OpenSuse

Sumario

Sobre OpenSuse

No ano 2004 a compañía Novell anunciou a compra de SuSE, unha distribución Linux desenvolvida por unha empresa alemana. Un ano despois, seguindo os pasos de RedHat Inc. con Fedora, anunciou a súa liberación que pasou a chamarse openSUSE. Antes da aparición de openSUSE, o desenvolvemento desta distribución, anteriormente coñecida como SUSE Linux, realizábase a porta pechada. Agora, o proceso está aberto a calquera programador e usuario que desexe contribuír ao desenvolvemento de openSUSE.

Novell continúa o desenvolvemento a porta pechada de dúas distribucións dedicadas ao ámbito empresarial, SUSE Linux Enterprise Desktop e SUSE Linux Enterprise Server.

OpenSuse é unha das distribucións máis coñecidas de Linux. Entre as súas principais virtudes atópase a facilidade de instalación e administración, xa que conta con varios asistentes gráficos para completar diversas tarefas, e en especial pola ferramenta de instalación e configuración YasT.

Configuración da rede paso a paso

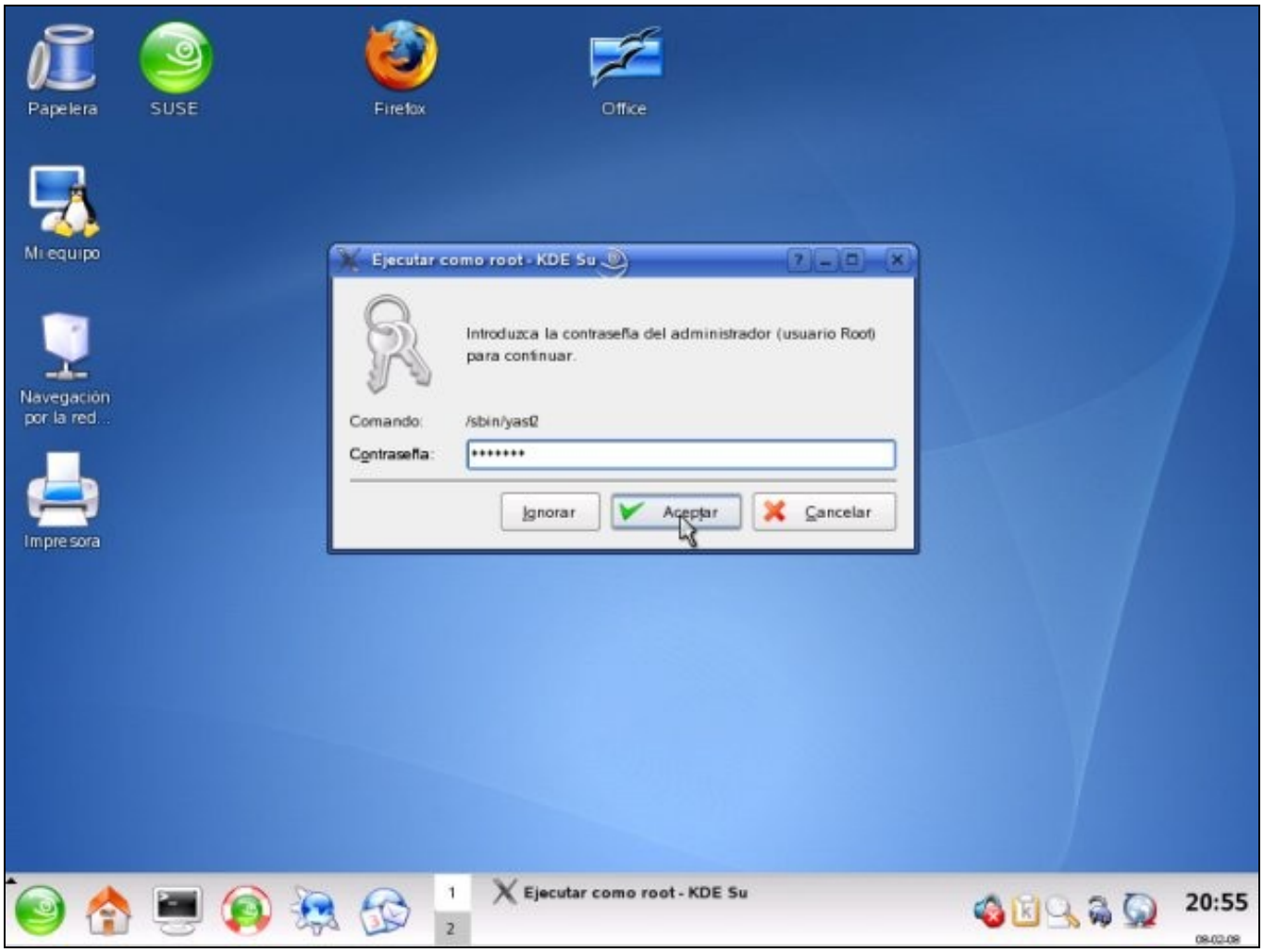
A configuración da rede pode facerse usando o programa YaST (*Yet Another Setup Tool*), aínda que existen outras ferramentas, gráficas e en modo consola (podes consultar máis información sobre este tema). Independentemente da ferramenta que se use para configurar unha rede necesitamos coñecer os seguintes datos:

- **Dirección IP da nosa máquina**. Identifica o noso computador en Internet. Podes consultar máis información sobre direccionamento IP e máscaras.
- **Máscara de rede**. Identifica o noso computador na subrede correspondente.
- **Dirección IP do encamiñador**. Permite a saída a Internet do noso computador.
- **Dirección IP do servidor de nomes (DNS)**. Resolve nomes de equipos a direccións IP.

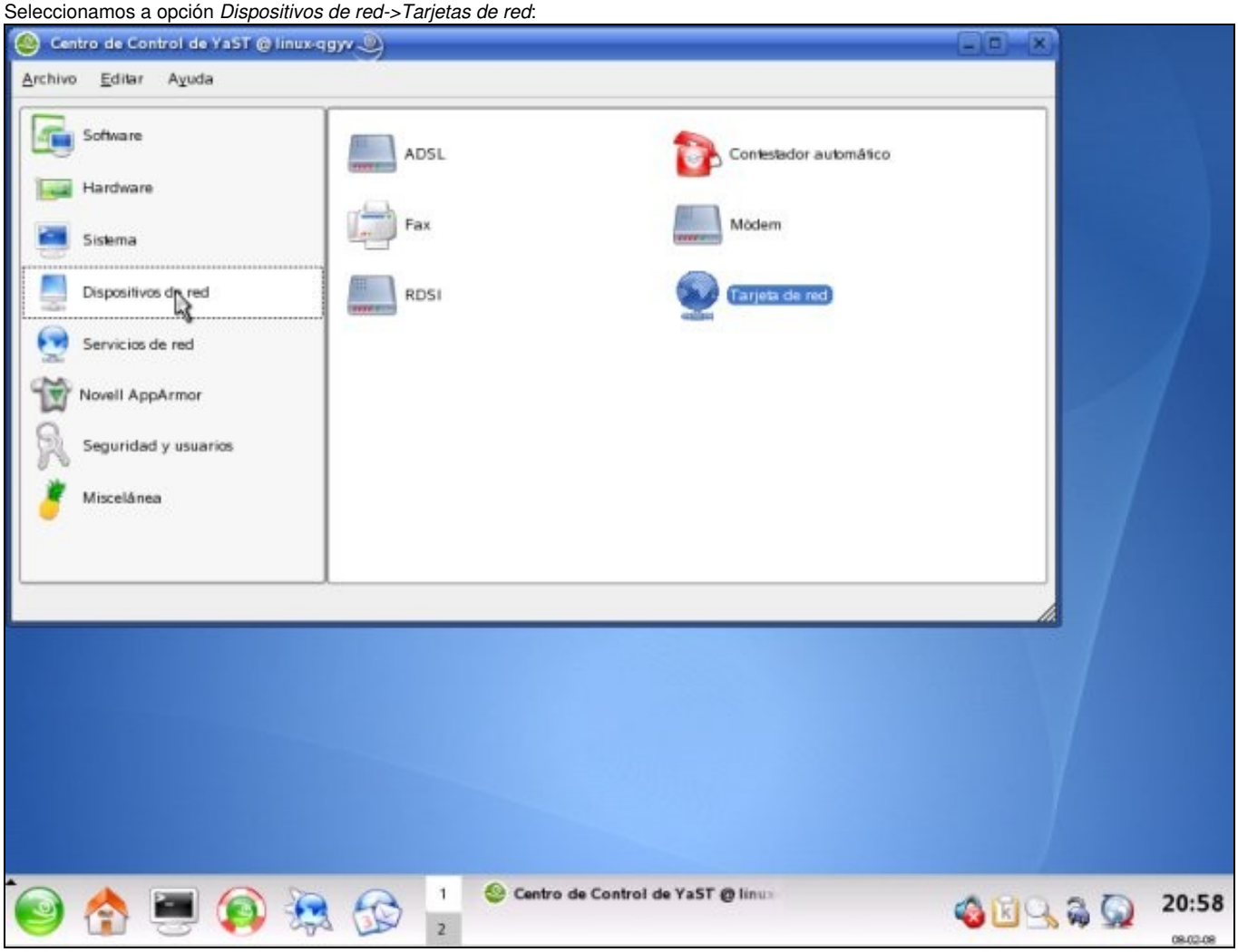
Seguiremos os seguintes pasos para configurar a rede:

1. Executamos a ferramenta YaST:

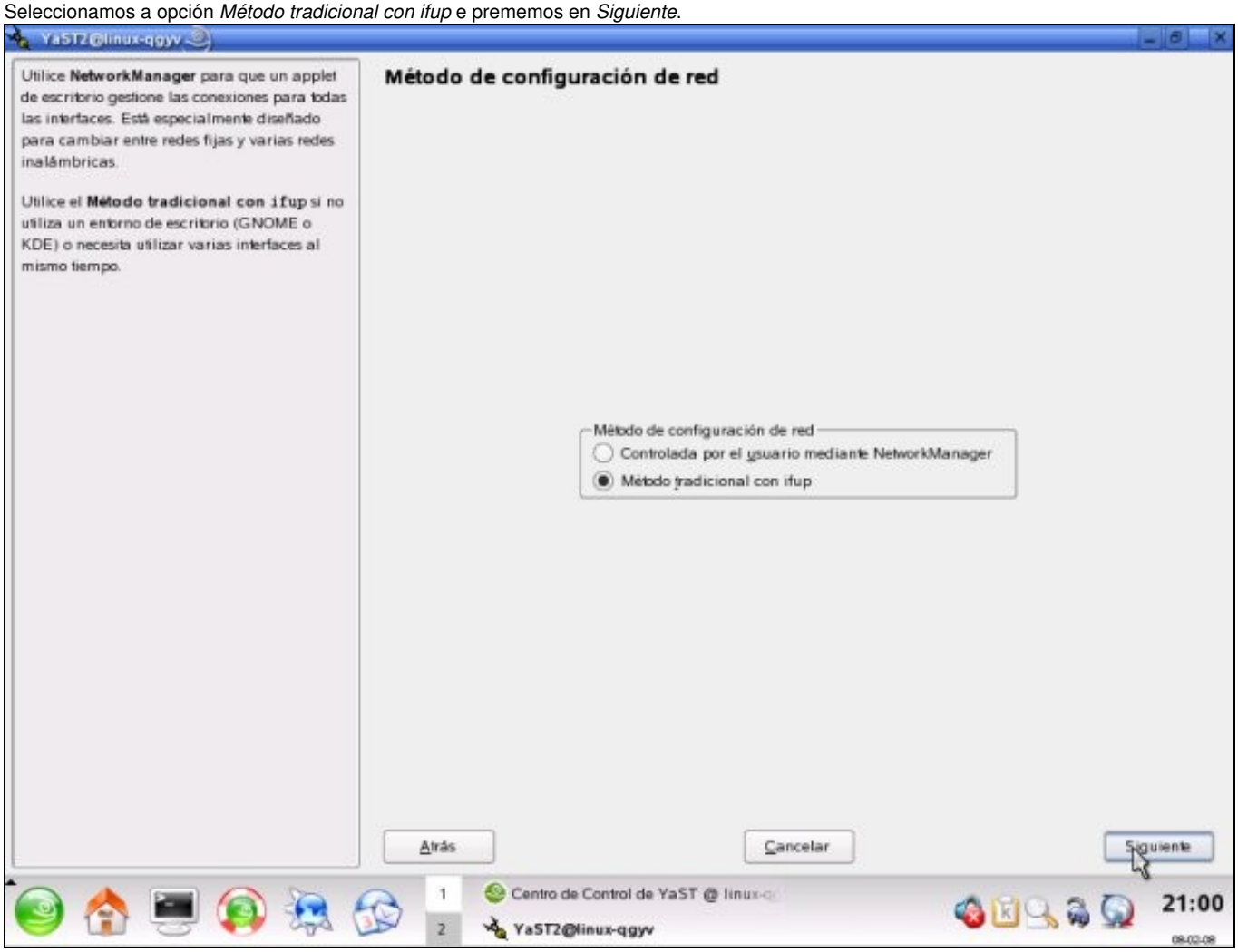
2. Introducimos o contrasinal de administrador:



3. Seleccionamos a opción *Dispositivos de red->Tarjetas de red*:

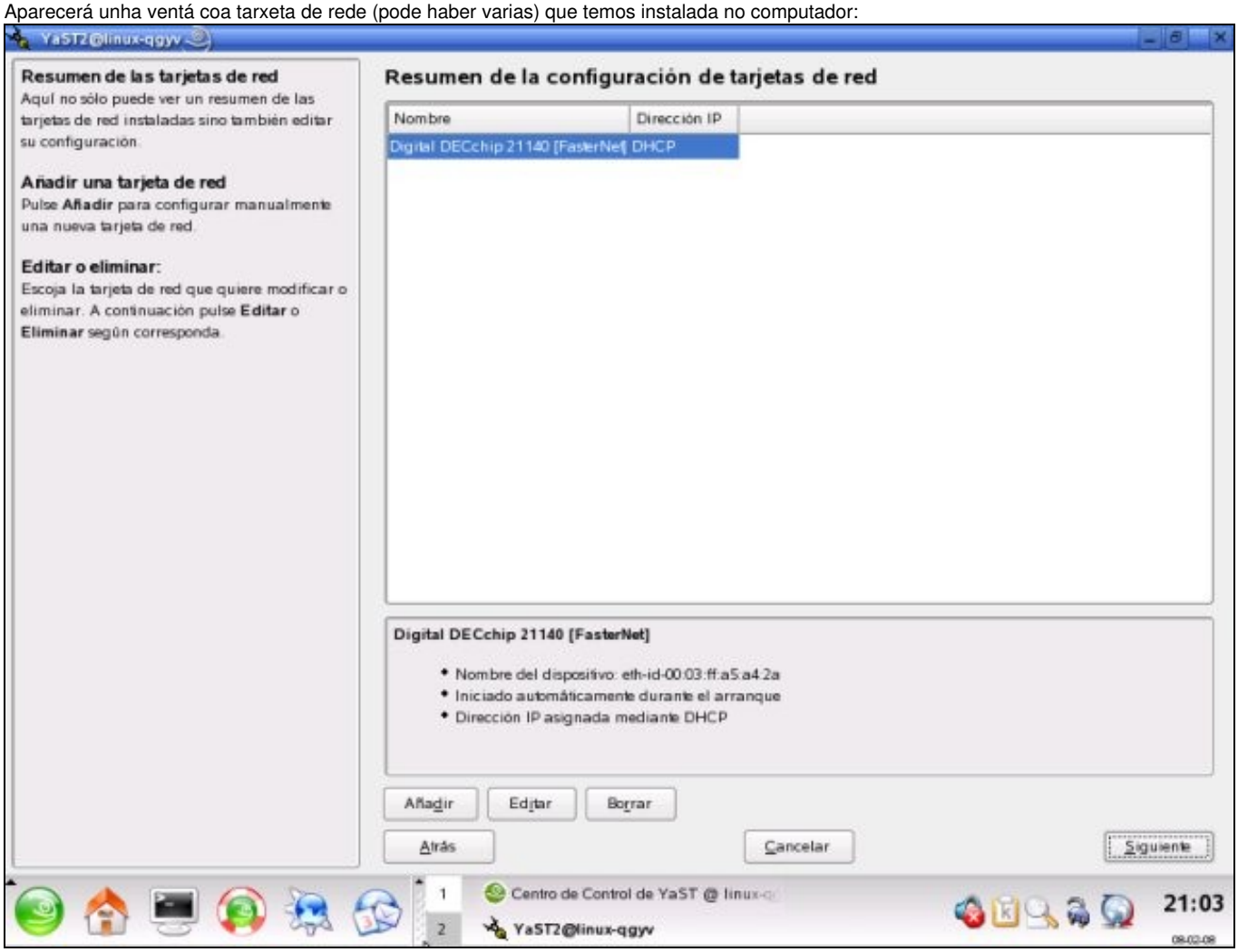


4. Seleccionamos a opción *Método tradicional con ifup* e prememos en *Siguiente*.

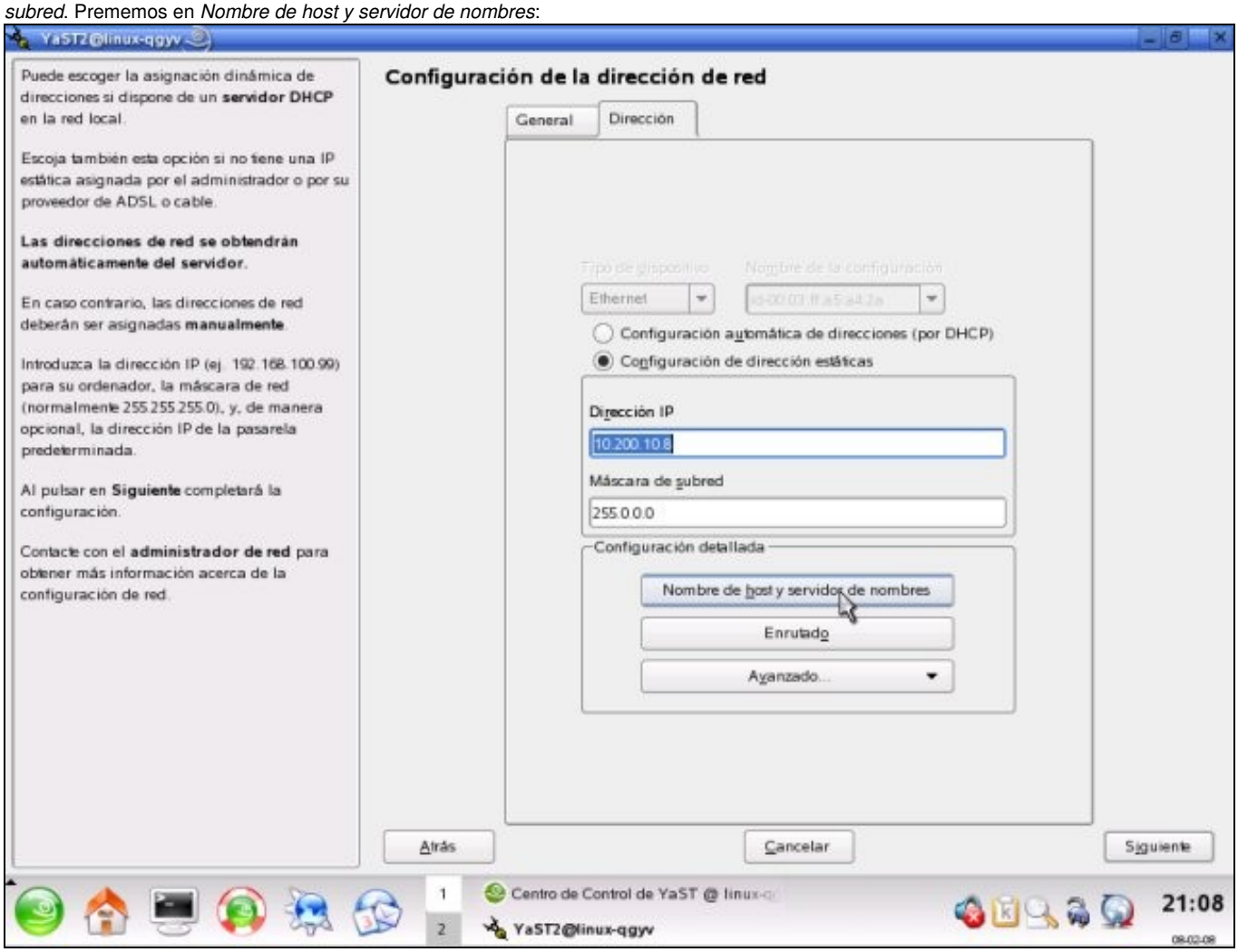


Se tivéramos instalado e configurado un servidor DHCP poderíamos escoller esta opción de configuración, que é moito máis sinxela, xa que é automática.

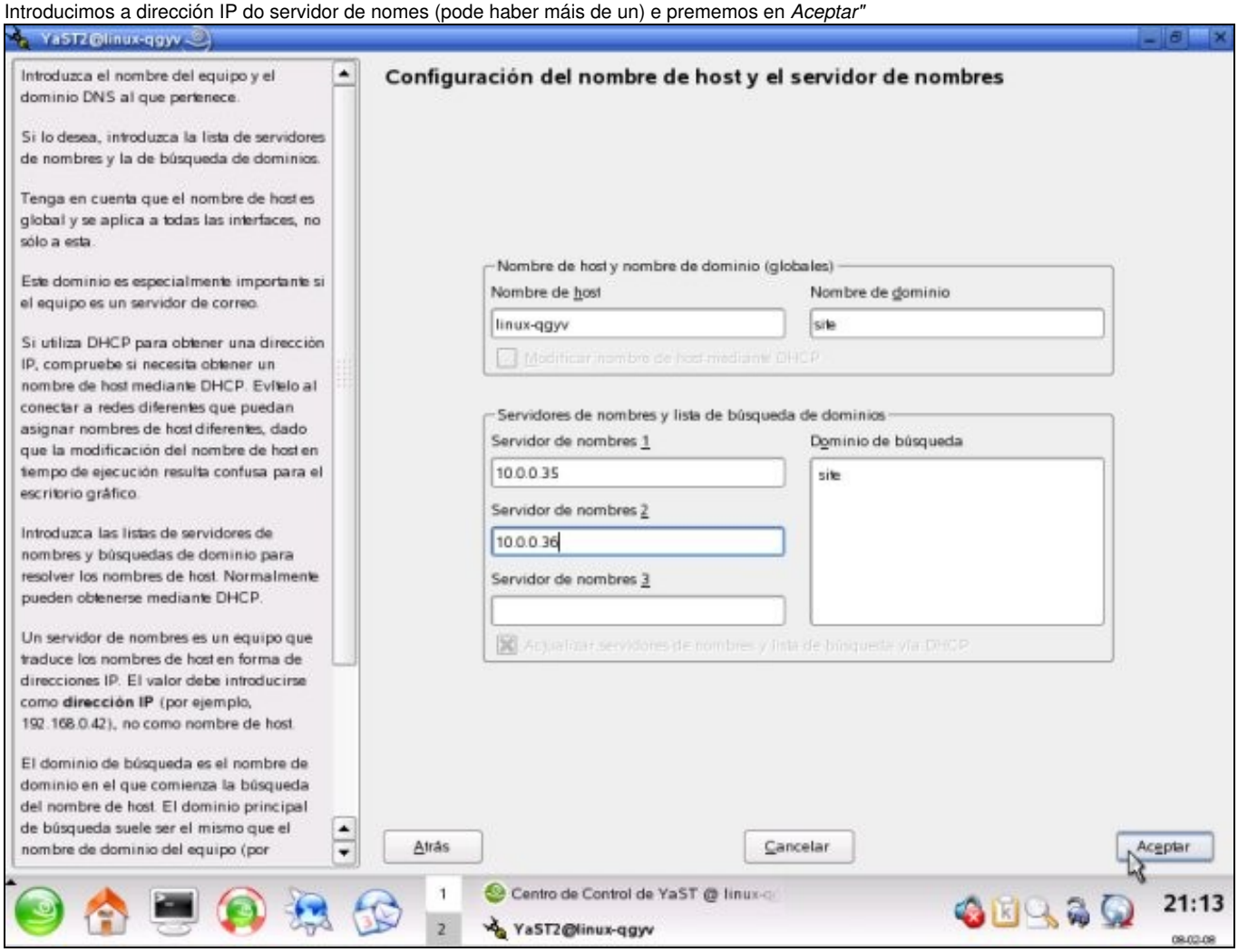
5. Aparecerá unha ventá coa tarxeta de rede (pode haber varias) que temos instalada no computador:



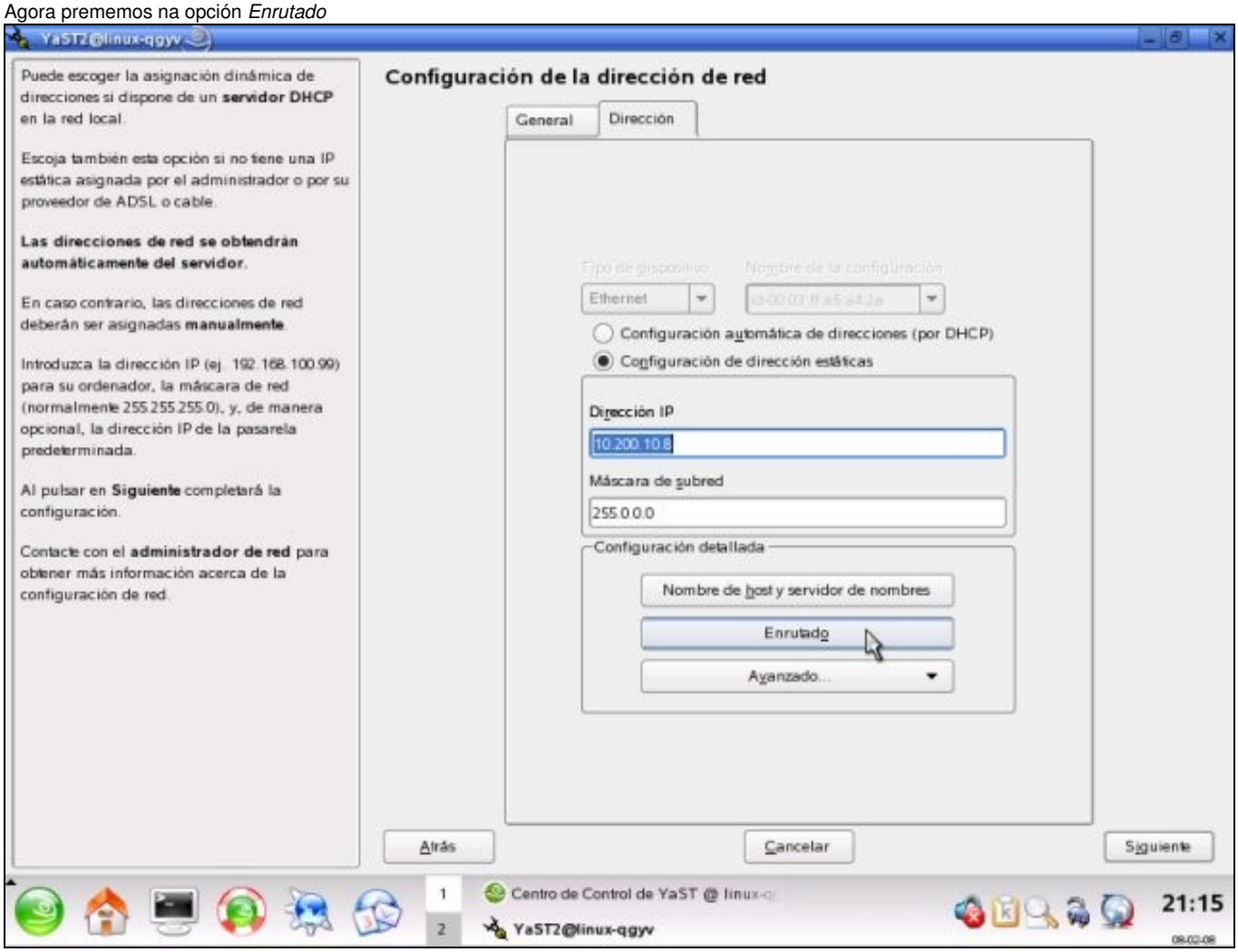
6. Prememos no botón *Editar* e seleccionamos a opción *Configuración de dirección estáticas*. Introducimos a *Dirección IP* e a *Máscara de subred*. Prememos en *Nombre de host y servidor de nombres*:



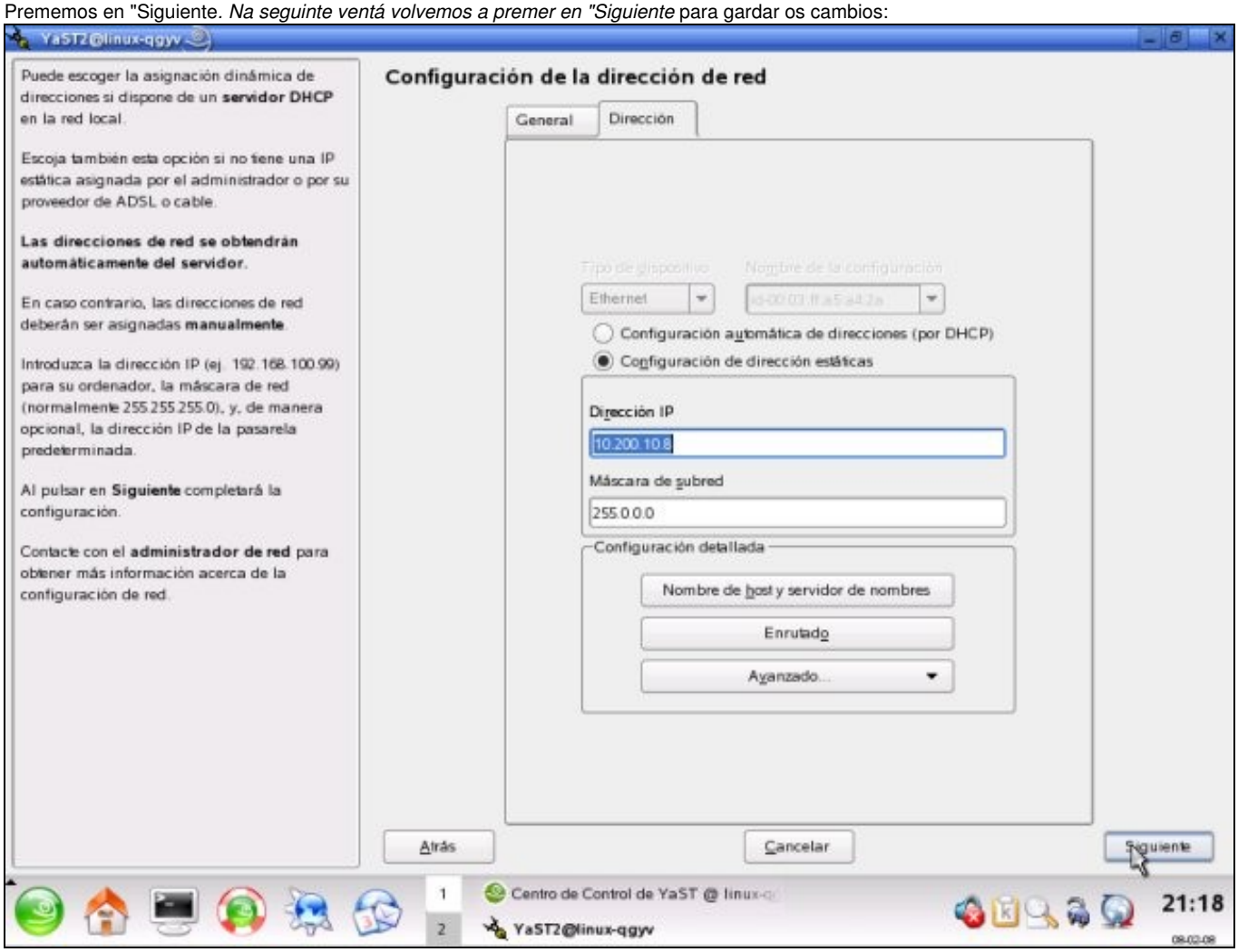
7. Introducimos a dirección IP do servidor de nomes (pode haber máis de un) e prememos en *Aceptar"*



8. Agora prememos na opción *Enrutado*

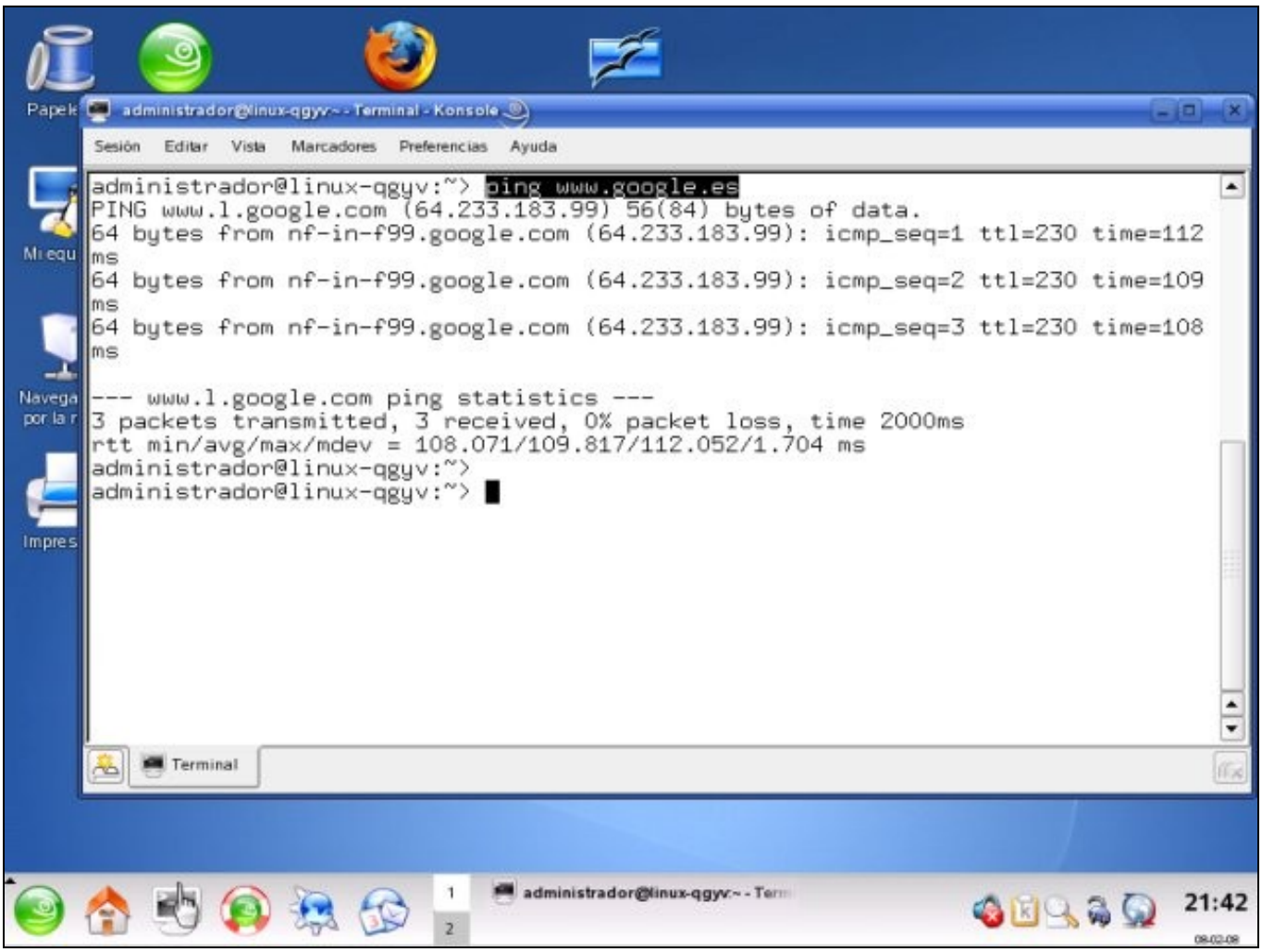


9. Introducimos a pasarela predeterminada que nos habilitará a saída a Internet e prememos en *Aceptar*
10. Prememos en "Siguiente. *Na seguinte ventá volvemos a premer en "Siguiente* para gardar os cambios:



Neste punto a rede debería estar configurada. Para comprobalo podes abrir unha consola e teclear:

```
ping www.google.es
```



Activación e configuración do firewall

Un *firewall* (cortalumes ou devasa en galego) é un programa que se usa para limitar o acceso entre computadores, normalmente en distintas redes, en función dunhas políticas de seguridade. A súa principal función é protexer a rede ou un equipo de posibles ataques externos. OpenSuse proporcina un *firewall* configurable mediante a ferramenta YaST. Para lanzalo prememos en *Seguridad->Firewall*.

Arrinque

Nesta opción determínase como se iniciará o *firewall*. Pódese arrincar automaticamente cando se inicie o sistema (recomendado) ou facelo manualmente.

Tamén se pode ver o estado actual do *firewall*, é dicir, se se está executando ou non; podemos paralo, modificar as políticas de seguridade, gardalas e rearrincalo para que teñan efecto.

Interfaces

Esta sección amosa as tarxetas de rede que hai no computador. Aquí pódese asignar as tarxetas a determinadas zonas, representando cada zona un nivel de seguridade distinto. Existen tres zonas, interna, desmilitarizada ou DMZ, e externa.

Servizos permitidos

Nesta sección especifícanse que servizos estarán dispoñibles para os computadores que estean fóra do firewall. Por exemplo, se o noso computador fai as funcións de servidor DHCP é necesario engadir este servizo á lista de permitidos ou os clientes non serán quen de obter a súa dirección IP automaticamente, xa que non poderán acceder ao servizo. Non convén ter nesta lista servizos que non se estean a usar, xa que son potenciais puntos de ataques externos.

Para engadir un servizo que non estea na lista hai que premer en *Avanzado* e introducir os parámetros correspondentes (porto TCP, UDP, etc.).

Enmascaramento IP ou NAT (*Network Address Translation*)

Para poder usar esta opción é necesario ter dúas tarxetas de rede, unha interna e outra externa. A tarxeta externa cunha dirección IP é quen recibe os datos e rediríxeos á interna, que ten outra dirección IP. O servizo de NAT ten varios usos como proporcionar maior nivel de seguridade a un computador ou proporcionar acceso a varios computadores cunha única dirección IP pública. NAT permite resolver os problemas de limitacións de direccións IP do protocolo IPV4.

Broadcast

Un broadcast é unha transmisión de datos que se envía a todos os computadores dunha rede. En si mesmos non son inseguros pero poden ralentizar o funcionamento da rede. Dende esta sección pódese configurar se este tipo de tráfico se acepta ou non para cada unha das zonas. Por defecto, está permitido na zona interna e na desmilitarizada pero non se aceptan envíos broadcast de computadores externos a esas dúas zonas.

Soporte para IPsec

Internet Protocol Security, ou IPsec, é un estándar de seguridade. Úsase moito nas VPN (*Virtual Private Networks*). Se queremos ter este servizo activo hai que habilitalo.

Rexistro de eventos

O firewall pode rexistrar nun ficheiro a súa actividade, tanto para as peticións que se aceptan como para as que non. Desde esta sección pódese configurar este comportamento, rexistrando todas as peticions, rexistrando só as consideradas críticas ou non rexistrando ningunha.

Gardar os cambios

Se prememos en *Siguiente* veremos un resumo das opcións que acabamos de configurar, servizos abertos, opcións de arrinque, etc. Se estamos de acordo prememos en Aceptar para gardar os cambios. Recoméndase reiniciar o firewall para que os cambios teñan efecto.

Xestión de actualizacións

A actualización e descarga de software realízase mediante repositorios. Un repositorio contén os programas que OpenSuse pode instalar. Os **repositorios oficiais**, é dicir, mantidos por OpenSuse, pódense atopar na seguinte ligazón: Repositorios oficiais. Á hora de engadir un repositorio hai que escoller o que se corresponda coa versión da distribución que esteamos a manexar. Para engadir un repositorio hai que arrincar YaST e seleccionar *Software-->Cambiar fuente de instalación*.

Prememos en *Añadir* e cubrimos os datos do repositorio que queiramos engadir.

Podes atopar unha listaxe completa de **repositorios adicionais** (non oficiais) para YaST na seguinte ligazón: Additional YaST Package Repositories

Compartir recursos

A compartición de recursos como cartafoles permite aumentar a produtividade, ademais de facilitar tarefas de administración, xa que o acceso a eses determinados cartafoles pódese organizar baixo unha serie de permisos personalizables para o equipo directivo, os departamentos, o profesorado, etc.

Algunhas das funcións para as que se poden usar cartafoles compartidos son:

- Intercambio de información entre profesorado e alumnado
- Entrega de traballos
- Colaboración na redacción de documentos, etc.

Samba é unha ferramenta que permite que computadores con Linux, Mac OS X ou Unix en xeral se vexan como servidores ou actúen como clientes en redes Windows. É dicir, permite compartir recursos, como ficheiros e impresoras, entre máquinas Windows e Linux.

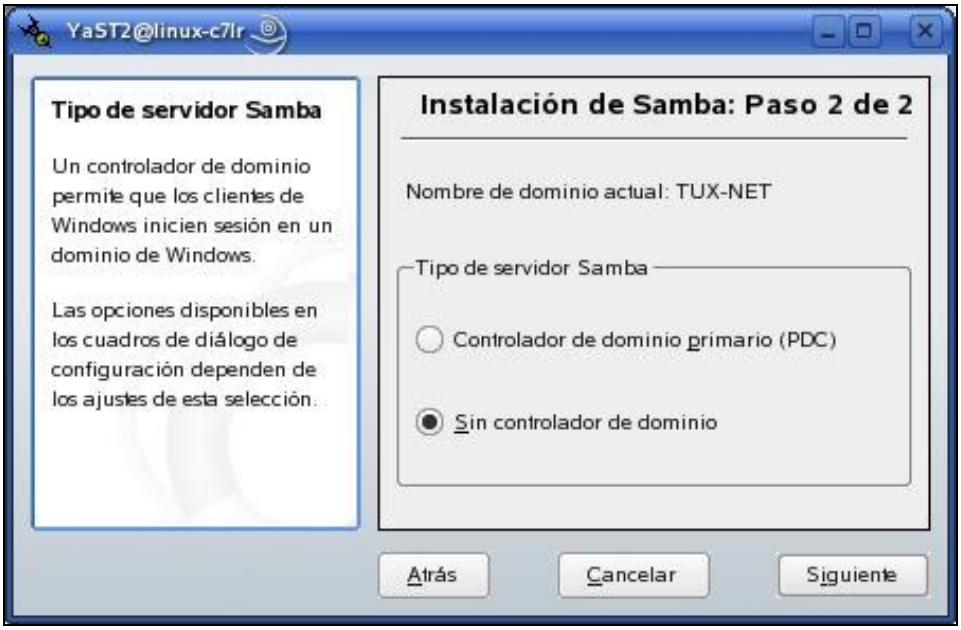
Samba é unha implementación libre para sistemas Linux do protocolo de ficheiros compartidos de Microsoft Windows, chamado SMB (*Server Message Block*), renomeado recentemente a CIFS.

Samba foi desenvolvido utilizando un *sniffer*, ou capturador de tráfico, para entender o protocolo a través de enxeñería inversa. O nome vén de inserir dous vogais ao protocolo estándar que Microsoft usa para as súas redes, o SMB.

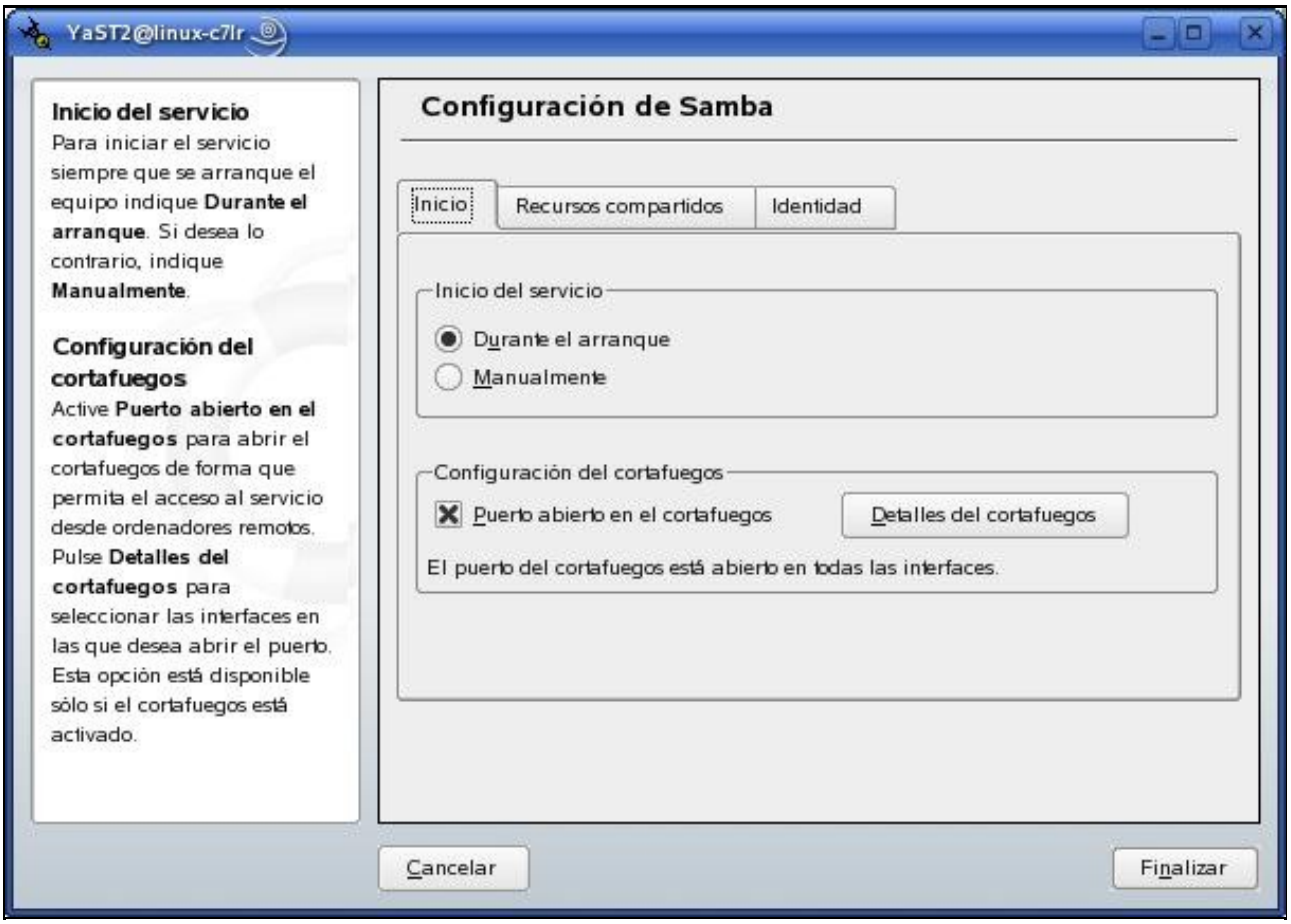
Instalación dun servidor Samba

A instalación dun servidor Samba en OpenSuse permite o acceso a cartafoles compartidos dende máquinas Windows e Linux. Para realizar a instalación arrancamos YaST e prememos en *Servicios de red-->Servidor Samba*. O primeiro que temos que escoller é o nome do grupo de traballo ou dominio dos usuarios que se van usar Samba:

A seguinte opción permite escoller se o servidor Samba vai ser un controlador de dominio (permite que os clientes de Windows inicien sesión nun dominio de Windows) ou non. Para este escenario escollemos a opción máis simple que é *Sin controlador de dominio*.



O terceiro paso abre unha ventá de configuración de Samba. Aquí temos que escoller se o servizo arrancará automaticamente (recomendado) ou non, así como habilitar os portos do firewall para que se poda acceder ao servizo:



Tamén podemos escoller que recursos se van compartir (pódense compartir cartafoles e impresoras) e incluso engadir algún novo:

Acceso ao servidor dende Windows

Unha vez instalado o servidor Samba e compartidos os cartafoles correspondentes podemos acceder a eles a través dun programa cliente. Samba permite o acceso encriptado, mediante SSH, ou sen encriptar. A opción de encriptado, loxicamente, é moito máis interesante. En calquera caso, podemos usar o programa Winscp para acceder aos cartafoles. Dependendo de como se teñan configurados os permisos poderase escribir ou só ler no cartafol.

Acceso dende Linux

O acceso desde unha máquina con OpenSuse é sinxelo. Abonda con abrir o Konkeror e teclear na barra de direccións o nome do computador que ten o servidor Samba (tamén serve coa dirección IP):

```
smb://nomeServidor/
```

O prefixo smb indícalle ao Konkeror que o protocolo que se usará é Samba.

Konkeror xa dá soporte para SSH, polo que poderemos acceder ao servidor Samba de xeito encriptado.

Servidor Web

O servidor web, ou servidor HTTP, é unha ferramenta de gran utilidade no centro, xa sexa para facer prácticas cos alumnos, publicar información interna ou implantar unha **intranet** que favoreza a comunicación e a posta en común de recursos. O software de servizo web máis usado é o Apache. O seu nome débese a que os seus creadores elixiron ese nome porque querían que tivese a connotación de algo que é firme e enérxico pero non agresivo, e a tribo Apache foi a última en renderse ao que se convertería en goberno de EEUU.

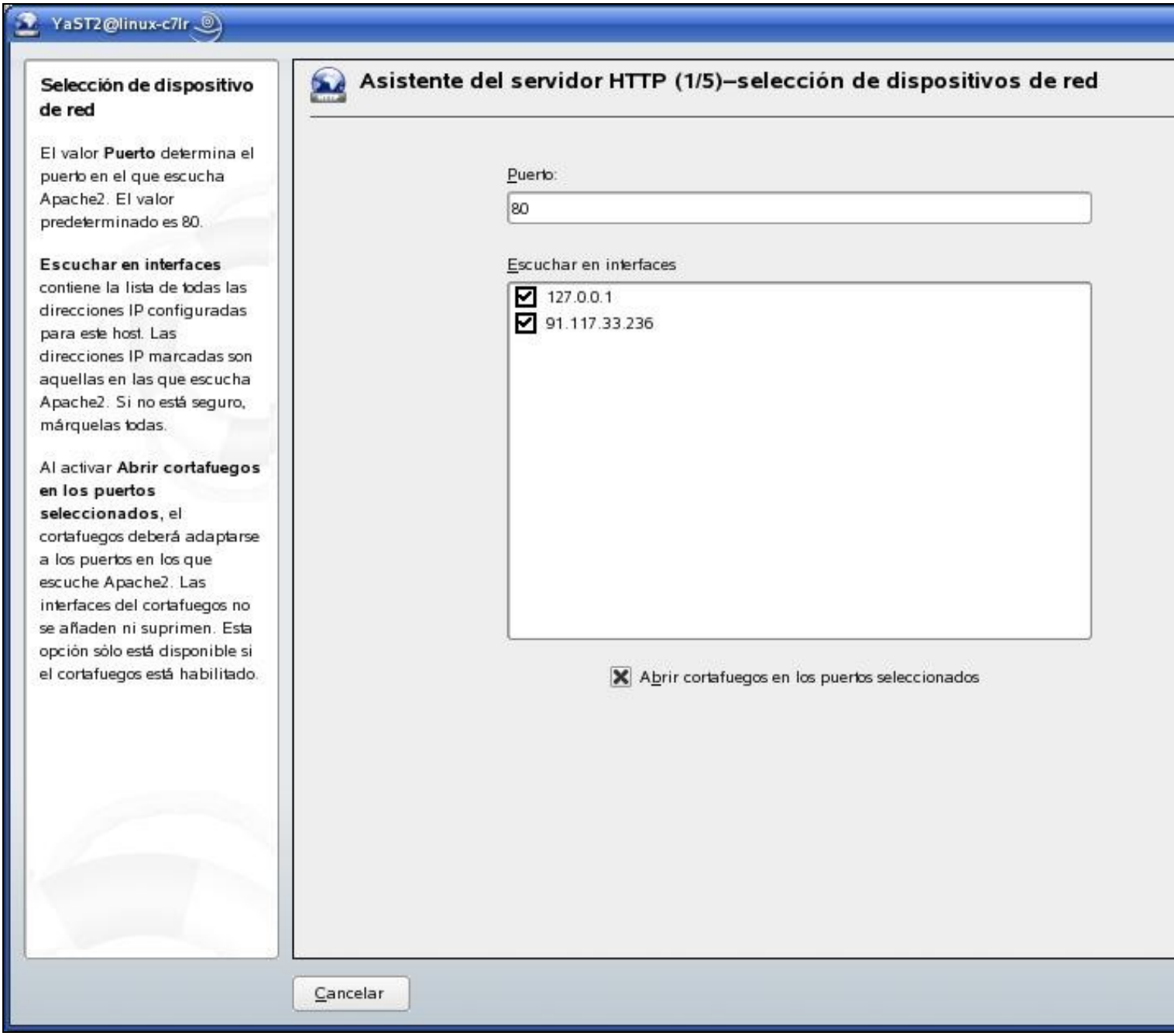
Instalación do servizo

Apache conta cun gran número de módulos que incrementan a súa funcionalidade como soporte para distintos tipos de autentificación, soporte de linguaxes de programación, comunicación segura, etc. Para instalar o servizo hai que executar YaST e premer en *Servicios de red-->Servidor HTTP*. Previamente hai que ter configurados os respositorios, tal e como se indicou na sección anterior. É tamén recomendable ter a man o CD/DVD de OpenSuse:

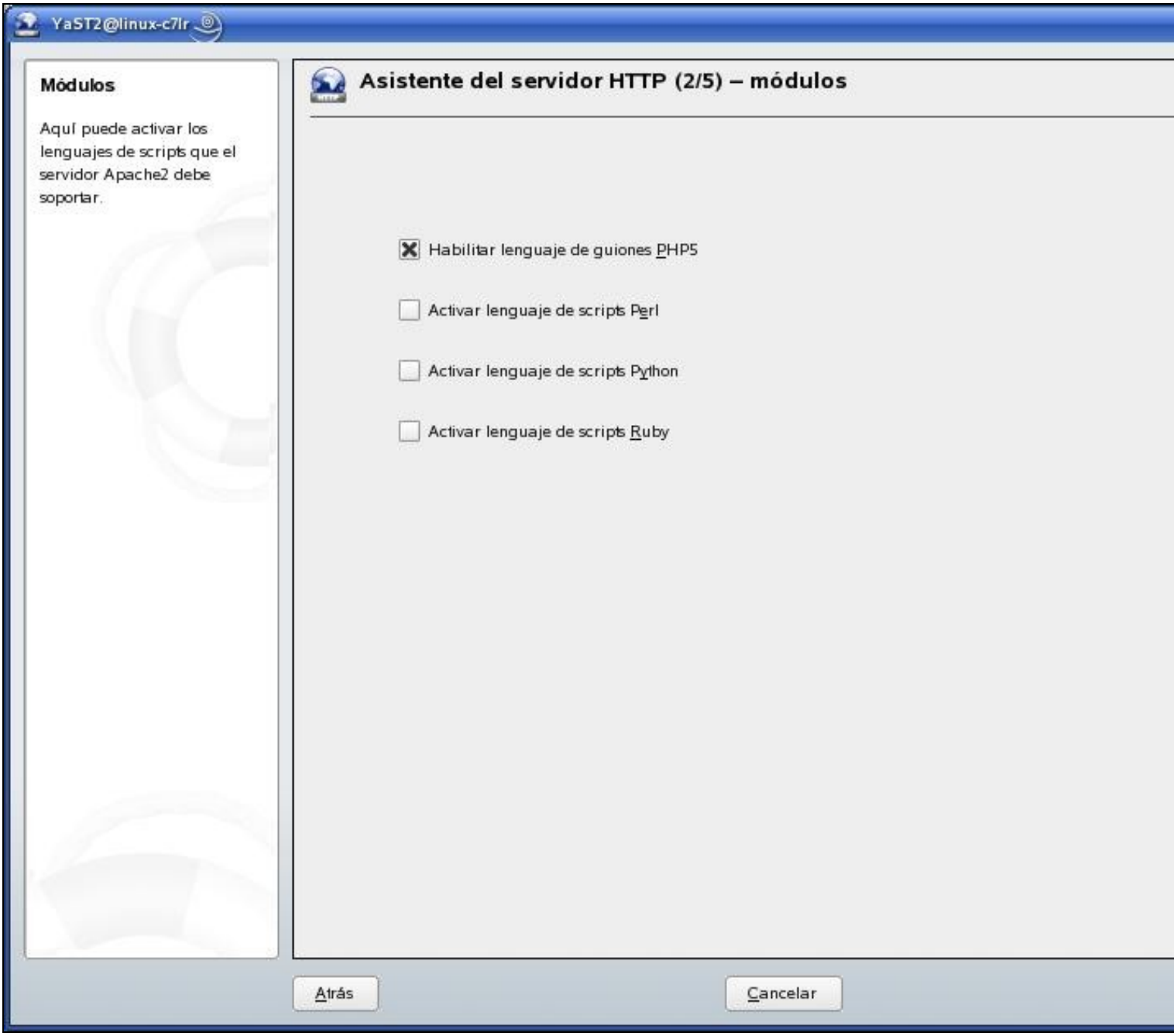
O sistema pídenos confirmación para instalar os paquetes necesarios:

Se non temos configurados todos os repositorios necesarios é necesario introducir tamén o CD/DVD de OpenSuse:

O sistema descargará e instalará a ferramenta. Posteriormente, lánzase un asistente de configuración. No **primeiro paso** do asistente hai que aceptar a configuración por defecto das tarxetas de rede que tamén habilita o firewall para poder conectarnos ao servizo:



No **paso 2** temos que indicar se queremos dar soporte ás diferentes linguaxes de programación coas que se constrúen páxinas web, como PHP, Python, etc. Dependedo das linguaxes seleccionadas pode ser preciso instalar módulos a maiores.



Nos **pasos 3 e 4** configúrase o computador por defecto e os servidores virtuais. É suficiente con aceptar os valores por defecto.

No **último paso** selecciónase a opción de arrinque manual ou atomático (recomendado). Tamén se pode facer unha configuración do servizo en modo experto:

Para comprobar que o servizo funciona correctamente podemos abrir un navegador no URL http://localhost

Configuración mediante Webmin

Para configurar o Apache, e outros servios, pódese usar a ferramenta Webmin que funciona en contorno gráfico cun navegador Web, facilitanto moito o traballo de administración. Webmin permite administrar sistemas UNIX /GNU-Linux, facendo uso de calquera navegador, posibilitando:

- Xestionar usuarios e grupos
- Servizos Apache, DNS e FTP
- Bases de datos: mysql, postgres
- Compartir ficheiros, editalos
- Configuración dos interfaces de rede
- Instalar/desinstalar paquetes, etc.

Ao ser o acceso mediante navegador web podemos administrar o sistema dende calquera parte do mundo. Asemade, ten o mesmo formato sexa cal sexa a distribución, o que permite homoxenizar a forma de traballo independentemente da distribución. O servidor de webmin está configurado para traballar con SSL no porto 10000. Polo tanto, unha vez instalada a ferramenta podemos acceder a ela tecleando:

```
https://<equipo>:10000
```

Na seguinte ligazón Configuración Apache con Webmin pódese consultar instrucións sobre a configuración dos parámetros máis importantes do Apache con Webmin.

Se queremos configurar o servizo web seguro (https) con Openssl é suficiente instalar o módulo de apche para ssl. Deste xeito xa temos automaticamente un servidor virtual que atende peticións seguras por https no porto 443. Na seguinte ligazón pódese atopar máis información: Webmin.

Publicación de páxinas no servidor

O cartafol por defecto para almacenar as páxinas en OpenSuse é `/svr/www/htdocs`, aínda que isto se pode configurar en función das nosas necesidades. Xa que logo, para publicar páxinas no servidor simplemente teremos que copialas a este cartafol. Por defecto só o usuario root ten permiso para poder escribir documentos nesta carpeta.

Instalación e configuración de FTP

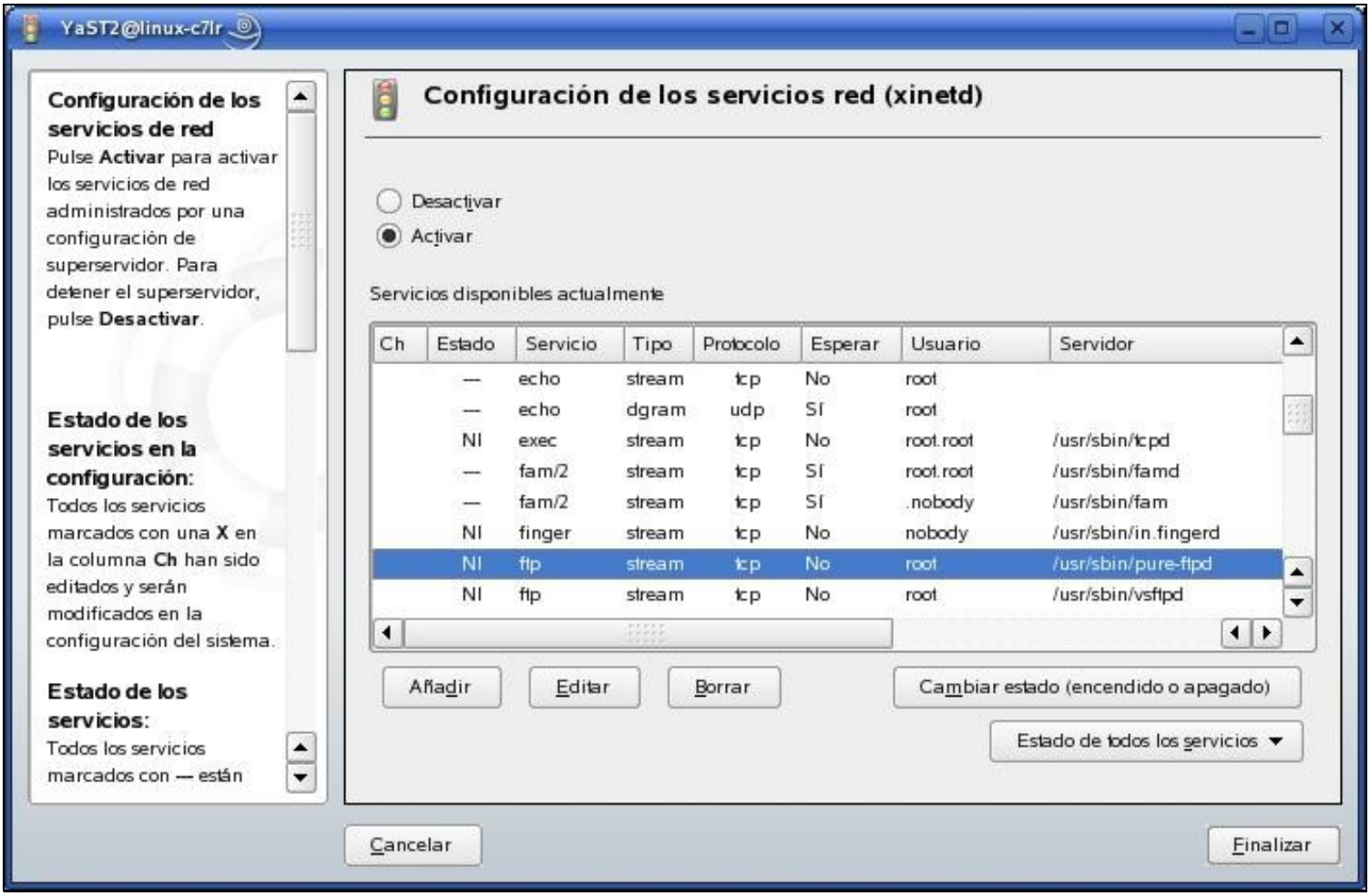
FTP (*File Transfer Protocol*) é unha ferramenta para a transferencia de ficheiros entre computadores. Está baseado na arquitectura cliente-servidor, de maneira que desde un equipo cliente podémonos conectar a un servidor para descargar ficheiros desde el ou para enviarlle os nosos propios ficheiros, independentemente do sistema operativo utilizado en cada equipo. Tamén é o protocolo que permite que funcione a ferramenta.

O acceso a un servizo FTP pode realizarse mediante usuario e contrasinal ou de xeito anónimo (**FTP anónimo**). Normalmente, nun FTP anónimo non se pode escribir pero si ler.

A instalación dun servidor FTP en OpenSuse é sinxela. Abonda con seguir os seguintes pasos:

Paso 1: Lanzamos YaST e prememos en *Servicios de red-->Servicios de red (xinetd)*

Paso 2: Seleccionamos *Activar*, prememos en *pure-ftpd* e volvemos premer no botón *Cambiar estado (encendido /apagado)*



Paso 3: Instalamos os paquetes necesarios:

Paso 4: Aínda que o servizo xa estea instalado hai que activalo volvendo á ventá de configuración do paso 2.

Conexión ao servidor

Para conectarnos ao servidor hai que abrir o Konkeror, que se atopa na barra de ferramentas de KDE, e teclear na barra de direccións

```
ftp://localhost/
```

En principio, o acceso que estamos facendo é anónimo polo que non se nos permitirá escribir nese cartafol.

Se o que queremos é conectarnos cun usuario concreto hai que especificalo na barra de direccións do Konkeror da seguinte forma:

```
ftp://usuario@nome.dominio.org
```

Onde *usuario* é o nome de usuario co que nos queremos conectar e *nome.dominio.org* o nome da máquina.

Aínda que o uso do FTP en determinados contextos é necesario, a tendencia é empregar acceso a ficheiros mediante un servidor de SSH, empregando clientes de tipo winscp para Windows ou Konkeror e Nautilus para os escritorios KDE e Gnome, respectivamente.

Copias de seguridade

Os dispositivos de almacenamento como os discos ríxidos, chaves USB, etc. poden fallar. Para evitar a perda de información importante é necesario facer copias de seguridade. A copia de seguirdade dos datos nun centro é un tema crucial, xa que sen unha boa política de recuperación ante desastres, a información pode perderse. É necesario ter presente que os datos se deberían copiar a diario dunha maneira íntegra, e acumular un historial de copias de seguridade que, dependendo da información de que se trate pode abarcar desde poucos meses até anos.

Dende o punto de vista do usuario, é importante destacar que as copias se poden facer no computador local ou nun servidor por rede. Neste último caso, as copias son moito máis sinxelas de realizar para o administrador do centro. As vantaxes de gardar a información na unidade de rede son evidentes, por exemplo, o cambio de computador por traslado de posto de traballo implicaría ter que levar os datos con nós; ou a perda de datos en caso de fallo do computador.

Para entender as diferentes **políticas e tipos de copias de seguridade** consulta a seguinte ligazón: Copias de seguridade.

Á hora de facer copias de seguridade podemos distinguir a copia de seguridade dos ficheiros de sistema e a copia dos datos propiamente ditos.

Sistema

En OpenSuse podemos facer copias de seguridade dos ficheiros do sistema mediante a ferramenta YaST premendo en *Sistema-->Copias de seguridad del sistema*. A ferramenta permite buscar ficheiros de sistema e salvagardalos en local ou por rede:


YaST2@linux-c7lr
Copia de seguridad
Para crear una copia de seguridad del sistema, indique la vía completa del archivo en el que desea almacenar la copia de seguridad en **Nombre de archivo**. Para guardar el archivo en un servidor NFS, seleccione **Red** como ubicación e introduzca los detalles del servidor.
El módulo de copia de seguridad crea un archivo tar con los archivos cambiados y un perfil de instalación automática para que resulte más rápido y sencillo reinstalar el sistema. Para guardar sólo los nombres de los archivos detectados y no crear un archivo, seleccione **Crear sólo lista de ficheros**
Ajustes del archivo
Nombre de archivo
Ubicación de la copia de seguridad
Archivo local
Red (NFS)
Dirección IP o nombre del servidor NFS
Seleccionar...
Directorio remoto
Seleccionar...
Tipo de archivo
Crear archivo de copia de seguridad
Tipo de archivo
tar con subarchivos tar gzip
Opciones...
Crear sólo lista de ficheros encontrados
Atrás
Cancelar
Siguiente

Datos de usuario

Hai moitas ferramentas para facer copias de seguridade dos datos, tanto en local como por rede, empregando servizos como, por exemplo, Samba. Dúas ferramentas que se poden instalar con OpenSuse son Kbackup e Konserve. A primeira empaqueta e comprime, cun sistema gráfico moi intuitivo, permitindo traballar por red (samba); a segunda, tamén é moi sinxela, permite facer copia periódica con perfís, indicando espazos de tempo, pero o proceso é máis lento que na anterior.

Onde gardar as copias

As copias de seguridade teñen tamén a finalidade de protexer a información do centro. Se se consegue chegar a onde están as copias a información estará comprometida.

Normalmente, os administradores conservan as copias cos servidores para poder recuperalas rapidamente en caso de fallo. Pero debe haber unha política de segundo nivel para protexer a información de intrusión física na zona dos servidores ou de desastre na organización que poda destruír esta zona (por exemplo, un incendio).

Sempre debería existir, aínda que non estuviera totalmente actualizada, unha **copia de seguridade fisicamente fóra do centro**.

Referencias

- **Páxina principal de OpenSuse en español**. Desde aquí pódese descargar a última versión, acceder a documentación, foros, etc.
- [http://es.opensuse.org/Documentaci%C3%B3n **Wiki de OpenSuse**].