

CORBA

(辛英美)

()

1999

CORBA

A CORBA-based Secure Session Service for Distributed Multimedia Collaborative Environments

A CORBA-based Secure Session Service for Distributed Multimedia Collaborative Environments

by

Young-Mi Shin

Department of Computer Science and Engineering

Pohang University of Science and Technology

A thesis submitted to the Pohang University of Science and Technology in partial fulfillment of the requirement for the degree of Master of Science in the Dept. Computer Science and Engineering.

Pohang, Korea

December 15, 1998

Approved by

Major Advisor

CORBA

.

1998 12 15

()

()

()

, Young-Mi Shin, A CORBA-based Secure Session Service for Distributed Multimedia Collaborative Environments, MCS 9725M17 CORBA, Department of Computer Science and Engineering, 1999, 52P, Advisor: J. Won-Ki Hong, Text in Korean.

ABSTRACT

Distributed multimedia applications are being developed and used for many fields of our lives today. There is a vast amount of single-purpose application software available, such as video audio conferencing, chatting, whiteboard, electronic notebook, and so on. The goal of distributed multimedia application is to exchange multimedia information among users. With these distributed multimedia applications, we can realize a collaborative environment that allows a group of users to collaborate from their desktops as effectively as if they were face-to-face.

In order to provide an effective collaborative environment, it needs to be secure and platform-independent. Moreover, the collaborative environment has to support facilities for creating, eliminating, joining, and leaving collaboration sessions. The service that serves these facilities is called a session service. OMG CORBA allows applications to communicate with one another no matter where they are located or who has developed them. So we use CORBA to realize our session service.

This thesis proposes a CORBA-based secure session service for multimedia collaborative environments. This secure session service is platform-independent, enhances the security and offers a session information generically. As a proof of concept, a secure session service has been developed as part of a CORBA-based distributed multimedia system called MAESTRO. Our secure session service can be proposed as a new Common Object Service in the OMG standard.

1	1
2	4
2.1	4
2.1.1	MBONE	4
2.1.2	NetMeeting	6
2.2	8
2.3	9
2.4	- SESAME.....	9
2.5	CORBA Security Service.....	11
2.5.1	11
2.5.2	CORBA	12
2.5.3	CORBA	12
2.5.4	13
2.5.5	CORBA	14
2.6	MBONE	15
2.6.1	(stream)	15
2.6.2	16
2.6.3	16
3	18
3.1	18
3.2	19

4	CORBA	21
4.1		22
4.2		23
4.2.1	가	23
4.2.2		25
4.3		29
5	CORBA	30
5.1		30
5.2		32
5.3		33
5.3.1	(authentication)	33
5.3.2		34
5.3.3		35
6	CORBA	37
6.1	MAESTRO	37
6.2	MAESTRO	39
6.2.1		40
6.2.2	MAESTRO	40
6.2.3		40
6.2.4		40
6.3		41
6.3.1		41
6.3.2		42
6.3.3		42
6.3.4		42

7	44
	46
1:	50

1: MBONE	(topology).....	5
2: MBONE	(Sdr)	5
3: ILS	7
4: SESAME.....		10
5: ORB	14
6:	16
7:	23
8:	26
9:	27
10:	33
11: MAESTRO	38
12:	41
13:	42

1

가 , , ,
가 가

[1, 2, 3].

,
,
가
(collaborative environment)

, 가
[4, 5, 6]

가

~~가~~ , 가
, 가

가

~~가~~ ,

~~가~~

가

가

가

가

[7],

가

가

[8],

[7]

가

가

가

Common Object Request

Broker Architecture (CORBA)

. CORBA [9]

가

가 CORBA

가

CORBA

가

가

(COSS) [10]

CORBA Common Object Services Specification

2

, CORBA COSS

. 3

. 3

4 5

. 6

. 7

2

CORBA

가

, CORBA

Common Object Services Specification (COSS) [10]

2.1

[7, 8, 11, 12] , 가
UNIX MBONE [7] Windows 95 NT
NetMeeting [8]

2.1.1 MBONE

MBONE (Multicast Backbone) [7, 13, 14]

IP

가

. 가

(tunneling)

가

(mrouter

)

가

IP

mrouter

unicast IP

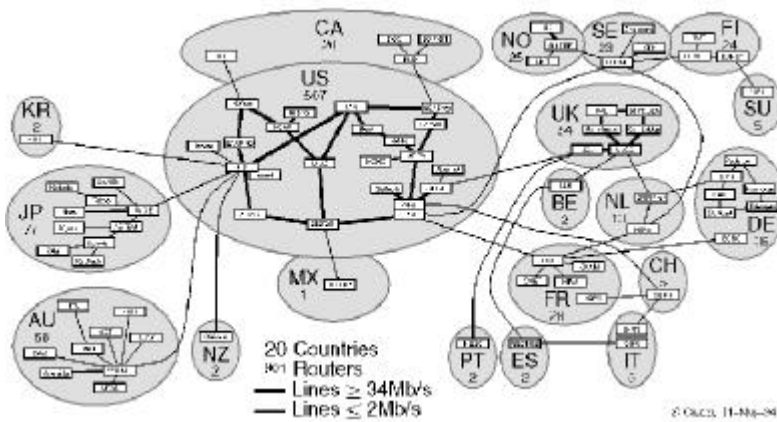
unicast

가

. MBONE IP

. 1 MBONE

가

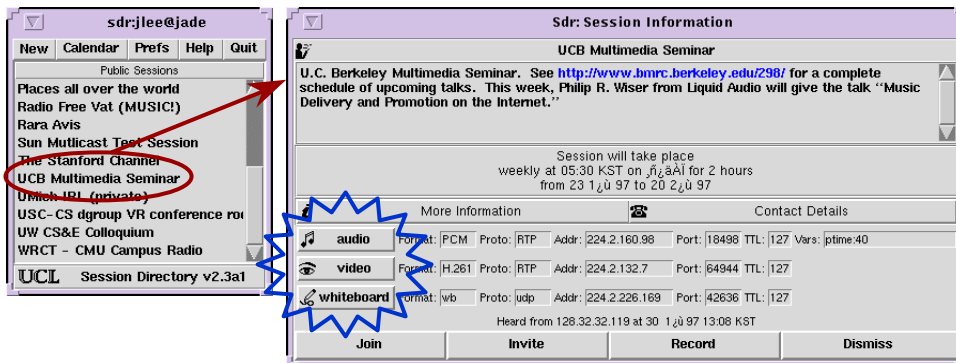


1: MBONE (topology)

MBONE

- (session directory),
 - (audio reference tool),
 - (video conference tool),
 - (whiteboard)
- (Sdr) [7]

, 가 , MBONE
 가
 가



2: MBONE (Sdr)

MBONE Session Announcement Protocol (SAP) [15], Session Description Protocol (SDP) [16], Session Initiation Protocol (SIP) [17] 가

SAP

가

가

가

가

(local cache)

가

SDP 1998 4 RFC 2327

가

. SDP

SIP

2.1.2 NetMeeting

NetMeeting [8]

Windows 95 NT

가

가

가

NetMeeting 가
(chat system), (whiteboard), (audio/
video conferencing)

NetMeeting (connection)

Internet Locator Service (ILS) [18], IP

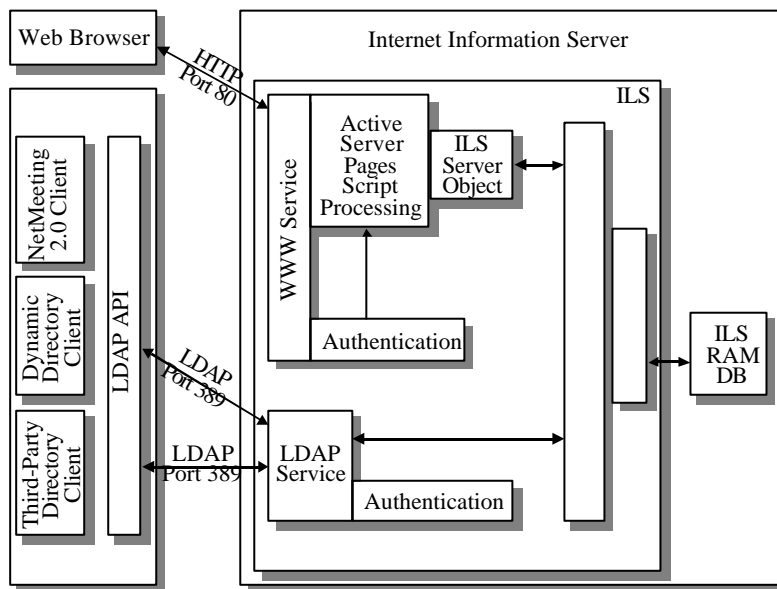
IP

ILS

ILS

NetMeeting IP (mapping)

NetMeeting 가 NetMeeting
, ILS 가 IP



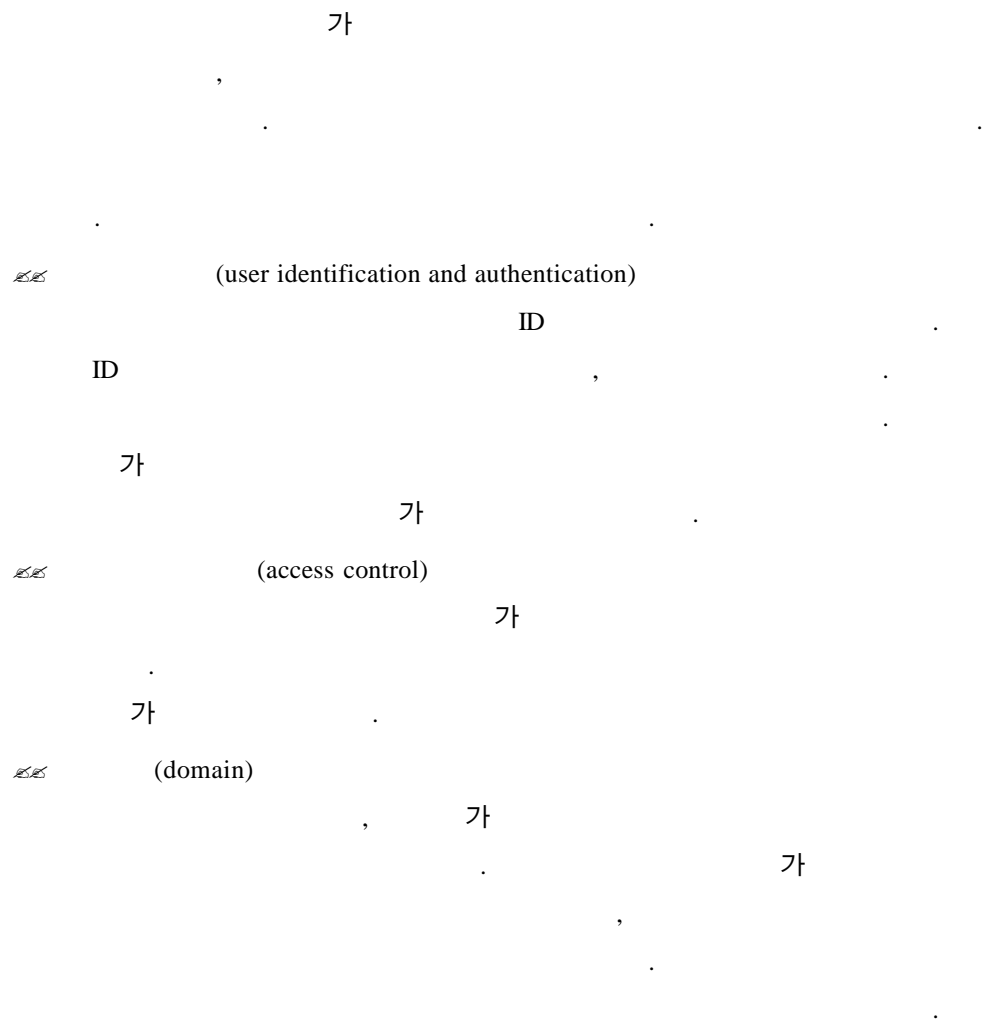
3: ILS

3 ILS . ILS
 . 가
 , IP ILS . ILS
 가, 가 , (entry)
 . ILS Lightweight Directory Access Protocol (LDAP) [19]
 ILS .
 ILS 가
 . ILS , 가 ILS
 .

2.2

(operation) .
~~///~~ (confidentiality) : .
~~///~~ (integrity) :
 .
 가 .
~~///~~ (availability) :
 .
 가 가 ,
 가 , 가
 .
 가 ,

2.3

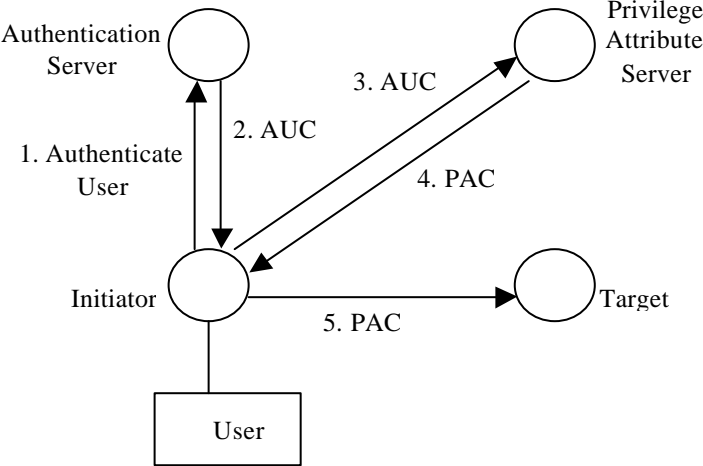


2.4

- SESAME

Secure European System For
Application in a Multivendor Environment (SESAME) [20, 21] . SESAME
, Multi-domain
SESAME

European Computer Manufacturers Association (ECMA)



4: SESAME

SESAME 4
 (authentication server) (privilege attribute server)
 AUC (:
 Authentication Certification) (privilege
 attribute server) AUC PAC (: Privilege Attribute
 Certificate) (initiator)
 PAC (target)
 PAC (access control
 list)
 PAC
 . PAC

SESAME
 (heterogeneous)

SESAME

가 가 ,

2.5 CORBA Security Service

CORBA [9] 가

. CORBA

가

, Common Object Services

Specification (COSS) [10]

. COSS

가

2.5.1

가

~~가~~

가

~~가~~

가

/

가

~~가~~

가

가

2.5.2 CORBA

CORBA 가

~~ㄷ~~ (information compromise)

가

~~ㄷ~~ (integrity violations)

가

가

~~ㄷ~~ (denial of service)

가

가

2.5.3 CORBA

CORBA

[10]

CORBA

~~ㄷ~~ (identification)

(authentication)

~~ㄷ~~ (authorization)

(access control)

가

~~ㄷ~~ (security auditing)

가

(method)

가

☞☞ (security of communication)

CORBA

가 가

(integrity)

(confidentiality)

☞☞ 가 (non-repudiation)

가 ,

☞☞ (administration)

가 .

2.5.4

(security reference model) CORBA

, CORBA

(meta-policy)

가 ,

가

COSS

, , (auditing), (delegation),
가 (non-repudiation)

ORB

가 가 가 5 . Object Request

Broker (ORB)

가

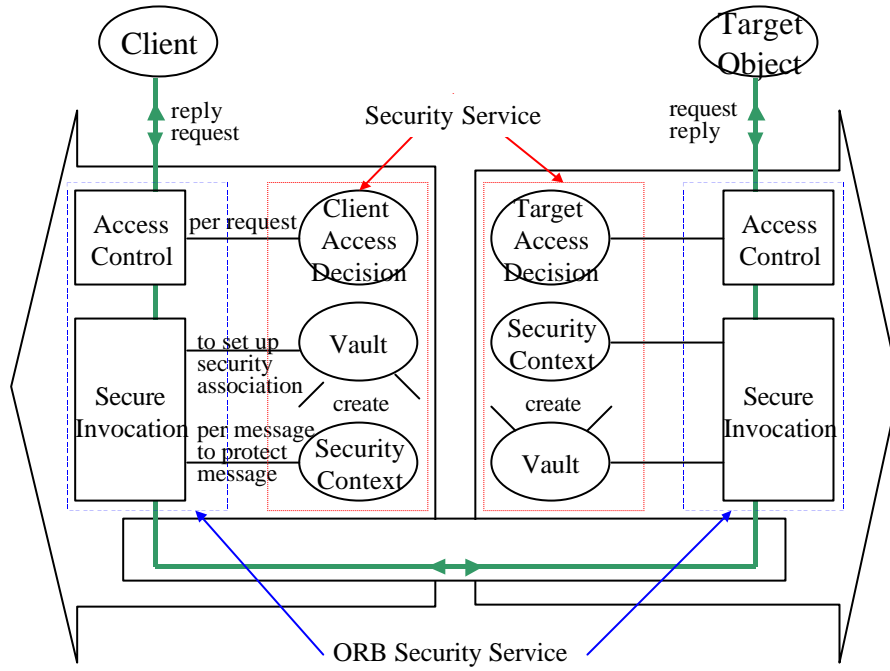
(auditing)

Secure Invocation

가

. Vault

Security context



5: ORB

2.5.5 CORBA

가

1: , 가

2 : 가

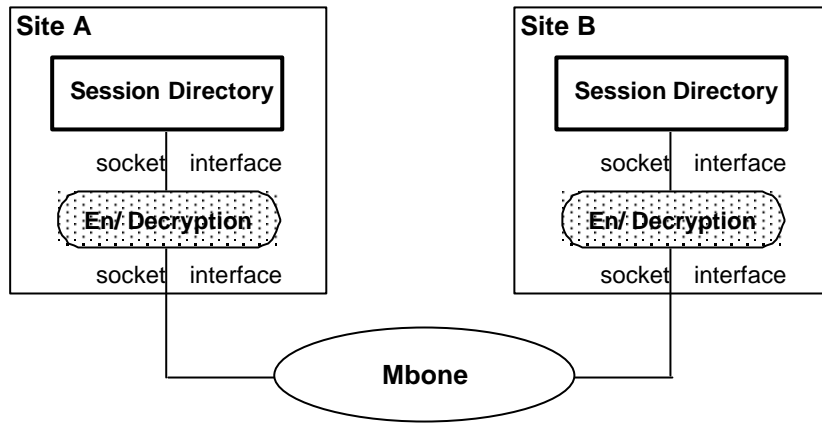
2 1 가

2.6 MBONE

MERCI [22] [23]
MBONE [7] . MBONE
가 . 가
가 MBONE (Sdr)
Session Announcement Protocol (SAP), Session Initiation Protocol (SIP)
가
가 가 ,

2.6.1 (stream)

가 . 가
가 .
(module) .
가 가
가 가
MBONE



6:

2.6.2

MBONE

, MBONE Session Announcement Protocol (SAP), Session Initiation Protocol (SIP) (format)

2.6.3

MBONE

Secure Conferencing User Agent (SCUA) [24]

가

. MICE [25]

ICE-

TEL [26]

Pretty Good

Privacy (PGP) [27], Secure/Multipurpose Internet Mail Extensions (S/MIME) [28],
MIME Object Security Services (MOSS) [29] SCUA

3

, 가

가

가

가

가

,

가 가

3.1

~~가~~

,

~~가~~

가

~~가~~

가

가

~~ㄱ~~

가

가

가

~~ㄱ~~

가

~~ㄱ~~

3.2

가

가

~~ㄱ~~

(authentication)

~~ㄱ~~

(access control)

가 가

가

~~ㄱ~~

(confidentiality)

가

가

~~EE~~

(integrity)

4 CORBA

3

가

[7],

[7, 8].

가

가

가

가

가

CORBA [9]

가

Common Object Services

Specification (COSS) [10]

CORBA

가

CORBA

가

가

COSS

4.1

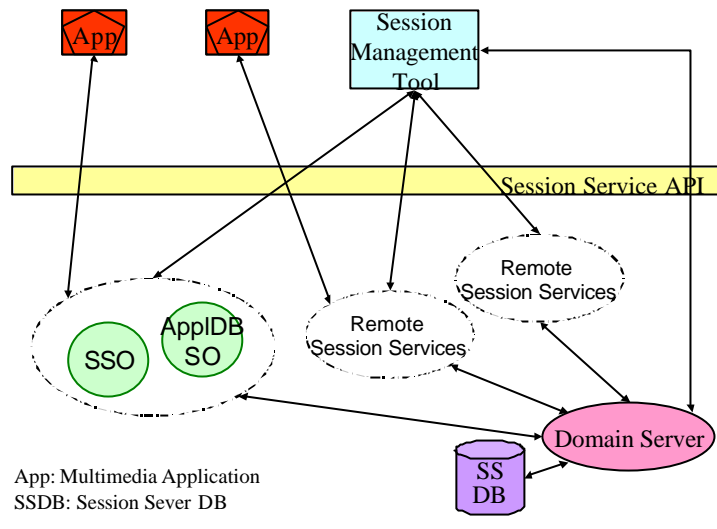
, 4.2

, 4.3

Rose [31]

4.1

가 , 가
 , ,
 , .
 .
 , .
 .
 ,
 가 가
 .
 가 .
 ,
 가 가 , 가 .
 .
 7 .



7:

(SSO)

(AppIDBSO)

CORBA

CORBA

가

4.2

가 가

4.2.1

가

가

가 가

. 가 가 . 가

~~가~~

, 가 ,

, 가 , 4.2.2 .

~~가~~

가

가 가
가

, ,

가 . CORBA

Any

Any
가

Any

Any pseudo CORBA:: 가 가

```

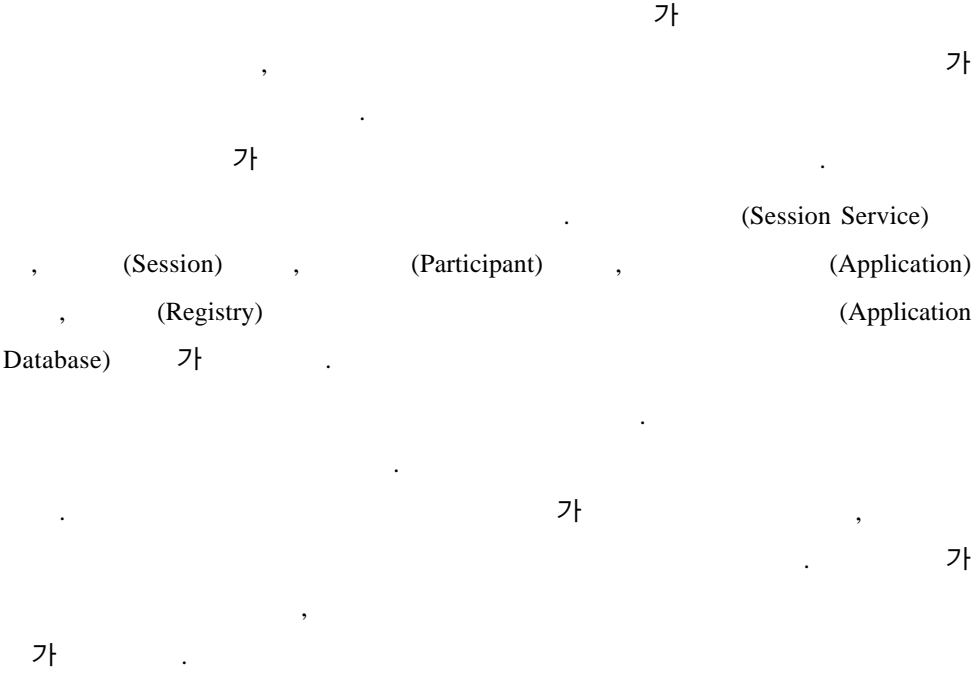
struct RegisterInfo {
    int port_num;
    char* domain;
    char *name;
}

CORBA:: Any a_info;
RegisterInfo info;
instantiate info;
a_info << info;
register a_info into Session Service

CORBA:: Any a_info;
RegisterInfo info
get a_info from Session Service
*a_info >>= info;
use a_info

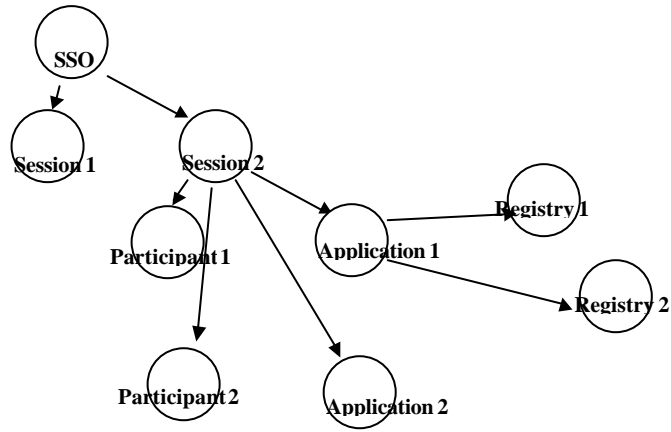
```

4.2.2



가

8



8:

(SSO)

가

CORBA:: Any

가

가

CORBA

가

Rose

9

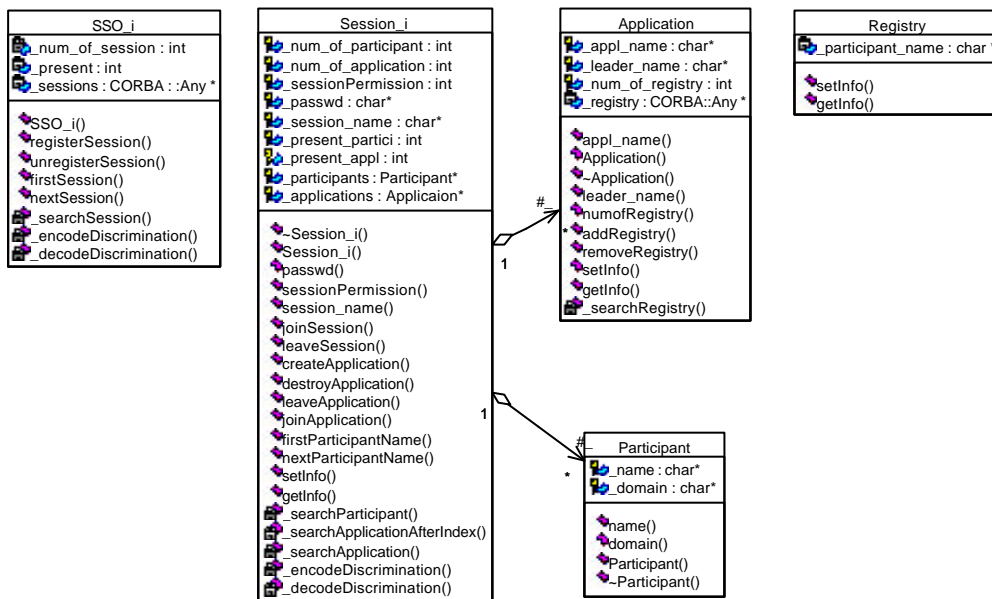
(SSO_i)

(Session_i)

가

가

CORBA::Any



9:

2525

가

CORBA

CORBA

IDL

가

가

가

CORBA Interface Definition Language (IDL)

~~///~~

CORBA

, 가
, 가

가

~~///~~

~~///~~

~~///~~

가

~~///~~

가

가

가

CORBA

가

가

4.3

가 가

가

5 CORBA

3

[23].

4

가 CORBA

5.1

5.2

, 5.3

5.1

(authentication)

(authorization)

가

가

(auditing)

CORBA

가

, CORBA

가

가

가 , 가
가 , 가 가

가

CORBA
CORBA ORB , ORB
가 . CORBA
(multi-thread)

(mutual exclusion)

~~가~~

가

가

~~가~~

~~가~~

가

가

~~5.1~~

~~5.1~~

~~5.1~~

~~5.1~~

가

5.2

5.1

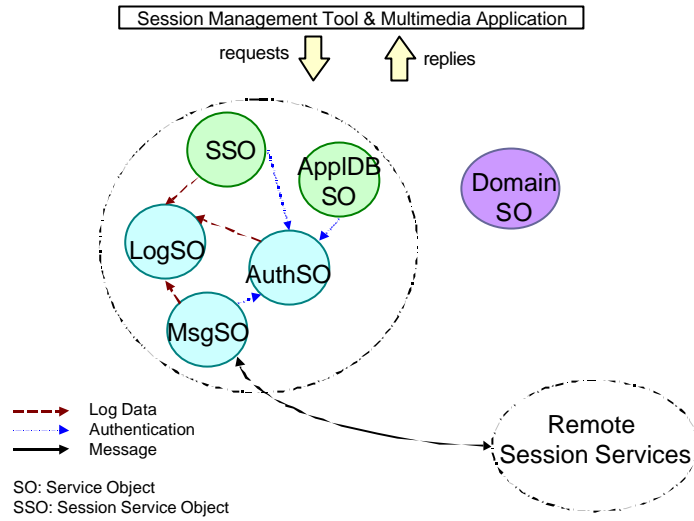
10

가

가

가

가



10:

5.3

5.3.1 (authentication)

~~ㄱ~~

- 가
- 가

가

가

~~ㄱ~~

~~ㄱ~~

ID

~~ㄱ~~

ID

5.3.2

가

~~ㄱ~~

(invite)

가

~~ㄱ~~

가

~~del~~

가

가

(timeout)

가

가

가

(format)

가

~~del~~

(type)

(acknowledge)

~~del~~

ID

가

가

~~del~~

ID

가

가

~~del~~

(time to live)

가

가

가

~~del~~

5.3.3

가

(auditing)

가

~~가~~

가

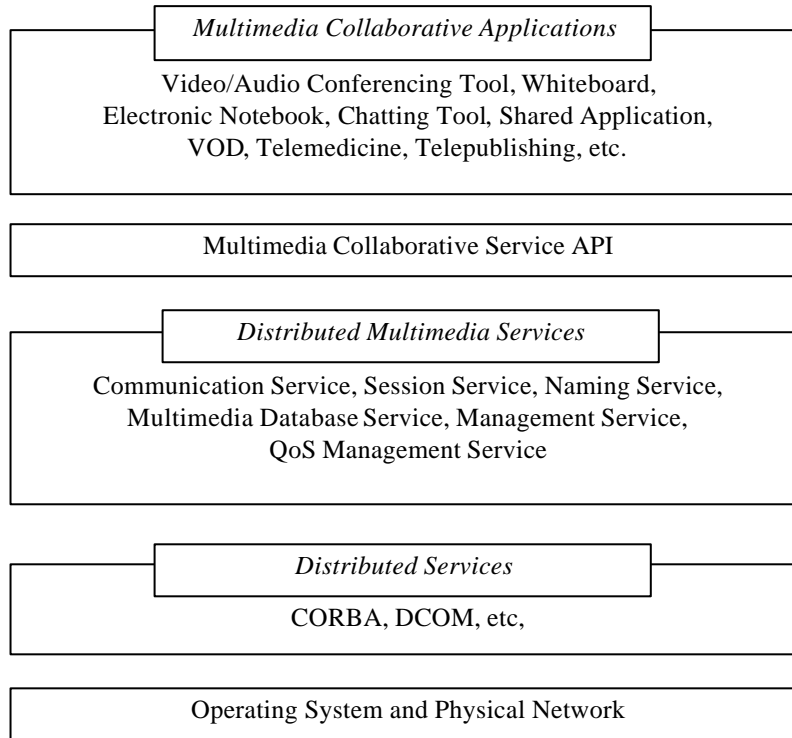
6 CORBA

4, 5 CORBA
가 . ,
MAESTRO .
, 6.1 MAESTRO , 6.2
MAESTRO , 6.3

6.1 MAESTRO

MAESTRO [32, 33, 34, 35]
, ,
11 MAESTRO .
Application Program Interface (API) . API
API
(Communication Service) [34, 35], (Session Service),
(Multimedia Database Service), (Name Service),
(Management Service) [36, 37, 38], (QoS Service) [39,
40], . CORBA [9, 10] DCOM [41]

가 , CORBA DCOM
가



11: MAESTRO

MAESTRO

1.

(synchronization)
(multi-point communication), (flow control)

2. :

3. :

API

4. : MAESTRO

5. : CORBA

6. :

가

6.2 MAESTRO

MAESTRO

MAESTRO

가

가

MAESTRO

가 CORBA IDL [9]

6.2.1

SUN
CORBA C++ . CORBA 가
IONA Orbix 2.3c [42] , C++ SUN
SPARCCompiler C++ 4.1 X-Window
Motif C++ .

Solaris 2.5

6.2.2 MAESTRO

. CORBA IDL , , , 1 .

6.2.3

MAESTRO

, 가 ,
가 ,

6.2.4

가

```
sso->setInfo(_discrimination, info);
```

_discrimination

CORBA:: Any info

```
sso-> destroyApplication(_discrimination);
```

6.3

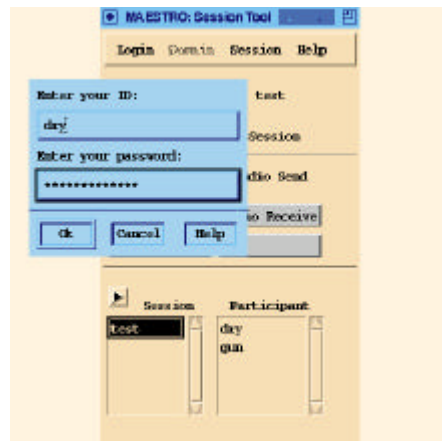
가
가

6.3.1

가

12

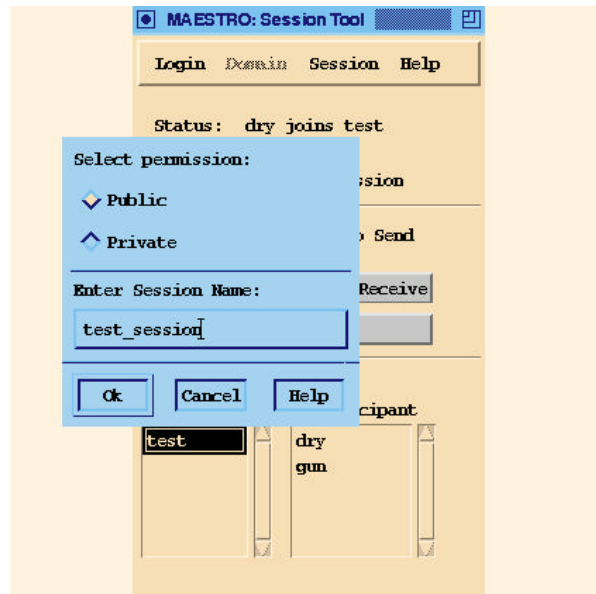
ID



12:

6.3.2

13



13:

6.3.3

가
가

6.3.4

7

가

가

가

가

가

CORBA 가

가

, CORBA Common Object Services Specification (COSS)

가

가 가

CORBA COSS

CORBA

CORBA

가

CORBA

Non-CORBA

가 CORBA

CORBA

Non-CORBA

가

TCP/ IP

Non-CORBA

가

- [1] Sun Microsystems, ShowMe,
<http://www.sun.com/products-n-solutions/sw/ShowMe/index.html>.
- [2] Intel, ProShare, <http://www.intel.com/proshare/conferencing/>.
- [3] Cornell Univ, Cu-SeeMe, <http://www.visc.vt.edu/succeed/conferencing/index.html>.
- [4] Silicon Graphics, InPerson 2.2,
<http://www.sgi.com/Products/software/InPerson/ipintro.html>.
- [5] M. Arango, "The Touring Machine System", *Communications of the ACM*, 36(1),
January 1993, pp. 68-77.
- [6] ETRI Mux, MuX Tutorial, Electronics and Telecommunications Research Institute,
1995.
- [7] MBONE, <http://www.mbone.com/>.
- [8] NetMeeting, <http://www.microsoft.com/netmeeting/>.
- [9] OMG, The Common Object Request Broker: Architecture and Specification Revision
2.2. OMG Document, February 1998.
- [10] OMG, CORBA services: Common Object Specification, OMG Document, March
1995.
- [11] K. Maly, H. Abdel-Wahab, R. Mukkamala, A. Gupta, A. Prabhu, H. Syed and C.
Vemuru, "Mosaic + XTV = CoReview", *Third International World Wide Web
Conference Documents*, 1995.
- [12] H. Gajewska, J. Kistler, M. Manasse and D. Redell, "Argo: A System for Distributed
Collaboration", In *Proceedings of the ACM Multimedia '94 Second International
Conference on Multimedia*, San Francisco, CA, 1994, pp. 433-440.
- [13] MBONE-Korea, <http://paro.etri.re.kr/>.
- [14] Eriksson and Hans, "MBone: The Multicast Backbone," *Communications of the ACM*,
Vol. 37, August 1994, pp.54-60.

- [15] M. Handley, SAP: Session Announcement Protocol, Internet Draft, November 1997.
- [16] M. Handley, V. Jacobson, SDP: Session Description Protocol, RFC 2327, Network Working Group, Standards Track, April 1998.
- [17] M. Handley, H. Schulzrinne, E. Schooler, Rosenberg, SIP: session Initiation Protocol, draft-ietf-mmusic-sip-09.ps, Internet Draft, September 18, 1998.
- [18] Microsoft, "Internet Locator Server", Operations Guide, Version 1.5, Microsoft Corporation, 1997.
- [19] W. Yeung, T. Howers and S. Kille, "Lightweight Directory Access Protocol", RFC 1777, Performance Systems International, University of Michigan, ISODE Consortium, March 1995.
- [20] P. Kaijser, T. Parker and D. Pinkas, "SESAME: The Solution To security for Open Distributed Systems", *Computer Communications*, 17(7), 1994, pp. 501-518.
- [21] P. Kaijser, "SESAME The European Solution to Security For Open Systems.", In *Proceedings of the 10th World Conference on Computer Security, Audit and Control COMPSEC*, London, UK, 1993, pp. 289-297.
- [22] MERCI, <http://www-mice.cs.ucl.ac.uk/multimedia/projects/merci/>.
- [23] K. Bahr, S. Braun, E. Hirsch, P. Kirstein, "Security Architecture for MERCI", *Work-Package contributing to the Deliverable*, September 1996.
- [24] E. Hirsch, A. Jaegemann, I. Roper, L. Wang, "The Secure Conferencing User Agent - A Tool to Provide Secure Conferencing with MBONE Multimedia Conferencing Applications", *Proc. Interactive Distributed Multimedia Systems and Services*, Berlin, March 1996.
- [25] MICE, <http://www-mice-nsc.cs.ucl.ac.uk/>.
- [26] ICE-TEL, <http://www.darmstadt.gmd.de/ice-tel>.
- [27] PGP, <http://www.ifi.uio.no/pgp>.
- [28] S/MIME, <http://www.rsa.com/rsa/S-MIME/home.html>.
- [29] J. Galvin, S. Murphy, MOSS: MIME Object Security Services, RFC 1848, TIS, October 1995.

- [30] Unified Modeling Language, version 1.1, September 1997.
- [31] <http://www.rational.com/products/rose/>.
- [32] T. H. Yun, J. Y. Kong and J. W. Hong, "A CORBA-Based Distributed Multimedia System", *Proc. of the Fourth Pacific Workshop on Distributed Multimedia Systems*, Vancouver, Canada, July 1997, pp. 1-8.
- [33] T. H. Yun, J. Y. Kong and J. W. Hong, "Object-Oriented Modeling of Distributed Multimedia Systems", *Proc. of the IEEE International Conference on Communications (ICC'97)*, Montreal, Canada, June 1997, pp. 777-781.
- [34] J. W. Hong, T. H. Yun, J. Y. Kong, and Y. M. Shin, "A Flexible and Reliable Distributed Multimedia System for Multimedia Information Superhighways", *Malaysian Journal of Computer Science*, Vol. 10, No. 2, December 1997, pp. 1-16.
- [35] , , , , , "MAESTRO (MAESTRO Communication Service for Supporting Distributed Multimedia Applications)", (A), Vol. 23, July 1998, pp. 681-694.
- [36] J. W. Hong, J. Y. Kong, T. H. Yun, J. S. Kim, J. T. Park and J. W. Baek, "Web-based Intranet Services and Network Management", *IEEE Communications Magazine*, Vol. 35, No. 10, October 1997, pp. 100-110 (SCI).
- [37] J. Y. Kong, J. W. Hong, J. T. Park and D. J. Kim, "A CORBA-Based Management Framework for Distributed Multimedia Services and Applications", *Proc. of the Distributed Systems: Operations and Management*, Sydney, Australia, October 1997, pp. 132-144.
- [38] J. Y. Kong, T. H. Yun, S. W. Park, S. H. Kim, Y. M. Shin and J. W. Hong, "Design and Implementation of a Management System for CORBA-Based Distributed Systems", *Proc. of the Asian-Pacific Network Operations and Management Symposium*, Seoul, Korea, October 1997, pp. 473-485.
- [39] J. W. Hong, J. S. Kim and J. T. Park, "A CORBA-based Quality-of-Service Management Framework for Distributed Multimedia Services and Applications",

Proc. of IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM'98), Newark, Delaware, USA, October 1998, pp. 105-116.

- [40] , , ,“
CORBA ”, *1998 KNOM
Conference*, , May 1998, pp. 129-136.
- [41] Microsoft, “DCOM: Technical Overview”, White Paper, Microsoft Corporation, 1996.
- [42] IONA, Orbix 2.3c Programming Guide, IONA Technologies.

1:

MAESTRO

CORBA IDL

IDL

~~SessionSO~~ SessionSO.idl

```
typedef sequence<short> PortSeq;
typedef sequence<string> DomainSeq;
module Session_Server {

    exception Reject {string reason;};
    exception NotDescription{};
    exception NotDiscrimination{};
    exception NotFound{};
    exception ObjectChanged{};

    interface SSO {
        /*****
    boolean registerSession(in any session)
        raises (Reject);
    boolean unregisterSession(in any session, in string passwd)
        raises (Reject, NotDescription);
    /** list *****/
    /* return session ptr*/
    any firstSession()
        raises (Reject, NotFound);
    any nextSession(in any session)
        raises (Reject, NotDescription, ObjectChanged);
    };

    interface Session {
    readonly attribute short sessionPermission;
    readonly attribute string passwd;
    readonly attribute string session_name;

    boolean joinSession (in string name, in string domain);
    boolean leaveSession (in string name);

    /** common to application*****/
    string createApplication(in string appl_name, in string name)
        raises (Reject, NotDescription);
```

```

boolean destroyApplication(in string discrimination)
    raises (Reject, NotDiscrimination);
boolean leaveApplication(in string discrimination)
    raises (Reject, NotDiscrimination);

/** join & leave to ONE leader application *****/
/** return discrimination made by name, session_name, appl_name **/
/** create & destroy to MULTI leader style application *****/
string joinApplication(in string appl_name, in string leader_name,
    in string name)
    raises (Reject, NotDescription);

/*return participant*/
string firstParticipantName()
    raises (NotDescription, NotFound);
string nextParticipantName(in string partici_name)
    raises (Reject, NotDescription, ObjectChanged);

/**for application interface*****/
boolean setInfo(in string discrimination, in any info)
    raises (Reject, NotDiscrimination);
any getInfo(in string discrimination)
    raises (Reject, NotDiscrimination, NotDescription);
};

interface ApplicationDB {
boolean addApplication(in string appl_name, in string description,
    in string location)
    raises (Reject);
boolean deleteApplication(in string appl_name) raises (Reject);

string firstApplication();
string nextApplication(in string appl_name);
};
};

```

~~Domain~~ Domain.idl

```

module Domain_Server {
interface Domain {
    boolean add (in string session_location);
    boolean remove (in string session_location);

    string firstDomainName();
    string nextDomainName(in string domain_name);
}
}

```

~~Message~~ Message.idl

```
module Message_Server {
  interface Msg {
    string get();
  };

  interface Invite_Msg: Msg {
    //YES, NO
    boolean result(in string result );
  };

  interface Deliver {
    boolean put (in any msg);
    boolean send (in any msg, in string host);
    Msg get(in string name);
  };
};
```

가

가

가

2

93

3

NOM

가 Adlib

s,

가

Ag,

6

:
 : 1974 9 13
 :
 : 18-410

1993 ~ 1997 : (B. S.)
 1997 ~ 1999 : (M.S.)

?? Journal Papers

?? J. W. Hong, Y. M. Shin, M. S. Kim, J. Y. Kim and Y. H. Suh, "Design and Implementation of a Distributed Multimedia Collaborative Environment", Accepted to be published in the Special Issue on Multimedia Collaborative Environments of Cluster Computing: Network Software Tools, and Applications, Baltzer Science, Fall 1998.

?? , , , , , " MAESTRO (MAESTRO Communication Service for Supporting Distributed Multimedia Applications)", (A), Vol. 23 July 1998, pp. 681-694.

?? J. W. Hong, T. H. Yun, J. Y. Kong, and Y. M. Shin, "A Flexible and Reliable Distributed Multimedia System for Multimedia Information Superhighways", Malaysian Journal of Computer Science, December 1997, pp 1-16.

?? Conference Papers

?? , , , , , "W/S", 1998 , , May 1998, pp. 298-303.

?? J. Y. Kong, T. H. Yun, S. W. Park, S. H. Kim, Y. M. Shin and J. W. Hong, "Design and Implementation of a Management System for CORBA-Based Distributed Systems", Proc. of the Asian-Pacific Network Operations and Management Symposium, Seoul, Korea, October 1997, pp. 473-485.

**C
O
R
B
A**

**1
9
9
9**