Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 16, 2009

K. Kim, Ed.
S. Shams
picosNet Corp/Ajou Univ.
S. Yoo
Ajou University
S. Park, Ed.
SAMSUNG Electronics
G. Mulligan
July 15, 2008

Commissioning in 6LoWPAN
draft-6lowpan-commissioning-02.txt

Status of this Memo

Copyright Notice

Abstract

The commisioning process defines the startup procedure executed by any 6LoWPAN device. This document defines the startup procedure that should be followed by a 6LoWPAN device in any open or secured network.

Table of Contents

1. Introduction

6LoWPAN is a low-power wireless personal area network(LoWPAN) which is comprised of the IEEE 802.15.4-2006 standard [ieee802.15.4] devices. One of the design goal for 6LoWPAN architecture is to ensure minimum human intervention during provisioning a sensor device in a PAN. However, a 6LoWPAN device requires a set of pre-deployed information, called LoWPAN Information Base(LIB), to find the right PAN,to successfully join with the PAN, and to establish communication within the PAN. A device needs specific procedure, what we named as a Bootstrapping protocol for 6LoWPAN device, to collect those information from LoWPAN Bootstrapping Server (LBS) and to start communication in a PAN. This procedure needs to be well defined for interoperability of devices from different vendors. This procedure involves extracting LIB, security credentials,becoming part of existing network, obtaining 16-bit short address, and IP settings.

2. Terminology

Active Scan
: An active scan is used by a device to locate all coordinators transmitting beacon frames within its personal operating space, which is provided by IEEE 802.15.4. It requests other devices to transmit the beacon frame.

Association
: An IEEE 802.15.4 device can be assigned a dynamic 16 bit short address during an association operation with a neighbor device (or router) which is also called as the parent device. After getting the short address, a device can communicate with its parent or child by using only the assigned short address.

Coordinator
: A full-function device (FFD) which is the principal controller of a 6LoWPAN. It is also called as PAN coordinator. It MAY initiate the synchronization of the entire 6LoWPAN by transmitting beacons.

ED Scan
: An ED scan allows a device to obtain a measure of the peak energy in each requested channel, which is provided by IEEE 802.15.4.

Full Function Device (FFD)
: A device implementing the complete protocol set of IEEE 802.15.4. It is capable of operating as a router (multi-hop packet forwarding) for its associated neighbors.

Neighbor Table
A table which has the information of neighbor devices in a personal operating space.

LoWPAN Bootstrapping Information Base (LIB)
A set of pre-deployed information that is necessary for a particular 6LoWPAN device to find the desired PAN and to successfully join with the PAN. We categorize this information into two groups; PAN Specific Information (PSI), which is the same for every device in a PAN, (for example, PAN ID), and Device Specific Information(DSI), which is specific for each particular node (for example short address).

PSI : PAN Specific Information
Inside the LIB, a portion of information, called PSI, is the same for every device in the target PAN. For example, PAN_ID, PAN_Type, etc.

DSI : Device Specific Information
Inside the LIB, other than PSI, there is some information that may vary from device to device. For example, Role_of_Device, Short_Addr, etc.

LoWPAN BootStrapping Device (LBD)
LBD is a device that is needed to be deployed in the target network. LBD is assumed to have no priori information about the 6LoWPAN within which it is going to join. The only information it has is the EUI-64 address and a "Join key" (in case of secured PAN).

LoWPAN BootStrapping Server (LBS)
An entity that contains LIB of each device to be bootstrapped. It indexes this information with the EUI-64 address of each 6LoWPAN device. LBS has two modules in it; Network management & Acccount Module (NAM) and Authentication Module (AM). NAM keeps track of the LIB of each device indexed by EUI-64 address whereas AM participates in authentication process on behalf of LBD using LBD’s ’Authentication credentials’. Based on the ’LBP Message’, LBS varifies LBD with the help of Authentication server (in case of secured PAN) and sends ACCEPT message with necessary information otherwise it sends DECLINE message. In the case of secured PAN, LBS initiates authentication mechanism issuing Authentication request into appropriate format that is acceptable by particular authentication server. Any challenge or reply message from the Authentication server is encapsulated in the ’LIB message’ by LBS and is sent back to the LBD through

LBA.

LoWPAN BootStrapping Agent (LBA)
A FFD that has already joined in the PAN and thus, it is already a member of the PAN. It is also a neighbor of a new LBD, and thus it helps the bootstrapping LBD by receiving LBP message from LBD and forwarding it to LBS.

Open 6LoWPAN
An open 6LoWPAN is a PAN where any device is welcomed.

Close 6LoWPAN
A close 6LoWPAN is a PAN where only pre-defined set of devices are allowed to join based on their EUI-64 address. This account is managed by LBS. If close 6LoWPAN is secured, it is called secured 6LoWPAN.

Secured 6LoWPAN
Secured 6LoWPAN is a Close 6LoWPAN that also maintains secured messange exchange in the PAN.

PAN Id
The 16 bit 6LoWPAN identifier which is administratively assigned to a 6LoWPAN and is unique within the PAN.

Passive Scan
A passive scan, like an active scan, is used by an FFD to locate all coordinators transmitting beacon frames within its personal operating space, which is provided by IEEE 802.15.4. The difference is that the passive scan is a receive-only operation and does not request the beacon frame.

Personal Operating Space (POS)
The area within the reception range of the wireless transmission of a IEEE 802.15.4 packet.

Reduced Function Device (RFD)
A IEEE 802.15.4 device of 6LoWPAN which does not have the functionality of the router. That is, it can not forward IPv6 packets to the next hop device. It can only be the end device of 6LoWPAN.

Short Address
A 16 bit address dynamically assigned to a device from the PAN.

2.1. Requirements notation

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 [RFC2119].

3. Bootstrapping

Bootstrapping is defined as collecting LIB from LBS, obtaining security credentials (optional), associating with the right PAN, obtaining 16-bit short address (optional), and constructing IPv6 address using IPv6 prefix. Specifically, this includes the process of starting the network, associating with other nodes, obtaining the unique IPv6 address, and constructing security credentials for 6LoWPAN.

3.1. Resetting the device

After the device is started, it first performs a MAC layer reset.

3.2. Scanning through channels

During this phase, functions supported by 802.15.4 are used for scanning channels. Appendix (A.1) shows the scanning process in 802.15.4.

For getting the information of other devices within POS, the device should perform scan. The device can use either an active scan or a passive scan. During scanning procedure, the device receive beacon frames from other devices.

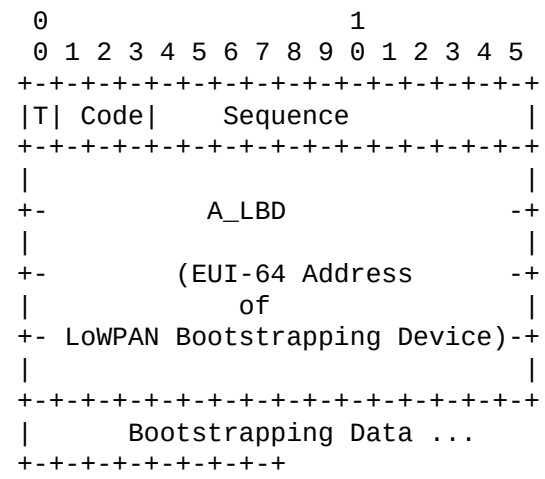
3.3. LoWPAN BootStrapping Mechanism

This protocol defines mechanism to extract LIB from currently unknown LBS and also defines a message format for LIB message exchange. In this protocol, LBD exchanges LBP message with LBS through its one hop neighbor LBA. So, at the beginning of LBP, it needs to find an LBA using 'LBA discovery phase' that is described in section 3.3.2

3.3.1. LoWPAN BootStrapping Protocol message format

In this section we define a message format which is necessary for LBP.

3.3.1.1. LBP message



T : Type of message
It defines message type. value '0' represents 'Message from LBD' and '1' represents 'Message to LBD'.

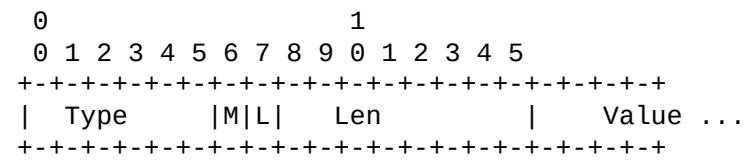
Code :
000, 1xx : Reserved.
001 : ACCEPTED. Authentication of LBD has been accepted.
010 : CHALLENGE. It indicates that authentication process has not been finished. Authentication server has sent some challenge that has to be replied by LBD.
011 : DECLINE. In the case of unsecured 6LoWPAN, LBS may send this code to indicate that LBD's EUI-64 address is not allowed to join the PAN.In case of secured 6LoWPAN, LBS may send this code to indicate that LBD's EUI-64 address is not allowed to join the PAN or the authentication of the LBD is failed.

Seq : Sequence Number
Seq identifies the number of messages transmitted by LBD. Corresponding incomming message from LBS should also have the same Seq.

A_LBD : Address of Bootstrapping Device (LBD)

64-bit EUI-64 address of LBD.

Bootstrapping Data: Format of bootstrapping data
is given below.



Type :
6-bit represents the ID of the attribute in
LIB if 'L' bit is set. Otherwise, this field
defines particular authentication type.
A list of authentication mechanism and their
corresponding 'Type' is TBD.

M : Type of the Attribute
This field defines the type of the attribute
in LIB; whether it is PAN Specific Information
(PSI) or Device Specific Information (DSI).
1 represents PSI and 0 represents DSI.

Len :
8-bit represents the length of the value in octet.

Value :
This field represents the corresponding data of the type.

3.3.2. LoWPAN Bootstrapping Information Base

One of the important goal of LBP is to receive a set of information from LBS by a joining LBD. This information comprises of PSI and DSI. Following table shows attribute name, attribute ID (attr_ID), purpose of the attribute and type of it.

Attribute Name.....Attribute ID.....Attribute Description PSI/DSI

Attribute Name	Attr_ID	Type	Attribute Description
PAN_ID	1	P	This is the network identification for the default network
PAN_type	2	P	Secured/closed/open
Address_of_LBS	3	P	Address of the LBS. 0x0000 in case of no LBS. For example in open 6LoWPAN.
Join_Time	4	P	It specifies the time when this node should start trying to join the target PAN.
Role_of_Device	5	D	Agent/No_Agent
Allow_LBA_To_Send_PSI	6	P	This attribute allows any SF to provide GI to CD after getting the positive reply from LBS.
Short_Addr	7	D	16-bit address for new device which is unique inside the PAN
Short_Addr_ Distribution_ Mechanism	8	P	Its Value is either 0 or 1 representing central or distributed respectively. If it is central, short address is provided by LBS itself otherwise assigning short address is
Other_Device_Specific _Info	15	D	Using this attribute, a device and LBS can exchange any types of data or security key required by the device.

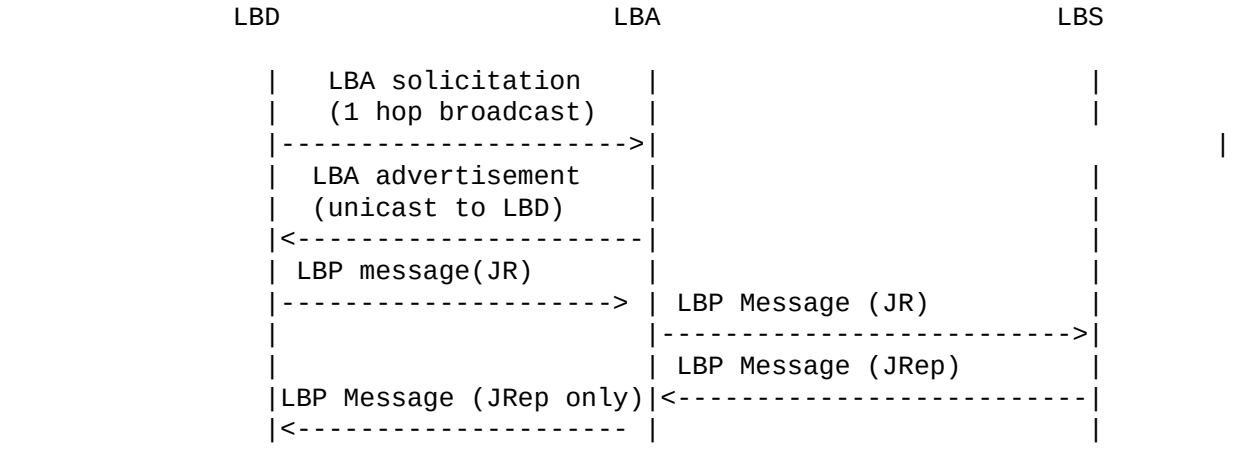
3.3.3. LBA discovering phase

LBD has to send LBP message to the LBS server under the support of a LBA. To find the LBA, it broadcasts a LBA solicitation message within its one hop neighbors and waits for a LBA advertisement. Any device capable of being LBS/LBA replies to the broadcast specifying its capability as LBS/LBA .If there is any LBS in its neighbor, LBD selects that LBS otherwise it selects one of the LBAs.

3.3.4. LoWPAN Bootstrapping Protocol (LBP)

LBD sends LBP message to LBA, as it doesn't know the address or path to the LBS of the target PAN. LBA forwards the LBP message to LBS on behalf of LBD. LBS replies with one or multiple LBP messages destined to LBA as LBD still is not part of the network. If the network is secured 6LoWPAN and the LBD is an authentic node, we assume that LBD has necessary pre-deployed keys and the knowledge of the authentication mechanism necessary to authenticate in target PAN. In this case, LBD sends necessary information in the 'bootstrapping data' field so that LBS can initiate the authentication process using that 'authentication credentials'. LBS converts the LBP message into appropriate authentication request for the particular authentication server and sends it. A reply/challenge from the authentication server, for example EAP authenticator or AAA server, is encapsulated in LBP message's 'bootstrapping data' field and is sent back to the LBD through LBA. LBA also keeps track of the successful authentication, failed authentication and incomplete conversation of the authentication process, and maintains a 'black list' of malicious devices to avoid repeated attack. Detecting malicious device based on those 3 information and marking that node as 'Black listed' belongs to the scope of security policy and out of the scope of this draft.

Following figure shows a simple example of Bootstrapping mechanism.

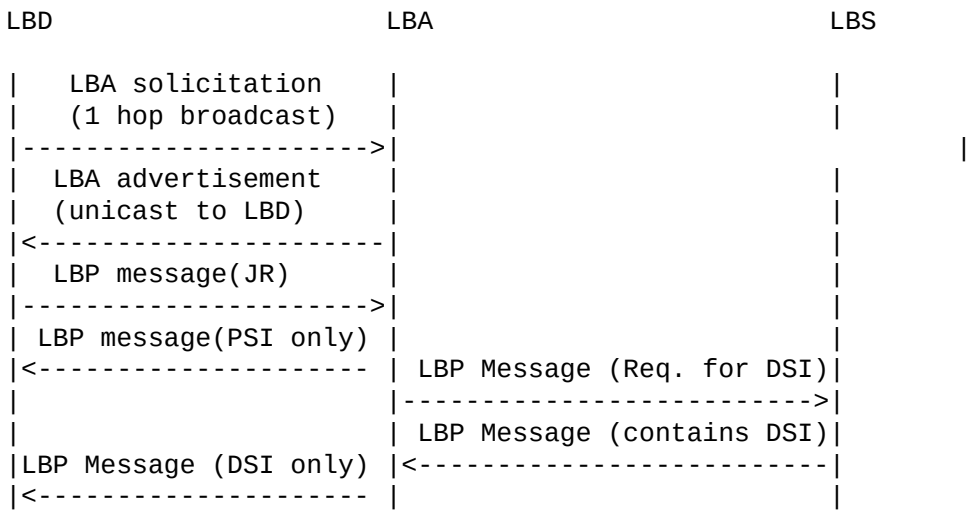


JR= Join Request, JRep= Join Reply

3.3.5. Bootstrapping in open 6LoWPAN:

An open 6LoWPAN network, usually welcomes any willing LBD. In this case, it doesn't need to wait for reply from LBS. Instead, LBA can provide GI from its own LIB and can forward LIB request to LBS

simultenously.



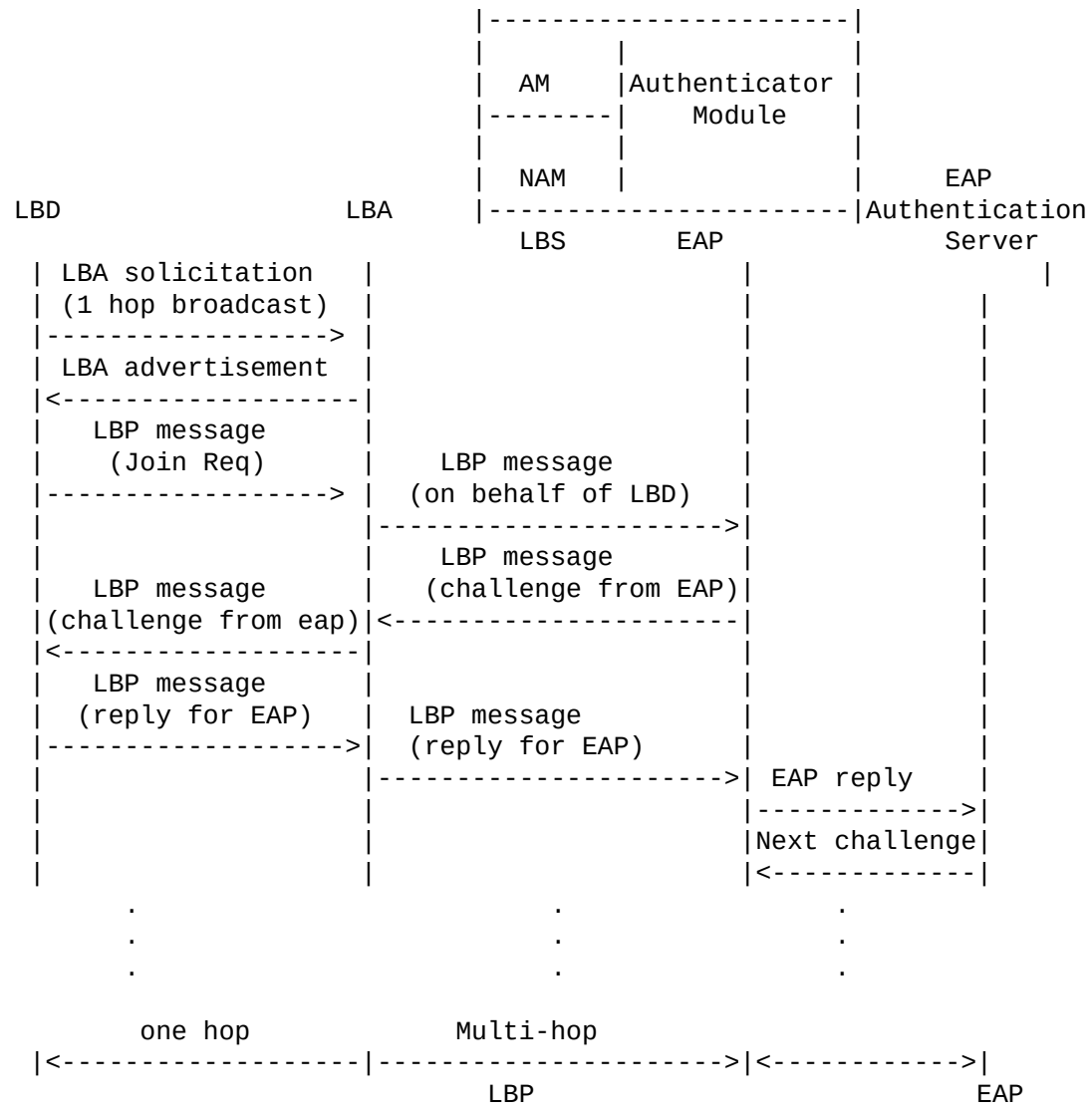
JR= Join Request.

3.3.6. LBP in secured 6LoWPAN

In secured 6LoWPAN, LBD must has to exchange authentication credentials using its join key. Apart from requesting network resources, in the case of secured network, this process may need to exchange several encrypted message between LBD and authentication server. LBA and LBS serves as 'secured tunnel' for authentication message exchange process.Both LBA and LBS keep the account of the last LIB request/reply processed by themselves.

Example: LBP with EAP

The following figure shows how LBP with other authentication protocol like EAP works. At first LBD broadcasts a LIB request(1 hop) to LBA. LBA already has a secured route to LBP so it just unicasts the LIB request to LBS. LBS sends an EAP packet prepared with LBD's authentication credentials and sends it to authenticator. it is also possible that LBS entity and authenticator entity resides on a single system. As discussed earlier, LBS serves as translator between LBP and EAP message exchange in this authentication process and finally when AM indicates the success of authentication, it sends all network resources along with the ACCEPTED code. In the case of failure in authentication process, DECLINE code is sent to LBD.



3.3.7. Role of Entities in LBP:

Role of LoWPAN Bootstrapping Device (LBD):

1. It selects LBA using LBA discovery phase.

2. If it doesn't find any LBA, it gives up after waiting for certain amount of time.

4. if it receives any LBP message with code "CHALLENGE", it must send

another LBP message containing the appropriate value against the challenge/query in the bootstrapping data field.

5. It MUST increment seq for every new LBP message. For retransmission seq should remain same.

Role of LoWPAN Bootstrapping Agent (LBA):

When LBA receives LBP message from LBD.

1. If the LBD is already in the Black List, discard

2. If the LBD is new, and 6LoWPAN is open network,

a) Send 'LBP message' with ACCEPTED along with all PSI from its own LIB

b) If there is any LBS in the PAN, Forward the 'LBP message' to LBS for DSI.

3. If the LBD is old, and 6LoWPAN is open network

a) if it matches with the last seq no. send the last reply.

b) otherwise discard.

4. If the LBD is new, and 6LoWPAN is secured network

a) forward the LBP message to LBS

5. If the LBD is old, and 6LoWPAN is secured network

a) if it matches with the last seq no. send the previously saved last LBP message 'for LBD'.

b) if the LBP has completed, discard.

c) if the LBP is 'CHALLENGE' and new seq is right next of the last one, forward the message to LBS.

When LBA receives LBP message from LBS (for LBD)

1. if it is ACCEPTED and 16-bit short address is the responsibility of LBA, it calculates and appends the 16-bit short address with the LIB reply.

2. Otherwise, if it is ACCEPTED, DECLINED or CHALLENGE, forward it to the corresponding LBD.

3. if it is not ACCEPTED or DECLINED, delete previously saved LBP message and save this LBP message.

3. if it is DECLINED, based on the security policy, mark it as 'Black listed'

4. if there is no activity in some of the flow (LBD-LBS pair), mark the LBD and based on the security policy include it in 'Black list'.

Role of LoWPAN Bootstrapping Server (LBS):

In the case of open 6LoWPAN

1. if the LBD is 'valid' that means its EUI-64 is in accepted list or not in the rejection list, it sends ACCEPTED code and necessary DSI and 16-bit short address(if the address should be assign centrally).

In the case of secured 6LoWPAN

1. AM of LBS determines authentication server for particular EUI address and sends authentication mechanism initiation with the authentication credentials to that authentication server.

2. when it gets reply from authentication server, if it is success, it prepares a success reply if it is failure, it prepares a failure reply f it is challenge/query, it prepares processing reply for LBD and sends to LBA.

3. When AM module receives success from authentication server, it informs success to NAM module and sends the success response to NAM. NAM then, sends DSI along with the response in LBP message.

3.4. Assigning the short address

During LBP procedure, LBD may set a short address either by itself or receiving the address from the PAN. The short address must be unique in a PAN and may be given by a centralized or distributed way.

One of the approach to distribute the short address among the LBDs is centralized fashion where a centralized entity (eg. LBS) assigns 16-bit short address for LBD. Allocation of short address MAY be based on First-Available-Address-First or randomly choosen one or using any other algorithm.

Distributed approach is another way to assign 16-bit short address to LBDs. In this approach, LBA assigns short address to the joining device, LBD. A hierarhical addressing scheme could be used by LBA in this purpose. Following figure describes the address calculation

scheme. This scheme requires one parameter MC, the maximum number of addresses a LBA can assign. If the present LBD is the first children, then it gets the short address by following formula,

FC = MC * AP + 1

, where FC is the LBD address, and AP is the address of the LBA.

If LBD is not the first child of this LBA, it receives the address which is next to the last address assigned by that LBA.

For example, if LBA(1) assigned address 6 to its last LBD, it assigns address 7 to its next LBD.

MC = 4

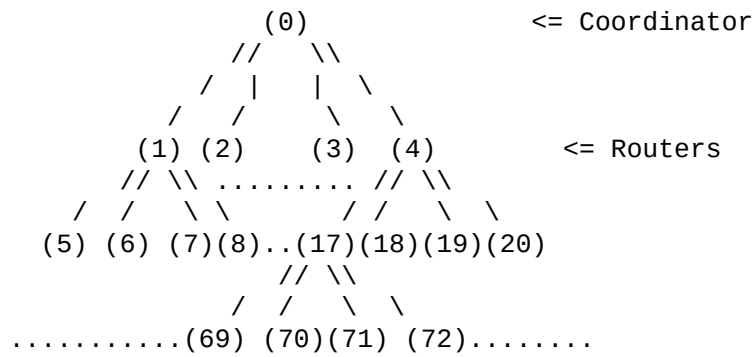


Fig. . The assignment scheme of the short address

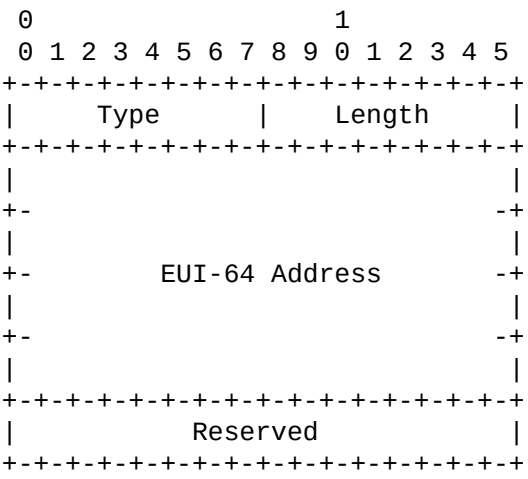
3.5. Obtaining IPv6 address

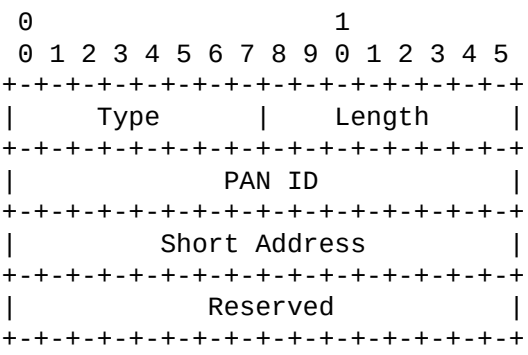
The IPv6 interface identifier of a device can be obtained as described in Section 6 of [rfc4944].

After having a unique IPv6 interface identifier, the device begins to obtain an IPv6 address prefix. The IPv6 address prefix for a particular 6LoWPAN is stored by the IPv6 router in the 6LoWPAN. ICMPv6 is used to share these parameters. Routers in 6LoWPAN are supposed to broadcast Router Advertisements(RA) messages periodically. The RA message must contain the prefix option which can be used in the 6LoWPAN. Devices wish to obtain IPv6 address prefix may wait for an RA message until RA_WAIT_TIME elapsed. After that, if no RA message is received, they may broadcast Router Solicitation(RS) message for requesting the RA message.

The RS and RA messages can have additional option fields as described in [rfc4861]. Source/Target link-layer address option field should contain the EUI-64 address or the combined address with PAN ID and 16bit short address of the source or target device as below.

The RS and RA messages can have additional option fields as described in [rfc4861]. Source/Target link-layer address option field should contain the EUI-64 address or the combined address with PAN ID and 16bit short address of the source or target device as below.





Source/Target Link-layer Address option field

Multiple IPv6 routers could form a single or multiple 6lowpan(s). If there are multiple routers in a 6LoWPAN, the device should consider which one is to be selected as a default router. One possible way of selection is to compare the hop counts traveled of the RA message of each router. The detailed algorithm for the selection is TBD.

3.6. Configuration Parameters

This section gives default values for some important parameters associated with the 6LoWPAN commissioning protocol. A particular node may wish to change certain of the parameters.

Parameter Name	Value
CHANNEL_LIST	0xFFFF800
SCAN_DURATION	3
SUPERFRAME_ORDER	15
BEACON_ORDER	15
START_RETRY_TIME	1000 msec
JOIN_RETRY_TIME	4000 msec
ASSOCIATION_RETRY_TIME	4000 msec

4. IANA Consideration

TBD.

5. Security Considerations

IEEE 802.15.4 devices is required to support AES link-layer security. MAC layer also provides all keying material necessary to provide the security services.

It isn't defined, however, when security shall be used especially combining with Bootstrapping. After the device start and join the network, security services such as key management and device authentication should be done automatically. Detailed algorithm for security on Bootstrapping is TBD.

6. Contributors

Thanks to the contribution from MD. Aminul Haque Chowdhury (Ajou Univ) and Chae-Seong Lim (Ajou Univ) for the review and useful discussion for writing this document.

7. Acknowledgments

Thanks to Hamid Mukhtar (PicosNet/Ajou Univ), Jae-ho Lee (NIA), and Dong-Gyu Nam (NIA) for their useful discussion and support for writing this document.

8. References

8.1. Normative References

[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.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[ieee802.15.4] IEEE Computer Society, "IEEE Std. 802.15.4-2006".

8.2. Informative References

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

Authors' Addresses

Ki-Hyung Kim (editor)
picosNet Corp/Ajou Univ.
San 5 Wonchun-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do 442-749
KOREA

Phone: +82 31 219 2433
Email: kkim86@picosnet.com

S M Saif Shams
picosNet Corp/Ajou Univ.
San 5 Wonchun-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do 442-749
KOREA

Phone: +82 010 8690 8532
Email: saif95bd@gmail.com

Seung Wha Yoo
Ajou University
San 5 Wonchun-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do 442-749
KOREA

Phone: +82 31 216 1603
Email: swyoo@ajou.ac.kr

Soohong Daniel Park (editor)
SAMSUNG Electronics
Mobile Platform Laboratory, SAMSUNG Electronics 416 Maetan-3dong
Yeongtong-gu, Suwon-si, Gyeonggi-do 442-742
KOREA

Phone: +82 31 200 4508
Email: soohong.park@samsung.com

Geoffrey Mulligan

Email: geoff@mulligan.com

Full Copyright Statement

Intellectual Property