Mobile Communications

IEEE and 3GPP Approaches

to

Macro-Mobility

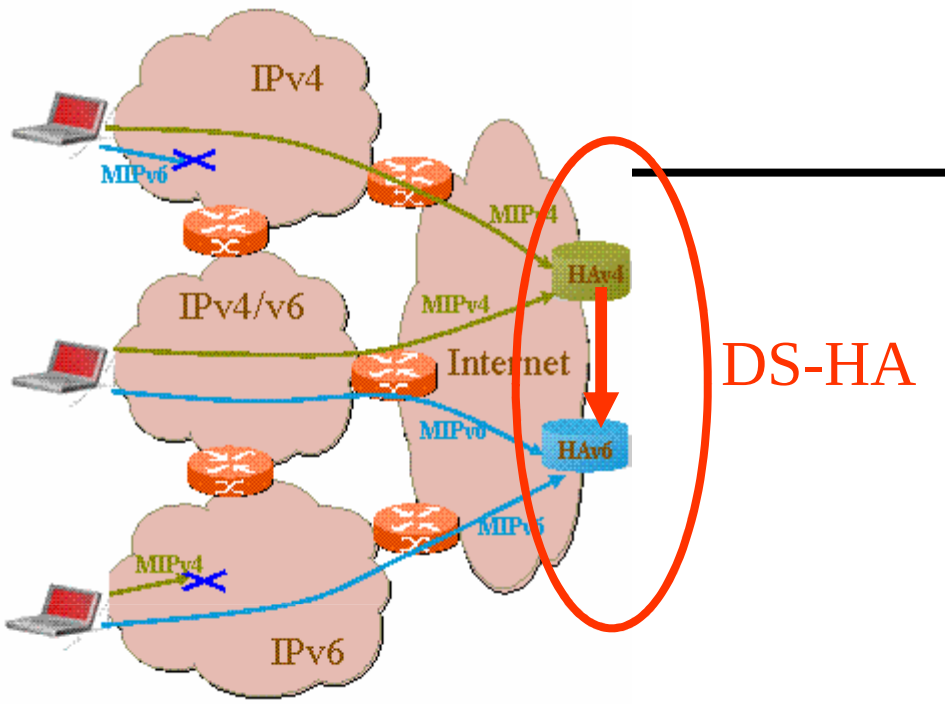
Manuel P. Ricardo

Faculdade de Engenharia da Universidade do Porto

- *How does the Dual Stack MIPv6 work?*

Dual Stack Mobile IPv6 (DSMIPv6)

DSMIPv6

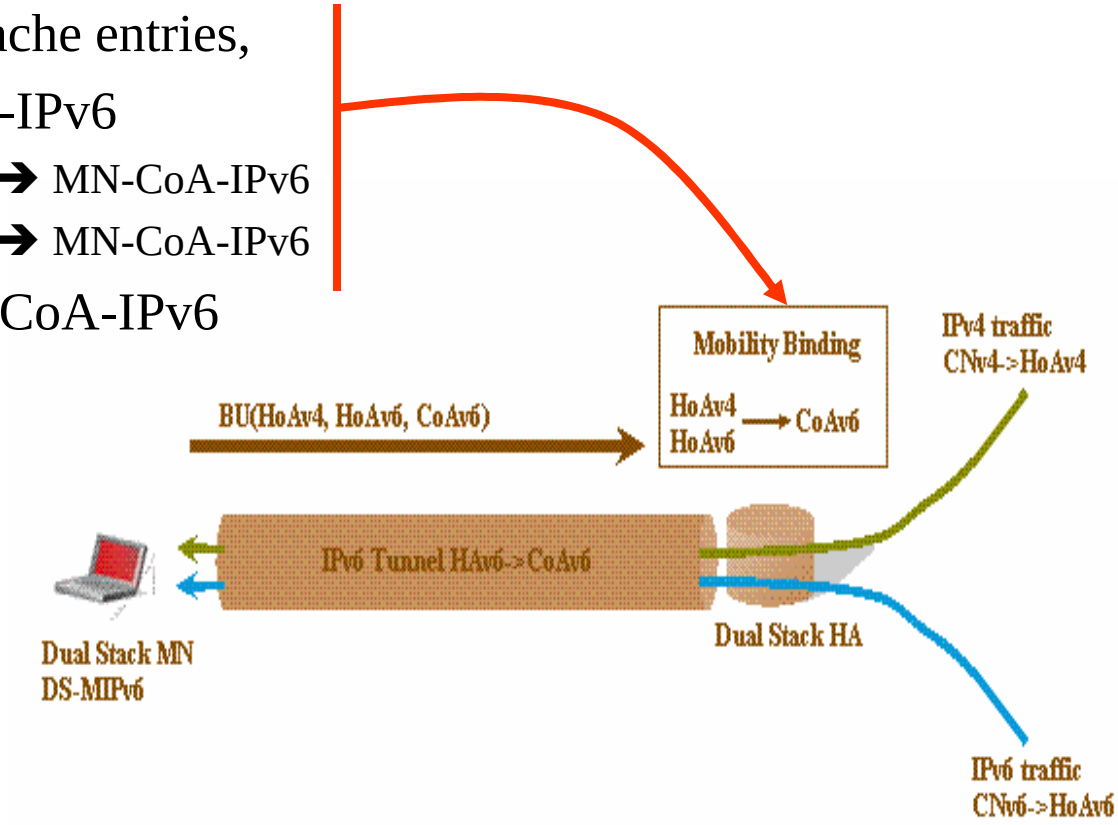


- Extends MIPv6 to allow
  - » registration of IPv4 addresses
  - » transport of both IPv4 and IPv6 packets in the tunnel to MN-HA
  - » MN to roam over IPv6 and IPv4 (public and private) networks
- Assumes
  - » MN and HA are both IPv4 and IPv6-enabled
  - » Uses only MIPv6 signalling

DSMIPv6 – Mobility Management

Visited network supports IPv6

- » MN sends regular MIPv6 *BindingUpdate*
- » MN registers IPv6 CoA to HA
- » HA creates two binding cache entries, both pointing to MN-CoA-IPv6
  - – MN-home-address-IPv6 ←→ MN-CoA-IPv6
  - – MN-home-address-IPv4 ←→ MN-CoA-IPv6
- » HA tunnels traffic to MN-CoA-IPv6



DSMIPv6 – Mobility Management

Visited network supports IPv4 only - public addresses

- » MN tunnels MIPv6 *BindingUpdate* message to the HA IPv4 address
- » HA creates two binding caches entries,
  both pointing to the MN-CoA-IPv4
  - – MN-home-address-IPv6 ←→ MN-CoA-IPv4
  - – MN-home-address-IPv4 ←→ MN-CoA-IPv4
- » All the packets addressed to MN-home-addresses (IPv4 or IPv6)
  are encapsulated in an IPv4 tunnel HAv4←→MN-CoA-IPv4

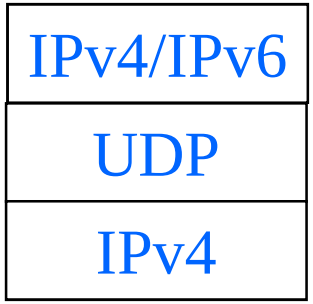
DSMIPv6 – Mobility Management

Visited network supports IPv4 only - private addresses

- » HA listens in an UDP port, over a public IPv4 address
- » MN tunnels MIPv6 *BindingUpdate* message to HA IPv4/port addresses
- » HA creates two binding caches entries,

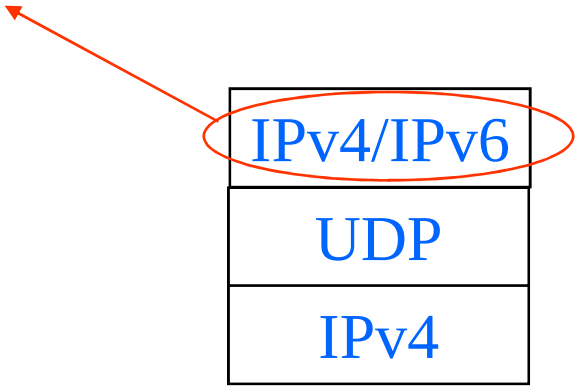
  both pointing to the public-MN-CoA-IPv4/port (recall NAT)
  - – MN-home-address-IPv6 ←→ public-MN-CoA-IPv4/port
  - – MN-home-address-IPv4 ←→ public-MN-CoA-IPv4/port
- » At the HA, the packets addressed to MN home addresses (IPv4 or IPv6)
  - – are first encapsulated in UDP packet (port to port),
  - – then encapsulated in an IPv4 tunnel ending at the public-MN-CoA-IPv4

    (recall the NAT functionality)



To think about

- Is the IPv4/IPv6 packet received in (linux) user or kernel space?



- How can the contents of this packet be delivered to, for instance, the Web-browser running on top of TCP/IPv4?

DSMIPv6 – Route Optimization

- Visited network supports IPv6 → similar to MIPv6
- Visited network supports IPv4 only

  not possible; communication always through the Home Agent
- Not possible

  for traffic addressed to the Mobile Node's IPv4 home address

3GPP plans for adopting Mobile IP

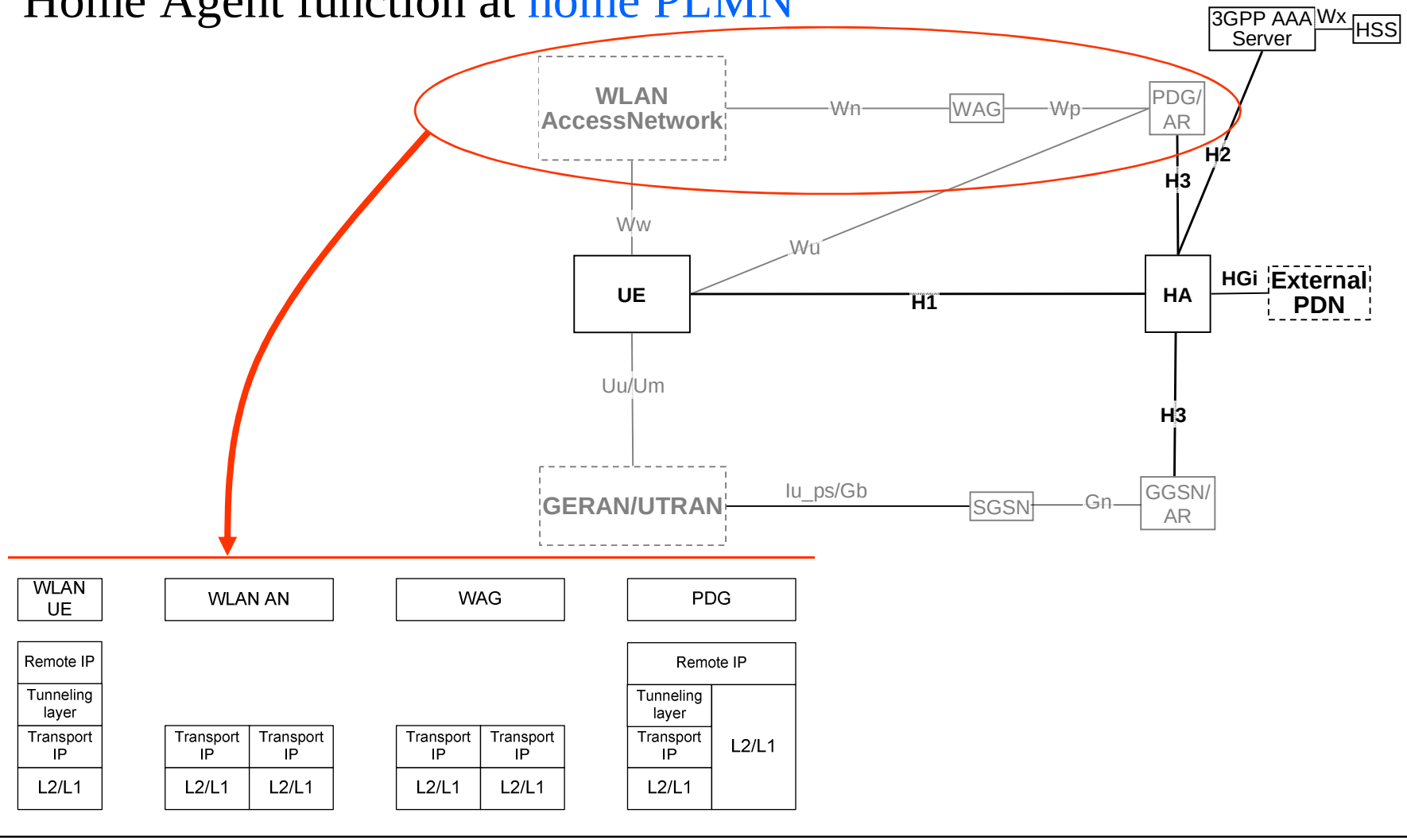
- *What MIP based solutions are currently being studied in 3GPP?*
- *How are these solutions expected to work?*

Mobility between 3GPP-WLAN Interworking and 3GPP Systems

- Plans for Release 8
- Requirements
  - » Smooth migration from legacy network with minimal impacts on dual mode UEs, I-WLAN and 3GPP systems
  - » Architecture, functions and procedures shall be re-used
  - » Both IPv4 and IPv6 addresses shall be supported
  - » Service continuity between 3GPP PS network and I-WLAN with IP address preservation
- Possible solution based on DSMIPv6
  - » 3GPP TS 23.327, TS 23.827
- Conclusions based on the SAE report may lead to other solutions
  - » See 3GPP TR 23.882

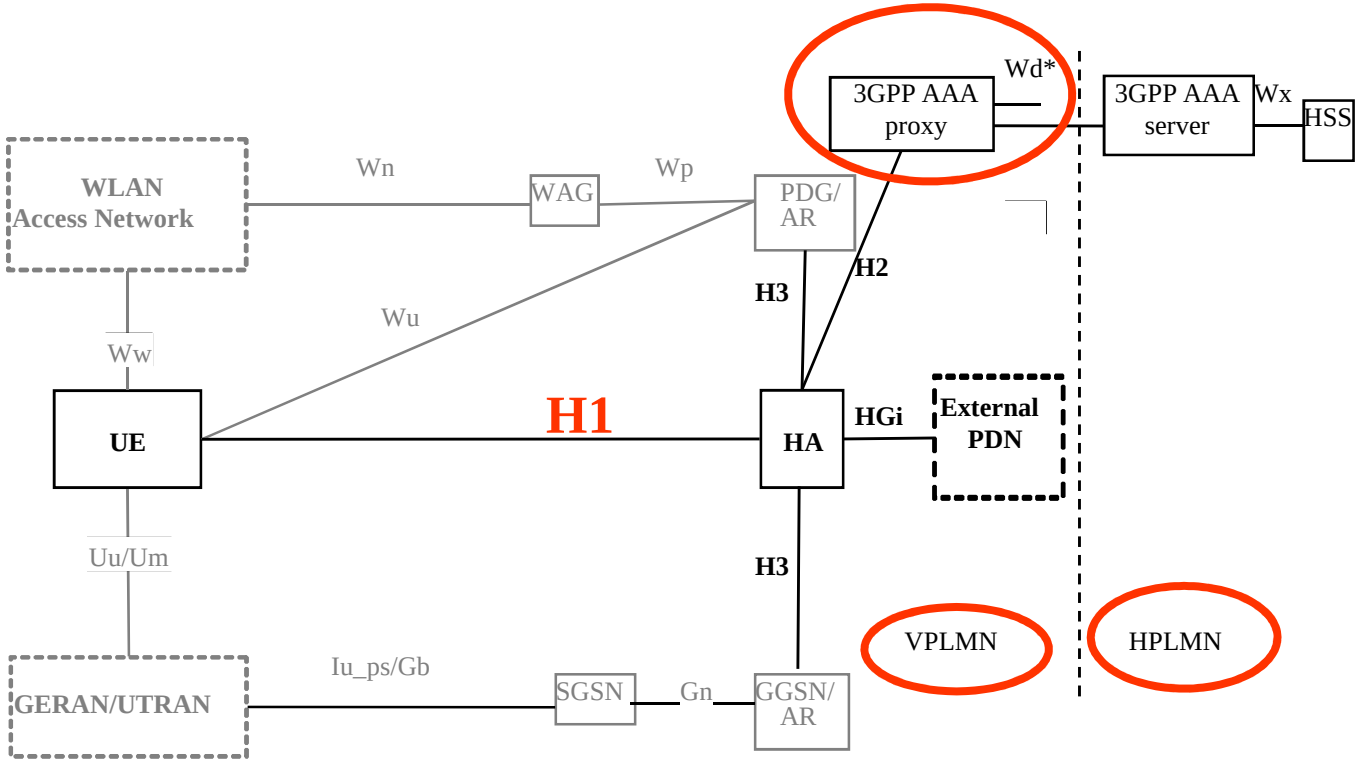
Home Mobility Service Architecture

Home Agent function at home PLMN

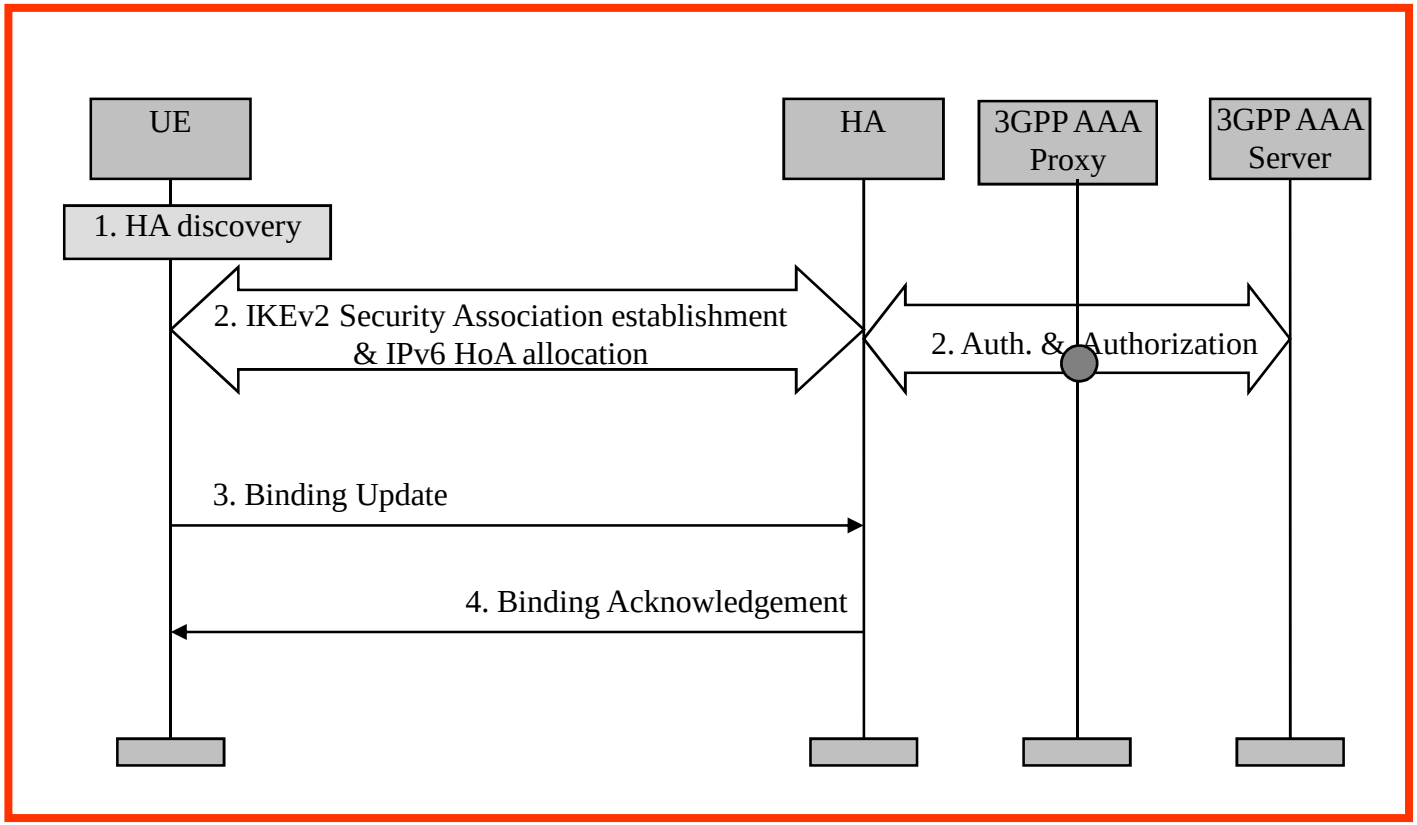


Visited Mobility Service Architecture

Home Agent function outside the hPLMN



H1 PDN Attach



H1 PDN Attach

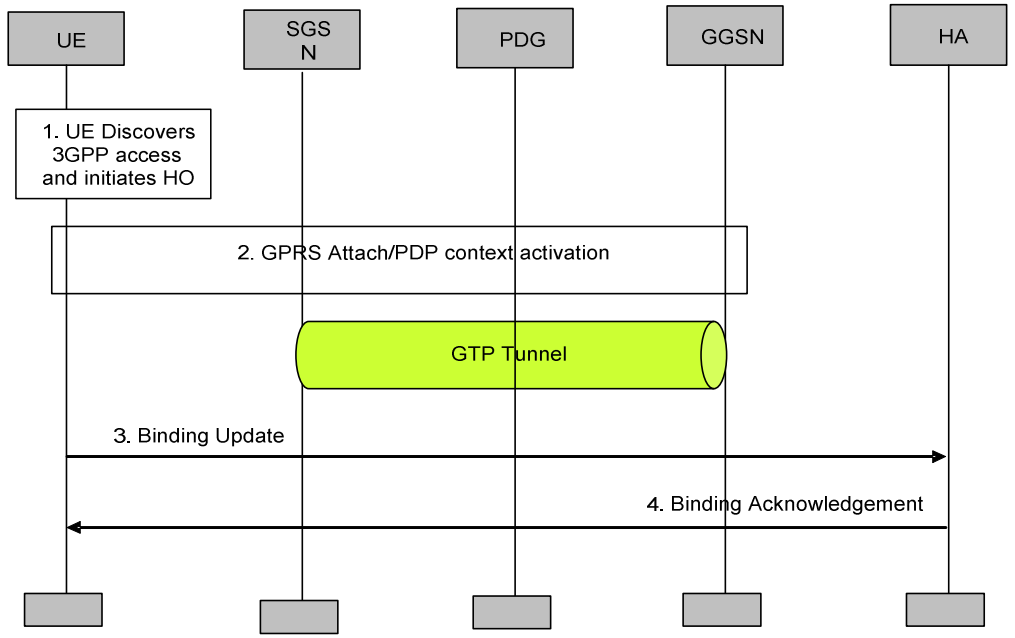
1. UE discovers the Home Agent (e.g using the DNS service)
2. A security association is established between UE and HA
   - » to secure the DS-MIPv6
   - » HA communicates with AAA infrastructure to complete authentication
   - » HA assigns IPv6 home address/prefix to UE
   - » If HA@ vPLMN
     - – interaction HA@**v**PLMN ←→ AAA/HSS@**h**PLMN involves AAA-Proxy@**v**PLMN
3. UE sends *BindingUpdate*
   - » UE may request an IPv4 home address from the HA
4. HA replies with *BindingAck*
   - » HA may assign IPv4 home address to UE

To think about

- Why does HA “assign home addresses”? What about the IP addresses gathered by the UE through the GPRS-attach and IWLAN-attach?

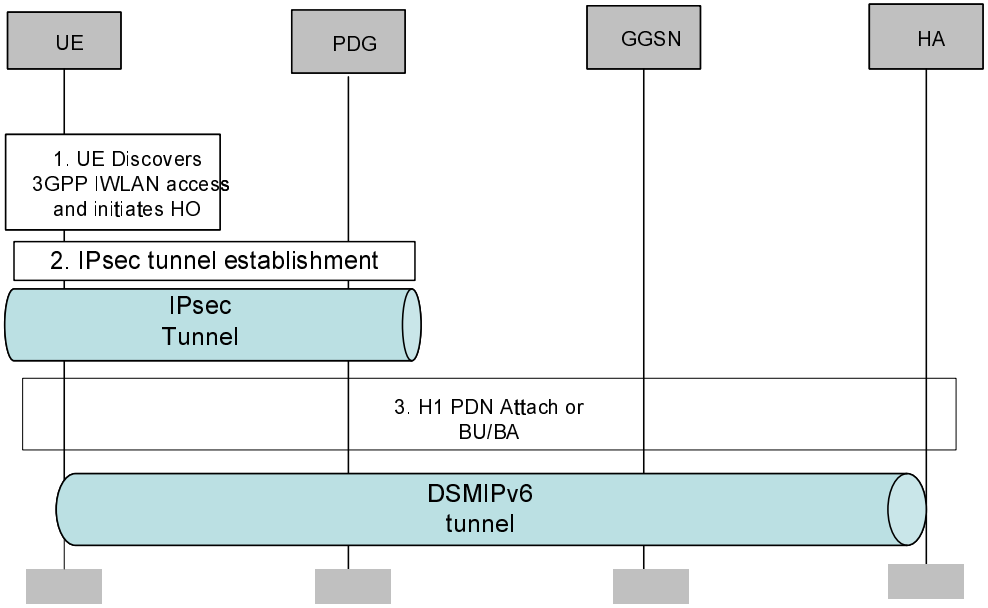
Handover from IWLAN to 3GPP access

1. UE discovers the GPRS,
   and decides to transfer sessions to GPRS
2. UE starts GPRS attach procedure, which includes
   - » GGSN selection, IP address assignment to the UE (CoA)
   - » GTP tunnel establishment between UE and GGSN
3. UE sends *BindingUpdate* message to HA
4. HA sends *BindingAck* to UE



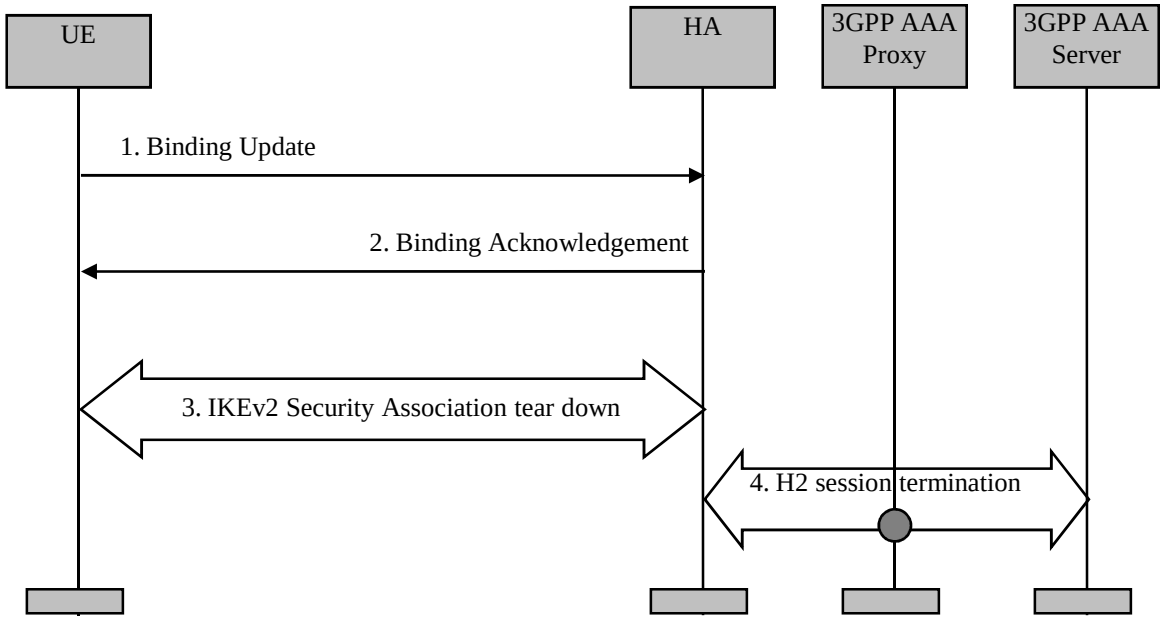
Handover from 3GPP access to IWLAN access

1. UE discovers the IWLAN,
   and decides to transfer sessions to IWLAN
2. UE establishes an IPsec tunnel with PDG,
   and gets new IP address (CoA)
3. UE sends *BindingUpdate* via IWLAN
4. DSMIPv6 tunnel established between UE and HA; UE can exchange data through IWLAN



UE Initiated Detach

1. UE sends *BindingUpdate* to HA with Binding-Lifetime = 0
2. HA sends the *BindingAck* to UE
3. UE tears down security association between UE and HA
4. The HA communicates with AAA infrastructure to tear down the H2 session



IEEE 802.21

- *What other efforts are being developed to help macro mobility?*
- *How does the 802.21 work?*

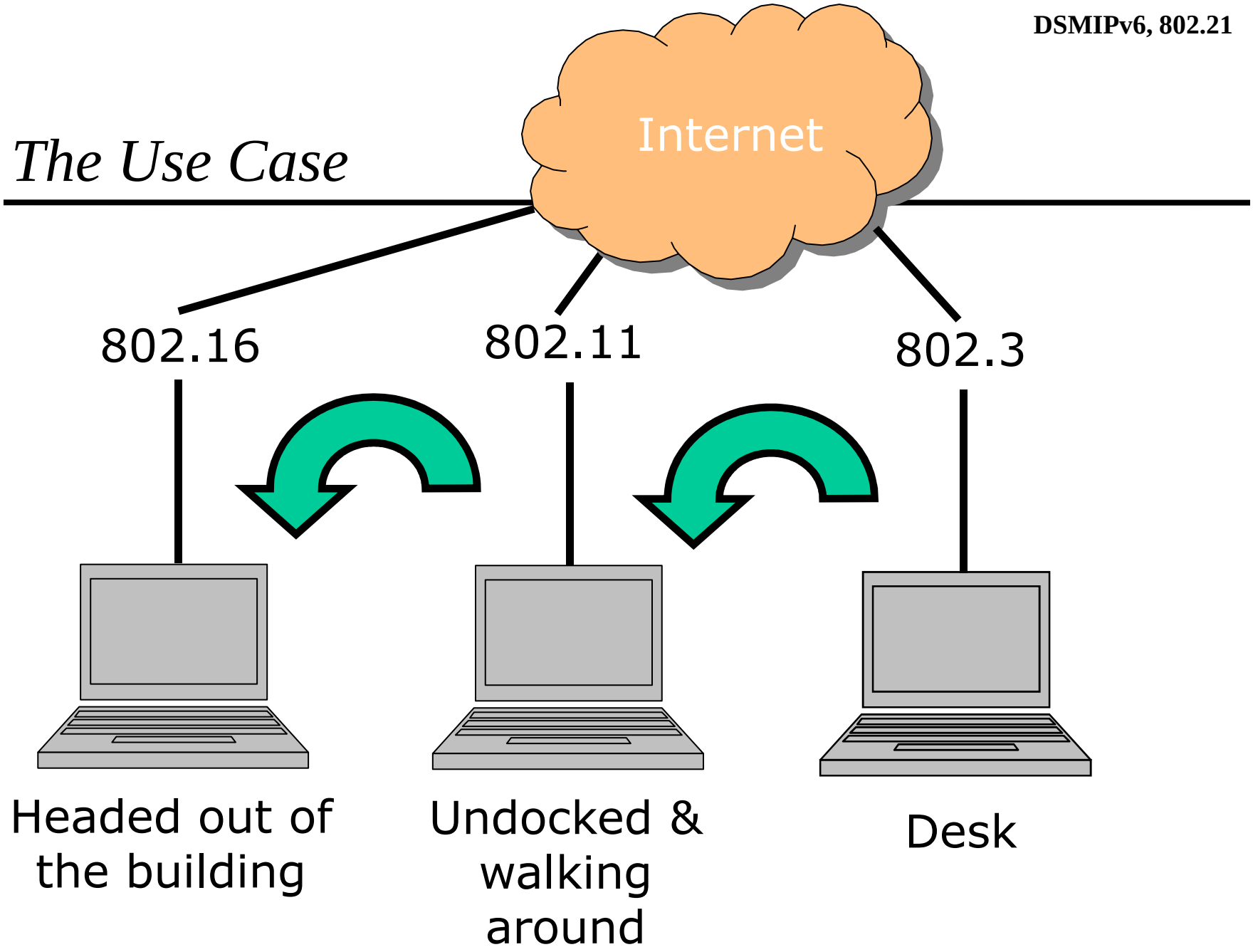
Problem Characterization

- Increasing number of interfaces on devices
  - » mostly radio interfaces
- Device has difficulties in finding its best connection
  - » connection at L2, but not at the network layer
  - » connect to the wrong of many APs available
    - based on signal strength criteria alone
- Many (vertical) handover mechanisms available
- Unified mechanism for handover decisions would help

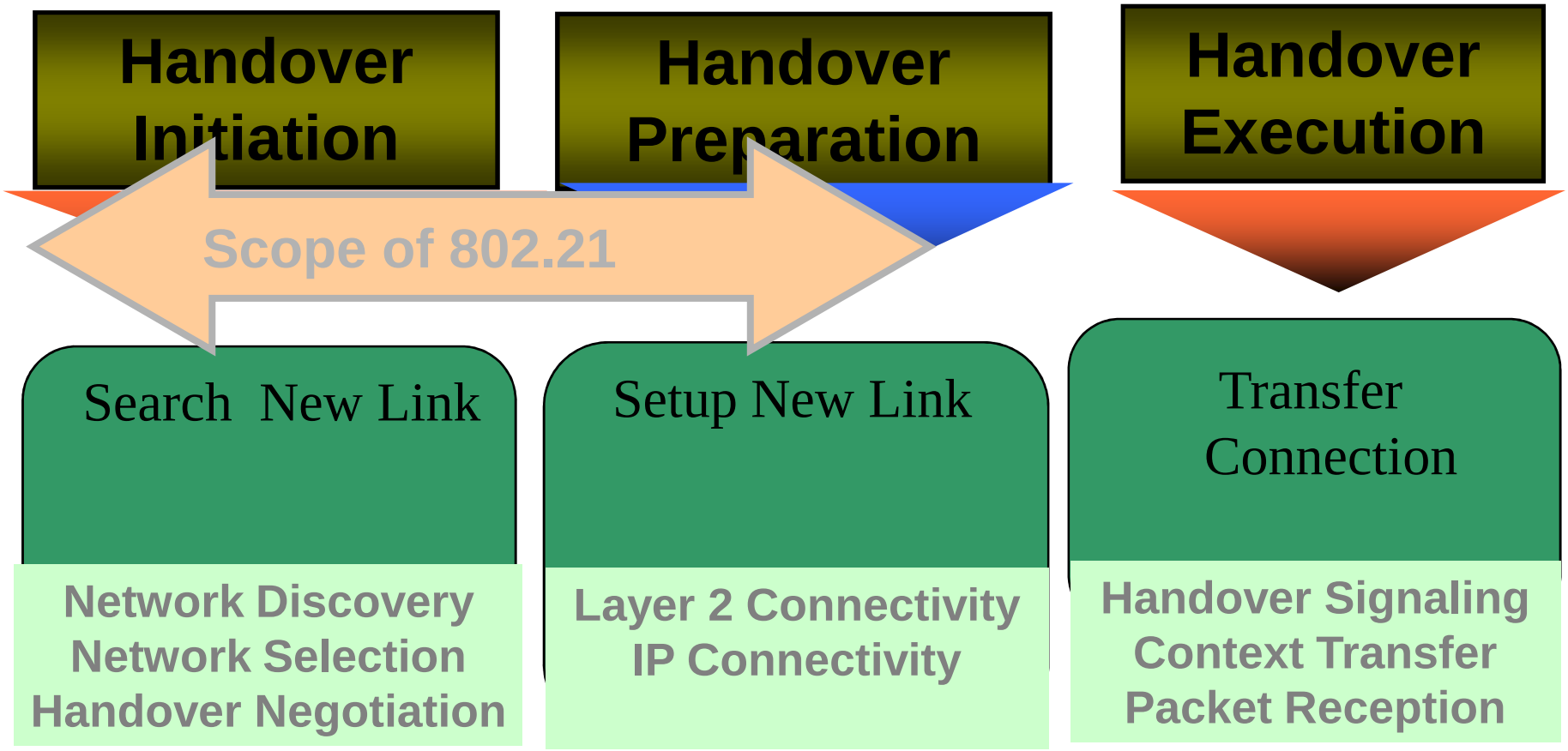
➔ new standard, IEEE 802.21

- » common across, at least, 802 media
- » based on L2 Triggers to make Mobile IP like protocols to work fast
- » based on media independent information

The Use Case

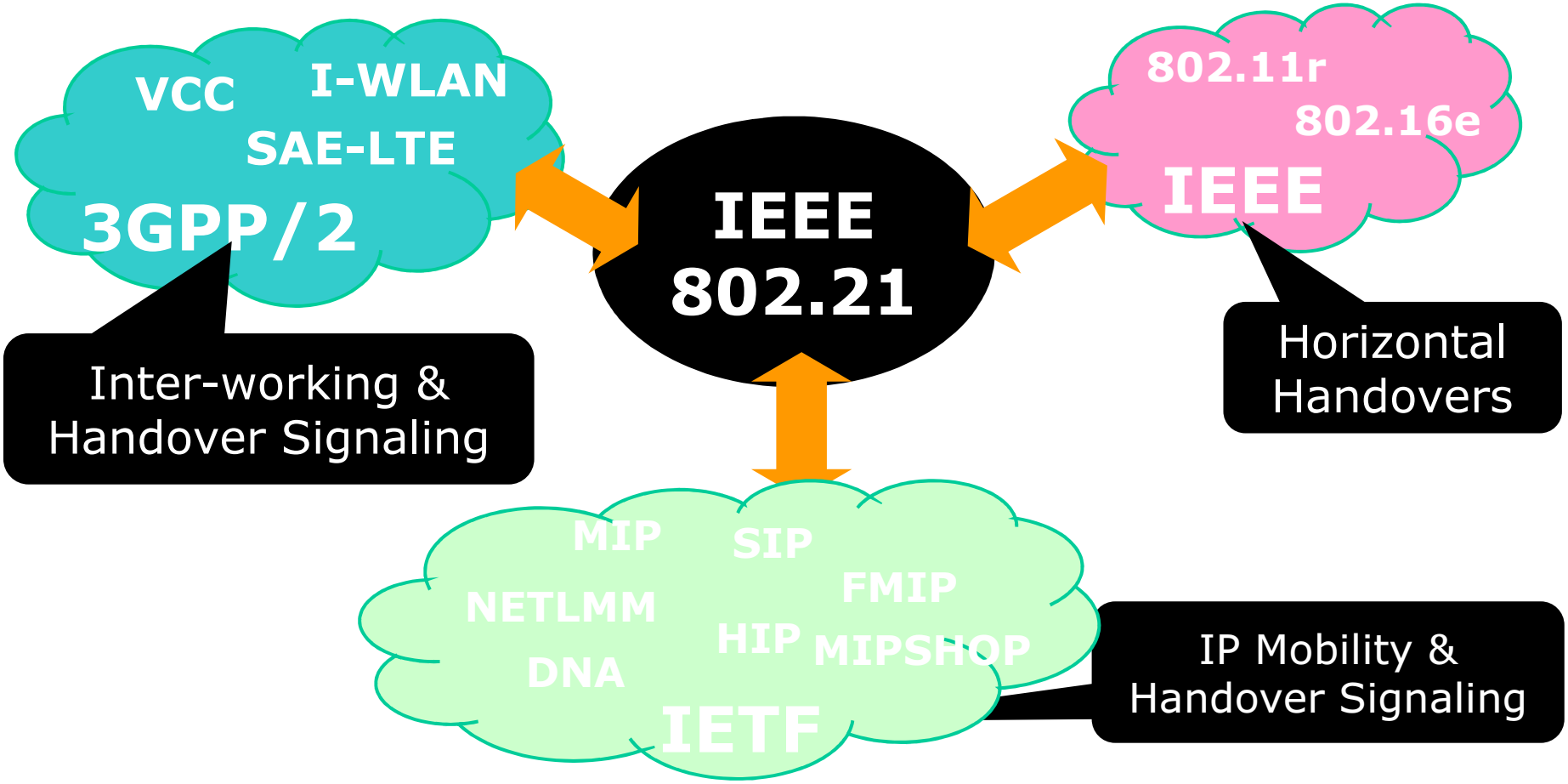

Internet
802.16
802.11
802.3
Headed out of the building
Undocked & walking around
Desk

Genesis for 802.21

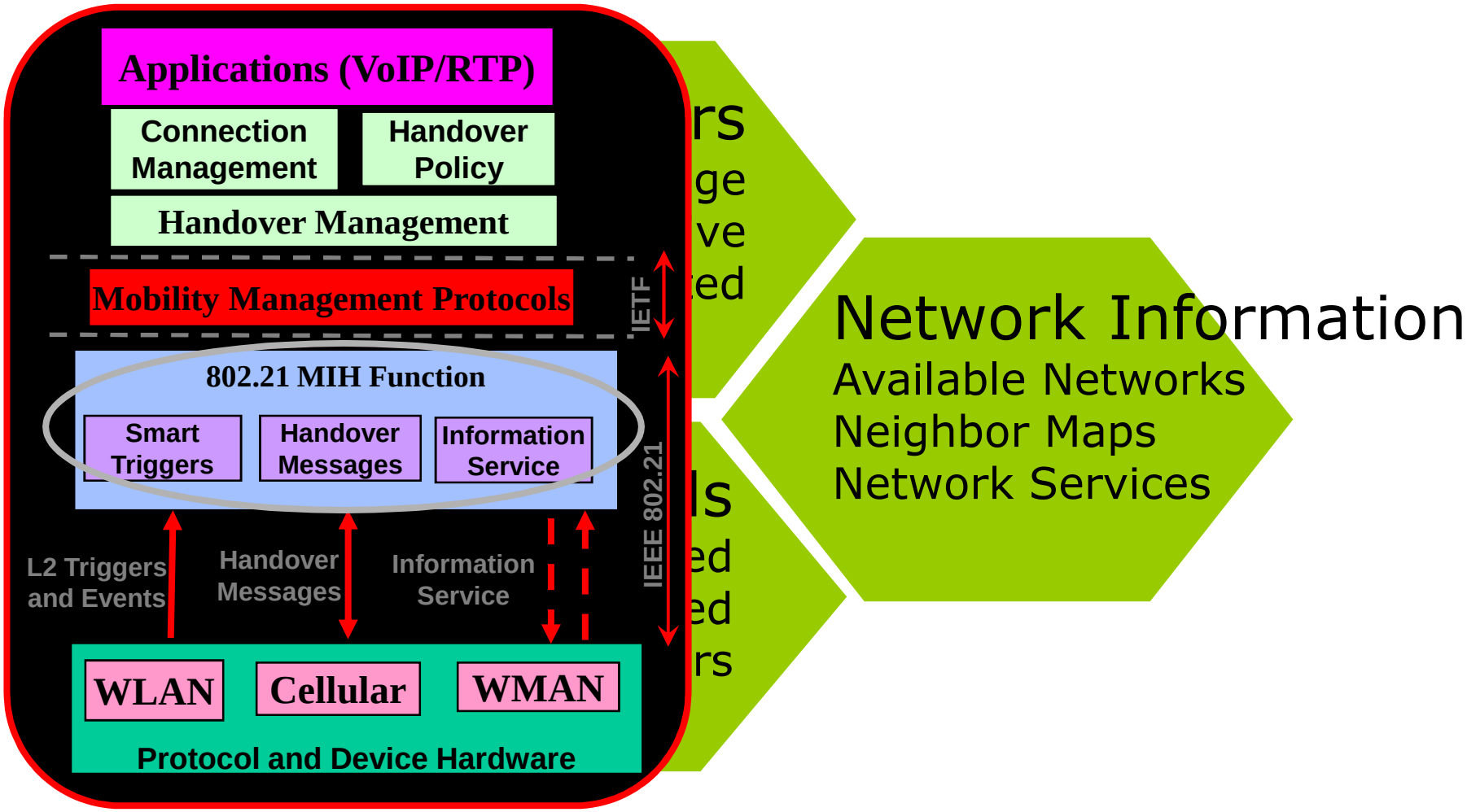


IEEE 802.21 helps with Handover Initiation, Network Selection and Interface Activation

The role of IEEE 802.21

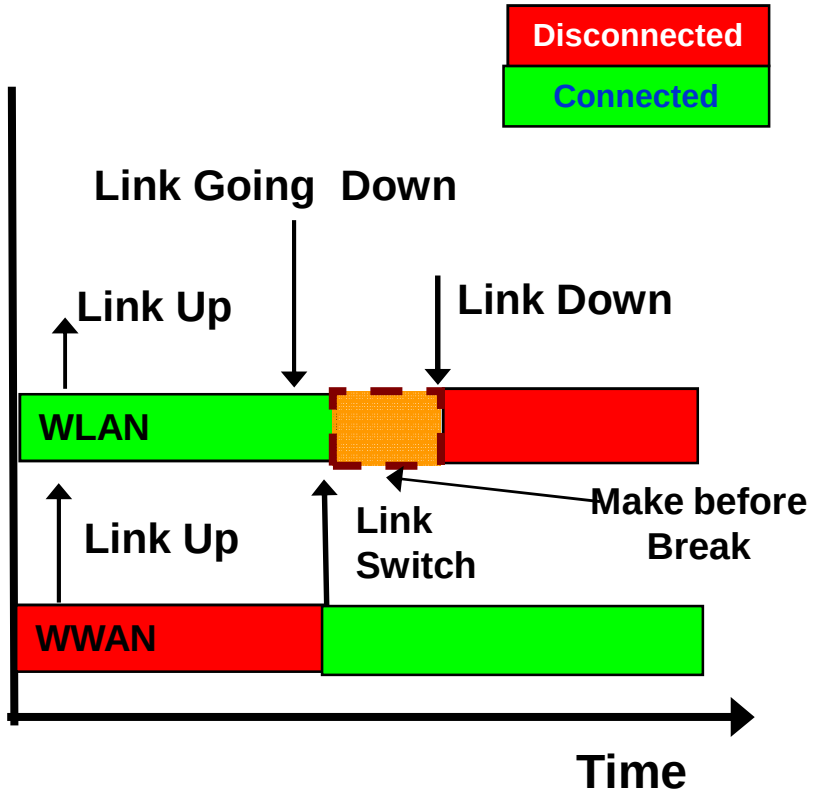


802.21 - Key Services



L2 Triggers and Events

- State Change Events
  - » Link Up
  - » Link Down
  - » Link Parameters Change
- Predictive Events
  - » Link Going Down
- Network Initiated Events
  - » Load Balancing
  - » Operator Preferences



Link Layer Events

No	Event Type	Event Name	Description
1	State Change	Link Up	L2 Connection established
2	State Change	Link Down	L2 Connection is broken
3	Predictive	Link Going Down	L2 connection breakdown imminent
4	State Change	Link Detected	New L2 link has been found
5	State Change	Link Parameters Change	Change in specific link parameters has crossed pre-specified thresholds (link Speed, Quality metrics)
6	Administrative	Link Event Rollback	Event rollback
7	Link Transmission	Link SDU Transmit Status	Improve handover performance through local feedback as opposed to waiting for end-to-end notifications
8	Link Synchronous	Link Handover Imminent	L2 intra-technology handover imminent (subnet change). Notify Handover information without change in link state.
9	Link Synchronous	Link Handover Complete	Notify handover state

Media Independent Information Service

Global Network Map

- List of Available Networks
  - 802.11/16/22, GSM, UMTS
- Link Layer Information
  - Neighbor Maps
- Higher Layer Services
  - ISP, MMS, ….

Network Type	SSID/ Cell ID	BSSID	Operator	Security	EAP Type	Channel	QoS	Physical Layer	Data Rate
GSM	13989	N/A	Oper-1	NA	NA	1900	N/A	N/A	9.6 Kbps
802.11n	Enterprise	00:00:…	Oper-2	.11i	EAP-PEAP	6	.11e	OFDM	100 Mbps
802.16e	NA	NA	Oper-3	PKM	EAP-PEAP	11	Yes	OFDM	40 Mbps

Information Elements

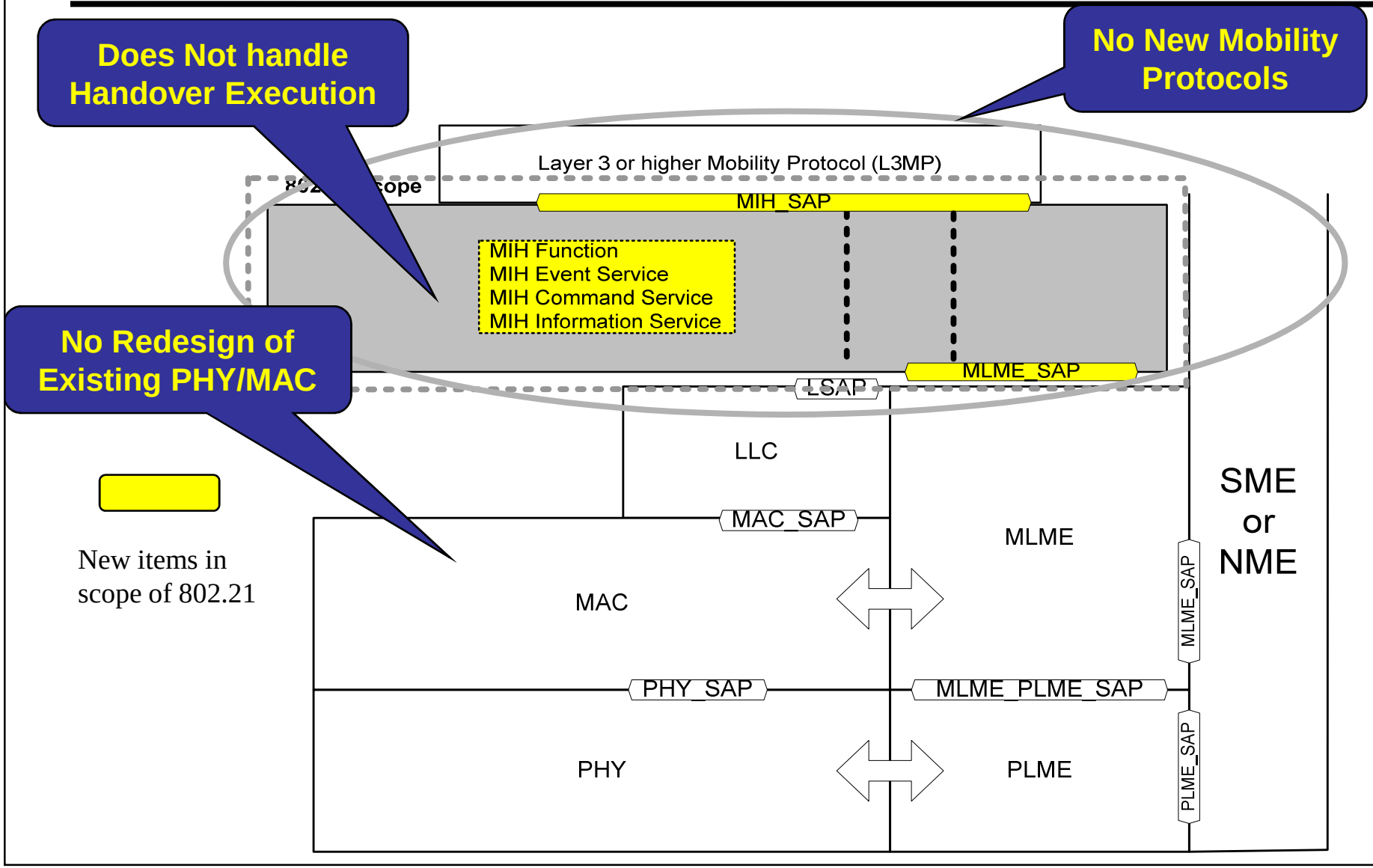
Information Element	Description	Comments
List of networks available	List all network types that are available given client location	E.g., 802.11, 802.16, GSM, GPRS/EDGE, UMTS networks
Location of PoA	Geographical Location, Civic address, PoA ID	E.g. GML format for LBS or network management purpose
Operator ID	Name of the network provider	E.g. Could be equivalent to Network ID.
Roaming Partners	List of direct roaming agreements	E.g. in form of NAIs or MCC+MNC
Cost	Indication of costs for service/network usage	E.g, Free/Not free or (flat rate, hourly, day or weekly rate)
Security	Link layer security supported	Cipher Suites and Authentication Methods, Technology specific, e.g. WEP in 802.11, 802.11i, PKM in 802.16, etc.
Quality of Service	Link QoS parameters	802 wide representation, application friendly
PoA Capabilities	Emergency Services, IMS Services, etc.	Higher Layer Services
Vendor Specific IEs	Vendor/Operator specific information	Custom information

Handover

- Types of Handover Based on Control Model
  - Terminal Controlled
  - Terminal Initiated, Network Assisted
  - Network Initiated and Network Controlled
- Handover Commands for Network Initiated Handovers

No	Command Name	MIHF <> MIHF	Description
1	MIH Handover Initiate	Client <> Network	Initiates handovers and sends a list of suggested networks and suggested PoA (AP/BS).
2	MIH Handover Prepare	Network <> Network	This command is sent by MIHF on old network to MIHF on suggested new network . This allows the client to query for resources on new network and also allows to prepare the new network for handover
3	MIH Handover Commit	Client <> Network	In this case the client commits to do the handover based on selected choices for network and PoA.
4	MIH Handover Complete	Client <> Network Network <> Network	This is a notification from new network PoA to old network PoA that handover has been completed, new PoA has been established and any pending packets may now be forwarded to the new PoA.

MIH Amendments for 802.11



MIH Amendments for 802.16