Internet Draft
Document: draft-choi-ipv6-signaling-interworking-00.txt
Expiration Date: April 2003

Jun Kyun Choi
Min Ho Kang
Gyu Myoung Lee
ICU
Joo Uk Um
Yong Jae Lee
KT(Korea Telecom)
Jeong Yun Kim
ETRI

October 2002

Signaling Interworking for IPv6 Network

Status of this Memo

Abstract

In this draft, we describe the features and requirements of QoS signaling in IPv6 network to explain the needs of end-to-end QoS signaling. We discuss the signaling interworking between IPv6 network and other network. The delivering methods of signaling messages in IPv6 network are also presented in Appendix.

Conventions

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.

Table of Contents

1. Introduction

The current Internet will smoothly transit from IPv4 to IPv6. Consequently, supporting IPv6 is an urgent task for services on the Internet. IPv6 has many features to support QoS and other capabilities for the emerged networks. Signaling point of view, we obviously need a practical strategy for supporting of IPv6 QoS services

Many signaling mechanisms are defined and developed to support Quality of Service (QoS) in IP networks. Those are chosen by users to satisfy their needs, objectives, and implementation costs. Also most of the signaling protocols are based on the underlying network infrastructure, i.e. IP networks, but they don't depend on the minor version of the network. For example, one signaling protocol designed for the IPv4 network can be used in IPv6 network without modifying the specification of the signaling mechanism. Rather than to do like that, the signaling protocol adopt itself to the different version of network implementation by defining option fields like IP version information field and related information like IPv4 addresses (32 bits) or IPv6 addresses (128 bits). Therefore, Signaling in IPv6 network MUST consider the interworking with IPv4 network and existing wireline/wireless telco network.

In this draft, we describe the features and requirements of QoS signaling in IPv6 network to explain the needs of end-to-end QoS signaling. We discuss the signaling interworking between IPv6 network and other network. In particular, deployment point of view, we explain three stages of evolution scenarios and mapping of IPv6 signaling with IPv4 in some detail. Finally, the delivering methods of signaling messages in IPv6 network are presented in appendix.

2. The Needs of QoS Signaling in IPv6 networks

2.1. The Features of QoS related Signaling in IPv6 Networks

We describe the features of signaling mechanisms in IPv6 network with supporting QoS to explain the needs of QoS signaling.

o QoS support

Information with QoS controlling is important context of signaling packet. With aggregated flow concept, IPv6 signaling mechanisms can provide finer QoS granularity than DiffServ model [1], and more scalable than IntServ model [2].

o Resource Reservation

The key role of signaling protocol is to allocate and reserve the network resource for the purpose of meeting end-to-end QoS requirements along the entire path. The signaling protocol MUST be able to deal with such resource allocation requests.

o Priority Flow Control

Each node has many flows with different priority of various data rates and QoS requirements. These flows are classified and scheduled with the capability of making intelligent decisions on how resource allocation SHOULD be controlled.

o Explicit route

In IPv6 specification [3], there is a route extension header to use explicit route. Explicit route is important for traffic engineering in IPv6 networks. There is already ROUTE object in RSVP-TE specification [4]. In the case of CR-LDP [5], some TLVs are defined to be used for this purpose. We discuss the explicit route setup for interworking with MPLS signaling in IPv6 network. (See section 4.2)

o Scalability

The performance of the signaling protocol SHOULD not largely depend on the scale of the network to which IPv6 is applied (e.g. the number of nodes, the number of physical links etc). The signaling function SHOULD keep constant performance as much as possible regardless of network size. Aggregating flows can reduce resource allocation and runtime management overhead.

o Flow Label Information Distribution

To make use of flow label field [6] of IPv6 basic header and identify the flow label between the routers on specific path, label-binding information SHOULD be delivered between the related routers. The related routers are on the path of the flow. Label value is only meaningful between a pair of routers. And the label value is predetermined before forwarding data packet along the path.

2.2. The Requirements of QoS Signaling Protocol in IPv6 Networks

Besides of features of signaling, we SHOUD consider the following requirements of QoS signaling in IPv6 networks.

o Backward compatibility

The existing signaling protocols such as RSVP, RSVP-TE, CR-LDP and so on are implemented in IPv4 network. These signaling protocols MUST be operated in IPv6 network. Therefore, they MUST support backward compatibility for operating both IPv6 and IPv4.

o Easy to implement

There are two aspects related with this issue. First, we can consider the compatibility of the new signaling with existing signaling. So the implementation can be done with minimum modification of previous architecture and components. Second we can omit some functions of previous signaling so that we just make a light-weight signaling mechanism. We are still studying about this carefully because it makes some effects with other various factors such like the capabilities of this new signaling and the signaling translation between two heterogeneous AS's. We can think above two factors simultaneously and SHOULD make some trade-off.

o Signaling interworking between IPv6 and IPv4

To be gradually deployed, we can consider the situation of mixed nodes that some implement the IPv6 signaling and others implement the IPv4 signaling. In this environment, we consider signaling interworking issues. So we will explain mapping for IPv6 signaling interworking with IPv4 in section 3.

o Traffic parameters for QoS negotiation

There are many traffic parameters such as peak data rate, peak burst size, committed data rate, committed burst size, excess burst size and so on. The QoS signaling applies the traffic parameters per aggregated flow. To make use of this, state of QoS information SHOLD be maintained per aggregated flow. Also the adding and deleting of a flow with respect to the aggregated flow SHOULD be carefully managed. An aggregated flow is not just used for label-related switching, but also used for classification information in routers on path. So the traffic parameter information SHOULD be stored in the router with the information related with an aggregated flow identifier(s).

o Mobility support

To provide the QoS in mobile environment, we SHOLD consider the mobility of nodes and dynamic behavior of related flows. In signaling, we are concerning two problems. First the flow management can be considered with per aggregated flow or per flow. In some point, snapshot of network can be described with many aggregated flows and related QoS management. But as time goes, some flow of mobile node departs one aggregated flow and join the other aggregated flow. Second the support of micro mobility issues. To make use of old flow related resources as much as possible, we should define Nearest Common Router (NCR) and provide the finding mechanism. This work is under working. We just consider the need of modification or adaptation of that mechanism in our work.

o Make use of IPv6 features

IPv6 have many features to make use of that to provide some new functions. We may use IPv6 extension header. See section 4 for more information on this issue.

o Inter-operation with other QoS-supporting networks

In this version, we cannot consider this issue.

3. Signaling Interworking for IPv6 network

3.1. Signaling Interworking Between IPv6 and IPv4

The current Internet will smoothly transit from IPv4 to IPv6. Deployment point of view, we consider three stages of evolution scenarios

- first stage (stage 1): IPv4 ocean and IPv6 island
- second stage (stage 2): IPv6 ocean and IPv4 island
- third stage (stage 3): IPv6 ocean and IPv6 island

In first stage shown in Figure 1, MPLS-based core network (e.g., IPv4 ocean) and IPv6 access network (e.g., IPv6 island)is deployed. In this environment, core signaling such as RSVP-TE and CR-LDP is used in IPv4 ocean and access signaling such as RSVP and RSVP-TE is used in IPv6 island. To support end-to-end QoS signaling, these protocols SHOUD perform the mapping of IPv6 with IPv4. Flow label information of IPv6 header is translated to FEC(Forwarding Equivalent Class) [7] information of MPLS. For this reason, signaling interworking function is needed. Using this QoS signaling, flow information is transmitted unchanged from source to destination and the required resource is reserved and end to end path is established.

```
+-------------+       +---------------+       +-------------+
| IPv6 island |-------|  IPv4 ocean   |-------| IPv6 island |
|             |-------|    (MPLS)     |-------|             |
+-------------+       +---------------+       +-------------+
  Flow Label -- mapping --   FEC   --  mapping -- Flow Label

|<----------->|       |<------------->|       |<----------->|
 RSVP/RSVP-TE          RSVP-TE/CR-LDP          RSVP/RSVP-TE
(Access signaling)     (Core signaling)    (Access signaling)

|<--------------------------------------------------------->|
                   end-to-end QoS signaling
```

Figure 1. Signaling mapping (stage 1)

In second stage shown in Figure 2, IPv6 network will dominate over IP4 network. This network is composed of IPv6-based core network (e.g., IPv6 ocean) and IPv4-based access network (e.g., IPv4 island). The existing IPv4 network is operated in MPLS. In this environment, core signaling such as RSVP-TE and CR-LDP is used in IPv6 ocean and access signaling such as RSVP and RSVP-TE is used in IPv4 island. FEC information of IPv4 is translated to flow label information of IPv6.

```
   +-------------+       +---------------+       +-------------+
   | IPv4 island |-------|  IPv6 ocean   |-------| IPv4 island |
   |   (MPLS)    |-------|               |-------|   (MPLS)    |
   +-------------+       +---------------+       +-------------+
         FEC -- mapping -- Flow Label   --  mapping -- FEC

   |<----------->|       |<------------->|       |<----------->|
     RSVP/RSVP-TE          RSVP-TE/CR-LDP          RSVP/RSVP-TE
   (Access signaling)     (Core signaling)    (Access signaling)

   |<--------------------------------------------------------->|
                      end-to-end QoS signaling
```

Figure 2. Signaling mapping (stage 2)

In third stage shown in Figure 3, IPv6 protocol is implemented both core network (e.g., IPv6 ocean) and access network (e.g., IPv6 island). Signaling protocol like RSVP-TE MAY be used without signaling translation.

```
   +-------------+       +---------------+       +-------------+
   | IPv6 island |-------|  IPv6 ocean   |-------| IPv6 island |
   +-------------+       +---------------+       +-------------+
    Flow Label - mapping -- Flow Label -- mapping - Flow Label

   |<----------->|       |<------------->|       |<----------->|
     RSVP/RSVP-TE          RSVP-TE/CR-LDP          RSVP/RSVP-TE
   (Access signaling)     (Core signaling)    (Access signaling)

   |<--------------------------------------------------------->|
                        end-to-end QoS signaling
```

Figure 3. Signaling mapping (stage 3)

3.2. Signaling Interworking Between IPv6 and Existing Telco Network

We SHOULD consider the signaling interworking between IPv6 and existing Telco network. Telco network may be composed of PSTN, cellular, IMT2000 network and so on. Using signaling, the physical/logical circuit is established. To support end-to-end QoS signaling, we consider two cases (see Figure 4-5). Both cases SHOUD perform the mapping of flow label and phsyiscal/logical circuit.

```
+-------------+      +-----------------+      +-------------+
| IPv6 Client |------|  PSTN/Cellular/ |------| IPv6 Client |
|   Network   |------| IMT2000-Network |------|   Network   |
+-------------+      +-----------------+      +-------------+
Flow label - mapping - physical/logical- mapping - Flow Label
                           Circuit
|<----------->|      |<--------------->|      |<----------->|
Acess Signaling        Telco Signaling      Access Signaling

|<--------------------------------------------------------->|
                   end-to-end QoS signaling
```

Figure 4. Signaling mapping for Telco network (case 1)


```
+-------------+      +-----------------+      +-------------+
|   PSTN      |------|      IPv6       |------|  Cellular   |
|   ISDN      |------|      Ocean      |------|  INT-2000   |
+-------------+      +-----------------+      +-------------+
Physical/  -- mapping - Flow Label-- mapping - Physical/
Logical Circuit                              Logical Circuit
|<----------->|      |<--------------->|      |<----------->|
Telephone Signaling     Core Signaling            Cellular/
                                           IMT-2000 Signaling
|<--------------------------------------------------------->|
                   end-to-end QoS signaling
```

Figure 5. Signaling mapping for Telco network (case 2)

3.3. Support of Domain Service Model on Optical Transport Network

IPv6 network SHOULD support the signaling interworking with optical transport network. The optical transport network control plane reuse IP-based protocols that are based on the signaling and routing mechanisms developed for IP traffic engineering applications. Core signaling such as Optical-UNI (User-Network-Interface) [8] and GMPLS signaling (RSVP-TE extensions [9], CR-LDP extensions [10]) are used in domain service model on optical transport network (see Figure 6). To support end-to-end QoS signaling, these protocols SHOULD perform the interworking with access signaling of IPv6 client network. Flow label information of IPv6 is translated to optical label information.

```
+-------------+      +-----------------+      +-------------+
| IPv6 Client |------|Optical Transport|------| IPv6 Client |
|   Network   |------|     Network     |------|   Network   |
+-------------+      +-----------------+      +-------------+
Flow label - mapping -- Optical Label -- mapping - Flow Label

|<----------->|      |<--------------->|      |<----------->|
Acess Signaling     O-UNI, GMPLS Signaling   Access Signaling

|<--------------------------------------------------------->|
                   end-to-end QoS signaling
```

Figure 6. Signaling mapping for optical network

4. Other Considerations

4.1. Support of VPN service in IPv6 network

One of many IPv6 applications may be VPN (Virtual Private Network) service. VPN [11] refers to the communication between a set of sites, making use of a shared network infrastructure. Multiple sites of a private network may therefore communicate via the public infrastructure, in order to facilitate the operation of the private network. For VPN service, we SHOULD consider security, economics and QoS etc. In particular, security point of view, IPv6 network can support security-enabled signaling function for VPN service using the authentication header and the encapsulation security payload header of IPv6.

4.2. Explicit route setup

In some situations, the network administrators may desire to forward certain classes of traffic along certain pre-specified paths, where these paths differ from the Hop-by-hop path that the traffic would ordinarily follow. The explicit route may be a configured one, or it may be determined dynamically by some means, e.g., by constraint-based routing [7]. The extension header of IPv6 may support explicit route setup.

For example, one can want to use the IPv6 Routing header to send signaling packet along the desired path rather than the shortest path. This is reasonable because the IPv6 routers may be implement routing header processing component so we can use that without any additional functional implementations. Also we can think about the hop-by-hop header to notify routers that the packets have some signaling and reservation information. These things are already considered in other signaling mechanism. That means we can use the IPv6 native features or don't use of them. There is another viewpoint related with this. If the same information is transferred with IPv6 header and payload, there may be the consistency problems. So some people want to make one of choices, not both of them.

5. IANA Considerations

The value field described in Appendix SHOULD be registered and maintained by IANA. The New values SHOULD be to be assigned via IETF Consensus as defined in RFC 2434 [12].

6. Security Considerations

This document does not have any security concerns. The security requirements using this document are described in the referenced documents.

Appendix. The delivering methods of signaling messages in IPv6 network

In this appendix, we will describe the delivering methods of existing signaling protocols in IPv6 networks via using IPv6 extension headers. The use of these methods in existing signaling protocols is discussed in the last of this section.

1. RSVP/RSVP-TE for IPv6 (including RSVP-TE extensions for GMPLS)

o Using Router Alert Option

Router alert option [13] within the IPv6 Hop-by-Hop option header has the semantic "routers should examine the datagram more closely". Using this option, IPv6 datagram containing signaling messages are indicated and taken actions.

The router alert option has the following format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0|0 0 1 0 1|0 0 0 0 0 0 1 0|        Value (2 octets)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   length = 2
```

The first three bits of the first byte are zero and the value 5 in the remaining five bits is the Hop-by-Hop Option Type number. RFC 2460 [3] specifies the meaning of the first three bits. By zeroing all three, this specification requires that nodes not recognizing this option type should skip over this option and continues processing the header and that the option must not change en route.

There MUST only be one option of this type, regardless of value, per Hop-by-Hop header.

Value: A 2 octets code in network byte order with the following values

0	Datagram contains a Multicast Listener Discovery message [14].
1	Datagram contains RSVP [15] message.
2	Datagram contains an Active Networks message.
3-65535	Reserved to IANA for future use.

Alignment requirement: 2n+0

Values are registered and maintained by the IANA.

We suggest the new value (= 3) for RSVP-TE messages. The value 3 is REQUIRED the approval of IETF and SHOULD be assigned by IANA. Other

signaling messages MAY be added. In this case, the value for new signaling message SHOULD be assigned by IANA.

The described method has some advantages and disadvantages. It is not necessary to implement the new protocol for signaling. The existing signaling message is used without change. However, all IPv6 datagram containing a signaling message MUST contain this option within the IPv6 Hop-by-Hop Option Header of such datagram. The additional option header is redundant.

o Next Header for signaling

This method uses the new Next Header value for signaling message. Message body includes signaling messages like RSVP/RSVP-TE. Every signaling message is preceded by an IPv6 header or by more IPv6 extension headers. The signaling message is identified by a Next Header value in the immediately preceding header.

The signaling messages have the following general format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+                                                               +
|                        Message Body                           |
+                     (signaling message)                       +
```

Version   4-bit Internet Protocol version number = 6.

Traffic Class   8-bit traffic class field.

Flow Label	20-bit flow label.
Payload Length	16-bit unsigned integer. Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets
Next Header	8-bit selector. Identifies the type of signaling message immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field [16].
Hop Limit	8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.
Source Address	128-bit address of the originator of the packet.
Destination Address	128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).

For this method, we MUST assign the new Next Header value of IPv6 header. Currently, RSVP is already assigned the value 46 decimal in RFC 1700 [16].

For example, if the Next Header value of IPv6 header is 46 decimal the following ISMP message is RSVP message. The Next Header value of other unassigned signaling messages SHOULD be assigned by IANA.

This second method may be used for the signaling protocols which are running on the IP layer.

Compared with the method using router alert option, this method is very simple because of no additional extension header. Therefore, the complexity of processing is reduced but this new function MUST be implemented within IPv6 header.

Note: the signaling protocols, like SIP (Session Initiation Protocol)[17], that are used for end-to-end path may use the option TLVs to indicate the presence of the signaling information. We already know that the real-time service cannot be served without support of intermediate node. If some end-to-end sessions are need to be guaranteed to their perceived QoS, the intermediate nodes those are on the path may use the information to do something related with QoS implicitly.

2. CR-LDP for IPv6 (including CR-LDP extensions for GMPLS)

In the case of RSVP-TE, if the header of a packet is indicating "This packet carries the signaling information." then the intermediate routers and the end host can make different treatment on just only look at the IP header.

On the other hand, like CR-LDP, the protocol running on the TCP(UDP) layer may also make use of the benefit that IP header already notify the existence of signaling information in the payload of IP packet. Originally in the CR-LDP protocol, the signaling information is transferred along the path per hop. If a router sees the notification of signaling information in the IP header, it can forward the signaling packet and processing the signaling information simultaneously. So the forwarding direction of packet can be done faster than old mechanisms.

References

[1] S. Blake, et al. "An Architecture for Differentiated Services", RFC 2475, December 1998.

[2] R. Braden, et al. "Integrated Services in the Internet Architecture: an Overview", RFC 1633, June 1994.

[3] S. Deering, et al. "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[4] D. Awduche, et al. "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[5] B. Jamoussi, et al. "Constraint-Based LSP Setup using LDP", RFC 3212, January 2002.

[6] J. Rajahalme, et al. "IPv6 Flow Label Specification", Internet-Draft draft-ietf-ipv6-flow-label-03.txt, work in progress, September 2002.

[7] E. Rosen, "Multiprotocol Label Switching Architecture", RFC3031, January 2001.

[8] The Optical Interworking Forum, "UNI 1.0 Signaling Specification," December, 2001.

[9] Lou Berger, et al. "Generalized MPLS Signaling - RSVP-TE Extensions", Internet-Draft draft-ietf-mpls-generalized-rsvp-te-

09.txt, work in progress, September 2002.

[10] Peter Ashwood-Smith, et al. "Generalized MPLS Signaling - CR-LDP Extensions", Internet-Draft draft-ietf-mpls-generalized-cr-ldp-07.txt, August 2002.

[11] E. Rosen, et al. "BGP/MPLS VPNs", RFC 2547, March 1999.

[12] T. Narten, et al. "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 2434, October 1998.

[13] C. Partridge, et al. "IPv6 Router Alert Option", RFC 2711, October 1999.

[14] S. Deering, et al. "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[15] R. Braden, Ed. et al. "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997

[16] J. Reynolds, et al. "Assign Numbers", RFC 1700, October 1994.

[17] A. Vemuri, et al. "Session Initiation Protocol for Telephones (SIP-T): Context and Architectures", RFC 3372, September 2002.

Acknowledgements

This work was supported in part by KOSEF (Korea Science and Engineering Foundation) and MIC (Ministry of Information and Communication) of Korean government.

Author's Addresses

Jun Kyun Choi
Information and Communications University (ICU)
58-4 Hwa Ahm Dong, Yuseong, Daejeon
Korea 305-732
Phone: +82-42-866-6122
Email: jkchoi@icu.ac.kr

Min Ho Kang
Information and Communications University (ICU)
58-4 Hwa Ahm Dong, Yuseong, Daejeon

Korea 305-732
Phone: +82-42-866-6136
Email: mhkang@icu.ac.kr

Gyu Myoung Lee
Information and Communications University (ICU)

58-4 Hwa Ahm Dong, Yuseong, Daejeon
Korea 305-732
Phone: +82-42-866-6231
Email: gmlee@icu.ac.kr

Joo Uk Um
KT(Korea Telecom)
206 Jungja-dong, Bungdang-gu, Sungnam-City
Kyunggi Province, 463-711, Korea
Phone:+82-31-727-6610
Email: Jooukum@kt.co.kr

Yong Jae Lee
KT(Korea Telecom)
206 Jungja-dong, Bungdang-gu, Sungnam-City
Kyunggi Province, 463-711, Korea
Phone:+82-31-727-6610
Email: cruiser@kt.co.kr

Jeong Yun Kim
ETRI (Electronics and Telecommunications Research Institute)
161 KaJong-Dong, Yusong-Gu, Daejeon
Korea 305-309
Phone: +82-42-866-5311
Email: jykim@etri.re.kr

Full Copyright Statement

Document: draft-choi-ipv6-signaling-interworking-00.txt

Expiration Date: April 2003