

Ldap vs x.500 DIRECTORIES

Introduction to Lightweight Directory Access Protocol (LDAP)

Article ID: 196455 - [View products that this article applies to.](#)

System TipThis article applies to a different version of Windows than the one you are using. Content in this article may not be relevant to you. [Visit the Windows 8 Solution Center](#)

This article was previously published under Q196455

[Expand all](#) | [Collapse all](#)

SUMMARY

To understand Lightweight Directory Access Protocol (LDAP) better, let's discuss X.500 and Directory Access Protocol (DAP).

In X.500, the Directory System Agent (DSA) is the database in which directory information is stored. This database is hierarchical in form, designed to provide fast and efficient search and retrieval.

The Directory User Agent (DUA) provides functionality that can be implemented in all sorts of user interfaces through dedicated DUA clients, Web server gateways, or e-mail applications.

The Directory Access Protocol (DAP) is a protocol used in X.500 Directory Services for controlling communications between the DUA and DSA agents. The agents represent the user or program and the directory, respectively.

The X.500 Directory Services are application-layer processes. Directory services can be used to provide global, unified naming service for all elements in a network, translate between network names and addresses, provide descriptions of objects in a directory, and provide unique names for all objects in the Directory. These X.500 objects are hierarchical with different levels for each category of information, such as country, state, and city, organization.

These objects may be files (as in a file system directory listing), network entities (as in a network naming services such as Novell's NDS), or other types of entities.

A lightweight protocol is any of a class of protocols designed for use on high-speed internetworks. High-Speed Transport Protocol (HSTP), Xpress Transfer Protocol (XTP), and Lightweight Directory Access Protocol (LDAP) are examples.

Lightweight protocols combine routing and transport services in a more streamlined fashion than do

traditional network and transport layer protocols. This makes it possible to transmit more efficiently over high-speed networks, such as ATM or FDDI, and media, such as fiber-optic cable.

Lightweight protocols use various measures and refinements to streamline and speed up transmissions, such as using connection-oriented transmissions, such as (TCP/IP) and a fixed header and trailer size to save the overhead of transmitting a destination address with each packet.

Lightweight Directory Access Protocol (LDAP) is a subset of the X.500 protocol. LDAP clients are, therefore, smaller, faster, and easier to implement than are X.500 clients. LDAP is vendor-independent and works with, but does not require, X.500.

Contrary to X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. LDAP is an open protocol, and applications are independent of the of server platform hosting the directory.

The Active Directory is not an X.500 directory. Instead, it uses LDAP as the access protocol and supports the X.500 information model without requiring systems to host the entire X.500 overhead. The result is the high level of interoperability required for administering real-world, heterogeneous networks.

The Active Directory supports access via the LDAP protocol from any LDAP-enabled client. LDAP names are less intuitive than Internet names, but the complexity of LDAP naming is usually hidden within an application. LDAP names use the X.500 naming convention called "Attributed Naming."

An LDAP URL names the server holding Active Directory services and the Attributed Name of the object. For example:

```
LDAP://SomeServer.Myco.Com/CN=jamesmith,CN=Sys,CN=Product,CN=Division,DC=myco,DC=domain-controller
```

LDAP C API (RFC 1823) is an informational RFC that is the de facto standard in C programming for LDAP applications.

By combining the best of the DNS and X.500 naming standards, LDAP, other key protocols and a rich set of APIs, the Active Directory allows a single point of administration for all resources, including: files, peripheral devices, host connections, databases, Web access, users, arbitrary other objects, services, and network resources.