UNIVERSIDAD DE LA AMAZONIA

FACULTAD DE INGENIERIA
DEPARTAMENTO DE EDUCACIÓN A DISTANCIA

PROGRAMA
TECNOLOGÍA EN INFORMÁTICA Y SISTEMAS

COMPILADO
ADMINISTRACIÓN EN REDES Y SERVIDORES

PREPARADO POR
YOIS S. PASCUAS RENGIFO
Ingeniera de Sistemas
Magíster en Ciencias de la Información y las Comunicaciones
y.pascuas@udla.edu.co

AGOSTO
2015

TABLA DE CONTENIDO

INTRODUCCIÓN

En las actuales condiciones de alta competitividad, las organizaciones tanto privadas como públicas, cualquiera sea la actividad a que se dediquen, necesitan elevar sus niveles de eficiencia, productividad y calidad para satisfacer los requerimientos de sus clientes. Para ello, dichas organizaciones deben contar con personal que se encuentre especialmente capacitado para alcanzar los objetivos, así mismo, las redes informáticas sirven para intercambiar información, por esta razón la administración de redes se está tornando compleja dado al surgimiento de diferentes tipos de red y configuraciones.

La administración de redes y servidores abarca las actividades para asegurar el uso eficiente de las redes; desde la configuración, control y monitoreo, así como la solución de problemas, permitiendo el correcto desarrollo de los objetivos misionales de las organizaciones. Es así como se requiere mecanismos y herramientas que apoyen el talento humano en la reducción del tiempo en el cual la red esté fuera de servicio y demás aspectos relacionados en el aumento de la eficiencia en el desarrollo de las tareas.

Con el fin de conocer los conceptos básicos de la administración de redes y servidores para la resolución de problemas de su funcionamiento, se muestra en este compilado los conceptos, orientadas a los estudiantes de la Universidad de la Amazonia específicamente para la Tecnología en Informática y Sistemas.

COMPETENCIA GENÉRICA PROPUESTA

Conocer y administrar los componentes principales de las redes informáticas para la resolución de problemas relacionados con aspectos propios de su funcionamiento.

1. GESTIÓN DE REDES

Es necesario que un administrador monitoree, gestione y controle un sistema complejo con muchos componentes interactuando entre sí. Por ejemplo, las plantas generadoras de energía eléctrica disponen de una sala de control en la que una serie de diales, medidores e indicadores luminosos monitorizan el estado (temperatura, presión, flujo) de diversas válvulas, conductos y recipientes remotos, así como de otro componentes de la planta. Estos dispositivos permiten al operador monitorizar la multitud de componentes que forman la planta y pueden alertarle cuando esté a punto de surgir un problema.

El operador de la planta llevará a cabo una serie de acciones para controlar a estos componentes. En este ejemplo el "administrador" monitoriza una serie de dispositivos remotos y analiza sus datos con el fin de cerciorarse de que esos dispositivos estén operativos y de que su operación se mantenga dentro de una serie de límites prescritos. Así mismo, controla reactivamente el sistema haciendo ajustes en respuesta a los cambios que el sistema o su entorno sufren y también administra proactivamente el sistema.

Por ejemplo, en una red sencilla como lo muestra la siguiente figura, existen muchos escenarios en los que un administrador de red podría aprovechar la disponibilidad de herramientas de gestión de red:

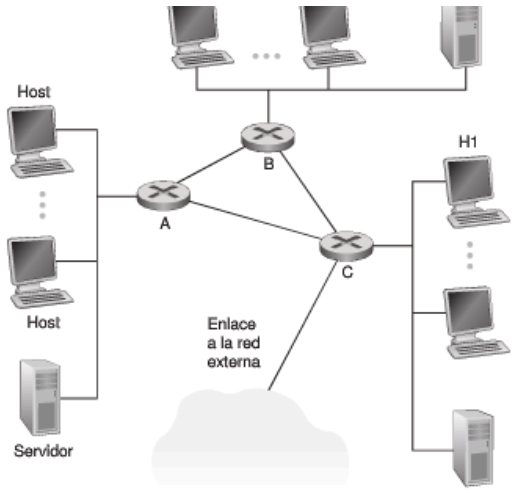


Figura. Ilustración de los usos de la gestión de red

- Detección de fallos en una tarjeta de interfaz en un host o un router. Con las herramientas de gestión de red apropiadas, una entidad de red podría informar al administrador de red que una de sus interfaces ha fallado.

- Monitorización de los hosts. El administrador de red puede realizar

comprobaciones periódicas para ver si todos los hosts de la red están encendidos y operativos.

- Monitorización del tráfico como ayuda a la implantación de recursos. Un administrador de red puede monitorizar los patrones de tráfico entre cada origen y cada destino y observar, por ejemplo, que si intercambian los servidores entre segmentos de una red LAN la cantidad de tráfico que atraviesa múltiples redes LAN podría reducirse significativamente.

- Detección de cambios rápidos en las tablas de enrutamiento. Las alteraciones rápidas de ruta (cambios frecuentes en las tablas de enrutamiento) pueden indicar inestabilidades en el enrutamiento o la existencia de un router mal configurado.

- Detección de intrusiones. Un administrador de red puede desear que se le notifique que ha lelgado un cierto tráfico de red prodcedente de un origen sospechoso o con destino a el. También podría detectar la existencia de ciertos tipos de tráfico que se sabe son característicos de los tipos de ataque.

- Monitorización de los acuerdos de nivel del servicio. Son contratos que definen métricas específicas de rendimiento y niveles aceptables de rendimiento del proveedor de la red (Kurose & Ross, 2010).

1.1 CONCEPTUALIZACIÓN[1]

Los términos administrador de red, especialista de red y analista de red se designan a aquellas posiciones laborales relacionadas con las redes de computadoras, o sea, las personas que se encargan de la administración de la red. Los administradores de red son básicamente el equivalente de los administradores de sistemas: mantienen el hardware y software de la red. Esto incluye el despliegue, mantenimiento y monitoreo del engranaje de la red: switches, routers,

[1] Imagen tomada de: http://www.smartupmarketing.com/wp-content/uploads/2012/09/gestion-redes-sociales.jpeg

cortafuegos, etc. Las actividades de administración de una red por lo general incluyen la asignación de direcciones, asignación de protocolos de ruteo y configuración de tablas de ruteo así como, configuración de autenticación y autorización de los servicios.

Frecuentemente se incluyen algunas otras actividades como el mantenimiento de las instalaciones de red tales como los controladores y ajustes de las computadoras e impresoras. A veces también se incluye el mantenimiento de algunos tipos de servidores como VPN, DNS, web, DHCP, correo electrónico, FTP, sistemas detectores de intrusos, etc. Los analistas y especialistas de red se concentran en el diseño y seguridad de la red, particularmente en la resolución de problemas relacionados con la red.

Algunas funciones de la administración de las redes incluyen:

- Proporcionar servicios de soporte.
- Asegurarse de que la red sea utilizada eficientemente.
- Asegurarse que los objetivos de calidad de servicio se alcance.
- Monitorear el buen funcionamiento de los sistemas, servidores y recursos de red existentes.
- Apagar el equipo.
- Configurar los programas que se inician junto con el sistema.
- Administrar cuentas de usuarios.
- Administrar los programas y la documentación instalada.
- Configurar los programas y los dispositivos.
- Configurar la zona geográfica, fecha y hora.
- Administrar espacio en discos y mantener copias de respaldo.
- Configurar servicios que funcionarán en red.
- Solucionar problemas con dispositivos o programas (Wikipedia, 2015).

1.1.1 DEFINICIÓN DE ADMINISTRACIÓN DE REDES

Es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada. Proceso que consiste en la planeación, organización y control de las actividades que envuelven el funcionamiento de los datos dentro de una organización. Es un servicio que utiliza una gran variedad de herramientas, aplicaciones y dispositivos,

para ayudar a los administradores de la red a supervisar y mantener las redes.

1.1.2. ADMINISTRADOR DE RED

Es la persona responsable de la configuración y administración de la red. El administrador generalmente configura la red, asigna contraseñas, permisos y ayuda a los usuarios. Es la persona responsable de supervisar y controlar el hardware y software de una red; incluye el control del esquema de seguridad y administración de procesos y aplicaciones en red. Las responsabilidades del administrador de la red se dividen en siete áreas:

1. Responder a las necesidades de los usuarios.
2. Diseñar la instalación, incluyendo el cableado, el lugar donde se van a instalar las estaciones, los derechos de acceso, los interfaces de los usuarios, y la seguridad.
3. Configurar la red al ponerla en marcha y siempre que se haga algún cambio.
4. Mantener y administrar la red.
5. Diagnosticar problemas y efectuar reparaciones sencillas.
6. Evaluar el rendimiento de la red.
7. Planificar los cambios a corto y largo plazo.

1.2 OBJETIVOS DE LA ADMINISTRACIÓN DE REDES

- Mantener operativa la red satisfaciendo las necesidades de los usuarios.
- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos.
- Asegurar el funcionamiento de la red, protegiéndola contra el acceso no autorizado, impidiendo que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

1.2.1 RETOS DE LA ADMINISTRACIÓN DE REDES

- Se mezclan diversas señales como voz, datos, imágenes, videos y gráficas.
- Se interconectan varios tipos de redes de acuerdo a su cobertura: LAN, MAN y WAN.
- El empleo de varios sistemas operativos.
- Se utilizan diversas arquitecturas de red.

1.3 PRINCIPALES OPERACIONES DE LA ADMINISTRACIÓN DE RED

- **Administración de fallas.** Maneja las condiciones de error en todos los componentes de la red, bajo las siguientes fases:
    - Detección de fallas.
    - Diagnóstico del problema.
    - Solución de problemas y mecanismos de recuperación.
    - Seguimiento y control.
- **Control de fallas.** Esta operación tiene que ver con la configuración de la red, así como el monitoreo continuo de todos sus elementos.
- **Administración de cambios.** Comprende la planeación, la programación de eventos e instalación.
- **Administración del comportamiento.** Asegura el funcionamiento óptimo de la red, lo que incluye: el número de paquetes que se transmiten por segundo, tiempos pequeños de respuesta y disponibilidad de la red.
- **Servicios de contabilidad.** Este servicio provee datos que van a la cargo por uso de la red, como:
    - Tiempo de conexión y terminación.
    - Número de mensajes transmitidos y recibidos.
    - Nombre de mensajes transmitidos y recibidos.
    - Razón por la que termino la conexión.
- **Control de Inventarios**. Debe llevar un registro de los nuevos componentes que se incorporen a la red, de los movimientos que se hagan y de los cambios que se lleven a cabo.
- **Seguridad.** La estructura administrativa de la red debe proveer mecanismos de seguridad, así como la confidencialidad, disponibilidad, integridad apropiados:
    - Identificación y autentificación del usuario.
    - Autorización de acceso a los recursos.

- Confidencialidad. Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía.

1.4 ARQUITECTURA DE LA ADMINISTRACIÓN DE REDES

Las arquitecturas para la administración de redes utilizan la misma estructura y conjuntos básicos de relaciones. Las estaciones terminales, como los sistemas de cómputo y otros dispositivos de red, utilizan un software que les permite enviar mensajes de alerta cuando se detecta algún problema. Al recibir estos mensajes de alerta las entidades de administración son programadas para reaccionar, ejecutando una o varias acciones que incluyen la notificación al administrador, el cierre del sistema, y un proceso automático para la posible reparación del sistema.

Las entidades de administración también pueden registrar la información de las estaciones terminales para verificar los valores de ciertas variables. Esta verificación puede realizarse automáticamente o ejecutada por algún administrador de red, pero los agentes en los dispositivos que se están administrando responden a todas las verificaciones.

Los agentes son módulos de software que, en primer lugar, compilan información acerca de los dispositivos administrados en los que residen, después almacenan esta información en una base de datos de administración y, por último la ponen a disposición de las entidades que forman parte de los sistemas de administración de la red vía un protocolo de administración de red, como por ejemplo, SNMP (Protocolo Simple de Administración de Redes) y CMIP (Protocolo de Información de Administración Común). Los proxy de administración son entidades que proporcionan información de parte de otras entidades.

1.5 FUNCIONES DE ADMINISTRACIÓN DEFINIDAS POR OSI

La OSI (en inglés, Open System Interconnection) define 5 funciones de administración:

- Configuración
- Fallas

- Contabilidad
- Comportamiento
- Seguridad

La configuración comprende las funciones de monitoreo y mantenimiento del estado de la red. La función de fallas incluye la detección, el aislamiento y la corrección de fallas en la red. La función de contabilidad permite el establecimiento de cargos a usuarios por uso de los recursos de la red. La función de comportamiento mantiene el comportamiento de la red en niveles aceptables. La función de seguridad provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves.

1.5.1 MODELO DE ADMINISTRACIÓN DE RED DE LA ISO

ISO (Organización Internacional de Normalización) ha contribuido en gran medida a la estandarización de las redes. Su modelo de administración de redes es de los principales para entender las funciones fundamentales de los sistemas de administración de redes. Este modelo consiste en cinco áreas conceptuales:

- Administración del desempeño.
- Administración de la configuración.
- Administración de la contabilidad.
- Administración de fallas.
- Administración de la seguridad.

1. **Administración del Desempeño**. Su objetivo es medir y proveer la información disponible del desempeño de la red para mantener el funcionamiento de la red interna en un nivel aceptable.
2. **Administración de la Configuración.** Su objetivo es supervisar la información de la configuración de la red y de los sistemas para rastrear y manejar los efectos sobre el desempeño de las versiones del software y hardware de la red.
3. **Administración de la Contabilidad.** Su objetivo es medir los parámetros de utilización en la red para regular apropiadamente las aplicaciones de un usuario o grupo en la red.
4. **Administración de Fallas.** Su objetivo es detectar, registrar y notificar los problemas que existen en la red, para después ejecutar un

proceso de corrección automática y lograr el funcionamiento óptimo de la red. La Administración de Fallas implica:

a. Primero se determinan los síntomas y se aísla el problema.
b. Entonces el problema es fijo, y la solución se prueba en todos los subsistemas importantes.
c. Finalmente la detección y la resolución del problema son registradas.

5. **Administración de la Seguridad.** Su objetivo es controlar el acceso a los recursos de la red con respecto a las normas de consulta locales, de modo que la red no pueda ser saboteada (intencionalmente o involuntariamente) y que la información que es vulnerable no pueda ser utilizada por aquellos sin una autorización apropiada. Los subsistemas de seguridad trabajan dividiendo los recursos de la red en áreas autorizadas y en áreas no autorizadas. Los subsistemas de seguridad realizan varias funciones. Estos subsistemas identifican los recursos de la red que son vulnerables (incluso los sistemas, archivos y otras entidades), determinan la relación entre estos recursos y su utilización. También supervisan los puntos en los recursos de la red que son vulnerables y registran los accesos sin autorización a estos recursos.

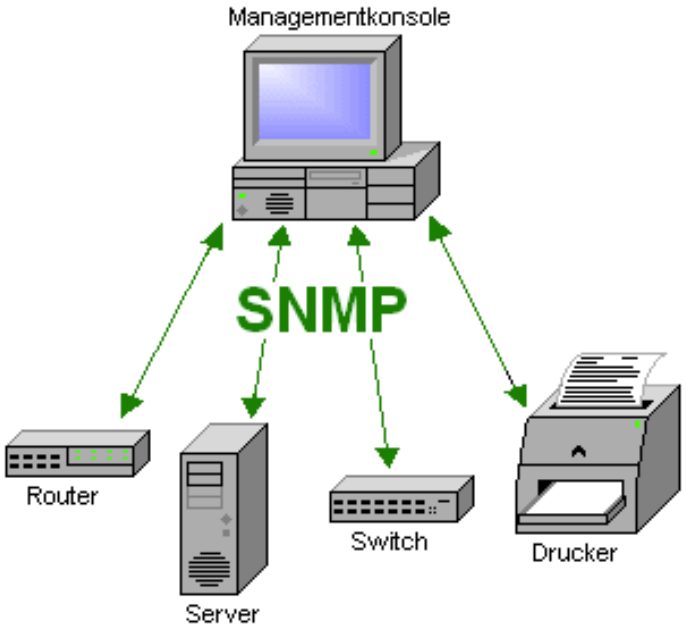
1.6 PROTOCOLO DE ADMINISTRACIÓN DE RED TCP/IP

El sistema de administración de red de TCP/IP se basa en el protocolo SNMP (Protocolo Simple de Administración de Redes), que ha llegado a ser un estándar de ISO en la industria de comunicación de datos para la administración de redes de computadora, ya que ha sido instalado por múltiples fabricantes de puentes, repetidores, ruteadores, servidores y otros componentes de red.

Para hacer más eficiente la administración de la red, la comunidad de TCP/IP divide las actividades en dos partes:

- Monitoreo, o proceso de observar el comportamiento de la red y de sus componentes, para detectar problemas y mejorar su funcionamiento.
- Control, o proceso de cambiar el comportamiento de la red en tiempo real ajustando parámetros, mientras la red está en operación, para mejorar el funcionamiento y repara fallas.

1.6.1 SNMP (PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED)[2]



SNMP surge para resolver los problemas de administración de redes TCP/IP, debido a que el crecimiento apresurado y desmesurado de este tipo de redes ha hecho que la administración y gestión de las mismas se convierta en una labor intensa. Un caso muy particular es el de Internet, debido a su complejidad y gran tamaño. La arquitectura de este protocolo se diseñó tomando en cuenta el modelo OSI. El protocolo sencillo de administración de red (SNMP) es el protocolo de administración de redes estándar usado en Internet. Este protocolo, define la comunicación de un administrador con un agente.

Es un protocolo de gestión de red muy utilizado. Permite obtener: información de dispositivos de la red, memoria libre, uso de CPU, detección de errores, establecer alarmas, estado de funcionamiento. SNMP está formado por cuatro componentes básicos:

1. **Base de datos lógica:** SNMP sigue el modelo de una base de datos lógica, en la misma se almacena información referente a la configuración, estado, error y rendimiento.
2. **Agentes:** El agente es un software, que permite el acceso a la información. Dicho agente responde a peticiones, realiza actualizaciones e informa los problemas.
3. **Administradores:** La estación de administración, contiene un software de administrador, el cual se encarga de enviar y recibir los mensajes SNMP. Además de esto existen otra serie de aplicaciones de

[2] Imagen tomada de: http://img.vinagreasesino.com/wp-content/uploads/2012/11/snmp.png

administración que se comunican con los sistemas de red mediante el administrador.

4. **Base de información de administración:** La base de información de administración, denominada MIB, constituye la descripción lógica de todos los datos de administración de la red. La MIB contiene información de estado y del sistema, estadísticas de rendimiento y parámetros de configuración.

SNMP es muy utilizado en redes TCP/IP y de intercambio de paquetes de Internet, para transportar información administrativa y comandos entre los programas de administración ejecutados por un administrador y el agente de administración de red que se ejecuta en un sistema principal o host; es decir SNMP funciona bajo TCP/IP, lo cual significa que desde un sistema central se puede gestionar cualquier computadora de una red LAN, WAN o Internet.

El SNMP define el formato y el significado de los mensajes que intercambian el administrador y el agente. En lugar de definir muchas operaciones, el SNMP utiliza el paradigma de obtención y almacenamiento. En el cual el administrador manda solicitudes de obtención y almacenamiento de valores en variables. Todas las operaciones se definen como efectos colaterales de las operaciones de almacenamiento.

1.6.2 TIPOS DE DATOS DE SNMP

SNMP maneja los siguientes tipos de datos:

- **Dirección IP:** Se expresa como cuatro bytes. Recuérdese que cada elemento de red se configura con al menos una dirección IP.
- **Dirección física:** Se expresa como una cadena de octetos de longitud adecuada; por ejemplo, para una red Ethernet o Token Ring, la dirección física es de 6 octetos.
- **Contador:** Es un entero no negativo de 32 bits, se usa para medir, por ejemplo, el número de mensajes recibidos.
- **Tabla:** es una secuencia de listas.
- **Cadena de Octetos:** Puede tener un valor de 0 a 255 y se usa para identificar una comunidad.

1.6.3 BASE DE DATOS DE ADMINISTRACIÓN

La MIB define los objetos de la red operados por el protocolo de administración de red, y las operaciones que pueden aplicarse a cada objeto. Una variable u objeto MIB se define especificando la sintaxis, el acceso, el estado y la descripción de la misma:

- **Sintaxis:** Especifica el tipo de datos de la variable, entero, cadena dirección IP, etc.
- **Acceso:** Especifica el nivel de permiso como: Leer, leer y escribir, escribir, no accesible.
- **Estado:** Define si la variable es obligatoria u opcional.
- **Descripción:** Describe textualmente a la variable.

1.6.4 OBJETOS DE ADMINISTRACIÓN DE MIB

- **Grupo de Sistemas.** Se usa para registrar información del sistema el cual corre la familia de protocolos.
- **Grupo de Interfaces.** Registra la información genérica acerca de cada interfase de red, como el número de mensajes erróneos en la entrada y salida, el número de paquetes transmitidos y recibidos, el número de paquetes de broadcast enviados.
- **Grupo de traducción de dirección.** Comprende las relaciones entre direcciones IP y direcciones específicas de la red que deben soportar.
- **Grupo IP.** Almacena información propia de la capa IP, como datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc.
- **Grupo TCP.** Este grupo incluye información propia del protocolo TCP, como estadísticas del número de segmentos transmitidos y recibidos, información acerca de conexiones activas como dirección IP, puerto o estado actual.
- **Grupo EGP.** En este grupo se requieren sistemas (ruteadores) que soporten EGP (Exterior Gateway Protocol).

1.7 AGENTES Y CONSOLAS

Los agentes y consolas son los conceptos claves en la administración de redes.

- **Consola:** es una estación de trabajo convenientemente configurada para visualizar la información recogida por los agentes.
- **Agentes**: son programas especiales que están diseñados para recoger información específica de la red.

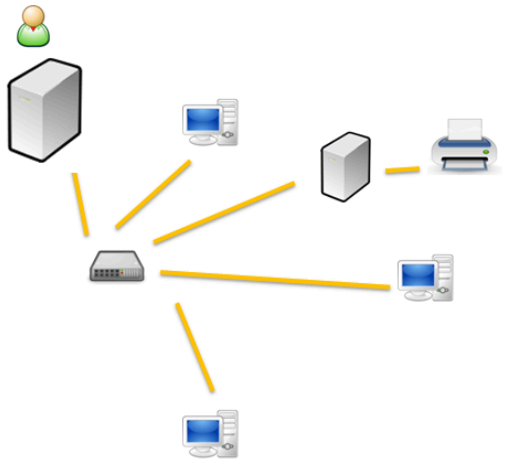
1.7.1 CARACTERÍSTICAS DE LOS AGENTES

- Están basados en software frente a monitores y analizadores basados en hardware.
- Son transparentes a los usuarios. Se ejecutan en los puestos de trabajo sin afectar al rendimiento de los mismos.
- La información que recogen la almacenan en bases de datos relacionales que después son explotadas a través de las consolas.
- Los agentes son configurados de forma remota a través de la consola para su correcta operación.

1.7.2 FUNCIONES QUE SOPORTAN LOS AGENTES

- Visualizar y manipular información de la red.
- Automatizar la distribución de ficheros.
- Mantener el inventario del hardware.
- Gestión y configuración del software remoto.
- Recibir notificación de alarmas de red.
- Automatizar tareas como copias de seguridad y detección de virus.
- Monitorizar la utilización de discos y de ficheros.
- Establecer y gestionar la seguridad en la red.

1.7.3 GESTIÓN DE USUARIOS[3]



La gestión de usuarios es la actividad referida a la creación y mantenimiento de cuentas de usuarios, así como la de asignación de recursos y

[3] Imagen tomada de: http://w
content/uploads/2012/04/ud2_image030.png

mantenimiento de la seguridad en los accesos a la red. Tareas principales en la gestión de usuarios:

a. Altas, bajas y modificaciones de usuarios en la red.
b. Establecimiento de políticas de passwords (contraseñas) como su longitud, tiempo de vida, seguridad de la base de datos de passwords, etc.
c. Asignación de permisos para la utilización de recursos de red.
d. Monitorización de la actividad de los usuarios.
e. Establecimiento de políticas generales y de grupo que faciliten la configuración de usuarios.

1.7.4 GESTIÓN DEL HARDWARE

La gestión del hardware es una actividad esencial para el control del equipamiento y sus costes asociados así como para asegurar que los usuarios disponen del equipamiento suficiente para cubrir sus necesidades.

Para evitar visita física a los equipos, se utilizan agentes que se ejecutan en los puestos de trabajo y que realizan el inventario del hardware de forma autónoma y remota. Una vez que la información de inventario es recogida, la administración de red puede hacer las siguientes funciones:

1. Añadir información relativa a puestos de trabajo no instalados en red.
2. Añadir información sobre otros aspectos como la localización física, condiciones en que se encuentra, etc.
3. Establecimiento de parámetros de configuración en los ficheros de configuración del Sistema Operativo.
4. Realizar el seguimiento de averías de los componentes de las estaciones de trabajo.
5. Anotar información al inventario referente a los componentes que forman la estación de trabajo (tarjetas, discos, etc.).

En los servidores, se realiza un seguimiento de los parámetros de funcionamiento como pueden ser actividad del CPU, de los discos, espacios disponibles, número de conexiones, etc. Este seguimiento permite analizar el comportamiento y, en su caso, detectar nuevas necesidades y adaptar las características hardware de los servidores.

1.7.5 GESTIÓN DEL SOFTWARE

El software de administración de red permite al administrador supervisar y controlar los componentes de una red; permite que el administrador investigue dispositivos como hosts, ruteadores, conmutadores y puentes para determinar su estado y obtener estadísticas sobre las redes a las que se conectan. El software también permite controlar tales dispositivos cambiando las rutas y configurando interfaces de red.

Las actividades relativas a la gestión de software permiten a la administración de red determinar si las aplicaciones necesitadas por los usuarios se encuentran instaladas y donde están localizadas en la red, además permiten el seguimiento de número de licencias existentes y el cumplimiento de su uso en la red. De igual forma que en el hardware, se utilizan agentes que realizan la función de obtener toda la información acerca del software en la red. Sus características particulares son:

- Obtienen su información revisando todos los discos de los puestos de trabajo en la red.
- Normalmente son capaces de identificar cientos de paquetes comerciales y se les puede añadir nuevos paquetes particulares de la empresa.
- Realizan mediciones del número de copias de un paquete que se están usando en la red de forma simultánea con objeto de comprobar su adecuación al número de licencias adquiridas. Las tareas que se realizan en la administración de red en esta área son:
    - Creación y mantenimiento del inventario de software instalado.
    - Especificación y requerimiento del número de copias disponibles de los distintos paquetes.
    - Seguimiento de la instalación no autorizada de software y de otros ficheros en prevención de introducción de virus.
    - Autorización a los usuarios para la utilización de los paquetes de software. La información que se suele extraer es la siguiente:
        - Información general del paquete: fabricante, versión, No de licencias.
        - Disponibilidad: quién usa el software, quién lo puede usar.
        - Archivos que componen el paquete.

- Información adicional establecida por el administrador.

1.7.6 DISTRIBUCIÓN DE ARCHIVOS

Debido a la enorme dispersión de puestos en red, la distribución de software y otros archivos se realiza mediante la utilización de agentes de distribución de archivos. Las características de los agentes de distribución de archivos son:

- Las funciones que realizan son instalación y actualización de software, descargas y eliminación de archivos.
- Pueden aplicarse a puestos individuales o a grupos de estaciones simultáneamente.
- Tienen en cuenta los permisos de accesos de los usuarios a más de una máquina para instalar el software en cada una de las máquinas a las que se accede.

1.7.7 MONITORIZACIÓN DE LA ACTIVIDAD DE RED

Las funciones de la monitorización de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas al personal responsable del buen funcionamiento de la red. Los eventos típicos que son monitorizados suelen ser:

- Ejecución de tareas como pueden ser realización de copias de seguridad o búsqueda de virus.
- Registro del estado de finalización de los procesos que se ejecutan en la red.
- Registro de los cambios que se producen en el inventario de hardware.
- Registro de las entradas y salidas de los usuarios en la red.
- Registro del arranque de determinadas aplicaciones.
- Errores en el arranque de las aplicaciones.

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención se pueden utilizar diferentes métodos de notificación como son:

- Mensajes por correo electrónico: conteniendo el nivel de prioridad y el nombre e información del evento.

- Mensajes a móviles: cuando el evento necesita intervención inmediata se suele comunicar a los técnicos de guardia a través de este método.

Además de los eventos, otra característica importante es la monitorización el tráfico de red:

- Se toman nuevas medidas sobre aspectos de los protocolos, colisiones, fallos, paquetes, etc.
- Se almacenan para su posterior análisis.
- Del análisis se obtienen conclusiones, bien para resolver problemas concretos o bien para optimizar la utilización de la red.

1.7.8 PLANIFICACIÓN DE PROCESOS

En vez de tener que recordar y realizar trabajos periódicos o en horas no laborables, el administrador puede programar un agente que realice las tareas programadas en los momentos previstos. Los agentes recogen información sobre el estado de finalización de los procesos para un posterior análisis por el administrador. Los procesos típicos que se suelen planificar son: copias de seguridad, búsqueda de virus, distribución de software, impresiones masivas, etc.

1.7.9 PROTECCIÓN CONTRA VIRUS

La protección contra la entrada de virus en la red se suele hacer mediante la utilización de paquetes especiales basados en una parte servidora y un conjunto de agentes distribuidos en los puestos de trabajo. La parte servidora realiza las tareas de actualización contra nuevos virus, realiza tareas de registro de virus, comunicación de alarmas al administrador, comunicación con otros servidores distribuidos en la red con software antivirus, protección de los discos y archivos de los propios servidores, etc. Los agentes por su parte evitan la entrada de virus en los propios puestos de trabajo comunicando al servidor la detección de los virus y eliminándolos automáticamente siempre que sea posible.

Nota: Hay que tener en cuenta que actualmente no solo se debe tener protección contra los virus sino también de otro tipo de software malicioso como por ejemplo los malware.

1.7.10 SOPORTE DE IMPRESORAS

La gestión centralizada de impresoras en la red permite reducir el tiempo y el esfuerzo que necesitan los usuarios para configurar la impresión desde unos puertos de trabajo y también permiten al administrador realizar una gestión unificada de todas las impresoras de la red. Las actividades relacionadas con el soporte de impresoras son dos:

1. Las relacionadas con el manejo de las impresoras por parte del administrador.
2. Las relacionadas con la selección de impresoras e impresión por parte de los usuarios.

El modo de operar suele ser el siguiente:

1. El administrador da de alta las impresoras en la red.
2. Posteriormente el administrador, establece las condiciones de acceso como permisos a los usuarios, horario de acceso a las impresoras, etc.
3. El usuario después selecciona las impresoras de las que tiene acceso permitido y las instala en un puerto de trabajo de forma remota y transparente.
4. Cuando el usuario imprime también tiene acceso a las colas de impresión de forma que puede añadir o eliminar trabajos de su propiedad.
5. El administrador a través de los agentes de impresión monitorea la actividad de las impresoras y soluciona problemas que puedan surgir.

1.7.11 GESTIÓN DEL ESPACIO DE ALMACENAMIENTO

El administrador utiliza agentes que recolectan información sobre el grado de ocupación de los discos con objeto de tomar decisiones al respecto de la redistribución de ficheros y de la adquisición de nuevos discos. La extracción de información que realiza el agente suele ser a nivel de:

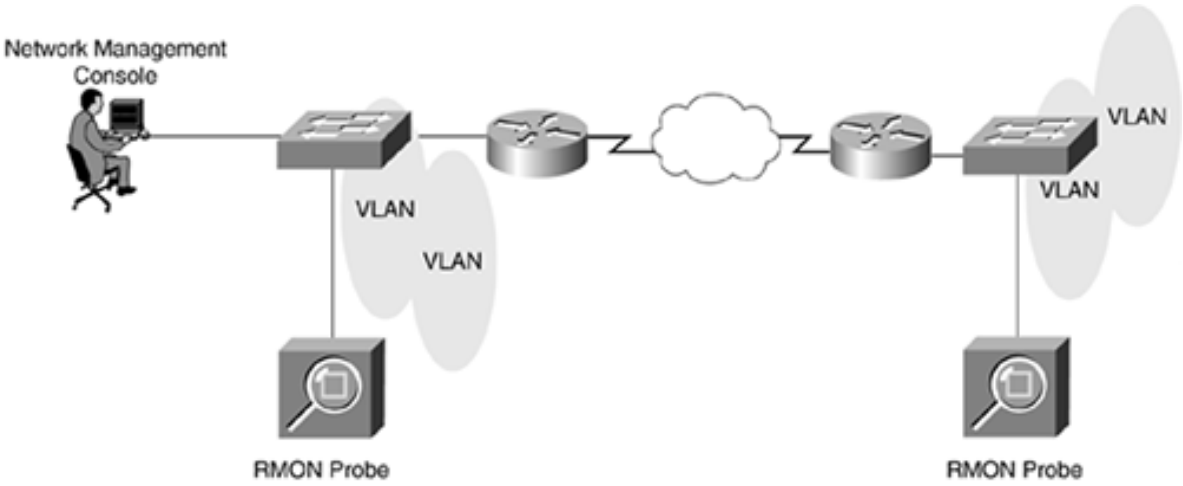
- Partición: utilización del espacio de la partición (poco nivel de detalle)
- Directorios: grado de utilización del espacio para los directorios.
- Ficheros: tamaño que ocupan los ficheros.

1.7.12 SEGURIDAD

La seguridad es un aspecto que afecta a todas las áreas de administración. Para cada recurso en la red, el administrador dispone de los mecanismos para establecer permisos de utilización, así como monitorizar el uso que se hace de los recursos. Todas estas tareas son muy complejas por lo que se utiliza actualmente son políticas de seguridad.

Las políticas de seguridad permiten establecer aspectos de seguridad en forma de perfiles que afectan a grupos de usuarios. Una vez definidas las políticas, el administrador sólo tiene que añadir los usuarios a los grupos establecidos con lo que adquieren los perfiles de seguridad. De esta forma la actualización de medidas de seguridad se hace sobre las políticas y no sobre los usuarios directamente. Otro aspecto a considerar es el de la monitorización y registro de las actividades de los usuarios pudiendo denegar el acceso de los usuarios en función de que intenten realizar actividades para los que no tienen permiso.

1.7.13 RMON (MONITOREO REMOTO)[4]

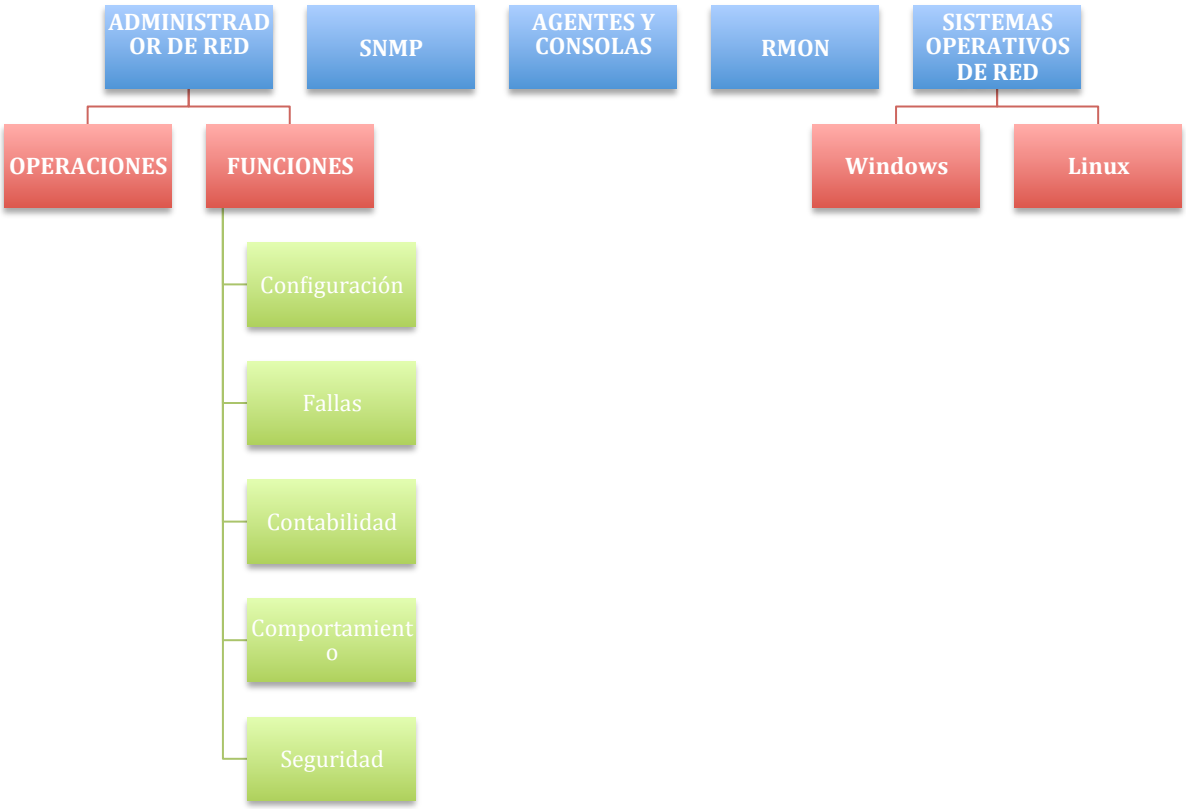


RMON es un estándar que define objetos actuales e históricos de control, permitiendo la captura de la información en tiempo real a través de la red entera. El estándar de RMON es una definición para Ethernet. Puede utilizar RMON para analizar y para vigilar datos del tráfico de la red dentro de segmentos alejados de la LAN. Esto permite detectar, aislar, diagnosticar, y señalar problemas potenciales y reales de la red antes de que se

[4] Imagen tomada de: http://etutorials.org/shared/images/tutorials/tutorial_59/11fig11.gif

extiendan a las situaciones de crisis. RMON permite instalar las historias automáticas, que el agente de RMON recoge durante todo el tiempo, proporcionando datos en la estadística básica tal como la utilización, colisiones (HERNÁNDEZ ESCOBAR, 2006).

El siguiente gráfico muestra el resumen de los principales conceptos relacionados con la administración de redes y servidores.



2. SISTEMAS OPERATIVOS DE RED

También conocido como NOS (Networh Operative System). Realmente se trata de un software que es necesario para integrar los componentes de la red, como archivos, periféricos y recursos, en un todo al cual el usuario final tiene un cómodo acceso. El sistema operativo de red controla y administra todos estos recursos, así el usuario se libra de posibles conflictos en el momento de usar la red.

Un equipo no puede trabajar sin sistema operativo, pero a su vez, una red de equipos es inútil sin un sistema operativo de red. De esta manera el usuario puede ver otros equipos conectados en red con sus sistemas operativos y usuarios o grupos de usuarios locales. Puede comunicarse con ellos e intercambiar información, ejecutar tareas, transferir archivos, permiten utilizar los servicios presentes en la red, etc. Es esto último la principal función de un sistema operativo de red, pero para ello el usuario debe copiar explícitamente el archivo de una instalación a otra, o sea, debe conocer el nombre del archivo y saber qué se ubica en éste o aquel equipo.

Nota: Actualmente las funciones de los sistemas operativos no se limitan a trasmitir archivos, van más allá, por las redes se trasmite voz, video y datos.

2.1 SISTEMAS OPERATIVOS PARA EQUIPOS SERVIDORES

Se debe desligar el concepto de servidor del PC, puesto que un servidor puede ser un router que asigne direcciones IP de forma dinámica. Un servidor es cualquier dispositivo que presta un servicio en una red de ordenadores. Los entornos de sistemas operativos de red más comunes son tres:

- Novell Netware
- Microsoft Windows
- UNIX/ Linux

La mayor diferencia entre estos sistemas es que, desde sus comienzos, Novell Netware ha sido un sistema cliente/servidor puro, mientras que Unix y Windows han desarrollado redes en las que cualquier estación de trabajo podía actuar como cliente o servidor de ciertas aplicaciones, con

independencia de la existencia de un equipo con un sistema operativo servidor instalado.

Un software servidor debe permitir:

- Compartir recursos: El sistema operativo debe encargarse de poner los recursos a disposición del resto de los equipos, especificar determinar el control y acceso que pueden realizar los distintos usuarios de dichos recursos y, por último, coordinar el acceso a los mismos.

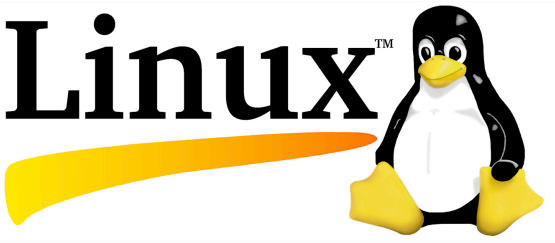
- Gestionar los usuarios de manera que se determine qué usuarios pueden acceder a la red y en qué situación.

- Administrar y controlar el estado de la red. Un equipo servidor, tal como ya hemos indicado, es aquel que presta una serie de servicios a otros equipos. Si tenemos en cuenta la posibilidad que un entorno de red (Novell, Windows o Unix/Linux) ofrece para la presencia de equipos que actúen como servidores, podríamos crear una gradación de situaciones en cuanto a la flexibilidad que proporciona cada uno de los sistemas operativos.

En las redes Novell es únicamente, el equipo servidor, con la aplicación de servidor instalada, el que puede realizar estas funciones. Los equipos con aplicaciones clientes no pueden encargarse de ninguna de estas tareas. En las redes Windows, equipos con sistemas operativos cliente, pueden ser habilitados para ofrecer servicios (actuar como servidor) al resto de los equipos de la red, sin embargo, sólo los sistemas operativos de servidor Windows Server pueden gestionar el acceso a la red. De este modo, en una red sin servidor Windows y con estaciones cliente de este sistema operativo, cada usuario controlaría el acceso a su equipo, sin la posibilidad de crear un control centralizado.

Por último, las redes Linux son completamente flexibles, en cualquier equipo, con independencia de la distribución que posea, puede actuar como servidor e implementar cualquier servicio, no hay ningún tipo de

restricciones en este sentido. Las situaciones que acabamos de plantear parten de la idea de redes con sistemas operativos homogéneos, sin embargo, actualmente, una red informática puede estar constituida por ordenadores que monten sistemas operativos distintos y será el sistema operativo servidor el que condicione el comportamiento de dicha red.



Para ello se han habilitado, desde las distintas empresas aplicaciones que se pueden instalar tanto en clientes como en servidores que posibilitan esta interoperatividad de sistemas. En cualquier caso, con independencia del sistema operativo que utilicen, deben comunicarse entre sí con un lenguaje común, es decir, debemos habilitar en todos ellos el mismo protocolo de comunicaciones ya sea NetBEUI, TCP/IP, IPX/SPX, etc. pues, en caso contrario, los equipos no podrían comunicarse entre sí.

2.2. ELEMENTOS CARACTERÍSTICOS DE LOS SISTEMAS OPERATIVOS

Los distintos sistemas operativos se diferencian por las soluciones que aportan a los requisitos de funcionamiento de un PC y de una red. Tal como hemos indicado, el sistema operativo se encarga de enlazar las aplicaciones con los dispositivos de hardware, por lo que deberá controlar elementos de ambas subestructuras.

- **Sistemas de archivos.** La forma de almacenar y localizar los ficheros en un disco duro es uno de los primeros problemas a resolver. Cada sistema operativo aporta una solución; así, Novell emplea el sistema DET o Windows 2000 NTFS. Además, cada sistema de almacenamiento supone la toma de decisiones sobre cómo se van a particionar las unidades de disco y cuáles van a ser los tamaños de las unidades mínimas de almacenamiento.

- **Servicios de directorio.** Base de datos centralizada de los recursos de la red. Cuando, en un principio existía un único servidor, y las redes no tenían un gran tamaño, la ubicación de los distintos objetos de la red y su administración era sencilla. Sin embargo, según fueron creciendo las

redes y aumentando el número de servidores este problema se agravó. Era necesario crear una base de datos que recogiera y centralizara toda la información. Los servicios de directorio como el NDS de Novell o el Active Directory de Windows son dos soluciones distintas a este mismo problema.

- **Seguridad de los servicios.** Otra tarea de los sistemas operativos es proporcionar seguridad para, por un lado administrar los servicios de directorio y, por otro para el servicio propiamente dicho. En muchos casos conviene que la base de datos esté repartida por varios servidores (aunque disponga de un único acceso), esta distribución permite que los datos almacenados se encuentren próximos a los elementos a los que hacen referencia, sin embargo, al estar la Base de datos repartida, es necesario establecer estrategias que coordinen las actualizaciones de datos, los accesos y las copias de seguridad.

- **Organización de la red.** Los distintos objetos que configuran una red se pueden agrupar en dominios o grupos de trabajo. La principal diferencia entre ambos es que el control de acceso sea centralizado o local. Los sistemas operativos pueden implementar una o ambas de estas estructuras posibilitando así la creación de distintos tipos de redes.

- **Protocolos de comunicación.** Protocolos nativos que emplean los sistemas operativos para la comunicación en la red.

2.3. REDES DE MICROSOFT WINDOWS

Las redes gestionadas por sistemas operativos Windows son redes entre iguales que pueden funcionar con independencia de la existencia o no de un equipo servidor. En este sistema, todos los ordenadores pueden actuar como clientes o servidores dentro de la red montando distintas versiones de sistemas operativos.

Cuando incluimos un equipo servidor, con software de sistema operativo servidor, podemos crear sistemas de acceso más seguros a la red,

administrarla de una forma centralizada y aportar una serie de servicios añadidos en función de la versión de sistema operativo instalada. Las redes Windows son ahora las más utilizadas debido a la facilidad de su instalación y a la similitud de procesos e interfaces con las versiones de usuarios.

2.3.1 GESTIÓN DE DISCOS

La gestión de discos de Windows es bastante conocida en sus aspectos básicos debido a que es el sistema operativo más utilizado. Un disco físico debe ser particionado, dimensionado y formateado. Una partición es una unidad de almacenamiento separada, es decir, en ella se puede instalar un sistema operativo, de este modo, un mismo PC puede incluir un disco con, por ejemplo, tres sistemas operativos, debiendo seleccionar con cuál queremos trabajar. Además de las particiones primarias podemos crear particiones extendidas, que no se formatean, pero que se dividen en unidades lógicas. Este sistema de almacenamiento requiere que configuremos una partición primaria como partición activa, de esta forma indicamos dónde vamos a instalar los archivos de inicio del sistema operativo.

Todo lo que acabamos de comentar es posible cuando empleamos un sistema de almacenamiento básico, el existente hasta la aparición de Windows 2000. Windows 2000 incorpora un nuevo sistema de almacenamiento, el almacenamiento dinámico que permite crear una única partición en lo que denominaríamos un disco dinámico, pero que puede ser dividido en volúmenes. La ventaja de los discos dinámicos es que podemos crear volúmenes que se extiendan a lo largo de distintos discos. La selección de un determinado sistema de volúmenes estará vinculado con la tolerancia a fallos que presente.

- Volumen simple: Se encuentra en un único disco y se puede extender hasta un máximo de 32 regiones. No es tolerante a fallos.

- Volumen distribuido: Volumen que se reparte a lo largo de varios discos dinámicos. No es tolerante a fallos. Se escribe en los discos de forma consecutiva, una vez que se llena la parte de volumen de un disco se

pasa a escribir en otro.

- Volumen con espejo: Para lograr tolerancia a fallos un sistema es crear un volumen de este tipo, que se compone de dos volúmenes simples en el que uno es una copia idéntica del otro.

- Volumen seccionado: Un volumen se distribuye a lo largo de varios discos dinámicos pero la escritura se distribuye en todos ellos, no se van llenando discos de forma secuencial. No es tolerante a fallos. Mejora el volumen distribuido pues permite una escritura y lectura más rápidas.

- Volumen RAID-5: Con un mínimo de tres discos duros se crea un volumen seccionado pero se añade información a cada partición de disco en el volumen de manera que se evita la pérdida de datos.

El sistema de discos dinámicos no se puede configurar como partición activa del disco aunque sí pueden incluir archivos del sistema operativo de manera que se garantice su tolerancia a fallos.

2.3.2 SISTEMA DE ARCHIVOS

Los sistemas operativos Windows pueden emplear como sistemas de archivos FAT16, FAT32 y NTFS. La utilización de uno u otro sistema va a permitir desarrollar o no una serie de posibilidades de utilización de ese mismo sistema operativo. No todas las versiones de Windows soportan todos los sistemas de archivos enumerados, así, sólo las versiones de Windows NT, Windows 2000 y Windows XP pueden instalarse sobre discos formateados con NTFS, mientras que todas las versiones desde Windows 95 en adelante se pueden instalar en FAT 32, MS-DOS y Windows 3.x son totalmente compatibles con FAT16, únicamente.

Los sistemas de archivo permiten determinar, entre otras cosas dónde se ubica cada una de las partes de un archivo, ya que, debido a la forma en que se escribe en los discos, los distintos ficheros no aparecen completos en las unidades de escritura (clusters) ni consecutivos.

2.3.3 SISTEMAS SERVIDORES DE WINDOWS

Desde la primera versión de Windows NT 3.1 los sistemas operativos servidores han sufrido una gran evolución. La utilidad de las redes de

ordenadores, sus ventajas han provocado un enorme crecimiento de las redes, en número y extensión. Redes mayores requerían mayores prestaciones y requisitos de administración y seguridad.

Windows ha mantenido una carrera en el diseño de sistemas operativos servidores aportando ideas que han inspirado a otras empresas del mismo modo que distintas versiones de Windows pueden haber adaptado ideas de otros sistemas de red.

Los SO de servidor de windows son muy similares en su arquitectura a los SO clientes, el núcleo es prácticamente idéntico, sin embargo, se caracterizan por incorporar servicios añadidos. Por ejemplo, en la última versión de Windows 2003 Server se incluyen, entre otros, los siguientes servicios:

- Servidor de archivos e impresión.
- Servidor Web y aplicaciones Web.
- Servidor de correo.
- Terminal Server.
- Servidor de acceso remoto/red privada virtual (VPN).
- Servicio de directorio, Sistema de dominio (DNS), y servidor DHCP.
- Servidor de transmisión de multimedia en tiempo real (Streaming).

Estos servicios deben ser aprovechados por las estaciones de trabajo que se conectan a la red controlada por este servidor. De Windows 2000 server podemos hablar de las versiones: Small Busisness Server 2000, Advanced Server 2000, Datacenter Server 2000, además del Windows Server 2000. Cada una de las versiones, tal como hemos indicado, incorpora distintos servicios, pero, además, presentan distintas capacidades en cuanto a soporte de procesadores y gestión de memoria. En este tema nos vamos a centrar en las versiones más adecuadas para el trabajo en un centro.

2.3.3.1 Windows NT

Windows NT posee un entorno muy similar a Windows 98, utilizan ambos la misma interfaz de red, los mismos protocolos, etc. En los dos sistemas se trabaja con la carpeta Entorno de red, de la misma forma. La principal diferencia, es que Windows NT es un sistema operativo concebido como servidor, al contrario que Windows 98, que estaba concebido como

cliente, aunque en ocasiones pueda hacer de servidor también. Windows NT, tiene un sistema de seguridad, con autentificación diferente. Exige una cuenta de usuario, con derecho de acceso a los recursos. Fue concebido para dar soporte a aplicaciones complejas que trabajan en modo multiusuario y con unos mecanismos de seguridad mínimos para la industria. Windows NT tiene una versión diseñada para los puestos de trabajo (Windows NT Workstation) y una familia de versiones para trabajar en los servidores (Windows NT Server).

Características de Windows NT

Las principales características son:

- **Sistema operativo a 32 bits:** Windows NT se creó para trabajar desde el principio con 32 bits, dejando en el olvido los sistemas anteriores de 16 bits. Sistema de archivos NTFS (New Technology File System): Es un sistema de almacenamiento de archivos que incorpora seguridad en archivos y directorios. Controla mejor la fragmentación de archivos. Windows NT también incluye soporte para FAT (aunque no para FAT32) y HPFS (sistema de archivos de OS/2).

- **Multiusuario:** Un servidor con Windows NT, permite el acceso de varios usuarios a la vez desde distintos puestos de la red. Cada usuario puede ser propietario de objetos (carpetas, servicios, etc.) y, por ello, pueden administrar y controlar el acceso a estos objetos.

- **Multitarea:** Permite la ejecución simultánea de distintas aplicaciones. Aunque el procesador atienda únicamente una tarea en cada momento. Esto aumenta la velocidad enormemente.

- **Multiprocesador:** Puede soportar varios procesadores en el mismo ordenador, y cada uno trabajando a la vez con una tarea distinta.

- **Espacios de memoria separados:** Windows NT, se creó a partir de un núcleo experimental de UNIX, llamado Mach OS, que trabaja en modo multihebra y con derecho preferente. Debido a esto, además de una tecnología de subsistemas protegidos, puede trabajar con programas y aplicaciones en espacios de memoria separados. Esto impide que

cuando falla un programa se produzca el fallo del resto de programas en ejecución. Se puede abortar dicho programa sin afectar al resto de los programas en funcionamiento.

- **Portabilidad:** Windows NT puede funcionar en distintos tipos de hardware.

- **Trabajo en entornos mixtos:** Windows NT puede trabajar en distintos tipos de redes, cada cual con su protocolo. Por ejemplo: Novell Netware con IPX/SPX, Unix mediante TCP/IP, Macintosh con AppleTalk, Windows mediante NetBEUI, etc.

- **Validación en un dominio:** Los controladores de dominio son los ordenadores que se encargan de la autentificación de los usuarios de ese dominio. Para ello tiene una base de datos de usuarios o SAM (Security Account Manager). De esta manera, el acceso a los recursos de la red está controlado.

Tolerancia a fallos: Windows NT posee mecanismos para trabajar aunque se produzca algún fallo. Un mecanismo orientado a esto es RAID (Redundant Array of Inexpensive Disk), que controla la pérdida de datos, incluso cuando falle el disco duro del ordenador.

2.3.3.2 Windows 2000 Server

Windows 2000, sería en realidad la versión 5 de Windows NT, pero Microsoft decidió en esta versión cambiar de nombre a Windows 2000. Por tanto es una extensión de Windows NT, y tiene la misma filosofía. Anteriormente existían dos líneas de Windows; Windows 98 para redes punto a punto, trabajo en grupo o individual en un ordenador aislado; y Windows NT, para trabajo en red, con servidores y, normalmente, dentro de un dominio. En Windows 2000 convergen estas dos líneas.

Windows 2000 está concebido, al igual que Windows NT, para dar soporte a aplicaciones complejas que trabajan en modo multiusuario y con unos mecanismos de seguridad mínimos para la industria. Dispone de una versión diseñada para empresas y usuarios finales (Windows 2000

Profesional) y varias versiones con herramientas de administración y gestión de red (Windows 2000 Server es la versión más basica de los servidores Windows 2000).

Características

- **Seguridad:** Identificación de usuarios. Seguridad local y de red. Revisión de carpetas, impresoras, etc. El protocolo Kerberos, utilizado en Windows 2000, es un protocolo de autenticación de red, para transmitir datos a través de redes inseguras. Las relaciones de confianza transitivas de Kerberos, permiten a Win2000 crear árboles y bosques de dominios. Kerberos utiliza la autenticación mutua, el servidor y el cliente verifican la autenticidad de su compañero. Win2000 utiliza el sistema de clave pública (PKI). PKI es un sistema de certificados digitales y Certificate Authorities (CAs), que hace que en una transacción, las dos partes verifiquen la autenticidad de la otra y encripten la transacción. PKI se usa en Internet para el comercio electrónico seguro.

- **Tolerancia a fallos.** Windows 2000 posee mecanismos para trabajar aunque se produzca algún fallo. Un mecanismo orientado a esto es RAID (Redundant Array of Inexpensive Disk), que controla la pérdida de datos, incluso cuando falle el disco duro del ordenador.

- **Integración con Internet.** Server incluye Internet Information Server (IIS), una plataforma segura de servidor Web.

- **Directorio activo:** sistema de servicios de directorio aplicable a redes ilimitadas en su tamaño. Mejora el sistema de Windows NT (SAM) y se asemeja al empleado en las redes Novell (NDS).

Arquitectura

Windows 2000, al igual que Windows NT, tiene dos capas, que separan en dos niveles las funciones. Cada capa tiene un modo de funcionamiento distinto: modo Kernel, con este modo se hacen las tareas más internas; y modo usuario, con el que se ejecutan las aplicaciones.

Modo Kernel o Núcleo:

El Kernel o Núcleo es, en Windows 2000, algo parecido al corazón. Hace de

intermediario entre el sistema operativo y el procesador del ordenador. Tiene acceso al sistema de datos y al hardware y ejecuta en un área de memoria protegida. Sus principales componentes del núcleo son:

1. Executive Services: cada servicio se encarga de una función. Las principales son:
    a. Administrar las Entradas/Salidas (I/O) hacia cualquier dispositivo.
    b. Administrador de objetos: gestiona todos los posibles objetos utilizados por Windows 2000.
    c. Administrador de procesos.
    d. Administrador de memoria virtual.
2. HAL (Hardware Abstraction Layer) (Capa de Abstracción de Hardware): controla la interacción del Núcleo con el Hardware. Su misión, es abstraer o hacer que el sistema ignore, el tipo de hardware de la máquina. Windows 2000, no permite al software el acceso directo al hardware, siempre tiene que pasar por el HAL. Gestiona las interfaces de Entrada/Salida, controladores de interrupción y la comunicación multiprocesador.

3. Controladores del modo núcleo: son un conjunto de componentes modulares, cada uno con una función.

Modo usuario:

En este modo, Windows 2000, usa un serie de subsistemas de entorno o ambiente, encargado cada uno de un tipo de aplicación, según el sistema operativo (Win32, OS/2, POSIX), emulándolos. Las aplicaciones y usuarios finales, no tienen porqué conocer nada de lo que pasa en el núcleo. Cada programa se ejecuta en un espacio de memoria diferente, así no puede haber interferencias entre ellos. Hay otra serie de subsistemas, llamados integrales, que gestionan la seguridad y el trabajo en red.

Servicios de directorio. Directorio Activo.

El Directorio Activo es una base de datos que almacena información sobre todos los recursos de la red y permite administrarlos. Nos da información sobre los recursos de la red, tales como usuarios, grupos, ordenadores, impresoras, etc. Estos recursos, son los llamados Objetos del Directorio Activo. Estos objetos son almacenados en unas Unidades Organizativas

(OUs, Organizational Units) de forma jerárquica. Las Unidades Organizativas, se usan para organizar objetos dentro de un dominio, de manera parecida a una estructura empresarial.

Todos estos objetos forman una gran base de datos, que guarda información sobre usuarios, recursos y seguridad de la red. Permite a los administradores gestionar y controlar la red. Un Servicio de directorio, proporciona los medios para la gestión de los diversos objetos del Directorio. Con el se pueden hacer:

- Administrar la seguridad de acceso a los diversos objetos de la red.
- Replicar o hacer copias de seguridad de un directorio en varios ordenadores.
- Repartir los diversos objetos de la red en distintos ordenadores.

Active Directory proporciona mejoras con respecto a SAM de Windows NT a la hora de administrar los objetos de una red. Mientras que SAM presentaba una estructura plana, en el que se gestionaban dominios, AD ofrece una estructura jerárquica en árbol, donde están representados todos los objetos de la red, que permite adaptarse mucho mejor a una red grande o en constante evolución. Aunque también trabaja con dominios, su principal ventaja es que éstos están integrados en la estructura y se pueden modificar dominios enteros de una forma sencilla.

Los dominios son las unidades organizativas básicas. Los dominios se pueden agrupar en árboles y los árboles pueden constituir un bosque. AD permite acceder, por ejemplo, a un árbol completo, con varios dominios y administrarlo como si fuera un único objeto. Ad permite gestionar los usuarios de varios dominios simultáneamente, mientras que SAM sólo permitía gestionar los usuarios de un único dominio.

Como podemos observar, la estructura de Active Directory de Windows 2000 Server es muy similar a NDS de Novell. La estructura jerárquica en árbol dispone de objetos contenedores (Unidades Organizativas), que pueden incluir otros objetos denominados hojas. La estructura de árbol que presenta active Directory no debe confundirse con la agrupación lógica que podamos hacer de usuarios o grupos, pues estos son objetos de Active Directory, no unidades jerárquicas.

Trabajo en red.

En Windows 2000 las funciones de red vienen ya integradas. Los ordenadores pueden operar como clientes o servidores, en una red de tipo cliente-servidor o punto a punto.Windows 2000 Server es un servidor de archivos, de aplicaciones, de impresión y servidor web. Windows 2000 Server, tiene un elemento fundamental para el trabajo en red, el Directorio Activo (AD).

Grupos de trabajo.

Cada ordenador del grupo, tiene una base de datos de seguridad local, con los usuarios y recursos del grupo. No hay una base de datos centralizada. Un grupo de trabajo, no necesita una administración centralizada, y no necesita tener instalado Windows 2000 Server en ningún ordenador.

Dominios.

Un dominio, es una agrupación lógica de ordenadores, que tienen una base de datos centralizada, o directorio. Esta base de datos contiene toda la información sobre los usuarios y recursos del dominio. En el dominio, hay siempre algún ordenador dedicado a contener el directorio, se le llama controlador de dominio. El dominio, necesita una administración centralizada, y necesita tener instalado Windows 2000 Server en el controlador de dominio. Los ordenadores del dominio pueden estar próximos, o repartidos geográficamente por cualquier parte del mundo. La característica esencial de un dominio es la organización centralizada, con todas las ventajas de control, seguridad y gestión que esto conlleva. El acceso a cualquier objeto del dominio, está controlado por el administrador, que define los derechos de acceso y la política de seguridad del dominio.

Los dominios se pueden agrupar jerárquicamente (padres, hijos) para formar un árbol. De esta forma los dominios del árbol pueden compartir información común. Hay un directorio único para todo el árbol, y cada dominio posee una parte de dicho directorio. Los árboles se pueden agrupar en un bosque. Todos los árboles del bosque tienen un esquema y

unas reglas comunes. Hay un catálogo global, con todos los objetos, para todos los dominios del bosque.

Sistema de Nombres de Dominio (DNS).

Windows, usa el protocolo DNS para resolver (convertir) los nombres de los ordenadores, a direcciones de IP (Protocolo Internet). Windows también usa DNS para su servicio de nombres de dominio. De esta forma el protocolo DNS, permite utilizar el mismo sistema de nombres en Internet y en la red local, para nombrar los dominios.

Windows emplea, igualmente, DNS Dinámico (Dynamic DNS, DDNS). Este protocolo, permite a los ordenadores clientes, que tienen direcciones IP asignadas dinámicamente (DHCP), poder registrarse directamente en un servidor DNS y actualizarla base de datos DNS. Este sistema, reduce la necesidad cambiar manualmente y replicar la base de datos DNS, cada vez que haya algún cambio en la configuración de un cliente.

DNS, utiliza una estructura jerárquica de nombres. Cada dominio tiene un nombre. Un dominio, en DNS, es un nodo que representa una partición de la base de datos de DNS. El nombre último, el de un ordenador concreto de una red (host), es el término situado más a la izquierda.

Control de acceso a objetos.

El modelo de seguridad de Windows 2000, se basa en el control de acceso a los objetos. Este control está basado en los permisos. Cada objeto del Directorio Activo, tiene definido qué tipo de acceso está permitido, y quién tiene permiso para acceder. A efectos prácticos, se pueden agrupar los objetos en Unidades Organizativas (OU), para asignar los mismos permisos a todos los miembros de la OU. Los permisos para acceder a un objeto, los da el propietario del objeto o el administrador.

Cada objeto tiene una lista (ACL) de permisos de acceso, con los usuarios, grupos, etc. y tipos de permiso. También un Descriptor de seguridad, que podemos concebir como una "cerradura". Cualquier usuario que quiera acceder a dicho objeto debe tener una "llave" para poder acceder. Cada usuario, al iniciar una sesión en un ordenador, obtiene una "llave", la

Señal de acceso de seguridad (SAT). Con esta "llave", podrá abrir unas "cerraduras" sí, y otras no, o sea, podrá, o no, acceder a los objetos.

Los permisos varían según el tipo de objeto. Por ejemplo, una carpeta puede tener permiso de lectura o escritura o para borrar; crear o modificar ficheros; mover un fichero de una carpeta a otra; etc. Un usuario concreto, puede pertenecer a uno o varios grupos y, por tanto, tener los permisos correspondientes a cada uno de los grupos. Los permisos se pueden conceder o negar. Siempre tiene prioridad un permiso denegado. Cada objeto debe tener al menos un usuario, lo normal es el propietario o el administrador, que tenga un permiso total. Los permisos se pueden heredar, desde un objeto padre a un hijo. También se puede delegar un permiso, desde el administrador a un usuario o grupo.

Usuarios.

Un usuario, como este nombre indica, es una persona que inicia una sesión de trabajo en Windows 2000. Para poder trabajar (iniciar una sesión), en Windows 2000, se debe tener una cuenta de usuario. Esta es un registro, con el nombre de usuario, contraseña, grupos a los que pertenece y los permisos de acceso a los recursos del sistema. Windows 2000, no te deja acceder a la red si no te identificas.

Las cuentas de usuarios, se almacenan en una base de datos llamada Administrador de cuentas de seguridad (SAM). Una cuenta de usuario, da la posibilidad de iniciar una sesión en un dominio, para acceder a los recursos de una red; o en un ordenador concreto, para acceder a los recursos de ese ordenador. Una cuenta de usuario de dominio, está dentro de una Unidad Organizativa (OU), y estará almacenada en la base de datos del Directorio Activo, en un controlador de dominio. Si hay varios controladores de dominio, la información se duplica en cada uno.

Una cuenta de usuario local, se almacena en la base de datos de seguridad (SAM) del ordenador, y no en el controlador de dominio. Hay algunas cuentas de usuarios predefinidas, como el Administrador e Invitado. La cuenta de usuario Administrador, tiene privilegios para crear y modificar cuentas de usuarios y grupos, definir directivas de seguridad, asignar permisos, etc. La cuenta de usuario Invitado, se usa para usuarios

ocasionales. Para una cuenta de usuario determinada, se puede crear un Perfil de usuario, que contiene una serie de carpetas y configuraciones con datos personales.

Grupos de Usuarios.

Lo más normal es que los usuarios se agrupen de una manera lógica, de acuerdo a algún criterio, en lo que se denomina grupo de trabajo, para ello se les asignará un nombre de grupo. Un grupo, es un conjunto de cuentas de usuarios. Los grupos se crean para simplificar la administración de una red. Así, los permisos y derechos, se pueden asignar a grupos, en lugar de hacerlo individualmente, a cada usuario. Un usuario puede pertenecer a uno o varios grupos. Además de usuarios, un grupo puede contener contactos, ordenadores y otros grupos.

Los permisos son reglas asociadas a objetos, como carpetas, archivos o impresoras. Definen qué usuarios pueden acceder a dichos objetos y qué pueden hacer. Las acciones que se pueden hacer en una carpeta, pueden ser leer, modificar o crear archivos en su interior. En una impresora, pueden ser eliminar tareas, configurar, etc. Los derechos son reglas que definen las acciones, que pueden hacer los usuarios, tales como, hacer una copia de seguridad de un ordenador, apagar el sistema, etc.

A cada usuario se le adjudica un permiso o privilegio, sobre los recursos del sistema. Según el permiso que tenga un usuario podrá o no acceder a un recurso, y también nos dirá qué acciones podrá o no hacer (leer, escribir, imprimir, etc.). Cada usuario puede tener un permiso o privilegio individual, pero es más práctico crear grupos de usuarios que tengan los mismos privilegios.

Tipos de Grupos.

Hay dos clases de grupos:

- Grupo de seguridad: son los utilizados para asignar permisos.
- Grupo de distribución: para funciones de correo. En este tipo de grupos no se pueden asignar permisos.

Ámbito de los Grupos.

Hay tres clases de grupos, según su ámbito de actuación:

1. Grupos locales de dominio: son los utilizados para asignar permisos, para acceder a los recursos de ese dominio exclusivamente. Pueden contener miembros de otro dominio.
2. Grupo globales: son los utilizados para agrupar usuarios del dominio desde el cual se crea el grupo, con las mismas necesidades de recursos de red. Pueden acceder a recursos de su dominio o de otros.
3. Grupos universales: son los utilizados para asignar permisos, para acceder a los recursos de varios dominios. Pueden contener miembros de cualquier dominio.

Normas para la creación de los Grupos.

Se recomienda seguir los siguientes pasos:

1. Creación de los grupos globales, incluyendo a los usuarios de cada grupo. Ejemplos: Contabilidad, Ventas.
2. Creación de los grupos locales de dominio, agrupando los recursos, y asignándolos a cada grupo local. Ejemplo: Impresoras color, Escáneres.
3. Agregar los grupos globales, que tengan que acceder a los recursos, al grupo local adecuado. Ejemplo: agregar Ventas a Escáneres y Contabilidad a Impresoras color.
4. Asignar los permisos pertinentes al grupo local de dominio.

Políticas o directivas de grupo.

Las políticas de grupo, son un conjunto de opciones de configuración de los ordenadores y de los usuarios. Estas opciones, se guardan en los objetos de políticas de grupos (Group Policy Objects, GPOs), y están asociados a objetos del Active Directory, tales como dominios o unidades organizativas. De esta forma se puede controlar el entorno de trabajo de un grupo de usuarios, una Unidad Organizativa o un dominio, de una forma centralizada.

En las directivas de grupo, se pueden incluir parámetros de software, de seguridad, programas disponibles a los usuarios, escritorio, acceso restringido a carpetas del sistema Windows 2000 , derechos de las cuentas de usuario, etc. Se puede evitar que los usuarios instalen software o accedan a programas o datos no autorizados, que borren datos o programas importantes, etc. Los administradores, son los que configuran estas directivas de grupo.

2.3.3.3 Windows Server 2003

Se trata del sistema operativo de Microsoft, heredero de Windows 2000 Server al que añade opciones que permiten una gestión más flexible de la red a la vez que se aumenta su seguridad. Mejora la administración del Directorio activo y de las unidades de almacenamiento, tanto discos dinámicos como unidades extraíbles. Incorpora un servidor web y permite el alojamiento y creación de sitios XML web dinámicos. Se trata de la evolución natural de Windows 2000 Server ofreciendo opciones mejoradas e implementando tecnologías que han aparecido en los últimos años.

2.3.3.4 Windows Server 2008

Algunas diferencias con respecto a la arquitectura del Windows Server 2008, afectan la manera en como se gestiona el sistema hasta el punto de que se pueden llegar a controlar hardware de forma más efectiva, se puede controlar de forma remota y cambiar de forma radical la política de seguridad. A continuación 10 de las mejoras:

- **Nuevo proceso de reparación de sistemas NTFS:** proceso en segundo plano que repara los archivos dañados.
- **Creación de sesiones de usuario en paralelo:** reduce tiempos de espera en los Terminal Services y en la creación de sesiones de usuario a gran escala.
- **Cierre limpio de Servicios:** se acabó el tiempo de espera antes de la finalización de servicios.
- **Kernel Transaction Manager:** mejoras en la gestión concurrente de recursos.
- **Sistema de archivos SMB2:** de 30 a 40 veces más rápido el acceso a los servidores multimedia.

- **Address Space Load Randomization (ASLR):** protección contra malware en la carga de drivers en memoria.
- **Windows Hardware Error Architecture (WHEA):** protocolo mejorado y estandarizado de reporte de errores.
- **Virtualización de Windows Server:** mejoras en el rendimiento de la virtualización.
- **PowerShell:** inclusión de una consola mejorada con soporte GUI para administración.
- **Server Core:** el núcleo del sistema se ha renovado con muchas y nuevas mejoras (Genbeta, 2007).

2.3.3.5 Windows Server 2012

Windows Server 2012 ofrece a las empresas y proveedores de servicios una infraestructura escalable, dinámica, para varios inquilinos y optimizada para la nube. Windows Server 2012 permite que las organizaciones se conecten de manera segura entre las diferentes instalaciones y sirve para que los profesionales de TI respondan en forma más rápida y eficaz a las necesidades de negocio (Center, 2015).

Novedades del acceso cableado autenticado mediante 802.1X
Nuevas características del acceso mediante cable con autenticación de 802.1X en Windows Server 2012 R2 y Windows 8,1.

Novedades del acceso inalámbrico autenticado mediante 802.1X
Nuevas características del acceso inalámbrico con autenticación de 802.1X en Windows Server 2012 R2 y Windows 8,1, como la pantalla inalámbrica Miracast y una conexión Wi-Fi más rápida con 802.11ac.

Novedades de Active Directory en Windows Server
Características de Active Directory para permitir que los empleados y socios puedan acceder a los datos corporativos protegidos desde sus dispositivos personales y, al mismo tiempo, controlar los riesgos y el uso de los recursos corporativos.

Novedades de Servicios de dominio de Active Directory (AD DS)
Los Servicios de dominio de Active Directory (AD DS) en Windows Server 2012 incluyen nuevas características que permiten implementar de manera más rápida y sencilla controladores de dominio (tanto locales como en la

nube), aumentar la flexibilidad y facilidad al auditar y autorizar el acceso a archivos con el control de acceso dinámico, así como realizar de manera sencilla tareas administrativas a escala local o remota a través de experiencias uniformes de administración mediante interfaz gráfica y mediante scripts.

Novedades de Active Directory Rights Management Services (AD RMS)

AD RMS es el rol de servidor que le proporciona herramientas de administración y desarrollo que funcionan con las tecnologías de seguridad de la industria (incluido el cifrado, los certificados y la autenticación) que ayudan a las organizaciones a crear soluciones de protección de información confiable.

BitLocker

BitLocker admite el cifrado de dispositivos en equipos basados tanto en x86 como en x64 con un Módulo de plataforma segura compatible con el modo de espera conectado. La nueva funcionalidad. BitLocker cifra las unidades de disco duro del equipo para proporcionar una protección mejorada frente al robo o la exposición de datos en equipos perdidos o robados.

Novedades de BranchCache

BranchCache en Windows Server 2012 y Windows 8 proporciona mejoras sustanciales en el rendimiento, la manejabilidad, la escalabilidad y la disponibilidad.

Servicios de certificado de Active Directory

Servicios de certificado de Active Directory en Windows Server 2012 R2 admite un módulo de directivas para el Servicio de inscripción de dispositivos de red, la atestación de la clave de TPM y nuevos cmdlets de Windows PowerShell para tareas de copia de seguridad y restauración. AD CS en Windows Server 2012 proporciona varias características y capacidades nuevas con respecto a versiones anteriores, entre ellas la nueva implementación, la manejabilidad y las capacidades agregadas a AD CS en Windows Server 2012.

Desduplicación

La desduplicación de datos puede instalarse en un recurso de archivos de escalabilidad horizontal y usarse para optimizar discos duros virtuales (VHD) dinámicos en cargas de trabajo de Infraestructura de escritorio virtual (VDI).

Novedades de la replicación DFS y los espacios de nombres DFS en Windows Server

Se han agregado a la Replicación DFS (DFSR o DFS-R) en Windows Server 2012 R2. Los espacios de nombres DFS y la Replicación DFS en Windows Server 2012 proporcionan una nueva funcionalidad de administración, así como la interoperabilidad con DirectAccess y la desduplicación de datos.

DHCP

El Protocolo de configuración dinámica de host (DHCP) en Windows Server 2012 R2 proporciona nuevas características y capacidades con respecto a las versiones anteriores. Nuevas características de implementación, administración y capacidades agregadas al rol de servidor DHCP en Windows Server 2012 R2. Protocolo de configuración dinámica de host (DHCP) es una norma del Grupo de trabajo en ingeniería de Internet (IETF) diseñada para reducir la carga administrativa y la complejidad de configurar hosts en una red TCP/IP, como una intranet privada.

Servidor DNS

Nuevas funcionalidades en el servicio Servidor DNS en Windows Server 2012 R2. Los servicios DNS (Domain Name System) se usan en redes TCP/IP para nombrar equipos y servicios de red. Los nombres de DNS encuentran equipos y servicios a través de nombres descriptivos.

Clústeres de conmutación por error

Funcionalidades de clústeres de conmutación por error que son nuevas o han cambiado en Windows Server 2012 R2. Los clústeres de conmutación por error ofrecen alta disponibilidad y escalabilidad para muchas cargas de trabajo de servidor. Entre ellas se incluye el almacenamiento de recursos compartidos de archivos para aplicaciones de servidor como Hyper-V y Microsoft SQL Server, y aplicaciones de servidor que se ejecutan en servidores físicos o en máquinas virtuales.

Novedades del Administrador de recursos del servidor de archivos en Windows Server

El Administrador de recursos del servidor de archivos proporciona un conjunto de características que permite administrar y clasificar los datos almacenados en los servidores de archivos.

Directiva de grupo

La directiva de grupo es una infraestructura que permite especificar configuraciones administradas para los usuarios y los equipos a través de la configuración de directiva de grupo y las preferencias de directiva de grupo.

Novedades de Hyper-V para Windows Server 2012 R2

El rol Hyper-V permite crear y administrar un entorno informático virtualizado mediante la tecnología de virtualización integrada en Windows Server 2012. Hyper-V virtualiza el hardware con el fin de proporcionar un entorno en el que es posible ejecutar varios sistemas operativos al mismo tiempo en un equipo físico, ejecutando para cada sistema operativo en su propia máquina virtual.

IPAM

La Administración de direcciones IP (IPAM) es una característica que apareció por primera vez en Windows Server 2012 y que proporciona funcionalidades de supervisión y administración muy personalizables para la infraestructura de direcciones IP en una red corporativa. IPAM en Windows Server 2012 R2 conlleva numerosas mejoras.

Autenticación Kerberos

Los sistemas operativos Microsoft Windows Server implementan el protocolo de autenticación Kerberos versión 5 y las extensiones para la autenticación basada en contraseña y clave pública. El cliente de autenticación Kerberos se implementa como un proveedor de compatibilidad para seguridad (SSP) al que se puede acceder a través de la interfaz del proveedor de compatibilidad para seguridad (SSPI).

Servicios de Escritorio remoto

El rol del servidor Servicios de Escritorio remoto proporciona tecnologías que permiten a los usuarios conectarse a escritorios virtuales, programas RemoteApp y escritorios basados en sesión. Con Servicios de Escritorio remoto, los usuarios pueden obtener acceso a conexiones remotas desde una red corporativa o desde Internet.

Administrador del servidor

Administrador de servidores en Windows Server 2012 permite que los administradores administren varios servidores remotos que ejecutan Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 o Windows Server 2003.

Tarjetas inteligentes

Las tarjetas inteligentes y sus números de identificación personal asociados (PIN) son un método rentable, confiable y cada vez más popular para autenticación de dos factores. Con los controles adecuados implementados, un usuario debe contar con la tarjeta inteligente y conocer el PIN para obtener acceso a los recursos de red.

TLS/SSL (Schannel SSP)

Schannel es un proveedor de compatibilidad para seguridad (SSP) que implementa los protocolos de autenticación estándar de Internet de SSL y TLS. La interfaz del proveedor de compatibilidad para seguridad (SSPI) es una API que usan los sistemas Windows para realizar funciones basadas en la seguridad, incluida la autenticación.

Servicios de implementación de Windows en Windows Server

Un servidor con Servicios de implementación de Windows (WDS) que ejecuta Windows Server 2012 R2 se puede administrar mediante cmdlets de Windows PowerShell para WDS. Con los cmdlets de Windows PowerShell se pueden agregar paquetes de controladores, agregar imágenes de cliente, habilitar y deshabilitar imágenes de arranque y de instalación y realizar otras muchas tareas comunes de WDS (Server, 2014).

2.4 REDES LINUX

Hablar de redes de ordenadores a menudo significa hablar de UNIX. Creado en los 70 por un grupo de programadores en los laboratorios Bell como un sistema operativo multiusuario y multitarea, pequeño y flexible, UNIX es uno de los más populares del mundo debido a su extenso soporte y distribución. Según muchos programadores, UNIX es el auténtico y único sistema operativo: Robusto, eficaz y versátil. Es uno de los primeros sistemas operativos creados en el lenguaje de programación de alto nivel C. Esto hace posible su instalación en cualquier máquina que tenga un compilador de C. UNIX es el sistema operativo más extendido en equipos servidores. Existen dos versiones de UNIX, Solaris y Linux. Optaremos por analizar más detenidamente esta última por sus características de desarrollo y su mayor extensión en el mundo educativo.

2.4.1 Protocolos de comunicación en redes con Linux

Siendo el resultado del esfuerzo concentrado de programadores de todo el mundo, Linux no habría sido posible sin la red global. Así que no sorprende que ya en los primeros pasos del desarrollo, varias personas comenzaron a trabajar en dotarlo de capacidades de red. Linux dispone de los dos principales protocolos de red para sistemas UNIX: TCP/IP y UUCP.

UUCP

UUCP (UNIX-to-UNIX Copy) es un viejo mecanismo usado para transferir ficheros, correo electrónico y noticias entre máquinas UNIX. Clásicamente las máquinas UUCP conectan entre ellas mediante líneas telefónicas y módem, pero UUCP es capaz de funcionar también sobre una red TCP/IP. Si no tiene acceso a una red TCP/IP o a un servidor SLIP, puede configurar su sistema para enviar y recibir ficheros y correo electrónico usando UUCP. Su principal aplicación es todavía en redes de área metropolitana (MAN) basadas en enlaces telefónicos.

Una de las principales desventajas de las redes UUCP es su bajo ancho de banda. Por un lado, el equipo telefónico establece un límite rígido en la tasa máxima de transferencia. Por otro lado, los enlaces UUCP raramente son conexiones permanentes; en su lugar, los nodos se llaman entre sí a intervalos regulares. Es por ello, que la mayoría del tiempo que le lleva a un

mensaje viajar por una red UUCP permanece atrapado en el disco de algún nodo, esperando al establecimiento de la próxima conexión.

A pesar de estas limitaciones, aun hay muchas redes UUCP funcionando en todo el mundo, utilizado principalmente por aficionados, ya que ofrecen acceso de red a usuarios privados a precios razonables. La razón fundamental de la popularidad del UUCP es que es baratísimo comparado con tener el ordenador conectado al Gran Cable de Internet. Para hacer de su ordenador un nodo UUCP, todo lo que necesita es un módem, software UUCP, y otro nodo UUCP que desee suministrarle correo y noticias.

TCP/IP

Aunque UUCP puede resultar una elección razonable para enlaces de red mediante llamada de bajo coste, hay muchas situaciones en las que su técnica de almacenamiento y reenvío se muestra demasiado inflexible, por ejemplo en Redes de Area Local (LANs). TCP/IP (Transmission Control Protocol/Internet Protocol) es un conjunto de protocolos de red que permite a sistemas de todo el mundo comunicarse en Internet.

Con Linux, TCP/IP y una conexión a la red, puede comunicarse con usuarios y máquinas por toda Internet mediante correo electrónico, noticias (USENET news), transferencias de ficheros con FTP y mucho más. Actualmente hay muchos sistemas Linux conectados a Internet. No todo el mundo tiene una conexión Ethernet en casa, así que Linux también proporciona SLIP (Serial Line Internet Protocol), el cual permite conectarse a Internet a través de un módem. Para poder usar SLIP, necesitará tener acceso a un servidor de SLIP, una máquina conectada a la red que permite acceso de entrada por teléfono.

Muchas empresas y universidades tienen servidores SLIP disponibles. De hecho, si su sistema Linux dispone de conexión Ethernet y de módem, puede configurarlo como servidor de SLIP para otros usuarios. Existe Net-3, que ofrece controladores de dispositivo para una amplia variedad de tarjetas Ethernet, así como SLIP (para enviar trafico de red sobre líneas serie), y PLIP (para líneas paralelo). Con Net-3, Linux tiene una implementación de TCP/IP que se comporta muy bien en entornos de red de área local, mostrándose superior a algunos de los Unix comerciales para PC (Redes en educación, sf).

Para complementar puede visitar el siguiente enlace:

Guía de Administración de Redes con Linux
http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/

2.5 SERVICIOS DE RED EMPRESARIAL

2.5.1 ADMINISTRACIÓN DEL SERVICIO NFS

El NFS permite que los ordenadores exporten (hagan disponibles) e importen (obtengan acceso) a directorios, sistemas de ficheros y dispositivos periféricos, de forma que los sistemas de ficheros de ordenadores remotos se comportan como si fueran locales. El servicio NFS utiliza, para su funcionamiento, los servicios proporcionados por el protocolo de representación de datos externos (eXternal Data Representation, XDR) de la capa de presentación del modelo OSI y el protocolo de llamada a procedimiento remoto (Remote Procedure Call, RPC) de la capa de sesión del modelo OSI. Por debajo, dependiendo de la versión del protocolo, se utiliza UDP y/o TCP para la capa de transporte e IP para la capa de red. En concreto, la versión 1 de NFS utiliza solo UDP, mientras que las versiones 2 y 3 de NFS utilizan TCP y UDP para la capa de transporte, mientras que la versión 4 solamente utiliza TCP[5].

2.5.2 SERVIDOR DE NFS

El servidor de NFS es el ordenador que exporta los sistemas de ficheros. La exportación de los sistemas de ficheros en las versiones 2 y 3 se realiza siempre a ordenadores remotos y nunca a usuarios concretos, por lo cual no existe la posibilidad de exportar un sistema de ficheros a un usuario concreto de un ordenador, sino que un sistema de ficheros exportado a un ordenador es accesible a todos los usuarios de ese ordenador. Este

[5] Imagen tomada de http://www.sincrack.com/wp-content/uploads/2013/05/nfs.png

aspecto es modificado en la versión 4, pues en ella se puede autenticar a usuarios y/o grupos mediante el protocolo de autenticación Kerberos.

El funcionamiento de NFS utiliza llamadas a procedimientos remotos (Remote Procedure Call), lo que requiere el que el servicio de rpcbind (antiguo servicio portmap) se encuentre arrancado previamente. En la versión 2 del protocolo solo es necesario que el servicio de rpcbind se encuentre arrancado en el servidor, mientras que en las versiones 3 y 4 es necesario que tanto cliente como servidor tenga arrancado el servicio de rpcbind, pues en caso contrario la exportación funciona de forma muy lenta y puede llegar a no funcionar (Bonet Esteban, sf).

2.5.3 SERVICIO SAMBA

Samba es un servicio que requiere de administración de usuarios para poder gestionar los permisos de éstos. En función del usuario que acceda, samba se comportará de una forma u otra ya que cuando accede un usuario normal, generalmente tiene unos permisos limitados y cuando accede un usuario administrador, deberá disponer de todos los permisos. Para que esa administración sea posible, samba dispone de su propia base de datos de 'usuarios samba' pero como los usuarios utilizan otros recursos del servidor como carpetas e impresoras, es necesario que estén creados en el sistema Unix. Resumiendo, podemos decir que para poder ser usuario de samba, es necesario disponer de una cuenta de usuario en Unix y de una cuenta de usuario en samba. Todo lo relativo a la creación y administración de usuarios y grupos en Unix se puede consultar en el apartado Usuarios del sistema Unix.

2.5.3.1 Gestión de usuarios de samba

La gestión de usuarios de samba se realiza con el comando smbpasswd. Con dicho comando, entre otras cosas podremos crear y eliminar usuarios, cambiar su contraseña, etc.

2.5.3.2 Gestión de grupos y permisos con samba

La gestión de grupos y permisos de usuarios y grupos es sustancialmente diferente en Sistemas Unix y en Sistemas Microsoft Windows. En los Sistemas Unix, la gestión de los permisos que los usuarios y los grupos de usuarios

tienen sobre los archivos, se realiza mediante un sencillo esquema de tres tipos de permisos (lectura, escritura y ejecución) aplicables a tres tipos de usuarios (propietario, grupo propietario y resto). Este sencillo esquema se desarrolló en los años 70 y aún hoy resulta adecuado para la gran mayoría de los sistemas en red que podamos encontrar en cualquier tipo de organización, desde pequeñas redes a las más grandes. Es cierto que tiene algunas limitaciones pero la ventaja de ser sencillo hace que su administración sea fácil y su rendimiento muy elevado.

En los Sistemas Microsoft Windows, la gestión de los permisos que los usuarios y los grupos de usuarios tienen sobre los archivos, se realiza mediante un complejo esquema de listas de control de acceso (ACLs = Access Control Lists) para cada carpeta y cada archivo. El sistema de ACL tiene la ventaja de ser mucho más flexible que el sistema Unix ya que se pueden establecer más tipos de permisos, establecer permisos solo a algunos usuarios y algunos grupos, denegar permisos, etc..., En la mayoría de los casos, con las prestaciones del Sistema Unix es suficiente. En el lado contrario, el sistema de ACL es más complejo de administrar y más lento ya que antes de acceder a las carpetas o archivos, el sistema debe comprobar listas mientras que en Unix hace una operación lógica de los bits que especifican los permisos lo cual es muchísimo más rápido.

Samba tiene también implementado el sistema de ACL y se gestiona utilizando el comando smbcacls, no obstante, la recomendación es utilizar el sistema de gestión de permisos de Unix. Aunque existan carpetas compartidas con samba, en última estancia imperan los permisos de Unix. Por ejemplo, si tenemos compartida una carpeta llamada 'profesores' con permisos de escritura para el grupo profesores, todos los usuarios que pertenezcan al grupo profesores podrán realizar cambios en la carpeta, pero si dentro de dicha carpeta existe otra llamada 'confidencial' sobre la cual no tiene permiso para entrar el grupo profesores, ningún profesor podrá ver su contenido aunque esté dentro de una carpeta compartida.

Para realizar una gestión eficaz de usuarios, grupos y permisos, se recomienda utilizar los permisos de Unix que permiten asignar permisos de lectura, escritura y ejecución al usuario propietario del archivo, al grupo propietario del archivo y al resto de usuarios del sistema (Samba, sf).

3. SERVICIOS DE RED BÁSICOS

La siguiente gráfica resumen los principales servicios de red que se pueden administrar a través de los sistemas operativos de red:

3.1 SERVIDORES DE NOMBRES DE DOMINIO (DNS)

El Servicio de Nombres de Dominio (DNS) es una forma sencilla de localizar un ordenador en Internet. Todo ordenador conectado a Internet se identifica por su dirección IP: una serie de cuatro números de hasta tres cifras separadas por puntos. Sin embargo, como a las personas les resulta más fácil acordarse de nombres que de números, se inventó un sistema (DNS - Domain Name Server) capaz de convertir esos largos y complicados números, difíciles de recordar, en un sencillo nombre.

Los nombres de dominio no sólo nos localizan, además garantizan nuestra propia identidad en la red. Al igual que en el mundo real existen diferentes formas de identificación como puede ser el DNI, el carnet de conducir, la

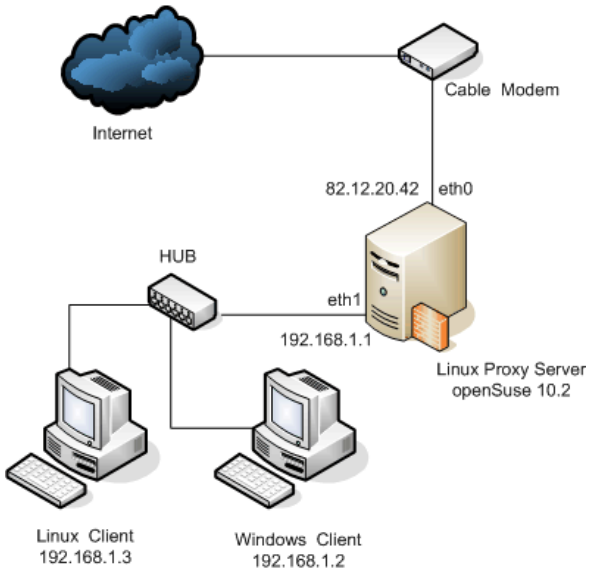
huella digital, etc. en Internet el dominio constituye el principal medio de identificación.

Por ejemplo, este servicio es fundamental para que el servicio de correo electrónico funcione. Un Servidor de Nombres de Domino es una máquina cuyo cometido es buscar a partir del nombre de un ordenador la dirección IP de ese ordenador; y viceversa, encontrar su nombre a partir de la dirección IP.

Ejemplo de resolución de nombres

¿Qué es lo que pasa entre un ordenador y el servidor DNS cuando el primero intenta conectarse con una máquina utilizando el nombre en lugar de la dirección IP?. Sea www.uned.es el nombre la máquina con la cual se desea conectar:

El ordenador local contacta con su servidor DNS (servidor-uno) (que se tiene configurado en el ordenador), y le solicita la dirección IP de www.uned.es. El servidor DNS mira en sus tablas de asignación, y si no lo encuentra entre los datos que guarda con las ultimas peticiones que ha servido, manda una petición a uno de los "servidores raíz" de Internet el cual averiguará qué servidor de nombres resuelve el dominio "uned.es" (Primo Guijarro, Tema 3. DNS, 2011)



3.2 SERVIDORES PROXY

Un proxy, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina A solicita un recurso a una C, lo hará mediante una petición a B; C entonces no sabrá que la petición procedió originalmente de A. Su finalidad más

habitual es la de servidor proxy, que sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.

Características

La palabra proxy se usa en situaciones en donde tiene sentido un unos algunos intermediario.

- El uso más común es el de servidor proxy, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.
- De ellos, el más famoso es el servidor proxy web (comúnmente conocido solamente como «proxy»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc.
- También existen proxy para otros protocolos, como el proxy de FTP.
- El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.
- Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.
- Un componente hardware también puede actuar como intermediario para otros.
- Como se ve, proxy tiene un significado muy general, aunque siempre es sinónimo de intermediario.

Tipos de proxy

Servidor Proxy

Un proxy es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor al que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud.

Servidor HTTP
Este tipo de servidor opera en la capa de aplicación de TCP/IP. El puerto de comunicación de entrada debe ser 80/http. Aunque generalmente suelen utilizar otros puertos de comunicación como el 3128, 8080 o el 8085.

Servidor HTTPS
Este tipo de servidor opera en la Capa de aplicación de TCP/IP. A diferencia de un Servidor HTTP, funciona bajo tecnologías de cifrado como SSL/TLS que proporcionan mayor seguridad y anonimato.

Servicio Proxy o Proxy Web
Su funcionamiento se basa en el del Proxy HTTP y HTTPs, pero la diferencia fundamental es que la petición se realiza mediante una Aplicación Web embebida en un Servidor HTTP al que se accede mediante una dirección DNS, esto es, una página web que permite estos servicios (Primo Guijarro , INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY, 2012).

3.3 CORREO ELECTRÓNICO (SMTP Y POP3)

El correo electrónico es una de las aplicaciones TCP/IP más utilizadas en estos días. En su forma más sencilla, el correo electrónico, es una manera de enviar mensajes o cartas electrónicas de un computador a otro.

Estructura y protocolos del correo electrónico

El correo electrónico de Internet se implementó originalmente como una función del protocolo FTP. En 1980 Suzanne Sluizer y Jon Postel realizaron trabajos con un protocolo que posteriormente se denominaría SMTP ("Simple Mail Transfer Protocol"). Hoy en día se sigue utilizando este protocolo, con los avances lógicos que requiere el tipo de transferencia actual.

El protocolo SMTP fue desarrollado pensando en que los sistemas que intercambiarían mensajes, eran grandes computadores, de tiempo compartido y multiusuario conectados permanentemente a la red Internet. Sin embargo, con la aparición de los computadores personales, que tienen una conectividad ocasional, se hizo necesaria una solución para que el

correo llegase a estos equipos. Para solventar esta limitación, en 1984 surge POP.
Este protocolo, en su especificación inicial, solo permite funciones básicas como recuperar todos los mensajes, mantenerlos en el servidor y borrarlos. En sucesivas versiones del protocolo (POP2 y POP3) se han ampliado las funciones, permitiendo una mejor gestión del correo.

3.3.1 SMTP (SIMPLE MAIL TRANSFER PROTOCOL)[6]

El significado de las siglas de SMTP es Protocolo Simple de Transmisión de Correo ("Simple Mail Transfer Protocol", RFC 821). Este protocolo es el estándar de Internet para el ***intercambio*** de correo electrónico. SMTP necesita que el sistema de transmisión ponga a su disposición un canal de comunicación fiable y con entrega ordenada de paquetes, con lo cual, el uso del protocolo TCP (puerto 25) en la capa de transporte, es lo adecuado. Para que dos sistemas intercambien correo mediante el protocolo SMTP, no es necesario que exista una *conexión interactiva,* ya que este protocolo usa métodos de almacenamiento y reenvío de mensajes.

Modo de comunicación SMTP

Cuando un servidor de SMTP, requiere transmitir un mensaje a otro servidor SMTP, el emisor (servidor que inicia la sesión SMTP) establece una conexión con el receptor (servidor que recibe petición de establecer sesión SMTP). Esta conexión es *unidireccional,* es decir, el emisor puede enviar correo al receptor, pero durante esa conexión, el receptor no puede enviar correo al emisor. Si el receptor tiene que enviar correo al emisor, tiene que esperar a que finalice la conexión establecida y establecer otra en sentido contrario, cambiando los papeles de emisor y receptor. Una vez establecida la conexión, el emisor envía comandos y mensajes.

Por lo tanto, el diseño de SMTP se basa en el siguiente modelo de comunicación:

[6] Imagen tomada de: http://cdn.makeuseof.com/wp-content/uploads/2012/08/Email.png?50fe7c

Como respuesta a una solicitud de un usuario de enviar un correo electrónico, el emisor SMTP establece una conexión con el receptor SMTP. El receptor SMTP debe ser el destinatario último del correo o un intermediario. Para ello el emisor genera los comandos SMTP en formato ASCII y los envía al receptor y el receptor genera las respuestas a los comandos enviados por el emisor. Una vez establecido el canal de transmisión, el emisor envía el comando MAIL para indicando que el es el emisor del correo. Si el receptor puede aceptar correo responde con el comando OK.

El emisor envía el comando RCPT identificando el destinatario del correo. Si el receptor puede aceptar correo para ese destino responde con una respuesta OK; si no, responde rechazando el correo para ese destino. Una vez negociado el destino, el emisor comienza a enviar datos (cabeceras y cuerpo), terminando con una secuencia especial. Si el receptor ha procesado correctamente los datos, responde con el comando OK.

3.3.2 POP (POST OFFICE PROTOCOL)

El protocolo de oficina de correo, POP, es un protocolo cuya misión es la de entrega final del correo al destinatario. Puesto que con SMTP lo único que se consigue es la transferencia del correo entre buzones, es necesario un protocolo como POP (o también IMAP) con el que podamos descargar el mensaje desde el buzón.

Modelo de comunicaciones POP

La descripción del protocolo POP la podemos encontrar en el RFC 1725, y como se acaba de comentar el modelo de comunicaciones POP se basa en mantener un buzón (estafeta) central en la que se almacenan los mensajes hasta que el usuario solicita la descarga de los mismos.

El cliente POP se conecta con el servidor a través del puerto TCP, 110. Para conectarse al servidor, es necesario una cuenta de identificación en dicha máquina (lo que le permite tener un espacio reservado para sus correos). A continuación es necesario verificar que es dueño de la cuenta a través de una clave. Una vez conectado al sistema, el cliente POP puede dialogar

con el servidor para saber, en otros, si existen mensajes en la casilla, cuántos mensajes son o para solicitar la descarga de alguno de ellos.

Para poder ofrecer estas funciones, el modelo de comunicación POP se basa en estados:

- Autorización
- Transacción

Actualización

Después de establecer la conexión, el servidor POP se encuentra en un estado de autorización, esperando que el cliente le envíe el nombre y clave de la cuenta de usuario. Cuando se verifica que el nombre y la clave son correctos, el servidor pasa a un estado de transacción. Antes de pasar a este estado, el servidor POP bloquea el buzón para impedir que los usuarios modifiquen o borren el correo antes de pasar al estado siguiente. En este estado de transacción el servidor atiende las peticiones del cliente. Después de enviar al servidor el comando QUIT, el servidor pasa al estado de actualización (estado siguiente). En este estado el servidor elimina los mensajes que están con la marca de borrado y finaliza la conexión (Escuela de Sistemas Informáticos).

3.4 FILE TRANSFER PROTOCOL[7]

FTP (siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

[7] Imagen tomado de: https://lh6.ggpht.com/_JGLE8kHGvMk_6sbuRVkP0EAHjaCPkYJtlSzdOBOIqsjwryTV-rLbwachNpjeZGPsIA=w300

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.

Para solucionar este problema son de gran utilidad aplicaciones como scp y sftp, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico.

4. REFERENCIAS

Kurose, J., & Ross, K. (2010). *Redes de computadoras. Un enfoque descendente*. Pearson Education .

Wikipedia. (2015). *Administrador de red*. Retrieved 03 de Agosto de 2015 from https://es.wikipedia.org/wiki/Administrador_de_red

HERNÁNDEZ ESCOBAR, J. (2006). *ADMINISTRACIÓN DE REDES BAJO EL ENTORNO DE WINDOWS XP*. Monografía , INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA LICENCIATURA EN SISTEMAS COMPUTACIONALES, PACHUCA DE SOTO.

Redes en educación. (sf). *Redes en educación*. Retrieved 03 de agosto de 2015 from Capítulo 5 Sistemas operativos de red: http://hera.cnice.mec.es/redes2/contenido/Pdf/mod1_5.pdf

KENDALL , J. E., & KENDALL , K. E. (2011). *ANÁLISIS Y DISEÑO DE SISTEMAS* (OCTAVA ed.). México: PEARSON EDUCACIÓN.

Cáceres , E. (2014). *Análisis y Diseño de Sistemas de Información* . Retrieved 29 de Diciembre de 2014 from http://www.facso.unsj.edu.ar/catedras/ciencias-economicas/sistemas-de-informacion-II/documentos/aydise14.pdf

Bermón Angarita, L. (n.d.). *Análisis y Diseño de Sistemas de Información*. (U. N. Colombia, Producer) Retrieved 29 de Diciembre de 2014 from Cursos Virtuales Universidad Nacional de Colombia : http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060030/html/descripcion.html

Bonet Esteban, E. (sf). Retrieved 3 de Agosto de 2015 from Ficheros compartidos en red I: NFS.: http://informatica.uv.es/it3guia/AGR/apuntes/teoria/documentos/NFS.pdf

Samba, S. N. (sf). *Instituto nacional de tecnologías educativas y de formación del profesorado*. Retrieved 05 de Agosto de 2015 from Gestión de usuarios, grupos y permisos de Samba: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m4/gestin_de_usuarios_grupos_y_permisos_de_samba.html

Genbeta. (2007). *Genbeta*. Retrieved 03 de Agosto de 2015 from 10 características novedosas de Windows Server 2008: http://www.genbeta.com/actualidad/10-caracteristicas-novedosas-de-windows-server-2008

Center, T. E. (2015). *TechNet Evaluation Center*. Retrieved 05 de Agosto de 2015 from https://technet.microsoft.com/es-ar/evalcenter/hh670538.aspx?wt.mc_id=TEC_108_1_8#&ocid=src-n-latam-jtc--SKI

Server, N. d. (2014). *Novedades de Windows Server*. Retrieved 05 de Agosto de 2015 from https://technet.microsoft.com/library/dn250019

Primo Guijarro, Á. (2011). Tema 3. DNS. In *Servicios de red e Internet*.

Primo Guijarro , Á. (2012). INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY. In *Seguridad Informática.*

Escuela de Sistemas Informáticos. (n.d.). EL SISTEMA DE CORREO ELECTRÓNICO (SMTP Y POP3). *Tecnologías de la comunicación en internet* .