Tdoc S2M99052

3G Wireless Data Provider Architecture Using Mobile IP and AAA

Tom Hiller
Editor TIA TR45.6 (TSG-P)
July 1999

Carriers and Vendors Involved...

- **US**
  - Airtouch
  - Ameritech
  - GTE
  - Sprint
- **Canadian**
  - Bell Mobility
- **Japan**
  - DDI
  - IDO
- **Vendors**
  - Fujitsu
  - LGIC
  - Lucent
  - Motorola
  - Nortel
  - Qualcomm
  - Samsung
  - SUN
  - 3Com

Goals of Architecture

- **Public Internet Access**
  - **Simple IP service**
    - » **PPP terminated in the cellular network**
  - **Mobile IP Service**
    - » **Home Agent is located in visited or home wireless carrier**
    - » **Dynamic Home Agent and Home Address assignment**
- **Private Network or Home ISP Access**
  - **Home Agent behind a firewall in a private network or ISP**
  - **Support for security and private addresses**
  - **Dynamic Home Agent and Home Address assignment**

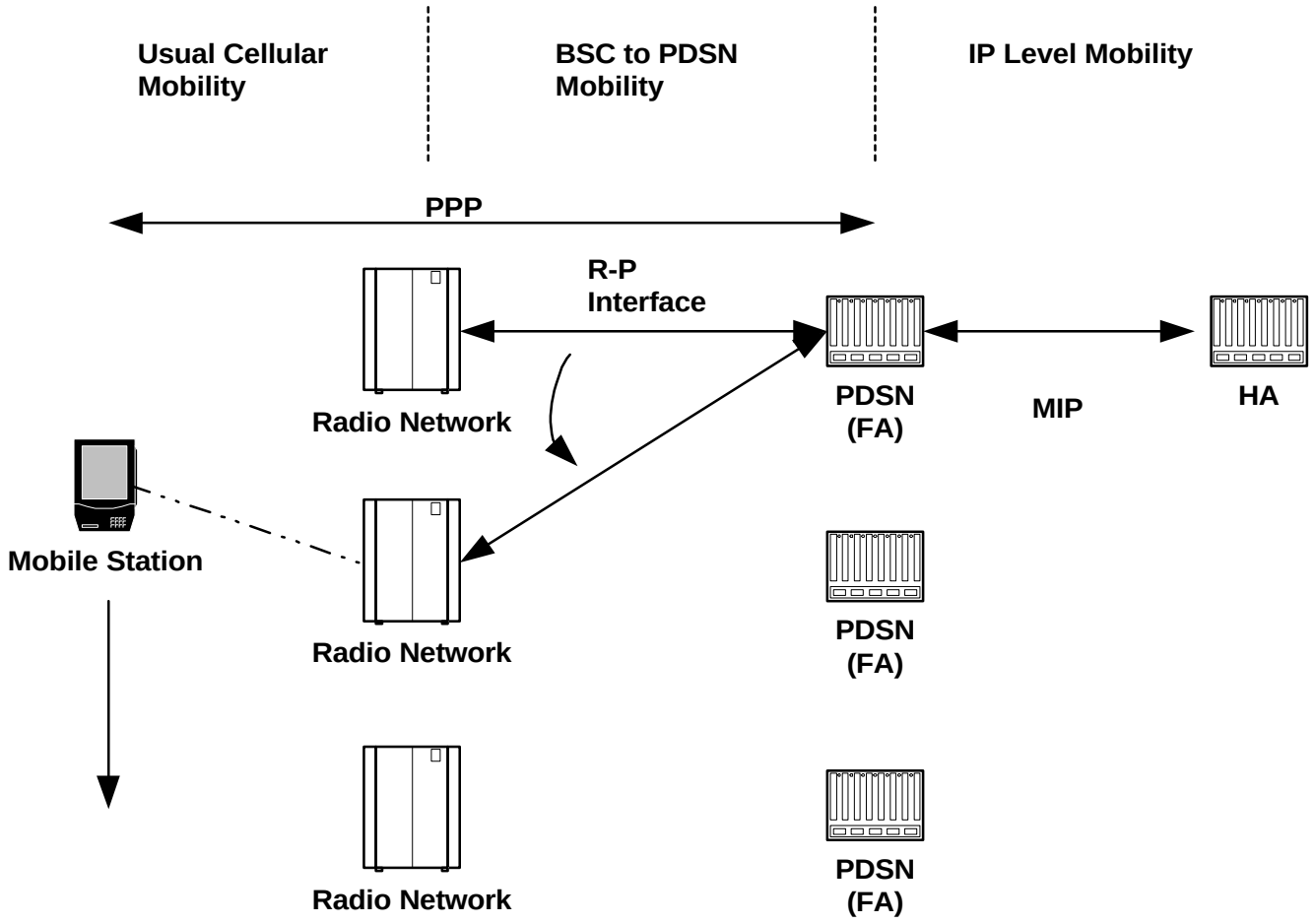
Standards Goals of Architecture

- Supports an overlay network with 3G public cellular
  - Two independent phases of authentication and authorization:
    - » Carrier phase
    - » Data network phase
- Heavy use of IETF protocols and directions
  - PPP, Mobile IP, Differentiated Services, IPsec, and AAA (including proxy AAA)
  - Vendor interoperable interfaces between RAN and Serving Node based on L2TP
- Security support for low end devices that can not support IPsec and/or will not pay overhead on air interfaces

Levels of Mobility

- **Level 1: Cellular mobility supported below RAN with existing mechanisms (Ax interfaces)**
- **Level 2: Mobility between RAN and PDSN "R-P interface"**
  - **Supports a connection that transports *data link layer frames* between RAN and PDSN**
  - **General "M RAN to N PDSN" problem space**
    - » **Helps load balancing, etc**
  - **Associated RANs and PDSNs belong to one carrier**
  - **Under Study: This interface may be based on Tunnel Establishment Protocol with GRE, or may be based on L2TP with extensions**
- **Level 3: Mobile IP with AAA extensions between FA and HA**

Levels of Mobility (cont'd)

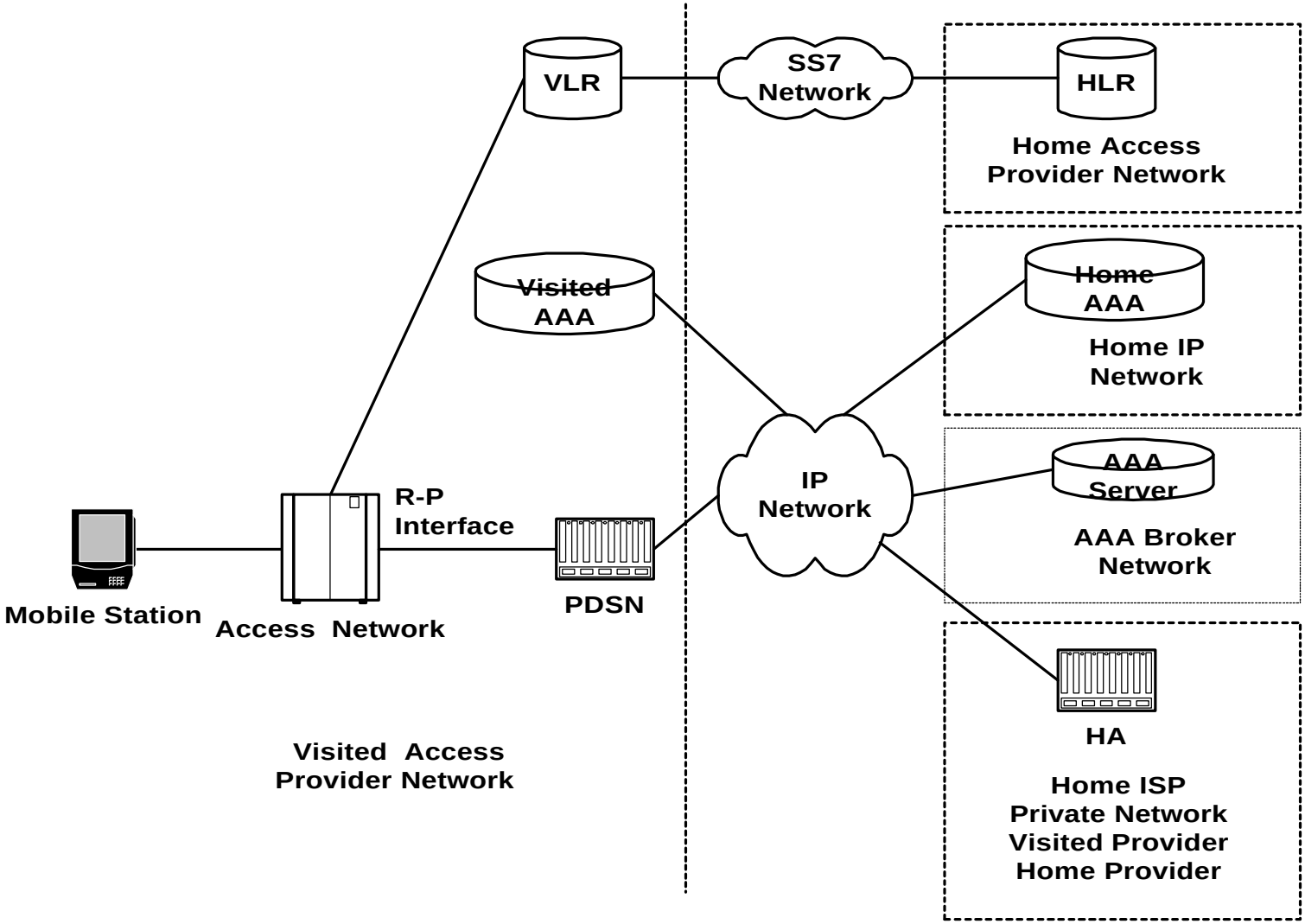


Lucent Technologies
Bell Labs Innovations

Comments

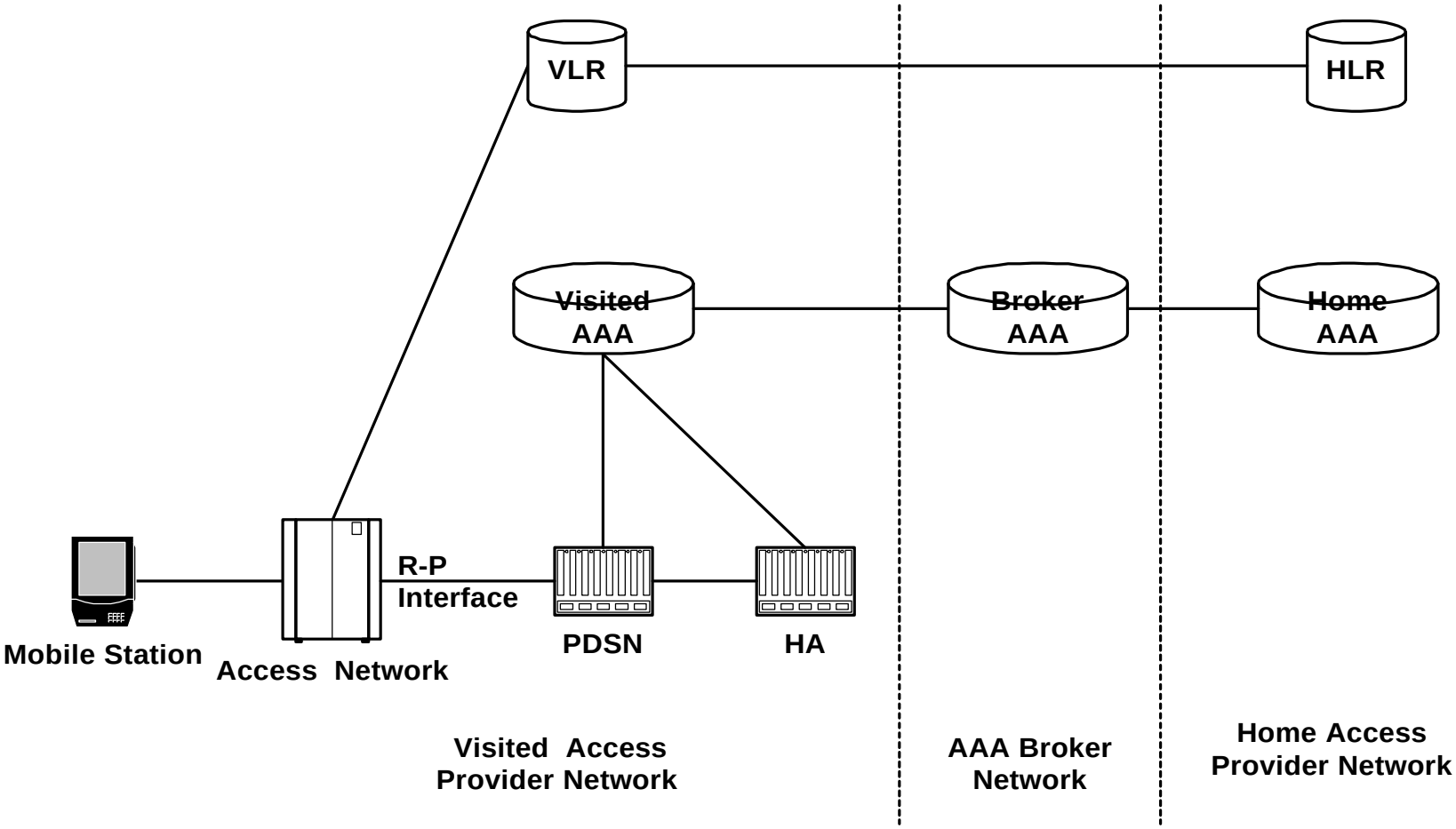
- Architecture supports many service variations
  - PPP
    - » Handoffs between multiple RANs, including dormant handoff
    - » Supports mobility for PPP based laptops in a moderate sized area (e.g. city)
    - » Authentication by home network using ISP roaming
  - Mobile IP
    - » Usual MIP mobility between serving nodes
    - » Dynamic or static address support (including private addresses)
    - » Home Agent static or dynamically assigned in either home or visited network (like a form of route optimization)
    - » Uses the NAI in the MIP RRQ to allow AAA functions (e.g. billing) to be performed on a user basis versus a device basis

Architecture



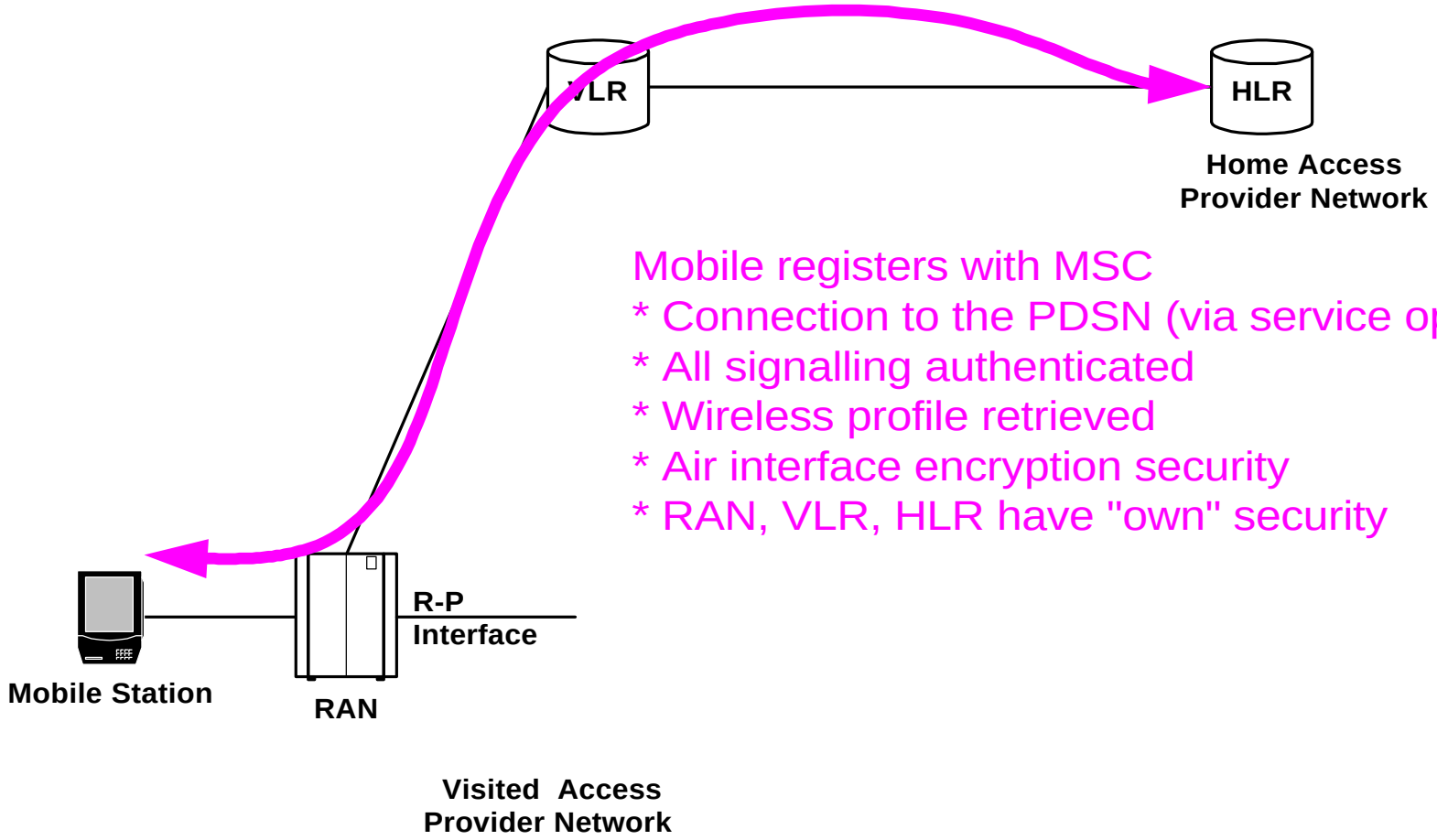
Lucent Technologies
Bell Labs Innovations

Tutorial: Visited Network Provider Assigns HA



Lucent Technologies
Bell Labs Innovations

(Step 1) MIP Registration

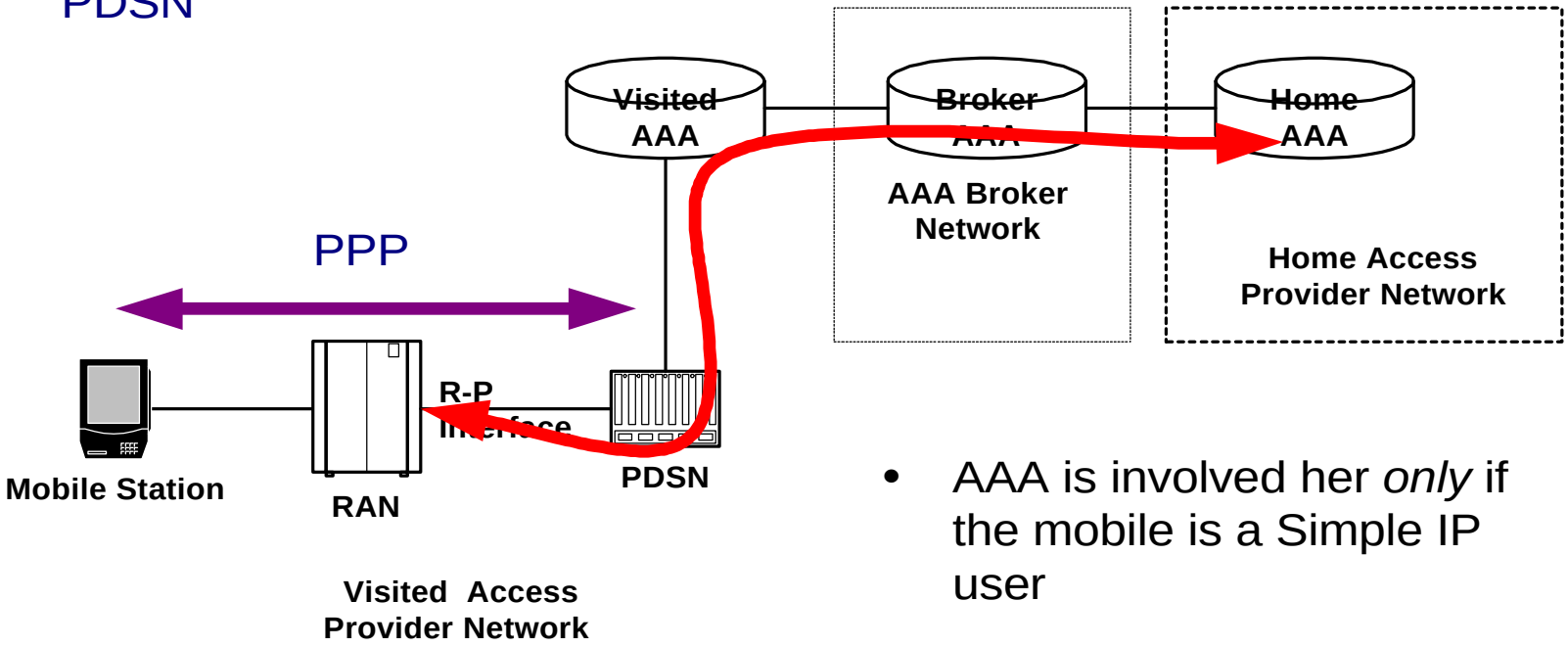


Mobile registers with MSC
* Connection to the PDSN (via service option)
* All signalling authenticated
* Wireless profile retrieved
* Air interface encryption security
* RAN, VLR, HLR have "own" security

(Step 2) Mobile Establishes PPP

- Mobile requests connection to RAN with IP Service Option
- RAN selects a PDSN, and establishes connection to PDSN
- Mobile establishes PPP link to PDSN

- PPP CHAP applies to Simple IP, not MIP; Authentication for SIP ues home AAA

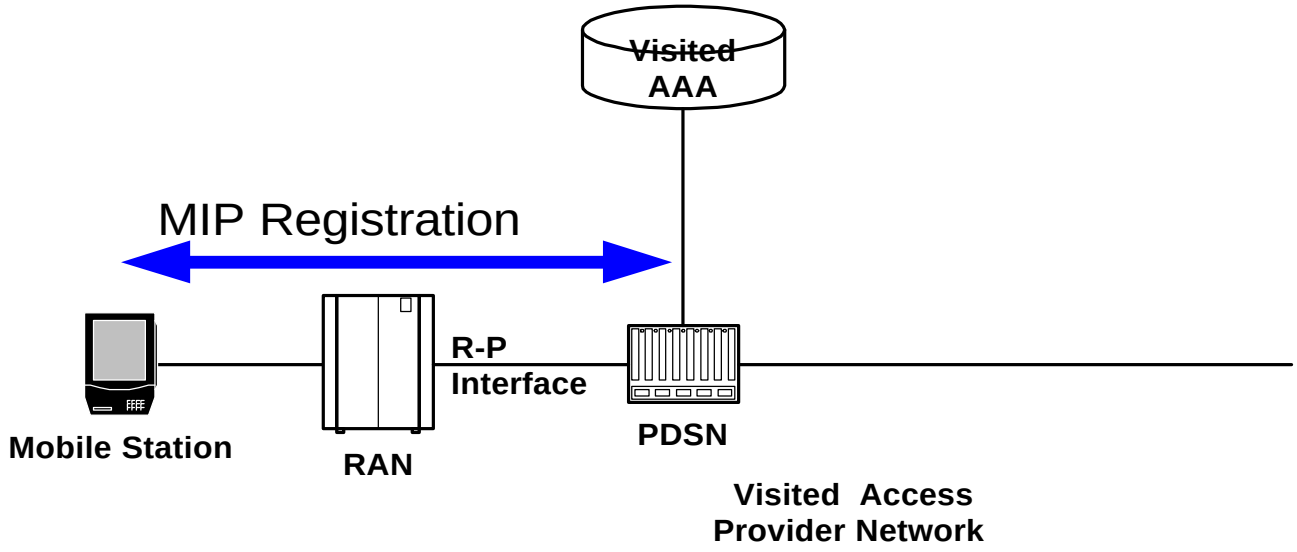


- AAA is involved her *only* if the mobile is a Simple IP user

Lucent Technologies
Bell Labs Innovations

(Step 3) MIP Advertisement and Registration

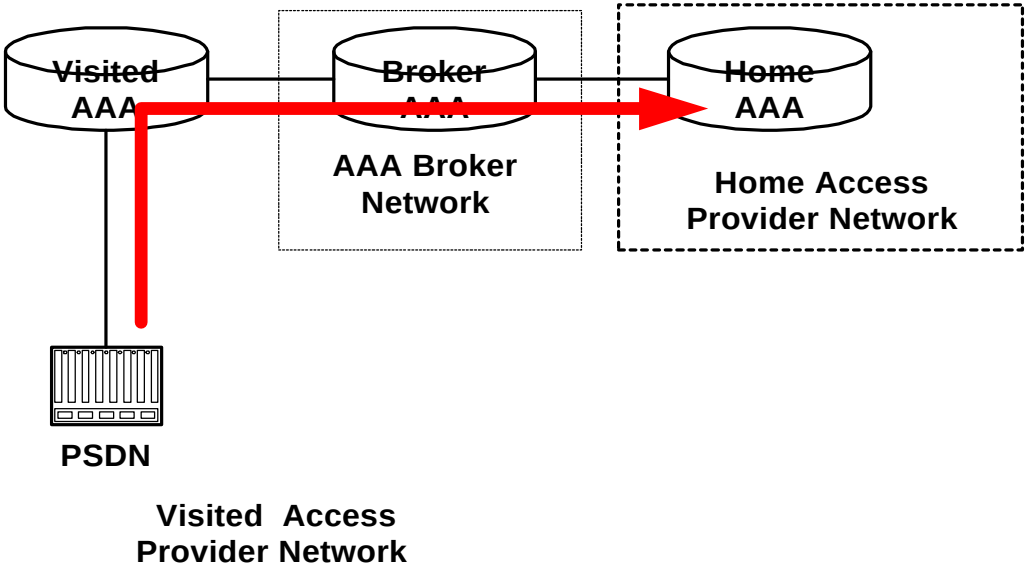
FA (inside the PDSN) advertises its presence to the MIP Client in the mobile
  * Random Challenge included in advertisement
Mobile registers and includes a challenge response
Mobile identifies Home Agent w/ NAI
  * NAI = user@realm
  * shared secret to the Home Agent is in the request



Lucent Technologies
Bell Labs Innovations

(Step 4) AAA Request to the Home AAA Server

FA (inside the PDSN) verifies random challenge was recently sent
FA creates an AAA message to visited AAA
FA indicates it is able to assign a HA for the mobile
Visited AAA sends to Broker AAA
  * visited AAA server uses the NAI to determine the broker AAA server
Broker AAA sends Home AAA
  * broker AAA server uses the NAI to determine the home AAA server



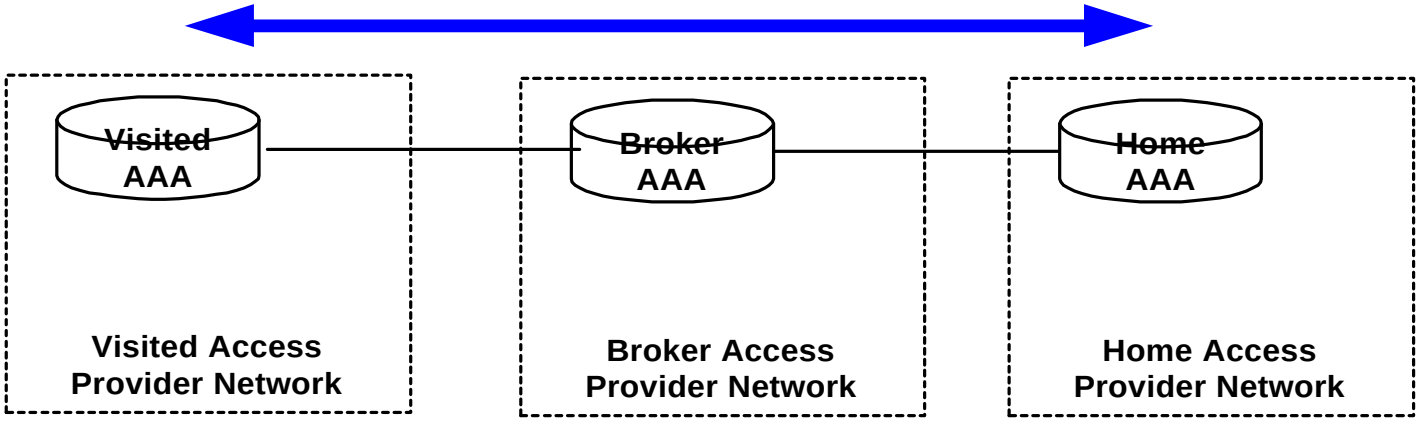
Lucent Technologies
Bell Labs Innovations

(Step 5) Home AAA Server Authenticates User

This example assumes that the user is configured for dynamic HA assignment by a serving network

Home AAA processes the AAA Request
* Verifies Foreign Agent Challenge
* Determines that a dynamic HA is required
* Determines that the FA is able to assign an HA

Sends an successful AAA Answer to the visited AAA containing the users shared MIP secret and NAI

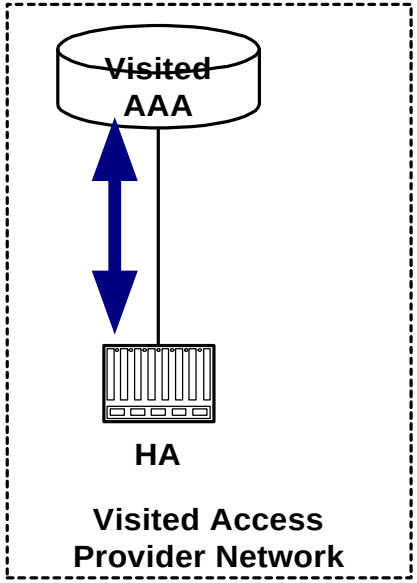


(Step 5) Visited AAA Server Assigns an HA

Visited AAA server determines dynamically assigned Home Agent, MN home address, and HA-FA keys, and MN-FA keys

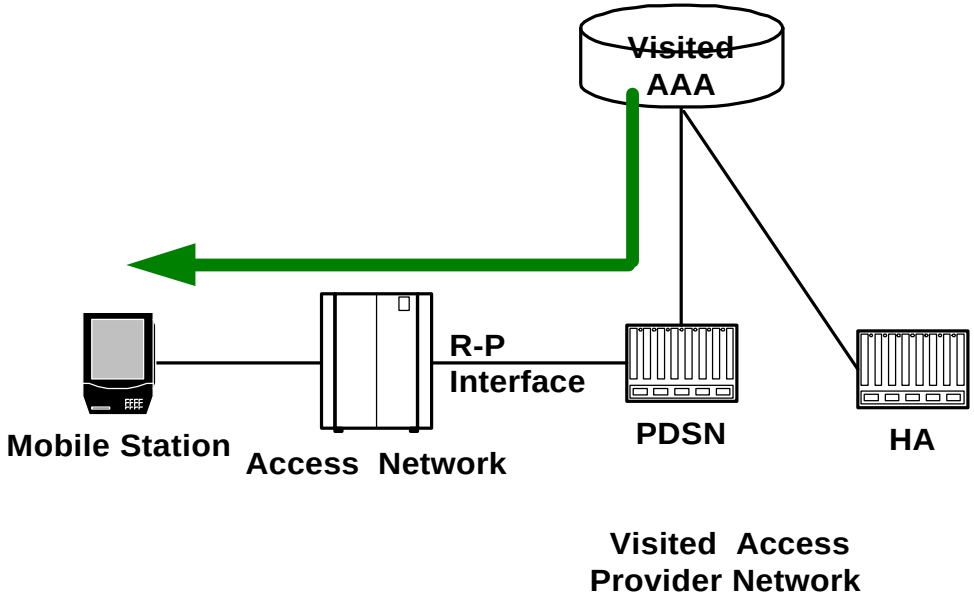
Visited AAA server sends AAA Request to the assigned HA with the MN address, shared secret, NAI and keys

HA allocates resources for user, and sends an AAA Answer to visited AAA. Answer contains a MIP Reply
* Hash code between HA and MN
* HA and MN addresses
* MIP options originally requested



(Step 6) Visited AAA Server and FA Reply to MN

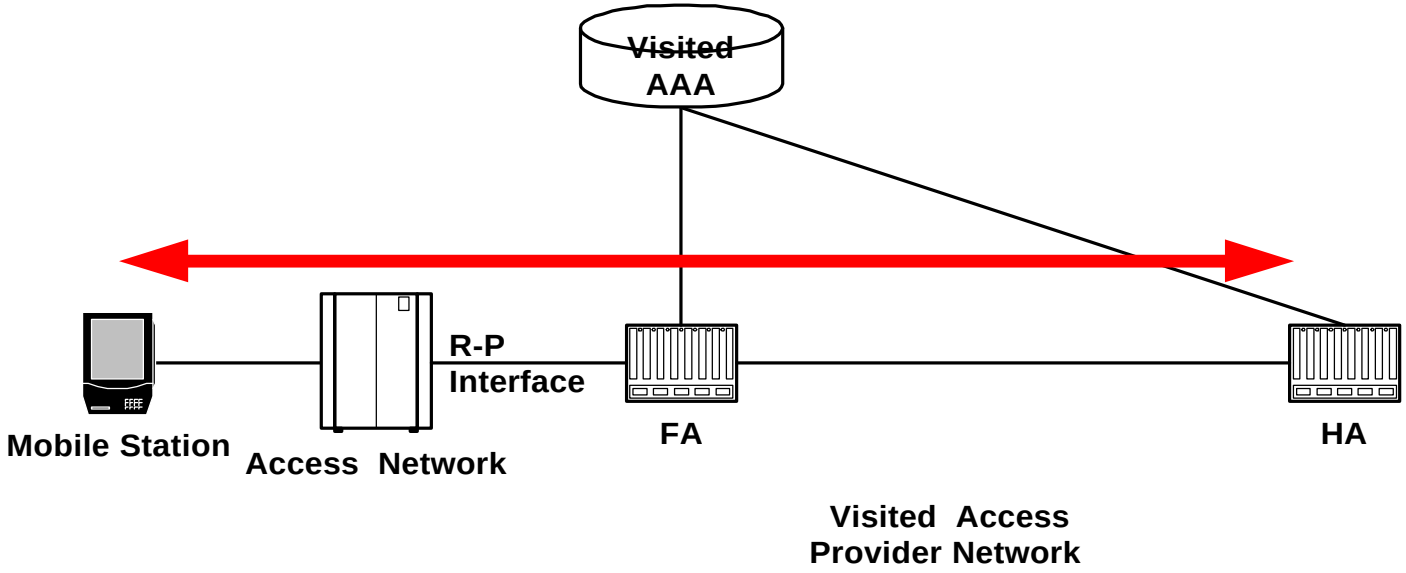
AAA Server sends AAA Answer to FA
FA extracts security information (FA/HA key)
FA sends Mobile IP Reply to MN
Done!



Lucent Technologies
Bell Labs Innovations

Re-registration

Eventually, registration times out
Mobile sends RRQ to FA, FA sends RRQ to HA (AAA not involved)
HA sends RRP to FA and FA sends RRP to Mobile
If security keys expire, AAA servers become involved again
If mobile moves to a new FA, AAA servers become involved again

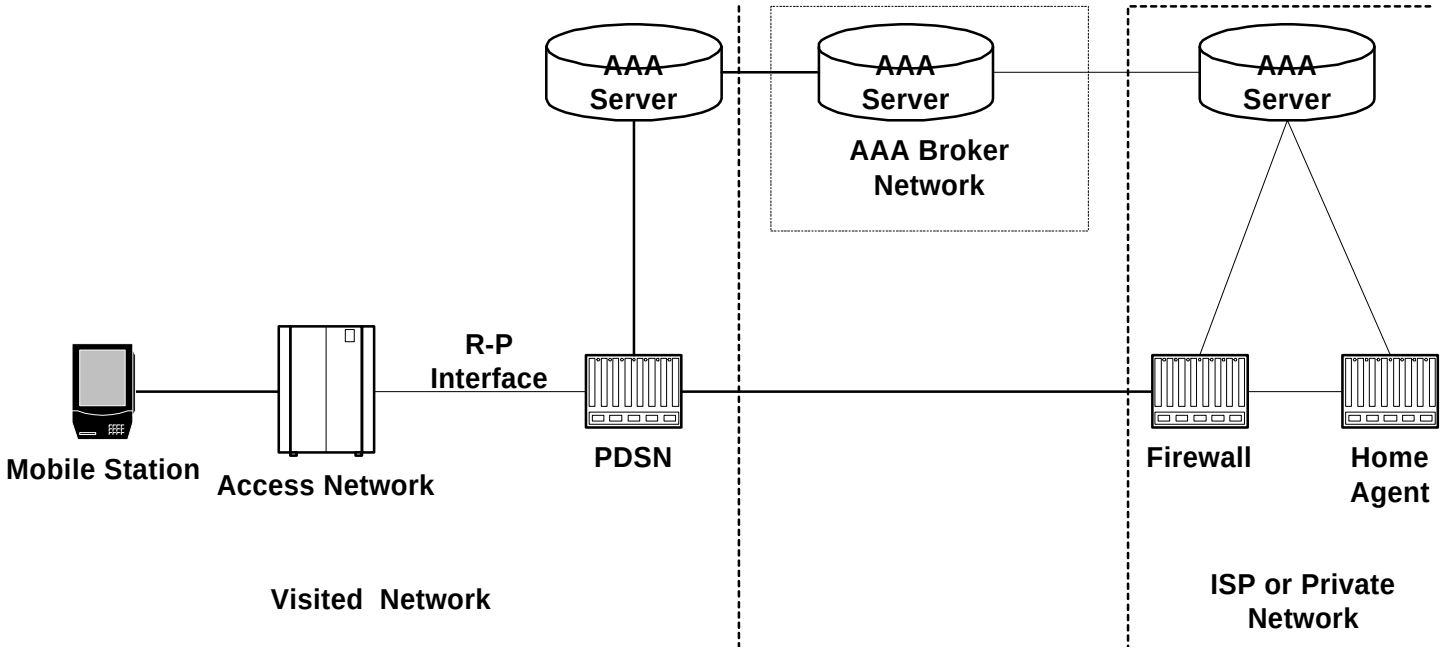


Lucent Technologies
Bell Labs Innovations

Private Network or Home ISP Assigns HA

Similar
- HA may be statically or dynamically assigned by private network
- Private addresses are not unique
- Home AAA server may assign security IPsec security between HA and FA

Firewalls must pass messages addressed to AAA server and HA

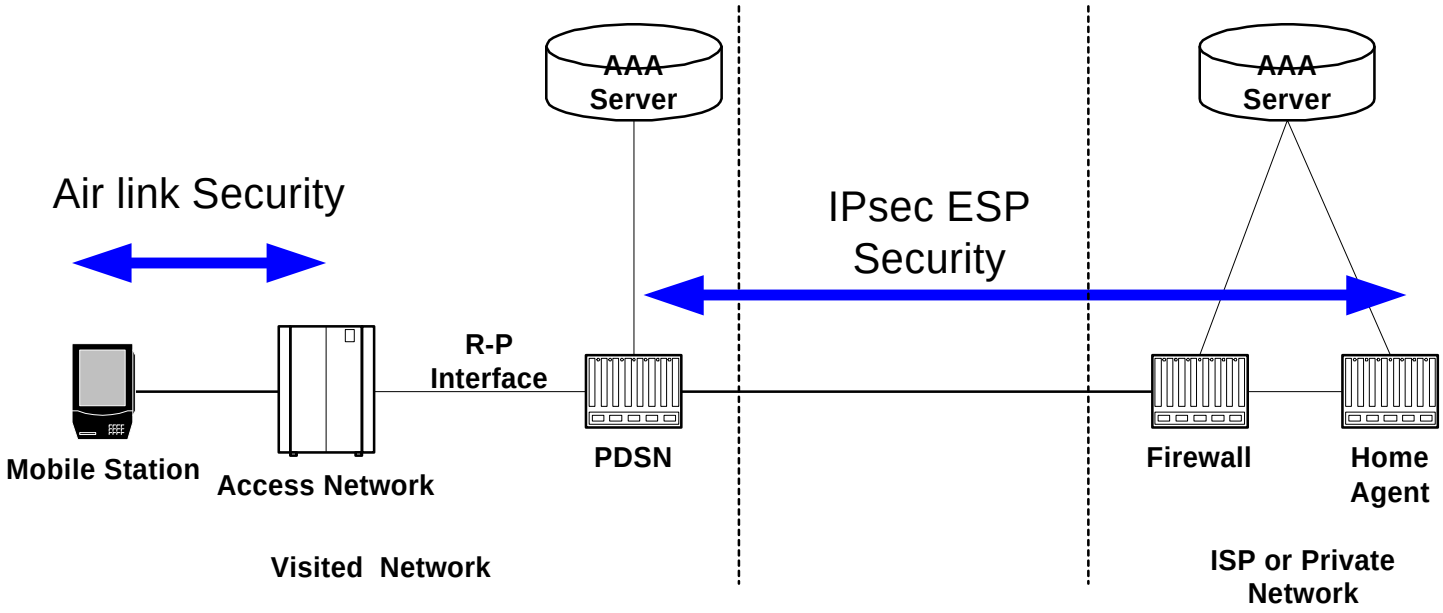


Lucent Technologies
Bell Labs Innovations

Optional Security Feature

Some mobiles may not be able to support IPsec and/or may not be willing to pay for overhead of IPsec on air interfaces.

This architecture provides the mobile with some level of privacy, if the mobile trusts the carrier. This will not be accepable for everyone! Note:The visited carrier IP network is not part of the public Internet



Lucent Technologies
Bell Labs Innovations

Roaming

- **Relationships:**
  - **Mobile has a single relation with one access service provider**
    - » **For wireless: IMSI, user-key, and user profiles are stored in HLR**
  - **User (identified via the NAI = user@realm) may have many home networks (e.g. private networks, ISPs, etc)**
    - » **NAI (I.e. name@realm) in MIP RRQ identifies home network**
    - » **Requires home AAA with user profile and shared secret**
    - » **This architecture uses "Proxy AAA" to direct AAA messages between home and visited network**
      - **Proxy AAA uses the NAI to "route" the AAA messages**

Security

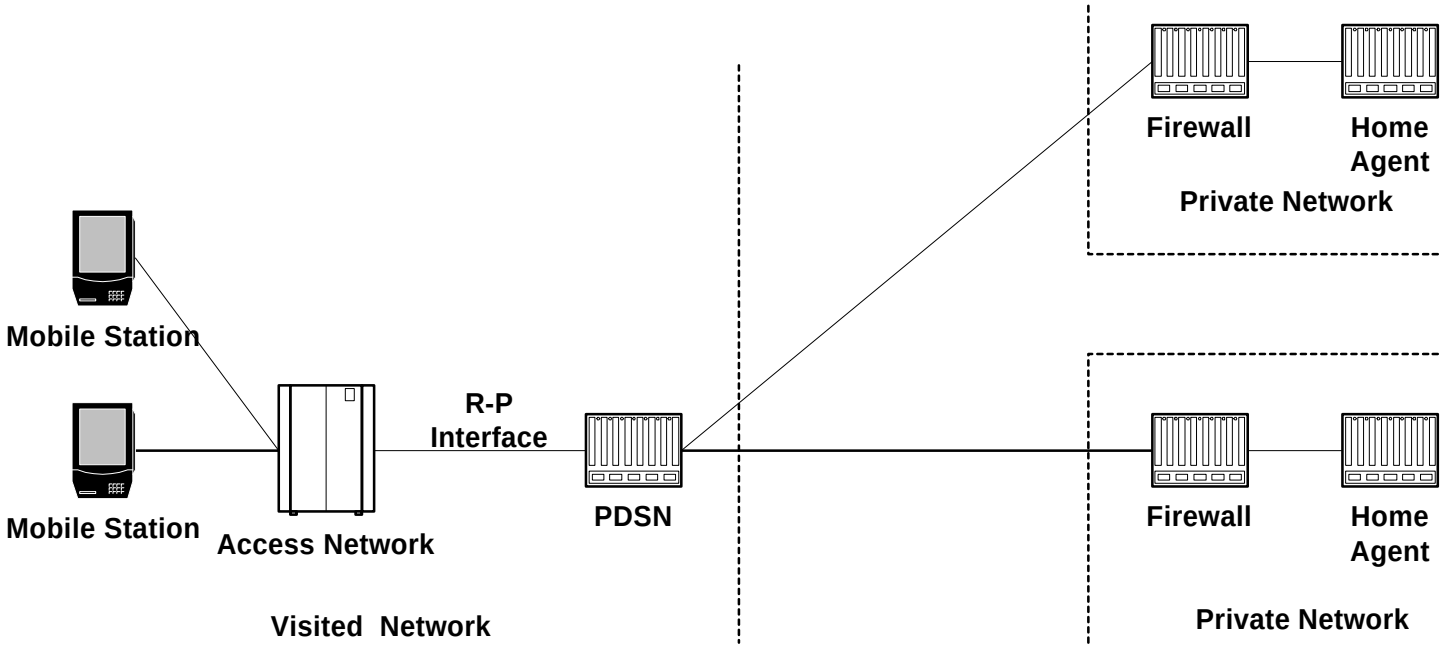
- **Between AAA servers**
  - AAA servers have pre-existing security based on relationships
  - Security associations established as part of business relationships
- **Between AAA servers and Agents**
  - Mobile Agents and local AAA server are owned by same provider
- **Security functions**
  - Key distribution by AAA server
    - » Dynamic security between FA/HA, MN/FA
    - » Static or dynamic security between MN/HA
    - » FA/HA optional security feature

Addresses

- Mobile home address: Dynamic or static
  - Statically assigned HA may dynamically assign home addresses
  - HA and AAA server may be in private network
  - Home addresses may be private and overlapping
  - Pool of address maintained by AAA server or HA
    - » HA/FA Security required by carriers without national footprint
- Dynamic assignment of HA by serving or home network
  - HA assignment is service dependent
  - Desirable to support users who roam great distances, e.g., from other continents
- Simple IP address assigned by either PDSN or AAA

Private Address Support in MIP

Problem:
Two mobiles have the same private address on the same FA
Two R-P connections exist, each with their own "link identifier"
The FA must "bind" the MN address, R-P link address, and the HA address
Note: The FA and HA addresses are both assumed to be publicly routable
Recent draft by C. Perkins proposes general framework



Lucent Technologies
Bell Labs Innovations

AAA Protocols

- **Reliable protocol**
  - Between AAA servers, AAA servers and Agents
  - Required by wireless carriers
  - Allows rapid detection of a dead Agent or AAA server
  - The network (re)configures with a different AAA or Agent
    - » Implementation specific, we understand
- **Proxy AAA protocol**
  - Allows support of encryption of specific AVPs
    - » A given message can have multiple AVPs encrypted differently
  - Signatures and next routing AVPs

Dual Authentication

- **Separation of air link resource and data network authentication**
  - **Air link authentication uses existing link layer mechanisms**
    - » **Access service providers have pre-existing relationships**
    - » **AAA "replacing" HLR/VLR entities is not under study**
  - **Data network authentication uses AAA servers**
    - » **Proxy AAA required when visited access provider has no relationship with home network**
    - » **Security associations pre-exist between visited and broker AAA server, and broker AAA server and home AAA server**

Mobile Station

- **Must support Mobile IP Client**
  - **Must support NAI and FA Challenge in RRQ**
  - **NAI identifies the home network**
    - » **Each network needs a shared secret provisioned in mobile**
    - » **MN shared secret for FA Challenge and HA may be different**
- **Optimized handoffs between FAs**
  - **Support for "optimized" intra-domain handoffs**
    - » **Requires dynamic MF/FA security, previous FA extension**
- **Two types of mobiles possible**
  - **"Relay Model" or "Network Model"**
    - » **Relay: laptop supports link layer and Mobile IP Client**
    - » **Network: Mobile station supports link layer and Mobile IP Client, and optional PPP link to the laptop**

Link Layers

- PPP
  - PPP compression
    - » Probably only applies to laptops due to power issues
  - VJ TCP header compression
  - PPP encryption not currently planned
  - IP address assignment
    - » User omits IPCP IP Address option so PPP does not assign an address; MIP then assigns the home address
    - » Static IP address passed to PPP server via extensions in RFC2290
      - This also applies to a registration on a new FA for a MIP session already in progress
  - For Simple IP, most carriers will require CHAP

Differentiated Services

- Home AAA server stores user “differentiated services ” profile
  - Example: Which class behaviors the user may invoke or
  - Example: Classifications to be performed by the PDSN for the mobile
- MN or FA may perform packet marking
  - FA can over-ride MN markings
- PDSN sends differentiated services indication per frame (e.g. outer tunnel DS field on R-P interface) to the RAN
- The RAN delivers the packets according to the differentiated services rules
  - Single PPP link or Multiple PPP link from PDSN is under study
- Carriers must meet Service Level Agreements with ISPs

Accounting Management

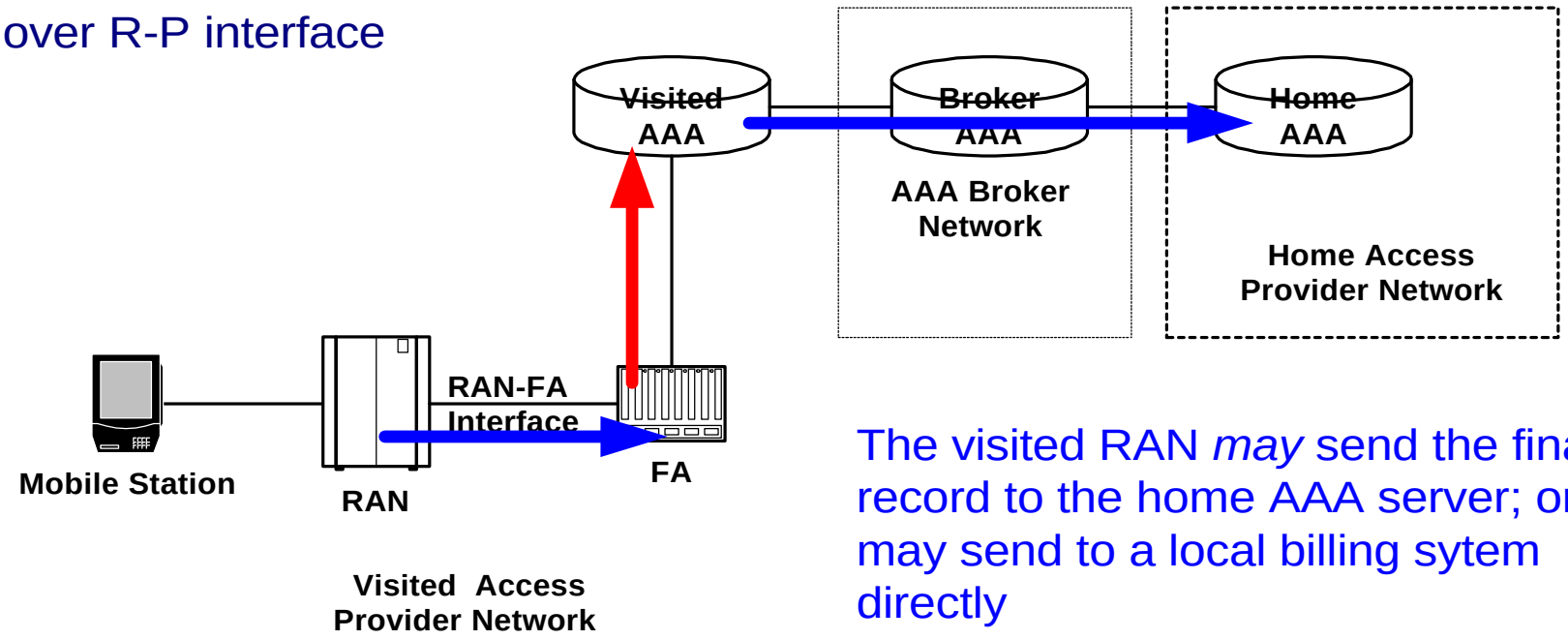
- Usage information is collected both in RAN and PDSN
  - RAN collects
    - » air link specific information such as active duration (non-dormant) periods and total length of session, Mobile Identifier (IMSI).
  - FA collects
    - » NAI, MIP options involved (e.g. home address or Agent assignment), data traffic usage on per diff-serv behavior class
- Reconciliation between carriers
  - May use ISP style reconciliation from IETF ROAMOPS group - commercially available
  - AAA may initially used as a point of accumulation only
- Retention and accuracy requirements TBD

Accounting Management

RAN collects air link specific usage and data, e.g. dormant/ active periods, IMSI

RAN sends these to the PDSN over R-P interface

PDSN collects data link and above specific usage and parameters e.g. NAI, number of packets and bytes. Later, the PDSN sends its collected information plus information from the RAN to the local AAA server



The visited RAN *may* send the final record to the home AAA server; or may send to a local billing sytem directly

Lucent Technologies
Bell Labs Innovations