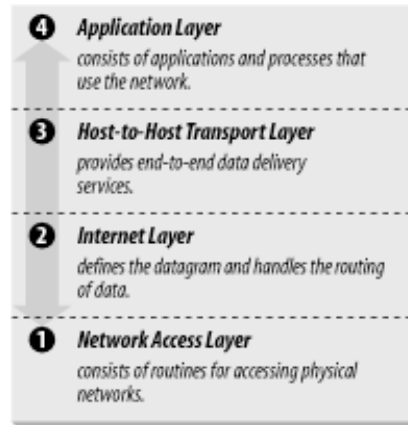


4. Configuración de la red y recursos compartidos

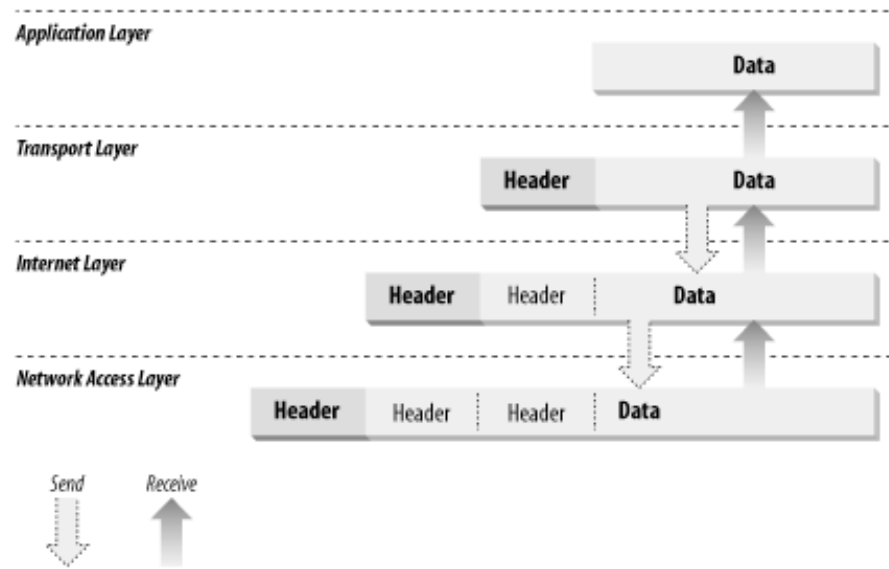
- Configuración de red.
- Autenticación en red (LDAP, Kerberos, Directorio Activo)
- Redes Windows. Directorio Activo. Dominios. Unidades organizativas
- Conceptos de IPV6

Configuración de red: Arquitectura TCP/IP



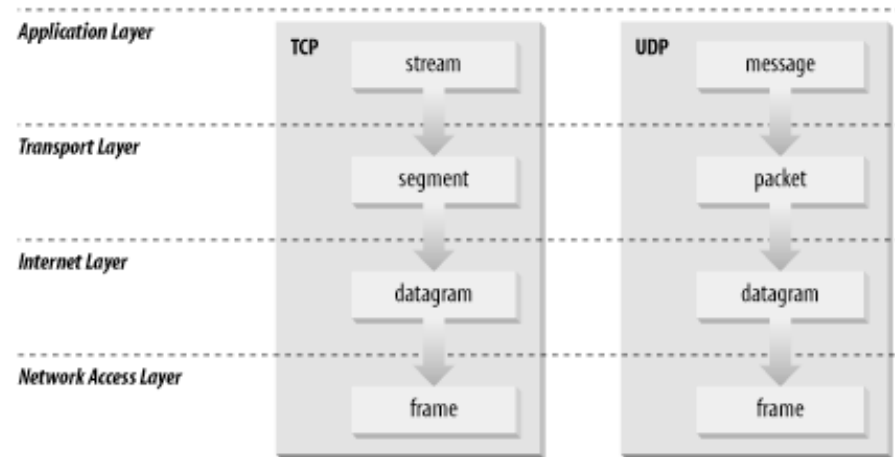
- Arquitectura: Normalmente se describe TCP/IP como un modelo con menos capas que las usadas en el modelo OSI. Usaremos un modelo basado en tres capas (Aplicación, Transporte, Acceso a la Red) con la adición de una capa “Internet”

Configuración de red: Encapsulación



- Los datos fluyen hacia abajo cuando se envía a la red, y de abajo a arriba cuando se reciben de la red. Cuando se envían datos, cada capa añade información de control o cabeceras, que se anteponen a los datos que se transmiten (el proceso se llama encapsulación). Cuando se reciben, cada capa procesa y elimina su cabecera

Configuración de red: Encapsulación



- Las diferentes capas de TCP/IP usan nombres distintos para referirse a los datos transmitidos. Las aplicaciones que usan TCP se refieren a los datos como un *stream*, mientras que las que usan UDP usan la palabra *message*. TCP llama a los datos *segment*, y UDP *packet*. La capa de internet usa el nombre *datagram*. Cada una de las redes usadas en TCP/IP usa una terminología distinta. Es corriente que se llame a los datos transmitidos *packet* o *frame*.

Configuración de red: Capa de acceso a la red

- Es la capa más baja de la jerarquía TCP/IP
- Los protocolos de esta capa proporcionan los medios para que el sistema envíe datos a otros dispositivos a través de una red directamente conectada al equipo.
- Esta capa define cómo usar la red para transmitir un datagrama IP
- Al contrario que los protocolos de nivel superior, los protocolos de acceso a la red deben conocer los detalles de la red física (estructura en paquetes, direccionamiento, etc.) para formatear correctamente los datos.
- Esta capa cubre las funciones de las tres capas de más bajo nivel del modelo de referencia OSI (Red, Enlace, Física). Normalmente ignoramos esta capa; todos los protocolos que manejaremos (IP, TCP, UDP, etc.) son de nivel más alto
- Las funciones de este nivel son proporcionar la encapsulación de los datagramas IP en los frames transmitidos por la red, y asociar las direcciones IP con las direcciones físicas usadas por la red (por ejemplo, asociar direcciones IP con direcciones MAC Ethernet)

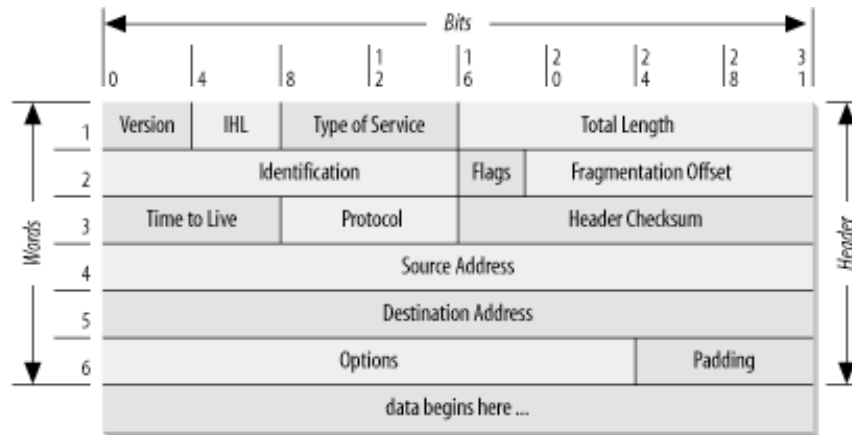
Configuración de red: Capa de Internet

- El protocolo más importante de la capa de internet es el protocolo IP, generalmente en su versión 4 (IPv4). IP 5 es un protocolo experimental de transporte de streams usado para repartir datos en tiempo real. IPv6 aumenta la capacidad de direccionamiento y no es interoperable con IPv4.
- El IP (Internet Protocol) proporciona el servicio básico de reparto de paquetes sobre el que se construyen las redes TCP/IP. Todos los protocolos en los niveles superiores al de Internet usan IP para repartir datos.
- IP es un protocolo sin conexión, lo cual significa que no realiza un handshake para establecer una conexión de extremo a extremo antes de transmitir datos. Un protocolo orientado a la conexión intercambiaría información de control con el sistema remoto para verificar que está disponible para recibir datos antes de intentar el envío. IP confía en las capas inferiores para establecer la conexión en los casos en que se requiera un servicio orientado a la conexión.
- IP confía también en los protocolos de los niveles inferiores para proporcionar detección de errores y recuperación ante los mismos. Se dice que es un protocolo “no fiable” porque no contiene código de detección de errores, lo cual no quiere decir que la integridad de la información transmitida no esté garantizada - sólo que esta verificación se realiza en otros niveles.

Configuración de red: Capa de Internet

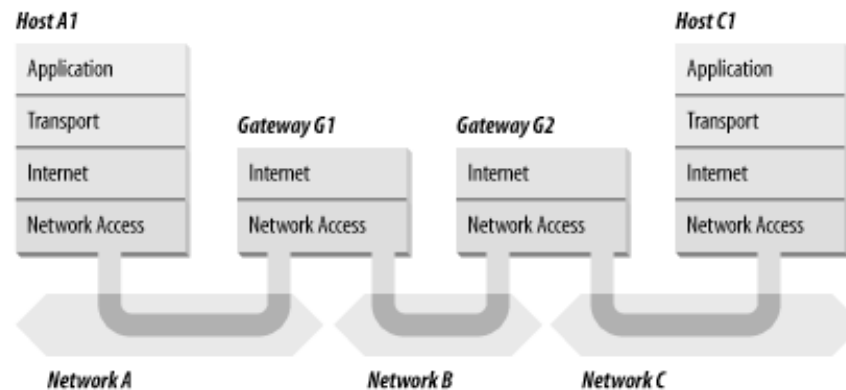
- Las funciones del protocolo IP son:
 - Definir el datagrama (unidad básica de transmisión en Internet)
 - Definir el esquema de direccionamiento
 - Mover datos entre la capa de acceso a la red y la capa de transporte
 - Enrutar datagramas a hosts remotos
 - Fragmentar y reensamblar los datagramas

Configuración de red: Datagramas



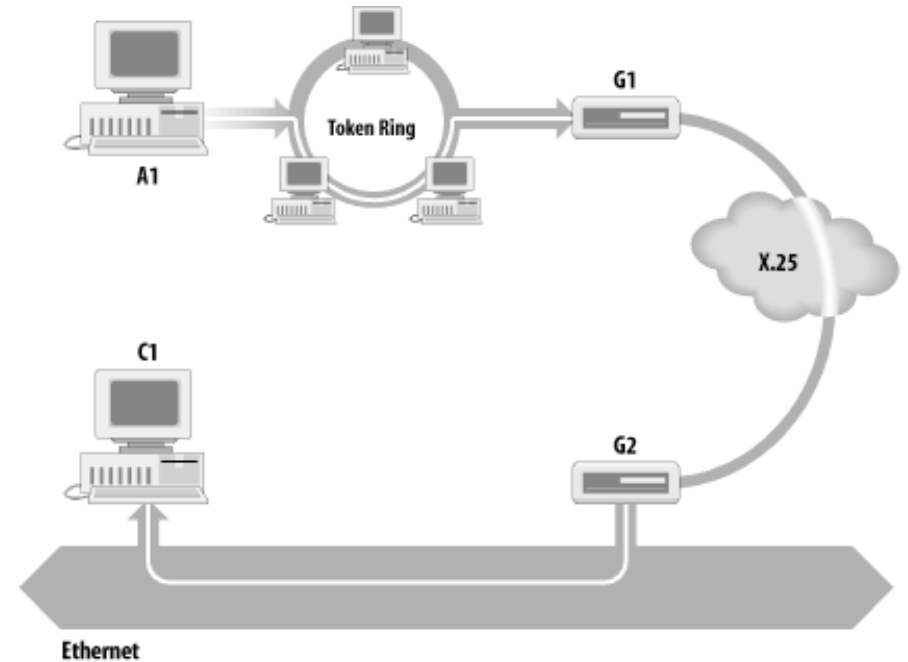
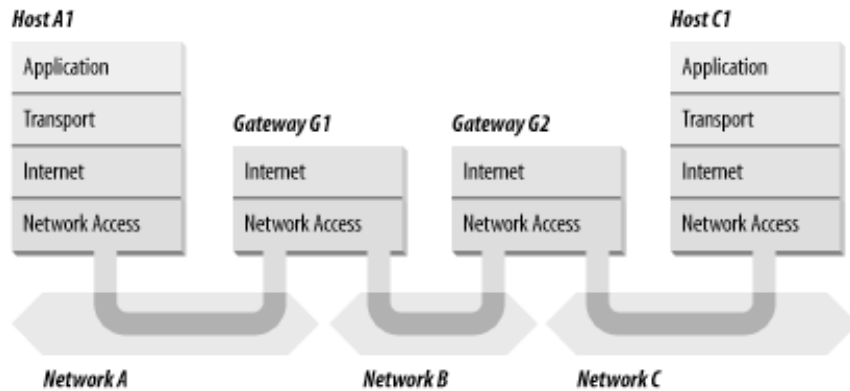
- El paquete transmitido por el protocolo IP o datagrama tiene una cabecera que puede tener cinco o seis palabras de longitud (el campo IHL, Internet Header Length indica la longitud de la cabecera) y contiene toda la información necesaria para entregar el paquete.
- El protocolo IP, para entregar el datagrama, comprueba la dirección de destino en la palabra quinta. Esta dirección consta de 32 bits (su estructura se vará más adelante). Si la dirección de destino está en un host de la red local, el paquete se entrega directamente. Si no, se entrega a una pasarela (*gateway*). Las pasarelas son dispositivos que intercambian paquetes entre redes físicas distintas. Decidir que pasarela debe usarse se llama enrutado (*routing*). IP decide el enrutado para cada paquete.

Configuración de red: Enrutado de datagramas



- Las pasarelas/gateways IP se conocen comúnmente como *routers IP*, porque usan el protocolo IP para enrutar paquetes entre redes.
- Sólo hay dos tipos de dispositivos de red: hosts y gateways. Los gateways reenvían paquetes entre redes, y los hosts no. Ahora bien, si un host está conectado a más de una red (multi-homed host) puede reenviar paquetes entre redes, y se puede considerar un gateway

Configuración de red: Enrutado de datagramas



- Sólo se pueden enviar paquetes a dispositivos en la misma red física. Los paquetes de A1 para C1 se envían mediante las pasarelas G1 y G2. El host A1 primero envía el paquete a G1, con el que comparte la red A. G1 envía el paquete a G2 por la red B, que se lo entrega a C1. El host A1 no tiene conocimiento de G2; manda paquetes destinados tanto a las redes B como C a través de G1

Configuración de red: Fragmentación de datagramas

- Cuando un datagrama se enruta hacia redes diferentes, puede ser necesario que el módulo IP en una pasarela divida el datagrama en trozos más pequeños, ya que cuando se conectan redes distintas el tamaño de paquete de una puede ser demasiado grande para la otra.
- Cada tipo de red tiene una MTU (maximum transmission unit) que es el tamaño del máximo paquete que puede transmitir. Si se recibe un paquete más largo que la MTU de la red de destino se fragmenta el paquete en trozos, cada uno de los cuales tiene el mismo formato que el datagrama original.
- La segunda palabra de la cabecera contiene información que identifica cada fragmento y que sirve para reensamblar los fragmentos. El campo "Identificación" indica el datagrama al que pertenece el fragmento, y el "Fragmentation Offset" indica el número de fragmento. El campo "Flags" tiene un bit "More Fragments" que le indica al IP si se han ensamblado ya todos los fragmentos.

Configuración de red: Paso de datagramas a la capa de transporte

- Cuando el IP recibe un datagrama que está direccionado al host local, pasa la porción de datos de dicho datagrama al protocolo correspondiente del nivel de transporte.
- Cada protocolo de la capa de transporte tiene un único número que lo identifica ante el protocolo IP (se verán más adelante esos números y cómo acceder a la tabla en que se almacenan en el host)

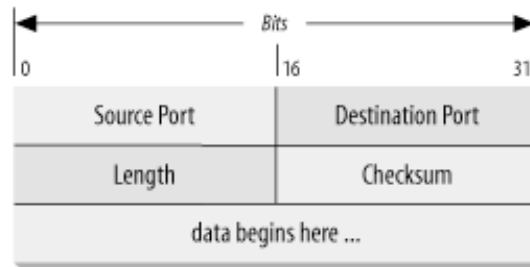
Configuración de red: ICMP (Internet Control Message Protocol)

- El ICMP es una parte integrante del protocolo IP que usa las facultades de IP para enviar datagramas para enviar mensajes de control, aviso de errores y otra información para TCP/IP:
 - *Control de flujo*: cuando los datagramas llegan demasiado deprisa, el host destinatario envía un ICMP Source Quench Message al emisor, que hace que éste deje de enviar datagramas temporalmente.
 - *Detección de destinos inalcanzables*: cuando un destino es inalcanzable, el sistema que detecta el problema envía el mensaje Destination Unreachable a la fuente del datagrama. Si el destino inalcanzable es una red o un host, este mensaje lo envía el gateway, y si lo que es inalcanzable es el puerto el mensaje es enviado por el propio host.
 - *Redirección de rutas*: un gateway envía el mensaje ICMP Redirect para decirle a un host que use otra pasarela como mejor opción. Este mensaje sólo puede emitirse cuando el host de origen está en la misma red que ambas pasarelas.
 - *Chequeo de hosts remotos*: un host puede enviar el mensaje ICMP Echo para ver si el protocolo IP de un sistema remoto está funcionando y es operacional. Cuando un sistema recibe el mensaje de eco, responde enviando un paquete con la misma información recibida de vuelta al host de origen (comando ping).

Configuración de red: Capa de transporte

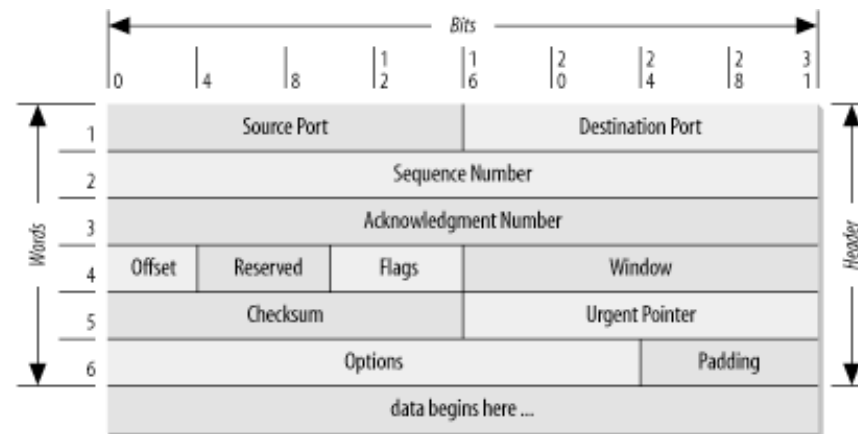
- La capa de protocolos por encima de la capa de internet es la capa de transporte de Host a Host. Los dos protocolos más importantes de esta capa son TCP (Transmission Control Protocol) y UDP (User Datagram Protocol). TCP proporciona un reparto de datos con detección y corrección de errores, y está orientado a la conexión. UDP tiene menor sobrecarga y el reparto no requiere de una conexión

Configuración de red: User Datagram Protocol



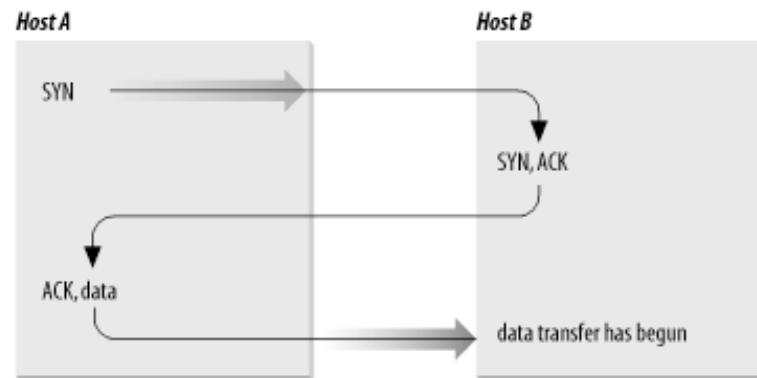
- El que UDP no sea “fiable” significa que no hay técnicas en el protocolo que verifiquen que los datos enviados han alcanzado correctamente el punto de destino.
- UDP usa números de 16 bit (source port y destination port) en la primera palabra de la cabecera para enviar datos a los procesos correctos.
- UDP se elige cuando hay que transmitir pocos datos, o bien la aplicación sigue un modelo “consulta-respuesta”, donde la respuesta sirve de confirmación de que la pregunta ha llegado.

Configuración de red: Transmission Control Protocol



- TCP tiene un mecanismo llama PAR (Positive Acknowledgement with Retransmission): un sistema usando PAR envía los datos de nuevo hasta que el sistema remoto indica que los datos han llegado correctamente. La unidad de información intercambiada se llama segmento (ver figura). Cada segmento contiene un checksum que el receptor usa para verificar que los datos no han sido cambiados. Si los datos son íntegros, el receptor envía un Positive Acknowledgement al emisor. Si no, el receptor descarta el paquete y tras un timeout adecuado el emisor lo volverá a enviar.

Configuración de red: Transmission Control Protocol

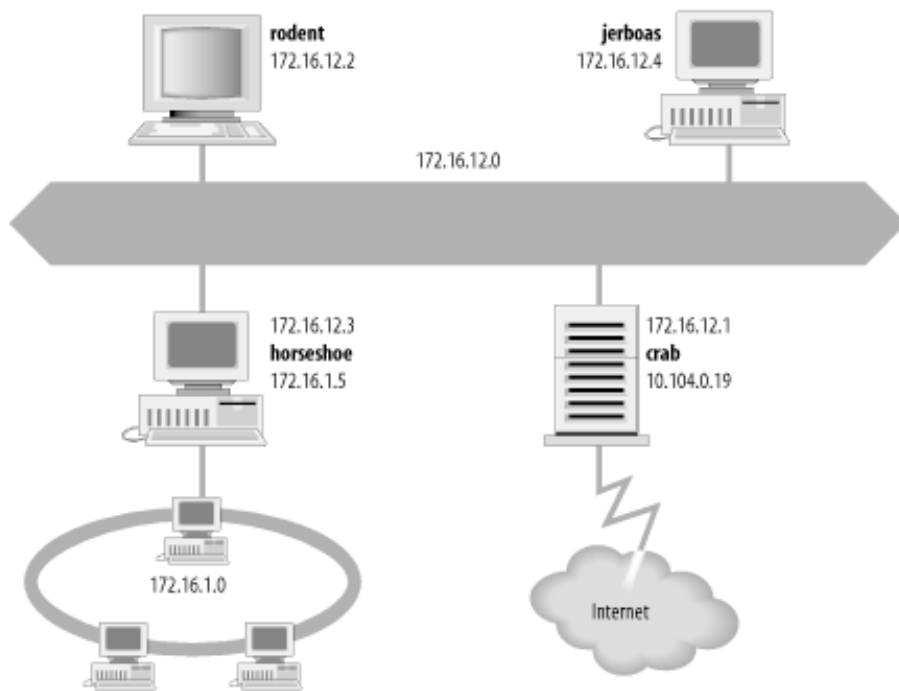


- TCP está orientado a la conexión, y para establecer una conexión lógica entre ambos hosts intercambia información de control (handshake). El segmento de control está marcado con un bit en la cuarta palabra de la cabecera del segmento.
- El handshake TCP se llama three-way porque se intercambian 3 segmentos: primero se envía un segmento con el bit SYN ("SYNchronize sequence numbers") activado. Este segmento le indica al host B que A quiere iniciar una conexión y el número del primer segmento que enviará. B le responde a A con un segmento que contiene los bits Acknowledgement (ACK) y SYN, y que informa a A del número del primer segmento que enviará B. Por último, A envía un paquete con el bit ACK y transfiere el primer bloque de datos.
- Cuando la conexión termina, hay un nuevo handshake con tres segmentos conteniendo el bit "No more data from sender" (FIN)
- El campo "Window" indica el número de bytes que el sma. remoto es capaz de aceptar: el emisor envía paquetes hasta llenar ese valor, y no hace falta que se envíen ACKs de cada paquete
- TCP también es responsable de entregar los datos a la aplicación correcta, identificada por un número de puerto de 16 bits, contenido en la cabecera.

Configuración de red: Capa de aplicación

- La capa de aplicación incluye todos los procesos que usan la capa de transporte para repartir datos. La mayoría de estas aplicaciones proporcionan servicios al usuario, cuya administración es el objeto de esta asignatura.
- Los protocolos de aplicación más conocidos son Telnet (Network Terminal Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol)
- Como administrador, otras aplicaciones TCP/IP son DNS (Domain Name Service), OSPF (Open Shortest Path First, usada por los routers para intercambiar información), NFS (Network File System), etc.
- Todos ellos se estudiarán más adelante.

Configuración de red: Direcccionamiento, Enrutado y Multiplexado



- Direcccionamiento: Las direcciones IP, que identifican a cada host en la red
- Enrutado: Las pasarelas envían los datos a la red correcta
- Multiplexado: Los protocolos y los números de puerto entregan los datos al módulo software adecuado dentro del mismo host
- Usaremos la red de la izquierda para ilustrar estos conceptos

Configuración de red: La dirección IP

- Un entero de 32 bits que identifica cada dispositivo en una red TCP/IP
- Los sistemas pueden ser accedidos de tres formas diferentes.
 - Los sistemas individuales se direccionan mediante una dirección de host, o dirección unicast.
 - Puede accederse simultáneamente a un grupo de sistemas con una dirección multicast, como 224.0.0.9: los routers en el camino entre el origen y el destino reconocen la dirección especial y enrutan copias del paquete a cada miembro del grupo
 - Todos los sistemas de una misma red pueden accederse simultáneamente mediante una dirección broadcast, como 172.16.255.255
- Una dirección IP con todos los bits de host a cero identifica a la red misma (172.16.0.0). Estas direcciones se usan en las tablas de rutas.
- Las direcciones con un primer byte mayor que 223 no pueden asignarse a una red física, están reservadas. La dirección 0.0.0.0 designa la ruta por defecto y la dirección 127.0.0.0 es la dirección loopback, usada para referirse al host local mediante una dirección IP.

Configuración de red: Estructura de una dirección IP

- Una dirección IP consta de una parte de red y de una parte de host. El número de bits usado para definir la red es variable, y la longitud de ese prefijo se determina por una máscara de bits.
- La máscara funciona de la forma siguiente: si el bit está en la máscara, el bit equivalente de la dirección está en la parte de red. Si no, en la parte de host. Por ejemplo, la dirección 172.22.12.4 con la máscara 255.255.255.0 se descompone en la dirección de host 4 en la red 172.22.12.
- Para indicar la longitud de la máscara se puede escribir 172.22.12.4/24, donde el 24 indica el número de unos en la máscara de red
- Las organizaciones compran bloques de direcciones de los proveedores de servicios de internet, p.e. podrían comprar 192.168.16.0/20, un bloque de 12 bits con 4096 direcciones desde 192.168.16.0 a 192.168.31.255. Cada uno de estos bloques de direcciones aparece ante el mundo como una única dirección de red: los routers externos tienen una ruta al bloque 192.168.16.0/20, aunque la compañía tenga varias redes físicamente separadas dentro del bloque de direcciones, subdivididas a su vez con otras máscaras.

Configuración de red: Subredes y la máscara natural

- Dentro de cada compañía, las redes se subdividen tomando bits de la parte de host como nuevos bits de red. Cada una de estas divisiones es gestionada por un nuevo router, y en general cada red física tendrá su propia dirección
- Originalmente el espacio de direcciones se dividía en clases (clase A, clase B, clase C). Ya no se usan, pero las mismas reglas que se usaban determinan la máscara por defecto, o “máscara natural”. Las reglas son:
 - Si el primer bit de la dirección IP es cero, la máscara por defecto es de 8 bits (antigua clase A)
 - Si los dos primeros bits son 10, 16 bits (clase B)
 - Si los tres primeros bits son 110, 24 bits (clase C)
 - Si los cuatro primeros bits son 1110, es una dirección multicast. Estas direcciones se usan para construir grupos de ordenadores que comparten una aplicación, como videoconferencia. La máscara tiene 32 bits
- Actualmente se pueden asociar rangos de direcciones contiguos a la misma red sin que formen una clase C. Para evitar tener que introducir una entrada separada para cada clase C en la tabla de rutas se usa Classless Inter-Domain Routing (CIDR)

Configuración de red: La tabla de rutas

- Todos los dispositivos de red, hosts y gateways, deben tomar decisiones de enrutado. Para la mayoría de los hosts, las decisiones de enrutado son simples:
 - Si el host de destino está en la red local, los datos se entregan al host de destino
 - Si el host de destino está en una red remota, los datos se reenvían a un gateway local
- Las decisiones de enrutado de IP son búsquedas en tablas. Los paquetes se enrutan a sus destinos de acuerdo con la tabla de rutas (forwarding table). Esta tabla asocia destinos al router y al interfaz de red que IP debe usar para alcanzar ese destino

Configuración de red: Tabla de rutas en Linux

```
# route -n
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.16.55.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
172.16.50.0	172.16.55.36	255.255.255.0	UG	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	172.16.55.1	0.0.0.0	UG	0	0	0	eth0

- Se usa el comando route, con la opción -n para que no se conviertan las direcciones IP a nombres
- El significado de los campos es:
 - Destination: Valor con el que se compara la dirección IP
 - Gateway: Router que se usará para llegar al destino
 - Genmask: Máscara de red relacionado con el campo destino
 - Flags: U (ruta operacional) H (ruta a un host, no a una red) G (ruta que usa un gateway externo) R (ruta instalada por un protocolo de enrutamiento dinámico con la opción reinstate) D (ruta añadida por un mensaje ICMP Redirect) M (instalada con la opción mod) A (cacheada y con entrada asociada en la tabla ARP) L (ruta local, a una de las direcciones de este host), B (ruta cuyo destino es una dirección Broadcast) ! (datagramas dirigidos a esta ruta serán rechazados)

Configuración de red: Tabla de rutas en Linux

```
# route -n
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.16.55.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
172.16.50.0	172.16.55.36	255.255.255.0	UG	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	172.16.55.1	0.0.0.0	UG	0	0	0	eth0

- **Metric:** El coste de la ruta, usando para elegir entre rutas duplicadas que aparezcan en la tabla
- **Ref:** Número de veces que esta ruta se ha usado para establecer una conexión (no usado en Linux)
- **Iface:** nombre del interfaz de red usado por esta ruta.
- IP usa la información de la tabla de rutas para construir las rutas usadas por las conexiones activas. Las rutas asociadas a las conexiones activas se almacenan en un cache, que puede consultarse con la orden `route -Cn`
- El cache es diferente de la tabla de rutas porque sólo se muestran las rutas establecidas: la tabla de rutas se usa para tomar decisiones, el cache lista las decisiones que ya se han tomado.

Configuración de red: Tabla de rutas en W2003

```
C:\>route print
```

```
IPv4 Route Table
```

```
=====
```

```
Interface List
```

```
0x1 ..... MS TCP Loopback interface
```

```
0x10003 ...00 50 ba 3f c2 5e ..... D-Link DFE-530TX+ PCI Adapter
```

```
=====
```

```
Active Routes:
```

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	172.16.12.1	172.16.12.20	30
	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
	172.16.12.0	255.255.255.0	172.16.12.20	172.16.12.20	30
	172.16.12.20	255.255.255.255	127.0.0.1	127.0.0.1	30
	172.16.12.255	255.255.255.255	172.16.12.20	172.16.12.20	30
	224.0.0.0	240.0.0.0	172.16.12.20	172.16.12.20	30
	255.255.255.255	255.255.255.255	172.16.12.20	172.16.12.20	1

```
Default Gateway: 172.16.12.1
```

```
=====
```

```
Persistent Routes:
```

```
None
```

- El comando route print muestra la tabla de rutas en tres secciones:
 - Lista de interfaces
 - Rutas activas: que pueden ser modificadas por la red
 - Rutas persistentes: rutas estáticas que han sido definidas por el administrador
- Cada ruta activa tiene los siguientes campos:
 - Destination
 - Netmask
 - Gateway
 - Interface: dirección del interfaz de red usado por la ruta
 - Metric: el coste de la ruta, usado si hay duplicados

Configuración de red: Resolución de direcciones en Linux

```
% arp -a
```

```
Net to Media Table: IPv4
```

Device	IP Address	Mask	Flags	Phys Addr
-----	-----	-----	----	-----
dnet0	rodent	255.255.255.255		00:50:ba:3f:c2:5e
dnet0	crab	255.255.255.255	SP	00:00:c0:dd:d4:da
dnet0	224.0.0.0	240.0.0.0	SM	01:00:5e:00:00:00

- El software ARP (Address Resolution Protocol) mantiene una tabla de traducciones entre direcciones IP y Ethernet, que se construye dinámicamente. Cuando ARP recibe una consulta, busca la dirección en la tabla. Si no la encuentra, hace broadcast de un paquete a cada host en la Ethernet, conteniendo la dirección IP de la máquina cuya dirección Ethernet se busca. Si el host identifica la dirección como suya, responde al paquete y ARP almacena la asociación.
- El flag P significa “publicar”. Es posible publicar direcciones de otros hosts (proxy ARP)

Configuración de red: Resolución de direcciones en W2003

```
C:\> arp -a
```

```
Interface: 192.168.0.20 --- 0x10003
```

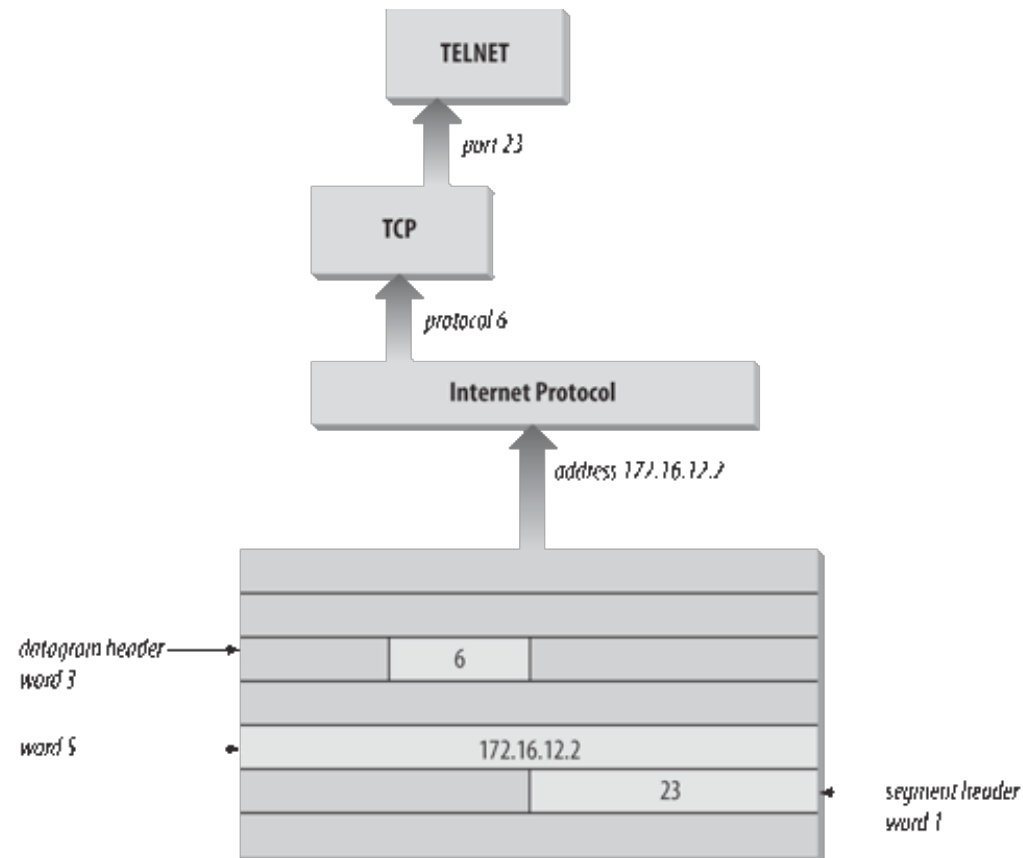
Internet Address	Physical Address	Type
192.168.0.2	00-e0-4c-9b-99-19	dynamic
192.168.0.3	00-00-c0-9a-72-ca	dynamic
192.168.0.12	00-10-a4-8b-8b-97	static

- La sintaxis es similar, a excepción del flag “P”

Configuración de red: Puertos, protocolos y sockets

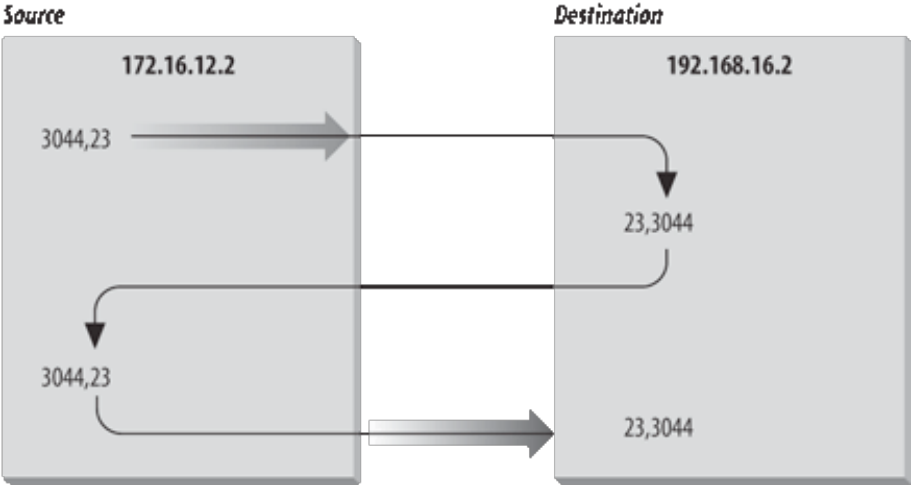
- El fichero /etc/protocols (Linux) contiene una lista con los nombres y los números de los protocolos asociados. Esta tabla sirve para que la capa IP entregue el datagrama a uno de los protocolos de transporte sobre él. Por ejemplo, un 6 indica que se debe usar el protocolo de transporte TCP, un 17 se corresponde con UDP, etc.
- En W2008 la tabla se encuentra en %SystemRoot%\system32\drivers\etc\protocol
- El fichero /etc/services (Linux) sirve para realizar una asociación similar entre el protocolo de transporte y la aplicación (el servicio de red), que está identificada por un número de 16 bits. Los puertos bajo 1024 están reservados para servicios como FTP o Telnet. Los puertos entre 1024 y 49151 son “puertos registrados”, los restantes son de uso libre. Los números de puerto no son únicos entre los protocolos de transporte.
- En W2008 el fichero está en %SystemRoot%\system32\drivers\etc\services

Configuración de red: Puertos, protocolos y servicios



- proceso de entrega de un datagrama

Configuración de red: Sockets



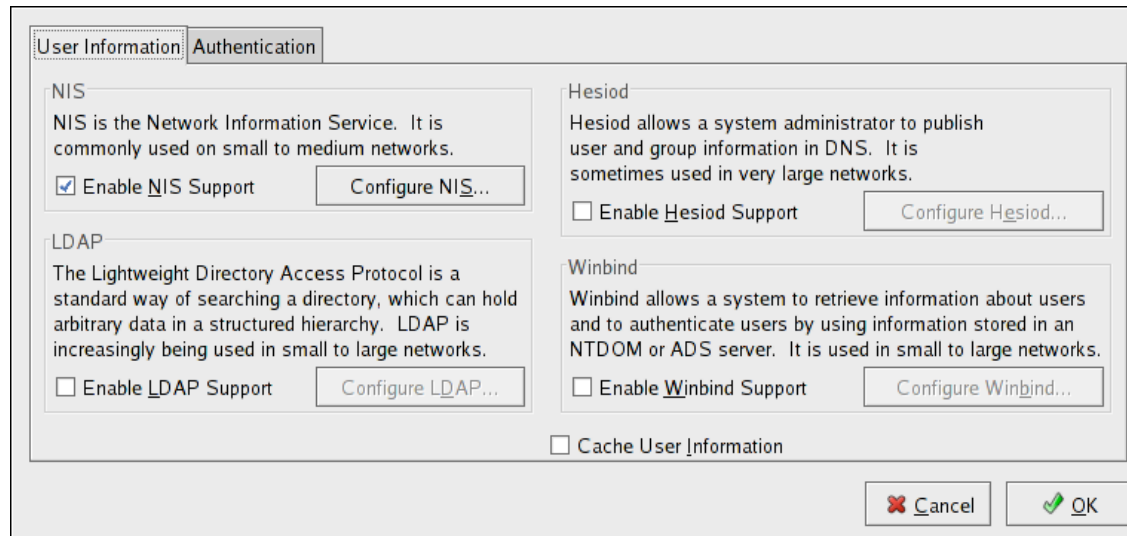
• D:\>netstat -na

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1029	0.0.0.0:0	LISTENING
TCP	192.168.0.20:135	192.168.0.12:32802	ESTABLISHED
TCP	192.168.0.20:139	0.0.0.0:0	LISTENING
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1027	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	127.0.0.1:123	*:*	
UDP	192.168.0.20:67	*:*	
UDP	192.168.0.20:68	*:*	
UDP	192.168.0.20:123	*:*	
UDP	192.168.0.20:137	*:*	
UDP	192.168.0.20:138	*:*	
UDP	192.168.0.20:2535	*:*	

Autenticación en red: Configuración de la Autenticación

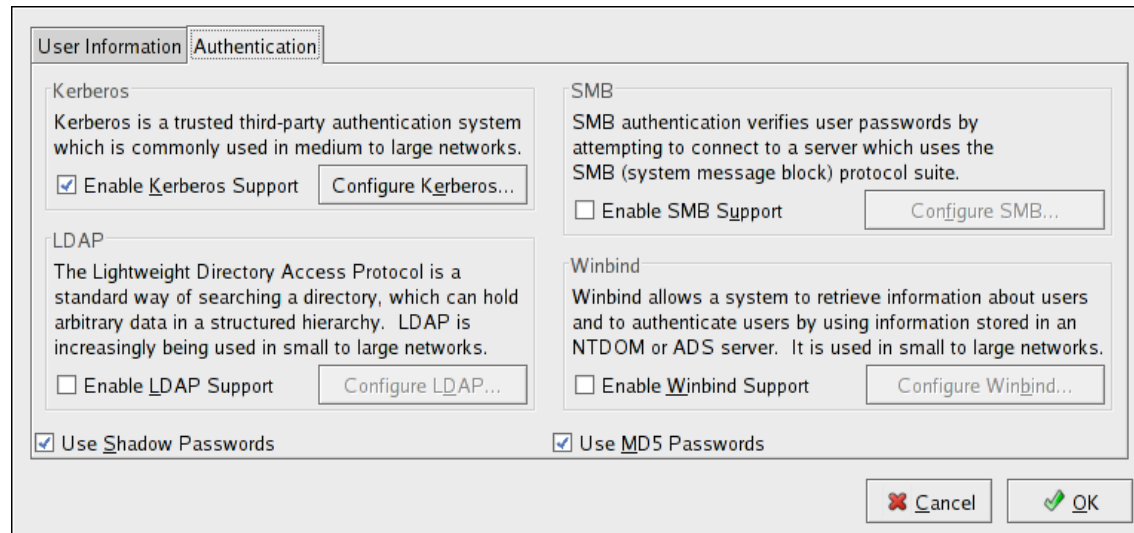
- Cuando un usuario accede al sistema, su nombre y clave debe ser verificados. En las transparencias anteriores se ha visto cómo se estructura la información cuando los datos de autenticación están en el sistema local. En otras ocasiones, el sistema delega la autenticación a una base de datos de usuarios localizada en un sistema remoto.
- La configuración de la autenticación puede hacerse con herramientas gráficas (system-config-authentication) o de texto (authconfig). Estudiaremos la versión gráfica

system-config-authentication



- Opciones para obtener de información del usuario:
 - NIS: El sistema se conecta a un servidor NIS. Depende del paquete ypbind, se arranca también portmap
 - LDAP: Recuperar información del usuario mediante LDAP
 - Hesiod: Mediante Hesiod (una base de datos en DNS)
 - Winbind: Windows Active Directory

system-config-authentication



- Opciones:
 - Kerberos (Opciones para Realm, KDC, Admin Servers)
 - LDAP mediante los módulos PAM correspondientes
 - Shadow Passwords (opción por defecto)
 - SMB: Samba mediante los módulos PAM
 - Winbind: Windows Active Directory o controlador de dominio
- La opción MD5 permite usar passwords de hasta 256 caracteres

NIS -Network Information Service

- Es un servicio de red que consiste en compartir unas bases de datos. Estas están en el equipo servidor, y contienen la información que localmente estaría almacenada en /etc/passwd, /etc/shadow y /etc/group
 - nombres de usuario, passwords, directorios HOME
 - información de grupo

NIS

- En cada red debe haber al menos una máquina actuando de servidor NIS. Pueden tenerse múltiples servidores, cada uno de los cuales sirve a un cierto “dominio”, o bien cooperar entre sí, de forma que uno de los servidores sea el maestro y otros los esclavos
- Los servidores esclavos almacenan copias de las bases de datos NIS desde el servidor maestro, y se actualizan cada vez que hay cambios. Cuando uno de los servidores cae, el cliente tratará de encontrar otro servidor.
- Las bases de datos NIS están en formato DBM, derivado de bases de datos ASCII. Hay herramientas que convierten a DBM ficheros de texto como `/etc/passwd` y `/etc/group`
- Los servidores esclavos son notificados de los cambios via el programa `yppush`, y se mantienen sincronizados. Los clientes no necesitan este sincronismo, ya que acceden directamente al servidor o leen la información almacenada en una de las bases en DBM

Instalación de un servidor NIS

- portmap tiene que estar en ejecución, y se tiene que permitir la autenticación con NIS con system-config-authentication
1. Se activa el nombre del dominio: *nisdomainname nombreNIS*
 2. En /etc/sysconfig/network se añade la línea *NISDOMAIN="nombreNIS"*
 3. En el fichero de configuración /etc/yp.conf se añaden las líneas
domain nombreNIS server nombreservidor
ypserver nombreservidor
 4. Se lanzan los demonios *ypserv* y *rpc.yppasswd*
 5. Se entra en el directorio /var/yp y se ejecuta la orden make para crear la base de datos que NIS gestiona
 6. Se lanza el demonio *ypbind*

Instalación de un cliente NIS

- portmap tiene que estar en ejecución, y se ha tenido que permitir la autorización con system-config-authentication
1. Se ejecuta *nisdomainname nombreNIS*
 2. En */etc/sysconfig/network* se añade la línea *NISDOMAIN="nombreNIS"*
 3. En el fichero de configuración */etc/yp.conf* se añade la línea
domain nombreNIS server nombreServidor
 4. Se lanza *ypbind*
 5. En */etc/passwd* se añade la línea **+:*:0:0:::**
 6. En */etc/group* se añade la línea **+:*:0:**
 7. Tiene que existir el directorio */var/yp*

Seguridad NIS

- En */var/yp/securenets* se indican las redes o equipos que tienen acceso permitido al dominio NIS
 - Formato: *netmask network* o bien *host IP*:

255.255.255.0 192.168.6.0

host 192.168.6.5
- el comando *yppasswd* permite cambiar la contraseña en el servidor, si en éste está corriendo el demonio *rpc.yppasswd*
- Otros comandos permiten cambiar el shell (*ypchsh*), parámetros del usuario (*ypchfn*), o ver el contenido de los ficheros de passwords (*ypcat passwd*) y servidores (*ypcat ypservers*).

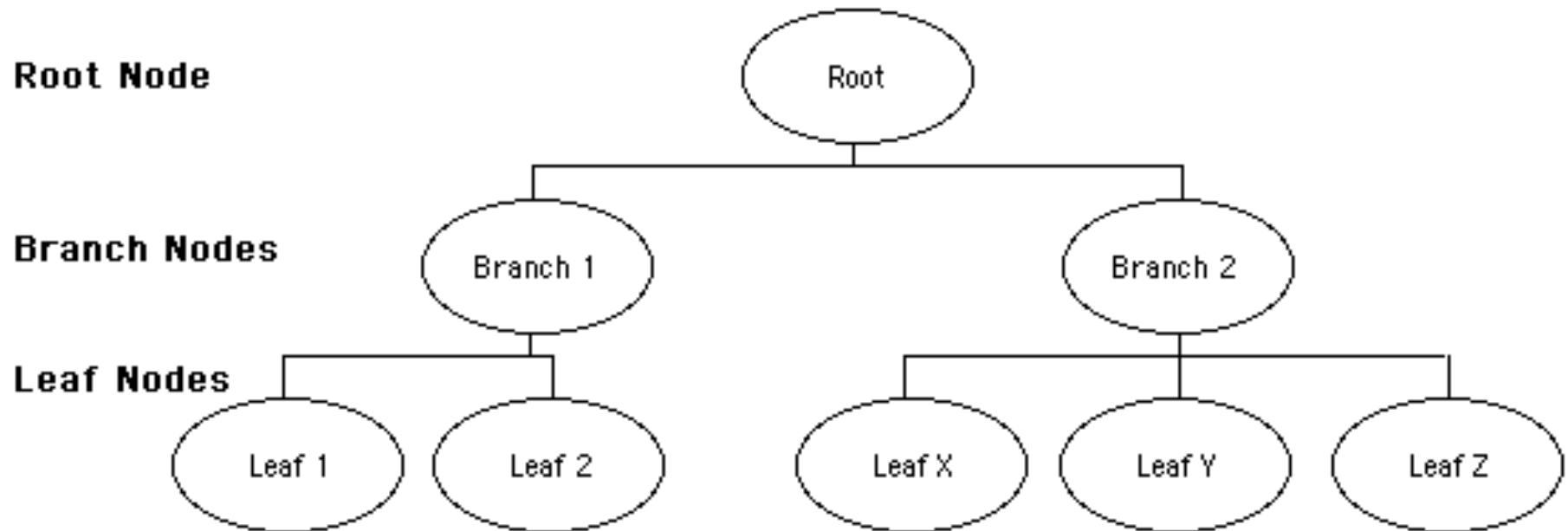
Qué es LDAP

- Un servicio de publicación de directorios
- Lightweight Directory Access Protocol a directorios X.500
- Almacena datos con atributos (una especie de base de datos)
- Optimizada para lectura (es más frecuente que la escritura)
- Implementación cliente/servidor
- Esquemas extensibles para la definición de atributos

Ventajas

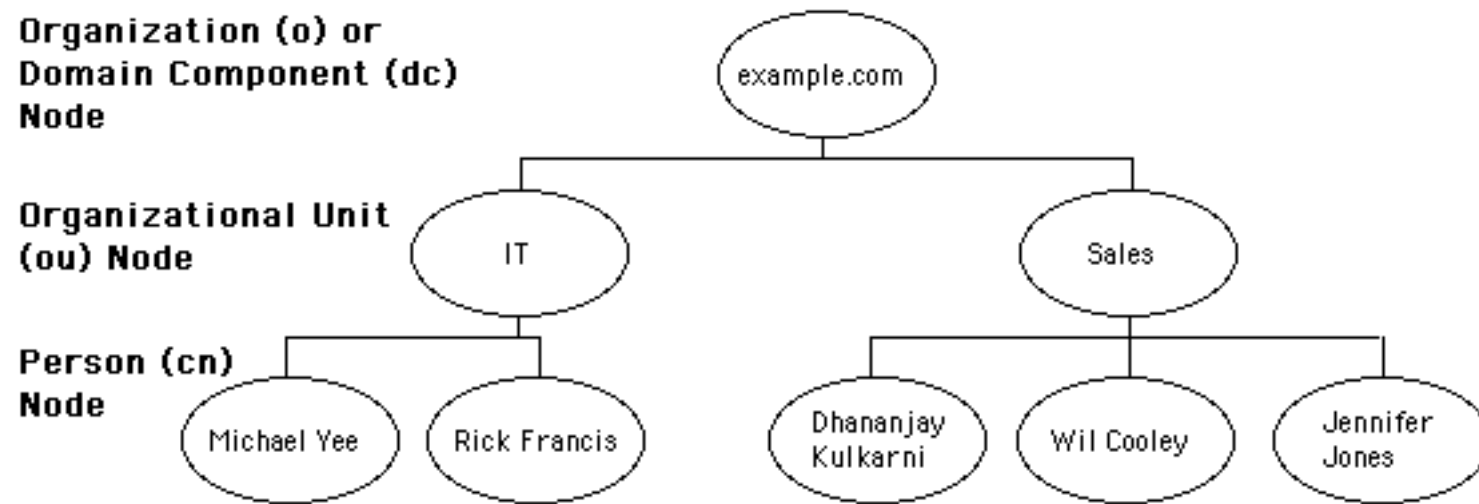
- Proporciona una forma estándar de acceder a datos a través de la red
- Búsquedas y recuperación de datos rápidos
- Buenos mecanismos de seguridad

Jerarquía LDAP



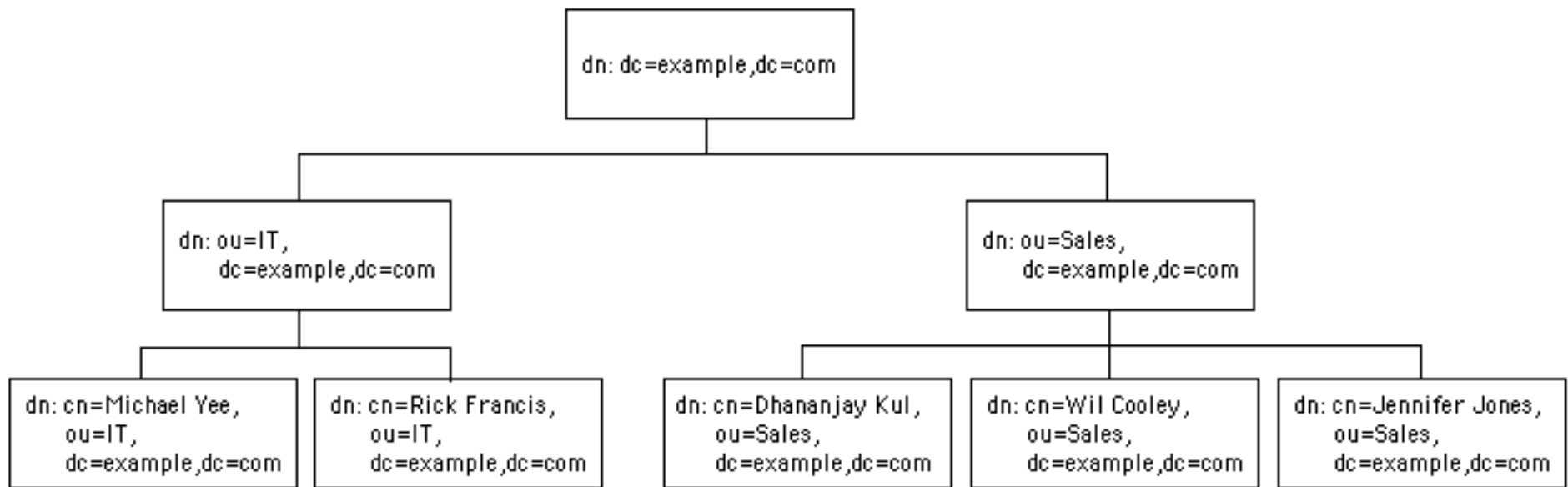
- Arbol de datos con raíz, ramas y hojas

Componentes de un directorio LDAP para una pequeña empresa



- Niveles de directorio:
 - Domain component (dc) or organization (o)
 - Organizational Unit (ou)
 - Common Names (cn)

Distinguished Names (dn)

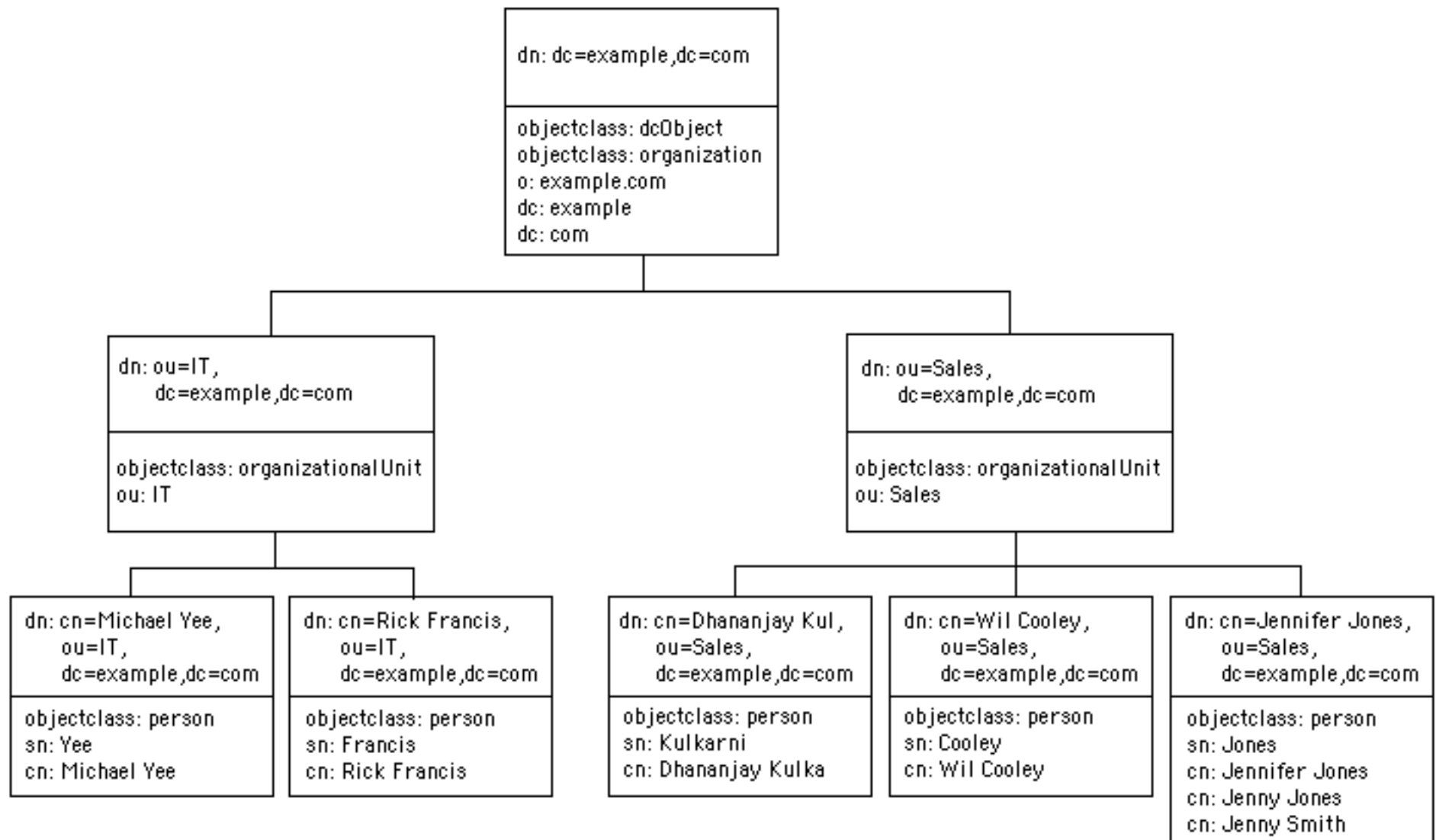


- **Distinguished name (dn)** es un nombre único en el árbol de directorios
- **dn:** dc=example, dc=com
- **dn:** ou=IT, dc=example, dc=com
- **dn:** cn=Michael Yee, ou=IT, dc=example, dc=com
- **dn:** cn=Rick Francis, ou=IT, dc=example, dc=com

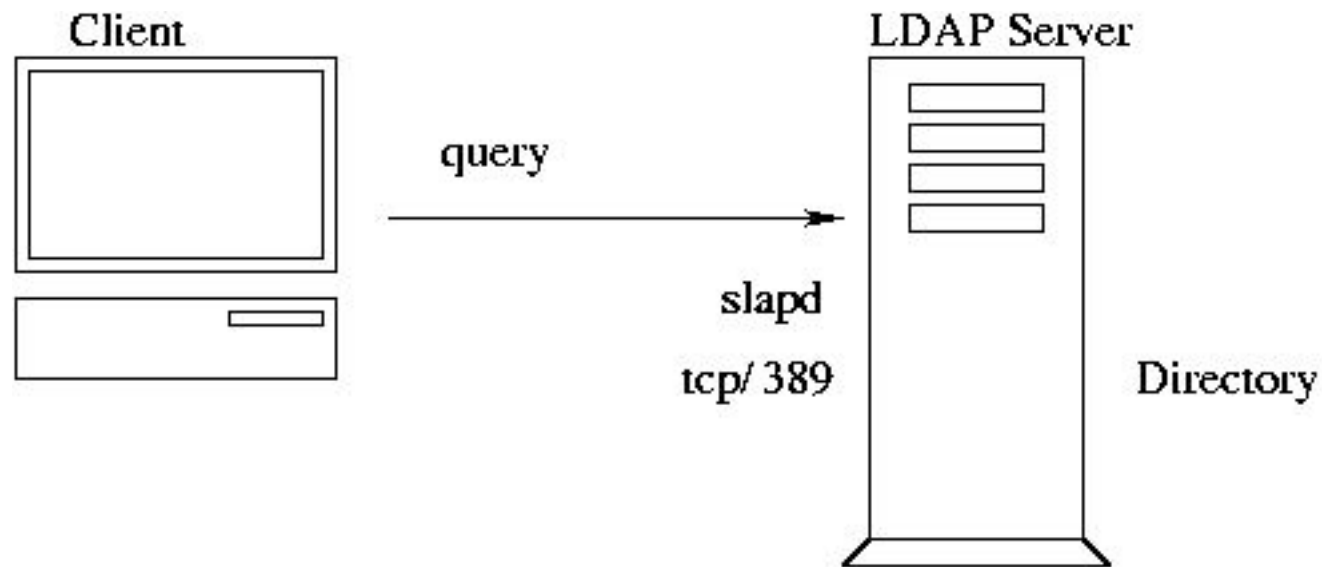
Esquemas

- Un esquema es un conjunto de reglas que describe qué clase de datos están almacenados
- Ayuda a mantener la consistencia y la calidad de los datos
- Reduce los datos duplicados
- El atributo Object Class define las reglas del esquema que la entrada debe seguir
- Un esquema contiene lo siguiente:
 - Atributos requeridos
 - Atributos permitidos
 - Cómo comparar atributos
 - Tipo de datos de los atributos (p.e., restringir a enteros, etc.)
 - Restricciones acerca de qué información se almacena (p.e., sin duplicados)

Arbol de datos con atributos dn, cn, sn y atributos Object Class



Acceso a un servidor LDAP



- Los clientes pueden consultar y modificar datos en el directorio usando comandos

Vendedores de LDAP

- OpenLDAP: gratuito
- Comerciales:
 - SunOne (iPlanet) Directory Server
 - Novell's eDirectory
 - IBM Directory Server
 - Microsoft Active Directory
 - Innosoft
 - Lotus Domino
 - Nexor
 - Critical Path

Instalación y configuración LDAP

- En un servidor: instalar los paquetes `openldap`, `openldap-servers`, `openldap-clients`, `nss_ldap`
- En un cliente: `openldap`, `openldap-clients`, `nss_ldap`

LDAP en servidor (I)

```
include          /usr/local/etc/openldap/schema/core.schema
include          /usr/local/etc/openldap/schema/cosine.schema
include          /usr/local/etc/openldap/schema/inetorgperson.schema
# Add personal schema files
#include          /usr/local/etc/openldap/schema/local.schema
database ldbm
suffix "dc=example,dc=com"
rootdn "cn=Manager,dc=example,dc=com"
rootpw secret
directory /usr/local/var/openldap-ldbm

#Below you can add Access Control directives for security

#Directives for additional databases and database groups can be added below
```

- Se modifica `/etc/openldap/slapd.conf` para definir la configuración del servidor
- Se arranca el demonio slapd (`/etc/rc.d/init.d/ldap start`)

LDAP en servidor (II)

```
# File: ldif00.ldif

# Root node
dn: dc=example,dc=com
objectclass: organization
objectclass: dcObject
o: example.com
dc: example.com

# The IT branch node
dn: ou=IT, dc=example,dc=com
objectclass: organizationalUnit
ou: IT

# The Sales branch node
dn: ou=Sales, dc=example,dc=com
objectclass: organizationalUnit
ou: Sales

# The Super-User's node
dn: cn=Manager, dc=example,dc=com
objectclass: organizationalRole
cn: Manager

# A leaf node
dn: cn=Michael Yee, ou=IT, dc=example,dc=com
objectclass: person
cn: Michael Yee
sn: Yee

# Another leaf node
dn: cn=Rick Francis, ou=IT, dc=example,dc=com
objectclass: person
cn: Rick Francis
sn: Francis

# Yet another leaf node
dn: cn=Dhananjay Kulkarni, ou=Sales, dc=example,dc=com
objectclass: person
cn: Dhananjay Kulkarni
sn: Kulkarni
```

- Se crea un fichero LDIF para añadir información
- El fichero LDIF contiene:
 - El nodo raíz
 - Los nodos rama
 - El nodo del superusuario
 - Los nodos hoja

LDAP en servidor (III)

- Se añaden las entradas a la base de datos con `ldapadd` o `ldapmodify`

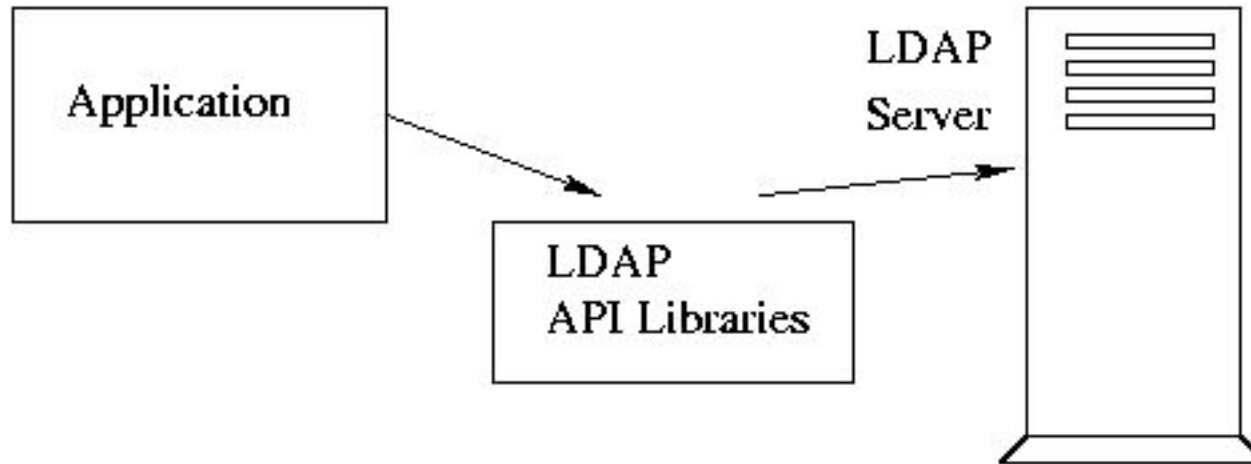
```
ldapadd -x -D "cn=Manager,dc=example,dc=com" -W -f ldif00.ldif
```

- Se pueden añadir las password de los usuarios, los discos que deben montarse, etc. Hay esquemas estándar para almacenar la información, y scripts que exportan `/etc/passwd` y otros ficheros a formato LDIF para que puedan añadirse a la base de datos

LDAP en cliente

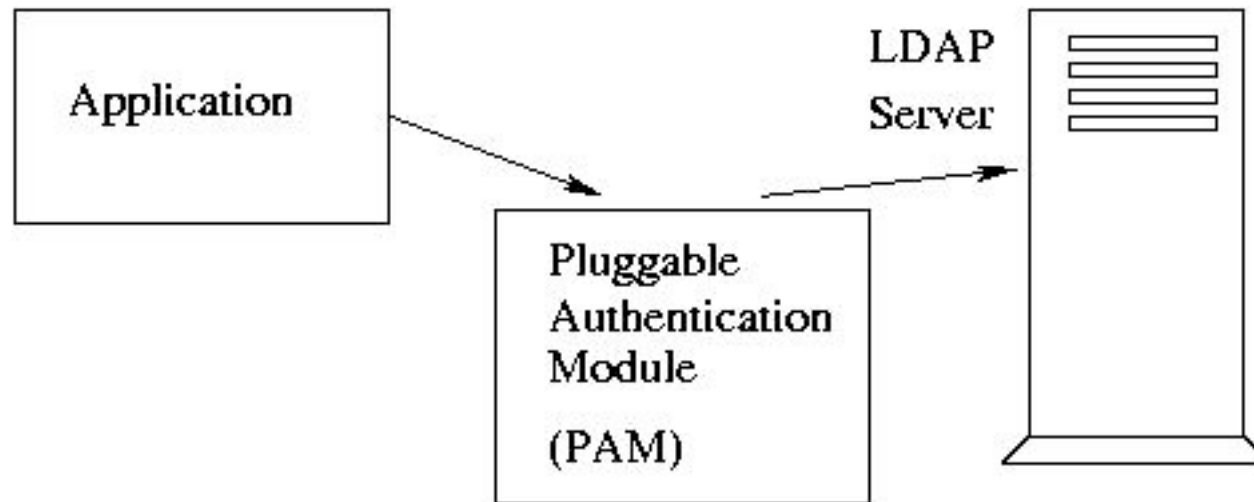
- Se modifica el fichero `/etc/openldap/ldap.conf` para que se asocie al servidor y su directorio (HOST `XX.XX.XX.XX`, BASE `dc=example, dc=com`)
- Se modifica `/etc/nsswitch.conf` para incluir ldap
- Se copian los módulos PAM necesarios (están en `/usr/share/doc/nss_ldap-226/pam.d/`) a `/etc/pam.d`
- O bien se usa la aplicación gráfica `system-config-authentication` y se indica la dirección IP del servidor LDAP y el dc base

Aplicaciones que son compatibles con LDAP



- La API de LDAP está disponible en varios lenguajes de programación (entre ellos, C, Java, Perl)

Autenticación de usuarios con LDAP



- Los módulos PAM correspondientes se usan desde las aplicaciones que hayan sido compiladas usando la API de PAM (login, rlogin, rsh, rexec, ftp, passwd, su, sudo, ssh, imap, pop3, xdm, etc.)

Kerberos: términos

- **Authentication Service (AS)** - Realiza la autenticación y es parte del Key Distribution Center (KDC).
- **Key Distribution Center (KDC)** - Mantiene las claves secretas para los "principals"; proporciona autenticación, crea y distribuye las claves de sesión. Utiliza criptografía simétrica. Un KDC tiene un Ticket Granting Service (TGS) y un Authentication Service.
- **Principal** - Cualquier objeto (usuario, aplicación, servicio o recurso) que utiliza Kerberos. Un KDC es responsable de un "reino" (realm). Cualquier principal confía en el KDC, pero los principales no confían uno en el otro. Sólo el KDC tiene una copia de la clave secreta de cada principal.
- **Reino (Realm)** - Conjunto de principales bajo responsabilidad de un KDC.
- **TGS (Ticket Granting Service)** - Parte del KDC que crea y distribuye tickets conteniendo claves de sesión a los principales
- **Ticket** - Fichas de autenticación digital enviadas desde el AS. El primer ticket enviado desde el AS a un principal se llama Ticket Granting Ticket (TGT).
- **Claves secretas y claves de sesión:** Claves de criptografía simétricas usadas para autenticación y encriptación.

Kerberos: Autenticación

- Con Kerberos, los usuarios tienen que demostrar su identidad ante cada aplicación, recurso o servicio antes de que puedan ser usados. El usuario hace login una única vez. Las fases de la autenticación son:
 1. Un usuario inicia sesión: se envía la información de la autenticación al AS (Authentication Service) del KDC (Key Distribution Center)
 2. El AS devuelve un ticket (encriptado) al computador del usuario.
 3. El ticket se descripta con la password del usuario. El usuario se autentifica ante la red si la contraseña es correcta

Kerberos: Usuario accede a recurso

1. El computador del usuario envía un ticket inicial al Ticket Granting Service (TGS) del Key Distribution Center (KDC).
2. TGS crea un nuevo ticket: Información de autenticación del usuario, más dos instancias de la misma clave de sesión. Este ticket vuelve al computador del usuario. Una instancia de la clave de sesión se encripta con la clave secreta del usuario. La otra instancia de la clave de sesión se encripta con la clave secreta del recurso deseado.
3. El software del computador del usuario (Kerberos) desencripta y extrae una instancia de la clave de sesión, inserta información de autenticación en el ticket y envía el ticket al recurso deseado. El recurso desencripta la segunda instancia de la clave de sesión con su propia clave secreta y recupera la información de autenticación del usuario.

Kerberos: Usuario accede a recurso (2)

- El recurso sabe que el ticket procede del KDC porque el ticket que ha recibido contiene una copia de la clave secreta del recurso y esa clave sólo es conocida por el KDC.
- El recurso confía en el ticket recibido porque contiene la clave secreta encriptada.
- El recurso compara también la información de usuario en el ticket con la información insertada por el usuario para asegurarse de que la identidad del usuario no ha sido suplantada.

Autenticación Kerberos



Cliente

Username: EPIGijon
Password: mipass

one way hash



Clave secreta del cliente



Authentication Server



Ticket Granting Server

Key Distribution Center



Servidor de archivos

2. AS comprueba si EPIGijon
está en la base de datos



Cliente



AS

3. AS genera una clave
secreta para EPIGijon



TGS

1. EPIGijon quiere acceder
al servidor de archivos



Servidor de Archivos



Cliente

1. Clave Sesión Cliente/TGS
(encriptada con la clave
secreta del cliente)



2. Ticket Granting Ticket: incluye
Client ID
Client network address
Ticket validity period
clave de sesión Client/TGS
(encriptado con la
clave secreta TGS)



AS



TGS



Servidor de Archivos



Cliente

Cliente decodifica
mensaje 1 y obtiene
clave de Sesión Cliente/TGS
Cliente no puede decodificar
mensaje 2
(no tiene la clave secreta TGS)



AS



TGS



Servidor de Archivos



Cliente



AS

3. Devuelve Ticket Granting Ticket
a partir del mensaje 2
(estaba encriptado con la clave secreta TGS) +
ID del servicio de archivos



4. Autenticador compuesto de
Client ID
Timestamp
(encriptado con la clave
Client/TGS del mensaje 1)



TGS



Servidor de Archivos



Cliente

TGS decodifica el mensaje 3
y obtiene el granting Ticket
(incluye Client ID,
Client Network address,
ticket validity period,
clave de sesión Client/TGS)

Ahora el cliente y el TGS
pueden hablar porque ambos
tienen la clave de sesión
Client/TGS



AS



TGS



Servidor de Archivos



Cliente

TGS decodifica el mensaje 4
usando la clave de sesión
Client/TGS
y obtiene
Client ID +
Timestamp
(con esto conoce cuándo
el cliente envió la solicitud)

TGS comprueba que Client ID
del mensaje 3 coincide con
Client ID de mensaje 4 y que
timestamp no excede el
periodo de validez del ticket



AS



TGS



Servidor de Archivos

5. Cliente-a-FS ticket:

Client ID

Network address

Validity Period

clave de sesión Cliente/Servidor
(Encriptado con la clave

secreta del

Servidor de Archivos,

sólo el FS puede decodificarlo)

6. Clave de sesión Cliente/Servidor
(encriptada con la clave de sesión
Cliente/TGS del mensaje 1)

Cliente



AS



TGS



Servidor de Archivos



Cliente

Decodifica mensaje 6
usando la clave de sesión Cliente/TGS
y obtiene la clave de sesión
Cliente/Servidor



AS



TGS



Servidor de Archivos

5. Cliente-a-FS ticket:

Client ID

Network address

Validity Period

clave de sesión Cliente/Servidor

(Encriptado con la clave
secreta del

Servidor de Archivos)

7. Autenticador, compuesto de

Client ID

Timestamp

(encriptado con la clave Cliente/Servidor
de 6)



Cliente



AS



TGS



Servidor de Archivos

Servidor de Archivos descripta (5) usando
la clave secreta del servidor de archivos
y obtiene

Client ID

Network Address

Validity Period

Clave de Sesión Cliente/Servidor



AS



TGS

Servidor de Archivos descripta (7)
usando la clave Cliente/Servidor
y obtiene

Client ID

Timestamp



Servidor de Archivos



Cliente

Servidor de Archivos comprueba que
Client ID de (5) = Client ID de (7)
y ticket no expiró (timestamp)

Servidor de Archivos envía al cliente un mensaje para comprobar su identidad y mostrar que puede realizar la petición

8: Timestamp (en 7) + 1
encriptada con la clave
de sesión Cliente/Servidor

Cliente descripta 8
y comprueba que
timestamp + 1 es correcto,
con lo que el cliente confía
en el servidor de archivos



Cliente



AS



TGS

Servidor de Archivos





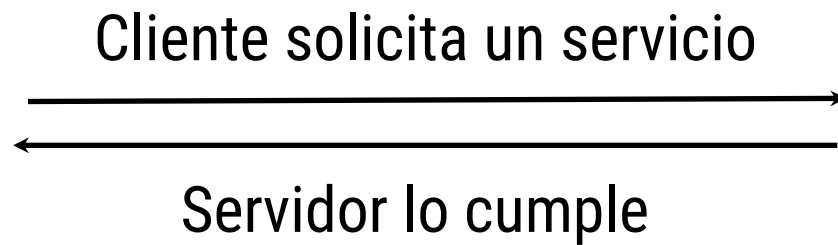
AS



TGS



Cliente



Servidor de Archivos



Directorio Activo - Active Directory Domain Services

- **Servicios de Dominio del Directorio Activo** es el nombre que recibe el conjunto de elementos que globalmente constituyen el servicio de directorio en dominios Windows Server 2008. Este servicio almacena información acerca de los recursos disponibles en el dominio y permite el acceso controlado de los usuarios y aplicaciones a dichos recursos.
- Al instalar el Directorio Activo en sistemas Windows Server 2008 convertimos a dichos sistemas en los **servidores del dominio**, o más correctamente, en los denominados Controladores de Dominio (Domain Controllers, o "DCs"). El resto de los equipos de la red pueden convertirse entonces en los clientes de dicho servicio de directorio, también denominados miembros del dominio, con lo que pueden consultar toda la información almacenada en los DCs.
- Esta información incluye las cuentas de usuario, grupo, ordenador, etc., así como otras características propias de sistemas Windows Server, como directivas de usuario o equipo, relaciones de confianza, aspectos sobre la replicación de datos entre servidores, etc.

Directorio Activo: estructuras lógica y física de red

- Directorio Activo separa conceptualmente la estructura lógica de la organización (dominios) de su estructura física (topología de red). Esto permite:
 - Independizar la estructuración de dominios de la organización de la topología de la red o redes que interconectan los sistemas
 - Administrar la estructura física explícitamente, de forma independiente de la administración de los dominios.

Directorio Activo: Servicios y estándares de red relacionados

- **DHCP** (Dynamic Host Configuration Protocol). Protocolo de configuración dinámica de ordenadores, que permite la administración desatendida de características de red.
- **DNS** (Domain Name System). Servicio de nombres de dominio que permite la administración de los nombres de ordenadores. Este servicio constituye el mecanismo de asignación y resolución de nombres (traducción de nombres simbólicos a direcciones IP) en Internet.
- **SNTP** (Simple Network Time Protocol). Protocolo simple de tiempo de red, que permite disponer de un servicio de sincronización de tiempo entre sistemas conectados por red.
- **LDAP** (Lightweight Directory Access Protocol). Protocolo ligero (o compacto) de acceso a directorio. Este es el protocolo mediante el cual las aplicaciones acceden para leer o modificar la información existente en la base de datos del directorio.
- **Kerberos V5**. Protocolo utilizado para la autenticación de usuarios y máquinas.
- **Certificados X.509**. Estándar que permite distribuir información a través de la red de una forma segura.

Directorio Activo y DNS

- DNS es el sistema de nombres usado en redes basadas en el protocolo TCP/IP. Windows Server 2008 utiliza DNS para localizar a otros ordenadores en la red.
- Cada dominio Windows Server 2008 se identifica mediante un nombre de dominio DNS (por ejemplo, miempresa.com). Cada ordenador basado en Windows Server que forma parte de un dominio tiene un nombre DNS cuyo sufijo es precisamente el nombre DNS de dicho dominio (siguiendo con el ejemplo, un ordenador de dicho dominio podría denominarse pc0100.miempresa.com). De esta forma, los dominios y ordenadores que se representan como objetos en Active Directory, són también nodos en DNS.
- Ambos espacios de nombres comparten idénticos nombres de dominio. La diferencia es que aunque comparten la misma estructura, almacenan información diferente: DNS almacena zonas y registros de recursos y el Directorio Activo almacena dominios y objetos de dominio.

Uso de DNS en Directorio Activo

- **Resolución de nombres:** DNS es el mecanismo por defecto de resolución de nombres en dominios Windows Server 2008, permitiendo localizar por nombre a los ordenadores de la red (al traducir nombres a direcciones IP).
- **Definición del espacio de nombres:** el Directorio Activo utiliza las convenciones de nomenclatura de DNS para asignar nombres a los dominios. Es decir, los dominios Windows Server 2008 se nombran necesariamente mediante nombres de dominio DNS.
- **Búsqueda de los componentes físicos de AD:** para iniciar una sesión de red o realizar consultas al Directorio Activo, los sistemas Windows miembros de un dominio deben encontrar primero a alguno de los DCs del dominio, y para ello realizan consultas DNS. Por tanto, debe existir un servidor DNS disponible que incluya la información necesaria para responder estas consultas. Más adelante se verá que esta información se almacena en DNS mediante registros de recursos SRV que especifican el servidor (o servidores) del dominio que proporcionan los servicios de directorio correspondientes (LDAP, Kerberos, catálogo global, etc.).

Active Directory: Evolución histórica

- En Windows NT 4.0, los dominios se representaban con nombres NetBIOS de 15 caracteres, que se registraban en una base de datos única, llamada Security Accounts Manager (SAM), que gestionaba usuarios, grupos y políticas.
- Esta base de datos se almacenaba en un servidor llamado Primary Domain Controller (PDC)

Active Directory: Evolución histórica

- Para evitar depender de un único equipo, existía un segundo tipo de servidor, el Backup Domain Controller (BDC), que almacenaba una versión de sólo lectura de la base de datos SAM.
- Los usuarios podían usar la BDC para autenticarse en un dominio o para determinar información relacionada con su cuenta o grupo, pero todos los cambios debían hacerse en el PDC

Sincronismo

- En este modelo, el PDC periódicamente actualiza la base de datos de los BDC para mantenerlos sincronizados.
- Si el PDC falla, uno de los BDC puede ser promovido a PDC, pero en el tiempo intermedio la SAM es de sólo lectura.

Modelo W2008

- En W2003 y superiores no se usa NetBIOS, sino DNS (p.e., en lugar de GRUPOASR se podría usar ASR.GRUPO.ES). Sin embargo, está permitido usar el nombre NetBIOS para referirse a un dominio.
- El concepto de SAM no existe: la información acerca de los usuarios, passwords y grupos se almacena en Active Directory: los servidores deben proporcionar el servicio LDAP que se usa para interaccionar con Active Directory.

Modelo W2003 y superiores


- A partir de W2003, los servidores que ofertan el servicio LDAP son los controladores de dominio.
- Al no existir los BDC/PDC, todos los controladores son iguales, y esta igualdad se mantiene mediante el proceso de *multi-master replication*, que se asegura de que los cambios en un objeto en uno de los controladores se repliquen a todos los controladores de dominio con los que haya una relación de confianza.

Modelo mixto

- Para que las redes puedan actualizarse gradualmente, se permite que los controladores BDC (pero no los PDC) convivan en una red W200X. Estos BDC dependen de un W200X que hace las funciones de PDC. Este controlador desempeña el papel de Flexible Single Master Operations (FMSO)
- En el modelo mixto, se usa NetBIOS o bien Active Directory, donde los clientes hacen consultas al servidor DNS del tipo _1dap._tcp.<nombredominio>, por lo que los controladores de dominio corren el DNS localmente.


Administre su servidor

Administre su servidor

Buscar en el Centro de ayuda y 

Dominios y confianzas de Active Directory

Archivo Acción Ver Ayuda



Dominios y confianzas de Active Dire

aso.local

Nombre	Tipo
aso.local	domainDNS

Cambiar el maestro de operaciones

El maestro de operaciones de nombres de dominio le garantiza nombres de dominio únicos. Sólo hay un controlador de dominio de la organización que realice esta función.

Maestro de operaciones de nombres de dominio:

servidor.aso.local

Para transferir al siguiente equipo la función de atribución de nombres de dominio, haga clic en Cambiar.

servidor.aso.local

Cambiar...

Cerrar

Schema

- Cada objeto en Active Directory es parte de una base de datos LDAP asociada a un *esquema* que define los atributos de cada objeto y las clases de objetos.
- El esquema se almacena en un fichero de texto SCHEMA.INI

schema.ini - Bloc de notas

Archivo Edición Formato Ver Ayuda

```
NTSecurityDescriptor=0:SYG:SYD:P(A;;;RPWPCCDCLCSWRCWDWOSD;;;SY)(A;;;RPLC;;;BA)
objectClass =container
ObjectCategory =container
description=Default container for deleted objects
showInAdvancedviewOnly=True
isDeleted=True
isCriticalsystemObject=True
;systemFlags=FLAG_CONFIG_DISALLOW_RENAME      |
;                FLAG_CONFIG_DISALLOW_MOVE      |
;                FLAG_DISALLOW_DELETE
systemFlags=0x8C000000

[Users]
NTSecurityDescriptor=0:DAG:DAD:(A;;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;;RPWPCRCCDCLCLORCWOWDSW;;;
objectClass =Container
ObjectCategory =Container
description=Default container for upgraded user accounts
showInAdvancedviewOnly=False
isCriticalsystemObject=True
;systemFlags=FLAG_CONFIG_DISALLOW_RENAME      |
;                FLAG_CONFIG_DISALLOW_MOVE      |
;                FLAG_DISALLOW_DELETE
systemFlags=0x8C000000

[Computers]
NTSecurityDescriptor=0:DAG:DAD:(A;;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;;RPWPCRCCDCLCLORCWOWDSW;;;
objectClass =Container
ObjectCategory =Container
description=Default container for upgraded computer accounts
showInAdvancedviewOnly=False
isCriticalsystemObject=True
;systemFlags=FLAG_CONFIG_DISALLOW_RENAME      |
;                FLAG_CONFIG_DISALLOW_MOVE      |
;                FLAG_DISALLOW_DELETE
systemFlags=0x8C000000

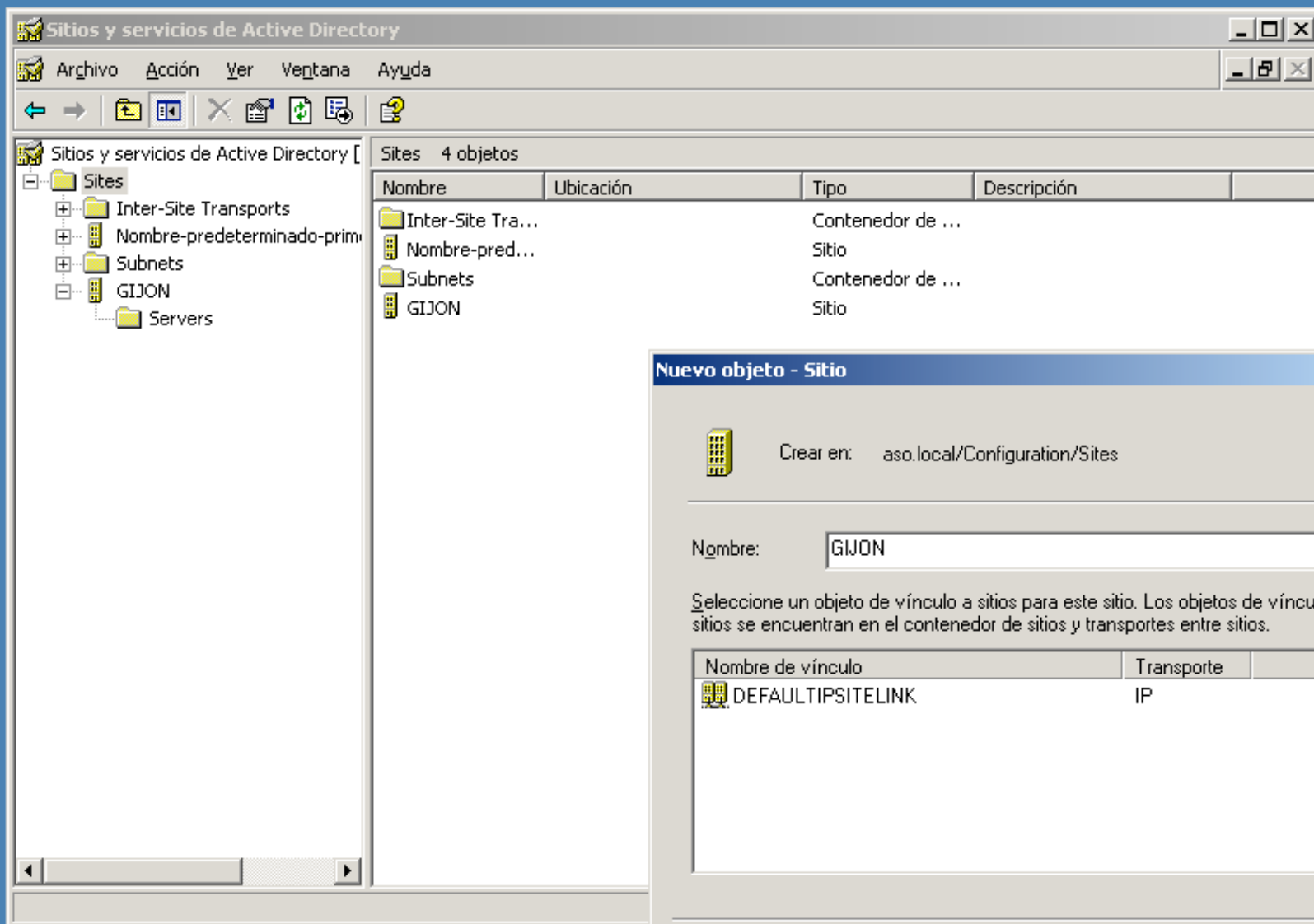
[System]
NTSecurityDescriptor=0:DAG:DAD:(A;;;RPLCLORC;;;AU)(A;;;RPWPCRCLCLOCCRCWDWOSW;;;DA)(A;;;RPWPCRCLCLOCC
objectClass =Container
ObjectCategory =Container
description=Builtin system settings
showInAdvancedviewOnly=True
isCriticalsystemObject=True
;systemFlags=FLAG_CONFIG_DISALLOW_RENAME      |
```

Catálogo global

- El catálogo global contiene todas las entradas para todos los objetos en un bosque de Directorio Activo (una colección de árboles de dominios). Consta de las definiciones completas de los objetos en su dominio y de un subconjunto parcial de las propiedades de los otros objetos del bosque.
- Los servidores que almacenan copias del catálogo global se llaman *servidores de catálogo global*. Todos ellos son también controladores de dominio.

Sites

- Los sitios (*sites*) son grupos de equipos que están físicamente próximos, y enlazados con otros por medio de conexiones WAN.
- La definición de sitios permite aprovechar mejor la red en la replicación de los controladores de dominio



Unidades organizativas

- Las unidades organizativas pueden contener otras unidades organizativas, grupos, usuarios y computadores
- Las OU pueden anidarse para crear una jerarquía similar a la estructura de la empresa
- Las OU permiten delegar la autoridad, haciendo que un usuario (o grupo) asuma ciertas tareas administrativas en la OU sin necesidad de darle control sobre el dominio

Usuarios y equipos de Active Directory

Archivo Acción Ver Ventana Ayuda

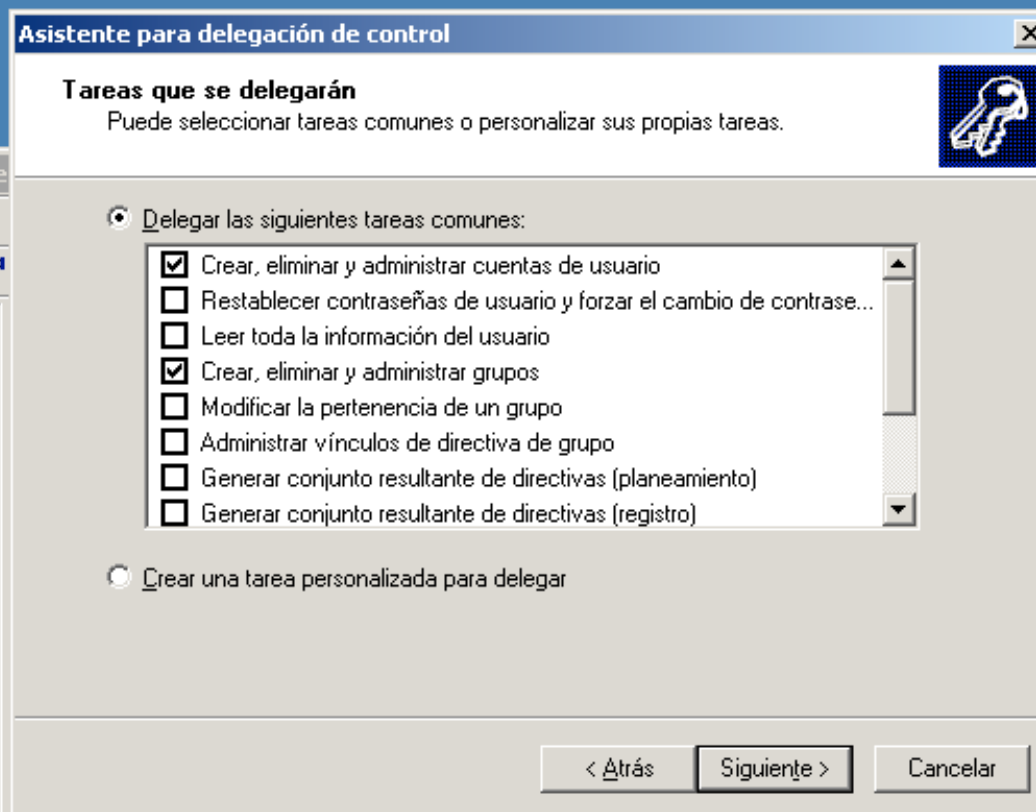
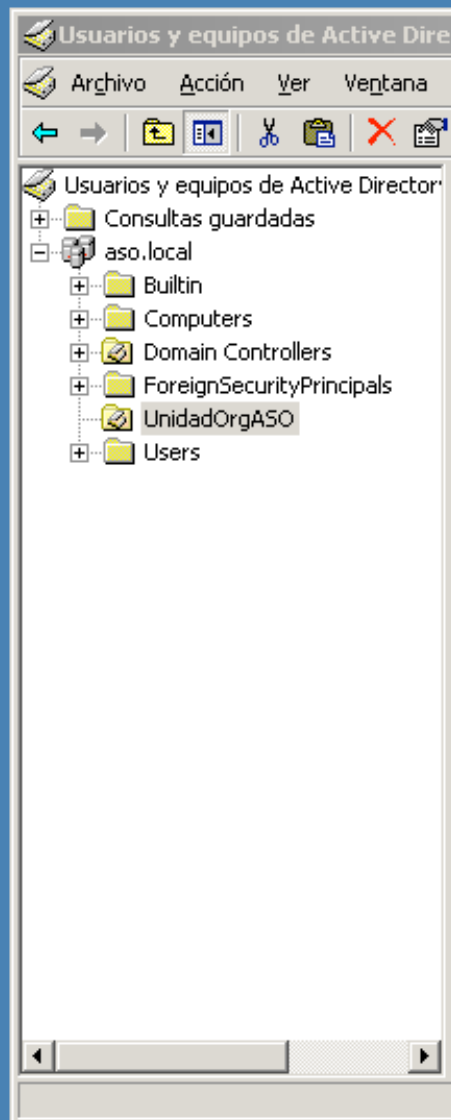
Usuarios y equipos de Active Director UnidadOrgASO 4 objetos

Consultas guardadas
aso.local
 Builtin
 Computers
 Domain Controllers
 ForeignSecurityPrincipals
 UnidadOrgASO
 Users

Nombre	Tipo	Descripción
asoadmin	Usuario	
empleadoaso	Usuario	
GrupoGlobal	Grupo de seguri...	
GrupoGlobal...	Grupo de seguri...	

- Delegar control...
- Mover...
- Buscar...
- Nuevo
- Todas las tareas
- Ver
- Nueva ventana desde aquí
- Cortar
- Eliminar
- Cambiar nombre
- Actualizar
- Exportar lista...
- Propiedades
- Ayuda

Delega el control de objetos en esta carpeta



Administración de AD

- Para crear y mantener objetos de Active Directory, se usa una consola MMC, o se lanza directamente el complemento “Usuarios y equipos de Active Directory”
- Las categorías de los contenedores son: builtin (antiguos grupos NT 4.0), Computers (cuentas de equipo que no están en unidades organizativas), Domain Controllers (una unidad organizativa que contiene a todos los controladores de dominio) y Users (usuarios que no están en otras OU)

Usuarios y equipos de Active Directory

Archivo Acción Ver Ventana Ayuda

Usuarios y equipos de Active Director: UnidadOrgASO 4 objetos

- Consultas guardadas
- aso.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - UnidadOrgASO**
 - Users

Nombre	Tipo	Descripción
asoadmin	Usuario	
empleadoaso	Usuario	
GrupoGlobal	Grupo de seguri...	
GrupoGlobalL...	Grupo de seguri...	

Usuarios y equipos de Active Directory

Archivo Acción Ver Ventana Ayuda

Usuarios y equipos de Active Director: Built-in 16 objetos

Nombre	Tipo	Descripción
Acceso compatible con versio...	Grupo de seguridad - Domini...	Un grupo de compatibilida...
Administradores	Grupo de seguridad - Domini...	Los administradores tiene...
Creadores de confianza de b...	Grupo de seguridad - Domini...	Los miembros de este gru...
Duplicadores	Grupo de seguridad - Domini...	Pueden replicar archivos e...
Grupo de acceso de autorizac...	Grupo de seguridad - Domini...	Los miembros de este gru...
Invitados	Grupo de seguridad - Domini...	Los invitados tienen prede...
Operadores de configuración ...	Grupo de seguridad - Domini...	Los miembros en este equi...
Operadores de copia	Grupo de seguridad - Domini...	Los operadores de copia p...
Oper. de cuentas	Grupo de seguridad - Domini...	Pueden administrar cuent...
Oper. de impresión	Grupo de seguridad - Domini...	Pueden administrar impres...
Oper. de servidores	Grupo de seguridad - Domini...	Los miembros pueden adm...
Servidores de licencias de Ter...	Grupo de seguridad - Domini...	Servidores de licencias de ...
Usuarios	Grupo de seguridad - Domini...	Los usuarios no pueden h...
Usuarios de escritorio remoto	Grupo de seguridad - Domini...	A los miembros de este gr...
Usuarios del monitor de sistema	Grupo de seguridad - Domini...	Los miembros de este gru...
Usuarios del registro de rendi...	Grupo de seguridad - Domini...	Los miembros de este gru...



Papelera de
reciclaje

Usuarios y equipos de Active Directory

Archivo Acción Ver Ventana Ayuda

← → ↗ ↘ ↙ ↚ ↛ ↜ ↝ ↞ ↠ ↡ ↢ ↣ ↤ ↥ ↦ ↧ ↨ ↩ ↪ ↫ ↬ ↭ ↮ ↯ ↰ ↱ ↲ ↳ ↴ ↵ ↶ ↷ ↸ ↹ ↺ ↻ ↼ ↽ ↾ ↿ ⇀ ⇁ ⇂ ⇃ ⇄ ⇅ ⇆ ⇇ ⇈ ⇉ ⇊ ⇋ ⇌ ⇍ ⇎ ⇏ ⇐ ⇑ ⇒ ⇓ ⇔ ⇕ ⇖ ⇗ ⇘ ⇙ ⇚ ⇛ ⇜ ⇝ ⇞ ⇟ ⇠ ⇡ ⇢ ⇣ ⇤ ⇥ ⇦ ⇧ ⇨ ⇩ ⇪ ⇫ ⇬ ⇭ ⇮ ⇯ ⇰ ⇱ ⇲ ⇳ ⇴ ⇵ ⇶ ⇷ ⇸ ⇹ ⇺ ⇻ ⇼ ⇽ ⇾ ⇿ ⇰ ⇱ ⇲ ⇳ ⇴ ⇵ ⇶ ⇷ ⇸ ⇹ ⇺ ⇻ ⇼ ⇽ ⇾ ⇿

Usuarios y equipos de Active Director

- Consultas guardadas
- aso.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - UnidadOrgASO
 - Users

Computers 1 objetos

Nombre	Tipo	Descripción
CLIENTE	Equipo	

Usuarios y equipos de Active Directory

Archivo Acción Ver Ventana Ayuda

← → ↗ ↘ ↙ ↚ ↛ ↜ ↝ ↞ ↠ ↡ ↢ ↣ ↤ ↥ ↦ ↧ ↨ ↩ ↪ ↫ ↬ ↭ ↮ ↯ ↰ ↱ ↲ ↳ ↴ ↵ ↶ ↷ ↸ ↹ ↺ ↻ ↼ ↽ ↾ ↿ ⇀ ⇁ ⇂ ⇃ ⇄ ⇅ ⇆ ⇇ ⇈ ⇉ ⇊ ⇋ ⇌ ⇍ ⇎ ⇏ ⇐ ⇑ ⇒ ⇓ ⇔ ⇕ ⇖ ⇗ ⇘ ⇙ ⇚ ⇛ ⇜ ⇝ ⇞ ⇟ ⇠ ⇡ ⇢ ⇣ ⇤ ⇥ ⇦ ⇧ ⇨ ⇩ ⇪ ⇫ ⇬ ⇭ ⇮ ⇯ ⇰ ⇱ ⇲ ⇳ ⇴ ⇵ ⇶ ⇷ ⇸ ⇹ ⇺ ⇻ ⇼ ⇽ ⇾ ⇿ ⇰ ⇱ ⇲ ⇳ ⇴ ⇵ ⇶ ⇷ ⇸ ⇹ ⇺ ⇻ ⇼ ⇽ ⇾ ⇿

Usuarios y equipos de Active Director

- Consultas guardadas
- aso.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - UnidadOrgASO
 - Users

UnidadOrgASO 4 objetos

Nombre	Tipo	Descripción
asoadmin	Usuario	
empleadoaso	Usuario	
GrupoGlobal	Grupo de seguri...	
GrupoGlobalL...	Grupo de seguri...	

Creación de objetos

- Para crear objetos de directorio (usuarios, grupos, etc.) se usa el menú contextual asociado al contenedor correspondiente

Usuarios y equipos de Active Directory

Archivo Acción Ver Ventana Ayuda

Usuarios y equipos de Active Director

- Consultas guardadas
- aso.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - UnidadOrgASO
 - Us...

Users 14 objetos

Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta para la administra...
Administrador...	Grupo de seguri...	Administradores designad...
Administrador...	Grupo de seguri...	Administradores designad...
Admins. del d...	Grupo de seguri...	Administradores designad...
Controladore...	Grupo de seguri...	Todos los controladores d...
DnsAdmins	Grupo de seguri...	Grupo de administradores ...
UpdatePr...	Grupo de seguri...	Cientes DNS que tienen p...
pos del d...	Grupo de seguri...	Todas los servidores y est...
		Cuenta para acceso como...
		.. Todos los invitados del do...
		.. Los miembros de este gru...
		.. Los miembros de este gru...
		.. Los servidores de este gr...
		.. Todos los usuarios del do...

Delegar control...
Buscar...

Nuevo
Todas las tareas
Ver
Nueva ventana desde aquí
Actualizar
Exportar lista...
Propiedades
Ayuda

Equipo
Contacto
Grupo
InetOrgPerson
Alias de cola de MSMQ
Impresora
Usuario
Carpeta compartida

Crea un objeto nuevo en este contenedor.



Usuarios y equipos de Active Directory

Archivo Acción Ver Ventana Ayuda

Usuarios y equipos de Active Director

- Consultas guardadas
- aso.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - UnidadOrgASO
 - Users

Users 14 objetos

Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta para la administra...
Administrador...	Grupo de seguri...	Administradores designad...
Administrador...	Grupo de seguri...	Administradores designad...
Admins. de		
Controlado		
DnsAdmins		
DnsUpdate		
Equipos de		
Invitado		
Invitados		
Propietario		
Publicador		
Servidores		
Usuarios d		

Nuevo objeto - Usuario

Crear en: aso.local/Users

Nombre: Iniciales:

Apellidos:

Nombre completo:

Nombre de inicio de sesión de usuario:
 @aso.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000):

< Atrás Siguiente > Cancelar

Grupos

- Un grupo es una colección de usuarios. Hay dos tipos diferentes de grupos:
 - Grupos de seguridad: Asignan permisos y derechos a los objetos y recursos de Active Directory
 - Grupos de distribución: Para enviar correo a todos los miembros del grupo

Ambito

- Ambos grupos pueden tener los siguientes ámbitos:
 - Grupos globales: Existen en el dominio. En modo 200X, pueden contener otros grupos globales.
 - Grupos locales de dominio: Existen en un único computador, no son visibles desde el dominio. Pueden incluir grupos globales, cuentas y grupos universales en modo 200X
 - Grupos universales: se extienden a todos los dominios del bosque

Forma de usar los grupos

- Aunque esto no es obligatorio, la práctica habitual es:
 - En cada equipo hay diferentes grupos locales, cada uno de los cuales tiene diferentes niveles de acceso a los recursos de ese equipo.
 - Todos los usuarios pertenecen a grupos globales o a grupos universales.
 - Los grupos globales o universales son miembros de los grupos locales.

Grupos

- Un usuario puede ser miembro de múltiples grupos locales o universales
- Un grupo global o universal puede ser miembros de varios grupos locales
- Un recurso puede tener asignados varios grupos locales, con permisos para leer, imprimir, control total, etc.

Perfiles

- El perfil de usuario es el conjunto de ajustes de entorno, red, escritorio, etc. que definen:
 - la configuración del menú inicio
 - el escritorio, salvapantallas, etc.
 - los bookmarks del navegador
 - las impresoras y discos de red
 - etc.

Perfiles

- Adicionalmente, el perfil incluye una copia de HKEY_CURRENT_USER en el fichero NTUSER.DAT
- Los perfiles pueden ser locales o móviles. Un perfil móvil se almacena en un disco de red, de forma que es accesible desde cualquier equipo en que se inicie sesión
- Un perfil local puede convertirse a móvil

Propiedades del sistema ? X

General Nombre de equipo Hardware
Opciones avanzadas Actualizaciones automáticas Acceso remoto

Debe iniciar la sesión como un Administrador para hacer la mayoría de los cambios.

Rendimiento
Efectos visuales, programación del procesador, uso de memoria y memoria virtual
[Configuración](#)

Perfiles de usuario
Configuración del escritorio relacionada con su inicio de sesión
[Configuración](#)

Inicio y recuperación
Inicio de sistema, error de sistema e información de depuración
[Configuración](#)

[Variables de entorno](#) [Informe de errores](#)

[Aceptar](#) [Cancelar](#) [Aplicar](#)

Perfiles de usuario ? X

Los perfiles del usuario contienen la configuración de escritorio y otro tipo de información relacionada con su cuenta de usuario. Se puede crear un perfil diferente en cada equipo o seleccionar el mismo perfil móvil para todos los equipos que se utilicen

Perfiles almacenados en este equipo:

Nombre	Tamaño	Tipo	Estado	Mo...
ASO\Administrador	607 KB	Local	Local	21...

[Cambiar tipo](#) [Eliminar](#) [Copiar a](#)

[Haga clic aquí](#) para crear cuentas de usuario.

[Aceptar](#) [Cancelar](#)

Cambiar tipo de perfil ? X

Cuando ASO\Administrador inicie sesión en este equipo, ¿debe el sistema operativo usar el perfil de acceso móvil o tan sólo la copia en caché local del perfil móvil?

☐ Perfil móvil
☒ Perfil local

[Aceptar](#) [Cancelar](#)