U6 Recursos compartidos

Parte I. Windows

Implantación de Sistemas Operativos

Índice

6.1 Introducción a las técnicas de red.

- En la actualidad no se concibe la idea de trabajar de forma aislada. Muy al contrario, cada vez está más presente la interconexión entre ordenadores formando redes.
- Desde redes pequeñas domésticas conocidas como PAN (Personal Area Network), redes de centros de trabajo LAN (Local Area Network) hasta las grandes redes WAN (Wide Area Network) que permiten interconectar redes entre sí, como lo es Internet.
- Por lo tanto será necesario un Sistema Operativo de Red (SOR) que gestione estas redes y los elementos que las componen.
- Sus tareas más importantes serán:

  Gestión centralizada de recursos
  Ofrecer servicios a clientes
  Proporcionar acceso seguro a los recursos
  Monitorización de lo que está pasando en la red

6.1 Introducción a las técnicas de red.

Grupos de trabajo (red entre iguales).

- **Configuración de red plana** entre iguales → ningún equipo realiza tareas de administración, solo de si mismo**.** Cada cliente es administrador de los recursos que ofrecen a la red y todos pueden acceder. Si se quiere limitar el acceso se establece una contraseña que deben conocer solo los usuarios con acceso al recurso. ¿Qué supone esto?
    - **No existe una administración centralizada.** Cada uno comparte lo que quiere cuando quiere.
    - **Muy fácil de configurar y difíciles gestionar.** No existe un control de quien tiene acceso y quien no a los recursos.
    - **Poca funcionalidad.**
    - **Recursos dispersos en la red.**
    - **Muy insegura (usuarios "avanzados").** Cada usuario toma sus propias decisiones con respecto a la seguridad y esos criterios no tienen por qué coincidir.

6.1 Introducción a las técnicas de red.

Servicios Individuales (red cliente – servidor).

Red no plana (existen servidores dedicados).

Es un modelo de aplicación distribuida, las tareas se dividen entre los proveedores de recursos y servicios. Los proveedores son los servidores y los equipos que demandan los servicios son los clientes. Un cliente realiza una petición a un servidor y éste le responde.

Es una separación lógica, el que ofrece los servicios no tiene por qué estar en una máquina separada, ni es necesariamente solo un programa. Además esta división lógica no es estricta, ya que un servidor puede actuar como cliente de otro proveedor de servicios.

Es una red en la que los clientes están conectados a un servidor en el que se centralizan los recursos y servicios con que cuenta la red. Todas las gestiones se concentran en el servidor, lo que facilita la localización de forma sencilla.

6.1 Introducción a las técnicas de red.

Servicios Individuales (red cliente – servidor).

Red no plana (existen servidores dedicados).

El problema surge cuando queremos agregar varios servidores a la red. Cada uno mantiene su propia lista de usuarios y recursos. Si un cliente necesita acceder a las aplicaciones de tres servidores necesitará tres cuentas con tres contraseñas. Cada una de esas cuentas será creada y mantenida por un servidor distinto de forma separada. Es fácil que los servidores pierdan sincronía cuando se actualizan manualmente.

La situación también se complica para el usuario que debe conectarse y tener una contraseña diferente para cada servidor. Aunque este proceso se puede automatizar, suele ser propenso a errores.

Este tipo de redes sigue siendo adecuada para situaciones simples en las que solo hay un servidor con funciones muy delimitadas, pero no es válido para la mayoría de situaciones actuales.

6.1 Introducción a las técnicas de red.

Servicios Individuales (red cliente – servidor).

Resumiendo:

Red no plana (existen servidores dedicados).

No existe administración centralizada
(cada servidor se administra de forma pormenorizada).

Fáciles de configurar y difíciles gestionar.

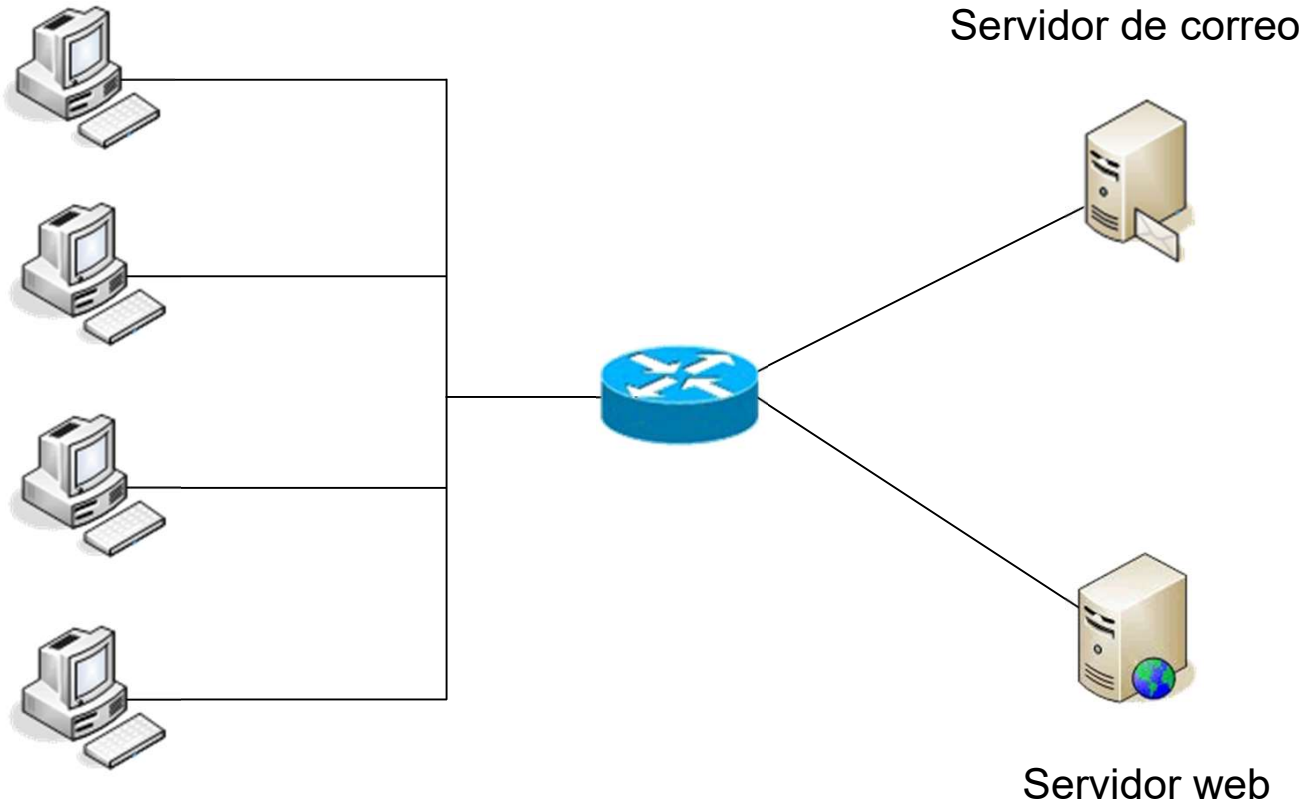
Funcionales (ofrecen servicios de red).

Recursos menos dispersos en la red.

Seguras (protección de los servidores).

6.1 Introducción a las técnicas de red.

Servicios Individuales.



6.1 Introducción a las técnicas de red.

Servicios de directorio. Dominios.

Con la configuración cliente – servidor hemos dado un paso hacia la gestión óptima de la red, pero la dispersión de la información plantea un problema de accesibilidad y control.

Por esta razón surgen los servicios de directorios, que son un conjunto de aplicaciones que guardan y administran toda la información sobre los elementos de una red.

Un servicio de directorio ofrece una infraestructura para localizar, administrar y organizar los componentes y recursos de una red, que serán tratados como objetos.

Un servicio de directorio es un componente fundamental del SOR (sistema operativo de red), ya que es la herramienta que los diferencia de los sistemas operativos cliente.

6.1 Introducción a las técnicas de red.

Servicios de directorio. Dominios.

Resumiendo:

Red no plana (existen controladores de Dominio).

La administración es centralizada (existe un Catálogo Global de datos).

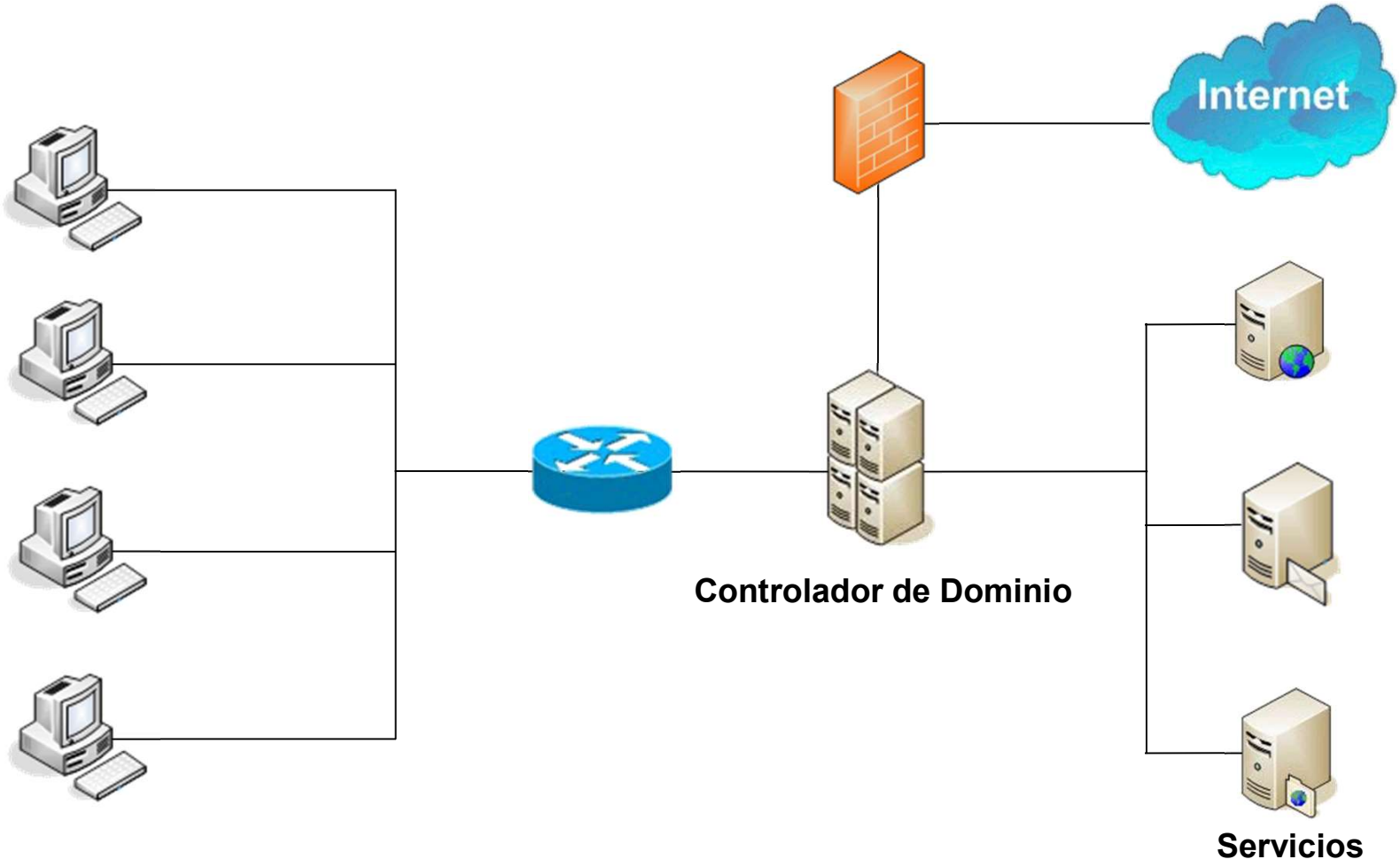
Difíciles de configurar y fáciles gestionar.

Muy funcionales (divididas en dominios, árboles y bosques).

Muy Seguras (protección del controlador de Dominio).

6.1 Introducción a las técnicas de red.

Servicios de directorio.



6.2 Servicios de directorios. Elementos.

Los servicios de directorio almacenan información sobre la organización, sitios, ordenadores, usuarios, objetos compartidos y cualquier otra cosa que pueda formar parte de la infraestructura de red. Los elementos del directorio activo pueden ser diferentes unos de otros (usuarios, grupos, políticas de acceso, permisos, etc.), por lo que la información almacenada variará según la naturaleza del objeto. Toda esta información se almacena en una base de datos jerárquica.

ELEMENTOS:
(algunos de ellos se desarrollarán más adelante)

- **Directorio:** es un repositorio único para la información relativa a los usuarios y recursos de una organización (objetos).
- **Dominio:** colección de objetos dentro de un directorio, que forman un subconjunto administrativo. Para poner nombre a los dominios se usa el protocolo DNS, por lo que es necesario al menos un servidor DNS, instalado en la red.

6.2 Servicios de directorios. Elementos.

- **Objeto:** Cualquiera de los componentes que forman parte del directorio. Pueden ser recursos, usuarios, relaciones de confianza, servidores, equipos, grupos, etc. Cada objeto tendrá un nombre específico que lo identificará y una serie de características que quedarán definidas en el Esquema de la base de datos.
  En general, los objetos se organizan en tres categorías:

  - **Usuarios:** identificados a través del binomio nombre/contraseña y que se pueden organizar en **grupos.**
    Desde el punto de vista informático, un usuario es un conjunto de permisos y privilegios sobre determinados recursos, no tiene que ser necesariamente una persona.

  - **Recursos:** elementos a los que los usuarios pueden acceder, según sus privilegios, para desarrollar su actividad. Pueden ser carpetas compartidas, impresoras, etc.

  - **Servicios:** funciones a las que los usuarios tienen acceso, como el correo electrónico, conexión a internet o copias de seguridad en la nube.

6.2 Servicios de directorios. Elementos.

- **Unidad Organizativa:** es un contenedor de objetos que permite organizarlos en subconjuntos de forma jerárquica. De esta forma podemos establecer una estructura lógica que represente de forma adecuada a nuestra organización y simplifique la administración.

- **Grupos:** conjunto de objetos **usuario**. Al igual que las unidades organizativas, facilitan la organización y administración de los objetos, en este caso concreto, usuarios.

- **Controlador de dominio:** es el equipo que contiene la base de datos de objetos del directorio para un determinado dominio, incluida la información de seguridad. Además será responsable de la autenticación de objetos dentro de su ámbito de control.

- **Maestro de operaciones:** existe un conjunto de operaciones que deben estar centralizadas para mantener la consistencia del sistema. El equipo encargado de estas operaciones adquiere este rol.

6.2 Servicios de directorios. Elementos.

- **Árbol:** conjunto de dominios dependientes de una raíz común y que tienen una estructura jerárquica. Dicha jerarquía se caracteriza por tener un espacio de nombres común (DNS).

  De esta forma sabemos que **iessanvicente.com, dam.iessanvicente.com** y **asir.iessanvicente.com** forman parte del mismo árbol, mientras que **iessanvicente.com** e **iessanvicente.es** no.

  El objetivo de esta fragmentación de la estructura es replicar solo las partes necesarias para disminuir el tráfico en la red.

  Si un usuario es creado dentro de un dominio, automáticamente será reconocido en todos los dominios que jerárquicamente dependan del dominio al que pertenece.

6.2 Servicios de directorios. Elementos.

- **Bosque:** es el mayor contenedor lógico dentro del directorio, conteniendo a todos los dominios dentro de su ámbito. Los dominios están interconectados por relaciones de confianza, de forma que los dominios dentro de un bosque confían automáticamente unos en otros y los diferentes árboles podrán compartir recursos (se verá más adelante).

  Varios árboles pueden integrarse en el mismo bosque, pero **NO** compartirán espacio de nombres (DNS)

  Un bosque contendrá por lo menos un dominio, que será el dominio raíz del bosque.

- **Esquema:** se refiere a la estructura de la base de datos.

6.2 Servicios de directorios. Elementos.

- **Sitio:** grupo de ordenadores que están relacionados de forma lógica, o geográfica o técnica particular, y que necesitan un conjunto de normas diferentes al resto. Por ejemplo, un controlador de dominio en el otro extremo del planeta que los clientes (siempre que estén unidos por la conexión adecuada), todos juntos formarán el mismo sitio.

- **Relaciones de confianza:** método de comunicación segura entre dominios, árboles y bosques, que permiten a los usuarios autentificarse en otra parte del directorio a la que no pertenecen.

En resumen, un servicio de directorio ofrece toda la información de los recursos de la red a través de una única ubicación. Para ello convierte cada recurso en un objeto y almacena su información en una base de datos jerárquica y opcionalmente distribuida. La gestión de estos datos se realiza a través de un protocolo determinado por la versión del servicio de directorio escogido. En nuestro caso **ACTIVE DIRECTORY con LDAP** (protocolo ligero de acceso a directorios)

6.3 Dominios, árboles y bosques.

Dominios.

- Conjunto de objetos que comparten un área y una nomenclatura específica.

- Nos permite:

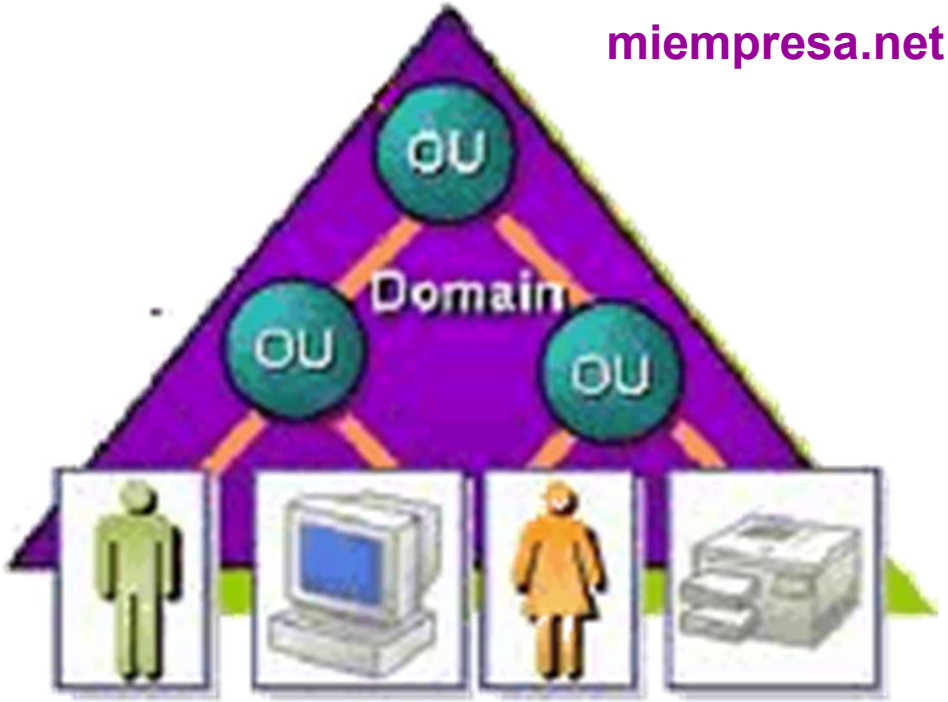
    - Delimitar la seguridad (usuarios, acceso, recursos…).
    - Replicar la información (unidades de copias de seguridad).
    - Aplicación de Políticas de Grupo (influyen al dominio).
    - Delegar permisos administrativos (entre dominios u objetos del dominio).
    - Organizado en Árboles y Bosques (estructura jerárquica).
    - Establecer relaciones de confianza (entre dominios).

6.3 Dominios, árboles y bosques.

Dominios.

Estructura jerárquica.

Dominio
miempresa.net



6.3 Dominios, árboles y bosques.

Dominios.

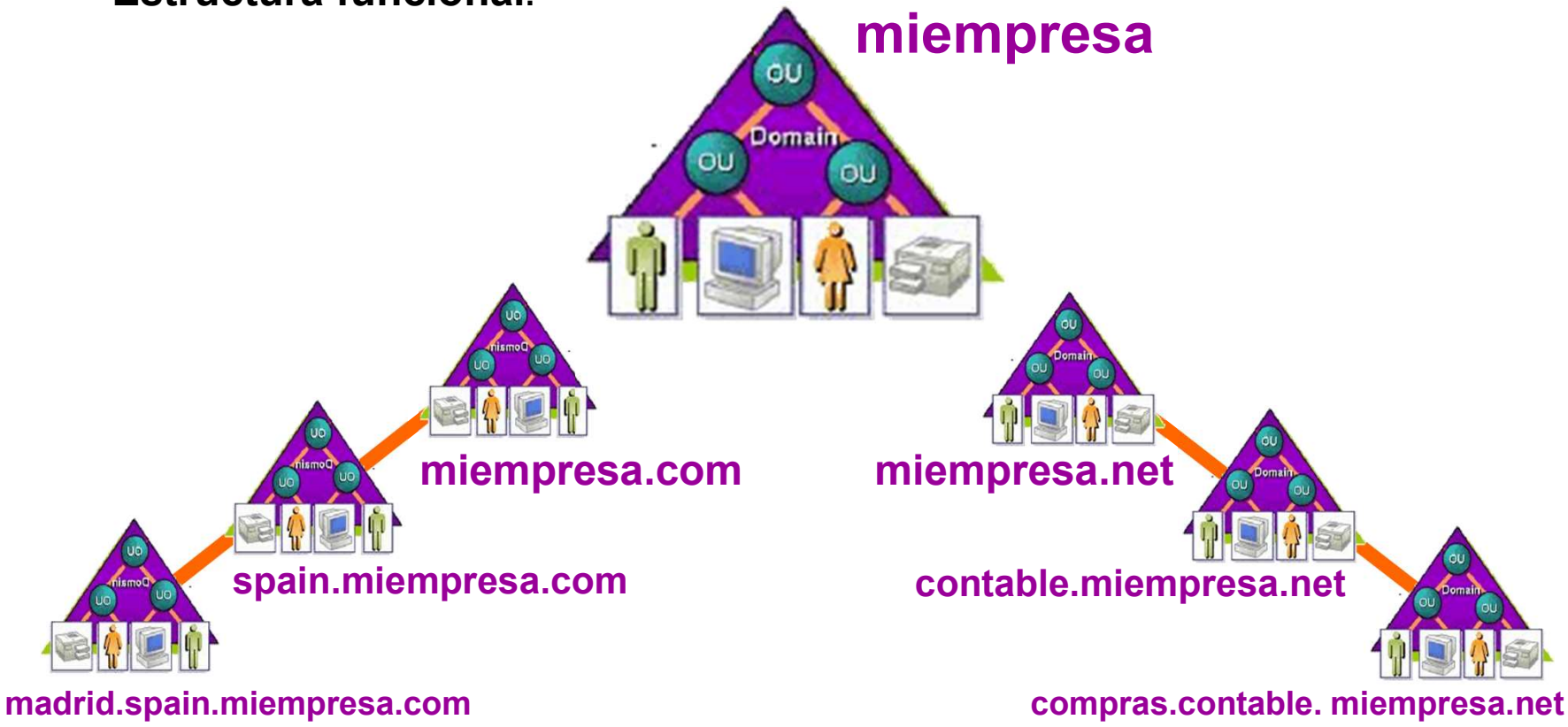
Estructura jerárquica.

Árbol de Dominios.

6.3 Dominios, árboles y bosques.

Dominios.

Estructura funcional.



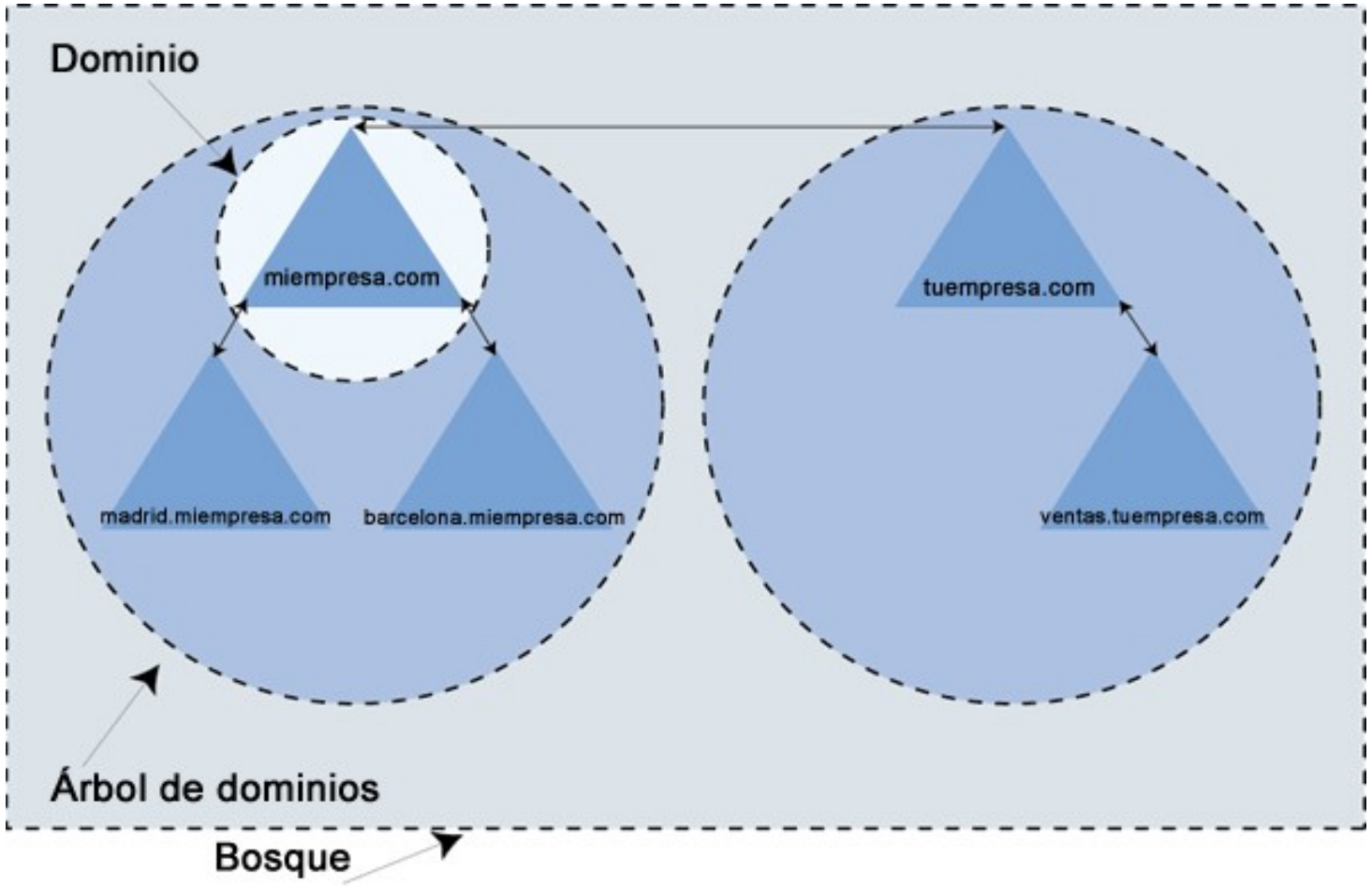
División espacial

División funcional

6.3 Dominios, árboles y bosques.

Dominios.

Estructura jerárquica. **Bosque.**

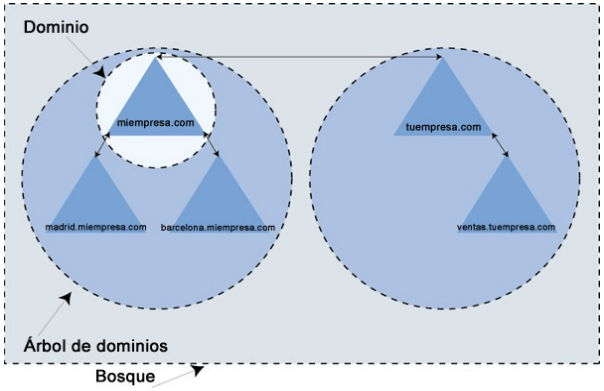


6.3 Dominios, árboles y bosques.

Dominios.

Estructura jerárquica.

Bosque.



En este ejemplo se ve como se han unido 6 dominios en un bosque. De estos 5 dominios 3 pertenecen a un árbol (raíz: miempresa.com) y los otros 2 a un segundo árbol (raíz: tuempresa.com).

Las flechas que vemos en el esquema son las relaciones de confianza entre dominios. Todas han sido creadas automáticamente por Windows Server. Todos los dominios pueden comunicarse entre sí gracias a las propiedades de las relaciones de confianza, que veremos ahora.

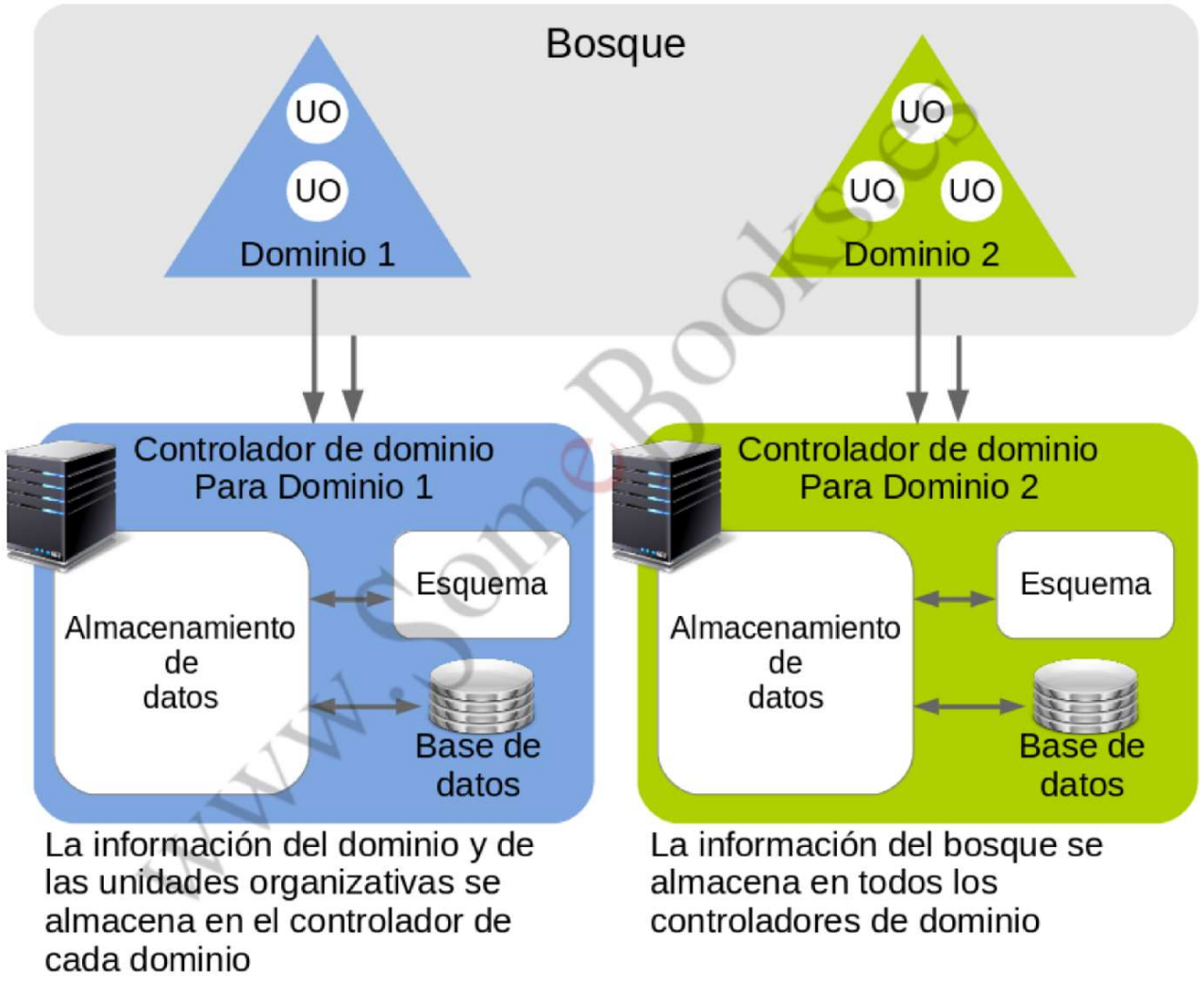
6.3 Dominios, árboles y bosques.

Dominios.

Estructura jerárquica.

Bosque.

Cada uno de estos dominios tendrá como mínimo un controlador de dominio Windows Server y un gran número de máquinas conectadas.



6.3 Dominios, árboles y bosques.

Relaciones de confianza: relación establecida entre dos dominios de forma que permite a los usuarios de un dominio ser reconocidos por otro dominio y acceder a sus recursos. Los administradores podrán definir los permisos de usuario para los usuarios de otro dominio.

Características de las Relaciones de confianza, según:

- **Método de creación.**
  Automática (implícita) o manual (explícita).
- **Dirección.**
  Unidireccionales o Bidireccionales.
- **Transitividad.**
  Dominio A confía en Dominio B. Dominio B confía en Dominio C. Dominio A confía en Dominio C.

6.3 Dominios, árboles y bosques.

Relaciones de confianza. Tipos.

Confianza raíz de árbol → Automática, bidireccional y transitiva.

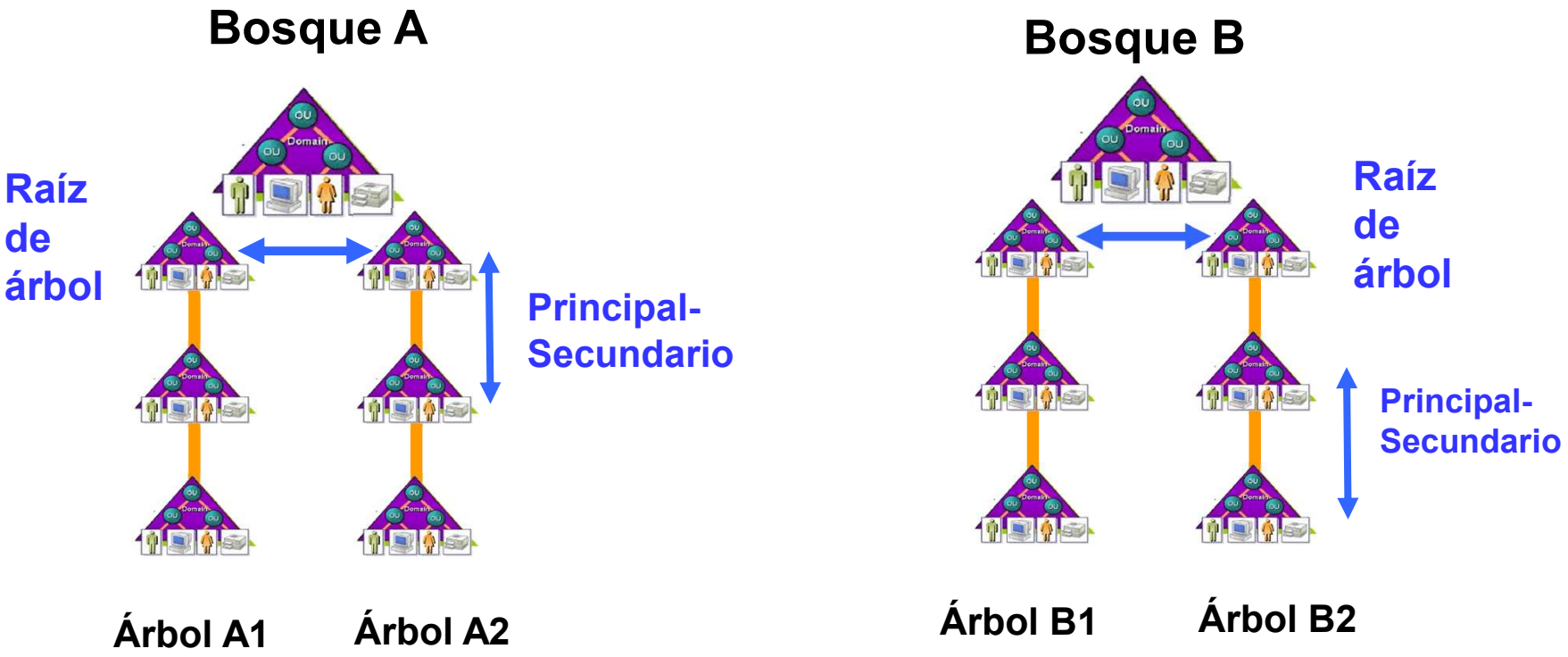
Esta relación se establece de forma automática entre los dominios raíz del mismo bosque.

6.3 Dominios, árboles y bosques.

Relaciones de confianza. Tipos

Confianza principal-secundario → **Automática, bidireccional y transitiva.**

Relación automática que se establece entre un dominio y sus subdominios.



6.3 Dominios, árboles y bosques.

Relaciones de confianza. Tipos.

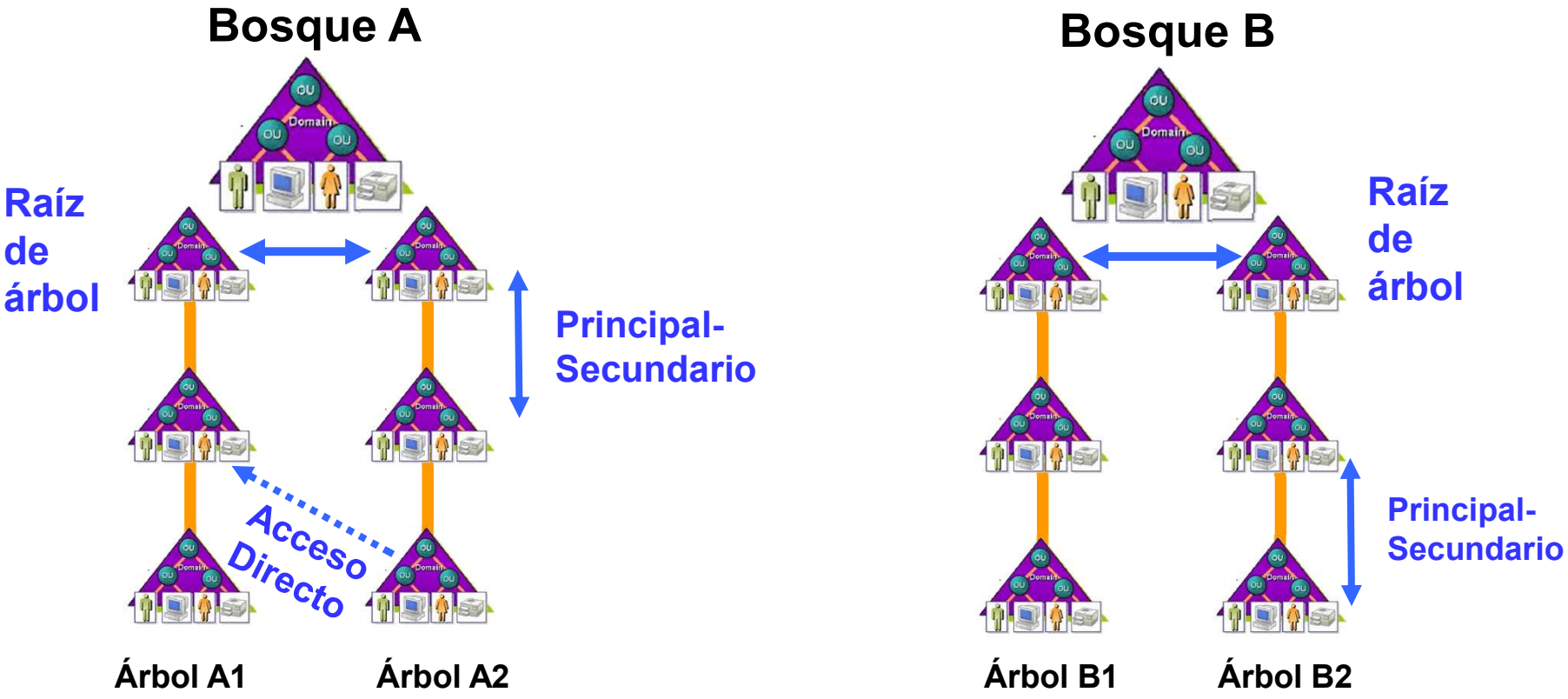
Confianza de acceso directo → Manual, unidireccional y transitiva.

Esta relación se establece de forma manual y su objetivo es mejorar la eficiencia y acelerar el inicio de sesión remotos. Si los usuarios de un dominio A acceden con frecuencia al dominio B y estos dominios están en árboles diferentes (“lejos” con muchos dominios intermedios), la confianza que ya tienen a través de otras relaciones, les permite crear una relación directa que acorta el tiempo de autentificación. Al ser unidireccional, sería necesaria una segunda relación de confianza si quisiéramos comunicación en el otro sentido.

6.3 Dominios, árboles y bosques.

Relaciones de Confianza. Tipos.

Confianza de acceso directo → Manual, unidireccional y transitiva.

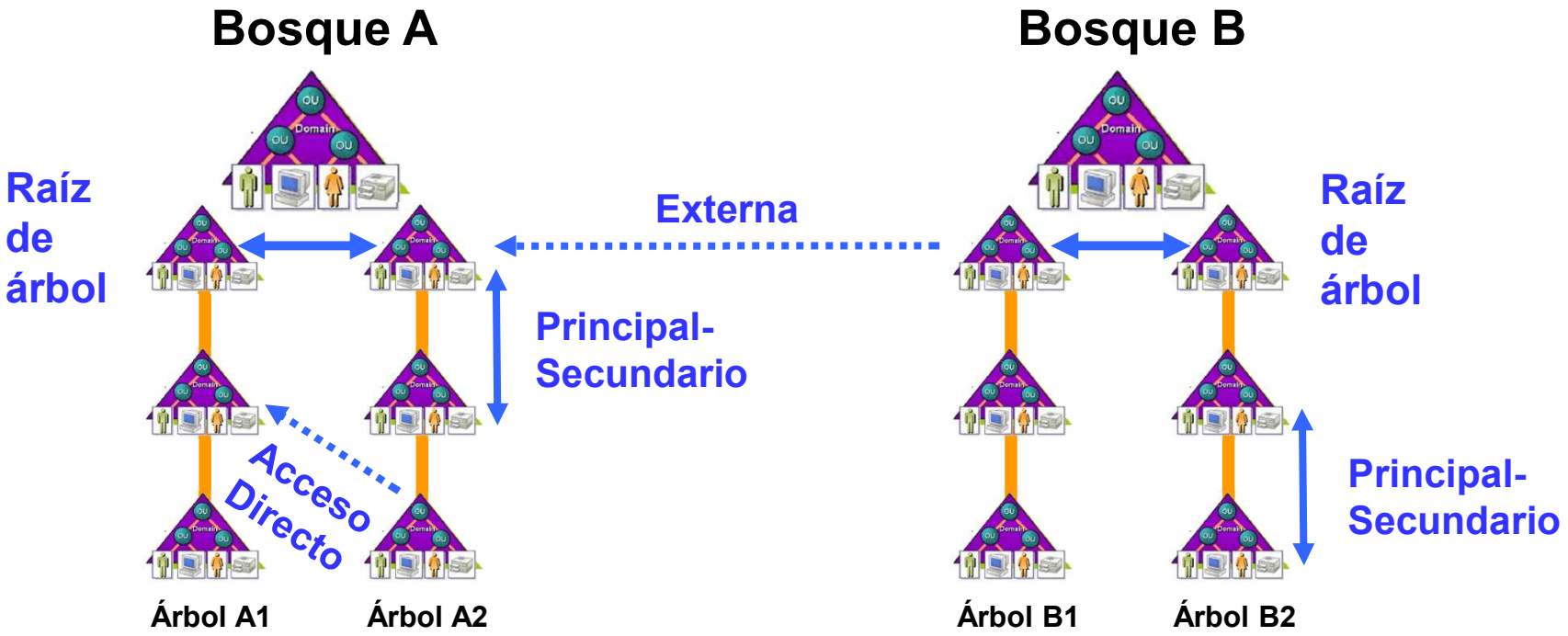


6.3 Dominios, árboles y bosques.

Relaciones de confianza. Tipos.

Confianza externa → Manual, unidireccional y no transitiva.

Permite a usuarios de un dominio Windows Server acceder a dominios de otro bosque, que no estén unidos por confianza de bosque o bien dominios de Windows NT4. Se tiene que crear manualmente.

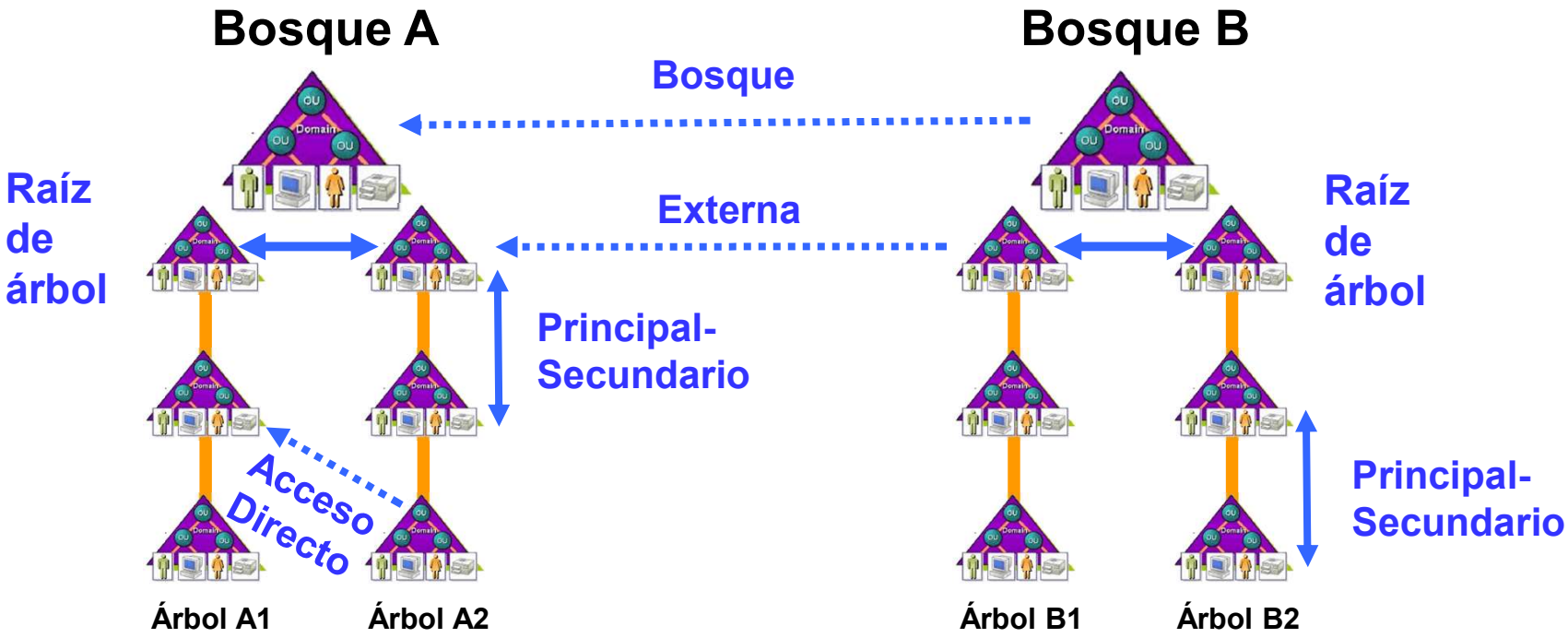


6.3 Dominios, árboles y bosques.

Relaciones de confianza. Tipos.

Confianza de bosque → **Manual, unidireccional y no transitiva.**

Relación entre dominios raíz de dos bosques distintos. Permite a los usuarios de cualquier dominio de un bosque acceder a los recursos de cualquier dominio de otro bosque.



6.3 Dominios, árboles y bosques.

Relaciones de Confianza. Resumen.

Las relaciones de confianza automáticas o implícitas, se crean por defecto en los dominios de forma bidireccional y transitiva. El efecto de estas relaciones es que de forma automática, los usuarios de cualquier dominio del bosque son conocidos y pueden acceder a los recursos en todos los dominios de dicho bosque.

Las relaciones de confianza manuales o explícitas están reservadas para casos en los que queramos mejorar la eficiencia o permitir interactuar con otros bosques o con otros dominios que no son de Windows Server.

6.3 Unidades Organizativas. OU.

- Una OU es un contenedor de objetos que permite organizarlos (como si fuera una carpeta de Windows). Puede contener cuentas de usuario, de grupo, de equipo, de recursos, etc., además de otras OU. Mediante OU podemos crear una jerarquía de objetos en el directorio. Su objetivo es estructurar y organizar el conjunto de objetos del directorio de forma coherente.

- Los objetos ubicados en una OU pueden moverse, posteriormente, de una OU a otra, pero no puede copiarse. Cada objeto es único en el directorio y su existencia es independiente de la OU a la que pertenezca.

6.3 Unidades Organizativas. OU.

- Las OU permiten:
    - **Delegar la administración:** cada OU puede administrarse de manera independiente y se puede otorgar la administración total o parcial a determinado usuario o grupo de usuarios con el nivel de responsabilidad adecuado.
    - **Establecer de forma centralizada comportamientos distintos a usuarios o equipos:** A cada OU podemos vincularle unas ***políticas de grupo,*** que aplican comportamientos a usuarios y equipos cuyas cuentas se ubican en dicha unidad. Así podemos aplicar restricciones distintas a subconjuntos de usuarios y equipos del dominio, en función de la unidad organizativa a la que pertenecen. Por ejemplo podemos limitar el acceso a ciertas aplicaciones, a los usuarios del departamento de contabilidad y que esto no aplique a los usuarios del departamento de informática.

6.3 Unidades Organizativas. OU.

Resumiendo:

- La unidad organizativa es un conjunto de usuarios, equipos y recursos administrados independientemente.

- En realidad, en Windows Server, el concepto de dominio va más bien, asociado a la distribución de los sitios (topología de red) y a la implementación de DNS que exista o quiera crearse en la empresa.

- En muchas ocasiones, para organizaciones de pequeño o mediano tamaño, resulta más adecuado implementar un modelo de dominio único con múltiples unidades organizativas que un modelo de múltiples dominios.

- Si es necesario cada unidad puede administrarse independientemente con administradores delegados y comportamientos (políticas) diferentes.

6.3 Controlador de dominio y catálogo global.

Controlador de dominio:

- Un controlador de dominio es un equipo donde se ejecuta Windows Server y que almacena una replica del directorio.
- En Windows Server, todos los controladores de dominio admiten cambios, y estos cambios se replican a todos los controladores de dominio.

Servidor de catálogo global:

- Un catálogo global es un depósito de información que contiene los atributos para todos los objetos de Active Directory. Contiene la información necesaria para determinar la ubicación de cualquier objeto del directorio.
- Funciones:
    - Permite que un usuario inicie sesión en la red proporcionando la información necesaria al controlador de dominio.
    - Permite que un usuario busque información en todo el bosque, independientemente de la ubicación de los datos.

6.3 Políticas de Grupo (GPO).

- Las GPO (Group Policy Object) son un conjunto de configuraciones específicas para usuarios y equipos de un dominio que se almacenan en objetos de directivas de grupo.
- Cuando una GPO se aplica en un controlador de dominio, todos los objetos del que es responsable, han de cumplir esa regla. El uso es sencillo y centralizado, bastará con habilitar/deshabilitar la opción en el gestor de GPO.
- Requisitos para usar GPO:
    - Que la red esté basada en una estructura de dominio y que exista al menos un controlador de dominio.
    - Equipos y usuarios deben estar unidos al dominio, usando credenciales de dominio para iniciar sesión en sus equipos. Es decir, que sean objetos del directorio.
- Las GPO tienen prioridad sobre la configuración del perfil de usuario en caso de conflicto. Es el nivel más alto en las restricciones de seguridad del sitio.

6.3 Políticas de Grupo (GPO).

- Las GPO no se pueden aplicar a un grupo de usuarios. Solo son aplicables a **equipos, sitios, dominios o unidades organizativas**, aunque su aplicación afecte a equipos y usuarios del dominio.
- Si queremos aplicar una serie de reglas a un conjunto de equipos, introduciremos estos equipos en una OU y aplicaremos la GPO o GPOs a esa OU. Si hay varias indicaremos el orden.
- Al habilitar una GPO el orden en que se aplica es el siguiente:
    - **Directivas de equipo local**: políticas que se aplican a los equipos que no están en el dominio, como servidores independientes.
    - **Directivas de sitio:** aplica a todos los equipos/usuarios del sitio, independientemente del dominio del mismo bosque al que pertenezcan.
    - **Directivas de dominio:** aplica a todos los equipos/usuarios del dominio.
    - **Directivas de unidades organizativas (OU):** aplica a todos los equipos/usuarios de la OU.

6.3 Políticas de Grupo (GPO).

- **Añadir GPO:**
  - **Con coherencia:** se añaden las nuevas GPOs a las existentes y aplican todas.
  - **Sin coherencia:** si hay contradicciones, las directivas aplicadas posteriormente sobrescriben a las directivas aplicadas con anterioridad.
- **Herencia:**
  - Si asignamos una GPO a una unidad organizativa, todos los objetos contenidos en esa OU heredan esa política. La herencia puede ser bloqueada o ejecutada en cada nivel. Si un administrador bloquea una GPO en un objeto de nivel superior, automáticamente deja de afectar a los objetos contenidos.

6.3 Políticas de Grupo (GPO).

DIRECTIVAS SEGÚN SU FUNCIÓN

- **Directivas de grupo por defecto o de seguridad:** Al crearse un dominio, se crean dos directivas de seguridad que afectan al dominio por defecto (caracteres de una contraseña, cada cuanto se cambia, etc.):
    - **A nivel de dominio**: Afecta a todos los equipos del dominio.
    - **A nivel de controlador de dominio**: solo aplica a los controladores de dominio, pero sin suplantar a las generales de dominio, si hay conflicto aplica la de dominio.
- **Directivas de entorno (GPO)**: por ejemplo, quien tiene acceso al panel de control. Pueden ser aplicadas:
    - A nivel de equipo local.
    - A nivel de sitio.
    - A nivel de dominio.
    - A nivel de unidad organizativa.

6.3 Políticas de Grupo (GPO).

DIRECTIVAS SEGÚN EL OBJETO QUE CONFIGURAN

En cada directiva aparecen dos ramas, que agrupan las directivas dependiendo de si vamos a configurar un **usuario** o un **equipo**. Aunque las ramas son las mismas, las políticas dentro de cada una de ellas es diferente.

- **Configuración de equipo:**
    - Configuración de software.
    - Configuración de Windows.
    - Plantillas administrativas.
- **Configuración de usuario:**
    - Configuración de software.
    - Configuración de Windows.
    - Plantillas administrativas.