Intro to Mobi-D

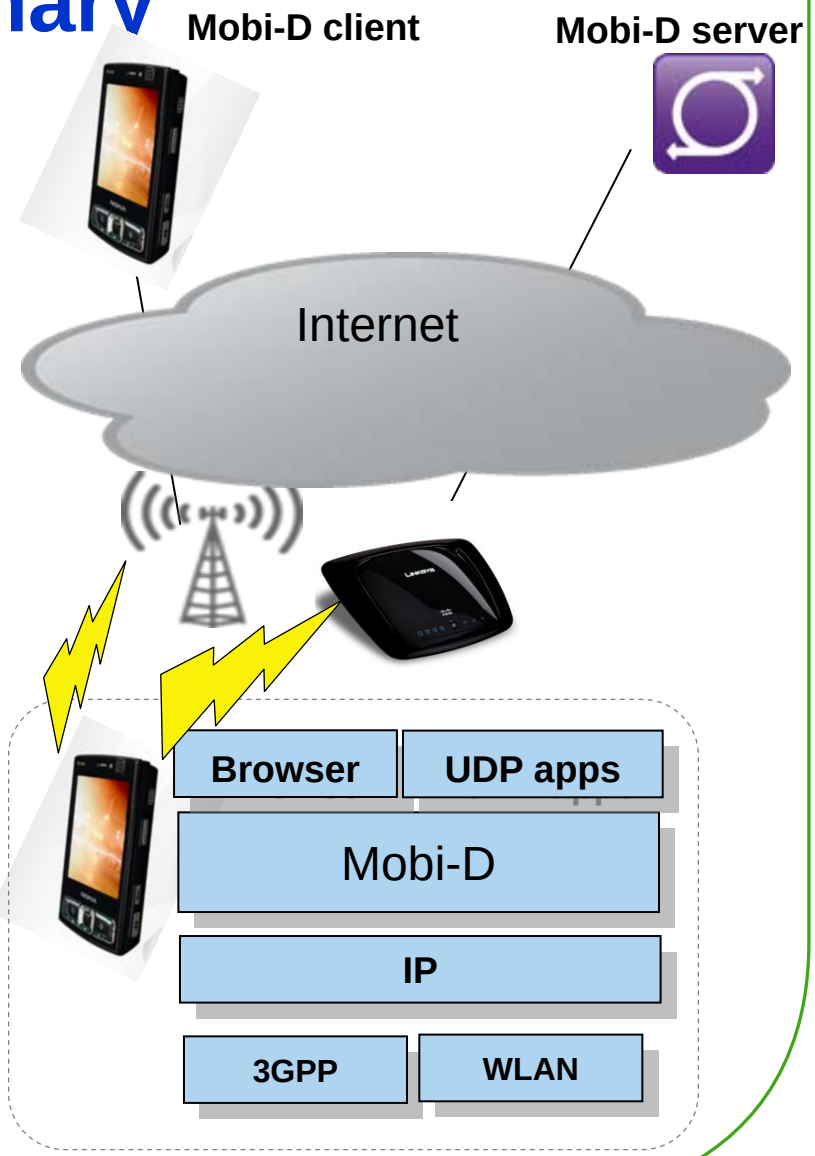
Host based mobility

Michael G. Williams, Jeremey Barrett

Mobi-D: Executive Summary

What:

- draft-barrett-mobile-dtls-00.txt
- **Host based mobility (HBM) using secure identities to provide end to end mobility**
  - A small extension to DTLS
  - DTLS (Datagram TLS) is IETF standard protocol (RFC 4347)
  - Extension provides mobility for single or multi access devices



Mobi-D: Executive Summary

Why: host based mobility (HBM)

- Avoids the considerable delay in doing a connection handshake when a mobility event occurs
- Avoids additional handshake overhead of application reconnecting after mobility
- Can add mobility to DTLS VPN
- Can be used where there is no support for PMIP or client MIP
- Can be used in client-server or mobile-to-mobile connectivity
- Can be implemented in application, middleware or in kernel
- Can be distributed to most existing clients as library or software upgrade
- Requires no proxy, agents, signaling or triangular routing needed
- Traverses NATs
- No privacy issues due to middle boxes or bindings between L2 or L3 addresses and higher layers

Host Based Mobility based on Secure Identities

Mobi-D extends DTLS in four ways:

1. A new DTLS Hello extension (Mobility)
2. A new TLS Hello extension (OP)
3. An additional field in the Record Layer (connection_id)
4. A new type of message (OP)

Flow instantiation follows TLS oriented client host and server model

- Host and server discover Mobility extension and OP extension
- Mutually authenticate each other, exchange keys
- Host and server each allocate a mobility connection (MoCo) identifier
- Host and server exchange packets using the MoCo and keys
- When host moves and gets new IP address (or uses another interface with a different IP address), host sends next packet from new IP address as usual
- Server accepts packet because it has the MoCo and valid key
- Server updates return IP address
- Host can send new TLS OP proactively to update IP address if there are no other packets to send

Current Status

- **DTLS**
  - Stable spec since 2006
  - Open SSL based implementations available
- **IETF**
  - I-D **draft-barrett-mobile-dtls-00.txt** in first draft
  - Review from some in TLS community expressed interest, positive feedback
- **Implementation**
  - Nokia working on implementation, looking for other partners
- **Is there working group interest?**

Backup slides

Host based mobility

Short Background of DTLS

- **TLS**
  - Extremely widely deployed
  - TLS layers between transport and application to provide security
  - TLS requires reliable transport
- **DTLS**
  - RFC 4347 (2006)
  - Datagram TLS provides UDP based transport while using TLS security
  - As with UDP, doesn’t re-order or re-transmit packets
  - DTLS developed to provide same ease of use and implementation as TLS but with UDP transport
  - Designed not to require kernel modifications to implement
- **Use in industry**
  - Work near completion to provide keying support for SIP / VoIP
  - Used as a transport for IETF’s CAPWAP protocol, connects APs and ACs

Short Description of Mobi-D

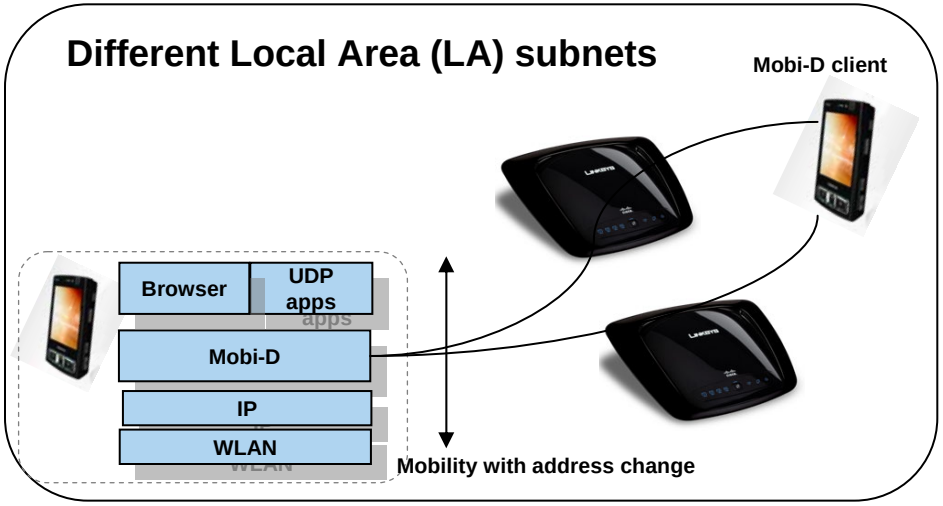
- **Differences from DTLS**
  - Adds mobile connection identifier (MoCo) to the DTLS record layer
  - Automatically updates IP address of mobile host with or without signalling
  - Adds TLS OP for optimized notifying TLS client or server of IP address change, and other uses
  - Enables multiplexing and mobility using the existing TLS Security Parameters
- **Host Based Mobility (HBM)**
  - Complements PMIP: PMIP supplies mobility in the network side without client support
  - Also compliments client MIP: Mobi-D supplies host based mobility, without network support
  - Can be used when neither PMIP nor MIP are available in the network
  - Individual flows can be switched between interfaces
  - Application doesn’t need to participate or be aware above middleware
    - Stack-Internal signalling available from Mobi-D implementation can notify app to handle mobility changes if desired

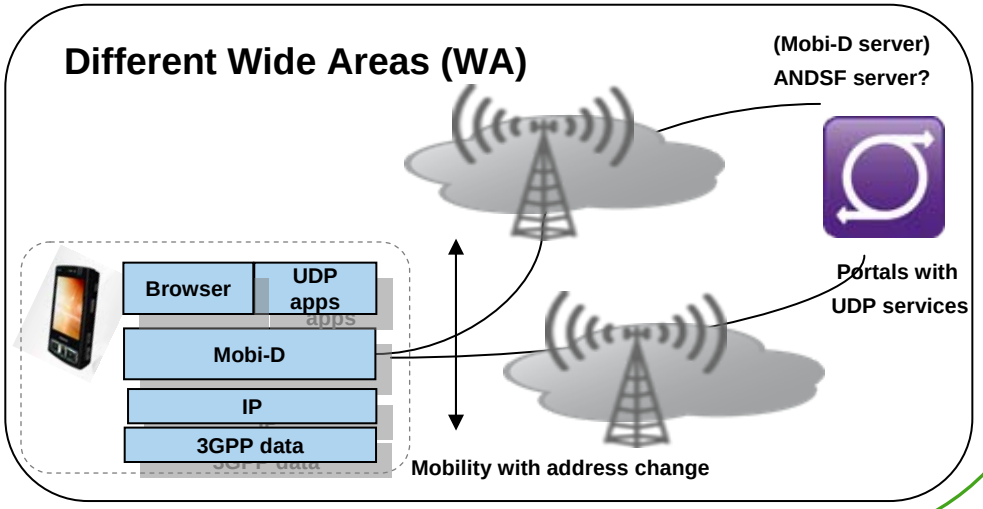
Use Cases for Mobi-D

- **For Wide Area only device**
  - Handover of UDP based applications between operators without operator support
    - Can work with any packet based wide area access including existing
- **For multi-access Local and Wide Area interface device**
  - Handover of UDP based applications between local and wide area
  - Can work with existing local area networks today
- **Applications**
  - Media players on Linux and Symbian
  - DTLS VPNs
  - Managed IP TV
  - Like Adobe and Flash RTMFP (Real time media flow protocol over UDP)
    - Legitimizing P2P, Air, Stratus rendezvous server
    - Server or serverless voice, Messaging
    - File transfer
  - Maps
  - Games
  - P2P mobile

Scenarios for Mobi-D (1 of 3)

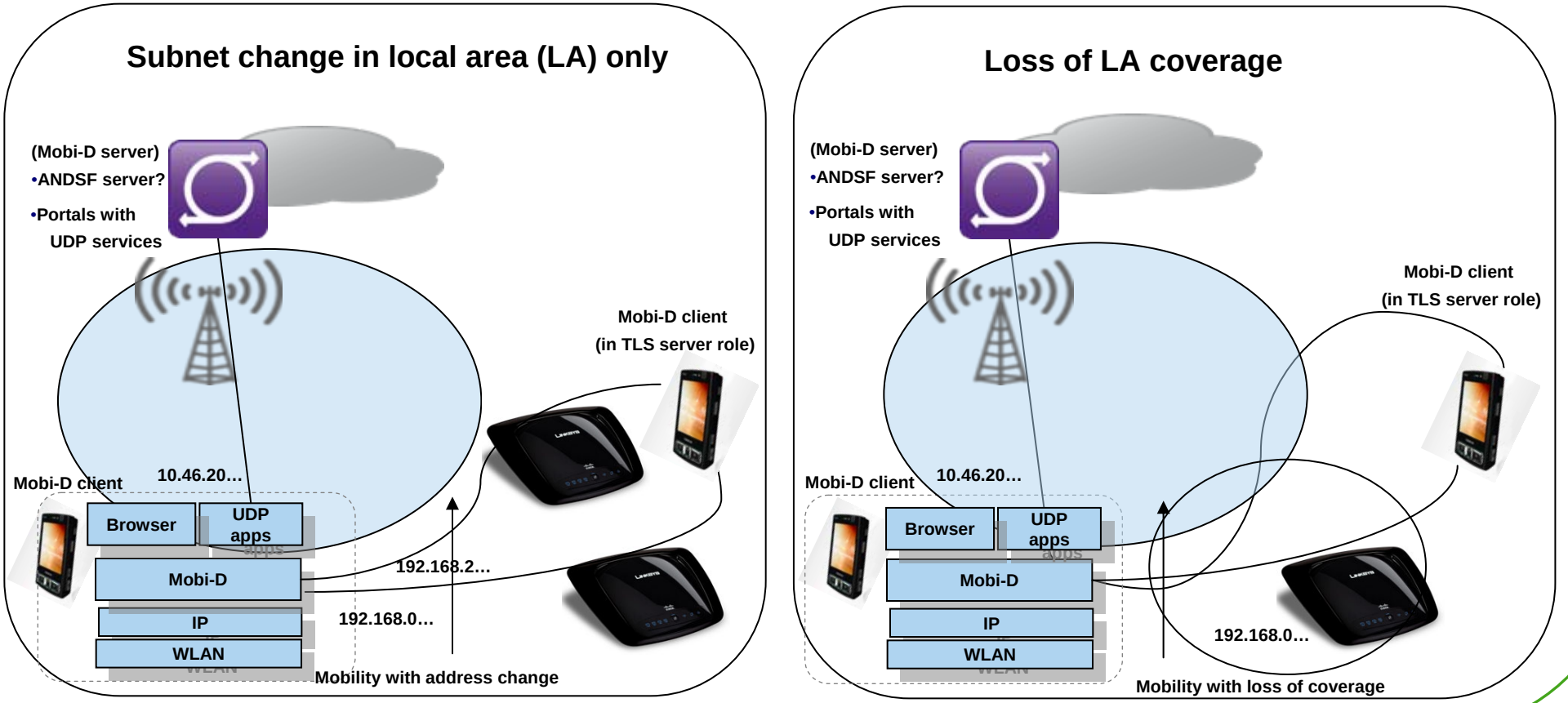
- **Single Interface device**
  - Device and server perform TLS handshake and MoCo allocation for each flow that needs multiplexing or mobility
  - Device moves to new network and changes IP address, with continuous connection
  - Other end continues connection that is using the MoCo and TLS Security Parameters
  - Automatically updates IP address of mobile host without signalling
  - MoCo per flow enables the device to have multiple flows on an interface





Scenarios for Mobi-D (2 of 3)

- **Multi Interface device**
  - A variety of possibilities with multiple interfaces



Scenarios for Mobi-D (3 of 3)

- **NAT**
  - Server based application or mobile to mobile scenario with NAT(s)