Challenges in New 4G Wireless Networks

Charlie Perkins
charliep@computer.org
Outline of presentation

- Objectives:
  - Describe likely future evolution of Internet (95+% wireless)
  - Suggest research directions
- Wireless networks today
- Competing “industry” standards
- IETF standards for mobility management
- Test case: how to use Mobile IP for LTE
- Seamless Mobility
- What’s next?
Wireless today

- [www.bbc.co.uk/news/10569081](http://www.bbc.co.uk/news/10569081): 5 billion cellphones
  - China has 815M, India has 670M (growing 15M/month!)
  - US is a distant third
  - Russia next, with 147% penetration!
  - less than 1 billion ten years ago

- Lots of bandwidth
  - People usually don’t lust after wired connectivity

- but not enough
  - iPhone meltdown

- Soon: vehicular networks, machine-machine
  - more pressure on address space
Wireless handsets today

- Internet access becoming very widespread
  - If it’s filtered, is it still “the Internet”?  
  - IETF Beijing – to me very surprising!
- 100 Gbytes is a lot of storage
  - Wikipedia is 20 Gbytes? 40?  
  - World phone book is 10 Gbytes?  
  - About a year's worth of music (.mp3, no repeats)  
  - could already fit well within a cellphone!
- 3-D, stereo, barcodes, security, micropayments, etc.
- General computing – AR/VR – Android – apps
With all of these technology advances, it “should” be straightforward to offer a fully functional mobile website.

- Trivializes data access model (security story needs work)

Why not??

- People are not asking for this feature yet
- Operators want to manage all such “services”
- Private addresses make it difficult (IPv6 **YES!**)  

Two ideas worth investigating in order to get there

- Better NAT
- Seamless interworking
Wireless Industry Standards

- **GSM / GPRS / EDGE / HSPA+** [3GPP]
  - Until HSPA, comparatively … sssllllloooowwww ….

- **CDMA / EVDO / HRPD** [3GPP2]
  - Better, but …

- **WiFi** [IEEE 802]
  - “max” range 150 miles 😊;
  - 802.11ac max bandwidth 1Gb/sec

- **WiMAX** [WimaxForum + IEEE 802]
  - max range 50 km; max speed 30Mb/sec, often < 10Mb/sec.

- **LTE** [3GPP Release 8]
  - max bandwidth 100 Mb/sec; max range > 1-3 km
IETF Standards

- IPv*, DHCP*, routing protocols
- Mobile IP, MIPv6, {P,H,F,DS}MIP, NEMO, MANET, “CMIP”
- AAA (RADIUS/Diameter) *is* economically important
- IPv6 is screwed in tightly enough to (inevitably) *become* economically important
- Utilized properly, *MIP* *should* have greatly simplified 4G wireless infrastructure
  - But, it did not … why??
  - Project: identify technical barriers and resolve
IPv4 address space exhausting

- IANA is out (Jan 2011)
- RIRs run out by Jan. 2012
- What’s next? eBay??
Movement towards IPv6

- Most major infrastructure vendors support IPv6 now
- Verizon mandating IPv6 for all LTE end-devices
- AT&T requiring IPv6 on all future infrastructure
- Google enables IPv6 on all websites
  - Significantly – including YouTube
  - But, for search, you had to be in the whitelist
  - Google “Google IPv6 Conference” for many papers
- US Govt: everything to be IPv6-capable by 2014
- IPv6 Day: June 2011  [Akamai, Google, Facebook …]
- Remaining problems: some applications … ?
IPv4 will dominate the internet for many years

- How many? Who knows?! 5-10 years? Longer?
  - Even 15% for v6 would be huge, business-wise
  - Steady growth, around 0.2%, doubled during 2010.
- Some people are much more optimistic
  - For example, LTE could make things change faster
- What to do in the meantime?
  - Specialized approaches like Skype or STUN
  - “CGNAT” [Carrier-grade NAT]
  - Suffer
Today’s solution (for v4): NAT

- NAT-based solutions have numerous problems
  - NAT traversal is quite problematic
  - Did you ever read your Skype agreement?
- Numerous ALGs required
  - Some features just can’t be supported
  - Try to figure out Bit-torrent, for instance!!
- IETF [behave] working group
  - For instance – check RFC 5382 for TCP reqs
- Very unfriendly to mobility / Mobile IP
Business pitfalls of moving to IPv6 today

- Practically all of the customers are using IPv4
- So, business must serve IPv4 web accesses
- Web presence is required 24 x 7 x 52 x …
- This is not compatible with today’s NAT solutions, or today’s IPv6 solutions
  - Customers need to be able to contact business
  - Not the other way around!
- Needed: “always on” NAT for v4→v6 translation
  - NOTE: NAT is needed for sure [“evil” or not]
Almost any approach tautologically requires use of DNS

IVI: one IPv4 address needed per IPv6 address:
- [no state → no demultiplexing → scalability issue]
- IVI + DHCP, to enable time-based re-use of addresses

SIPNAT (Source-IP NAT), enables simultaneous re-use of each IPv4 address for many different IPv6 addresses
- Demultiplexing based on source IP address
SIPNAT: bidirectional NAT v4 ⇔ v6 (uses DNS)

- Modeled as a flow-management problem
- No changes to IPv6-only hosts or IPv4-only hosts
- No dual-stack; No tunneling
- No port translation required; can use for extra scalability if available
- Would usually delegate special domain to NAT box
For step 3, NAT receives the v4 address request and:

- Overlays a new flow record for v6host at the v4 address NAT_addr4
- Sets BIND_TIMEOUT
- Awaits packet arrival at NAT_addr4 from v4-internet; NATv4 address is “PENDING”

Flow is not complete until source IPv4 addr. known
A few SIPNAT details

- Two failure modes
  - Too many pending NATv4 allocations
  - Too many destinations for a source
  - Rare events, strong dependence on # of IPv4 addresses
- For some protocols (e.g., HTTP v1) 100% accuracy is easy with DPI and other flow-management techniques
- Hybrid / adaptive service foreseen
- Many research papers possible (hint)
SIPNAT current status

- Has been submitted to [behave] wg
- Likely will be combined with IVI + variants
- To each VI address, IVI *assigns* an IV address
  - Not scalable, but good for popular servers
- IVI+DHCP good for time-multiplexed availability
  - IVI multiplexes on port range; not application transparent
WiMAX network architecture -- standardized by WimaxForum

- HA (opt.) Internet gw
- ASN-gw for WiMAX mobility management
  - R3 for ASNgw ↔ HA
  - R6: tunnel to BS
  - R4 for ASNgw ↔ ASNgw
- R8 for BS→BS handover
CDMA network architecture -- standardized by 3GPP2

- PDSN Internet gw (HA+FA)
  - Top-level mobility mgmt

- PCF for each access network
  - A10/A11 ↔ PDSN
  - A8/A9 ↔ BS
  - A23 ↔ PCF
LTE architecture [ >= Release 8] standardized by 3GPP

- LTE access network
- MME
- S-GW
- eNodeB
- UE
- P-GW
- Internet
- GTP-\{C,U\} or PMIP/GRE
Mobile IP (standardized by IETF)

- Routing Prefix from local Router Advertisement
- *Seamless Roaming*: Mobile Node appears “always on” home network
- Address autoconfiguration → care-of address
- Binding Updates → home agent & correspondent nodes
  - (home address, care-of address, binding lifetime)
With PMIP, network handles all mobility management signaling

- LMA ~ HA
- MAG ~ “Foreign Agent”
- UE = “User Equipment”
- CN = “Correspondent Node”
MAP: Mobility Access Point enables localized signaling in an operator domain

“Regional care-of address” reported to MAP, not HA
IETF FMIP (RFC 5568): Smooth/Fast/Seamless Handover

- Smooth handover == low loss
- Fast handover == low delay [30 ms?]
  - Can router pre-empt Duplicate Address Detection??
- Seamless handover:
  - Fast [localized context transfer via HI and HAck]
  - Smooth [buffering]
Mobile-IP based LTE project: Constraints & Goals

Constraints

- eNodeB and MME shouldn’t be changed
- Use existing LTE authentication procedures
- Use existing policy interface via HA

Goals

- Smooth and quick handovers
- Identify Mobile IP features needed to support inferred LTE design goals
- Present at IETF, publish

Currently under consideration as part of DMM effort in [mext] wg
Results: what IETF should do

- GTP should be enabled as a tunnel type for HA ↔ MN
- GTP-C interface to HA
- Foreign agent for IPv6 with FMIP capabilities
- Home Agent → “HA-C”/”HA-D”
- Should specify Hierarchical PMIP
- New MN identifiers
- Revamped CARD / FMIP
- Alternative security has to be enabled
- < for starters>
Seamless Handover: The nightmare has arrived

- Each pair of radio technologies has yet another bulky, incomplete specification [“it’s complicated”]
- Each standards group seems to treat their technology as “owning” the MN (especially LTE)
- Each specification requires operators to administer internal databases according to changes in external networks
- Specifications treat 802.11 as “untrusted / undesirable”
  - Better: should determine trust based on the device
- Mobile IP was originally designed specifically to avoid this outcome
General comments for handover

- Single-radio is the case of interest – otherwise make-before break is available, but battery lifetime is reduced
- Domains assumed to be operated by roaming partners
  - Mutual access to AAA
- Need to “pre-register” – i.e., establish context and allocate datapath resources
- Pre-registration depends on pre-authentication
- Can be generally architected as “SFF” + (AN or pAN)
- ANDSF model is assumed (? Questionable ?)
It would be possible to use Mobile IP for handovers between 4G technologies – BUT:

- LTE does not provide spec for an external home agent

FMIP could be used for smooth handovers, BUT:

- CARD (RFC 4066) is lacking for finding neighborhoods
- Handover context for each technology is wildly dissimilar
- 00033_r000_SR_IWK_Between_Non-WiMAX_and_WiMAX
- R9 is defined for external access to SFF
**S101: LTE → HRPD**

*(one call flow of dozens)*

---

0. UE connected via E-UTRAN

1. CDMA measurements

2. Handover decision

3. Handover from E-UTRA preparation request

4. UL handover preparation transfer

5. Uplink S1 CDMA2000 Tunneling

6. Direct Transfer Request

7. A11 Signalling

8. Direct Transfer Request

9a. Create forwarding tunnels Request

9b. Create forwarding tunnels Response

10. Downlink S1 CDMA2000 Tunneling

11. Mobility from E-UTRA

11. Data Forwarding

12. HRPD AN acquires UE

13. HRPD TCC

14a. A11 Request Signalling

14b. Proxy Binding Update

14c. Proxy Binding Acknowledge

14a. A11 Request Signalling

14d. A11 Response Signalling

15a. Notification Request (HO Complete)

15b. Notification Response

16. UE Context Release

17a. Delete Bearer Request

17b. Delete Bearer Response

18. P-GW initiates resource allocation deactivation procedure at E-UTRAN

---
A few comments on LTE → eHRPD

- A new “S101” identifier is required
- Basestation makes the handover decision
- MME identifies the target access network
- Doesn’t work for WiMAX or WiFi
- Not clear how MME relay to HRPD AN is secure
- LTE P-GW owns the UE [including IP address]
- “It’s complicated”
- Didn’t even talk about S103 yet for “smoothness”
- Didn’t even talk about S102 for voice call continuity
WiMAX → HRPD Handover

- X.S00{57,58}
  - Depending on whether AT context is located in PCF or AN
- Relies on establishing state at a “special” AN
- Uses A23 for handover from “special” AN to target AN
- HRPD SFF mediates signaling (Ref. pt. X1)
- Preregistration sets up PPP tunnel to PDSN (A10/A11)
- Preauthentication straightforward because of HRPD reliance on Mobile IP and AAA (AAAF → AAAH)
Hypothesis: this is unstable and will evolve

- It’s too complicated (but, that has not fazed 3GPP yet!)
- The ownership model could cause heartburn
- Mobile IP needs a number of new features, but can evolve
- We should do it now to prepare for the next opportunity, and bring a proposal to SA2(?)
- If new spectrum comes online, the whole game may change yet again
  - Recent example: “white space” access to Internet?
What’s next?

- Guaranteed – continued growth of coverage, revenue, access, and social impact
- For sure – continued growth of infrastructure capacity
- For sure – more amazing applications, interactivity
- Extremely likely – major evolution of IP addressability
- Very likely – increasing demand for uplink capacity
- Likely – smaller cell sizes, to increase frequency reuse
- Maybe – more emphasis on user access convenience
- Maybe – smoother handovers, smooth IPv6 transition
- Up to you – improvements in wireless engineering
Operation of SIPNAT: request phase...

- Note: DNS Query does not have source address of host
Operation of SIPNAT: flow completion

IPv4 Internet

BIND_TIMEOUT not yet expired
Packet arrival at NAT_addr4 from v4-internet
When packet arrives, resets timeout, adds source_v4
Flow is then “ESTABLISHED” with all four addresses and ports
Is it really like flow management?

- Incoming $< v4dev, \text{sport}, \text{NATaddr}, dport, \text{TOS} > \rightarrow < v4\text{mapped}, \text{sport}, v6\text{dev}, dport, \text{TOS} >$

- Deep-packet inspection can determine which ALG to use

- Have to search overlapping flow records per v4addr
  - Determine maximum degree of overlap?
  - This is what provides scalability for the solution

Ans: “yes” – and so can use existing sophisticated flow management hardware
The system can fail if Src S tries to access too many destinations

- At each IPv4 address of the NAT, a source IP address (and, possibly, source port) identifies the flow

- Can have one flow per source per NATv4 address (+port), if lucky
The system will fail if there are too many new flow requests (i.e., DNS requests) at about the same time

- Have to keep the request “pending” until a packet arrives to provide the exact source IP address
- Thus, each flow request temporarily (WAIT_TIME) consumes a NATv4 interface address
- Since the DNS Request does not have the source IP address, the allocated flow will go to the source of the first packet to arrive that is not already deliverable
- May need also to keep “pending” address open just a little longer to mitigate DoS
LTE Architecture needs changes to enable an external HA