPv4 (Router)

Si un equipo posee dos tarjetas de red no significa que puede realizar el reenvío de paquetes (función de pasarela de red o router), Tanto en los equipos Windows como Linux es necesario habilitar la opción de reenvío de paquetes de una tarjeta a otra. (En equipos con Windows sólo las versiones para servidor poseen esta opción. Sin embargo se puede descargar software de terceros para implementar el ruteo de paquetes)

Paso 1 – Consultar la opción del kernel

```
router1:/# sysctl -a |grep ipv4.ip*

. . .
. . .
net.ipv4.icmp_ratelimit = 1000
net.ipv4.icmp_ratemask = 6168
net.ipv4.igmp_max_memberships = 20
net.ipv4.igmp_max_msf = 10
net.ipv4.inet_peer_maxttl = 600
net.ipv4.inet_peer_minttl = 120
net.ipv4.inet_peer_threshold = 65664
net.ipv4.ip_default_ttl = 64
net.ipv4.ip_dynaddr = 0
net.ipv4.ip_early_demux = 1
net.ipv4.ip_forward = 0
net.ipv4.ip_local_port_range = 32768    61000
net.ipv4.ip_local_reserved_ports =
net.ipv4.ip_no_pmtu_disc = 0
net.ipv4.ip_nonlocal_bind = 0
net.ipv4.ipfrag_high_thresh = 4194304
net.ipv4.ipfrag_low_thresh = 3145728
net.ipv4.ipfrag_max_dist = 64
net.ipv4.ipfrag_secret_interval = 600
net.ipv4.ipfrag_time = 30
```

Paso 2 – Activar el reenvío de paquetes IPv4 en el kernel

```
router1:/# sysctl -w net.ipv4.ip_forward=1

net.ipv4.ip_forward = 1
```

Paso 3 – Verificar que se haya activado el reenvío de paquetes IPv4 en el kernel

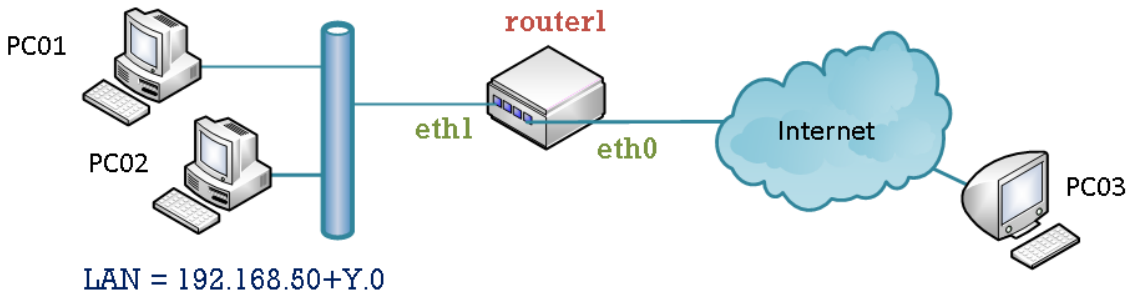
```
router1:/# sysctl -a |grep ipv4.ip_forward
sysctl: error reading key 'net.ipv4.route.flush': Permission denied
net.ipv4.ip_forward = 1
sysctl: error reading key 'net.ipv6.route.flush': Permission denied
sysctl: error reading key 'vm.compact_memory': Permission denied
```

Paso 4 –Verificar que el router funcione.

Nota: En los escenarios reales un router siempre tiene direcciones IP estáticas, recuerde que por portabilidad de los equipos virtuales la eth0 es automática. Si se desea modificar la dirección de eth0 o eth1 se utiliza el comando **setup-interfaces**.

Para esta guía se ha utilizado las siguientes direcciones de red:

- Red LAN de la EMPRESAY = 192.168.50+Y.0
- IPv4 del router1 en eth0 = 192.168.2.191 (podría ser 10.10.3.191)
- IPv4 del router1 en eth1 = 192.168.50.1
- PC01 (sugerido TinyCore6.4) = 192.168.50+Y.101
- PC03 (Equipo Windows del laboratorio o laptop) = 192.168.2.122 (podría ser 10.10.3.122)



4.1 Verifique las IPv4 y la tabla de ruteo en el router1

```
router1:~# ifconfig |grep "inet addr"

          inet addr:192.168.2.191  Bcast:0.0.0.0  Mask:255.255.255.0
          inet addr:192.168.50.1    Bcast:0.0.0.0  Mask:255.255.255.0
          inet addr:127.0.0.1       Mask:255.0.0.0

router1:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.1     0.0.0.0         UG    202    0        0 eth0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.50+Y.0  0.0.0.0         255.255.255.0   U     0      0        0 eth1
```

De dicha tabla se concluye que:

- Cualquier red de destino con cualquier máscara utilizará el Gateway externo 192.168.2.1 (10.10.3.254 en laboratorio)
- La red 192.168.2.0 es la red para internet y se comunica con la eth0
- La red 192.168.50+Y.0 es la red para la LAN de la EMPRESAY y se utiliza la interfaz eth1

4.2 Verifique las IPv4 y la tabla de ruteo en el equipo PC01 (TinyCore)

```
tc@box:”$ ifconfig |grep "inet addr"

          inet addr:192.168.50+Y.101  Bcast:0.0.0.0  Mask:255.255.255.0
          inet addr:127.0.0.1         Mask:255.0.0.0


tc@box:”$ route -n

Kernel IP routing table
Destination     Gateway         Genmask          Flags Metric Ref    Use Iface
0.0.0.0         192.168.50+Y.1  0.0.0.0           UG    0      0        0   eth0
127.0.0.1       0.0.0.0         255.255.255.255  UH    0      0        0   lo
192.168.50+Y.0  0.0.0.0         255.255.255.0    U     0      0        0   eth0
```

4.3 Verifique las IPv4 y la tabla de ruteo en el equipo PC03 (Windows host)

```
C:\>ipconfig
Configuración IP de Windows
Adaptador de LAN inalámbrica WIFI:
   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.2.122
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.2.1


C:\>route print -4
===========================================================================
IListe de interfaces
 13...68 17 29 91 5c 9e ......Intel(R) Centrino(R) Wireless-N 2230
 12...f0 92 1c 52 37 cc ......Realtek PCIe GBE Family Controller
 25...6a 17 29 91 5c 9e ......Microsoft Hosted Network Virtual Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      192.168.2.1    192.168.2.122     31
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    306
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    306
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1    306
      192.168.2.0    255.255.255.0      En vínculo     192.168.2.122    286
    192.168.2.122  255.255.255.255      En vínculo     192.168.2.122    286
    192.168.2.255  255.255.255.255      En vínculo     192.168.2.122    286
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1    306
        224.0.0.0        240.0.0.0      En vínculo     192.168.2.122    286
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1    306
  255.255.255.255  255.255.255.255      En vínculo     192.168.2.122    286
===========================================================================
Rutas persistentes:
      Ninguno
```

Para que el equipo Windows que simula estar en Internet pueda comunicarse con la LAN hay dos opciones:

Opción 1

Configurar que el GW no sea 192.168.2.1 (en el laboratorio podría ser 10.10.3.254) sino que sea la dirección IPv4 de la interfaz eth0 del router1.

- Ventaja: Es más fácil la configuración.
- Desventaja: El equipo Windows ya no tendría comunicación a Internet.
- Comandos:

```
C:\> route delete 0.0.0.0
C:\> route add 0.0.0.0 mask 0.0.0.0 192.168.2.1 metric 25
```

Tabla final (está resumida)

```
IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0     192.168.2.1    192.168.20.122     55
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    306
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    306
      192.168.20.0    255.255.255.0      En vínculo    192.168.20.122    286
===========================================================================
Rutas persistentes:
 Ninguno
```

Opción 2

Agregar una dirección estática a la red 192.168.50+Y.0 que direccione el tráfico a la dirección IPv4 de la interfaz eth0 del router1.

- Ventaja: El equipo Windows tendrá salida a Internet y comunicación con la LAN usando router1.
- Desventaja: Al principio genera confusión (en estudiantes con bajas competencias)
- Comandos:

```
C:\> route delete 0.0.0.0
C:\> route add 0.0.0.0 mask 0.0.0.0 192.168.2.1 metric 25
C:\> route add 192.168.50+Y.0 mask 255.255.255.0  192.168.2.191
metric 10
```

Tabla final (está resumida)

```
IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0     192.168.20.1   192.168.2.122     55
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    306
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    306
      192.168.20.0    255.255.255.0      En vínculo    192.168.2.122    286
      192.168.50+Y.0  255.255.255.0    192.168.2.191   192.168.2.122     31
===========================================================================
Rutas persistentes:
  Ninguno
```

4.5 Establezca comunicación entre los equipos de la LAN e Internet

Envíe paquetes ICMP desde la LAN de la EMPRESAY hacia el equipo PC03

```
tc@box:"$ ping -c 2 192.168.2.191

PING 192.168.2.191 (192.168.2.191) 56(84) bytes of data.
64 bytes from 192.168.2.122: icmp_seq=1 ttl=64 time=0.258 ms
64 bytes from 192.168.2.122: icmp_seq=2 ttl=64 time=0.292 ms

tc@box:"$ ping -c 2 192.168.2.122

PING 192.168.2.122 (192.168.2.122) 56(84) bytes of data.
64 bytes from 192.168.2.122: icmp_seq=1 ttl=127 time=0.467 ms
64 bytes from 192.168.2.122: icmp_seq=2 ttl=127 time=0.338 ms
```

Envíe paquetes ICMP desde el equipo PC03 a la PC01 de la LAN de la EMPRESAY

```
C:\>ping 192.168.50+Y.1 –n 2

Haciendo ping a 192.168.50+Y.1 con 32 bytes de datos:
Respuesta desde 192.168.50+Y.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.50+Y.1: bytes=32 tiempo<1m TTL=64

C:\>ping 192.168.50+Y.101 –n 2

Haciendo ping a 192.168.50+Y.3 con 32 bytes de datos:
Respuesta desde 192.168.50+Y.3: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.50+Y.3: bytes=32 tiempo<1m TTL=63
```

Si no obtiene respuesta en el envío de paquetes ICMP verifique lo siguiente.

- No debe utilizar NAT
- Compruebe la tarjeta que utiliza como bridge en VirtualBox para eth0 y eth1
- Verifique el valor de las IPv4
- Verifique que se activó el reenvío IPv4 en el router1 (ipv4_forward)
- Compruebe que el firewall le permite el paso de paquetes ICMP

2.6 Configuración del firewall (shorewall)

Paso 1 – Instalar Shorewall

```
router1:/# apk add shorewall

WARNING: Ignoring /media/cdrom/apks/x86_64/APKINDEX.tar.gz: No such file or directory
(1/5) Installing shorewall-core (4.5.21.3-r0)
(2/5) Installing perl (5.18.1-r0)
(3/5) Installing iptables (1.4.20-r0)
(4/5) Installing iproute2 (3.11.0-r0)
Executing iproute2-3.11.0-r0.post-install
(5/5) Installing shorewall (4.5.21.3-r0)
Executing busybox-1.21.1-r0.trigger
Executing uclibc-utils-0.9.33.2-r26.trigger
OK: 233 MiB in 77 packages
```

Paso 2 – Editar los archivos de configuración de Shorewall

Los archivos que se deben configurar son lossiguientes:

1) **shorewall.conf**: Archivo de configuración general.
2) **zones**: Donde se definen las zonas y su tipo.
3) **interfaces**: Donde se asigna las interfaces a las zonas.
4) **policy**: Donde se declaran las políticas globales, denegar todo es lo recomendable.
5) **rules**: Donde se definen las execpciones a policy, por ejemplo acceso a un servicio.
6) **masq**: Para permitir el enmascaramiento IP de una tarjeta a otra

2.1 Active shorewall

```
router1:/#  mcedit /etc/shorewall/shorewall.conf
##############################################################################
#                      S T A R T U P   E N A B L E D
##############################################################################
#cuc ori= No
STARTUP_ENABLED=Yes
```

2.2 Defina las zonas

```
router1:/# mcedit /etc/shorewall/zones
#ZONE   TYPE            OPTIONS         IN                      OUT
#                                       OPTIONS                 OPTIONS
fw      firewall
inter   ipv4
lan     ipv4
```

2.3 Asocie las interfaces para las zonas

```
router1:/# mcedit /etc/shorewall/interfaces
#ZONE           INTERFACE       BROADCAST       OPTIONS
inter           eth0
lan             eth1
```

2.4 Defina las políticas globales

Nota: En esta guía se permitirá el acceso desde la LAN (zona lan) hacia Internet (inter) y viceversa

```
router1:/# mcedit /etc/shorewall/policy
#SOURCE DEST    POLICY          LOG     LIMIT:          CONNLIMIT:
#                               LEVEL   BURST           MASK
fw      all     ACCEPT
lan     inter   ACCEPT
all     all     ACCEPT
```

2.5 Definir las reglas de reenvío

Nota: No es necesario agregar reglas porque se ha permitido al todo el acceso, en la vida real se debería agregar los servicios autorizados, por ejemplo DHCP, DNS, Web, etc. Pero para permitir la descarga desde los repositorios de los demás equipos se permitirá todo el tráfico.

```
router1:/# mcedit /etc/shorewall/rules
#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE
ORIGINAL RATE           USER/   MARK    CONNLIMIT       TIME
HEADERSSWITCH           HELPER
#PORT    PORT(S)        DEST            LIMIT           GROUP
?SECTION ALL
?SECTION ESTABLISHED
?SECTION RELATED
?SECTION INVALID
?SECTION UNTRACKED
?SECTION NEW
```

2.6 Definir el enmascaramiento de direcciones IPv4

```
router1:/# cat /etc/shorewall/masq

#INTERFACE:DEST  SOURCE  ADDRESS  PROTO  PORT(S) IPSEC  MARK  USER/ SWITCH ORIGINAL
#   GROUP         DEST
eth0    eth1
```

Paso 3 – Iniciar el firewall

3.1 Iniciar manualmente el firewall

```
router1:/# /etc/init.d/shorewall start
 * Starting shorewall ...      [ ok ]
```

3.2 Configurar que el firewall se inicie al cuando arranque el sistema operativo

```
router1:~# rc-update add shorewall
 * service shorewall added to runlevel default
```

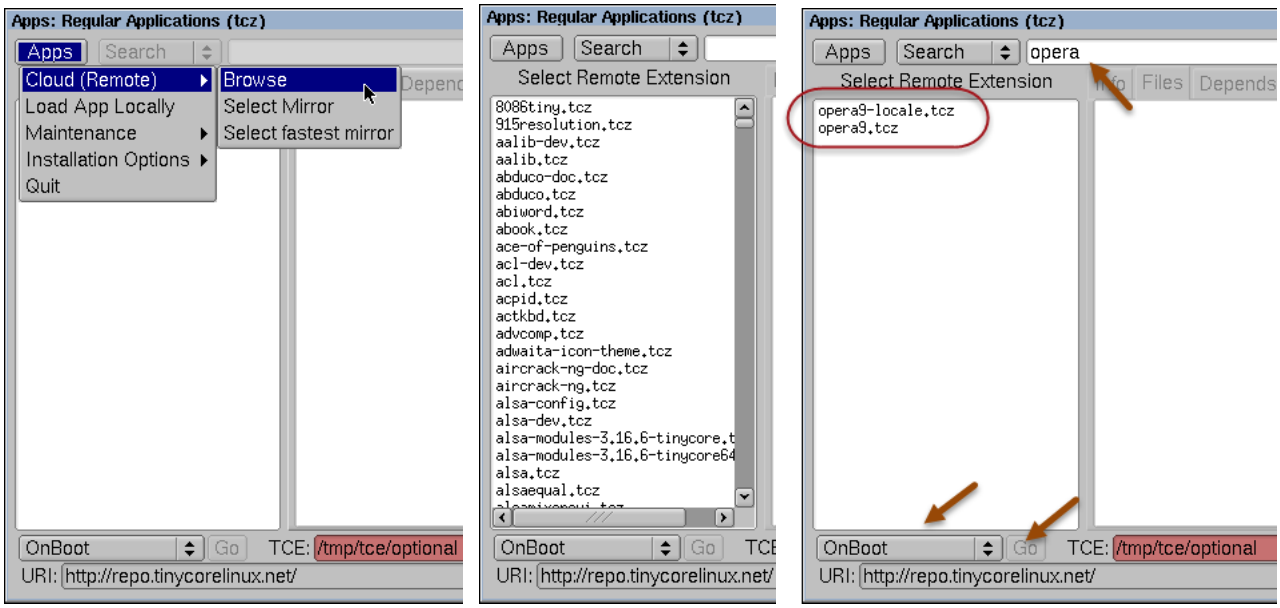
Paso 4 – Verificar navegación de los equipos de la LAN en Internet

Conectar un equipo en donde pueda verificarse que se tiene salida a Internet. Si utiliza TinyCore 6.4, instale una aplicación pequeña como Opera (Navegador Web), 8 MB

4.1 Clic en el botón “Apps” de la barra de aplicaciones
4.2 Clic en el botón “Apps” de la ventana
4.3 Seleccione Cloud(Remote)
4.3 Seleccione Browse

Debe aparecer el listado de paquetes tcz
4.5 Digite Opera
4.6 Seleccione OnBoot en el botón inferior izquierdo
4.7 Dar clic en botón “**OK**”

Se debe instalar el programa opera y debe aparecer en la barra de aplicaciones el icono de Opera



Tareas

Conteste las siguientes preguntas:

- ¿Cuál es la diferencia entre la zona directa e inversa en una servidor DNS?
- ¿Cuál es la función de los forwarders o reenviadores?
- ¿Por qué razón se ha seleccionado un rango IPv4 que comienza desde la 192.168.20Y.101?
- Si una misma red LAN existen dos servidores DHCP, ¿Cómo puede un cliente DHCP seleccionar un servidor determinado?
-

Investigue los siguientes puntos:

- Los servidores nsd y unbound son servidores que consumen muy pocos recursos y son convenientes en escenarios pequeños. ¿Cuál es la diferencia principal entre ellos?
- ¿Por qué es necesario instalar y configurar shorewall en la nube híbrida?

Información para configuración de red
http://wiki.alpinelinux.org/wiki/Configure_Networking

Información para agregar paquetes a Alphine
http://wiki.alpinelinux.org/wiki/Alpine_Linux_package_management

Información de servidores reenviadores http://technet.microsoft.com/en-us/library/cc754931.aspx.

Anexos

A1 – Configuración de red IPv4 para los equipos virtuales

De manera general todo equipo virtual o físico deberá tener configurados los siguientes parámetros:

- Dirección IPv4 y máscara válida para la red 192.168.50+Y.X
- La dirección IPv4 del GW de la red: 192.168.50+Y.1
- La dirección IPv4 del DNS de la red: 192.168.50+Y.1

Sistema operativo utilizado:	Comandos a utilizar:	Archivos a editar
Alpine Linux	• `setup-hostname` • `setup-interfaces` • `setup-dns` • `/etc/init.d/networking restart`	• `/etc/network/interfaces` • `/etc/resolv.conf`
Opensuse 13.X	• `yast2` • `etc/init.d/network restart`	• `/etc/sysconfig/network/ifcfg-br0` • `/etc/sysconfig/network/ifcfg-eth0` • `/etc/sysconfig/network/routes` • `/etc/resolv.conf`

Acción a realizar	Sistemas Linux	Sistemas Windows
Para ver la dirección IPv4:	`ifconfig |more`	`ipconfig |more`
Para ver la dirección IPv4 del DNS	`cat /etc/resolv.conf`	`ipconfig /all | find "Servidores"`
Para ver la ruta por defecto 0.0.0.0 0.0.0.0 (GW)	`route -n`	`route print`
Para asignar una IPv4 en la interfaz eth0/LAN	`ifconfig eth0 192.168.200.51 netmask 255.255.255.0`	`netsh interface ip set address LAN static 192.168.200.52 255.255.255.0 192.168.200.1 10`
Para definir la IPv4 del GW por default	`Route add default gw 192.168.200.1`	`Se incluye con la IP de la interfaz`
Para definir la IPv4 del DNS principal	`Se agrega la en el archivo /etc/resolv.conf: nameserver 192.168.2.1`	`netsh interface ip set dns "LAN" static 192.168.200.1`

A2 – Configuración del servidor DNS liviano nsd

Instale el servidor DNS

```
router1:/# apk add nsd
OK: 177 MiB in 63 packages

router1:/# ls /etc/nsd/nsd.*
/etc/nsd/nsd.conf.sample

router1:/# cp /etc/nsd/nsd.conf.sample  /etc/nsd/nsd.conf

router1:/# mcedit /etc/nsd/nsd.conf

router1:/etc/nsd# apk add nsd
WARNING: Ignoring /media/cdrom/apks/x86_64/APKINDEX.tar.gz: No such file or directory
OK: 178 MiB in 66 packages
```

Edite el archivo de configuración del servidor nsd
Ingrese al directorio de configuración del servidor DNS

```
router1:/# cd /etc/nsd/
```

Cree el archivo de configuración a partir del archivo de ejemplo

```
router1:/etc/nsd# cp /etc/nsd/nsd.conf.sample  /etc/nsd/nsd.conf
```

Verifique que haya copiado el archivo

```
router1:/etc/nsd# ls -l
total 20
-rw-r--r--    1 root     root          7238 Dec 27 04:37 nsd.conf
-rw-r--r--    1 root     root          7132 Dec 10 07:14 nsd.conf.sample
```

Edite las siguientes opciones

```
router1:/etc/nsd# mcedit  /etc/nsd/nsd.conf
server:
        ip-address: 192.168.20Y.1
        do-ip4: yes
        port: 53
        zonesdir: "/etc/nsd"

        identity: "empresay.com.sv"
remote-control:

zone:
        name: "empresay.com.sv"
        zonefile: "empresay.com.sv.zone"
```

```
router1:/etc/nsd# ls -l
total 20
-rw-r--r--    1 root     root           849 Dec 27 05:02 empresay.com.sv.zone
-rw-r--r--    1 root     root             0 Dec 27 04:39 empresay.inversa.zone
-rw-r--r--    1 root     root          7238 Dec 27 04:37 nsd.conf
-rw-r--r--    1 root     root          7132 Dec 10 07:14 nsd.conf.sample
```

Zona directa del nsd

```
$ORIGIN empresay.com.sv.    ; zona predeterminada (default)
$TTL 86400           ; segundos para 24 horas

@ IN SOA empresay.com.sv admin@empresay.com.sv (
           2014011001  ; contador serie
           28800       ; Refrescamiento 8 horas
           14400       ; Reintento 4 horas
           864000      ; Expira 24 horas
           86400       ; TTL Minimo
           )

           NS      ns1.empresay.com.sv.
           MX      10 mail.empresay.com.sv.

ns1                     IN    A     192.168.200.1
datastore1        IN    A     192.168.200.2
hipervisor1       IN    A     192.168.200.3
hipervisor2       IN    A     192.168.200.4
hipervisor3       IN    A     192.168.200.5
front-end1        IN    A     192.168.200.6
mail                    IN    A     192.168.200.11
datos                   IN    A     192.168.200.12
srvapp                  IN    A     192.168.200.13

*          IN     A    192.168.200.1
@          IN     A    192.168.200.1


router1:/etc/nsd# nsd-checkconf /etc/nsd/nsd.conf
router1:/etc/nsd# nsd-control rebuild
router1:/etc/nsd# /etc/init.d/nsd start
```