# Redes, sus elementos fundamentales y seguridad

**En este artículo veremos un panorama general de los elementos básicos en los que se basan las redes de computadoras hoy. Muchas tecnologías entran en juego y durante las próximas apariciones de NEX discutiremos detalles de cada una de ellas.**

(Para complementar éste artículo los invitamos a ver una excelente presentación en video (de 12 minutos) donde se ejemplifica todo el proceso de uso de TCP / IP en redes). (download: www.warriorsofthe.net)

**1- Qué beneficio obtenemos en tener una red?**

Respuesta: Tener máquinas en red nos ayuda resolver un gran número de problemas.
El fin último de cualquier proyecto de redes es la de proveer algún tipo de servicio. Ejemplos:
-Necesito ver la página web de Ovis Link para conocer los precios de routers, hubs, switches, productos wireless. Existe un Web Server que aloja las páginas del dominio ovislink.com
-Necesito enviar un e-mail. Deberá existir un mail server y deberé ejecutar una aplicación cliente que me envíe y reciba una posible respuesta.
-Necesito compartir archivos y carpetas a toda mi empresa. Y, que estén en un solo server (file server) de modo de centralizar los back-ups.
-Necesito comprar una flauta travesera de plata: www.ebay.com y tipear ¨traverse flutes¨.

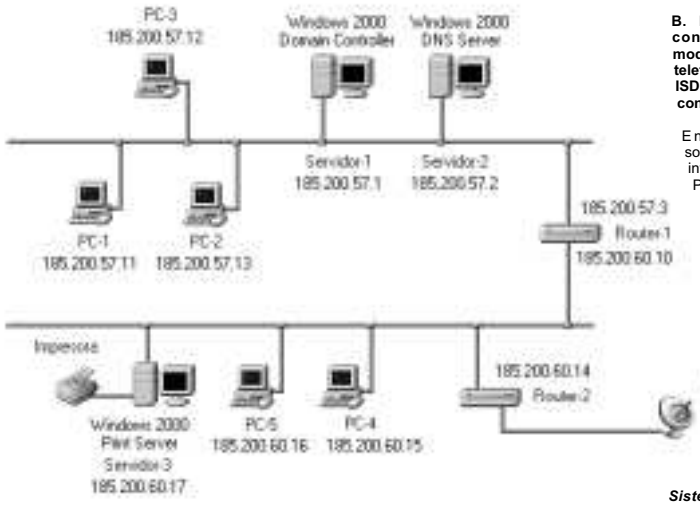
**2. Cuáles son los elementos fundamentales en una red ?**

**A. Todo tipo de servicio de red necesita un server-software y un client-software. Relación ¨cliente servidor¨ entre maquinas.**

Conectamos las máquinas en red con un propósito: la computadora que actúa como cliente se beneficia de las computadoras que actúan como servidores: (ver figura)

-En la maquina cliente debe correr un programa que sepa solicitar un servicio y saber como recibir y mostrar lo que recibió: "aplicación cliente"
-Necesito en el servidor un programa que esté atento y sepa escuchar pedidos y enviar la información solicitada: "aplicación servidor"
Un ejemplo muy popular es el de Web browser (cliente) web server (servidor):
Si quiero ver la página web del periódico NEX utilizo mi "web-browser" (cliente web) y en algún lugar tipeo: http://www.nexweb.com.ar (http hipertext transfer protocol, es el protocolo que permite transferir hipertexto)
He dicho a la red: "quiero la página web de www.nexweb.com.ar que esta alojada en algún servidor." En nuestro caso no está en las oficinas de NEX sino en un proveedor de web-hosting (towebs)
Los paquetes saben encontrar donde esta el servidor. Cómo?

Se lo preguntan al servidor DNS: "cuál es el número IP del servidor (llamado www) que aloja la página web de nexweb.com.ar". DNS devuelve el IP correcto y los paquetes con el pedido viajan hasta la máquina con ese IP. El web-server (servidor) que está constantemente "escuchando" (tiene corriendo un pequeño programa llamado daemon, demonio), toma el pedido y envía, por ejemplo, el archivo index.html. El cliente lee el html y me lo muestra en pantalla
***Web-browsers más conocidos*: netscape, mozilla , internet explorer.**




***Web-servers más conocidos*: apache (normalmente bajo Linux) e IIS (Internet Information Server) solo trabaja bajo Windows.**

Otros tipos de servidores incluyen: file servers (servidores para compartir archivos); print servers (servidores de impresión); E-Mail servers; Servers de Negocios online (E-commerce).

**B. Las redes necesitan hardware para conectarse (switches, hubs, routers, modems) y conexiones (cables de red, líneas telefónicas, frame relay, DSL, cable modem, ISDN y otros). Sino los clientes NO pueden conectarse a los servidores.**

En la figura vemos un esquema sobresimplificado de una LAN con conexión a internet.
Por ejemplo la subnet (red) 192.168.57.0 se conecta con 192.168.60.0 a través de un router (Router 1) El router tiene dos interfases (una en cada subnet). Las máquinas de cada subnet están conectadas por un hub o switch.
La conexión a internet la realiza un Router 2.


**C. Los clientes y servidores deben hablar los mismos protocolos de red.**

Las máquinas (sus sistemas operativos) deben hablar el mismo "idioma de red" (network transport protocol)

***Sistemas operativos más usados*: UNIX, Windows, Linux, Novell**

Han existido diversos protocolos de comunicación:
-NetBEUI (Network Basic Input /Output System Extended User Interfase). Un Viejo protocolo de Microsoft /IBM/ Sytex usado para soportar pequeñas redes).
-IPX / SPX (Internet Packet Exchange / Sequenced Packet Exchange) el protocolo que Novell NetWare utilizó durante muchos años.
-TCP / IP (Transmition Control Protocol/ Internet Protocol) el protocolo casi universal utilizado hoy.

Si TCP/IP es nuestro protocolo de comunicación, utilizaremos ciertos servidores fundamentales para soportar su implementación:

-Servidor DNS (Domain Naming System) que conoce los nombres de las computadoras en la red y nos traduce a su numero IP

-Servidor DHCP (Dynamic Host Configuration Protocol) nos ayuda a configurar las maquinas de nuestra red con su configuración IP
-WINS (Windows Internet Name Service) hace algo parecido a DNS pero sobre los nombres Net BIOS de nuestras maquinas. Como NETBIOS es una interfase (API) de la implementación de redes Microsoft WINS NO será necesario en un entorno exclusivo UNIX.

**D. Las redes necesitan seguridad.**

Una vez establecidos los puntos A, B y C el trabajo ha concluido: Puedo leer y escribir archivos en el file server, ver páginas web en el web server, imprimir en impresoras manejadas por el print server…
Pero ésta idea de compartir y de estar ofreciendo los servicios lleva implícita un peligro. Nos está faltando entender cómo me protejo de alguien que quiera aprovechar ésta configuración para hacer un daño o robar información La palabra seguridad aparece junto con dos conceptos fundamentales: autenticación y permisos.
1. Debo autenticar (verificar, identificar) a quien pretenda entrar a mi red y obtener un servicio.
2. Una vez autenticado debo tener almacenado en algún lugar la información de "qué" tiene permitido hacer en la red. (sus permisos).

El punto 1 de seguridad llamado autenticación normalmente se logra con una "cuenta" (nombre de usuario, user id) y un password (contraseña). Hoy existen variantes más sofisticadas: smart cards y tecnologías biométricas (huellas digitales, cara, voz, retina).
Ahora debo guardar la información de usuarios y sus passwords en alguna base de datos centralizada, y necesito "encriptar" esa información. Recordar que siempre existe la posibilidad de que alguien acceda o robe esa base de datos. Por ejemplo los servidores NT4 guardaban información de usuarios en un archivo llamado SAM. Aún cuando el archivo estaba encriptado un grupo de hackers logró saber como crackear la información. Hoy Windows 2000 y 2003, que se basan en dominios, usan un modo más sofisticado de encriptación cuya información también es posible descifrar (el archivo se llama NTDS.DIT en lugar de SAM).

Aclaremos que el peligro está si alguien accede físicamente a esos servidores (domain controlers, DC) donde se guardan las cuentas / passwords. Por eso normalmente esos servidores deberán estar a buen resguardo.

Síntesis: Tenemos un servidor en algún lugar de la red con las cuentas y passwords. Por ejemplo la infraestructura que MS usa para organizar la red se llama Active Directory . Y el servidor con cuentas y passwords (Domain Controler) DC que lo podemos pensar como un servidor de logueo.
Ahora cualquiera que quiera acceder a los "beneficios" de la red se deberá sentar en alguna máquina y entrar user ID y password: logonearse.

Pero ahora surge un problema muy serio. Yo tipeo mi user ID y password y estos deberán viajar por la red para ser verificados en el DC. Pero no existen programas llamados "sniffers" que pueden ver los paquetes que viajan? Sí. Por eso diferentes estrategias han sido y son utilizadas para realizar ésta acción de logonearme para poder acceder a algún recurso de red compartido sin comprometer el password.
Por ejemplo MS utilizó hasta los servidores NT un método de autenticación llamado NTLM (NT LAN MANAGER). Hoy en una red que use Active Directory se usará un viejo método del mundo UNIX (1980) llamado Kerberos. (en NEX 6, Marzo 2004 veremos detalles).
Aparecen hoy otros modos de autenticarse como por ejemplo las llamadas "smart cards". Ellas utilizan una infraestructura diferente llamada PKI (Public Key Infrastructure) basada en certificados y dos claves (keys), una pública y otra privada (en NEX 6; Marzo 2004 veremos detalles).
Aclaremos que hemos ejemplificado el proceso de autenticación al de una persona (usuario). Pero también deberán autenticarse las máquinas entre sí y los servicios. Las infraestructuras detalladas antes también serán usadas en estos casos.

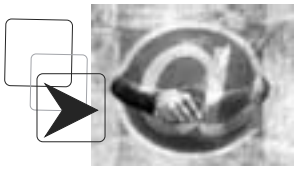
El segundo punto son los Permisos y Access Control Lists (ACLs). Una vez autenticado la pregunta es a qué tiene derecho dentro de la red. Eso se gobierna con una infraestructura de permisos también llamados derechos y privilegios. Ejemplos:

-El file server de la empresa tiene 6 carpetas compartidas pero el usuario "Pepe"solo puede acceder (tiene permiso) para una sola. Y quizás el permiso solo lo deje "read" (leer) los archivo pero no modificarlos
-El usuario "administrador" tiene derecho a crear cuentas de usuarios

Con lo anterior (autenticación y permisos) ejemplificamos uno de los temas que componen la seguridad en el mundo IT. Pero no son los únicos. Por ejemplo
- Cuando solicito información a un website o envío/recibo un e-mail, cómo puedo hacer para que nadie vea los contenidos? La respuesta es encriptándola
- Como me aseguro de quien me envía un cierto e-mail?. Respuesta: digital signing.
- Como hago una compra segura con mi tarjeta de crédito via web?. Normalmente aparece https y no http en el browser. La comunicación a partir de ahí se hará encriptada usando SSL (Secure Sockets Layer) que utiliza encriptación asimétrica de llaves publica y privada (PKI).
- Porque un hacker puede acceder a mi computadora utilizando las llamadas "vulnerabilidades"?
- Que significa que el programa .exe que llega como attachment en un e-mail me cree un back-door?
Todos estos y otros conceptos que conforman la seguridad informatica (ingeniería social, hashes, virus, gusanos, troyano…) también serán expuestas en sucesivos números de NEX.

**E. Las redes deben proveer modos para que los usuarios encuentren los servicios (servidores y recursos compartidos (shares))**

Hace no mucho tiempo utilizar web servers no era tan común y básicamente file y print sharing eran las dos funcionalidades más comunes de las redes. Estas dos acciones siguen siendo importantes solo que los file servers y print servers en la red, pueden ser muchísimos. La pregunta es cómo hago para encontrar un recurso compartido en mi red? Por ejemplo la respuesta de MS en W2000 y W2003 ha sido: Active Directory. Pero ésta tecnología está aún en proceso. Hoy lo más utilizado es una vieja tecnología conocida por "Network Neighborhood o en W2000 y 2003 "My Network Places" que utilizan toda una infraestructura de "browse masters" y "browser lists".



## Windows Services para Unix (SFU) (Mejorado y GRATIS!!)

**SFU permite a los clientes utilizar varias opciones de interoperabilidad, como autenticar usuarios de UNIX y Linux en contra de Active Directory (AD); compartir recursos a través de todas las plataformas con un manejo apropiado de los privilegios de usuario, permitiendo correr aplicaciones UNIX en Windows.**

Microsoft presentó la última versión de su herramienta Windows SFU versión 3.5, la cual tiene como característica varias reformas técnicas importantes. Lo mas impresionante de esta versión es su costo. Por primera vez, Microsoft está entregando licencias SFU gratuitamente a sus clientes de Windows. Así otro producto que previamente se comercializaba por separado es incluido dentro del producto Windows, así como en el caso de Microsoft Internet Explorer (IE) ó Windows Media technologies. No es claro si esta combinación es el resultado de la competencia con Linux. Si, que será un beneficio para cualquier corporación que quiera migrar sus aplicaciones Unix a Windows o mejor aún para quienes integren Windows, UNIX y Linux en un ambiente heterogéneo.

El SFU es una herramienta de interoperabilidad diseñada para integrar varias versiones de Windows (Windows Server 2003, Windows XP, Windows 2000 Server y Win2k Professional) (Windows NT 4.0 no está soportado en esta edición) con UNIX y cada vez más, Linux. SFU incluye un entorno runtime para aplicaciones UNIX basada en tecnología y scripts de Interop Systems y que deja correr aplicaciones UNIX, en máquinas de Windows y soporta tecnologías UNIX tal como NFS y Network Information Service (NIS). "Pocos de nuestros clientes tienen entornos Windows puros" dijo Oldroy (director Windows Server Group en Microsoft). "

En vez de esto tienen una mezcla de Windows, UNIX y Linux. En éstas empresas, la interoperabilidad es tan importante; (las empresas) quieren tener servicios de directorio y servidores de archivos a través de estas plataformas, y lo quieren hacer sin tener que comprar nuevo software".

SFU permite a los clientes utilizar varias opciones de interoperabilidad, como autenticar usuarios de UNIX y Linux en contra de Active Directory (AD); compartir recursos a través de todas las plataformas con un manejo apropiado de los privilegios de usuario, permitiendo correr aplicaciones UNIX en Windows.

También provee herramientas familiares con las cuales cuentan los desarrolladores de UNIX, profesionales IT y administradores: se encontrará con shells C y Korn, aplicaciones y comandos tales como gcc, make, emacs, vi, sendmail y ftp. SFU también incluye Perl 5.6.1 y ActivePerl de ActiveState con esto puede simplificar la migración de los scripts de administración UNIX a Windows.

Cuando usted necesita mover aplicaciones UNIX a una plataforma más accesible, la opción obviamente es Linux. Sin embargo, Microsoft sostiene que SFU en Windows es la solución más barata. Usted tiene que basar cualquier estimación de costo en la experiencia de su empresa con varios sistemas operativos. Pero con el movimiento a una licencia libre en SFU 3.5, Microsoft está terminando con una de las permanentes quejas. Aunque la versión anterior fue vendida por U$s 99 a cada cliente o servidor, SFU es ahora discutiblemente tan barata (o más barata) como una solución Linux.

Entonces, ¿qué es lo nuevo en SFU 3.5? "Esta versión es una actualización de SFU 3.0 (publicado en Mayo del 2002)", dijo Oldroyd. "Tiene el mismo núcleo de funcionalidad pero está mejorado con nuevas características.

Todavía es la migración más completa que existe, y está soportada y patrocinada por Microsoft, lo que muchos de los clientes han estado reclamando. Ellos nos dijeron que entreguemos esta funcionalidad para que ellos puedan evaluar su inversión en su Windows back end." Específicamente, SFU 3.5 incluye rediseños para herramientas de interoperabilidad NFS, NIS y medios Interix; soporte para aplicaciones UNIX P-Thread, permitiendo así migrar aplicaciones multi-threaded (algo que no era posible previamente); mejor soporte POSIX; las últimas versiones de X11 (X11R.6) y muchos utilidades UNIX command-line.

La primera versión en soportar Windows 2003 es SFU 3.5, el cual es más escalable que versiones antiguas y es cluster aware para una mejor disponibilidad.
También soporta características nativas de Windows 2003 tales como Volume Shadow Copy Service (VSS), suministrando copias de recursos compartidos point-in-time y backup y posibilidades de recuperación.

El SFU 3.5 se instala fácilmente. El set de instalación por defecto es diferente para sistemas operativos clientes y servidores.

Las predicciones son que el SFU 3.5 motivará compañías que se hayan estandarizado en infraestructura Windows pero que siguen manteniendo sistemas UNIX. Esas compañías, que todavía utilizan sus más importantes servicios en sistemas UNIX, se dividirán con igualdad entre Windows y Linux, dependiendo de sus necesidades. De cualquier manera el SFU3.5 es un "killer deal" y es un producto que debe evaluar si tiene que migrar UNIX o necesidades de interoperabilidad.

Se puede bajar SFU 3.5 desde el sitio web de Microsoft (http://www.microsoft.com/windows/sfu)

## Un RAM Tester Gratis para Microsoft

La supuesta inestabilidad de muchos sistemas Operativos Windows en muchas casos puede provenir de un problema con la RAM (módulos de memoria mal emparejadas, sobrecalentamiento de sistemas de memoria con ventiladores defectuosos o inadecuados, o sistemas con fuentes eléctricas defectuosas (nótese que los dos últimos no son realmente problemas de memoria. Son muy difíciles de detectar parececiendo "verdaderas" fallas de RAM).

Existe un gran número de RAM testers económicos pero no muy buenos. Los buenos son caros. Ahora, sin embargo, Microsoft está regalando un programa RAM tester.

Se puede encontrar en http://oca.microsoft.com/en/windiag.asp -- un URL que probablemente reconozca. oca.microsoft.com viene de "análisis crash online". Si usted ha tenido una "blue screen" en un sistema XP, entonces recordará que un mensaje ofrece analizarlo por usted - es oca.microsoft.com que contiene el código que hace esto.

El RAM tester parece muy exhaustivo y le resolverá sin duda problemas de RAM.