Inventions on using LDAP for Different Purposes (Part-2) - A TRIZ Based Analysis of US Patents

Umakant Mishra
Inventions on using LDAP for Different Purposes (Part-2)
-A TRIZ based Analysis of US Patents

By- Umakant Mishra, Bangalore, India
http://umakantm.blogspot.in

[This article is divided into 3 parts for convenience of size. The first part of the article includes 6 patents using LDAP for “e-commerce” and “Policy Management”. The second part includes 10 patents using LDAP for “Network Management” and “Telecommunications”. The third part of the article includes 11 patents using LDAP for “World Wide Web” and “Java and CORBA”.

Contents

Contents .............................................................................................................................................1
5. Inventions on using LDAP for network management .................................................................2
  5.1 Using LDAP to unify RADIUS and DHCP .............................................................................2
  5.2 Trusted processing of Unique Identifiers in LDAP .................................................................3
  5.3 Active polling by network LDAP directory .............................................................................4
  5.4 Global sign-on method using LDAP .......................................................................................5
  5.5 Network directory access mechanism .....................................................................................5
6. Inventions on using LDAP for telecommunications .................................................................6
  6.1 Using LDAP to redirect telephone calls .................................................................................6
  6.2 Integrated directory services .....................................................................................................7
  6.3 Using LDAP to direct the transmission of facsimiles .............................................................8
  6.4 IP based wireless messaging using LDAP .............................................................................8
  6.5 Spoken name announcement feature in a messaging environment ......................................9
Reference to patents: .........................................................................................................................9
Other References: ...........................................................................................................................10
5. Inventions on using LDAP for network management

The following patents have been analyzed under this section.

- US Patent 6614788, “Network address management”,


- US Patent 6801946, “Open architecture global sign-on apparatus and method therefore”,

- US Patent 6553368, “Network directory access mechanism”,

- US Patent 6101541, “Active polling by network LDAP directory”,

5.1 Using LDAP to unify RADIUS and DHCP

Background problem:

In a dynamic address management system, the systems request their IP (Internet Protocol) address from a common pool of addresses. The dynamic IP allocation is managed either by Remote Authentication Dial-In User (RADIUS) protocol or by Dynamic Host Configuration Protocol (DHCP). These two protocols are managed independently with separate pool of IP addresses being kept for each protocol.

This arrangement works in principle, but it is an inefficient way of managing IP addresses particularly in organizations where users may operate both on the local network and at a remote location requiring external access. There is a need to maintain a common pool in order to optimize the management of IP addresses.

Solution provided by patent 6614788

US Patent 6614788 provides a method of allocating IP addresses using LDAP. There will be a common single pool of network (IP) addresses, which will be allocated by LDAP server in response to requests by clients. LDAP also maintains a record of network address allocation to users. Thus the IP allocation under RADIUS and DHCP can be unified using a common address pool and mappings between IP addresses and centralizing the allocation by using a Directory service.
Thus the new method comprises the steps: a) receiving a request from a client for an IP address through at least one of RADIUS and DHCP; b) sending the request to a directory service for an unused IP address; c) returning a response to the client including an unused IP address allocated to the client; and d) updating the directory service for the allocated IP address–hostname/user binding.

TRIZ based analysis

The invention maintains a common network address pool to be used for both RADIUS and DHCP protocols (Principle-5: Merging).

The common address pool is maintained by LDAP directory service, which takes care of taking the request and allocating the IP address (Principle-24: Intermediary).

5.2 Trusted processing of Unique Identifiers in LDAP

Background problem:

Many security systems are moving their databases to LDAP. But each of those security systems must store and protect its own set of unique identifiers on LDAP. A unique identifier is unique within the database of a security system, usually created by the security system while adding a user or group. When the security systems move to LDAP they create, store and take precautions to protect their unique identifiers, as LDAP does not provide any mechanism to generate, verify or protect a unique identifier. It would be nice to have common set of unique identifiers, which could be shared by different security systems using the LDAP directory.

Solution provided by Patent 6714930

US Patent 6714930 presents a method, which allows different security systems to store and retrieve unique identifiers that are shared or common to the entire directory. According to the invention, there will be trusted process, which will allow LDAP users to store and retrieve unique identifiers using standard LDAP interfaces. The trusted process generates or verifies a unique identifier,
guarantees the uniqueness of a unique identifier within the entire directory (rather than just within a single security system), and guarantees that any unique identifier returned to an LDAP user is a trusted unique identifier.

**TRIZ based analysis**

The invention generates unique identifiers and guarantees the uniqueness of the unique identifier within the entire directory and allows all the security systems to share the unique identifier information (*Principle-6: Universality*).

### 5.3 Active polling by network LDAP directory

**Background problem**

Using a directory server to manage Quality of Service (QoS) in a network offers many advantages. The devices in the network can access the information from their local directory, and also store their information in the directory. But using a centrally administered directory for the control of network operations has some performance problems.

(i) **Update Lag:** While an edge-device maintain its classification rules in consistent with the classification rules in an LDAP server, an operator may change the rules in the directory server. This may cause some latency between the edge-device queries the server and the data is updated, and the edge-device may operate using out-of-date rules during that period.

(ii) **Server Overload:** When there are hundreds of edge-devices that store information in the directory, the directory can be easily overloaded. This may cause some devices to be unable to connect for long time.

(iii) **Encrypted data:** When the IP payload is encrypted using a protocol such as IP-sec, an intermediate box is unable to obtain the information such as port numbers etc.

There is a need to address the problems of server overload when an intermediary edge-device is used to classify packets, and a directory server is used as the site for network administration.

**Solution provided by US Patent 6101541:**

The invention is an apparatus for controlling client node access to data items maintained in a directory. The data items include volatile data items. The apparatus comprises a communication device for communicating with multiple client nodes; and a processor, coupled to the storage device for polling the client nodes to exchange (e.g., retrieve and/or transmit) data related to the volatile data items, via the communication device. The processing system further controls client node access to the data items of the storage device. In this way, the apparatus and method of the present invention remedies the problems associated with directory server overload.
TRIZ based analysis

The invention uses polling techniques. The directory server contacts the client nodes (or polls client nodes) to exchange information related to data items stored in directory server, instead of clients contacting the server (Principle-13: Other way round). As the clients don’t need to contact the server, the possibility of server overload is reduced.

The server may poll the clients at periodic intervals or upon a triggering event (Principle-19: Periodic Action).

According to the invention, all the fields are not updated each time. Only a subset of fields for each entry is flagged to be volatile (Principle-35: Change Parameter). These volatile fields are used to update the client nodes or to be updated with data from the client nodes.

5.4 Global sign-on method using LDAP

US Patent 6801946 discloses a method of implementing a global sign-on using LDAP. Users in an enterprise-computing environment typically access several different systems each having unique user-id and password. It is desired to implement a global sign-on mechanism to sign only once and login to all other systems. According to the invention, the Global sign-on (GSO) maintains a GSO database in an LDAP server. The user login once into the GSO and authenticated in other systems by using the GSO LDAP schema (Principle-10: Prior Action, Principle-24: Intermediary, Principle-6: Universal).

5.5 Network directory access mechanism

US patent 6553368 discloses a method to integrate LDAP directory to other directories without converting the data. As per the invention, the data in the first directory remains in its own format and data in the other directories also remain in their own formats. The access rights and access methods of directory entries are stored in a Directory Access Control Domain (DACD). But the directory access mechanism is capable of accessing different directories through different protocols (Principle-33: Homogeneity).
6. Inventions on using LDAP for telecommunications

- US Patent 6778544, “Method and system for redirecting calls”,
- US Patent 6906817, “Network system for directing the transmission of facsimiles”,
- US Patent 6779025, “IP web based messaging system for localized management of wireless messaging”,
- US Patent 6810113, “Methods and systems to make spoken name data available”.

6.1 Using LDAP to redirect telephone calls

Background problem
The calls placed in the PSTN (Public Switched Telephone Network) use offboard lookups to redirect the calls to the correct destination. For example, when a caller makes an 800 or 888 long-distance calls, the service access code (SAC) is translated into a directory number. Similarly when the caller makes a local number portability (LNP) call, the local routing number is used alongside the original directory number to route the call to its destination.

The drawback of using this system to perform SAC/LNP queries is that it consumes 30-40% more time to route the redirected calls than routing the non-redirected calls.

Solution provided by patent 6778544
US Patent 6778544 discloses a method for redirecting calls more efficiently, whereby an LDAP query is encoded with a called telephone number. The LDAP query is transmitted from a TCP/IP to an LDAP server via an IP network, and the TCP/IP awaits a response back from the LDAP server, which response identifies a corrected destination address, and may include translated digits which may be used in telephony routing.

According to the present invention, SAC and/or LNP queries and the redirecting of calls is improved by using a TCP/IP stack and LDAP protocol in lieu of an SS7/TCAP stack, SCP, and STP. This permits the use of Internet protocols, which are less expensive and faster than an SS7/TCAP stack, SCP, and STP, thereby reducing telephone line blockage and increasing the traffic capacity of telephone switches.
TRIZ based analysis
The invention uses TCP/IP stack (faster and cheaper) and LDAP protocol (open standard) in lieu of an SS7/TCAP stack, SCP and STP (Principle-28: Mechanics substitution).

6.2 Integrated directory services

Background problem
Traditionally a corporate enterprise has both data communication system (such as email server) and a voice communication system (such as EPABX) and directory servers, which contain some data in common. But a directory server is physically and logically separate from the telephone directory. As a result, every time a change is made to the common data, it is changed manually and independently in both the directories. This duplicate data entry increases burden on the network administrator and the PBX system administrator, besides leads to occasional errors and inconsistencies.

There is a need to have a single data entry (and administration) point for all the directories that share common data (like a telephone number).

Solution provided by US Patent 6377950
US patent 6377950 provides an Integrated Directory Services system (IDS) which automatically synchronizes data in a central Directory server with a telephone directory of a PBX. The IDS provides a single administration point for all additions, deletions and data changes, which are then automatically propagated to the other databases. This eliminates the need of independent entry to each existing system and ensures consistency in all the databases.
TRIZ based analysis

All directory databases should be updated automatically as and when a change is required (IFR). All directories should be automatically updated when the modifications are done at one central place (Desired Result).

The invention uses Integrated Directory Services (IDS) which works as an intermediary between the telephone directory and the directory database (Principle-5: Merging, Principle-24: Intermediary) and provides a single administration point to update all directory databases (Principle-6: Universality).

6.3 Using LDAP to direct the transmission of facsimiles

Although there are stand-alone fax machines in existence, it has become common to incorporate a facsimile transmission and reception function into computers. US Patent 6906817 discloses a method of sending facsimiles using an external LDAP database. According to the invention the document recognition system is setup to recognize various document types and the rules as to how to extract destination data from each document type. The system will try to get the fax number or some other identify of the intended recipient from the document. If it gets the fax number of the destination it sends the fax, on the other hand if it gets some other identity of the destination (such as name, etc.) it will send a query to the LDAP server to find the fax number of the recipient and send the fax (Principle-10: Prior Action, Principle-24: Intermediary).

6.4 IP based wireless messaging using LDAP

US Patent 6779025 discloses a method of executing a messaging application by using HTML documents, HTTP protocol and LDAP server. According to the invention, there will be a messaging server, which will send the call to the destination address by referring to the destination address in the LDAP server. The media content (voice message) and control tags are enclosed in an HTML document (Principle-7: Nested Doll) and sent to the destination address. This
Inventions on using LDAP for different purposes, by Umakant Mishra

The invention uses IP network and HTTP protocols that provide an easier and cheaper solution of wireless messaging (Principle-28: Mechanics Substitution).

6.5 Spoken name announcement feature in a messaging environment

US Patent 6810113 discloses a method of using LDAP in a messaging system which would allow messaging services to provide senders with announcements regarding the recipients. According to the invention, the information on the senders and recipients will be stored in LDAP server (Principle-24: Intermediary). When a message sender's messaging platform (MP) finds the spoken name data of the recipient from the Directory (or other sources) the MP makes a presentation to the sender (Principle-23: Feedback). With the implementation of the spoken name announcement feature, the sender becomes sure that his or her message will be made available to the recipient intended by the sender.

Reference to patents:


Other References:


