Telcordia

the elements of success

Network-Layer Assisted Mechanism to Optimize Authentication Delay during Handoff in 802.11 Networks

Authors:

Rafa Marin Lopez (Toshiba America Research)

Ashutosh Dutta (Telcordia Research) **Presenter**

Yoshihiro Ohba (Toshiba America Research)

Henning Schulzrinne (Columbia)

Antonio F. Gomez Skarmeta (University of Murcia)

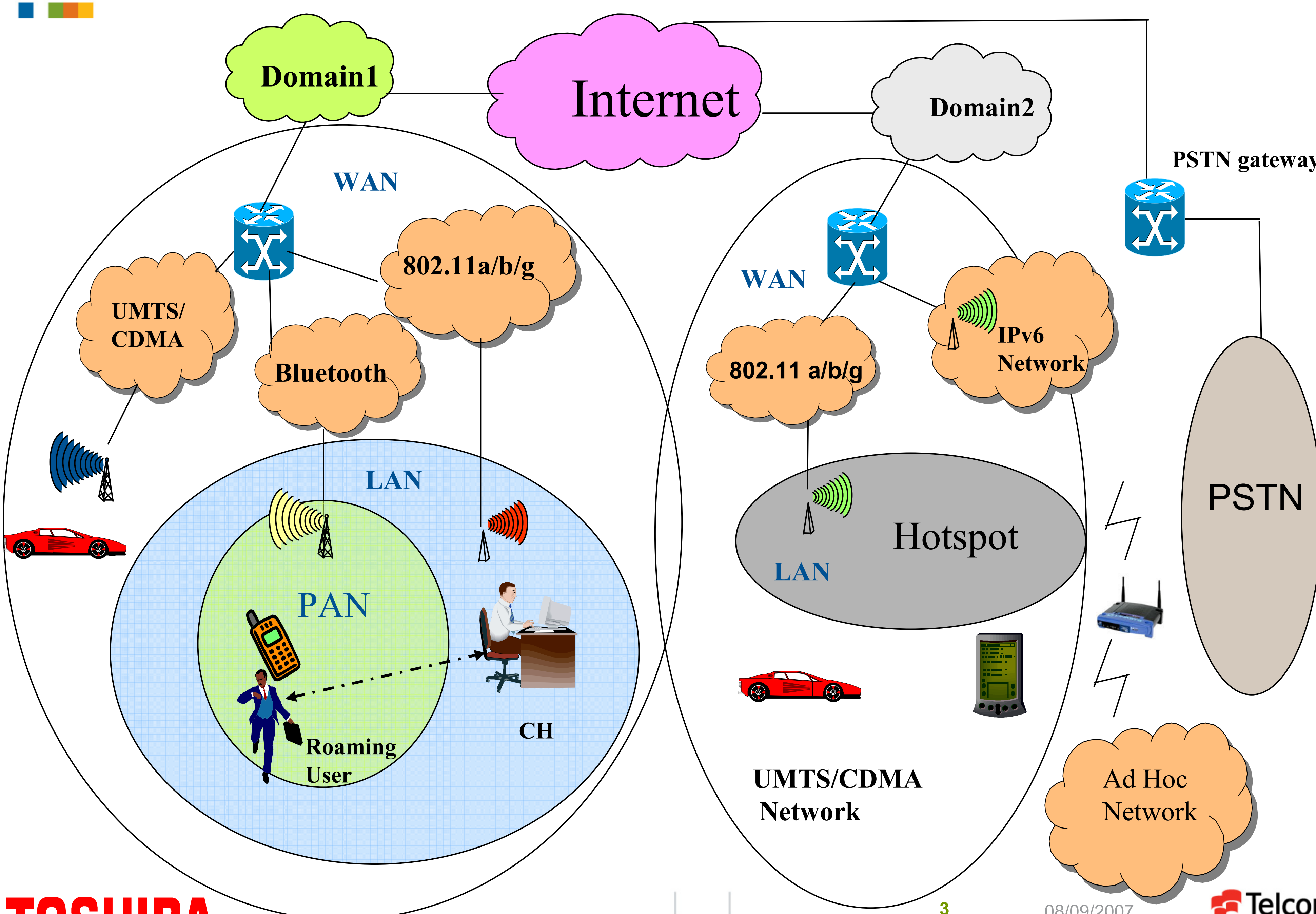
08/09/07

TOSHIBA

Outline

- Motivation
- Handoff Delay Components
- Effect of Authentication on Handoff delay
- Pre-authentication - Related Work
- Network Layer Assisted Pre-authentication
- Protocols and Experiments
- Conclusion & Future Work

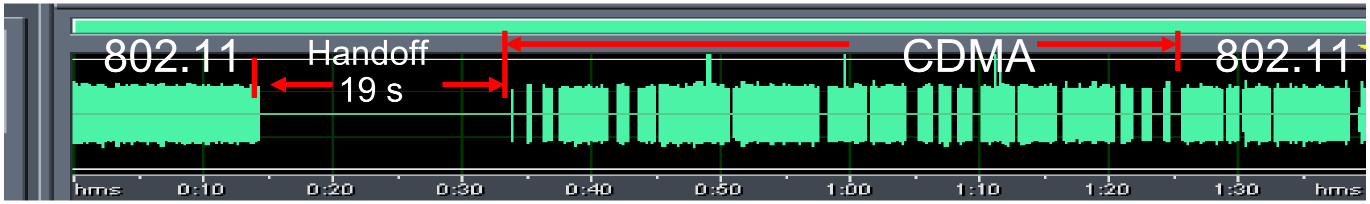
Mobile Wireless Internet: A Scenario



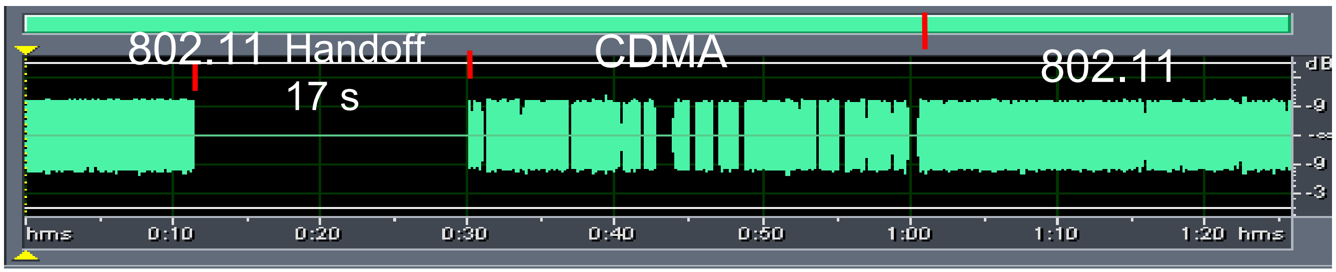
Motivation

- Secured and seamless mobility accross heterogenous access networks needs optimization at all layers to support real-time communication
- Authentication and security association at link-layer is one of the major components during handoff.
- We propose a network-layer assisted proactive handoff process to jump-start link-layer security accross multiple subnets and domains

Effect of handoff delay during non-optimized mobility management (experimental results)



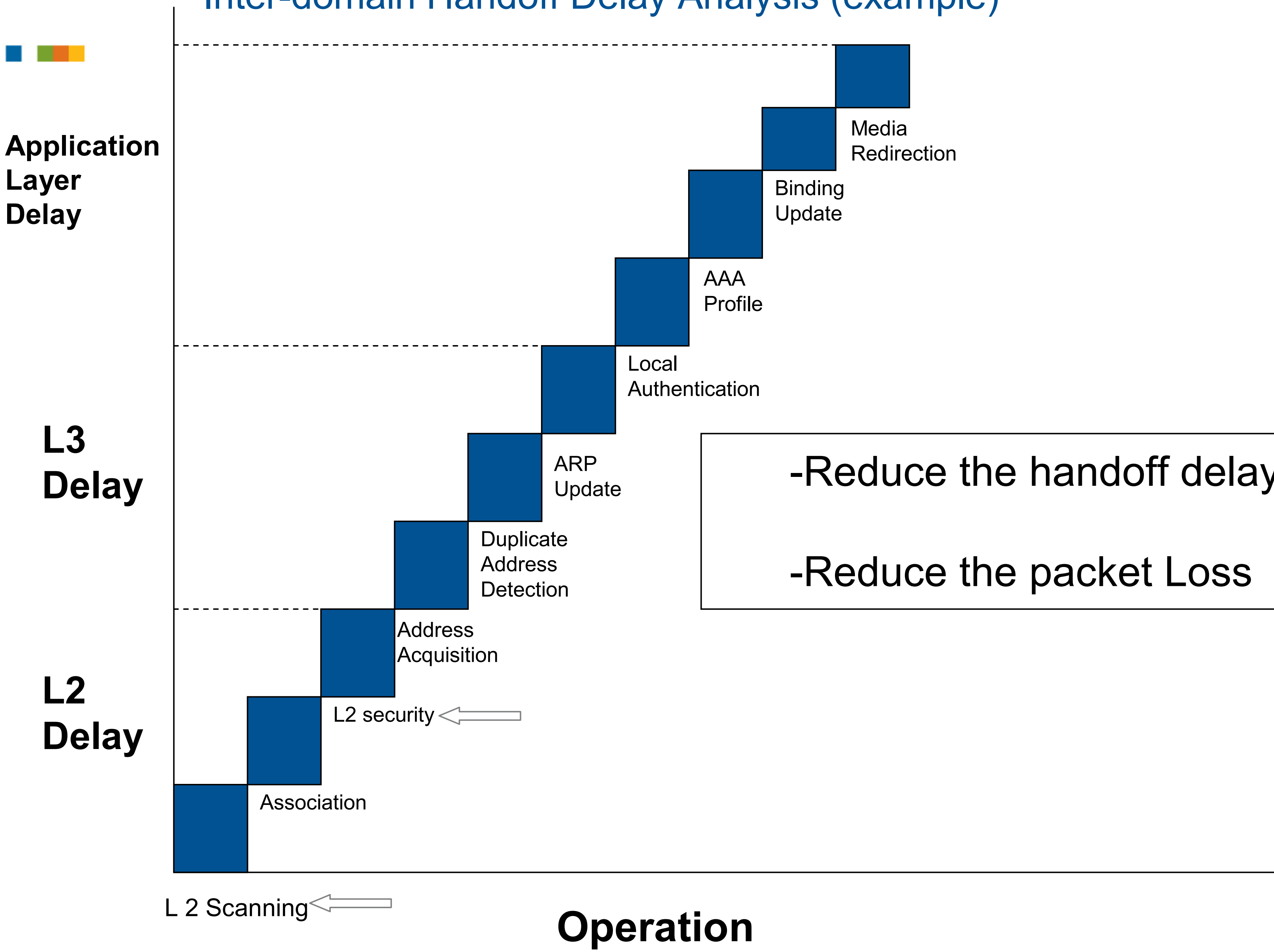
Multiple Interface Case (802.11b – CDMA1XRTT) – MIP as mobility protocol



Multiple Interface Case (802.11b – CDMA1XRTT) – SIP as mobility protocol

Single Interface Case (802.11b – 802.11b) – SIP as mobility

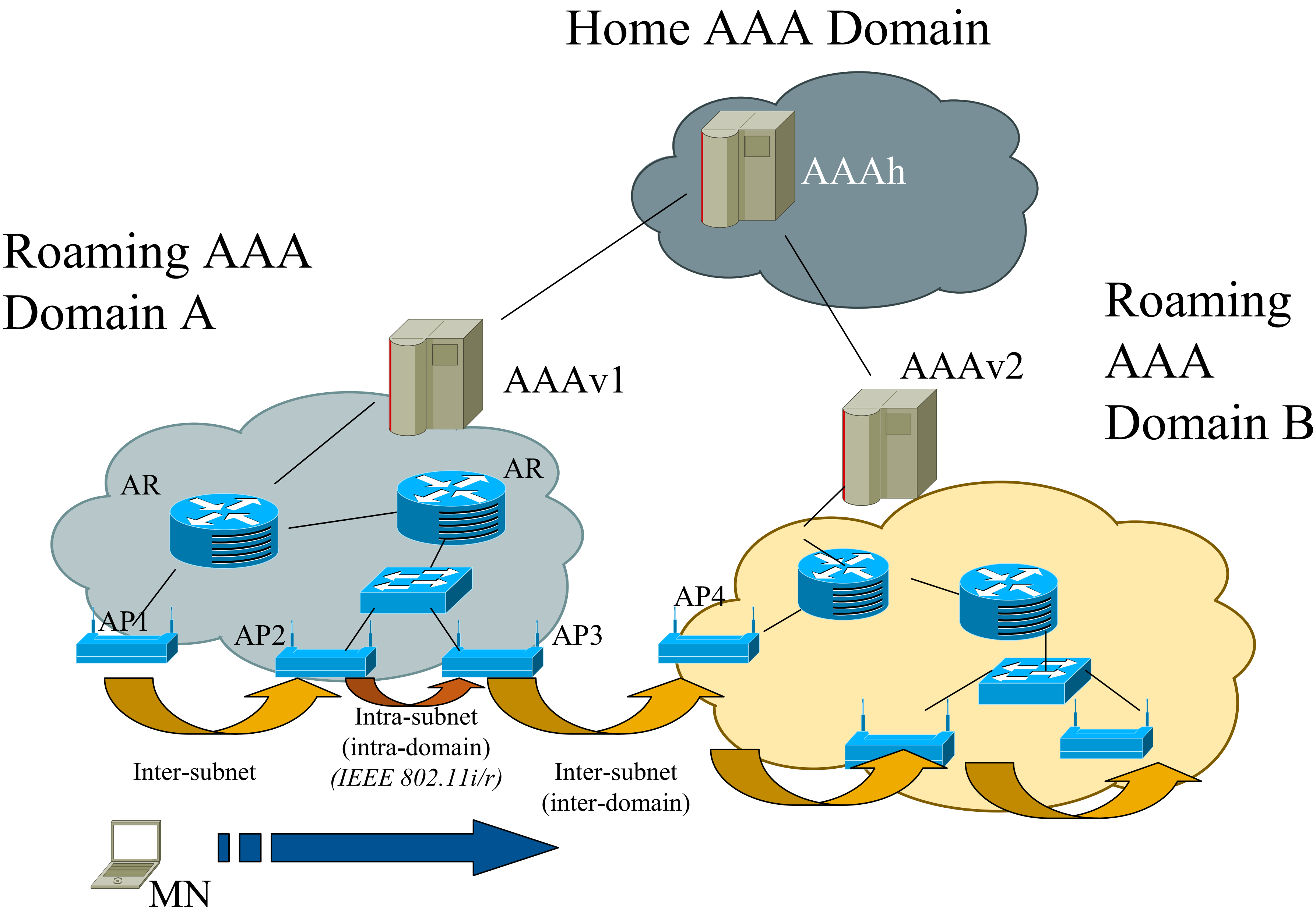
Inter-domain Handoff Delay Analysis (example)



-Reduce the handoff delay

-Reduce the packet Loss

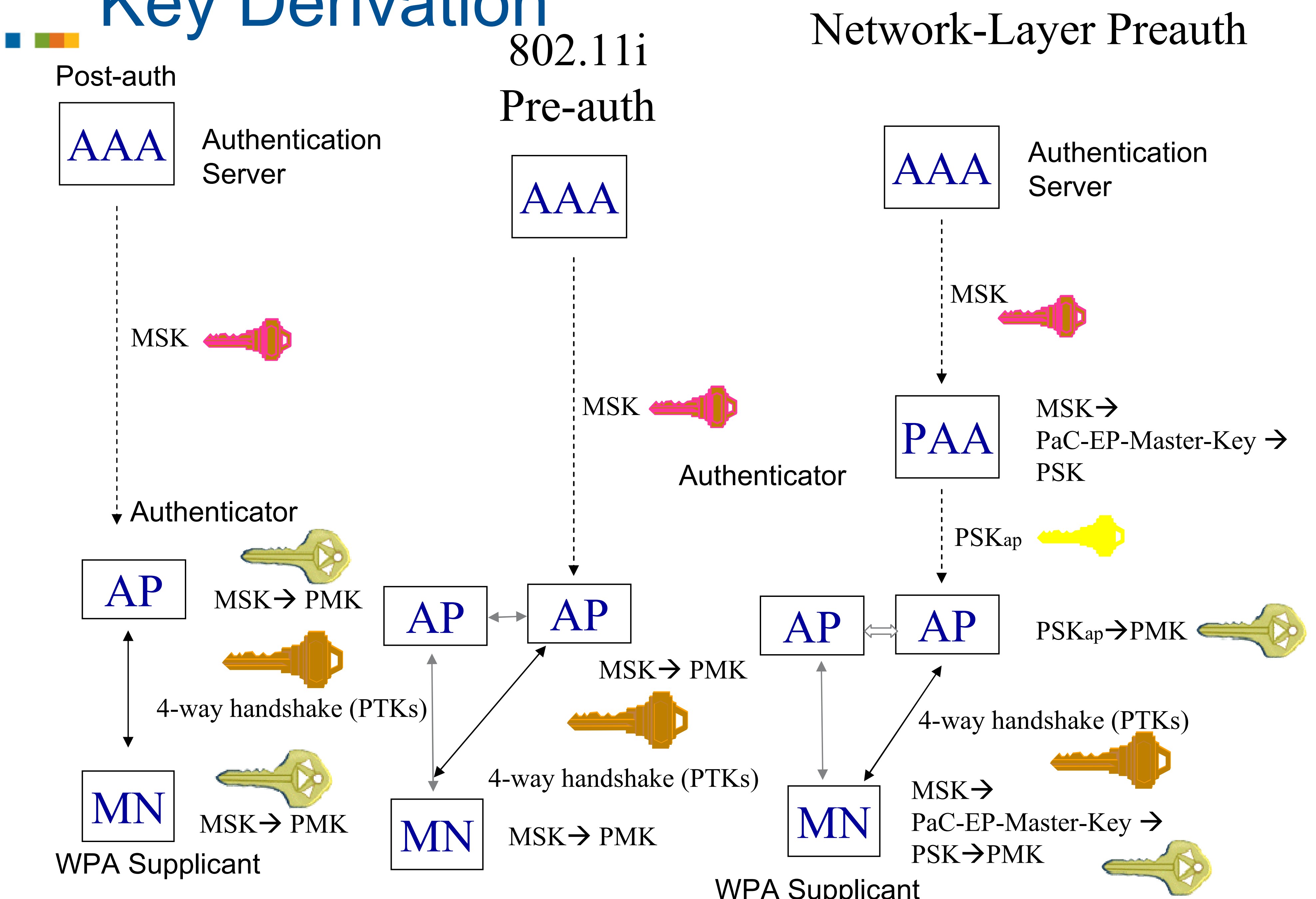
Example Roaming Environment



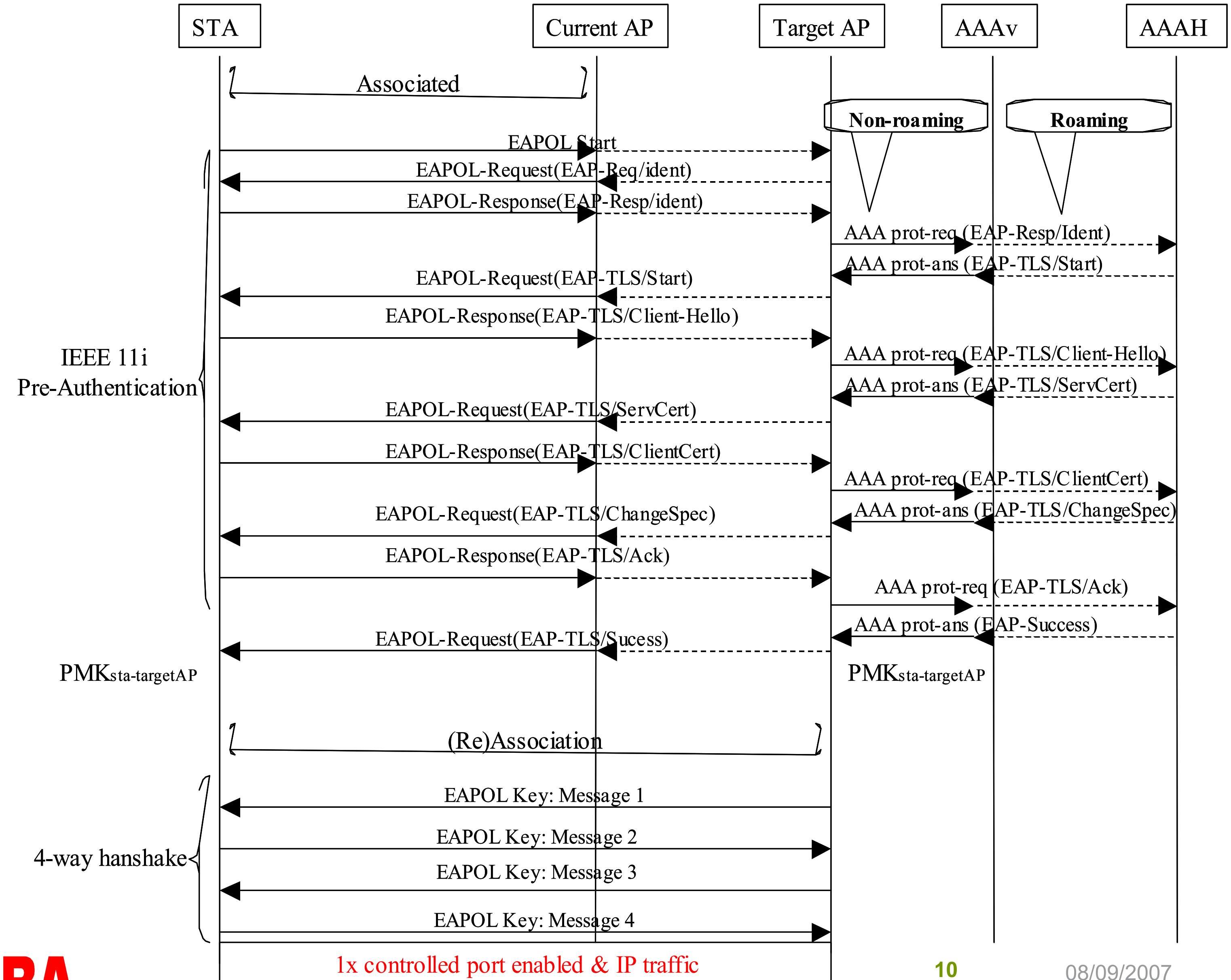
Related Work

- **IEEE Standards**
  - IEEE 802.11i provides pre-authentication at link-layer in the distribution system (DS)
  - IEEE 802.11r improves 11i by introducing a new key hierarchy but it does not work between DSs either.
- **Context transfer solutions (Bargh et al, Georgiades et al, Duong et al)**
  - Security problems such as “domino effect”
  - Assume certain trust relationships which might not be possible in certain scenarios.
  - Oriented towards the same technology
- **Pre-installation based on movement pattern (Mishra et al, Pack et al)**
  - AAA assisted key installation
  - Works within the same administrative domain
- **MIPv6 and AAA assisted (Ruckforth et al)**
  - Limited to MIPv6 and within the same domain
- **Cooperative Roaming (Forte et al)**
  - Works within a domain

Key Derivation



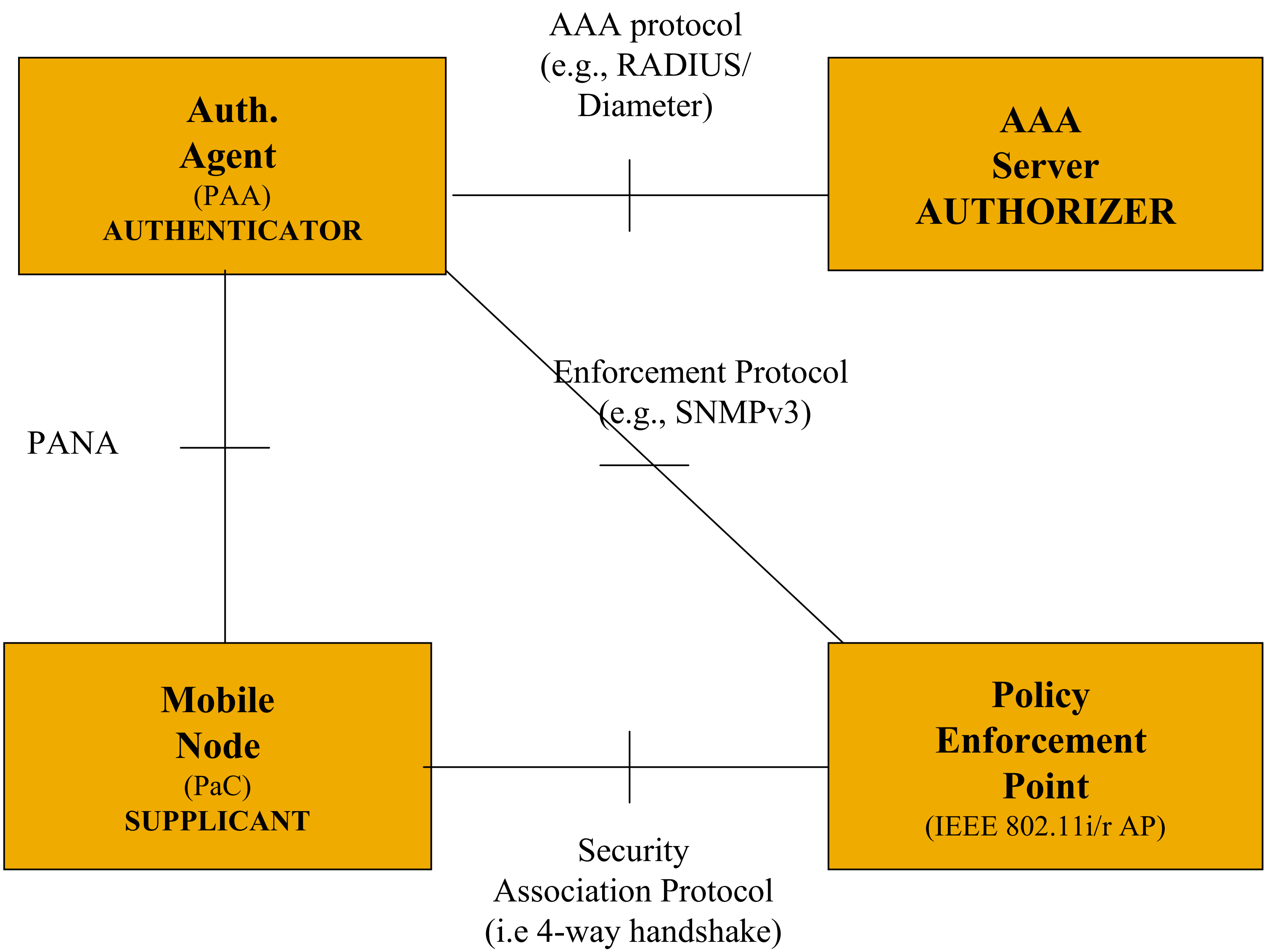
802.11i – Pre-authentication Flow



Network-Layer Assisted Pre-Authentication Technique

- Assists link-layer optimization mechanism to work accross subnets and domains
- It is independent of link-layer technology (e.g., 802.11, CDMA)
- It does not suffer from context transfer security problems and only assumes basic trust relationship
- It supports handover across inter-technology, inter-subnet and inter-domain.

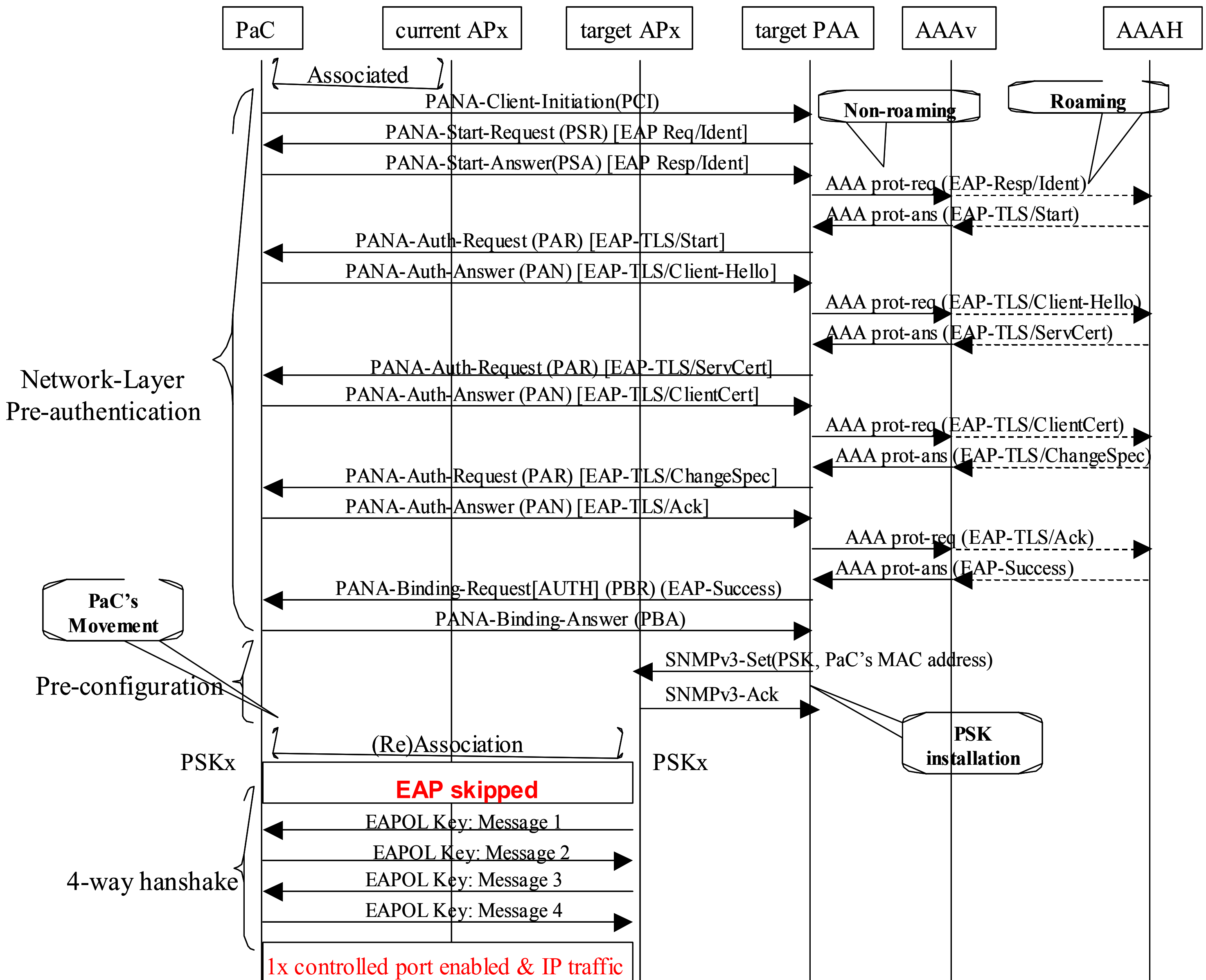
Logical Architecture



Network Layer-assisted Pre-authentication Operations

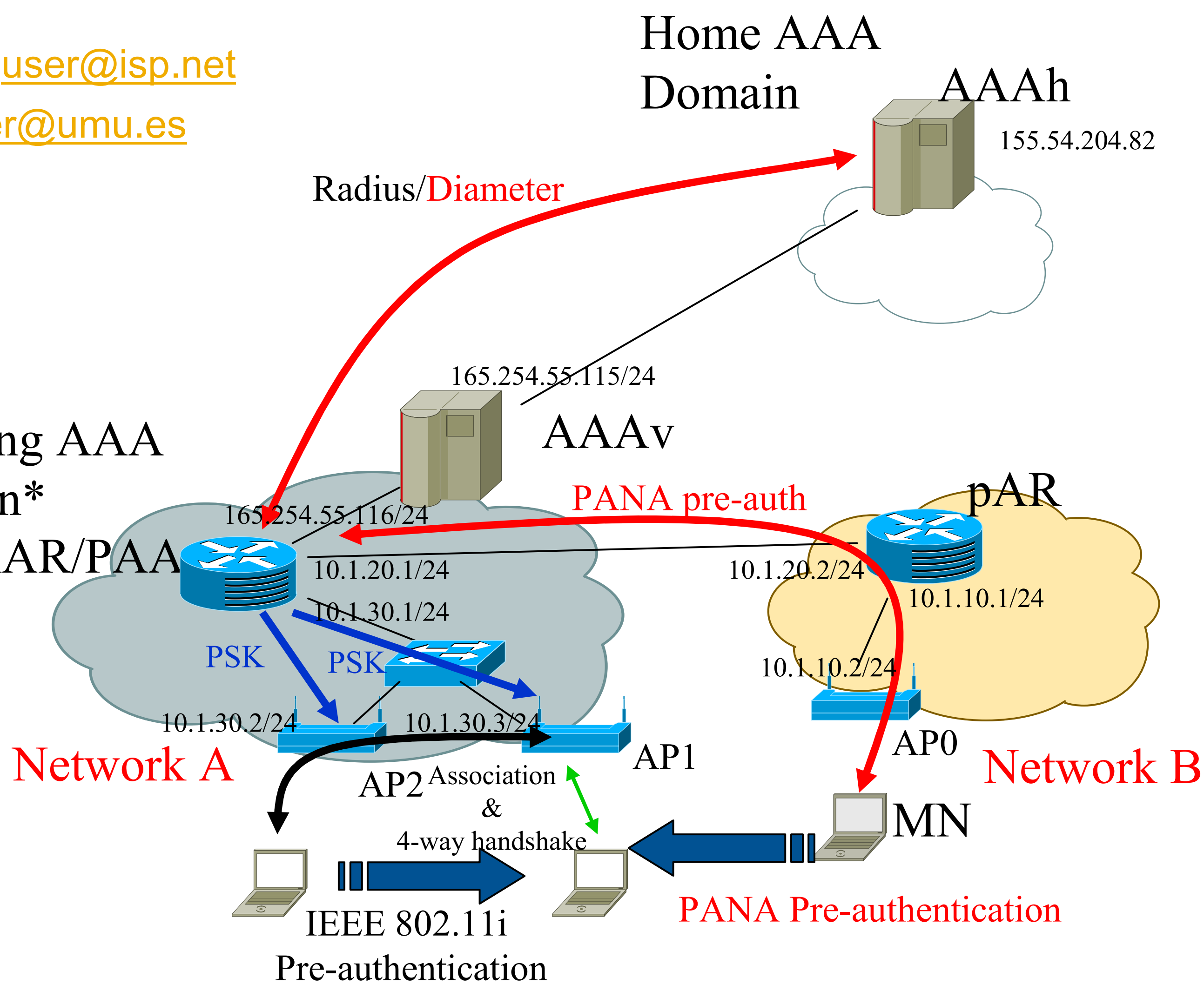
1. Discovering target PAAs and Access Points
   - External mechanism such as IEEE 802.21
2. Pre-authentication Mechanism based on PANA
   - EAP-TLS
   - AAA as the backend AS
3. PSK derivation
   - PAA derives distinct PSK per AP from MSK
4. Key Installation Process

Network Pre-authentication Flows



Experimental Testbed

Non-Roaming: user@isp.net
Roaming: user@umu.es



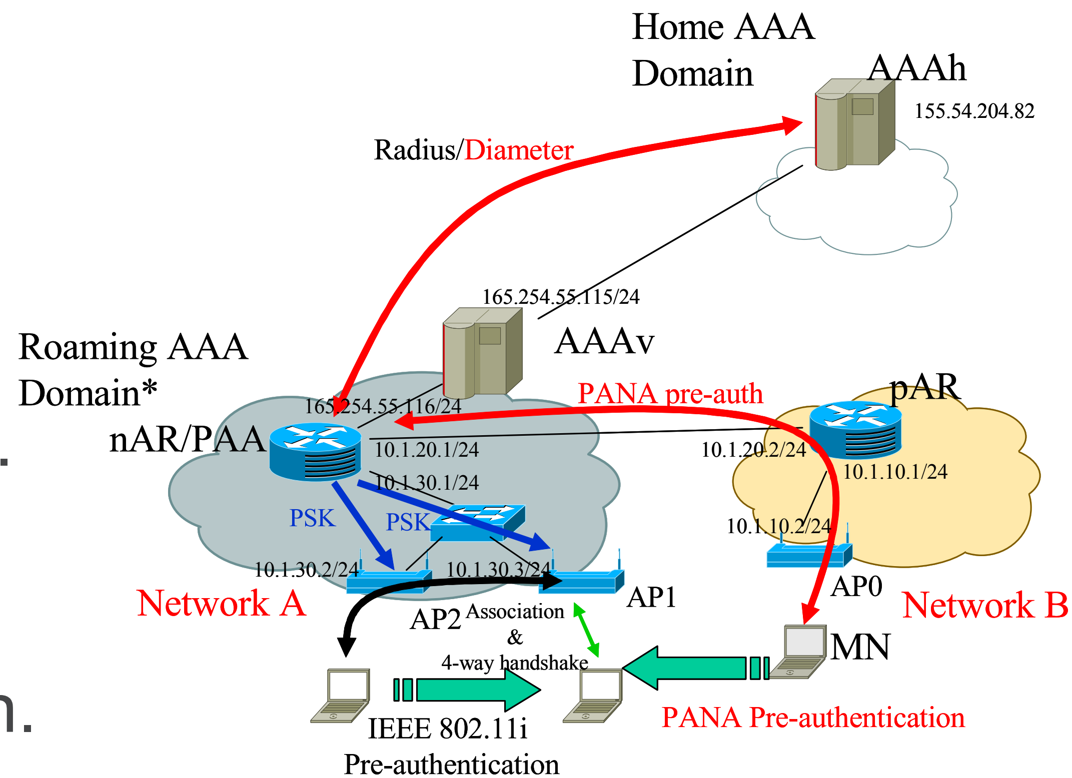
* Roaming AAA Domain in roaming case.
For non-roaming case, it acts as MN's home AAA domain.

Experimental Network Elements

- **Mobile Node**
  - wpa_supplicant (IEEE 802.11i)(Auth. Methods : EAP-TLS)
  - Open Diameter PANA Client (Auth Methods. EAP-TLS)
- **Access Points**
  - Hostapd (IEEE 802.11i and RADIUS Client)
  - Net-SNMP (SNMP Agent)
- **Authentication Agent**
  - Open Diameter, PANA Agent
  - Net-SNMP (SNMP Manager)
- **AAA server**
  - Open Diameter (Diameter EAP server for network assisted pre-authentication)
  - Free RADIUS (RADIUS server for rest of scenarios)

Experimental Scenarios

- Scenario 1: No pre-authentication involved. (AP0 → AP1)
- Scenario 2: Pre-authentication at link-layer. (AP2 → AP1)
- Scenario 3: Network assisted pre-authentication. (AP0 → AP1)



* Roaming AAA Domain in roaming case.
For non-roaming case, it acts as MN's home AAA domain.

Results for analyis (I)

- **Tauth**: authentication time with EAP-TLS
- **Tconf**: key installation time (only useful for network-layer pre-authentication)
- **Tassoc+4way**: time spent in the 802.11 association plus 4-way handshake
- **Tscanning** - Avoided due to prior discovery

Results (II)

TABLE I. COMPARISON OF POST-AUTHENTICATION AND PRE-AUTHENTICATION

Types of Authentication	IEEE 80211i post-authentication		IEEE 802.11i pre-authentication		Network-layer -assisted pre-authentication	
Operation	Non Roaming	Roaming	Non Roaming	Roaming	Non Roaming	Roaming
Tauth	61 ms	599 ms	99 ms	638 ms	177 ms	831 ms
Tconf	--	--	--	--	16 ms**	17 ms**
Tassoc+4way	18 ms	17 ms	16 ms	17 ms	15 ms	17 ms
Total	79 ms	616 ms	115 ms	655 ms	208 ms	865 ms
Handover Delay	*79 ms*	*616 ms*	*16 ms**	*17 ms**	*15 ms*	*17 ms*

*This time is only applicable within same DS.

**This time includes key installation for two APs in our testbed.

Conclusions & Future Work

- Secure handover optimization is important to support inter-domain and inter-access handover
- Current techniques have some limitations to support inter-subnet, inter-domain and inter-technology handover
- We have demonstrated that the network layer-assisted pre-authentication helps to overcome these limitations
- Currently under discussion in IRTF/IETF
- Integrate Layer-2 pre-authentication with network layer and application layer mobility protocols
- Integrate Layer-2 pre-authentication with MIPv6

PSK/PMK derivation Process

- IEEE 802.11i can work in two modes
  - 1X EAP mode (MSK)
  - PSK mode.
- Using a Master Session Key (1X EAP mode) or a pre-shared key (PSK), STA and AP can derive a PMK to perform a security association protocol (4-way handshake)
- In PSK mode, it needs a pre-shared key pre-installed. No EAP authentication is needed in this mode.
- With network-assisted pre-authentication we derive and install a different dynamically generated PSK in each AP under the same authentication agent.
- PSK is derived from a key named PaC-EP-Master-Key which, in turn, is derived from the EAP authentication performed at network-layer preauth.