MIPSHOP WG
Internet Draft
Intended Status: Proposed Standard
Expires: January 11, 2010

G. Bajko
Nokia

July 12, 2009

# Locating IEEE 802.21 Mobility Servers using DNS
## draft-ietf-mipshop-mos-dns-discovery-07

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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 January 11, 2010.



Abstract

This document defines application service tags that allow service location without relying on rigid domain naming conventions, and DNS procedures for discovering servers which provide IEEE 802.21 [IEEE802.21] defined Mobility Services. Such Mobility Services are used to assist a Mobile Node (MN) supporting IEEE 802.21

[IEEE802.21], in handover preparation (network discovery) and

handover decision (network selection). The services addressed by this document are the Media Independent Handover Services defined in [IEEE802.21].

Conventions used in this document

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.

Terminology and abbreviations used in this document

Mobility Services: comprises of a set of different services provided by the network to mobile nodes to facilitate handover preparation and handover decision, as described in [IEEE802.21].

Mobility Server: a network node providing IEEE 802.21 Mobility Services.

MIH: Media Independent Handover, as defined in [IEEE802.21].

MIH Service: MIHIS, MIHES or MIHCS type of service, as defined in [IEEE802.21].

Application service: is a generic term for some type of application, independent of the protocol that may be used to offer it. Each application service will be associated with an IANA-registered tag.

Application protocol: is used to implement the application service. These are also associated with IANA-registered tags.

Home domain: the DNS suffix of the operator with which the Mobile Node has a subscription service. The suffix is usually stored in the Mobile Node as part of the subscription.

Table of Content

1. Introduction.....2
2. Discovering a Mobility Server.....3
2.1 Selecting a Mobility Service.....4
2.2 Selecting the transport protocol.....4
2.3 Determining the IP address and port.....6
3. IANA Considerations.....6
4. Security Considerations.....7
5. Normative References.....8
6. Informative References.....8
7. Author's Address.....9

## 1. Introduction

IEEE 802.21 [IEEE802.21] defines three distinct service types to facilitate link layer handovers across heterogeneous technologies:

a) MIH Information Services (MIHIS)
IS provides a unified framework to the higher layer entities across the heterogeneous network environment to facilitate discovery and selection of multiple types of networks existing within a geographical area, with the objective to help the higher layer mobility protocols to acquire a global view of the heterogeneous networks and perform seamless handover across these networks.

b) MIH Event Services (MIHES)
Events may indicate changes in state and transmission behavior of the physical, data link and logical link layers, or predict state changes of these layers. The Event Service may also be used to indicate management actions or command status on the part of the network or some management entity.

c) MIH Command Services (MIHCS)
The command service enables higher layers to control the physical, data link, and logical link layers. The higher layers may control the reconfiguration or selection of an appropriate link through a set of handover commands.

In IEEE terminology these services are called Media Independent Handover (MIH) services.
While these services may be co-located, the different pattern and type of information they provide does not necessitate the co-location.

"Service Management" service messages, i.e., MIH registration, MIH capability discovery and MIH event subscription messages, are considered as MIHES and MIHCS when transporting MIH messages over L3 transport.

An Mobile Node (MN) may make use of any of these MIH service types separately or any combination of them.

It is anticipated that a Mobility Server will not necessarily host all three of these MIH Services together, thus there is a need to discover the MIH Service types separately.

This document defines a number of application service tags that allow service location without relying on rigid domain naming conventions.

## 2. Discovering a Mobility Server

The Dynamic Delegation Discovery System (DDDS) [RFC3401] is used to

implement lazy binding of strings to data, in order to support dynamically configured delegation systems. The DDDS functions by

mapping some unique string to data stored within a DDDS Database by iteratively applying string transformation rules until a terminal condition is reached. When DDDS uses DNS as a distributed database of Rules, these Rules are encoded using the Naming Authority Pointer (NAPTR) Resource Record (RR). One of these Rules is the First Well Known Rule, which says where the process starts.

In current specifications, the First Well Known Rule in a DDDS application [RFC3403] is assumed to be fixed, ie the domain in the tree where the lookups are to be routed to, is known. This document proposes the input to the First Well Known Rule to be dynamic, based on the search path the resolver discovers or is configured with.

The search path of the resolver can either be pre-configured, discovered using DHCP or learned from a previous MIH Information Service (IS) query [IEEE802.21] as described in [ID.ietf-mipshop-mstp-solution].

When the MN needs to discover Mobility Services in its home domain, the input to the First Well Known Rule MUST be the MN's home domain, which is assumed to be pre-configured in the MN.

When the MN needs to discover Mobility Services in a local (visited) domain, it SHOULD use DHCP as described in [ID.ietf-mipshop-mos-dhcp-options] to discover the IP address of the server hosting the desired service, and contact it directly. In some instances, the discovery may result in a per protocol/application list of domain names which are then to be used as starting points for the subsequent NAPTR lookups. If neither IP address or domain name can be discovered with the above procedure, the MN MAY request for a domain search list, as described in [RFC3397] and [RFC3646], and use it as input to the DDDS application.

The MN may also have a list of cached domain names of Service Providers, learned from a previous MIH Information Service (IS) query [IEEE802.21]. If the cache entries have not expired, they can be used as input to the DDDS application.

When the MN does not find valid domain names using the procedures above, it MUST stop any attempt to discover MIH Services.

The dynamic rule described above SHOULD NOT be used for discovering services other than MIH Services described in this document, unless stated otherwise by a future specification.

The procedures defined here result in an IP address, port and transport protocol where the MN can contact the Mobility Server which hosts the service the MN is looking for.

## 2.1 Selecting a Mobility Service

The MN should know the characteristics of the Mobility Services defined in [IEEE802.21] and based on that it should be able to select the service it wants to use to facilitate its handover. The services it can choose from are:

- Information Service (MIHIS)
- Event Service (MIHES)
- Command Service (MIHCS)

The service identifiers for the services are "MIHIS", "MIHES", and "MIHCS" respectively.
The server supporting any of the above services MUST support at least UDP and TCP as transport, as described in [ID.ietf-mipshop-mstp-solution]. SCTP and other transport protocols MAY also be supported.

## 2.2 Selecting the transport protocol

After the desired service has been chosen, the client selects the transport protocol it prefers to use. Note, that transport selection may impact the handover performance.

The services relevant for the task of transport protocol selection are those with NAPTR service fields with values "ID+M2X", where ID is the service identifier defined in the previous section and X is a letter that corresponds to a transport protocol supported by the domain. This specification defines M2U for UDP, M2T for TCP and M2S for SCTP. This document also establishes an IANA registry for NAPTR service name to transport protocol mappings.

These NAPTR [RFC3403] records provide a mapping from a domain to the SRV [RFC2782] record for contacting a server with the specific transport protocol in the NAPTR services field. The resource record MUST contain an empty regular expression and a replacement value, which indicates the domain name where the SRV record for that particular transport protocol can be found. If the server supports multiple transport protocols, there will be multiple NAPTR records, each with a different service value. As per [RFC3403], the client discards any records whose services fields are not applicable.

The MN MUST discard any service fields that identify a resolution service whose value is not "M2X", for values of X that indicate transport protocols supported by the client. The NAPTR processing as described in RFC 3403 will result in the discovery of the most preferred transport protocol of the server that is supported by the client, as well as an SRV record for the server.

As an example, consider a client that wishes to find MIHIS service in the example.com domain. The client performs a NAPTR query for that domain, and the following NAPTR records are returned:

```
          order pref flags  service     regexp       replacement
   IN NAPTR  50   50   "s"  "MIHIS+M2T"    ""  _MIHIS._tcp.example.com
```

```
IN NAPTR  90   50   "s"  "MIHIS+M2U"    ""  _MIHIS._udp.example.com
```

This indicates that the domain does have a server providing MIHIS services over TCP and UDP, in that order of preference. Since the client supports TCP and UDP, TCP will be used, targeted to a host determined by an SRV lookup of _MIHIS._tcp.example.com. That lookup would return:

```
;;          Priority  Weight    Port        Target
     IN  SRV    0        1      XXXX   server1.example.com
     IN  SRV    0        2      XXXX   server2.example.com
```

If no NAPTR records are found, the client constructs SRV queries for those transport protocols it supports, and does a query for each. Queries are done using the service identifier "_MIHIS" for the MIH Information Service, "_MIHES" for the MIH Event Service and "_MIHCS" for the MIH Command Service. A particular transport is supported if the query is successful. The client MAY use any transport protocol it desires which is supported by the server.

Note, that the regexp field in the NAPTR example above is empty. The regexp field MUST NOT be used when discovering MIH services, as its usage can be complex and error prone; and the discovery of the MIH services do not require the flexibility provided by this field over a static target present in the TARGET field.

If the client is already configured with the information about which transport protocol is used for a mobility service in a particular domain, it can directly perform an SRV query for that specific transport using the service identifier of the Mobility Service. For example, if the client knows that it should be using TCP for MIH IS service, it can perform a SRV query directly for _MIHIS._tcp.example.com.

### 2.3 Determining the IP address and port

Once the server providing the desired service and the transport protocol has been determined, the next step is to determine the IP address and port.

The response to the SRV DNS query contains the port number in the Port field of the SRV RDATA.

According to the specification of SRV RRs in [RFC2782], the TARGET field is a fully qualified domain name (FQDN) which MUST have one or more address records; the FQDN must not be an alias, i.e., there MUST NOT be a CNAME or DNAME RR at this name. Unless the SRV DNS query already has reported a sufficient number of these address records in the Additional Data section of the DNS response (as recommended by [RFC2782]), the MN needs to perform A and/or AAAA

record lookup(s) of the domain name, as appropriate. The result will

be a list of IP addresses, each of which can be contacted using the transport protocol determined previously.

If the result of the SRV query contains a port number, then the MN SHOULD contact the server at that port number. If the SRV record did not contain a port number then the MN SHOULD contact the server at the default port number of that particular service. A default port number for MIH services is requested from IANA in [ID.ietf-mipshop-mstp-solution].

## 3. IANA considerations

The usage of NAPTR records described here requires well known values for the service fields for each transport supported by Mobility Services. The table of mappings from service field values to transport protocols is to be maintained by IANA.

The registration in the RFC MUST include the following information:

Service Field: The service field being registered.

Protocol: The specific transport protocol associated with that service field. This MUST include the name and acronym for the protocol, along with reference to a document that describes the transport protocol.

Name and Contact Information: The name, address, email address and telephone number for the person performing the registration.

The following values have been placed into the registry:

| Service Fields | Protocol |
|---|---|
| MIHIS+M2T | TCP |
| MIHIS+M2U | UDP |
| MIHIS+M2S | SCTP |
| MIHES+M2T | TCP |
| MIHES+M2U | UDP |
| MIHES+M2S | SCTP |
| MIHCS+M2T | TCP |
| MIHCS+M2U | UDP |
| MIHCS+M2S | SCTP |

New Service Fields are to be added via Standards Action as defined in [RFC5226].

New entries to the table that specify additional transport protocols for the existing Service Fields may similarly be registered by IANA through Standards Action [RFC5226].

IANA is also requested to register MIHIS, MIHES, MIHCS as service names in the port registry.

## 4. Security considerations

A list of known threats to services using DNS is documented in [RFC3833]. For most of those identified threats, the DNS Security Extensions [RFC4033] does provide protection. It is therefore recommended to consider the usage of DNSSEC [RFC4033] and the aspects of DNSSEC Operational Practices [RFC4641] when deploying IEEE 802.21 Mobility Services.

In deployments where DNSSEC usage is not feasible, measures should be taken to protect against forged DNS responses and cache poisoning as much as possible. Efforts in this direction are documented in [ID.ietf-dnsext-forgery-resilience].

Where inputs to the procedure described in this document are fed via DHCP, DHCP vulnerabilities can also cause issues. For instance, the inability to authenticate DHCP discovery results may lead to the mobility service results also being incorrect, even if the DNS process was secured.

## 5. Normative References

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC3397] B. Aboba and S. Cheshire, "DHCP Domain Search Option", RFC 3397, November 2002.

[RFC3646] R. Droms, "DNS Configuration options for DHCPv6", RFC 3646, December 2003.

[ID.ietf-mipshop-mstp-solution] Mobility Services Transport Protocol Design, Melia et al, April 2008, work in progress

[ID.ietf-mipshop-mos-dhcp-options] DHCP Options for IEEE 802.21 Mobility Services (MoS) Discovery, Bajko et al, May 2009, work in progress

## 6. Informative References

[IEEE802.21] IEEE 802.21 Standard for Local and Metropolitan Area Networks: Media Independent Handover Services http://www.ieee802.org/21/private/Published%20Spec/802.21-2008.pdf (access to the document requires membership)

[RFC4641] Kolkman, O. and R. Gieben, "DNSSEC Operational Practices", RFC 4641, September 2006.

[RFC3401] M. Mealling, "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS", RFC 3401, October 2002.

[RFC3833] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, August 2004.

[ID.ietf-dnsext-forgery-resilience] Measures for making DNS more resilient against forged answers, Hubert et al, August 2008, work in progress

## 7. Author's Addresses

Gabor Bajko
gabor(dot)bajko(at)nokia(dot)com