INSTANT MANAGEMENT INFRASTRUCTURE
Through Network Management Support Systems and Software Agents Coordination

José A. Folha
Responsible Network & Systems Management, Superior School of Biotechnology of the Portuguese Catholic University, MsC student, Electrical and Computer Engineering's Department, Engineering Faculty of University of Porto, Portugal,

Bruno F. Marques
Lecturer, Electrical Engineering Department, Polytechnic Institute of Viseu's Superior School of Technology, PhD student, Electrical and Computer Engineering Department, Engineering Faculty of University of Porto, Portugal,

José A. Oliveira
Lecturer, Computer Science Department, , Polytechnic Institute of Viseu's Superior School of Technology; PhD student, Electrical and Computer Engineering Department, Engineering Faculty of University of Porto, Portugal,

Paulo M. Coelho
Lecturer, Computer Science Department, , Polytechnic Institute of Viseu's Superior School of Technology; PhD student, Electrical and Computer Engineering Department, Engineering Faculty of University of Porto, Portugal,

Raul F. Oliveira
Auxiliary Professor, Electrical and Computer Engineering's Department, Engineering Faculty of University of Porto, Portugal,

Keywords: Internet services, Networking Management Applications, LDAP, Basic Internet Protocols, Software Agents, Instant Messaging.

Abstract: Enterprises need to automate manual and routine aspects of IT infrastructure management. In this paper a new concept that integrates different autonomous and management level applications through Instant Messaging protocol (XMPP) is introduced. This is achieved by means of a common management information model implemented in LDAP. A content language implemented in XML is also described, allowing autonomous application integration to carry out management tasks dynamically.

1 INTRODUCTION

When we speak about IP network management, we increasingly see the need for proactive actions that, by their own characteristics, autonomous applications replace Human action.

These actions are only possible to implement if we speak about autonomous applications. If we think of them, we easily realize that they might be used to manage a network proactively at different levels (Oliveira R., 1998). From the Human point of view, management is more easily achieved.

A. Folha J., F. Marques B., A. Oliveira J., M. Coelho P. and F. Oliveira R. (2006).
INSTANT MANAGEMENT INFRASTRUCTURE - Through Network Management Support Systems and Software Agents Coordination.
In *Proceedings of the International Conference on e-Business*, pages 69-74
DOI: 10.5220/0001428600690074
Copyright © SciTePress

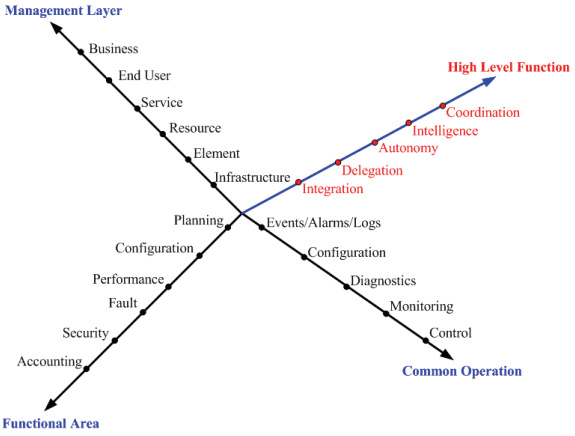

Figure 1: Management Dimensions.

Despite the concepts which exist on how to approach this problem, we want to explore a new one, Instant Messaging. XMPP will be used as base of communication between applications, and XML as a content language.

Existing management applications are used to implement a common management information model. Besides network topology discovery, alarms can be triggered to a management console or sent by email to the network administrator.

We know network administrators either do not have permanent contact with the screen, or they are away from the managed domain. These situations may lead to delays and complications in the network as well as the systems involved.

Autonomous applications should have an important role here in how they can help solve some of these problems.

Objective

The main goal is to automate the manual and routine aspects of IT infrastructure management and develop a way that allows different management applications to communicate/share information in a standard and open way. To achieve this, we propose a multi-agent architecture based on the concept of Instant Messaging (using XMPP protocol) which integrates different autonomous and existing proprietary management applications. This architecture is based on a new and common management information model, called LMIB (LDAP based Management Information Bus) (Marques B., Nogueira E., Oliveira J., Oliveira R., 2004).

The model was designed for use in different management applications to allow them to share their management information easily without the use of proprietary interfaces/APIs.

2 MULTI AGENT ARCHITECTURE MODEL

The traditional multi agent architecture defined by FIPA/KQML, establishes the logical reference model for the creation, registration, location, and communication of agents (FIPA, 2004).

This model is made up of several blocks:

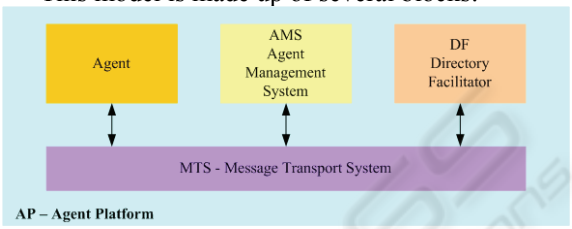

Figure 2: Agent Management Reference Model.

Our work tries to implement this concept through LDAP, as we are also using this protocol to implement a common management information model. Another major reason to use LDAP is that it supports all the functions implemented by the DF and AMS, such as registration, searching, modifying, etc.

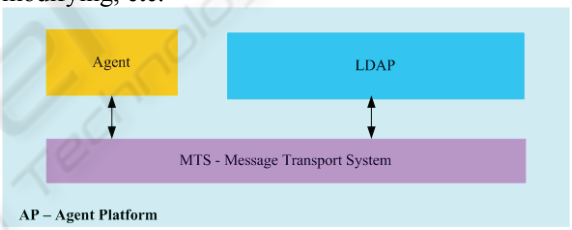

Figure 3: LDAP Agent Management Model.

The MTS will be replaced by an Instant Messaging Server that implements the XMPP Protocol (Jabber Software Foundation, 2006).

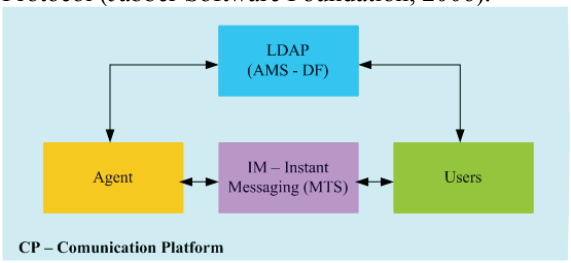

Figure 4: Communication Platform.

At this point we now have what we call a Communication Platform. Agents may communicate in two different ways:

LDAP Queries: whenever an Agent wants to find a service or another agent, on the LDAP server;

IM: whenever an Agent wants to communicate with another agent or service;

One advantage of the Communication Platform is that users can communicate directly with agents.

This allows users to query for services, and know what the agents are doing (status of the agent: away, busy, online, etc…).

This model will be the base of our work to explore the concepts which follow.

3 FRAMEWORK ARCHITECTURE

Supposing that all the information needed is in the global LDAP information model, autonomous applications will behave like a user, acting on behalf of network administrators. Autonomous applications will use alarms triggered by network management applications, providing state information and services to solve the problem.

3.1 Information Model

The information model is based on global management information called LDAP Management Information Bus (Marques B., Oliveira J., Coelho P., Oliveira R., 2006).

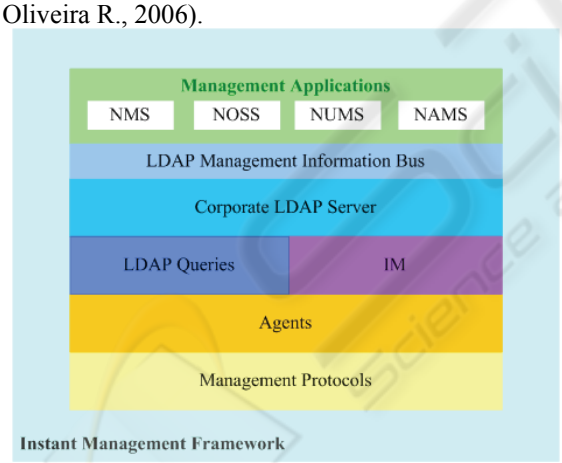

Figure 5: Instant Management Framework.

To manage the IT infrastructure, a Network Management System (NMS) is used, providing the information model with all necessary management information. Similarly, a Network Operations Support System (NOSS) is used to manage network services. A Network Users Management System (NUMS) station is also used to manage network users' profiles. A Network Asset Management System (NAMS) is responsible for the network inventory (Coelho P., Marques B., Oliveira J., Oliveira R, 2005). One of several problems found in such a management environment is the integration of each of these applications.

In order to solve this problem, a network management information bus, supported on LDAP Directory Services, was developed, playing an essential role in integrating these management applications. The global information model LDAP implemented (Marques B., Oliveira J., Coelho P., Oliveira R., 2006) is also used by autonomous applications which communicate between them using Instant Messaging and with LDAP queries with the corporate LDAP server to find other agents or services. Those autonomous applications will be registered on the same LDAP based model.

3.2 LDAP Schema for the Autonomous Applications

An LDAP schema is specified to allow the support of the entire life cycle of autonomous management applications. The schema specification (OpenLDAP Foundation, 2004.) is based on the FIPA Abstract Architecture Specification (FIPA, 2004).

The resulting DIT – Data Information Tree to the agency is shown in the figure 6.

Agents and Services on the DIT are kept separated, because agents may perform one or more services, and Services may be achieved by one or more agents.

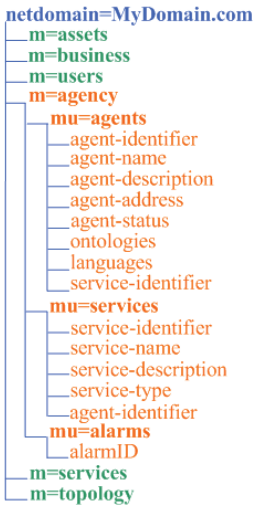

Figure 6: DIT for autonomous applications.

Agent Directory

An agent-directory is a shared information repository in which agents may publish their agent-

directory entries and in which they may search for agent-directory-entries of interest.

agent-identifier: A globally unique identifier (name or number) for the agent that will allow an agent to be identified by other agents.

agent-name: A globally unique name for the agent. An agent-name is a means of agent identification for other agents and services. It is expressed as a key-value-pair, which is unchangeable (that is, it is immutable), and unique under normal circumstances of operation.

agent-description: The agent-description contains information about the agent and his services.

agent-address: An agent-address consists of the address, which can be used to communicate with an agent. An agent-address may be used by a message-transport-service to select a transport for communicating with the agent, such as an agent or a service.

agent-status: An agent-status consists of the status of an agent, if he is available, busy, online, and so on. Basically it is the presence effect on the IM server (Saint-Andre, 2004).

ontologies: An ontology provides a vocabulary for representing and communicating knowledge about some topic and a set of relationships and properties that hold for the entities denoted by that vocabulary.

languages: The language used to express the content of communication between agents.

service-identifier: A globally unique identifier (name or number) for the service that will allow identification of a service.

Service Directory

The basic role of the service-directory is to provide a consistent means by which agents and services can locate services. Operationally, the service-directory-service provides a location where services can register their service descriptions as service-directory-entries. Also, agents and services can search the service-directory-service to locate services which are appropriate to their needs.

service-identifier: A globally unique identifier (name or number) for the service that will allow identification of a service.

service-name: A globally unique name for the service.

service-description: The service-description contains information about the services.

service-type: The categorized type of the service.

agent-identifier: A globally unique identifier (name or number) for the agent that will allow an agent to be identified by other agents.

LDAP Agent Registration LDIF format sample code

Bellow is a sample code for the Agent registration on the Corporate LDAP Server.

```
# Agent Account [dispatcher]
dn:
uid=dispatcher,ou=AgentDirectory,ou=Age
ncy,dc=example,dc=com
cn: Dispatcher Agent
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
uid: dispatcher
userPassword: password
structuralObjectClass: inetOrgPerson
mail: dispatcher@example.com
```

4 IMPLEMENTATION SCENARIO

Let us suppose that these management applications already have an LDAP interface implemented and that all the information needed is in the global LDAP information model.

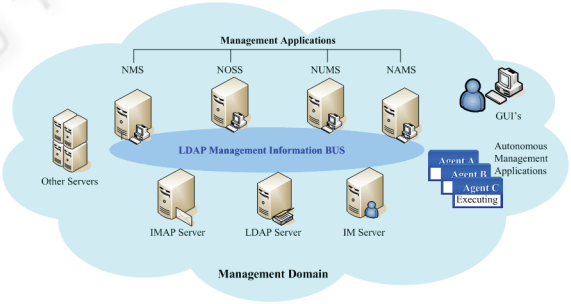

Figure 7: Network Environment.

Besides these kinds of management applications in our network environment (see figure 7) we also find email servers (IMAP, SMTP, POP), Web Servers and a Corporate LDAP Server to implement the root of the Management Information Bus. Network administrators and other users have regular PCs as GUIs. Through them, administrators can perform management tasks using standard Internet protocols (HTTP, XML/XSL) without needing proprietary GUIs. Firewalls/Proxies implement secure network interconnections.

The Corporate LDAP root server supports the network management information model so as to take advantage of the existence of LDAP interfaces on the management applications (NMS, NOSS, NUMS, NAMS, etc.) and use CMIP and DEN network concepts. Here, a particular management domain can implement its own network policies. Let us look at the concept in more depth. In the next figure, it is possible to see management application integration and how users, autonomous applications and Instant Messaging can take advantage of this mechanism based on simple Internet protocols that everyone knows and uses.

Autonomous applications using Instant Messaging and management tasks

One big problem we foresee is what happens if the human manager is out of his management domain. How can he perform management tasks?

The operational scenario presented is similar to a burning house where the owner receives an email with the video/images of his house on fire. Since he is not there, he can do nothing but watch it burn! For that situation, our concept gives us a means to act fast on network incidents using autonomous management applications that act on behalf of the human manager. Let us see how.

NMS and NOSS are performing the tasks they are expected to carry out. Similarly, NUMS can collect network information from these stations through the LDAP interface which is supposed to be implemented. Each time a network incident occurs, an email is sent to an IMAP server (figure 8 (1)).

An autonomous management application, Dispatcher agent, can get the information by email (figure 8 (2)), analyze it and act accordingly. This means that the dispatcher can search the LDAP for an agent/service (figure 8 (3)) capable of solving the problem. Once the agent/service is found the dispatcher agent looks at the status of the agent, who, if online, passes all the information needed via IM to solve the problem (figure 8 (4/5)).

This means that autonomous applications can act directly on the network elements using SNMP/CMIP (figure 8 (6)), or go directly to a network element that hosts a particular service, using Telnet/SSH, and try to get it back up.

If the autonomous application cannot resolve the incident by itself, it may use the LDAP Server and look for other autonomous applications capable of solving the problem (figure 8 (3)), or look for a trouble ticket that the LMIB might have.

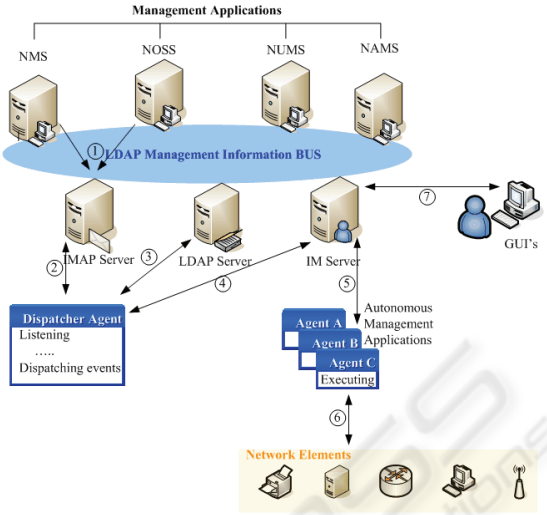

Figure 8: Autonomous applications using Instant Messaging and management tasks.

All of this is possible very simply. All management actors must have a standard way of communicating (LDAP queries or Instant Messaging) in order to share network management information at different management levels (Oliveira R., 1998).

5 SECURITY ISSUES

There is several security issues associated with IM services, such as:

Virus Attack

IM is an Internet-based tool incorporating "presence" and suffers from virus vulnerabilities common to other Internet applications. There are more than 200 IM-related viruses reported to date (Messaging Pipeline, 2004).

The effect of such virus attacks is more critical in the case of IM, where attacks can spread much faster as compared to e-mail based virus attacks. Also, the IM administrators need to react much faster to control IM based virus spreading.

Spim messages

Spam messages in IM context are referred to as spim messages. Unwanted spim messages can pop up anytime and momentarily disrupt work. As with e-mail spam there are anti-spim tools available to block the messages and allow users/agents to work free of uninvited interruptions.

Appropriate anti-spim tools need to be deployed at the user-end or the presence servers need to adopt the required measures to control spim messages.

Privacy
The user/agent's information should not be passed on or distributed to a buddy(s) if not permitted by the user/agent.

The presence information, if sent without permission, to agencies such as promotional products companies, can actually harm user interests.

6 CONCLUSION

Agents can publish their information on the corporate LDAP server and share it with others in order to make communication and services more sensitive and "personal". This information may include services, descriptions, supported languages, ontologies, addresses, as well the agent's status.

The LDAP protocol is the most widely adopted directory service. As a standard protocol, it can play an essential role in the integration of management applications in networked environment consisting of one or more administrative domains.

Instant Messaging has built up a substantial user base and is finding its place among other forms of communication such as telephony and email. It is near real-time and can offer degrees of efficiency and effectiveness that are not supported by voice and email. The most important aspect of IM which differentiates it from earlier systems is the integration of presence awareness, providing the ability to monitor the status of other users/agents on the network. The concept of the "buddy list" arose out of IM and is used in combination with presence.

A buddy list is a list of known users/agents whose presence is indicated. If a user/agent is online and available to receive a message an indicator is displayed to communicate this information to other users/agents who have subscribed to that user/agent's presence information.

Furthermore, there is an increasing trend toward extending presence to independent applications, not just human users, and enabling everything from automatic alerts and notifications to database queries via an instant messaging interface.

7 FUTURE WORK

Our next step will be to develop a content language which will allow autonomous applications to communicate with each other, as well Human User interaction.

The effect of presence on the network through the use of the XMPP protocol (P. Saint-Andre, 2004) (FIPA, 2002) is also the object of future work.

REFERENCES

Oliveira R., 1998. Gestion des Réseaux avec Connaissance des Besoins: Utilisation des Agents Logiciel, Ph.D Thesis, Ecole Nationale Supérieure des Télécommunications, January 1998.

Marques B., Nogueira E., Oliveira J., Oliveira R., 2004. "Ldap role in network management," 11th HP OpenView University Associations Workshop, Paris, June 2004.

FIPA, 2004. Agent Management Specification, SC00023K, 2004 http://www.fipa.org/specs/fipa00023/index.html

Jabber Software Foundation, 2006. http://www.jabber.org

Marques B., Oliveira J., Coelho P., Oliveira R., 2006. " Using LDAP for Network Topology and Service Management Applications Integration", WTC – World Telecommunications Congress, Budapest – Hungary, May 2006.

Coelho P., Marques B., Oliveira J., Oliveira R, 2005. "Using LDAP for Network Management Interoperability," Proceedings of the 12th HP OpenView University Associations Workshop, Porto, July 2005.

OpenLDAP Foundation, 2004. "Openldap schema specification: Extending schema," http://www.openldap.org/doc/admin22/schema.html, February 2004.

FIPA, 2004. Abstract Architecture Specification, SC00001L, 2004 http://www.fipa.org/specs/fipa00001/index.html

Messaging Pipeline, 2004. http://www.messagingpipeline.com/showArticle.jhtml ?articleID=51000335, October 2004

P. Saint-Andre, 2004. RFC 3921. Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence, October 2004

FIPA, 2002. Abstract ACL Message Representation in XML Representation, SC00071E, 2002 http://www.fipa.org/specs/fipa00071/index.html