Inventions on using LDAP for different purposes-
Part-1

Umakant Mishra
Inventions on using LDAP for Different Purposes, Part-1
-A TRIZ based Analysis of US Patents

By- Umakant Mishra, Bangalore, India
http://umakanmt.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
1. Introduction .................................................................................................................2
2. Study on using LDAP for different purposes ..........................................................2
   2.1 The objective of the study is to know: ...............................................................2
   2.2 Major areas of Invention ....................................................................................2
3. Inventions on Using LDAP for e-commerce .........................................................3
   3.1 Using LDAP to store and retrieve schemas for e-commerce documents ....3
   3.2 Implementing e-commerce and directory authenticated bank drafts using LDAP .................................................................4
4. Inventions on Using LDAP for Policy Management ...............................................5
   4.1 Unified policy management system using LDAP for high availability units ..5
   4.2 Storing Policies in LDAP for policy-based management ............................6
   4.3 Storing policies in LDAP for policy based management of network Quality of Service ........................................................................8
   4.4 Generating configuration files using policy descriptions ...........................8
Reference to patents .....................................................................................................8
Other References .......................................................................................................9
1. Introduction

Lightweight Directory Access Protocol (LDAP) is an IETF open standard to provide directory services in the network. LDAP was initially developed at the University of Michigan with an objective to include most of the features of X.500, while eliminating the burdens and difficulties of the same.

The current Version of LDAP is LDAP V.3 released in December 1997 (RFC 2251). Other specifications of LDAP can be found in different RFCs on the IETF (Internet Engineering Task Force) website.

With the growing use of Internet, LDAP is becoming more and more popular to provide directory services to a wide range of applications. This led to patenting several inventions relating to LDAP operation and application. This study on LDAP data storage is a part of the main study on LDAP based on 60 selected patents on LDAP from US Patent database.

2. Study on using LDAP for different purposes

This study on using LDAP for different purposes is a part of the above-mentioned study “Inventions on LDAP- A study based on US Patents”. While the main article contains the study objectives, methodology and general findings, the analysis of patents on different aspects LDAP are presented in separate articles.

Unlike other parts of the study which have tried to improve certain aspect of LDAP technology and application, this article includes the inventions that use LDAP for various different purposes.

2.1 The objective of the study is to know:

- What are the inventions that use LDAP for different purposes?
- Which Inventive Principles or other TRIZ techniques can be used to analyze those patents.
- Which areas of LDAP usage is not explored yet?

2.2 Major areas of Invention

- Using LDAP for e-commerce
- Using LDAP for policy management
- Using LDAP for network management
- Using LDAP for telecommunications
- Using LDAP for World Wide Web
- Using LDAP for Java and CORBA
3. Inventions on Using LDAP for e-commerce

The following patents have been analyzed under this heading.


3.1 Using LDAP to store and retrieve schemas for e-commerce documents

Background problem:

There are techniques like EDI (Electronic Data Interchange) to exchange messages for Business-to-Business communications. The messages are compiled into business documents, which are exchanged to facilitate transactions between trading partners. However, each organization using EDI typically stores its data in a private format. Hence two EDI partners have to agree in advance on a common format to exchange their private data sets and develop or configure their software to recognize that format.

This has a disadvantage of writing a new translation program for each time a new trading partner is added to a client list which increases software development overhead. It is desirable to establish an effective communication standard, which should allow new document types to facilitate new transactions, while preserving the integrity of the existing document types and transactions they support.

Solution provided by patent 6591260

US Patent 6591260 invents a method of using LDAP for commercial data Interchange. According to the invention, the messages relating to business transactions, such as purchase orders, purchase order acknowledgements, order status checks, availability checks, invoices, invoice acknowledgements etc. are all written in XML. The XML documents will be polymorphic to allow any extension of the document type. Further according to invention, the document instances will contain the identifiers or Uniform Resource Names (URNs) of the schemas they use. The URN registry consisting of URNs with their URIs (Uniform Resource Identifiers) are stored in a LDAP server. The LDAP directory is used to search a URI (the location of URN) for a URN (the document type definition). Each trading partner will query the directory server to resolve their document types (URNs) to find their locations (URIs) and get the document definitions to interpret their business documents.
TRIZ based analysis

The invention proposes to share common schemas or formats for interpreting e-commerce documents to be shared by all trading partners in the marketplace (Principle-6: Universal).

The method first stores the common formats in LDAP server to be retrieved later by the trading partners to interpreting their e-commerce documents (Principle-10: Prior Action).

The LDAP directory is used to store the URNs (Uniform Resource Names) with their URIs (Uniform Resource Identifiers). The same directory is searched to find the URIs to resolve the document types (Principle-24: Intermediary).

3.2 Implementing e-commerce and directory authenticated bank drafts using LDAP

Background problem

Although there is so much of developments in Internet trading and e-commerce, the banks have not been integral parties to the web based financial transaction between the web-customers and web-venders. Although the money is ultimately debited from the web-customer’s back account, or charged to his/her credit card, the customer’s bank is typically not involved in e-commerce transactions. There is a need for a system that can include financial institutions such as banks as integral participants in e-commerce transactions.

Solutions provided by patent 6898577

US Patent 6898577 discloses a method of computer-implemented draft authentication for use in e-commerce. This allows financial transactions to be
carried out on the web by maintaining security and confidentiality of the web-
customer’s personal and financial information.

According to the invention, the draft authentication method will first include,
establishing partner relationships between a financial institution and a plurality of
World Wide Web (Web) vendors. Then it will store the unique identification
information for the web-customer’s financial information. The drafts of web-
customers will be authenticated by matching the encrypted identification data of
the web-customers, such as passwords, ID and biometric data. The drafts are
honored by the bank only after successful matching of the authentication. It is
proposed to use LDAP compatible directory software to store, process and
replicate the web customer’s identification information to each of the web venders.

TRIZ based analysis
The invention finds a method of computer-implemented draft authentication
method that can be used in e-commerce (Principle-28: Mechanics Substitution).

4. Inventions on Using LDAP for Policy Management

The following patents have been analyzed under this section.

- US Patent 6678835, “State transition protocol for high availability units”,
- US Patent 6463470, “Method and apparatus of storing policies for policy-
based management of quality of service treatments of network data traffic
flows”,
- US Patent 6718380, “Method and apparatus for storing policies for policy-
based management of network quality of service”,
- US Patent 6598057, “Method and apparatus for generating configuration
files using policy descriptions”.

4.1 Unified policy management system using LDAP for high
availability units

Background:
In a computer network, it is necessary to do network policy management, such
as firewall protection, Network Address Translation, spam filtering, DNS caching,
web caching, URL blocking etc. When the network grows, the number of devices
grows and creates a tremendous load to configure, manage and monitor the
devices.

There is a need for a unified policy management system where various policies
may be defined and managed from a single location. It is desirable to have a
high-availability of mission critical units configured in the system to prevent a failure.

**Solution provided by patent 6678835:**

US Patent 6678835 discloses a method of unified policy management system for an organization using a central policy server and remotely situated policy enforcers. The central database and policy enforcer databases will be stored in LDAP servers.

Each high availability device will be marked as whether primary unit (first class unit) or backup unit (second class) or a stand-alone unit (third class). The configuration information of the primary and backup units are synchronized by transitioning the first class unit to an active state and transferring the configuration changes to the second-class unit. When the primary unit transitions to an inactive state, the backup unit stores the second database configuration changes on the second class unit and transfers those changes to the primary unit after it re-transitions to the active state.

**TRIZ based analysis**

The invention uses backup devices for mission critical units and the configuration changes for the primary devices are also synchronized in the backup devices (Principle-26: Copying).

When the primary devices become inactive, the backup devices use the backup configurations and become active (Principle-11: Cushioning).

**4.2 Storing Policies in LDAP for policy-based management**

**Background problem**

Every network follows certain protocols, which consists of a set of rules defining how entities interact with each other. All hardware, software (and even others) have to follow the policies and protocols for effective interaction in the network. Currently the application programs that execute in network devices rarely invoke QoS functions, and therefore they do not take full advantage of QoS features that are available in the network devices. There is a need to integrate applications into a policy-based networking system.

One approach of the prior art is to apply QoS based on the IP address or port number associated with a traffic flow. This approach has several advantages, such as, it is centralized; it works with multiple applications; and it is application independent. However, the approach also has significant disadvantages. It is based on limited or no knowledge of application traffic flows. A network manager cannot define and apply QoS policies for individual applications. It has only limited applicability to encrypted packets.
In another approach of the prior art, applications use QoS signaling mechanisms, such as RSVP or DS (differentiated services) to request a particular QoS for a particular traffic flow. Although this approach can take advantage of detailed knowledge of different traffic flows produced by an application, practically the RSVP requests may not comply with network-wide policies. In such cases the devices are often configured to ignore the signaling and treat all traffic equally.

Thus there is a need for a mechanism that integrates applications into a policy-based networking system and enables the applications to get advantage of it.

**Solution provided by patent 6463470**

Patent 6463470 discloses a method of integrating a network with policies representing quality of service treatments. According to the method the policies are stored in LDAP in the form of policy statements. The application program and other network devices can retrieve the policy information from the Repository and associate with them. The Quality of Service treatments are determined depending on that policy information.

![Diagram of policy server and LDAP](image)

**TRIZ based analysis**

All network devices and applications should get the benefit of QoS features available in a network (Ideal Final Result).

One solution in the prior art is to add additional information like user-priority and type-of-service in the MAC address header on the IP packet which is read by the intermediate devices and treat them in a predefined manner (Principle-31: Hole, Principle-10: Prior Action).

The current invention uses LDAP as a repository of predefined policy statements (Principle-24: Intermediary). A device or application can access the LDAP server to access the policy information and avail the desired Quality of Service (Principle-15: Dynamize).
4.3 Storing policies in LDAP for policy based management of network Quality of Service

US Patent 6718380 discloses a method of storing policies in LDAP directory to manage network quality of service. The invention has similarity with patent 6463470 (by the same inventors) illustrated above. According to the invention the policy server will create and store policies in the LDAP directory in the form of policy statements. Each policy statement applies to a specific application that runs in the network. The application program and the network devices can retrieve the policy information from the LDAP server using LDAP protocol.

4.4 Generating configuration files using policy descriptions

US Patent 6598057 discloses a method of generating binary configuration files using policy descriptions. According to the invention, the policy descriptions are stored in an LDAP server. The binary configuration-files (in DOCSIS format) are generated by using the configuration policy data which are obtained by parsing the identification encode filename. The other aspect of invention is that the configuration policy data is optimally cached on a TFTP server. This method is claims better configuration file management and more effective broadband provisioning.

Reference to patents:


Other References:


About the author

After working for more than 18 years in various fields of Information Technology Umakant is currently doing independent research on TRIZ and IT since 2004. He last worked as Director and Chief Technology Officer (2000-2004) in CREAX Information Technologies (Bangalore). Before that he worked as IS/IT manager (1996-2000) for ActionAid India (Bangalore).

Umakant is a Master in Philosophy (MA), Master in Business Administration (MBA), Bachelor in Law and Logic (LLB), Microsoft Certified Systems Engineer (MCSE+I), Certified Novell Engineer (CNE), Master Certified Novell Engineer (MCNE), Certified Intranet Manager (CIM), Certified Internet Professional (CIP), Certified Software Test Manager (CSTM) and holds many other global IT certifications.