Centralized Authentication and Speed up Approach for Clients of Multiple Multimedia Conferencing Systems Using Lightweight Directory Access Protocol

Dr. Ahmad Saleh Al-Sukkar
Amman Arab University
Jordan

Mohammad Abdelmo'ti Abu Saleh
Al Hussein Bin Talal University
Jordan

Abstract

Video conferencing systems are rapidly growing and spreading through various computing areas due to their benefits in efficiently producing communication between people from just about many different locations all over the world. One of the systems that is widely being used in Malaysia is the Multimedia Conferencing System (MCS). In ordinary cases, MCS users need to know the address of the server they have account on to be able to login and use the system. If that particular server is down or off-line users need to have a different account on a different MCS server to be able to use the system. we propose a new entity to be added in the MCS system, which is the LDAP server and directory. By using the centralized LDAP server for multiple MCS servers and redesigning the MCS server to communicate with LDAP, users can easily login through any server since their database will be located at the LDAP server and can securely be accessed from any other connected user of the MCS servers. LDAP does more than just providing authentications to users. The proposed system supported the users can easily login through any server that measurements in term of centralization risk and authentication of "log in" for MCS. On the other hand, the new MCS server design speeds up the invitations among users where they can discover each other faster based on the usage of the LDAP query and the use of centralized LDAP servers to distribute the load between Multiple LDAP servers. As a result, our approach proved that the time taken for the invitation process was less than that time taken through the old system.

1.1 Introduction

Recently, Multimedia Conferencing Systems (MCS) that become more popular as they are conducted through many suitable applications that require gathering distant people to make them virtually meet inside a virtual conference room/hall. Once people are connected together through these systems, they may visually interact with each other using video signals to carry their image animated data. This depends on the use of a webcam from a side and the screen from another side and vice-versa. People may also vocally interact with each other by using microphones that carry voice and sounds signals from one user of a speaker system to other user and vice-versa. People may further interact by exchanging documents between each other. All the above mentioned methods of communication can be combined with an online text exchange service, also known as chatting.

Multimedia Conferencing Systems (or MCS) are a revolutionary system that overcomes the obstacles of gathering distant people into one virtual room or hall for conferencing (Ramadass, S. and Abouabdalla, O., 1999). Another additional benefit of MCS is that it connects as many people as it can to communicate with each other, especially distant people. The MCS systems may connect people throughout the internet rather than the LAN/intranet (Garcia *et al*., 2001). In MCS, only authorized users are allowed to join the conference, this is called "Authentication". Currently there is no proper authentication in MCS. Nevertheless, this research has established a new idea, which involves leaving authentication process to separate entity and redesign the MCS server to be able to communicate with the new entity.

After doing research on authentication methods and systems, we found out that LDAP (Lightweight Directory Access Protocol) server is the appropriate solution to be used as the authentication entity. LDAP is considered to be as a set of directory services that provides a protocol and a data model for naming and authentication (http://en.wikipedia.org/wiki/Ldap, 2012). This approach for authentication requires a dedicated LDAP server and an interconnecting module to connect into the login interface in the MCS. As the user enters his credentials, these credentials will be passed to the LDAP server which will test them in the LDAP directory.

1.2 Problem Statement

In the current MCS, a user's information is stored in the MCS servers as plain text file. Users can only login to the server they had account on. If the MCS server is down, users will need to have account on another MCS server to be able to use such services. Moreover, when a user wants to invite a user from different server to a conference, he has to go through the user's lists in all other servers (one-by-one) in order to locate the user he is looking for. This invitation process will take a long time if the number of servers connected to one system is big. As an example, if the number of servers in a single system is 20, the user has to check 20 user lists (in worst case) to find and invite another user.

1.3 Motivation and Justification

When signing up, process is done on the same MCS system where all users are required to login into the same server, however, when making authentication using LDAP server, the authentication process will be centralized. Hence, any permitted user will connect to one MCS system that might login into that particular MCS by connecting the MCS to the LDAP server. Consequently, any user may be invited if he either has a name in the same MCS server or his name is registered in another server. Centralized authentication process will bring many benefits for example, the user will have to have only one unique username, and thus, the time consumed to set up a new account for MCS system will be minimized. This research will concentrate on redesigning the MCS server to be able to communicate with LDAP server.

1.4 Objectives of the Research

In this research, the objective comprises redesigning current MCS for faster invitation among users**.** Use one single user name and password to login and use MCS services.

1.5 Scope of the Research

This research overcomes the problem of creating multiple accounts for the same user in multiple MCS servers. It concentrates on providing central and authentication for MCS users. It will also enhance the speed of inviting users from multiple MCS servers to a video conference. Other services for MCS users are outside the scope of our research even though the proposed solution may enhance other services provided to MCS users.

1.6 Contributions

Several studies have discussed the issue of using LDAP as directory service and authentication entity. Some of these used an integrated approach while others focused on specific features and functionalities that LDAP can provide. The main contribution of this research is to redesign and implement the new MCS server that is able to communicate with a centralized authentication entity (LDAP server) which will result of MCS users will use one single user name and password to login and use MCS services and faster invitation among users.

1.7 Research Methodology

The following highlighted steps are a base for research procedures of this research:

- Analyzing Multimedia Conferencing System (MCS).
- Investigate and search for centralized authentication method or system suitable for MCS.
- Analyzing the new centralized authentication method or system.
- Designing interconnectivity between MCS and the new centralized authentication method or system.

2-Background and Literature Review

2.1 Multimedia Conferencing System (MCS)

Video conferencing systems are divided into three types: point-to-point, point-to-multipoint and multipoint-to-multipoint as showing in Figure 2.1. In the point-to-point conventional communication, both ends should use ISDN WAN links. This type of Video conferencing system has some setbacks such as: communication is only point-to-point and WAN link has to be dedicated for video conferencing only. In the point-to-multipoint video conferencing system, it becomes possible for more than two ends to communicate at the same time using a Multipoint Conference Unit (MCU). However, WAN links should be dedicated for video conferencing and additional WAN links should be found if one end wants to send data and emails as well as conducting a video conference; in addition the WAN bandwidth needs to be increased according to the multipoint ends linked to the conference (mlabs, 2009).

MCS is a multipoint-to-multipoint video conferencing system. This system is considered to be the most efficient conferencing system (Ramadass *et al*., 1995). It allows holding conferences to as many people as required from any point of the world as it uses the existing LAN infrastructure (mlabs, 2009). Hence, ISDN lines and cabling are no more required. Moreover, the required bandwidth remains constant apart from number of the participants.

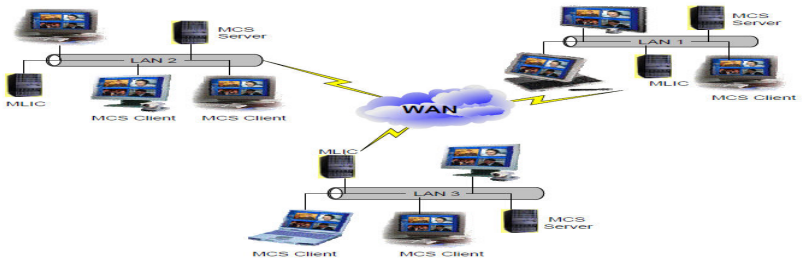

Figure 2.1: Multipoint-to-multipoint Systems (Mlabs, 2005)

MCS is based on distributed network entities architecture and uses RSW control criteria to as a control mechanism. The main MCS entities are:

- The MCS server entity.
- The MCS client entity.
- The multilan IP converter (MLIC) entity as showing in Figure 2.2.

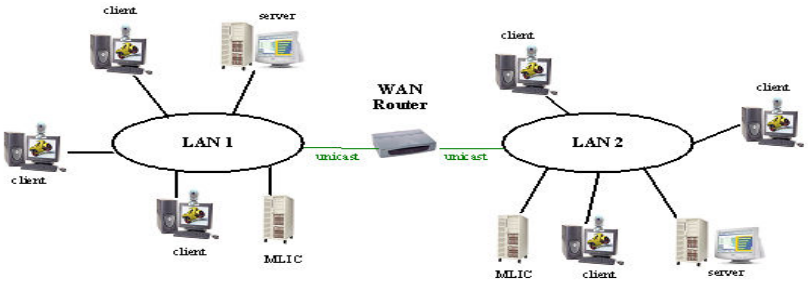

Figure 2.2: MultiLAN with MLIC (Saravanan and Sureswaran, 2000)

2.2 Reflector Server

The reflector entity is to provide a platform for centralized data sharing and communication among all reflector server entities, by combining and monitoring the sites with better and optimized messaging and files distribution. In a multi-server architecture, servers may not be able to always communicate directly and exchange data among themselves. This can be due to, for example, limited processing capacity (for frequent file exchanges and updates), network limitation (e.g., disjoint networks or limited network capacity), and connectivity problems (e.g., uncooperative service providers or security issues). Therefore, servers in our proposed solution communicate and exchange files through the reflector (star topology). This reflector is mainly used for minimizing inter-server communication and server monitoring as well.

Some MCS network has a reflector server. This reflector is connected with all MCS servers. In this type of network, the clients in server A can connect with sever B through this server by manually searching for certain clients in different servers. When a user requests the list of users of other servers through a reflector server, the user will choose the other side from this list. Figure 2.3 shows this type of network.

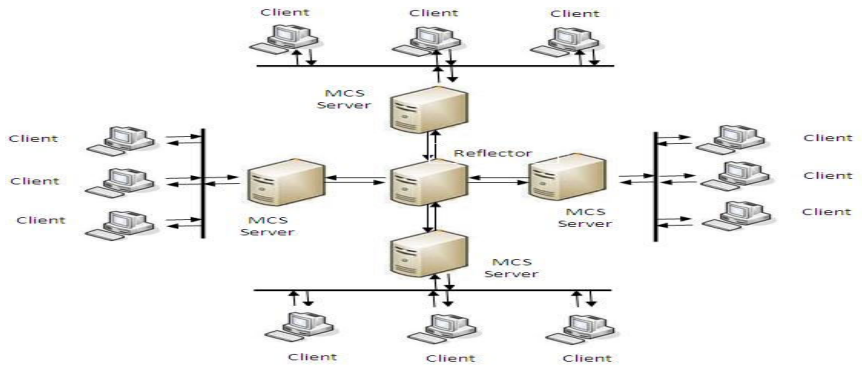

Figure 2.3: MCS Network with Reflector Server

2.3 Lightweight Directory Access Protocol: History and Future

The protocol LDAP is a standard for facilitating accessing directory services. It was derived from OSI X.500 model, namely (DAP). LDAP is better than DAP where it is accessed via the simpler TCP/IP instead of OSI stack. LDAPv3 includes an important security enhancement. The LDAP provides a protocol and a data model for naming and authentication. The main function of LDAP servers is to answer queries. The LDAP information model is also called the LDAP schema where it provides unique names by providing a name from a node to a root.

LDAP directory is accessed via authentication, queries and update operations. Access control lists (ACL's) manages accessing data under authorization. (Jill Gemmill *et al*., 2005). There are common applications for the LDAP. One of these applications comprises querying and modifying directory services running over TCP/IP .A directory can be imagined as a group of objects with related attributes organized logically or hierarchically. Depending on the model chosen, an LDAP directory tree is bounded according to politics, geography and/or organization. The most used structure for LDAP is the Domain Name System (DNS) for organization the uppermost levels of the tree or hierarchy. The deeper leaves in the LDAP tree may represent any particular object, such as: PCs, people, documents or anything representing a tree entry (or multiple entries). The current version of LDAP is LDAPv3 which is a version that accumulates previous versions and its specifications and requirements to be defined in a series of the Internet Engineering Task Force (IETF) standard track Requests for Comments (RFCs) (http://en.wikipedia.org/wiki/Ldap , 2012).

The directory services known as X.500 were based on the X.500 Directory Access Protocol (DAP). In the matter of fact, they need the Open Systems Interconnection (OSI) protocol stack. The LDAP directory servers lately replaced the X.500 directory servers as they support both DAP and LDAP, besides, the OSI suite is provided. Currently, X.500 directory protocols including DAP are used directly over TCP/IP as shown in Figure 2.4.

The LDAP protocol was created by the University of Michigan (Timothy Howes *et al*., 2003). Earlier, this protocol was known as a Lightweight Directory Browsing Protocol (LDBP). It was renamed after adding directory updating functions in addition to directory browsing and searching functions. Moreover, this protocol has also influenced X.500 upcoming Internet protocols, including XML, XED, DSML, SPML and SLP (Amrita *et al*., 2007).

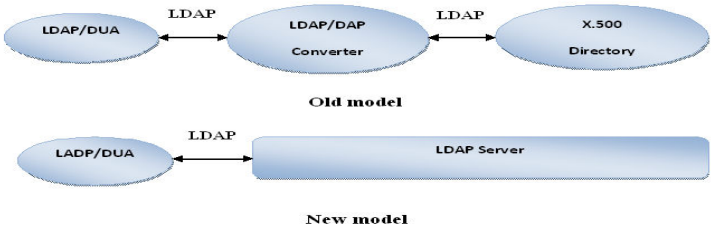

Figure 2.4: An old model and a new model of the LDAP server (Amrita *et al*., 2007)

2.4 The LDAP Framework

LDAP operations are based on the client–server model. Each LDAP client uses the LDAP protocol, which runs over TCP/IP, to retrieve data stored in a directory server's database. LDAP clients are either directly controlled by an LDAP installed server or managed by an LDAP collaborating application. Figure 2.5 gives an overview of the LDAP framework in which many devices (such as printers and routers) and servers (such as mail servers) can access the data being stored in a given LDAP server database. LDAP client's accessing\ LDAP servers should be authorized through authentication mechanisms which can implement various security protocols. replication in which a primary LDAP server (master) sends updates to a read-only Replica server (slave) is common among collaborating LDAP servers. Two components are crucial to the LDAP framework: the LDAP-tailored database, or the directory.

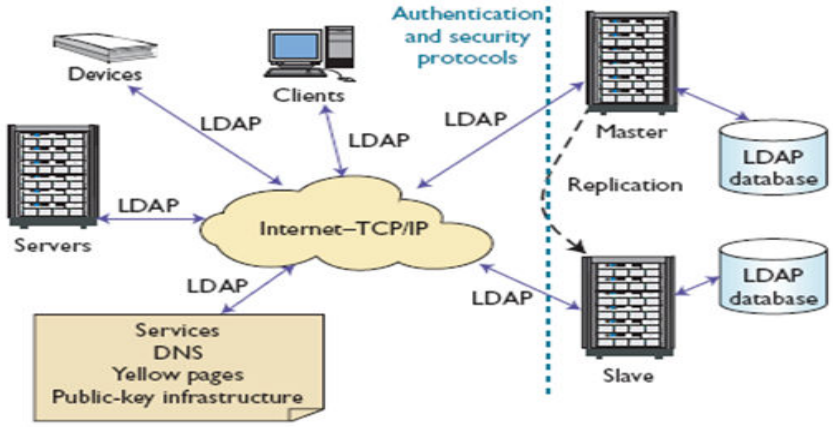

Figure 2.5: LDAP Framework (Qadeer *et al.*, 2009)

3-Centralized Authentication for MCS

3.1 Research Procedures

First of all, the authentication process in existing MCS system will be separated in a single module. Normally, the authentication process is done by using a user form which calls a function to check the availability of a password. If a user has an account in a certain MCS server, he should be able to sign in another MCS server in another location with the same username and password. In ordinary cases, the user has to create a new account for every new MCS server in order to start a conference with users registered on the new MCS server. Therefore, the suggested system will be illustrated in the following Figure 3.1.

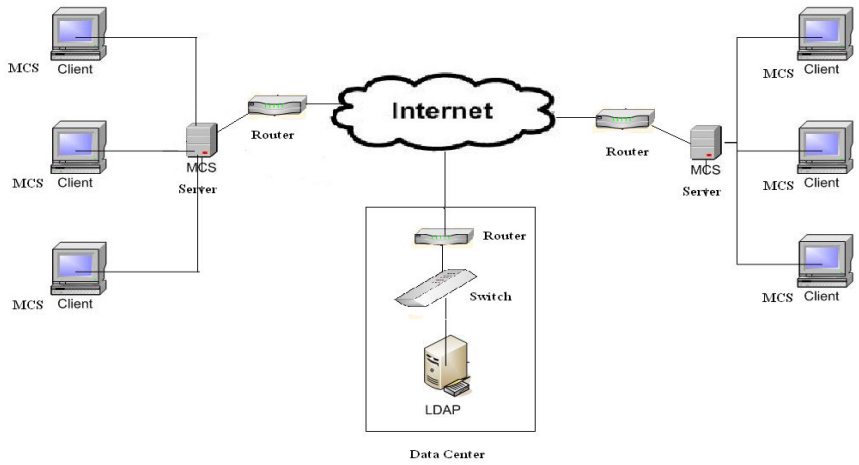

Figure 3.1: LDAP & MCS Suggested Solution

In the above-mentioned figure, there is a unique LDAP server, LDAP directory and several MCS servers, which have access over the Internet using a TCP/IP secure link. Accordingly, every user will have a unique username and password combination that can be used to login and get connected to several MCS systems and thus several users in different MCS systems.

3.2 Theoretical Framework

The suggested framework is to build a system model that act as a cooperative system between a reliable MCS server and the LDAP server. The new model will be part of the MCS server. The MCS should contain a user form to obtain the username from a user or other application within the MCS system, which will hand the username and password to the application who in turn will be the client of the LDAP server. The LDAP server in turn will perform the required operations on the LDAP directory. The connection between client, which is the application that will contact LDAP server and the server should be itself is authenticated with administration permissions in order to perform functions on LDAP directory. In this research, the authentication process is studied. However, other types of operations and other ideas in utilizing the best of LDAP technology may be dealt with. Therefore, the assumed system model will concentrate on authentication process.

In the authentication process, the MCS system will use the LDAP lightweight directory to authenticated users by verifying username and password using several LDAP operations. First of all, it should be clear that there is no way to manipulate LDAP directory rather than negotiating the server which will indirectly translate the clients request in a secured manner using its built-in encryption over a secured connection procedures. Secondly, MCS and LDAP technologies should be used as two separate technologies. We prefer that MCS and LDAP should not be mixed in a single server, this is to avoid that when the server goes down other MCS servers will not be able to authenticate other users. Another issue is to facilitate handling failures and detecting error sources and also by adopting this idea, the data hiding concept in object oriented models will be useful to hind any chances of compromising the users' database. In this case, it is the LDAP directory. Figure 3.2 below should clarify the suggested framework.

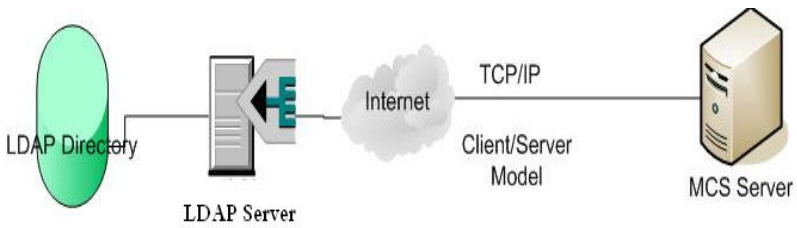

Figure 3.2: Framework between LDAP and MCS

3.3 Connection Requirements between LDAP and MCS

In order to establish a reliable connection between LDAP and MCS, the following requirements should be taken into consideration:

- MCS authentication interface should be secured from the brutal force technique that may threaten the security of the LDAP directory. For instance, the form or application should not provide information that may help attackers to utilize hacking software that generate possible values of passwords.
- MCS system should contain a map of the LDAP directory in order to facilitate operating the LDAP server efficiently.
- MCS should be separated from LDAP server and directory to enforce security by data hiding. Therefore, they should not be on the same machine.
- TCP/IP support by MCS as LDAP utilizes the TCP/IP suite for making a client/server connection.

3.4 Connect LDAP to MCS

The solution of the research should be divided into two sets of procedures that run over a TCP/IP connection for a client/model. At the client, which is the MCS system, the following procedures (LightYear Design, 2009) has to be done on the MCS login screen:

1. Validate username and password format masks
2. Submit username and password
3. Post IP address and time stamp

On the other hand, the following sequence lists the procedures that happened for authentication :

1- Connect
2- Bind
3- Verify binding
4- Search for username
5- Create Result Set
6- Search for password
7- Check the group of the user
8- Create session
9- Bind user; and by the end of the session…
10- Unbind

In more details, the authentication will be handled as in the following sequence:

1. Connect to LDAP server
2. Binding to LDAP server
3. Verifying Binding
4. Searching for the account name in the directory tree
5. Creating result set

   a. If the bind failed it means that the user could have typed in the wrong ID or password.
      i. Display login form again.
   b. If the account exists, attempt a bind with it.
      i. Check the groups that the user is a member of and see if the specific group is in the list.
      ii.
         1. If the user is a member of the group, a session will be created and then returns true.
         2. Else could not bind, so display an error message and the login form.
6. Unbind from the resource account.

Nevertheless, the following steps specify the actions to be handled for the user form just before the execution of the above mentioned steps. The location of the LDAP is broken down into the following procedures: first of all, removing special characters wrongly inserted by users. Secondly, the form variables will be set up. Thirdly, the IP Address and the User Agent information will be gotten.

Fourthly, the Timestamp will be gotten as well based on two cases. The first case is that if a user has valid credentials and has created a new session variable with the user name, then the login is successful where the user will be redirected to the protected page. Otherwise, in the second case, if a user has no valid credentials and has not created a new session variable with the user name, then the login is no longer to be successful where the login form will be displayed again and an unbinding will occur.

4-Implementation and Testing

4.1 Time Testing Scenario using One Centralized LDAP

In the first scenario, we created a conference and invited 3 users from a local server and 3 users from remote servers (each remote user from different server). As shown in Table 4.1, the number of users started from 100 users up to 1000 users. The access time for MCS with reflector was 122 seconds when tested with 100 users in MCS database, where the access time for MCS with LDAP was 98 seconds. For 1000 users, the access time for MCS with reflector was 423 seconds, where the access time for MCS with LDAP was 398 seconds. We conclude from this that the access time for the new MCS architecture (with LDAP) was faster than the access for the old MCS architecture (with reflector only). In addition, the access time for both the reflector and the LDAP maintained their increase while the number of users was increasing.

Table 4.1: Access time result testing for scenario 1 using single LDAP

Number of user's in DB	Access time in Seconds for MCS with reflector	Access time in Seconds for MCS with single LDAP
100	122	98
200	161	154
300	198	184
400	236	223
500	275	245
600	294	275
700	332	301
800	361	332
900	397	366
1000	423	398

In the second scenario, we created a conference and invited one user from a local server and one user from a remote server. As shown in Table 4.2, the number of users started from 100 users and increased by 100 users for every test up to 1000 users. The access time for MCS with reflector was 55 seconds when tested with 100 users in MCS database, where the access time for MCS with LDAP was 23 seconds. For 1000 users, the access time for MCS with reflector was 213 seconds, where the access time for MCS with LDAP was 189 seconds. We conclude from this that the access time for the new MCS architecture (with LDAP) was faster than the access for the old MCS architecture (with reflector only). In addition, the access time for both the reflector and the LDAP maintained increasing when the number of users was increasing.

Table 4.2: Access time result testing for scenario 2 using single LDAP

Number of user's in DB	Access time in Seconds for MCS with reflector	Access time in Seconds for MCS with single LDAP
100	55	23
200	67	43
300	78	56
400	99	69
500	112	87
600	130	111
700	153	123
800	168	134
900	190	156
1000	213	189

In the third scenario, we created a conference and invited one user from a remote server. As shown in Table 4.3, the number of users started from 100 users and increased by 100 users for every test up to 1000 users. The access time for MCS with reflector was 46 seconds when tested with 100 users in MCS database, where the access time for MCS with LDAP was 18 seconds. For 1000 users, the access time for MCS with reflector was 245 seconds, where the access time for MCS with LDAP was 204 seconds. We conclude from this that the access time for the new MCS architecture (with LDAP) was faster than the access for the old MCS architecture (with reflector only). In addition, the access time for both the reflector and the LDAP maintained their increase while the number of users was increasing.

Table 4.3: Access time result testing for scenario 3 using single LDAP

Number of user's in DB	Access time in Seconds for MCS with reflector	Access time in Seconds for MCS with single LDAP
100	46	18
200	75	42
300	90	69
400	123	98
500	134	102
600	156	123
700	178	140
800	190	160
900	213	196
1000	245	204

The 3 scenarios represent Figures 4.1, 4.2 and 4.3, respectively. It was shown from these figures that the new MCS architecture (using LDAP) access time was faster than the access time of the old MCS architecture (using reflector only). This maintained the scalability of our system. Furthermore, note that the increase was maintained when the number of users was increased.

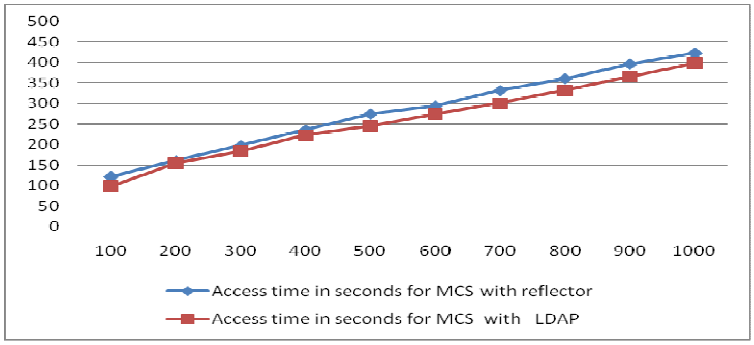

Figure 4.1: Access time result testing for scenario 1 using single LDAP

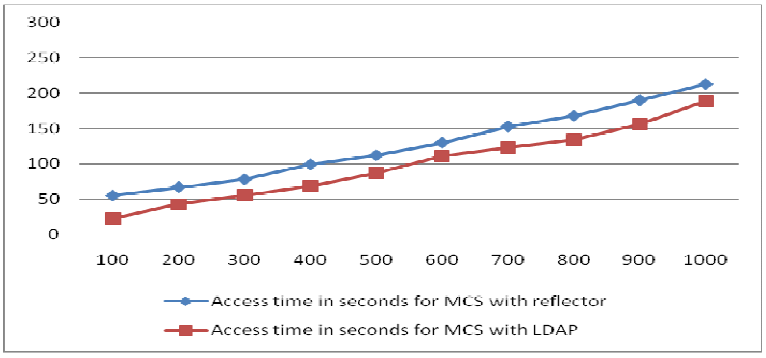

Figure 4.2: Access time result testing for scenario 2 using single LDAP

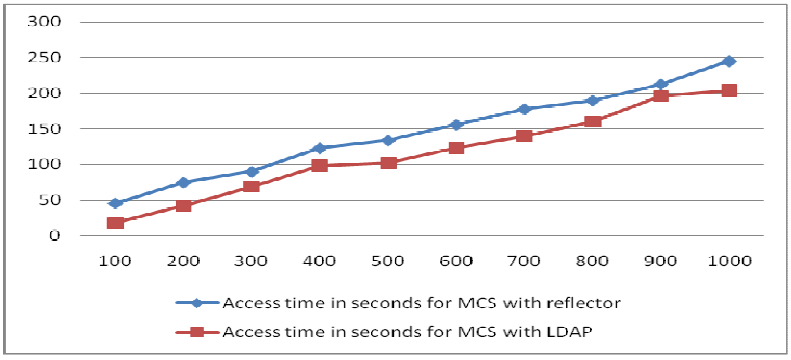

Figure 4.3: Access time result testing for Scenario 3 using single LDAP

4.2 Summary

The testing result clearly shows that using the new MCS architecture that includes LDAP as a new entity for authentication and user information query speeds up the process of inviting users to an MCS conference. The authentication process could not be measured since current MCS did not support authentication in its proper format. After the centralized LDAP had been used, the delay of time was efficiently reduced.

References

GARCIA, E. & LAPAYRE, J. & SURESWARAN, R. & THARMARAJ. (2001) Centralized or Distributed Algorithm for Concurrency Management in Multimedia Conferencing System. In: Proceedings of Asia Pacific Advanced Network Conference 2001: Penang. P.108-119.

JILL GEMMILL & JASON, L. & W. LYNN. (2005) Directory Services Middleware for Multimedia Conferencing [Online]. [07th Jan 2010] Available from World Wide Web: <http://metric.it.uab.edu/vnet/cookbook/v2.1/index.html>.

LightYear Design (2010) [Online]. [14th Jan 2010] Available from World Wide Web: <http://lightyeardesign.com/2009/06/ldap-and-php-login-script>.

MLABS. (2005) MCS Ver. 6.0, multimedia conferencing system. System discretion, Multimedia Research Lab Sdn. Bhd. Malaysia. [Online]. [25th Feb 2010]. Available from World Wide Web: <http://www.mlabs.com.my/WhitePaper.htm>.

QADEER, A. MOHAMMED & SALIM MOHAMMAD & AKHTAR M SANA. (2009) Profile Management and Authentication Using LDAP. Computer Engineering and Technology, ICCET '08, International Conference on Singapore IEEE.

RAMADASS, S. & ABOUABDALLA, O. (1999) A Server recovery procedure to manage distributed network entities for multimedia conference system *Proceedings* WEC 99 Subang Kuala Lumpur, Malaysia.

RAMADASS, S. & SUBRAMANIAM, R. K. (1995) A control criteria to optimize collaborative document and multimedia conferencing bandwidth requirements. In: Proceedings of IEEE Singapore International Conference on 'Electrotechnology 2000: Communications and Networks'. Singapore. P.555-559.

SARAVANAN, K. & SURESWARAN, R. (2000) A Bi-Directional Multicast Tunneler to Support the distributed Multimedia Conferencing Environment Architecture. Proceedings of of IWS (Internet Workshop on Asia Pacific Advanced Network and its Applications). Tsukuba, Japan. P.135-139.

TIMOTHY A. HOWES & MARK C. SMITH. & GORDON S. GOOD (2003) Understanding and Deploying LDAP Directory Services. 2nd Edition.

Wikipedia: LDAP. (2012) [Online]. [05th April 2012] Available from World Wide Web: <http://en.wikipedia.org/wiki/Ldap>.