Slide 1

Scalability and Security with Mobile IPv6

Nokia Research Center
Mountain View, CA USA
Charles E. Perkins
http://people.nokia.net/charliep
charliep@iprg.nokia.com

NOKIA

Slide 2

Outline of Presentation

- Mobile IP in General
- What's great for mobility about IPv6?
- How Mobile IPv6 works
- Recent results from Mobile IPv6
- Challenges for the future

NOKIA

Slide 3

Earth with 2 Billion Mobile devices

- One billion is a large number; we'll be there this year or next
- 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

Slide 4

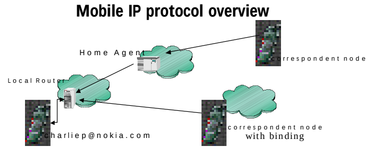
Why Mobile IP?

- 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!

Slide 5

Mobile IP protocol overview



- 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)

Slide 6

IPv6 features used for Mobile IPv6

- Enough Addresses
- Enough Security (we thought)
- Address Autoconfiguration for getting care-of addresses
- Destination Options (and, now, Mobility) extension headers
- also, reduced Soft-State, etc., not covered here

Slide 7

Features added for Mobile IPv6

- Binding Cache management in new Mobility Header
  - (a lot like the existing Destination Options header)
- Route optimization using new Route Header
  - But, it's almost exactly like the existing one
- New ICMP messages
  - For Home Agent discovery
- New Router Advertisement extension
  - For renumbering
  - Binding Request message type

NOKIA

Slide 8

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 Asia now
  - China has 22 million IPv4 addresses and 130+ million handsets

NOKIA

Slide 9

Security issues: (*almost sufficient*)

- 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

Slide 10

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

Slide 11

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

Slide 12

Ingress Filtering and Home Address Option

- Ingress filtering border routers enforce topologically correct source IP address fields
- End-to-end applications want to deal with home address exclusively
- Topological correctness requires the care-of address to be in the Source IP address field
- IP traditionally passes the Source IP address field up to higher level protocol (e.g., TCP)
- Home Address Option changes this behavior, so that the option data is passed instead (i.e., the *home address*!)
- Result: topological correctness AND stable identification for higher-level protocols

NOKIA

Slide 13

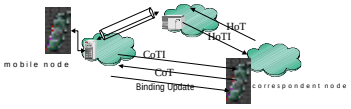
Establishing a Binding Security Association

- 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

Slide 14

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

Slide 15

Home Address Test Initiate (HoTI)

- Mobility Header message type 1
- Contains 32-bit mobile cookie
- Can contain a Unique Identifier option
- Cannot contain a Home Address destination option
- Source IP address is the mobile node's claimed Home Address

NOKIA

Slide 16

Care-of Address Test Initiate (CoTI)

- Mobility Header message type 2
- Contains (possibly different) 32-bit mobile cookie
- Can contain a Unique Identifier option
- Source IP address is the mobile node's claimed Care-of Address
- HoTI/CoTI expected to be sent at about the same time, but after sending the Binding Update to the Home Agent

NOKIA

Slide 17

Home Address Test (HoT) message

	Reserved (16 bits)
Nonce Index (16 bits)	Reserved (16 bits)
Mobile Cookie (32 bits)	
Home Cookie (128 bits)	

- Nonce Index to be used in Nonce Indices option to Binding Update
- Mobile Cookie copied from Home Address Test Initiate message
- Home Cookie used as input for creating security association
- Type 3 message using Mobility Header

NOKIA

Slide 18

Care-of Address Test (CoT) message

- Nonce Index also to be used in Nonce Indices option to Binding Update
- Mobile Cookie copied from Care-of Address Test Initiate message
- Care-of Cookie also used as input for creating security association
- Type 4 message using Mobility Header
- When mobile node receives HoT and CoT, it can then send the Binding Update to the correspondent node

NOKIA

Slide 19

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 ...-17.txt issued last week, may go to Last Call
  - Draft ...-18.txt likely to be needed early June

NOKIA

Slide 20

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

Slide 21

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
- Binding Update now has a lightweight key establishment protocol
  - *"First, do no harm"*

NOKIA