

Network Working Group
Internet-Draft
Expires: July 3, 2000

Ott
TZI, Universitaet Bremen
Perkins
University College London
Kutscher
TZI, Universitaet Bremen
January 3, 2000

A Message Bus for Local Coordination
draft-ietf-mmusic-mbus-transport-01.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on July 3, 2000.

Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

Abstract

In a variety of conferencing scenarios, a local communication channel is desirable for conference-related information exchange between co-located but otherwise independent application entities, for example those taking part in application sessions that belong to the same conference. In loosely coupled conferences such a mechanism allows for coordination of applications entities to e.g. implement synchronization between media streams or to configure entities without user interaction. It can also be used to implement tightly coupled conferences enabling a conference controller to enforce conference wide control within a end system.

The local Message Bus (Mbus) provides a means to achieve the

Ott, et. al.

Expires July 3, 2000

[Page 1]

Internet-Draft

A Message Bus for Local Coordination

January 2000

necessary amount of coordination between co-located conferencing applications for virtually any type of conference as postulated in a companion requirement document[11]. The Message Bus comprises two logically distinct parts: a message transport infrastructure and a

set of common as well as protocol/ media/tool-specific messages along with a conference-specific addressing scheme. This document deals with message addressing, transport, and security issues and defines the message syntax for the Mbus. It does not define application oriented semantics and procedures for using the message bus. Application specific command sets and procedures for applications using the Mbus are expected to be defined in follow-up documents.

This document is intended for discussion in the Multiparty Multimedia Session Control (MMUSIC) working group of the Internet Engineering Task Force. Comments are solicited and should be addressed to the working group's mailing list at confctrl@isi.edu and/or the authors.

Table of Contents

| | | |
|-----|--|----|
| 1. | Introduction | 4 |
| 1.1 | Background | 4 |
| 1.2 | Purpose | 4 |
| 1.3 | Terminology for requirement specifications | 4 |
| 2. | General Outline | 5 |
| 3. | Message Format | 7 |
| 4. | Addressing | 9 |
| 4.1 | Mandatory Address Elements | 10 |
| 5. | Reliability | 11 |
| 6. | Transport | 13 |

| | | |
|------|--|----|
| 7. | Message Syntax | 15 |
| 7.1 | Message Encoding | 15 |
| 7.2 | Message Header | 15 |
| 7.3 | Command Syntax | 15 |
| 8. | Messages | 18 |
| 8.1 | mbus.hello | 18 |
| 8.2 | mbus.bye | 19 |
| 8.3 | mbus.quit | 19 |
| 8.4 | mbus.waiting | 19 |
| 8.5 | mbus.go | 20 |
| 9. | Timer and Counters | 21 |
| 10. | Mbus Security | 22 |
| 10.1 | Security Model | 22 |
| 10.2 | Message Authentication | 22 |
| 10.3 | Encryption | 23 |
| 11. | Mbus Configuration | 24 |
| 11.1 | File based parameter storage | 25 |
| 11.2 | Registry based parameter storage | 26 |
| 12. | Security Considerations | 28 |
| 13. | IANA Considerations | 29 |
| | References | 30 |
| | Authors' Addresses | 31 |
| A. | Mbus Addresses for Conferencing | 32 |
| | Full Copyright Statement | 34 |

1. Introduction

1.1 Background

The requirement specification as defined in the requirements draft[11] provides a set of scenario descriptions for the usage of a local coordination infrastructure. The Message Bus defined in this and a companion document provides a suitable means for local communication that serves all of the purposes mentioned in the requirement document.

1.2 Purpose

Two components constitute the Message Bus: the (lower level) message passing mechanisms and the (higher level) messages and their semantics along with their addressing scheme.

The purpose of this document is to define the characteristics of the lower level Mbus message passing mechanism which is common to all Mbus implementations. This includes the specification of

- o the generic Mbus message format;
- o the addressing concept for application entities (note that addressing details are defined by the application environment);
- o the transport mechanisms to be employed for conveying messages between (co-located) application entities;
- o the security concept to prevent misuse of the Message Bus (as taking control of another user's conferencing environment);
- o the details of the Mbus message syntax; and
- o a set of mandatory application independent commands that are used for bootstrapping Mbus sessions.

1.3 Terminology for requirement specifications

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119[1] and indicate requirement levels for compliant Mbus implementations.

2. General Outline

The Mbus is supposed to operate in a variety of scenarios as outlined in the companion requirement document[11]. From these scenarios, the following (minimum) requirements are derived that have to be met by the Mbus design to provide a suitable local communication infrastructure.

Local coordination involves a widely varying number of entities: some messages (such as membership information, floor control notifications, dissemination conference state changes, etc.) may need to be destined for all local application entities. Messages may also be targeted at a certain application class (e.g. all whiteboards or all audio tools) or agent type (e.g. all user interfaces rather than all media engines). Or there may be any (application- or message- specific) subgrouping defining the intended recipients, e.g. messages related to media synchronization. Finally, there will be messages that are directed to a single entity, for example, specific configuration settings that a conference controller sends to a application entity or query-response exchanges between any local server and its clients.

The Mbus concept as presented here satisfies these different communication models by defining different message transport mechanisms (defined in Section 6) and by providing a flexible addressing scheme (defined in Section 4).

Furthermore, Mbus messages exchanged between application entities

may have different reliability requirements (which are typically derived from their semantics). Some messages will have a rather informational character conveying ephemeral state information (which is refreshed/updated periodically), such as the volume meter level of an audio receiver entity to be displayed by its user interface agent. Certain Mbus messages (such as queries for parameters or queries to local servers) may require a response from the peer(s) thereby providing an explicit acknowledgment at the semantic level on top of the Mbus. Other messages will modify the application or conference state and hence it is crucial that they do not get lost. The latter type of message has to be delivered reliably to the recipient, whereas message of the first type do not require reliability mechanisms at the Mbus transport layer. For messages confirmed at the application layer it is up to the discretion of the application whether or not to use a reliable transport underneath.

In some cases, application entities will want to tailor the degree of reliability to their needs, others will want to rely on the underlying transport to ensure delivery of the messages -- and this may be different for each Mbus message. The Mbus message passing mechanism described in this paper provides a maximum of flexibility

Ott, et. al.

Expires July 3, 2000

[Page 5]

Internet-Draft

A Message Bus for Local Coordination

January 2000

by providing reliable transmission achieved through transport-layer acknowledgments (in case of point-to-point communications only) as well as unreliable message passing (for unicast, local multicast, and local broadcast). We address this topic in Section 4.

Finally, accidental or malicious disturbance of Mbus communications through messages originated by applications from other users needs to be prevented. Accidental reception of Mbus messages from other users may occur if either two users share the same workstation for conferencing or are using end systems spread across the same physical network: in either case, the Mbus multicast address and the port number may match leading to reception of the other party's Mbus messages in addition to a user's own ones. Malicious disturbance may happen because of applications multicasting (e.g. at a global scope) or unicasting Mbus messages (which could contain a "conf.terminated" command). To eliminate the possibility of receiving bogus Mbus messages, the Mbus protocol contains message digests for authentication. Furthermore, the Mbus allows for encryption to ensure privacy and thus enable using the Mbus for local key distribution and other functions potentially sensitive to eavesdropping. This document defines the framework for configuring Mbus applications with regard to security parameters in Section 11.

3. Message Format

A Mbus message comprises a header and a body. The header is used to indicate how and where a message should be delivered, the body provides information and commands to the destination entity. The following information is included in the header:

The MsgDigest is a Base64-encoded (see RFC1521[5]) calculated hash value of the entire message (starting from the ProtocolID field) as described in Section 10 and Section 11.

A fixed ProtocolID field identifies the version of the message bus protocol used. The protocol defined in this document is "mbus/1.0" (case-sensitive).

A sequence number (SeqNum) is contained in each message. The first message sent by a source SHOULD have SeqNum equal to zero, and it MUST increment by one for each message sent by that source. A single sequence number is used for all messages from a source, irrespective of the intended recipients and the reliability mode selected. SeqNums are decimal numbers in ASCII representation.

The TimeStamp field is also contained in each message and SHOULD contain a decimal number representing the time at message construction in seconds since 00:00:00, UTC, January 1, 1970.

A MessageType field indicates the kind of message being sent. The value "R" indicates that the message is to be transmitted reliably and MUST be acknowledged by the recipient, "U" indicates an unreliable message which MUST NOT be acknowledged.

The SrcAddr field identifies the sender of a message. This MUST be a complete address, with all address elements specified. The addressing scheme is described in Section 4.

The DestAddr field identifies the intended recipient(s) of the message. This field MAY contain wildcards by omitting address element and hence address any number (including zero) of application entities. The addressing scheme is described in Section 4.

The AckList field comprises a list of SeqNums for which this message is an acknowledgment. See Section 5 for details.

The header is followed by the message body which contains one or more commands to be delivered to the destination entity. The syntax for a complete message is given in Message syntax (Section 7).

Ott, et. al.

Expires July 3, 2000

[Page 7]

Internet-Draft

A Message Bus for Local Coordination

January 2000

If multiple commands are contained within the same Mbus message payload, they MUST to be delivered to the Mbus application in the same sequence in which they appear in the message payload.

Ott, et. al.

Expires July 3, 2000

[Page 8]

4. Addressing

Each entity on the message bus SHOULD respond to messages sent to one (or more) addresses. Addresses are sequences of address elements that are tag/value pairs. The tag and the value are separated by a colon and tag/value pairs are separated by whitespace, like this:

```
(tag:value tag:value ...)
```

The formal ABNF syntax definition for Mbus addresses and their elements is as follows:

```
mbus_address    = "(" *address_element ")"
address_element = *WSP address_tag ":" address_value *WSP
address_tag     = 1*32(ALPHA)
address_value   = 1*64(%x21-7F)
                 ; any 7-bit US-ASCII character
                 ; excluding white space
                 ; and control characters
```

Each entity has a fixed sequence of address elements constituting its address and MUST only process messages sent to addresses that either match all elements or consist of a subset of its own address elements. Each element value in this subset must match the corresponding value of the receiver's address element value. The order of address elements in an address sequence is not relevant. For example, an entity with an address of:

```
(conf:test media:audio module:engine app:rat id:4711-1@134.102.218.45)
```

will process messages sent to

```
(media:audio module:engine)
```

and

```
(module:engine)
```

but must ignore messages sent to

```
(conf:test media:audio module:engine app:rat id:123-4@134.102.218.45 foo:bar)
```

and

```
(foo:bar)
```

A message that should be processed by all entities requires an empty set of address elements.

4.1 Mandatory Address Elements

Each Mbus entity MUST provide one mandatory address element that

allows to identify the entity. The element name is "id" and the value MUST be composed of the following components:

- o The IP address of the interface that is used for sending messages to the Mbus. For IPv4 this the address in decimal dotted notation. For IPv6 the interface-ID-part of an address in textual representation as specified in [3] MUST be used. In this specification, this part is called the "host-ID".
- o An identifier ("entity-ID") that is unique within the scope of single host-ID. The entity comprises two parts. For systems where the concept of a process ID is applicable it is RECOMMENDED this identifier be composed using a process-ID and a per-process disambiguator for different Mbus entities of a process. If a process ID is not available, this part of the entity-ID may be randomly chosen (it is recommended that at least a 32 bit random number is chosen). Both numbers are represented in decimal textual form and MUST be separated by a '-' character.

Note that the entity-ID cannot be the port number of the endpoint used for sending messages to the Mbus because implementations MAY use the common Mbus port number for sending to and receiving from the multicast group (as specified in Section 6). The total identifier has the following structure:

```
id-element      = "id:" id-value
id-value        = entity-id "@" host-id
entity-id       = 1*10DIGIT "-" 1*5DIGIT
host-id         = (IPv4address / IPv6address)
```

Please refer to [3] for productions of IPv4address and IPv6address.

An example for an id element:

```
id:4711-99@134.102.218.45
```

A set of the address elements that are to be used by conferencing applications is specified in "Mbus Addresses for Conferencing" (Appendix A).

5. Reliability

While most messages are expected to be sent using unreliable transport, it may be necessary to deliver some messages reliably. Reliability can be selected on a per message basis by means of the MessageType field. Reliable delivery is supported for messages with a single recipient only; i.e., all components of the DestAddr field have to be specified. An entity can thus only send reliable messages to known addresses, i.e. it can only send reliable messages to entities that have announced their existence on the Mbus (e.g. by means of mbus.hello() messages (Section 8.1)). A sending entity MUST

NOT send a message reliably if the target address is not unique. (See Transport (Section 6) for the specification of an algorithm to determine whether an address is unique.) A receiving entity MUST only process and acknowledge reliable message if the destination address exactly matches its own source address (the destination address MUST NOT be a subset of the source address).

Disallowing reliable message delivery for messages sent to multiple destinations is motivated by simplicity of the implementation as well as the protocol. Although ACK implosions are not really an issue and losses are rare, achieving reliability for such messages would require full knowledge of the membership for each subgroup which is deemed too much effort.

Each message is tagged with a message sequence number. If the MessageType is "R", the sender expects an acknowledgment from the recipient within a short period of time. If the acknowledgment is not received within this interval, the sender SHOULD retransmit the message (with the same message sequence number), increase the timeout, and restart the timer. Messages MUST be retransmitted a small number of times (see below) before the recipient is considered to have failed. If the message is not delivered successfully, the sending application is notified. In this case, it is up to this application to determine the specific action(s) (if any) to be taken.

Reliable messages are acknowledged by adding their SeqNum to the AckList field of a message sent to the originator of the reliable message. Multiple acknowledgments MAY be sent in a single message. It is possible to either piggy-back the AckList onto another message sent to the same destination, or to send a dedicated acknowledgment message, with no other commands.

The precise procedures are as follows:

Sender: A sender A of a reliable message M to receiver B SHOULD transmit the message via multicast or via unicast, keep a copy of M, initialize a retransmission counter N to '1', and start a

retransmission timer T (initialized to T_r). If an acknowledgment is received from B, timer T MUST BE cancelled and the copy of M is discarded. If T expires, the message M SHOULD BE retransmitted, the counter N SHOULD BE incremented by one, and the timer SHOULD BE restarted (set to $N \cdot T_r$). If N exceeds the retransmission threshold N_r , the transmission is assumed to have failed, further retransmission attempts MUST NOT be undertaken, the copy of M SHOULD BE discarded, and the sending application SHOULD BE notified.

Receiver: A receiver B of a reliable message from a sender A SHOULD acknowledge receipt of the message within a time period $T_c < T_r$. This MAY be done by means of a dedicated acknowledgment message or by piggy-backing the acknowledgment on another message addressed only to A.

Receiver optimization: In a simple implementation, B may choose to immediately send a dedicated acknowledgment message. However, for efficiency, it could add the SeqNum of the received message

to a sender-specific list of acknowledgments; if the added SeqNum is the first acknowledgment in the list, B SHOULD start an acknowledgment timer TA (initialized to T_c). When the timer expires, B SHOULD create a dedicated acknowledgment message and send it to A. If B is to transmit another Mbus message addressed only to A, it should piggy-back the acknowledgments onto this message and cancel TA. In either case, B should store a copy of the acknowledgment list as a single entry in the per-sender copy list, keep this entry for a period T_k, and empty the acknowledgment list. In case any of the messages kept in an entry of the copy list is received again from A, the entire acknowledgment list stored in this entry is scheduled for (re-)transmission following the above rules.

Constants:

Suggested values are T_r=100ms, N_r=3, T_c=70ms,
T_k=(N_r)*(N_r+1)/2)*T_r.

Ott, et. al.

Expires July 3, 2000

[Page 12]

Internet-Draft

A Message Bus for Local Coordination

January 2000

6. Transport

All messages are transmitted as UDP messages with two ways of sending messages being possible:

1. Local multicast (host-local or link-local, see Mbus configuration (Section 11)) to a fixed, yet to be assigned (see Section 13) link-local address of the administratively scoped multicast space as described in RFC 2365[10]. There will also be a fixed, registered port number that all Mbus entities MUST use. Until the address and port number are assigned, 224.255.222.239 is used as the multicast address and 47000 (decimal) as the port number.
2. Directed unicast (via UDP) to the port of a specific application. This still requires the DestAddr field to be filled in properly. Directed unicast is intended for situations where node local multicast is not available. It MAY also be used by Mbus implementations for delivering messages addressed at a single application entity only -- the address of which the Mbus implementation has learned from other message exchanges before. Every Mbus entity SHOULD use a unique endpoint address for every message it sends to the Mbus multicast group or to individual receiving entities. A unique endpoint address is a tuple consisting of the entity's IP address and a port number, where the port number is different from the standard Mbus port number (yet to be assigned, see Section 13). When multicast is

available, messages MUST only be sent via unicast if the Mbus target address is unique and if the sending entity can verify that the receiving entity uses a unique endpoint address. The latter can be verified by considering the last message received from that entity. (Note that several Mbus entities, say within the same process, may share a common transport address; in this case, the contents of the destination address field is used to further dispatch the message. Given the definition of "unique endpoint address" above the use of a shared endpoint address and a dispatcher still allows other Mbus entities to send unicast messages to one of the entities that share the endpoint address. So this can be considered an implementation detail.) When multicast is not available messages can be sent via unicast but all messages that do not contain a unique target address MUST be sent to all known entities via unicast. Messages with an empty target address list MUST always be sent to all Mbus entities (via multicast if available). The following algorithm can be used by sending entities to determine whether a Mbus address is unique considering the current set of Mbus entities:

Ott, et. al.

Expires July 3, 2000

[Page 13]

Internet-Draft

A Message Bus for Local Coordination

January 2000

```
let ta=the target address;
iterate through the set of all
currently known Mbus addresses {
  let ti=the address in each iteration;
  count the addresses for which
  the predicate isSubsetOf(ta,ti) yields true;
}
```

If the count of matching addresses is exactly 1 the address is unique. The following algorithm can be used for the predicate `isSubsetOf`, that checks whether the second message matches the first according to the rules specified in Section 4. (A match means that a receiving entity that uses the second Mbus address must also process received messages with the first address as a target address.

```
isSubsetOf(addr a1,a2) yields true, iff
  every address element of a1 is contained
  in a2's address element list
```

An address element is contained in an address element list if the list contains an element that provides same values for the two address element fields key and value.

If a single application system is distributed across several co-located hosts, link local scope SHOULD be used for multicasting Mbus messages that potentially have recipients on the other hosts. The Mbus protocol is not intended (and hence deliberately not designed) for communication between hosts not on the same link.

Since messages are transmitted in UDP datagrams, a maximum size of 64 KBytes MUST NOT be exceeded. It is RECOMMENDED that applications using a non host-local scope do not exceed a message size of the network's MTU.

7. Message Syntax

7.1 Message Encoding

All messages MUST use the UTF-8 character encoding. Note that US ASCII is a subset of UTF-8 and requires no additional encoding, and that a message encoded with UTF-8 will not contain zero bytes.

Each Message MAY be encrypted using a secret key algorithm as defined in Section 10.

7.2 Message Header

A message starts with the header. The first field in the header is the message digest calculated using a keyed hash algorithm as described in Section 10 followed by a newline character. The other fields in the header are separated by white space characters, and followed by a newline. The format of the header is as follows:

```
msg_header = MsgDigest LF "mbus/1.0" 1*WSP SeqNum 1*WSP TimeStamp 1*WSP
           MessageType 1*WSP SrcAddr 1*WSP DestAddr 1*WSP AckList
```

The header fields are explained in Message Format (Section 3). Here are the ABNF syntax definitions for the header fields:

```
MsgDigest   = base64
SeqNum      = 1*DIGIT
TimeStamp   = 1*DIGIT
MessageType = "R" / "U"
SrcAddr     = mbus_address
DestAddr    = mbus_address
AckList     = "(" *(1*DIGIT) ")"
```

The syntax definition of a complete message is as follows:

```
mbus_message = msg_header LF msg_payload
msg_payload  = mbus_command *(LF mbus_command)
```

See Figure 19 for the definition a Mbus command.

7.3 Command Syntax

The header is followed by zero, or more, commands to be delivered to

the application(s) indicated by the DestAddr field. Each message comprises a command followed by a list of zero, or more, parameters, and is followed by a newline.

```
command ( parameter parameter ... )
```

Syntactically, the command name MUST be a 'symbol' as defined in the following table. The parameters MAY be any data type drawn from the following table:

| Data Type | Syntax | Description |
|-----------|---|--------------------------------------|
| val | (Integer / Float / String / List Symbol Data) | a value can be of one of these types |
| Integer | "-" 1*DIGIT | |
| Float | "-" 1*DIGIT "." 1*DIGIT | |
| String | DQUOTE *CHAR DQUOTE | See below for escape characters |
| List | "(" *(val *(WSP val)) ")" | |
| Symbol | ALPHA *(ALPHA / DIGIT / "_" / "-" / ".") | A predefined protocol value |
| Data | "<" *base64 ">" | Opaque Data |

Boolean values are encoded as an integer, with the value of zero representing false, and non-zero representing true (as in the 'C' programming language).

String parameters in the payload MUST be enclosed in the double quote (') character. Within strings, the escape character is the backslash (\), and the following escape sequences are defined:

| Escape Sequence | Meaning |
|-----------------|---------|
| \\ | \ |
| \" | " |
| \n | newline |

List parameters do not have to be homogeneous lists, i.e. they can contain parameters of varying types.

Opaque data is represented as Base64-encoded (see RFC1521[5]) character strings surrounded by "< " and "> "

The ABNF syntax definition for Mbus commands is as follows:

```
mbus_command = command_name arglist
command_name = ALPHA *(ALPHA / DIGIT / "_" / ".")
arglist      = "(" *(WSP parameter *WSP) ")"
parameter   = Integer / Float / String / List
              Symbol / Data
```

Command names SHOULD be constructed using hierarchical names to group conceptually related commands under a common hierarchy. The delimiter between names in the hierarchy is "." (dot).

The Mbus addressing scheme defined in Addressing (Section 4) provides for specifying incomplete addresses by omitting certain elements of an address element list, enabling entities to send commands to a group of Mbus entities. Therefore all command names SHOULD be unambiguous in a way that it is possible to interpret or ignore them without considering the message's address.

A set of commands within a certain hierarchy that must be understood by every entity is defined in Messages (Section 8).

The section defines some basic application independent messages that MUST be understood by all implementations. This specification does not contain application specific messages which are to be defined outside of the basic Mbus protocol specification.

Before components of a distributed system can communicate with one another using the Mbus, they need to mutually find out about their existence. After this bootstrap procedure that each Mbus entity goes through all other entities listening to the same Mbus know about the newcomer and the newcomer has learned about all the other entities. Furthermore entities need to be able to notice the failure (or leaving) of other entities.

Any Mbus entity is supposed to announce its presence (on the Mbus) after starting up. This is to be done repeatedly throughout its lifetime to address the issues of startup sequence: Entities should always become aware of other entities independent of the order of starting.

Any Mbus entity should frequently indicate that it is still alive. This mechanism may be combined with the aforementioned self-announcement.

An Mbus entity should be able to indicate that it is waiting for a certain event to happen (similar to a P() operation on a semaphore but without creating external state somewhere). In conjunction with this, an Mbus entity should be capable of indicating to another entity that this condition is now satisfied (similar to a semaphore's V() operation).

An appropriate command set to implement the aforementioned concepts is presented in the following sections.

8.1 mbus.hello

Syntax:
mbus.hello()

Parameters: - none -

Each Mbus entity MUST send HELLO messages after startup to the global Mbus channel. After transmission of the HELLO message, it shall start a timer after the expiration of which the next HELLO message shall be transmitted. The timer shall be set to a random value $t_hello \leq t \leq t_hello + t_dither$ to avoid synchronization of HELLO messages. Transmission of HELLO messages MUST NOT be stopped unless the entity detaches from the Mbus. Section 9 defines

concrete values for those parameters.

HELLO messages MUST be sent unreliably to all Mbus entities.

Each Mbus entity learns about other Mbus entities by observing their HELLO messages and tracking the sender address of each message.

The HELLO message is also used to track the liveness of any Mbus entity. Whenever an Mbus entity has not heard for a time span of $n_dead * (t_hello + t_dither)$ from another Mbus entity it may consider

this entity to have failed (or have quit silently). Note that no need for any action is necessarily implied from this observation.

8.2 mbus.bye

Syntax:

Parameters: - none -

An Mbus entity that is about to terminate (or "detach" from the Mbus) SHOULD announce this by transmitting a BYE message.

The BYE message MUST be sent unreliably to all receivers.

8.3 mbus.quit

Syntax:

mbus.quit()

Parameters: - none -

The QUIT message is used to request other entities to terminate themselves (and detach from the Mbus). Whether this request is honoured by receiving entities or not is up to the discretion of the application.

The QUIT message can be multicast or sent reliably via unicast to a single Mbus entity or a group of entities.

8.4 mbus.waiting

Syntax:

mbus.waiting(condition)

Parameters:

symbol condition

The condition parameter is used to indicate that the entity transmitting this message is waiting for a particular event to

occur.

The WAITING messages may be broadcast to all Mbus entities, multicast an arbitrary subgroup, or unicast to a particular peer. Transmission of the WAITING message MUST be unreliable and hence has to be repeated at an application-defined interval (until the condition is satisfied).

If an application wants to indicate that it is waiting for several conditions to be met, several WAITING messages are sent (possibly included in the same Mbus payload). Note that HELLO and WAITING messages may also be transmitted in a single Mbus payload.

8.5 mbus.go

Syntax:

mbus.go(condition)

Parameters:

symbol condition

This parameter specifies which condition is met.

The GO message is sent by an Mbus entity to "unblock" another Mbus entity -- the latter of which has indicated that it is waiting for a certain condition to be met. Only a single condition can be specified per GO message. If several conditions are satisfied simultaneously multiple GO messages MAY be combined in a single Mbus payload.

The GO message MUST be sent reliably via unicast to the Mbus entity to unblock.

9. Timer and Counters

The following values for timers and counters mentioned in this document SHOULD be used by implementations:

| Timer / Counter | Value |
|-----------------|------------------|
| t_hello | 1 second |
| t_dither | 100 milliseconds |
| n_dead | 5 |

As the Mbus is designed for a local system architecture it is not considered necessary to provide dynamic adaptation of these timers and counters to the number of Mbus entities.

10. Mbus Security

10.1 Security Model

In order to prevent accidental or malicious disturbance of Mbus communications through messages originated by applications from other users message authentication is deployed (Section 10.2). For each message a digest is calculated based on the value of a shared secret key value. Receivers of messages can check if the sender belongs to the same Mbus security domain by re-calculating the digest and comparing it to the received value. Only if both values are equal the messages must be processed further. In order to allow different simultaneous Mbus sessions at a given scope and to compensate defective implementations of host local multicast ([18]) message authentication MUST be provided by conforming implementations.

Privacy of Mbus message transport can be achieved by optionally using symmetric encryption methods (Section 10.3). Each message can be encrypted using an additional shared secret key and a symmetric encryption algorithm. Encryption is OPTIONAL for applications, i.e. it is allowed to configure an Mbus domain not to use encryption. But conforming implementations MUST provide the possibility to use message encryption (see below).

Message authentication and encryption can be parameterized by certain values, e.g. by the algorithms to apply or by the keys to use. These parameters (amongst others) are defined in an Mbus configuration entity that is accessible to all Mbus entities that participate in an Mbus session. In order to achieve interoperability conforming implementations SHOULD consider the given Mbus configuration entity. Section 11 defines the mandatory and optional parameters as well as storage procedures for different platforms. Only in cases where none of the options for configuration entities

mentioned in Section 11 is applicable alternative methods of configuring Mbus protocol entities MAY be deployed.

10.2 Message Authentication

Either MD5 [14] or SHA-1 [15] SHOULD be used for message authentication codes (MACs). An implementation MAY provide SHA-1, whereas MD5 MUST be implemented. To generate keyed hash values the algorithm described in RFC2104[4] MUST be applied with hash values truncated to 96 bits (12 bytes). The resulting hash values MUST be Base64 encoded (16 characters). The HMAC algorithm works with both, MD5 and SHA-1.

HMAC values, regardless of the algorithm, MUST therefore always consist of 16 Base64-encoded characters.

Ott, et. al.

Expires July 3, 2000

[Page 22]

Internet-Draft

A Message Bus for Local Coordination

January 2000

Hash keys MUST have a length of 96 bit (12 bytes), that are 16 Base64-encoded characters.

10.3 Encryption

Either DES, 3DES (triple DES) or IDEA SHOULD be used for encryption. Encryption MAY be neglected for applications, e.g. in situations where license regulations, export or encryption laws would be offended otherwise. However, the implementation of DES is RECOMMENDED as a baseline. DES implementations MUST use the DES Cipher Block Chaining (CBC) mode. For algorithms requiring en/decryption data to be padded to certain boundaries octets with a value of 0 SHOULD be used for padding characters. The padding characters MUST be appended after calculating the message digest when encoding and MUST be erased before recalculating the message digest when decoding. IDEA uses 128-bit keys (24 Base64-encoded characters). DES keys (56 bits) MUST be encoded as 8 octets as described in RFC1423[12], resulting in 12 Base64-encoded characters.

The mandatory subset of algorithms that MUST be provided by implementations is DES and MD5.

See Section 11 for a specification of notations for Base64-strings.

11. Mbus Configuration

An implementation MUST be configurable by the following parameters:

Configuration version

The version number of the given configuration entity. Version numbers allow implementations to check if they can process the entries of a given configuration entity. Version numbers are integer values. The version number for the version specified here is 1.

Encryption key

The secret key used for message encryption.

Hash key

The hash key used for message authentication.

Scope

The Internet scope to be used for sent messages.

The upper parameters are mandatory and MUST be present in every Mbus configuration entity.

The following parameters are optional. When they are present they MUST be honoured but when they are not present implementations SHOULD fall back to the predefined default values (as defined in Transport (Section 6)):

Address

The non-standard multicast address to use for message transport.

Port

The non-standard port number to use for message transport.

Two distinct facilities for parameter storage are considered: For Unix-like systems a configuration file SHOULD be used and for Windows-95/98/NT/2000 systems a set of registry entries is defined that SHOULD be used.

The syntax of the values for the respective parameter entries remains the same for both configuration facilities. The following defines a set of ABNF (see RFC2234[13]) productions that are later

referenced for the definitions for the configuration file syntax and registry entries:

```

algo-id           = "NOENCR" / "DES" / "3DES" / "IDEA" /
                   "HMAC-MD5-96" / "HMAC-SHA1-96"
scope             = "HOSTLOCAL" / "LINKLOCAL"
key               = base64string
version_number   = 1*10DIGIT
base64string     = *(ALPHA / DIGIT / "+" / "/" / "=")
key_value        = "(" algo-id ", " key ")"
ipv4_addr        = ipv4_octet 3*3("." ipv4_octet)
ipv4_octet       = 1*3DIGIT
port             = 1*5DIGIT

```

A key entry **MUST** be specified using this notation:

```
"("algo-id","base64string")"
```

algo-id is one of the character strings specified above. For algo-id='`NOENCR`' the other fields are ignored. The de-limiting commas **MUST** always be present though.

A Base64 string consists of the characters defined in the Base64 char-set (see RFC1521[5]) including all eventual padding characters, i.e. the length of Base64-string is always a multiple of 4.

The version_number parameter specifies a version number for the used configuration entity.

11.1 File based parameter storage

The file name for a Mbus configuration file is ".mbus" in the user's home-directory. If an environment variable called MBUS is defined implementations **SHOULD** interpret the value of this variable as a fully qualified file name that is to be used for the configuration file. Implementations **MUST** ensure that this file has appropriate file permissions that prevent other users to read or write it. The file **MUST** exist before a conference is initiated. Its contents **MUST** be UTF-8 encoded and **MUST** be structured as follows:

```
mbus-file = mbus-topic LF *(entry LF)
```

```

mbus-topic      = "[MBUS]"
entry           = 1*(version_info / hashkey_info
                  / encryptionkey_info / scope_info
                  / port_info / address_info)
version_info    = "CONFIG_VERSION=" version_number
hashkey_info    = "HASHKEY=" key_value
encrkey_info    = "ENCRYPTIONKEY=" key_value
scope_info      = "SCOPE=" scope
port_info       = "PORT=" port
address_info    = "ADDRESS=" ipv4_addr

```

The following entries are defined: CONFIG_VERSION, HASHKEY, ENCRYPTIONKEY, SCOPE, PORT, ADDRESS.

The entries CONFIG_VERSION, HASHKEY and ENCRYPTIONKEY are mandatory, they MUST be present in every Mbus configuration file. The order of entries is not significant.

An example Mbus configuration file:

```

[MBUS]
CONFIG_VERSION=1
HASHKEY=(HMAC-MD5-96,MTIzMTU2MTg5MTEy)
ENCRYPTIONKEY=(DES,MTIzMTU2MQ==)
SCOPE=HOSTLOCAL
ADDRESS=224.255.222.239
PORT=47000

```

11.2 Registry based parameter storage

For systems lacking the concept of a user's home-directory as a place for configuration files the suggested database for configuration settings (e.g. the Windows9x-, Windows NT-, Windows 2000-registry) SHOULD be used. The hierarchy for Mbus related registry entries is as follows:

```
HKEY_CURRENT_USER\Software\Mbone Applications\Mbus
```

The entries in this hierarchy section are:

| Name | Type | ABNF production |
|----------------|--------|-----------------|
| CONFIG_VERSION | DWORD | version_number |
| HASHKEY | String | key_value |
| ENCRYPTIONKEY | String | key_value |
| SCOPE | String | scope |
| ADDRESS | String | ipv4_addr |
| PORT | DWORD | port |

+-----+-----+-----+

The same syntax for key values as for the file based configuration facility MUST be used.

Ott, et. al.

Expires July 3, 2000

[Page 27]

Internet-Draft

A Message Bus for Local Coordination

January 2000

12. Security Considerations

The Mbus security mechanismns are specified in Section 10.1.

It should be noted that the Mbus transport specification defines a mandatory baseline set of algorithms that have to be supported by implementations. This baseline set does not neccessarily provide the best security due to the cryptographic weaknesses of the individual algorithms. For example, it has been stated in [4] that MD5 had been shown to be vulnerable to collision search attacks (although this was believed not to compromise the use of MD5 within HMAC generation). However, SHA-1 is usually considered to be the cryptographically stronger function ([16]).

Similar remarks can be made on the encryption functions. The base specification requires DES, an algorithm that has shown to be vulnerable to brute-force attacks ([16], [17]).

We do not consider the well-known weaknesses of the mentioned algorithms a problem:

- o The problem of receiving unauthenticated messages is considered to be the main security threat for Mbus communication. We believe that HMAC-MD5 is sufficiently secure as a baseline algorithm. For application requiring special security concerning authentication of messages there is the option of using implementations that implement SHA-1.
- o Encryption is optional anyway, i.e. users can decide to have their implementations sending clear text Mbus messages. Given the local nature of Mbus communication this is feasible for most use cases. In case the base DES encryption is not considered sufficient there is still the possibility to use implementations that implement 3DES or IDEA.

However, application developers should be aware of incorrect IP implementations that do not conform to RFC 1122[2] and do send datagrams with TTL values of zero, resulting in Mbus messages sent to the local network link although a user might have selected host local scope in the Mbus configuration. In these cases the use of encryption SHOULD be considered if privacy is desired.

13. IANA Considerations

The IANA is requested to assign a port number and a multicast address. For the time being the tentative multicast address 224.255.222.239 and the port number 47000 (decimal) SHOULD be used.

References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, March 1997.
- [2] Braden, R., "Requirements for Internet Hosts -- Communication Layers", RFC 1122, October 1989.
- [3] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.
- [4] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.
- [5] Borenstein, N. and N. Freed, "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1521, September 1993.
- [6] Handley, M., Crowcroft, J., Bormann, C. and J. Ott, "The Internet Multimedia Conferencing Architecture", Internet Draft draft-ietf-mmusic-confarch-02.txt, October 1999.
- [7] Schulzrinne, H., Casner, S., Frederick, R. and V. Jacobsen, "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, January 1996.
- [8] Handley, M., Schulzrinne, H., Schooler, E. and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, March 1999.
- [9] Handley, M. and V. Jacobsen, "SDP: Session Description Protocol", RFC 2327, April 1998.

- [10] Meyer, D., "Administratively Scoped IP Multicast", RFC 2365, July 1998.
- [11] Ott, J., Perkins, C. and D. Kutscher, "Requirements for Local Conference Control", Internet Draft draft-ietf-mmusic-mbus-req-00.txt, December 1999.
- [12] Balenson, D., "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", RFC 1423, February 1993.
- [13] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.
- [14] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

Ott, et. al.

Expires July 3, 2000

[Page 30]

Internet-Draft

A Message Bus for Local Coordination

January 2000

- [15] U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1, April 1995.
- [16] Schneier, B., "Applied Cryptography", Edition 2, Publisher John Wiley & Sons, Inc., 1996.
- [17] distributed.net, "Project DES", WWW <http://www.distributed.net/des/>, 1999.
- [18] Microsoft, "BUG: Winsock Sends IP Packets with TTL 0", WWW <http://support.microsoft.com/support/kb/articles/Q138/2/68.asp>, March 19

Authors' Addresses

Joerg Ott
 TZI, Universitaet Bremen
 Bibliothekstr. 1
 Bremen 28359
 Germany

Phone: +49.421.218-7028
 Fax: +49.421.218-7000
 EMail: jo@tzi.de

Colin Perkins
 University College London
 Gower Street
 London WC1E 6BT
 United Kingdom

EMail: c.perkins@cs.ucl.ac.uk

Dirk Kutscher
 TZI, Universitaet Bremen
 Bibliothekstr. 1
 Bremen 28359
 Germany

Phone: +49.421.218-7595

Appendix A. Mbus Addresses for Conferencing

For conferencing application 5 address element keys are predefined:

| | |
|--------|---|
| conf | conference identifier |
| media | media type processed by application |
| module | module type of Mbus entity in a application |
| app | application name |

The conf element is used to designate the name of a conference in order to distinguish between entities that are present in more than one conference. See Transport (Section 6) for further notes concerning multiple presences using the Mbus.

The media element identifies the type of media processed by an application. Currently defined values are:

| | |
|------------|--|
| audio | An RTP audio stream |
| video | An RTP video stream |
| workspace | A shared workspace |
| whiteboard | A shared whiteboard |
| editor | A shared text editor |
| sap | A session announcement tool, using SAP |
| sip | A session invitation tool, using SIP |
| h323 | An ITU-T H.323 conference controller |
| rtsp | An RTSP session controller |
| control | A local coordination entity |

Other values are likely to be defined at a later date.

The module element defines a logical part of an application. The value 'ui' denotes the user-interface of an application, and the value 'engine' defines a media/protocol engine, and 'transcoder' defines a media transcoder. Other values may be defined in future.

The app element identifies the application being used (e.g.: rat, vic, etc.).

The instance element is used to distinguish several instances of the same application. This is a per-instance-unique identifier, which is not necessarily an integer. Many Unix applications will use the process-id (PID) number, although this is not a requirement. Note that if an end system is spread across several hosts, the instance MUST NOT be the process-id, unless e.g.. the host name or its IP address are included as well. Section 8 defines a bootstrap procedure ensuring that entities can track the abandoning and restarting of application instances as long as unique instance values are being used.

The following examples illustrate how to make use of the addresses:

| | |
|---|--|
| (conf:test media:audio module:ui app:rat id:4711-99@134.102.218.45) | The user interface of the rat application with the given id is taking part in conference test |
| (media:workspace module:ui) | The user interfaces of all workspace applications |
| (media:audio) | All audio applications |
| (app:rat) | All instances of the rat application |
| () | All entities |

Full Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC editor function is currently provided by the Internet Society.