

UD.4.- Integración de Sistemas Operativos Libres e Propietarios	18 sesións
Obxectivos asociados ao R.A.6.	
<ul style="list-style-type: none"> • Integrar na mesma rede servizos e sistemas heteroxéneos. • Coñecer e configurar accesos de recursos compartidos dende diferentes sistemas operativos. • Establecer diferentes niveis de seguridade na rede dos recursos compartidos por diferentes sistemas operativos. 	
Contidos conceptuais	
<ul style="list-style-type: none"> • Descrición de escenarios heteroxéneos. • Instalación, configuración e uso de servizos de rede para compartir recursos. • Configuración de recursos compartidos en rede. • Seguridade dos recursos compartidos en rede. • Terminais gráficos para acceso remoto. • Uso en redes heteroxéneas. 	

1. Descripción de redes heterogéneas.

En las UD's anteriores comenzamos a estudiar redes de ordenadores de carácter homogéneo, es decir, los equipos llevaban instalado el mismo SO. A continuación y de forma más práctica profundizaremos sobre redes y compartición de todo tipo de recursos con equipos que lleven instalados SO, concretamente de la familia Linux y la familia Windows, que son los de mayor implantación, sobre todo el segundo.

Como herramientas de configuración usaremos:

- en Windows sus asistentes para compartir recursos. Utilizaremos **XP** y en menor medida **7**.
- en el caso de Linux la herramienta **samba, cups y webmin**. **Debian** como servidor y **Ubuntu-Desktop** como cliente.

Para realizar las prácticas que llevaremos a cabo restableceremos el fichero de configuración original a partir de la copia que realizamos en su momento. También es factible crear el **smb.conf desde cero, de esta forma conoceremos mejor su estructura**. Daremos de baja todos los usuarios creados de forma completa (incluidos sus directorios de trabajo) y los recursos que podamos haber compartido en su momento.

- **Práctica:** tal como se indica en el párrafo anterior elimina todos aquellos objetos (usuarios y sus directorios, impresoras virtuales, ...) del equipo con el Sistema Debian instalado.

El protocolo **SMB - Session Message Block** es utilizado en las redes implementadas por los SO de Microsoft tal como vimos en la UD3. Tiene dos niveles de control de acceso **share (leve)** que fue complementado luego con el nivel **user**. Con la aparición de **NT-ntfs** apareció el concepto de propiedad de los objetos con respecto a los usuarios, que se potenció en los Primary Domain Control (PDC) que veremos en la unidad 6.

Un concepto fundamental en las redes es el **"Browsing"**, o visibilidad de equipos y servicios que **establece el intercambio de información** de lo que existe en ese momento en una red de recursos. De esta manera cuando un equipo se enciende en algún tiempo (0 a 15 minutos) todos los potenciales Clientes están enterado de presencia. La identificación de servicios en la red se representa en tres datos:

Grupo de Trabajo

que corresponde a algo similar al conceto de dominio en TCP/IP. Es un nombre textual, que es parte de la configuración de la red.

Nombre del Equipo

es un nombre textual que permite conocer un equipo y relacionándolo con una IP determinada (hablamos de redes locales)

Nombre del recurso compartido

designa el directorio o la cola de impresión... etc que esta disponible para otros objetos de la red. Todo recurso compartido debe tener la siguiente notación: **\\equipo\nombrecurso**

- **Práctica:** vamos a trabajar con Debian y con XP. Vamos a compartir una carpeta en Debian para que sea visible desde equipos con XP. Supongamos la empresa **Turiasa** cuyos empleados utilizan los dos SO. Crearemos una carpeta llamada **viajes** donde se guardarán

los folletos informativos de los viajes. Pasos a realizar:

- a. Crea la carpeta en /home/viajes
- b. Edita el fichero nuevo de smb.conf y escribe los siguientes datos en el apartado **home directories**

```
[viajes] # es el nombre con el que se verá desde Windows
path = /home/viajes
        # ruta de la carpeta que queremos compartir
        # Con eso es suficiente. Pero podemos añadir
comment = Folletos ofertas viajes 2010
        #comentario que se verá en Windows si activamos la opción Ver/Detalle
writeable = no          # para poder escribir en esa carpeta compartida
guest ok = yes          # permite accesos anónimos al recurso
guest only = yes       # accesos anónimos
browseable = yes       # el usuario no puede acceder al recurso
```

Evidentemente previamente deberemos configurar los tres siguientes parámetros (al menos el primero) en **Global Settings**, a saber: **workgroup**, **netbios** y **server string**. En Debian será necesario instalar el paquete **samba**. En **Ubuntu-Desktop** viene instalado como cliente pero no como servidor.

En nuestro caso por ejemplo:

workgroup = Turiasa

netbios name = turiasa-ubuntu1 (cambiar el número según alumno)

server string = Equipo con Folletos de Ofertas de Viajes

wins support = no

encrypt passwords = true

Por otro lado deberemos incluir al equipo de XP dentro del grupo de trabajo y como nombre de equipo **turiasa-xp1**. Daremos por echo que los equipos tienen la configuración de IP's en la misma red. Si pide contraseña pulsamos *cancelar*. También se puede corregir estableciendo en **Global Settings** la directiva **security = share**.

En el supuesto caso de que siga dando problemas daremos de alta un **samba** y cuando desde XP nos pida usuario y contraseña le indicaremos los datos introducidos.

Ahora, comparte una carpeta en modo **solo lectura e intenta acceder** a ella desde Ubuntu-Desktop.

Existe un comando **testparm** que nos permite comprobar y verificar que la configuración que hemos realizado de smb.conf están correctos. Si es así podemos **reiniciar samba**.

Hay dos conceptos importantes relacionados con TCP/IP y Samba, ambos del apartado de parámetros globales.

interfaces = lo eth0 192.168.21.2/24 10.10.1.1

Esta línea establece que segmentos de red escuchará peticiones el servidor Samba. Cualquier otra interfaz no listada aquí no será escuchada.

hosts allow = 127. 192.168.21. 192.168.

Similar al anterior.

Fichero **/etc/samba/lmhosts** similar al **/etc/hosts**, la estructura habitual es la siguiente:

127.0.0.1 localhost

192.168.21.12 servidor.empresa #debe coincidir con netbios name

Práctica.- Configura estos parámetros en el fichero **smb.conf** del ejercicio anterior.

- **Modos de seguridad Samba**

Hay dos tipos de modos de seguridad para Samba, **share-level** y **user-level**, que se conocen de forma colectiva como *niveles de seguridad*. El segundo nivel tiene cuatro formas de configuración de las que veremos dos, dejando las otras dos para la UD6 cuando veamos el Active Directory:

- seguridad a nivel de usuario con la directiva **security = user**

Es la configurada por **defecto**. El servidor solicita **usuario/contraseña** y le será mostrado todos los recursos disponibles en el servidor.

- seguridad a nivel de usuarios (plural) con la directiva **security = share**

En este caso solicita contraseña para cada recurso sin tener en cuenta el nombre de usuario. Han aparecido problemas de compatibilidad desde Windows 2000. No es recomendable. En principio debería permitir el acceso de forma anónima (guest)

Práctica.- Realiza diferentes cambios en **smb.conf** para comprobar las diferentes opciones.

- **Cuentas de equipo y cuentas de usuario. Comando smbpasswd**

Los servicios Windows usan las **Cuentas de Equipo** para identificar a los mismos en una red tratándolos incluso de la misma forma que los usuarios (incluyendo contraseñas). Incluso un usuario autorizado se le puede denegar el acceso si el mismo se realiza desde un equipo no autorizado. Las cuentas de equipo se añaden al archivo de contraseñas de samba mediante el comando siguiente:

smbpasswd -a -m NOMBRE_EQUIPO

¡Ojo! El NOMBRE_EQUIPO debe coincidir con el nombre real.

Práctica.- Añade el equipo XP al servidor Samba. A continuación con Webmin lee la configuración realizada hasta ahora de **smb.conf**.

Hablamos del archivo de contraseñas Samba, Localízalo. Si es necesario busca en Internet.

Las **Cuentas de Usuario** permiten el acceso a los recursos compartidos en red tal como vimos en el apartado anterior. Su creación tal como la vimos en apartados anteriores sería mediante línea de comando

smbpasswd -a NOMBRE_USUARIO

Para acceder desde línea de comandos a recursos deberemos tener instalada la utilidad **smbclient** que permite el acceso a archivos remotos de forma similar a FTP. Supongamos que queremos acceder a un equipo XP con una carpeta compartida llamada **cruceros** al directorio /home/viajes desde un equipo llamado **XPepito**. La forma de hacerlo es mediante la orden modo texto:

smbclient //Xpepito/cruceros -U NOMBRE_USUARIO

Nos aparecerá un intérprete de comandos donde introducir órdenes para manipular y transferir archivos. Si lo hacemos así:

smbclient -U NOMBRE_USUARIO -L NOMBREMAQUINA

Se nos mostrará los datos que la máquina comparte.

Una forma más cómoda si los accesos son repetitivos es “montar” los recursos en red como si fuesen locales. Por ejemplo, la carpeta anterior la podemos tener “anclada” en el servidor linux con la orden siguiente:

mount -t smbfs -o username=NOME_USUARIO //XPepito/cruceros /mnt/cruceroslin

Evidentemente deberemos tener creado el directorio en linux **cruceroslin**

Si deseamos desmontar el recurso

umount /mnt/crucerolin

Para finalizar mencionar a los grupos. Para introducirlos en el fichero **smb.conf** solo hay que anteponer el símbolo **@** delante del nombre del grupo, p.e., **@ventas** en diferentes directivas: **valid users, write list, admin users...**

Una vez establecidos los grupos y/o usuarios se aplicarán las directivas de acceso que se aplicarán a aquellos y que es algo similar a las GPO que veremos en el Directorio Activo.

Práctica.- Realiza diferentes cambios en **smb.conf** con los conceptos anteriores y comprueba los resultados.

- **Impresoras en redes heterogéneas.**

La herramienta en Linux para compartir impresoras es **cups**. Consideraremos que está instalado. Para realizar las prácticas instalaremos una impresora **PDF**. Para ellos instalaremos el paquete **cups-pdf**. Para que esta impresora sea vista por todos los usuarios habrá que modificar los permisos. En una terminal en Ubuntu o Debian escribimos:

```
# chmod u+s /usr/lib/cups/backen/cups-pdf (se ejecuta con permisos de propietario, suid)
```

A continuación añadimos la impresora pdf según el sistema que estemos utilizando. Por ejemplo, si es **ubuntu-desktop**, en modo gráfico

Sistemas => Administración => Impresoras

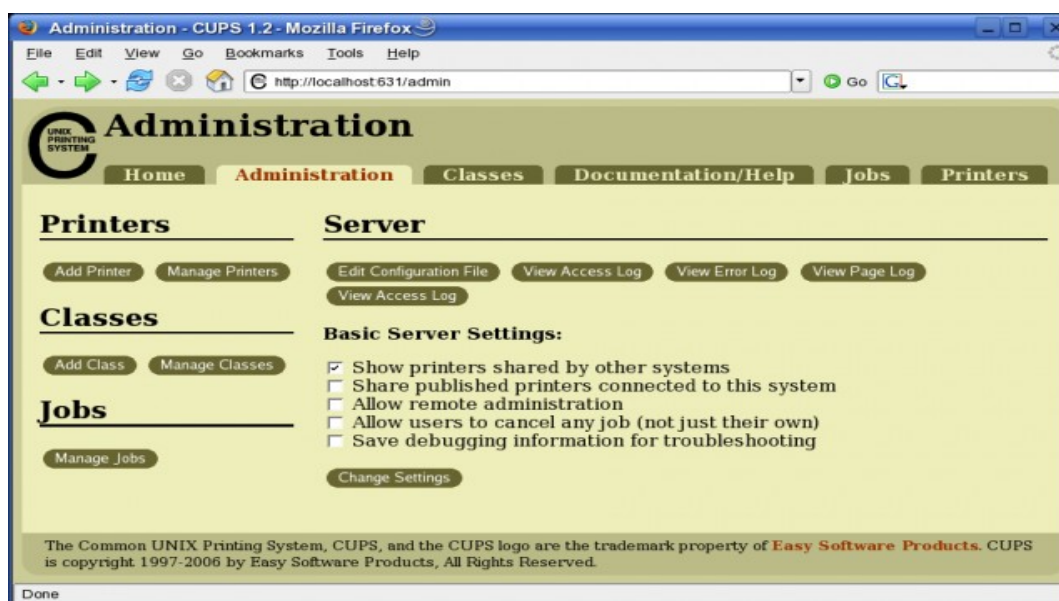
hacemos clic sobre *Impresora Nueva* y seleccionamos *PDF Printer*, luego *Generic* y como modelo *postscript color printer rev3b* (o algún término similar). Los archivos se guardan por defecto **\$home/pdf** por lo que se debe crear esa carpeta en cada usuario.

En el caso de Debian, tal como vimos en la UD anterior, se accede a **http://localhost:631** Sea como fuere los pasos siguientes para compartir la impresora comienzan con ejecutar en un **terminal** los siguientes comandos (con sudo delante en Ubuntu-Desktop):

```
# adduser cupsys shadow
```

```
# sudo /etc/init.d/cupsys restart
```

Así entramos en **http://localhost:631** sin problemas. Ahí podremos elegir la impresora a compartir en red marcando todas las casillas.



Nos vamos al ordenador en Windows y le damos a añadir impresora, seleccionamos **Impresora en Red**, aquí tenemos dos formas, **buscar impresora**, más cómodo o en el cuadro de dirección escribir

`http://ipdebianubuntu:631/printers/nombreimpresora`

Práctica: analiza los cambios producidos en **smb.conf**

[printers]

comment = Todas las impresoras

security = server

path = /var/spool/lpd/lp

browseable = no

printable = yes

public = yes

writable = no

create mode = 0700

Escribe aquí la configuración en smb.conf de la impresora PDF compartida.

Práctica.- instala una impresora PDF en XP e intenta acceder a ella desde Ubuntu-Desktop. Desde Debian tienes que tener instalado **smb-client**.

- **Compartir la Unidad de CDROM**

Hasta ahora hemos compartido los dos recursos por excelencia. Por un lado **impresoras** y por otro **ficheros y directorios**. Pero todo recurso, software o hardware, susceptible de ser necesario en una red puede ser compartido. Un ejemplo lo veremos con la unidad de CD-ROM.

Supongamos que deseamos compartir la Unidad de DVD de Ubuntu-Desktop. La configuración de **smb.conf** sería aproximadamente esta:

[cdrom]

comment = Cd Rom Compartido

path = /media/cdrom0

public = yes

writable = no

browseable = yes

En primero lugar observemos **path o ruta** debemos asegurar que es esa. Por otro lado el término **browseable** para poder acceder desde Windows o Linux de forma remota.

En el caso de **Debian**, tal como lo tenemos configurado, la opción es algo más complicada. La configuración **smb.conf** es similar a la anterior. Generalmente deberemos, aunque no siempre depende de la configuración, dos pasos:

1. Añadir la entrada en **/etc/fstab**. Este fichero indica que sistema de ficheros o dispositivos debe montar el Debian. Deberemos de investigar un poco escribiendo en la línea de comandos `ls /dev` para localizar el dispositivo y a continuación añadirlo, si no está, en el fichero `fstab`

```
/dev/dvd    /media/cdrom0    udf, iso9660 user,noauto    0 0
```

Si no existe el directorio **/media/cdrom0** habrá que crearlo.

2. A continuación montar la unidad a modo (con algún dvd o cd dentro)

```
#mount /dev/dvd    /media/cdrom
```

Antiguamente solían montarse en el directorio **mnt**, ahora suele ser en **media**.

Práctica.- Comparte la Unidad CD e intenta acceder a ella desde Linux tanto Debian como Ubuntu-Desktop.

- **Acceso a los recursos compartidos**

Desde Windows

Colocamos en la barra de direcciones de alguna ventana:

```
\\192.168.3.1\publico
```

Desde Linux

Debemos instalar **el paquete samba-client**. Luego, abrimos una carpeta y colocamos en la barra de direcciones:

```
smb://192.168.3.1/publico/
```

o

```
smbclient //192.168.3.1/publico/
```

donde 192.168.3.1 es la "IP privada" del host Linux con la carpeta `/home/public`

Ejemplo completo de un fichero de configuración de Samba

```

[global]                // Sección global, parámetros generales

security = user           // Seguridad por usuarios
workgroup = Aula5        // Grupo de trabajo 'Aula5'
encrypt passwords = yes  // Las contraseñas se deberán enviar encriptadas
wins support = yes       // Samba será servidor wins
log level = 1
max log size = 1000
read only = no           // Por defecto, lectura y escritura
load printers = yes      // Se comparten también las impresoras

[homes]                // Sección homes, carpetas home de usuarios

comment = Carpetas home // Comentario
browsable = no           // No explorables
create mask = 0700       // Máscara de creación de archivos (rxw-----)
directory mask = 0700    // Máscara de creación de carpetas

[printers]            // Sección printers, impresoras

path = /var/tmp
printable = yes
min print space = 2000

[profesores]          // Carpeta común profesores
path = /home/samba/profesores // Ruta de la carpeta compartida
browsable = yes          // Explorable
read only = no           // Lectura y escritura
create mask = 0770       // Máscara de creación de archivos (rxwrxw---)
directory mask = 0770    // Máscara de creación de carpetas

[alumnos]            // Carpeta común alumnos

browsable = yes
read only = no
path = /home/samba/profesores/alumnos

[programas]          // Carpeta común del centro (solo lectura)

browsable = yes
read only = yes
guest ok = yes           // Se admiten invitados
path = /home/samba/programas

[laserjet5]          // Parámetros impresora

path = /tmp
printable = yes          // Se permite imprimir

```

ANEXO: Parámetros de configuración

Globales

- *check password script*: permite definir un script que verificará la complejidad de la contraseña definida, retornando 0 si es aprobada por el programa indicado
- *debug uid*: permite registrar los uid, gid, euid y egid del usuario que solicita un recurso en el log del servidor
- *domain master*: habilita a nmbd con un nombre NetBios específico que lo identifica como maestro de dominio del grupo de trabajo indicado
- *guest account*: usuario utilizado para acceder a los recursos que tienen definido "guest ok"
- *include*: incluye otro archivo de configuración complementario
- *debuglevel* o *log level*: permite definir el nivel de detalle del log; incluso por módulo: all ,tdb ,printdrivers ,lanman ,smb ,rpc_parse ,rpc_srv ,rpc_cli ,passdb ,sam ,auth ,winbind ,vfs ,idmap ,quota ,acls ,locking ,msdfs ,dmapi ,registry
- *map to guest*: le indica al servidor la acción a tomar cuando falla el inicio de sesión de un usuario. inútil en security = share o server
- *max log size*: tamaño máximo del log
- *message command*: le indica al servidor la acción al recibir un mensaje tipo WinPopup
- *netbios name*: nombre netbios del servidor samba
- *null passwords*: permite el acceso a usuarios con contraseñas vacías
- *panic action*: comando a realizar al caerse smbd o nmbd
- *prefered master* o *preferred master*: indica samba como maestro principal en el grupo de trabajo
- *security*: determina cómo los clientes responden el logeo (usuario y contraseña) según el "security mode bit" enviado en las negociaciones de protocolo.
 - *share*: clientes se registran al solicitar un recurso (permite ver la lista de recursos)
 - *user*: clientes se registran al solicitar la lista de recursos o solicitar un recurso
 - *domain*: idéntico al anterior, pero los datos de registro se consultan con controlador de dominio
 - *server*: idéntico al anterior, pero los datos de registro se consultan con servidor SMB
- *server string*: texto desplegado como nombre completo del servidor

usershares

Parámetros de configuración aplicables a las carpetas compartidas a través de nautilus ("Opciones de compartición"):

- *usershare allow guests*: las carpetas compartidas son accedidas por usuarios sin registrarse
- *usershare max shares*: número máximo de carpetas compartidas por usuario
- *usershare owner only*: permite compartir sólo las carpetas pertenecientes al usuario
- *usershare path*: ruta donde se almacenan las carpetas compartidas por cada usuario (los permisos de la carpeta indicada controlan quienes pueden compartir a través de este medio)
- *usershare prefix allow list*: lista separada por comas de las rutas absolutas permitidas para compartir (incluye directorios dentro de estas rutas)
- *usershare prefix deny list*: lista separada por comas de las rutas absolutas no permitidas para compartir (incluye directorios dentro de estas rutas)

Recursos

- *administrative share*: recurso administrativo. creado por defecto en sistemas MS. Por Ejemplo: C\$, D\$, IPC\$.
- *admin users*: lista de usuarios con total permiso sobre los recursos (no aplica si security = share)
- *browsable* o *browseable*: define si el recurso es apreciable en la lista de recursos del servidor
- *comment*: permite definir un comentario aplicado al recurso, desplegable en los recursos de toda la red; a través de net view o de smbclient
- *create mode* o *create mask*: permite restringir los permisos de los archivos/directorios creados en un recurso a través de una máscara de permisos
- *force create mode*: permite aplicar permisos a los archivos/directorios creados en un recurso
- *directory mode* o *directory mask*: similar a create mode o create mask, aplicado a directorios
- *force directory mode*: similar a force create mode, aplicado a directorios
- *directory security mask*: mascara de permisos aplicado a clientes Windows NT.
- *group* o *force group*: grupo utilizado como gid del usuario conectado
- *user* o *force user*: usuario utilizado como uid del usuario conectado
- *guest ok*: permite acceder a un recurso sin identificarse
- *only guest* o *guest only*: permite acceder sólo a usuarios sin identificación. requiere el parámetro "guest ok"
- *allow hosts* o *hosts allow*: equipos permitidos de acceder al recurso. puede aplicar como global
- *deny hosts* o *hosts deny*: equipos no permitidos de acceder al recurso. puede aplicar como global
- *invalid users*: lista de usuarios no permitidos de acceder al recurso
- *only user*: permite el acceso sólo a los usuarios en la lista user
- *directory* o *path*: ruta del recurso indicado
- *read list*: lista de usuarios que tienen acceso de sólo lectura
- *read only* o *writable*: no se permite crear ni modificar los archivos/directorios del recurso
- *user*, *users* o *username*: usuarios con los cuales se probará la contraseña entregada
- *valid users*: lista de usuarios permitidos de acceder al recurso
- *invalid users*: lista de usuarios no permitidos de acceder al recurso
- *writable* o *writable*: permite escribir/modificar en el recurso indicado

de impresión

- *print ok* o *printable*: clientes pueden enviar trabajos de impresión a la carpeta indicada
- *printer* o *printer name*: nombre de la impresora a la cual serán enviados los trabajos