Mobiarch 2007 - Kyoto, August 27th, 2007

Embedding Identity in Mobile Environments

Alfredo Matos <alfredo.matos@av.it.pt>

Susana Sargento <ssargento@det.ua.pt>

Rui L. Aguiar <ruilaa@ua.pt>

INSTITUIÇÕES ASSOCIADAS:

INSTITUTO SUPERIOR TÉCNICO

Faculdade de Ciências e Tecnologia da Universidade de Coimbra

universidade de aveiro

PT Inovação

SIEMENS Communications

instituto de telecomunicações

creating and sharing knowledge for telecommunications

Overview

- Motivation
- Architecture
  - Identity Referral and Bindings
  - Terminal and Network Support
- Detailed Operations
  - Bootstrap and Handover
- Identity Based Mobility
- Privacy and Multiple Identities
- Benefits and Drawbacks
- Conclusion and Future Work

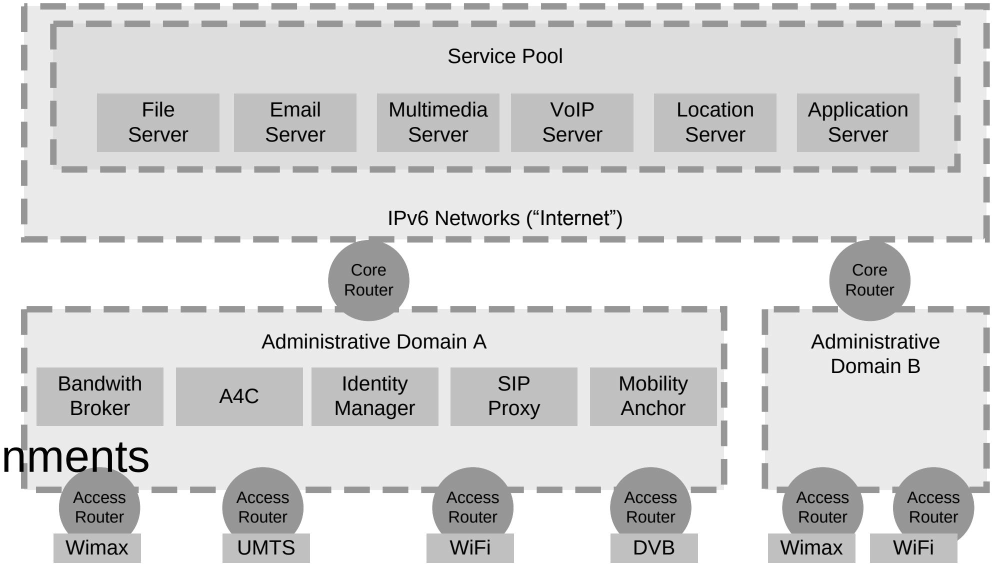
Motivation

- Next Generation Networks
  - Complexity
  - Multiple protocols and services
  - Mobility
  - Security
- “talks of” User-Centric Architectures
  - But lack of user oriented approaches
- Identity has been….
  - a second class citizen (up until now)
  - but taking strong steroids by web 2.0
  - and thus facing growth problems (passwords, identity theft, etc.)

THIS IS NOT ENOUGH

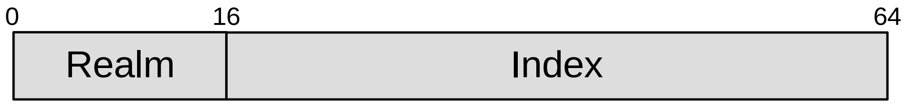
NGN Identity-biased Architecture

- Several Administrative domains
- Different Access Technologies
  - WiFi, UMTS, DVB
- Mobility
  - MIPv6, HIP, SIP
- A4C
  - Restricted and controlled environments
- Bandwidth Brokers
  - Restricted QoS environments
- Identity Managers
  - Operator power and user driven identity
- Services
  - Multiple user oriented services: VoIP, Location, Multimedia, File, Mail...



Identity Referral – the Glue

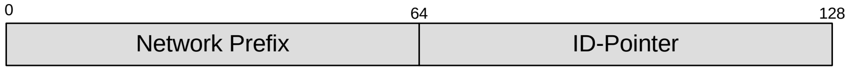
- Identity Manager
  - Identity Information
  - User oriented policies
  - Identity Namespace
- Identity Manager and different protocols
  - Bringing Identity to the network level
  - Implicit identity referral
  - Compatibility
- ID-Pointer
  - 64 bit public Identifier
  - Realm – the Identity Manager Domain
  - Index – information index on the Identity Manager Database
  - Easily resolvable



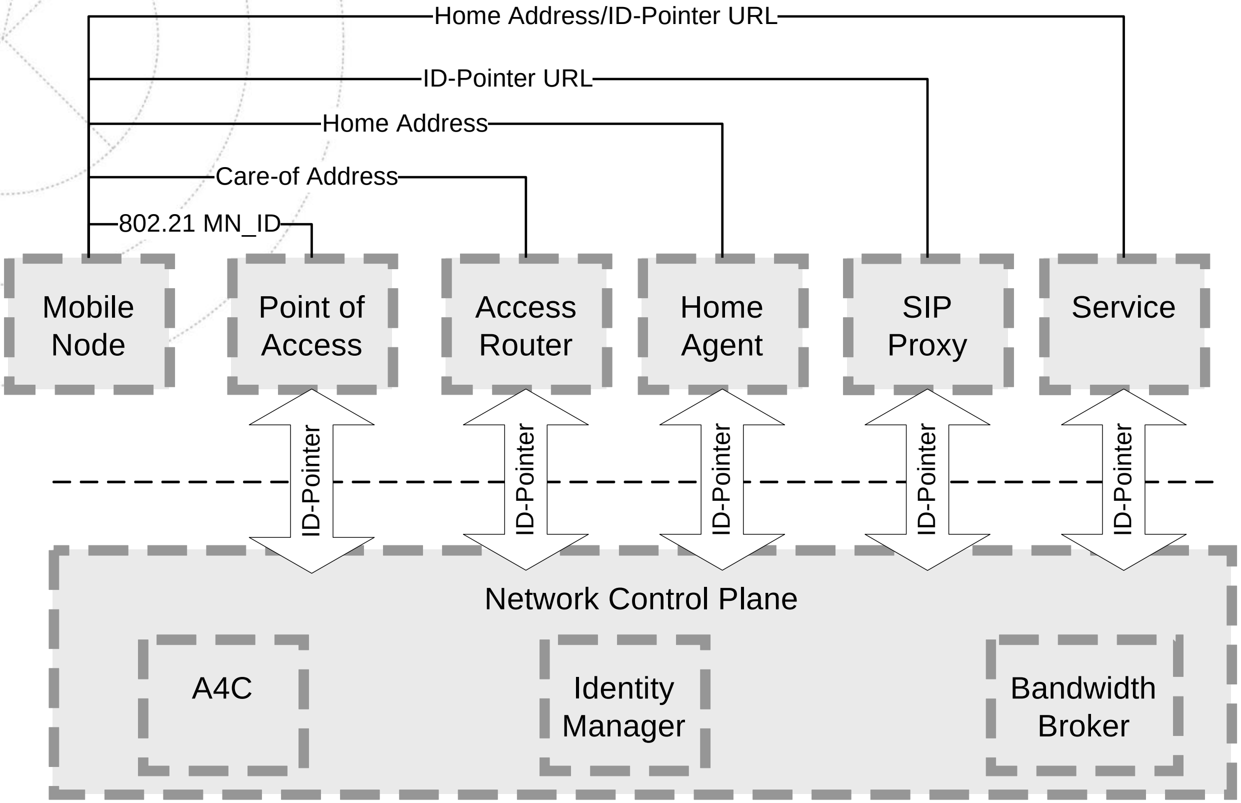
Identity Bindings (I)

- Implicit
  - Embedded ID-Pointer
- Explicit
  - Identifier mapping to an ID-Pointer on a database

- Network Bindings
  - Link Layer
    - 802.21 MN_ID or PANA ID
  - Network Layer
    - ID-Pointer in the IP Address
    - MIPv6 CoA
  - Transport Layer
    - ID-Pointer in the MIPv6 HoA
  - Application Layer
    - URI mapped to ID-Pointer

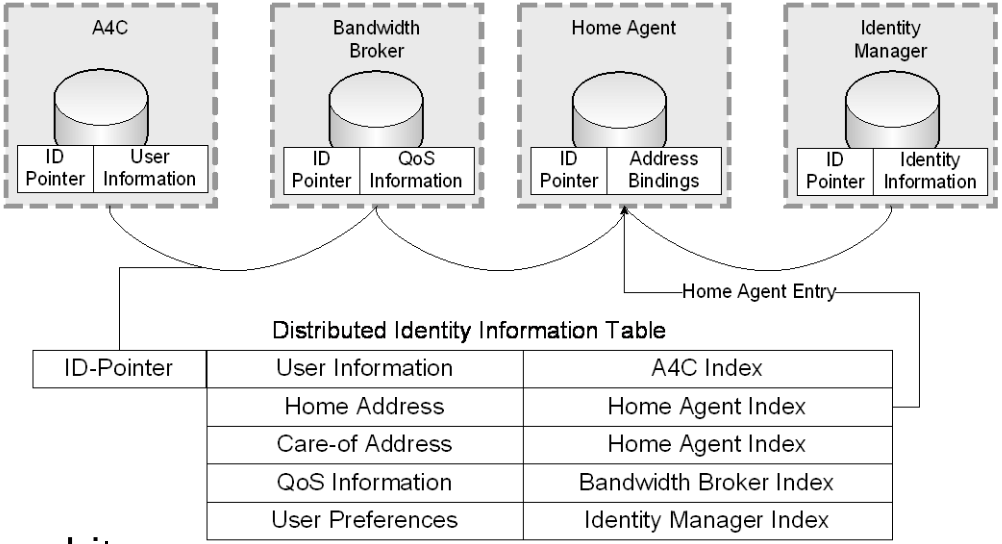


Identity Bindings (II)



Networks: Support

- Identity Oriented Network Distributed Database
  - Distributed Information
  - Common access methods
    - ID-Pointer
  - Common storage index
    - ID-Pointer



Distributed Identity Information Table

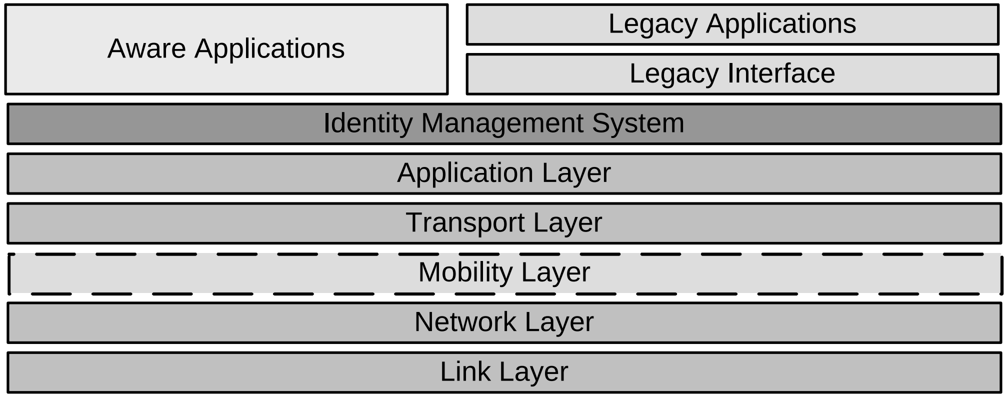
ID-Pointer	User Information	A4C Index
	Home Address	Home Agent Index
	Care-of Address	Home Agent Index
	QoS Information	Bandwidth Broker Index
	User Preferences	Identity Manager Index

- Distributed User View
  - Sum of all distributed information bits
  - Reachable with an ID-Pointer and the right permission
  - Strong access control

Terminals: Support and features

- Control Plane
  - New Identity Management Layer
    - Identity is a control plane task
  - Identity aware applications
  - Legacy interfaces
- Data Plane
  - Preserved

- Mobility
  - New paradigm for control
  - Identity Layer
    - Point of decision
    - Intelligence
  - Mobility Protocols
    - Signaling
  - Common Mobility Interface
    - Triggers
    - APIs



Aware Applications

Legacy Applications

Legacy Interface

Identity Management System

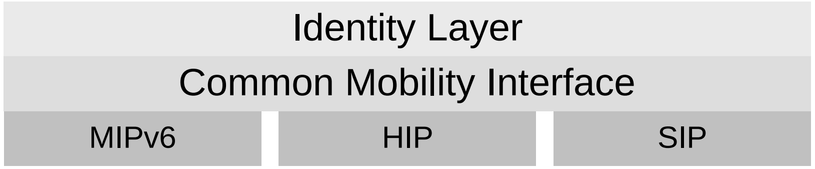
Application Layer

Transport Layer

Mobility Layer

Network Layer

Link Layer



Identity Layer

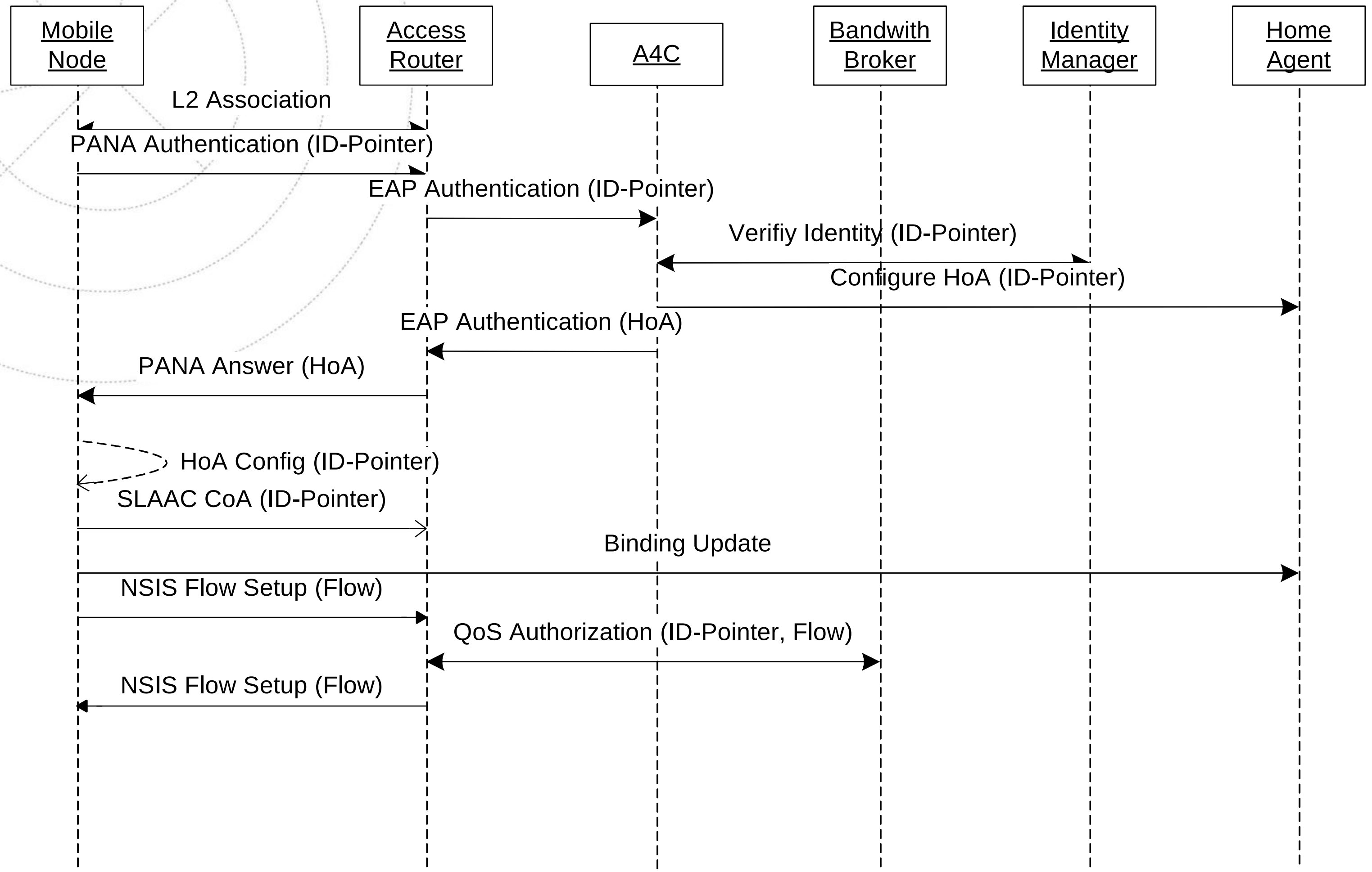
Common Mobility Interface

MIPv6

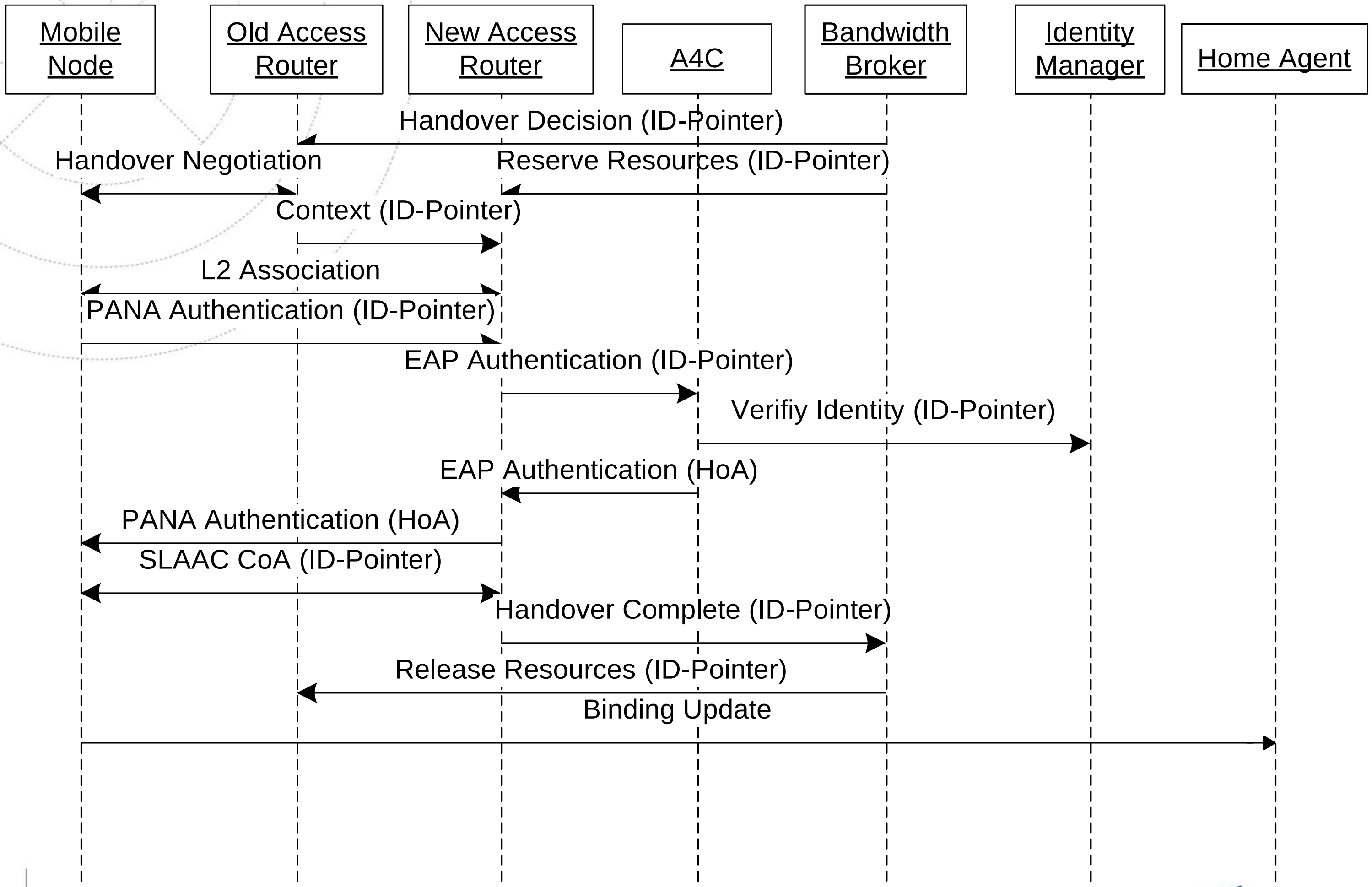
HIP

SIP

Example: Bootstrap



Example: Handover


Mobile Node
Old Access Router
New Access Router
A4C
Bandwidth Broker
Identity Manager
Home Agent
Handover Decision (ID-Pointer)
Handover Negotiation
Reserve Resources (ID-Pointer)
Context (ID-Pointer)
L2 Association
PANA Authentication (ID-Pointer)
EAP Authentication (ID-Pointer)
Verifiy Identity (ID-Pointer)
EAP Authentication (HoA)
PANA Authentication (HoA)
SLAAC CoA (ID-Pointer)
Handover Complete (ID-Pointer)
Release Resources (ID-Pointer)
Binding Update

Results in:

Identity Based Mobility

- Consistent Approach across the network
  - Addresses change
  - ID-Pointer does not change
  - Update ONLY mobility tables
    - not everything else: triggers and referrals are consistent.
- Modularized mobility
  - Control is in the identity layer
  - Identifiers are embedded in the protocols and remain constant
    - Pick your own protocol
- New paradigms
  - Addresses don’t move, Entities do.
  - Can be decoupled from the terminal
  - Mobility between terminals
  - Multiple identities or users in the same terminal

IdBM Privacy and Multiple Identities

- Identifiers raise privacy issues
  - Identity related information in addressing structures
  - Resolvable pointers
  - Passive listeners can reach identity information
  - Strong security is required
    - Authentication for requesters
    - Non-public user information only allowed after the authentication
    - Multi-tier access control
- Cross Layer Identifiers raise linkability issues
  - More actions under the same identifiers
  - Higher probability of correlation
  - More security required
    - Per layer encryption hides upper layer identifiers

Benefits

- Cross-layer and cross-protocol integration
  - Distributed database model with consistent indexes
- Not bound by specific protocol Identifiers
  - Distributed meta-system
- Different addresses, same Identity
  - Simplification of network processes
- Simpler user profiles
  - Identity is not the profile
  - Different information exists in different places under the same identity
- Abstraction Layer enables access
  - Larger information set
  - Same access means
  - User-centric paradigms
- Better APIs
  - Abstraction layer
  - User-centric software
- Legacy support

Drawbacks

- Mandatory Identity Resolution
  - Resolution of the ID-Pointer at each network element
  - ID-Pointer to ID-Manager
    - Reverse DNS, Distributed Hash Tables
    - Minimized by caching
    - Optimized through deduction (e.g. if the A4C receives a preconfigured HoA it can safely infer the *Realm* by looking at the address).
  - Longer setup phases are unavoidable
    - But mobility can be as fast as before
- Strong Security is a <u>requirement</u> not an option
  - If you believe in “free networks”, you have here a challenge
  - Per requester Access Control
  - Multi-tier access control

Conclusions

- Identity in the communication stack
  - Both as a 6th (presentation) layer AND a vertical control layer
- Greatly simplified network processes
- Technology and protocol independent mobility
- Re-focus around the identity of the customer in all its actions
  - Open path to a decoupling of mobility management (user, device, session) from underlying technologies, smoothing network evolution and driving optimization aspects at all levels of the OSI stack.
- Necessary infrastructure enabling a distributed linkable database (somewhat implicit already in management systems)
- Modifications to resolution systems (to transverse these databases) and on the protocol stack on the equipments

Future (hum, hum… on-going) Work

- Mapping of this architecture in specific protocol instances
  - Including evolution path from current 3G networks
- Performance and scalability analysis
- Further study on mobility control common layer
  - Technology independence
  - Easier migration paths from current technologies and protocols
  - Implementation
- Mobility-aware and Identity-aware services.
- Cross-protocol identifiers and privacy

Thank You.

Questions ?