The requirement of extending RFC4666 for the M3UA deployment
draft-zhang-sigtran-m3ua-req-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

This document may not be modified, and derivative works of it may not be created, except to publish it as an RFC and to translate it into languages other than English.

This document may only be posted in an Internet-Draft.

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/1id-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 August 18, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).
Abstract

RFC 4666 defines a protocol for supporting the transport of any SS7 MTP3-User signalling (e.g., ISUP and SCCP messages) over IP using the services of the Stream Control Transmission Protocol.

M3UA is designed for SEP-(TDM)-SG-(IP)-IPSEP and IPSEP-(IP)-IPSEP applications, so the network level management function isn't required. SSNM (SS7 Signalling Network Management) messages defined in M3UA are only used for interworking with SS7. RFC 4666 doesn’t define IPSEP-IPSTP-IPSEP application of M3UA. The signalling network management function for this application needs to be extended.

Some parts of the specification are unclear, which may lead to misinterpretations and may weaken interoperability.

This document provides extensions and clarifications to RFC 4666.

Conventions used in this document

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [1].
1. Introduction

RFC 4666 defines a protocol for supporting the transport of any SS7 MTP3-User signalling (e.g., ISUP and SCCP messages) over IP using the services of the Stream Control Transmission Protocol.

M3UA is designed for SEP-(TDM)-SG-(IP)-IPSEP and IPSEP-(IP)-IPSEP applications, so the network level management function isn’t required. SSNM (SS7 Signalling Network Management) messages defined in M3UA are only used for interworking with SS7. RFC 4666 doesn’t define IPSEP-IPSTP-IPSEP application of M3UA. The signalling network management function for this application needs to be extended.

Some parts of the specification are unclear, which may lead to misinterpretations and weaken interoperability.

This document provides extensions and clarifications to RFC 4666.

2. The requirement for IP based signalling network

The application of SIGTRAN standard for SG has ever solved the problems of interworking between No.7 Signalling System and IP system. It also helps to settle the problems about transmission of access network signalling in R4 CS core network.

The world trend of IP bearer for signalling will make SIGTRAN standard widely used in signalling network, and also make IP based signalling network possible.

An IP based SS7 signalling network using M3UA/SCTP/IP as transport layer has been defined by 3GPP, SEPs such as HLR, MSC can communicate with each other directly by accessing to this IP based signalling network. When deploying a large scale signalling network based on IP, it is better to separate the network into several sections, keep the number of SEPs in each section in an appropriate degree. IPSTPs are needed between different sections to simplify the GT data and converge the SCTP association data. And it is recommended that M3UA should be used on the IPSTP-IPSEP interface, while M2PA may be used on the IPSTP-IPSTP interface.
The architecture of IP based signalling network is as follows:

![Diagram of IP based signalling network]

Figure 1 The architecture of IP based signalling network.

3. The requirement for the extension of signalling network management function of M3UA for IPSEP-IPSTP-IPSEP application

As same as the traditional TDM based SS7 signalling network, an IP based SS7 signalling network also provides signalling network management functions, such as signalling traffic management, signalling link management, and signalling route management, to insure the availability and traffic transport capacity of a signalling network in case of failures and congestion.

For a large scale signalling network based on IP with IPSTPs, the usage of M2PA on IPSTP-IPSTP interface can help to realize the signalling network management between different sections of the signalling network. But M3UA can not fulfil the signalling network management within a section completely at present, the extension of it for this application is needed. The reason for the extension will be discussed in this section.
Within a section of a large scale signalling network based on IP with IPSTPs, the normal signalling transport route between two IPSEPs will transit an IPSTP. When the destination IPSEP is not available, Scenario 1, the IPSTP must notify the source IPSEP to choose another route. And when the user part of the destination IPSEP is not available, Scenario 2, the IPSTP must also notify the source IPSEP to stop the signalling traffic.

M3UA is designed for SEP-(TDM)-SG-(IP)-IPSEP and IPSEP-(IP)-IPSEP applications, so the network level management function isn’t required. SSNM (SS7 Signalling Network Management) messages defined in M3UA are only used for interworking with SS7. M3UA specification doesn’t define signalling network management function for the IPSEP-(IP)-IPSEP-(IP)-IPSEP application.

Scenario 1: the destination SP is not available

In Scenario 1, when IPSTP1 finds the destination IPSEP (AS,IPSEP2) in IP domain is not available, and there is no connection between IPSTP1 and IPSTP2, or the connection between IPSTP1 and IPSTP2 is not available. It is a matter of M3UA spec interpretation whether IPSTP1 sends a DUNA message or not to IPSEP1 upon failure of signaling connection towards IPSEP2. M3UA spec does not prohibit this, but it seems there is a bit of unclarity on whether SSNM Message can be sent by the IPSTP in the context of a AS->SG-AS interworking, while it is very clear that IPSTP can send such message in the context of SEP -> SG -> AS. In result, the source IPSEP (AS,IPSEP1) doesn’t know the route is unavailable and still sends traffic to IPSTP1, which makes the signalling transport failure.
Scenario 2: the user part of the destination SP is not available

In Scenario 2, when the user part of the destination IPSEP(AS, IPSEP2) is not available, M3UA doesn’t define the destination SP (AS, IPSEP2)’s M3UA layer can send proper SSNM message (DUPU) to notify the source IPSEP (AS, IPSEP1), and doesn’t define IPSTP’s M3UA layer can transfer the DUPU to the proper IPSEP (AS, IPSEP1) either. In addition, DUPU contains no DPC field to indicate the address of the source IPSEP (AS, IPSEP1) which is the originator of the message (DATA) that triggered the DUPU. In result, the source IPSEP (AS, IPSEP1) doesn’t know the user part of IPSEP2 is unavailable and still sends traffic to IPSEP2, which makes the signalling transport failure.
4. About the terminology

In section 1.2 it provides the terminology of the SEP and STP, but there all are nodes in SS7 network. After introducing M3UA, if all those IP SEP are connected each other, each IP SEP should configure all the other IP SEP’s SCTP and M3UA information. The maintenance and management work is too heavy.

So IP STP should be introduced into the network and each IP STP covers a number of IP SEP and each IP SEP need only configure the IP STP’s SCTP/M3UA information.

IP SEP sends correlative messages to IP STP, and it is the responsibility of IP STP to relay those message to another IP SEP.
For the scenario of IP STP, there is the need to introduce IPSTP and IPSEP.

5. About the sample configuration

In section 1.5 there are three examples where M3UA is used. But the examples focus on the scenarios of SG implement and IPSP to IPSTP. If the IPSTP is deployed in the IP based signalling network, the network model should be extended. At least, the network model about IPSEP-IPSTP-IPSEP, IPSEP-IPSTP/IPSTP/STP/SEP should be added in order to extend the application of M3UA in the IP based singling network.

6. About SCTP Client/Server Model

In section 1.4.8 there is a statement about the SCTP Client/Server Model for SG and IPSP to IPSP scenarios. In order to avoid the interoperability after IPSTP is deployed in the IP based signalling network, the SCTP Client/Server Model for IPSTP and IPSEP should be specified.

7. About the functional area

In section 1.4 the function areas which should be supported by SG and IPSP are listed. And the network management messages are defined in section 3.4 and it is the mandatory function to be supported by the nodes which deploy M3UA protocol. But the function about the network management function is not specified in section 1.4. Especially after the IPSTP is deployed in IP based signalling network, the network management function is more important. It is necessary to add M3UA signalling network management function in section 1.4 especial for the IPSTP and IPSEP.

8. About Destination User Part Unavailable (DUPU)

In section 3.4.5, the DUPU message is defined. But when the message is defined, it only considers the scenarios of SG and IPSP and not the scenario where IPSTP is deployed in the IP based signalling network. If IPSEP A sends a message to IPSEP B by through IPSTP, after the IPSEP B receives the M3UA layer DATA message, and finds that it could not be sent to appointed upper layer user, IPSEP B will feedback DUPU to the source point with the correlation reason. But if DUPU is not extended, the DUPU perhaps could not be returned back to IPSEP A by through IPSTP because DUPU only can be sent to IPSTP with the DPC is IPSTP. Only the source point code is included in the DUPU message, the DUPU can be feedback to the source point after the IPSTP’s M3UA Parses the source PC field to transmits it to
corresponding signalling point if the source PC not point to the IPSTP.

9. About procedures

This section describes the M3UA procedures in response to the M3UA special events. If the IPSTP is deployed in the IP based signalling network, the procedures to support DUPU in IPSEP-IPSTP interface and the procedures to support DUNA/DAVA/SCON/DAUD in IPSEP-IPSTP interface should be specified.

10. About sample configuration for BICC

In section 1.5 there are three examples where M3UA is used. But the examples focus on the scenarios of SG implement and IPSP to IPSTP. To IPSP-IPSP scenario, only the SCCP over M3UA is presented. As the popular call control protocol, BICC is widely used in the telecommunication network. And BICC is also based on M3UA. So the sample configuration for BICC Transport between IPSPs should also be presented.

11. About Message Length for M3UA message format

In section 3.1.4 the statement whether the message length should include the padding octets is inconsistent. The text states that the message length should include the padding octets but the note says that the message length can not include the padding octets. The inconsistent statements can bring on the interoperability problem. It is suggested that the note in the section 3.1.4 should be deleted.

12. About Destination State Audit (DAUD)

In section 3.4.3, the DAUD message is defined. But it does not specify whether IPSP can send DAUD with its own Point Code or not which brings on the divarication for understanding.

The statement should be declared definitely whether it is allowed or not. And if the IPSTP receives a DAUD message from IPSEP A with the Affected Point Code parameter which is just the IPSEP A, the IPSTP should refuse it or return the status. It should also be declared definitely to avoid interoperability problem.
13. Formal Syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in RFC-2234 [2].

14. Security Considerations

Implementations MUST follow the normative guidance of RFC3788 on the integration and usage of security mechanisms in SIGTRAN protocol.

15. IANA Considerations

This document contains no new actions for IANA.

16. Conclusions

According to this document, it is needed to supplement and extend RFC4666 for its widely usage in the IP based Signalling Network.

17. Acknowledgments

The authors wish to thank Zhao Yuyi, Peng Jin, Zhang Juan, and many others for their invaluable comments.
18. References

18.1. Normative References


Author’s Addresses

Zhang Hao
China Mobile
53A XiBianMenNei Ave, XuanWu District, Beijing, China
Phone: 86 10 66006688 3281
Email: zhanghao@chinamobile.com

Chen Xu
China Mobile
53A XiBianMenNei Ave, XuanWu District, Beijing, China
Phone: 86 10 66006688 3163
Email: chenxu@chinamobile.com

Duan Xiaodong
China Mobile
53A XiBianMenNei Ave, XuanWu District, Beijing, China
Phone: 86 10 66006688 3062
Email: duanxiaodong@chinamobile.com

Peng Jin
China Mobile
53A XiBianMenNei Ave, XuanWu District, Beijing, China
Phone: 86 10 66006688 3252
Email: pengjin@chinamobile.com
Zhao Yuyi  
China Mobile  
53A XiBianMennei Ave, XuanWu District, Beijing, China  
Phone: 86 10 66006688 3072  
Email: zhaoyuyi@chinamobile.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Copyright Statement

Copyright (C) The IETF Trust (2008).
This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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