Protocolo ligero de acceso a directorios (LDAP)

El Protocolo ligero de acceso a directorios (en inglés, Lightweight Directory Access Protocol, LDAP) es un conjunto de protocolos abiertos usados para acceder información guardada centralmente a través de la red. Está basado en el estándar X.500 para compartir directorios, pero es menos complejo e intensivo en el uso de recursos. Por esta razón, a veces se habla de LDAP como "X.500 Lite." El estándar X.500 es un directorio que contiene información de forma jerárquica y categorizada, que puede incluir nombres, directorios y números telefónicos.

X.500 es un conjunto de estándares de redes de ordenadores de la ITU-T sobre servicios de directorio, entendidos estos como bases de datos de direcciones electrónicas (o de otros tipos). El estándar se desarrolló conjuntamente con la ISO como parte del Modelo de interconexión de sistemas abiertos, para usarlo como soporte del correo electrónico X.400.

Como X.500, LDAP organiza la información en un modo jerárquico usando directorios. Estos directorios pueden almacenar una gran variedad de información, permitiendo que cualquiera pueda acceder a su cuenta desde cualquier máquina en la red acreditada con LDAP.

Sin embargo, en la mayoría de los casos, LDAP se usa simplemente como un directorio telefónico virtual, permitiendo a los usuarios acceder fácilmente la información de contacto de otros usuarios. Pero LDAP va mucho más lejos que un directorio telefónico tradicional, ya que es capaz de propagar su consulta a otros servidores LDAP por todo el mundo, proporcionando un repositorio de información ad-hoc global. Sin embargo, en este momento LDAP se usa más dentro de organizaciones individuales, como universidades, departamentos del gobierno y compañías privadas.

LDAP es un sistema cliente/servidor. El servidor puede usar una variedad de bases de datos para guardar un directorio, cada uno optimizado para operaciones de lectura rápidas y en gran volúmen. Cuando una aplicación cliente LDAP se conecta a un servidor LDAP puede, o bien consultar un directorio, o intentar modificarlo. En el evento de una consulta, el servidor, puede contestarla localmente o puede dirigir la consulta a un servidor LDAP que tenga la respuesta. Si la aplicación cliente está intentando modificar información en un directorio LDAP, el servidor verifica que el usuario tiene permiso para efectuar el cambio y después añade o actualiza la información.

Razones por las cuales usar LDAP

La mayor ventaja de LDAP es que se puede consolidar información para toda una organización dentro de un repositorio central. Por ejemplo, en vez de administrar listas de usuarios para cada grupo dentro de una organización, puede usar LDAP como directorio central, accesible desde cualquier parte de la red. Puesto que LDAP soporta la Capa de conexión segura (SSL) y la Seguridad de la capa de transporte (TLS), los datos confidenciales se pueden proteger de los curiosos.

LDAP también soporta un número de bases de datos back-end en las que se guardan directorios. Esto permite que los administradores tengan la flexibilidad para desplegar la base de datos más indicada para el tipo de información que el servidor tiene que diseminar. También, ya que LDAP tiene una interfaz de programación de aplicaciones (API) bien definida, el número de aplicaciones acreditadas para LDAP son numerosas y están aumentando en cantidad y calidad.

Características de OpenLDAP

OpenLDAP incluye un número de características importantes.

- Soporte LDAPv3 — OpenLDAP soporta la Capa de autenticación y seguridad (SASL), la Seguridad de la capa de transporte (TLS) y la Capa de conexión segura (SSL), entre otras mejoras. Muchos de los cambios en el protocolo desde LDAPv2 han sido diseñados para hacer LDAP más seguro.

- Soporte IPv6 — OpenLDAP soporta la próxima generación del protocolo de Internet versión 6.

- LDAP sobre IPC — OpenLDAP se puede comunicar dentro de un sistema usando comunicación interproceso (IPC). Esto mejora la seguridad al eliminar la necesidad de comunicarse a través de la red.

- API de C actualizada — Mejora la forma en que los programadores se conectan para usar servidores de directorio LDAP.

- Soporte LDIFv1 — Provee compatibilidad completa con el formato de intercambio de datos, Data Interchange Format (LDIF) versión 1.

- Servidor Stand-Alone mejorado — Incluye un sistema de control de acceso actualizado, conjunto de hilos, herramientas mejoradas y mucho más.

Terminología LDAP

Cualquier discusión sobre LDAP requiere un entendimiento básico del conjunto de términos específicos de LDAP:

- **Entrada** : Una entrada es una unidad en un directorio LDAP. Cada entrada se identifica por su único Nombre distinguido (Distinguished Name (DN)).

- **Atributos** : Los atributos son piezas de información directamente asociada con la entrada. Por ejemplo, una organización puede ser representada como una entrada LDAP. Los atributos asociados con la organización pueden ser su número de fax, su dirección, etc. En un directorio LDAP las entradas pueden ser también personas, con atributos comunes como el número de teléfono y la dirección de e-mail.

Algunos atributos son obligatorios mientras que otros son opcionales. Una definición objectclass determina qué atributos se requieren y cuáles no para cada entrada. Las definiciones de objectclass se encuentran en varios archivos de esquema, dentro del directorio /etc/openldap/schema/.

LDIF — El Formato de intercambio de datos de LDAP (LDIF) es una representación de texto ASCII de entradas LDAP. Los archivos usados para importar datos a los servidores LDAP deben estar en formato LDIF. Una entrada LDIF se ve similar al ejemplo siguiente:

[<id>]
dn: <distinguished name>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>

Una entrada puede contener tantos pares <attrtype>: <attrvalue> como sean necesarios. Una línea en blanco indica el final de una entrada.

Todas las parejas <attrtype> y <attrvalue> deben estar definidas en el archivo esquema correspondiente para usar esta información.

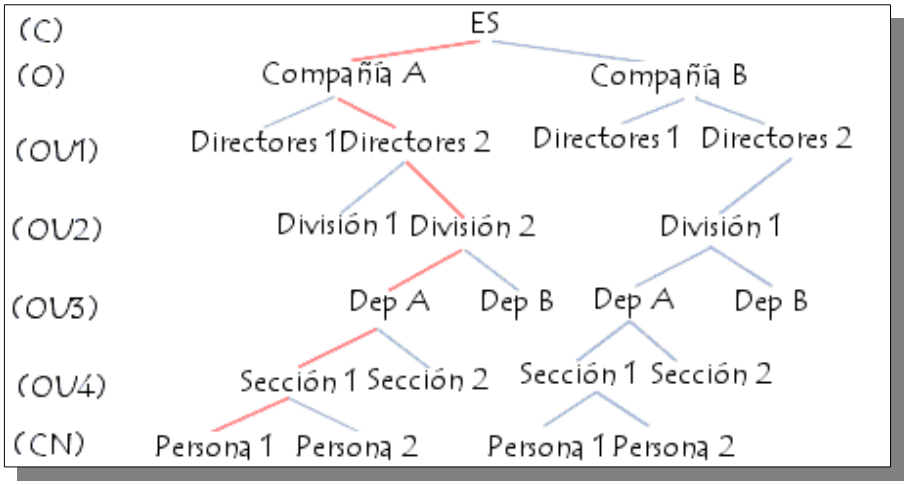
Cualquier valor comprendido dentro de < y > es una variable y puede ser configurado cuando se cree una nueva entrada LDAP. Sin embargo, esta regla no se aplica a <id>. El <id> es un número determinado por la aplicación que se usa para modificar la entrada.

Estructura de árbol de la información (DIT)

LDAP presenta la información bajo la forma de una estructura jerárquica de árbol denominada DIT (Árbol de información de directorio), en la cual la información, denominada entradas (o incluso DSE, Directory Service Entry), es representada por bifurcaciones.
Una bifurcación ubicada en la raíz de una bifurcación se denomina entrada raíz.

Cada entrada en el directorio LDAP corresponde a un objeto abstracto o real (por ejemplo, una persona, un objeto material, parámetros, etc.).

Cada entrada está conformada por un conjunto de pares clave/valor denominados atributos.



Atributos de entrada

Cada entrada está compuesta por un conjunto de atributos (pares clave/valor) que permite caracterizar el objeto que la entrada define. Existen dos tipos de atributos:

- Atributos normales: éstos son los atributos comunes (apellido, nombre, etc.) que distinguen al objeto.
- Atributos operativos: éstos son atributos a los que sólo el servidor puede acceder para manipular los datos del directorio (fechas de modificación, etc.).

Una entrada se indexa mediante un nombre completo (DN) que permite identificar de manera única un elemento de la estructura de árbol.

Un DN se constituye tomando el nombre del elemento denominado Nombre distintivo relativo (RDN, es decir, la ruta de la entrada en relación con sus entradas superiores) y agregándole el nombre entero de la entrada principal.
Se trata de utilizar una serie de pares clave/valor para poder localizar una entrada de manera única. A continuación encontrará una serie de claves generalmente utilizadas:

uid (id de usuario)	ésta es una identificación única obligatoria
cn (nombre común)	éste es el nombre de la persona
givenname	éste es el nombre de pila de la persona
sn (apellido)	éste es el apellido de la persona
o (organización)	ésta es la compañía de la persona
u (unidad organizacional)	éste es el departamento de la compañía para la que trabaja la persona
mail	ésta es la dirección de correo electrónico de la persona (por supuesto)
c	Esta es el Pais ó Region de la persona

Por lo tanto, un nombre completo tendrá la siguiente forma:

uid=jeapil,cn=pillou,givenname=jean-francois

Le Relative Distinguished Name étant ici "uid=jeapil".

Así, el conjunto de definiciones de objetos y atributos que un servidor LDAP puede administrar se denomina esquema. Esto permite, por ejemplo, definir si un atributo puede poseer uno o varios valores. Además, un atributo llamado objectclass permite definir si los atributos son obligatorios u opcionales.

Protocolo de Aplicación X.400

Correo electrónico X.400

Esta modalidad de envío apunta a personalizar la comunicación, sin importar donde se encuentre el

usuario y dirigiendo los mensajes no a un aparato de fax que no cuenta con la debida confidencialidad, sino a su casilla electrónica personal, además permite la posibilidad de adjuntar archivos (attachments) dentro del correo. A través de éste protocolo se pueden enviar y recibir mensajes en forma local, nacional o internacional. Cada casilla es identificada con un nombre que actúa como receptor de mensajes de correo electrónico y/o telex sin intermediarios. Esta identificación es única y permite intercambiar mensajes con la mayoría de los correos electrónicos reconocidos internacionalmente. Los mensajes son almacenados en la casilla hasta que el usuario acceda a ella para leerlos. Una vez que el usuario leyó su correo, estos se transfieren a un archivo de respaldo donde se retienen por un plazo de 6 días ante la eventual necesidad de una nueva consulta, luego de lo cual se eliminan definitivamente. Esto lo protege contra perdidas imprevistas de mensajes.

Permite enviar y recibir formatos de archivos ASCII o Binarios, esto facilita las operaciones cuando hay necesidad de enviar o recibir información del tipo de planillas electrónicas o bases de datos para ser integradas a un programa de gestión. La confidencialidad y seguridad que brindan este medio de comunicación, es solo comparable con los servicios de mensajería bancaria, ya que los mensajes van encriptados y dirigidos directamente a la casilla personal del destinatario. Esto hace que toda persona que quiera acceder a la información recibida tenga que conocer las claves de la casilla y la del desencriptador.

En cuanto al uso de los servicios, ya sea envío o recepción de mensajes de e-mail, fax o telex, estos actúan automáticamente sin necesidad de la intervención manual. El sistema cuenta con un administrador de mensajes (entrantes y salientes) en forma local, esto brinda un ahorro importante en costo de archivado, impresión y en tiempos para búsquedas de dichos mensajes.

En lo que refiere al funcionamiento sobre una red local (LAN) este servicio puede ser implementado sobre el propio correo interno. Luego degenerar el mensaje (Email, Fax o Telex) los mismos se depositan en la cola de salida de la conexión para su posterior envío a través de un router. Dependiendo de la necesidad, se pueden generar diferentes parámetros para la activación del router la que pude ser: inmediata, programada o periódica.

Al producirse la comunicación, automáticamente se envían todos los mensajes (Fax, Telex, correo electrónico X.400 y/o Internet) encolados por los usuarios, en una sola conexión. Realizada la conexión para el envío, también solicitará una recepción en forma automática de los mensajes pendientes en la casilla de usuario, estos mensajes podrán incluir los provenientes de otras redes X.400 y de Internet Mail, además de los acuses de recibo y avisos de cancelación motivados por los mensajes enviados por los usuarios.

Principales característica del servicio

- Estándar Internacional (CITT X.400, X.500)
- Multiplataforma (desde PC a Mainframe)
- Envío multidestino
- Acceso por múltiples medios de comunicación
- Interconexión con correos privados de empresas
- Acceso a otros servicios

El sistema X.400 ofrece una serie de importantes beneficios para sus usuarios, entre los que se

destacan:

- Intercambio de Mensajes y Archivos
- Puede intercambiar entre distintos usuarios hojas de cálculo, textos, imágenes, etc., e integrarlos directamente en aplicaciones internas con su propio formato y características.
- Envios Multidestino
- Enviando una sola vez el mensaje, X.400 lo remite a todos los destinos solicitados.
- Acuse de Recibo
- Cuando el mensaje es recibido por el destinatario, se emite un acuse de recibo de dicho envío hacia el remitente.
- Seguridad en Identificación de Remitente y Destinatario
- Cada usuario cuenta con una identificación única a nivel mundial.
- Confidencialidad
- Los usuarios disponen de claves de acceso e identificación única y personal. Además el servicio permite conformar grupos cerrados de utilizadores.
- Fax-Telex
- El X.400 posibilita la comunicación con fax y con telex tanto en mensajes aislados como multi destino.

Sintaxis Protocolo X.400 y sus Atributos

Norma ISO y CCIT. Sintaxis basada en atributos, no en dominios. Donde las direcciones basadas en dominios tienen carácter posicional, las basadas en atributos son aposicionales.

Sintaxis de direcciones basadas en atributos:

G.I.S@OU.O.PRMD.ADMD.C

- G= Given Name. Nombre propio de la persona.
- I = Initial Name. No muy utilizado. Normalmente la inicial del segundo nombre, en el caso de los nombres compuestos.
- S = Surname. Apellido de la persona, también alias con que se le conoce.
- OU = Organization Unit. grupo específico de buzones o subdominios agrupados bajo una misma característica organizativa, funcional, geográfica, etc.
- O = Organization. Organismo al que hace referencia de forma inequívoca.
- PRMD = Private Management Domain. Dominio de gestión privado. Institución gestora de las tareas de registro de organizaciones que participan en el servicio. (Rediris)
- ADMD = Administration Management Domain. Dominio de gestión administrativo. Normalmente recae en una compañía telefónica del país.
- C = Country. País. Utiliza el mismo código ISO que RFC822.

Ventajas del servicio

- Bajo costo
- Ahorro de dinero, tiempo y papel
- Capacidad de tratar alto volumen de información
- Optimiza los recursos informáticos de la organización, sin necesidad de invertir en nuevo equipamiento.
- Crecimiento racional en función de las necesidades del usuario
- Cobertura internacional
- Disponibilidad inmediata las 24 horas los 365 días del año

Aplicaciones

Los campos de aplicación de este servicio es muy variados entre los que podemos mencionar se encuentran Sectores de actividad (Turismo, Finanzas, Transporte, Distribución. Educación, Fuerzas Armadas), Grupos de interés común (Cámaras, Asociaciones profesionales, Administración pública), Organizaciones empresariales (Grandes empresas, Pymes), Particulares,

SMTP vs X.400

Como solución a las variedades de mensajes de e-mail totalmente incompatibles, surgieron dos soluciones, dos estándares.

Aunque parezca contradictorio, el primer estándar es el de facto de la Internet que se publicó en 1982 bajo la forma de la RFC 821 y se denominó SMTP (simple mail transfer protocol), el protocolo simple de transferencia de mail, como su nombre lo indica la intención de la gente que creó este estándar era mantener cierta simplicidad.

Un par de años más tarde, y quizá demasiado tarde, llegó el estándar oficial de la CCITT para el manejo de mensajes en Internet y se llamó X.400, este estándar nunca llegó a imponerse en la Internet debido a su complejidad, lo poco flexible de sus direcciones y a que llegó demasiado tarde, el hecho es que el estándar de Internet para la transferencia de correo es el SMTP que se usa aún hoy ampliamente en toda la red, con algunas excepciones, que debido a su formato de transferencia no soporta los caracteres extendidos que son imprescindibles en idiomas como el francés y el alemán, en particular los gobiernos de Francia y Canadá impulsaron el X.400 como estándar ya que se adaptaban mucho mejor a sus necesidades, debido a esto se necesitó la creación de pasarelas (gateway) de conversión de un sistema al otro.

Protocolo de Aplicación X.500

¿Qué es el Directorio X.500?

A medida que las redes crecían, las bases de datos locales eran insuficientes y se pensó en almacenar

toda la información que estaba hasta esos momentos dispersa en una única base de datos de ámbito universal. Esta gran base de datos estaría distribuida, es decir, repartida en pequeñas bases de datos por todo el mundo de forma que pudiesen comunicar unas con otras y dieran al usuario la sensación de estar trabajando con una sola base de datos global.

Desde 1986 hay un fuerte interés por el uso de OSI en Europa para conseguir facilitar las comunicaciones entre los computadores de diferentes fabricantes y tecnologías.

COSINE (Co-operation for Open System Interconnection Networking in Europe) forma parte del proyecto EUREKA y fue fundada por 18 países de Europa y la Comisión Europea, con objeto de crear una infraestructura OSI común que diera soporte a la comunidad investigadora europea.

Durante los primeros años del proyecto COSINE se dieron unas especificaciones para un conjunto de proyectos y servicios que garantizasen el funcionamiento correcto de los mismos. Una de esas especificaciones iba encaminada al desarrollo de un servicio piloto internacional de directorio en Europa con acceso a Norteamérica y al resto del mundo. Este proyecto se llamó PARADISE.

Para este desarrollo se pensó en la UCL (University College London), pioneros en el tema de directorios distribuidos y que habían participado en el desarrollo del software X.500, QUIPU, bajo el proyecto INCA. Junto a la ULCC (University of London Computer Center) comenzaron el trabajo. En octubre de 1990 se presentó en las Jornadas Técnicas de IRIS un piloto de directorio para la red nacional. Durante 1991 se instalaron máquinas para formar una infraestructura básica del servicio consistente en servidores X.500, acceso público al directorio y servidores de archivo con software y documentación

El directorio es una base de datos destinada a mantener determinada información sobre objetos del mundo real. Es una base de datos distribuida ya que la información que contiene se encuentra repartida en lugares diferentes, pero el usuario se relaciona con el directorio como si la información estuviese centralizada, por lo tanto la búsqueda de la información se realiza de una forma transparente a él.

El Servicio de Directorio X.500 permite tener almacenados datos públicos de las Unidades organizativas y las personas que las componen, para poder realizar búsquedas de las mismas. La información contenida en el directorio se conoce como la Base de Información del Directorio, DIB (Directory Information Base).El directorio X.500 se compone de:

Agentes de Sistema de Directorio, DSAs (Directory System Agent), que mantienen la información distribuida del directorio. Éstos constan de:

Una base de datos propia que mantiene una parte de la información global del directorio (por eso es distribuida).

Unos procedimientos de comunicaciones que permiten el diálogo entre los DSAs así como entre ellos y los usuarios por medio de los Agentes de Usuario de Directorio, DUAs (Directory User Agent).

La relación entre estos componentes se muestra en la siguiente figura:

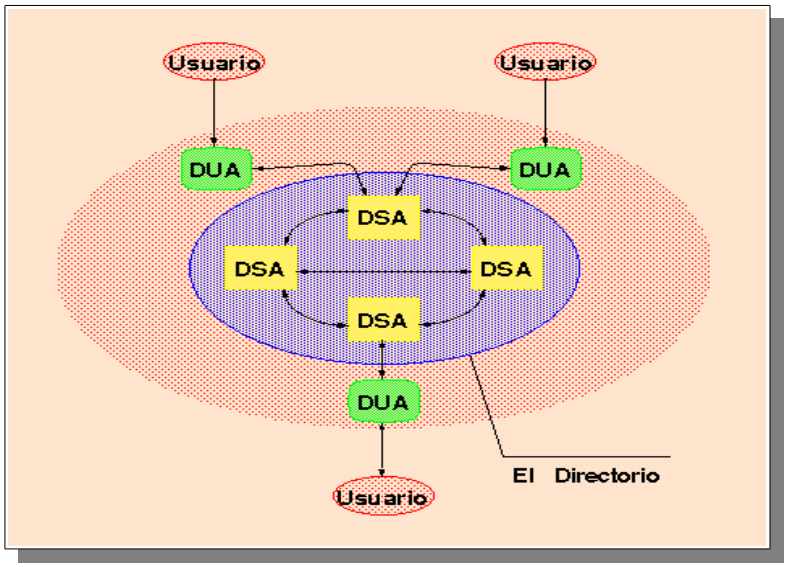


Figura - 1. Relación entre los componentes del directorio

La información que se mantiene en el directorio está compuesta por objetos, entendiendo por éstos, entes muy diversos como cosas, animales, personas, grupos, organizaciones, países, aplicaciones OSI, etc...

Estructura de un objeto del directorio

Cada objeto tiene un nombre que es único de forma que permite localizarlo dentro del directorio. Este nombre, llamado Nombre Distintivo, DN (Distingued Name), está formado por campos denominados atributos como: país (c), organización (o), unidad de organización (ou), nombre del objeto (cn) y muchas más propiedades del objeto.

El DN, se encuentra formado por una secuencia unida a Nombres Distintivos Relativos, RDN (Relative Distingued Name). La secuencia se forma, con el DN del padre y el atributo nombre del objeto, que actúa como Nombre Distintivo Relativo.

DN: "@c=CL@o=Departamento Ing. Infomatica Uscah@cn= Juan Pérez"

RDN 1: c = CL

RDN 2: o = Departamento Ing. Infomatica Uscah

RDN 3: cn = Juan Pérez

Estructura. (DIT)

La información contenida en el directorio se estructura de una forma jerárquica en niveles, partiendo de un punto ficticio llamado raíz que se sitúa en el nivel superior de la información y del que parten todos los demás.

Algunos de los niveles utilizados en el servicio son:

Figura - 2. Niveles en el árbol de directorio De estos niveles pueden colgar todo tipo de objetos (personas, organismos internacionales, etc...).

En cada uno de los niveles hay una persona encargada del mantenimiento de éste. Esta estructuración forma lo que se llama el Arbol de Información del Directorio, DIT (Directory Information Tree), que pretende posibilitar una búsqueda de cada objeto, de la forma más rápida, segura y sencilla posible.

El usuario podrá acceder al directorio mediante los Agentes de Usuario de Directorio (DUA's) que como se mencionó anteriormente, son los intermediarios entre el directorio y el usuario.

Estos agentes, los DUA's, pueden permitir al usuario hacer varias operaciones sobre el directorio como:

Añadir una entrada.

Modificar la entrada del propio usuario.

Borrar la entrada del usuario.

Lectura de atributos que describen un objeto, ya sean del usuario o de cualquier otro objeto.

Listado de objetos que pertenecen a un país, organización, unidad de organización, etc...

Búsqueda de objetos que cumplan unas determinadas condiciones.

Aplicaciones suministradas por el directorio

La aplicaciones suministradas se pueden dividir en dos clases dependiendo del tipo de usuarios que hagan uso del directorio.

a) Aplicaciones interpersonales

En este tipo de aplicaciones se realiza un diálogo entre usuario y directorio mediante un DUA. Existen dos tipos:

b) Aplicaciones de Páginas Blancas

Se accede a la información detallando el DN del objeto a buscar y seleccionando un conjunto de atributos que son los que el directorio mostrará.

Obtener la lista:

nombre y dirección, de todos los funcionarios de la Usach

Obtener la lista:

usuarios del Departamento de Informática de la Universidad de Santiago de Chile.

Esto despliega listado de los atributos mencionados como: teléfono, direcciones de mensajería, etc...

c) Aplicaciones de Páginas Amarillas

Se pueden obtener datos de forma selectiva, sólo de los registros cuyos atributos coincidan con los valores de los atributos buscados, como cuando buscamos en las páginas amarillas de la guía telefónica a los médicos, abogados, etc...

Obtener los datos de las personas que se llamen Javier, vivan en

Chile y beban Coca Cola.

Obtener las personas que trabajen en el Diinf y no beban nada.

Estas aplicaciones de comunicación interpersonal son el objetivo inicial del servicio.

Aplicaciones entre sistemas

En este caso, los usuarios que acceden al directorio son aplicaciones OSI. El directorio permite que los usuarios accedan a las aplicaciones de una forma más amigable. Para ello el usuario especifica el servicio que desea ejecutar y el directorio llama a la aplicación que realiza ese servicio en la máquina correspondiente.

Por otra parte, también facilita a los técnicos de la red su gestión y administración, ya que cualquier cambio en alguna de las direcciones en el directorio, será visible automáticamente por todas las aplicaciones que la utilicen.

FTAM, transferencia, acceso y gestión de archivos distribuidos. En este caso, el usuario especifica la aplicación FTAM a la que se quiere conectar. El directorio busca en la base de datos la información e inicia la aplicación relacionada con ese servicio en la máquina adecuada (en esa misma máquina pueden existir otras aplicaciones iguales con otras configuraciones).

Glosario

ad hoc :
Es aquella red (especialmente inalámbrica) en la que no hay un nodo central, sino que todos los dispositivos están en igualdad de condiciones. Ad hoc es el modo más sencillo para el armado de una red.