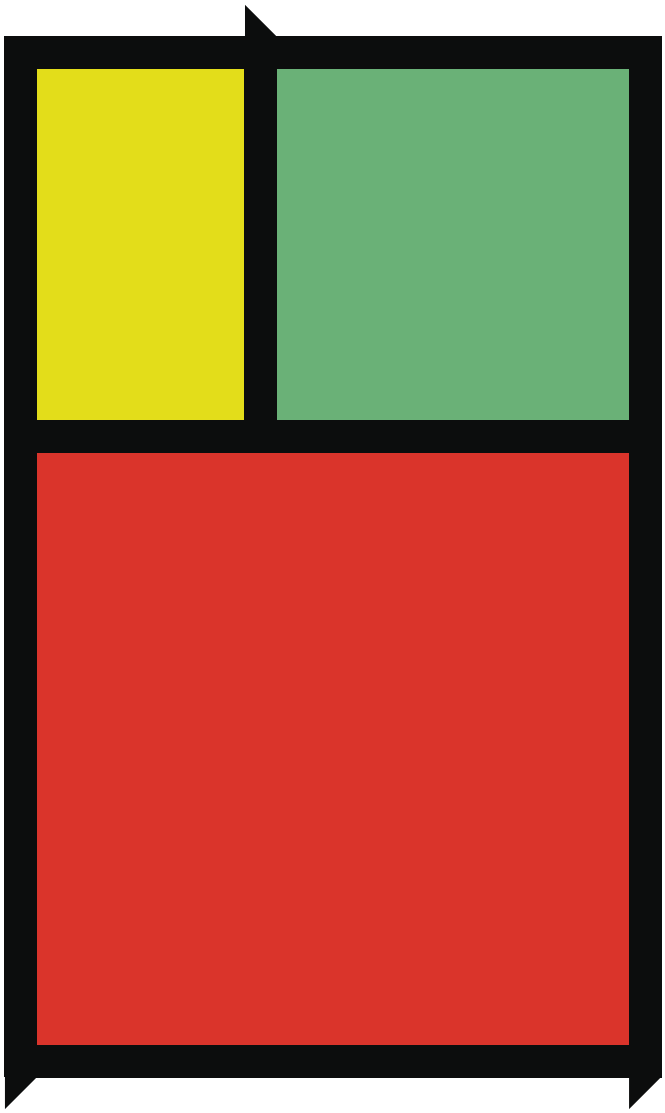


LDAPC

Lightweight Directory Access Protocol Client

interpeak

Interpeak LDAP Client

Configuration of distributed embedded systems is often a complex task which requires careful consideration. The Interpeak LDAP client provides directory services through a client/server model, allowing networked nodes to be configured in a simple and uniform way.

LDAP stands for Lightweight Directory Access Protocol, and is a networked directory access protocol that runs over TCP/IP. LDAP specifies a number of directory services that a client application can get from an LDAP-enabled directory server.

LDAP Directories

LDAP directories are fast, network enabled catalogues, similar to databases in most ways but with a couple of major differences. First, directories are for the most part hierarchical, while databases often have a flat organization. The other major difference is that directories are built to be searched often but rarely modified. Databases on the other hand are designed for an equal amount of searching, modifying, deleting and adding of entries.

Powerful yet Simple Protocol

The LDAP protocol is simple, but still provides a wealth of features capable of supporting any kind of application. LDAP offers both access and update capabilities, allowing directory information to be managed as well as queried.

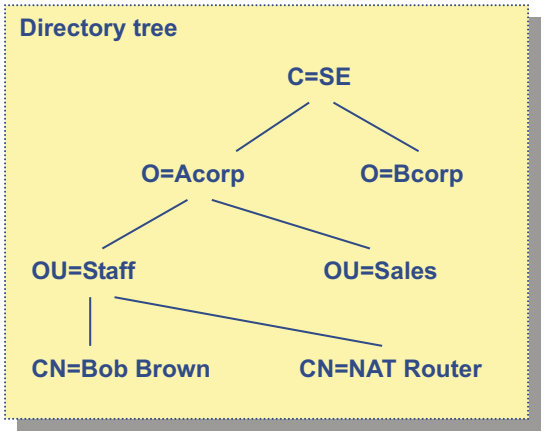
Hierarchical Entries

Each entry, except for the root entry, has one parent and zero or more children. An LDAP search operation is normally done by specifying a entry as the search root and the search is done in the subtree below that entry.

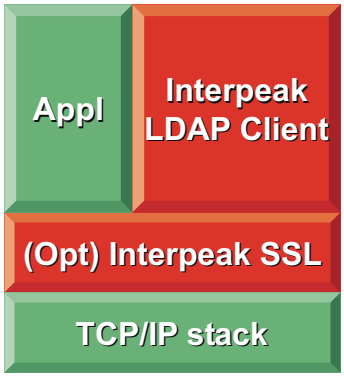
Attributes

Data is stored in an entry as name/value pairs called attributes. The attribute name determines the type and format of the data while the attribute value contains the actual data. The value of a *mail* attribute may for example be an e-mail address as a text string, while the value of a *photo* attribute may be a binary JPEG image.

Attributes are often used as constraints during search operations. It is for example possible to get all entries that have a *serialnumber* attribute or to get all entries that have a *mail* attribute containing the string “Interpeak”.



Each LDAP entry is identified by a Distinguished Name (DN). A DN consists of one or more Relative Distinguished Names (RDN). Examples of RDNs are country (C), organization (O), organizational unit (OU) and common name (CN). The DN is constructed by writing the most specific RDN to the left, followed by more and more generic RDNs. Example: Bobs DN is ’CN=Bob Brown, OU=Staff, O=Acorp, C=SE’ and the DN for ’Acorp’ is ’O=Acorp, C=SE’.



The LDAP Client combined with SSL to provide secure directory services.

Uniform Directory Services

LDAP directory services can for example allow people and devices to locate other users, resources, services and information in a simple and uniform way. Modification of a resource, like changing the IP address, only has to be published to the directory to be propagated to all entities that use that resource.

Industry (IETF) standard

LDAP is an open Internet standard, specified by the Internet Engineering Task Force, IETF. It is implemented by a large number of well-known vendors in the IT industry, e.g. Microsoft, Netscape, Novell, etc.

Typical LDAP Session

The following text is a description of how to use the Interpeak LDAP client to perform directory services:

1. Specify the host address and get a handle to the connection

The first step is to specify the host address and the TCP port to use. A handle for the connection is returned and must be used in all subsequent calls.

2. Set LDAP options

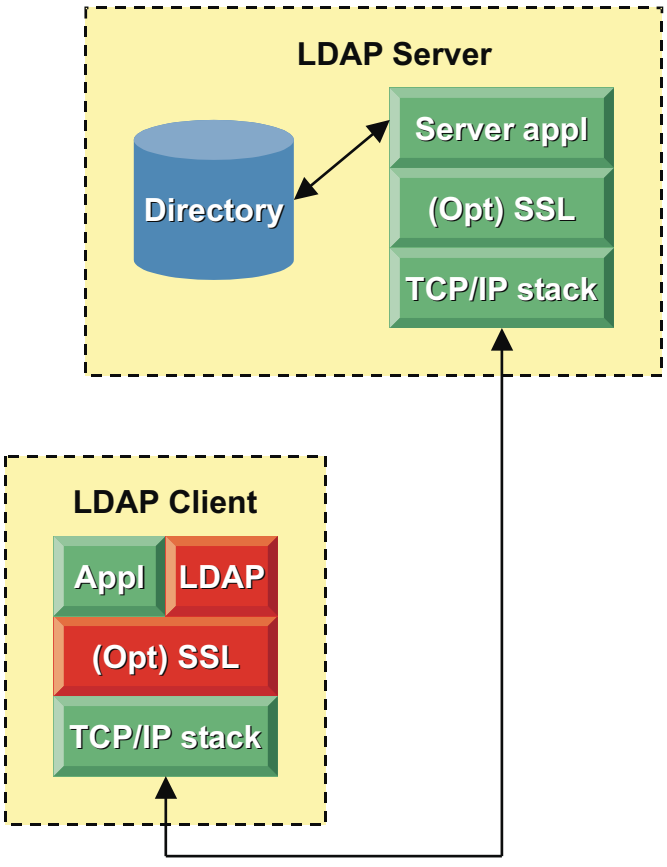
LDAP options includes the maximum time an LDAP operation is allowed to take, the maximum number of entries that can be returned by a search operation and if LDAP over SSL should be used. This step can be skipped if the default settings are satisfying.

- **Implements LDAP v2 (RFC 1777)**
- **Implements the standard LDAP API (RFC 1823)**
- **Uses the standard LDAP search filter syntax (RFC 2254)**
- **Supports LDAP over SSL (LDAPS)**
- **Tested with Netscape LDAP server version 3.x and 4.x**
- **Tested with OpenLDAP server version 1.2.x**
- **High performance**
- **Delivered in ANSI compliant "C" source code.**
- **Complete ready-to-run RTOS integration with examples, makefiles etc.**

Interpeak LDAP Client features.

3. Bind to the LDAP server

The client authenticates itself to the LDAP server in this operation. The identity of the client determines which operation that can be done on the directory. It is possible to bind several times on the same connection if the access level must be changed. The last successful bind operation determines the access level of the following calls.



4. Issue LDAP commands

The client can now do all the operations that the current identity allows. All operations can be used in either synchronous or asynchronous mode. Synchronous calls blocks until the operation is finished and the result of the operation is returned. Asynchronous calls returns immediately with a ID number that identifies the request.

The client can issue several asynchronous request in parallel to the LDAP server. The LDAP API also has a function that, given the ID, will return the result for a asynchronous request.

5. Unbind

The last operation must always be unbind. Unbind tells the LDAP server that the client is done using its services and that used resources can be freed.

Interpeak Secure Networking Software

Interpeak provides state-of-the-art networking solutions specifically designed for embedded systems. The company´s embedded networking and security software is currently used in thousands of applications across the globe.

Headquartered in Stockholm, Sweden, Interpeak operates through a global network of distribution channels and has its own sales and field application force dispersed in strategic locations worldwide, including the USA, Europe, and Asia. For additional information, please visit our homepage *www.interpeak.com*.