

Mobile authentication and access control

Wolfgang Fritsche, IABG

May 10th

INET'2004 Barcelona



Security for the pervasive computing world

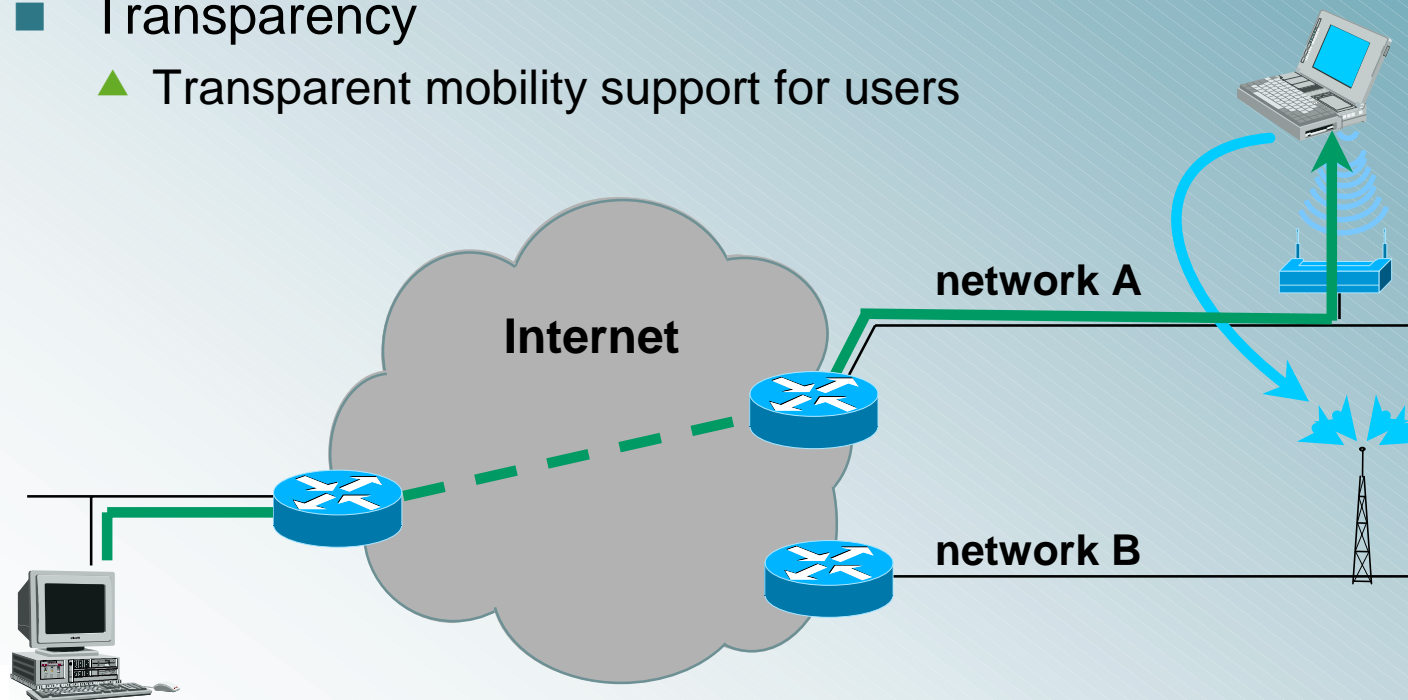


Agenda

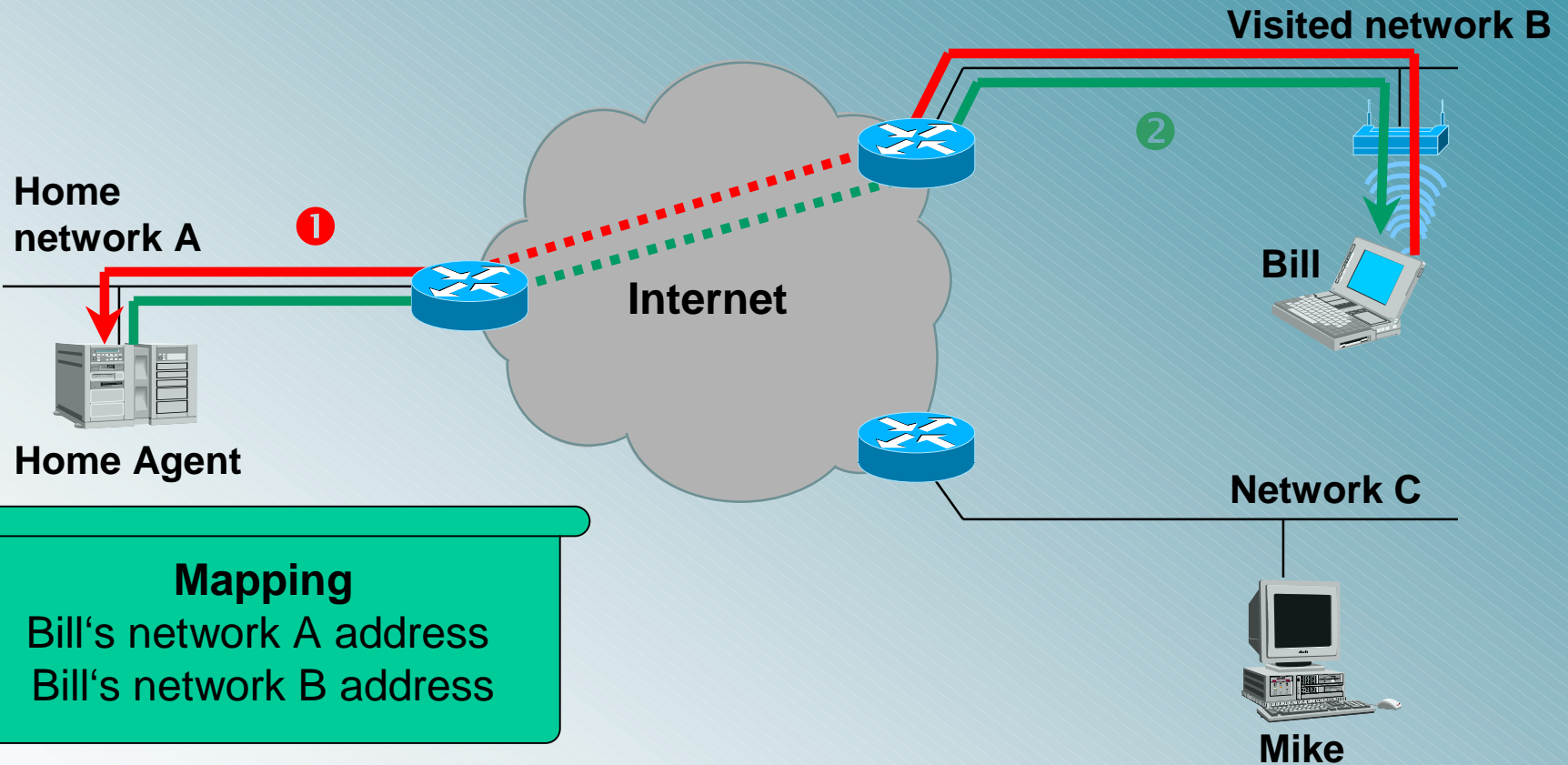
- Threats to Mobile IPv6
- Mobile IPv6 security
- Cryptographically generated addresses
- PANA

Mobile IPv6 - intention

- Mobility
 - ▲ Growing number of mobile Internet users
 - ▲ Mobility support in the Internet required
- Addressing
 - ▲ Reachability of user under one fixed IP address
 - ▲ Automatic configuration
- Transparency
 - ▲ Transparent mobility support for users

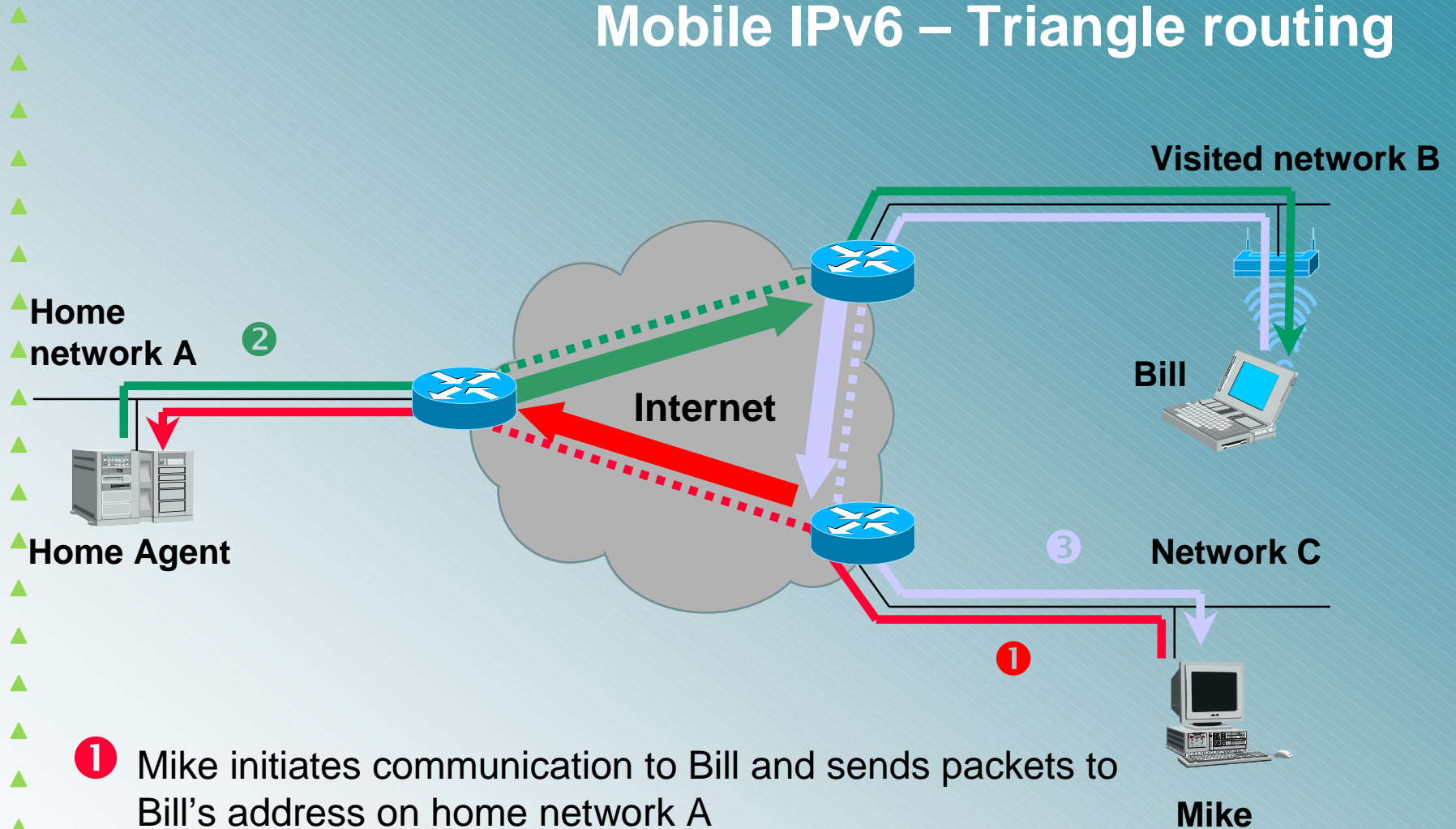


Mobile IPv6 – Home registration



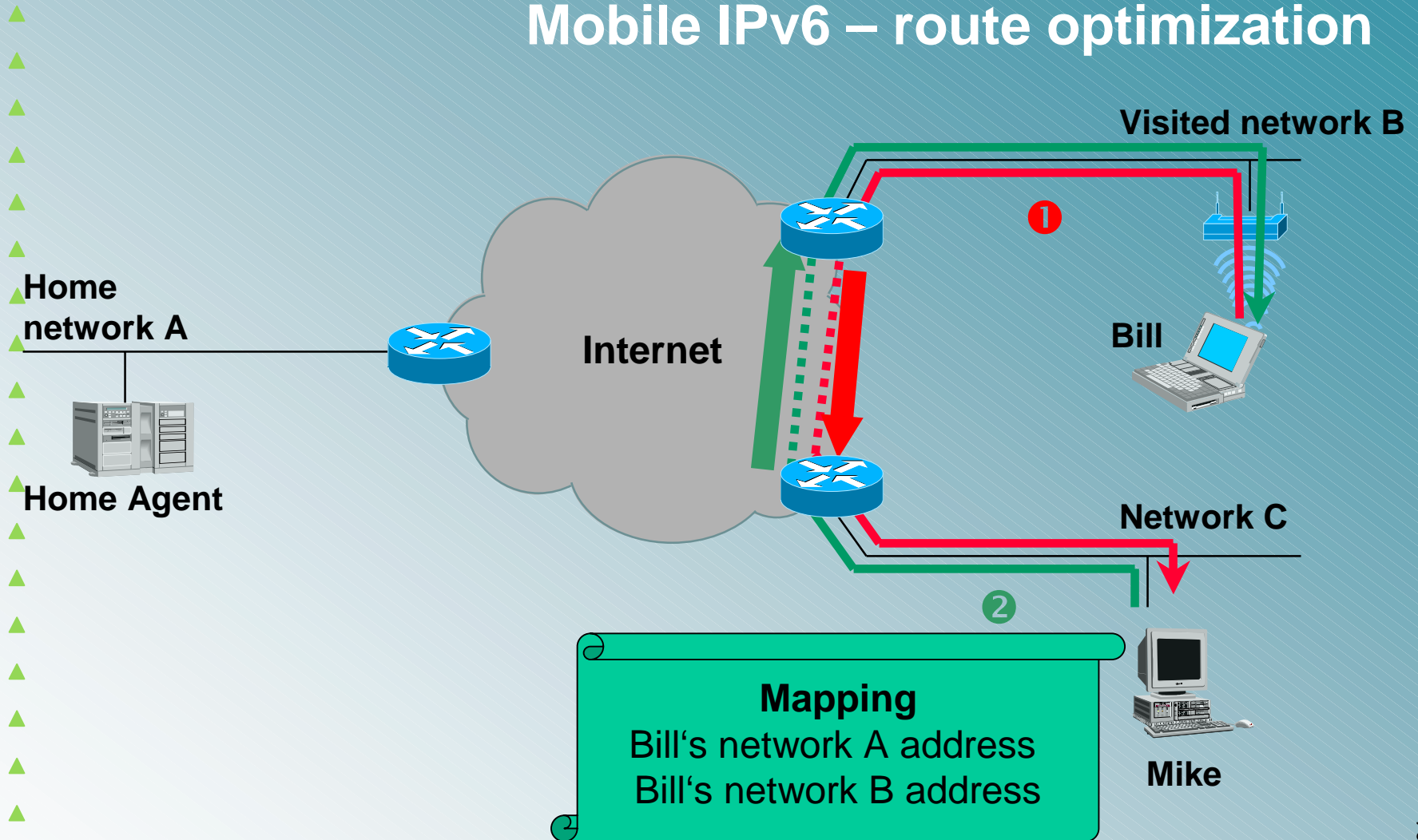
- 1 Bill sends mapping to Home Agent (registration)
- 2 Home Agent confirms receipt of mapping and start to receive packets for Bill (proxy)

Mobile IPv6 – Triangle routing



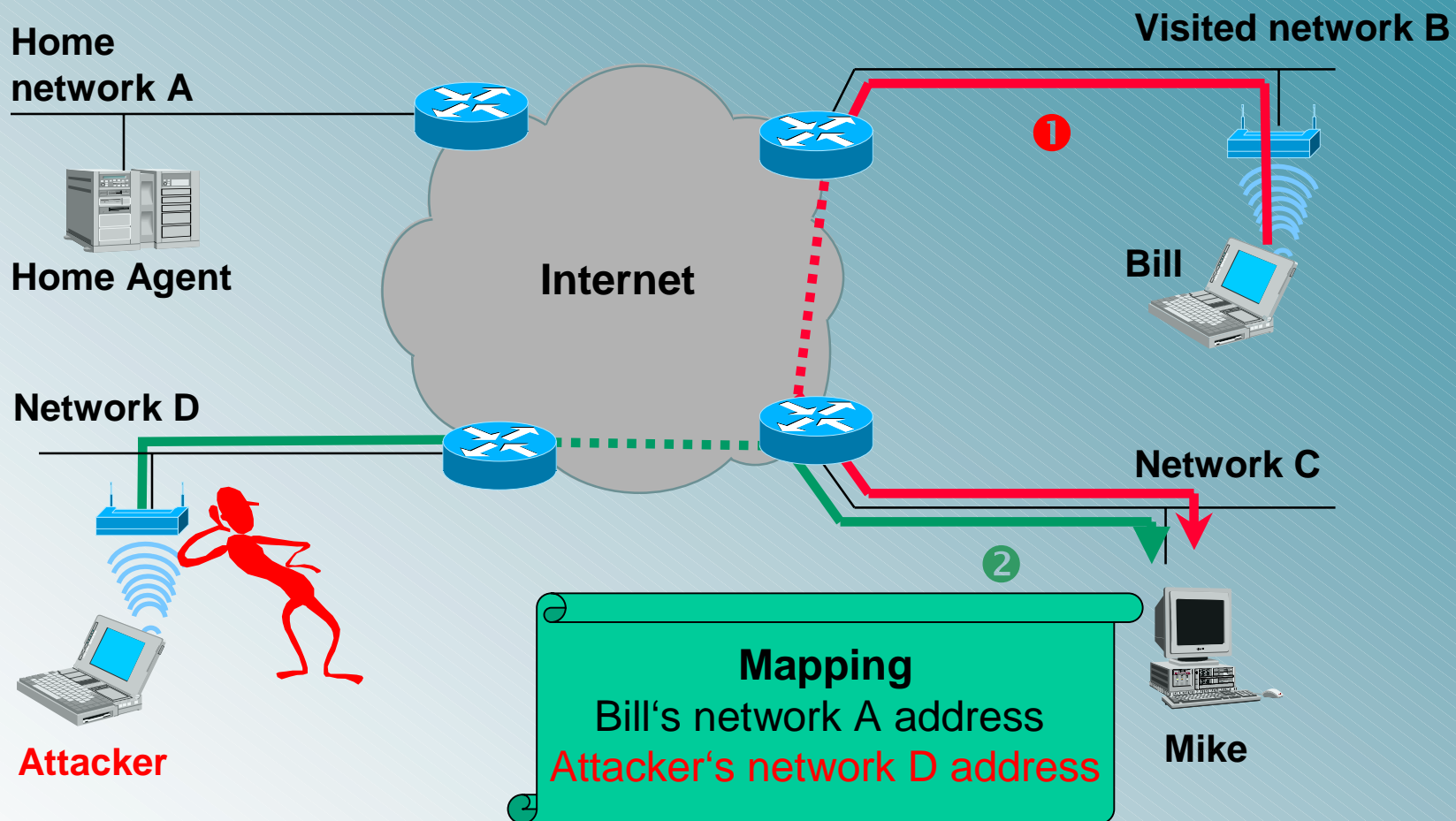
- 1 Mike initiates communication to Bill and sends packets to Bill's address on home network A
- 2 Home Agent intercepts packets and forward them to Bill's address on visited network B
- 3 Bill replies directly to Mike

Mobile IPv6 – route optimization



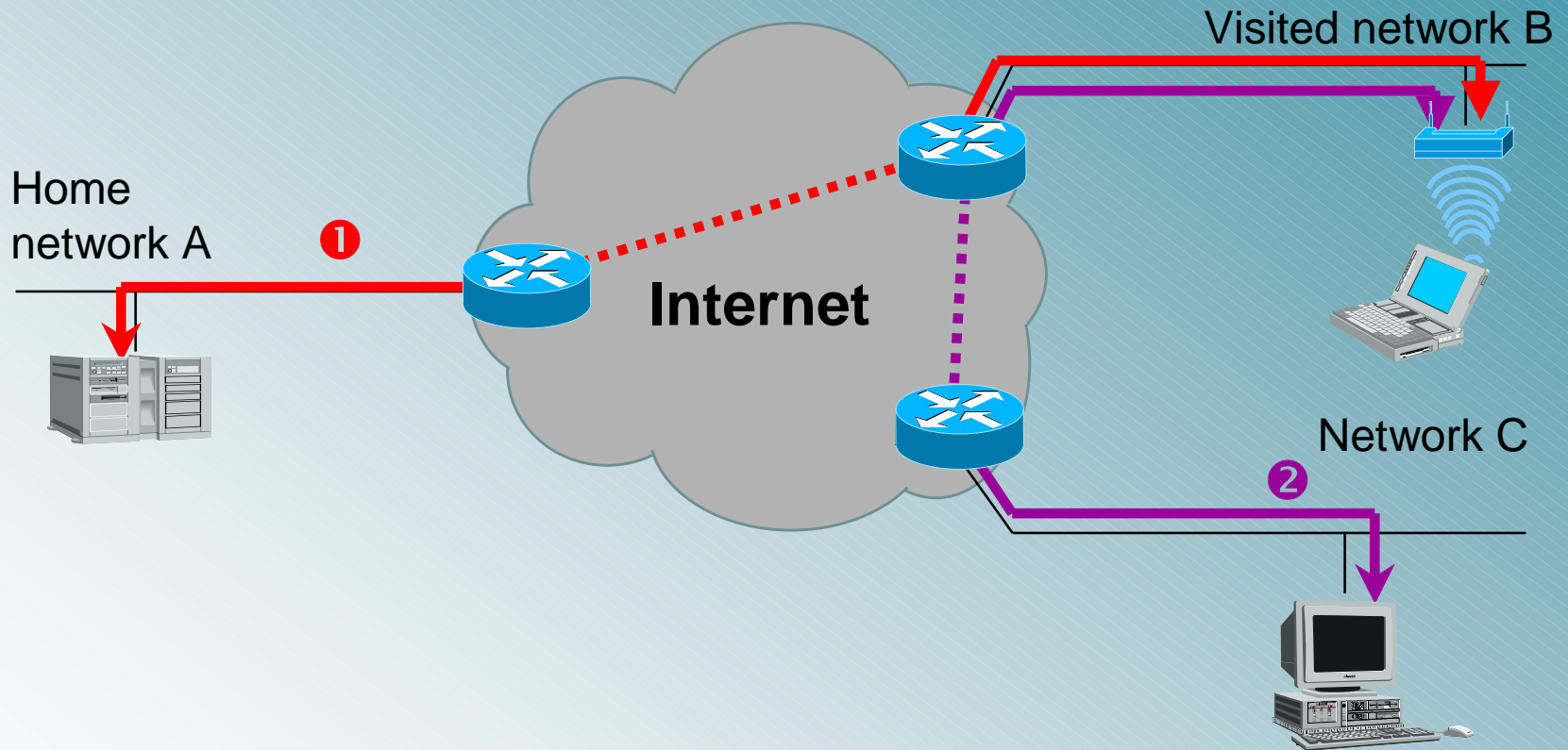
- 1 Bill sends mapping to Mike
- 2 Mike sends following packets directly to Bill's address on visited network B

Mobile IPv6 – attack scenario



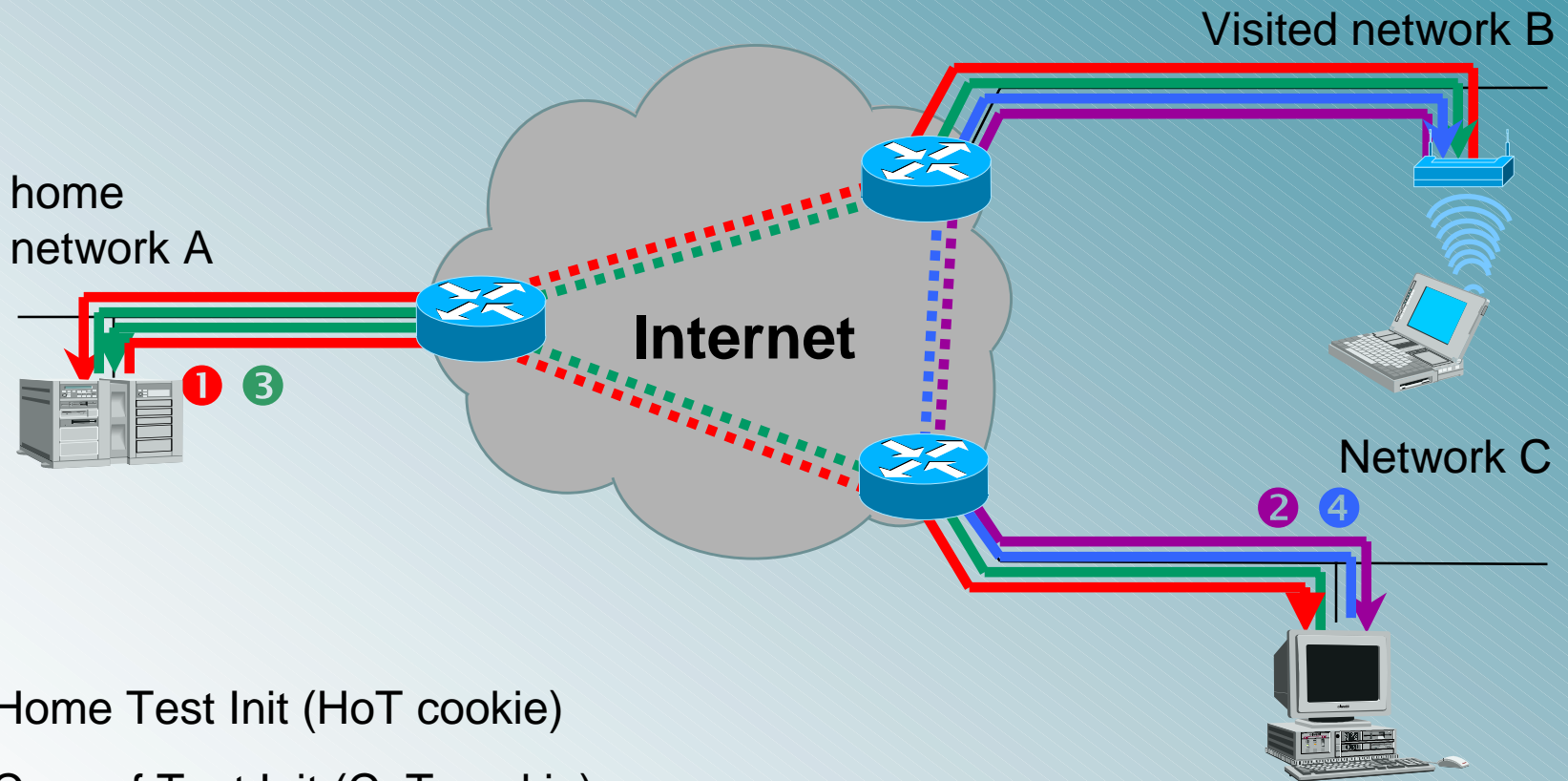
- 1 Bill sends mapping to Mike
- 2 Attacker re-directs traffic sent from Mike to Bill towards himself

Mobile IPv6 - Trust relationship



- 1 Trust relationship between MN and HA --> IPSec can be used
- 2 No trust relationship between MN and CN --> ???

Mobile IPv6 - Return routability



- 1 Home Test Init (HoT cookie)
- 2 Care-of Test Init (CoT cookie)
- 3 Home Test (HoT cookie, home keygen token, home nonce index)
- 4 Care-of Test (CoT cookie, care-of keygen token, care-of nonce index)

Mobile IPv6 – remaining security issues

- Attacker on the path between HA and CN plus between MN and CN will be able to receive all Return Routability packets
- This attacker could still send Binding information on behalf of the MN
- Cryptographically Generate Addresses can help here (see next slides)
- This still requires Return Routability itself to proof reachability of MN's addresses

CGA - overview

- IPv6 addresses, which carry hashed information about public key in the identifier part
- Benefits
 - ▲ Provide similar to certificates a binding of IP address to public keys without requiring a key management infrastructure
 - ▲ Help to secure IPv6 Neighbor Discovery (resolve chicken-egg problem of IPsec)
 - ▲ Could help to further secure Mobile IPv6 Binding information

CGA - parameters

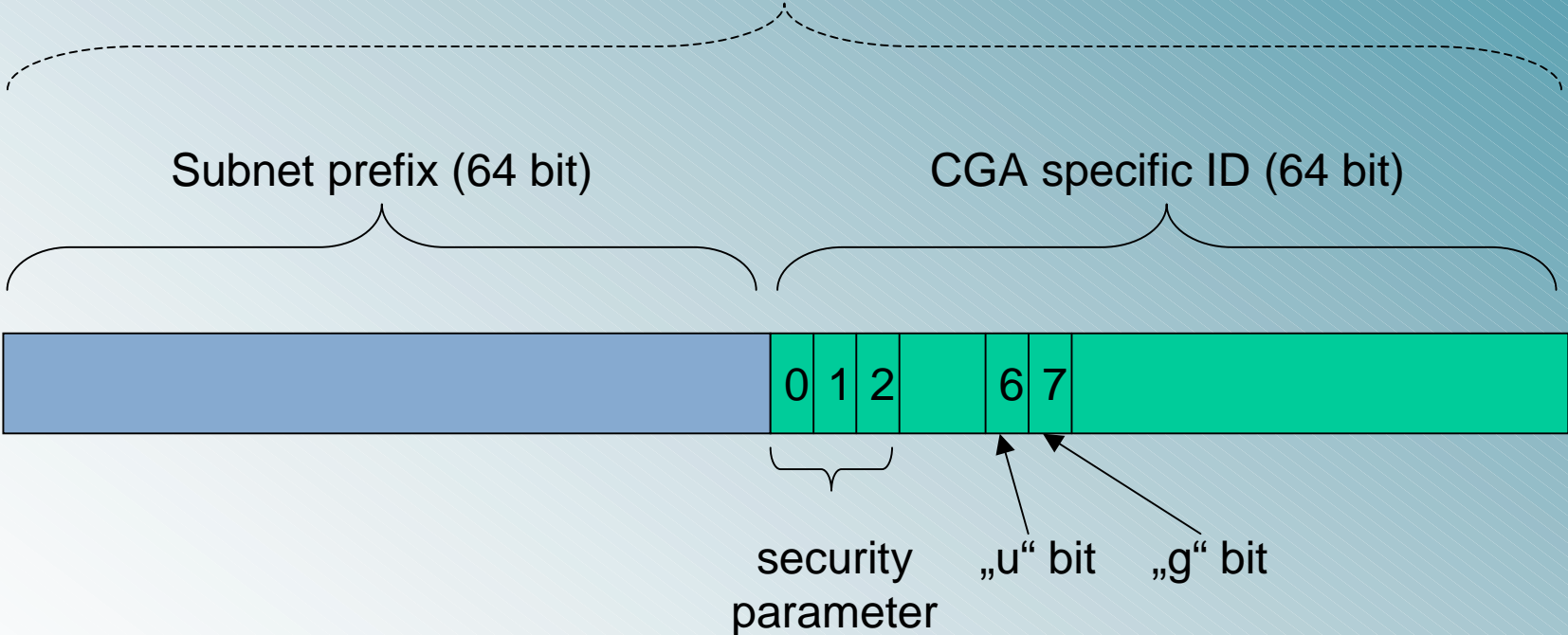
- Modifier
 - ▲ 16 octets long
 - ▲ Chosen arbitrarily
- Address prefix
 - ▲ 8 octet long
 - ▲ Prefix valid on the respective link
- Collision count
 - ▲ 1 octet long
- public key
 - ▲ Variable length

CGA - generation

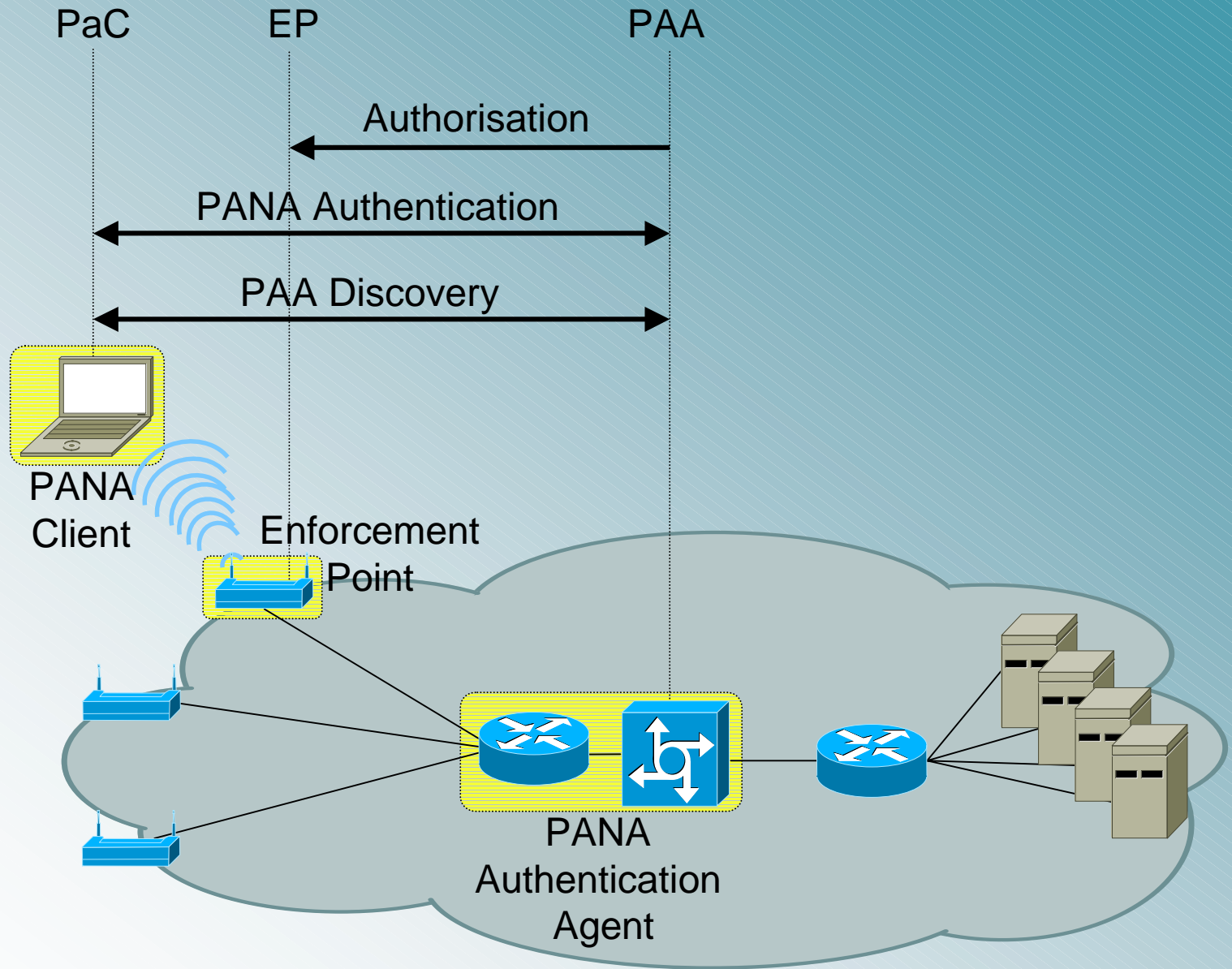
1. Generate public / private key pair
2. Choose an arbitrary value for the 16 octet modifier
3. Select an appropriate value for the security parameter (0: « low resistance » to brute-force to 7: « high resistance to brute-force »)
4. Hash (SHA-1) concatenation of modifier, address prefix (set to zero), collision count (set to zero) and public key
5. If first 16 times security parameter bits are not zero, increase modifier by 1 and repeat hash computation (back to 4)
6. Hash (SHA-1) concatenation of final modifier, real address prefix, collision count (set to zero) and public key
7. The identifier are the first 64 bits of the result with overriding the first 3 bits by the security parameter and setting u and g bit
8. If duplicate address detection fails, increase collision counter and go back to 6

CGA - structure

Cryptographically Generated Address

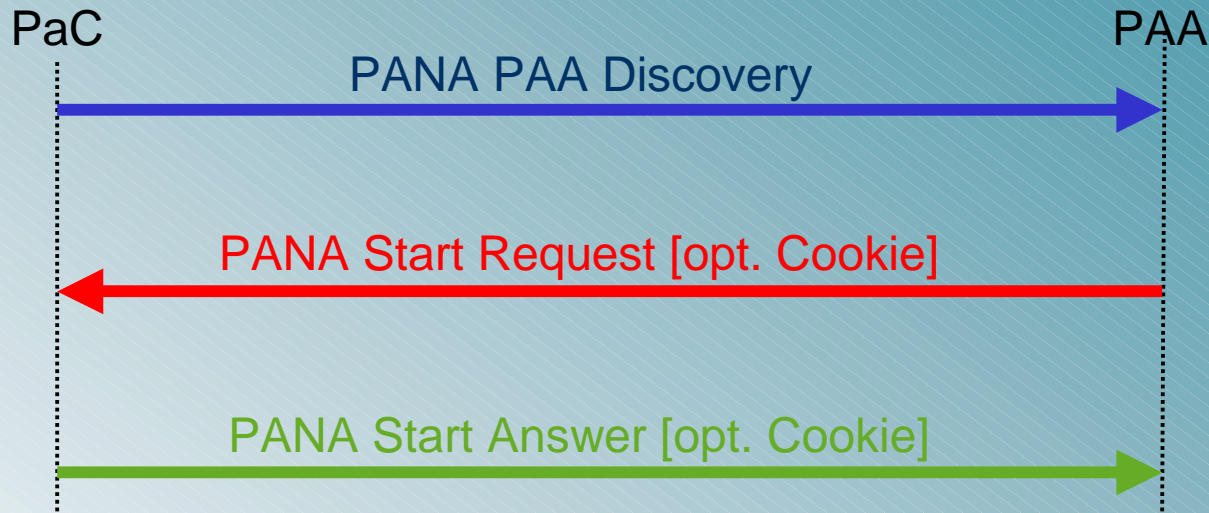


PANA - architecture

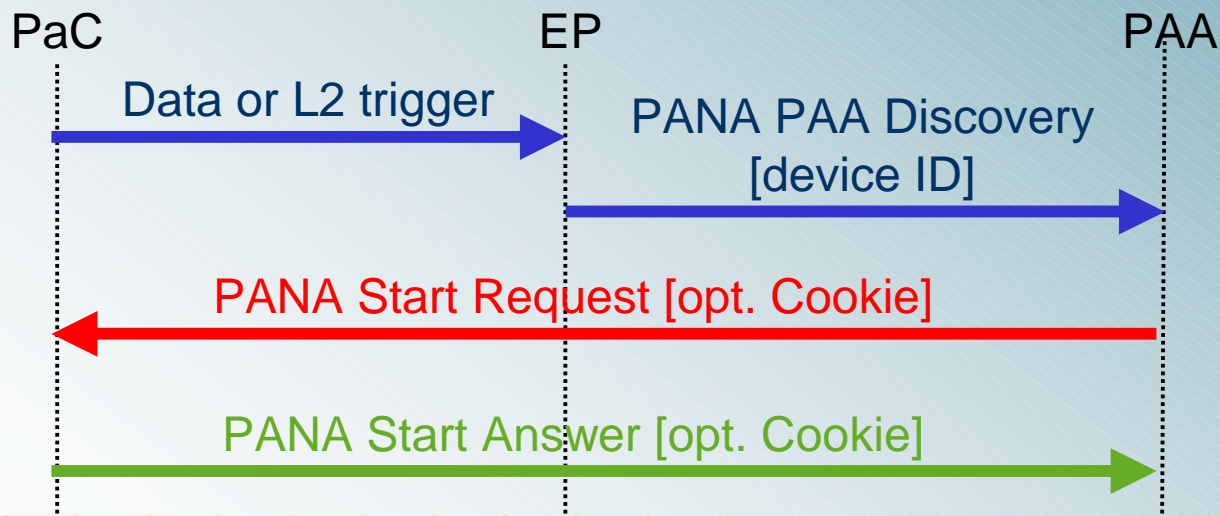


PANA - PAA discovery phase

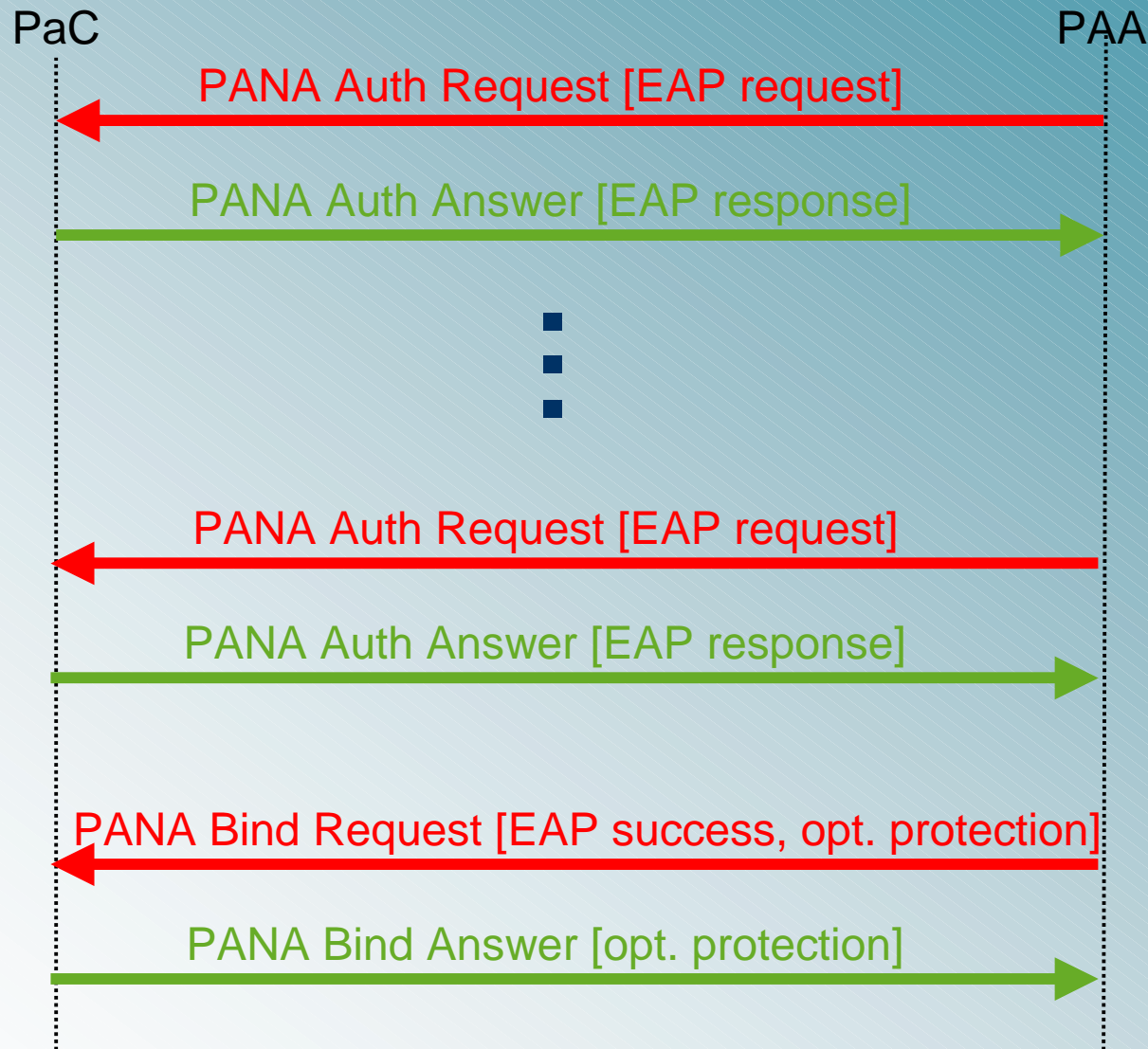
Client triggered



Data / L2 triggered



PANA - authentication phase



PANA - termination phase

PAA triggered

PaC

PAA

PANA Termination Request [MAC]

PANA Termination Answer [MAC]

Client triggered

PaC

PAA

PANA Termination Request [MAC]

PANA Termination Answer [MAC]

PANA – open issues

- Separation between EP and PAA
 - ▲ Requires communication between both
 - ▲ Not in scope of the PANA specification
 - ▲ COPS, SNMP, Diameter could be candidates here

- Mobility support
 - ▲ If client roams between different PAAs a re-use of existing PANA session would be nice
 - ▲ Communication between involved PAAs required
 - ▲ Not in scope of the PANA specification
 - ▲ Context Transfer Protocol could be a candidate here