(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 562 448**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04L 12/24 (2006.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.04.2009 E 09746900 (1)**

(97) Fecha y número de publicación de la concesión europea: **06.01.2016 EP 2294792**

(54) Título: **Descubrimiento y visualización de controladores de dominio de directorio activo en mapas topológicos de redes**

(30) Prioridad:

15.05.2008 US 153273

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.03.2016

(73) Titular/es:

SOLARWINDS WORLDWIDE, LLC (100.0%)
7171 Southwest Parkway, Building 400
Austin, TX 78735, US

(72) Inventor/es:

SWAN, MICHAEL JON

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Descubrimiento y visualización de controladores de dominio de directorio activo en mapas topológicos de redes.

Campo de la invención

La presente invención se refiere al uso de técnicas de mapeo de topologías de red para descubrimiento e integración dentro de mapas topológicos de redes con el fin de descubrir Controladores de Dominio (DC) de Directorio Activo (AD).

Antecedentes de la invención

Los documentos XP2556498, US2006/056306A1 y XP15053254 constituyen técnica anterior conocida referente a la invención.

El DC de AD, o nodos de red funcionalmente similares, lleva a cabo funciones administrativas importantes en la red. Por ejemplo, los DC de AD gestionan típicamente el registro y el acceso de usuarios y dispositivos.

Con el tiempo, a medida que una red crece, se amplía, y evoluciona, las posiciones de los DC de AC pueden llegar a perderse. Las herramientas conocidas de mapeo de DC de AD comienzan con un conjunto de nodos conocidos y recurren a características de los nodos para identificar los DC de AD. No obstante, si los nodos dejan de ser conocidos, estos nodos no se pueden sondear para determinar si son DC de AD. Por otra parte, cada sección de la red necesita tener típicamente un DC de AD local, y la aplicación conocida puede no identificar correctamente ningún DC de AD para cada agrupamiento localizado de nodos. Así, las herramientas convencionales de mapeo de AD visualizan la infraestructura de AD sin ningún sentido de integración en la infraestructura de red de la topología de esta última.

La topología de redes es el estudio de la disposición o mapeo de los elementos (vínculos, nodos, etcétera) de una red, especialmente las interconexiones físicas (reales) y lógicas (virtuales) entre nodos. Una red de área local (LAN) es un ejemplo de red que presenta tanto una topología física como una topología lógica. Cualquier nodo dado en la LAN tendrá uno o más vínculos con otro u otros nodos de la red y el mapeo de estos vínculos y nodos sobre un grafo da como resultado una forma geométrica que determina la topología física de la red. De manera similar, el mapeo del flujo de datos entre los nodos de la red determina la topología lógica de la misma.

Así, la topología de redes describe la disposición física o lógica específica de los elementos de una red. Los elementos pueden ser físicos o lógicos de tal manera que los elementos físicos son reales, y los elementos lógicos pueden ser, por ejemplo, elementos virtuales o una disposición de los elementos de una red. Dos redes pueden compartir una topología similar si la configuración de las conexiones es igual, aunque las redes pueden diferir en otros aspectos tales como interconexiones físicas, dominios, distancias entre nodos, velocidades de transmisión y/o tipos de las señales. Una red puede incorporar múltiples redes más pequeñas. A título de ejemplo, una central telefónica privada es una red y dicha red forma parte de una central telefónica local. La central local forma parte de una red mayor de teléfonos que permiten llamadas internacionales, y está conectada en red con redes de telefonía celular.

Cualquier topología de red particular se determina únicamente por el mapeo gráfico de la configuración de conexiones físicas y/o lógicas entre nodos. Por lo tanto, la Topología de Red LAN es técnicamente una parte de la teoría de grafos. Las distancias entre nodos, interconexiones físicas, velocidades de transmisión y/o tipos de señal pueden diferir en dos redes y sin embargo sus topologías pueden ser idénticas. La disposición o mapeo de los elementos de una red da origen a ciertas topologías básicas las cuales a continuación se pueden combinar para formar topologías más complejas (topologías híbridas). Los más comunes de estos tipos básicos de topologías incluyen el bus (tal como Bus Lineal, Distribuido), la estrella, el anillo, la malla (que incluye una malla parcial o totalmente conectada), el árbol, híbrido que está compuesto por una o más topologías de red, y de punto-a-punto.

La topología lógica se corresponde con un mapeo de las conexiones aparentes entre los nodos de una red, según evidencia el trayecto que parecen tomar los datos cuando se desplazan entre los nodos. La clasificación lógica de las topologías de red sigue en general las mismas clasificaciones que las correspondientes de las clasificaciones físicas de topologías de red, utilizándose para determinar la topología el trayecto que toman los datos entre nodos por oposición al uso de las conexiones físicas reales para determinar la misma. Normalmente las topologías lógicas están íntimamente asociadas a métodos y protocolos de control de acceso a los medios (MAC). En general, las topologías de red vienen determinadas por protocolos de red en contraposición a su determinación por la distribución física de cables, y los conductores, y dispositivos de red o por el flujo de las señales eléctricas, aunque, en muchos casos, los trayectos que toman las señales eléctricas entre nodos pueden coincidir considerablemente con el flujo lógico de datos, y de ahí la convención de usar de manera intercambiable las expresiones “topología lógica” y “topología de señales”. Típicamente, las topologías lógicas se pueden reconfigurar de manera dinámica mediante tipos especiales de equipos, tales como encaminadores y conmutadores.

Sumario de la invención

La invención queda definida por el objeto de las reivindicaciones independientes.

Formas de realización de la presente solicitud se refieren al descubrimiento de Controladores de Dominio (DC) de directorio activo (AD) a través de una aplicación y un método de mapeo topográfico que forman un mapa topológico de red, utilizan consultas de Protocolo Ligero de Acceso a Directorios (LDAP) y análisis de datos devueltos para identificar los DC de AD, y a continuación integran los dispositivos que ejecutan el LDAP en el mapa topológico.

Ciertas formas de realización de la presente solicitud se refieren a un descubrimiento de DC de AD que incluye la determinación de la topología de la red, tal como los nodos y las conexiones de la red. Después de determinar la topología de la red, se determinan los modos y las conexiones de la misma. A continuación, se crean (enlazan) conexiones de LDAP con o bien (a) el punto extremo ("servidor") de LDAP de usuarios actuales o bien (b), si el usuario ha especificado una o más credenciales de dominio, el punto extremo de LDAP asociado a dichas credenciales. Las conexiones de LDAP se pueden crear utilizando técnicas y órdenes convencionales. Seguidamente, se realiza una búsqueda de datos de LDAP utilizando las conexiones creadas para devolver cualesquiera Nombres de Dominio Totalmente Cualificados (FQDN) conocidos de Controladores de Dominio. A continuación se lleva a cabo una búsqueda de Servidor de Nombres de Dominio (DNS) inverso para cada Controlador de Dominio (DC) descubierto, con el fin de establecer una dirección IP para el DC. Cualquier DC del cual se encuentre que tiene una dirección IP dentro de los intervalos de direcciones de red descubiertos en la topología de red se puede insertar en la lista existente de nodos descubiertos, identificado cada uno de ellos como el DC. Finalmente, las conexiones de LDAP se cierran o se desenlazan.

Breve descripción de los dibujos

Para entender correctamente la invención, debe hacerse referencia a los dibujos adjuntos, en los que:

la figura 1 es un diagrama esquemático de alto nivel de un sistema de mapeo de DC de AD de acuerdo con formas de realización de la presente solicitud;

la figura 2 es un diagrama de flujo de un método de mapeo de red de acuerdo con formas de realización de la presente solicitud; y

la figura 3 es un diagrama de flujo de un método de mapeo de DC de AD de acuerdo con formas de realización de la presente solicitud.

Descripción detallada de las formas de realización preferidas

Haciendo referencia a la figura 1, formas de realización de la presente solicitud se refieren a una unidad de mapeo de DC de AD 100 configurada para conectarse a una red 10 que incluye múltiples nodos 1a, 1b. En particular, la red 10 incluye el DC de AD 1a y otros nodos 1b, según se describe de forma más detallada posteriormente.

En ciertas redes, los DC de AD 1a son servidores que responden a solicitudes de autenticación de seguridad (inicio de sesión, permisos de comprobación, etcétera) dentro del dominio del servidor. Típicamente, uno de los DC por cada dominio se configuraba como Controlador de Dominio Principal (PDC); la totalidad del resto de DC era Controladores de Dominio de Reserva (BDC). Un BDC podía autenticar los usuarios en un dominio, pero todas las actualizaciones para el dominio (usuarios nuevos, contraseñas cambiadas, membresía de grupo, etcétera) únicamente se podían realizar por medio del PDC, el cual a continuación propagaría estos cambios a todos los BDC del dominio. Si el PDC no estaba disponible (o no puede comunicarse con el usuario que solicitaba el cambio), la actualización fallaría. Si el PDC estaba permanentemente indisponible (por ejemplo, si la máquina fallaba), un BDC existente podría promoverse para ser PDC. Debido a la naturaleza crítica del PDC, las prácticas más adecuadas dictaminaban que el PDC debería dedicarse meramente a servicios de dominio, y no debería usarse para servicios de archivos/impresión/aplicación que podrían ralentizar o colgar el sistema.

En las redes más nuevas, el AD eliminó en gran medida el concepto de PDC y BDC en favor de la tecnología de replicación multi-maestro. No obstante, siguen habiendo varias funciones que solamente puede llevar a cabo un Controlador de Dominio, denominadas funciones de Operación de Maestro Único Flexible. Algunas de estas funciones deben ser cubiertas por un DC por cada dominio, mientras que otras únicamente requieren un DC por cada bosque de AD. Si el servidor que lleva a cabo una de estas funciones se pierde, el dominio puede seguir funcionando, y si el servidor no estuviera disponible nuevamente un administrador puede designar un DC alternativo que adopte la función, en un proceso conocido como toma (*seizing*) de la función.

Típicamente, el AD se gestiona usando una Consola de Gestión Gráfica. El AD es una implementación de servicios de directorio del Protocolo Ligero de Acceso a Directorios (LDAP), lo cual se escribirá posteriormente. Una finalidad principal del AD es proporcionar servicios centralizados de autenticación y autorización. El AD permite también que los administradores asignen políticas, implanten software, y apliquen actualizaciones críticas para una organización.

El AD almacena información y configuraciones en una base de datos central. Las redes de AD pueden variar desde una pequeña instalación con unos pocos cientos de objetos, hasta una gran instalación con millones de objetos.

El AD es un servicio de directorios utilizado para almacenar información sobre los recursos de red en un dominio. Una estructura de AD es un marco jerárquico de objetos. Los objetos se sitúan en tres categorías amplias: recursos (por ejemplo, impresoras), servicios (por ejemplo, correo electrónico), y usuarios (cuentas y grupos de usuarios). El AD proporciona información sobre los objetos, organiza los objetos, controla el acceso y establece la seguridad.

Cada objeto representa una entidad única ya sea un usuario, un ordenador, una impresora, o un grupo y sus atributos. Ciertos objetos también pueden ser contenedores de otros objetos. Un objeto queda identificado de manera exclusiva por su nombre y tiene un conjunto de atributos, las características e información que puede contener el objeto, definidas por un esquema, que determina también el tipo de objetos que se pueden almacenar en el AD.

Cada objeto de atributo se puede usar en varios objetos de clase de esquema diferentes. Estos objetos de esquema existen para permitir que el esquema se amplíe o modifique cuando sea necesario. No obstante, debido a que cada objeto de esquema es esencial para la definición de objetos de AD, la desactivación o cambio de estos objetos puede tener serias consecuencias ya que cambiará fundamentalmente la estructura del propio AD. Un objeto de esquema, cuando se modifique, se propagará automáticamente a través del AD, y una vez que se haya creado el objeto, típicamente dicho objeto únicamente se puede desactivar aunque no eliminar. De manera similar, el cambio del esquema requiere habitualmente una cantidad importante de planificación.

La estructura que contiene los objetos se interpreta en varios niveles. En la parte superior de la estructura se encuentra el Bosque – la colección de cada objeto, sus atributos, y reglas (sintaxis de atributos) en el AD. El bosque contiene uno o más Árboles con vínculos de confianza, transitivos. Un árbol contiene uno o más Dominios y árboles de dominio, nuevamente vinculados en una jerarquía de confianza transitiva. Los dominios se identifican por su estructura de nombres de DNS, el espacio de nombres.

Los objetos contenidos dentro de un dominio se pueden agrupar en contenedores denominados Unidades Organizacionales (OU). Las OU proporcionan una jerarquía a un dominio, facilitan su administración, y pueden proporcionar un aspecto de la estructura de una organización en términos organizacionales o geográficos. Una OU puede contener OU más pequeñas y puede contener múltiples OU anidadas. Típicamente, se recomienda tener el menor número posible de dominios en el AD y basarse en las OU para producir una estructura y mejorar la implementación de políticas y la administración. La OU es el nivel común en el cual se aplican políticas de grupo, que son objetos de AD, denominados Objetos de Directiva de Grupo (GPOs), aunque también pueden aplicarse políticas en dominio o sitios. La OU es el nivel en el cual comúnmente se delegan poderes administrativos, aunque también se puede llevar a cabo una delegación granular sobre objetos o atributos individuales.

El AD también soporta la creación de sitios, los cuales son agrupamientos físicos, en lugar de lógicos, definidos por una o más subredes de IP. Los sitios diferencias entre ubicaciones conectadas por conexiones de baja velocidad (por ejemplo, redes de área extensa (WAN), redes privadas virtuales (VPN)) y de alta velocidad (por ejemplo, redes de área local (LAN)). Los sitios son independientes del dominio y de la estructura de OU y son comunes en el bosque completo. Los sitios se usan para controlar tráfico de red generado por replicación y también para remitir clientes a los Controladores de Dominio más Próximos. El Exchange 2007 también utiliza la topología de sitios para el encaminamiento de correo. En el dominio de los sitios también se pueden aplicar políticas.

La división real de la infraestructura de información de la empresa en una jerarquía de uno o más dominios y OU de nivel superior es normalmente una decisión clave. Los modelos comunes son por unidad de negocio, por ubicación geográfica, por tipo de servicio, o por tipo de objeto. Normalmente, estos modelos también se utilizan combinados. Las OU se deberían estructurar principalmente para facilitar la delegación administrativa, y en segundo lugar, para facilitar la aplicación de políticas de grupo. Aunque las OU pueden formar un límite administrativo, el único límite de seguridad verdadero es el propio bosque y debe confiarse en un administrador de cualquier dominio del bosque en todos los dominios del mismo.

Físicamente, la información de AD está contenida en uno o más DC pares iguales. Típicamente, cada uno de los DC tiene una copia del AD, y los cambios en un ordenador están sincronizados, o convergen, entre la totalidad de los ordenadores de DC por la replicación multi-maestro. Los servidores que se integran, que no son DC, se denominan Servidores Miembros.

La base de datos de AD se divide típicamente en almacenes o particiones diferentes. La partición de “Esquema” contiene la definición de clases y atributos de objetos dentro del Bosque. La partición de “Configuración” contiene información sobre la estructura física y la configuración del bosque (tal como la topología de sitios). La partición “Dominio” contiene todos los objetos creados en ese dominio. Las dos primeras particiones se replican para todos los DC del Bosque. La partición de Dominio se replica únicamente para el DC dentro de su dominio. Los subconjuntos de objetos en la partición de dominio se replican también para los DC que están configurados como catálogos globales.

En general el AD está totalmente integrado con el DNS y el TCP/IP. La replicación del AD es una tecnología *pull* más que *push*, en la cual se distribuyen datos por solicitud. El Comprobador de Coherencia de la Información (KCC) crea una topología de replicación de vínculos a sitios utilizando los sitios definidos para gestionar tráfico. La replicación intra-sitio es frecuente y automática como consecuencia de la notificación de cambios, lo cual desencadena que las entidades pares den inicio a un ciclo de replicación *pull*. Los intervalos de replicación entre sitios son menos frecuentes y no utilizan notificación de cambios por defecto, aunque esto es configurable y se puede hacer que sea idéntico a la replicación intra-sitio. Se puede asignar un coste computacional diferente a cada vínculo y la topología de vínculos a sitios será modificada en consecuencia por el KCC. La replicación entre DC se puede producir de manera transitiva a través de varios vínculos a sitios en puentes de vínculos a sitios del mismo protocolo, si el "coste" es bajo, aunque el KCC valora automáticamente un vínculo directo de sitio-a-sitio menos que las conexiones transitivas. La replicación de sitio-a-sitio se puede configurar para que se produzca entre un servidor de cabeza de puente en cada sitio, el cual a continuación replica los cambios para otro DC dentro del sitio.

En un bosque de múltiples dominios, llegan a crearse particiones en la base de datos de AD. Es decir, cada dominio mantiene una lista de solamente aquellos objetos que pertenecen a ese dominio. Por ejemplo, un usuario creado en el Dominio A se enumeraría únicamente en el DC del Dominio A. Los servidores de catálogos globales (GC) se usan para proporcionar un listado global de todos los objetos del Bosque. El Catálogo Global se mantiene en DC configurados como servidores de catálogos globales. Los servidores de Catálogos Globales replican en ellos mismos todos los objetos de todos los dominios y por tanto proporcionan un listado global de objetos en el bosque. No obstante, para reducir al mínimo el tráfico de replicación y para mantener la base de datos del GC a un tamaño pequeño, se replican únicamente atributos seleccionados de cada objeto. A esto se le denomina conjunto de atributos parcial (PAS). El PAS se puede modificar modificando el esquema y marcando atributos para su replicación en el GC.

La replicación del Directorio Activo utiliza llamadas a procedimientos remotos. Por ejemplo, entre sitios, un usuario puede escoger utilizar el SMTP para la replicación, aunque únicamente para cambios en el Esquema o el Configuración. El SMTP no se puede usar para replicar la partición de Dominio. En otras palabras, si existe un dominio en los dos lados de una conexión WAN, para la replicación se usan RPC.

El Directorio Activo es un componente necesario para muchos servicios en una organización tal como un intercambio de correos electrónicos. Las funciones de Operaciones de Maestro Único Flexible (FSMO) son también conocidas como funciones de maestro de operaciones. Aunque los DC de AD funcionan en un modelo multi-maestro, es decir, pueden producirse actualizaciones en múltiples lugares a la vez, existen varias funciones que son necesariamente de instancia única:

Típicamente, el AD soporta nombres UNC (\), URL (/), LDAP URL para el acceso a objetos. El AD usa internamente la versión LDAP de la estructura de nombres X.500. Cada objeto tiene un nombre común (CN) y un Nombre distintivo (DN). El DC es la clase de objeto de dominio y puede tener muchas más que cuatro partes. El objeto también puede tener un Nombre canónico, esencialmente el DN a la inversa, sin identificadores, y utilizando barras. Para identificar el objeto dentro de su contenedor, se utiliza el Nombre Distintivo Relativo (RDN): cada objeto tiene también un Identificador Único Global (GUID), una cadena exclusiva e invariable de 128 bits que es usada por el AD para la búsqueda y la replicación. Ciertos objetos también tienen un Nombre Principal de Usuario (UPN), un formato de nombre nombreobjeto@dominio.

Para permitir que los usuarios de un dominio accedan a recursos de otro, el AD utiliza confianzas. Las confianzas dentro de un bosque se crean automáticamente cuando se crean dominios. El bosque fija los límites de confianza por defecto, no el dominio, y la confianza transitiva, implícita, es automática para todos los dominios dentro de un bosque. Además de la confianza transitiva bidireccional, las confianzas de AD pueden ser directas (unen dos dominios en árboles diferentes, transitivas, unidireccionales o bidireccionales), de bosque (transitivas, unidireccionales o bidireccionales), de dominio kerveros (transitivas o no transitivas, unidireccionales o bidireccionales), o externas (no transitivas, unidireccionales o bidireccionales) para conectarse a otros bosques o dominios que no sean de AD. Con la confianza unidireccional, un dominio permite el acceso a usuarios en otro dominio, pero el otro dominio no permite el acceso a usuarios en el primer dominio. Con la confianza bidireccional, dos dominios permiten el acceso a usuarios en el otro dominio. En este contexto, un dominio que confía es el dominio que permite acceso a usuarios de un dominio en el que se confía, un dominio en el que se confía es el dominio en el que se ha puesto confianza, cuyos usuarios tienen acceso al dominio que confía.

La distribución de software es ejecutada por un servicio aparte que utiliza atributos de esquemas privativos adicionales que funcionan en combinación con el protocolo LDAP. El Directorio Activo no automatiza la distribución de software, sino que proporciona un mecanismo en el cual otros servicios pueden aportar distribución de software.

La unidad de mapeo de DC de AD 100 incluye un módulo de mapeo 110. En particular, el módulo de mapeo 110 está configurado para mapear los nodos 1a, 1b en la red 10 y opcionalmente también para mapear las conexiones 2 que conectan los nodos 1a, 1b. Se conocen varias técnicas de mapeo de topografías de red y las mismas se pueden integrar en las formas de realización de la presente solicitud, según se describe de forma más detallada

posteriormente.

El módulo de mapeo 110 descubre automáticamente todo lo que se encuentre en la red, incluyendo ordenadores de sobremesa, servidores, impresoras, concentradores, conmutadores y encaminadores con el uso de métodos de identificación y descubrimiento (ping/ICMP, SNMP, VoIP basado en SIP, NetBIOS y más) para explorar intervalos de direcciones IP y encontrar nodos, según se describe posteriormente en la figura 2.

Haciendo referencia a continuación a la figura 2, se proporciona un método de mapeo 200 de acuerdo con formas de realización de la presente solicitud. En particular, el método de mapeo 200 incluye la etapa de definir criterios de datos de mapeo en la etapa 210. Por ejemplo, un usuario puede definir un intervalo de direcciones IP, el número de saltos (o dispositivos conectados desde cada dispositivo descubierto), y tipos de dispositivos (por ejemplo, dispositivos SNMP o clientes respondedores) a descubrir durante la búsqueda.

Continuando con la figura 2, en la etapa 220, se lleva a cabo una búsqueda de nodos. Por ejemplo, los tipos de métodos de descubrimiento tales como el Ping ICMP, NetBIOS, clientes SIP, etcétera, conllevan la transmisión de pequeños paquetes de UDP o ICMP a cada dirección IP del intervalo definido, así como el descubrimiento de dispositivos que se encuentran dentro del número de saltos desde los dispositivos descubiertos. Así, se envían y se realiza un seguimiento de datos para cada dirección IP definida con el fin de determinar el dispositivo asociado a una dirección IP y los trayectos físicos y virtuales utilizados para alcanzar la dirección IP respectiva. Opcionalmente, los intervalos grandes de direcciones IP se subdividen en bloques de 10 direcciones, buscándose respuestas de entre esas 10 direcciones. Buscando en la red de esta manera, se minimizan efectos notorios en el ancho de banda de la red o los dispositivos.

Continuando con la figura 2, se describe más detalladamente el descubrimiento de nodos en la etapa 220. Se buscan nodos en bloques de un número pre-seleccionado N de direcciones IP utilizando métodos de descubrimiento configurados por el usuario, etapa 221. A continuación, se puede determinar la conectividad de la capa 3 a partir de nodos descubiertos en la etapa 222. Si se definió un recuento de saltos > 0, se repite la etapa 221 con intervalos de red recién descubiertos hasta que se alcance el recuento de saltos, etapa 223. A continuación, se determina la conectividad de la capa 2 a partir de cualesquiera nodos descubiertos que se han identificado como conmutador o concentrador gestionado en la etapa 224. Seguidamente se correlacionan los datos de direcciones de la capa 2 y la capa 3 de las etapas 221 a 224, por ejemplo, mediante el uso de tablas de traducción de direcciones (ARP) y tablas de árboles de expansión recopiladas a partir de nodos descubiertos con capacidad SNMP en la etapa 225. A continuación, en la etapa 226 se determina la conectividad de la red examinando cada dirección(es) IP de nodos descubiertos. Se usa la conectividad de la capa 2 cuando la misma esté disponible; en caso contrario se usa la conectividad de la capa 3.

Los resultados de la búsqueda de topología de red se almacenan en la etapa 230. Por ejemplo, el módulo de mapeo 110 puede recopilar y almacenar toda la información de topología en una base de datos 140, proporcionando una fuente de información de topología y activos para estrategias de bases de datos de gestión de configuración (CMDB) empresariales. El módulo de mapeo 110 también mantiene automáticamente estos datos para actualizar los nodos de red, proporcionando así a los ingenieros de la red una representación constantemente precisa de la red en relación con los requisitos de visibilidad y cumplimiento.

Opcionalmente, en la etapa 230 se almacenan los resultados de búsqueda de topología de la red. Por ejemplo, una vez que se han descubierto nodos de la red, el módulo de mapeo 110 puede compilar la información en un mapa de topología de red cohesionado, sencillo de ver, por ejemplo con iconos de nodos y líneas coloreadas que representan la velocidad de conectividad de la red en una interfaz de usuario 130. De esta manera, el módulo de mapeo 110 permite que los ingenieros de la red vean exactamente cómo están conectados los dispositivos en la misma. El módulo de mapeo 110 puede acceder a conmutadores y concentradores gestionados, con el fin de realizar diagramas precisos de la conectividad de los puertos para todos los dispositivos de la red, dando como resultado un mapa completo que ilustra todos los nodos conectados directamente a un conmutador o concentrador gestionado, con la información de los puertos visualizada de manera adyacente al nodo.

Haciendo referencia de nuevo a la figura 1, en una implementación de la presente solicitud, el módulo de mapeo 110 lleva a cabo un mapeo de la capa 2. La capa 2, o capa de enlace de datos, proporciona los medios funcionales y procedimentales para transferir datos entre entidades de red y para detectar y posiblemente corregir errores que se pueden producir en la capa física. Originalmente, esta capa estaba destinada a medios de punto-a-punto y punto-a-multipunto, característicos de medios de área extensa en el sistema telefónico. La arquitectura de las redes de área local (LAN), que incluían medios multi-acceso con capacidad de difusión general, se desarrolló con independencia del trabajo ISO, en el Proyecto 802 del IEEE. Los servicios LAN disponen típicamente bits, de la capa física, en secuencias lógicas que se denominan tramas. Subcapa de Control de Enlace Lógico

La subcapa situada más arriba es el Control de Enlace Lógico (LLC). Esta subcapa multiplexa protocolos que se ejecutan encima de la capa de enlace de datos, y proporciona opcionalmente control de flujos, acuse de recibo, y recuperación de errores. El LLC proporciona direccionamiento y control del enlace de datos. Especifica qué mecanismos se van a usar para direccionar estaciones sobre el medio de transmisión y para controlar los datos

intercambiados entre el originador y máquinas destinatarias.

La subcapa por debajo del LLC es el Control de Acceso a Medios (MAC). En ocasiones, esta se refiere a la subcapa que determina a quién se le permite acceder a los medios en un momento cualquiera (habitualmente CSMA/CD), y en otras ocasiones esta expresión se refiere a una estructura de tramas con direcciones MAC en su interior. En general existen dos formas de control de acceso a los medios: distribuida y centralizada. La subcapa de Control de Acceso a los Medios determina también dónde finaliza una trama de datos y comienza la siguiente.

Continuando con la figura 1, en una implementación de la presente solicitud, el módulo de mapeo 110 lleva a cabo el mapeo de la capa 3. La capa 3, o capa de red, es la tercera capa de entre siete en el modelo OSI y la tercera capa de entre cinco en el modelo TCP/IP. Esencialmente, la capa de red es responsable de la entrega de paquetes de extremo a extremo (de origen a destino), mientras que la capa de enlace de datos es responsable de la entrega de tramas de nodo a nodo (de salto a salto). La capa de red proporciona los medios funcionales y procedimentales de transferencia de secuencias de datos de longitud variable desde un origen a un destino por medio de una o más redes, al mismo tiempo que manteniendo la calidad de servicio, y funciones de control de errores. La capa de red trata la transmisión de información en todo su trayecto desde el origen al destino.

Llevando a cabo el descubrimiento multi-nivel, el módulo de mapeo 110 se aprovecha de múltiples métodos de descubrimiento para proporcionar un mapa de topología integrada de capa 3 y capa 2 OSI que incluye

- Dirección IP
- Dirección MAC
- Último usuario que ha iniciado sesión (requiere los Clientes Respondedores opcionales)
- Nombre de DNS
- Nombre de nodo (determinado por el SNMP u otro protocolo de cliente)
- Conexión de puertos de conmutación

Este descubrimiento multi-nivel de datos de infraestructura de la red proporciona a los ingenieros de la misma un acceso sencillo a características significativas con ahorro de tiempo, incluyendo una representación automatizada de topología en niveles, para mostrar encaminadores y subredes, conmutadores y concentradores gestionados adicionalmente, o de manera adicional nodos extremos que se pueden filtrar por tipo o grupo para mejorar aún más la precisión de las distribuciones.

Continuando con la figura 1, la unidad de mapeo de DC de AD 100 incluye además una unidad de descubrimiento de DC de AD 120. En particular, una vez que el módulo de mapeo 110 ha formado el mapa de topología, la unidad de descubrimiento de DC de AD 120 puede usar estos datos de mapeo para determinar las ubicaciones del DC de AC 1a dentro de la red 10 del módulo.

La unidad de descubrimiento de DC de AD 120 usa órdenes 121 del Protocolo Ligero de Acceso a Directorios (LDAP) para formar consultas y análisis de datos devueltos con el fin de identificar el DC de AD, y a continuación integra los dispositivos que ejecutan el LDAP en el mapa topológico.

El LDAP es un protocolo de aplicación para consultar y modificar servicios de directorio que se ejecuta sobre TCP/IP. Un directorio es un conjunto de objetos con atributos similares organizados de una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, el cual está compuesto por una serie de nombres (ya sea de personas o bien de organizaciones) organizados alfabéticamente, presentando cada nombre una dirección y un número de teléfono adjuntos. Debido a este diseño básico (entre otros factores), el LDAP es usado normalmente por otros servicios para la autenticación, a pesar de los problemas de seguridad que provoca esto.

Un árbol de directorio de LDAP refleja normalmente diversos límites políticos, geográficos y/o organizacionales, en función del modelo seleccionado. En la actualidad, las implantaciones del LDAP tienden a usar nombres del Sistema de Nombres de Dominio (DNS) para estructurar los niveles de la jerarquía situados más arriba. Más en el interior del directorio podrían aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier otra cosa que represente una entrada de árbol dada (o múltiples entradas).

En una serie de Solicitudes de Comentarios (RFCs) de la Vía Convencional (*Standard Track*) del Grupo de Trabajo de Ingeniería de Internet (IETF), según se detalla en la RFC 4510, se especifica una versión actual del LDAPv3.

Un cliente inicia una sesión de LDAP conectándose a un servidor de LDAP, por defecto en el puerto TCP 389. A continuación, el cliente envía solicitudes de operación al servidor, y el servidor a su vez envía respuestas. Con

algunas excepciones, no es necesario que el cliente espere por una respuesta antes de enviar la siguiente solicitud, y el servidor puede enviar las respuestas en cualquier orden. El cliente puede solicitar varias operaciones diversas.

El LDAP se define en términos de ASN.1, y los mensajes de protocolo se codifican en el formato binario BER, y usa representaciones textuales para una serie de campos/tipos de ASN.1.

- El protocolo accede a directorios de LDAP:
- Un directorio es un árbol de entradas de directorio.
- Una entrada está compuesta por un conjunto de atributos.
- Un atributo tiene un nombre (un tipo de atributo o descripción de atributo) y uno o más valores. Los atributos se definen en un esquema (véase más adelante).
- Cada entrada tiene un identificador exclusivo: su Nombre Distintivo (DN). Este está compuesto por su Nombre Distintivo Relativo (RDN) construido a partir de cierto(s) atributo(s) de la entrada, seguido por el DN de la entrada padre, siendo el DN un nombre de archivo completo y el RDN es un nombre de archivo relativo en una carpeta.

Un DN puede cambiar durante el tiempo de vida de la entrada, por ejemplo, cuando se mueven entradas dentro de un árbol. Para identificar de manera fiable e inequívoca entradas, se podría proporcionar un UUID en el conjunto de los atributos operacionales de la entrada.

Un servidor contiene un subárbol que comienza a partir de una entrada específica, por ejemplo, “dc=example,dc=com” y sus hijos. Los servidores también pueden contener referencias a otros servidores, con lo que un intento de acceso “ou=department,dc=example,dc=com” podría devolver una referencia o continuación de referencia a un servidor que contiene esa parte del árbol de directorio. A continuación, el cliente puede contactar con el otro servidor. Algunos servidores soportan también el encadenamiento, lo cual significa que el servidor contacta con el otro servidor y devuelve los resultados al cliente.

El LDAP rara vez define alguna ordenación: el servidor puede devolver los valores en un atributo, los atributos en una entrada, y las entradas encontradas por una operación de búsqueda en cualquier orden. Esta característica se deduce de las definiciones formales, y una entrada se define como un conjunto de atributos, y un atributo es un conjunto de valores, y no es necesario que los conjuntos estén ordenados.

En una operación de LDAP, el cliente asigna a cada solicitud un ID de Mensaje positivo, y la respuesta del servidor tiene el mismo ID de Mensaje. La respuesta incluye un código de resultado numérico que indica éxito, alguna condición de error o algunos otros casos especiales. Antes de la respuesta, el servidor puede enviar otros mensajes con otros datos de resultado. Por ejemplo, cada entrada encontrada por la operación de Búsqueda se devuelve en un mensaje del tipo mencionado.

La operación de Búsqueda de LDAP se puede usar tanto para buscar como para leer entradas. El servidor devuelve las entradas coincidentes y tal vez continuaciones de referencia (en cualquier orden), seguidas por el resultado final con el código de resultado. La operación de Comparación toma un DN, un nombre de atributo y un valor de atributo, y comprueba si la entrada nombrada contiene ese atributo con ese valor.

El contenido de las entradas en un subárbol está gobernado por un esquema. El esquema define los tipos de atributo que las entradas de directorio pueden contener. Una definición de atributo incluye una sintaxis, y la mayoría de valores no binarios en el LDAPv3 usan una sintaxis de cadenas UTF-8. El esquema define clases de objeto. Cada entrada debe tener un atributo objectClass (clase de objeto), que contiene clases nombradas definidas en el esquema. La definición del esquema de las clases de una entrada define qué tipo de objeto puede representar la entrada – por ejemplo, una persona, organización o dominio. Las definiciones de clases de objeto enumeran también qué atributos son obligatorios y cuáles son opcionales. Por ejemplo, una entrada que representa una persona podría pertenecer a las clases “top” y “person”. La membresía en la clase “person” requeriría que la entrada contuviese los atributos “sn” y “cn”, y permitiría que la entrada también contuviera “userPassword”, “telephoneNumber”, y otros atributos. Puesto que las entradas pueden pertenecer a múltiples clases, cada entrada tiene un complejo de conjuntos de atributos opcionales y obligatorios formados a partir de la unión de las clases de objeto que representa. Las ObjectClasses se pueden heredar, y una única entrada puede tener múltiples objectClasses para definir los atributos disponibles y requeridos de la propia entrada. Un aspecto paralelo al esquema de una objectClass es una definición de clase y una instancia en la programación orientada a objetos, que representan respectivamente una objectClass de LDAP y una entrada de LDAP.

El esquema incluye también otra diversa información que controla entradas de directorio. La mayoría de elementos del esquema tiene un nombre y un Identificador de Objeto (OID) único global. Los servidores de directorios pueden publicar el esquema de directorio que controla una entrada en un DN de base dado por el atributo operacional de

subesquema/subentrada de la entrada (un atributo operacional describe la operación del directorio más que la información de usuario y se devuelve únicamente a partir de una búsqueda cuando la misma se solicita explícitamente). Los administradores de servidores pueden definir sus propios esquemas además de los convencionales. A un esquema para representar personas individuales dentro de organizaciones se le denomina esquema de páginas blancas.

Haciendo referencia nuevamente a la figura 1, en una de las configuraciones, un usuario inicia sesión en la unidad de descubrimiento de DC de AD con acceso del administrador, y a continuación el módulo de descubrimiento de DC de AD 120 accede a la base de datos de nodos 130 y dirige las funciones de LDAP sintéticas a los nodos identificados 1a, 1b en la red 10 para determinar el DC de AD 1a en la red.

Una vez que esta información de la ubicación del DC de AD 1a es localizada por el módulo de descubrimiento de DC de AD 120, la base de datos de nodos 130 se puede actualizar para reflejar esta información sobre las ubicaciones del DC de AD 1a, y la pantalla 140 puede visualizar especialmente el DC de AD 1a, por ejemplo designando el DC de AD 1a con un símbolo, color o gráfico especial.

Haciendo referencia a continuación a la figura 3, formas de realización de la presente solicitud se refieren a un método y descubrimiento de DC de AD 300, que incluye las etapas de determinar la topología de la red en la etapa 310, tal como los nodos y conexiones de la red. Por ejemplo, según se ha descrito anteriormente, en la etapa 310, se pueden transferir datos sintéticos dentro de la red y se pueden rastrear los mismos para determinar la presencia y las relaciones de los diversos componentes de la red. Alternativamente, otras técnicas de mapeo se basan en el mapeo de un conjunto conocido de nodos para determinar la relación de los nodos.

A continuación, se crean (enlazan) conexiones de LDAP en la etapa 320 para (a) el punto extremo (o un “servidor”) de LDAP del usuario actual. Alternativamente, si el usuario ha especificado una o más credenciales de dominio, se crea un enlace con el punto extremo de LDAP asociado a esas credenciales. Se pueden crear conexiones de LDAP utilizando técnicas y órdenes convencionales.

A continuación, se usan órdenes de LPAD para localizar el DC de AD en la etapa 330. Por ejemplo, se puede llevar a cabo una búsqueda de datos de LDAP utilizando las conexiones creadas para devolver cualquier Nombre de Dominio Totalmente Cualificado (FQDN) conocido de DC en las etapas 331 y 332. En particular, en la etapa 331, se lleva a cabo una búsqueda del FQDN de DC en la unidad de organización. De manera similar, en la etapa 332, se lleva a cabo una búsqueda del FQDN de DC en la configuración específica citada. De esta manera, se puede materializar un DC de AD localizado fuera del punto extremo de LDAP identificado en la etapa 320 utilizando los datos de mapeo de la etapa 310. En la búsqueda del FQDN en las etapas 331 y 332, se puede usar la orden *ldapsearch API (ldap_search_s())*, y a continuación se pueden efectuar iteraciones de cualquier (cualesquiera) respuesta(s) para su re-evaluación. Esta(s) respuesta(s) contienen el FQDN de uno o más DC.

A continuación, en la etapa 333, se lleva a cabo una búsqueda de Servidor de Nombres de Dominio (DNS) inverso para cada Controlador de Dominio (DC) descubierto en las etapas 331 y 332 con el fin de establecer una dirección IP para el DC. En la etapa 334, cualquier DC del cual se encuentra que tiene una dirección IP dentro de los intervalos de direcciones de red descubiertos en la etapa 310 se inserta en la lista existente de nodos descubiertos, identificado cada uno de ellos como DC. En la etapa 340, cada conexión de LDAP creada en la etapa 320 se cierra o desenlaza para devolver el nodo al estado original.

Tal como se ha descrito anteriormente, varias formas de realización de la invención se pueden configurar en numerosos elementos físicos, o se pueden configurar en un único elemento de red o pueden configurarse en una serie de elementos que tengan varias funciones de las dadas a conocer, distribuidas en todos ellos. El control del IP SLA u otras configuraciones de monitorización y otras funciones se puede llevar a cabo en diversos componentes de red, tales como en el equipo de usuario, en el servidor de VOIP, en una pasarela de acceso o en otro componente de red asociado a la red VOIP y pueden acceder a la red.

Un experto ordinario en la materia entenderá que las formas de realización de la invención antes descritas tienen se proporcionan a título ilustrativo, y que la invención se puede materializar en numerosas configuraciones según se ha descrito anteriormente. De manera adicional, la invención se puede implementar en forma de un programa de ordenador en un soporte legible por ordenador, controlando el programa de ordenador un ordenador o un procesador para llevar a cabo las diversas funciones que se describen como etapas de método y también descritas como elementos de hardware o hardware/software.

REIVINDICACIONES

1. Método para descubrir un controlador de dominio, DC, de directorio activo, AD, que comprende:

mapear una topología de una red;

crear una conexión de protocolo ligero de acceso a directorios, LDAP, por enlace a un punto extremo de LDAP;

usar órdenes de LDAP para llevar a cabo una búsqueda de LDAP del DC de AD utilizando la conexión de LDAP creada, y devolver por lo menos un nombre de dominio totalmente cualificado, FQDN, de un DC de AD descubierto; y

desenlazarse del punto extremo de LDAP,

en el que el mapeo de la topología de la red comprende buscar nodos en un número predefinido de direcciones del protocolo de internet, ip, y repetir la búsqueda para un número predefinido de saltos.

2. Método según la reivindicación 1, en el que el mapeo de una topología de una red comprende:

transferir datos sintéticos dentro de la red; y

rastrear los datos sintéticos.

3. Método según la reivindicación 1, en el que el mapeo de la topología de la red además comprende:

determinar la conectividad de la capa 2 y de la capa 3 a partir de cualesquiera nodos descubiertos;

correlacionar los datos de dirección de la capa 2 y de la capa 3; y

determinar la conectividad de red de direcciones ip descubiertas.

4. Método según la reivindicación 1, en el que el mapeo de la topología de la red comprende recibir y almacenar preferencias de usuario que comprenden el tamaño del bloque de direcciones ip y el número de saltos.

5. Método según la reivindicación 1, en el que el enlace del punto extremo de LDAP comprende crear una conexión de LDAP con un punto extremo de LDAP actual.

6. Método según la reivindicación 1, en el que el enlace del punto extremo de LDAP comprende crear un enlace de LDAP con un nodo asociado a credenciales de dominio especificadas por el usuario.

7. Método según la reivindicación 1, en el que el uso de las órdenes de LDAP para llevar a cabo una búsqueda del DC de AD comprende:

llevar a cabo una búsqueda del servidor de nombres de dominio, DNS, inverso para cada DC de AD descubierto con el fin de establecer una dirección ip para el DC de AD;

insertar, en una lista, un DC de AD descubierto que tiene una dirección ip dentro de unos intervalos de direcciones de red descubiertos en el mapeo.

8. Método según la reivindicación 1, en el que la devolución de por lo menos un FQDN comprende:

buscar el FQDN de controladores de dominio en una unidad de organización; y

buscar el FQDN de controladores de dominio en una configuración específica citada.

9. Aparato para descubrir un controlador de dominio, DC, de directorio activo, AD, comprendiendo el aparato:

un servidor configurado para

mapear una topología de una red;

crear un protocolo ligero de acceso a directorios, LDAP, por enlace a un punto extremo de LDAP;

usar órdenes de LDAP para llevar a cabo una búsqueda de LDAP del DC de AD utilizando la conexión de LDAP creada, y devolver por lo menos un nombre de dominio totalmente cualificado, FQDN, de un DC de AD descubierto; y

desenlazarse del punto extremo de LDAP,

en el que, cuando se mapea la topología de la red, el servidor está configurado además para buscar nodos en un número predefinido de direcciones ip y repetir la búsqueda para un número predefinido de saltos.

10. Aparato según la reivindicación 9, en el que, cuando se mapea la topología de la red, el servidor está configurado para

transferir datos sintéticos dentro de la red, y

rastrear los datos sintéticos.

11. Aparato según la reivindicación 9, en el que, cuando se mapea la topología de la red, el servidor está configurado además para:

determinar la conectividad de la capa 2 y de la capa 3 a partir de cualesquiera nodos descubiertos;

correlacionar los datos de dirección de la capa 2 y de la capa 3; y

determinar la conectividad de red de direcciones IP descubiertas.

12. Aparato según la reivindicación 9, en el que, cuando se mapea la topología de la red, el servidor está además configurado para:

recibir y almacenar preferencias de usuario que comprenden el tamaño del bloque de direcciones ip y el número de saltos.

13. Aparato según la reivindicación 9, en el que, cuando se enlaza el punto extremo de LDAP, el servidor está configurado además

para crear una conexión de LDAP con un punto extremo de LDAP actual.

14. Aparato según la reivindicación 9, en el que, cuando se enlaza el punto extremo de LDAP, el servidor está configurado además para crear un enlace de LDAP con un nodo asociado a credenciales de dominio especificadas por el usuario.

15. Aparato según la reivindicación 9, en el que, cuando se usan las órdenes de LDAP para llevar a cabo una búsqueda del DC de AD, el servidor está configurado además para:

llevar a cabo una búsqueda del servidor de nombres de dominio, DNS, inverso para cada DC de AD descubierto, con el fin de establecer una dirección ip para el DC de AD;

insertar, en una lista, un DC de AD descubierto que tiene una dirección ip dentro de unos intervalos de direcciones de red descubiertos en el mapeo.

16. Aparato según la reivindicación 15, en el que, cuando se devuelve por lo menos un FQDN, el servidor está configurado además para:

buscar el FQDN de controladores de dominio en una unidad de organización; y

buscar el FQDN de controladores de dominio en una configuración específica citada.

17. Programa de ordenador para descubrir un controlador de dominio, DC, de directorio activo, AD, materializado en un soporte legible por ordenador, no transitorio, estando el programa de ordenador configurado para controlar un procesador, con el fin de llevar a cabo operaciones, que comprenden:

mapear una topología de una red;

crear una conexión de protocolo ligero de acceso a directorios, LDAP, por enlace a un punto extremo de LDAP;

usar órdenes de LDAP para llevar a cabo una búsqueda de datos de LDAP del DC de AD utilizando la conexión de LDAP creada, y devolver por lo menos un nombre de dominio totalmente cualificado, FQDN, de un DC de AD descubierto; y

desenlazarse del punto extremo de LDAP,

en el que el mapeo de la topología de la red comprende buscar nodos en un número predefinido de direcciones ip y repetir la búsqueda para un número predefinido de saltos.

18. Programa de ordenador según la reivindicación 17, en el que el mapeo de una topología de una red comprende: transferir datos sintéticos dentro de la red; y rastrear los datos sintéticos.

19. Programa de ordenador según la reivindicación 17, en el que el mapeo de la topología de la red además comprende:

determinar la conectividad de la capa 2 y de la capa 3 a partir de cualesquiera nodos descubiertos;

correlacionar los datos de dirección de la capa 2 y de la capa 3; y

determinar la conectividad de la red de direcciones ip descubiertas.

20. Programa de ordenador según la reivindicación 17, en el que el mapeo de la topología de la red comprende recibir y almacenar preferencias de usuario que comprenden el tamaño del bloque de direcciones ip y el número de saltos.

21. Programa de ordenador según la reivindicación 17, en el que el enlace del punto extremo de LDAP comprende crear una conexión de LDAP con un punto extremo de LDAP actual.

22. Programa de ordenador según la reivindicación 17, en el que el enlace del punto extremo de LDAP comprende crear un enlace de LDAP con un nodo asociado a credenciales de dominio especificadas por el usuario.

23. Programa de ordenador según la reivindicación 17, en el que el uso de las órdenes de LDAP para buscar el DC de AD comprende:

llevar a cabo una búsqueda del servidor de nombres de dominio, DNS, inverso para cada DC de AD descubierto, con el fin de establecer una dirección ip para el DC de AD;

insertar, en una lista, un DC de AD descubierto que tiene una dirección ip dentro de unos intervalos de direcciones de una red descubiertos en el mapeo.

24. Programa de ordenador según la reivindicación 23, en el que la devolución de por lo menos un FQDN comprende:

buscar el FQDN de controladores de dominio en una unidad de organización; y

buscar el FQDN de controladores de dominio en una configuración específica citada.

Figura 1

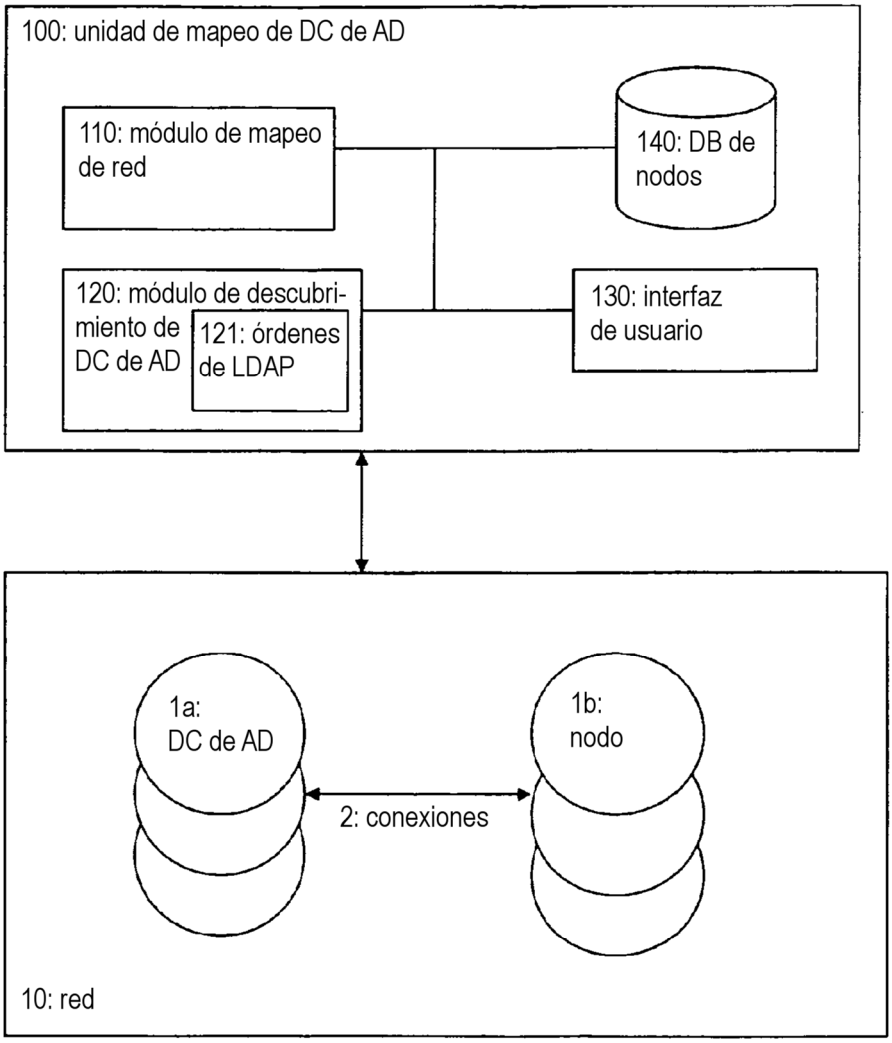

100: unidad de mapeo de DC de AD
110: módulo de mapeo de red
140: DB de nodos
120: módulo de descubrimiento de DC de AD
121: órdenes de LDAP
130: interfaz de usuario
1a: DC de AD
1b: nodo
2: conexiones
10: red

Figura 2

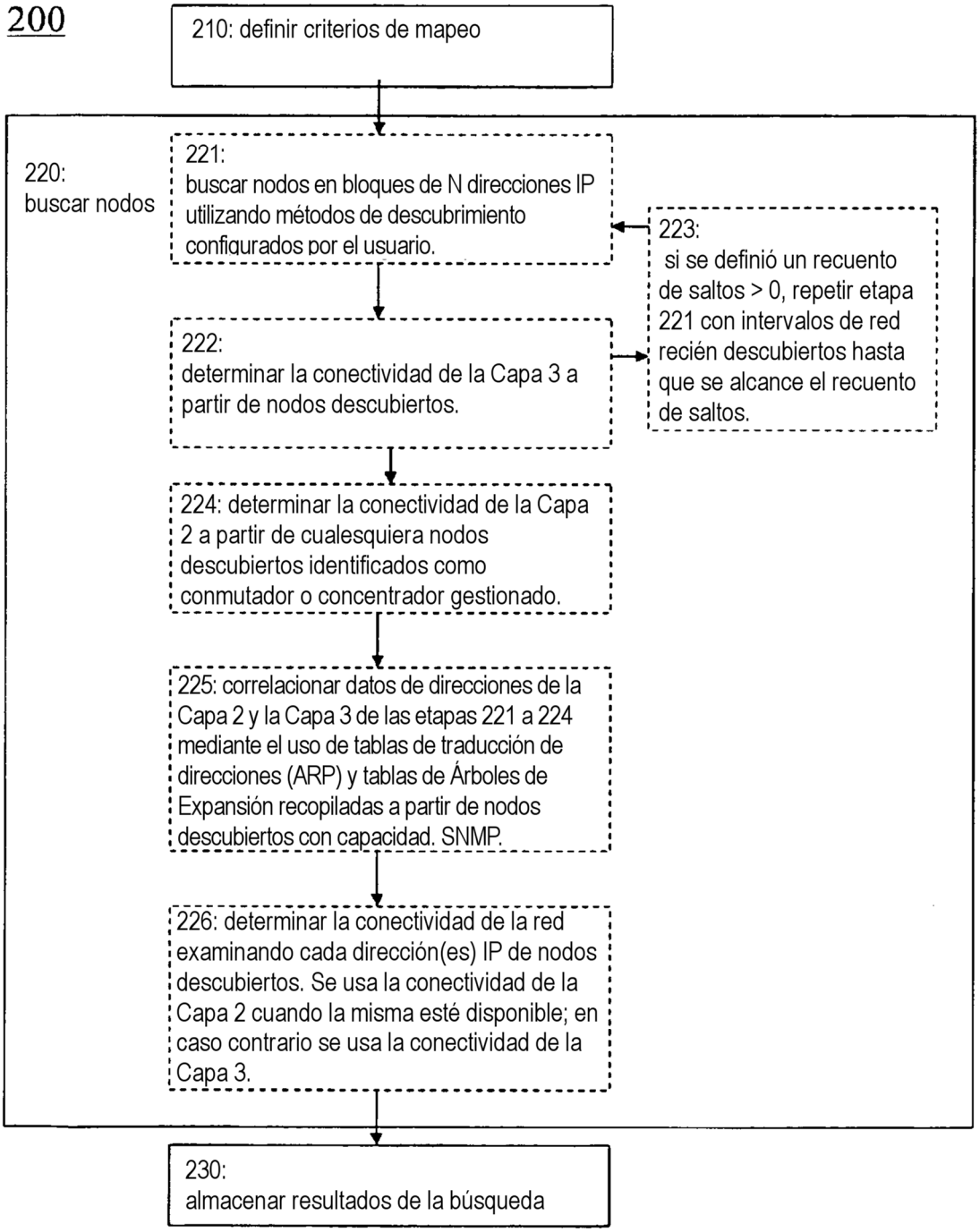
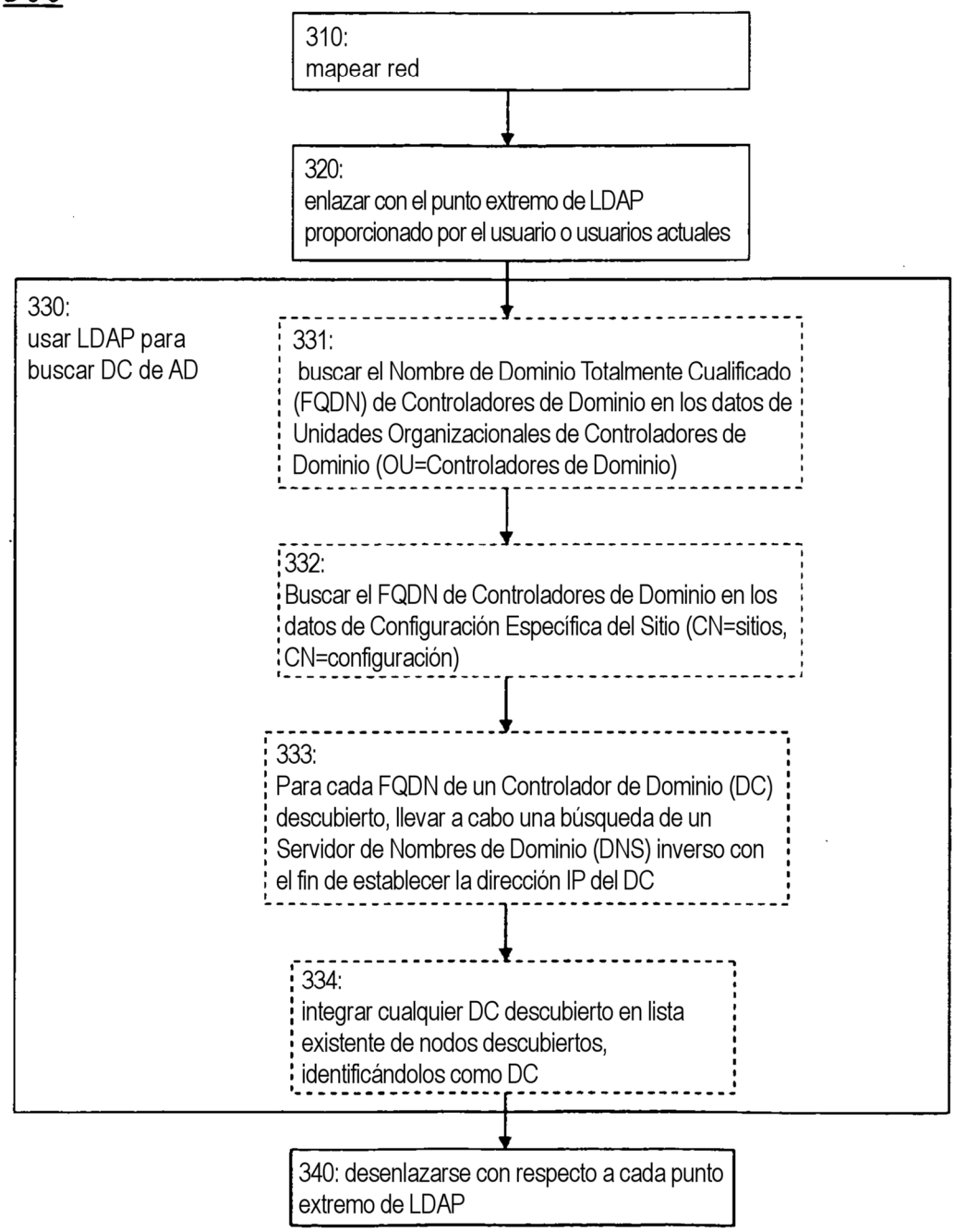

200
210: definir criterios de mapeo
220: buscar nodos
221: buscar nodos en bloques de N direcciones IP utilizando métodos de descubrimiento configurados por el usuario.
223: si se definió un recuento de saltos > 0, repetir etapa 221 con intervalos de red recién descubiertos hasta que se alcance el recuento de saltos.
222: determinar la conectividad de la Capa 3 a partir de nodos descubiertos.
224: determinar la conectividad de la Capa 2 a partir de cualesquiera nodos descubiertos identificados como conmutador o concentrador gestionado.
225: correlacionar datos de direcciones de la Capa 2 y la Capa 3 de las etapas 221 a 224 mediante el uso de tablas de traducción de direcciones (ARP) y tablas de Árboles de Expansión recopiladas a partir de nodos descubiertos con capacidad. SNMP.
226: determinar la conectividad de la red examinando cada dirección(es) IP de nodos descubiertos. Se usa la conectividad de la Capa 2 cuando la misma esté disponible; en caso contrario se usa la conectividad de la Capa 3.
230: almacenar resultados de la búsqueda

Figura 3


300
310:
mapear red
320:
enlazar con el punto extremo de LDAP proporcionado por el usuario o usuarios actuales
330:
usar LDAP para buscar DC de AD
331:
buscar el Nombre de Dominio Totalmente Cualificado (FQDN) de Controladores de Dominio en los datos de Unidades Organizacionales de Controladores de Dominio (OU=Controladores de Dominio)
332:
Buscar el FQDN de Controladores de Dominio en los datos de Configuración Específica del Sitio (CN=sitios, CN=configuración)
333:
Para cada FQDN de un Controlador de Dominio (DC) descubierto, llevar a cabo una búsqueda de un Servidor de Nombres de Dominio (DNS) inverso con el fin de establecer la dirección IP del DC
334:
integrar cualquier DC descubierto en lista existente de nodos descubiertos, identificándolos como DC
340: desenlazarse con respecto a cada punto extremo de LDAP