Media-Independent Pre-Authentication

(draft-ohba-mobopts-mpa-framework-00.txt)

Ashutosh Dutta, Telcordia Technologies

Yoshihiro Ohba (Ed.), Kenichi Taniuchi

Toshiba America Research Inc.

Henning Schulzrinne, Columbia University

Prepared for IRTF MOBOPTS WG
March 8th, 62nd IETF, Minneapolis

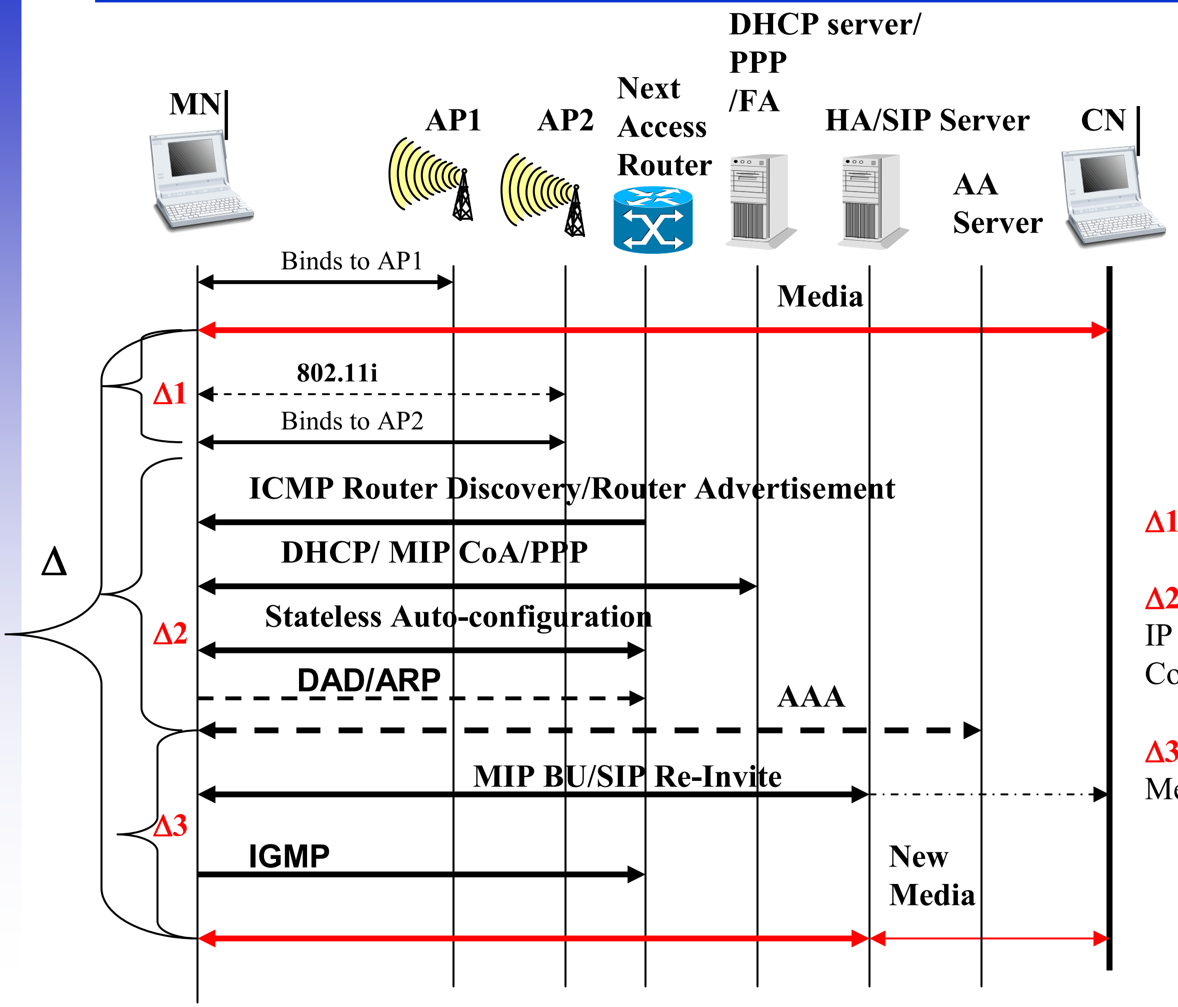
Outline

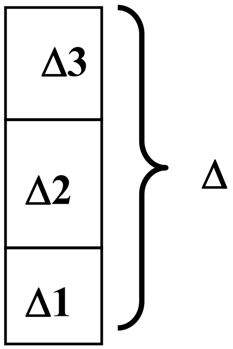
- Motivation
- Handoff Delay during Wireless Internet Roaming
- Fast Handoff Related Work
- Proposed Method: Media-independent Pre-Authentication
- Demonstration and Results
- Conclusions/Future Work

Motivation

- It is desirable to limit the jitter, delay and packet loss for real-time and non-real-time traffic
  - e.g.,150 ms end-to-end delay for interactive traffic such as VoIP, 2% packet loss is allowed
- Delay due to handoff takes place at several layers
  - Layer 2 (handoff between AP)
  - Layer 3 (IP address acquisition, Configuration, Authentication, Authorization)
  - Binding Update, Media Redirection
- Rapid handoff will contribute to overall delay and packet loss
- Thus it is essential to reduce the handoff delay introduced at different layers
- We propose a fast-handoff mechanism to reduce the handoff-delay and packet loss

Handoff Latency





Δ1- L2 Hand-over Latency Delay

Δ2 – Delay due to
IP Address Acquisition and
Configuration, authentication, authorization

Δ3 – Binding update and
Media Redirection delay

Problem in Mobility Management Protocols

- Problem 1 (performance): Operations for updating higher-layer context (i.e., IP address acquisition, mobility binding update, authentication etc.) occur after link-layer handover
  - Processing and/or signaling delay for each operation accumulates
  - Longer packet loss period due to handoff delay
  - No solutions exist for <u>single-interface host</u>
- Problem 2 (security): Existing mobility optimization mechanisms do not provide secure handover signaling especially for roaming cases
  - A secure mobility optimization mechanism that is tied with AAA (Authentication, Authorization and Accounting) and can deal with inter-subnet and inter-domain handover is needed
- Problem 3 (applicability): Existing mobility optimization mechanisms are tightly coupled with particular mobility management protocols
  - FMIPv6 and HMIP are defined for Mobile IPv6 only
  - A mobility optimization mechanism that is applicable to any mobility management protocol is needed

Mobility Optimization - Related Work

- Cellular IP, HAWAII - Micro Mobility
- MIP-Regional Registration, Mobile-IP low latency, IDMP
- HMIPv6, FMIPv6 (IPv6)
- Yokota et al - Link Layer Assisted handoff
- Shin et al, Velayos et al - Layer 2 delay reduction
- Gwon et al, - Tunneling between FAs, Enhanced Forwarding PAR
- SIP-Fast Handoff - Application layer mobility optimization
- DHCP Rapid-Commit, Optimized DAD - Faster IP address acquisition

Media-independent Pre-Authentication (MPA)

- MPA is:
  - a mobile-assisted higher-layer authentication, authorization and handover scheme that is performed prior to establishing L2 connectivity to a network where mobile may move in near future
- MPA provides a secure and seamless mobility optimization that works for
  - Inter-subnet handoff
  - Inter-domain handoff
  - Inter-technology handoff
    - Use of multiple interfaces
- MPA works with any mobility management protocol
  - MIP(v4,v6), SIPMM etc.

Functional Components of MPA

1) Pre-authentication/authorization

- Used for establishing a security association (SA) between the mobile and a network to which the mobile **may** move
- L2 pre-authentication can also be enabled based on the established SA

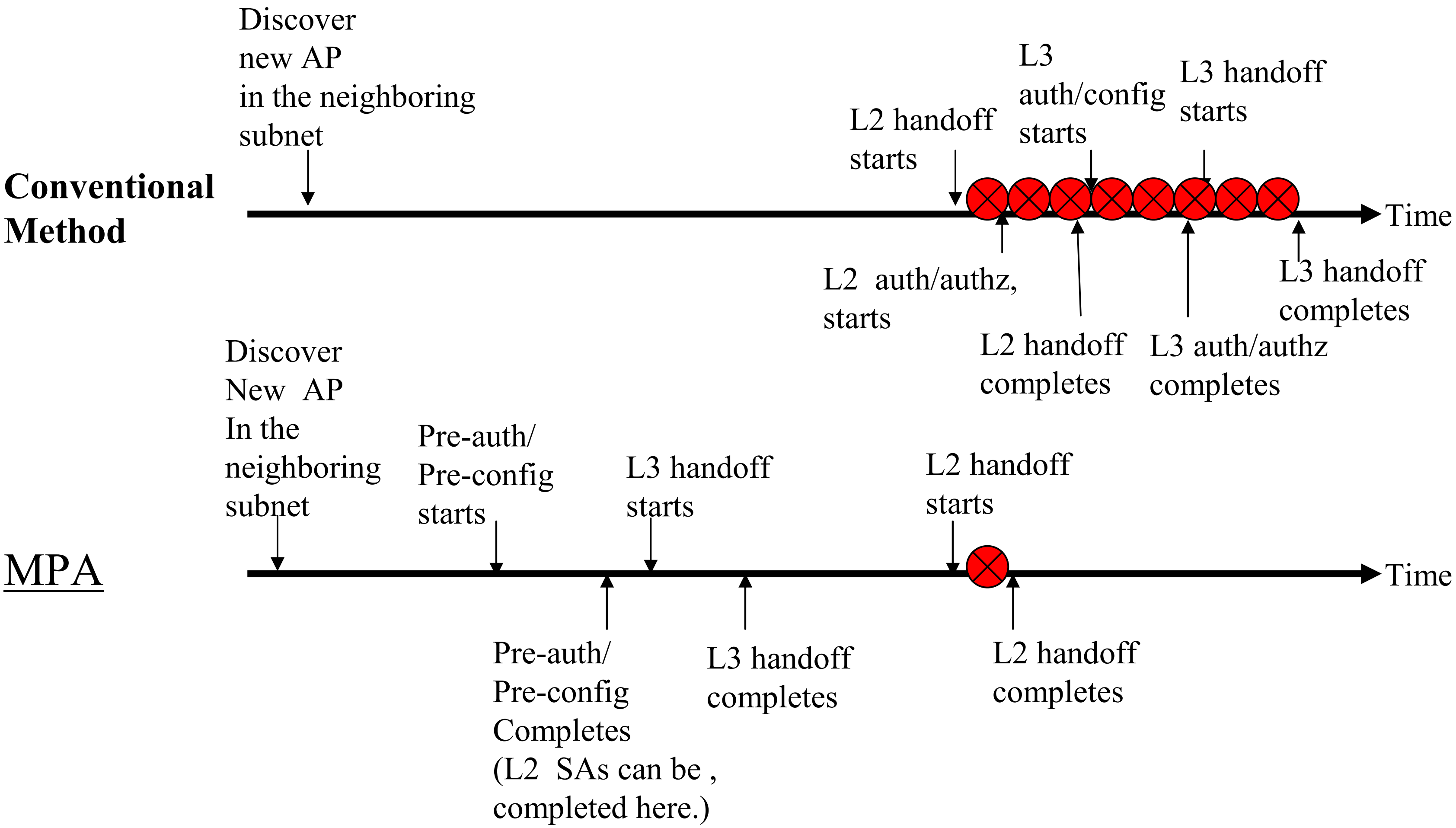
2) Pre-configuration

- Used for establishing contexts specific to the network to which the mobile **may** move (e.g., nCoA)
- The SA created in (1) are used to perform secured configuration procedure

3) Secured Proactive Handover

- Used for sending/receiving IP packets based on the pre-authorized contexts by using the contexts of the current network

Expected Result during handoff



Conventional Method

Discover new AP in the neighboring subnet

L2 handoff starts

L3 auth/config starts

L3 handoff starts

Time

L2 auth/authz, starts

L2 handoff completes

L3 auth/authz completes

L3 handoff completes

MPA

Discover New AP In the neighboring subnet

Pre-auth/ Pre-config starts

L3 handoff starts

L2 handoff starts

Time

Pre-auth/ Pre-config Completes (L2 SAs can be , completed here.)

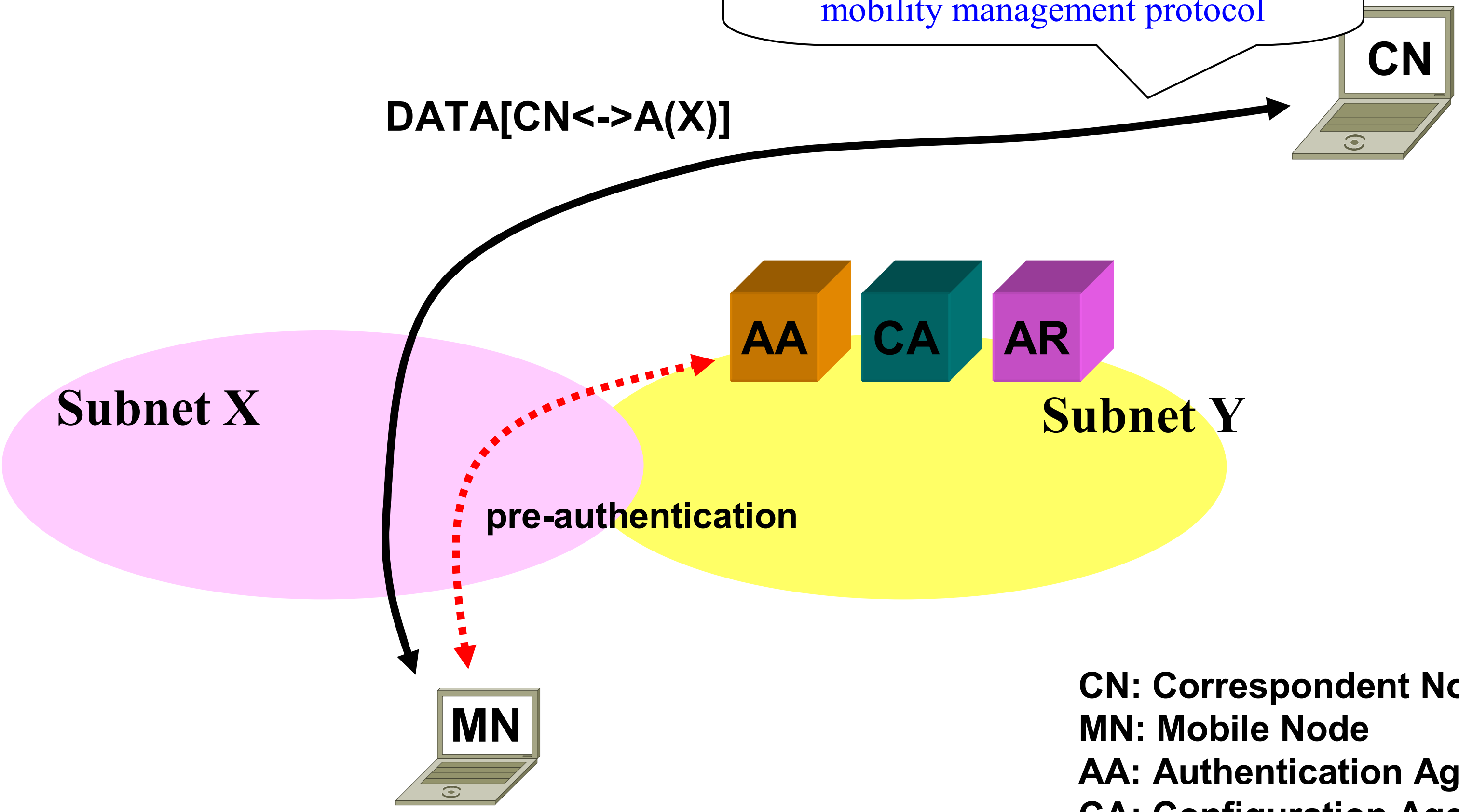
L3 handoff completes

L2 handoff completes

⊗ Critical period (communication interruption can occur)

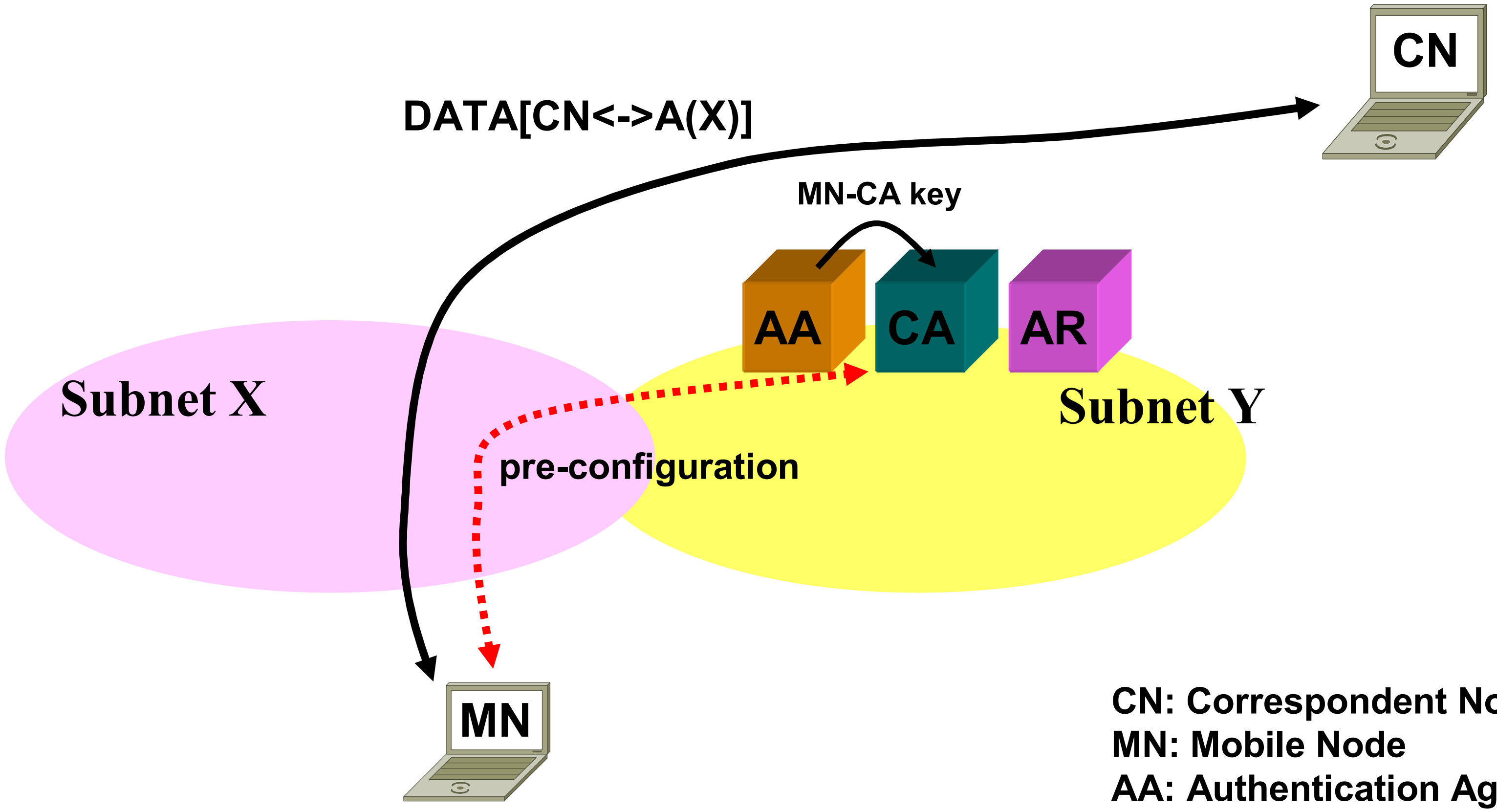
Pre-Authentication

SIP mobility is just an example mobility protocol. MPA works for any mobility management protocol



CN: Correspondent Node
MN: Mobile Node
AA: Authentication Agent
CA: Configuration Agent
AR: Access Router

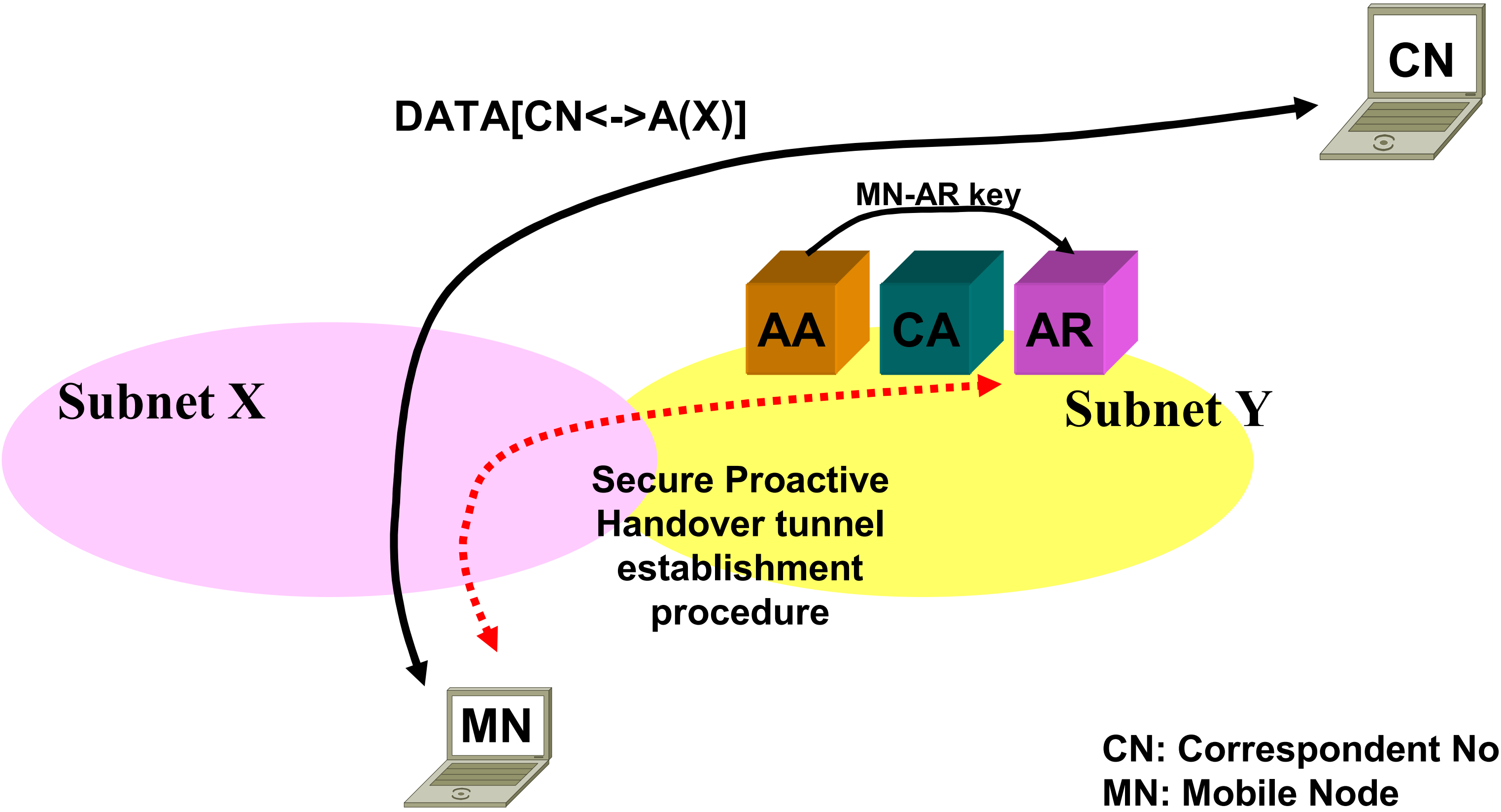
Pre-configuration



IP address: A(X)
Current subnet: X
Status: Pre-authentication done
Action: pre-configuration

CN: Correspondent Node
MN: Mobile Node
AA: Authentication Agent
CA: Configuration Agent
AR: Access Router

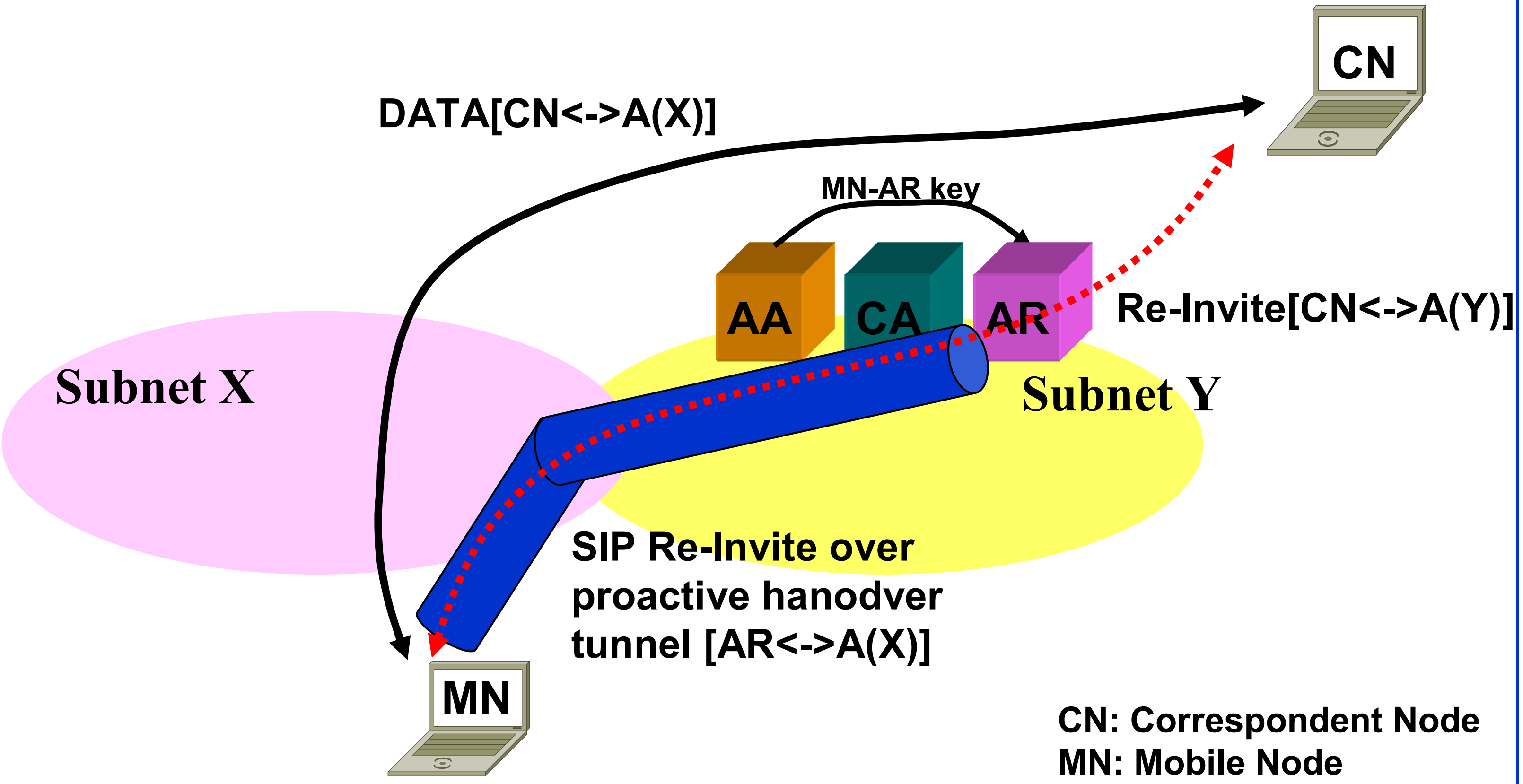
Pre-Configuration (Cont.)



IP address: A(X), A(Y)
Current subnet: X
Status: <u>Pre-configuration done</u>
Action: SPH Initiation

CN: Correspondent Node
MN: Mobile Node
AA: Authentication Agent
CA: Configuration Agent
AR: Access Router

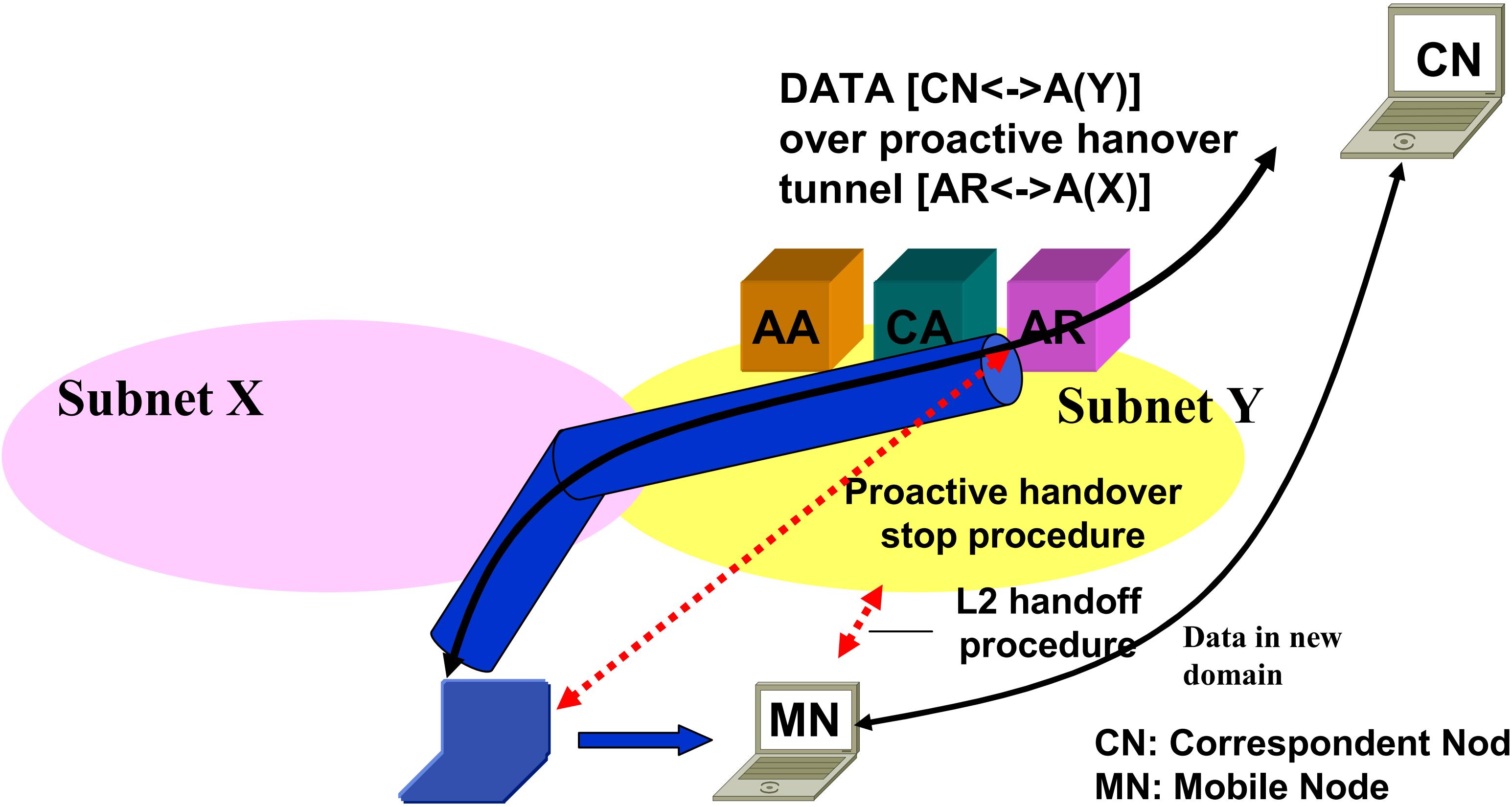
Secured Proactive Handover: Main Phase



IP address: A(X), A(Y)
Current subnet: X
Status: PH tunnel established
Action: SIP Re-Invite

CN: Correspondent Node
MN: Mobile Node
AA: Authentication Agent
CA: Configuration Agent
AR: Access Router

Secured Proactive Handover: Completion



CN

DATA [CN<->A(Y)]
over proactive hanover
tunnel [AR<->A(X)]

AA

CA

AR

Subnet X

Subnet Y

Proactive handover
stop procedure

L2 handoff
procedure

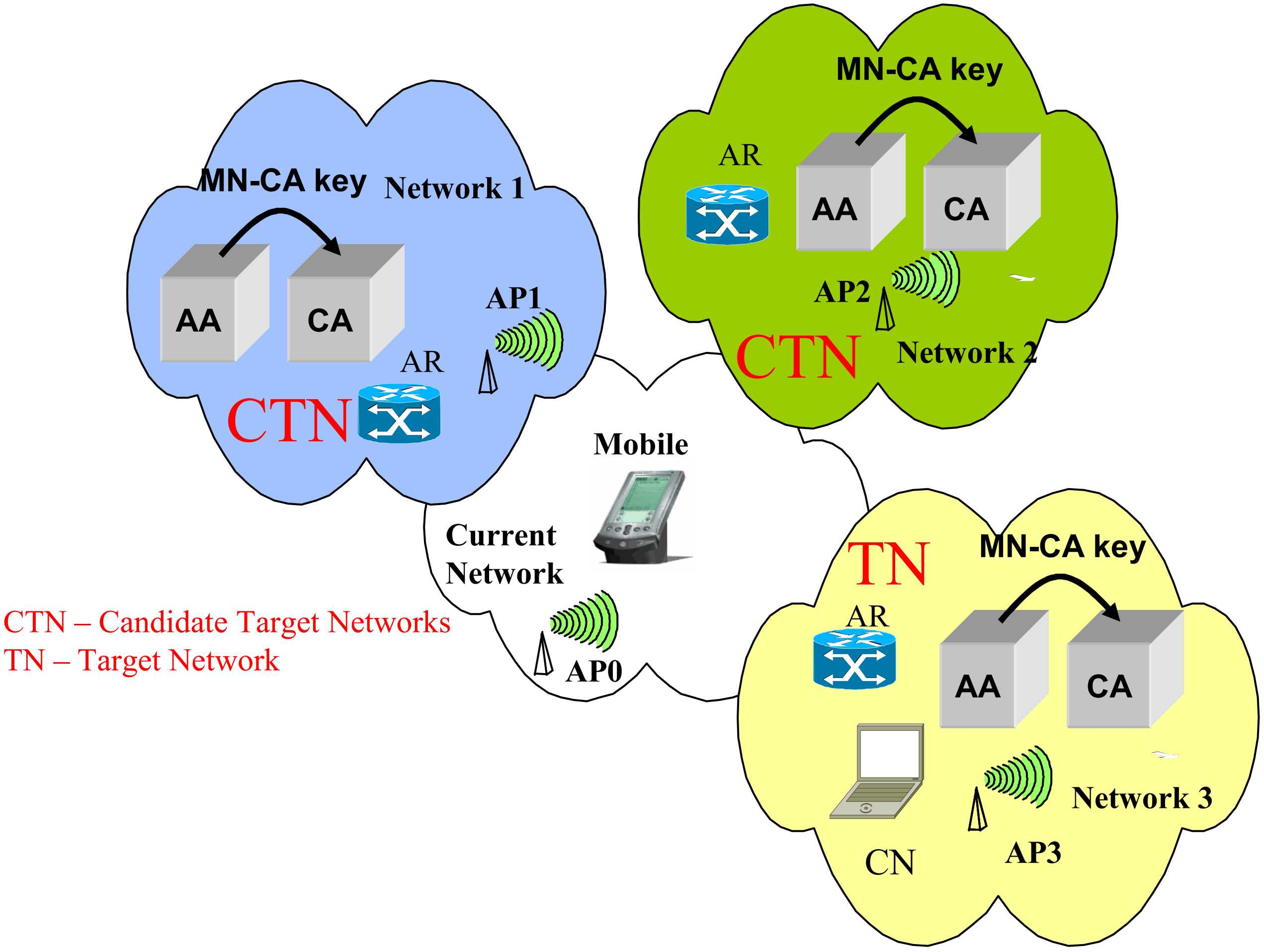
Data in new
domain

MN

IP address: A(X), A(Y)
Current subnet: X
Status: SIP Re-Invite done
Action: PH Completion

CN: Correspondent Node
MN: Mobile Node
AA: Authentication Agent
CA: Configuration Agent
AR: Access Router

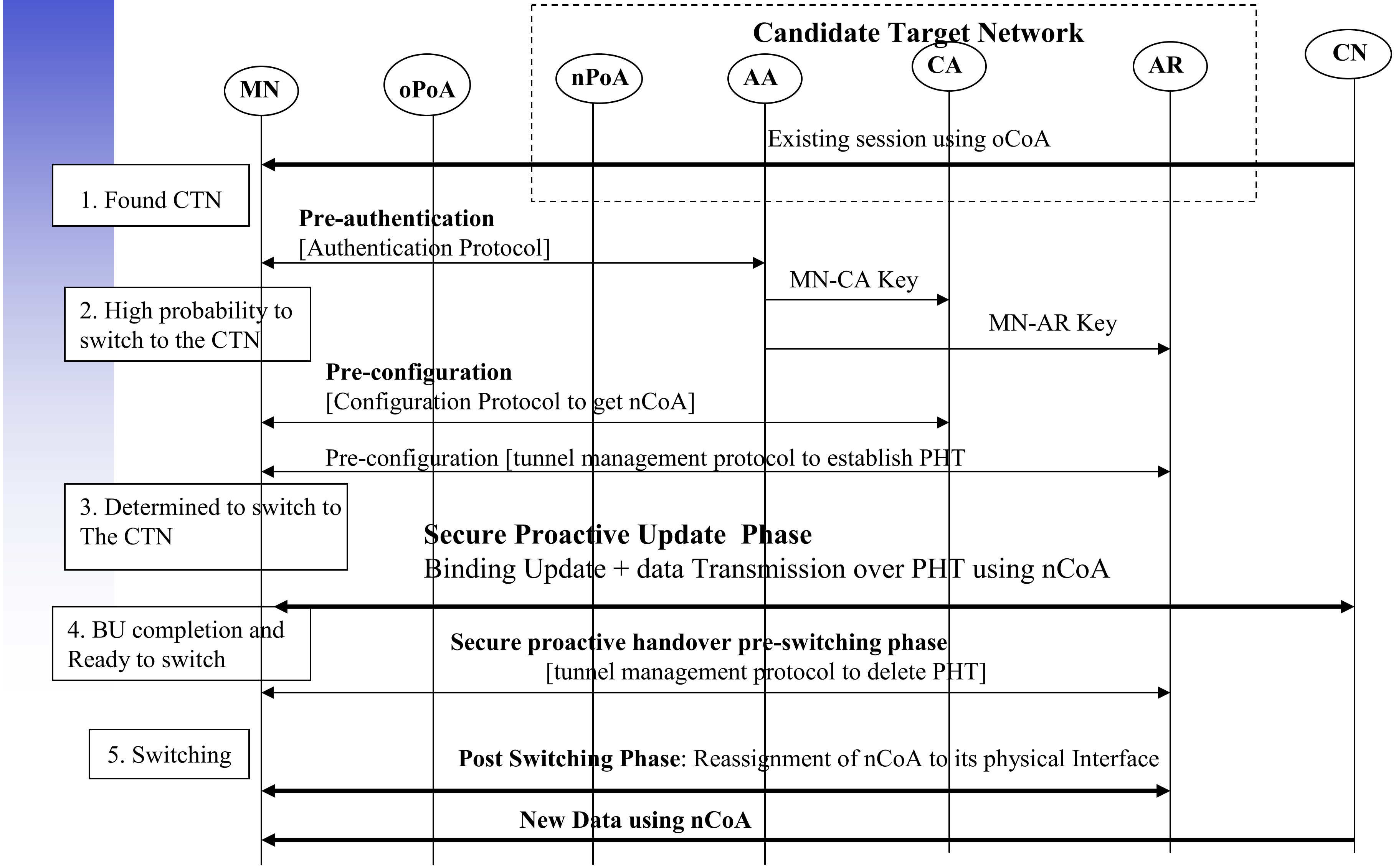
Mobile-assisted Seamless Handoff (a scenario)



CTN – Candidate Target Networks
TN – Target Network

Information Service (e.g.,802.21) mechanism can help locate the neighboring network elements in the candidate target networks (CTN)

MPA Communication Flow


Candidate Target Network
MN
oPoA
nPoA
AA
CA
AR
CN
Existing session using oCoA
1. Found CTN
Pre-authentication
[Authentication Protocol]
MN-CA Key
MN-AR Key
2. High probability to switch to the CTN
Pre-configuration
[Configuration Protocol to get nCoA]
Pre-configuration [tunnel management protocol to establish PHT
3. Determined to switch to The CTN
Secure Proactive Update Phase
Binding Update + data Transmission over PHT using nCoA
4. BU completion and Ready to switch
Secure proactive handover pre-switching phase
[tunnel management protocol to delete PHT]
5. Switching
Post Switching Phase: Reassignment of nCoA to its physical Interface
New Data using nCoA

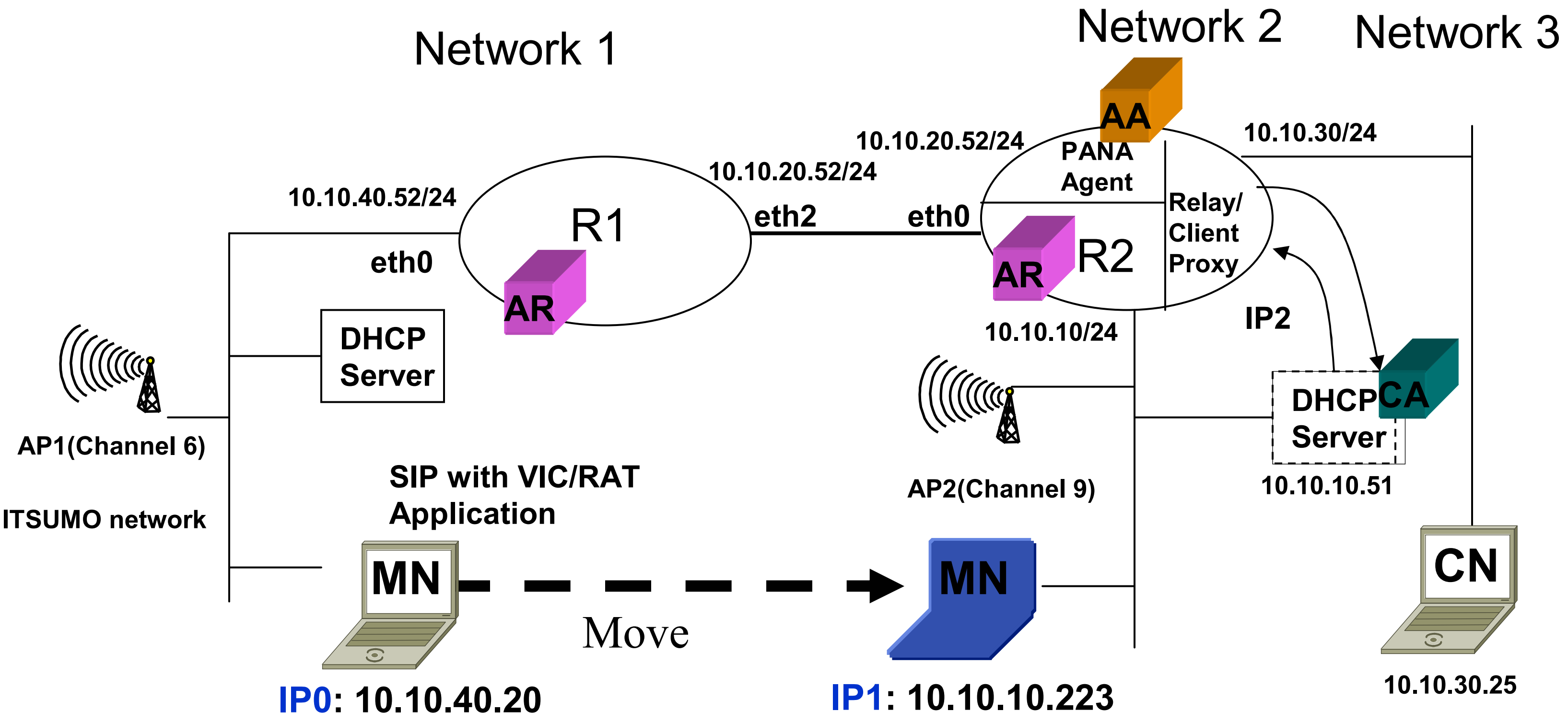
MPA Optimization Issues

- Network Discovery
  - Discover the neighboring network elements (e.g., Routers, APs, Authentication Agents)
  - 802.21 (Information Service), 802.11u, WIEN SG, CARD, DNS/SLP
- Proactive IP Address Acquisition
- Proactive Duplicate IP address Detection
- Proactive Address Resolution
- Proactive Tunnel Management
- Proactive Mobility Binding Update
- Bootstrap Link-layer Security in CTN using L3 Pre-authentication

Protocol Set for the MPA demonstration

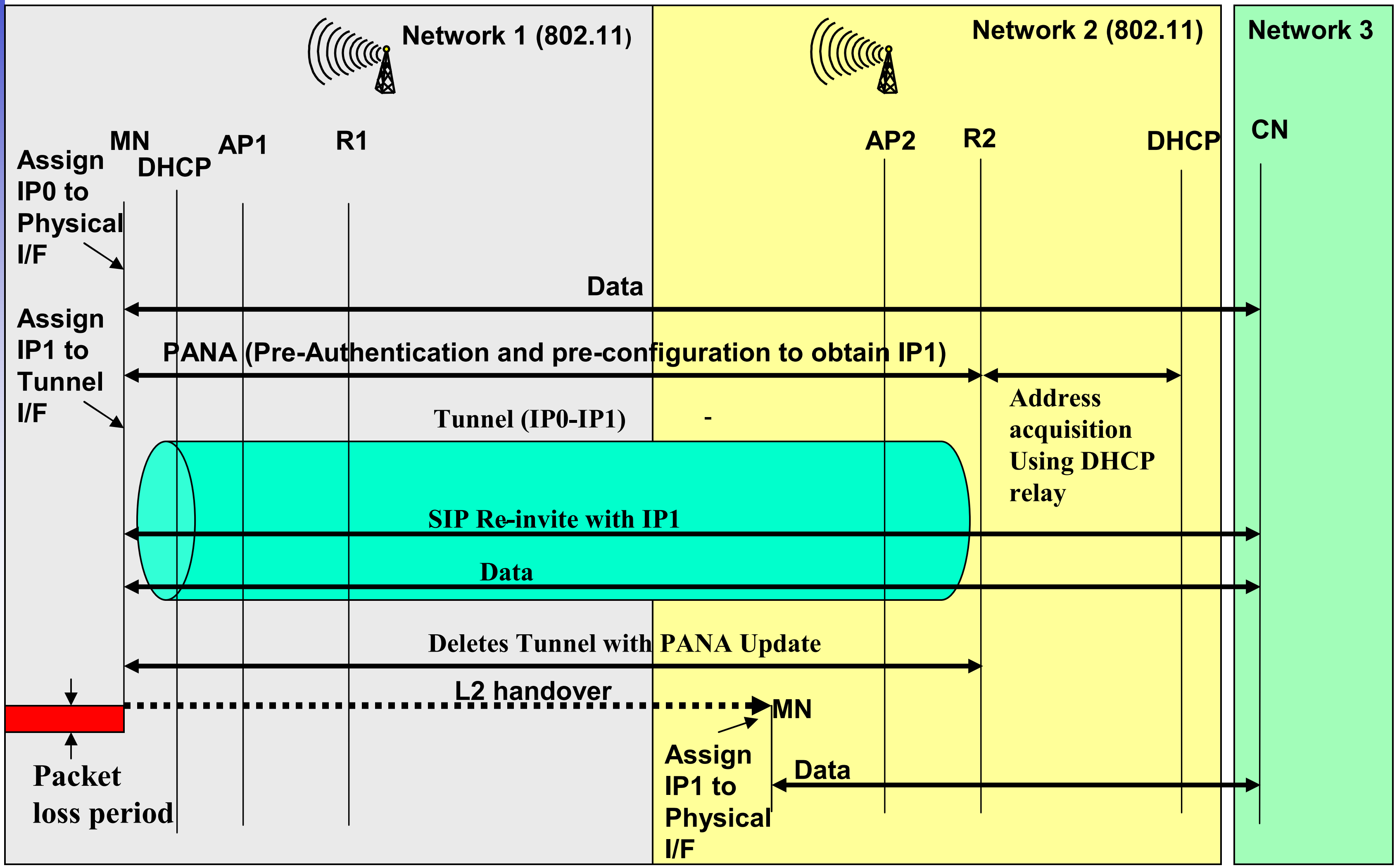
Pre-authentication protocol	PANA
Pre-configuration protocol	PANA, DHCP Relay
Proactive handover tunneling protocol	IP-in-IP
Proactive handover tunnel management protocol	PANA
Mobility management protocol	SIP Mobility
Link-layer security	None

Experimental Network in the Lab.

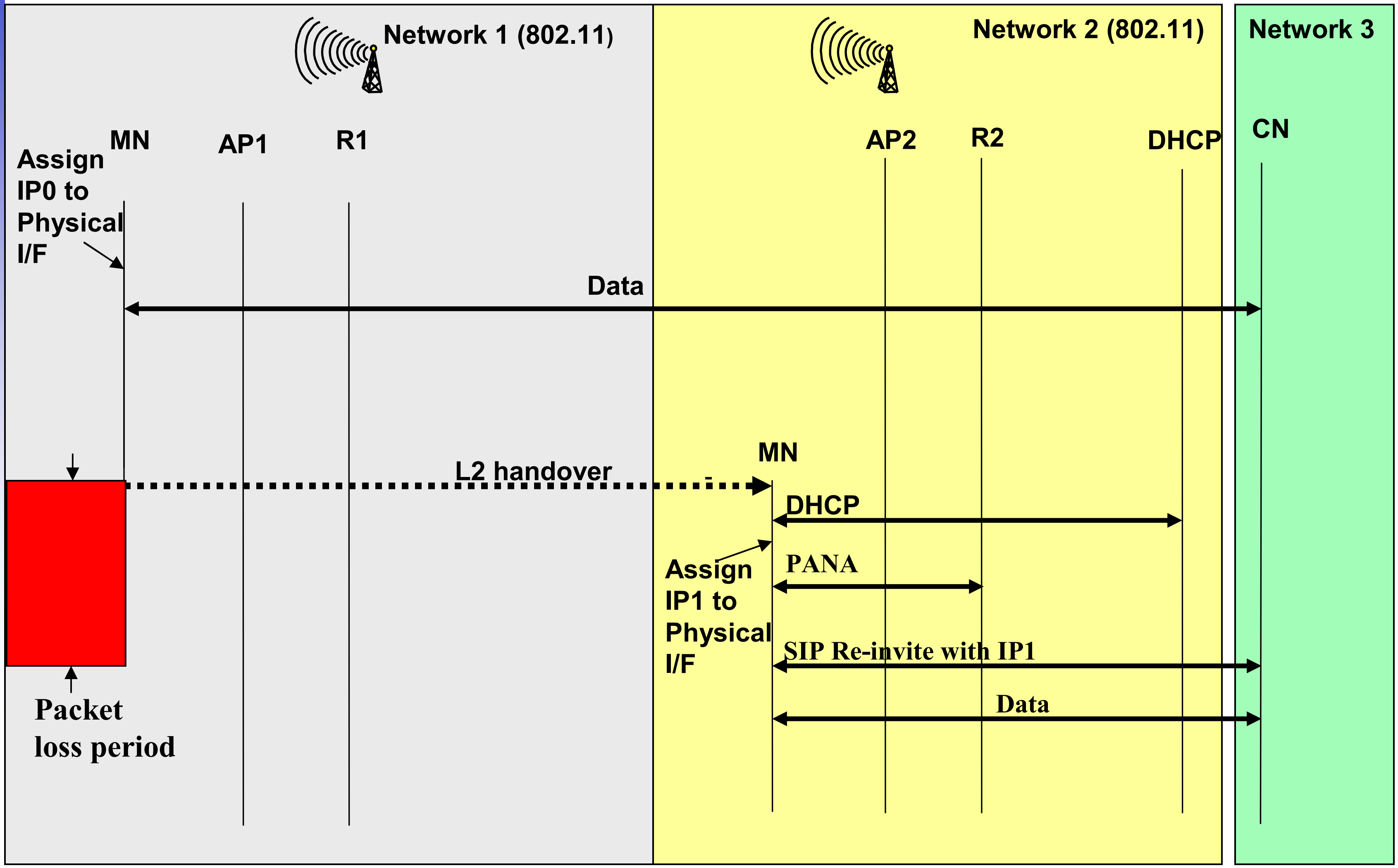


AP1, AP2: Access Point
R1, R2: Access Router
MN: Mobile Node
CN: Correspondent Node
IP0, IP1: IP address of MN

Protocol flow for MPA

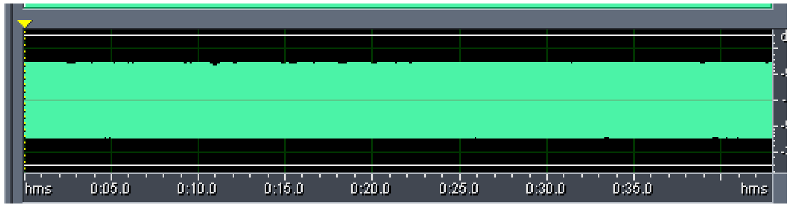

Network 1 (802.11)
Network 2 (802.11)
Network 3
MN
DHCP
AP1
R1
AP2
R2
DHCP
CN
Assign IP0 to Physical I/F
Data
Assign IP1 to Tunnel I/F
PANA (Pre-Authentication and pre-configuration to obtain IP1)
Address acquisition Using DHCP relay
Tunnel (IP0-IP1)
-
SIP Re-invite with IP1
Data
Deletes Tunnel with PANA Update
L2 handover
MN
Assign IP1 to Physical I/F
Data
Packet loss period

Protocol Flow for Non-MPA



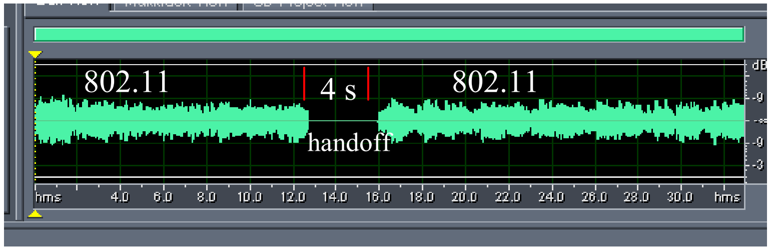
Performance (MPA-Non-MPA)

- MPA
  - No packet loss during pre-authentication, pre-configuration and pro-active handoff before L2 handoff
  - Only 1 packet loss, 14 ms delay during handoff mostly transient data
    - Includes delay due to layer 2, update to delete the tunnel on the router
    - We also reduced the layer 2 delay in hostap Driver
    - L2 delay depends upon driver and chipset



MPA Approach

- non-MPA
  - About 200 packets loss, ~ 4 s during handover
    - Includes standard delay due to layer 2, IP address acquisition, Re-Invite, Authentication/Authorization
  - Could be more if we have firewalls also set up



Non-MPA Approach

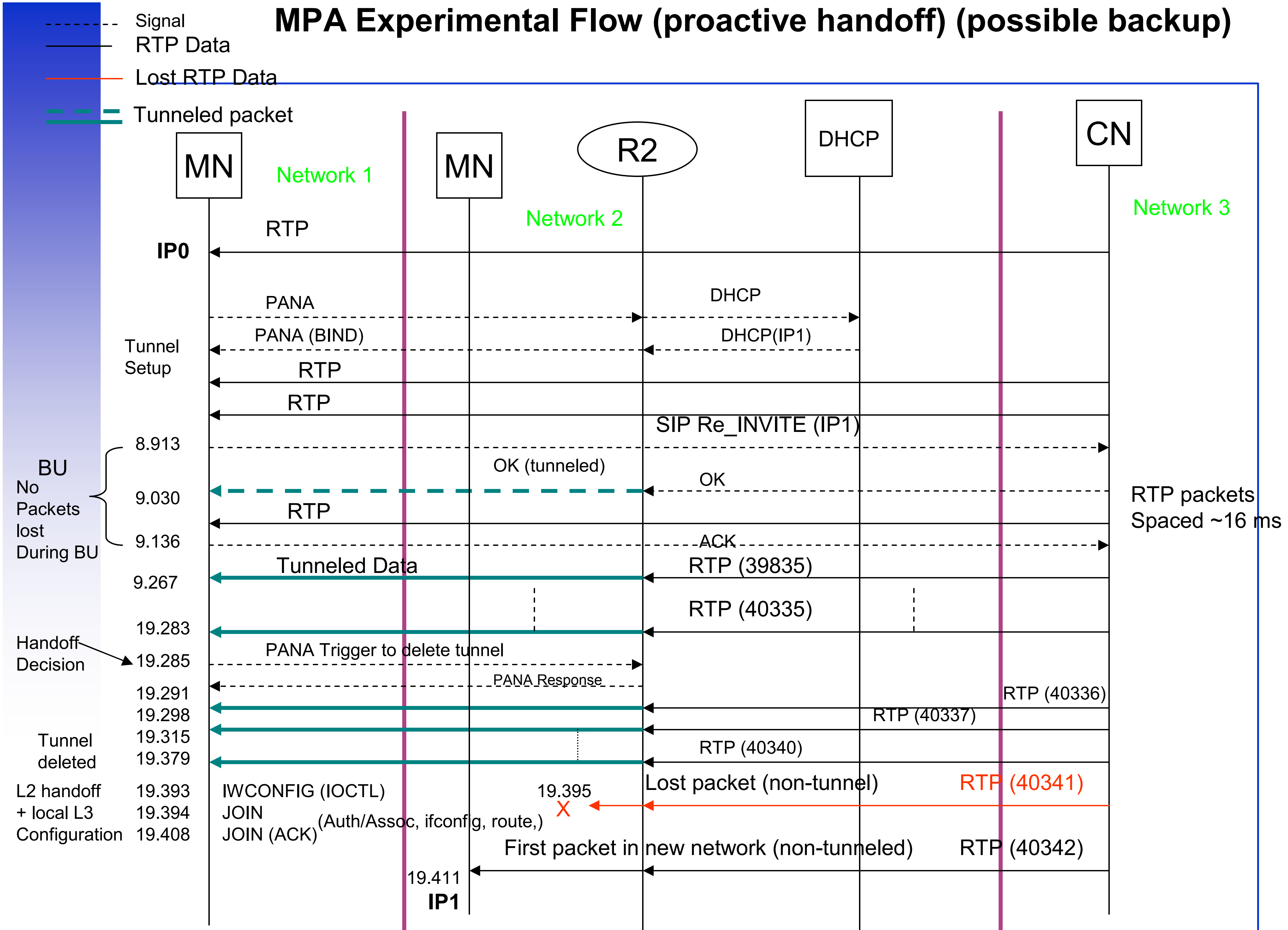
Conclusions/Future Work

- MPA framework provides an optimized mobility management solution independent of mobility protocol used
- We demonstrated an initial prototype implementation and results
- MPA works over single interface and multiple interfaces (e.g., 802.11, CDMA)
- Define a more integrated architecture that works in conjunction information discovery scheme (e.g.,802.21, 802.11u)
- Comments/Suggestions/Questions
- Next steps?

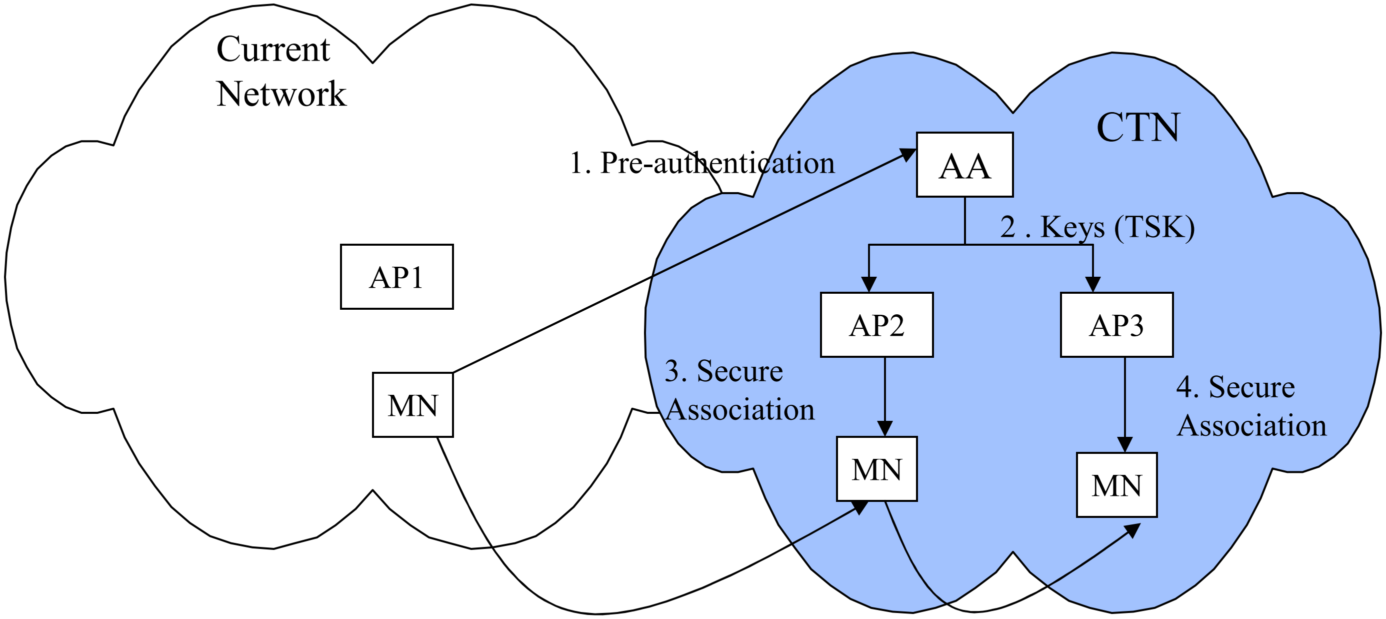
Thank you!

Backup Slides

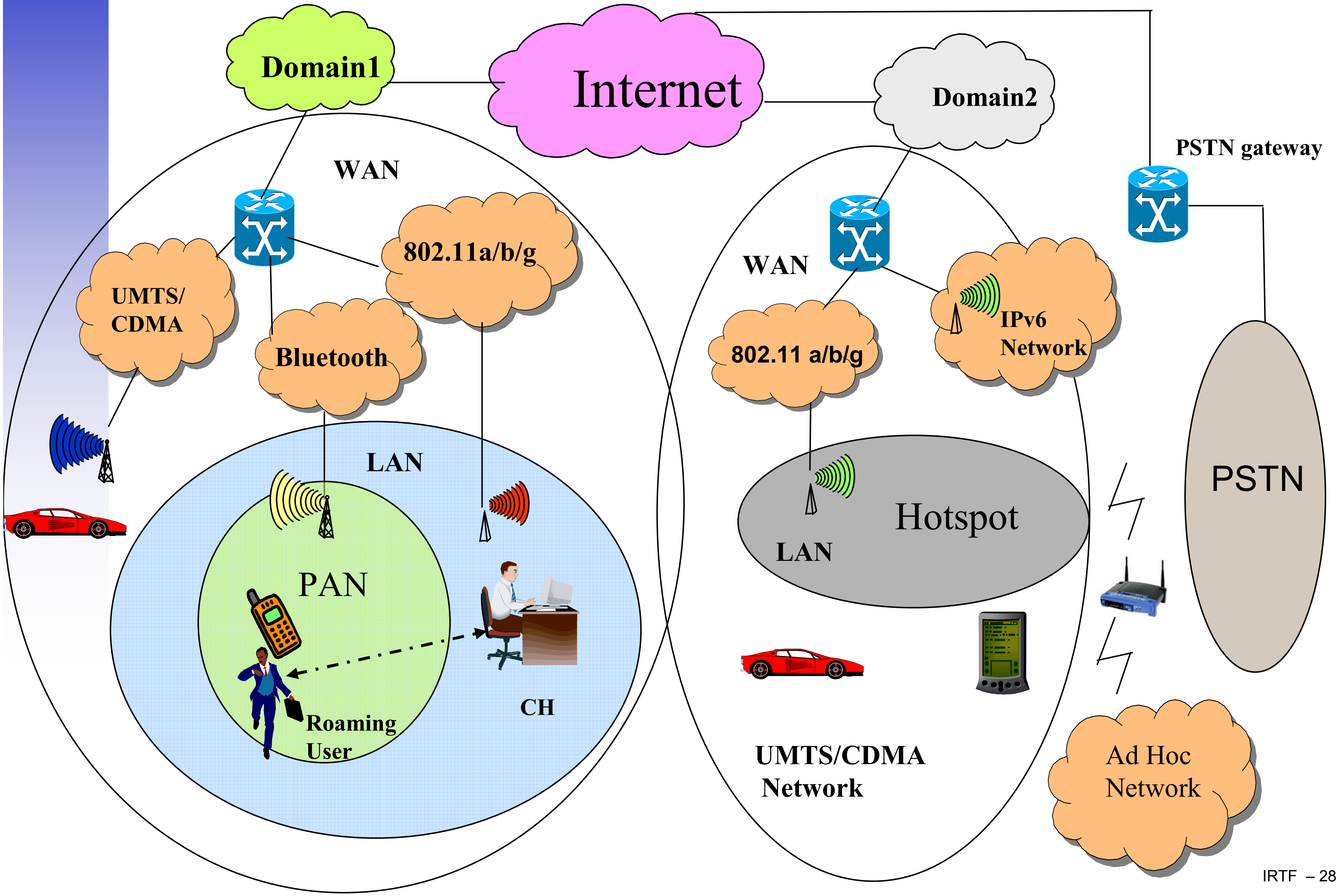
MPA Experimental Flow (proactive handoff) (possible backup)



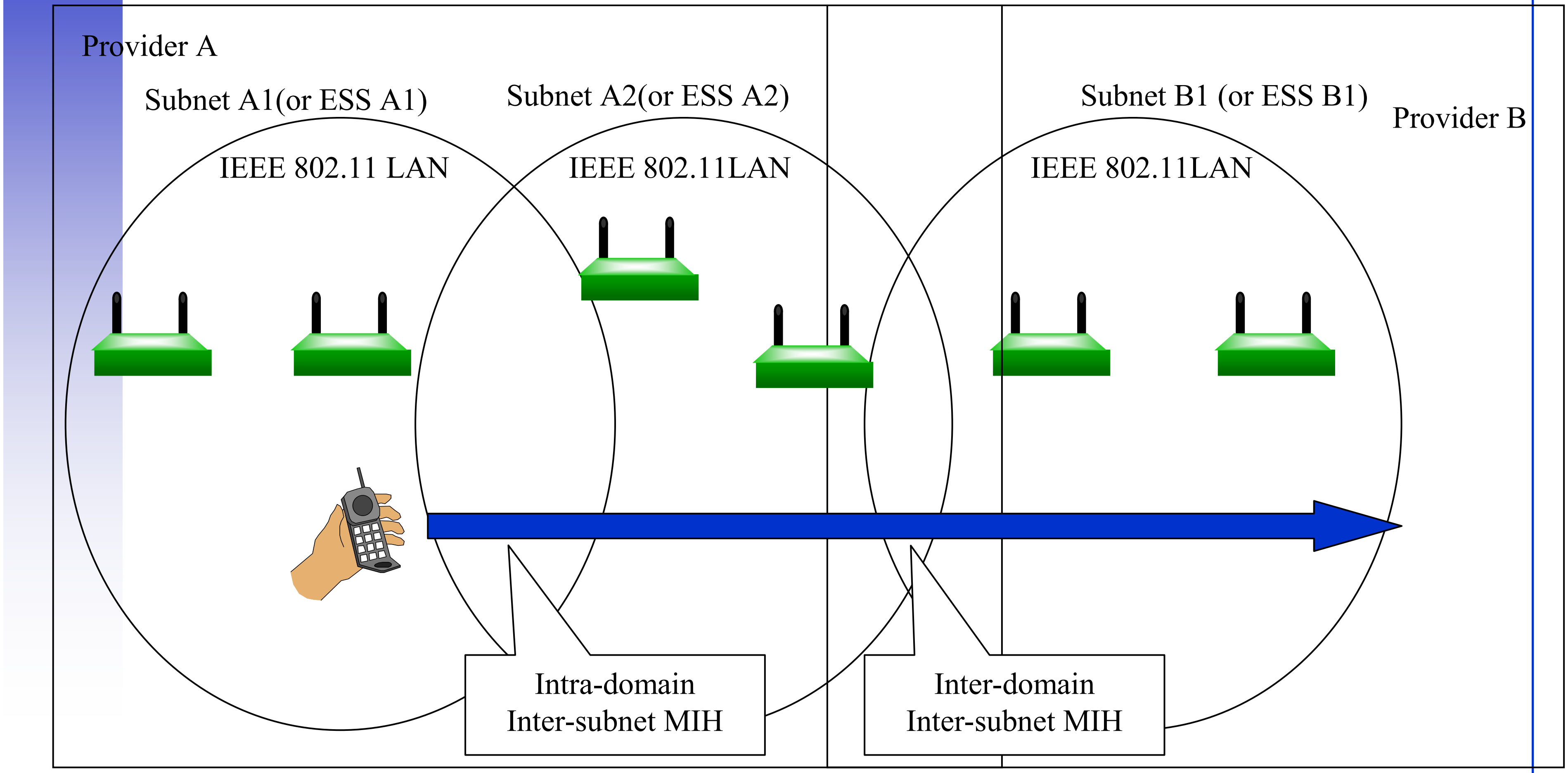
Bootstrapping Link-layer security using L3-Preauth



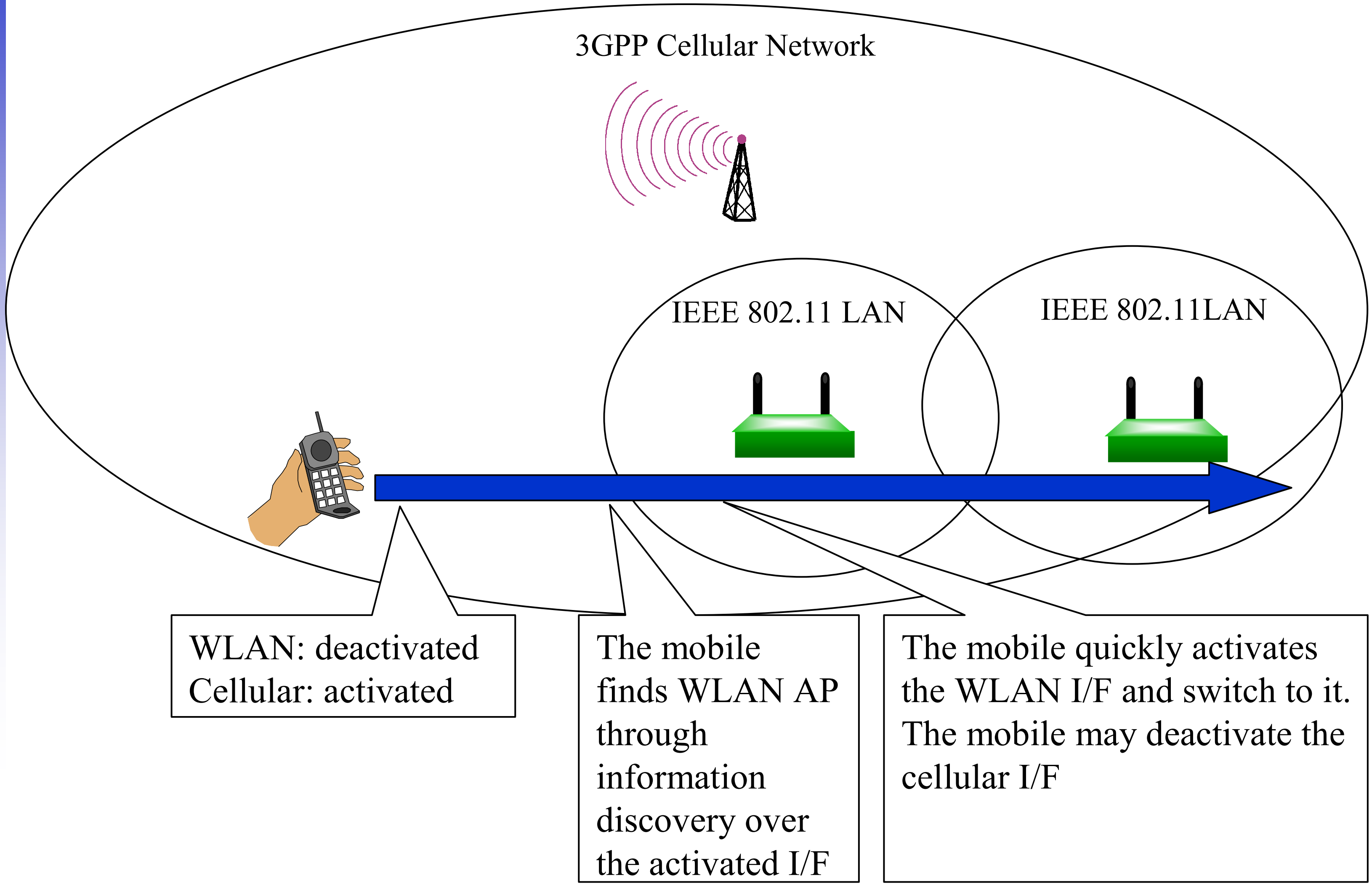
Mobile Wireless Internet: A Scenario (possible backup)



Single Radio Interface Roaming Scenario (possible backup)



Multiple Radio Interface Roaming Scenario (possible backup)



WLAN: deactivated
Cellular: activated

The mobile finds WLAN AP through information discovery over the activated I/F

The mobile quickly activates the WLAN I/F and switch to it. The mobile may deactivate the cellular I/F