

Integración en Red Local de Estaciones de Trabajo

Datos personales:

Orlando Alemán Ortiz

Samuel Díaz Cabrera

Curso 2005/06

Grupo 2

Licencia



Esta obra ha sido publicada bajo licencia "Reconocimiento-NoComercial-CompartirIgual 2.5 Spain" de Creative Commons, la cual implica que:

Usted es libre de:

- copiar, distribuir y comunicar públicamente la obra
- hacer obras derivadas

Bajo las condiciones siguientes:



Reconocimiento. Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador.



No comercial. No puede utilizar esta obra para fines comerciales.



Compartir bajo la misma licencia. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

Y además:

- Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.
- Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor
- Los derechos derivados de usos legítimos u otras limitaciones reconocidas por ley no se ven afectados por lo anterior.

Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nc-sa/2.5/es/> o envíe una carta a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Índice de contenidos

1. Previos.....	2
Introducción.....	2
Equipamiento empleado.....	2
2. Integración de las tarjetas de red.....	3
Conexión física.....	3
Proxy NAT (Enmascaramiento) / Routing.....	3
Empleando un encaminador (Router).....	4
Descubrimiento de las tarjetas a nivel de sistema operativo.....	5
Windows.....	5
Fedora Linux.....	6
3. Configuración de nombres de máquina	7
Windows.....	7
Fedora Linux.....	7
4. Configuración TCP/IP.....	9
Incorporación de computadores a sus redes locales.....	9
Windows.....	9
Fedora Linux.....	11
Compartiendo la conexión a una red externa.....	13
Windows.....	13
Fedora Linux.....	14
5. Compartición de recursos.....	15
Windows.....	15
Fedora Linux.....	16
6. Sesión remota.....	18
Escritorio Remoto.....	18
Windows.....	18
Asistencia remota.....	19
Windows.....	19
Fedora Linux.....	20
7. Configuración del Router.....	22
8. Herramientas de diagnóstico.....	24
9. Gestión de servicios en Fedora Linux.....	25
10. Referencias.....	27
Artículos online.....	27
Bibliografía electrónica.....	27

1. Previos

Introducción

El presente documento representa la memoria de la práctica 2 de Redes de Computadores, asignatura de la carrera de Ingeniería en Informática. en la cual se aborda la integración de estaciones de trabajo en una red local.

Llevaremos a cabo esta labor en dos sistemas operativos tan dispares como lo son *Windows* y *Fedora Linux*, y mostraremos de forma breve cómo compartir recursos y asistir remotamente a través de la red ya constituida.

Para llevar a cabo la exposición, seguiremos el orden de realización práctico de las tareas.

Equipamiento empleado

Hardware:

- 1 x PC con 2 tarjetas de red, que actuará como pasarela en la primera parte del trabajo.
- 1 x PC con 1 tarjeta de red, que actuará de estación.
- 2 x cable de red UTP Cat.5 plano con conectores RJ45
- 1 x cable de red UTP Cat.5 cruzado y con conectores RJ45
- 1 router de 4 puertos

Software:

- Por cada PC, una instalación base de *Microsoft Windows XP* y otra de *Fedora Linux*
- En las instalaciones de *Fedora*, los paquetes de utilidades y servidor de SAMBA.
Opcionalmente el asistente de configuración gráfico
- Controladores de los dispositivos de red en el caso de *Windows XP*

2. Integración de las tarjetas de red

Esta fase comprende tanto la conexión física de los dispositivos como la instalación en el entorno operativo donde se utilicen. No obstante, la segunda de ellas se aleja de nuestro objetivo y, por tanto, no la trataremos aquí.

Conexión física

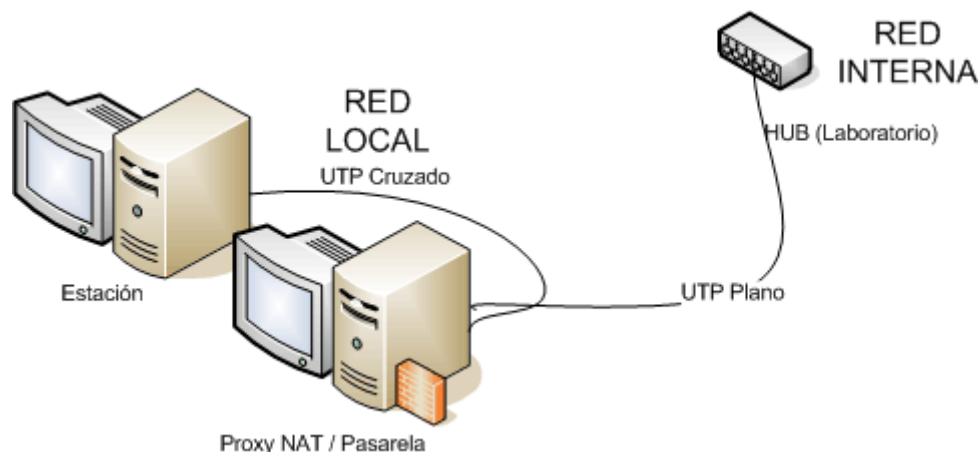
Para llevar a cabo nuestra labor emplearemos dos esquemas organizativos distintos. En el primero de ellos, comúnmente llamado *Proxy NAT*, un computador (llamase *proxy* o *pasarela*) dispone de acceso a una red externa y permite a otros conectarse a esa red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el *proxy* quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. A todos los efectos, en la red externa todas las peticiones son vistas como propias del proxy, no de sus *estaciones* y por tanto, no se conoce la existencia de esa subred.

En cambio, en el segundo esquema, denominado *encaminamiento a través de router*, todos los computadores de la red se conectan individualmente a un dispositivo físico denominado *router*, que actúa como pasarela a otra red de nivel superior (generalmente *Internet*). El *router* interconecta a todos los computadores y toma decisiones lógicas con respecto a la mejor ruta para el envío de los datos.

Proxy NAT (Enmascaramiento) / Routing

Para implementar este modelo de organización requerimos de tantas tarjetas de red en el computador pasarela como estaciones a las que dé servicio. Adicionalmente, tendremos otra tarjeta de red para conectarnos a la red interna del laboratorio.

En cambio, el computador estación sólo requiere, para este propósito, de una única tarjeta de red, que será la que usará para ser servido por la *pasarela*.



(Figura 1)

Conexionado (1 → 1 → N):

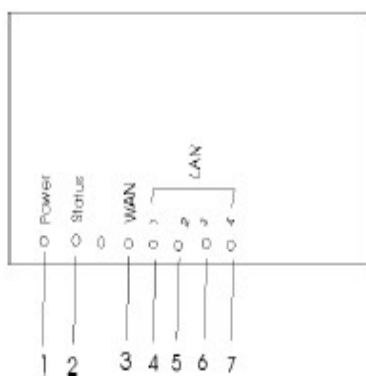
1. Haciendo uso de un cable de red cruzado conectamos la tarjeta de red de la estación a una de las tarjetas de red del computador *Proxy*.
2. Tomando otro cable de red, pero esta vez plano, conectamos la tarjeta de red de “salida” del computador pasarela al *HUB* de la red interna del laboratorio.

Empleando un encaminador (Router)

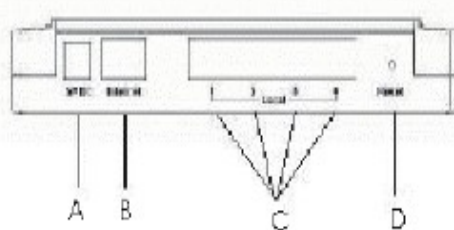
En este modelo los terminales sólo necesitan una única tarjeta de red para conectarse al *router*. Ninguno de ellos hará de pasarela, si bien podrían hacerlo perfectamente hacia otro equipo si, siguiendo el esquema anterior, le añadiésemos otra tarjeta de red. También es posible hacer una conexión en cascada de *routers*.

El conexionado que requiere este esquema es bien sencillo, como veremos a continuación. Antes no viene mal reseñar algunas características del *router* que vamos a utilizar:

LED Indicators on the Front Panel



Ports on the Rear Panel



(Figura 2)

Características físicas:

- 1 puerto para la conexión a Internet (WAN). [B en la figura 2]
- 4 puertos para la conexión de dispositivos terminales. [C en la figura 2]
- Botón de *reset*, para restaurar la configuración de fabrica. [D en la figura 2]

Modos de funcionamiento:

Admite los 2 modos de funcionamiento más comunes, *monopuerto* y *multipuerto*.

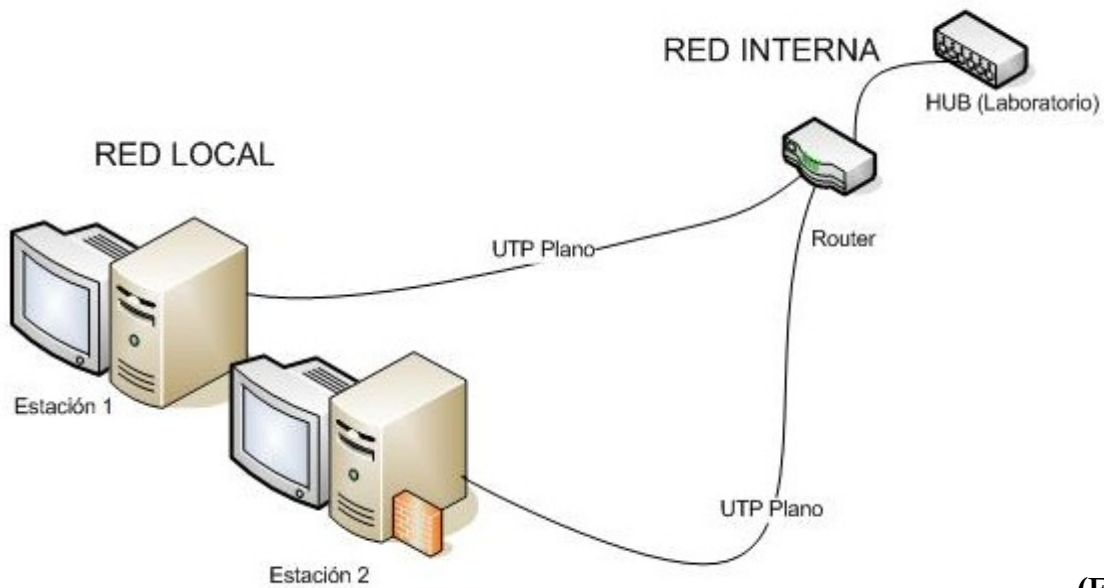
El primer modo convierte al *router* en un simple intermediario, dejando que pasen todos los datos desde *Internet* a un ordenador directamente, y en caso de varios ordenadores sólo uno tiene, en principio, salida a *Internet*, ya que *router* asigna la IP pública a éste y es por lo que recibe la información sin problema alguno

En cambio, en modo *multipuerto*, el *router* actúa como filtro y muro de entrada, distribuyendo los datos entre los dispositivos. Los datos son gestionados por el router, que es quien realiza la función de *NAT*, permitiendo que varios equipos accedan a la Internet (o red de salida) sin necesidad de que otros terminales estén encendidos.

En nuestro caso, planeamos trabajar en modo multipuerto, así que el esquema de configuración (figura 3) que debemos seguir es responde al conexionado siguiente:

Conexionado (2 → 1 → N → 1):

1. Los 2 terminales se conectarán al *router* a través de sendos cables planos, ocupando 2 conexiones de las 4 que dispone.



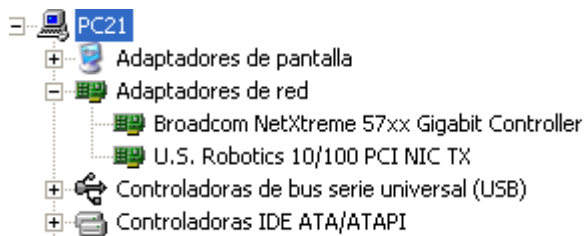
(Figura 3)

Descubrimiento de las tarjetas a nivel de sistema operativo

Windows

Para comprobar que los adaptadores de red están correctamente instalados en el sistema operativo y que no presentan conflictos, accedemos a *Inicio>Panel de Control>Sistema>Hardware>Administrador de dispositivos>Adaptadores de red* y observamos si se encuentran en el listado desplegable. En tal caso, haciendo click en *Propiedades del dispositivo* podremos ver si su estado es correcto.

A partir de ahora podremos configurar las conexiones de red yendo a *Inicio>Panel de Control>Conexiones de red*. Los dispositivos se denominan según su fabricante/modelo y, si coincidiesen, se les distinguiría con la cadena #1, #2, etc. en orden de antigüedad, IRQ, etc.



(Figura 2)

Fedora Linux

En el caso de *Fedora Linux*, para conocer si las tarjetas de red han sido autodetectadas y sus módulos se encuentran cargados en memoria, hacemos lo siguiente:

- Leer el fichero `/etc/sysconfig/hwconf`, que contiene toda la información referente al hardware que *Kudzu*¹ ha detectado en el sistema (driver, dispositivo, etc) y buscamos las entradas referentes a dispositivos de red (*net*). Si todo es correcto, deberían haber tantas entradas como tarjetas de red hayan integradas. Conviene tomar nota de qué dispositivo representa (*eth0*, *eth1*, etc) a cada tarjeta, ya que esta información la necesitaremos posteriormente.
- Leer el fichero `/proc/net/dev` y comprobar que actualmente hay mapeados tantos dispositivos como detectados en `/etc/sysconfig/hwconf` o en su defecto, que estén activos los que vamos a utilizar.

Existe un método alternativo, aunque menos exhaustivo y que requiere ejecutar el entorno gráfico, de conocer esta información. Consiste en ejecutar la herramienta *system-config-network* y ver si aparecen las distintas interfaces en la pestaña *Hardware*.



(Figura 4)

¹ *Kudzu* es el sistema de descubrimiento y autodetección de hardware en *Fedora Linux*

3. Configuración de nombres de máquina

Un aspecto importante a tener en cuenta cuando integramos computadores a una red es asignarles un nombre identificativo a cada máquina. Esto se debe a que a los humanos nos resulta mucho más fácil referirnos a los equipos por el nombre que le hallamos asignado que por direcciones físicas.

Por lo general, se utilizan se utilizan dos métodos distintos de resolución de nombres. El primero de ellos es el “*nombre NetBios*”, que se utiliza para identificar las computadoras que compartan recursos en una red *Windows*. El *hostname*, por el contrario, se utiliza para ofrecer servicios *TCP/IP* (*FTP, telnet, ping, etc*) a nivel local o en red .

Windows

Por defecto, a partir de *Windows 2000* tanto *hostname* como *nombre NetBios* se configuran como un único valor. Para fijarlo, accedemos a *Inicio>Panel de Control>Sistema>Nombre de Equipo* y seleccionamos “*Cambiar*”.

Además del nombre de la máquina, en esta localización podemos establecer dos datos interesantes más: el “*grupo de trabajo*” y la “*descripción del equipo*”, útiles en la compartición de recursos *Windows*.

Aquí mostramos un ejemplo de la configuración usada en uno de ellos equipos, en este caso el *pasarela*:

The image shows a screenshot of the Windows 'Nombre de equipo' (Computer Name) settings window. It contains three input fields: 'Descripción del equipo:' with the value 'Pasarela', 'Nombre de equipo:' with the value 'PC-21', and 'Grupo de trabajo:' with the value 'REDES'. The 'Grupo de trabajo' field is highlighted with a yellow background.

(Figura 5)

	<i>Nombre NetBios</i>	<i>Hostname</i>	<i>Descripción</i>	<i>Grupo de trabajo</i>
<i>Pasarela</i>	PC-21	PC-21	Pasarela	REDES
<i>Estación</i>	PC-22	PC-22	Estación	REDES

Si cambiamos el grupo de trabajo, windows nos pedirá reiniciar el ordenador para validar los cambios.

Fedora Linux

Como ya se ha dicho con anterioridad, el protocolo *NetBios* responde a la necesidad de *Microsoft*, creadora de *Windows*, de tener su propio sistema de compartición de recursos y, en principio, hablar de “*nombre NetBios*” en redes *Linux* parece no tener mucho sentido.

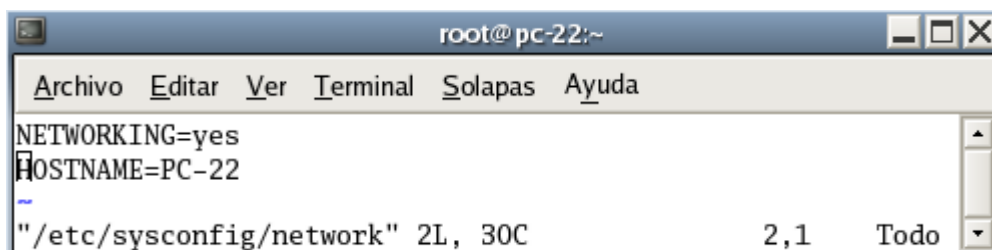
Desde 1984 los programadores de sistemas *UNIX* desarrollan su propio sistema de archivos distribuido, *NFS*, que permite el acceder a los archivos de una red de forma tan fácil a un disco

duro local. Sin embargo, este protocolo usa el propio *hostname* de la máquina.

En principio, sólo se requerirá un “*nombre NetBios*” en el caso de que se decida implementar una red mixta, en que tanto los sistemas *Windows* como *Linux* compartan archivos, impresoras etc.

La compartición de recursos en una red *Windows* la abordaremos más adelante, cuando expliquemos cómo configurar *SAMBA*. En este apartado sólo nos fijaremos en el *hostname*.

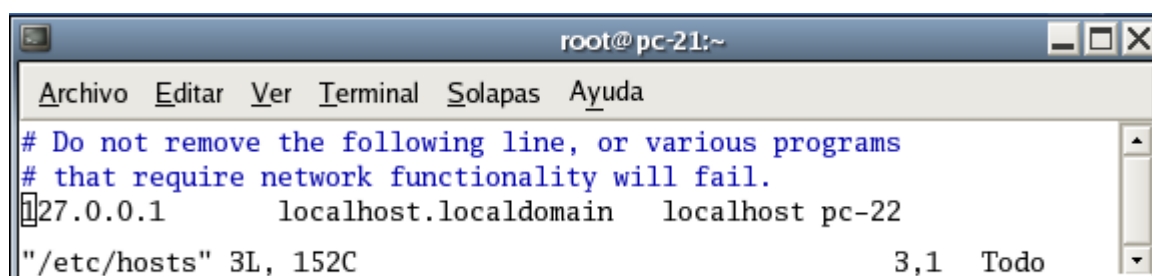
Para fijar el nombre de la máquina, editamos el fichero `/etc/sysconfig/network` y establecemos la entrada “*HOSTNAME*” al valor deseado. Por ejemplo, la estación tendría el siguiente valor:



```
root@pc-22:~
Archivo  E_ditar  V_er  T_erminal  S_olapas  A_yuda
NETWORKING=yes
HOSTNAME=PC-22
~
"/etc/sysconfig/network" 2L, 30C      2,1  Todo
```

(Figura 6)

Para referenciar a nuestra máquina localmente usando *PC-22* podemos añadir a a entrada “172.0.0.1” de `/etc/hosts` el alias *PC-22*. Quedando una cosa así:



```
root@pc-21:~
Archivo  E_ditar  V_er  T_erminal  S_olapas  A_yuda
# Do not remove the following line, or various programs
# that require network functionality will fail.
172.0.0.1      localhost.localdomain  localhost pc-22
"/etc/hosts" 3L, 152C      3,1  Todo
```

(Figura 7)

Como siempre, existe un método alternativo y gráfico, configurarlo en la pestaña *Hosts* de la herramienta *system-config-network*.

NOTA: El nombre de la máquina continuará siendo PC-22 hasta que se reinicie el sistema, salvo que se ejecute “hostname <nombre>” para fijar un nuevo valor en caliente. Esta práctica es poco recomendada, ya que pueden existir aplicaciones que estén usando el anterior nombre para referenciar a servicios en ejecución (por ejemplo, Gnome).

4. Configuración TCP/IP

Incorporación de computadores a sus redes locales

Por cada interfaz de red que tengamos en un sistema computador, se tiene una *IP* identificativa. Dependiendo del modelo escogido tenemos una configuración *TCP/IP* u otra.

Las 3 tablas siguientes muestran las configuraciones con que debemos configurar nuestras computadoras para corresponder a la implementación física que se haya escogido. Las dos primeras, establecen unas configuraciones *TCP/IP* estáticas, con valores fijados por nosotros mismos, mientras que la última delega esta responsabilidad al router, quien actúa como servidor DHCP en nuestra red local.

<i>Proxy NAT (Enmascaramiento) / Routing</i>			
<i>Descripción</i>	<i>Pasarela ip externa</i>	<i>Pasarela ip interna</i>	<i>Estación</i>
Dirección IP	172.16.1.3	172.16.3.1	172.16.3.2
Máscara	255.255.255.0	255.255.255.0	255.255.255.0
Puerta de Enlace	172.16.1.1	-	172.16.3.1
D.N.S primaria	193.145.143.100	-	193.145.143.100
D.N.S secundaria	193.145.147.22	-	193.145.147.22

<i>Empleando un encaminador (Router) – Conf. estática</i>		
<i>Descripción</i>	<i>Estación 1</i>	<i>Estación2</i>
Dirección IP	192.168.1.1	192.168.1.2
Máscara	255.255.255.0	255.255.255.0
Puerta de Enlace	192.168.1.254	192.168.1.254
D.N.S primaria	193.145.143.100	193.145.143.100
D.N.S secundaria	193.145.147.22	193.145.147.22

<i>Empleando un encaminador (Router) – DHCP</i>		
<i>Descripción</i>	<i>Estación 1</i>	<i>Estación2</i>
Dirección IP	Gestionado por DHCP	Gestionado por DHCP
Máscara		
Puerta de Enlace		
D.N.S primaria		
D.N.S secundaria		

A continuación explicamos, mediante un ejemplo, cómo configurar nuestros sistemas operativos para usar estos datos.

Windows

Si accedemos a *Inicio>Panel de Control>Conexiones de Red* podremos ver las conexiones de red activas. Cada icono como los que salen en la figura 8 representa una conexión. El número de conexiones depende del terminal en el que estemos trabajando; por ejemplo, en el esquema *Proxy NAT / Routing* la estación tiene sólo una conexión relacionada con la única tarjeta de red que existe, pero en la pasarela existen 2 conexiones, una para la tarjeta de red que da salida y otra para

la que permite la conexión interna.



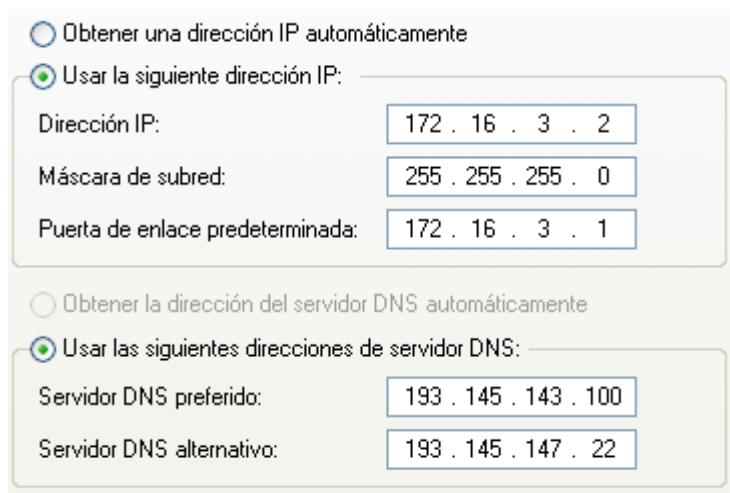
(Figura 8)

Para configurar las propiedades *TCP/IP* hacemos click con el botón derecho sobre la conexión que vayamos a configurar y accedemos a sus “Propiedades”



(Figura 9)

En *TCP/IP > Propiedades*, podemos fijar si queremos que *Windows* se encargue de hacer una petición de *DHCP* (primera opción) cuando se active la conexión o si debe ceñirse a una configuración manual. Por ejemplo, los valores a poner en la conexión de salida de la pasarela hacia la red local según la primera tabla sería:



(Figura 10)

Téngase en cuenta que ésto aún no permite que se comparta la conexión a Internet con la estación, aunque sí que se podrán compartir archivos e impresoras entre los equipos de una misma red.

Fedora Linux

Para configurar la red en Linux podemos optar entre una configuración volátil, es decir, con ajustes que se perderán al reiniciar la computadora o al cargar perfiles por defecto, o estática, configurando un perfil de red. El método volátil de *Fedora* respeta la forma estándar de configurar una red en *Linux*, mediante el conjunto de herramientas denominado “*net-tools*”. En cambio, para la configuración estática *Fedora* opta por un sistema de perfiles y configuraciones guiado por asistentes, que hace tediosa la configuración manual.

Configuración volátil – Estática

Para configurar una de interfaz de red debemos conocer qué fichero dispositivo lo representa. Este dato ya lo obtuvimos en el Capítulo 2. Por ejemplo, en nuestro equipo estación se trata del dispositivo *eth0*.

Los pasos que debemos seguir son los siguientes:

1. Deshabilitar la interfaz de red en caso de que esté activa. Para comprobarlo, ejecutamos “*ifconfig*”, que nos debe devolver el listado de dispositivos activos. En caso de que el dispositivo a configurar aparezca, ejecutamos “*ifconfig eth0 down*”
2. Comprobar que la tabla de rutas sólo tiene referencias a redes que ya hayamos configurado y que deban estar activas: comando “*route*”
3. Habilitarla nuevamente, pero con la nueva configuración IP, haciendo uso de *ifconfig*, en el caso de la estación sería así:
“*ifconfig eth0 inet 172.16.3.2 netmask 255.255.255.0 broadcast 172.16.3.255*”
4. Ingresar en el caso de ser necesaria, la información relacionada con el enrutado o puerta de enlace. Para nuestro ejemplo,
“*route add default gw 172.16.3.1*”
5. Comprobamos que todo es correcto, ejecutando sin parámetros “*ifconfig*” y “*route*”.
6. Añadir las direcciones de los servidores *DNS* de nuestro proveedor de Internet al fichero */etc/resolv.conf*

Configuración volátil – Dinámica

Los pasos que debemos seguir son los siguientes:

1. Deshabilitar la interfaz de red en caso de que esté activa. Para comprobarlo, ejecutamos “*ifconfig*”, que nos debe devolver el listado de dispositivos activos. En caso de que el dispositivo a configurar aparezca, ejecutamos “*ifconfig eth0 down*”
2. Comprobar que la tabla de rutas sólo tiene referencias a redes que ya hayamos configurado y que deban estar activas: comando “*route*”
3. Habilitarla nuevamente, pero con la nueva configuración IP, haciendo uso de *dhclient*:
“*dhclient eth0*”
4. Comprobamos que todo es correcto, ejecutando sin parámetros “*ifconfig*” y “*route*”.

En la siguiente figura podemos ver el resultado de nuestra ejecución de los pasos de configuración estática en el computador estación:

```
[root@pc-22 ~]# ifconfig eth0 inet 172.16.3.2 netmask 255.255.255.0 broadcast 172.16.3.255
[root@pc-22 ~]# ifconfig
lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:1566 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1566 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:1567464 (1.4 MiB)  TX bytes:1567464 (1.4 MiB)

eth0       Link encap:Ethernet  HWaddr 00:0F:1F:DA:0E:F7
            inet addr:172.16.3.2  Bcast:172.16.3.255  Mask:255.255.255.0
            inet6 addr: fe80::20f:1fff:feda:ef7/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:0 (0.0 b)  TX bytes:378 (378.0 b)
            Interrupt:11

[root@pc-22 ~]# route
[root@pc-22 ~]# route add default gw 172.16.3.1

[root@pc-22 ~]# route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
default        172.16.3.1     255.255.255.0  UG    0      0      0 eth0
172.16.3.0     *              255.255.255.0  U     0      0      0 eth0
```

(Figura 11)

Configuración persistente

Existen hasta 3 asistentes de configuración de red en *Fedora*, aunque sólo prestaremos atención al asistente gráfico, *system-config-network*. Si lo ejecutamos, podremos configurar fácilmente nuestra red, accediendo a *Dispositivos>Nuevo*. En el primer dialogo seleccionamos “Conexión Ethernet”; en el siguiente, el dispositivo que vamos a utilizar, que en el caso de la estación del esquema sin “router” será *eth0* y finalizamos indicando los datos de la conexión (*IP*, máscara de red, *DNS* y puerta de enlace) para una conexión estática o activando la opción de configuración dinámica para el caso de usar *DHCP*.

Compartiendo la conexión a una red externa

Para compartir la conexión de un equipo pasarela con sus estaciones son posibles dos formas. La primera de ellas, denominada *enmascaramiento* o *NAT*, consiste en mantener ocultos al exterior los detalles de las subredes que cuelgan del computador *pasarela*, modificando en caso de envío a un equipo externo el campo “IP origen” de los datagramas enviados por éstos para enviarlos al exterior con la IP de la pasarela. Se trata, por tanto, de un mecanismo de traducción en que los paquetes se envían y se reciben con firma de la pasarela y luego vueltos a “firmar” para devolverlos al computador destino del datagrama respuesta.

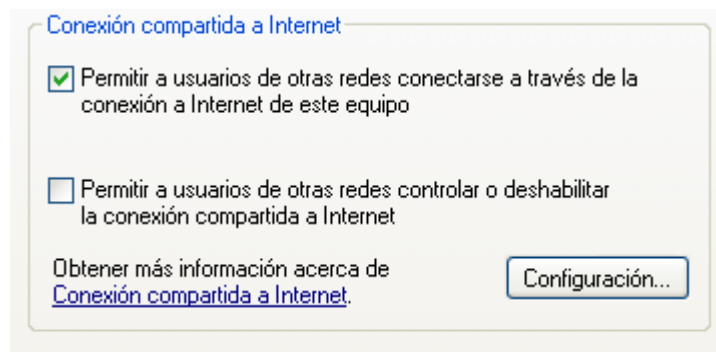
La otra forma, *routing*, consiste en dejar intacto el datagrama y simplemente enviarlo tal cual al siguiente nivel. Los nodos de los siguientes niveles deben conocer cómo llegar al origen y al destino, lo que implica que al menos el computador pasarela/router de la primera red superior debe conocer detalles de la organización de nuestra red. El conocimiento en niveles de red superiores depende de si se usa en ellos *NAT* o *routing*.

Windows

Para compartir una conexión podemos en *Windows* tendremos en cuenta las dos formas explicadas anteriormente:

Enmascaramiento o NAT

Situándonos en el equipo pasarela, accedemos a *Inicio*»*Panel de Control*»*Conexiones de Red* y sobre la conexión de salida, hacemos click en “Propiedades”. En la pestaña “Opciones Avanzadas” activamos “Permitir en otras redes conectarse a través de la conexión a Internet de este equipo”.



(Figura 13)

Es posible que el *Windows* decida unilateralmente cambiar las propiedades *TCP/IP* usadas en esta conexión. Es recomendable revisarlas.

Routing

Para habilitar “*routing*” necesitamos modificar una clave del registro de *Windows*. Para ello vamos a *Inicio*»*Ejecutar* y tecleamos “*regedit*”.

A través del árbol de la izquierda accedemos a la entrada “*HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters*”

y fijamos *IPEnableRouter* a "1" (activado).

Fedora Linux

En el caso de *Fedora Linux*, sólo abordaremos cómo activar "routing". También es posible usar *enmascaramiento* a través del firewall del núcleo, "iptables", o de "Firestarter", aunque se sale fuera de nuestra labor de prácticas.

Routing

Activar este método de transmisión es tan fácil como editar el fichero */etc/sysctl.conf* y poner la entrada *ipv4.ip_forward* a "1".

Es conveniente reiniciar el demonio de red para que la nueva configuración sea cargada:
"/etc/init.d/network restart"

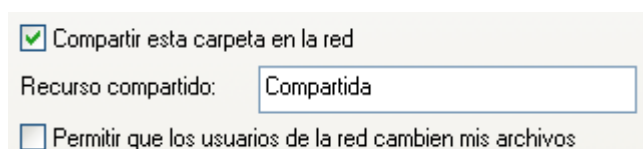
5. Compartición de recursos

En este apartado trataremos la compartición de recursos (carpetas e impresoras) en red mediante el protocolo *NetBios*. Como contamos en el capítulo de configuración de nombres de máquina, *NetBios* es el protocolo de compartición por excelencia en redes *Windows*. Son posibles otros protocolos de compartición de ficheros o de servicio, pero no los abordaremos aquí.

En lo que sigue explicaremos como compartir en *Windows* y *Linux* siguiendo este protocolo.

Windows

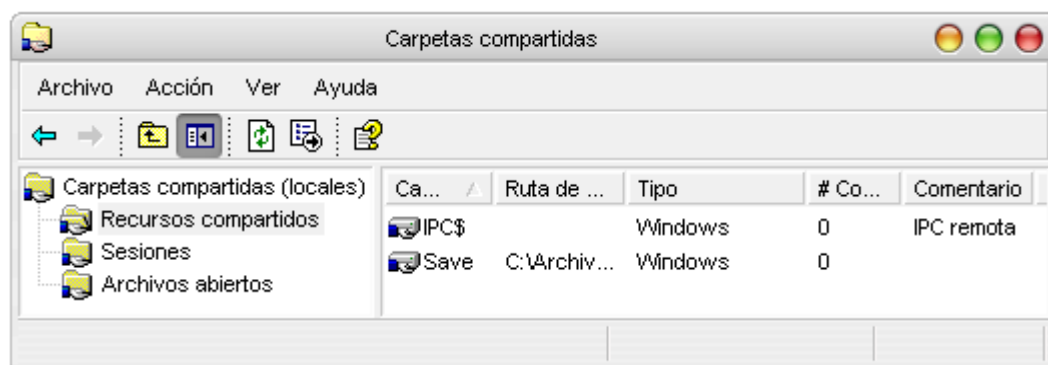
La forma de compartir recursos en *Windows XP* es muy sencilla. Seleccionamos el recurso (una carpeta o una impresora) a compartir y con un click derecho accedemos al menú contextual del archivo. Con otro click, escogemos la opción “*Compartir y seguridad*” y activamos la casilla correspondiente a la compartición del recurso, asignándole el nombre con que creamos que sea accesible desde la red. Tenemos la opción también de habilitar permisos de escritura sobre el contenido de la carpeta.



(Figura 14)

Si ejecutamos la versión “Professional” de *Windows* dispondremos de un menú donde fijar explícitamente los permisos de acceso al recurso compartido.

Una vez hechos los cambios, aceptamos y ya tenemos el recurso compartido. Para comprobar si el proceso se ha realizado de forma correcta, podemos acceder a un servicio de administración de recursos compartidos que ofrece *Windows*. Para ello ejecutamos el comando “*fsmgmt.msc*” :



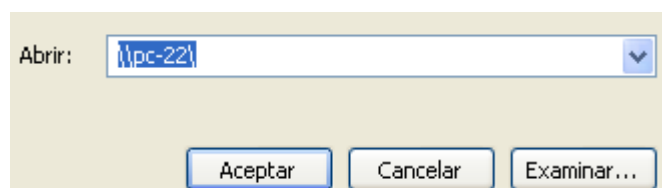
(Figura 15)

La herramienta nos permite ver los recursos compartidos que se comparten en la máquina, si alguien ha iniciado sesión remota por *NetBios*, o si se está accediendo a ellos. También permite gestionar las comparticiones, de forma más centraliza.

Acceso a los recursos compartidos

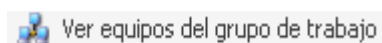
En *Windows* existen 2 formas para acceder a los archivos compartidos por un equipo. Una de ellas es directamente especificando la ruta del recurso compartido en la red. En la primera opción, en *Inicio*>*Ejecutar* se introduce la ruta y tras aceptar obtendremos trascurridos unos instantes la

ventana del recurso compartido.



(Figura 16)

La otra forma consiste en acceder usando el explorador del sistema, accediendo a “*Mis Sitios de red*”. Ejecutamos *Inicio>Mis Sitios de Red* y aparecerá una ventana con los recursos compartidos usados recientemente. Para acceder a todos los recursos disponibles en nuestro grupo de trabajo, hacemos click en:



(Figura 17)

y nos aparecerán los equipos conectados a nuestro mismo grupo de trabajo:



(Figura 18)

Haciendo doble click sobre cualquiera de ellos, veremos los recursos que comparte.

Si quisiésemos compartir una impresora simplemente seguimos la rutina de instalación normal, con la salvedad de situar como situación de la impresora la ruta remota.

ANOTACION: Puede ser necesario tener acceso local en el sistema de archivos para que funcione correctamente. Para más información mirar la herramienta de ayuda del sistema

Fedora Linux

En *Linux* se dispone de un conjunto de herramientas + servidor denominado “*SAMBA*” que implementa la compartición de componentes a través de redes *NetBios*, permitiendo la homogeneización aparente de la red. Suponiendo instalado este pack en la máquina objetivo, procedemos a configurar de forma básica el sistema para compartir una carpeta.

El primer paso es asegurarnos de que actualmente el servidor de *Samba* no está activo. Para ello ejecutamos “*/etc/init.d/smb stop*”. Debemos tener en cuenta que si actualmente no está activo, posiblemente el sistema no haya sido configurado para ejecutarlo en el nivel de ejecución actual. Para solventar esto, debemos activar el servicio “*smb*” al inicio según la forma explicada en el capítulo 9 o arrancarlo manualmente con “*/etc/init.d/smb start*” cuando lo vayamos a necesitar.

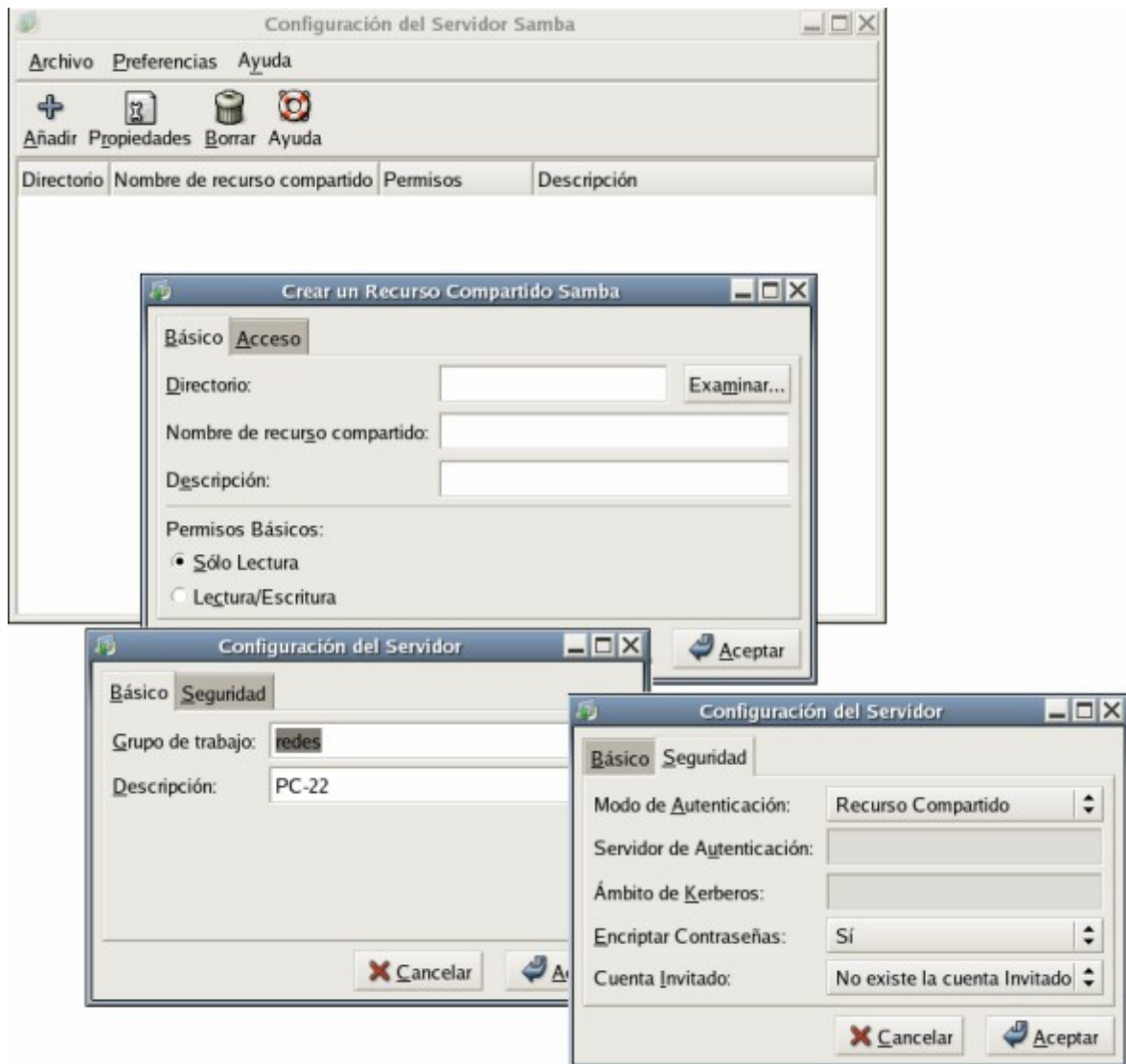
A continuación, editamos el fichero */etc/samba/smb.conf*. Podemos hacerlo manualmente o simplemente ejecutando un asistente que nos proporciona *Fedora*. Dado que nuestra intención es sólo probar su funcionamiento, nos da igual una forma u otra. Optamos por la segunda opción.

Ejecutamos “*system-config-samba*” y mediante una sencilla ventana podremos configurar las comparticiones.

Mediante la opción “Añadir” podremos agregar carpetas compartidas. En nuestro caso, compartiremos a modo de ejemplo /share (nota: necesitamos crear y dar los permisos locales pertinentes a ese directorio). Podemos fijar en este instante, los permisos que deseamos dar a quien acceda al recurso (lectura/escritura) y añadir un comentario explicativo.

Haciendo click en *Preferencias*>*Configuración del servidor* podremos fijar el nombre *NetBios* que utilizará el servidor *Samba* y la configuración de seguridad a utilizar a nivel global. Existen tres niveles, *Usuario*, *Servidor* y *Compartido*. Dado que no deseamos jugar con los usuarios del sistema ni de samba y tampoco es nuestra intención fijar una contraseña de acceso, optamos por la la opción *Compartido*, que permite el acceso a toda la red.

Ya ha terminado la configuración. Ahora tan sólo tenemos que arrancar el el servicio: “*/etc/init.d/smb start*”



(Figura 19)

6. Sesión remota

Entendemos por sesión remota la posibilidad de conectarnos a un computador remoto para realizar algún tipo de tarea como si fuera local. En este apartado abordaremos dos formas de sesión orientadas a la ejecución de un entorno de escritorio remoto.

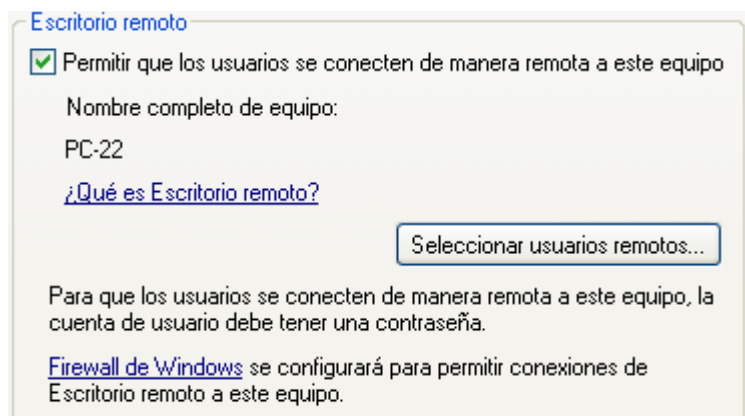
Por una parte tenemos, “escritorio remoto”, que consiste en conectarse a un computador y para realizar tareas de usuario. Para ello requerimos de una cuenta de usuario en el destino. Por otra, “asistencia remota”, que consiste en compartir la sesión de un usuario que se encuentra utilizando el computador remoto. Esta segunda posibilidad permite “asistir”, entre otras cosas, al usuario remoto en la resolución de problemas en su computador.

Escritorio Remoto

Permite el inicio de una sesión en un equipo remoto, accediendo a sus recursos de forma remota.

Windows

Para conectarnos remotamente a una máquina realizando “*Escritorio remoto*”, necesitamos una cuenta de usuario en ese computador. La máquina destino debe además tener habilitada la opción correspondiente en *Propiedades de MiPC > Acceso Remoto*. Y, si la cuenta del usuario a emplear no tiene privilegios de administrador, hay agregarlo a la lista de permitidos.



(Figura 20)

Se ejecuta en *Inicio > Accesorios > Comunicaciones > Asistente para escritorio remoto* o mediante el comando “*mstsc.exe*”.



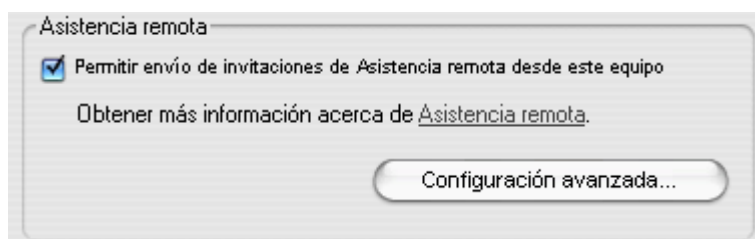
(Figura 21)

En “opciones” introducimos tanto el usuario como su contraseña con la que conectar a la máquina remota; además de éstas incluye diversas opciones de rendimiento basadas en la conexión a usar.

Asistencia remota

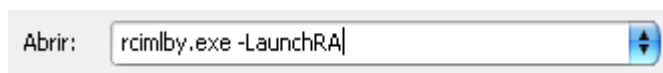
Windows

Al igual que el escritorio remoto, la asistencia remota permite acceder a otro equipo, compartiendo la sesión con otro usuario. Para activar esta opción debemos habilitar la opción “Permitir envío de invitaciones de Asistencia remota desde este equipo” en *Propiedades de MiPC>Acceso Remoto*.



(Figura 22)

La invitación de asistencia remota se puede realizar desde el programa “*Windows Messenger*” ó desde el programa de correo “*Microsoft Outlook*”, otra opción es ejecutar el siguiente comando “rcimlby.exe -LaunchRA”:



(Figura 23)

Se muestra en pantalla una ventana donde poder elegir como realizar la invitación:

Invite alguien en quien confíe para que le ayude. Usando una conexión Internet, cualquiera que esté ejecutando Windows XP puede charlar con usted, ver su pantalla, y con su permiso, trabajar en su equipo.

 Invitar a alguien para que le ayude

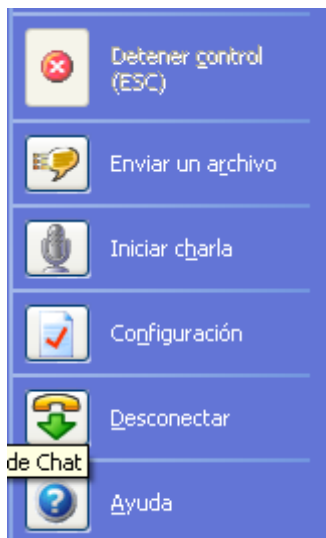
 Ver el estado de la invitación (0)

Más información acerca de Asistencia remota

(Figura 24)

Con la primera opción enviamos la invitación a algún contacto de *windows messenger* ó a otra persona mediante su correo electrónico; La segunda opción nos detalla la fase en la que se encuentra nuestra invitación, si ha sido recibida o no, cuando caduca, etc....

Cuando es aceptada la invitación tenemos un menú con el que poder colgar la conexión, detener el control del invitado, enviar un archivo, iniciar una charla, etc...



(Figura 25)

En cualquier momento podemos desconectar la conexión presionando la tecla ESC.

Fedora Linux

En el caso de *Fedora Linux* disponemos de las herramientas del entorno de escritorio *KDE* que nos permiten realizar una conexión de red privada (*VPN*) entre dos computadores, para compartir el escritorio de uno de ellos.

Realizar una petición

Al igual que en *Windows*, es necesario realizar una petición de asistencia desde el equipo a ser asistido al otro computador. Para ello, *KDE* nos genera un usuario y una contraseña temporales y nos facilita los medios (por ejemplo, vía *KMail* o *Kopete*) para su envío.

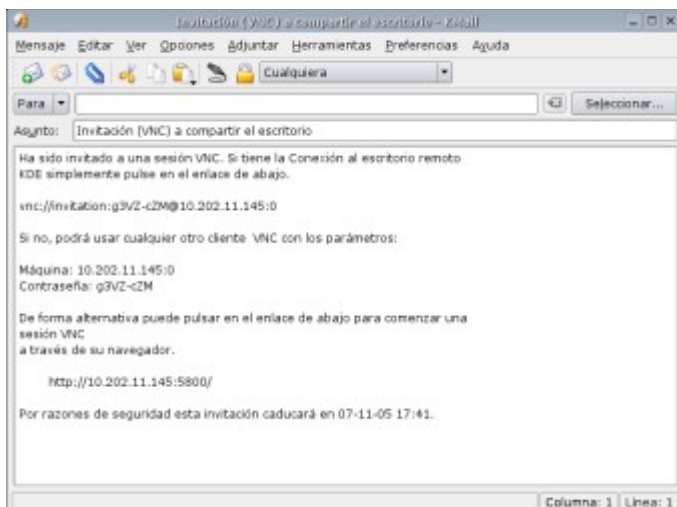
Para realizar una petición de asistencia, ejecutamos la herramienta “*krfb*”. Ante nosotros aparecerá un sencillo panel para gestionar peticiones.



(Figura 26)

Si hacemos click en “Crear una invitación temporal” obtendremos los datos que el usuario remoto debe usar para compartir nuestro escritorio. También podemos optar por enviar la petición por correo electrónico directamente a nuestro destinatario. En ese caso, el correo que recibirá el

destinatario será similar al de la siguiente figura:



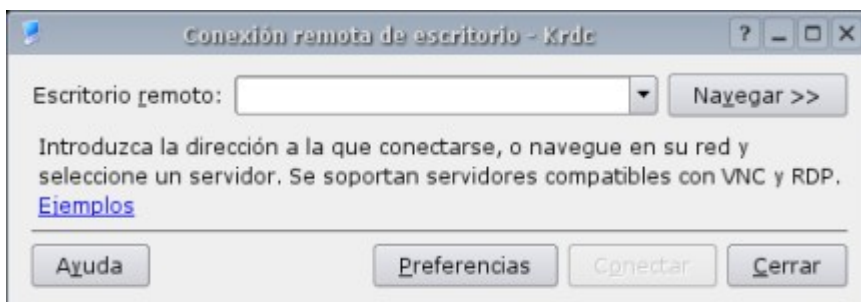
(Figura 27)

Atender una petición

Existen varias formas de atender a una petición remota, aunque todas ellas tienen como fin último establecer un túnel *VPN* entre las máquinas implicadas. Si disponemos de los datos, podemos ejecutar *krdc* e introducirlos, o bien arrancar *Konqueror* e ingresar una dirección con la siguiente sintaxis:

```
vnc://[usuario]:[password]@[Máquina]
```

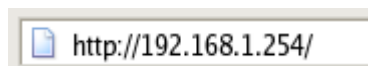
La siguiente figura muestra el panel de conexión de *krdc*.



(Figura 28)

7. Configuración del Router

Tanto en *Windows* como en *Linux*, la configuración del router se realiza de la misma forma. Tomando el router recién reseteado, éste activa el modo *DHCP*; en nuestras configuraciones de red debemos activar la obtención de dirección *IP* y *D.N.S.* Automáticas. Para acceder al router usamos cualquier explorador; en su barra de direcciones introducimos la dirección ip de éste: 192.168.1.254



(Figura 29)

El router nos pedirá un nombre de usuario y una clave. Por defecto estos campos hay que dejarlos vacíos, en caso de que no acepte los campos vacíos, habrá que resetear el router para devolverlo a su configuración de fábrica.

Dentro de la configuración tenemos las siguientes opciones:



(Figura 30)

En la primera de ellas se gestiona el acceso a internet, eligiendo la forma para conectarse a esta. Las diversas opciones son:

Obtener la configuración automática con “*CATV dinamic mode*”.

Usar una configuración estática, introduciendo a mano la configuración de internet.

PPTP (DSL dinamic mode)

PpoE (DSL dinamic mode)

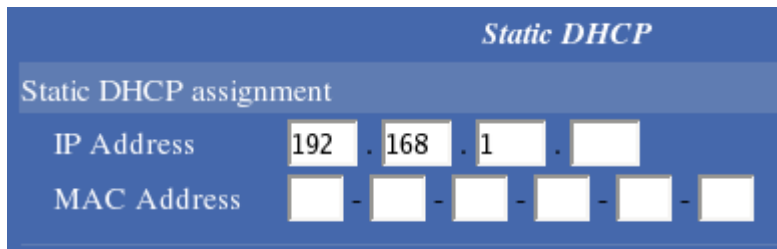
En la segunda opción (local port) configuramos la gestión del router sobre la red local. Configurando su *IP* local, la máscara a usar y activando o desactivando el servidor *DHCP* para que asigne direcciones *IP* automáticamente o use una configuración estática.

Dejando activa la distribución de *IPs*, el router proporciona *IPs* entre el rango indicado a los equipos que se conecten con la obtención de *DHCP* activa. Ejecutando el botón “*Config...*”

Local Port	
Private Network	
IP Address	192 . 168 . 1 . 254
Subnet Mask	255 . 255 . 255 . 0
DHCP Server	
<input type="radio"/>	Do not distribute IP address to local computers
<input checked="" type="radio"/>	Distribute IP address to local computers
Start IP address	192 . 168 . 1 . 1
Number of IP address	128 (1~253)
Static DHCP IP & MAC addr.	Config...
WINS Server	0 . 0 . 0 . 0

(Figura 31)

podemos indicar al router que asigne *IPs* fijas a las máquinas que le indiquemos.



Static DHCP						
Static DHCP assignment						
IP Address	192	.	168	.	1	.
MAC Address		-		-		-

(Figura 32)

Las diversas opciones de “*Advanced Setup*” nos permiten configurar aspectos avanzados de la configuración del router, como el cambio del *user* y su *password* del router, cambiar la asignación de los puertos, crear un servidor virtual de ftp, redirigir los puertos del router a los distintos equipos, etc.

“*Network Status*” nos permite monitorizar parámetros de configuración del router, actividad del router, lista de usuarios, etc...

Y por último “*Others*”, nos permite resetear el router, guardar la configuración actual y actualizar su firmware.

8. Herramientas de diagnóstico

Para comprobar el estado de las interfaces de red de un sistema computador se dispone de un conjunto de comandos sencillos más o menos comunes entre sistemas operativos.

Ping: [*Windows/Linux*] Nos informa del estado de un host. Es necesario permitir la respuesta a peticiones *ICMP* de eco para que funcione.

Tracert: [*Linux*] Indica la ruta por la que pasa nuestra petición hasta llegar al host destino.

Traceroute: [*Linux*] Idem que el anterior.

PathPing: [*Windows*] Mezcla entre el comando *Ping* y *Tracert*. Es necesario permitir la respuesta a peticiones *ICMP* de eco y de control de tiempo excedido saliente para que funcione.

Ipconfig: [*Windows*] Proporciona información sobre *TCP/IP*, adaptadores, etc
Opciones:

- **Ipconfig:** muestra información general sobre la red
- **Ipconfig /all:** ofrece información detallada sobre todas las t. de red y conexiones activas.
- **Ipconfig /renew:** renueva petición a un servidor *DHCP*.
- **Ipconfig /release:** libera la Ip asignada por *DHCP*.
- **Ipconfig /registerdns:** registra todos los nombres *DNS*.
- **Ipconfig /flushdns:** borrar todas las entradas *DNS*.

Netstat: [*Windows/Linux*] Muestra todas las conexiones activas en el equipo.

Opciones:

- **Netstat -a:** nos muestra todas las conexiones y puertos.
- **Netstat -e:** muestras las estadísticas Ethernet
- **Netstat -n** muestra direcciones y puertos en forma de numero.
- **Netstat -o:** muestra que programa esta asociado a la conexión activa
- **Netstat -p** (protocolo): permite especificar que protocolo se desea ver. *TCP/UDP*
- **Netstat -s:** muestra estadísticas clasificas por protocolo.

Ifconfig: [*Linux*] Sin parámetros, muestra las interfaces de red configuradas y activas, así como los parámetros de la conexión. También permite configurar interfaces, tal y como se mostró en capítulos anteriores. Se remite al lector a leer las páginas '*man*'

Route: [*Windows/Linux*] Permite visualizar la tabla de rutas. También permite añadir o eliminar entradas de dicha tabla.

9. Gestión de servicios en Fedora Linux

Todos los sistemas *Unix* arrancan usando el programa *init*, que se convierte en el proceso número 1 y se encarga de ejecutar el resto de programas que hacen que el sistema funcione.

En primer lugar se ejecutan los scripts que se encuentran bajo */etc/rcS.d*, que son las tareas básicas para arrancar el sistema. Luego se ejecutan otra serie de *scripts* correspondientes a un *runlevel*. Los *runlevels* son el mecanismo que permite al ordenador trabajar con diferentes configuraciones de arranque. La idea consiste esencialmente en el hecho de que diferentes sistemas se pueden usar de diferentes formas. Algunos servicios no se pueden utilizar hasta que el sistema se encuentre en un estado particular, o modo, como puede ser preparado para más de un usuario, o con la red disponible.

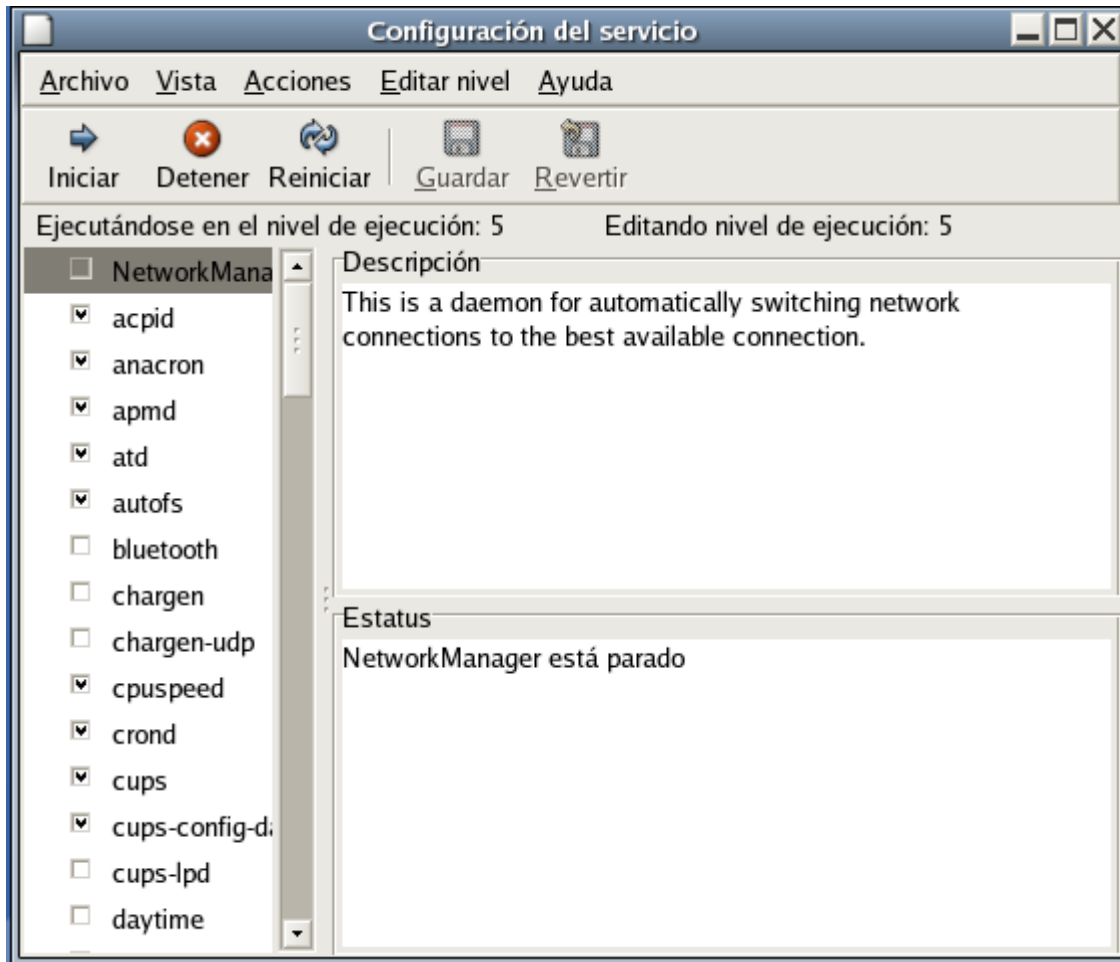
Fedora usa 7 niveles de ejecución:

- 0 .- **Halt**. Este nivel detiene el sistema
- 1 .- **Single**. User Modo de administración. El sistema crea un *shell* con los privilegios del superusuario sin solicitar nombre de usuario o contraseña.
- 2 .- **Multiuser**. .Modo de funcionamiento normal sin algunos servicios de red.
- 3 .- **Multiuser + network**. Como el modo 2 pero con todos los servicios de red activos, NFS por ejemplo.
- 4 .- Generalmente no utilizado
- 5 .- **Modo gráfico multiusuario completo**. Con una pantalla de inicio de sesión basada en X
- 6 .- **Reboot**. Se reinicia el sistema.

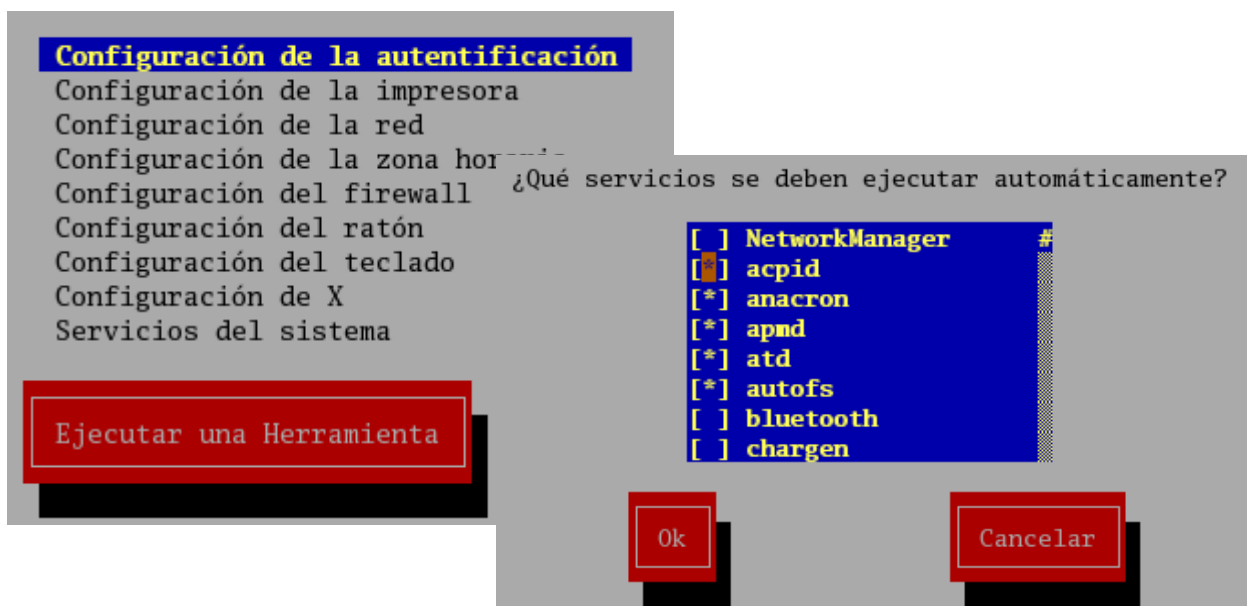
Cada nivel de ejecución ejecuta los scripts situados en *“/etc/RC(nivel de ejecución).d”* éstos son enlaces simbólicos que apuntan a los scripts ubicados en *“/etc/init.d/”*. Nótese que la primera letra del nombre del enlace simbólico indica si el script es para iniciar servicios, si empiezan por “s” ó por “k” para matarlos. Los números que acompañan a las iniciales determinan el orden de ejecución, así los scripts con un número menor se ejecutarán antes que los de un número superior.

Los scripts que se ejecutan en cada nivel los podemos controlar con un gestor de servicios, un programa que se encarga de mover los enlaces dinámicos de las distintas carpetas. En esta memoria hemos utilizado 2 programas suministrados por *Fedora*. Uno de ellos con interfaz gráfica, y otro sin ella, el primero se ejecuta con *“system-config-services”* y el segundo con *“setup”*.

El primero muestra un entorno donde podemos seleccionar para cada nivel los servicios a ejecutar. El nivel a configurar lo seleccionamos en *“Editar nivel”*, a continuación se nos listará en la columna de la izquierda los servicios que podemos activar o desactivar.



El segundo programa, “*setup*” no hace uso del entorno gráfico, es un programa de configuración de *Fedora* con múltiples opciones a configurar, entre ellas esta la configuración de los servicios. A diferencia del programa anterior, éste muestra todos los servicios juntos, no los separa por niveles de ejecución.



10. Referencias

Artículos online

- Artículos sobre *Routing*, *Nat*, *NFS* y *Router* en la edición inglesa de Wikipedia. URL: <http://en.wikipedia.org>
- “Aprende a hacer redes domésticas” URL: http://www.principiantes.info/menu/menu_lan.php
- “Resolución de Nombres de Máquina”. URL: <http://www.mug.org.ar/Infraestructura/ArticInfraestructura/215.aspx>
- “Enable IP forwarding” URL: http://www.microsoft.com/windows2000/en/advanced/help/sag_TCPIP_pro_EnableForwarding.htm

Bibliografía electrónica

- Osamu Aoki, “*Guía de referencia Debian*”
- Mauro Strione, “*Manual oficial de referencia de Red Hat Linux*”, Red Hat Inc. 2002
- Kirch, Olaf; Terry Dawson. “*Guía de Administración de Redes con Linux*”, O'Reilly (*printed version*) (c) 2000 O'Reilly & Associates