Mobile IP in Wireless Cellular Systems

from several perspectives

Charles E. Perkins
Nokia Research Center

AAA and Cellular Telephony

- Terminology
- Protocol overview from Mobile IPv4
- Key Distribution
- Scalability and Performance
- IETF Status

Terminology

- Authentication – verifying a node's identity
- Authorization – for access to resources
  - according to authentication and policy
- Accounting – measuring utilization
- Network Access Identifier (NAI) – user@realm
- Challenge – replay protection from foreign agent
- AAAF for foreign domain
- AAAH for home domain

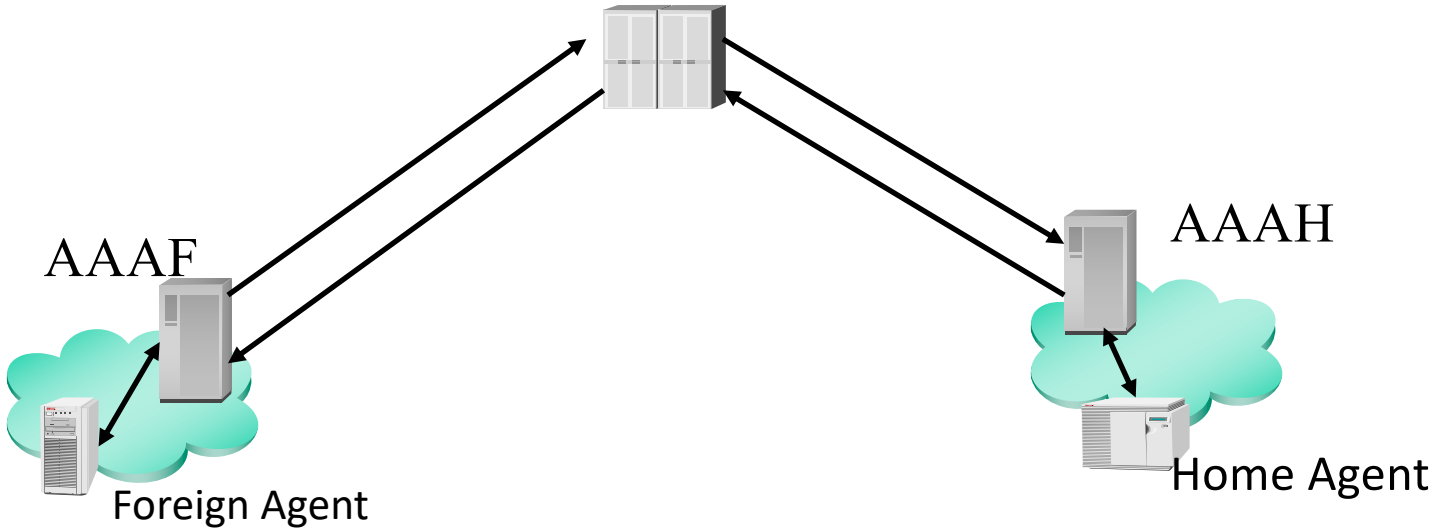
AAA & Mobile IPv4 protocol overview

- Advertisement from Foreign Agent
- Registration Request w/MN-NAI from Mobile Node
- Foreign Agent asks AAAF for help
- AAAF looks at realm to contact AAAH
- AAAH authenticates & authorizes, starts accounting
- AAAH, optionally, allocates a home address
- AAAH contacts Home Agent

Key Distribution

- New security model
  - mobile node ←→ AAAH
- Association needed HA ←→ mobile node
- TR45.6, others, want also:
  - foreign agent ←→ mobile node
  - foreign agent ←→ home agent
- AAAH allocates three keys for this

Brokers



- Needed when there are 1000's of domains
- NAI is perfect to enable this
- AAAF decides whether to use per realm
  - may prefer bilateral arrangement
- iPASS, GRIC

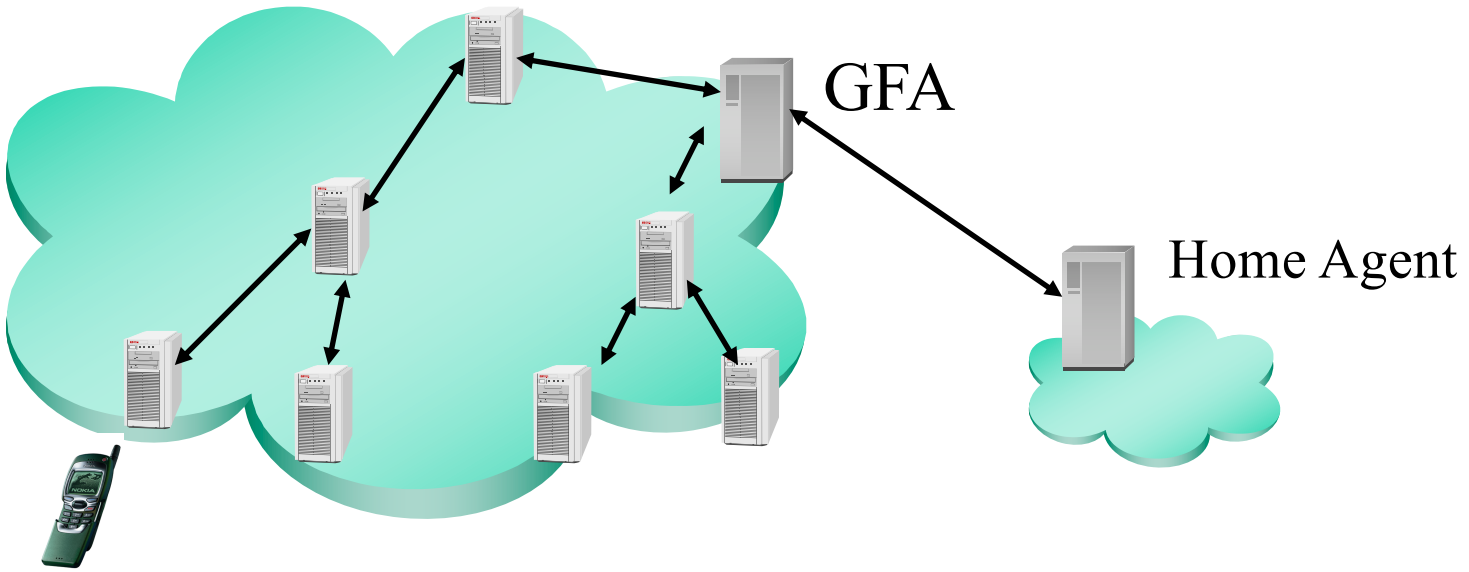
Scalability and Performance

- Single Internet Traversal
- Brokers
- Eliminate all unnecessary AAA interaction
- Handoff between foreign agents
  - can use keys from previous foreign agent
- Regional Registration
- Can use single *care-of address* per domain

Mobile IPv4/AAA Status

- AAA working group has been formed
- Mobile IP (v4) AAA requirements draft
  - Last Call possible by Adelaide
- Several 3G requirements documents online
- Mobile IP/AAA extensions draft

Hierarchical Foreign Agents



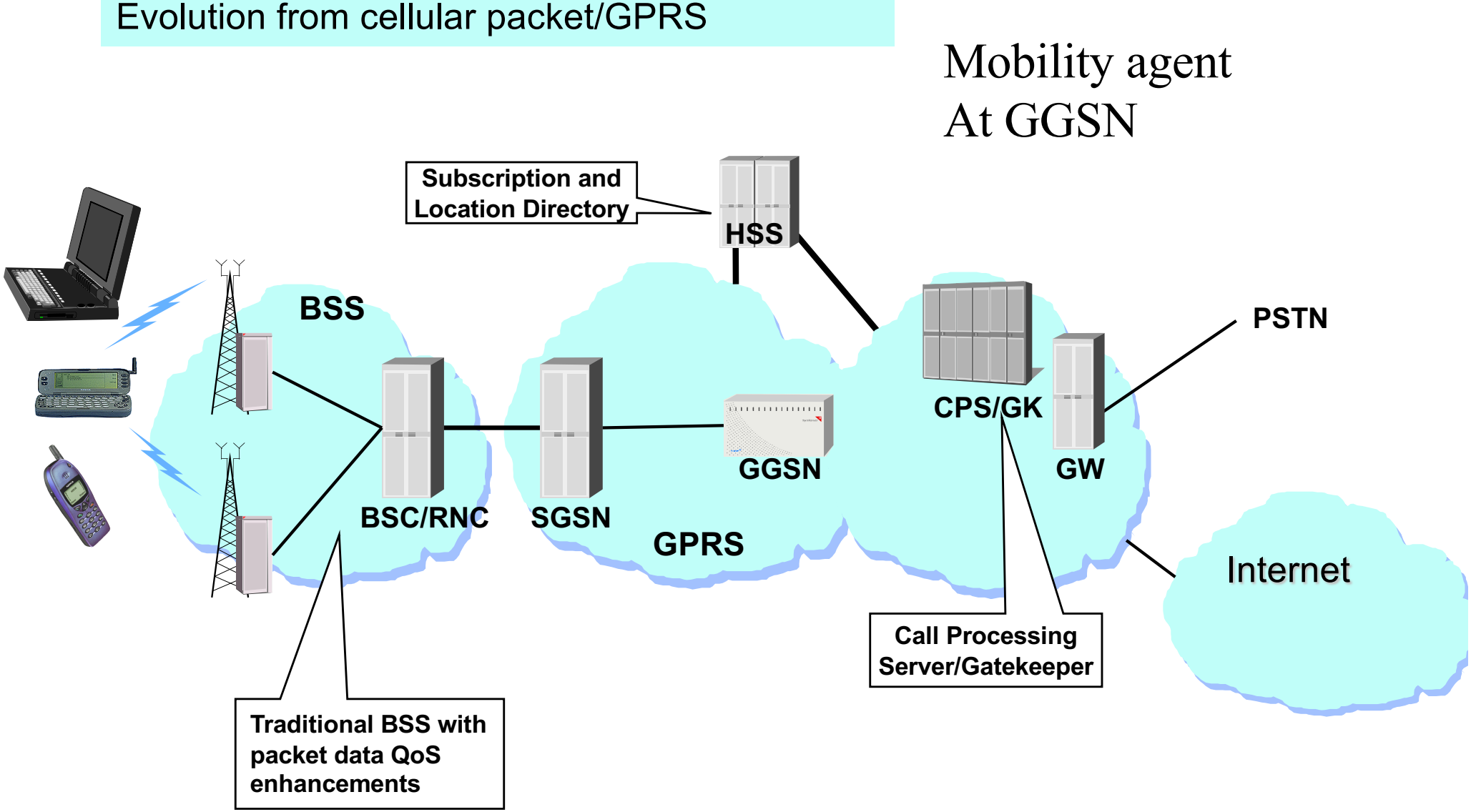
Home Agent stores GFA address as the Care-of Address

Mobile Node registers only once with Home Agent

Usually, only one level of hierarchy is being considered

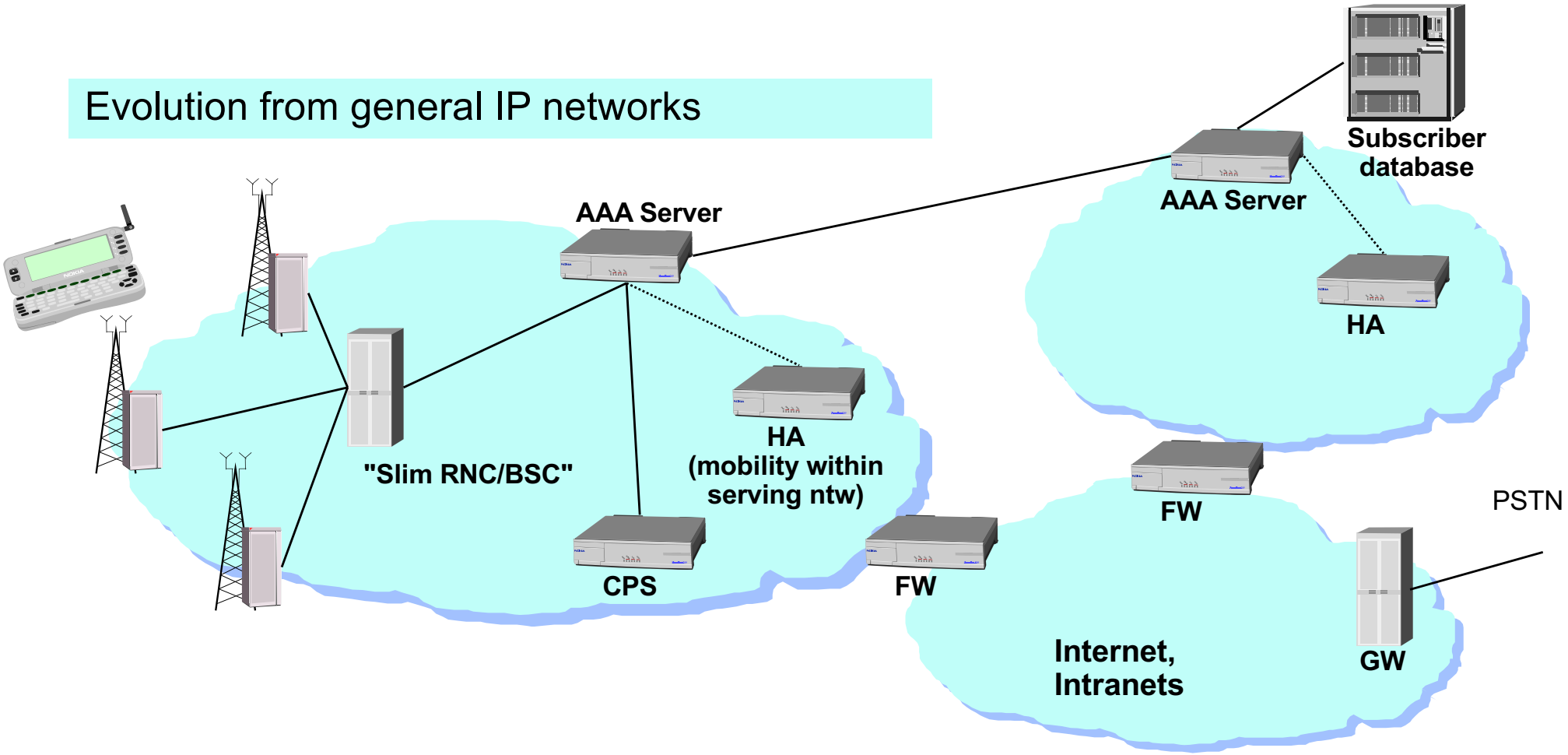
3GPP with GPRS

Evolution from cellular packet/GPRS

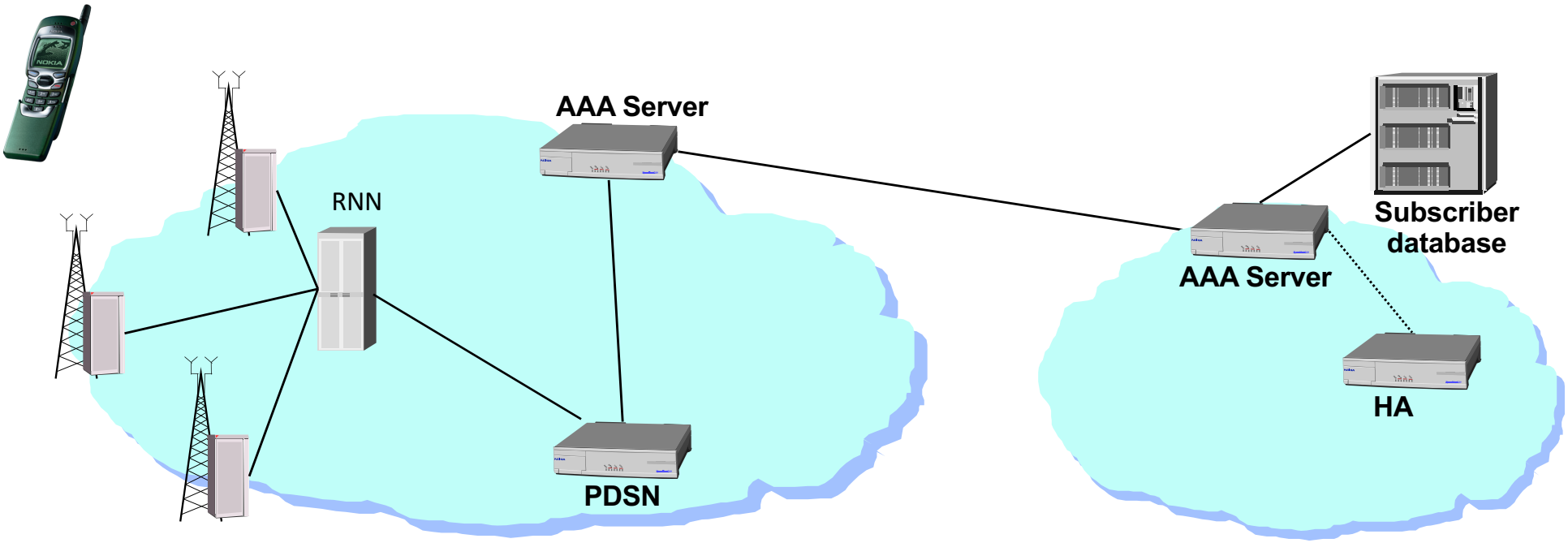


One (of many) “ALL-IP” visions

Evolution from general IP networks



CDMA2000 3G micromobility



CDMA2000 3G *micromobility*

- Terminate physical layer distant from “FA”
- Protected, private n/w between FA and MN
- PDSN (Packet Data Serving Node) ~ GFA
- RNN (Radio Network Node) ~ LFA
- RNN manages the physical layer connection to the mobile node

CDMA2000 3G Requirements

- GRE encapsulation (but will it survive?)
- Reverse Tunneling (RFC 2344)
- Registration Update
- Registration Acknowledge
- Session-specific registration extension
  - contains MN-ID, type, MN Connection-ID
  - contains Key field for GRE

CDMA2000 Registration Update

- Used for handovers to new RNN
- Acknowledgement required
  - allows PDSN/old RNN to reclaim resources
- New authentication extension required
- Home address ← 0
- Home agent ← PDSN
- Care-of address ← RNN

IMT-2000/UMTS/EDGE reqt's

- Independent of access technology
  - so should work for non-GSM also
- Interoperation with existing cellular
- Privacy/encryption (using IPsec)
- QoS for Voice/IP and videoconferencing
  - particular concern during handover
- Fixed/mobile convergence desired

IMT-2000 reqt's, continued

- Charge according to QoS attribute request
- Roaming to diverse access technologies
  - e.g., Vertical IP
- Route optimization
- Identification/authorization based on NAI
- Proxy registration for legacy mobile nodes
- Signaling for firewall traversal

IMT-2000 reqt's, continued

- Reverse tunneling
- Private networks
  - but, still allow access to networks other than the mobile node's home network
- Dynamic home address assignment
- Dynamic home agent assignment
  - even in visited network
  - even when roaming from one visited network to another

Mobile IPv6 Design Points

- Enough Addresses
- Enough Security
- Address Autoconfiguration
- Route Optimization
- Destination Options
- Reduced Soft-State

Enough Addresses

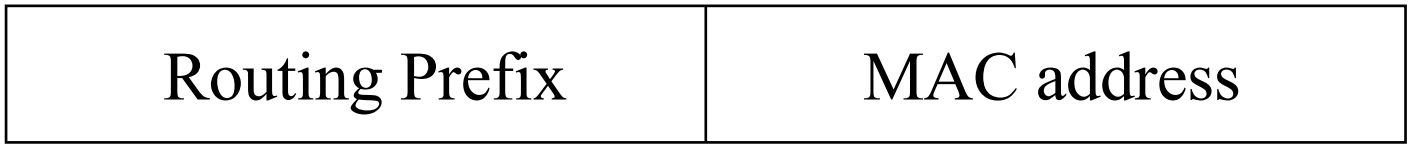
- Billions of IP-addressable wireless handsets
- Address space crunch is already evident
  - recent unfulfilled request to RIPE
- Multi-level NAT unknown/unavailable
- Even more addresses for embedded wireless

Enough Security (almost)

- Authentication Header
- Needed for Binding Update
  - Remote Redirect problem
- Encapsulating Security Payload
- Required from *every* IPv6 node
- Key distribution still poorly understood
  - PKI?
  - AAA?

Address Autoconfiguration

- A new *care-of address* on every link
- Stateless Address Autoconfiguration



- Link-Local Address → Global Address
- Stateful Autoconfiguration (DHCPv6)
- Movement Detection

Destination Options

- Binding Updates without control packets
  - allows optimal routing
  - replaces IPv4 Registration Request messages
- Home Address option
  - better interaction with *ingress filtering*
  - supported by *all* IPv6 network nodes
- Binding Acknowledgement
  - replaces Registration Reply

Route Optimization

- Most Internet devices will be mobile
- Reduces network load by ~50%
  - (depending on your favorite traffic model)
- Route Optimization could double Internet-wide performance levels…
- Binding Update *SHOULD* be part of every IPv6 node implementation

Improved ICMP messages

- IPv4 ICMP returns only 8 payload bytes
- IPv4 home agents could not relay errors
  - insufficient inner header information
  - some data sources might never find out about broken links
- IPv6 ICMP messages return enough data
- Also used for *anycast home agent discovery*

Mobile IPv6 status

- Interactions with IPsec fully worked out
- Mobile IPv6 testing event Sept 15-17
  - Bull, Ericsson, NEC, INRIA
- Connectathon next week
- Internet Draft is ready for Last Call
- API support needed

Mobile IPv6 & AAA

- Model comparison
- Protocol comparison
- Key management

Model Comparison

- 3G business AAA considerations the same
- AAA servers may use same protocol
  - except wherever IP addresses are indicated
- Network vs. Link authorization
- Service architecture

Protocol Comparison

- Routers used instead of foreign agents
- Regional registration needs new agents, too
  - GGSNs/border routers are candidates
- UDP Lite
- Robust Header Compression
- Challenge generation (not from HLR?)
- Privacy considerations?

IPv6 Key Management

- Still needed for smooth handovers
- Ideas from IPv4 Registration Key:
  - Public Key from mobile node or router
  - Diffie-Hellman key exchange
    - via exponentiation or elliptic curve
  - Using any existing security association
- Interaction with Regional Registration

Summary and Conclusions

- Future Internet is largely wireless/mobile
- IPv6 needed for billions of wireless devices
- Mobile IPv6 is far better and more efficient
- Autoconfiguration suitable for the mobile Internet
- Security is a key component for success
- AAA has a big role to play for cellular rollout
- Leverage from current cellular interest