Introducción (I)

- SAMBA esta formado por un conjunto de aplicaciones que utilizan:
  - El protocolo de aplicación Server Message Block.
  - El protocolo de sesión NetBIOS.
- SAMBA permite:
  - Compartir sistemas de archivos e impresoras.
  - Autenticar y autorizar usuarios.
  - Resolución de nombres en WINS.
  - Anuncio de servicios.

Introducción (II)

- SAMBA funciona mediante:
  - smbd:
    - Servicio de acceso remoto a sistemas de ficheros e impresoras.
    - Autenticación y autorización de usuarios.
  - nmbd:
    - Anuncio del ordenador en el grupo de trabajo.
    - Gestión de la lista de ordenadores de un grupo.
- Utilidades adicionales:
  - smbclient: Conectarse desde Linux a recursos SMB.
  - smbtar: Realizar copias de recursos compartido.
  - smbpasswd: Manejar claves cifradas.
  - smbstatus: Información de las conexiones existentes a los recursos del equipo.
  - testparm: Validación del fichero de configuración.
  - testprns: Comprobación de la validez de una impresora.

El servidor de SAMBA (I)

- Es arrancado mediante:

```
systemctl start smb.service
systemctl start nmb.service
```

- Se ejecutan los programas:
  - /usr/sbin/smbd:
    - Puerto TCP 139: Versiones 95/98/Millenium/NT.
    - Puerto TCP 445: Versiones 2000/XP/2003.
  - /usr/sbin/nmbd:
    - Puertos UDP 137 y 138.

El servidor de SAMBA (II)

- El fichero de configuración, tanto del servidor como del cliente es:

`/etc/samba/smb.conf`

- Todas las líneas que empiezan por # ó ; son comentarios.
- El fichero esta formado por secciones:
  - El comienzo de las secciones se indican mediante *[nombre de sección]*.
  - El final de una sección se indica con el comienzo de otra sección o el final del fichero.

El servidor de SAMBA (III)

- Existen tres secciones especiales:
  - [global]: Parámetros globales de SAMBA y valores por defecto para el resto de secciones.
  - [homes]: Define un recurso para cada directorio raíz de los usuarios.
    - Funciona como opción por defecto.
    - SAMBA intenta encontrar una sección con el nombre especificado y si no existe mira si concuerda con el nombre de un usuario.
  - [printers]: Define un recurso para cada impresora especificada en */etc/printcaps*.
    - Funciona de forma similar a [homes].

El servidor de SAMBA (IV)

Opción	Descripción	Valor por defecto
workgroup	Nombre del grupo de trabajo o dominio de SAMBA.	Ninguno.
server string	Descripción del equipo en el dominio o grupo de trabajo.	Ninguno.
netbios name	Nombre del ordenador SAMBA.	Nombre DNS.
interfaces	Interfaces que utilizará SAMBA. Puede ser un interface (eth0), una dirección IP, una dirección IP/mascara o una dirección broadcast/mascara.	Todos los interfaces excepto el de loopback.
security	Nivel de seguridad.	user
passdb backend	Modo de almacenamiento de las contraseñas.	tdbsam
smb passwd file	Fichero con las contraseñas almacenadas.	En el ejecutable.
encrypt passwords	Utilizar contraseñas cifradas de Windows.	yes
password server	Servidores Windows para la autentificación.	Ninguno.
null password	Permitir el acceso de usuarios con contraseña nula.	no
map to guest	Indica cuando un acceso debe considerarse como invitado.	Never
hosts allow	Permite restringir los ordenadores y/o redes que pueden acceder al servidor.	Permiso a todos los ordenadores.
log file	Fichero de log	/var/log/samba/log.%m
max log file	Tamaño máximo del fichero de log.	50 KBytes.

El servidor de SAMBA (V)

- Ejemplo:

```
[global]
workgroup = ROBLIS
server string = SAMBA %v en %L
netbios name = glup
passdb backend = smbpasswd
smb passwd file = /etc/samba/smbpasswd
security = user
encrypt passwords = yes
map to guest = Never
hosts allow = 147.156.222. 147.156.223.
```

- Donde:
  - %v -> Versión de SAMBA.
  - %L -> Nombre del ordenador.

El servidor de SAMBA (VI)

Opción	Descripción	Valor por defecto
read only	Exportación del recurso en solo lectura.	yes
writeable	Exportación del recurso en modo escritura.	no
browseable	El servicio aparece en la lista de recursos en la red de Windows.	yes
path	Ruta absoluta al recurso	Ninguno.
comment	Descripción del servicio.	Ninguno.
guest ok	Permitir acceso como invitado.	no
guest account	Usuario que identifica el acceso como invitado.	nobody
guest only	Todos los accesos se realizan como invitado	no
force user	Fuerza a que el acceso al recurso se realice como el usuario especificado.	Ninguno.
force group	Fuerza a que el acceso al recurso se realice como el grupo especificado.	Ninguno.
hosts allow	Lista de ordenadores desde el que se permite el acceso.	Lista vacía (todos los ordenadores).
hosts deny	Lista de ordenadores a los que se les deniega el acceso.	Lista vacía (ningún ordenador).
printable	Indica si un dispositivo compartido es una impresora.	no
valid users	Lista de usuarios que pueden acceder al recurso.	Lista vacía (todos los usuarios).
follow symlinks	Permite el seguimiento de enlaces simbólicos	Yes

El servidor de SAMBA (VII)

- Ejemplos:
  - Sección [homes]:

```
[homes]
comment = Directorios raiz de los usuarios
browseable = yes
writeable = yes
```

  - Sección [printers]:

```
[printers]
comment = Impresoras
path = /var/spool/samba
browseable = no
guest ok = no
writeable = no
printable = yes
```

El servidor de SAMBA (VIII)

- Ejemplos:
  - Sección [tmp]:

```
[tmp]
comment = Espacio temporal de disco
path = /tmp
browseable = yes
read only = no
guest ok = yes
```

El servidor de SAMBA (IX)

Variable	Definición
%a	Arquitectura del cliente (SAMBA, WinNT, UNKNOWN, etc.)
%I	Dirección IP del cliente.
%m	Nombre NetBIOS del cliente.
%M	Nombre DNS del cliente.
%g	Grupo primario del usuario en Linux.
%G	Grupo primario del usuario que requiere el acceso.
%H	Directorio raíz del usuario en Linux.
%u	Usuario en Linux.
%U	Usuario que requiere el acceso.

El servidor de SAMBA (X)

Variable	Definición
%p	Directorio donde montar el recurso compartido.
%P	Directorio raíz compartido.
%S	Nombre del recurso compartido.
%d	Identificador del proceso.
%h	Nombre DNS del servidor
%L	Nombre NetBIOS del servidor.
%N	Directorio raíz del servidor.
%v	Versión de SAMBA.
%R	Versión del protocolo SMB.
%T	Día y hora actual del servidor.

Seguridad en el servidor (I)

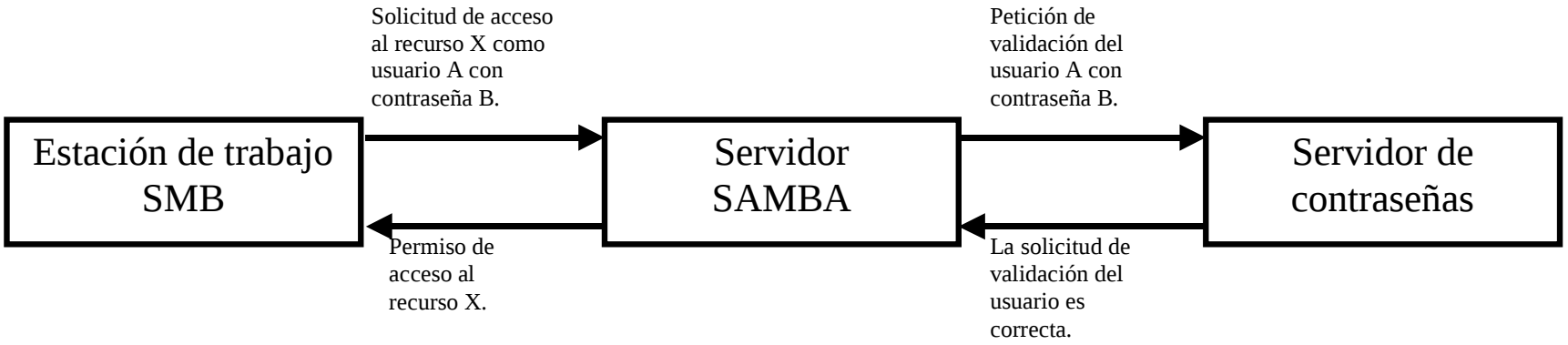
- Se indica con la opción *security* en la sección *[global]*.
  - share:
    - Cada recurso posee su propia contraseña asociada.
    - El usuario debe proporcionar la contraseña de cada recurso para acceder al mismo.
    - Utilizado por Windows 95/98/Millenium.
  - user, server y domain:
    - La validación es a nivel de usuario.
    - Un usuario, al autenticarse, puede acceder a los recursos a los que tenga permiso de forma local.
    - No necesita proporcionar una contraseña para acceder a cada recurso.

Seguridad en el servidor (II)

- user:
  - La autenticación la realiza el sistema Linux donde se ejecuta SAMBA.
  - Deben existir los mismos usuarios en Linux y Windows.
  - Windows NT4.0 (service pack 3), 2000 y XP transmiten por defecto la contraseñas cifradas:
    - Indicar que transmitan las contraseñas sin cifrar.
    - Utilizar un fichero adicional de contraseñas para almacenar las contraseñas cifradas de Windows.

Seguridad en el servidor (III)

- server:
  - La autenticación se realiza en otro ordenador, generalmente Windows 2000/XP.
  - El esquema es el siguiente:



- domain:
  - Igual que server excepto que la validación la hace un servidor de dominio.

Autenticación mediante user (I)

- Para permitir que un servidor de SAMBA autentique mediante user usando contraseñas cifradas:
  - Se utilizan los ficheros /var/lib/samba/private/passdb.tdb y /var/lib/samba/private/secrets.tdb.
- Los usuarios se manejan con el comando:

`/usr/bin/smbpasswd`

Autenticación mediante user (II)

Opción	Descripción
-a	Añade un usuario y su contraseña a SAMBA o modifica su contraseña si el usuario ya existe. El usuario debe existir como usuario de Linux para poder ser añadido a SAMBA.
-x	Elimina un usuario de SAMBA.
-d	Deshabilita la cuenta de un usuario de SAMBA.
-e	Habilita la cuenta de un usuario de SAMBA.
-n	Asigna un password nulo al usuario especificado. El usuario solo podrá acceder si se ha permitido en la sección global la validez de los passwords nulos.

Autenticación mediante user (III)

- Añadir usuario:

```
/usr/bin/smbpasswd -a <usuario>
```

- Sincronizar contraseñas de SAMBA y Linux:
  - Introducir en la sección *[global]*:

```
unix password sync = yes
passwd program = /usr/bin/passwd %u
```

El cliente de SAMBA (I)

- Desde el punto de vista del cliente existen dos mecanismos de autenticación:
  - share: Enviar una contraseña al servidor para acceder al recurso.
    - Una vez accedido al recurso no existe restricción en el uso del mismo.
  - user: Enviar un usuario y contraseña al servidor para acceder a todos los recursos del usuario.
    - Para el cliente es independiente de si la autenticación la realiza el servidor (user), otro ordenador (server) o un servidor de dominio (domain).
    - El uso del recurso depende de los permisos del usuario con el que se accede.

El cliente de SAMBA (II)

- En el fichero de configuración de SAMBA se puede especificar los modos de envío de contraseñas del cliente al servidor:

```
client {plaintext | lanman | ntlmv2} auth = {yes|no}
```

- Si no se especifica ningún modo se utiliza NTLMv2.
- Si se especifican varios modos explícitamente, se utiliza solo el más seguro.
  - plaintext: Contraseñas sin cifrar.
  - lanman: Contraseñas cifradas utilizando LANMAN.
  - ntlmv2: Contraseñas cifradas utilizando NTLMv2.

El cliente de SAMBA (III)

- El cliente de Linux de SAMBA es /usr/bin/smbclient.
- Su ejecución básica es:

```
/usr/bin/smbclient <recurso compartido> [clave] [-U usuario]
```

- Donde <recurso compartido> es:

```
//<nombre NetBIOS>/<recurso>
```

- [clave] es la contraseña.
  - Si no se especifica se solicita por teclado.
- [-U usuario] es el usuario que enviaremos al cliente.
  - Por defecto es el usuario con el que se ejecuta el comando.
- Una vez conectados es posible cerrar la conexión con el comando *quit*.

El cliente de SAMBA (IV)

- Un ordenador Windows puede ser cliente de un servidor SAMBA de Linux mediante:
  - Interfaz gráfico:
    - Conectar a equipo remoto.
  - Línea de comandos:
    - Conexión a un servidor Linux:

```
net use {unidad|*} <recurso compartido> [clave] [/u:<usuario>]
```

    - Desconexión de un servidor Linux:

```
net use <unidad> /delete
```