

# Práctica 7: Administración de la Red y Servicios Básicos

## Objetivos

En los sistemas actuales la configuración de la red y de los servicios de red es otro de los pilares fundamentales de la administración. En esta práctica revisaremos los aspectos básicos de la configuración de la red, y de algunos servicios de red básicos.

## Contenidos

### Preparando el entorno...

#### Introducción al entorno de Red

Configuración manual

Archivos de configuración de red

Resolución de nombres.

#### Configuración dinámica de hosts (DHCP)

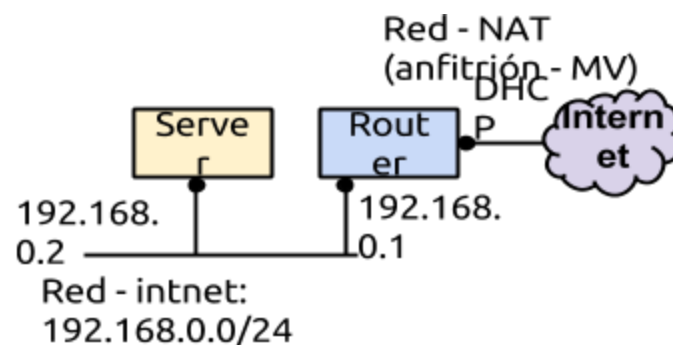
#### Monitorización de la Red

#### Acceso Remoto Seguro

Para saber más...

## Preparando el entorno...

En esta práctica necesitaremos dos máquinas virtuales según la topología que se muestra en la figura, al igual que en prácticas anteriores la máquina virtual Server y Router son clones enlazados de la instalación CentOS 7 disponible en el laboratorio. Antes de hacer los clones es importante **reinicializar las direcciones MAC de los interfaces de red**.



**Figura 1.** Topología de red usada en la Práctica 7.

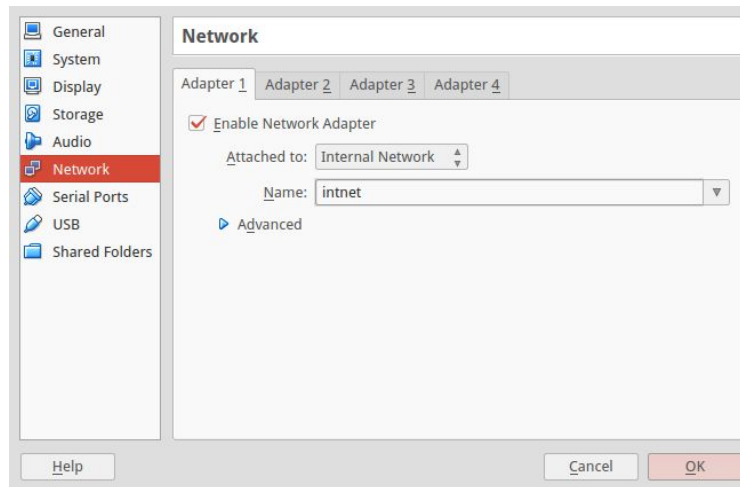
La configuración de la red se realizará de la siguiente forma:

- **[Server]** La máquina virtual Server tendrá un único interfaz de red del tipo 'Red Interna' y

conectado a la red intnet

- **[Router]** La máquina virtual Router tendrá dos interfaces de red: El Adaptador 1 será de tipo 'Red Interna' conectado a la red intnet; el Adaptador 2 que será de tipo NAT. Es importante mantener el orden de los interfaces para que el nombre de los dispositivos de red sea consistente con los enunciados de los ejercicios de la práctica.

La Figura 2 muestra la configuración de los interfaces para la máquina Router.



**Figura 2.** Configuración de los interfaces de red de la máquina virtual Router.

**Nota.** En la práctica cada ejercicio está etiquetado con el máquina virtual donde debe realizarse **[Server]** o **[Router]**.

## Introducción al entorno de Red

En primer lugar estudiaremos los comandos básicos para manejar el entorno de red, que se pueden clasificar en:

- Configuración: ip (o ifconfig, route) e ifup/ifdown
- Monitorización: ss (o netstat)
- Diagnóstico y análisis: ip, ping, arp y tcpdump/wireshark

Después veremos los principales archivos de configuración del sistema:

- Configuración de interfaces: `/etc/sysconfig/network-scripts/ifcfg-*`
- Resolución de nombres: `/etc/resolv.conf`, `/etc/nsswitch.conf` y `/etc/hosts`

### Importante

RedHat Enterprise Linux desde su versión 7, recomienda el uso del servicio NetworkManager para la gestión y configuración de interfaces de red. Este servicio permite la configuración dinámica de los interfaces de red y es de utilidad para equipos móviles.

Sin embargo, su uso en servidores no está muy extendido y habitualmente se deshabilita este servicio. Esta es la aproximación que seguiremos en este curso.

En **primer lugar desactivar en [Router, Server] el servicio NetworkManager (práctica 2)**

Junto con la introducción de systemd también se ha cambiado la **designación de los interfaces de red** (e.g. el tradicional `eth0` ó `wlan0`) por un modelo determinista basado en la información del Firmware del interfaz, la MAC o su ubicación física. También es posible mantener la denominación tradicional pasando `net.ifname=0` como argumento de arranque del kernel.

## Configuración manual

**Ejercicio 1. [Router]** Ejecutar el comando `ip link` para ver los interfaces del sistema. Observar la salida del comando y determinar el estado de cada interfaz: activo (UP) o inactivo (DOWN). El nombre de cada interfaz será de la forma `enp<pci>s<slot>`, por ejemplo `enp0s3` es la controladora ethernet de la controladora pci 0 y slot 3. Comprobar la correspondencia con la salida del comando `lspci`.

**Ejercicio 2. [Router]** Los interfaces se pueden activar/desactivar con este mismo comando: `ip link set <nombre_interfaz> <up|down>`. Comprobar el funcionamiento desactivando y activando el interfaz `enp0s3`. **Nota:** Además del estado se pueden fijar otras propiedades del enlace, p.ej. MTU o el nombre. Consultar la página de manual de `ip`, sección `ip link`.

**Ejercicio 2. [Router]** Las direcciones de cada interfaz se pueden ver con el comando `ip addr`. Observar la salida del comando y determinar las direcciones (número y tipo) asociadas a cada interfaz.

**Ejercicio 3. [Router, Server]** Configurar la red interna entre las dos máquinas usando el comando `ip address` (ver la sección correspondiente de la página de manual del comando `ip`). La dirección debe fijarse según la topología mostrada en el esquema. Comprobar los resultados con el comando `ip address`, observar la dirección de broadcast de cada interfaz.

**Ejercicio 5. [Router, Server]** Al configurar la red en un interfaz, automáticamente se añade la ruta para esa red. Las rutas se pueden ver con el comando `ip route`. Comprobar las rutas en todas las máquinas e interpretar la salida del comando.

**Ejercicio 6. [Router, Server]** Una vez configurada la capa de red (nivel 3, IP) debería comprobarse la conectividad a ese nivel con el comando `ping`.

- Comprobar la conectividad Server-Router en ambos extremos.

- Estudiar las opciones de ping. Especialmente interesantes son el número de solicitudes echo, el tamaño de los datos enviados, y ttl.

**Ejercicio 7. [Router, Server]** Para establecer la comunicación entre las dos máquinas es necesario disponer de las direcciones físicas. En IPv4, el protocolo ARP realiza esta resolución de direcciones.

- Después del ping, Router debe tener las direcciones MAC de Server. Averiguar la MAC con el comando `ip neigh`. Verificar con la información que muestra `ip link` en Server.
- Consultar la página de manual `ip`, sección `ip neighbour`. Estudiar cómo añadir y eliminar entradas manualmente.

**Ejercicio 8. [Router]** Las herramientas anteriores `ip` y `ping`, junto un monitor de red (sniffer), son de gran utilidad para determinar problemas en la red.

- Eliminar las entradas arp de la tabla en Router.
- Abrir un terminal monitorizar el tráfico del interfaz `enp0s3` (`tcpdump -i enp0s3`).
- Hacer ping a Server y ver el tráfico: pregunta-respuesta ARP y solicitud-respuesta ICMP-ECHO.
- Consultar la página de manual de `tcpdump` y estudiar algunas opciones de filtrado, especialmente por protocolo y direcciones de host destino y origen.

## Archivos de configuración de red

**Ejercicio 1. [Router, Server]** La configuración global de la red se puede configurar en `/etc/sysconfig/network`. El servicio `network` configura los interfaces de red definidos cuando arranca. Comprobar el servicio `network` con el comando `systemctl status`.

**Ejercicio 2. [Router, Server]** La configuración por defecto de cada interfaz de red se guarda en un archivo separado en la ruta: `/etc/sysconfig/network-scripts/ifcfg-<dev>`. Esto permite:

- Usar los comandos `ifup/ifdown`. Por ejemplo, `ifup enp0s3` aplicaría la configuración de `/etc/sysconfig/network-scripts/ifcfg-enp0s3`
- Hacer la configuración de red persistente para todos los interfaces de red

La configuración de un interfaz de red en IPv4 puede ser básicamente de dos tipos: DHCP y estática. A continuación se muestra un ejemplo de configuración para ambos casos

### Listado 2. Configuración de enp0s3 con DHCP

```
# Configuración DHCP
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

### Listado 3. Configuración de enp0s8 con IPv4 estática

```
# Configuración estática
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
NETWORK=192.168.0.0
NETMASK=255.255.255.0
```

IPADDR=192.168.0.1

- Configurar los archivos ifcfg-enp0s3 e ifcfg-enp0s8 para las máquinas según la sección anterior.
- Comprobar la red (`ip addr show enp0s3`), desactivar el interfaz (`ifdown enp0s3`), comprar la red (`ip addr`), activar el interfaz (`ifup enp0s3`). Verificar la conectividad en cada caso.
- Los ficheros admiten más opciones, estudiarlas.

**Nota:** Las configuraciones de red puede activarse reiniciando el servicio network.

## Resolución de nombres.

**Ejercicio 1. [Router]** La resolución de nombres se configura en `/etc/resolv.conf`. Este archivo contiene los servidores DNS (nameserver) y el dominio por defecto (search).

- Consultar el contenido en router. Verificar que el servidor DNS es el correcto y accesible por el host. En este caso VirtualBox en el anfitrión podrá actuar como servidor DNS.
- Comprobar el funcionamiento con la orden `host` (consulta DNS). Por ejemplo `host www.google.com`.
- Añadir el servidor 8.8.8.8, y repetir la consulta.

**Ejercicio 2. [Router, Server]** El sistema guarda (opcionalmente) una traducción estática de nombres de host en `/etc/hosts`, con el formato "dirección nombre1 nombre2...".

- Añadir el nombre de las máquinas y sus direcciones IP en `/etc/hosts`, una entrada para cada máquina, ej. `192.168.0.2 server`.
- Comprobar que ahora es posible hacer `ping server`
- El fichero que determina qué servicios usar (DNS ó `/etc/hosts`) es `/etc/nsswitch.conf`. Examinar su contenido, especialmente la línea "host:".

## Configuración dinámica de hosts (DHCP)

### Importante

Para poder atender las peticiones DHCP hay que desactivar las reglas de filtrado que por defecto aplica la instalación de CentOS. **Desactivar en Router el servicio firewalld (práctica 2)**

**Ejercicio 1. [Router]** El protocolo DHCP permite configurar la red de un host, incluyendo direcciones IP o servidores DNS, entre otros parámetros. Vamos a configurar el servicio dnsmasq, que además de servidor DHCP implementa un proxy DNS.

- El servicio se configura en `/etc/dnsmasq.conf`. Estudiar los comentarios referidos a dhcp.
- Configurar dhcp para la red `192.168.0.0/24` con `dhcp-range`. Escoger un rango y tiempo de lease para cada uno (ej. `dhcp-range=192.168.0.100,192.168.0.150,12h`).
- Reiniciar el servicio dnsmasq (usando el comando `systemctl`).

**Ejercicio 2. [Server]** Desactivar los interfaces y configurarlos con la orden (`dhclient -v enp0s3`).

**Ejercicio 3. [Server]** Cambiar la configuración `ifcfg-enp0s3` para que use dhcp y probarla con `ifdown/ifup`. Observar el tráfico con `tcpdump` intercambiado en otro terminal durante la configuración del interfaz ¿Cómo se podría filtrar la salida del comando `tcpdump` para que sólo muestre

los mensajes DHCP?.

**Ejercicio 4. [Server]** También funcionará el proxy DNS. Configurar Server de forma que resuelva los nombres de hosts usando router. Probar la traducción con por ejemplo con host [www.google.com](http://www.google.com). Probar a hacer ping desde Server a [www.google.com](http://www.google.com), ¿por qué no se recibe la respuesta?.

## Monitorización de la Red

Además de monitorizar el tráfico con tcpdump o wireshark es muy útil determina las conexiones establecidas con otras máquinas y los servicios que hay activos.

**Ejercicio 1. [Router]** Comprobar las estadísticas de cada interfaz con `ip -s link`, comprobar los bytes transmitidos y recibidos en cada caso.

**Ejercicio 2. [Router]** Los procesos que están escuchando en el sistema se pueden ver con `ss` (opción `-ta` para TCP o `-ua` para UCP) o con `lsof -i`. Establecer qué procesos en el sistema tienen puertos abiertos y las conexiones establecidas.

**Ejercicio 3. [Router]** Los números de puerto bien conocidos están definidos en `/etc/services`. Comprobar las correspondencia para TCP usando la opción `-n` de `ss` (`-tan`).

## Acceso Remoto Seguro

Habitualmente es necesario conectarse a otros sistemas para su administración o uso. Este acceso por terminal de forma remota se hace con `ssh` (secure shell).

**Ejercicio 1. [Server]** Comprobar que está en ejecución `sshd` y determinar el de puerto escucha.

**Ejercicio 2. [Router]** Acceder a Server como root (`ssh root@server`).

**Ejercicio 3. [Router]** Copiar segura de ficheros. Copiar el fichero `/etc/passwd` a server (`scp/etc/passwd root@server:/tmp/copia_passwd`). Observar la sintaxis y comprobar que la copia se ha realizado correctamente.

**Ejercicio 4. [Router]** Autenticación con par de claves pública/privada:

- Generar el par de claves con `ssh-keygen`. (no encriptar la clave privada)
- Copiar la clave pública a server1 (`ssh-copy-id -i .ssh/id_rsa.pub root@server`).
- Entrar en server como root (no pedirá clave). Ver los contenidos de `.ssh/authorized_keys` en server, contiene los contenidos de `id_rsa.pub`.
- Observar los permisos del directorio `.ssh` y sus contenidos.
- Comprobar la conexiones con `lsof` o `ss`.

**Ejercicio 5. [Server]** El servidor `ssh` dispone de múltiples opciones para ajustar su funcionamiento. Estudiar el fichero `/etc/ssh/sshd_config`

- Deshabilitar el login como root
- Reiniciar el servidor `sshd`
- Verificar el funcionamiento de la nueva configuración

### **Para saber más...**

- Túneles ssh que permiten conexiones seguras (opción -L)
- Uso de claves encriptadas, estudiar los comandos ssh-agent y ssh-add
- Redirigir conexiones gráficas (-X) y claves (-A)