UNIDAD 1. REDES Y SERVIDORES EN ENTORNO EMPRESARIAL

1.1. Introducción a sistemas Windows Server

1.1.1. Evolución de sistemas Windows Server

1.1.2. Ediciones de Windows Server 2008 R2

1.1.3. Nuevas características de Windows Server 2008 R2

1.1.4. Windows Server core 2008

1.2. Terminología y conceptos básicos de red

1.2.1. Modelo OSI

1.2.2. Pila de Protocolos TCP/IP

1.2.3. Topologías de red

1.2.4. Direccionamiento IPv4

1.3. Fundamentos de IPv6

1.3.1. Motivos para el cambio

1.3.2. Características de IPv6

1.3.3. Cabecera de IPv6

1.3.4. Direccionamiento IPv6

1.3.5. Autoconfiguración en IPv6

1.4. Terminología y conceptos básicos de Windows Server

1.4.1. Concepto de directorio y Active Directory Domain Services (AD DS)

1.4.2. Estructura lógica

1.4.3. Estructura física

1.4.4. Objetos de Active Directory

1.4.5. Protocolos de autenticación

Índice

• Objetivos

- Conocer la infraestructura de red de Microsoft y su evolución en los sistemas operativos para servidores.
- Identificar las principales características de Windows Server 2008.
- Introducir la novedad que supone la instalación de Windows Server Core.
- Recordar conocimientos necesarios de redes y de direccionamiento IP en su versión IPv4.
- Introducir los conceptos relativos a IPv6.
- Dominar la terminología de Active Directory

Introducción a sistemas Windows Server

En este capítulo vamos a realizar una primera aproximación a los sistemas operativos de la familia Windows Server.

Para ello, en primer lugar realizaremos un repaso sobre la evolución histórica de estos sistemas, para acabar contando las principales novedades de la última ersión Windows Server 2008, en sus diferentes ediciones, destacando una de sus principales características: Windows Server Core.

1.1.1. Evolución de sistemas Windows Server

Para comenzar con esta unidad de introducción a los sistemas operativos de Windows Server, es conveniente tener una perspectiva histórica de la evolución que han sufrido las diferentes versiones del sistema operativo de Windows en lo que a ediciones orientadas a servidor se refiere.

En primer lugar, vamos a mostrar un cuadro histórico con las diferentes versiones aparecidas, su nombre comercial, las ediciones con las que salieron al mercado y su fecha de lanzamiento:

Versión	Nombre Comercial	Edición	Fecha de lanzamiento
NT 3.5	Windows NT 3.5	Server	21 Septiembre 1994
NT 3.5.1	Windows NT 3.51	Server	30 Mayo 1995
NT 4.0	Windows NT 4.0	Server, Server Enterprise Edition. Terminal Server, Embedded	29 Julio 1996
NT 5.0	Windows 2000	Server, Advanted Server, Datacenter Server, Advanced/Datacenter Server Limited Edition	17 Febrero 2000
NT 5.2	Windows Server 2003	Enterprise, Datacenter, Web, Storage, Small Business Server, Compute Cluster	24 Abril 2003
NT 6.0	Windows Server 2008	Standard, Enterprise, Datacenter, Web Server, HPC Server, Itanium-Based Systems	27 Febrero 2008
NT 6.1	Windows Server 2008 R8	Standard, Enterprise, Datacenter, Web Server, HPC Server, Itanium-Based Systems	22 Octubre 2009

Figura 1.1. Evolución sistemas Windows Server.

A continuación, vamos a comentar brevemente las características de cada uno de ellos.

Windows NT 3.5

En realidad, antes de NT 3.5 hubo una versión previa denominada NT 3.1, pero solo se trataba de una continuación de la edición para escritorio.

Windows NT 3.5 fue la primera versión en dividirse en dos ediciones: Workstation y Server. Soportaba OpenGL y nombres de fichero de hasta 255 caracteres. Como primera revisión, enseguida surgió Windows NT 3.5.1 que incorporaba actualizaciones notables como la posibilidad de trabajar en equipos con procesadores Pentium o superiores. En las anteriores versiones, si en el proceso de instalación se detectaba un procesador superior a Pentium se detenía el proceso. Otra de las mejoras era la incorporación de una librería de controladores

más extensa, soporte para BackOffice y el arranque y la instalación remota de Windows 95 en los clientes. Windows NT 4.0

Windows NT 4.0 incorporaba diversos componentes tecnológicos de vanguardia y, además, era capaz de soportar plataformas como MIPS, ALPHA, Intel, etc.. Aparecieron diferentes versiones como Workstation, Server, Terminal Server y Advanced Server que posibilitaban la adaptación a las necesidades de los clientes. Surgió a raíz del éxito de Windows 95, y aunque al principio fue muy criticado, se adaptó a la interfaz y filosofía de trabajo del Windows doméstico. No obstante, esta versión tenía problemas que terminaron por no convencer a los usuarios. Por ejemplo, tenía una mala implementación de la tecnología Plug & Play, mala compatibilidad con dispositivos multimedia, una configuración y mantenimiento complicados. En definitiva, se tuvieron que desarrollar muchos Services Packs para solventar todos estos problemas. Windows 2000

Fue la primera versión que agradaba realmente a los administradores de red ya que incluía numerosos servicios de red que eran muy útiles, y sobre todo, porque por fin se resolvía el problema de la admisión sin problemas de los dispositivos Plug & Play, que fue uno de los principales problemas de NT 4.0.

Salió al mercado con una edición para estaciones de trabajo, Windows 2000 Professional, y con otras versiones para servidores: W2000 Server, Advanced Server y Datacenter Server.

Microsoft, tanto en nuevos servicios como en la mejora de los existentes. Algunas de las características que poseía eran:

Almacenamiento:

_ Soporte para FAT16, FAT32 y NTFS.

_ Encriptación de ficheros (EFS).

_ Servicio de indexación.

_ Sistema de archivos distribuido (DFS).

_ Nuevo sistema de backup (ASR).

_ Sistema de tolerancia a fallos (RAID) con discos dinámicos (software).

Comunicaciones:

_ Servicios de acceso remoto (RAS, VPN, RADIUS y Enrutamiento).

_ Nueva versión de IIS con soporte para HTTP/1.1.

_ Directorio activo.

_ Balanceo de carga (clustering).

_ Servicios de instalación desatendida por red (RIS).

_ Servicios nativos de Terminal Server.

Estos avances marcan un antes y un después en la historia de Microsoft.

Windows Server 2003

Las características más importantes de Windows Server 2003 serían las siguientes:

_ Sistema de archivos NTFS:

_ Cuotas.

_ Cifrado y compresión de archivos y carpetas en lugar de unidades completas.

_ Permitía montar dispositivos de almacenamiento sobre sistemas de archivos de otros dispositivos al estilo unix.

_ Gestión de almacenamiento y backups: incluía gestión jerárquica del almacenamiento, que consiste en utilizar un algoritmo de caché para pasar los datos menos usados de discos duros a medios ópticos o similares más lentos, y volverlos a leer a disco duro cuando se necesitaban.

_ Windows Driver Model: implementación básica de los dispositivos más utilizados, de esa manera los fabricantes de dispositivos solo tenían que programar ciertas especificaciones de su hardware

_ Active Directory: Directorio de organización basado en LDAP, que permitía gestionar de forma centralizada la seguridad de una red corporativa a nivel local.

_ Autentificación Kerberos5.

_ DNS con registro de IP's dinámicamente.

_ Políticas de seguridad.

Con Windows 2003 Server, ya era posible poder instalar una elevada cantidad de diferentes tipos de servidores, como los siguientes:

_ Servidor de archivos.

_ Servidor de impresiones.

_ Servidor de aplicaciones.

_ Servidor de correo (SMTP/POP).

_ Servidor de terminal.

_ Servidor de redes privadas virtuales (VPN) o acceso remoto al servidor.

_ Controlador de Dominios (mediante Active Directory).

_ Servidor DNS.

_ Servidor DHCP.

_ Servidor de Streaming de Vídeo.

_ Servidor WINS.

_ Servidor RIS (Remote Installation Services): servicios de instalación remota.

Windows Server 2008

De las características de Windows Server 2008 pasamos a ocuparnos en los

siguientes capítulos.

1.1.2. Ediciones de Windows Server 2008 R2

Microsoft Windows Server 2008, es el nombre del sistema operativo de Microsoft diseñado para Servidor. Es el sucesor de Windows Server 2003, distribuido al público casi cinco años antes. Al igual que Windows Vista, Windows Server 2008 se basa en el núcleo Windows NT 6.0. Posteriormente, se lanza una segunda versión, denominada "Windows Server 2008 R2".

A continuación, vamos a detallar las diferentes ediciones que podemos encontrar para esta nueva versión de Windows Server 2008 R2:

_ Windows Server 2008 Foundation R2: es una base tecnológica rentable y de nivel básico orientada a pequeñas empresas.

_ Windows Server 2008 Standard R2: es el sistema operativo de Windows Server más robusto hasta la fecha. Con capacidades de virtualización y Web mejoradas e incorporadas, está diseñado para incrementar la confiabilidad y flexibilidad de la infraestructura de servidor.

_ Windows Server 2008 Enterprise R2: es una plataforma de servidor avanzada que ofrece un soporte más rentable y confiable para cargas de trabajo de misión crítica. Ofrece características innovadoras para la virtualización, ahorros en energía y manejabilidad y ayuda a facilitar, a los empleados móviles, el acceso a los recursos corporativos.

_ Windows Server 2008 Datacenter R2: ofrece una plataforma de clase empresarial para desplegar aplicaciones comerciales críticas y virtualización a gran escala en servidores grandes y pequeños. Con esta edición podremos escalar de dos a 64 procesadores. Windows Server R2 2008 Datacenter ofrece una base en la que se puede crear virtualización de clase empresarial y soluciones escalables.

_ Windows Web Server 2008 R2: es una plataforma de servicios y aplicaciones Web. Incluye Internet Information Services (IIS) 7.5 y está diseñado exclusivamente como servidor orientado a Internet. Con roles de Web Server y DNS Server incluidos, esta plataforma permitirá desde un servidor Web dedicado a un todo un centro de servidores Web.

_ Windows HPC Server 2008: Es la última generación de informática de alto rendimiento (HPC), pudiendo escalar de forma eficiente a miles de núcleos de procesamiento e incluye consolas de administración que le ayudan a monitorear en forma proactiva y mantener la salud y estabilidad del sistema. La flexibilidad e interoperabilidad de programación de trabajos permite la integración entre plataformas HPC basadas en Windows y Linux y brinda soporte a cargas de

trabajo de aplicaciones orientadas a servicios (SOA) y lotes.

_ Windows Server 2008 for Itanium-based Systems R2: esta diseñado para desplegar aplicaciones comerciales críticas. Mejora la disponibilidad con capacidades de agrupamiento ante fallas y partición dinámica de hardware. Podremos virtualizar despliegues con derechos para ejecutarse con una cantidad ilimitada de instancias virtuales de Windows Server.

_ Hyper-V no está disponible para sistemas basados en Itanium.

1.1.3. Nuevas características de Windows Server 2008 R2

La nueva versión de Windows Server 2008 R2 nos ofrece una plataforma mediante la cual podremos ofrecer virtualización de bajo coste, mejorar las prestaciones de ahorro de energía y un escenario sencillo e intuitivo para los usuarios finales. En cuanto a las ventajas ofertadas para los administradores de sistemas, podemos destacar las siguientes novedades:

_ Gestión optimizada y mayor tiempo de actividad: la virtualización nos va a permitir reducir de forma drástica los costes operativos y el consumo de energía. Hyper-V™, una tecnología avanzada de hypervisor que incorporan las ediciones Estándar, Enterprise y Datacenter de Windows Server 2008 R2, está diseñada para una óptima gestión de las actuales máquinas virtuales.

Windows Server 2008 R2 mejora la tecnología Hyper-V con Live Migration, una herramienta que permitirá transferir máquinas virtuales entre máquinas físicas en pocos milisegundos, de manera que las operaciones de migración puedan ser realizadas sin que el usuario apenas lo note. Además, en R2, Hyper-V agiliza la administración y mejora los tiempos de actividad con la posibilidad de arrancar desde discos duros virtuales (VHD) y añadir y eliminarlos sin necesidad de reiniciar el sistema.

_ Mejora de la productividad con Windows 7: Windows Server 2008 R2 incorpora dos nuevas características que mejoran la productividad del usuario que emplea el sistema operativo de cliente Windows 7 en ubicaciones remotas.

DirectAccess™ es una alternativa para que los usuarios remotos puedan acceder a los recursos de la organización, sin tener que conectarse mediante VPN, con la ventaja de no tener que instalar software adicional en los clientes. De esta forma, se consigue que no haya distinciones entre las conexiones locales y remotas.

BranchCache™ es una nueva solución de acceso a contenidos que mejora los tiempos de respuesta para los empleados en redes de oficinas. Con

BranchCache, cuando los usuarios solicitan acceso a datos o archivos de la red de su organización, pueden descargar el contenido desde la propia red local de la oficina remota si el archivo ya había sido descargado previamente y, por tanto, guardado en algún sistema local. BranchCache mejora la productividad de los usuarios remotos, ya que aumenta la capacidad de respuesta de las aplicaciones, reduce el tiempo de espera en transferencias de archivos y hace un uso más eficiente del ancho de banda en la WAN. BranchCache está optimizado para los protocolos HTTP, SMB y BITS, y puede reducir sensiblemente los costes de utilización de las redes de área extensa (WAN), liberando ancho de banda que se puede utilizar para otros fines.

_ Mejoras del acceso remoto y virtualización: se pueden destacar dos principales mejoras en lo que a capacidades de acceso se refiere.

VDI es una arquitectura de escritorio centralizado que posibilitará a las organizaciones centralizar el almacenamiento, la ejecución y la administración de un escritorio Windows en el centro de datos. Permite que Windows y otros entornos de escritorio puedan ejecutarse y gestionarse en forma de máquinas virtuales sobre un servidor centralizado.

Terminal Services se llama a partir de ahora Remote Desktop Services (RDS), e incorpora y amplía todas las funcionalidades que anteriormente se incluían dentro de Terminal Services. Microsoft ha mejorado las características de gestión y rendimiento de RDS para dotar de mayor flexibilidad a la virtualización de la presentación.

_ Gestión mejorada del consumo de energía: entre las mejoras que incorpora Windows Server 2008 R2 para la administración de la energía destacan:

_Mejoras en el motor de gestión y la configuración del consumo de energía de los procesadores.

_Parking de núcleos, que permite consolidar tareas en un número menor de núcleos de procesador con baja carga, para reducir el consumo al dejar inactivos algunos núcleos.

_Capacidades de medición del consumo, incluyendo la posibilidad de ver el consumo de energía en el monitor de rendimiento o recopilar este tipo de datos en el centro de datos mediante WMI, scripts o herramientas como System Center.

_Funciones de planificación del consumo de energía.

_Almacenamiento más eficiente mediante el uso de SAN (Storage Area Network) centralizada.

Hasta un 18% de mejora en la eficiencia energética sobre el mismo hardware, en comparación con Windows Server 2003.

_ Mejor aprovechamiento del Hardware: Windows Server 2008 R2 es capaz de soportar hasta 256 núcleos de procesador lógico para cada instancia individual del sistema operativo. Hyper-V puede utilizar hasta 64 procesadores lógicos.

1.1.4. Windows Server core 2008

Dentro de las diferentes posibilidades de instalación que nos ofrece Windows Server 2008, la instalación de la opción Server Core nos va a suministrar la posibilidad de trabajar con un entorno mínimo donde se ejecutarán exclusivamente los roles de servidor mínimos.

De esta forma, podremos limitar las funciones y características del servidor, y así nos garantizamos que vamos a mejorar en cuanto a prestaciones relativas a la seguridad y manejabilidad del servidor. Los servicios y componentes que van a estar ejecutándose, al ser más limitados, nos otorgan cierta ventaja frente a la posibilidad de que intrusos quieran acceder a nuestro sistema, ya que habremos reducido el área de ataque.

Otra ventaja que vamos a obtener con la instalación de Server Core es la relativa a la mejora de rendimientos del servidor, ya que al tener menos servicios y componentes instalados, necesitará de menos actualizaciones de las habituales, reduciendo la carga de trabajo del servidor.

A continuación, vamos a describir las funcionalidades soportadas por Server Core:

_ Servicios de dominio de Active Directory.

_ Servidor DHCP.

_ Servidor DNS.

_ Servidor de impresión.

_ Servicios de archivo.

_ Servicios de transmisión de medios.

_ Servicios de directorio ligero de Active Directory (AD LDS).

_ Servidor Web IIS (no podrá ser instalado como servidor web estático-ASP.NET).

En cuanto a las características opcionales que es capaz de soportar, serán las siguientes:

_ Balaceo de carga de red.

_ Copias de seguridad de Windows.

_ Administración de almacenamiento extraíble.

_ Protocolo de administración de una red simple (SNMP).

_ Cliente Telnet.

_ Clúster de conmutación por error de Microsoft.

_ Subsistema para aplicaciones UNIX.

_ Multiples rutas I/O.

_ Cifrado de unidad Bitlocker de Windows.

_ Servidor WINS.

_ Servicios de calidad (QoS).

1.2. Terminología y conceptos básicos de red

A partir de la unidad 2, comenzaremos a instalar y configurar diferentes servicios y servidores sobre Windows Server 2008 tales como DNS, WINS, DHCP, etc.
Como recorrido natural hasta llegar a estos conocimientos, es necesario dejar bien asentados ciertos aspectos imprescindibles sobre la terminología y los conceptos básicos de los entornos de redes.

1.2.1. Modelo OSI

En las últimas décadas, hubo un gran aumento en el número y tamaño de redes. Muchas de ellas, se crearon empleando soluciones de hardware y software diferentes, lo que produjo incompatibilidad entre ellas, ya que utilizaban especificaciones diferentes y entonces no podían comunicarse entre sí.
Para intentar resolver este problema, la Organización Internacional de Normalización (ISO), reconoció la necesidad de crear un nuevo modelo de red, a partir del cual todos los constructores tuvieran que desarrollar sus redes y de esta forma obtener la compatibilidad deseada.
Para ello se creó el modelo OSI, el cual propone la división de las comunicaciones de red en siete capas, para así dividir la comunicación de red en partes más pequeñas, sencillas y fáciles de desarrollar. Como consecuencia, se facilitaba la normalización de los componentes de la red, permitiendo que diferentes tipos de hardware y software se comuniquen entre sí.
Cada uno de los siete problemas más pequeños está representado por su propia capa en el modelo. Las siete capas del modelo OSI son:

_ Capa 7: la capa de aplicación.

_ Capa 6: la capa de presentación.

_ Capa 5: la capa de sesión.

_ Capa 4: la capa de transporte.

_ Capa 3: la capa de red.

_ Capa 2: la capa de enlace de datos.

_ Capa 1: la capa física.

Los principios aplicados para la definición de siete capas son los siguientes:

1. Una nueva capa es creada cuando se necesite un nivel diferente de abstracción.
2. Cada capa debe realizar una función bien definida.
3. Las funciones a ejecutar en cada capa deben seleccionarse considerando la definición futura de protocolos estandarizados internacionalmente.
4. Los límites de cada capa deben ser elegidos de forma tal que se minimice el intercambio de datos a través de las interfaces.
5. El número de capas debe ser lo suficientemente grande para evitar que funciones diferentes sean implementadas juntas, y lo suficientemente pequeño para que la arquitectura no se torne inmanejable.
6. Cada capa es bastante autónoma, para que las tareas asignadas a cada capa puedan llevarse a cabo independientemente. Esto permite que las soluciones ofrecidas por una capa sean llevadas a cabo sin afectar adversamente a las otras capas.
7. Cada capa realizará algunas de las siguientes funciones (entre otras): segmentación y reensamblado, encapsulado, control de la conexión, entrega ordenada, control de flujo, control de error, direccionamiento, etc.

Al dividir el problema en partes, una tarea o grupo de tareas se asigna entonces a cada una de las siete capas de OSI.

En la figura 1.2 podemos observar el recorrido por las diferentes capas del modelo OSI que realizan los datos que son transmitidos por un usuario, hasta que son recogidos en destino.

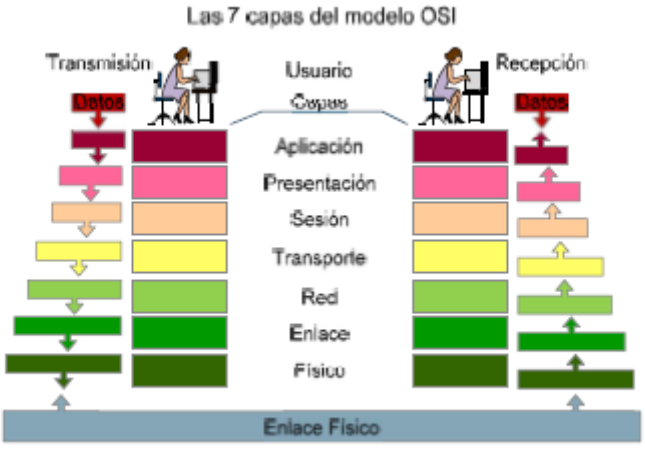


Figura 2.2. Proceso de transmisión-recepción en el modelo OSI.

Características de las capas de OSI:

_ Las siete capas del modelo de referencia OSI pueden ser divididas en dos categorías: las capas superiores (las 4 superiores) y las capas más bajas

(las 3 inferiores).

_ Las capas superiores del OSI tratan con las aplicaciones y generalmente solo se llevan a cabo en software.

_ La capa más alta, la de aplicación, es más íntima al usuario final. Ambos, usuarios y procesos de la capa de aplicación, interactúan recíprocamente con aplicaciones de software que contienen componentes de comunicación. El término capa superior se usa a veces para referirse a cualquier otra capa superior del modelo OSI.

_ Las capas más bajas del OSI tratan cuestiones de transporte de datos. La capa de red y la capa de enlace de datos se implementan en hardware y software. La capa más baja, la capa física, está relacionada íntimamente al medio de red físico (el cableado de la red, por ejemplo) y es el responsable real de poner la información en el medio.

1.2.2. Pila de Protocolos TCP/IP

Aunque el modelo OSI es el que está universalmente reconocido, el estándar que realmente es utilizado en Internet es el protocolo para el control de la transmisión TCP/IP. Básicamente, la pila TCP/IP unifica las capas de aplicación, presentación y sesión en una única capa de aplicación. El resto, con ligeras diferencias de matiz en algún nivel que van mucho más allá de nuestros objetivos, podremos decir que son coincidentes.

Podemos ver un esquema gráfico de las 4 capas de TCP/IP, en comparación con el modelo OSI, junto con la pila de protocolos que podemos encontrar en cada una de ellas:

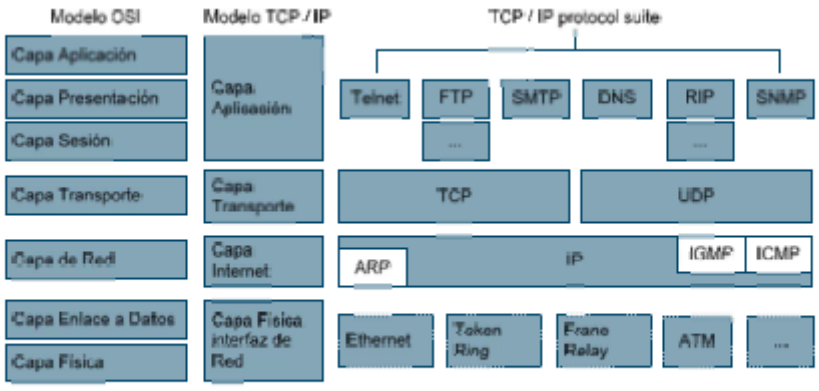


Figura 2.3. Comparación modelo OSI y TCP/IP con su pila de protocolos.

Si tuviéramos que hacer una comparativa entre ambos modelos, podríamos encontrar las siguientes semejanzas y similitudes:

Similitudes

_ Ambos se basan en un modelo de capas.

_ Ambos tienen capa de aplicación, aunque incluyan servicios diferentes.

_ Ambos tienen capa de red y transporte comparables.

_ Asumen la tecnología de conmutación de paquetes (no de circuitos conmutados).

Diferencias

_ TCP/IP combina las funciones de las capas de presentación y sesión en su capa de aplicación.

_ TCP/IP combina las capas física y de enlace de datos OSI en una capa.

_ TCP/IP es la norma sobre la cual se ha desarrollado el crecimiento de Internet. Por el contrario, las redes no se construyen normalmente con los protocolos OSI, aunque sí que se utiliza como guía.

1.2.3. Topologías de red

A través de la implementación de las topologías, podremos definir nuestra estructura de red.

Podríamos separarlas conceptualmente en dos tipos: la topología física, que estará basada en el diseño real del cableado (medios); y la topología lógica, que definirá cómo los diferentes hosts pueden acceder a los medios.

A continuación, vamos a describir brevemente las principales topologías que pueden ser empleadas.

_ En bus.

_ En estrella.

_ En estrella extendida.

_ En árbol.

_ En anillo.

_ En mall.

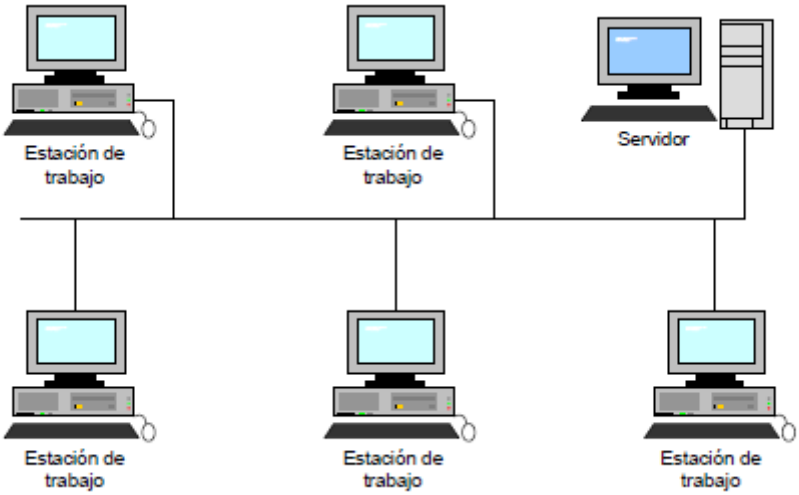
_ Jerárquica.

Topología en bus

En una topología de red en bus, cada uno de los hosts que la componen, podrá supervisar la actividad que se pueda producir en la línea. Los mensajes podrán ser detectados por cada uno de los hosts, aunque solo podrán ser aceptados por el host o los hosts a los que vayan dirigidos.

Cuando uno de los hosts tiene algún problema, simplemente deja de comunicarse, pero no interrumpe ninguna operación, como por ejemplo veremos que sucede con la topología en anillo.

Para intentar evitar que no se produzcan las colisiones que pueden ser producidas al intentar utilizar la línea dos o más hosts, las redes que utilicen una topología en bus, tendrán que implementar soluciones en detección de colisiones para regular el tráfico.



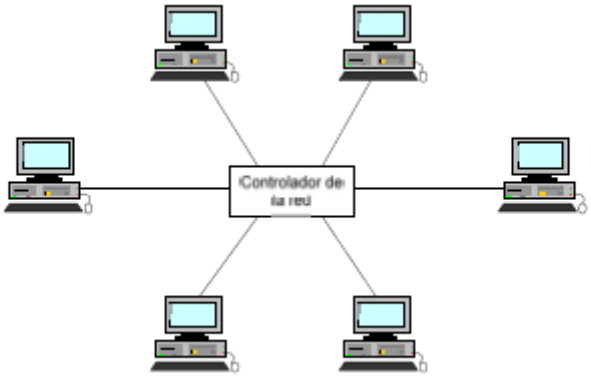
Las principales ventajas que aporta es que es fácil de instalar y de mantener y que no existen elementos centrales de los que vaya a depender toda la red, donde un posible fallo podría dejar inoperativas al resto de estaciones.

El principal inconveniente que tiene es que si el cable a través del cual están todas las estaciones conectadas sufre alguna avería, la red quedará fuera de línea por completo.

Topología en estrella

En una red que implementa una topología en estrella, existirá la figura de dispositivo que se encuentre en el centro de la red, al cual se conectará todo el cableado. Todos los mensajes que circulen por esta red pasarán a través de este dispositivo, que gestionará la redistribución de la información al nodo correspondiente.

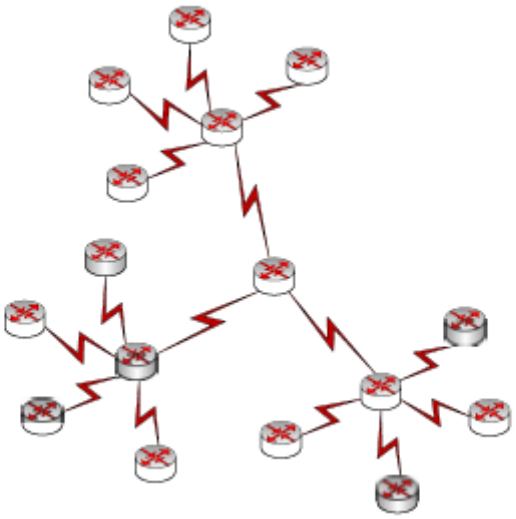
Al igual que en la topología en bus, si un nodo falla, no afecta de ninguna forma al resto de los nodos de la red. Lo que sí supone un grave problema es que el elemento central de conexión sufra una avería, puesto que en ese caso la red pasará a estar inoperativa



Topología en estrella extendida

Para la implementación de una topología de estrella extendida, se parte de la base de la utilización de una topología en estrella, de tal forma que se enlazarán estrellas

individuales con la utilización de dispositivos de conectividad, como routers o switches. El objetivo final será extender la red en cuanto a longitud y a tamaño.



Topología en árbol

Una topología en árbol será similar a la topología en estrella extendida, salvo por la diferencia principal de que no va a utilizar un nodo central.

En su lugar, va a añadir un nodo troncal desde el que se ramificarán el resto de los nodos, como podemos ver en la figura 1.7.

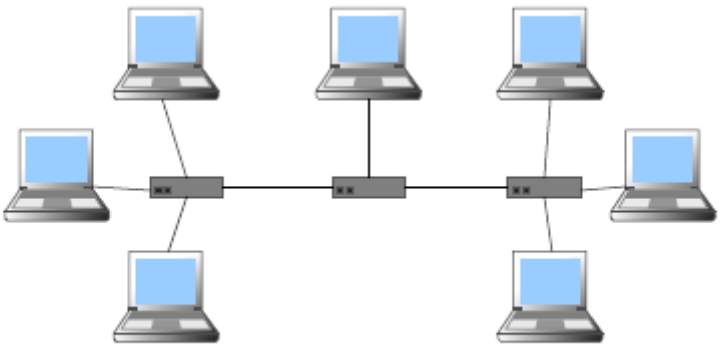


Figura1.1. Topología en árbol.

Podremos encontrar a su vez dos tipos de topologías en árbol:

_ Árbol binario, donde cada nodo se dividirá en dos enlaces.

_ Árbol backbone, donde cada nodo podrá tener muchas ramificaciones que partan de él. El troncal suele ser un cable que tendrá varias capas de ramas y el flujo de información es jerárquico.

Topología en anillo

Esta topología se basa en conectar un nodo o host, con el siguiente, y el último host con el primero. De esta forma, se podrá crear un anillo físico de cableado.

Se trata de un bucle cerrado donde los mensajes de la red pasarán de un nodo a otro en una dirección concreta. A medida que el mensaje está circulando por el anillo, cada uno de los nodos va a examinar la dirección de destino que lleva

incorporada el mensaje, hasta llegar al nodo de destino que aceptará el mensaje.
El principal inconveniente de este tipo de topologías es que si se avería el cable que forma el anillo, toda la red se verá afectada.

Figura 2.7. Topología en anillo.

Topología en malla

La topología en malla suele ser utilizada cuando no es aceptable la posibilidad de que se produzca cualquier tipo de corte en las comunicaciones entre todos los hosts.
En una topología en malla, todos los hosts tendrán sus propias conexiones con el resto de los hosts.
Una malla parcial podría reflejar el diseño de Internet, donde siempre habrá múltiples rutas para poder llegar a un destino final, aunque obviamente no habrá interconexiones entre todos los hosts.

Topología jerárquica

La topología jerárquica, seguramente es el modelo más extendido en el diseño de redes, ya que nos va a proporcionar la posibilidad de separar nuestro diseño en varias capas, donde situar los diferentes dispositivos de ínter-conectividad y estaciones de trabajo.
Cada capa podrá centrarse en las funciones específicas diseñadas para esa capa, otorgándonos la posibilidad de elegir los sistemas y características apropiados para cada capa.
Además, la implementación de una red con esquema jerárquico nos va a facilitar la posibilidad de introducir cambios. La modularidad de este diseño nos permitirá crear elementos de diseño que pueden ser reproducidos a medida que nuestra red vaya creciendo. Como nuestras redes también irán necesitando de actualizaciones tanto en sus dispositivos como en sus configuraciones, el coste y la complejidad asociada a realizar estas actualizaciones quedará limitado a una pequeña parte de nuestra red.
El modelo jerárquico en división de niveles también va a facilitar mucho el trabajo de los administradores de sistemas, puesto que les será mucho más sencillo poder localizar los puntos en los que pueda fallar la red corporativa. . El motivo es que podremos estructurarla a nuestra conveniencia en partes más pequeñas dónde

será más fácil entender donde se producen los puntos de transición de la red, ayudando a localizar los problemas.

Las principales ventajas del uso de un modelo jerárquico de red serán las siguientes:

_ Facilidad de implementación: este modelo de red va a definir unas funciones y objetivos a conseguir en cada una de las capas de tal forma que nos va a facilitar la implementación de nuestra red.

_ Ayuda en la solución de situaciones problemáticas: al estar definidas las funciones a nivel de cada una de las capas, el poder concretar dónde se están produciendo los posibles problemas en nuestra red será una tarea menos complicada. Nos permitirá también segmentar la red de forma temporal para reducir el alcance de un problema.

_ Escalabilidad: las redes que siguen este modelo podrán crecer de una forma más sencilla sin tener que sacrificar el control o la administración.

_ Predicción: al haber distribuido las funciones a nivel de capa, el comportamiento de nuestra red será bastante predecible, facilitando, de esta forma, la planificación para el crecimiento de nuestra red y permitiéndonos realizar análisis capa por capa.

_ Administración: todas las ventajas anteriormente comentadas van a facilitar la tarea de administración de redes.

La estructura jerárquica en una red estará compuesta por tres capas: núcleo, distribución y acceso, donde cada una de las cuales tendrá sus propias funciones. Podemos ver un avance en la figura 1.10:

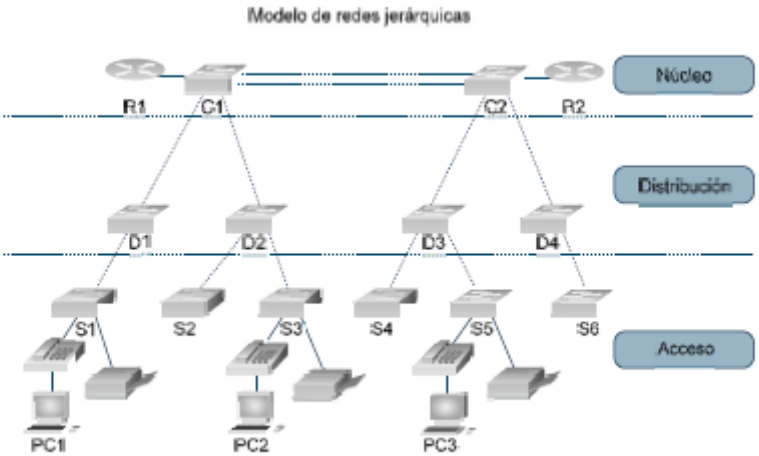


Figura 2 9. Topología jerárquic a de redes.

1.2.4. Direccionamiento IPv4

La forma más cómoda de crear nuestro propio espacio de direccionamiento IP privado en nuestra organización, es mediante el empleo de direcciones de 32 bits, que son el formato en el que se basa el protocolo IPv4. En el siguiente capítulo veremos los fundamentos de IPv6 y las principales diferencias con este método de direccionamiento, pero en este capítulo explicaremos de forma breve, la forma habitual de trabajo con este esquema de direccionamiento.

Mediante una dirección IP, podremos codificar de forma variable los bits que vamos a utilizar para especificar la red y por otra parte el equipo. Mediante esta forma de trabajo, ganaremos en flexibilidad a la hora de decidir cómo queremos asignar las direcciones IP a los equipos de nuestra red, permitiéndonos poder mezclar los tamaños de red en un conjunto de redes.

Los 32 bits, cuyos valores solo podrán ser 0 y 1, estarán repartidos en 4 bloques de 8 bits para cada uno. Cada grupo de 8 bits, conforma un byte, que será traducido a su notación decimal para identificar las direcciones IP de una forma más clara, tal y como podemos ver en el siguiente ejemplo:

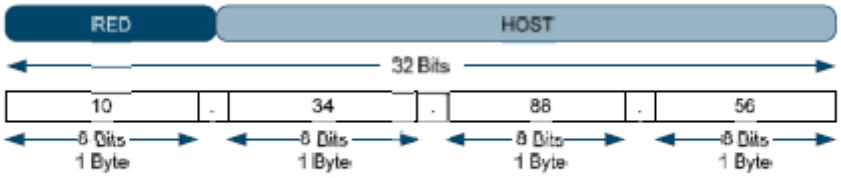


Figura 2.10. Dirección IP en 4 grupos de 8 bits.

En el anterior ejemplo, los primeros 8 bits son utilizados para identificar la red a la cual pertenece el equipo, y el resto de los 24 bits, servirán para identificar al equipo dentro de esa red.

Una consecuencia de esta forma de organizar los bits es que dada una dirección IP podemos determinar rápidamente si pertenece o no a una red. En particular, los enrutadores (dispositivos que se encargan de mover todo el tráfico de Internet) se aprovechan de esta propiedad de las direcciones IP para enrutar los paquetes, o sea, enviarlas al siguiente enrutador que cree que está más cerca de la red destino.

Pero, ¿cómo sabemos qué bits identifican a la red y cuáles identifican a los dispositivos? Hay dos respuestas: las clases y la máscara de red.

En IPv4 podemos encontrarnos hasta cinco clases de redes:

_ Clase A: el primer bit es 0, y por lo tanto, el primer byte puede tener valores entre 0 y 127, lo cual nos dará 128 redes y como el resto de los 32 bits sirven para identificar a los dispositivos, tenemos hasta 2^24 o más de 16 millones. Estas direcciones van del 0.0.0.0 hasta el 127.255.255.255.

_ Clase B: los dos primeros bits son 1 y 0, lo cual nos dará el rango 128-191. En este caso, se toman los dos primeros bytes para las direcciones de redes, con lo cual tenemos 2^14, o más de 16000 redes de hasta 65536

dispositivos (2^16).

_ Clase C: los tres primeros bits son 1, 1 y 0, dando el rango 192 hasta 223. Para la dirección de red se toman los tres primeros bytes. Esto nos proporciona más de 2 millones de redes de hasta 256 dispositivos.

_ Clase D: los primeros cuatro bits son 1, 1, 1 y 0. Es utilizado para multicast.

_ Clase E: los primeros cuatro bits son 1, 1, 1 y 1. Reservado para un uso futuro.

En la siguiente imagen podemos ver de forma gráfica las distintas clases de redes existentes, los bits que reservan para redes y para host, y las posibilidades en direcciones IP que otorgan:

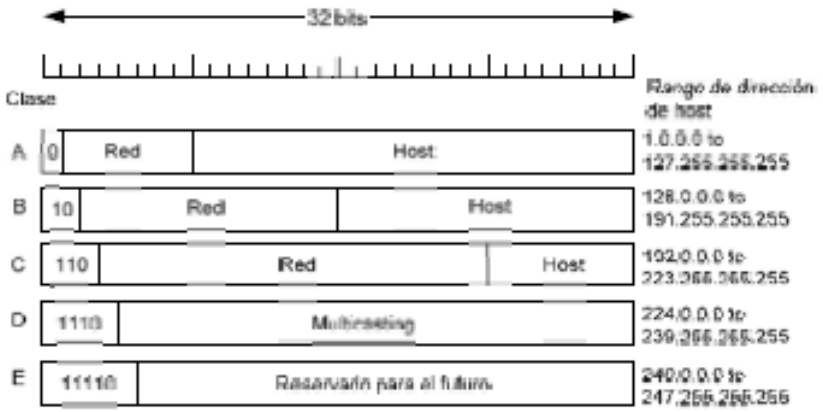


Figura 2.11. Clases de direcciones IP.

Una vez tenemos una dirección IP, para poder determinar cuál es la parte de dicha dirección que corresponde con la dirección de red, tendremos que utilizar la denominada máscara de red.

La máscara de red también será una dirección de 32 bits, que al realizar una operación AND sobre una dirección IP, nos dará como resultado la dirección de red. Veamos un ejemplo. Partimos de la IP 172.17.23.4 y la máscara de red 255.255.0.0. Recordamos que en una operación AND obtendremos el valor 1 como resultado solamente cuando ambos bits tengan el valor 1. En caso contrario el resultado es cero. Como 255 en decimal equivale al número binario 11111111, la dirección de red que conseguimos es 172.17.0.0.

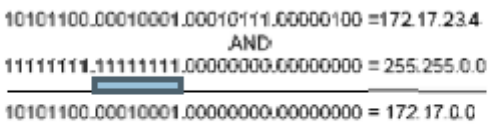


Figura 2.12. Cálculo de dirección de red.

Observemos que la máscara es una secuencia de 1 (unos) binarios seguidos de 0 (ceros) binarios. Así, para las redes clase A, como el primer byte identifica a la red, la máscara debe ser 255.0.0.0; para la clase B la máscara es 255.255.0.0 y para la

clase C, la máscara es 255.255.255.0.
Estas máscaras de red son resultados de reservar 8, 16 o 24 bits para los equipos, que son cifras redondas y que equivalen a 1, 2 o 3 bytes. Pero se puede dar el caso, de que a lo mejor no necesitemos reservar un byte completo para la reserva de bits para los equipos. Aprovecharemos esta circunstancia para la creación de subredes.
Si, por ejemplo, tenemos a nuestra disposición una red de clase C, pero necesitamos solo 50 direcciones IP para los 50 equipos que tenemos en nuestra red, estaríamos perdiendo más de 200 direcciones utilizables. Entonces, podemos tomar la determinación de dividir una red clase C en varias subredes de tal forma que podremos aprovechar mejor ese espacio de direccionamiento. Para ello, se toman varios bits que pertenecen a la dirección de dispositivos, se añaden a la dirección de red y se construye la máscara apropiada.
Por ejemplo, partamos de que tenemos la siguiente dirección de red: 192.168.55. Reservamos 2 de los bits de la dirección de dispositivo y tendremos cuatro subredes: 192.168.55.0, 192.168.55.64, 192.168.55.128 y 192.168.55.192 con la posibilidad de tener 64 equipos en cada una de estas subredes. Como la red es clase C, la máscara resultante, incluyendo los dos bits prestados, es 255.255.255.192.
En la siguiente imagen, podremos ver cómo se reservan los dos bits para las subredes, y el resto del espacio que queda disponible para que los equipos de la red puedan recibir una dirección IP:

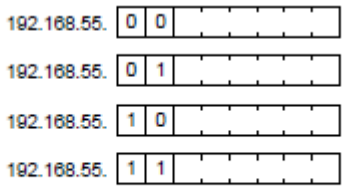


Figura 2.13. Creación de cuatro subredes IP.

1.3. Fundamentos de IPv6

El Protocolo Internet (IP), tal y como hemos visto en el anterior capítulo, ha sido el protocolo fundamental en Internet para poder identificar a los dispositivos, ya sean de una red pública o de una red privada.
No obstante, la principal desventaja de este protocolo es que está llegando al fin de su periodo útil, y en su lugar, se ha definido una nueva revisión del protocolo, cuya denominación es IPv6, que finalmente lo acabará reemplazando.

1.3.1. Motivos para el cambio

La principal limitación que ofrece IPv4 es la referida al campo de dirección. IPv4 tiene un espacio de direcciones de 32 bits, es decir, 2_{32} (4294967296). En cambio, IPv6 nos

ofrece un espacio de 2^{128} (340282366920938463463374607431768211456). Cuando fue creado el protocolo IPv4, poco se podían imaginar sus desarrolladores que pocos años después, este espacio de direccionamiento iba a estar agotado y que necesitaría una ampliación. Otras de las razones por las cuales podemos determinar que un campo de 32 bits es inadecuado serían las siguientes:

_ La estructura en dos niveles de la dirección IP (número de red y de host) puede ser útil, pero es una forma poco económica de utilizar el espacio de direcciones, ya que una vez reservados los bits que determinará la dirección de red, el resto de bits tendrán que ser utilizados para los hosts, vayamos a utilizarlos todos o no.

_ Con este modelo de direccionamiento IP, es necesario asignar un número de red único a cada red IP, sin importar si la red va a estar conectada a Internet o no.

_ El uso masivo de los últimos años del protocolo TCP/IP para todo tipo de tecnologías emergentes (VoIP, Internet TV, etc.) ha supuesto el definitivo agotamiento de direcciones IP útiles.

_ Por norma general, asignaremos una dirección única a cada ordenador. Una disposición más flexible sería poder permitir múltiples direcciones IP para cada equipo, y esto nos llevaría al punto anterior, con los problemas que la demanda de IP han supuesto.

Por lo tanto, la necesidad de un incremento en el espacio de direcciones ha supuesto la renovación del protocolo IP, que por otra parte, ya se estaba quedando desfasado y necesitaba de una revisión de requisitos en cuanto a las áreas de configuración de red, flexibilidad en el encaminamiento y facilidades para el tráfico.

1.3.2. Características de IPv6

Los principales detalles de este protocolo se recogen en documentos como la especificación general de IPv6 (RFC 2460) o en el RFC que trata con la estructura de direccionamiento de IPv6 (RFC 2373).

A modo de resumen, vamos a describir las principales características que define a IPv6:

_ Espacio de direcciones mayor: IPv6 va a utilizar 128 bits para la reserva de direcciones en lugar de los 32 bits de IPv4.

_ Un mecanismo de opciones mejorado: estas mejoras se pueden encontrar en las cabeceras. Serán opciones separadas situadas entre la cabecera de IPv6 y la cabecera de la capa de transporte. La mayoría de estas cabeceras no serán revisadas por ningún dispositivo de encaminamiento en la trayectoria del paquete, lo cual simplificará y

acelerará el procesamiento que realice dicho dispositivo en comparación a los paquetes de IPv4.

_ Direcciones de autoconfiguración: mediante esta funcionalidad, se podrán proporcionar asignaciones dinámicas de direcciones IPv6.

_ Aumento en la flexibilidad en el direccionamiento: en este sentido se introduce el concepto de dirección monodistribución (anycast), a través de la cual un paquete se entrega solo a un nodo que haya sido seleccionado dentro de un conjunto. De esta forma se mejora la escalabilidad del encaminamiento multidistribución con la incorporación de un campo de acción a las direcciones multidistribución.

_ Facilidad para la asignación de recursos: IPv6 introduce el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el que el emisor solicita un tratamiento especial, ayudando al tratamiento del tráfico especializado como puede ser el vídeo en tiempo real o el tráfico VoIP.

_ Introducción de los conceptos de Calidad de Servicio (QoS) y Clase de Servicio (CoS).

1.3.3. Cabecera de IPv6

Para empezar a comentar la cabecera IPv6, en primer lugar vamos a observar una imagen de una cabecera IPv4, y mediante los diferentes colores podemos observar cuáles son los campos que desaparecen con el nuevo formato (en naranja) y los que van a ser modificados (color verde):

Figura 3.14. Cabecera IPv4.

La primera conclusión que obtenemos es que pasaremos de tener un encabezado con 13 campos a tan solo 8 con IPv6.

La razón principal por la que se eliminan estos campos es por evitar una redundancia innecesaria, ya que en IPv4 se estaba facilitando la misma información de varias maneras. Por ejemplo, el campo de “Desplazamiento de Fragmentación”, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total “inutilidad” de este campo. En IPv6 los encaminadores no fragmentan los paquetes, y si fuera necesario, el proceso de fragmentación o desfragmentación se realizará de extremo a extremo.

Veamos el nuevo formato de cabecera para un paquete IPv6:

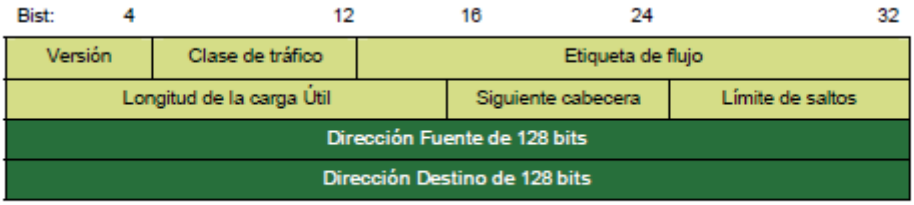


Figura 3.15. Cabecera IPv6.

Si seguimos realizando la comparación, podemos detallar cuáles son algunos de los campos modificados:

_ Longitud total por longitud de carga útil (payload length): es la longitud de los propios datos, y puede ser de hasta 65536 bytes. Tiene una longitud de 16 bits (2 bytes).

_ Protocolo por siguiente cabecera (next header): desaparece el campo de opciones de protocolo, ya que no van a utilizarse cabeceras de longitud variables, sino sucesivas cabeceras encadenadas. Tiene una longitud de 8 bits (1 byte).

_ Tiempo de vida por límite de saltos (Hop Limit): tiene una longitud de 8 bits (1 byte).

Y por último, los dos nuevos campos, que son los que nos van a permitir introducir los conceptos de Calidad de Servicio (QoS) y Clase de Servicio (CoS). Serían los siguientes:

_ Clase de Tráfico (Traffic Class): también denominado Prioridad (Priority), o Clase (Class). Tiene una longitud de 8 bits (1 byte).

_ Etiqueta de Flujo (Flow Label): para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits.

Como resumen, vamos a detallar las principales ventajas de la cabecera IPv6 respecto a la de IPv4:

_ Longitud de cabecera de 40 bytes, el doble que para IPv4, pero con ventajas al haberse eliminado campos innecesarios.

_ Esta longitud fija de cabecera facilitará las tareas de proceso a los encaminadores y conmutadores de paquetes.

_ Al estar los campos alineados a 64 bits, permite procesar de una manera mucho más eficaz estos encabezados a los procesadores de 64 bits.

_ El valor del campo “siguiente cabecera”, va a especificar cuál va a ser la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras no serán

revisadas en cada nodo de la ruta, sino solo en el nodo o nodos de destino final.

1.3.4. Direccionamiento IPv6

Las direcciones IPv6 ya hemos comentado que van a tener una longitud de 128 bits. Estas direcciones serán asignadas a interfaces individuales en los dispositivos, no a los dispositivos en sí. De esta forma, una interfaz podrá tener múltiples direcciones únicas, y todas ellas podrán ser utilizadas para identificar de forma única al dispositivo.

IPv6 va a especificar tres tipos de direcciones:

_ Unidistribución (unicast): identificador para una única interfaz. Cuando un paquete es enviado a una dirección unicast será solo recibido por la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

_ Monodistribución (anycast): identificador para un conjunto de interfaces (diferentes nodos). Cuando un paquete es enviado a una dirección anycast será entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la que esté más cerca). Esta característica nos permitirá crear, ámbitos de redundancia, de manera que varios equipos podrán ocuparse del mismo tráfico según una secuencia determinada si la primera tiene algún problema.

_ Multidistribución (multicast): identificador para un conjunto de interfaces (diferentes nodos). Cuando un paquete es enviado a una dirección multicast será entregado a todas las interfaces identificadas por dicha dirección. Son utilizados, por ejemplo, para aplicaciones de retransmisión múltiple (broadcast).

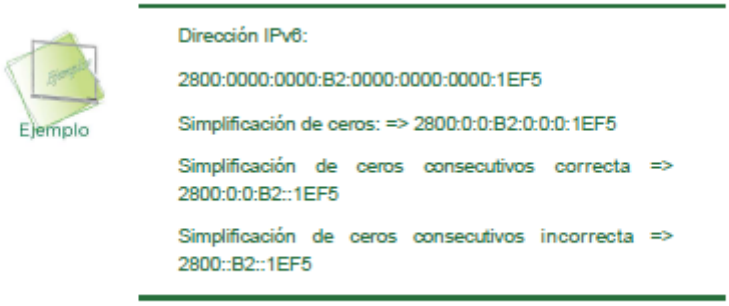
Mientras en un esquema de direccionamiento IPv4 utilizábamos 4 agrupaciones de 8 bits para alcanzar un total de 32 bits, para representar direcciones IPv6, el estándar se basa en el siguiente esquema:

Donde cada una de las “x” será un valor hexadecimal de 16 bits. No será necesario escribir ceros a la izquierda de cada campo. Veamos algún ejemplo:

Como podemos comprobar en el ejemplo anterior, se puedan dar situaciones en las

que nos encontremos con varios “0” consecutivos. En este caso, podremos realizar una abreviación mediante la inclusión de “ ::” , que servirá para representar múltiples grupos consecutivos de 16 bits “cero”. No obstante, este símbolo solo podrá aparecer una vez en cada dirección IPv6.
Veamos algunos ejemplos de los diferentes tipos de direcciones explicados Anteriormente

Hay que tener especial cuidado en no caer en errores de abreviaciones como el siguiente:



1.3.5. Autoconfiguración en IPv6

Un host podrá decidir cómo quiere configurar sus propias interfaces IPv6 mediante el proceso de autoconfiguración.
Las direcciones podrán obtenerse de una forma manual, mediante la implementación del protocolo DHCPv6 (stateful o configuración predeterminada), o de una forma automática (stateless o descubrimiento automático, sin intervención).
Si se utiliza la autoconfiguración en modo stateful, el dispositivo va a obtener una dirección para la interfaz y/o la información y parámetros de configuración desde un servidor, que albergará una base de datos con direcciones que serán asignadas a cada host.
Mediante una autoconfiguración en modo stateless, no será necesaria la configuración de forma manual del dispositivo, ni necesita servidores adicionales, ni configuración alguna de routers. Será el propio host el que construya su propia dirección mediante una combinación de información que estará accesible de forma local y otra información que le suministrarán los routers. La dirección estará compuesta por la siguiente información:

_ Un prefijo que identificará la red o subred asociada al enlace, y que será anunciado por un router.

_ Un identificador de interfaz que generará el dispositivo, y que servirá para identificar de forma única la interfaz en la subred.

Si no se tuviera ningún router, solo podrá generar la dirección de enlace local, que sería suficiente al menos para poder comunicarse con los otros dispositivos que se encuentren conectados al mismo enlace.

Ambos tipos de autoconfiguración, stateless y stateful, son complementarios. Un dispositivo podrá usar autoconfiguración stateless, para generar su propia dirección, y conseguir el resto de parámetros mediante autoconfiguración stateful.

El mecanismo de autoconfiguración "sin intervención" suele ser necesitado cuando no importa la dirección exacta que se asigne a un dispositivo, pero sí es necesario asegurarse que es única y que se pueda enrutar de forma correcta.

El mecanismo de autoconfiguración predeterminada, por el contrario, nos asegura que cada host tiene una determinada dirección, asignada manualmente.

La autoconfiguración está diseñada para dispositivos como equipos, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente.

1.4. Terminología y conceptos básicos de Windows Server

Antes de comenzar con la parte más práctica de este libro a partir de la segunda unidad, tenemos que dominar la terminología más habitual que vamos a encontrarnos a la hora de instalar, configurar y mantener sistemas de servidores basados en la familia Windows. A continuación, vamos a explicar los más relevantes.

1.4.1. Concepto de directorio y Active Directory Domain Services (AD DS)

En un entorno empresarial, los usuarios, sus equipos informáticos y el resto de dispositivos que conformen la red de la organización, podrán compartir información entre ellos. Para un administrador de sistemas, la forma más sencilla de poder organizar todos estos recursos es mediante la creación de un dominio de sistemas, a partir del cual podamos realizar todas las tareas asociadas con la parte administrativa y de seguridad de una forma centralizada en un servidor, o en varios si es necesario.

Para ello, el sistema operativo Windows Server 2008 utiliza el concepto de directorio para la implementación de estos dominios de sistemas Windows, ya sean en versión para servidores como para equipos clientes (Windows XP, Windows

Vista o Windows 7).

Un directorio

Se puede definir como una estructura jerárquica cuyo objetivo principal es el de guardar la información de los objetos (más adelante explicamos este concepto) que se encuentran en nuestra organización. Este directorio suele estar basado en una base de datos que está especialmente diseñada para operaciones de lectura y consulta.

En la actualidad, existen varios estándares para la implementación de servicios de directorio, como por ejemplo el Directory Access Protocol, o la versión más utilizada del mismo, que es más simplificada, denominada LDAP (Lightweight Directory Access Protocol).

El servicio de directorio utilizado en Windows Server 2008 es el comúnmente denominado Directorio Activo o Servicios de Dominio del Directorio Activo (Active Directory Domain Services, AD DS). Mediante el directorio activo, almacenaremos la información sobre los recursos que tenemos a nuestra disposición en el dominio y podemos otorgar permisos de acceso a usuarios y aplicaciones para que puedan acceder a los mismos. De esta forma, los administradores de sistemas, tienen a su disposición una herramienta a partir de la cual le serán más sencillas las tareas de organización, administración y control del acceso a estos recursos, todo ello de una manera centralizada. Podemos ver un ejemplo en la figura 1.17:

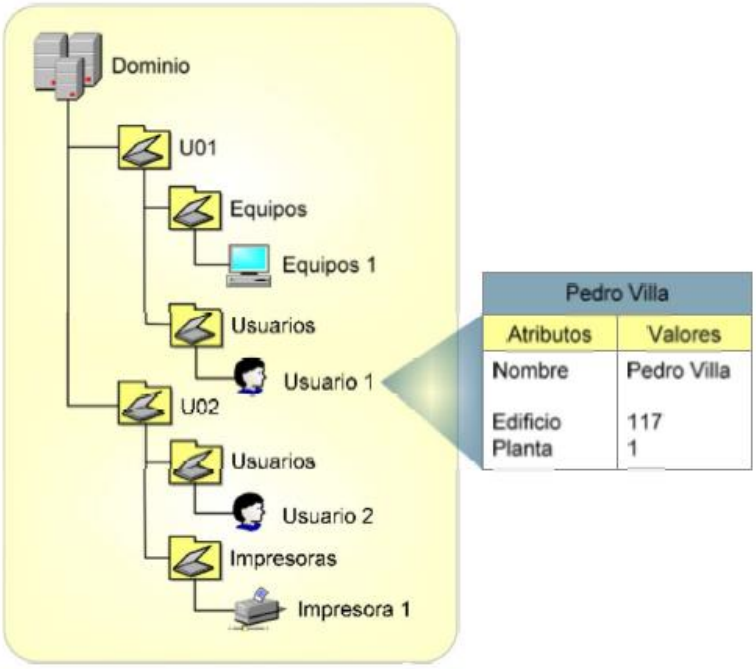


Figura 4.16. Base de datos Active Directory

La instalación de Active Directory en un servidor que tiene instalado Windows Server 2008 lo convertirá en un Controlador de Dominio (Domain Controller, DC, concepto que explicaremos más adelante en este capítulo), mientras que el resto de los equipos informáticos de la red pasarán a ser miembros de este dominio, pudiendo consultar la base de datos para sus operaciones.

Mediante la implementación de servicios de directorio para administrar los dominios, podremos separar nuestra organización, aunque sea de una manera conceptual, en una estructura lógica (los dominios) y en una estructura física (topología de red). De esta forma, conseguiremos independizar la forma en la que queramos estructurar nuestros dominios en la organización de la topología de red o redes que vayan a interconectar nuestros sistemas.

En cuanto a las tareas de administración, igualmente conseguiremos separar las labores relacionadas con la administración de la estructura física, de la administración de los dominios.

Para finalizar con el concepto de directorio, veamos las principales funciones que nos va a aportar Active Directory:

_ Realizar el control de los recursos de red de una forma centralizada: de esta forma, podremos administrar recursos como servidores, archivos compartidos e impresoras, y otorgar permisos de uso solo a usuarios autorizados para que puedan tener acceso a los recursos de Active Directory.

_ Centralizar y descentralizar la administración de recursos: los administradores pueden administrar equipos clientes distribuidos, servicios

de red y aplicaciones desde una ubicación central mediante una interfaz de administración coherente o pueden distribuir tareas administrativas mediante la delegación del control de los recursos a otros administradores.

_ Almacenar objetos de forma segura en una estructura lógica: Active Directory almacena todos los recursos como objetos en una estructura lógica, jerárquica y segura.

_ Optimizar el tráfico de red: la estructura física de Active Directory nos posibilitará el uso del ancho de banda de una manera más eficiente.

1.4.2. Estructura lógica

Como acabamos de explicar, en la parte relativa a la estructura lógica de nuestra organización, el elemento más importante en la que se basa es el dominio, dentro del cual podremos administrar los diferentes usuarios, ordenadores, grupos, directivas, etc.

A su vez, un dominio podrá ser dividido en unidades organizativas, que nos evitará tener que crear varios dominios para nuestra organización de tal forma que puedan ser administradas de forma independiente. Pero si fuera necesaria la creación de otros dominios, podríamos hacerlo mediante los conceptos de árbol y bosque. Los dos son jerarquías de dominios a distintos niveles, en función de si los dominios van a compartir o no un espacio de nombres común.

Por otro lado, estarán los objetos, que serán los diferentes recursos y usuarios, y son la unidad mínima dentro de la estructura lógica de Active Directory.

En la figura 1.18, podemos observar de forma gráfica todos estos conceptos:

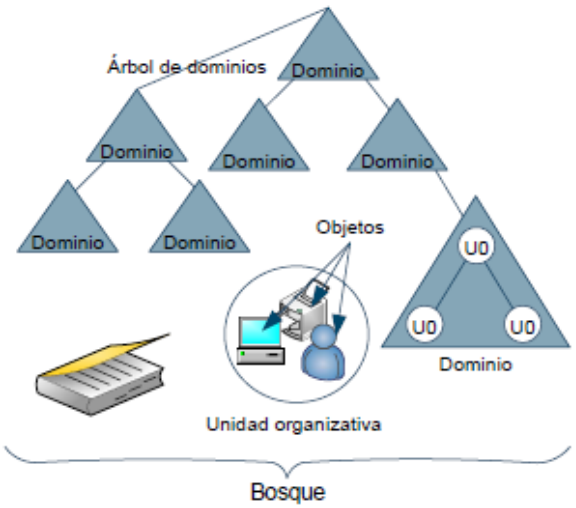


Figura 4.17. Estructura lógica de Active Directory.

A continuación, pasamos a detallar todos estos conceptos.

Dominio

El dominio será el principal elemento dentro de una estructura de Active Directory.

Estará formado por un conjunto de equipos, que van a compartir información almacenada en una base de datos.

En un dominio, al menos, tendrá que existir un servidor que tenga instalado Windows Server 2008 y que esté actuando como Controlador de Dominio, y un número variable de equipos clientes, que recibirán la denominación de miembros del dominio. Este dominio, estará unívocamente identificado gracias a un nombre de dominio DNS, que a su vez será el sufijo DNS principal de todos los miembros del dominio, y esto incluye también a el o los controladores de dominio.

Mediante la implementación de dominios, podremos obtener las siguientes funcionalidades:

_ Delimitar la seguridad: aunque tengamos un escenario donde coexistan varios dominios que puedan tener relación, todos los aspectos relacionados con la seguridad que hayan sido configurados para cada uno de ellos, serán independientes unos de otros.

_ Replicación de la información: en capítulos posteriores explicaremos la forma en la que se realizan las tareas de replicación entre dominios. El motivo de realizar esta tarea es que en cada uno de los controladores de dominio, existirá la denominada partición del dominio, que va a almacenar la base de datos del directorio. Esta partición, es, en sí misma es una unidad de replicación que tendrá copias idénticas en el resto de los controladores de dominio que formen su unidad de replicación, todos ellos pertenecientes al mismo dominio.

_ Uso de políticas de grupo: mediante la creación de políticas de grupo, que serán aplicadas a dicho dominio, podremos delimitar cómo queremos que se comporten los equipos y usuarios que formen parte del mismo.

_ Delegación de los permisos administrativos: en ocasiones, en organizaciones amplias, puede ser interesante la idea de tener varios usuarios o unidades organizativas, que puedan realizar las tareas de administración. Como ya hemos dicho que un dominio representa un límite de seguridad, estos permisos serán limitados al dominio.

Creación de múltiples dominios: árbol y bosque

Cuando en una organización sea necesario disponer de varios dominios, mediante Active Directory podremos almacenar y organizar toda la información del directorio de todos estos dominios de forma independiente unos de otros, aunque la información siempre estará disponible para todos ellos.

Un bosque

Será una estructura lógica formada por un conjunto de dominios que a su vez podrá estar compuesto por uno o varios dominios, distribuidos en uno o varios árboles de dominios.

Esta forma de organizar los dominios se basa en una estructura de árbol invertida, donde la raíz estará en la parte superior, y la vinculación que exista entre los diferentes dominios quedará detallada mediante la configuración de relaciones de confianza, que explicaremos más adelante.

El dominio raíz del bosque será creado al instalar el primer controlador de dominio dentro de la organización, y será el encargado de almacenar la configuración y esquema del bosque, que será compartido con el resto de dominios. Una vez creado este dominio raíz, podremos añadir otros subdominios a dicha raíz (árbol de dominios), o podremos crear otros dominios “hermanos” del dominio inicial, para, así, ampliar el número de árboles del bosque de dominios, que a su vez podrá crear también subdominios.

continuación, vamos a definir de forma más específica los conceptos de árbol y bosque:

_ Árboles de dominio: un árbol estará formado por uno o más dominios dentro de un mismo bosque y compartirán un espacio de nombres contiguo (sufijo DNS común).

El primer dominio que se crea será el dominio raíz del bosque, que será creado en ese momento y siendo el primer árbol de dicho bosque. Cuando se decida añadir un nuevo dominio, éste se convertirá en un dominio secundario de alguno de los dominios existentes, que se convertirá en un dominio padre. Estos dominios secundarios suelen ser utilizados para delimitar zonas geográficas de la organización o diferentes departamentos, por ejemplo.

Una vez formado el árbol de dominios, las relaciones padre-hijo entre ellos es una relación de confianza, donde cada uno seguirá manteniendo sus propias características e independencia. De esta forma, un dominio padre no será automáticamente el administrador del dominio hijo, ni las políticas que tenga configuradas en su dominio, serán automáticamente aplicadas al hijo.

_ Bosques: un bosque estará compuesto por un grupo de árboles que no van a compartir un espacio de nombres contiguo, y que estarán interconectados a través de relaciones de confianza bidireccionales. Es importante comprender que independientemente de cuál sea la cantidad y

estructuración de los dominios que puedan localizarse dentro de una organización, todos juntos formarán un único bosque.
De esta forma, todos los dominios que formen parte del bosque, van a compartir la misma configuración, el mismo esquema de directorio y el mismo catálogo global (concepto que definiremos más adelante).
Cuando queramos añadir nuevos dominios a un bosque, tendremos que tener en cuenta las siguientes consideraciones:

_ No podrán ser movidos dominios de Active Directory entre diferentes bosques.

_ Un dominio dentro de un bosque solo podrá ser eliminado si no tiene dominios hijo.

_ Una vez que se haya creado el dominio raíz de un árbol, no podrán ser añadidos al bosque nuevos dominios cuyo nombre de dominio pertenezca a un nivel superior.

_ No podrá ser creado un dominio padre de un dominio ya existente

La estructuración de los dominios de una organización en un bosque, el cual pueda estar compuesto por uno o varios árboles, nos posibilitará la opción de tener una estructura de nombres de dominios contiguos y discontiguos. En la siguiente imagen podemos ver un esquema de nombres para un bosque:

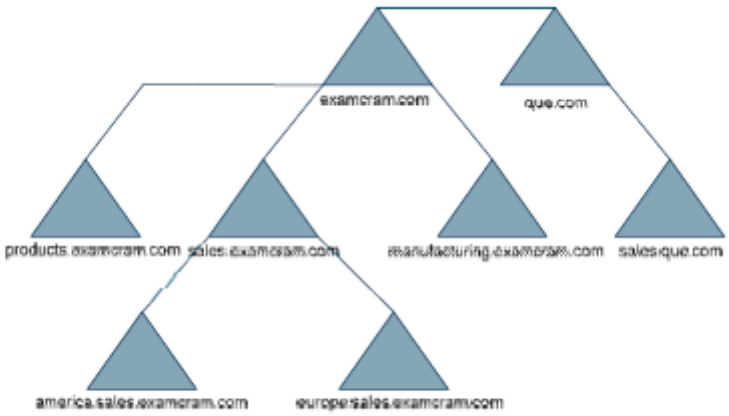


Figura 4.18. Bosque con múltiples árboles, con árboles múltiples niveles de dominios hijo.

Unidades organizativas

Una unidad organizativa (Organizational Unit, OU) es un objeto del Directorio Activo que a su vez va a contener a otros objetos del directorio. Por lo tanto, dentro de una Unidad Organizativa, podremos encontrar objetos como cuentas de usuario, de grupo, de equipo, recursos compartidos como impresoras e incluso otras unidades organizativas.
Mediante las unidades organizativas, podremos crear estructuras jerárquicas de objetos pertenecientes al directorio, que podrán ser movidos de una unidad organizativa a otra si fuera necesario. Podremos conseguir los siguientes objetivos fundamentales:

_ Configurar políticas independientes a usuarios y equipos: una de las

operaciones más comunes será la de establecer determinadas políticas o directivas de grupo a los usuarios o a los equipos que se encuentren dentro de una unidad organizativa. Para ello, podremos vincular directamente estas políticas o directivas directamente a las unidades organizativas, y de esta forma poder realizar distinciones en el comportamiento de usuarios y equipos en función de la OU en la que se encuentren alojados. Si por ejemplo en nuestra organización, creáramos tantas unidades organizativas como departamentos la conformarán, podríamos establecer políticas independientes a cada uno de ellos, y así los usuarios que trabajen en cada departamento tendrían comportamientos distintos e independientes.

_ Delegación de tareas administrativas: podremos otorgar permisos administrativos a un usuario o grupos de usuarios, para que puedan administrar de forma total o parcial una unidad organizativa.

1.4.3. Estructura física

Con la estructura lógica hemos aprendido que podemos organizar todos los recursos de una organización. En la estructura física, el objetivo que perseguimos es el de configurar y administrar el tráfico de red.

Una estructura física de Active Directory estará compuesta por los sitios y los controladores de dominio. Podremos controlar los lugares y momentos en los que se produce el tráfico de replicación y de inicio de sesión de usuarios.

Sitios

Un sitio es una combinación de una o varias subredes IP en nuestra organización que estarán conectadas entre ellas. Aprovechando esta circunstancia, configuraremos la topología de replicación y la forma de acceder al Active Directory, para que de esta forma los sistemas Windows Server 2008 puedan realizar de manera más eficiente el tráfico de inicio de sesión y la replicación.

Un sitio será creado por dos razones principalmente:

_ Optimizar el tráfico de replicación.

_ Que los usuarios puedan conectarse a un controlador de dominio a través de una conexión de alta velocidad.

En resumen, podríamos decir que los sitios definen la estructura física de la red mientras que los dominios definirán la estructura lógica de la organización.

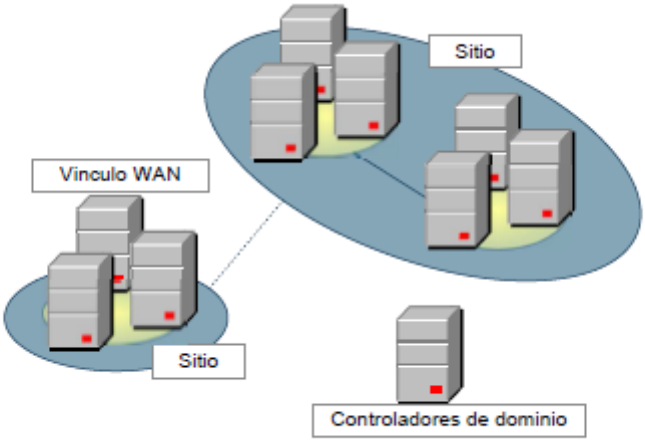


Figura 4.19. Sitios y controladores de dominio.

Los controladores de dominio pertenecientes a un sitio podrán replicar las modificaciones que se realicen de una forma casi inmediata. Sin embargo, las replicaciones entre sitios serán más lentas si las comparamos con las que se producen en el interior de un sitio.

Controladores de dominio

El controlador de dominio (Domain Controller, DC), será un equipo que tendrá instalado un sistema operativo Windows Server, ya sea 2008 o anteriores versiones, y que almacenará una réplica del directorio activo. Otras operaciones importantes que realizará serán la de otorgar a los usuarios la posibilidad de autenticarse mediante el protocolo Kerberos, así como la consulta de información del directorio mediante el protocolo LDAP.

La información que va a almacenar cada controlador de dominio está dividida en cuatro particiones, que van a constituir las unidades de replicación, y serán las siguientes:

_ Partición del directorio de esquema: contendrá la definición de los tipos de objetos que pueden ser creados, y que serán comunes a todos los dominios del bosque, replicándose por todos los controladores de dominios del bosque. Por cada bosque, solo habrá un controlador de dominio que podrá modificar el esquema, mientras para el resto, la partición será de solo lectura.

_ Partición de directorio de configuración: contendrá los datos relativos a la estructura de los dominios y la topología de replicación, que serán comunes a todos los dominios del bosque, y que serán replicados por todos los controladores de dominio. A diferencia de la partición anterior, cuando cualquier controlador de dominio necesite modificar esta partición, tendrá permiso para ello y los cambios serán replicados al resto de controladores de dominio del bosque.

_ Partición de directorio de dominio: contendrá la información relativa a los

objetos que va a contener exclusivamente un dominio en concreto, y podrá ser replicada al resto de controladores de dominio de ese dominio, pero no al resto.

_ Particiones de directorio de aplicaciones: en este caso contendrá los datos relativos a aplicaciones específicas. Estos datos podrán ser de cualquier tipo a excepción de objetos de cuentas de usuarios, grupos y equipos.

Catálogo global y esquema

Aparte de las cuatro particiones principales que hemos comentado que tiene un controlador de dominio, habría que añadir una quinta, que sería la destinada a almacenar el catálogo global de la organización.

Este catálogo global es una partición de solo lectura que almacenará una copia de todos los objetos de cada dominio de una forma reducida. Concretamente, se copian aquellos objetos que son usados de forma más frecuente en las consultas al directorio, aunque este punto puede ser configurado en el esquema.

Un esquema será una definición para todo el bosque de las clases de objetos y atributos que se podrán extender.

Las clases de objetos, como los usuarios, equipos o impresoras, describirán los objetos de directorio que pueden ser creados. Por cada clase de objeto, encontraremos un conjunto de atributos. Por ejemplo, el atributo Nombre podrá ser utilizado por muchas clases de objetos, pero solo será necesario que sea definido una vez en el esquema.

Los atributos, podrán ser creados de forma independiente a las clases de los objetos. Cada uno podrá ser definido una sola vez y podrá ser utilizado para varias clases de objetos. Los cambios en el esquema, se podrán volver a definir o desactivar.

El catálogo global incluirá la información necesaria para que pueda determinarse la ubicación de cualquier objeto de la organización. Los siguientes elementos formarán parte del catálogo global:

_ Atributos que sean utilizados con más frecuencia en las consultas: nombre, apellido o nombre de inicio de sesión de un usuario, por ejemplo.

_ Información que sea relevante para poder concretar la ubicación de un objeto en el directorio.

_ Un subconjunto predeterminado de atributos para cada tipo de objeto.

_ Permisos de acceso para cada uno de los objetos y atributos que estén en el catálogo global. De esta forma, los permisos de acceso nos garantizarán que los usuarios no podrán encontrar objetos para los que no tengan asignados permisos de acceso.

De esta forma, un servidor de catálogo global será el controlador de dominio que va a almacenar una copia de dicho catálogo y se encargará de ejecutar las

consultas que se puedan realizar al mismo. Por cada bosque será necesario la existencia de, al menos, un controlador de dominio que esté configurado para realizar estas tareas, y que será creado en el momento en el que se crea el primer controlador de dominio del bosque.

Si tenemos una cantidad considerable de dominios, será necesario que otros controladores ejerzan también las funciones de servidor de catálogo global, para poder balancear el tráfico de autenticación de inicios de sesión y transferencias de consultas.

A modo de resumen, podemos decir que un catálogo global tendrá dos objetivos fundamentales que cumplir:

_ Permitir a un usuario que pueda iniciar sesión a través de la información de pertenencia a grupos universales de un controlador de dominio. Esta pertenencia solo está almacenada en los catálogos globales.

_ Permitir a un usuario la posibilidad de buscar información en el directorio en todo el bosque, sin importar donde se encuentre la ubicación de los datos.

Maestros de operaciones

Cada vez que se realiza un cambio en un dominio, este cambio puede ser replicado a través de todos los controladores de dominio. De la misma forma, cada vez que se produce un cambio en el esquema, podrá replicarse en todos los dominios del bosque. A este tipo de replicaciones se les denomina replicación de varios maestros.

Un servidor que realice las tareas de maestro de operaciones, será un controlador de dominio que tendrá asignadas una o varias funciones de maestro único en un dominio o en el bosque del directorio activo. Este servidor, realizará operaciones que no podrán ser realizadas de forma simultánea en otros controladores de dominio de la red. Por ejemplo, se podría producir un conflicto de replicación si las actualizaciones que lo han originado son realizadas de forma simultánea sobre el mismo atributo de un objeto en dos controladores de dominio a la vez.

De esta forma, no podrán ser introducidos cambios en distintos lugares al mismo tiempo. En cualquier momento, podremos transferir esta propiedad a cualquier equipo del resto de los controladores de dominio.

Active Directory define cinco tipos de funciones para el maestro de operaciones, y cada una de ellas tendrán una ubicación por defecto. Estas funciones podrán ser aplicadas a todo el bosque o a todo el dominio.

Las funciones que serán únicas para todo el bosque serían las de maestro de esquema y maestro de nombres de dominio. Solo habrá un maestro de esquema y un maestro de nombres de dominio en todo el bosque:

_ Maestro de esquema: su función será de controlar las actualizaciones que se realicen en el esquema. Dispondrá de una partición de lectura o escritura.

_ Maestro de nombres de dominio: su función será la de controlar si se

añaden, renombran o eliminan dominios del bosque. Solo podrá añadir un nuevo dominio aquel controlador de dominio que tenga el rol de maestro de nombres de dominio. También deberá permitir la creación o eliminación de particiones de aplicación en cualquier dominio del bosque

Por otra parte, todos los dominios de Active Directory tendrán que tener controladores de dominio que realicen las siguientes tres operaciones de maestro único:

_ Emulador del controlador de dominio principal (Primary Domain Controller, PDC): antiguamente el PDC se encargaba principalmente de mantener la compatibilidad a nivel de servidor con los sistemas anteriores Windows NT4. Aunque en Windows 2008 se ha eliminado esta función, aún sigue siendo necesario para otras dos funciones: autenticar usuarios que inicien sesión en miembros del dominio previos a Windows 2000 y realizar de manera urgente la replicación de una contraseña que acaba de ser cambiada por un usuario de un controlador de dominio en concreto. De esta forma, si un usuario obtuviera un error a la hora de validarse por un problema con la contraseña, se intentará validar a continuación en el emulador de PDC, por si dicha contraseña hubiera sido cambiada recientemente y este cambio aún no hubiera sido replicado en todos los controladores de dominio.

_ Maestro de identificadores relativos (RID): cuando se crea un objeto, el controlador de dominio asignará una entidad nueva principal de seguridad que va a representar a dicho objeto, y también un identificador único de seguridad (Security Identifier, SID). Este SID estará formado por los siguientes dos elementos:

_SID de dominio: será el mismo para todas las entidades principales de seguridad que hayan sido creadas en el mismo dominio.

_Identificador Relativo (Relative Identifier, RID): será único para cada entidad principal de seguridad creada en el dominio.

Por lo tanto, el controlador de dominio maestro RID, se encargará de asignar secuencias de identificadores relativos a todos los controladores de dominio. De esta forma nos aseguramos que dos controladores de domino no asignarán el mismo SID a dos objetos principales de seguridad, como pueden ser los usuarios, grupos o equipos.

_ Maestro de infraestructuras: cuando se desplazan objetos de un domino a otro, el maestro de infraestructuras tendrá que actualizar las referencias de los objetos de su dominio que estén apuntando al objeto en el otro dominio. Esta referencia al objeto contendrá el identificador único global del objeto

(Globally Unique Identifier, GUID), el nombre completo y un SID.

Para comprender mejor todos los roles que acabamos de comentar, podemos observar la siguiente imagen:

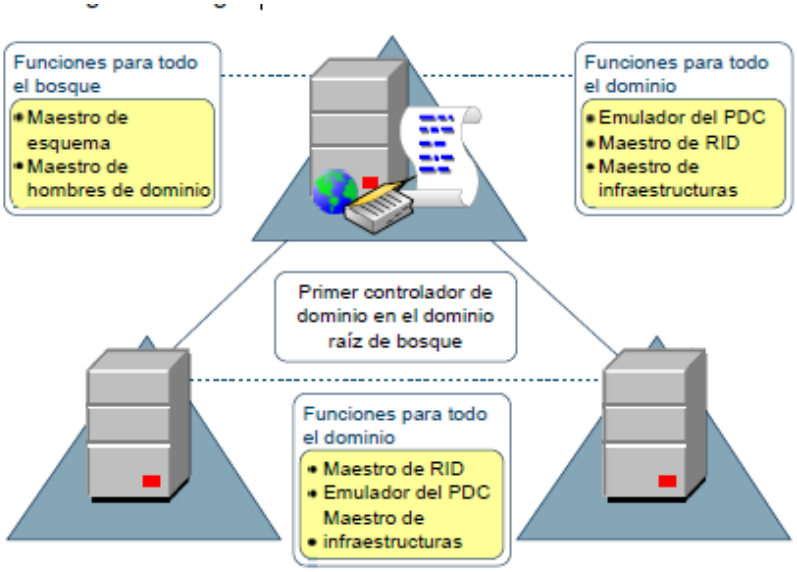


Figura 4.20. Resumen de maestros de operaciones.

1.4.4. Objetos de Active Directory

En este capítulo vamos a explicar los principales objetos que pueden ser creados en Active Directory, comentando para cada uno de ellos cuáles pueden ser sus mejores configuraciones y cuáles son sus principales cometidos en la infraestructura de un dominio.

Usuarios globales

Cualquier controlador de un dominio podrá crear cuentas de usuario global, también conocidas como cuentas de usuario del dominio, de tal forma que podrán ser administradas desde Active Directory y ser visibles desde todos los equipos que estén incluidos en el bosque, y por lo tanto, en toda la organización.

A esta cuenta se le podrán asignar los permisos que el administrador considere oportuno, para que el usuario pueda acceder a los recursos que estén situados en cualquier dominio del bosque, siempre que tenga los permisos oportunos.

Cada cuenta de usuario, para que pueda ser distinguida de forma unívoca del resto, llevará asociado un identificador único en el bosque denominado SID, que ya hemos comentado anteriormente.

Este estará formado por el prefijo común de las cuentas de un mismo dominio y el identificador relativo RID, que será único para las cuentas del dominio. Podremos encontrar tres tipos de cuentas que tendrán asignado este atributo: las cuentas de usuario, las de grupos y equipos. Son las consideradas “cuentas principales de seguridad”.

Es importante no confundir los usuarios de dominio, con los usuarios locales, que cualquier equipo perteneciente a un dominio es capaz de crear, pero que su ámbito de trabajo estará restringido al propio equipo. A este usuario local, no podremos asignarle permisos de acceso a los recursos del dominio, ya que dicha cuenta no será localizada en la base de datos de Active Directory, y por lo tanto, es como si no existiera para el dominio.

La primera cuenta de usuario de dominio que es creada de forma automática cuando creamos un dominio, es la cuenta “Administrador”, que será quien tenga la totalidad de los permisos administrativos para la gestión del dominio, y por lo tanto, tendrá pleno control de la base de datos de Active Directory, así como de cada equipo que sea miembro del dominio, como si fuera un administrador local del equipo. Como particularidad, podemos decir que esta cuenta no podrá ser borrada, ni bloqueada, aunque sí podrá ser renombrada.

Cuando una cuenta de usuario del dominio es creada, entre los diferentes campos que tendremos que rellenar, existe uno que será de especial importancia para que el usuario pueda ser identificado dentro del dominio en el proceso de inicio de sesión. Nos referimos al nombre de inicio de sesión.

El nombre de inicio de sesión, es el identificador nativo en sistemas Windows Server 2008 para que un usuario pueda validarse en cualquier dominio del bosque. Estará formado por dos partes, separadas del símbolo “@” : usuario@dominio.

Este nombre también es conocido como nombre principal de usuario (User Principal Name, UPN), y será único en el bosque.

Grupos

En el directorio podremos crear dos tipos de grupos: grupos de distribución y grupos de seguridad.

Mientras que los grupos de distribución se utilizan para crear listas de distribución de correo electrónico, los grupos de seguridad son los que se van a utilizar para las tareas administrativas, y por eso vamos a centrarnos principalmente en estos últimos.

Un grupo de seguridad, podrá ser definido en tres ámbitos distintos, que comentamos a continuación:

_ Grupos locales de dominio: podrán contener cuentas de usuario de todos los dominios del bosque, cuentas de grupos globales o universales de cualquier dominio del bosque, así como otros grupos locales de dominio del mismo dominio. Su visibilidad estará reducida al dominio en el que hayan sido creados y por lo general suelen ser utilizados para administrar recursos que estén localizados en los equipos del dominio.

_ Grupos globales: en este caso sólo estarán formados por los usuarios del mismo dominio y de otros grupos globales del mismo dominio. Podrán ser

visibles en todos los dominios del bosque y suelen ser utilizados para formar conjuntos de usuarios según sean los trabajos que realizan dentro de la organización y de los roles que tienen en el dominio.

_ Grupos universales: podrán contener cuentas de usuario, grupos globales y otros grupos universales de cualquier dominio del bosque. Podrán ser visibles para todo el bosque, y suelen ser empleados para administrar recursos que puedan estar localizados en ordenadores de varios dominios del bosque.

Las recomendaciones a la hora de crear grupos de dominios, serían las siguientes:

1. En función de las labores que realicen los usuarios dentro de la organización, crear grupos globales con estos propósitos e incluir a dichos usuarios.
2. En función del nivel de acceso que vayan a tener en los recursos del dominio los usuarios y/o grupos globales, incluirlos en grupos locales del dominio.
3. Asignar permisos en dichos recursos exclusivamente a los grupos locales del dominio.

En la siguiente imagen podemos ver de forma gráfica lo que acabamos de comentar:

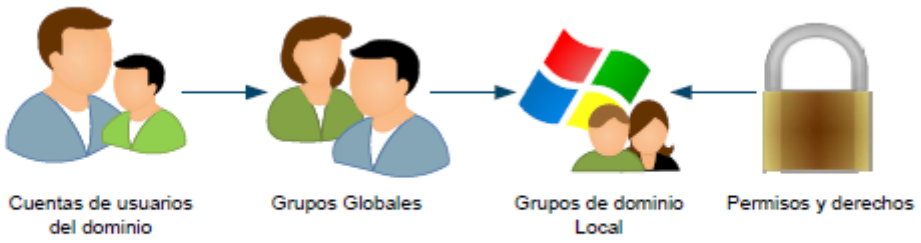


Figura 4.21. Recomendaciones en la creación de cuentas y grupos.

Podremos encontrarnos numerosos grupos que ya habrán sido creados en la instalación de Active Directory. Por ejemplo, en el contenedor “Builtin”, podremos encontrar grupos que serían equivalentes a los que podemos encontrar en cualquier grupo local de cualquier sistema Windows que no sea miembro de un dominio. Serían los casos de los grupos “administradores”, “Operadores de copia”, etc.

Pero lo grupos que sean propios de Active Directory los podremos encontrar en el contenedor “Users”. Estos grupos están asociados a los diferentes niveles de acceso preasignados en el directorio. Algunos de ellos serían, por ejemplo, los grupos “administradores del dominio” o “usuarios del dominio”.

Equipos

El directorio activo también va a almacenar información sobre las cuentas de equipo, que servirá para identificar a todos los ordenadores de la organización, ya sean simples miembros del dominio, en cuyo caso estarán alojados por defecto en

el contenedor “Computers”; o los propios controladores de dominio, que estarán alojados por defecto en el contenedor “DomainControllers”.
Algunos de los datos que cada cuenta de equipo es capaz de almacenar son los siguientes:

_ Nombre del equipo: que va a coincidir con el nombre real del equipo.

_ Contraseña: que será la utilizada por el equipo para validarse en el dominio, al igual que los usuarios del dominio.

_ SID: ya hemos comentado anteriormente, que existían tres tipos de cuentas principales de seguridad: las cuentas de usuario, las de grupo y las de equipo.

Unidades organizativas

En el capítulo de estructura lógica, ya hemos comentado lo que eran las Unidades Organizativas y cuáles eran sus principales propósitos.
En este capítulo las recordamos porque al fin y al cabo también son objetos pertenecientes al directorio, que además, podrán contener a otros objetos. De esta forma, podremos delegar la administración de todos los objetos que contenga a otros usuarios del dominio que estimemos oportuno, o personalizar el comportamiento de sus objetos contenidos mediante el uso de directivas de grupo específicas.

1.4.5. Protocolos de autenticación

Windows Server 2008 trabaja con dos protocolos para las tareas de autenticación de sistemas y usuarios para acceder a los recursos en el dominio. Estos son los protocolos NTLM y Kerberos V5.
NTLM (NT LAN Manager), era el protocolo de autenticación en dominios en los antiguos sistemas Windows NT4, y que en la actualidad se sigue utilizando para poder soportar a estos sistemas. No obstante, con el tiempo han ido apareciendo mejoras para dicho protocolo, como por ejemplo, un protocolo de cifrado de 128 bits para su última versión NTLMv2.
Kerberos, es el protocolo de autenticación recomendado si exclusivamente vamos a trabajar con sistemas de Windows 2000 hacia las versiones más modernas. Las ventajas que tiene frente a NTLM, básicamente serán las siguientes:

_ En Kerberos se va a producir una autenticación mutua entre el servidor y el cliente, asegurándonos que no han sufrido una suplantación de identidad.
Sin embargo, en NTLM solo es el servidor quien autentifica al cliente.

_ En Kerberos, cuando un usuario quiere acceder al recurso de un dominio, el ordenador desde el que está trabajando recibirá un ticket procedente del controlador del dominio a través del cual podrá acceder a múltiples servidores del dominio, de tal forma que éstos no tengan que volver a

contactar con el controlador de dominio. Sin embargo, en NTLM, cada vez que el usuario intenta acceder a un recurso que esté localizado en un servidor, éste tendrá que contactar con un controlador de dominio para autenticar al usuario.

_ En Kerberos, las confianzas son bidireccionales y transitivas, y serán configuradas de forma automática a medida que se van añadiendo dominios al bosque. Además, admitirá confianzas entre bosques y entre dominios Kerberos que no sean Windows. Las relaciones en NTLM serán manuales, unidireccionales y no transitivas.