Multicast Mobility in MIPv6: Problem Statement and Brief Survey
<draft-irtf-mobopts-mmcastv6-ps-01.txt>

IPR Statement

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 [1].

Status of this Memo

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

This document is a submission of the IRTF MobOpts RG. Comments should be directed to the MobOpts RG mailing list, mobopts@irtf.org.

Abstract

In this document we discuss mobility extensions to current IP layer multicast solutions. Problems arising from mobile group communication in general, in the case of multicast listener mobility and for mobile Any Source Multicast as well as Source Specific Multicast senders are documented. Characteristic aspects of multicast routing and deployment issues for fixed IPv6 networks are summarized. The principal approaches to the multicast mobility problems are outlined subsequently.
Table of Contents

1. Introduction and Motivation........................................3
2. Problem Description................................................4
   2.1 Generals......................................................4
   2.2 Multicast Listener Mobility................................6
   2.3 Multicast Source Mobility..................................6
     2.3.1 Any Source Multicast Mobility.........................6
     2.3.2 Source Specific Multicast Mobility....................7
   2.4 Deployment Issues...........................................8
3. Characteristics of Multicast Routing Trees under Mobility.......9
4. Layer 2 Aspects...................................................10
   4.1 General Background........................................10
   4.2 Multicast for Specific Technologies........................10
     4.2.1 802.11 WLAN........................................10
     4.2.2 802.16 WIMAX.........................................11
     4.2.3 3GPP................................................12
     4.2.4 DVB-H / DVB-IPDC.....................................13
   4.3 Vertical Multicast Handovers................................13
5. Solutions........................................................13
   5.1 General Approaches.........................................13
   5.2 Solutions for Multicast Listener Mobility...................14
     5.2.1 Agent Assistance......................................14
     5.2.2 Hybrid Architectures................................14
     5.2.3 MLD Extensions.......................................15
   5.3 Solutions for Multicast Source Mobility....................15
     5.3.1 Any Source Multicast Mobility Approaches.............16
     5.3.2 Source Specific Multicast Mobility Approaches......16
6. Security Considerations..........................................17
7. IANA Considerations.............................................18
   Appendix A. Implicit Source Notification Options................18
8. References.......................................................18

Acknowledgments....................................................24
Author’s Addresses..................................................24
Intellectual Property Statement......................................24
1. Introduction and Motivation

Group communication forms an integral building block of a wide variety of applications, ranging from public content distribution and streaming over voice and video conferencing, collaborative environments and (massive multiplayer) gaming up to the self-organization of distributed systems, services or autonomous networks. Its support by network layer multicast will be needed, whenever globally distributed, scalable, serverless or instantaneous communication is required. As broadband media delivery more and more emerges to be a typical mass scenario, scalability and bandwidth efficiency of multicast routing continuously gains relevance. The idea of Internet multicasting already arose in the early days [2], soon leading to Deering’s fruitfully adopted host group model [3]. Its realization will be of particular importance to mobile environments, where users commonly share frequency bands of limited capacity. The rapidly increasing mobile reception of ‘infotainment’ streams may soon require a wide deployment of mobile multicast services. Multicast mobility consequently has been a concern for about ten years [4] and led to innumerous proposals, but no generally accepted solution.

The fundamental approach to deal with mobility in IPv6 [5] is stated in the Mobile IPv6 RFCs [6,7]. MIPv6 [6] only roughly treats multicast mobility, in a pure remote subscription approach or through bi-directional tunneling via the Home Agent. Whereas the remote subscription suffers from slow handovers, as it relies on multicast routing to adapt to handovers, bi-directional tunneling introduces inefficient overheads and delays due to triangular forwarding. Therefore none of the approaches can be considered solutions for a deployment on large scale. A mobile multicast service for a future Internet should admit ‘close to optimal’ routing at predictable and limited cost, robustness combined with a service quality compliant to real-time media distribution.

Intricate multicast routing procedures, though, are not easily extensible to comply with mobility requirements. Any client subscribed to a group while in motion, requires delivery branches to pursue its new location; any mobile source requests the entire
delivery tree to adapt to its changing positions. Significant effort has already been invested in protocol designs for mobile multicast receivers. Only limited work has been dedicated to multicast source mobility, which poses the more delicate problem [50].

In multimedia conference scenarios, games or collaborative environments each member commonly operates as receiver and as sender for multicast based group communication. In addition, real-time communication such as voice or video over IP places severe temporal requirement on mobility protocols: Seamless handover scenarios need to limit disruptions or delay to less than 100 ms. Jitter disturbances are not to exceed 50 ms. Note that 100 ms is about the duration of a spoken syllable in real-time audio.

It is the aim of this document, to specify the problem scope for a multicast mobility management as to be refined in future work. The attempt is made to subdivide the various challenges according to their originating aspects and to present existing proposals for solution, as well as major bibliographic references.

2. Problem Description

2.1 Generals

Multicast mobility must be considered as a generic term, which subsumes a collection of quite distinct functions. At first, multicast communication divides into Any Source Multicast (ASM) [3] and Source Specific Multicast (SSM) [8,9]. At second, the roles of senders and receivers are asymmetric and need distinction. Both may individually be mobile. Their interaction is facilitated by a multicast routing function such as DVMRP [10], PIM-SM/SSM [11,12], Bi-directional PIM [13], CBT [14], BGMP [15] or inter-domain multicast prefix advertisements via MBGP [16] and the multicast listener discovery protocol [17,18].

Any multicast mobility solution must account for all of these functional blocks. It should enable seamless continuity of multicast sessions when moving from one IPv6 subnet to another. It should preserve the multicast nature of packet distribution and approximate optimal routing. It should support per flow handover for multicast traffic, as properties and designations of flows may be of distinct nature.

The host group model extends network layer unicast service capabilities. In concordance with the architecture of fixed networks, multicast mobility management should transparently utilize or smoothly extend the unicast functions of MIPv6 [6], its security extensions [7,19], its expediting schemes FMIPv6 [20] and HMIPv6
[21], its context transfer protocols [22] and its multihoming capabilities [23,24]. It is desirable to avoid multicast-specific solutions, whenever a general approach jointly supporting unicast and multicast can be derived.

Multicast routing dynamically adapts to session topologies, which then may change under mobility. However, depending on the topology and the protocol in use, routing convergence may arrive at a time scale close to seconds, or even minutes and is far too slow to support seamless handovers for interactive or real-time media sessions. The actual temporal behavior strongly depends on the routing protocol in use and on the geometry of the current distribution tree. A mobility scheme that arranges for adjustments, i.e., partial changes or full reconstruction of multicast trees, is forced to comply with timing sufficiently tolerant for protocol convergence. Special attention is needed with a possible rapid movement of the mobile node, as this may occur at much higher rates than compatible with protocol convergence.

IP layer multicast packet distribution is an unreliable service, which is bound to connectionless transport protocols. Packet loss thus will not be handled in a predetermined fashion. Mobile multicast handovers should not cause significant packet drops. Due to statelessness the bi-casting of multicast flows does not cause foreseeable degradations of the transport layer.

Group addresses in general are location transparent, even though there are proposals to embed unicast prefixes or Rendezvous Point addresses [25]. Addresses of sources contributing to a multicast session are interpreted by the routing infrastructure and by receiver applications, which frequently are source address aware. Multicast therefore inherits the mobility address duality problem for source addresses, being a logical node identifier, i.e., the home address (HoA) at the one hand, and a topological locator, the care-of-address (CoA) at the other. The network layer of group members, i.e., multicast senders, forwarders and receivers, needs to carefully account for address duality issues by means of binding caches, extended multicast states or signaling.

Multicast sources in general operate decoupled from their receivers in the following sense: A multicast source submits data to a group of unknown receivers and thus operates without any feedback channel. It neither has means to inquire on properties of its delivery trees, nor will it be able to learn about the state of its receivers. In the event of an inter-tree handover, a mobile multicast source therefore is vulnerable to losing receivers without taking notice. (Cf. Appendix A for implicit source notification approaches). Applying a MIPv6 mobility binding update or return routability procedure will likewise break the semantic of a receiver group remaining
unidentified by the source and thus cannot be applied in unicast analogy.

2.2 Multicast Listener Mobility

A mobile multicast listener entering a new IP subnet faces the problem of transferring the multicast membership context to its new point of attachment. This can either be achieved by (re-)establishing a tunnel or by transferring the MLD Listening State information of MN’s moving interface(s) to the new access router(s). In the latter case it may encounter either one of the following conditions: The new network may not be multicast enabled or the specific multicast service in use may be unsupported or prohibited. Alternatively, the requested multicast service may be supported and enabled in the new network, but the multicast groups under subscription may not be forwarded to it. Then current distribution trees for the desired groups may reside at large routing distance. It may as well occur that data of some or all groups under subscription of the mobile node are received by one or several local group members at the instance of arrival and that multicast streams flow natively.

The problem of achieving seamless multicast listener handovers is thus threefold:
- Ensure multicast reception even in visited networks without appropriate multicast support.
- Expedite primary multicast forwarding to comply with a seamless timescale at handovers.
- Realize native multicast forwarding whenever applicable to preserve network resources and avoid data redundancy.

Additional implications for the infrastructure remain. In changing its point of attachment a mobile receiver may not have enough time to leave groups in the previous network. Also, packet duplication and disorder may result from the change of topology.

2.3 Multicast Source Mobility

2.3.1 Any Source Multicast Mobility

A node submitting data to an ASM group either defines the root of a source specific shortest path tree (SPT), distributing data towards a rendezvous point or receivers, or it forwards data directly down a shared tree, e.g., via encapsulated PIM register messages. Aside from tunneling or shared trees, forwarding along source specific delivery trees will be bound to a topological network address due to reverse path forwarding (RPF) checks. A mobile multicast source moving away is solely enabled to either inject data into a previously established delivery tree, which may be a rendezvous point based shared tree, or to (re-)define a multicast distribution tree compliant to its new
location. In pursuing the latter the mobile sender will have to proceed without control of the new tree construction due to decoupling of sender and receivers.

A mobile multicast source consequently must meet address transparency at two layers: In order to comply with RPF checks, it has to use an address within the IPv6 basic header’s source field, which is in topological concordance with the employed multicast distribution tree. For application transparency the logical node identifier, commonly the HoA, must be presented as packet’s source address to the socket layer at the receiver side.

Conforming to address transparency and temporal handover constraints will be major problems for any route optimizing mobility solution. Additional issues arrive from possible packet loss and from multicast scoping. A mobile source away from home must attend scoping restrictions, which arise from its home and its visited location [6].

Within intra-domain multicast routing the employment of shared trees may considerably relax mobility related complexity. Relying upon a static rendezvous point, a mobile source may continuously submit data by encapsulating packets with its previous topologically correct or home source address. Constraints even weaken, when bi-directional PIM is used. Intra-domain mobility is transparently covered by bi-directional shared domain-spanning trees, eliminating the need for tunneling data to reach a rendezvous point.

However, issues arise in inter-domain multicast scenarios, whenever notification of source addresses is required between distributed instances of shared trees. A new CoA acquired after a mobility handover will necessarily be subject to inter-domain record exchange. In presence of embedded rendezvous point addresses [25], e.g., for inter-domain PIM-SM, the primary rendezvous point will be globally appointed and the signaling requirements obsolete.

2.3.2 Source Specific Multicast Mobility

Fundamentally, Source Specific Multicast has been designed for static addresses of multicast senders. Source addresses in client subscription to SSM groups are directly used for route identification. Any SSM subscriber is thus forced to know the topological address of its group contributors. SSM source identification invalidates, when source addresses change under mobility. Hence client implementations of SSM source filtering MUST be MIPv6 aware in the sense that a logical source identifier (HoA) is correctly mapped to its current topological correspondent (CoA).

Consequently source mobility for SSM packet distribution requires a dedicated conceptual treatment in addition to the problems of mobile
ASM. As a listener is subscribed to an \((S,G)\) channel membership and as routers have established an \((S,G)\)-state shortest path tree rooted at source \(S\), any change of source addresses under mobility requests for state updates at all routers and all receivers. On source handover a new SPT needs to be established, which partly will coincide with the previous SPT, e.g., at the receiver side. As the principle multicast decoupling of a sender from its receivers likewise holds for SSM, client updates needed for switching trees turns into a severe problem.

An SSM listener subscribing to or excluding any specific multicast source, may want to rely on the topological correctness of network operations. The SSM design permits trust in equivalence to the correctness of unicast routing tables. Any SSM mobility solution should preserve this degree of confidence. Binding updates for SSM sources thus should have to prove address correctness in the unicast routing sense, which is equivalent to binding update security with a correspondent node in MIPv6 [6].

All of the above severely add complexity to a robust SSM mobility solution, which should converge to optimal routes and, for the sake of efficiency, should avoid data encapsulation, as well. Like in ASM handover delays are to be considered critical. The routing distance between subsequent points of attachment, the \(\text{step size}\) of the mobile from previous to next designated router, may serve as an appropriate measure of complexity [26,27].

Finally, Source Specific Multicast has been designed as a lightweight approach to group communication. In adding mobility management, it is desirable to preserve the principle leanness of SSM by minimizing additional signaling overheads.

2.4 Deployment Issues

IP multicast deployment in general has been hesitant over the past 15 years, even though all major router vendors and operating systems offer a wide variety of implementations to support multicast [28]. While many (walled) domains or enterprise networks operate multicast, group service rollout has been largely limited in public inter-domain scenarios [29]. A dispute arose on the appropriate layer, where group communication service should reside, and the focus of the research community turned towards application layer multicast. This debate on "efficiency versus deployment complexity" now overlaps into the mobile multicast domain [30]. Hereunto Garyfalos and Almeroth [31] derived from fairly generic principles that when mobility is introduced the performance gap between IP and application layer multicast widens in different metrics up to a factor of four.
Facing deployment complexity it is desirable that any solution to mobile multicast should leave routing protocols unchanged. Mobility management in such deployment-friendly schemes should preferably be handled at edge nodes, preserving the routing infrastructure in mobility agnostic condition. Regarding the current state of proposals, the urge remains open to search for such simple, infrastructure transparent solutions, even though there are reasonable doubts, whether the desired can be achieved in all cases.

Nevertheless, multicast services in mobile environments may soon become indispensable, when multimedia distribution services such as DVB-H or IPTV will develop as a strong business cases for IP portables. As IP mobility will unfold dominance and as efficient link utilization will show a larger impact in costly radio environments, the evolution of multicast protocols will naturally follow mobility constraints.

3. Characteristics of Multicast Routing Trees under Mobility

Multicast distribution trees have been studied well under the focus of network efficiency. Grounded on empirical observations Chuang and Sirbu [32] proposed a scaling power-law for the total number of links in a multicast shortest path tree with m receivers (prop. m^k). The authors consistently identified the scale factor to attain the independent constant k = 0.8. The validity of such universal, heavy-tailed distribution suggests that multicast shortest path trees are of self-similar nature with many nodes of small, but few of higher degrees. Trees consequently would be shaped rather tall than wide.

Subsequent empirical and analytical work, cf. [33,34], debated the applicability of the Chuang and Sirbu scaling law. Van Mieghem et al. [33] proved that the proposed power law cannot hold for an increasing Internet or very large multicast groups, but is indeed applicable for moderate receiver numbers and the current Internet size N = 10^5 core nodes. Investigating on self-similarity Janic and Van Mieghem [35] semi-empirically substantiated that multicast shortest path trees in the Internet can be modeled with reasonable accuracy by uniform recursive trees (URT) [36], provided m remains small compared to N.

The mobility perspective on shortest path trees focuses on their alteration, i.e., the degree of topological changes induced by movement. For receivers, and more interestingly for sources this may serve as an outer measure for routing complexity. Mobile listeners moving to neighboring networks will only alter tree branches extending over a few hops. Source specific multicast trees subsequently generated from source handover steps are not independent, but highly correlated. They most likely branch to the identical receivers at one or several intersection points. By the self-similar nature, the persistent subtrees (of previous and next
distribution tree), rooted at any such intersection point, exhibit again the scaling law behavior, are tall-shaped with nodes of mainly low degree and thus likely to coincide. Tree alterations under mobility have been studied in [27], both analytically and by simulations. It was found that even in large networks and for moderate receiver numbers more than 80 % of the multicast router states remain invariant under a source handover.

4. Layer 2 Aspects

4.1 General Background

Scalable group data distribution admits highest potentials in leaf networks, where large numbers of end system reside. Consequently it is not surprising that most LAN network access technologies natively support point-to-multipoint or multicast services. Of focal interest to the mobility domain are wireless access technologies, which always operate on a shared medium of limited frequencies and bandwidth.

Several aspects need consideration. At first connectionless and connection oriented technologies both occur in radio links, the first being bound to limited reliability, the latter causing specific complexity and reduced efficiency on the multicast control side.

At second, point-to-multipoint service activation at the network access layer requires a mapping mechanism from network layer requests. This function is commonly achieved by L3 awareness, i.e., IGMP/MLD snooping [52], which occasionally is complemented by Multicast VLAN Registration (MVR). MVR allows sharing of a single multicast IEEE 802.1Q Virtual LAN in the network, while subscribers remain in separate VLANs. This layer 2 separation of multicast and unicast traffic can be employed as a workaround for point-to-point link models to establish a common multicast link.

Thirdly, an address mapping between the layers is needed for common group identification. Address resolution schemes depend on framing details for the technologies in use, but commonly cause a significant address overlap at the lower layer.

4.2 Multicast for Specific Technologies

4.2.1 802.11 WLAN

IEEE 802.11 WLAN is a broadcast network of Ethernet type, which inherits multicast address mapping concepts from 802.3. In infrastructure mode an access point operates as repeater, only bridging data between the Base (BSS) and the Extended Service Set (ESS). A mobile node submits multicast data to an access point in
point-to-point acknowledged unicast mode (ToDS bit on). An access point receiving multicast data from a MN simply repeats multicast frames to the BSS and propagates them to the ESS as unacknowledged broadcast. Multicast frames received from the ESS are treated likewise.

Multicast frame delivery is burdened with the following issues:

- As an unacknowledged service it attains limited reliability. Frames admit increased loss probability due to interferences, collisions, or time-varying channel properties.

- Data distribution may be delayed, as access points buffer multicast packets while waiting for DTIM, whenever stations are using power saving mode.

- Multipoint data may cause congestion, as the distribution system experiences multicast as flooding. Without further control, all access points of the same subnet replicate multicast frames.

To limit or prevent the latter, many vendors have implemented a configurable rate limiting for multicast packets. Additionally, IGMP/MLD snooping may be active at the bridging layer between BSS and ESS or at switches interconnecting access points.

### 4.2.2 802.16 WIMAX

IEEE 802.16 WIMAX combines a family of connection oriented radio transmission services, operating in distinguished, unidirectional channels. The channel assignment is controlled by Base Stations, which assign channel IDs (CIDs) within service flows to the subscriber stations. Service flows may provide an optional Automatic Repeat Request (ARQ) to improve reliability and may operate in point-to-point or point-to-multipoint (without ARQ) mode.

A WIMAX Base Station operates as L2 switch in full duplex mode, where switching is based on CIDs. Two possible IPv6 link models for mobile access deployment scenarios exist: Shared IPv6 prefix and point-to-point link model [37]. The latter treats each connection to a mobile node as a single link, which on the IP layer conflicts a consistent group distribution via a shared medium (cf. section 4.1 for a workaround).

To invoke a multipoint data channel, the base station assigns a common CID to all Subscriber Stations of that group. IPv6 multicast address mapping to these 16 bit IDs is proposed for copying either the 4 lowest bits, while sustaining the scope field, or by utilizing the 8 lowest bits derived from Multicast on Ethernet CS [38]. For
selecting group members, a Base Station may implement IGMP/MLD snooping or even IGMP/MLD proxying as foreseen in 802.16e-2005.

A Subscriber Station will issue multicast data to a Base Station as point-to-point unicast stream, which is passed on and discovered as such at the access router. The access router may return multicast data by feeding into a multicast service channel. On the reception side a Subscriber Station cannot distinguish multicast from unicast streams.

Multicast services bear the following issues:

- The mapping of multicast addresses to CIDs needs standardization, as different entities (Access Router, Base Station) may have to perform the mapping.

- CID collisions for different multicast groups are very likely due to the short ID space. As a consequence, multicast data transmission may occur in joint point-to-multipoint groups of reduced selectiveness.

- The point-to-point link model for mobile access contradicts a consistent mapping of IP layer multicast onto 802.16 point-to-multipoint services.

- Multipoint channels cannot operate ARQ service and thus experience a reduced reliability.

4.2.3 3GPP

The 3GPP System architecture spans a circuit switched (CS) and a packet switched (PS) domain, the latter General Packet Radio Services (GPRS) incorporates the Internet Multimedia Subsystem (IMS). 3GPP PS is connection oriented and based on the concept of Packet Data Protocol (PDP) Contexts. PDPs define point-to-point links between the Mobile Terminal and the Gateway GPRS Support Node (GGSN). Internet service types are PPP, IPv4 and IPv6, where the recommendation for IPv6 address assignment associates a prefix to each (primary) PDP context [39]. Current packet filtering practice causes inter-working problems between Mobile IPv6 nodes connected via GPRS [40].

As of UMTS Rel. 6 the IMS has been extended to include Multimedia Broadcast and Multicast Services (MBMS). A point-to-multipoint GPRS connection service is operated on radio links, while the gateway service to Internet multicast is handled at the GGSN. Local multicast packet distribution is used within the GPRS IP backbone resulting in the common double encapsulation at GGSN: global IP multicast datagrams over GTP (with multipoint TID) over local IP multicast.
4.2.4 DVB-H / DVB-IPDC

Digital Video Broadcasting for Handhelds (DVB-H) is a physical layer broadcasting specification for the efficient delivery of broadband, IP-encapsulated data streams. It was formally adopted as ETSI standard (EN 203 204, see www.dvb-h.org). DVB uses a mechanism called multi-protocol encapsulation, which enables a transport of network layer protocols on top of MPEG-2 transport streams and includes a forward error correction (FEC). Thereby DVB cannot only support TV broadcasting, but offers an IP Datacast Service. DVB-IPDC consists of a number of individual, application layer specifications, some of which still under development. Transport Streams (TS) form the basic logical channels, identified by a 13 bit TS ID (PID). Multicast distribution services are defined by a mapping of groups onto appropriate PIDs, which is managed at the IP Encapsulator [41]. Mobility is supported in the sense that changes of cell ID, network ID or Transport Stream ID are foreseen.

4.3 Vertical Multicast Handovers

A mobile multicast node may operate homogeneous (horizontal) or heterogeneous (vertical) layer 2 handovers with or without layer 3 network changes. Consequently, multicast configuration context transfer at network access’ needs dedicated treatment. Media Independent Handover (MIH) is addressed in IEEE 802.21, but continues to admit relevance beyond IEEE protocols. Mobility services transport for MIH naturally reside on the network layer and are currently under preparation [42].

MIH need to assist in more than service discovery. Keeping in mind complex, media dependent multicast adaptations, a possible absence of MLD signaling in L2-only transfers and requirements originating from predictive handovers, a multicast mobility services transport needs to be sufficiently comprehensive and abstract to initiate a seamless multicast handoff at the network access.

5. Solutions

5.1 General Approaches

Three approaches to mobile Multicast are commonly around [43]:

- Bi-directional Tunnelling guides the mobile node to tunnel all multicast data via its home agent. This fundamental multicast solution hides all movement and results in static multicast trees. It may be employed transparently by mobile multicast listeners and sources, on the price of triangular routing and possibly significant performance degradations due to widely spanned data tunnels.
Remote Subscription forces the mobile node to re-initiate multicast distribution subsequent to handover by submitting an MLD listener report within the subnet it newly attached to. This approach of tree discontinuation relies on multicast dynamics to adapt to network changes. It not only results in rigorous service disruption, but leads to mobility driven changes of source addresses, and thus disregards session persistence under multicast source mobility.

Agent-based solutions attempt to balance between the previous two mechanisms. Static agents typically act as local tunnelling proxies, allowing for some inter-agent handover while the mobile node moves away. A decelerated inter-tree handover, i.e. tree walking, will be the outcome of agent-based multicast mobility, where some extra effort is needed to sustain session persistence through address transparency of mobile sources.

MIPv6 [6] introduces bi-directional tunnelling as well as remote subscription as minimal standard solutions. Various publications suggest utilizing remote subscription for listener mobility, only, while advising bi-directional tunnelling as the solution for source mobility. Such approach avoids the ‘tunnel convergence’ or ‘avalanche’ problem [43], which denotes the home agent responsibility to multiply and encapsulate packets for many receivers of the same group, even if they are located within the same subnetwork. However, it suffers from the drawback that multicast communication roles are not explicitly known at the network layer and may change or mix unexpectedly.

It should be noted that none of the above approaches address SSM source mobility, except the bi-directional tunnelling.

5.2 Solutions for Multicast Listener Mobility

5.2.1 Agent Assistance

There are proposals of agent assisted handovers compliant to the unicast real-time mobility infrastructure of Fast MIPv6 [20], the M-FMIPv6 [44,45], and of Hierarchical MIPv6 [21], the M-HMIPv6 [46], and to context transfer [47], which have been thoroughly analyzed in [26,48]. An approach based on dynamically negotiated inter-agent handovers is presented in [49]. Aside from IETF work, countless publications present proposals for seamless multicast listener mobility, cf. [50] for a comprehensive overview.

5.2.2 Hybrid Architectures
Stimulated by avoidance of deployment complexity at the Internet core network, application layer and overlay proposals for (mobile) multicast raised interest in recent times. The prospect on integrating multicast distribution on the overlay into the network layer is taken by the IRTF Scalable Adaptive Multicast Research Group (SAM).

An early hybrid architecture of reactively operating proxy-gateways located at the Internet edges is introduced by Garyfalos and Almeroth in [31]. The authors present Intelligent Gateway Multicast as a bridge between mobility aware native multicast management in access networks and mobility group distribution services in the Internet core, which may be operated on the network or application layer.

Currently SAM is developing general architectural approaches for hybrid multicast solutions [51], which require detailed design in future work.

5.2.3 MLD Extensions

MLD timer defaults [18] cause slow reactions of the multicast routing infrastructure as well as of layer-3-aware access devices [52] on client leaves, which may be disadvantageous for wireless links. This tardy adaptation may be improved by carefully adjusting the Query Interval. MNs operating predictive handovers may submit early exclude reports, which allow for a possible withdrawal in case of an erroneous prediction. A further optimisation is introduced by Jelger and Noel [53] for the special case of the HA being a multicast router. A leave message received through a tunnel established to a mobile end node (in general, via a point-to-point link directly connecting the MN) should initiate a membership query with subsequent timeout according to the MLD standard. These steps may be suppressed with the result of traffic reduction and significant acceleration of the control protocol.

While away a MN may want to rely on a proxy or standby multicast membership service, which is facilitated by a HA or proxy agent. Such function relies on the ability to restart fast packet forwarding; it may be desirable for the proxy router to remain part of the multicast delivery tree, even though transmission of group data is paused. To enable such proxy control, the authors in [53] propose to extend MLD by a Listener Hold message exchanged between MN and HA. This idea has been taken up in [46] and further developed to a multicast router attendance control, allowing for a general deployment of group membership proxies.

5.3 Solutions for Multicast Source Mobility
5.3.1 Any Source Multicast Mobility Approaches

Solutions for the multicast source mobility problem can be sorted in three categories:

- **Statically Rooted Distribution Trees:**

  Following a shared tree approach, Romdhani et al. [54] propose to employ Rendezvous Points of PIM-SM as mobility anchors. Mobile senders tunnel their data to these "Mobility-aware Rendezvous Points" (MRPs), whence in restriction to a single domain this scheme is equivalent to the bi-directional tunneling. Focusing on interdomain mobile multicast, the authors design a tunnel- or SSM-based backbone distribution of packets between MRPs.

- **Reconstruction of Distribution Trees:**

  Several authors propose to construct a completely new distribution tree after the movement of a mobile source and thereby have to compensate routing delays. M-HMIPv6 [46] tunnels data into previously established trees rooted at mobility anchor points to compensate for routing delays until a protocol dependent timer expires. The RBMoM protocol [55] introduces additional Multicast Agents (MA), which advertise their service range. The mobile source registers with the closest MA and tunnels its data through it. When moving out of the previous service range, it will perform a MA discovery, a re-registration and continue data tunneling with its newly established Multicast Agent in its current vicinity.

- **Tree Modification Schemes:**

  In the case of DVMRP routing, Chang and Yen [56] propose an algorithm to extend the root of a given delivery tree for incorporating a new source location in ASM. To fix DVMRP forwarding states and heal reverse path forwarding (RPF) check failures, the authors rely on a complex additional signaling protocol.

5.3.2 Source Specific Multicast Mobility Approaches

The shared tree approach of [54] has been extended to SSM mobility by introducing the HoA address record to Mobility-aware Rendezvous Points. These MRPs operate on extended multicast routing tables, which simultaneously hold HoA and CoA and are thus enabled to logically identify the appropriate distribution tree. Mobility thus re-introduces rendezvous points to SSM routing.

Approaches of reconstructing SPTs in SSM have to rely on client notification for initiating new router state establishment. At the same time they need to preserve address transparency to the client.
To account for the latter, Thaler [57] proposes to employ binding caches and to obtain source address transparency analogous to MIPv6 unicast communication. Initial session announcements and changes of source addresses are to be distributed periodically to clients via an additional multicast control tree based at the home agent. Source tree handovers are then activated on listener requests. Jelger and Noel [58] suggest handover improvements by employing anchor points within the source network, supporting a continuous data reception during client initiated handovers. Client updates are to be triggered out of band, e.g. by SDR. Receiver oriented tree construction in SSM thus remains unsynchronized with source handovers.

To address this synchronization problem at the routing layer, several proposals concentrate on direct modification of distribution trees. Based on a multicast Hop-by-Hop protocol, a recursive scheme of loose unicast source routes with branch points, Vida et al [59] optimize SPTs for moving sources on the path between source and first branching point. O’Neill [60] suggests a scheme to overcome RPF check failures originating from multicast source address changes in a rendezvous point scenario by introducing extended routing information, which accompanies data in a Hop-by-Hop option "RPF redirect" header. The Tree Morphing approach of Schmidt and Waehlisch [61] uses source routing to extend the root of a previously established SPT, thereby injecting router state updates in a Hop-by-Hop option header. Using extended RPF checks the elongated tree autonomously initiates shortcuts and smoothly reduces to a new SPT rooted at the relocated source. Lee et al. [62] introduce a state update mechanism for re-using major parts of established multicast trees. The authors start from initially established distribution states centered at the mobile source’s home agent. A mobile leaving its home network will signal a multicast forwarding state update on the path to its home agent and, subsequently, distribution states according to the mobile source’s new CoA are implemented along the previous distribution tree. Multicast data then is intended to natively flow in triangular routes via the elongation and updated tree centered at the home agent. Consequently this mechanism refrains from using shortest path trees. Unfortunately the authors do not address the problem of RPF check failures in their paper.

6. Security Considerations

This document discusses multicast extensions to mobility. Security issues arise from source address binding updates, specifically in the case of source specific multicast. Threats of hijacking unicast sessions will result from any solution jointly operating binding updates for unicast and multicast sessions. Admission control issues may arise with new CoA source addresses being introduced to SSM.
channels (cf. [63] for a comprehensive discussion). Due to lack of feedback, admissions [64] and binding updates [65] of mobile multicast sources require self-consistent authentication as achievable by CGAs. Future solutions must address the security implications.

7. IANA Considerations

There are no IANA considerations introduced by this draft.

Appendix A. Implicit Source Notification Options

A multicast source will transmit data to a group of receivers without any option of an explicit feedback channel. There are attempts though to implicitly obtain information on listening group members. One approach has been dedicated to inquire designated routers on the pure existence of receivers. Based on an extension of IGMP, the Multicast Source Notification of Interest Protocol (MSNIP) [66] was designed to allow for the multicast source querying its designated router. However, work on MSNIP has been terminated by IETF.

A majority of real-time applications employ RTP [67] as its application layer transport protocol, which is accompanied by its control protocol RTCP. RTP is capable of multicast group distribution and RTCP receiver reports are submitted to the same group in the multicast case. Thus RTCP may be used to monitor, manage and control multicast group operations, as it provides a fairly comprehensive insight into group member statuses. However, RTCP information is neither present at the network layer nor does multicast communication presuppose the use of RTP.

8. References

Normative References


Informative References


52 Christensen, M., Kimball, K. and Solensky, F. "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, May 2006.


Acknowledgments

The authors would like to thank Mark Palkow (DaViKo GmbH) and Hans L. Cycon (FHTW Berlin) for valuable discussions and a joyful collaboration. They also thank Stig Venaas (UNINETT) for many advices.

Author’s Addresses

Thomas C. Schmidt
HAW Hamburg, Dept. Informatik
Berliner Tor 7
D-20099 Hamburg, Germany
Phone: +49-40-42875-8157
Email: Schmidt@informatik.haw-hamburg.de

Matthias Waehlisch
link-lab
Hoenowerstr. 35
D-10318 Berlin, Germany
Email: mw@link-lab.net

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.

Copyright Notice

Copyright (C) The IETF Trust (2007) 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.

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."

Acknowledgement

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