

Seamless and Secure Handover for Heterogeneous Mobility using PANA, IEEE 802.21 and Pre-authentication

Yoshihiro Ohba (yohba@tari.toshiba.com)
Toshiba America Research, Inc.

**B3G Cluster Workshop on Mobility Technologies in the Internet
Brussels, October 3rd 2006**

Contents

- Secure handover optimization using PANA
- Media-Independent Handover: IEEE 802.21
- Advanced Topic: MPA (Media-Independent Pre-authentication)
- New activity in IETF for secure handover optimization - HOKEY

Secure Handover Optimization Using PANA

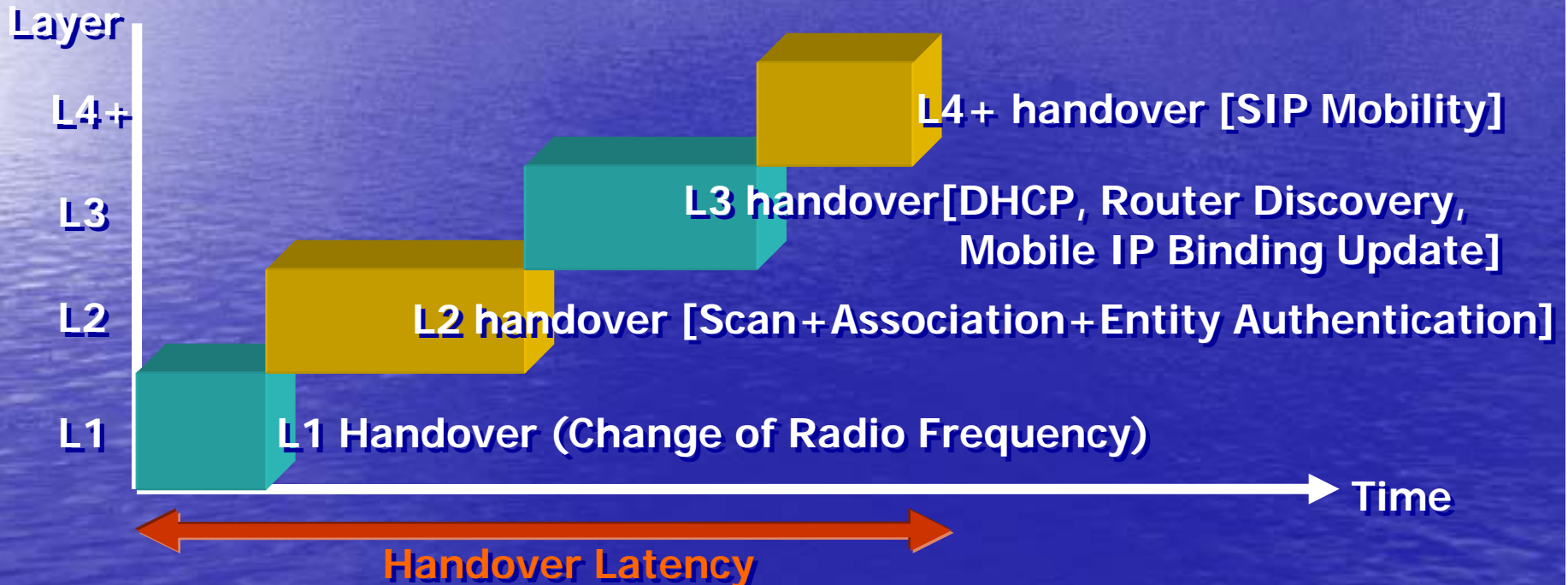
October 3rd, 2006

B3G Cluster Workshop on Mobility
Technologies in the Internet

3

Handover spans multiple layers

- The entire handover signaling consists of handover signaling at each layer
- Without optimization, handover delay at each layer contributes to the entire handover processing delay
- Handover signaling needs to be secured

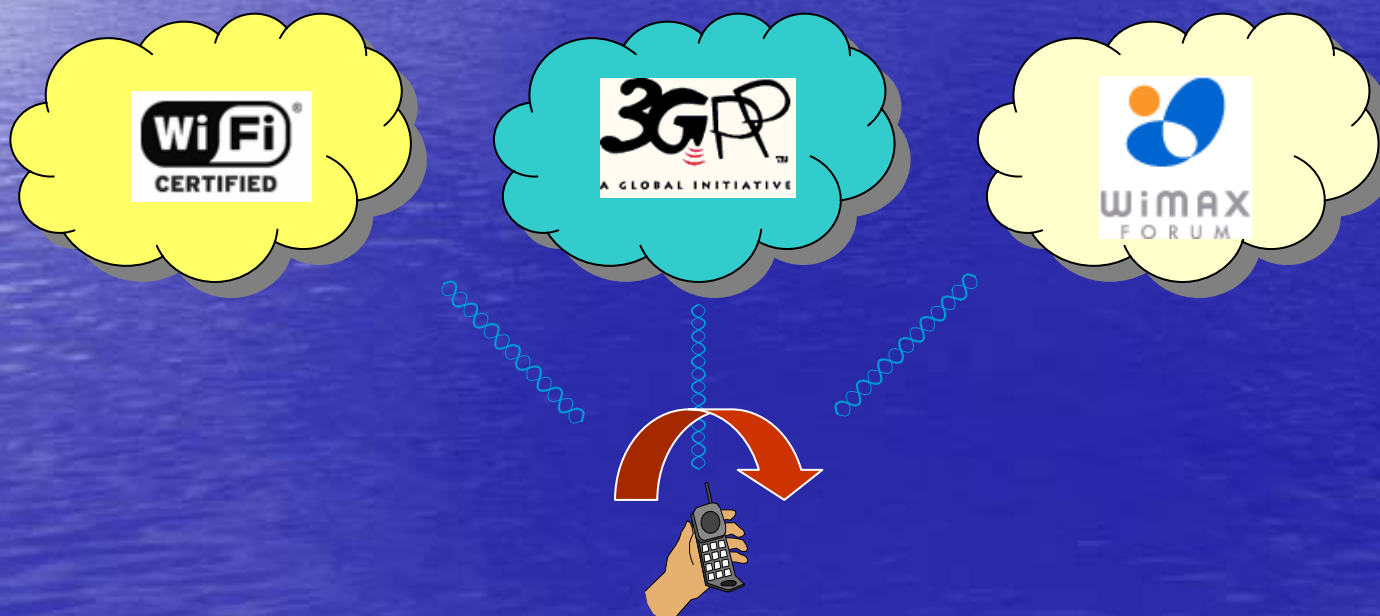


Need for Secure & Low-Latency Handover Signaling

B3G Cluster Workshop on Mobility
Technologies in the Internet

Handover spans multiple access technologies

- Handover between different access technologies is becoming important
 - IEEE 802.21
 - FMC (Fixed Mobile Convergence)
- WIMAX is recognized as another important wireless technology
- Need for inter-technology handover



Handover needs secure operation

- Handover signaling would need to be secured at each layer to avoid various attacks
- Specifically the following security threats exist in general
 - Eavesdropping and alteration of messages
 - Man-in-The-Middle (MiTM) attacks
 - Deniable of Service (DoS) attacks
- Secure handover support by link-layer
 - 802.11i/r, 802.16e
- Security Associations (SAs) used for securing handover signaling need to be established
 - Handover SAs

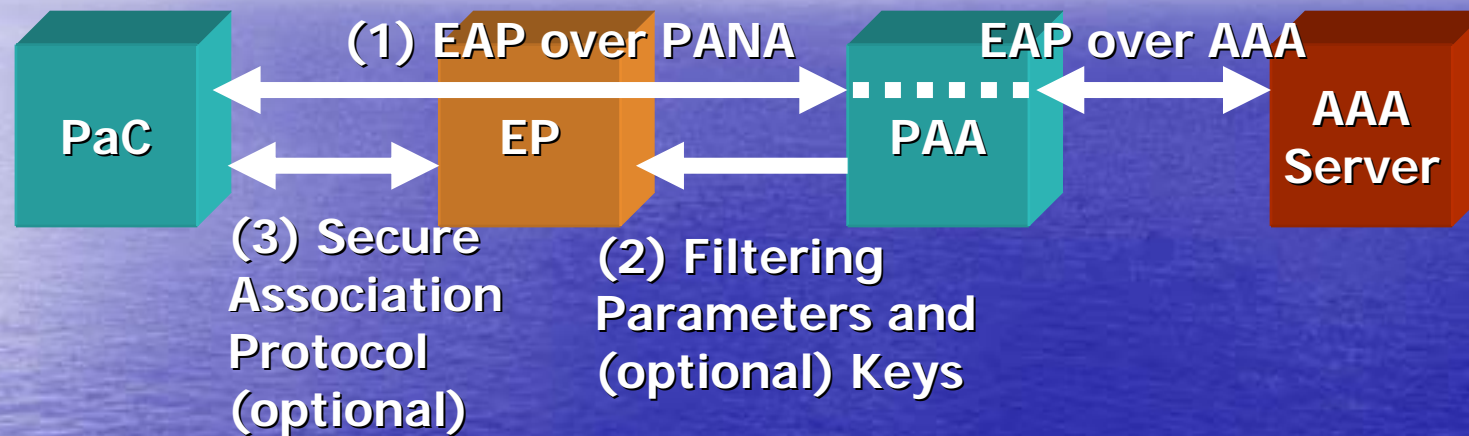
Establishment of Handover SAs

- A mobile needs to be able to make a handover to a visited network with which it does not have a statically configured handover SA
- An SA needs to be dynamically established (i.e., bootstrapped) based on “roaming-capable” infrastructure, i.e., AAA (Authentication, Authorization and Accounting)
- Considering inter-technology handover, it is better to use
 - L2-agnostic way of establishing a handover SA
 - Use of one handover SA for securing multiple access technologies
- PANA provides these two functionalities

What is PANA

- Protocol for carrying Authentication for Network Access
- An EAP transport protocol defined over UDP
- Basic Features
 - Allow decoupling of an entity that authenticates clients and an entity that executes access control
 - Establishment of a secure “session” for authentication and authorization
 - Bootstrapping lower-layer security (e.g., PSK mode of IKEv2 and 802.11i)
 - Service Provider Selection
- Status as of September 2006:
 - To go through 2nd IETF Last Call before IESG review
 - The specification is subject to change

PANA Framework



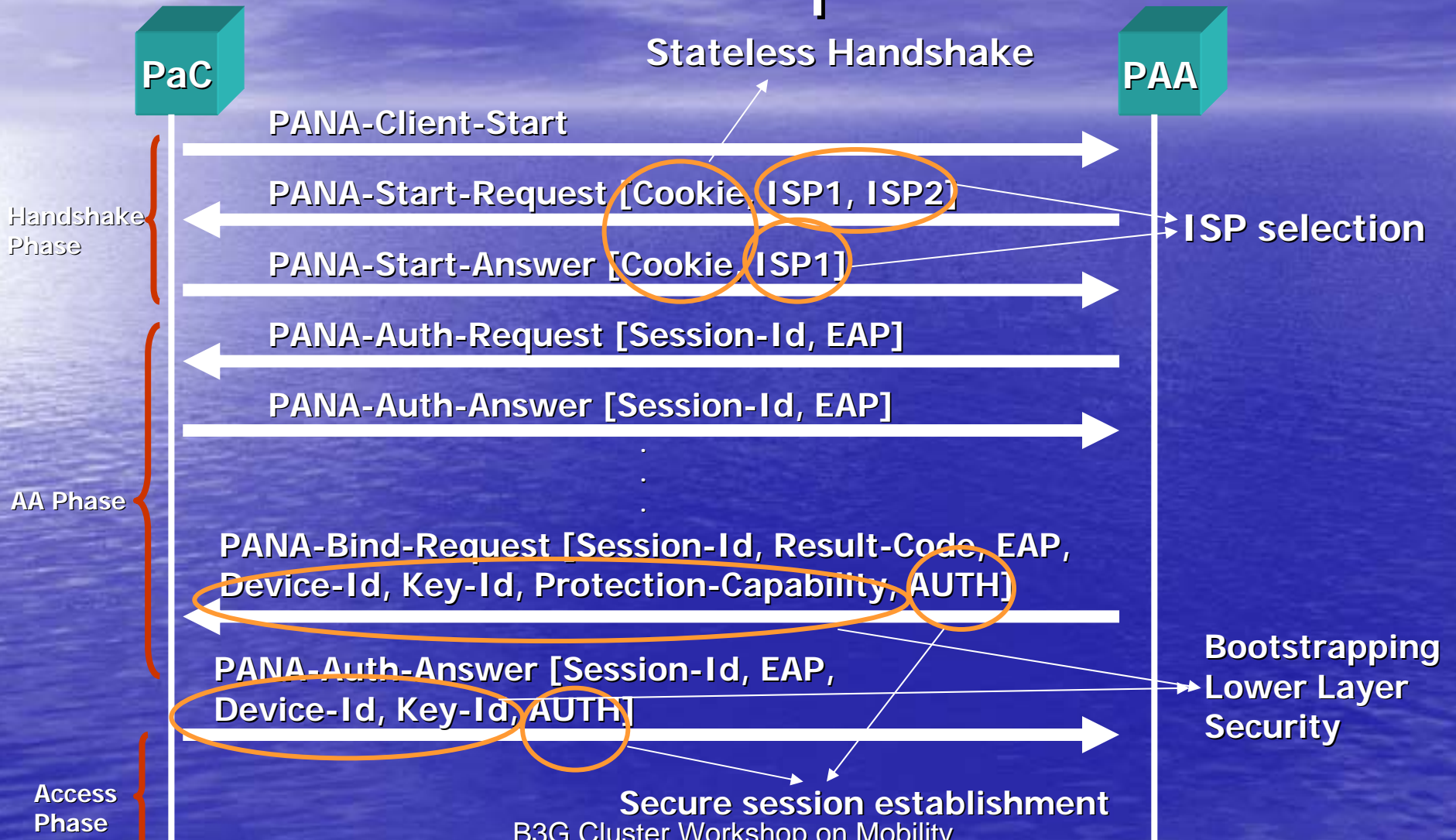
Example of Secure Association Protocol:
IKEv2, IEEE 802.11i 4-way handshake, etc.

PaC: PANA Client
PAA: PANA Authentication Agent
EP: Enforcement Point

PANA Protocol Phases

- **Handshake Phase**
 - Exchanging initial sequence numbers
 - Stateless and stateful handshake
- **Authentication and Authorization Phase**
 - EAP transport
 - Proof of possession of EAP Master Session Key (MSK)
 - PANA session establishment
- **Access Phase**
 - Use of EP for application traffic
 - Secure peer liveness test
- **Re-authentication Phase**
 - Protected EAP transport for re-authentication
- **Termination Phase**
 - PANA session teardown

PANA Protocol Sequence



Bootstrapping Lower Layer Security

- Media-independent master key derivation

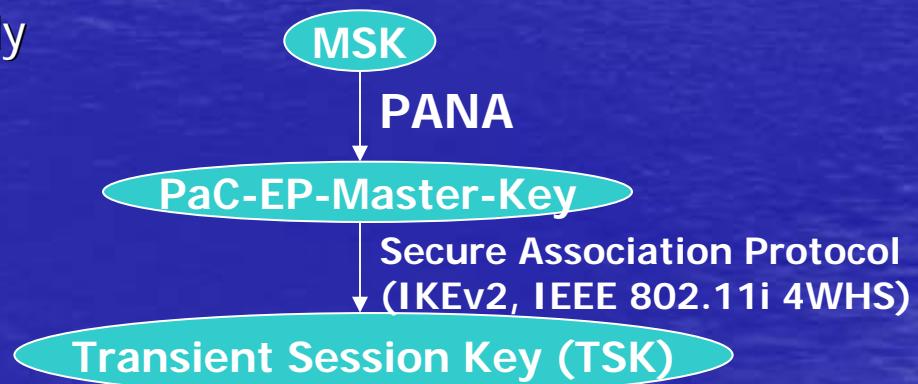
**PaC-EP-Master-Key = The first 64 octets of
prf+(MSK, "PaC-EP master key" |
Session ID | Key-ID | EP-Device-Id)**

prf+: Pseudo random function defined IKEv2

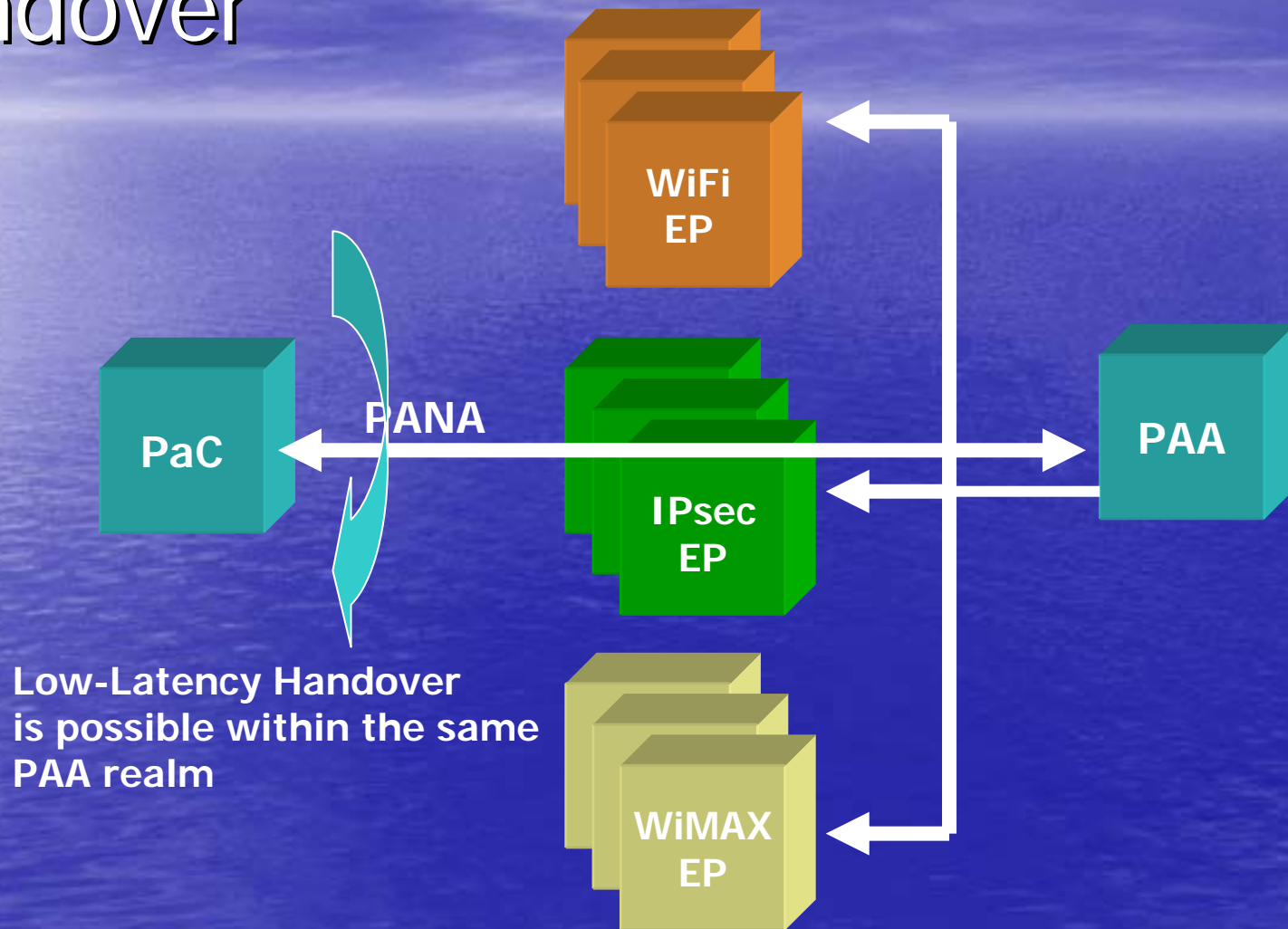
EP-Device-Id: Device Identifier of EP consisting of:

One-octet Address Family

Variable-length Address



PANA usage for Inter-technology handover

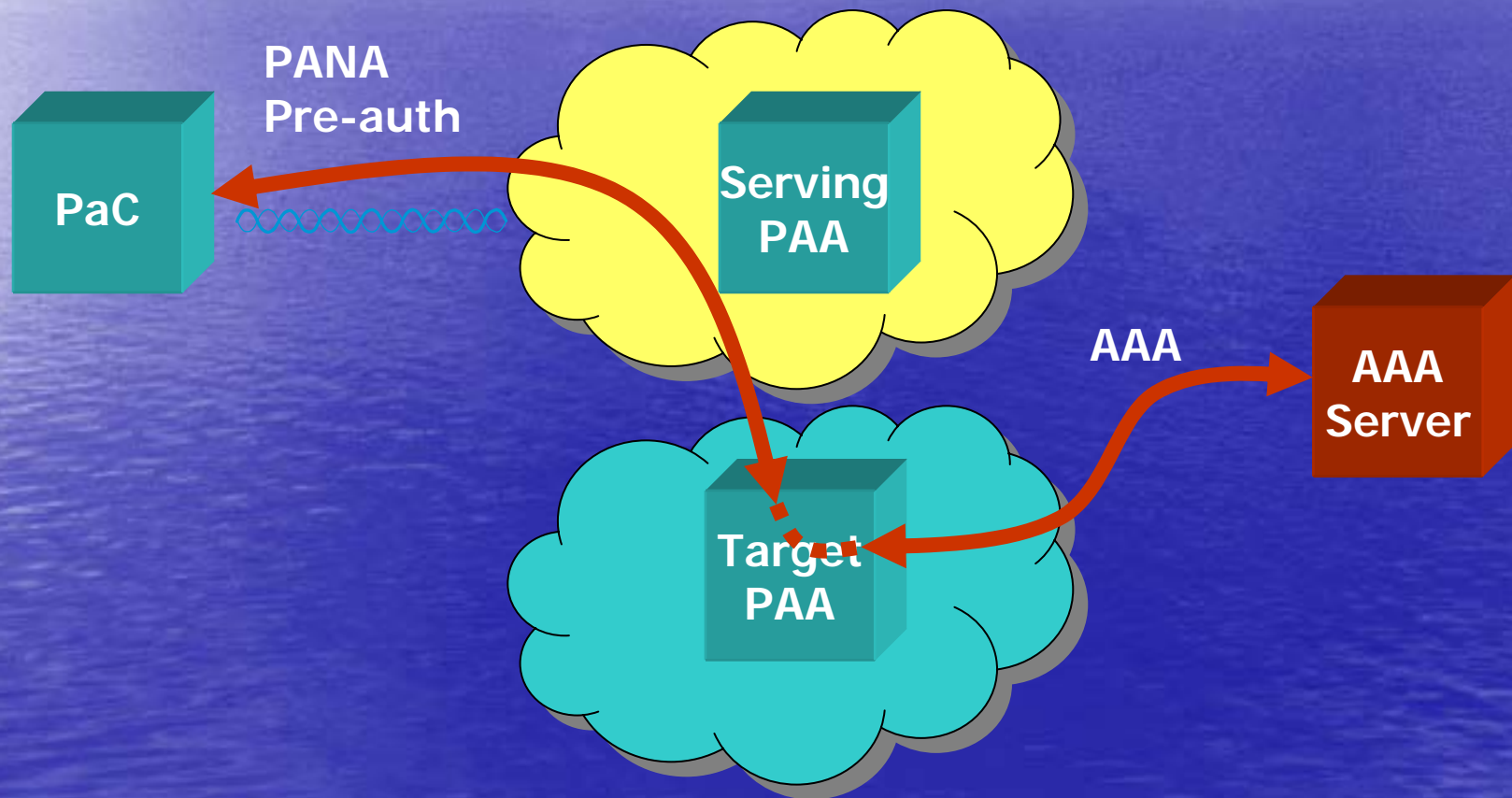


Low-Latency Handover
is possible within the same
PAA realm

PANA Pre-authentication

- PaC may handover to a network of a different PAA realm
 - If there is no trust relationship between serving and target PAAs, a new EAP run is inevitable
- It is better to proactively run EAP for a target PAA before handover
 - EAP pre-authentication using PANA

PANA Pre-authentication Example



Media-Independent Handover: IEEE 802.21

October 3rd, 2006

B3G Cluster Workshop on Mobility
Technologies in the Internet

16

What is 802.21?

- An IEEE specification that provides link layer intelligence and other related network information to upper layers to optimize handovers between heterogeneous media
 - 802.21 can also be used for homogeneous handovers such as inter-ESS transition within IEEE 802.11 media
- Status as of September 2006:
 - First 802.21 WG Letter Ballot
 - The specification is subject to change

Scope of 802.21

- Defining Media-Independent Handover Function (MIHF)
 - Defining handover-related services
 - Defining SAP (Service Access Point) and Primitives for handover-related services
- Defining a protocol to be used for communicating two MIHFs in different network nodes
 - MIHF protocol

Outside the Scope of 802.21

- Defining Handover Decision Making Engine
- Security Mechanisms
- Upper layer enhancements
- Media-specific link-layer enhancements

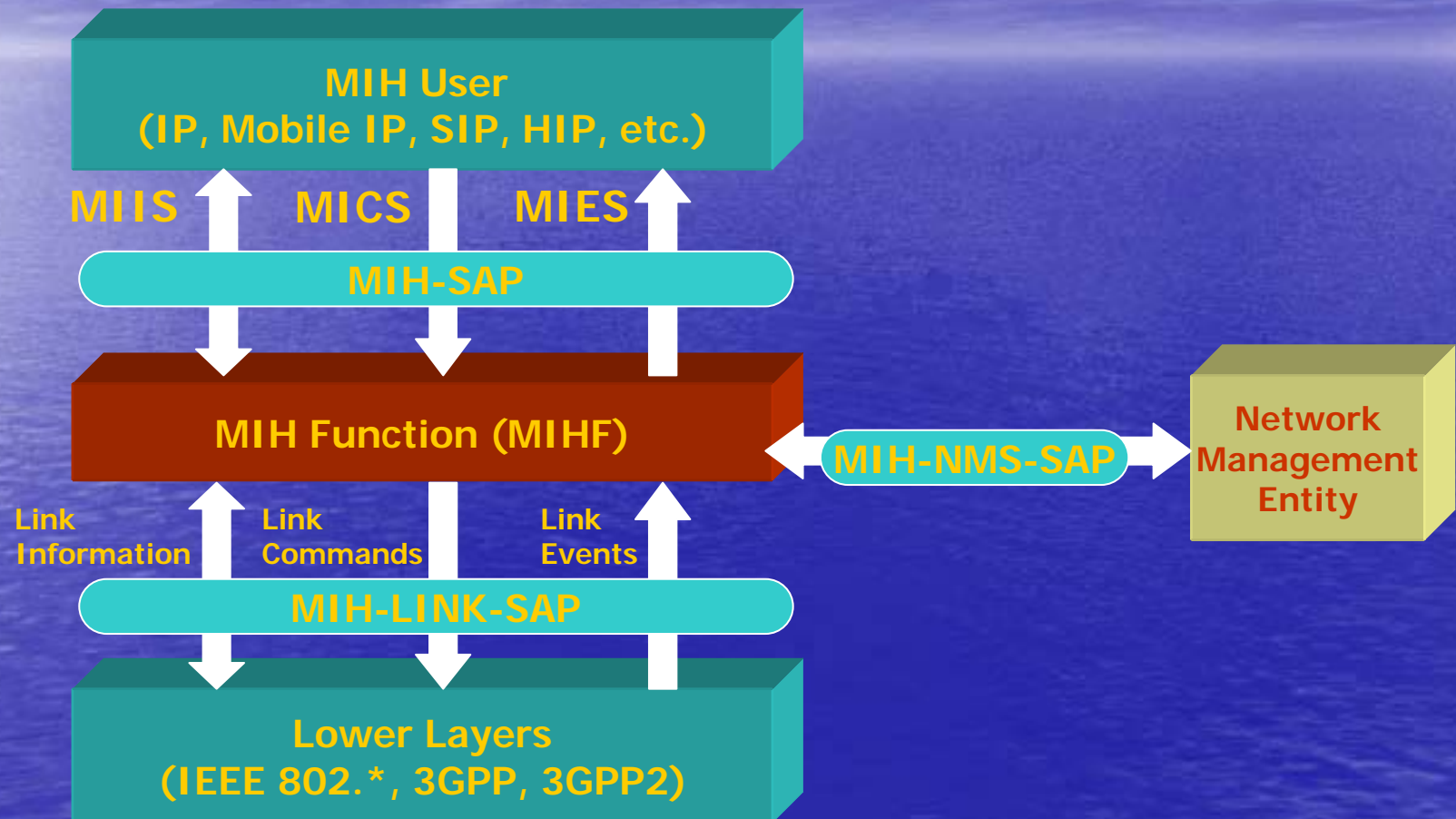
Type of Handovers Supported by 802.21

- Heterogeneous (Vertical) Handovers
 - Across different access technologies
- Homogeneous (Horizontal) Handovers
 - Within a single access technology
 - 802.11r, 802.16e, 3GPP, 3GPP2
 - Mostly solved by each link-layer, but ...
 - Some type of homogeneous handover is not supported by each link-layer, e.g., inter-ESS transition
 - 802.21 can fill the gap

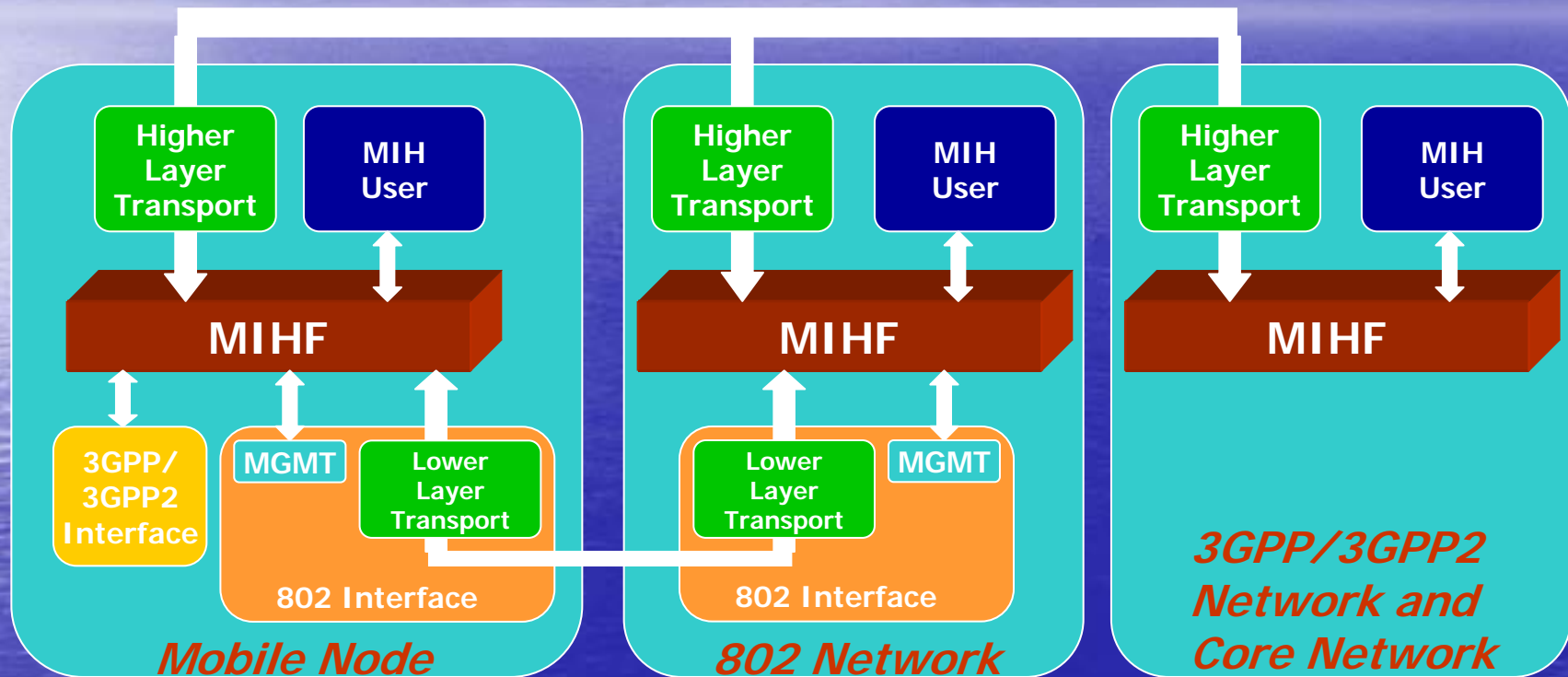
Services provided by MIHF

- **Media-Independent Event Service (MIES)**
 - Deliver link-layer events to MIH User
 - Events may be generated by local stack or propagated to remote stack (i.e., local events and remote events)
- **Media-Independent Command Service (MICS)**
 - Allow MIH User to control multi-interface device to make efficient handovers
 - Commands may be executed within local stack or propagated to remote stack (i.e., local commands and remote commands)
- **Media-Independent Information Service (MIIS)**
 - Provide MIH User with information on neighboring networks

MIHF Relationship in Local Stack



MIHF Relationship with Remote Communication (Example)



Media-Independent Event Service – Type of events

- MAC and PHY state change events
 - Generated when a link state changes (e.g., link-up/down)
- Link parameter events
 - Generated when a detailed link parameter (e.g., bit error rate) changes with crossing a certain threshold
- Predictive events
 - Generated when a link state is likely to change in future (e.g., link-going-down)
- Link synchronous events
 - Generated to indicate to MIH users about link activities that are directly related to handover
- Link transmission events
 - Generated to indicate to MIH users about frame transmission status (success or failure)
- Administrative events
 - Other type of events

List of Events

Event Type	MIH Event Name	Remote Direction C: Client, N: Network	Description
State Change	MIH Link Up	C to N, N to N	L2 connection is established and link is available for use
State Change	MIH Link Down	C to N, N to N	L2 connection is broken and link is not available for use
Predictive	MIH Link Going Down	C to N, N to N, N to C	Link conditions are degrading & connection loss is imminent
State Change	MIH Link Detected	C to N, N to N	New link has been detected
Link Parameters	MIH Link Parameters Report	C to N, N to N, N to C	Link parameters have crossed specified threshold
Administrative	MIH Link Event Rollback	C to N, N to N, N to C	Previous link event needs to be rolled back
Link Transmission	MIH Link SDU Transmit Status	N/A	Indicate transmission status of all PDU segments
Link Synchronous	MIH Link Handover Imminent	C to N, N to N, N to C	L2 handover is imminent based on changes in link conditions
Link Synchronous	MIH Link Handover Complete	C to N, N to N, N to C	L2 link handover to a new PoA has been completed

Media-Independent Command Service - Overview

- MIH users may utilize command services to determine the status of links and/or control the multi-mode device for optimal performance
- Command services may also enable MIH users to facilitate optimal handover policies such as network-initiated and/or network-controlled handover

List of Commands

MIH Command	Remote Direction Client(C), Network(N)	Description
MIH Get Status	N to C	Get the status of links
MIH Switch	N to C	Switch the links as specified
MIH Configure	N to C	Configure a link
MIH Scan	N to C	Scan a link
MIH Handover Initiate	N to C, C to N	Network or client may initiate handover and send a list of suggested networks and associated PoAs
MIH Handover Prepare	N to N	This command is sent by current MIHF entity to target MIHF entity to allow for resource query and handover preparation
MIH Handover Commit	C to N, N to C	In this case the client or network commits to do the handover and sends the choice of selected network and associated PoA
MIH Handover Complete	C to N, N to N	Notification from new serving MIHF to previous serving MIHF indicating handover completion, and any pending packets may now be forwarded to the new MIHF
MIH Network Address Information	N to N	Sent from serving MIHF to target MIHF to obtain reconfigured network address on target network for the client

Media-Independent Information Service - Overview

- MIIS provides a framework by which an MIHF may discover and obtain network information within a geographical area to facilitate heterogeneous handovers
- MIIS also defines information organization, information representation format and query methods on the defined information
 - Two ways of information representation types are supported, i.e., TLV and XML
 - Query capability depends on the information representation types in use
- A piece of information is referred to as **Information Element (IE)**

Note: Both information representation types are encoded in TLV in MIHF protocol

List of Information Elements

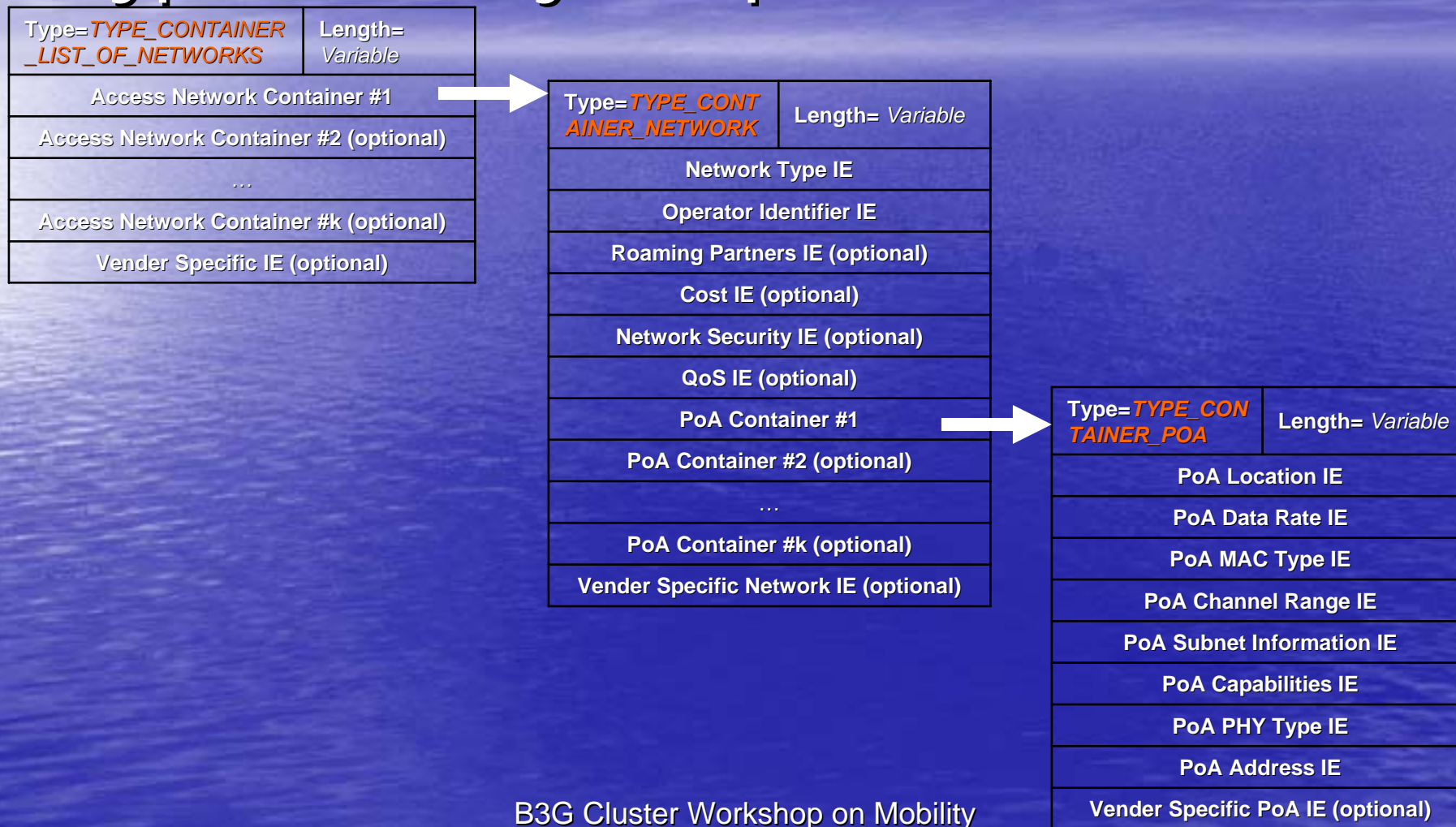
Name of IE	Description
Network Type	Link type of a network
Operator Identifier	Name of an operator
Roaming Partners	List of names of roaming partners
Cost	Charging related information
QoS	Static QoS information
PoA Location	Location of PoA. Both geospatial and civic address location types are supported
PoA Data Rate	Data rate provided by the PoA
PoA Network Standards	Network Standard types (802.11a/b/g/n, 802.16a/e/g, etc.)
PoA Channel Range	Lowest and highest channel frequencies
PoA Subnet Information	List of subnets available via the PoA
PoA Capabilities	A bitmap of PoA capabilities,
PoA Address	An address of PoA
Vendor Specific	Any vendor specific IEs

TLV Representation Type – Query Request format

Type= <i>MIIS_TLV_REPORT_TEMPLATE</i>	Length= <i>Variable</i>
<i>TYPE_CONTAINER_LIST_OF_NETWORKS</i> [4 octets] (optional)	
<i>TYPE_CONTAINER_NETWORK</i> [4 octets] (optional)	
<i>TYPE_IE_NETWORK_TYPE</i> [4 octets] (optional)	
<i>TYPE_IE_OPERATOR_IDENTIFIER</i> [4 octets] (optional)	
<i>TYPE_IE_ROAMING_PARTNERS</i> [4 octets] (optional)	
<i>TYPE_IE_COST</i> [4 octets] (optional)	
<i>TYPE_IE_NETWORK_SECURITY</i> [4 octets] (optional)	
<i>TYPE_IE_QOS</i> [4 octets] (optional)	
<i>TYPE_CONTAINER_POA</i> [4 octets] (optional)	
<i>TYPE_IE_POA_LOCATION</i> [4 octets] (optional)	
<i>TYPE_IE_POA_DATA_RATE</i> [4 octets] (optional)	
<i>TYPE_IE_POA_MAC_TYPE</i> [4 octets] (optional)	
<i>TYPE_IE_POA_CHANNEL_RANGE</i> [4 octets] (optional)	
<i>TYPE_IE_POA_SUBNET_INFORMATION</i> [4 octets] (optional)	
<i>TYPE_IE_POA_CAPABILITIES</i> [4 octets] (optional)	
<i>TYPE_IE_POA_PHY_TYPE</i> [4 octets] (optional)	
<i>TYPE_IE_POA_ADDRESS</i> [4 octets] (optional)	

TLV Information Representation

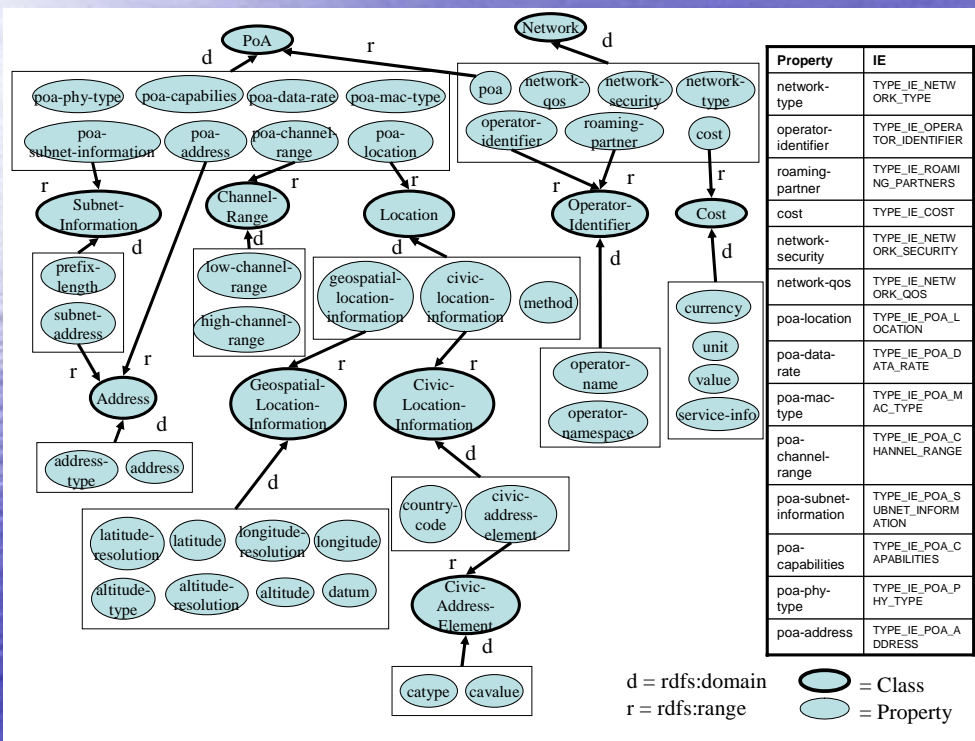
Type – Query Response format



XML Representation Type - Schema

- Schema specifies relationship among IEs as well as data type of each IE in a specially defined language
- Query language is also defined for the schema
 - Use of query language allows mobile devices to minimize the amount of information by specifying filters in detail
- 802.21 uses RDF (Resource Description Framework) Schema as the schema language and SPARQL for query language
- For extensibility, the schema consists of two parts: Basic Schema and Extended Schema
 - Basic schema is specified in 802.21
 - Extended schema can be defined by each vendor and operator and can be dynamically updated without revising 802.21 specification

XML Representation Type – Basic Schema



Graphical View

Property	IE
network-type	TYPE_IE_NETWORK_TYPE
operator-identifier	TYPE_IE_OPERATOR_IDENTIFIER
roaming-partner	TYPE_IE_ROAMING_PARTNERS
cost	TYPE_IE_COST
network-security	TYPE_IE_NETWORK_SECURITY
network-qos	TYPE_IE_NETWORK_QOS
poa-location	TYPE_IE_POA_LOCATION
poa-data-rate	TYPE_IE_POA_DATA_RATE
poa-mac-type	TYPE_IE_POA_MAC_TYPE
poa-channel-range	TYPE_IE_POA_CHANNEL_RANGE
poa-subnet-information	TYPE_IE_POA_SUBNET_INFORMATION
poa-capabilities	TYPE_IE_POA_CAPABILITIES
poa-phy-type	TYPE_IE_POA_PHY_TYPE
poa-address	TYPE_IE_POA_ADDRESS

```
<?xml version="1.0"?>

<!DOCTYPE rdf:RDF [
  <!ENTITY rdf "http://www.w3.org/1999/02/22-rdf-syntax-ns#">
  <!ENTITY rdfs "http://www.w3.org/2000/01/rdf-schema#">
  <!ENTITY mihbasic "URL_TO_BE_ASSIGNED">
  <!ENTITY owl "http://www.w3.org/2002/07/owl#">
  <!ENTITY xsd "http://www.w3.org/2001/XMLSchema#">
] >

<rdf:RDF xmlns:rdf="&rdf;" xmlns:rdfs="&rdfs;" xmlns:mihbasic="&mihbasic;"
xml:base="&mihbasic;" xmlns:owl="&owl;" xmlns:xsd="&xsd;">
  <owl:Ontology rdf:about="">
    <rdfs:label>Basic Schema for IEEE 802.21 Information Service</rdfs:label>
  </owl:Ontology>
  <owl:Class rdf:ID="Network">
    <rdfs:label>TYPE_CONTAINER_NETWORK</rdfs:label>
    <rdfs:subClassOf>
      <owl:Restriction>
        <owl:onProperty rdf:resource="#network-type"/>
        <owl:cardinality
rdf:datatype="&xsd;nonNegativeInteger">1</owl:cardinality>
      </owl:Restriction>
    </rdfs:subClassOf>
  </owl:Class>
  ....
```

XML Representation Type – Query Example

- Client is asking for PoA information owned by operator “blue-mobile”

Query Request

```
PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
DESCRIBE ?y
WHERE {?x mihbasic:poa ?y .
       ?x mihbasic:operator-identifier ?z .
       ?z mihbasic:operator-name "blue-mobile"}
```

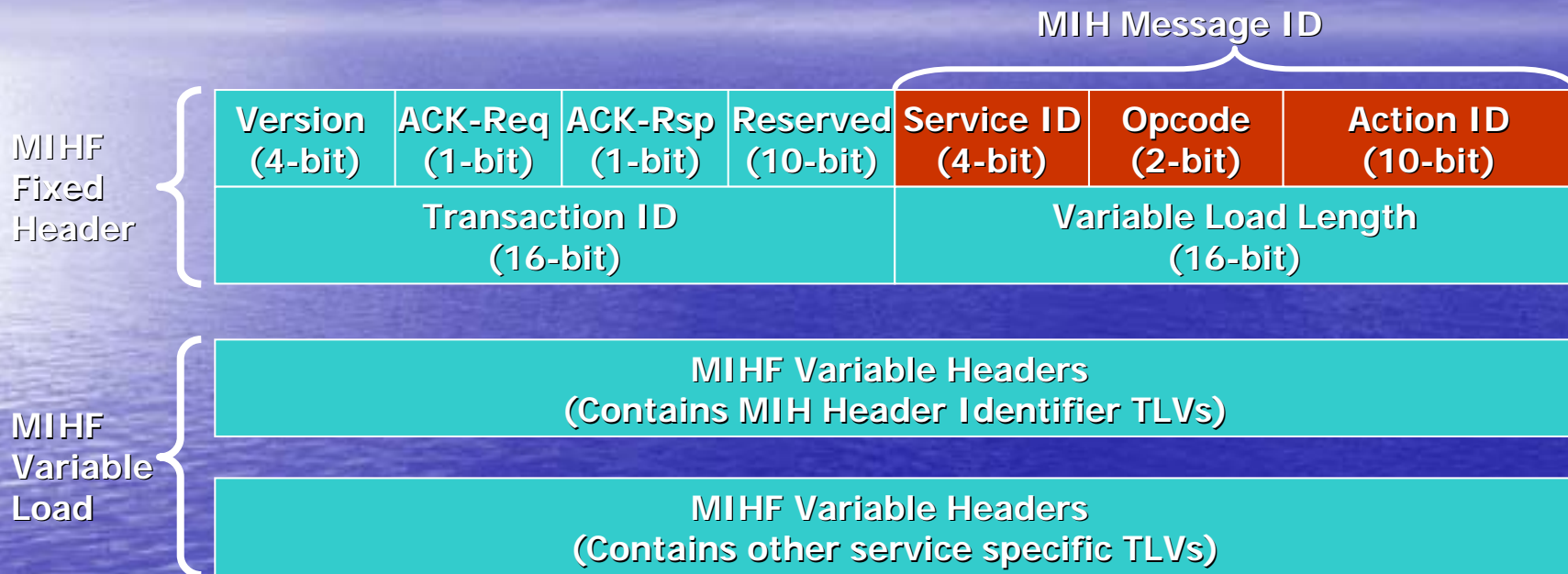
Query Reponse (N3 format):

```
@prefix : <http://www.mih.org/2006/09/rdf-basic-schema#> .
[   :poa-address [
      :address "ddddddddddd"; :address-type "6" ];
    :poa-capabilities "00b1";
    :poa-channel-range [
      :high-channel-range "470";
      :low-channel-range "450" ];
    :poa-data-rate "95";
    :poa-location [
      :geospatial-location-information [
        :altitude "6800";
        :altitude-resolution "30";
        :altitude-type "2"; :datum "1";
        :latitude "053c1f751";
        :latitude-resolution "21";
        :longitude "f50ba5b97";
        :longitude-resolution "20" ];
      :method "0" ];
    :poa-mac-type "802.16";
    :poa-subnet-information [
      :prefix-length "48";
      :subnet-address [
        :address "2002522d94d100000000000000000000";
        :address-type "2" ] ] ].
```

MIHF Protocol

- Used for remote events, remote commands and remote information queries
- MIHF protocol can use both link-layer transport and higher-layer transport
- MIHF protocol has its own reliable delivery mechanism in case underlying transport is unreliable

MIHF Protocol Format



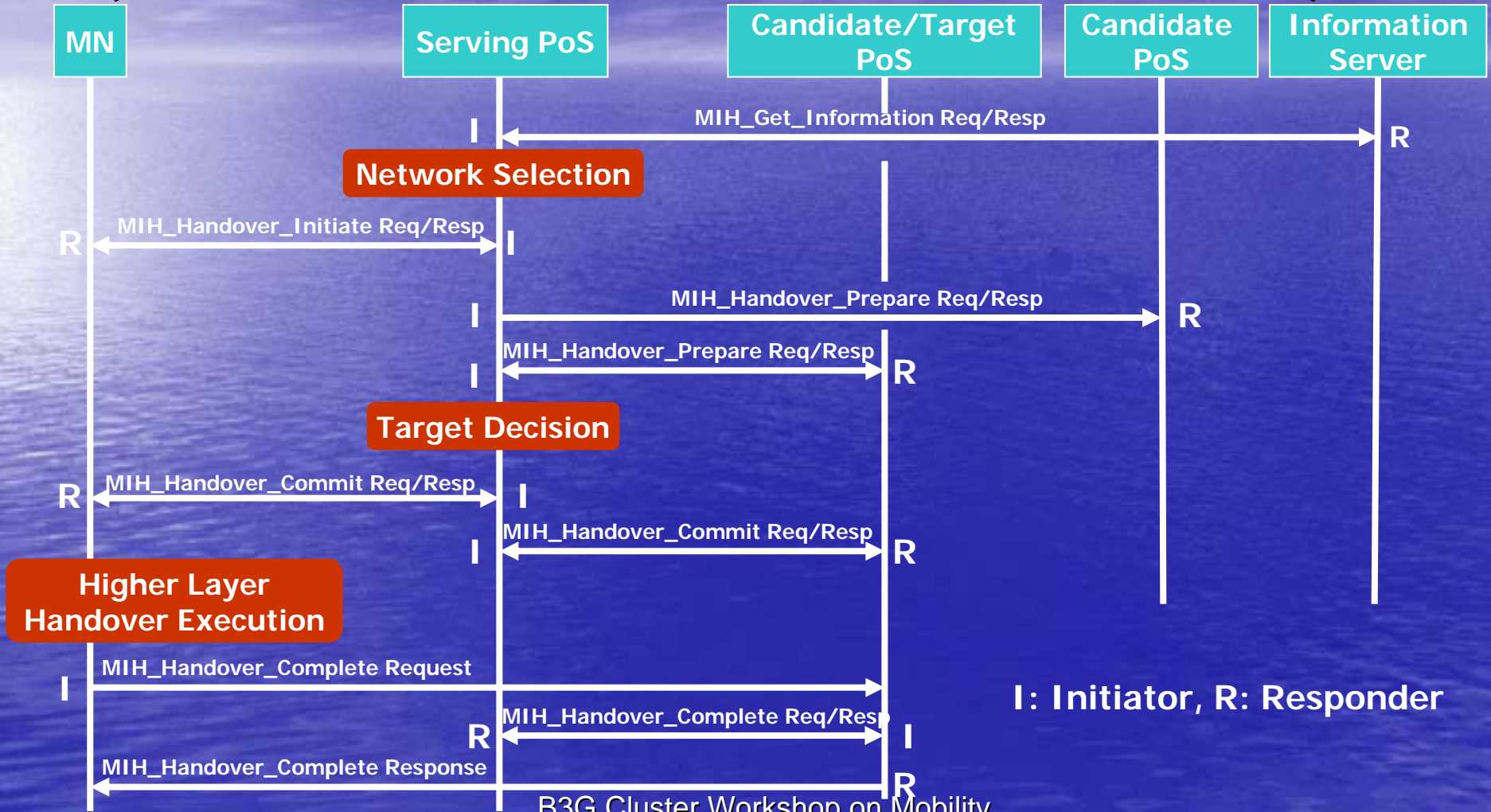
Service ID = {System Mgmt (1), MIES (2), MICS(3), MIIS (4)}

Opcode = {Request(1), Response(2), Indication(3)}

Action ID = {MIH Capability Discover(1), MIH Event Register(2)...}

MIHF Variable Header = {Session-ID TLV, MIHF-ID TLV}

Example Handover Sequence (network initiated & controlled handover)



802.21 and other SDOs

- IEEE 802.11u and 802.16g are working on amendment for MIH support
- IETF MIPSHOP WG is defining higher-layer transport of MIHF protocol
 - Candidate transport protocols: UDP, GIST, DHCP
- Information service functionality is being proposed to 3GPP SAE: S2-062992

Advanced Topic: MPA (Media-Independent Pre-authentication)

October 3rd, 2006

B3G Cluster Workshop on Mobility
Technologies in the Internet

40

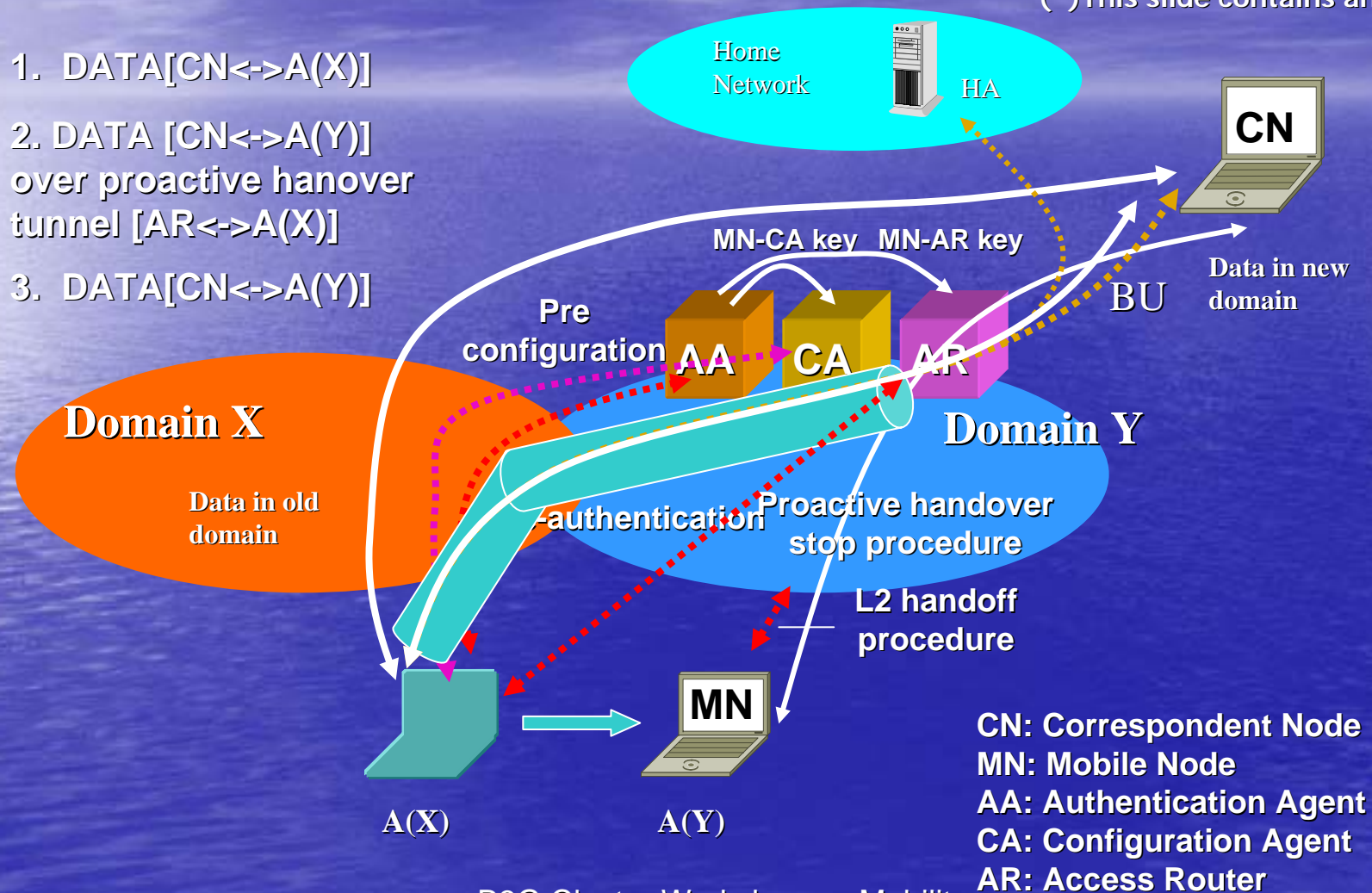
MPA Concept

- PANA pre-authentication allows MSK to be proactively established between PaC (MN) and target PAA
- The MSK can be used for bootstrapping SAs for subsequent handover signaling
 - IPsec between MN and AR in the target network can be also established before L2 handover
- This allows higher-layer handover procedure (IP address acquisition, MIPv6 Binding Update, etc.) be completed before L2 handover
 - New CoA can be usable for application traffic before L2 handover

MPA Overview

(*)This slide contains animation

1. DATA[CN \leftrightarrow A(X)]
2. DATA [CN \leftrightarrow A(Y)]
over proactive hanover
tunnel [AR \leftrightarrow A(X)]
3. DATA[CN \leftrightarrow A(Y)]

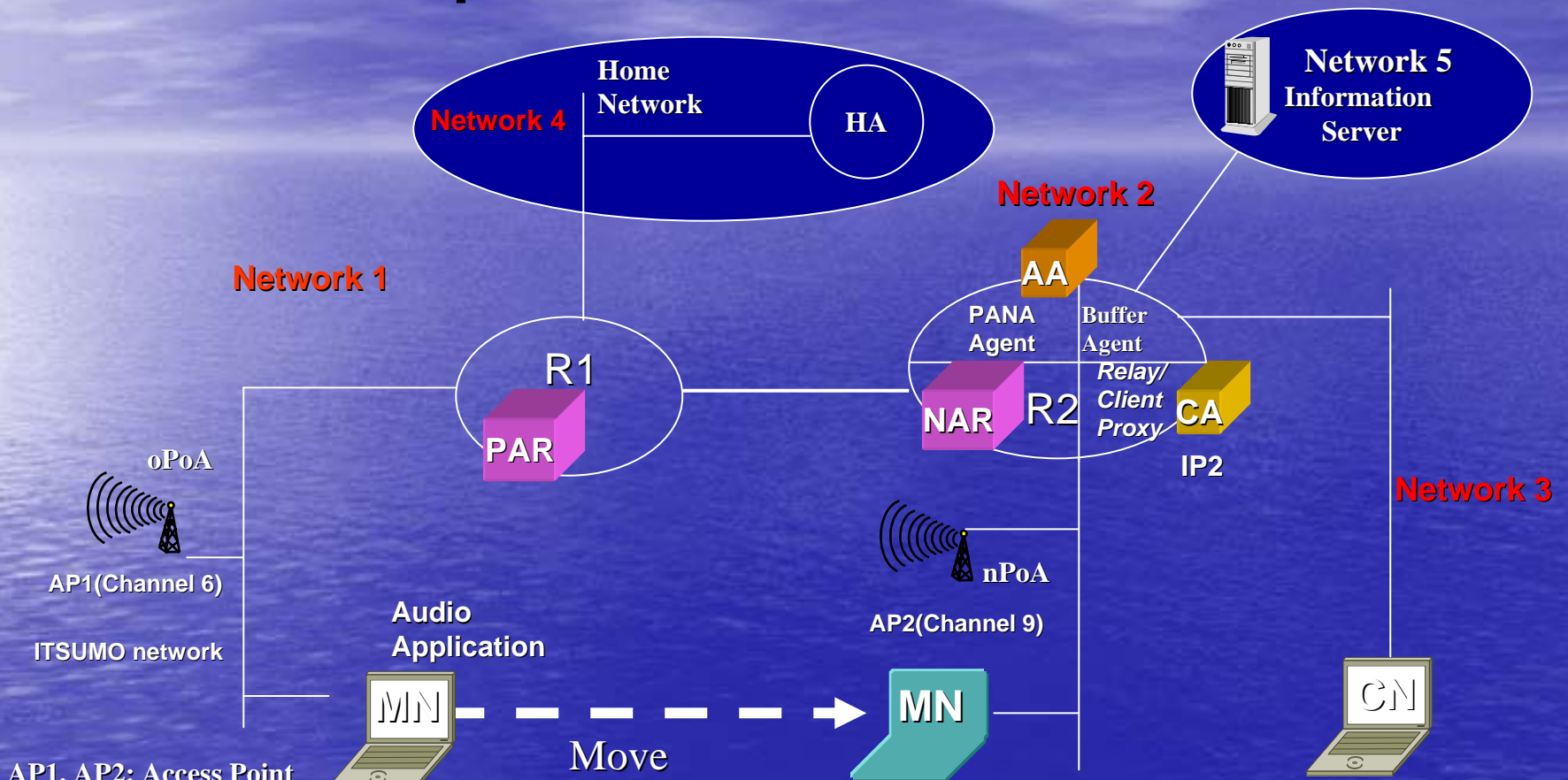


B3G Cluster Workshop on Mobility
Technologies in the Internet

Protocol Set for the MPA prototype

Mobility Management Protocol	MIPv6	SIPM
Network Discovery Scheme (802.21)	XML/RDF	XML/RDF
Pre-authentication protocol	PANA	PANA
Pre-configuration protocol	PANA, Stateless	PANA, DHCP Relay
Proactive handover tunneling protocol	IPSec	IP-in-IP
Proactive handover tunnel management protocol	PANA	PANA
Buffer Management Protocol	PANA	PANA
Link-layer security	None	None

MPA Experiment with MIPv6



AP1, AP2: Access Point
 R1: Previous Access Router
 R2: New Access Router
 MN: Mobile Node
 CN: Correspondent Node
 HA: Home Agent
 BA: Buffer Agent

October 3rd, 2006

MPA Experimental Results

Mobility Type	MIPv6			SIP Mobility		
Handoff Parameters [RO: Route Optimization]	Buffering Disabled + RO Disabled	Buffering Enabled + RO Disabled	Buffering Disabled + RO Enabled	Buffering Enabled + RO Enabled	Buffering Disabled	Buffering Enabled
L2 handoff (ms)	4.00	4.33	4.00	4.00	4.00	5.00
Avg. packet loss	1.33	0	0.66	0	1.50	0
Avg. inter-packet interval (ms)	16.00	16.00	16.00	16.00	16.00	16.00
Avg. inter-packet arrival time during handover (ms)	n/a	45.33	n/a	66.60	n/a	29.00
Avg. packet jitter (ms)	n/a	29.33	n/a	50.60	n/a	13.00
Buffering period (ms)	n/a	50.00	n/a	50.00	n/a	20.00
Buffered Packets	n/a	2.00	n/a	3.00	n/a	3.00

New Activity in IETF for Secure Handover Optimization - HOKEY

October 3rd, 2006

B3G Cluster Workshop on Mobility
Technologies in the Internet

46

HOKEY (Handover Keying)

- Key topics (subject to change)
 - Handover keying and Low-latency re-authentication
 - Secure handover framework of re-using previously established EAP keying material for inter-authenticator handover and re-authentication
 - Pre-authentication
 - A mechanism for proactively executing EAP between mobile and target authenticator prior to handover
- Two BOF meetings (March/July 2006)
- External Review of HOKEY WG charter until October 9th
- Mailing List Information:
<http://www.opendiameter.org/mailman/listinfo/hokeyp>



Thank you!

October 3rd, 2006

B3G Cluster Workshop on Mobility
Technologies in the Internet

48