Recent Activities in Mobile IPv6
May 31, 2001

Nokia Research Center

Mountain View, CA USA

Charles E. Perkins

http://people.nokia.net/~charliep

charliep@iprg.nokia.com

NOKIA

Earth with 1 Billion Mobile devices

- One billion is a large number, but we will be there next year
- It's never been done before!
- In the beginning, most of them will not be Internet enabled, but they will come online rapidly
- If IPv4 can do it at all, it will be at a tremendous (unimaginable, even) cost in complexity
- Only IPv6 offers enough addresses; the Internet is still young!
- IPv6 also offers the features needed for mobile networking
- Only Mobile IPv6 takes advantage of the IPv6 features to offer seamless roaming.
- Network-layer roaming also enables significant cost reductions and improved deployability

NOKIA

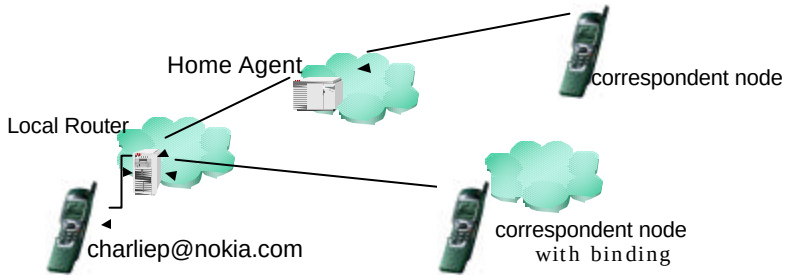
Why Mobile IP?

- 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

Mobile IPv6 protocol overview



- Advertisement from local router contains routing prefix
- *Seamless Roaming*: mobile node always uses home address
- Address autoconfiguration for care-of address
- Binding Updates sent to home agent & correspondent nodes
  - (home address, care-of address, binding lifetime)
- Mobile Node "*always on*" by way of home agent

NOKIA

Mobile IPv6 Design Points

- Enough Addresses
- Enough Security
- Address Autoconfiguration
- Route Optimization
- Destination Options
- also, reduced Soft-State, etc., not covered here

NOKIA

Enough Addresses

- 340 undecillion addresses
  - (340,282,366,920,938,463,463,374,607,431,768,211,456) total!
- Needed for billions of IP-addressable wireless handsets over the next 20 years
- IPv4 address space crunch driving current deployment of NAT
  - But, multi-level NAT unknown/unavailable
  - Besides, NAT not useful for *always on* operation
- Even more IP addresses needed for embedded wireless!
- Especially interesting for China now
  - 8 million IPv4 addresses and 70+ million handsets

NOKIA

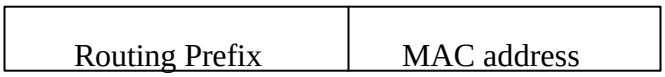
Enough Security (almost)

- Authentication Header *mandatory to implement*
- Encapsulating Security Payload *mandatory to implement*
- Needed for Binding Update
  - Remote Redirect problem
- Key distribution still poorly understood
  - PKI?
  - AAAv6 w/ symmetric key?
- Can your m-commerce server manage 10 million security associations?
- Can your light bulb manage 10 security associations?
- *"First, do no harm"*

NOKIA

Address Autoconfiguration

- Stateless Address Autoconfiguration
- First, use routing prefix == FE80::0/64 for *link-local* address
- Then, construct Link-Local Address → Global Address by changing link-local prefix to advertised routing prefix



- A new *care-of address* on every link
- Stateful Autoconfiguration (DHCPv6)
- Movement Detection
  - by monitoring advertisement of new prefix
  - by hints from physical layer and/or lower-level protocol
  - by monitoring TCP acknowledgements, etc.

NOKIA

Destination Options used by Mobile IPv6

- Destination Options *much better* than IPv4 options
- Binding Updates sent in data packets to Correspondent Nodes
  - allows optimal routing with minimal packet overhead
  - *SHOULD* be supported by *all* IPv6 network nodes
- Binding Update also sent (typically with no data) to Home Agent
  - replaces IPv4 Registration Request messages
- Home Address option
  - better interaction with *ingress filtering*
  - *MUST* be supported by *all* IPv6 network nodes
- Binding Acknowledgement Destination Option
  - replaces Registration Reply

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-wide performance
  - reduced latency
  - better bandwidth utilization
  - reduced vulnerability to network partition
  - eliminate any potential Home Agent bottleneck

NOKIA

Mobile IPv6 status

- Mobile IPv6 testing event Sept 15-17, 1999
  - Bull, Ericsson, NEC, INRIA
- ETSI bake-off October 2-6, 2000
- Connectathon March 2000 – success!
- New Requirement for Key Establishment (excitement!)
- Distinguishing between renumbering and movement
  - tunneled router solicitations and advertisements
- Authentication data in options, no longer in AH
- Fast handover design team has issued Internet Draft
- Connectathon March 2001 – success!
- Projected (re-!)completion by July IETF

NOKIA

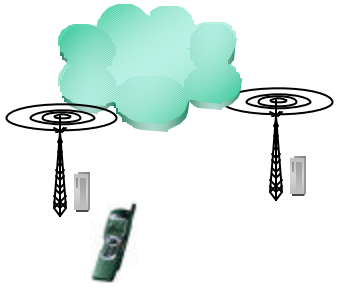
Other Relevant Working Groups

- Seamless Mobility [seamoby]
  - Paging
  - Context Transfer
  - "Micro-mobility" – localized binding management
- Robust Header Compression [rohc]
  - 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.
  - Option inclusion needs consideration
- Authentication, Authorization, and Accounting [aaa]
  - DIAMETER chosen
  - Mobile-ip extension defined for IPv4; IPv6 in works
  - AAAv6 Internet Draft available, uses Neighbor Cache

NOKIA

Smooth/Fast/Seamless Handover

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



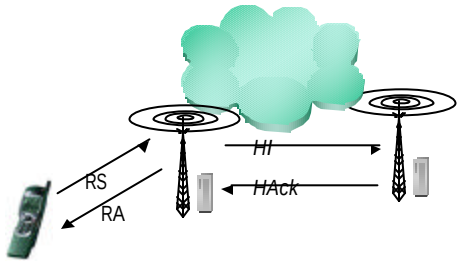
NOKIA

Context Features for Transfer

- Feature state established to minimize connection overhead
  - Mainly, to conserve bandwidth
- Care-of Address, MAC address, etc.
- Header Compression
- Buffered Data
- Quality of Service
- Security Associations
- Application context transfer also needed, but not appropriate for resolution within mobile-ip, aaa, rohc, or seamoby working groups

NOKIA

Mobile-controlled seamless handover

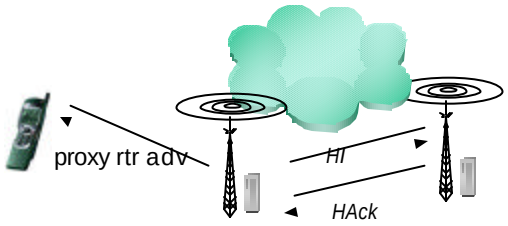


One scenario: mobile sends special Router Solicitation (RS)

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

NOKIA

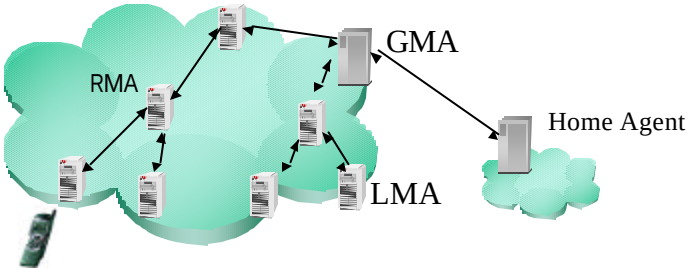
Network Controlled Handover



- Previous access router sends Proxy Router Advertisement on behalf of the new access router – contains prefix and lifetime information, etc.
- Previous access router sends *Handover Initiate* message to new access router
- Mobile node *MAY* finalize context transfer at new access router

NOKIA

Hierarchical Mobility Agents



Problem: how to reduce latency due to signaling to Home Agent

Solution: Localize signaling to Visited Domain

Method: Regional Registration/Regional Binding Update

Often, only one level of hierarchy is being considered

NOKIA

Regional Registration for IPv6

- Uses an *Anycast Address* for all regional routers
- Allows arbitrary hierarchical topology without disclosing details to mobile nodes roaming from other domains
- Specifies an optimal method for forwarding
- Compatible with smooth/fast handovers
- Enables quick yet optimal routing through the visited domain
- Compatible with normal security for Binding Updates
- Can benefit from context transfer for security parameters
  - Using security association between leaf routers

NOKIA

Cellular architectures

- Involve SS7 over "control plane" to set up virtual circuits for "user plane" traffic
- Are highly optimized for voice traffic (low delay, guaranteed bandwidth), not data
- Tend toward "intelligent network" philosophy which for IP is a misplaced locus of control.
- We have a tremendous legacy that needs a lot of attention

NOKIA

IPv6 status for cellular telephony

- Has been mandated for 3GPP
- MWIF recommendation for IPv6
- 3GPP2 study group favorable towards IPv6
- Seems difficult to make a phone call to a handset behind a NAT (not impossible, just expensive and cumbersome and protocol-rich)
- IETF design team designated for fast/smooth/seamless handover
- AAA adaptation layer for HLR(HSS) under consideration
- Smooth evolution from GPRS envisioned
- ROHC working group considering header compression
- Mobile IPv6 *should* be mandated after Proposed Standard

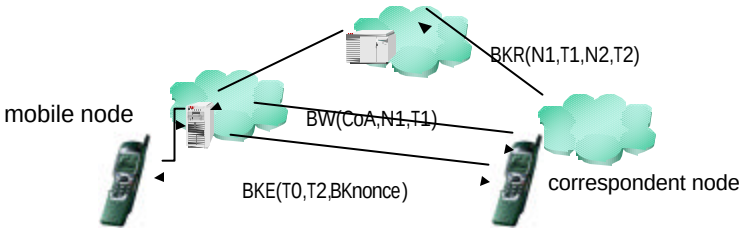
NOKIA

Binding Authentication Key Establishment

- "First, do no harm"
  - That is, we must be as safe as communications between statically located IPv4 network nodes
- A security association is needed specifically for validating Binding Updates
  - No longer relying on AH, as per IESG stipulation
- BAKE provides *authorization* but not *authentication*
  - Latter would require validation via *certificate authority*
  - Means that the receiver only has assurance that the Binding Update comes from the same node as started with
- BAKE offers resistance against Denial of Service (DoS) attack
- Only nodes between correspondent node and home network can disrupt traffic

NOKIA

Protocol Overview



- Correspondent node does not have to save T1 or T2
- BKnonce and N2 are combined to create the binding key
- Very few nodes see both BKnonce and N2
- Node that sends T0 has to be the same one that sent T1.
- Diffie-Hellman is another option
  - but it's either expensive or patented
- Authentication by mobile node also possible, then CN

NOKIA

AAA and Cellular Telephony

- Terminology
- Protocol overview for Mobile IPv4 (current specification)
  - IPv6 mobility will be managed similarly
- Key Distribution
- Scalability and Performance
- IETF Status

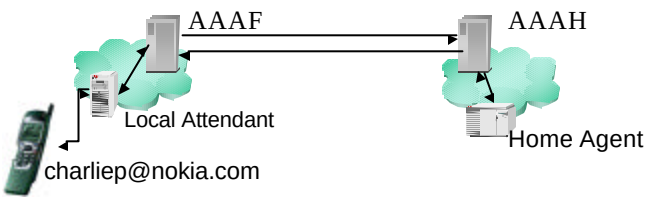
NOKIA

Terminology

- Authentication – verifying a node's identity
- Authorization – for access to resources
  - according to authentication and policy
- Accounting – measuring utilization
- For IPv4, Network Access Identifier (NAI) – user@realm
  - For IPv6, network address may be sufficient & simpler
- Challenge – replay protection from local attendant
- AAAF for foreign domain
- AAAH for home domain

NOKIA

AAA & Mobile IP protocol overview



- Advertisement from local attendant (e.g., router)
- Connectivity request from Mobile Node
- Local Attendant asks AAAF for help
- AAAF parses ID (*realm* within MN-NAI) to contact AAAH
- AAAH authenticates & authorizes, starts accounting
- AAAH, optionally, allocates a home address
- AAAH contacts & initializes Home Agent

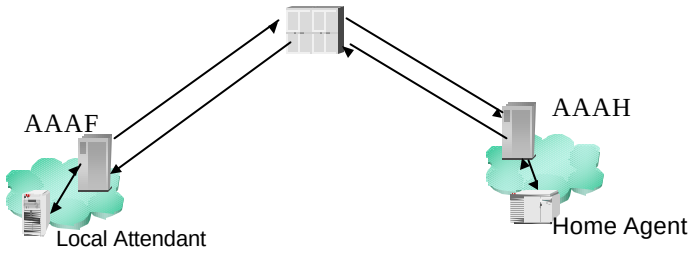
NOKIA

Key Distribution

- New security model
  - just *one security association* (SA): mobile node ←→ AAAH
- Mobile IP needs an association between HA ←→ mobile node
- 3GPP2, others, want also:
  - local attendant ←→ mobile node
  - visited mobility agent ←→ home agent
- AAAH can dynamically allocate all three of these keys
  - passed back along with authorization and Binding Acknowledgement

NOKIA

Brokers



- Needed when there are 1000's of domains
- IPv6 address or NAI are perfect to enable this
- AAAF decides whether to use broker
  - may prefer bilateral arrangement
- iPASS, GRIC
- *redirect* mode also allowable

NOKIA

Scalability and Performance

- Single Internet Traversal
- Brokers
- Eliminate all unnecessary AAA interaction
- Handoff between local attendants (routers)
  - can use existing keys from previous router
- Regional Registration helps also
  - HA can use single *regional care-of address* per domain

NOKIA

Mobile IP/AAA Status

- AAA working group has been formed
- Working from experience with RADIUS
- Mobile IP (v4) AAA requirements draft
  - RFC 2989
  - Several 3G requirements documents online
- DIAMETER has been selected for IPv4, and IPv6
- Interoperability event suggested protocol improvements
- Mobile IPv4/AAA extensions draft revised
- AAAv6 Internet Draft(s) submitted
  - stateless and stateful variations
  - access control needed at *neighbor cache*
- Mobile IPv6/AAA extensions draft prepared
- AAA working group interim meeting may push to Last Call

NOKIA

Summary and Conclusions

- Future Internet is largely wireless/mobile
- IPv6 addressability needed for billions of wireless devices
- Mobile IPv6 is better and more efficient than Mobile IPv4
- Autoconfiguration is suitable for the mobile Internet
- Security is a key component for success
- Seamless handover needed for VoIPv6
- AAA has a big role to play for cellular rollout

We expect Mobile IPv6 (with AAA & Seamless handover) to be the future 3G++ converged wired/wireless, voice/data network

NOKIA

Other features (for IPv6 or seamless h/o)

- Integration of Regional Registration with GPRS
- Header Compression
- Buffer Management
- UDP Lite
- AAA ←→ HLR adaptation layer
- Challenge generation (optionally from HLR?)
- Privacy considerations
- QoS handover
- Smooth handover mechanisms for keys

NOKIA