

Ad-Hoc Network Autoconfiguration
(Autoconf)
Internet-Draft
Intended status: Standards Track
Expires: January 14, 2010

T. Boot
Infinity Networks
A. Holtzer
TNO ICT
July 13, 2009

Border Router Discovery Protocol (BRDP) based Address Autoconfiguration
[draft-boot-autoconf-brdp-02.txt](#)

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#). This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

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 14, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

Mobile Ad hoc Networks (MANET) may be attached to a fixed infrastructure network, like the Internet. This document specifies a mechanism for Border Router discovery and utilization in such a subordinate, possibly multi-homed, MANET. It provides facilities for choosing preferred Border Router(s) and configuring IP address(es) needed for communication between MANET nodes and nodes on the Internet via the selected Border Router. Autonomous MANETs do not have Border Routers; a self-sufficient Address Autoconfiguration mechanism for Autonomous MANETs is defined as well.

Table of Contents

1.	Introduction	4
2.	Terminology	6
3.	Protocol overview and functioning	7
3.1.	Border Router Discovery Protocol (BRDP)	7
3.2.	BRDP-based Address Autoconfiguration	7
3.3.	Issues with Address Autoconfiguration in a MANET	8
4.	Border Router Discovery Protocol	9
4.1.	Border Router Information Option (BRIO)	9
4.1.1.	BRIO Base option	9
4.1.2.	BRIO suboptions	12
4.2.	BRDP processing	13
4.2.1.	BRDP message generation and transmission	13
4.2.2.	BRDP message reception	15
4.2.3.	BRIO-Cache maintenance	16
4.2.4.	BRDP loop prevention	17
4.3.	Unified Path Metric (UPM)	18
5.	BRDP-based Address Autoconfiguration	20
5.1.	Border Router selection	20
5.1.1.	Border Router Selection based on UPM	20
5.1.2.	Border Router Selection based on BRIO flags and options	21
5.2.	MANET address generation and configuration	21
5.3.	Support for Autonomous MANETs	22
6.	Support for IPv4	23
7.	IANA considerations	23
8.	Security Considerations	23
9.	Acknowledgments	24
10.	References	24
10.1.	Normative reference	24
10.2.	Informative Reference	24
Appendix A.	Change Log From Previous Versions	26
Authors' Addresses		26

1. Introduction

This document describes a complete solution for configuring globally routable and/or unique local IPv6 addresses for ad hoc network nodes.

The new Border Router Discovery Protocol (BRDP) is defined for Border Router discovery. Existing IETF mechanisms can be used for address generation, but may use BRDP provided information as an enhancement. BRDP provided information may also be used for other purposes, such as source address selection [[RFC3484](#)].

The Address Autoconfiguration solution for subordinate MANETs uses two phases:

- o Discovery of one or more Border Routers
- o Selection of a Border Router and Address Autoconfiguration of globally routable IPv6 addresses to be used in conjunction with that Border Router

In case of an Autonomous MANET no Border Routers have to be discovered. In that case Unique Local Addresses [[RFC4193](#)] are generated by individual MANET routers.

BRDP is a simple distance vector protocol that distributes Border Router information, where each MANET Router selects one or more Border Routers and forwards the Border Router information in the MANET. It extends the IPv6 Neighbor Discovery Protocol (NDP) [[RFC4861](#)] to make it carry information, such as prefix information and metrics which help a MANET Router to select a Border Router and to help to configure globally unique addresses for communication with nodes on the Internet.

Address uniqueness is assured by the IPv6 address generation mechanisms used. Additional mechanisms may be used, such as Duplicate Address Detection. However, in a MANET the overhead of performing Duplicate Address Detection can easily outweigh the benefits. For such a case, [[RFC4862](#)] specifies that Duplicate Address Detection can be disabled.

Additional mechanisms may be used for solving problems with ingress filtering, which occur when traffic is sent to the Internet via a border router that doesn't correspond with the source address of the packets. In a multi-homed MANET, the probability of such a problem to occur is highly increased due to mobility. This problem can be solved by using BRDP based routing [[I-D.boot-brdp-based-routing](#)] in which the routing mechanism assures traffic to the Internet is forwarded to the Border Router that corresponds with the source

address of the packets.

2. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

Readers are expected to be familiar with all the terms defined "Mobility Related Terminology" [[RFC3753](#)], "Mobile Ad hoc Network Architecture" [[I-D.ietf-autoconf-manetarch](#)] and "Address Autoconfiguration for MANET: Terminology and Problem Statement" [[I-D.ietf-autoconf-statement](#)].

Border Router

MANET Router that connects the MANET to the Internet

BRDP

Border Router Discovery Protocol

BRIO

Border Router Information Option

BRIO-Cache

Table, populated with information on discovered Border Routers, learned through received or initiated Border Router Information Options

MANET

A routing domain containing MANET routers
[[I-D.ietf-autoconf-manetarch](#)]

Subordinate MANET

a MANET, connected to the Internet

Autonomous MANET

a MANET, not connected to the Internet

MANET Generated Address

Globally unique and topologically correct IPv6 address generated to enable connectivity between nodes in the MANET and Corresponding Nodes on the Internet via a Border Router

UPM

Uniform Path Metric

3. Protocol overview and functioning

In this section, the subcomponents of BRDP-based Address Autoconfiguration are briefly introduced.

3.1. Border Router Discovery Protocol (BRDP)

BRDP is a simple distance vector protocol that distributes Border Router information, where each MANET Router selects one or more Border Routers and forwards the Border Router information in the MANET. It extends the IPv6 Neighbor Discovery Protocol (NDP) [[RFC4861](#)] to make it carry information and metrics which help a MANET Router to generate and configure globally unique addresses for communication with nodes on the Internet.

BRDP is a derivative of Tree Discovery [[I-D.thubert-tree-discovery](#)]. It suits the Autoconf Working Group Charter and is particularly designed for Address Autoconfiguration in subordinate, possibly multi-homed, Mobile Ad hoc Networks.

BRDP uses ICMP Router Advertisement (RA) messages in NDP to distribute Border Router information by extending it with the Border Router Information Option (BRIO). BRDP allows MANET Routers to advertise Border Router reachability, including information for selecting a preferred Border Router. A MANET Router selects at least one BRIO from its cache, for dissemination in the MANET.

BRIOS are distributed hop by hop from a Border Router downwards in the MANET using a tree structure. The presence of multiple Border Routers results in multiple, potentially overlapping logical trees, i.e. a Directed Acyclic Graph (DAG).

The amount of flooding of BRDP messages MAY be reduced. A MANET Router MAY filter BRIOS, based on the Unified Path Metric (UPM). The UPM is the advertized bidirectional distance to the Internet Default Free Zone (DFZ), via that Border Router.

BRDP MAY carry more detailed information of the Border Router, such as a provider name and AAA options. AAA enables access network providers to control access to their network. MANET Routers MAY select a Border Router based on preferences for a provider.

3.2. BRDP-based Address Autoconfiguration

BRDP provides prefix information to configure MANET Generated Addresses. The prefix information is sent in the BRIO in the form of the Border Router address and the prefix length. A MANET Generated Address is a globally unique and topologically correct IPv6 address

generated to enable connectivity between nodes in the MANET and Corresponding Nodes on the Internet via a Border Router.

The nodes using BRDP-based Address Autoconfiguration MUST implement a mechanism to generate a unique 64-bit Interface Identifier. An extremely high probability of uniqueness can be achieved by using Modified EUI-64 format-based Interface Identifiers [[RFC4291](#)] or by generating these identifiers randomly [[RFC4941](#)] or by means of a well-distributed hash function [[RFC3972](#)].

The generated Interface Identifier is combined with a 64-bit prefix, which is provided by BRDP, thus forming a topologically correct address.

In this document, it is assumed the MANET is connected to the Internet and globally unique addresses are used. Border Routers MUST have a globally unique and reachable 64-bit prefix. The mechanisms described in this document are compatible with private networks and usage of Unique Local Addresses [[RFC4193](#)]. An implementation MAY provide configuration options for Border Router selection based on offered global prefixes or unique local prefixes, in cases where both types are used in the same MANET.

3.3. Issues with Address Autoconfiguration in a MANET

After Address Autoconfiguration, additional mechanism(s) would be needed to enable usage of the correct Border Router and to enable session continuity. This document does not prescribe any solutions for this purpose. Usage of the correct Border Router is provided by BRDP Based Routing [[I-D.boot-brdp-based-routing](#)] and session continuity can be arranged with Mobility Support in IPv6 [[RFC3775](#)], NEMO basic support [[RFC3963](#)] or Shim6 [[RFC5533](#)].

4. Border Router Discovery Protocol

This section explains the details of the BRDP protocol. Topics are the Border Router Information Option (BRIO), the generation, transmission, forwarding and reception of BRIOs and BRIO cache maintenance.

4.1. Border Router Information Option (BRIO)

The Border Router Information Option carries information that allows a MANET Router to select and utilize a Border Router.

4.1.1. BRIO Base option

The BRIO is a container option, which MAY contain a number of suboptions. The BRIO base option groups the minimum information set that is mandatory in all cases.

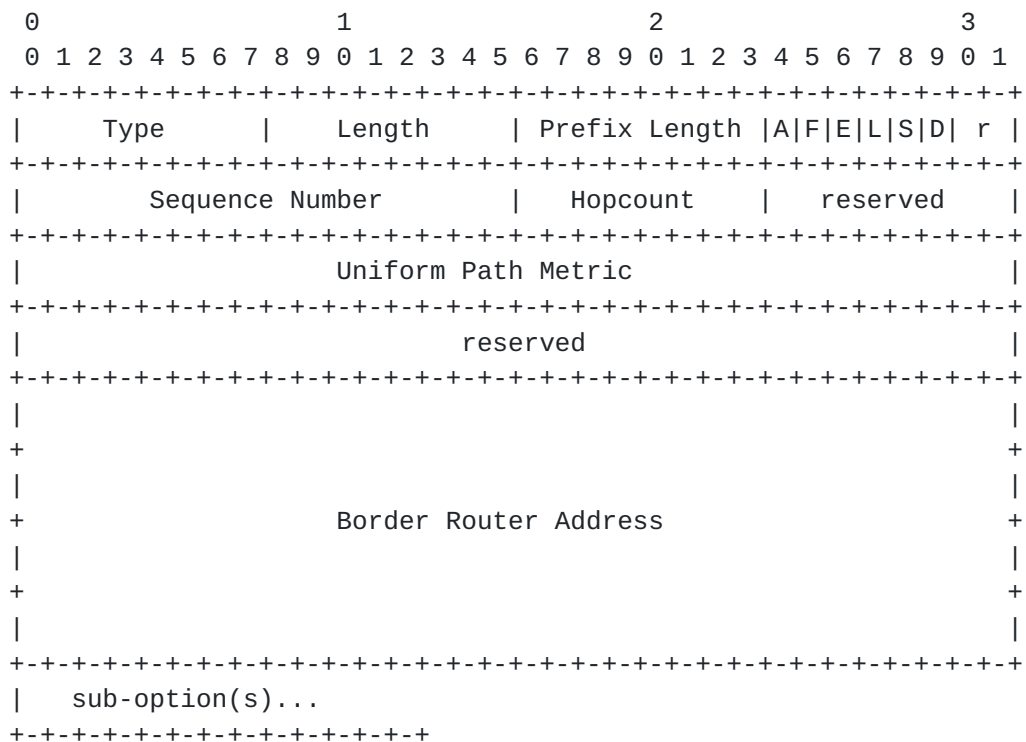


Figure 1: BRIO base option

Fields:

Type:

8-bit identifier of the Border Router Information Option type.
The value of this option identifier is to be determined.

Length:

8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. A BRIO without suboptions has a length value of 4.

Prefix Length:

8-bit unsigned integer. The number of leading bits in the Border Router Address, that indicates the assigned prefix for that Border Router. The Prefix Length is used for BRDP Based Routing [[I-D.boot-brdp-based-routing](#)].

AAA(A):

Flag indicating whether the Border Router requires authentication, authorization and accounting. When set, a Service Selection suboption immediately follows the BRIO base option. This document only describes BRIO forwarding rules considering the A-flag and Service Selection suboption. Details on performing AAA are out-of-scope for this document.

Floating(F):

When the F-flag is set, the Border Router has lost contact with the Internet. MANET Routers SHOULD stop using MANET generated source addresses based on the prefix of a Border Router that indicates that it is floating.

Emergency Response Services(E):

When the E-flag is set, the Border Router provides support for emergency response services. Details on applications for emergency response services are out-of-scope for this document. The E-flag contributes to the distribution of BRIOs in the MANET in the BRIO selection mechanism. Access to emergency response services SHOULD be enabled for all MANET nodes.

Loop-prone(L):

When the L-flag is set, an upstream MANET Router cannot guarantee a loop-free path to the Border Router advertized in this BRIO.

Solicitation Response(S):

When the S-flag is set, the Border Router requests forwarding of the BRIO downstream the BRIO forwarding tree as a response to a special Router Solicitation. This provides a mechanism to speed up convergence, requested by a downstream MANET Router.

DHCP (D):

When the D-flag is set, the Border Router is acting as a DHCP server or DHCP relay agent [[RFC3315](#)].

r, reserved:

Reserved bits. Currently unused, set to 0.

Sequence Number:

16-bit unsigned integer. It is set by the Border Router and incremented with each new BRIO it sends on a link. The sequence number is propagated without change down the tree.

Hopcount:

8-bit field registering the number of hops from the advertizing MANET Router to the Border Router. Border Routers send an original BRIO with its Hopcount set to zero. MANET Routers increment the Hopcount by one when forwarding a BRIO.

Uniform Path Metric (UPM):

A measure for the quality of the bi-directional path between the MANET Router and the Default Free Zone of the Internet. Uniform Path Metric is set to some initial value by the Border Router and is incremented by each MANET Router forwarding the BRIO.

Border Router Address:

128-bit address of the Border Router. The Border Router is expected to add its own address as a /128 prefix in the MANET routing system.

4.1.2. BRIO suboptions

In addition to the BRIO Base option, a number of suboptions are defined. Suboptions MAY have alignment requirements.

4.1.2.1. Pad suboption

The Pad suboption format is as follows:

```

0
0 1 2 3 4 5 6 7
+---+---+---+---+
|   Type = 0   |
+---+---+---+---+
```

Figure 2: Pad suboption

Fields:

Type = 0

8-bit identifier of the Pad suboption type. The option identifier is determined as 0.

The format of the Pad suboption has neither an suboption length nor suboption data fields. The Pad suboption is used to insert one octet of padding in the BRIO to enable alignment, either between suboptions or for the whole suboption container.

4.1.2.2. Service Selection suboption

Each BRIO MAY have a single Service Selection suboption, identifying the Service Provider and/or the provided service offered by the Border Router. The Service Selection suboption MUST be the first BRIO suboption.

The Service Selection suboption is equivalent to the Service Selection Mobility Option defined in "Service Selection for Mobile IPv6" [[RFC5149](#)].

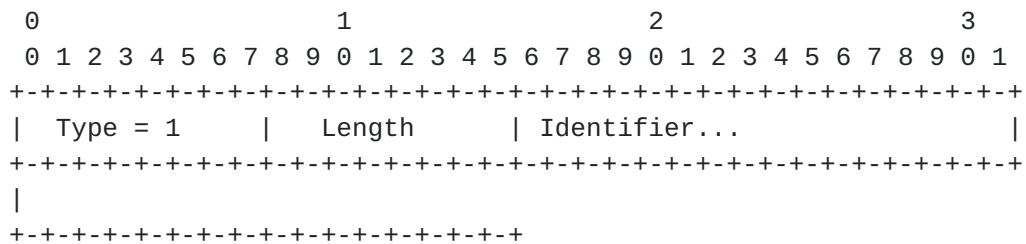


Figure 3: Service Selection suboption

Fields:

Type = 1

8-bit identifier of the Service Selection suboption type. The suboption identifier is determined as 1.

Length:

8-bit unsigned integer. The length represents the length of the Service Selection Identifier in octets, excluding the suboption type and length fields. Usage of the Length field is equivalent to [\[RFC5149\]](#).

Identifier:

A variable length UTF-8 encoded Service Selection Identifier string used to identify the Border Router service provider and optionally the type of service. Valid examples are 'ims', 'voip' and 'voip.companyxyz.example.com'.

A Border Router MAY offer multiple services using multiple BRIOs. However, each of those BRIOs MUST use a unique Border Router address.

4.2. BRDP processing

The main BRDP processing functions of a MANET Router are BRDP message generation, transmission and reception and the maintenance of a BRIO-Cache. MANET Routers forward BRDP messages using ICMP ND Router Advertisements.

4.2.1. BRDP message generation and transmission

A BRDP message is part of a Router Advertisement and includes a set of BRIOs. It provides the current state of paths to the Border Routers listed in the set of BRIOs. BRIOs originate from a Border

Router, and contain initially metric information on connectivity to the Internet. BRIOs are forwarded downwards in the MANET.

When a MANET Router sends a ICMP ND Router Advertisement, it SHOULD include a set of BRIOs by appending them to the message. The maximum number of BRIOs in a single BRDP message is a MANET Router configuration parameter. BRIO selection for advertisement is done based on the information stored in the BRIO-Cache. As a minimum, the following rules apply to a MANET Router selecting BRIOs for advertisement:

- o BRIOs with the L-flag set SHOULD NOT be selected.
- o BRIOs that do not pass the loop prevention check described in [Section 4.2.4](#) SHOULD NOT be selected.
- o At minimum, one BRIO with the E-flag set MUST be selected, when such an entry exists in the BRIO-Cache.
- o BRIO selection SHOULD select a number of BRIOs with distinct Service Selection Identifiers. The BRIO selection mechanism MAY use a preference scheme selecting and filtering Service Selection Identifiers.

The UPM and Hopcount fields of the advertised BRIOs are updated. An UPM-increment, based on uniformized bi-directional link metrics, is added to the UPM and the Hopcount is incremented by 1. UPM-increment MAY be governed by a hysteresis and dampening mechanism. Also forecasted information MAY be used.

Each BRIO originating from a Border Router has an increased Sequence Number. This BRIO is forwarded in the MANET and refreshes entries in BRIO-Caches of downstream MANET Routers.

Router Advertisements are sent in response to Router Solicitation messages or unsolicited with a uniformly-distributed random interval between MinRtrAdvInterval and MaxRtrAdvInterval [[RFC4861](#)]. The MaxRtrAdvInterval falls between a minimum of 30 milliseconds, specified in [[RFC3775](#)] and a maximum of 1800 seconds, specified in [[RFC4861](#)]. In addition, the MANET Router MAY send a Router Advertisement when an important change in a to be sent BRIO would occur.

When a MANET Router sends Router Advertisements more frequently than an upstream MANET Router, this MANET Router MAY repeatedly send BRIOs with a constant Sequence Number but with an updated UPM or Hopcount.

The ICMP ND Router Advertisement SHOULD include the Advertisement

Interval Option [[RFC3775](#)]. This option contains the interval at which the sending router sends unsolicited multicast Router Advertisements.

The Border Router MAY request that the sent BRIO SHOULD be forwarded instantly downstream in the MANET, by setting the S-flag.

A MANET Router SHOULD inform downstream MANET Routers in case the path to a previous advertized Border Router is lost, by at least 3 times retransmitting the previously sent BRIO with a UPM value of 4294967295. When an alternative BRIO for the same Service Selection Identifier is available, this BRIO SHOULD be advertised, for continued connectivity to this Service.

In case a Border Router loses its connection to the infrastructure it will lose its Border Router functionality and become a normal MANET Router. In that case it performs the same procedure as a MANET Router that has lost the path to a previous advertised Border Router. In addition, it sets the F-flag.

For each Border Router listed in the BRIO-Cache, the UPM-loop-prevention-threshold and the Hopcount-loop-prevention-threshold variables are maintained. These variables are used by the loop prevention mechanism described in [Section 4.2.4](#). The thresholds are set or updated when sending BRDP messages. When sending a BRIO with a higher Sequence Number than the previously sent BRIO for that Border Router, the threshold variables are set to the UPM and Hopcount values in BRIO to be sent. When sending a BRIO with the same Sequence Number as the previously sent BRIO, the loop-prevention-thresholds are independently updated if either the UPM or Hopcount of the outgoing BRIO is lower than their thresholds.

A MANET Router that detects an attractive candidate BRIO but is prohibited from using it because of the loop prevention check, MAY send a special Router Solicitation message to the Border Router. The Border Router responds to such a Router Solicitation message with a BRIO with the S-flag set. Sending Router Solicitations MUST be rate limited. A next version of this document would include a specification for the special Router Solicitation message.

4.2.2. BRDP message reception

When a BRDP message is received, the Sequence Number fields of the contained BRIOS are checked; the Sequence Number of a received BRIO MUST be equal to or higher than the Sequence Number in the cache for an existing entry in the cache, with wrap-around checking. Otherwise, the BRIO will be discarded.

BRIO messages do not need to be forwarded at fixed time intervals, because the RA intervals on different MANET Routers are not synchronized. Therefore, large gaps in Sequence Numbers may occur. Increment values between 0 and 65000 are accepted. Increment values between 65001 and 65535 are rejected.

Information in received BRIOs is stored in a BRIO-Cache table. Other information is stored as well, such as the BRIO sender, a timestamp indicating when the most recent message was received and the measured or signaled RA interval.

4.2.3. BRIO-Cache maintenance

Each MANET Router maintains a BRIO-Cache that stores all information on Border Routers. Unique cache entries are maintained on (Border Router Address, address of the neighbor router that forwarded the BRIO) tuples. This information is obtained by receiving BRIOs or, in case of a Border Router, by getting information from the interface that connects to the Internet. The BRIO-Cache also maintains context information for the BRIO such as the BRIO sender, link metrics and UPM-increment for this sender, history, statistics and status information. History information includes a timestamp indicating when the most recent message was received and a measured or signaled RA interval. Status information includes the BRIO selection outcome for BRIO forwarding as explained in [Section 4.2.1](#) and the Border Router selected for address generation as explained in [Section 5.1](#).

BRIO entries in the BRIO-Cache stay valid for a certain period of time. During this period, they can be used for Border Router selection by the MANET Router, for forwarding BRIOs and for address generation. BRIO-Cache information could also be useful for source address selection [[RFC3484](#)]. The lifetime of a BRIO is determined by using the timing information sent along with the RA ([\[RFC3775\]](#), [section 7.3](#)) or statistics of received BRIOs.

Some values in the BRIO-Cache can be updated independent of incoming BRDP messages. A MANET Router MAY update the UPM-increment based on link quality measurements performed in an environment with changing link metrics. A MANET Router SHOULD indicate in its BRIO-Cache which BRIO entries are currently selected for forwarding and for address generation. Border Router Selection MAY take place after the UPM of a BRIO entry has been updated.

In case the link to the MANET Router from which a BRIO has been received is broken, the UPM and the Hopcount of the BRIO entry in the cache are set to the maximum value, i.e. 4294967295 and 255.

A cache cleanup routine SHOULD run at regular intervals to get rid of

stale entries. Stale entries are removed when the entry is not updated for 5400 seconds or all of the following conditions are met:

- o The stale entry is not used by the MANET Router itself for address generation.
- o The stale entry was not selected for forwarding in the last three Router Advertisement.
- o The stale entry was not recently updated by a received BRIO. In this context, recently is defined as the maximum of a) three times its own unsolicited multicast Router Advertisements interval and b) three times the senders unsolicited multicast Router Advertisements interval.

Cache entries MAY also be removed, under the condition that the BRIO-Cache has reached a configured maximum number of entries and a new, to be stored BRIO is received. A removal candidate is selected based on:

- o The candidate entry is not used by the MANET Router itself.
- o The candidate entry was not selected for forwarding in the last Router Advertisement.
- o The candidate entry is redundant; other information for the same Border Router is stored in the cache with a better UPM and / or was received more recently.
- o The candidate entry is redundant; other information for the same Service Selection Identifier is stored in the cache with a better UPM and / or was received more recently.
- o The candidate entry is less attractive; other Border Routers are stored in the cache with better UPM and / or were received more recently.

4.2.4. BRDP loop prevention

A BRDP loop check mechanism prevents that a MANET Router forwards an earlier advertized BRIO.

BRDP loop-free operation is guaranteed as long as at least one of the following conditions is true:

- o The to be sent BRIO has a higher Sequence Number than a BRIO for this Border Router that was sent before. The loop check mechanism uses wrap-around logic. Increments up to 32768 are acceptable

(wrap-around logic needs checking).

- o The to be sent BRIO is generated from the same BRIO-Cache entry as the BRIO that was sent most recently.
- o The to be sent BRIO has the same Sequence Number as the BRIO for this Border Router that was sent before but the BRIO-Cache entry UPM is equal to or lower than the UPM-loop-prevention-threshold for this Border Router.
- o The to be sent BRIO has the same Sequence Number as the BRIO for this Border Router that was sent before but the BRIO-Cache entry Hopcount is equal to or lower than the Hopcount-loop-prevention-threshold for this Border Router.

In some circumstances, a MANET Router MAY select a BRIO for forwarding that fails the loop prevention check or with the L-flag set. For example, the link to the upstream neighbor is lost and an alternative path is available, with a higher UPM and a higher Hopcount or with a lower Sequence Number. The MANET Router cannot assure this candidate BRIO is not reflecting its own advertized message, but it could be better sending this BRIO than sending nothing or repeatedly sending a BRIO with a maximum UPM and Hopcount value. When a MANET Router forwards a BRIO that failed the loop prevention check, the L-flag MUST be set. A looped BRIO results in a Hopcount counting to infinity.

4.3. Unified Path Metric (UPM)

Unified Path Metric (UPM) is a measure for the quality of the path between the MANET Router and the Internet Default Free Zone. It is a united metric for both inbound and outbound paths. On each hop, the UPM is incremented with an UPM-increment, which is derived from the routing protocol and / or is obtained from lower layers.

It is on forehand not known what is more important; Border Router selection based on path metric to the Border Router or the path metric for the reverse path. In BRDP, UPM is used for optimizing Border Router selection for both the inbound and the outbound traffic. Note that actual traffic will use the path provided by the routing protocols, not by BRDP.

Since the UPM uses 32 bits, its maximum value is 4294967295. On each hop, an UPM-increment is calculated for each MANET Router from which a BRIO has been received. UPM-increments have a value between 1 and 16777215.

Further discussion on metrics and how the UPM-increment value is

determined is outside the scope of this document.

5. BRDP-based Address Autoconfiguration

5.1. Border Router selection

When a MANET Router needs to communicate to nodes on the Internet, it MUST select a set of Border Routers for address generation. A MANET Router MAY generate multiple addresses for smooth handover implementing make-before-break or distributing traffic over multiple Border Routers. A description how Border Routers can be used concurrently is out-of-scope for this document.

Information concerning available Border Routers is kept in the BRIO-Cache.

The Border Router selection mechanism MAY be triggered by received BRDP messages, changes in metrics on links to neighbors advertising BRDP messages, changes in MANET metrics to Border Routers used or on a time-driven basis.

The Border Router selection algorithm SHOULD be based on Service Selection Identifiers (if available) and UPM. UPM is used for selecting the Border Router with the best connectivity to the Internet. However, such a Border Router MAY require authorization. The A-flag and the Service Selection Identifier provide the prime information for selecting a preferred provider or preferred service. The Border Router selection algorithm MAY be extended with any other information. Future defined BRIO suboptions could provide additional information. Border Router selection MAY be based on the type of the Border Router Address, e.g. a globally unique address or a unique local address.

Border Router selection does not select a routing path to the Border Router.

5.1.1. Border Router Selection based on UPM

Assuming authentication requirements (if any) are satisfied, the MANET Router uses the UPM for Border Router selection preferring the best bi-directional path between the MANET Router and the Internet. Note that the BRIO UPM includes the initial metric set by the Border Router and is not solely a metric between the MANET Router and the Border Router. The initial metric set by Border Routers can be used for Border Router preference and for load balancing.

In order to use an up-to-date UPM in the selection procedure the UPM-increment is calculated by the MANET Router before selecting a Border Router. UPM is discussed in [Section 4.3](#).

5.1.2. Border Router Selection based on BRIO flags and options

Some BRIO flags MUST and some flags MAY assist in Border Router selection.

- o The A-flag and the Service Selection Identifier provide the prime information for selecting a preferred provider or preferred service. Details on authentication and authorization to the Border Router are out-of-scope of this document.
- o A (previous) Border Router could indicate that it is not connected to the Internet anymore, signaled with the F-flag. Usage of this Border Router SHOULD be avoided.
- o For emergency response applications, a Border Router providing such services, indicated by the E-flag, SHOULD be selected.
- o The guarantee for a loop-free path to a Border Router can temporary be withdrawn, indicated by the L-flag set. Usage of this Border Router SHOULD be avoided.

The Border Router selection algorithm could be extended with using future defined BRIO suboptions or other information.

5.2. MANET address generation and configuration

The MANET Router MUST use a topologically correct address when communicating with corresponding nodes on the Internet. Topologically correct addresses SHOULD be generated for each Border Router used.

A MANET Generated Address has a /128 prefix. It is constructed from a 64-bit Interface Identifier and a 64-bit prefix from the Border Router Address. A 64-bit prefix length from the Border Router is used since for a 64-bit Interface Identifier the use of a 64-bit prefix for Stateless Address Autoconfiguration (SLAAC) is prescribed in [[RFC2464](#)]. The generated 128-bit address SHOULD be advertised in the MANET routing system. The MANET Generated Address MAY also be used for other traffic, either inside the MANET or towards the Internet.

For the Interface Identifier used, the BRDP-based MANET Address Generation MUST implement a mechanism for generating a unique Interface Identifier. Known mechanisms are:

- o Modified EUI-64 format-based Interface Identifier, [[RFC4291](#)], based on IEEE 802 48-bit MAC address or IEEE EUI-64 identifier. However, this method does not guarantee identifiers are unique as

duplicate MAC addresses can occur.

- o Generation of randomized Interface Identifiers, [[RFC4941](#)].
- o Well-distributed hash function, [[RFC3972](#)].

After MANET Address Generation, [RFC4429](#) Optimistic Duplicate Address Detection [[RFC4429](#)] MAY be used, if one thinks the benefit outweigh the overhead. A passive Duplicate Address Detection could be used as an alternative. Still, uniqueness is not fully guaranteed. Main reasons for non-uniqueness are merging of MANET segments, node movement, node misbehavior or address spoofing attacks. Details on handling a duplicate address condition are out-of-scope for this document.

Address generation for globally unique addresses and unique local addresses [[RFC4193](#)] is similar. Nodes SHOULD NOT use unique local addresses to communicate with a Border Router with a globally unique address. Nodes SHOULD NOT use globally unique addresses to communicate with a Border Router with a unique local address.

A MANET Generated Addresses clean-up routine SHOULD run at regular intervals to get rid of stale addresses.

When a node has selected a Border Router for which the D-flag is set, it MAY use DHCP [[RFC3315](#)] for configuration parameters or prefix delegation [[RFC3633](#)]. DHCP processing makes use of co-located DHCP Client and DHCP Relay functions and is unicast only. DHCP is not used for address configuration, since it could introduce a lot of overhead in a MANET.

5.3. Support for Autonomous MANETs

Autonomous MANETs do not have Border Routers, and MANET Routers will have empty BRIO-Caches. No 64-bit prefixes from the Border Router Addresses are available, and globally unique IPv6 addresses cannot be generated. For communication within the MANET, a MANET Router MAY generate an address using a self-generated unique local addresses [[RFC4193](#)] /64 prefix. Alternatively some mechanism could provide already in-use /64 unique local prefix(es) in the MANET, these prefixes MAY be used as well.

6. Support for IPv4

BRDP-based Address Autoconfiguration is currently designed for IP version 6. The used mechanism for address generation extends the functionality specified in "IPv6 Stateless Address Autoconfiguration" [RFC4862]. Because of certain scenarios where IPv4 and IPv6 coexist in a network, BRDP support for IPv4 is currently under consideration.

7. IANA considerations

The IANA is requested to define a new IPv6 Neighbor Discovery option for the Border Router Information Option, defined in this document.

Type	Description	Reference
TBA	Border Router Information Option	[RFCXXXX]

Figure 4: IANA BRIO assignment

The registry for these options can be found at:

<http://www.iana.org/assignments/icmpv6-parameters>

The IANA is requested to create a new registration for BRIO suboptions.

8. Security Considerations

BRDP-based Address Autoconfiguration inherits security considerations from MANET technology. Since it is a new mechanism based on ND it inherits security considerations from ND.

Traffic anonymity and traffic flow confidentiality are important issues in MANET communications. Considerations related to traffic flows should be discussed in context with the mechanisms that are chosen to perform path setup, routing and session continuity and are therefore not covered by this document.

A more detailed description on Address Autoconfiguration security considerations is to be included in a next version of this document.

9. Acknowledgments

The authors want to thank anyone involved in IETF on MANET and NEMO technology for their efforts on mobile network infrastructures. Special thanks to Pascal Thubert, Thomas Clausen and Ryuji Wakikawa for their efforts in defining MANEMO technology, which inspired the authors to compose this document. Also special thanks to Ronald in 't Velt for reviewing.

10. References

10.1. Normative reference

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.

10.2. Informative Reference

- [RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", [RFC 2464](#), December 1998.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.
- [RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", [RFC 3484](#), February 2003.
- [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", [RFC 3633](#), December 2003.
- [RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", [RFC 3753](#), June 2004.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol",

[RFC 3963](#), January 2005.

- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", [RFC 4193](#), October 2005.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 4291](#), February 2006.
- [RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", [RFC 4429](#), April 2006.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 4941](#), September 2007.
- [RFC5149] Korhonen, J., Nilsson, U., and V. Devarapalli, "Service Selection for Mobile IPv6", [RFC 5149](#), February 2008.
- [RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", [RFC 5533](#), June 2009.
- [I-D.ietf-autoconf-statement]
Bacelli, E., Mase, K., Ruffino, S., and S. Singh,
"Address Autoconfiguration for MANET: Terminology and
Problem Statement", [draft-ietf-autoconf-statement-04](#) (work
in progress), February 2008.
- [I-D.ietf-autoconf-manetarch]
Chakeres, I., Macker, J., and T. Clausen, "Mobile Ad hoc
Network Architecture", [draft-ietf-autoconf-manetarch-07](#)
(work in progress), November 2007.
- [I-D.boot-brdp-based-routing]
Boot, T., "Border Router Discovery Protocol (BRDP) Based
Routing", [draft-boot-brdp-based-routing-00](#) (work in
progress), November 2008.
- [I-D.thubert-tree-discovery]
Thubert, P., "Nested Nemo Tree Discovery",
[draft-thubert-tree-discovery-08](#) (work in progress),
June 2009.

[Appendix A](#). Change Log From Previous Versions

00:

Initial Document.

Changes from -00 to -01:

Added fields in BRI0: D-flag, Prefix Length

Added section on DHCP for obtaining configuration parameters

Added section on autonomous MANETs

Removed section about path setup, routing and session continuity

Changes from -01 to -02:

Made several changes to the text throughout the document, mainly for clarification.

Authors' Addresses

Teco Boot
Infinity Networks B.V.
Elperstraat 4
Schoonloo 9443TL
The Netherlands

Email: teco@inf-net.nl

Arjen Holtzer
TNO Information and Communication Technology
Brassersplein 2
Delft 2612CT
The Netherlands

Email: arjen.holtzer@tno.nl

