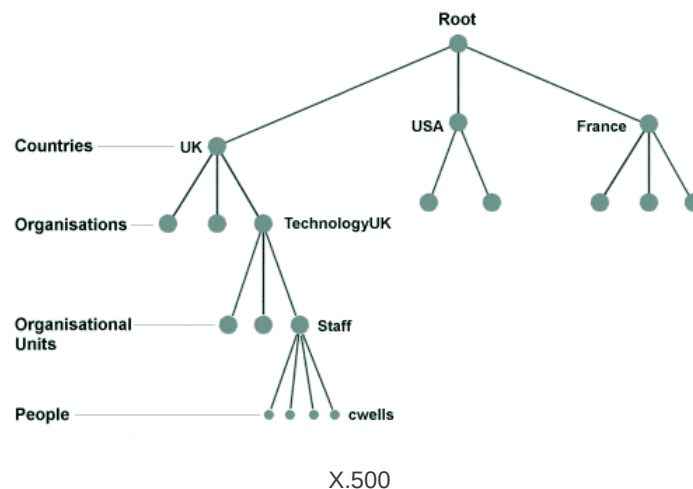


X.500

Definition of X.500 in Network Encyclopedia.

What is X.500?

X.500 is a recommendation from the [International Telecommunication Union \(ITU\)](#) that specifies a global, hierarchical directory service.



Features of X.500 include the following:

- A standards-based directory service for those applications that require directory information
- A single, global, hierarchical namespace of objects and their attributes
- Data management functions for viewing, adding, modifying, and deleting directory objects
- Search capabilities for customizing complete data queries

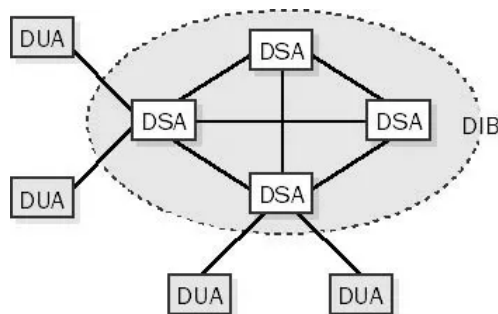
How X.500 Works

X.500 defines a [global directory service](#) that consists of several components. From an administrative point of view, the building blocks of the X.500 directory service are Directory Management Domains (DMDs). An X.500 DMD is a collection of X.500 components that includes at least one Directory System Agent (DSA) and is managed by a Domain Management Organization (DMO). There are two types of DMDs:

- **Administrative Directory Management Domains (ADDMDs):** Directory services managed by a registered private agency that provide public directory services. Examples of ADDMDs are Four11 and Bigfoot, which provide public X.500 directory services over the Internet.
- **Private Directory Management Domains (PRDMDs):** Directory services that provide private directory access. An example is a domain controller hosting [Active Directory](#) on a network running Microsoft Windows Server.

Three main components are involved in maintaining and accessing X.500 directory services:

- **Directory Information Base (DIB):** The actual hierarchical database that contains all the information in the directory. X.500 uses a distributed directory hierarchy in which different subsets of the DIB are found on different servers at different locations. From the user's point of view, however, the entire global X.500 directory appears to be accessible from the local directory server that the Directory User Agent (DUA) connects to. A schema is used to define the various classes of objects and their attributes, which can be stored in the directory. The Directory Information Tree (DIT) is the naming hierarchy that describes the hierarchical structure of the DIB.
- **Directory System Agent (DSA):** A particular server that maintains a subset of the DIB and provides an access point to the directory for DUAs to connect. Each DSA is responsible for a subset of the DIB and includes a set of naming contexts that define objects that are near each other in the DIT. DSAs also communicate with each other for [directory replication](#) purposes to ensure that each DSA's subset of the DIB is current and complete and to maintain the integrity of the whole X.500 directory system.
- **Directory User Agents (DUAs):** The client software that accesses the X.500 directory on behalf of the user. DUAs can perform such actions as searching, reading, updating, and deleting information in the directory, depending on the level of functionality of the client and the level of access granted to the user. The functionality of a DUA can be built into any type of software, including e-mail clients, Web browsers, or even the operating system itself.



The X.500 directory service

To access information in the directory, a DUA connects to a local DSA and queries the directory by using the Directory Access Protocol (DAP), the standard X.500 protocol for locating, accessing, and modifying information in an X.500 directory. Various attribute-based search methods are possible using X.500-based directory services, including the following:

- White pages searches, for name-to-address lookups
- Yellow pages searches, for looking up a category
- Browsing, for listings related to a given attribute

When a DUA issues a query, the query travels through a chain of DSAs and a result set travels back along the same chain. These queries use DAP, while DSAs communicate with each other using the Directory System Protocol (DSP).

NOTE

X.500 forms the basis of Active Directory in Windows Server, the directory service of Microsoft Exchange Server, and [Novell Directory Services \(NDS\)](#).

A simplified version of DAP called the [Lightweight Directory Access Protocol \(LDAP\)](#) is more widely implemented than the feature-heavy DAP. LDAP was developed by the University of Michigan for use on [TCP/IP networks](#) such as the Internet and is widely

implemented in [Simple Mail Transfer Protocol \(SMTP\)](#) client software such as Microsoft Outlook Express for querying online directories about SMTP users.