Mobile IPv6 and Seamless Mobility

Nokia Research Center

Mountain View, CA USA

Charles E. Perkins

http://people.nokia.net/charliep

Charles.Perkins@nokia.com

NOKIA

Outline of Presentation

- Mobile IP overview
- Recent results from Mobile IPv6
- Context Transfer and Seamless Handover
- Challenges for the future

NOKIA

Why Mobile IP?

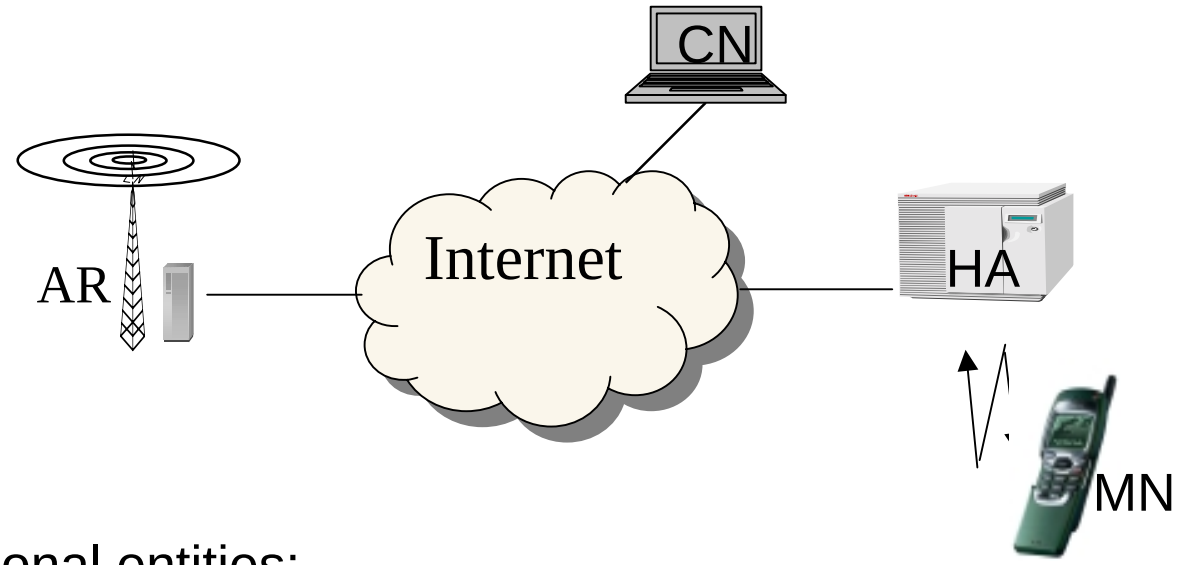
- Both ends of a TCP session (connection) need to keep the same IP address for the life of the session.
  - This is the *home address*, used for end-to-end communication
- IP needs to change the IP address when a network node moves to a new place in the network.
  - This is the *care-of address*, used for routing

Mobile IP considers the mobility problem as a *routing* problem

- managing a *binding* – that is, a dynamic tunnel between a care-of address and a home address
- *Of course*, there is a lot more to it than that!

NOKIA

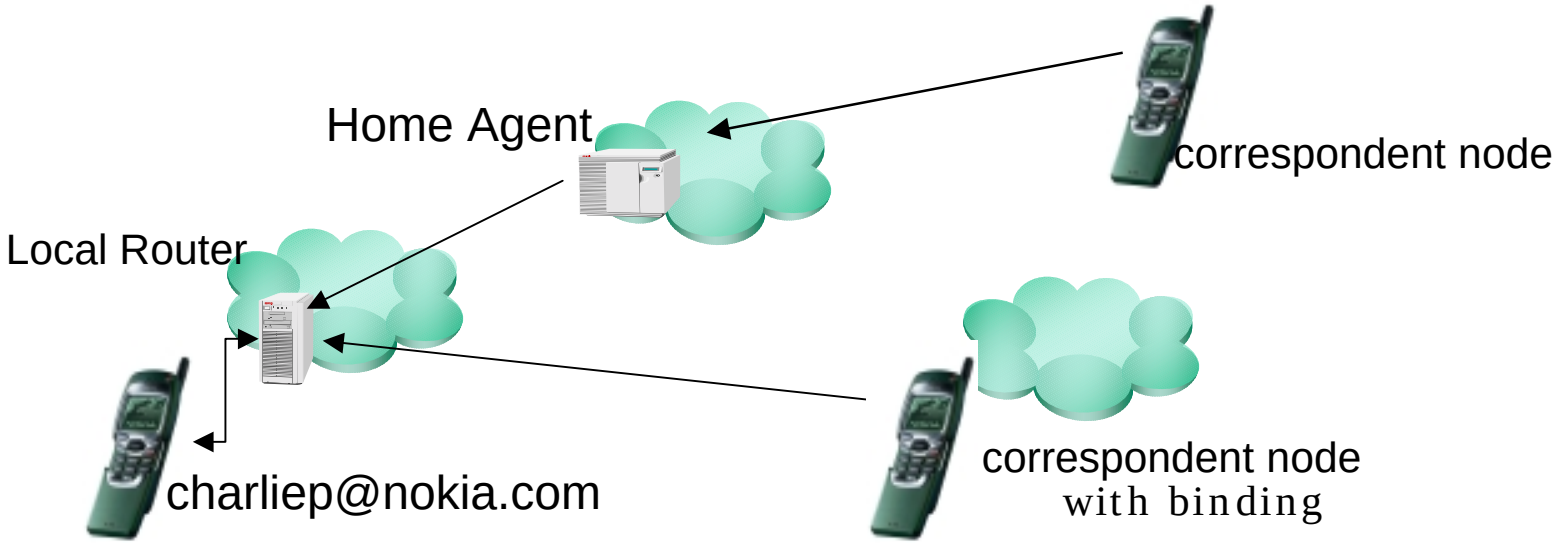
Overview of Mobile IP



- Functional entities:
  - Mobile Node (MN) (shown on Home Network)
  - Home Agent (HA)
- Other entities
  - Access Router (AR)
  - Correspondent Node (CN)

NOKIA

Mobile IPv6 protocol overview



- Routing Prefix from local Router Advertisement
- Address autoconfiguration → care-of address
- Binding Updates → home agent & correspondent nodes
  - (home address, care-of address, binding lifetime)
- *Seamless Roaming*: Mobile Node appears "*always on*" home network

Features of Basic Mobile IPv6

- Scalable approach to transparent mobility management
- Applications really can continue to work without modification
- Performance is quite acceptable, and rarely should burden network capacity
- Uses IPv6 features with very little change
  - address autoconfiguration
  - authentication
  - requires no address-space partitioning
  - reduced implementation requirements
- Scalable approach to establishing Binding Security Associations
- Network renumbering in home domain or foreign domain without restarting mobile device
- Home Agent discovery

NOKIA

Message Types

- Binding Cache Maintenance
  - Binding Update
  - Binding Acknowledgement
  - Binding Request
- Home Address Option
- Return Routability Tests
  - Home Address Test Initiate
  - Care-of Address Test Initiate
  - Home Address Test
  - Care-of Address Test
- Renumbering Messages
  - Mobile Prefix Solicitation
  - Mobile Prefix Advertisement
- Home Agent Discovery

NOKIA

Route Optimization

- Most Internet devices will be mobile, so we should design for that case for the health of the future Internet
- Binding Update *SHOULD* be part of every IPv6 node implementation, according to IETF specification
- Reduces network load by ~50%
  - (depending on your favorite traffic model)
- Route Optimization could *double* Internet performance
  - reduced latency
  - better bandwidth utilization
  - reduced vulnerability to network partition
  - eliminate any potential Home Agent bottleneck

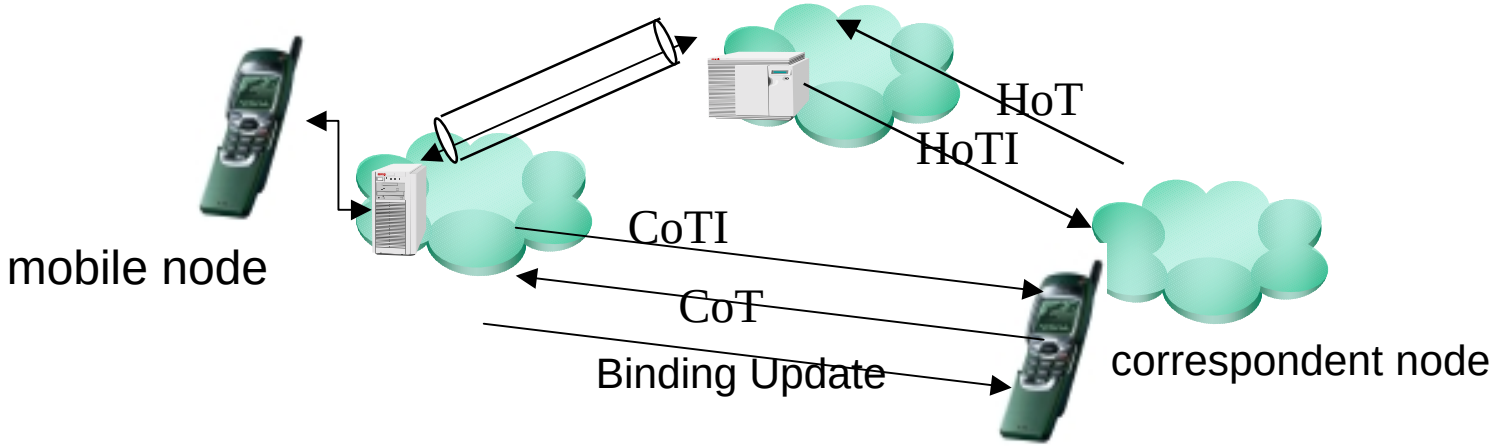
NOKIA

Establishing a Binding Security Association

- BSA is needed specifically for authenticating Binding Updates
- Return Routability (RR) tests rely on routing infrastructure
- Mobile IPv6 RR enables mobile *authentication* not *identification*
  - Latter could require validation via *certificate authority*
  - The correspondent node only has assurance that the Binding Update comes from the same node as before
- Mobile IPv6 solution resists Denial of Service (DoS) attacks
- “First, do no harm”
  - That is, we must be as safe as communications between statically located IPv4 network nodes
  - Only nodes between correspondent node and home network can disrupt traffic

NOKIA

RR Protocol Overview



- Test return routability for home address (HoTI, HoT)
- Test return routability for care-of address (CoTI, CoT)
- HoT and CoT carry nonces to be combined to make K*bu*
- Very few nodes see nonces in both HoT and CoT
- BSA in current specification is short-lived
- Correspondent node keeps no *per-mobile* state during HoT/CoT
- Diffie-Hellman could be another option
  - but it's either expensive or patented

NOKIA

Mobile IPv6 status

- Mobile IPv6 testing event Sept 15-17, 1999
  - Bull, Ericsson, NEC, INRIA
- ETSI bake-offs, 2000 & 2001 – success!
- Connectathon March 2000, 2001, 2002 – success!
- Return Routability for Key Establishment
- Distinguishing between renumbering and movement
  - tunneled router solicitations and advertisements
- Authentication data in option, as well as in AH or ESP
- Fast handover design team has issued Internet Draft
- Chairs and ADs are pushing for re-completion
  - Draft …-19.txt is has returned with Area Director comments
  - We hope draft …-20.txt will be available this week

NOKIA

Relevant IETF Working Groups

- seamoby (Seamless Mobility)
  - Paging (not any more!)
  - Context Transfer
  - “Micro-mobility” – localized binding management
- rohc (Robust Header Compression)
  - Reducing 40/60 bytes of header overhead to 2-3 bytes
  - Profiles developed for IPv4/UDP/RTP
  - Profiles expected for IPv6/UDP/RTP, IPv?/TCP, etc.
  - Destination Option inclusion needs consideration
- aaa (Authentication, Authorization, Accounting)
  - DIAMETER chosen
  - Mobile-IP extension defined for IPv4; IPv6 in works
  - AAAv6 Internet Draft available, uses Neighbor Cache
- pana (Protocol for Carrying Network Authorization)

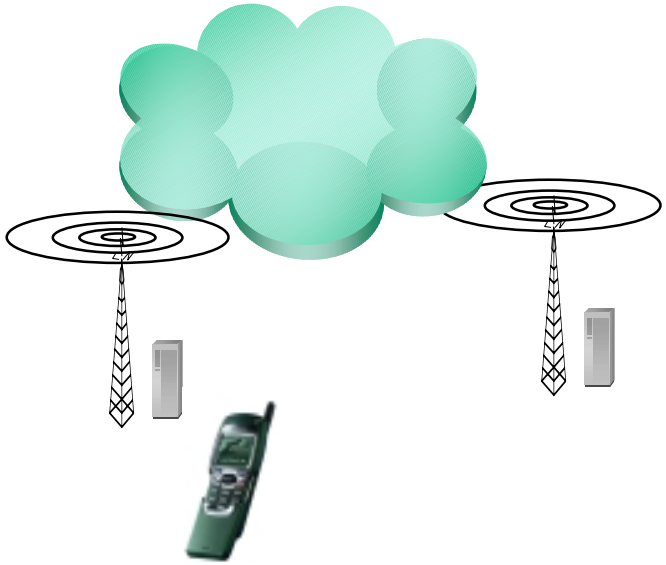
NOKIA

More Relevant IETF working groups

- `manet` (Mobile Ad hoc Networks)
  - Can work in absence of Internet infrastructure
  - Four protocols to be published as Experimental
  - Charter reorganization for future Proposed Standard
  - IRTF group to be formed
- `nemo` (Network Mobility)
  - What happens when a router moves with its subnets?
  - Useful for trains, automobiles, airplanes, Personal Area Networks (PANs)
  - Difficult security issues caused original split from Mobile IP
  - Also questions about how to handle route optimization
- New Mobile IP group?
  - Proposal: split between Mobile IPv4 and Mobile IPv6
  - Or, between “new specification” and “operational details”?

Smooth/Fast/Seamless Handover

- Smooth handover == low loss
- Fast handover == low delay
  - 30 ms?
  - Can router pre-empt Duplicate Address Detection??
- Seamless handover == *smooth* and *fast*



NOKIA

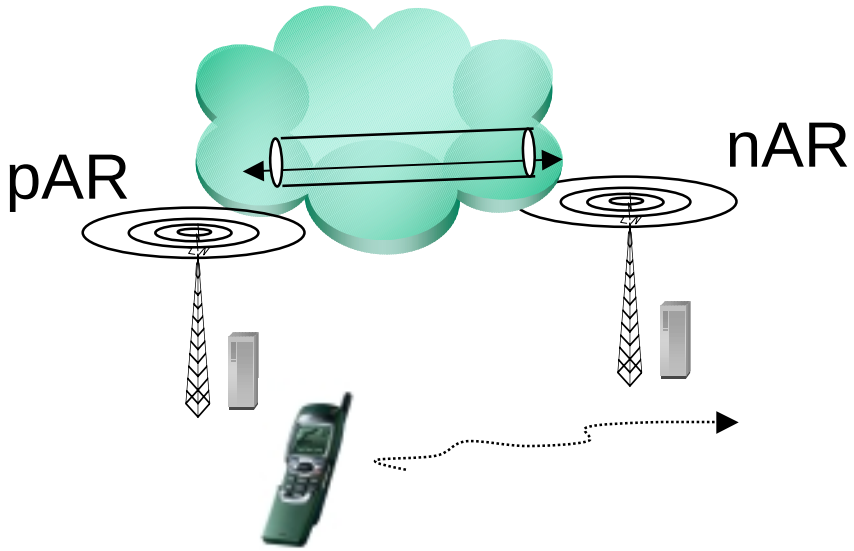
Entities and terminology

- MN – the mobile node
- AR – an access router which is able to operate these protocols
- pAR – the previous access router. Mobile started out here.
- nAR – the new access router. Mobile ends up here.
- Reactive – carried out after the handover has started
- Predictive – carried out before the handover has started
- When does a handover start, and when is it finished?

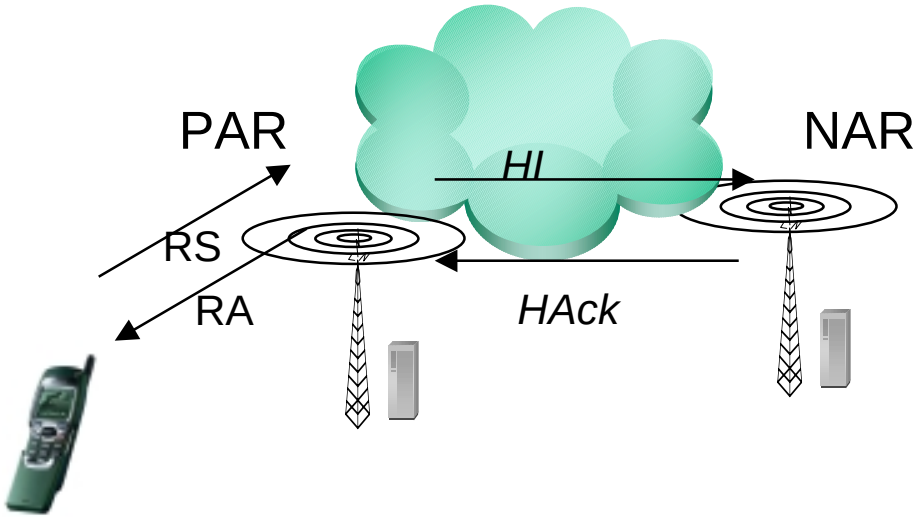
NOKIA

Getting packets to the New Access Router

- nAR needs mobile node's care-of address, MAC address
- Mobile node ← IP address, MAC address of new default router
- pAR needs to establish tunnel to forward incoming packets
- Soon, mobile node needs to send Binding Update to Home Agent



Mobile-controlled handover



One scenario: mobile sends special Router Solicitation (RS), along with NAR's address and candidate care-of address

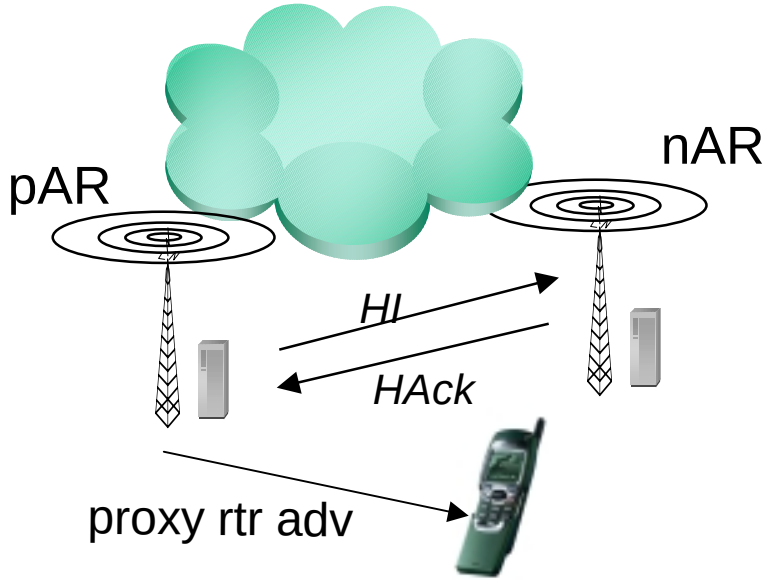
- Previous Access Router → *Proxy* Router Advert. (RA)
- Previous Access Router sends Handover Initiate (HI)
- New Access Router → Handover Acknowledge (HACK)

NOKIA

Handover actions after HI

- NAR checks for availability of candidate care-of address
- NAR sends Hack to PAR
- When PAR receives Hack, tunnel setup between PAR and NAR
  - Packets tunneled to new care-of address if valid
  - Packets tunneled to old care-of address otherwise
- NAR awaits mobile node
- Mobile node supplies *Fast Neighbor Advertisement* upon arrival
- NAR uses this to *finalize* the handover
- Fast Neighbor Advertisement requires authentication to avoid any possible disruption from masquerading nodes
  - Mobile node must prove that IT is the one coming from PAR

Network Controlled Handover



- Previous access router (pAR) sends Proxy Router Advertisement on behalf of the new access router (nAR)
  - Contains prefix and lifetime information, etc., as before
  - Signals mobile node that it's time to move!
- pAR and nAR exchange HI and Hack, as before
- Mobile node finalizes (securely) handover data at nAR

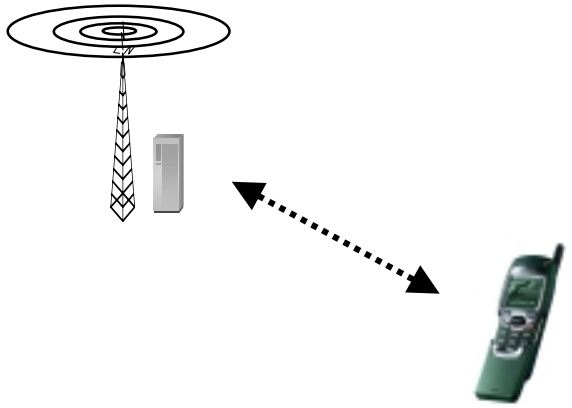
Updating the Routing is NOT enough!

- Care-of Address, MAC address, etc. handled via *fast handover*
- State (for various features) established to minimize overhead
  - Mainly, to conserve wireless capacity (it's *expensive*!)
- Header Compression feature
- Buffered Data
- Quality of Service requirements, and perhaps accounting data
- Security Association with access router, authorization tokens
- Application context transfer also needed, but not appropriate for resolution within mobile-ip, aaa, rohc, or seamoby working groups

NOKIA

Header Compression Context

- Access Router and mobile node maintain records to represent the expected content of protocol headers
- Header fields that have the expected values do NOT need to be transmitted, since they can be inferred
- Access Router compressor state has to match the mobile node's decompressor state
- Mobile node's compressor state has to match the access router's decompressor state
- Has to be *ROBUST* against errors!
- Depends on the protocol(s)!



NOKIA

Buffered Data

- Specifically designed to help smooth handovers (as opposed to header compression context, for instance)
- Data is constantly buffered (does NOT introduce delay!), but the buffered data is never used except after handover
- Experiments have shown that, for frequent-enough beaconing, buffering helps to achieve smooth handovers for VoIP
- One or two packets are enough
- Timeliness matters: delivering stale voice packets is a mistake
- Alternate solution: *bicasting* – but this introduces ambiguity and is unfriendly to solutions with mobile routers

NOKIA

Security Associations

- Presumption: mobile node has already established a security association with previous access router (PAR)
- This can be done by way of AAA, or proprietary methods, but the mechanism by which the SA is established does not matter here
- Usually, it takes a long time to initiate and establish a security association
- If PAR and NAR themselves share a security association, then NAR can authorize the mobile node to continue access to the same level of service.
- For seamless handover with secure access, timeliness is crucial.
- Mobile node must present believable credentials
- New security association should be *derived* from the previous SA

Context Transfer Protocol

- What are the signaling messages?
  - HI and Hack (ICMP messages) from Mobile IPv6 fast handover design team are good candidates
  - What about scenarios besides smooth handovers?
  - In this case, context features requested/provided as options
- Could use another ICMP message, or SCTP, or Dest Opt, or ??
- CTSR – Context Transfer Start Request. Sent by Mobile Node or nAR (for *reactive* transfers)
- CTIN-Ack – Context Transfer Initiate Acknowledge. Sent by nAR to pAR. Indicates that nAR is willing to receive contexts.
- CTD – Context Transfer Data. Transfers the feature contexts. Sent by pAR to nAR

Transport considerations

- Protecting the network vs. fast performance
  - But what is being protected against?
  - These are not application data streams!
  - Do we need to analyze transport protocols more?
- TCP: good for reliability, bad for timely transfer
- Suboptions to *Fast Handover*: but should work independently
- UDP: good for timely transfer, complicated for reliability, and in other scenarios is known to be unfriendly to the core Internet
- SCTP: Probably better than TCP for *known neighbors*
- ICMP: Good definitionally, but seems to be deprecated
- IPv6 extension headers: but this should also work for IPv4
- ??? (DCCP?)
- Likely: multiple possibilities depending on use scenario

Generic Profile types (proposed!)

- Most kinds of context features will have a number of variants, each with different profile types (e.g., QoS, or [rohc])
- The layout of the context features could be identified according to a *profile type*
- Profile types would be registered with IANA, and each specification would lay out fields for use by the context transfer protocol
- Default values, if specified, are already indicated by profile type and so do not need to be included
- Presence vector indicates which fields are present, and thus indicated values which are NOT default values

Open Issues

- Choice of transport
- Candidate Access Router Discovery
  - For mobile-controlled, how does the mobile node know?
  - For network controlled, how does pAR know?
- Security model
- Message types and semantics
- Intra-domain / inter-domain operation
- Failure model needs to be specified.
- Handling multiple contexts when their reliability and/or performance requirements are different (*bundling*)

NOKIA

Challenges for Mobile IPv6

- Achieving Proposed Standard (esp. re: HAO)
- Legacy equipment and smooth transition (esp. with HLR)
- Walled Gardens (mobile access to all Internet services desired)
- Application adaptations to mobility (new APIs needed)
- Security protocol development, deployment (key distribution)
- Maintaining same level of quality as in current cellular (help from [seamoby])
- Enabling ad hoc networking (what is the business model?)
- Governmental considerations (Location)
- Harmonizing 3GPP and 3GPP2
- Video?
- QoS?
- Social awareness to restore the end-to-end application model (vs., e.g., NATs)

NOKIA

Summary and Conclusions

- Mobile IPv6 offers *scalable*, *secure*, and *high-performance* mobility management
- Mobile IPv6 is working, and new issues are resolved
  - There's lots of interoperability experience, but new draft is different
  - Implementation is natural under IPv6 and IPsec
- Fast Handover has been developed for improved handover performance (goal: smooth voice handovers – and, *video*!)
- Context Transfer to preserve link contexts to avoid re-establishment (gaining further performance improvements)

NOKIA