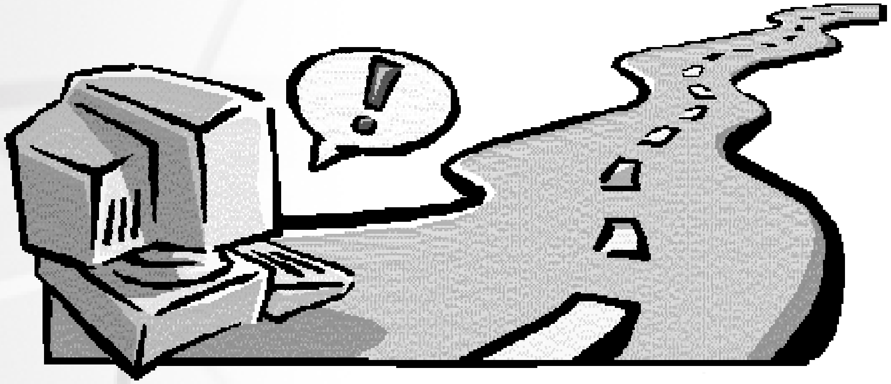
NORTEL NETWORKS

IP Mobility
“Always on, Everywhere”



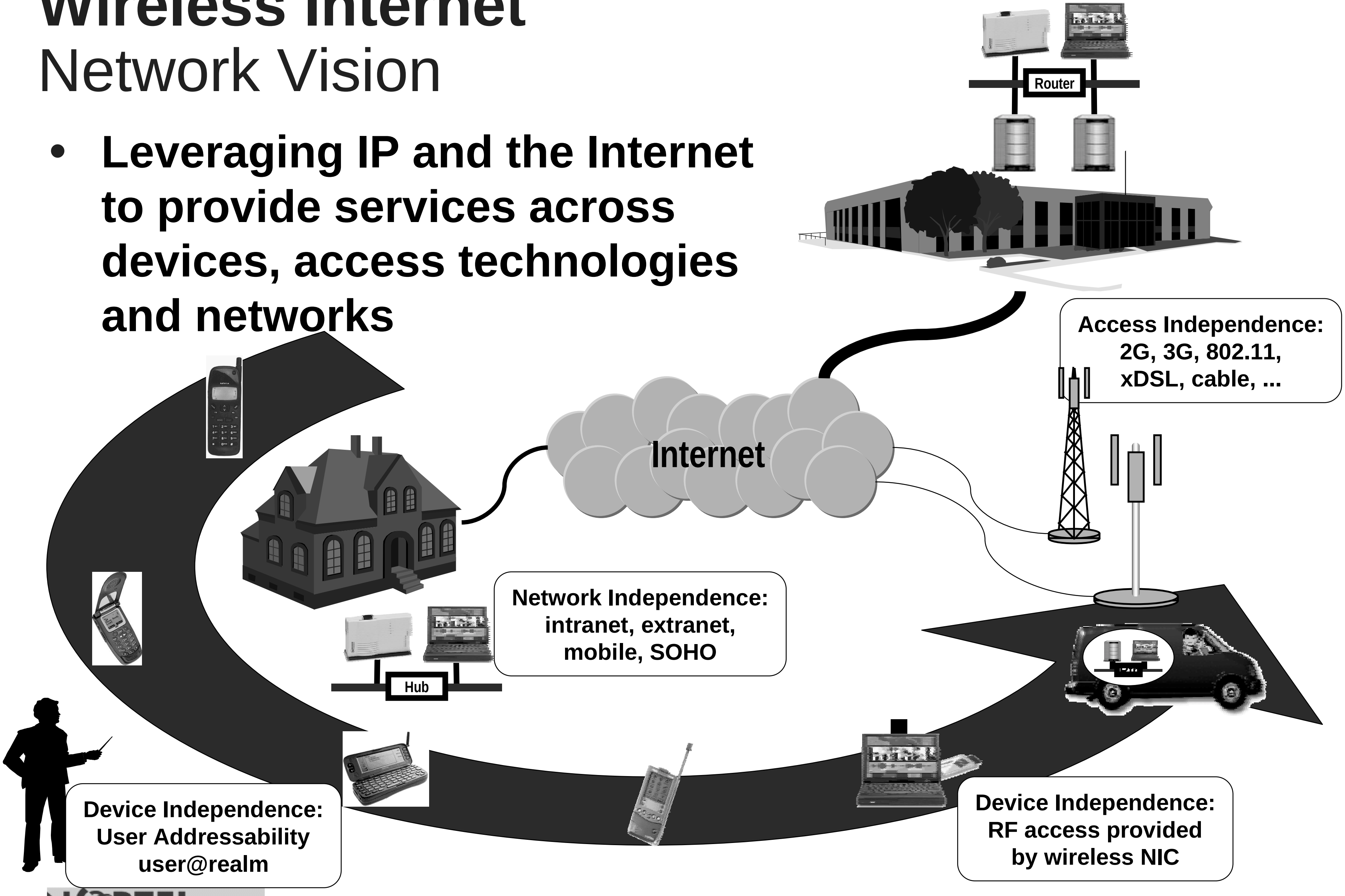
Sprint Research Symposium

March 8-9, 2000

Emad Qaddoura, IPMobility Group

Wireless Internet
Network Vision

- **Leveraging IP and the Internet to provide services across devices, access technologies and networks**



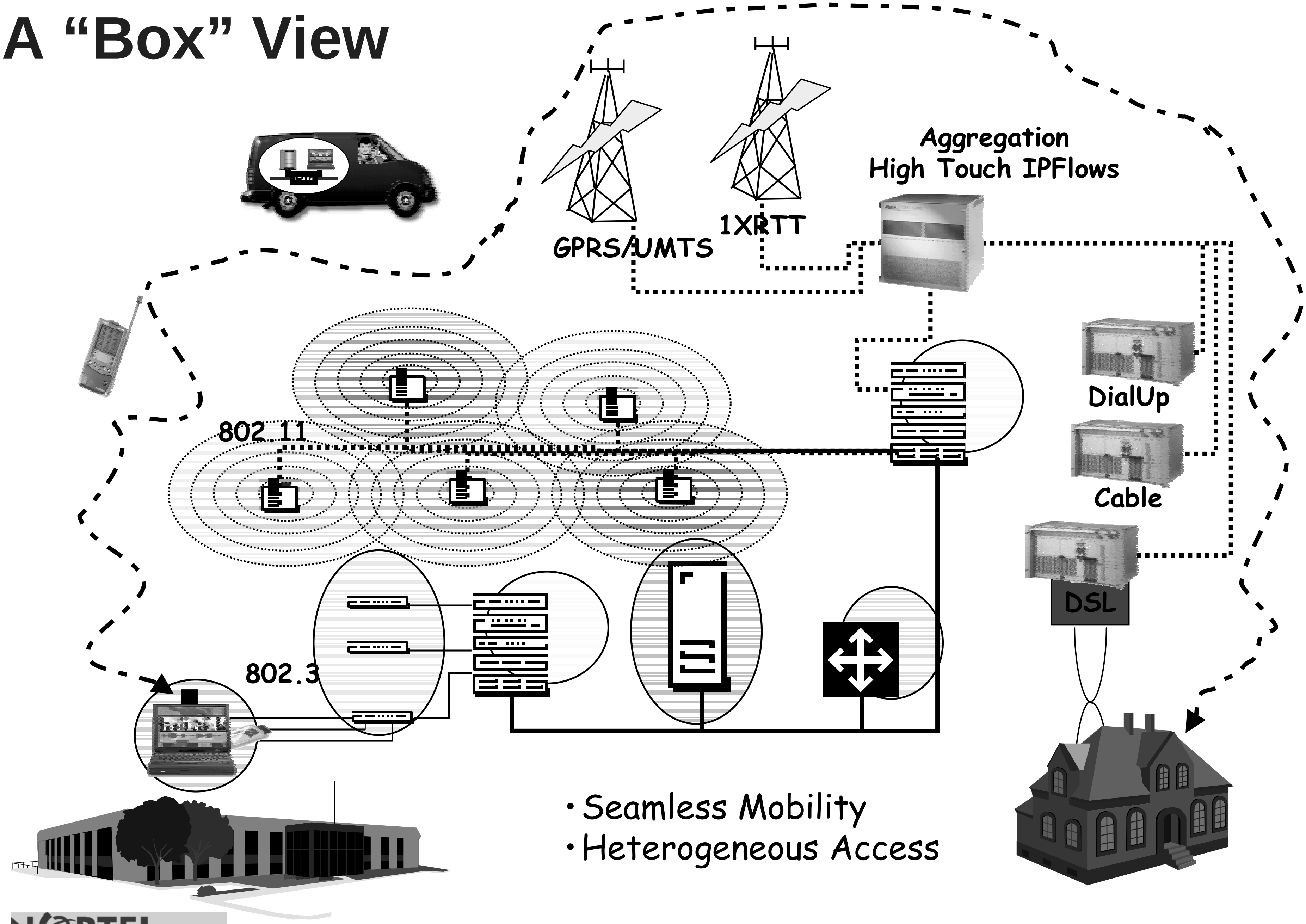
Access Independence:
2G, 3G, 802.11,
xDSL, cable, ...

Network Independence:
intranet, extranet,
mobile, SOHO

Device Independence:
User Addressability
user@realm

Device Independence:
RF access provided
by wireless NIC

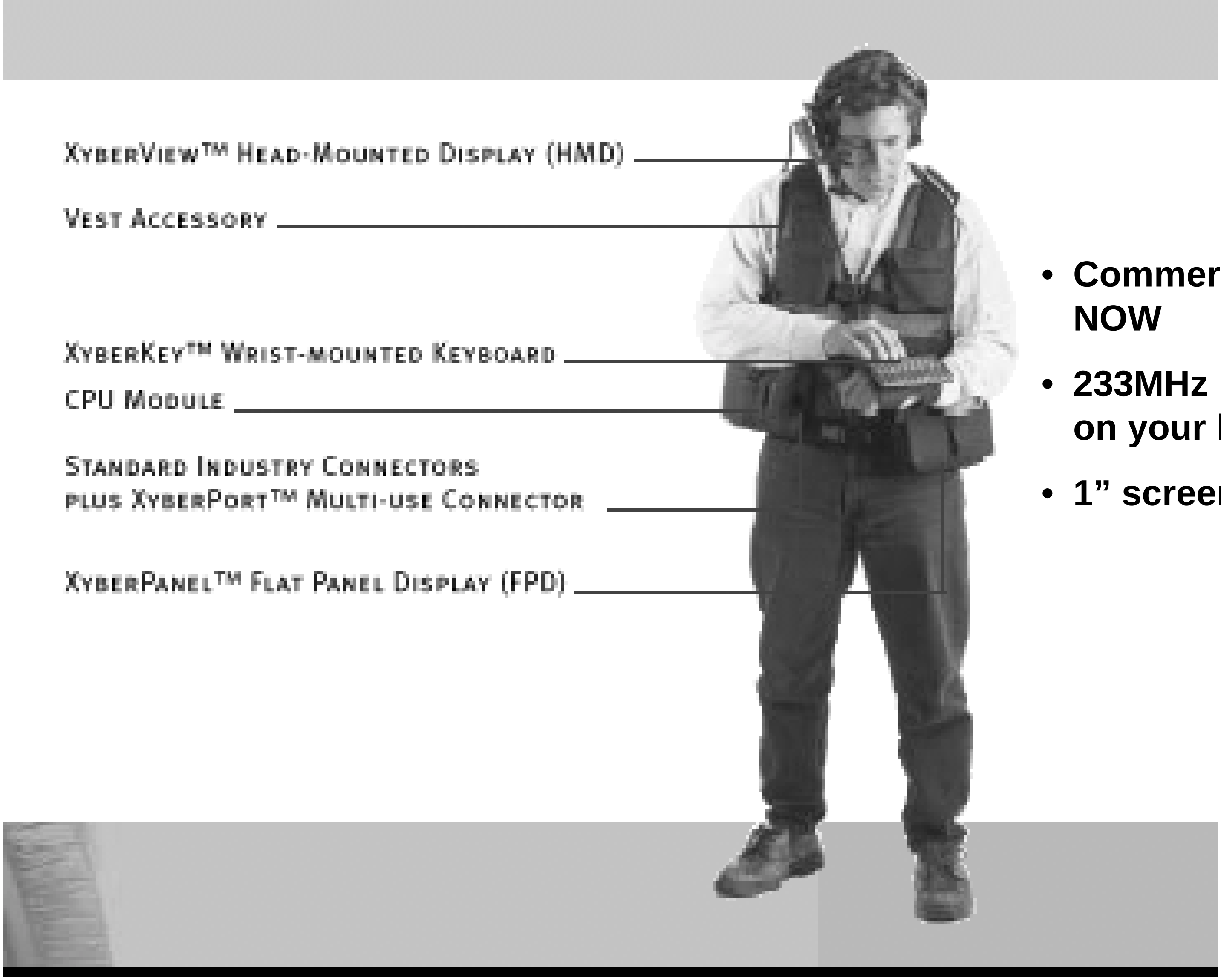
A "Box" View



- Seamless Mobility
- Heterogeneous Access

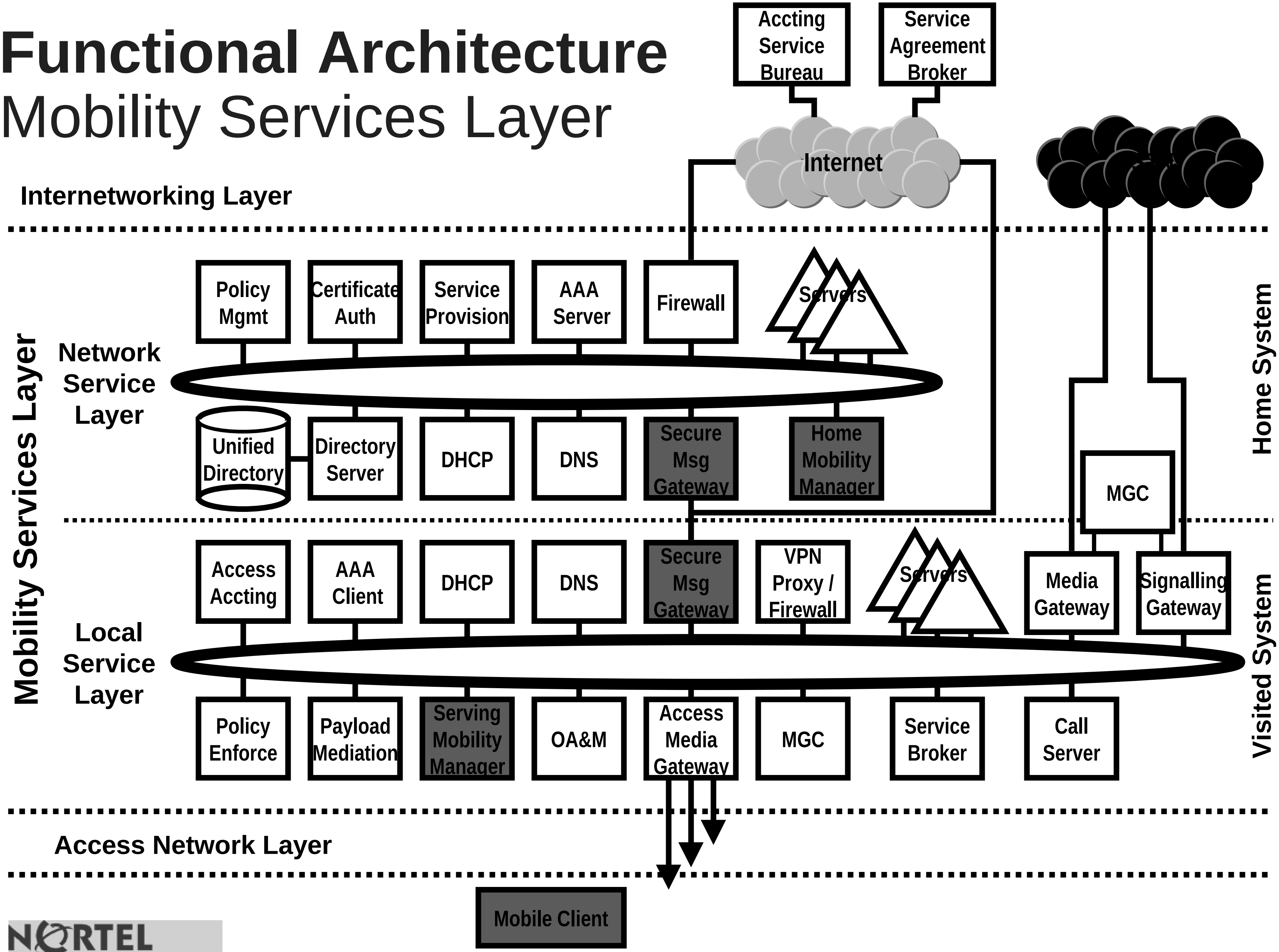
NORTEL NETWORKS

“Future” Mobile Terminals

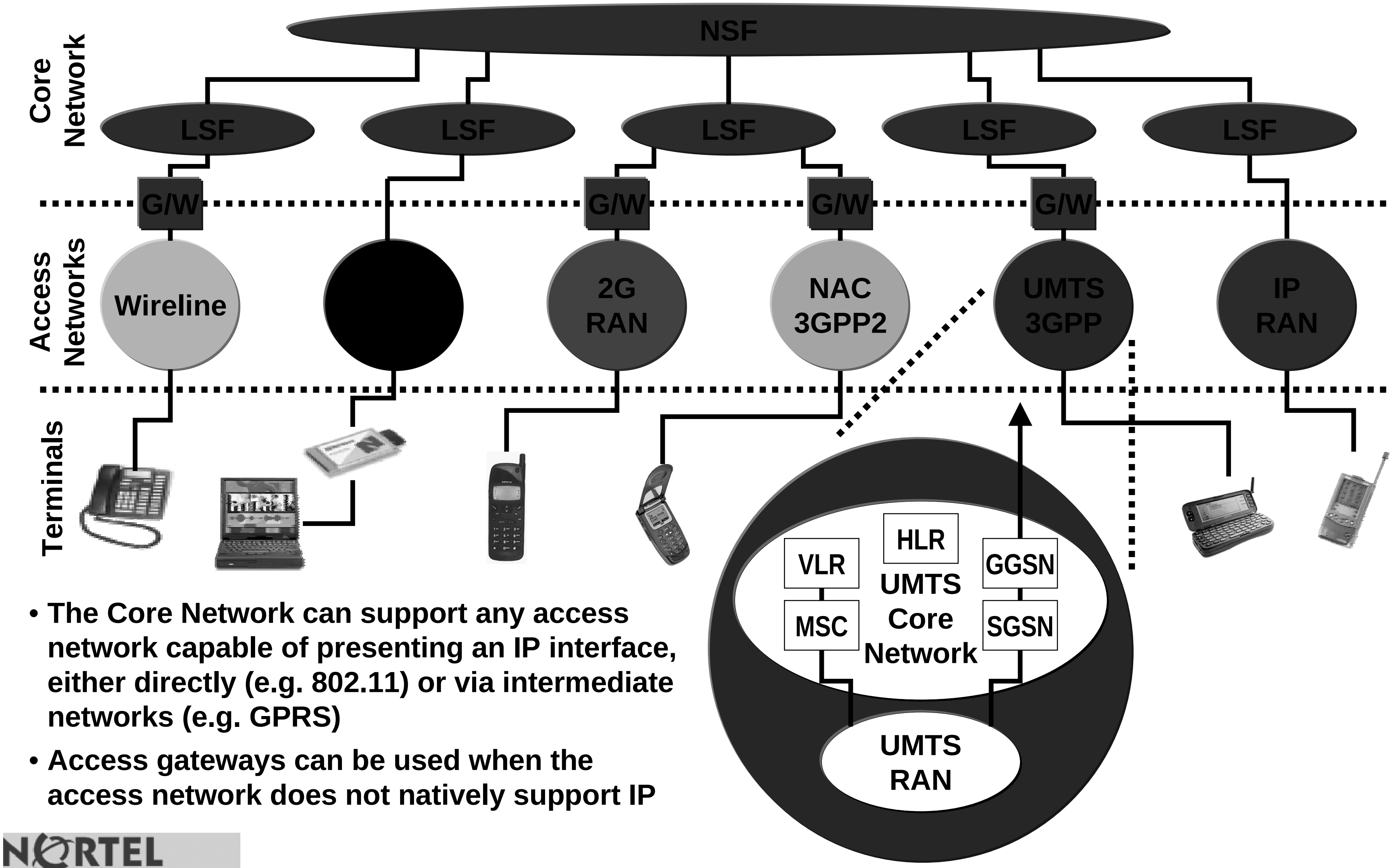

XyberView™ Head-Mounted Display (HMD)
Vest Accessory
XyberKey™ Wrist-mounted Keyboard
CPU Module
Standard Industry Connectors
plus XyberPort™ Multi-use Connector
XyberPanel™ Flat Panel Display (FPD)

- **Commercially available NOW**
- **233MHz Pentium II MMX on your belt**
- **1” screen = 17” monitor**

Functional Architecture
Mobility Services Layer



Functional Architecture
Access Independence



- The Core Network can support any access network capable of presenting an IP interface, either directly (e.g. 802.11) or via intermediate networks (e.g. GPRS)
- Access gateways can be used when the access network does not natively support IP

IP Mobility
Definitions

- **The Wireless Internet is an IP-centric, mobility-enabled network**
  - — IP addresses are used for all routing within the core network
  - — IP protocols and technologies are used in the control plane
  - — The network is functionally equivalent to a traditional cellular network (especially with respect to mobility and roaming)
- **IP Mobility focuses on Layer 3 of the core network**
  - — Mobility functions are independent of the access technology (2G, 3G, wireline, etc.) and the underlying network transport technology (ATM, Ethernet, etc.)
- **The IP Mobility framework is a functional architecture**
  - — There are many alternative implementations

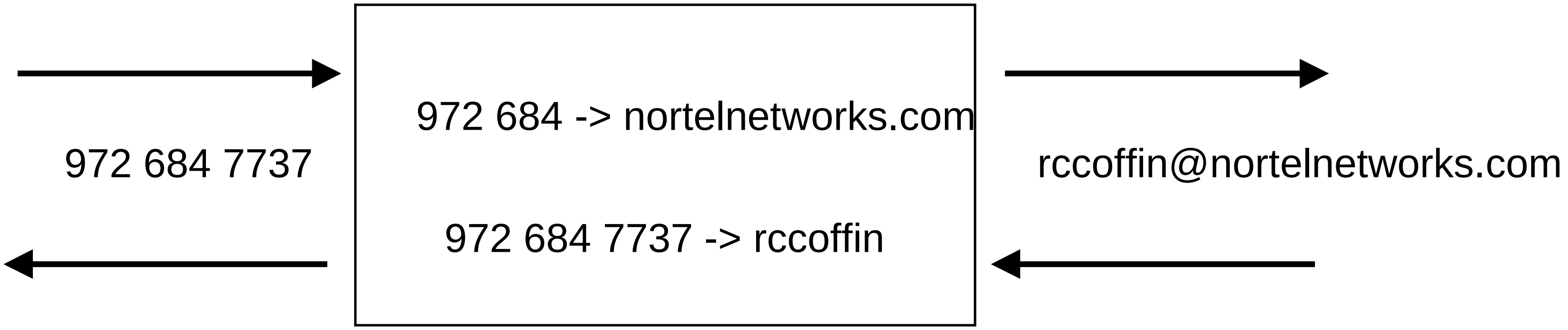
IP Mobility
Key Principles

- **Mobility is based on the user, not the terminal**
  - — Users will have a single subscription in a home network
- **Security is essential within and between networks**
  - — Networks will employ a single network security framework
  - — Service Level Agreements (SLAs) must exist between all networks users will roam in
- **IP protocols will be used wherever practical**
  - — Terminals will support the IP stack (end-to-end packet data)
- **The network architecture should be simple**
  - — The architecture will employ a single control plane protocol
  - — The architecture should avoid having anchor points

User / Mobile Node / Server Addressing

- **Identity of all components based on the IETF Network Access Identifier (NAI)**
  - — User, Mobile Node, Serving & Home Domains
  - — The NAI grammar based on IETF RFC 2486
  - — The general format is “user@realm” (rccoffin@nortelnetworks.com)

NAI/E.164 Interworking



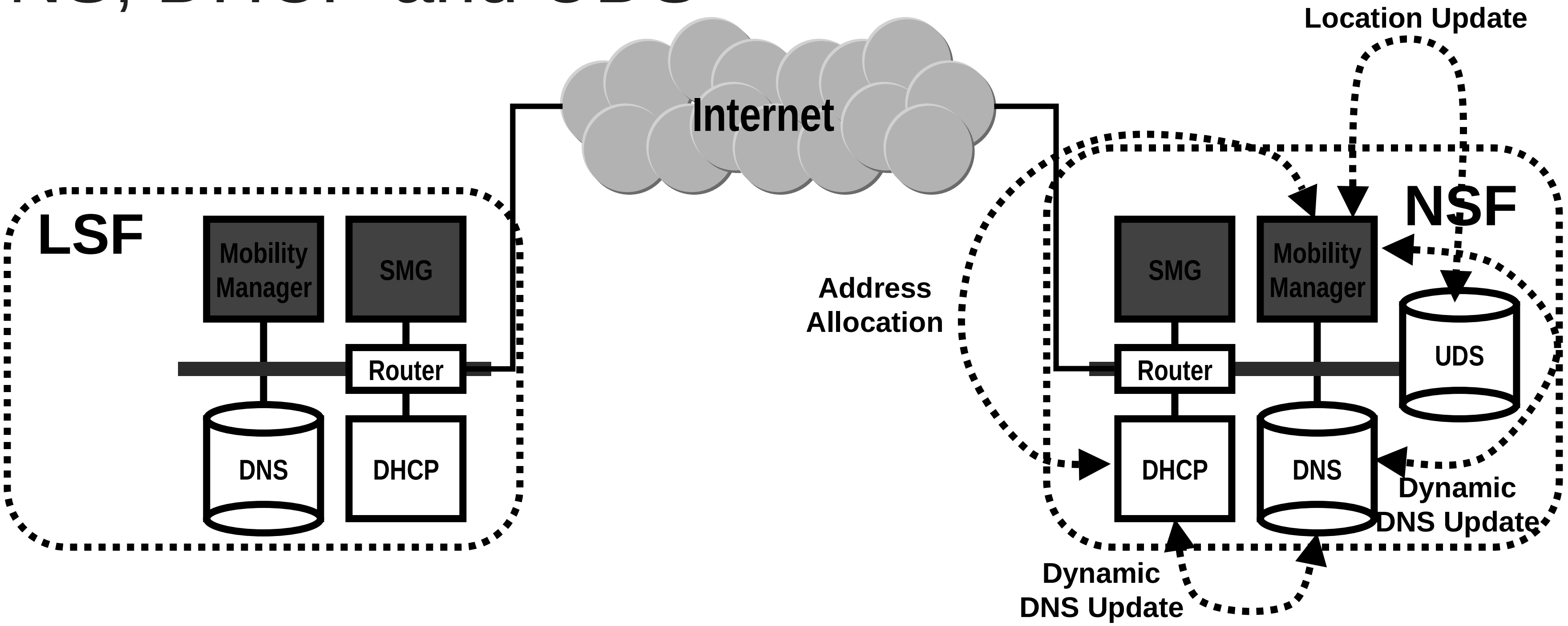
972 684 7737

972 684 -> nortelnetworks.com

972 684 7737 -> rccoffin

rccoffin@nortelnetworks.com

IP Mobility
DNS, DHCP and UDS



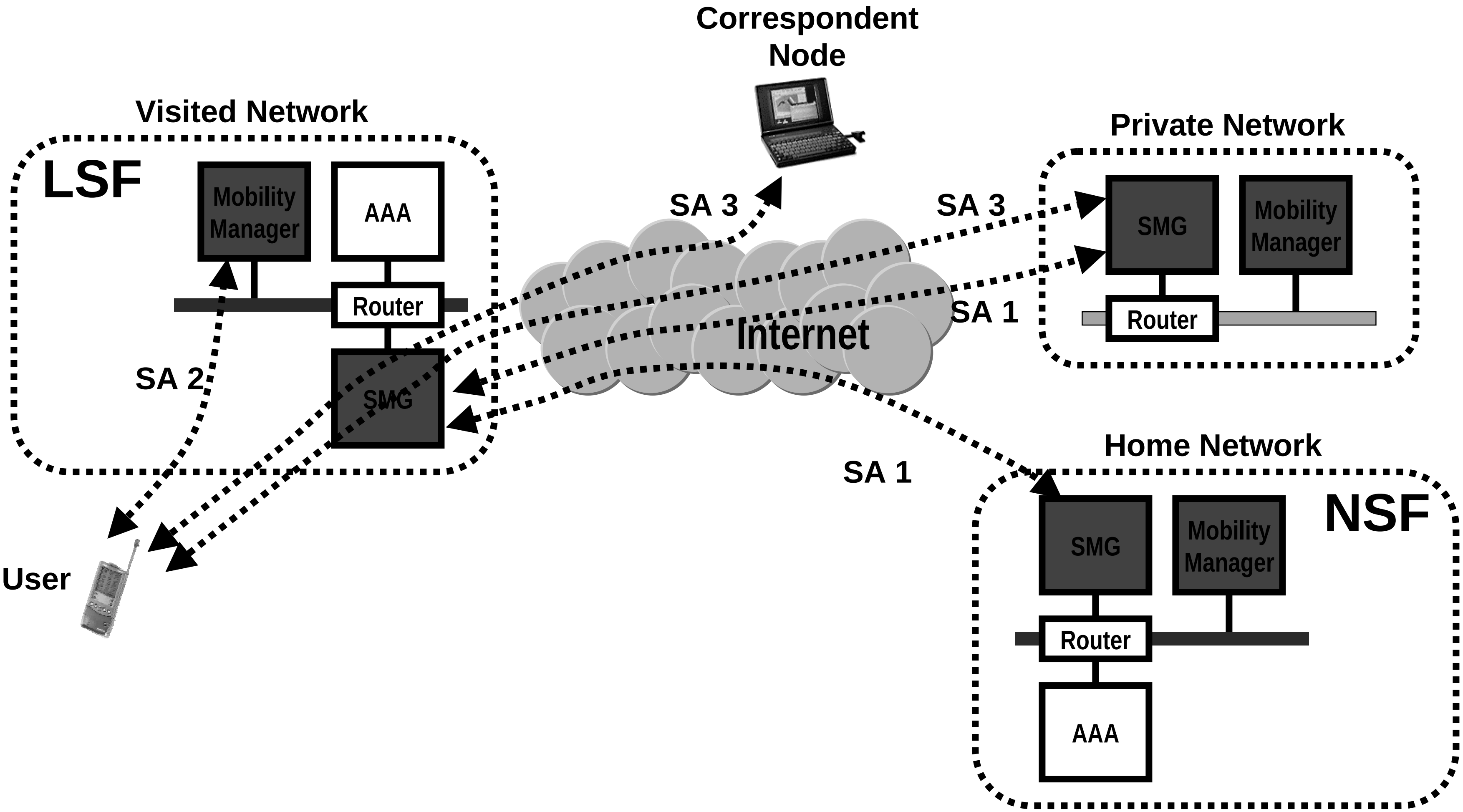
In the LSF:

- The DHCP server is used to assign local COAs to the terminals that access the network
- The DNS server in the LSF is used by the terminal for address resolution functions

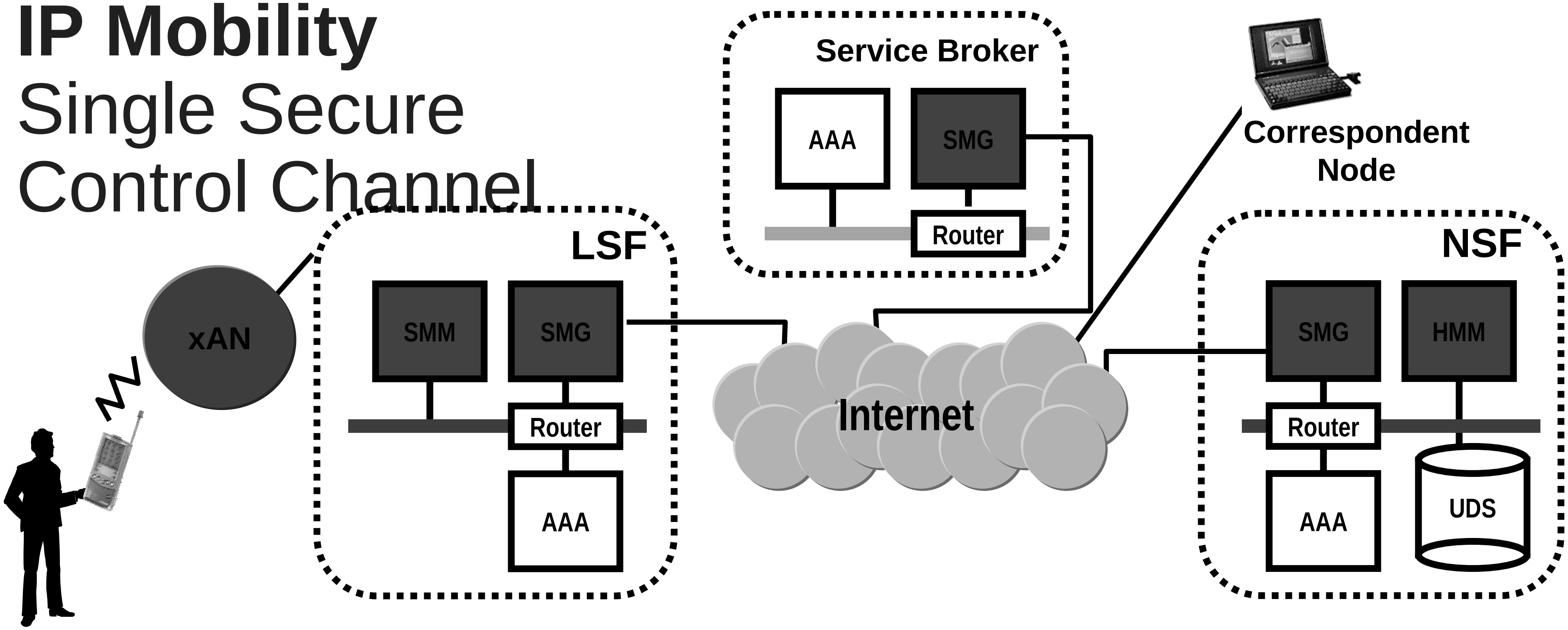
In the NSF:

- The DHCP server is used to assign temporary IP addresses to roaming mobile nodes that do not have configured (permanent) IP address
- The DNS server is updated with the terminal's allocated IP address by the DHCP server and with the terminal's COA by the Mobility Manager
- The Mobility Manager updates the location of the terminal in the UDS

IP Mobility
Security Associations

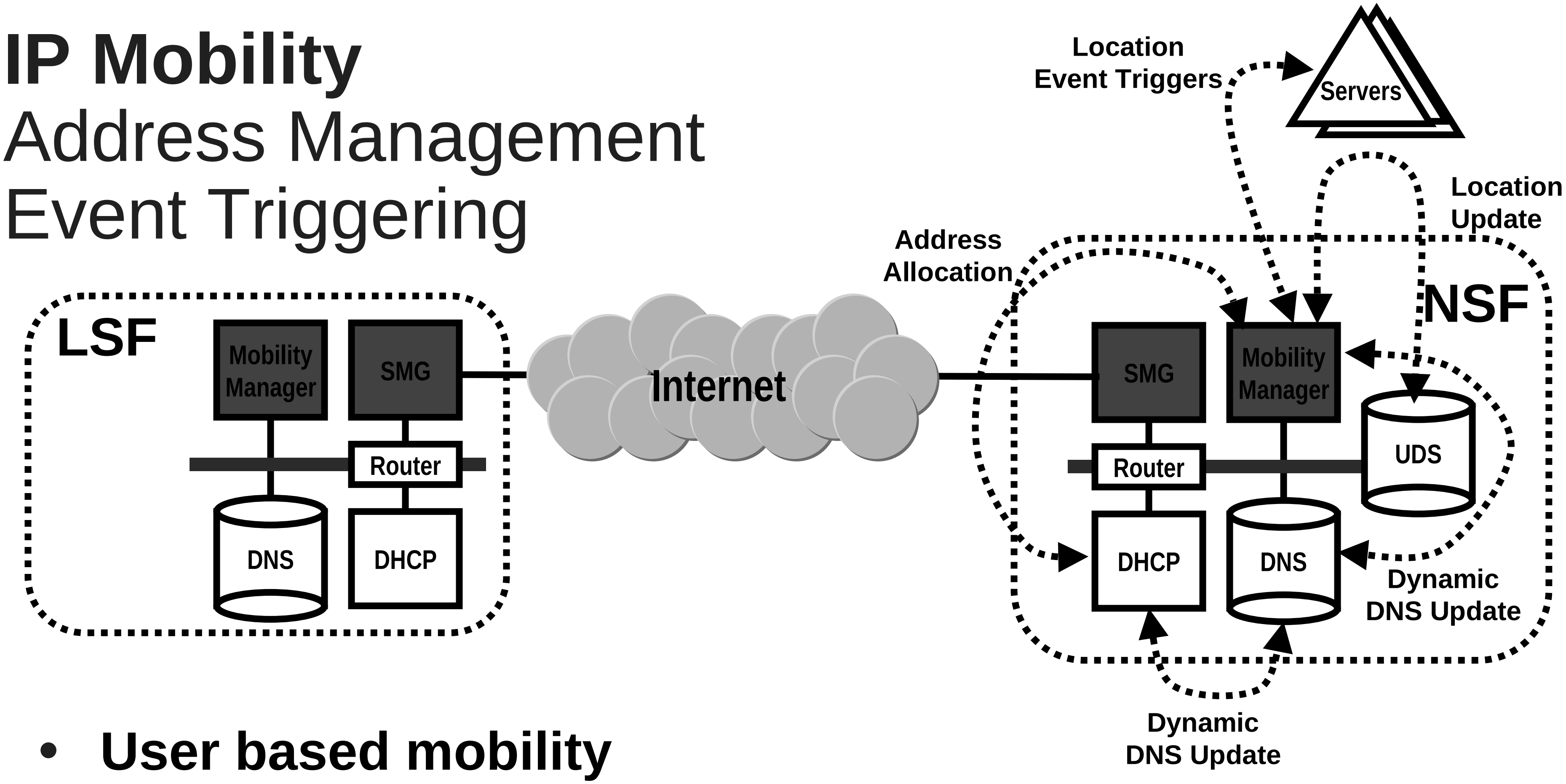


IP Mobility
Single Secure Control Channel



- **Single protocol for Mobility and AAA functions**
  - — AAA functions (Diameter based) are extended to include mobility functions
  - — NAI based routing relaxes the usage of IPv4 address space
- **Single tunnel between LSF and NSF entities through SMG**
  - — Service providers maintain only one secure tunnel
  - — All entities (AAA, UDS, SMM, HMM etc.) can communicate securely

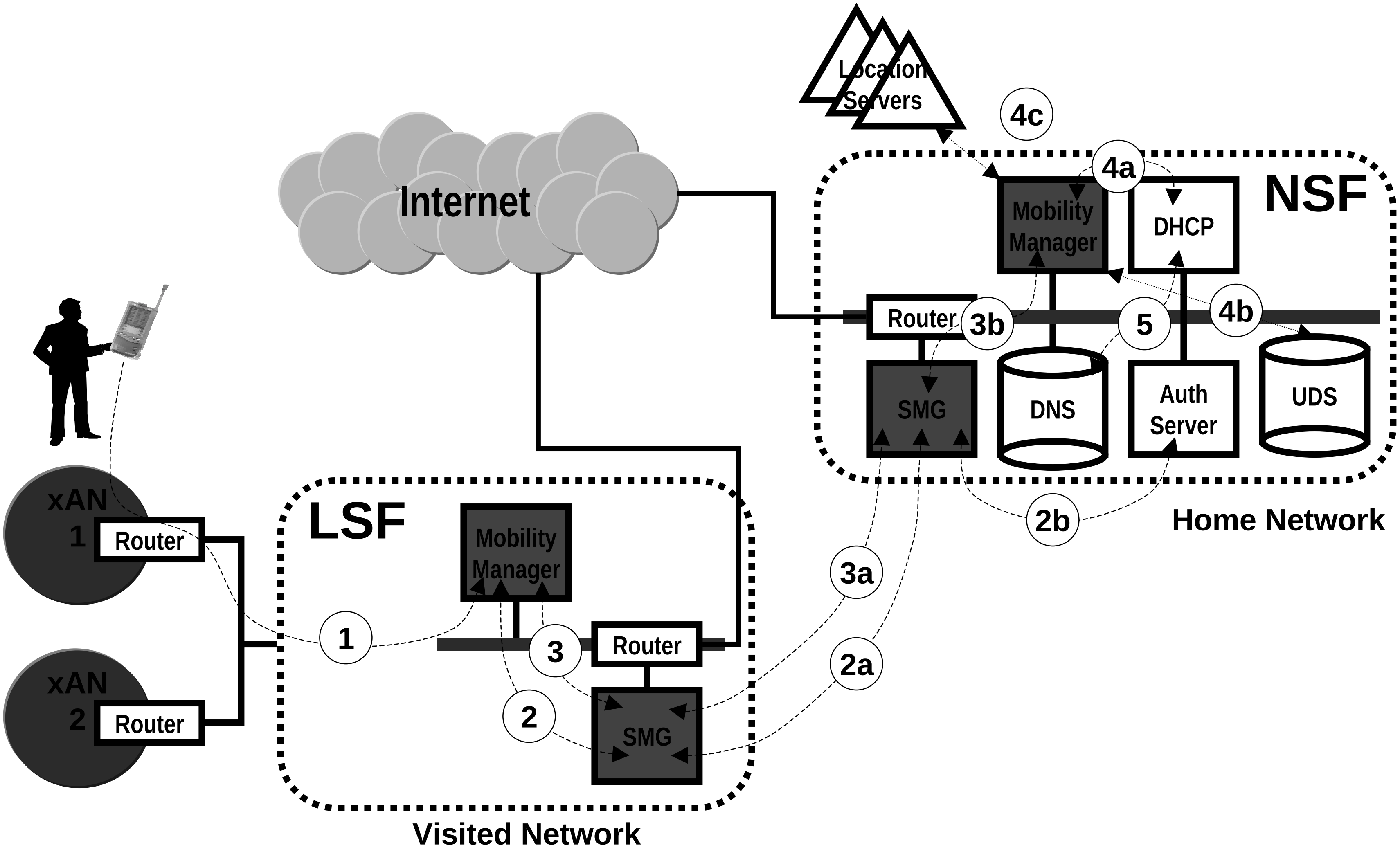
IP Mobility
Address Management
Event Triggering



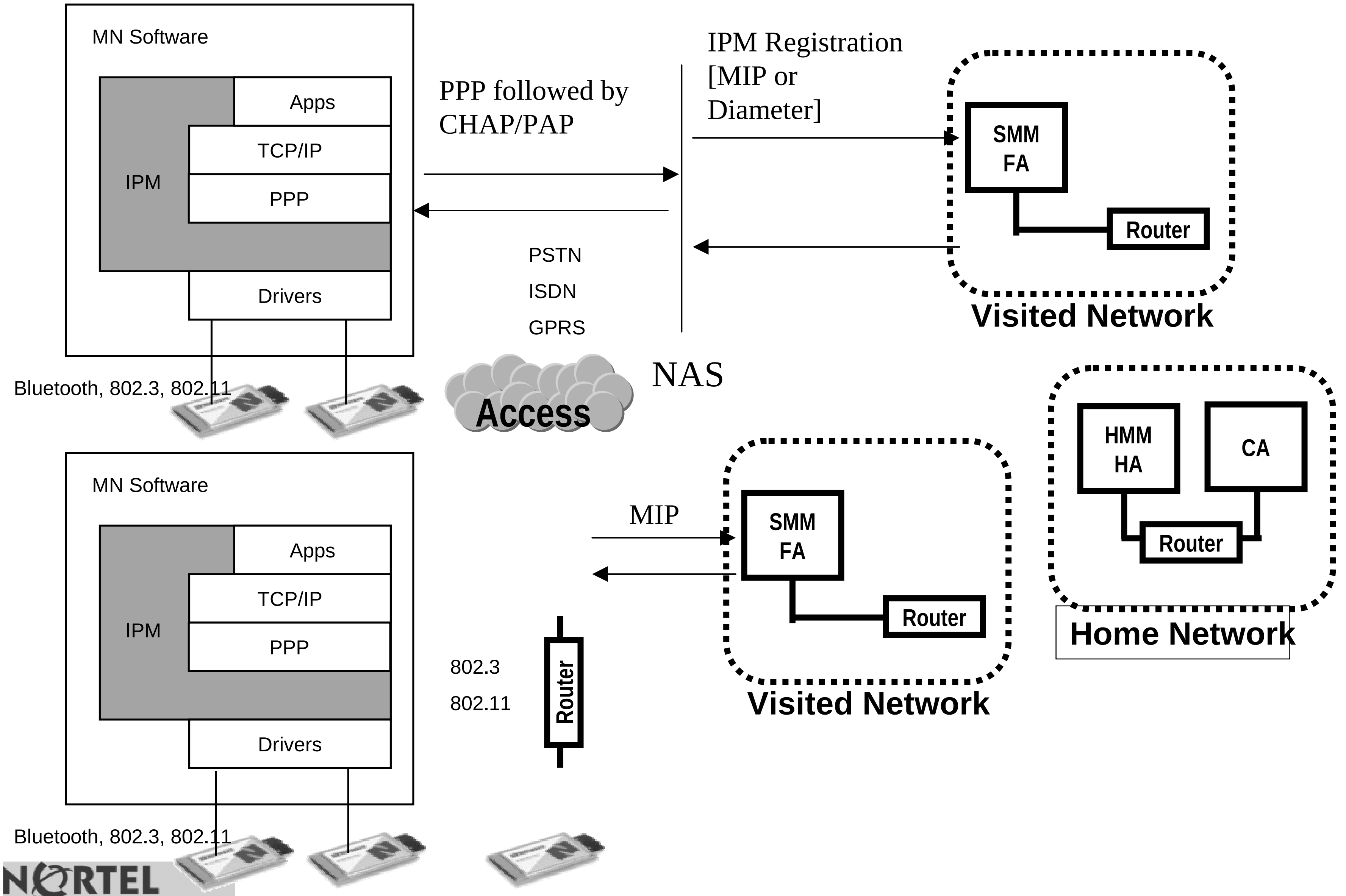
- **User based mobility**
  - — Dynamic allocation of IP addresses using NAI
  - — Integrated with DNS/DHCP
  - — Terminal based mobility supported
  - — Trigger for location based services

IP Mobility

Message Flows - Initial Registration

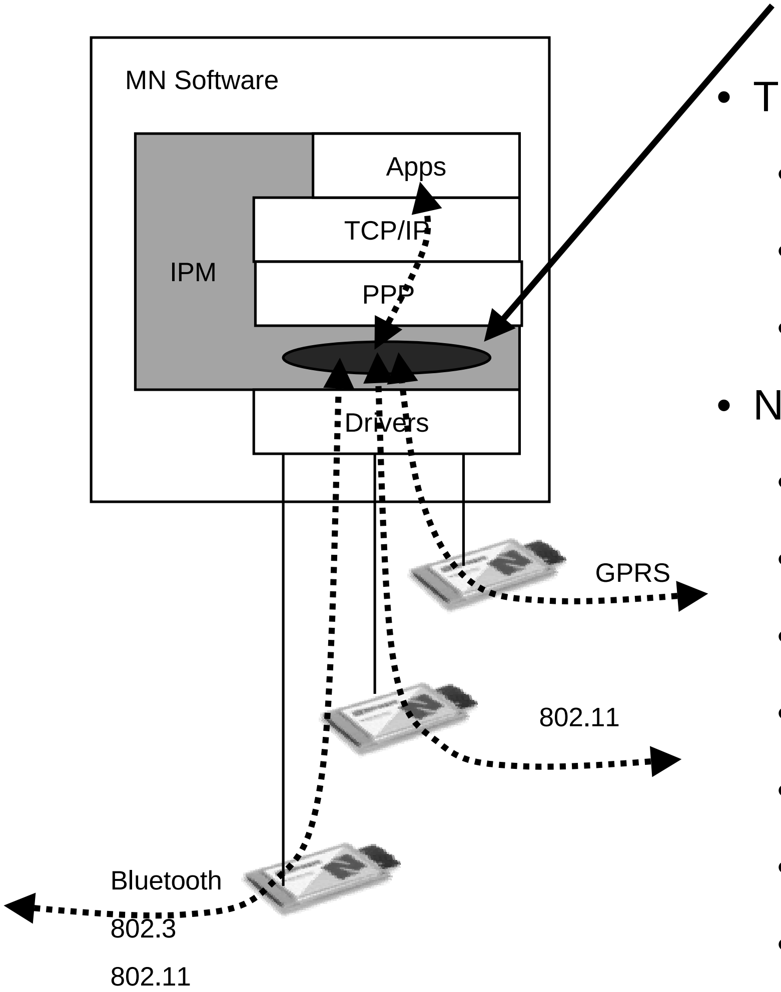


Registration with Other Access Networks



NORTEL NETWORKS

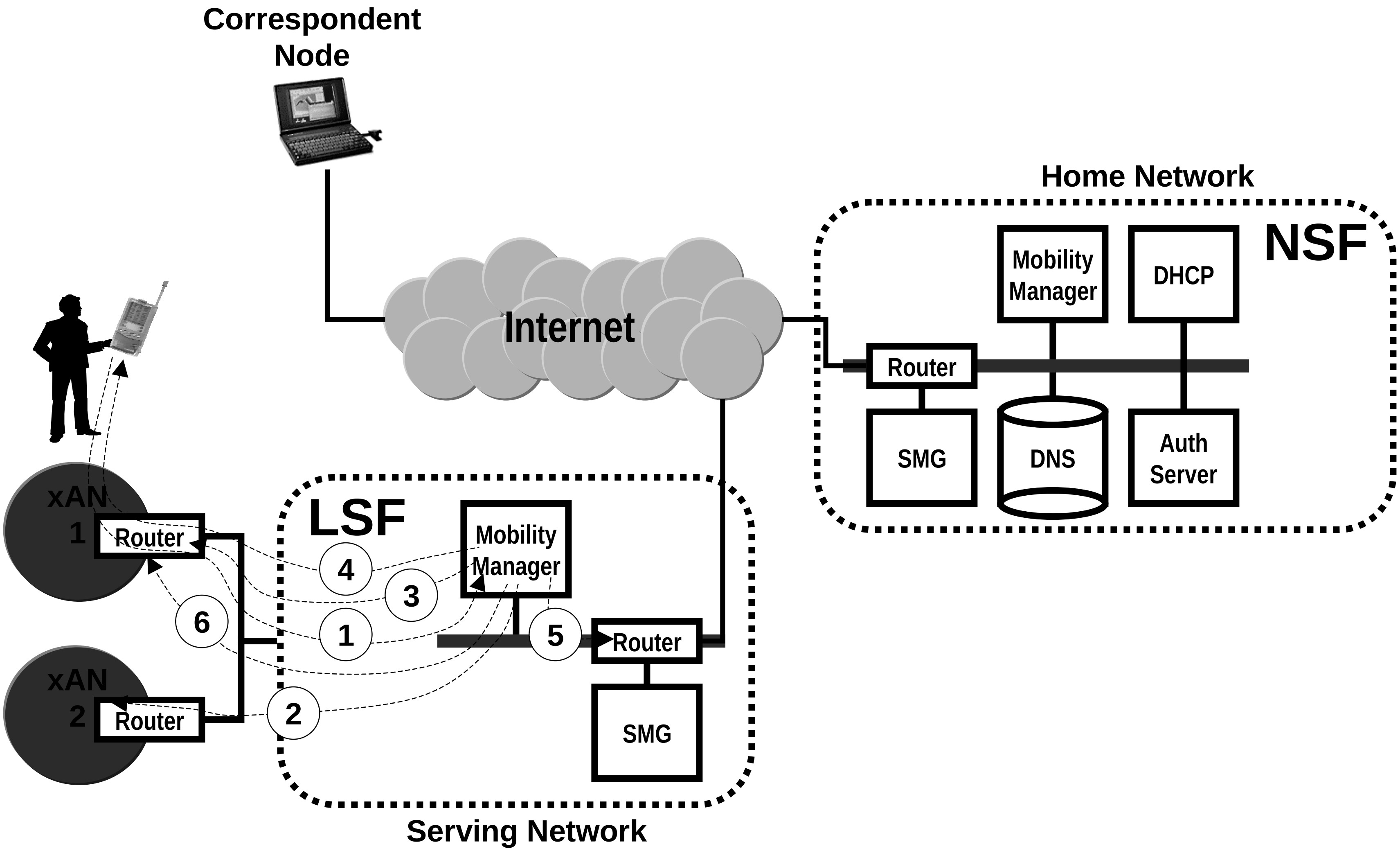
GPRS (and others) Wireless LAN Interworking



Mobile Node Arbitrator

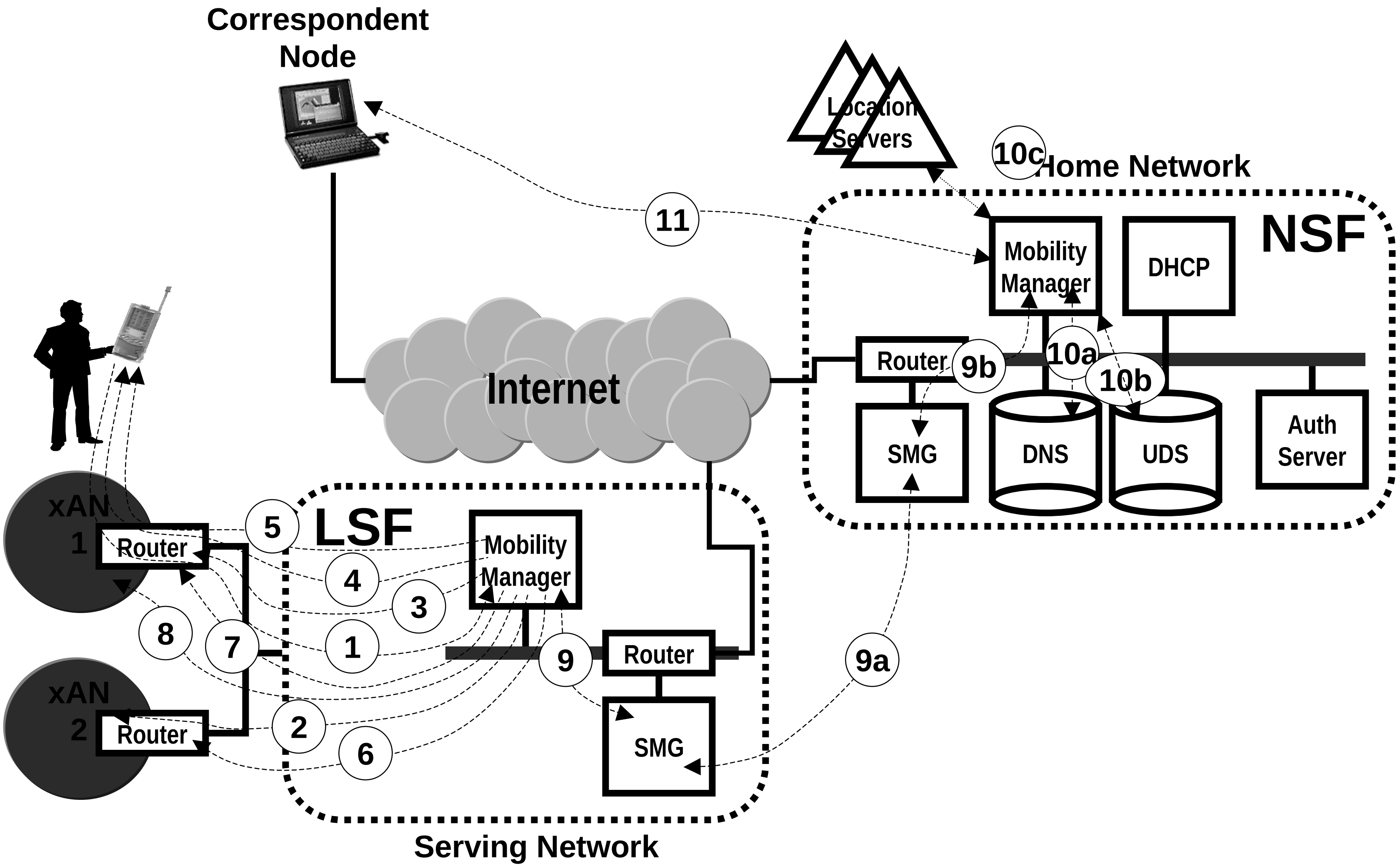
- Transparency between driver and IP layer
  - Tunneling and encapsulation
  - IP Address manipulation
  - Network point of attachment selection
- Network selection on
  - Default
  - Bandwidth
  - Cost
  - Signal Strength
  - BER
  - TOD
  - …

IP Mobility
Message Flows - Handoff (Same COA)

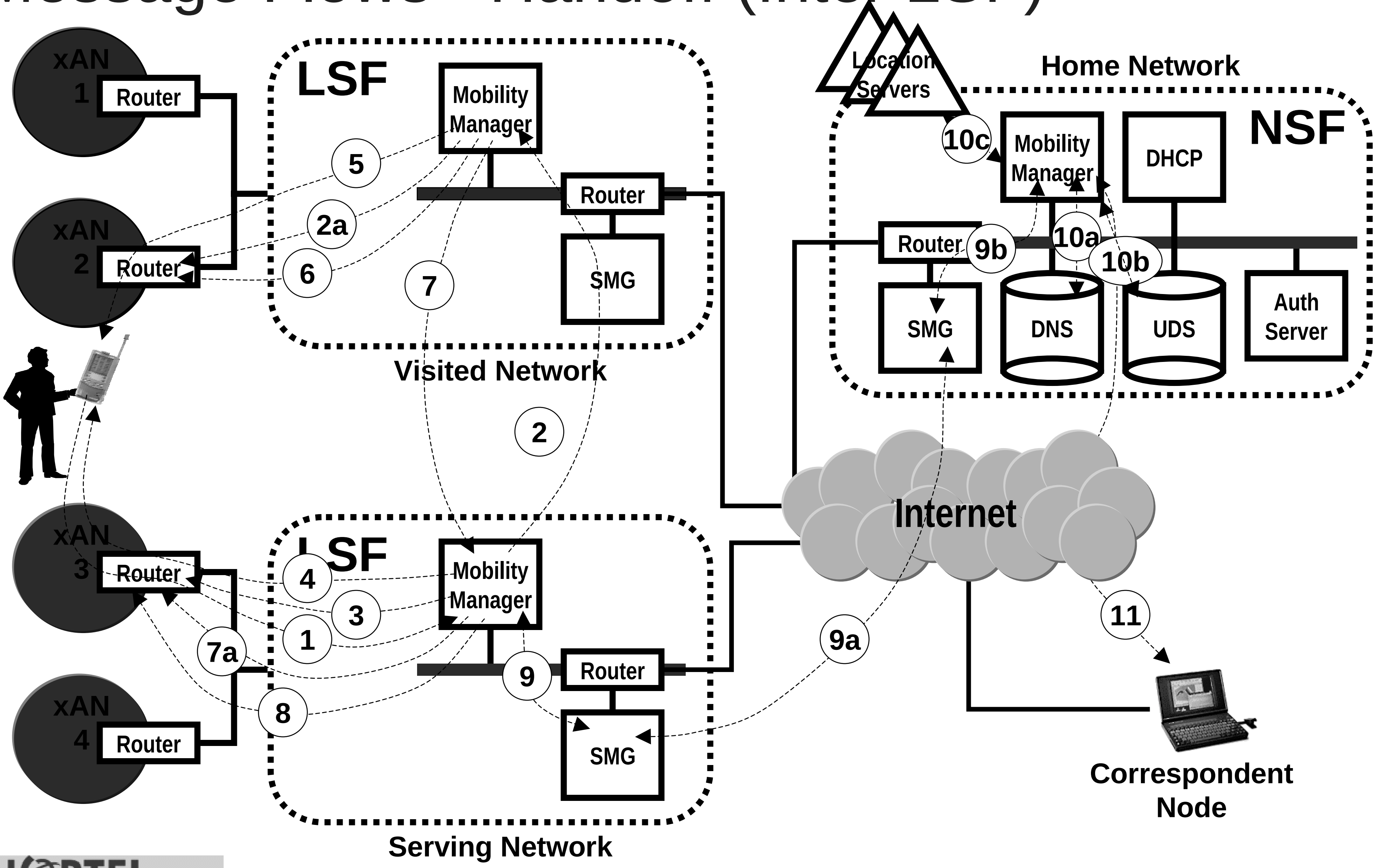


NORTEL NETWORKS

IP Mobility
Message Flows - Handoff (New COA)

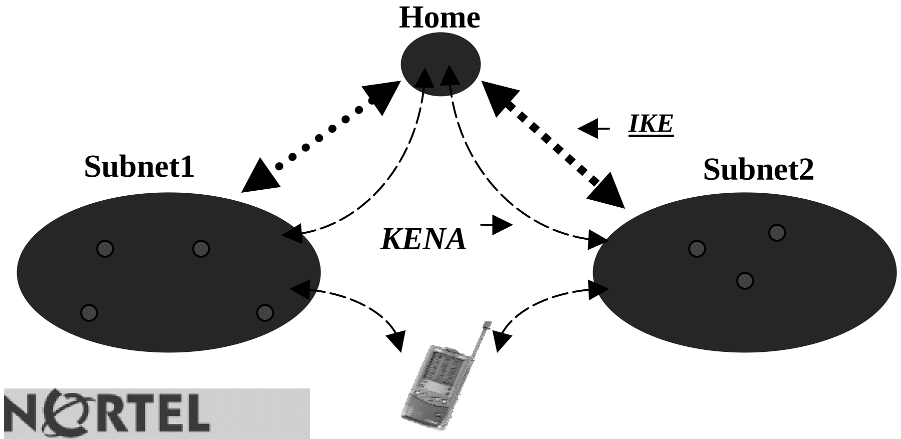


IP Mobility
Message Flows - Handoff (Inter LSF)



IP Mobility
Key Enabled Network Architecture (KENA)

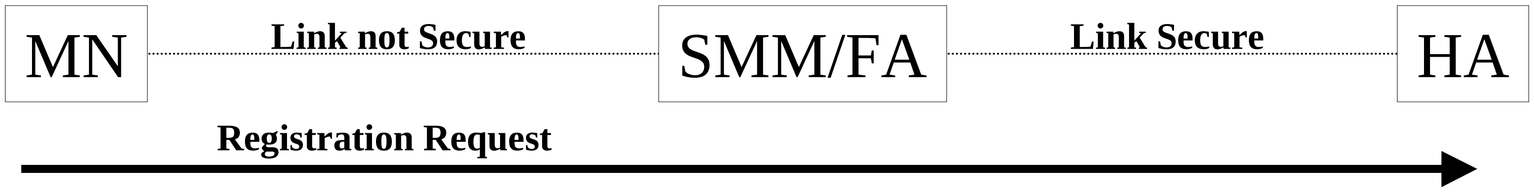
- **Fast security setup between two administrative domains**
  - one step and one process vs. two steps and four messages
- **Real time sensitive and proactive key distribution**
  - Secure path is setup prior to need, I.e, during handoff
- **Multitude of nodes in a sub-network share single security relationship**
  - Distributed vs. point-to-point
- **Security on per user (per communication channel) basis**
  - Also supports per session basis
- **Centralized key generation and distribution**
- **Complements IKE and ISAKMP**



- **Use IKE/ISAKMP for Primary [Home - Subnetwork] security**
- **Use KENA for Secondary [Session based] security**

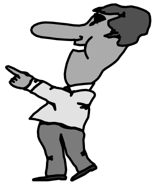
IP Mobility
KENA over Mobile IP

Assumptions
- Shared Secret or Asymmetric Keys between MN and Home
- Secure path between the SMM/FA and Home

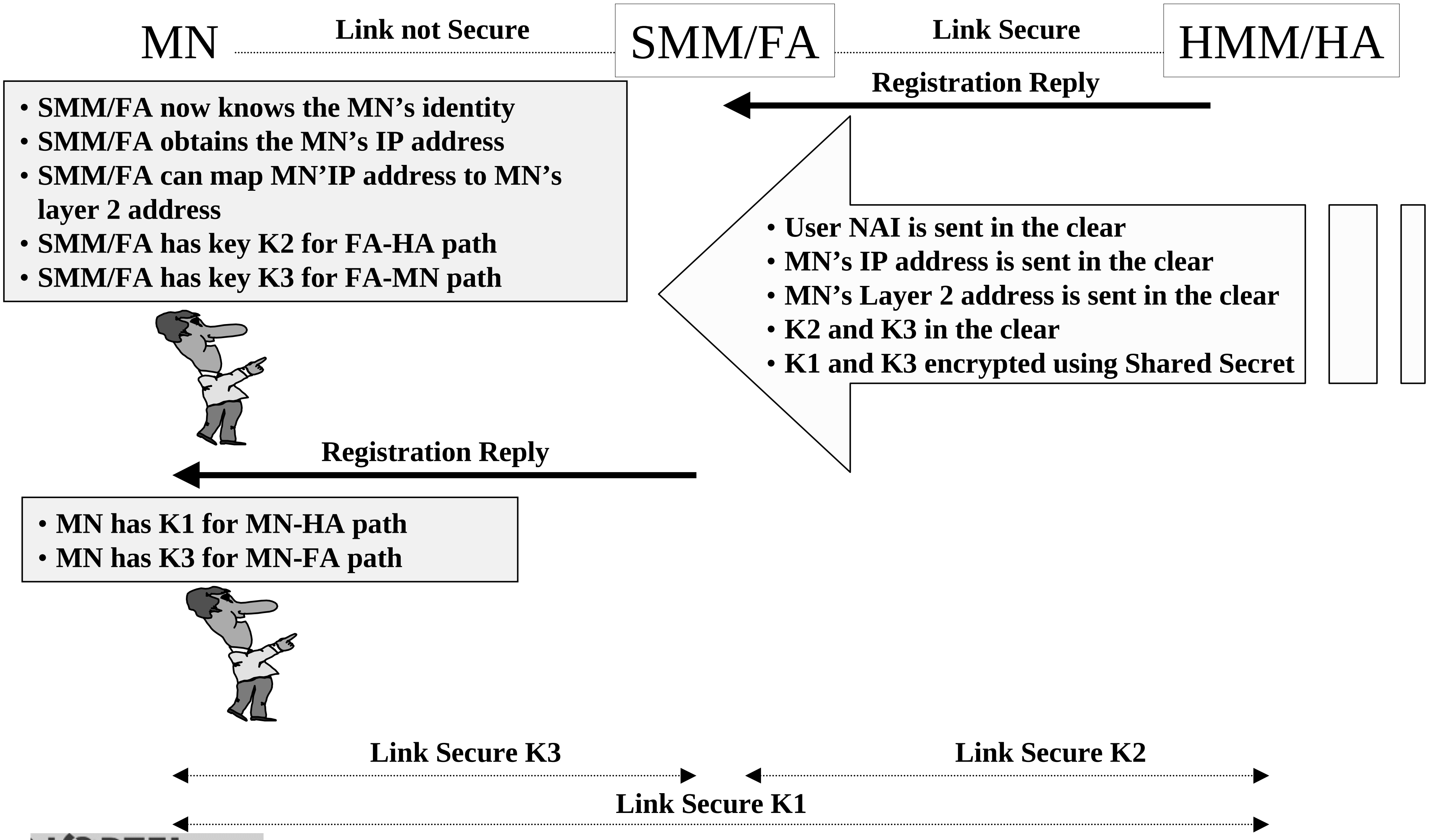


- Home IP address is blank
- HMM/HA's IP address is in the clear
- User NAI is encrypted
- MN's Layer 2 address is sent in the clear

We achieve PRIVACY and Authentication



IP Mobility
KENA over Mobile IP Continued



MN

Link not Secure

SMM/FA

Link Secure

HMM/HA

Registration Reply

- SMM/FA now knows the MN’s identity
- SMM/FA obtains the MN’s IP address
- SMM/FA can map MN’IP address to MN’s layer 2 address
- SMM/FA has key K2 for FA-HA path
- SMM/FA has key K3 for FA-MN path

- User NAI is sent in the clear
- MN’s IP address is sent in the clear
- MN’s Layer 2 address is sent in the clear
- K2 and K3 in the clear
- K1 and K3 encrypted using Shared Secret

Registration Reply

- MN has K1 for MN-HA path
- MN has K3 for MN-FA path

Link Secure K3

Link Secure K2

Link Secure K1

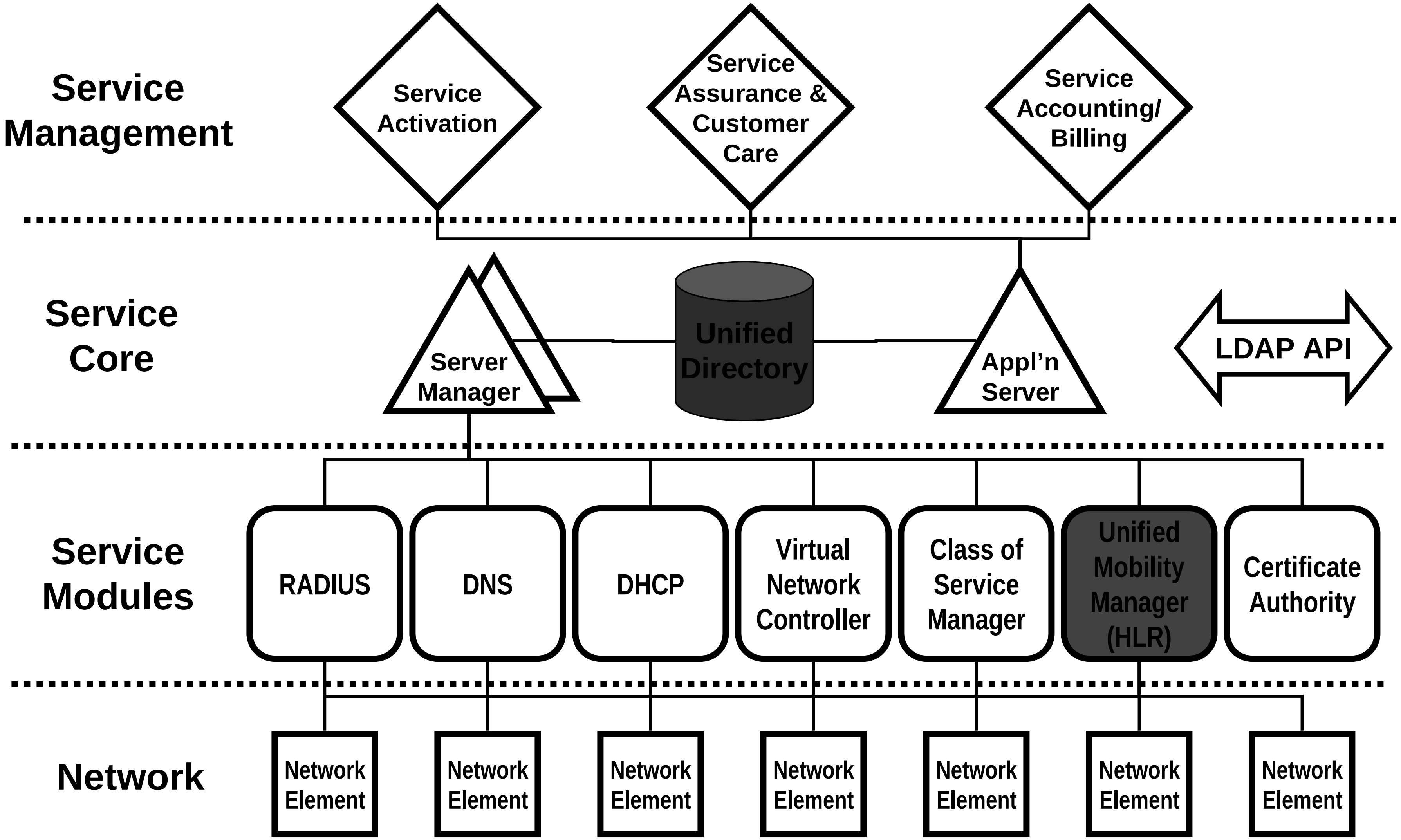
IP Mobility
KENA Accomplishes

- Mobile IP AAA Key Distribution Requirements
- MN and FA authentication
- Protection of user privacy until FA is authorized
- Distribution of keys per MN's registration session
- Facilitation of Layer 3 encryption
- Central authority for key generation and distribution
- Enhances smooth handoff through proactive key generation and distribution

Unified Directory Services
Key Architectural Principles

- **Carrier-focused, directory schema for profile management (end-users and served networks)**
- **Virtual grouping/context management across all NEs**
- **Open and extensible directory schema enabling third-party integration**
- **Integration with leading customer care and billing systems**
- **Support carrier-grade requirements for scaleability and availability**
- **Allow functionality to be deployed as required by network operator (modularity)**

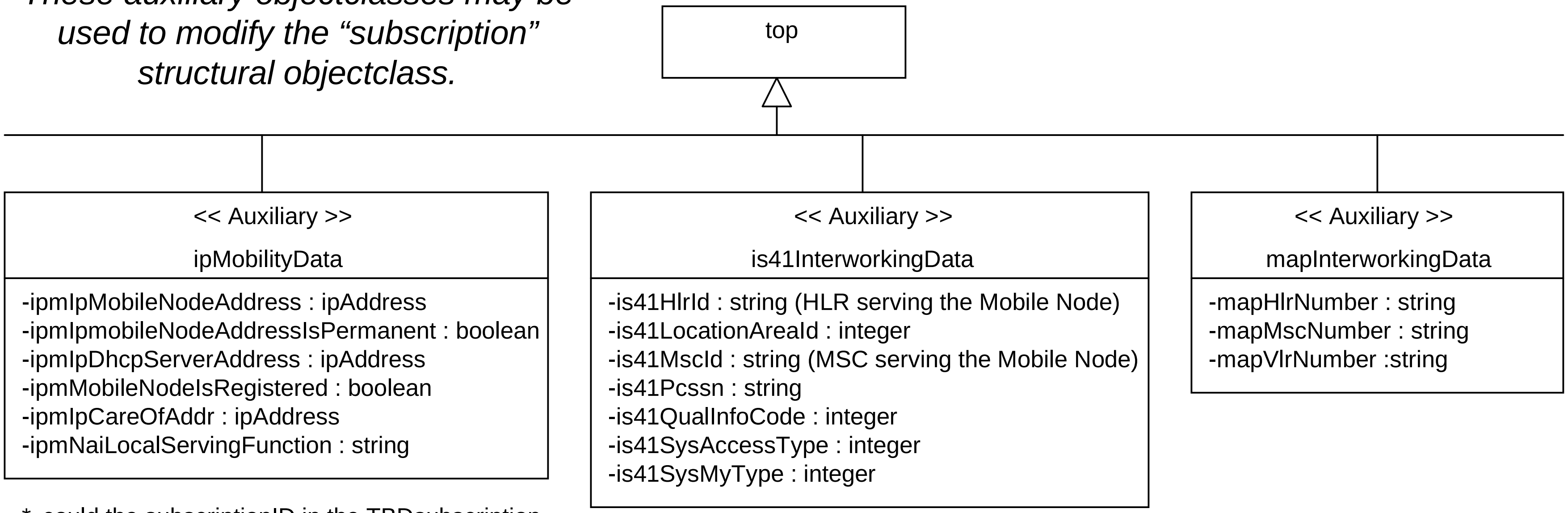
Unified Directory Services
Architecture Framework



NORTEL NETWORKS

Common Schema/DIT Definition

These auxiliary objectclasses may be used to modify the “subscription” structural objectclass.



top

<< Auxiliary >>

ipMobilityData

-ipmIpMobileNodeAddress : ipAddress
-ipmIpmobileNodeAddressIsPermanent : boolean
-ipmIpDhcpServerAddress : ipAddress
-ipmMobileNodeIsRegistered : boolean
-ipmIpCareOfAddr : ipAddress
-ipmNaiLocalServingFunction : string

<< Auxiliary >>

is41InterworkingData

-is41HlrId : string (HLR serving the Mobile Node)
-is41LocationAreaId : integer
-is41MscId : string (MSC serving the Mobile Node)
-is41Pcssn : string
-is41QualInfoCode : integer
-is41SysAccessType : integer
-is41SysMyType : integer

<< Auxiliary >>

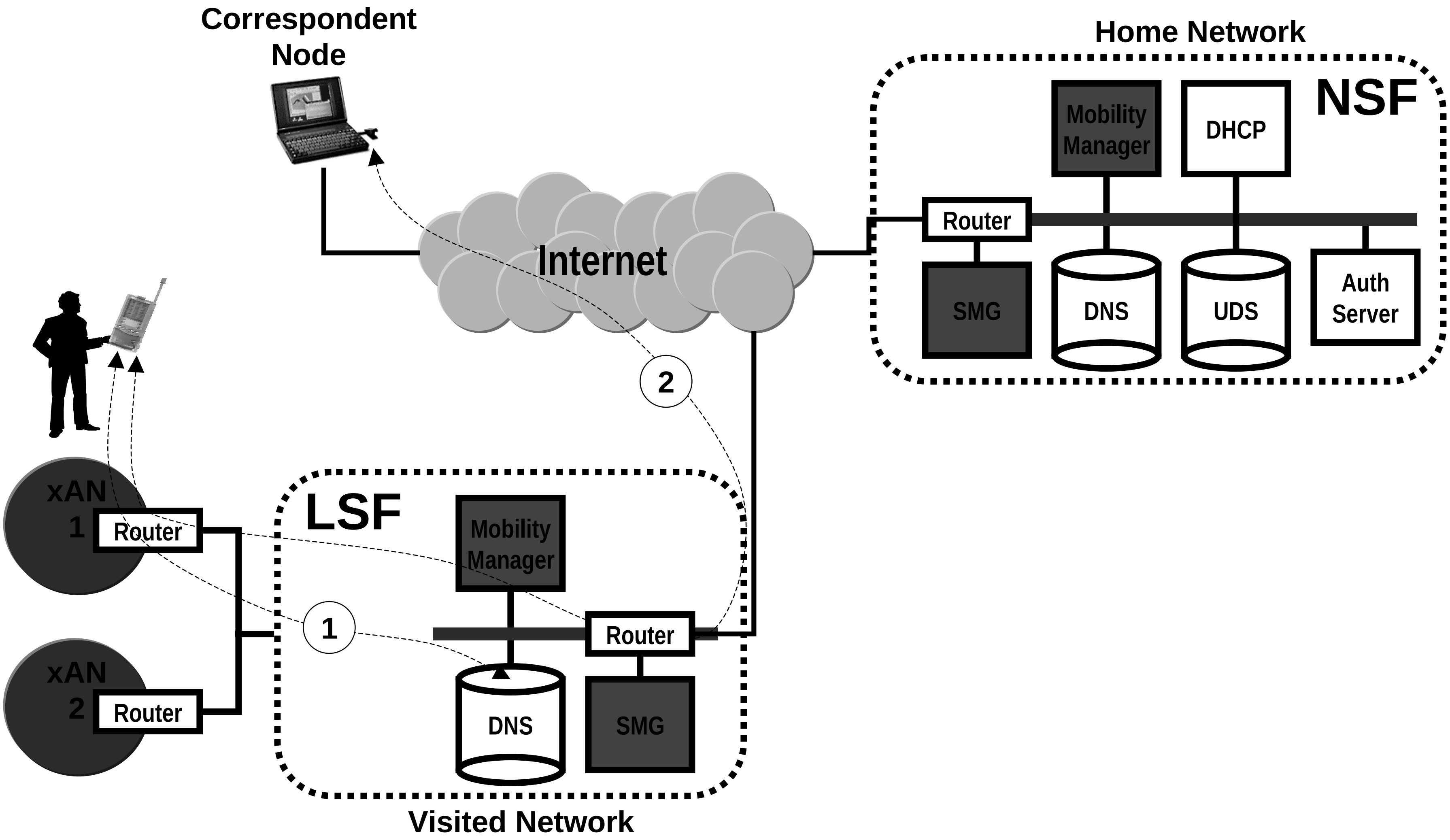
mapInterworkingData

-mapHlrNumber : string
-mapMscNumber : string
-mapVlrNumber :string

* could the subscriptionID in the TBDsubscription entry be the NAI for the subscription?

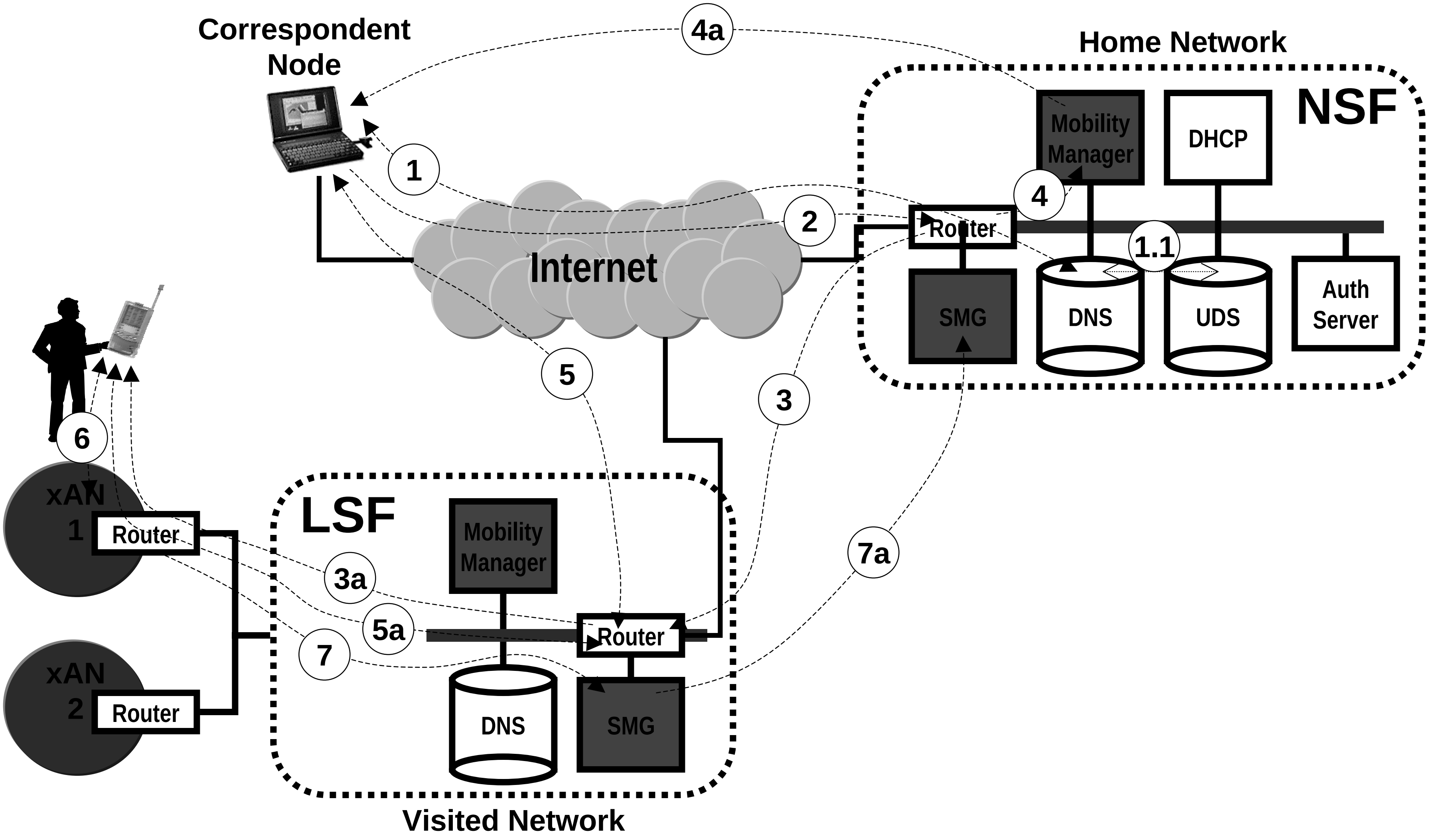
If there are really multiple terminals under each TBDsubscription, then it’s possible this and other auxiliary object classes must modify the structural terminal entry as opposed to the TBDsubscription entry.

Call and Session Management
Message Flows - Mobile Initiated Session

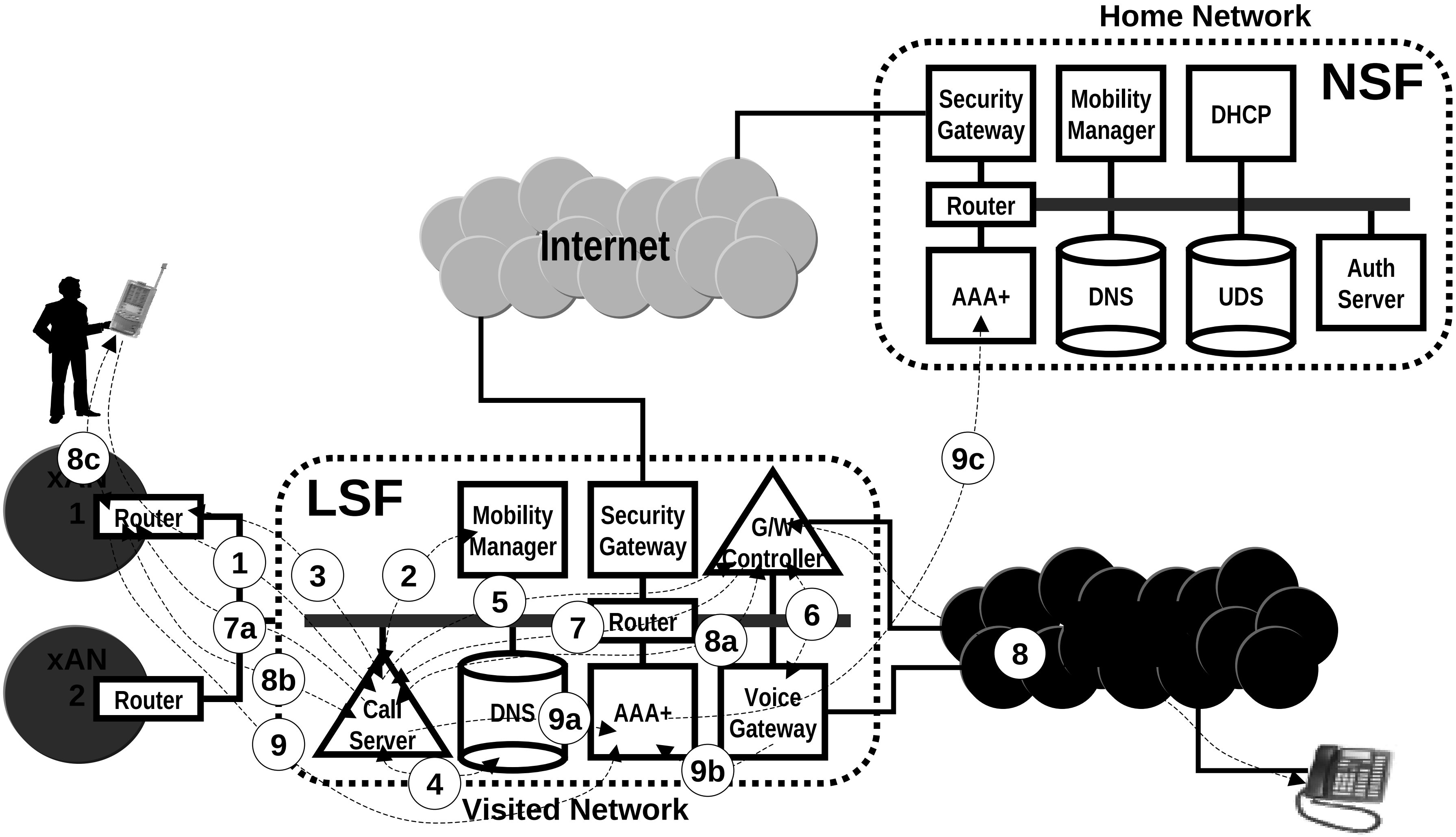


Call and Session Management

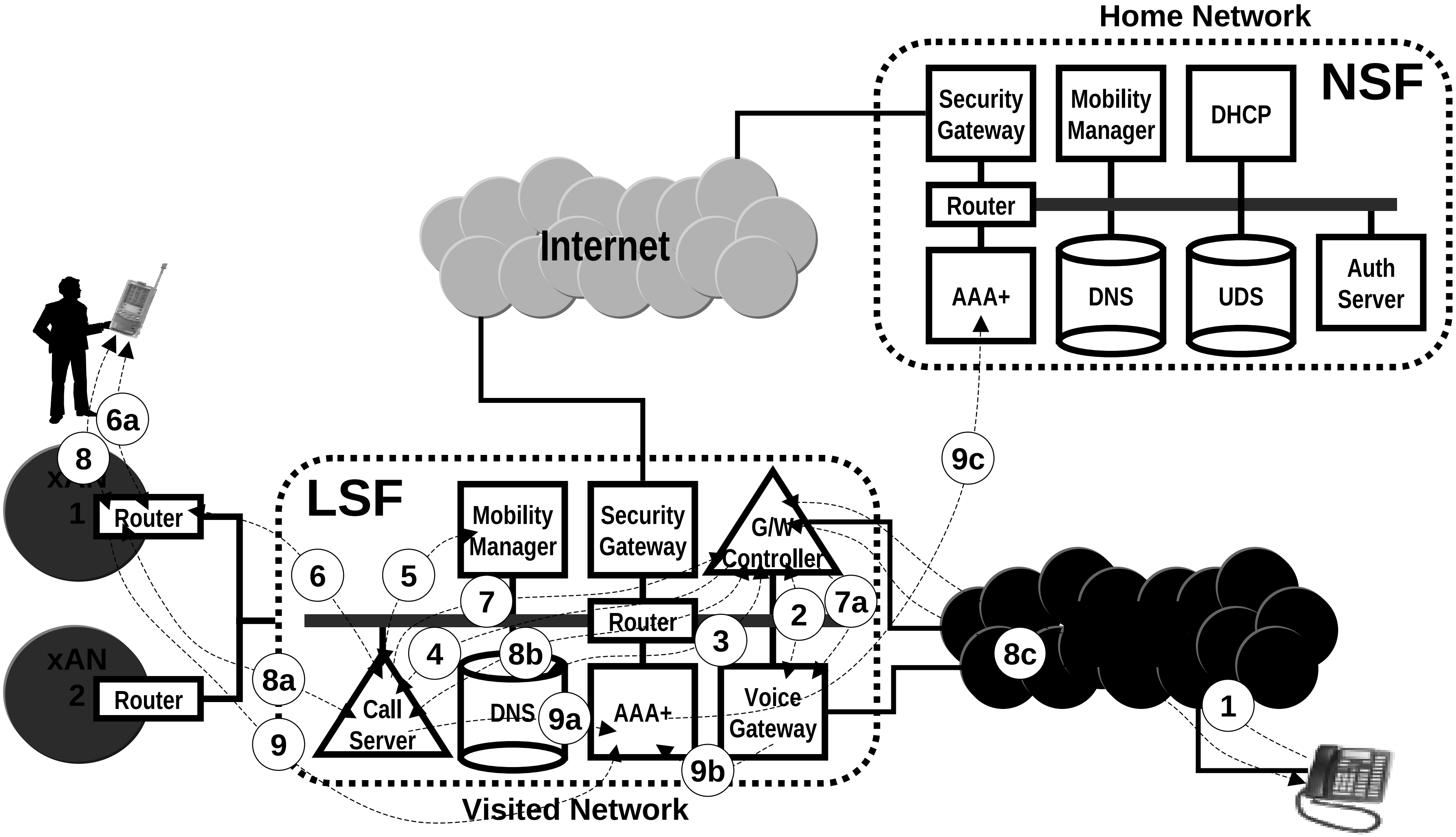
Message Flows - Mobile Terminated Session



Call and Session Management
Message Flows - Mobile Initiated Call



Call and Session Management
Message Flows - Mobile Terminated Call



Conclusions

- **System approach makes the Internet fully mobile**
  - — Security, Trusted Relationships, Business Relationships
  - — Directories, Address Management, Address Resolution
  - — Heterogeneous Access, MAC layer independence
- **New “Mobile Client” Paradigm**
  - — Not just a phone – rather an information appliance
  - — Small, Cheap, Very Powerful, …, Soon!
- **Mobile Applications already exist**
  - — Heterogeneous Applications, TCP/IP layer independence
  - — Network Aware applications next step