

# Transmission of IPv6 Packets over Near Field Communication

*draft-ietf-6lo-nfc-14 & 15*  
*(Since the reviews of 1<sup>st</sup> TELECHAT)*

Younghwan Choi (ETRI),  
Y-G. Hong (ETRI), J-S. Youn (DONG-EUI Univ.),  
D-K. Kim (KNU), J-H. Choi (Samsung)

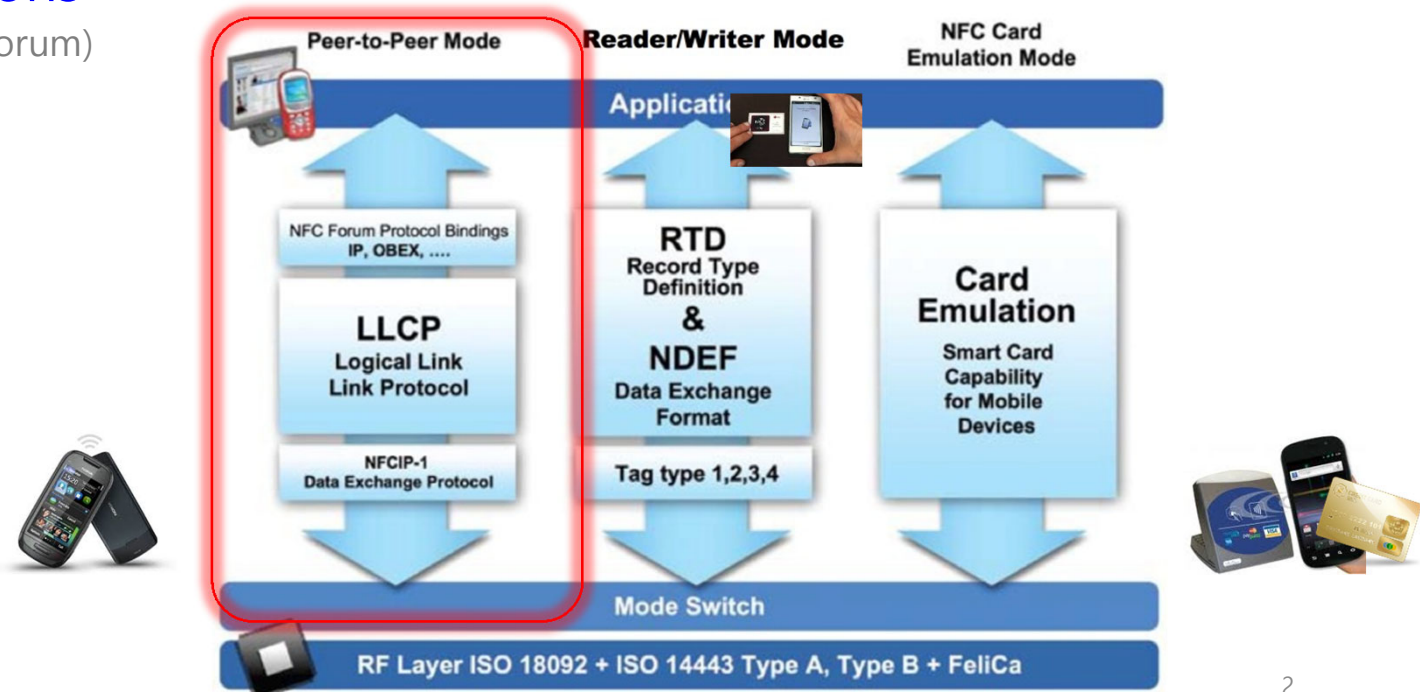
**6lo WG Meeting@IETF105 – Montreal, Canada**  
**2019. 7. 22.**

# What is Near Field Communication (NFC) ?

- NFC technology enables (Source: NFC Forum)
  - simple and **safe two-way interactions** between electronic devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices **with a single touch**.

- NFC Functions

(Source: NFC forum)



# History and status of IPv6-over-NFC

- **WG Adoption: draft-ietf-6lo-nfc-00**  
(Mar 03, 2015)

- Update Stateless address autoconfiguration

- **1<sup>st</sup> ~ 5<sup>th</sup> Revision**

- **ver-01** (July, 2015)
  - MAC PDU size and MTU
  - SLAAC and IPv6 link local address
  - Fragmentation and Reassembly
- **ver-02** (Oct, 2015) @Buenos Aires
  - Dispatch Header (added)
  - Header Compression (modified for GHC)
- **ver-03** (Apr. 2016) @Berlin, DE
  - Some typos fixed
  - Section 7. Security Considerations
- **Ver-04** (Jul. 2016)
  - NFC FAR-related sentence updated
  - Related to "multi-hop topologies"
- **ver-05** (Oct. 2016) @Seoul, KR
  - Feedback from NFC forum
  - IID generation (feedback from Dave)

- **Revisions for WGLC**

- **ver-06** (by Dave Thaler, Sep. 2016)
  - IID generation (2<sup>nd</sup> rev.)
- **ver-07** (by James Woodyett Jun. 2017)
  - IID generation (4<sup>th</sup> rev.) -> RFC7217
  - Neighbor Discovery -> Reworded
- **ver-08,-09** (by Pascal Thubert, Nov. 2017)
  - Neighbor Discovery -> Reworded
- **ver-10, -11** (by Shepherd, Jul. 2018)
  - Revised texts for clarification about NFC MTU & FAR, ND, Security
- **No more feedback from NFC forum** (since Jan. 2017)
- **WGLC** (Mar. 2018~Jul. 2018)
  - **New Shepherd: Samita Chakrabarti**
- **ver-11, -12** (by IOTdir & INTdir, Nov. 2018)
- **ver-13** (1<sup>st</sup> IESG reviews, Mar. 2019)
- **ver-14, -15 (Montreal, Jul. 2019)**

# 1<sup>st</sup> IESG Reviews (1/5)

- **Marketing Expressions**

- > **Removed or Reworded with only technical point**

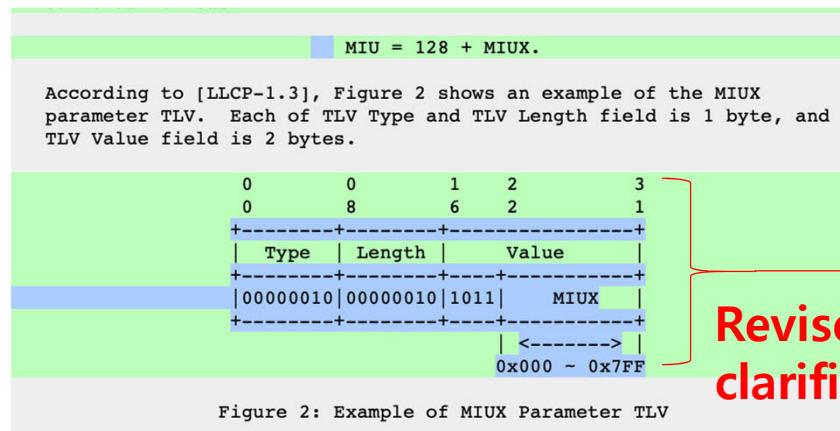
- § 5.2, outstanding performance ("outstanding" is removed)
  - § 1, "NFC builds upon RFID systems by allowing two-way communication between endpoints, where earlier systems such as contactless smart cards were one-way only"
    - > "NFC builds upon RFID systems by allowing two-way communication between endpoints." :
  - § 1, "NFC also has the strongest ability (e.g., secure communication distance of 10 cm) to prevent a third party from attacking privacy."
    - > "NFC can provide secured communications with its short transmission range."
  - § 3, "NFC technology enables simple and safe two-way interactions between electronic devices"
    - > "NFC enables simple and two-way interaction between two devices" :
  - § 3, "NFC's bidirectional communication ability is ideal for establishing connections with other technologies by the simplicity of touch." (removed)

- **Editorial Changes**

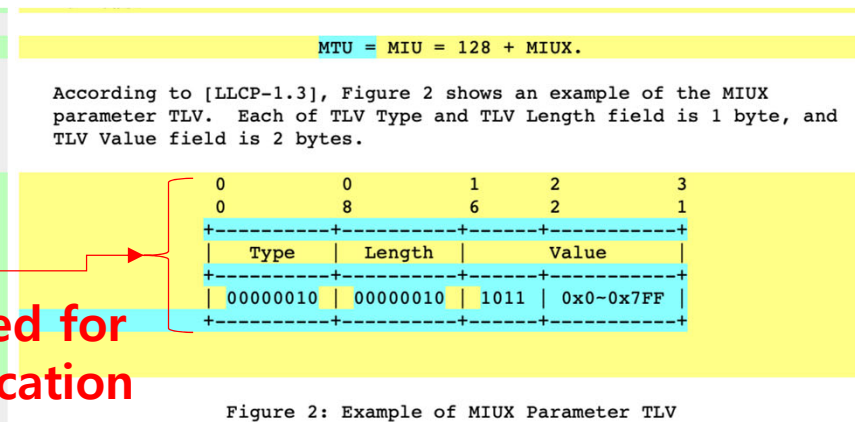
- Abstract. "no more than 10 cm" -> "no more than 10 cm apart", "6LowPAN" -> "6LoWPAN"
  - § 1, "It had been used" -> "It has been used", "It was expected" -> "It is expected", "running the other operating systems" -> "running other operating systems", remove "potential for".
  - § 5.1, "the a 6LBR" --> "a 6LBR", "LNs" --> "6LNs"
  - § 5.2, "LRs" --> "6LRs"
  - about RFC2119, "SHOULD, MAY, MUST, NOT RECOMMEND..."

# 1<sup>st</sup> IESG Reviews (2/5)

- § 3.4, about MIUX



Revised for clarification



# 1<sup>st</sup> IESG Reviews (3/5)

- § 4.1, about Figure 3..

## 4.1. Protocol Stacks

Figure 3 illustrates IPv6 over NFC. Upper layer protocols can be transport layer protocols (TCP and UDP), application layer protocols, and others capable running on top of IPv6.

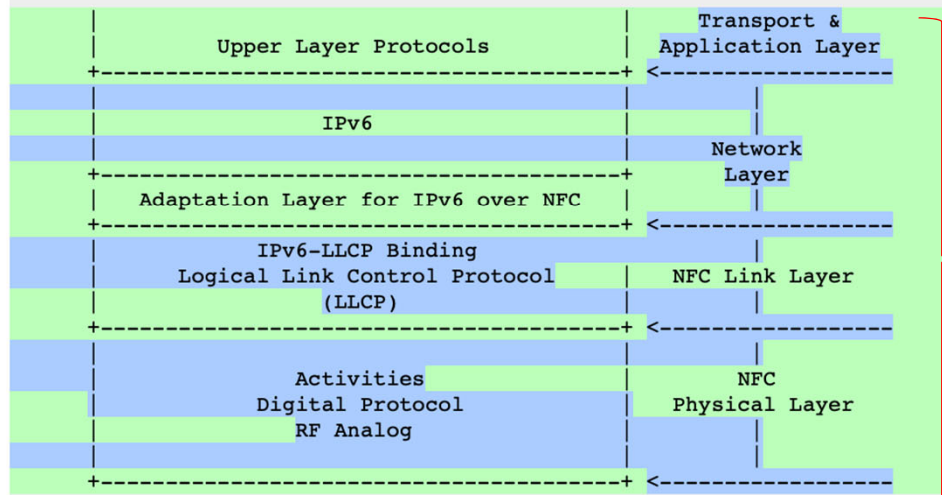
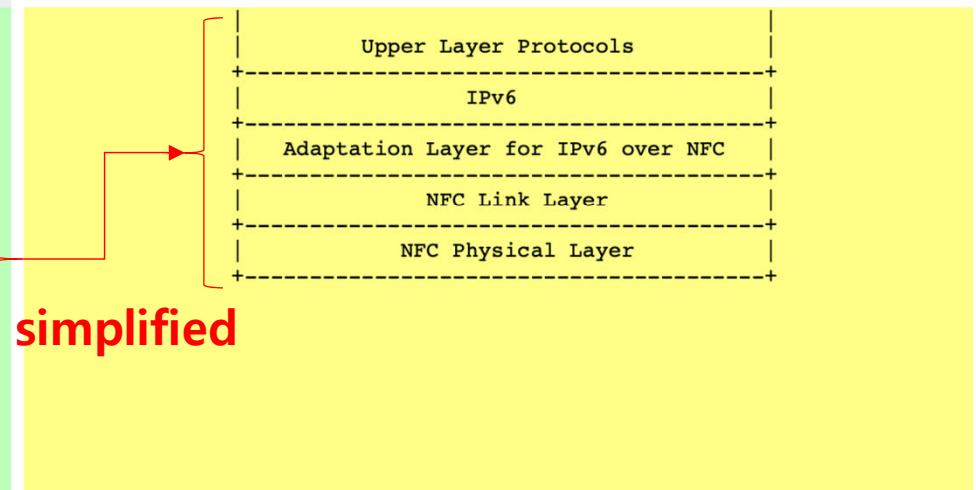


Figure 3: Protocol Stacks for IPv6 over NFC

## 4.1. Protocol Stacks

Figure 3 illustrates IPv6 over NFC. Upper layer protocols can be transport layer protocols (TCP and UDP), application layer protocols, and others capable running on top of IPv6.



simplified

Figure 3: Protocol Stacks for IPv6 over NFC

# 1<sup>st</sup> IESG Reviews (4/5)

- § 4.5, about ND

## 4.5. Neighbor Discovery

Neighbor Discovery Optimization for 6LoWPANs ([RFC6775]) describes the neighbor discovery approach in several 6LoWPAN topologies, such as mesh topology. NFC does not support a complicated mesh topology but only a simple multi-hop network topology or directly connected peer-to-peer network. Therefore, the following aspects of RFC 6775 are applicable to NFC:

- o When an NFC-enabled device (6LN) is directly connected to a 6LBR, an NFC 6LN MUST register its address with the 6LBR by sending a Neighbor Solicitation (NS) message with the Address Registration Option (ARO) and process the Neighbor Advertisement (NA) accordingly. In addition, if DHCPv6 is used to assign an address, Duplicate Address Detection (DAD) is not necessary.
- o When two or more NFC 6LNs(or 6LRs) meet, there are two cases. One is that three or more NFC devices are linked with multi-hop connections, and the other is that they meet within a single hop range (e.g., isolated network). In a case of multi-hops, all of 6LNs, which have two or more connections with different neighbors, MAY be a router for 6LR/6LBR. In a case that they meet within a single hop and they have the same properties, any of them can be a router. When the NFC nodes are not of uniform category (e.g., different MTU, level of remaining energy, connectivity, etc.), a performance-outstanding device can become a router. Also, they MUST deliver their MTU information to neighbors with NFC LLCp protocols during connection initialization. The router MAY also communicate other capabilities which is out of scope of this document.

## 4.5. Neighbor Discovery

Neighbor Discovery Optimization for 6LoWPANs ([RFC6775]) describes the neighbor discovery approach in several 6LoWPAN topologies, such as mesh topology. NFC does not support a complicated mesh topology but only a simple multi-hop network topology or directly connected peer-to-peer network. Therefore, the following aspects of RFC 6775 are applicable to NFC:

- o When an NFC-enabled device (6LN) is directly connected to a NFC-enabled 6LBR, an NFC 6LN MUST register its address with the 6LBR[RFC4944] by sending a Neighbor Solicitation (NS) message with the Address Registration Option (ARO) and process the Neighbor Advertisement (NA) accordingly. In addition, when the 6LN and 6LBR are directly connected, DHCPv6 is used for address assignment. Therefore, Duplicate Address Detection (DAD) is not necessary between them.
- o When two or more NFC 6LNs[RFC4944](or 6LRs) are connected, there are two cases. One is that three or more NFC devices are linked with multi-hop connections, and the other is that they meet within a single hop range (e.g., isolated network). In a case of multi-hops, all of 6LNs, which have two or more connections with different neighbors, is a router for 6LR/6LBR. In a case that they meet within a single hop and they have the same properties, any of them can be a router.

Under-specified -> removed



# 1<sup>st</sup> IESG Reviews (4/5)

- § 7, about Security considerations

## 7. Security Considerations

**moved**

When interface identifiers (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.

IPv6-over-NFC is, in practice, not used for long-lived links for big size data transfer or multimedia streaming, but used for extremely short-lived links (i.e., single touch-based approaches) for ID verification and mobile payment. This will mitigate the threat of correlation of activities over time.

IPv6-over-NFC uses an IPv6 interface identifier formed from a "Short Address" and a set of well-known constant bits (such as padding with '0's) for the modified EUI-64 format. However, the short address of NFC link layer (LLC) is not generated as a physically permanent value but logically generated for each connection. Thus, every single touch connection can use a different short address of NFC link with an extremely short-lived link. This can mitigate address scanning as well as location tracking and device-specific vulnerability exploitation.

Thus, this document does not RECOMMEND sending NFC packets over the Internet or any unsecured network.

If there is a compelling reason to send/receive the IPv6-over-NFC packets over the unsecured network, the deployment SHOULD make sure that the packets are sent over secured channels. The particular Security mechanisms are out of scope of this document.

**revised for clarification**

## 7. Security Considerations

This document does not RECOMMEND sending NFC packets over the Internet or any unsecured network.

When interface identifiers (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.

**unclear -> removed**

IPv6-over-NFC uses an IPv6 interface identifier formed from a "Short Address" and a set of well-known constant bits for the modified EUI-64 format. However, NFC applications use short-lived connections, and the every connection is made with different address of NFC link with an extremely short-lived link.

This document does not RECOMMEND sending NFC packets over the Internet or any unsecured network. Especially, there can be a threat model in the scenario of Section 5.1. when the NFC-enabled device links to a NFC-enabled gateway for connectivity with the Internet, the gateway can be attacked. Even though IPv6 over NFC guarantees security between the two NFC devices, there can be another threat during packet forwarding.



**Any Questions & Comments?**