Stream: Internet Engineering Task Force (IETF)
RFC: 9428
Category: Standards Track
Published: July 2023
ISSN: 2070-1721
Authors: Y. Choi, Ed. (*ETRI*); Y-G. Hong (*Daejon Univ*); J-S. Youn (*Dongeui Univ*)

RFC 9428
Transmission of IPv6 Packets over Near Field Communication

Abstract

Near Field Communication (NFC) is a set of standards for smartphones and portable devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than 10 cm apart. NFC standards cover communication protocols and data exchange formats and are based on existing Radio Frequency Identification (RFID) standards, including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum. The NFC technology has been widely implemented and available in mobile phones, laptop computers, and many other devices. This document describes how IPv6 is transmitted over NFC using IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) techniques.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9428.

Copyright Notice

Table of Contents

1. Introduction

NFC is a set of short-range wireless technologies, typically requiring a distance between a sender and receiver of 10 cm or less. NFC operates at 13.56 MHz and at rates ranging from 106 kbps to 424 kbps, as per the ISO/IEC 18000-3 air interface [ECMA-340]. NFC builds upon RFID systems by allowing two-way communication between endpoints. NFC always involves an initiator and a target; the initiator actively generates a radio frequency (RF) field that can power a passive target. This enables NFC targets to take very simple form factors, such as tags, stickers, key fobs, or cards, while avoiding the need for batteries. NFC peer-to-peer communication is possible, provided that both devices are powered.

NFC has a very short transmission range of 10 cm or less; thus, the other hidden NFC devices outside of that range cannot receive NFC signals. Therefore, NFC is often regarded as a secure communications technology.

In order to benefit from Internet connectivity, it is desirable for NFC-enabled devices to support IPv6 because of its large address space and the availability of tools for unattended operation, along with other advantages. This document specifies how IPv6 is supported over NFC by using 6LoWPAN techniques [RFC4944] [RFC6282] [RFC6775]. 6LoWPAN is suitable, considering that it was designed to support IPv6 over IEEE 802.15.4 networks [IEEE802.15.4] and some of the characteristics of the latter are similar to those of NFC.

2. Conventions and Terminology

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This specification requires readers to be familiar with all the terms and concepts that are discussed in "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919], "Transmission of IPv6 Packets over IEEE 802.15.4 Networks" [RFC4944], and "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) [RFC6775].

6LoWPAN Node (6LN):
: A 6LoWPAN node is any host or router participating in a LoWPAN. This term is used when referring to situations in which either a host or router can play the role described.

6LoWPAN Router (6LR):
: An intermediate router in the LoWPAN that is able to send and receive Router Advertisements (RAs) and Router Solicitations (RSs), as well as forward and route IPv6 packets. 6LoWPAN routers are present only in route-over topologies.

6LoWPAN Border Router (6LBR):
: A border router located at the junction of separate 6LoWPAN networks or between a 6LoWPAN network and another IP network. There may be one or more 6LBRs at the 6LoWPAN network boundary. A 6LBR is the responsible authority for IPv6 prefix propagation for the 6LoWPAN network it is serving. An isolated LoWPAN also contains a 6LBR in the network that provides the prefix(es) for the isolated network.

3. Overview of NFC Technology

This section presents an overview of NFC, focusing on the characteristics of NFC that are most relevant for supporting IPv6.

NFC enables a simple, two-way interaction between two devices, allowing users to perform contactless transactions, access digital content, and connect electronic devices with a single touch. NFC utilizes key elements in existing standards for contactless card technology, such as ISO/IEC 14443 A&B and JIS-X 6319-4. NFC allows devices to share information at a distance up to 10 cm with a maximum physical layer bit rate of 424 kbps.

3.1. Peer-to-Peer Mode of NFC

NFC defines three modes of operation: card emulation, peer-to-peer, and reader/writer. Only the peer-to-peer mode allows two NFC-enabled devices to communicate with each other to exchange information bidirectionally. The other two modes do not support two-way communication between two devices. Therefore, the peer-to-peer mode **MUST** be used for IPv6 over NFC.

3.2. Protocol Stack of NFC

NFC defines a protocol stack for the peer-to-peer mode (Figure 1). The peer-to-peer mode is offered by the Activities Digital Protocol at the NFC Physical Layer. The NFC Logical Link Layer comprises the Logical Link Control Protocol (LLCP), and when IPv6 is used over NFC, it also includes an IPv6-LLCP Binding. IPv6 and its underlying adaptation layer (i.e., IPv6-over-NFC Adaptation Layer) are placed directly on the top of the IPv6-LLCP Binding. An IPv6 datagram is transmitted by the LLCP with guaranteed delivery and two-way transmission of information between the peer devices.

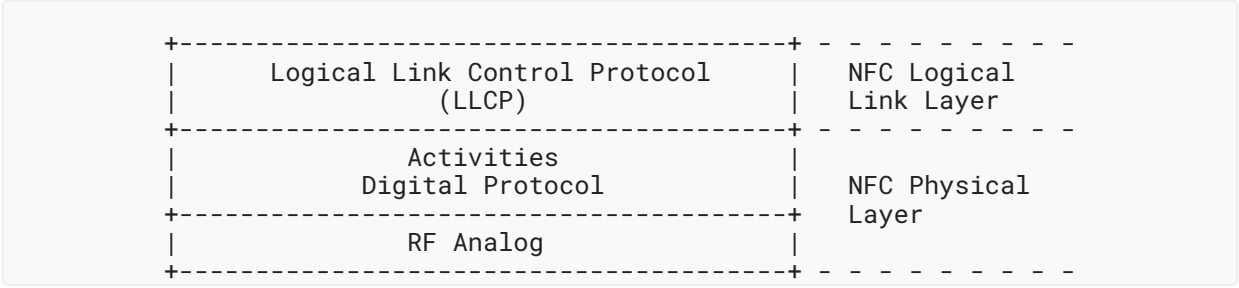

Figure 1: Protocol Stack of NFC

The LLCP consists of Logical Link Control (LLC) and MAC Mapping. The MAC Mapping integrates an existing radio frequency (RF) protocol into the LLCP architecture. The LLC contains three components: Link Management, Connection-oriented Transmission, and Connectionless Transmission. The Link Management is responsible for serializing all connection-oriented and connectionless LLC PDU (Protocol Data Unit) exchanges; it is also responsible for the aggregation and disaggregation of small PDUs. The Connection-oriented Transmission is responsible for maintaining all connection-oriented data exchanges, including connection setup and termination. However, NFC links do not guarantee perfect wireless link quality, so some types of delay or variation in delay would be expected in any case. The Connectionless Transmission is responsible for handling unacknowledged data exchanges.

In order to send an IPv6 packet over NFC, the packet **MUST** be passed down to the LLCP layer of NFC and carried by an Information field in an LLCP Protocol Data Unit (I PDU). The LLCP does not support fragmentation and reassembly. For IPv6 addressing or address configuration, the LLCP **MUST** provide related information, such as link-layer addresses, to its upper layer. IPv6-LLCP Binding **MUST** transfer the Source Service Access Point (SSAP) and Destination Service Access Point (DSAP) values to the IPv6-over-NFC Adaptation Layer. The SSAP is an LLC address of the source NFC-enabled device with a size of 6 bits, while the DSAP is an LLC address of the destination NFC-enabled device. Thus, the SSAP is a source address and the DSAP is a destination address.

In addition, NFC links and hosts do not need to consider IP header bits for QoS signaling or utilize these meaningfully.

3.3. NFC-Enabled Device Addressing

According to [LLCP-1.4], NFC-enabled devices have two types of 6-bit addresses (i.e., SSAP and DSAP) to identify service access points. Several service access points can be installed on an NFC device. However, the SSAP and DSAP can be used as identifiers for NFC link connections with the IPv6-over-NFC Adaptation Layer. Therefore, the SSAP can be used to generate an IPv6 Interface Identifier (IID). Address values between 00h and 0Fh of SSAP and DSAP are reserved for identifying the well-known service access points that are defined in the NFC Forum Assigned Numbers Register. Address values between 10h and 1Fh are assigned by the local LLC to services

registered by a local service environment. In addition, address values between 0x2 and 0x3f are assigned by the local LLC as a result of an upper-layer service request. Therefore, the address values between 0x2 and 0x3f can be used for generating IPv6 IIDs.

3.4. MTU of NFC Link Layer

As mentioned in Section 3.2, when an IPv6 packet is transmitted, the packet **MUST** be passed down to LLCP of NFC and transported to an I PDU of LLCP of the NFC-enabled peer device.

The Information field of an I PDU contains a single service data unit. The maximum number of octets in the Information field is determined by the Maximum Information Unit (MIU) for the data link connection. The default value of the MIU for I PDUs is 128 octets. The local and remote LLCs each establish and maintain distinct MIU values for each data link connection endpoint. Also, an LLC may announce a larger MIU for a data link connection by transmitting an optional Maximum Information Unit Extension (MIUX) parameter within the Information field. If no MIUX parameter is transmitted, the MIU value is 128 bytes. Otherwise, the MTU size in NFC LLCP **MUST** be calculated from the MIU value as follows:

```
MTU = MIU = 128 + MIUX
```

According to [LLCP-1.4], Figure 2 shows an example of the MIUX parameter TLV. The Type and Length fields of the MIUX parameter TLV have each a size of 1 byte. The size of the TLV Value field is 2 bytes.

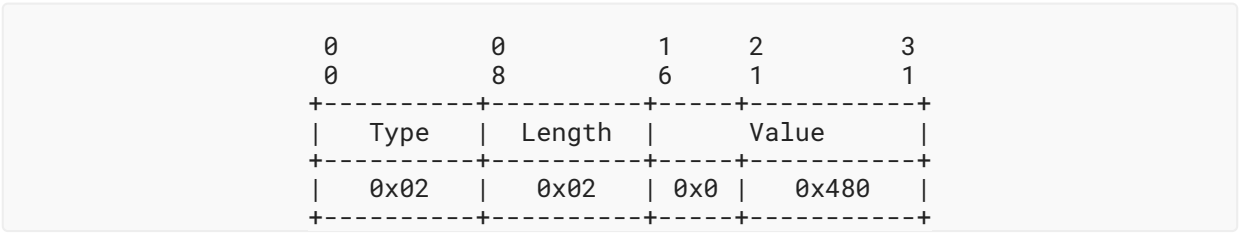

Figure 2: Example of MIUX Parameter TLV

When the MIUX parameter is used, the TLV Type field is 0x02 and the TLV Length field is 0x02. The MIUX parameter is encoded into the least significant 11 bits of the TLV Value field. The unused bits in the TLV Value field are set to zero by the sender and ignored by the receiver. The maximum possible value of the TLV Value field is 0x7FF, and the maximum size of the LLCP MTU is 2175 bytes. As per the present specification [LLCP-1.4], the MIUX value **MUST** be 0x480 to support the IPv6 MTU requirement (1280 bytes) [RFC8200].

4. Specification of IPv6 over NFC

NFC technology has requirements owing to low power consumption and allowed protocol overhead. 6LoWPAN standards [RFC4944] [RFC6775] [RFC6282] provide useful functionality for reducing the overhead of IPv6 over NFC. This functionality consists of link-local IPv6 addresses and stateless IPv6 address autoconfiguration (see Sections 4.2 and 4.3), Neighbor Discovery (see Section 4.4), and header compression (see Section 4.6).

4.1. Protocol Stack

Figure 3 illustrates the IPv6-over-NFC protocol stack. Upper-layer protocols can be transport-layer protocols (e.g., TCP and UDP), application-layer protocols, and other protocols capable of running on top of IPv6.

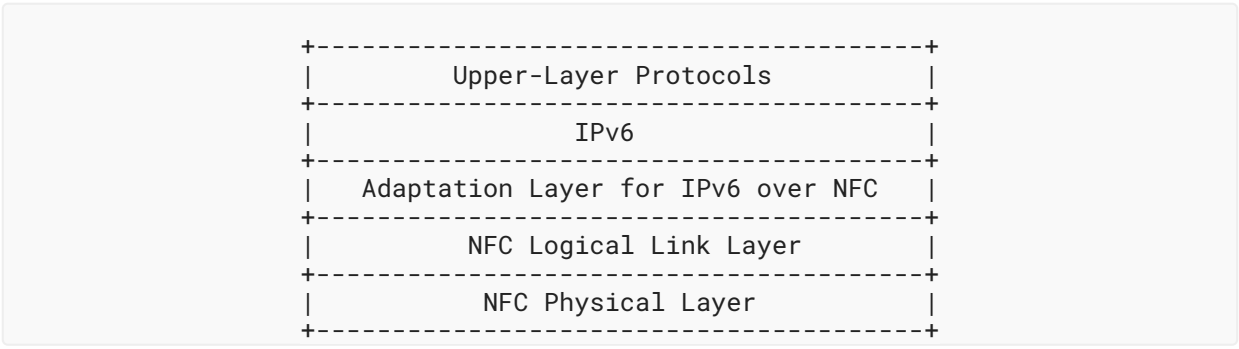

Figure 3: Protocol Stack for IPv6 over NFC

The Adaptation Layer for IPv6 over NFC supports Neighbor Discovery, stateless address autoconfiguration, header compression, and fragmentation and reassembly, based on 6LoWPAN. Note that 6LoWPAN header compression [RFC6282] does not define header compression for TCP. The latter can still be supported by IPv6 over NFC, albeit without the performance optimization of header compression.

4.2. Stateless Address Autoconfiguration

An NFC-enabled device performs stateless address autoconfiguration per [RFC4862]. A 64-bit IID for an NFC interface is formed by utilizing the 6-bit NFC SSAP (see Section 3.3). In the viewpoint of address configuration, such an IID should guarantee a stable IPv6 address during the course of a single connection because each data link connection is uniquely identified by the pair of DSAP and SSAP included in the header of each LLC PDU in NFC.

Following the guidance of [RFC7136], IIDs of all unicast addresses for NFC-enabled devices are 64 bits long and constructed by using the generation algorithm of random identifiers (RIDs) that are stable [RFC7217].

The RID is an output created by the F() algorithm with input parameters. One of the parameters is Net_Iface, and the NFC Link-Layer Address (i.e., the SSAP) **MUST** be a source of the Net_Iface parameter. The 6-bit address of the SSAP of NFC is short and can easily be targeted by attacks from a third party (e.g., address scanning). The F() algorithm with SHA-256 can provide secured and stable IIDs for NFC-enabled devices. In addition, an optional parameter, Network_ID, is used to increase the randomness of the generated IID with the NFC Link-Layer Address (i.e., SSAP). The secret key **SHOULD** be at least 128 bits. It **MUST** be initialized to a pseudorandom number [RFC4086].

4.3. IPv6 Link-Local Address

The IPv6 Link-Local Address for an NFC-enabled device is formed by appending the IID to the prefix fe80::/64, as depicted in Figure 4.

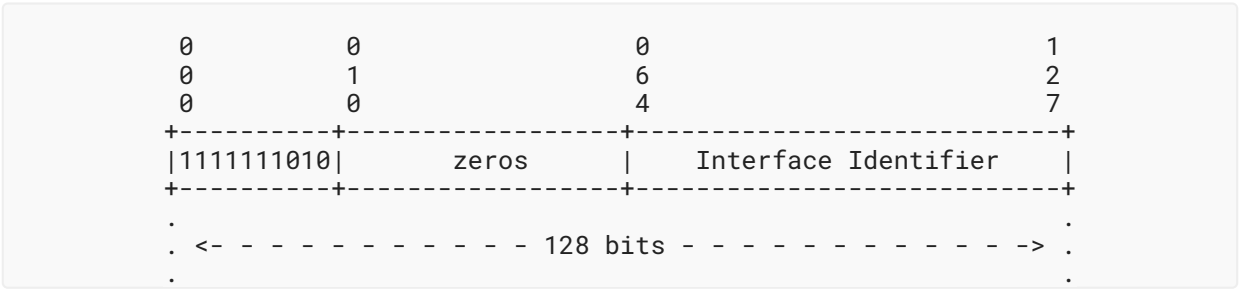

Figure 4: IPv6 Link-Local Address in NFC

The "Interface Identifier" can be a random and stable IID.

4.4. Neighbor Discovery

Neighbor Discovery Optimization for 6LoWPANs [RFC6775] describes the Neighbor Discovery approach in several 6LoWPAN topologies, such as mesh topology. NFC supports mesh topologies, but most applications would use a simple multi-hop network topology or directly connected peer-to-peer network because the NFC RF range is very short.

- When an NFC 6LN is directly connected to a 6LBR, the 6LN **MUST** register its address with the 6LBR by sending Neighbor Solicitation (NS) with the Extended Address Registration Option (EARO) [RFC8505]; then Neighbor Advertisement (NA) is started. When the 6LN and 6LBR are linked to each other, an address is assigned to the 6LN. In this process, Duplicate Address Detection (DAD) is not required.
- When two or more NFC 6LNs are connected to the 6LBR, two cases of topologies can be formed. One is a multi-hop topology, and the other is a star topology based on the 6LBR. In the multi-hop topology, 6LNs that have two or more links with neighbor nodes may act as routers. In star topology, any of 6LNs can be a router.
- For receiving RSs and RAs, the NFC 6LNs **MUST** follow Sections 5.3 and 5.4 of [RFC6775].
- When an NFC device is a 6LR or 6LBR, the NFC device **MUST** follow Sections 6 and 7 of [RFC6775].

4.5. Dispatch Header

All IPv6-over-NFC encapsulated datagrams are prefixed by an encapsulation header stack consisting of a dispatch value [IANA-6LoWPAN]. The only sequence currently defined for IPv6 over NFC **MUST** be the LOWPAN_IPHC compressed IPv6 header (see Section 4.6) followed by a payload, as depicted in Figure 5 and Table 1.

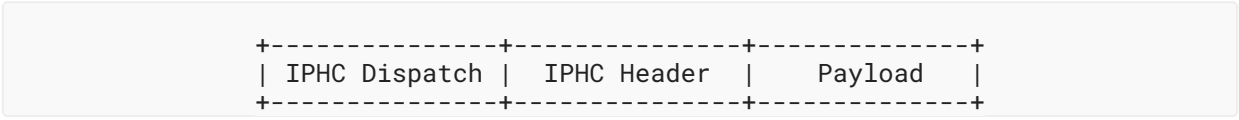

Figure 5: An IPv6-over-NFC Encapsulated LOWPAN_IPHC Compressed IPv6 Datagram

The dispatch value (1 octet in length) is treated as an unstructured namespace. Only a single pattern is used to represent current IPv6-over-NFC functionality.

Pattern	Header Type	Reference
01 1xxxxx	LOWPAN_IPHC	[RFC6282] [RFC8025]

Table 1: Dispatch Values

Other IANA-assigned 6LoWPAN dispatch values do not apply to this specification.

4.6. Header Compression

Header compression as defined in [RFC6282], which specifies the compression format for IPv6 datagrams on top of IEEE 802.15.4, is **REQUIRED** in this document as the basis for IPv6 header compression on top of NFC. All headers **MUST** be compressed according to the encoding formats described in [RFC6282].

Therefore, IPv6 header compression in [RFC6282] **MUST** be implemented. Further, implementations **MUST** also support Generic Header Compression (GHC) as described in [RFC7400].

If a 16-bit address is required as a short address, it **MUST** be formed by padding the 6-bit NFC SSAP (NFC Link-Layer Node Address) to the left with zeros as shown in Figure 6.

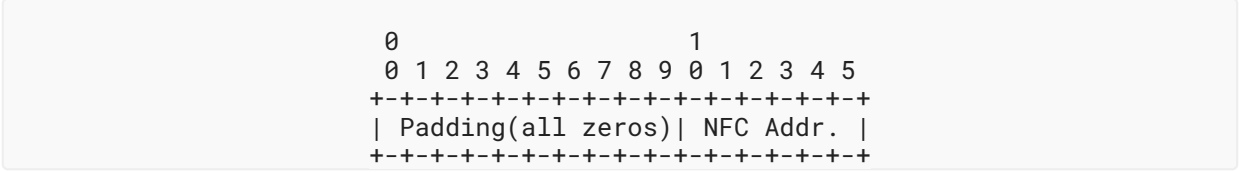

Figure 6: NFC Short Address Format

4.7. Fragmentation and Reassembly Considerations

IPv6 over NFC **MUST NOT** use fragmentation and reassembly (FAR) at the adaptation layer for the payloads as discussed in Section 3.4. The NFC link connection for IPv6 over NFC **MUST** be configured with an equivalent MIU size to support the IPv6 MTU requirement (1280 bytes). To this end, the MIUX value is 0x480.

4.8. Unicast and Multicast Address Mapping

The address resolution procedure for mapping IPv6 non-multicast addresses into NFC Link-Layer Addresses follows the general description in Sections 4.6.1 and 7.2 of [RFC4861], unless otherwise specified.

The Source/Target Link-Layer Address option has the following form when the addresses are 6-bit NFC SSAP/DSAP (NFC Link-Layer Node Addresses).

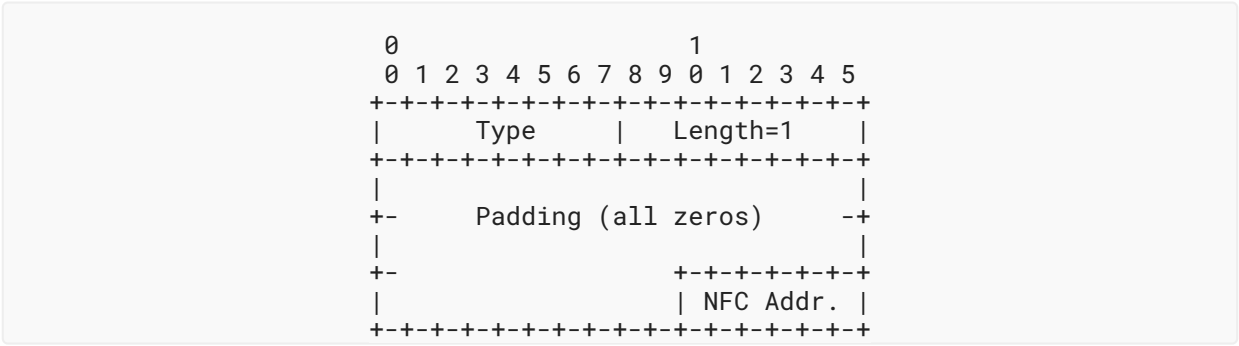

Figure 7: Unicast Address Mapping

Option fields:

Type:

1: This is for the Source Link-Layer Address.

2: This is for the Target Link-Layer Address.

Length:

This is the length of this option (including the Type and Length fields) in units of 8 bits. The value of this field is 1 for 6-bit NFC node addresses.

NFC address:

The 6-bit address in canonical bit order. This is the unicast address the interface currently responds to.

The NFC Link Layer does not support multicast. Therefore, packets are always transmitted unicast between two NFC-enabled devices. Even in the case where a 6LBR is attached to multiple 6LNs, the 6LBR cannot multicast to all the connected 6LNs. If the 6LBR needs to send a multicast packet to all its 6LNs, it has to replicate the packet and unicast it on each link. However, this is

not energy-efficient; the central node, which is battery-powered, must take particular care of power consumption. To further conserve power, the 6LBR **MUST** keep track of multicast listeners at NFC link-level granularity (not at subnet granularity), and it **MUST NOT** forward multicast packets to 6LNs that have not registered as listeners for multicast groups the packets belong to. In the opposite direction, a 6LN always has to send packets to or through the 6LBR. Hence, when a 6LN needs to transmit an IPv6 multicast packet, the 6LN will unicast the corresponding NFC packet to the 6LBR.

5. Internet Connectivity Scenarios

5.1. NFC-Enabled Device Network Connected to the Internet

Figure 8 illustrates an example of an NFC-enabled device network connected to the Internet. The distance between 6LN and 6LBR is typically 10 cm or less. For example, a laptop computer that is connected to the Internet (e.g., via Wi-Fi, Ethernet, etc.) may also support NFC and act as a 6LBR. Another NFC-enabled device may run as a 6LN and communicate with the 6LBR, as long as both are within each other's range.

Figure 8: NFC-Enabled Device Network Connected to the Internet

Two or more 6LNs may be connected with a 6LBR, but each connection uses a different IPv6 prefix. The 6LBR is acting as a router and forwarding packets between 6LNs and the Internet. Also, the 6LBR **MUST** ensure address collisions do not occur because the 6LNs are connected to the 6LBR like a start topology, so the 6LBR checks whether or not IPv6 addresses are duplicates, since 6LNs need to register their addresses with the 6LBR.

5.2. Isolated NFC-Enabled Device Network

In some scenarios, the NFC-enabled device network may permanently be a simple isolated network as shown in Figure 9.

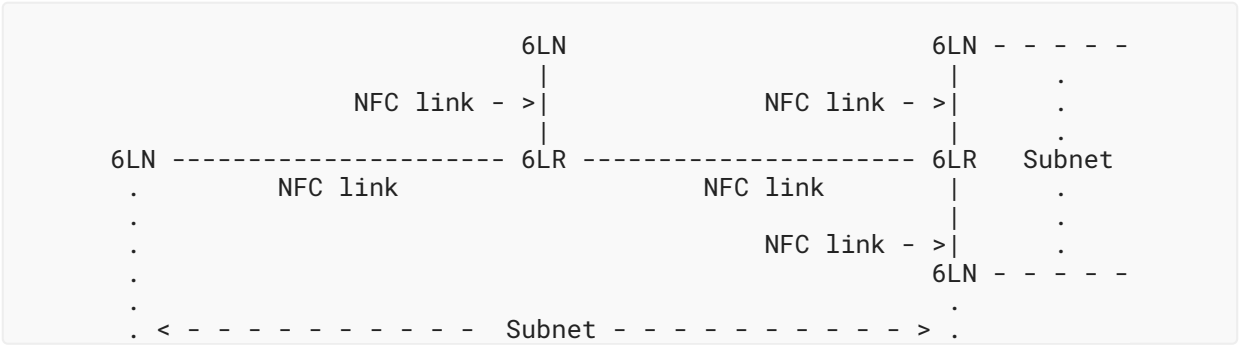

Figure 9: Isolated NFC-Enabled Device Network

In multihop (i.e., more complex) topologies, the 6LR can also do the same task. DAD requires the extensions for multihop networks, such as the ones in [RFC6775].

6. IANA Considerations

This document has no IANA actions.

7. Security Considerations

Neighbor Discovery in unencrypted wireless device networks may be susceptible to various threats as described in [RFC3756].

Per the NFC Logical Link Control Protocol [LLCP-1.4]:

- LLCP of NFC provides protection of user data to ensure confidentiality of communications. The confidentiality mechanism involves the encryption of user service data with a secret key that has been established during link activation.
- LLCP of NFC has two modes (i.e., ad hoc mode and authenticated mode) for secure data transfer. Ad hoc secure data transfer can be established between two communication parties without any prior knowledge of the communication partner. Ad hoc secure data transfer can be vulnerable to on-path attacks. Authenticated secure data transfer provides protection against on-path attacks. In the initial bonding step, the two communicating parties store a shared secret along with a Bonding Identifier.
- For all subsequent interactions, the communicating parties reuse the shared secret and compute only the unique encryption key for that session. Secure data transfer is based on the cryptographic algorithms defined in the NFC Authentication Protocol [NAP-1.0].

Furthermore, NFC is considered by many to offer intrinsic security properties due to its short link range. When IIDs are generated, devices and users are required to consider mitigating various threats, such as correlation of activities over time, location tracking, device-specific vulnerability exploitation, and address scanning. However, IPv6 over NFC uses an RID [RFC7217] as an IPv6 IID; NFC applications use short-lived connections and a different address is used for each connection where the latter is of extremely short duration.

8. References

8.1. Normative References

[LLCP-1.4] NFC Forum, "Logical Link Control Protocol Technical Specification", Version 1.4, December 2022, <https://nfc-forum.org/build/specifications>.

[NAP-1.0] NFC Forum, "NFC Authentication Protocol Technical Specification", Version 1.0, December 2022, <https://nfc-forum.org/build/specifications>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <https://www.rfc-editor.org/info/rfc4086>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007, <https://www.rfc-editor.org/info/rfc4919>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <https://www.rfc-editor.org/info/rfc4944>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/info/rfc6282>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>.

[RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <https://www.rfc-editor.org/info/rfc7136>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <https://www.rfc-editor.org/info/rfc7400>.

[RFC8025] Thubert, P., Ed. and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch", RFC 8025, DOI 10.17487/RFC8025, November 2016, <https://www.rfc-editor.org/info/rfc8025>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <https://www.rfc-editor.org/info/rfc8505>.

8.2. Informative References

[ECMA-340] ECMA International, "Near Field Communication - Interface and Protocol (NFCIP-1)", 3rd Edition, ECMA 340, June 2013, <https://www.ecma-international.org/wp-content/uploads/ECMA-340_3rd_edition_june_2013.pdf>.

[IANA-6LoWPAN] IANA, "IPv6 Low Power Personal Area Network Parameters", <https://www.iana.org/assignments/_6lowpan-parameters>.

[IEEE802.15.4] IEEE, "IEEE Standard for Low-Rate Wireless Networks", IEEE Std 802.15.4-2020, DOI 10.1109/IEEESTD.2020.9144691, July 2020, <https://ieeexplore.ieee.org/document/9144691>.

[RFC3756] Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, DOI 10.17487/RFC3756, May 2004, <https://www.rfc-editor.org/info/rfc3756>.

Acknowledgements

We are grateful to the members of the IETF 6lo Working Group.

Michael Richardson, Suresh Krishnan, Pascal Thubert, Carsten Bormann, Alexandru Petrescu, James Woodyatt, Dave Thaler, Samita Chakrabarti, Gabriel Montenegro, Erik Kline, and Carles Gomez Montenegro have provided valuable feedback for this document.

Authors' Addresses

Younghwan Choi (EDITOR)
Electronics and Telecommunications Research Institute
218 Gajeongno, Yuseung-gu
Daejeon
34129
South Korea
Phone: +82 42 860 1429
Email: yhc@etri.re.kr

Yong-Geun Hong
Daejon University
62 Daehak-ro, Dong-gu
Daejeon
34520
South Korea
Phone: +82 42 280 4841
Email: yonggeun.hong@gmail.com

Joo-Sang Youn
DONG-EUI University
176 Eomgwangno Busan_jin_gu
Busan
614-714
South Korea
Phone: +82 51 890 1993
Email: joosang.youn@gmail.com