Transmission of IPv6 Packets over Near Field Communication

draft-hong-6lo-ipv6-over-nfc-02.txt

Y. Hong, Y. Choi (ETRI),
J. Youn (DONG-EUI Univ.), D. Kim (KNU)
JH. Choi (Samsung)

6lo WG Meeting@IETF 91 – Honolulu, USA
2014.11.11

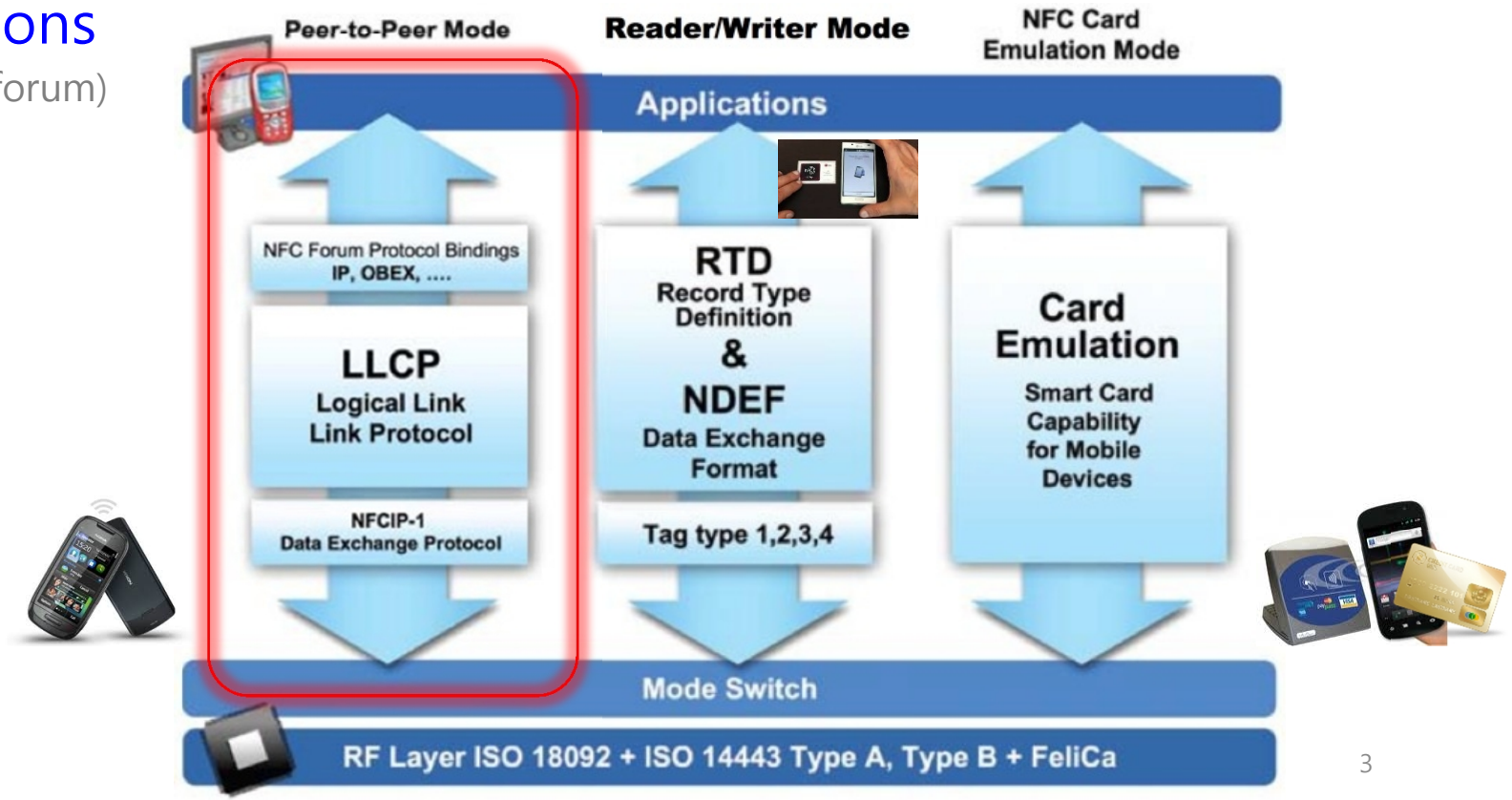
History and status

- Initial: draft-hong-6lo-ipv6-over-nfc-00.txt (July.7.2014)
  - Presented at IETF-90 6lo WG meeting
  - Positive feedback from Michael Richardson, Pascal Thubert, Suresh Krishnan
- Update 01: draft-hong-6lo-ipv6-over-nfc-01.txt (Aug.14.2014)
  - Suresh comment at IETF 90: It needs detail address mapping
  - Resolve: Add Uncast address mapping and multicast address mapping respectively
- Update 02 : draft-hong-6lo-ipv6-over-nfc-02.txt (Aug.26.2014)
  - Complete TBD parts

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)



What Are Differences ?

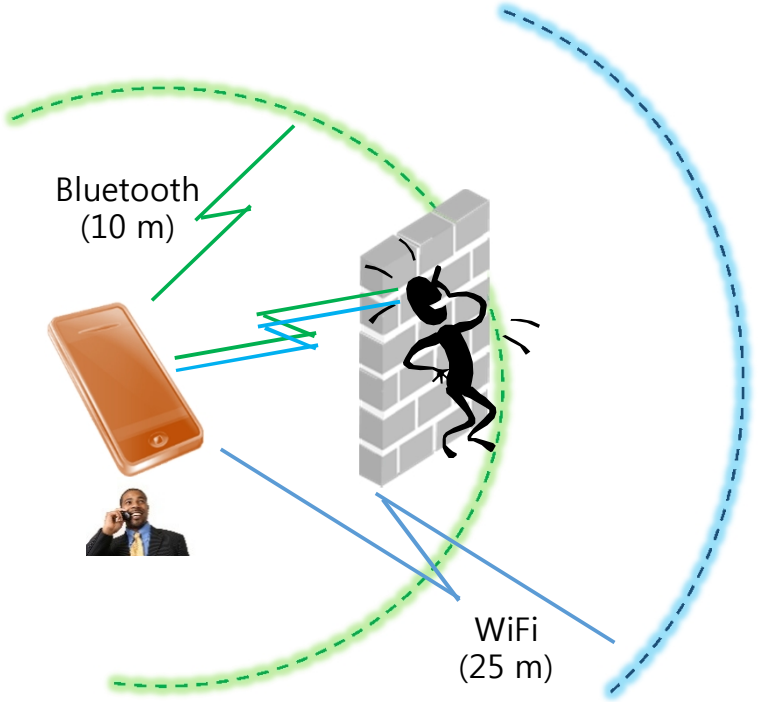
- Comparison with Bluetooth (Source: Wikipedia)

Aspect	**NFC**	Bluetooth	Bluetooth Low Energy
RFID compatible	ISO 18000-3	active	active
Standardisation body	ISO/IEC	Bluetooth SIG	Bluetooth SIG
Network Standard	ISO 13157 etc.	IEEE 802.15.1	IEEE 802.15.1
Network Type	**Point-to-point**	WPAN	WPAN
Cryptography	not with RFID	available	available
Range	**< 0.2 m**	~100 m (class 1)	~50 m
Frequency	13.56 MHz	2.4–2.5 GHz	2.4–2.5 GHz
Bit rate	**424 kbit/s**	2.1 Mbit/s	1 Mbit/s
Set-up time	**< 0.1 s**	< 6 s	< 0.006 s
Power consumption	**< 15mA (read)**	varies with class	< 15 mA (read and transmit)

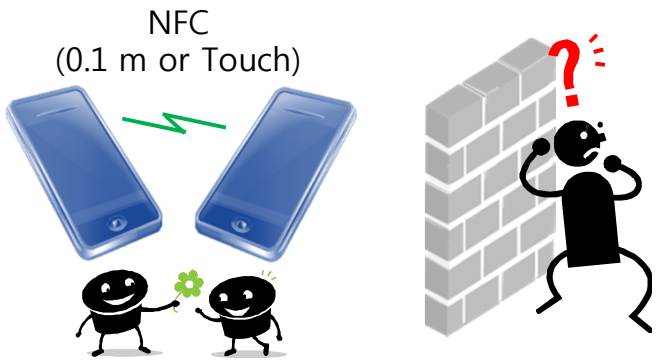
Why Possible and Useful ?

- Private Devices (especially, mobile phones)
  - have a lot of personal information (secured and private)
  - should be protected from hidden hackers

- NFC can be the one of the best solutions for Security
  - Due to short range communication (< 20 cm)
  - WiFi or Bluetooth cannot be safe from hidden hackers than NFC when we provide our personal information because of a long range.

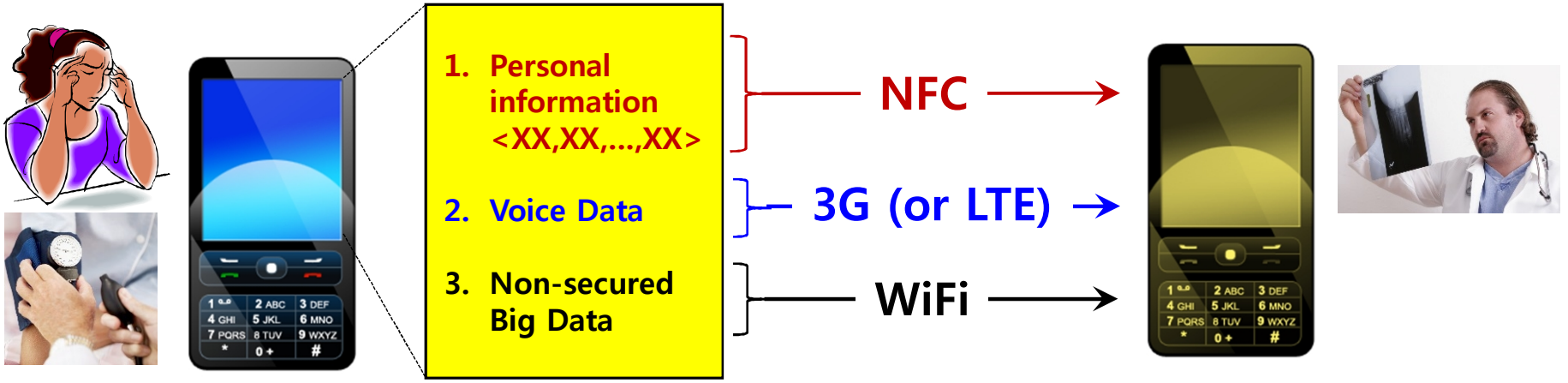


- In addition, 271 NFC Phones Available Now (source: www.nfcworld.com)
  - made by Samsung, LG, Acer, Amazon, Asus, BlackBerry, HTC, Huawei, Nokia, Sony, ZTE, etc.
    (Rumoured NFC devices: iPhone 6)
  - NFC technology would be widely used with WiFi and Bluetooth in IoT environments.



With a Possible Example for NFC Use

- Scenario
  - A User wants to securely provide his personal information (e.g., certificate or results of blood pressure measurement, etc.) to his doctor via an app. in a mobile phone.
  - The app usually sends non-secured big data through WiFi, but it can securely send the personal information to his doctor by using only NFC.
  - Then the personal information can be secured from hidden hackers.



draft-hong-6lo-ipv6-over-nfc-02

Table of Contents

Key Issues 1: Connectivity

- NFC-enabled device connected to the Internet

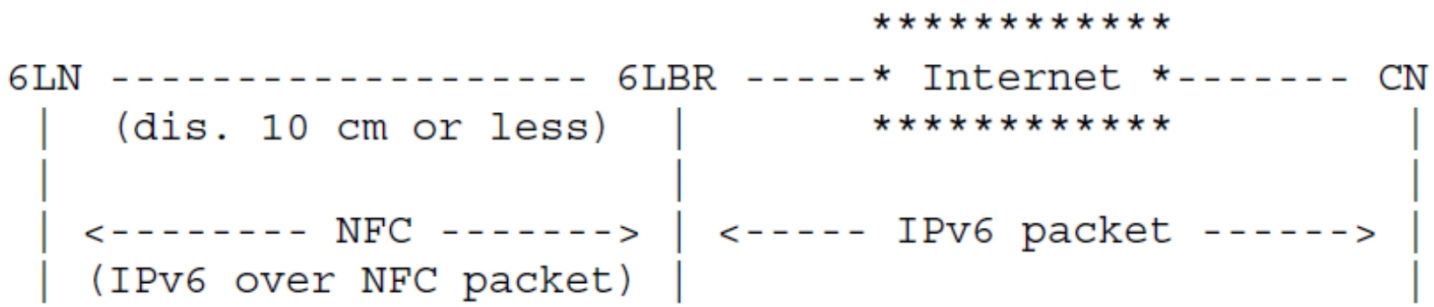


Figure 5: NFC-enabled device network connected to the Internet

- Isolated NFC-enabled device network

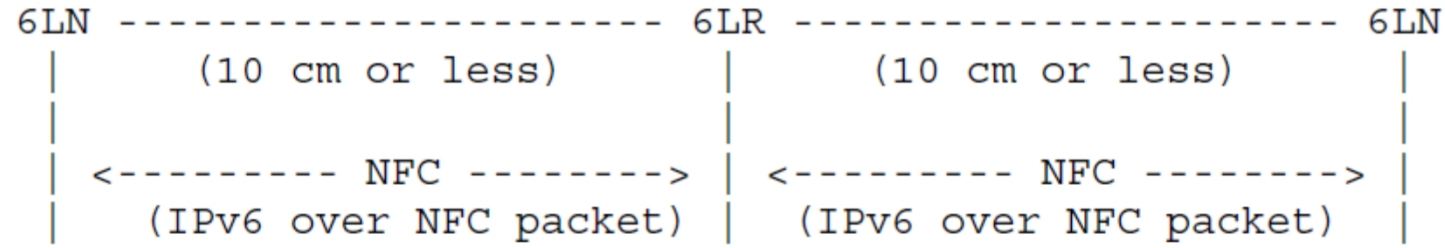


Figure 6: Isolated NFC-enabled device network

Key Issue 2: Address configuration

- Stateless address auto configuration
  - A 64-bit IID for a NFC interface MAY be formed by utilizing the 6-bit NFC LLCP address

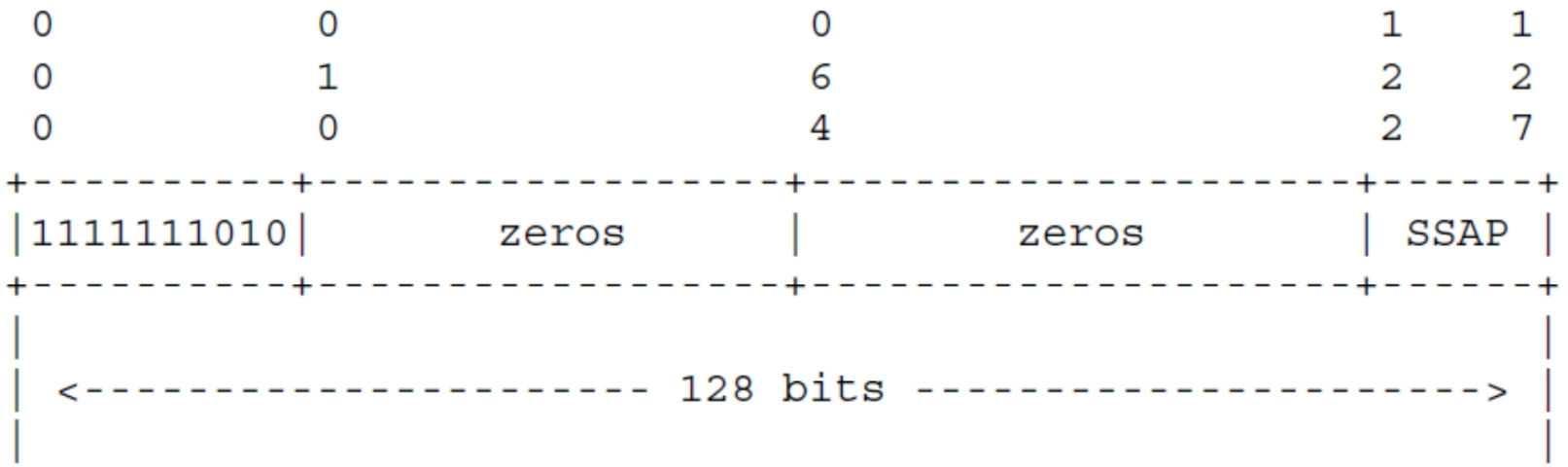


Figure 4: IPv6 link-local address in NFC

Key Issue 3: Header Compression

- Header compression as defined in RFC 6282 [5] , 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 RFC 6282 encoding formats.

- (TBD) Two Approaches According to Connectivity Pattern
  - When a NFC-enabled device is connected to the Internet ?
    -> possibly more compressible
  - When a Isolated NFC-enabled device network ?

Key Issue 4: Fragmentation and Reassembly (FAR)

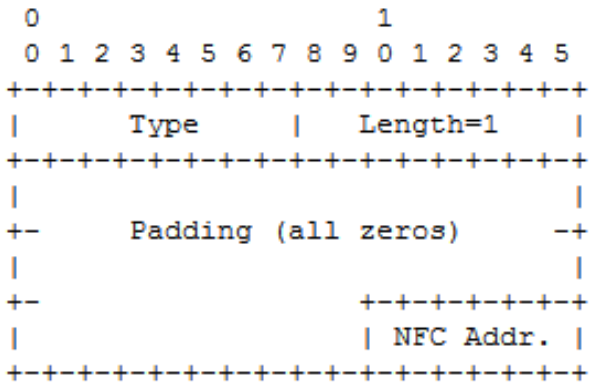
- Fragmentation and reassembly (FAR) as defined in RFC 4944, which specifies the fragmentation methods for IPv6 datagrams on top of IEEE 802.15.4, is REQUIRED in this document as the basis for IPv6 datagram FAR on top of NFC.

- All headers MUST be compressed according to RFC 4944 encoding formats.

- Considerations
  - Default MTU of NFC is 128 bytes.
  - NFC Link Local Layer does not support Fragmentation and Reassembly.
  - FAR SHOULD be conducted while NFC devices are single-touched

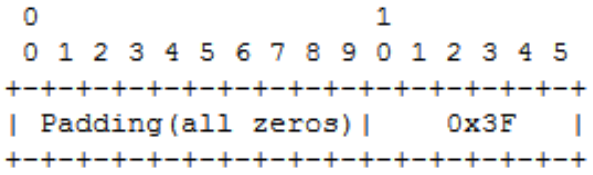
Key Issue 5: Unicast/Multicast address mapping

- Unicast address mapping



- Type:
  1: for Source Link-layer address
  2: for Target Link-layer address
- Length:
  The length of this option (including type and length)
  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

- Multicast address mapping

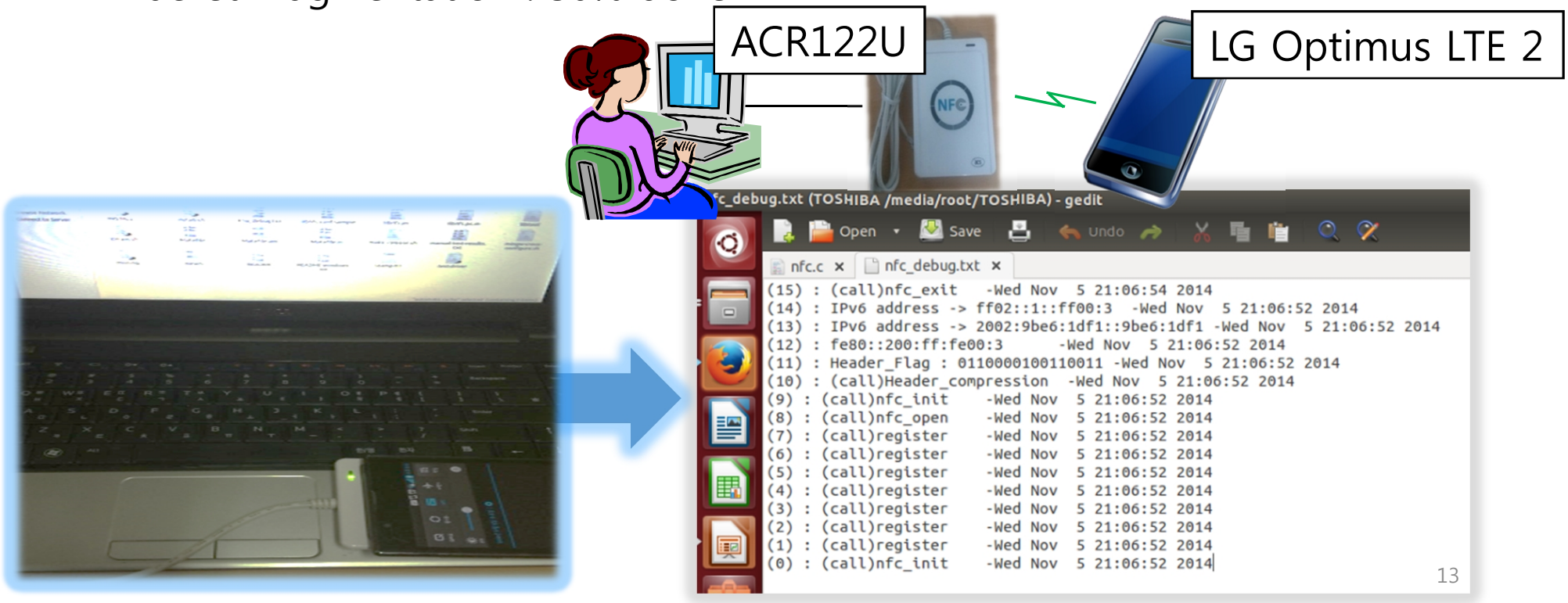


- All IPv6 multicast packets MUST be sent to NFC Destination Address 255 (broadcast) and filtered at the IPv6 layer.
- When represented as a 16-bit address in a compressed header, it MUST be formed by padding on the left with a zero.

Implementation of IPv6 over NFC

- Test-bed
  - ACR112U NFC Chipset & LG Optimus (NFC-enabled)

- Current Status
  - Compressed Header generation : done (verifying)
  - IPv6 address of the source node compression : done (verifying)
  - Packet Fragmentation : 50% done



Conclusions

- IPv6 over NFC
  - IPv6-over-foo adaptation layer specifications using 6LoWPAN
- Key issues of IPv6 over NFC
  - Key Issue 1: Connectivity
  - Key Issue 2: Address configuration
  - Key Issue 3: Header Compression
  - Key Issue 4: Fragmentation and Reassembly (FAR)
  - Key Issue 5: Unicast/Multicast address mapping
- Next step
  - Become a WG document?