



# Mobile IPv6 Security

## IPv6 Forum

December 7, 2004

Richard Graveman – RFG Security

[rfg@acm.org](mailto:rfg@acm.org)

# Lightening Fast Review

- ✓ Advantages of IPv6
- ✓ IPv6 basics:
  - Addresses (length, types, scope)
  - Headers and extension headers
  - ICMPv6, auto-configuration, DAD, etc.
- ✓ Notion of IP-layer mobility
- Cryptographic protocol security:
  - Services: authentication, message integrity, replay detection, confidentiality
  - Mechanisms: key agreement, encryption, signatures, MACs, hash functions
- IPsec basics:
  - Security Associations, ESP, AH, IKE



# Protocol Security: IPsec

- The big change in IPsec from IPv4 to IPv6 is that IPsec is **mandatory** in IPv6 implementations
- IPsec can provide authentication, integrity, confidentiality, and replay detection for *any* IP datagram
  - Provided ...

# Protocol Security: IPsec

- Provided we can trust identities and implement it correctly on a secure platform
  - It's not an alternative for firewalls
- IPsec provides an extraordinarily sound protocol security infrastructure, but details matter:
  - Implementing IPsec is somewhat difficult
  - We have to figure out how to use it, case by case
  - Changes in IPsec are still in the works
- "If you think cryptography is the solution to your problem, you don't know what your problem is."
  - Roger Needham

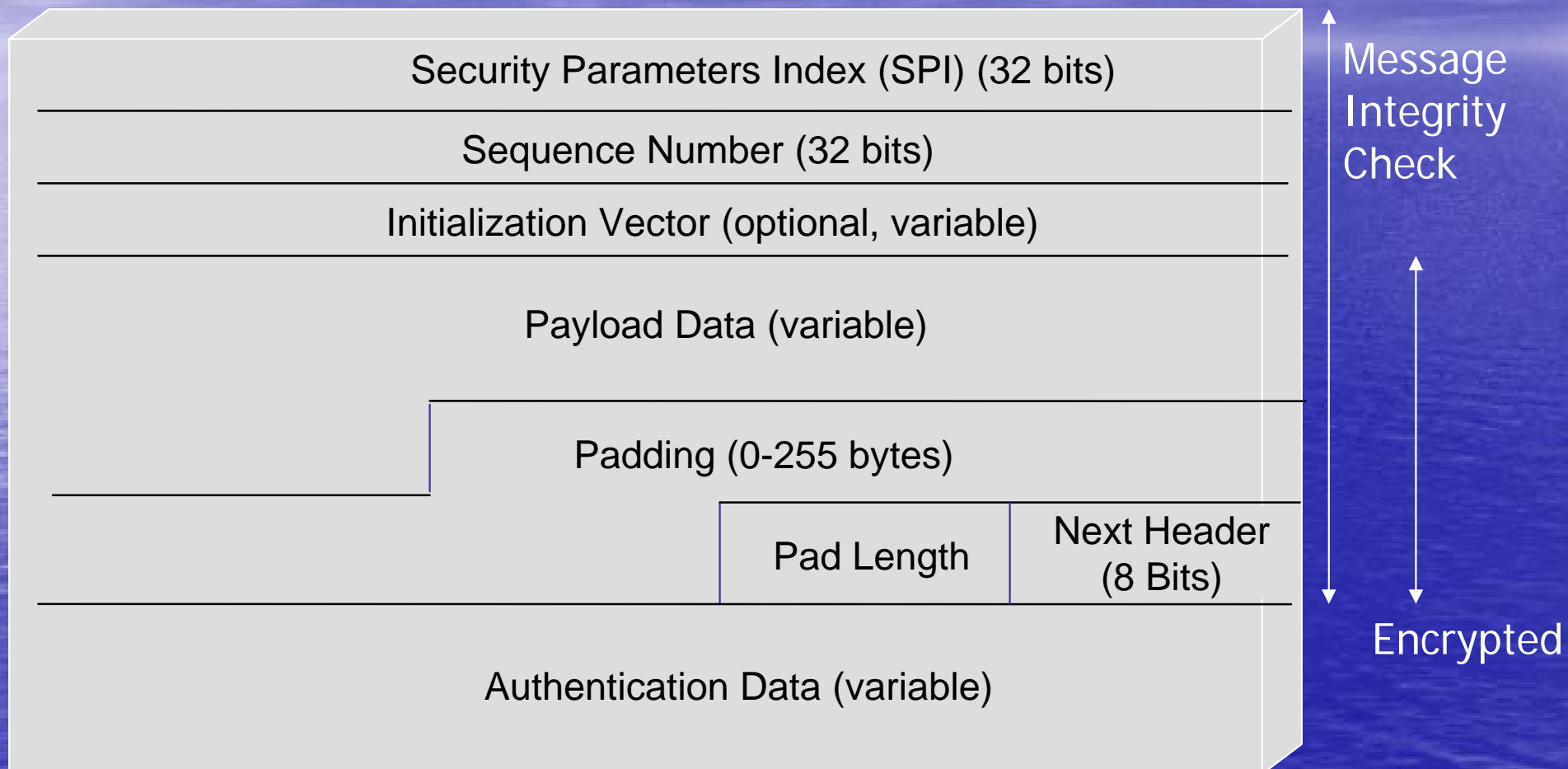


# IPsec and IKE(v1)

- IPsec: architecture and two extension headers
  - RFC 2401: Security Architecture
  - RFC 2402: Authentication Header
    - Message origin authentication and connectionless integrity
    - Replay detection
  - RFC 2406: Encapsulating Security Payload
    - Everything in AH plus confidentiality
- Key management for IPsec: IKE (Internet Key Exchange)
  - RFCs 2407, 2408, 2409
    - Entity authentication
    - Security Association (SA) negotiation
    - Key exchange
- Many other RFCs
- All of the core RFCs will be revised in the next year (or so)



# IPsec: Encapsulating Security Payload (ESP) Packet Format



# IPsec: Security Associations

- Contain all the parameters needed to specify
  - When and how the source applies security
  - When and how the destination verifies security
- Named by a destination address, protocol, and Security Parameters Index
- Usually configured in pairs
  - One in each direction
- Security Policy Database (SPD)
  - “When” to apply “what” IPsec capabilities
- Security Association Database (SAD)
  - “How” to apply IPsec

# Mobile IPv6 Security: Outline

1. Introduction to Mobile IPv6
2. Threats and Attacks against Mobile IPv6
3. Security between Mobile Host and Home Agent
  - Changes to IKE and IPsec
4. Security between Mobile Host and Correspondent Host
  - Type 2 Routing Header and Home Address Option
5. Summary and References

# 1. Introduction to Mobile IPv6

- Motivation
- Overview
- Components
- Terminology
- Protocols
- Differences from Mobile IPv4



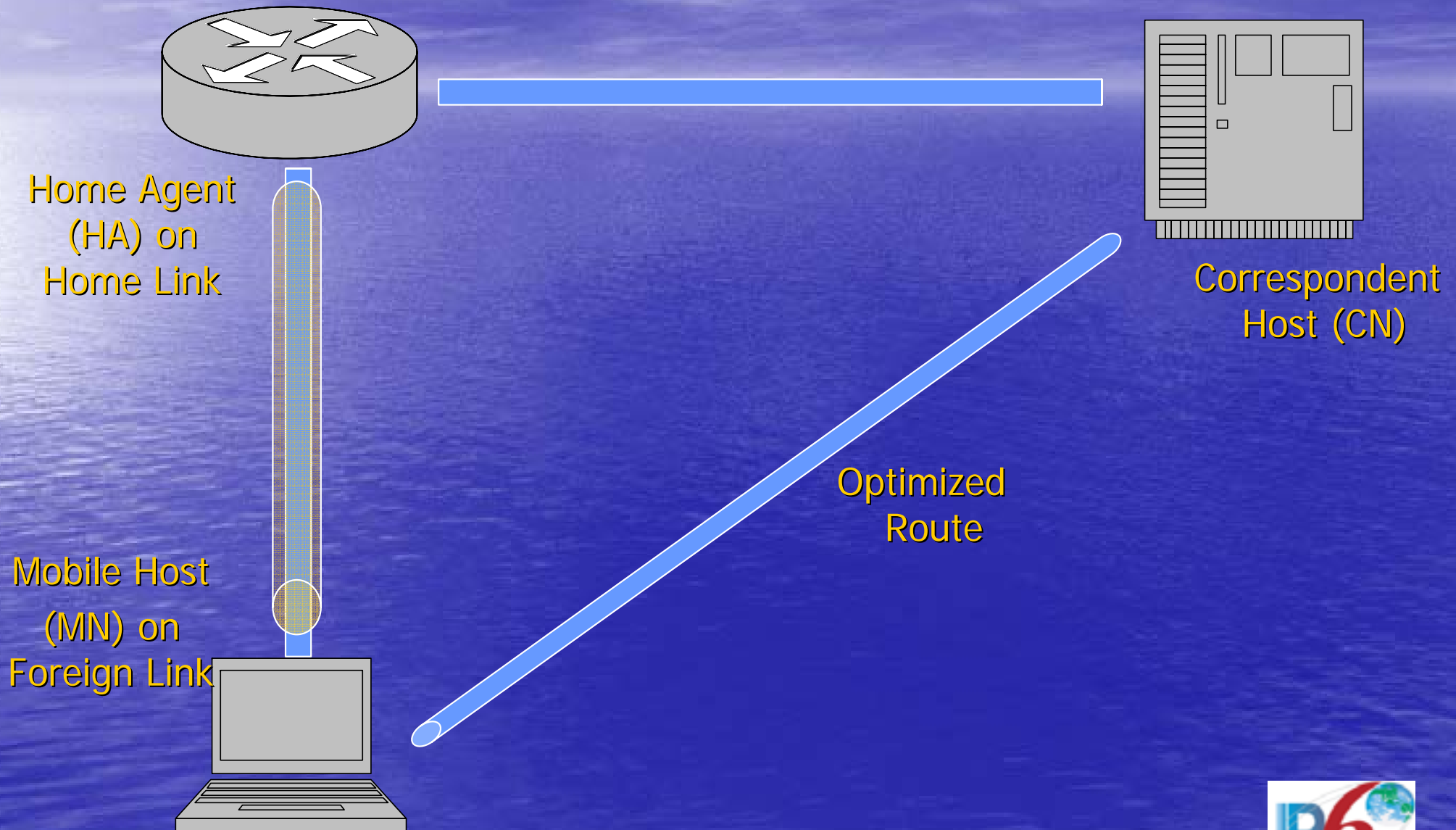
# Mobile IPv6 Motivation

- Roaming laptop computer
  - Reachability
  - Transparency
  - Continuity of connections
    - Otherwise changing IP addresses breaks connections
  - Tradeoff between optimal routing and location privacy
- “Third generation” mobile phones

# Mobile IPv6 Overview

- IP addresses are used for both **identity** and **location**
- Identity: Mobile host (MN) keeps a permanent home address (HoA)
- Location: A router on home link called home agent (HA) knows where MN really is (care-of address, CoA)
  - A **binding** exists between the home and care-of addresses

# Mobile IPv6, the Main Players



# Mobile IPv6 Terminology

- MN: Mobile Host
- CN: Correspondent Host
- HA: Home Agent
- HoA: Home Address
- Home Link
- Foreign Link
- CoA: Care-Of Address
- Binding
- Binding Cache (on HA or CN)
- Binding Update List (on MN)
- Route optimization

# Mobile IPv6 Protocols

- MN announces a new Care-Of address:
  - Binding Update (BU) and Binding Update Acknowledgement (BUA) between MN and:
    - HA
    - CN
- MN finds a HA
  - Dynamic Home Agent Address Discovery (DHAAD)
- MN learns about home link renumbering
  - Mobile Prefix Solicitation (MPS)
  - Mobile Prefix Advertisement (MPA)
- Protocol elements:
  - IPv6 Mobility Header and Destination Options
    - BU and BUA
  - IPv6 Mobility Header and Destination Options
    - Home Address Option
  - IPv6 Type 2 Routing Header
  - ICMPv6

# Main Changes: Mobile IPv4 to IPv6

- IPv6 has autoconfiguration, unreachability detection, globally unique addressing (without NAT), routing and mobility headers, home agent address discovery, and mandatory IPsec
- Two-way tunneling used
  - Better for handling ingress filtering
- No need for “foreign agent” or special AAA support
  - Handled directly at MN
- Route optimization is standard
  - New approach to security

# Mobile IPv6 Security: Outline

1. Introduction to Mobile IPv6
2. Threats and Attacks against Mobile IPv6
3. Security between Mobile Host and Home Agent
  - Changes to IKE and IPsec
4. Security between Mobile Host and Correspondent Host
  - Type 2 Routing Header and Home Address Option
5. Summary and References

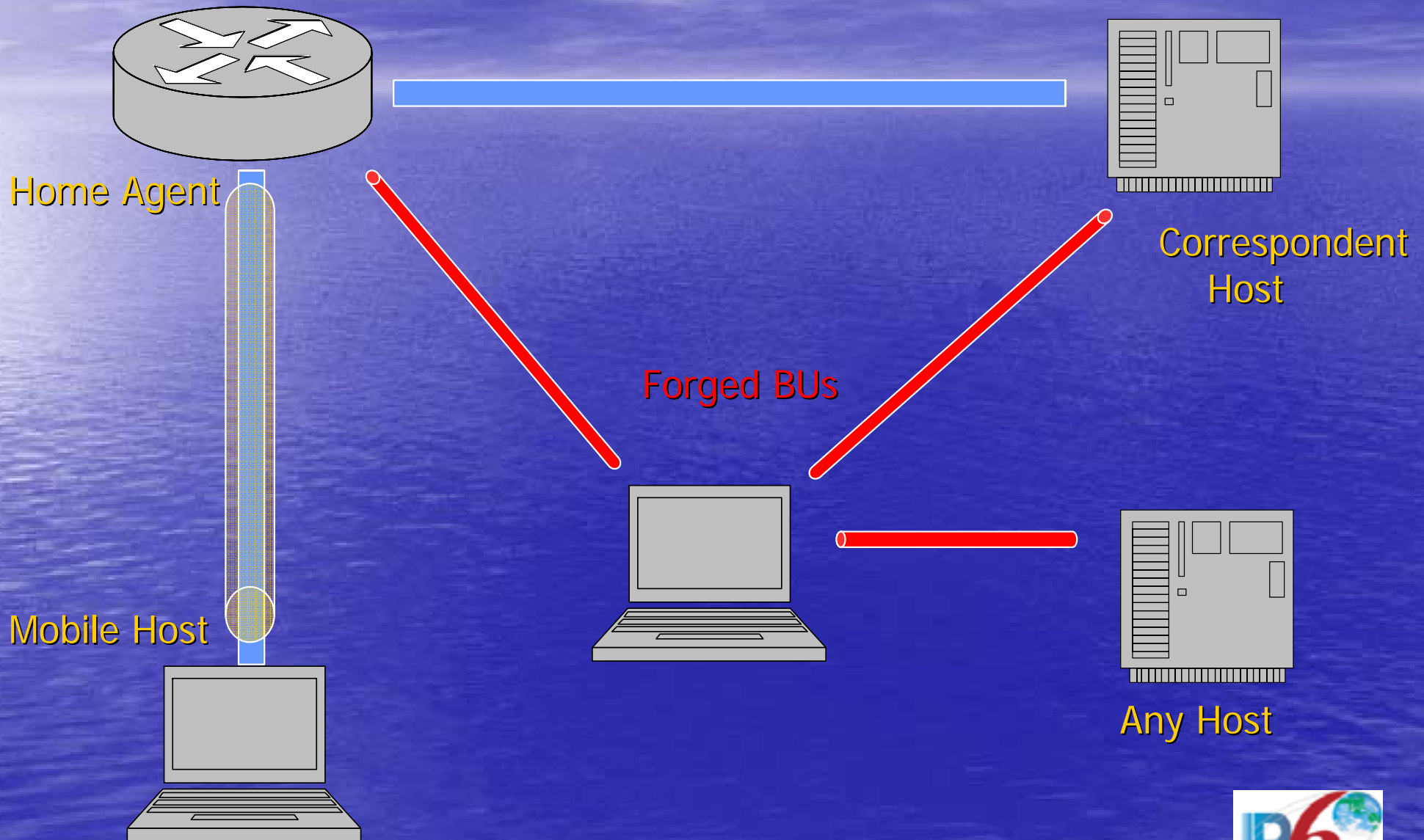
## 2. Threats and Attacks

- Security goals:
  - Don't make anything worse
  - Use what exists where practical
- Attacks exist against:
  - BU between MN and HA
  - BU between MN and CN
  - IPv6 headers and options:
    - Routing and Mobility Headers
    - Home Address and alternate Care-of Address options
  - ICMPv6
- Actually used threat analysis in design

# Threats against Binding Updates

- Most of the threats to MIPv6 involve Binding Updates
  - Many result in Denial of Service (DoS)
    - Starve the MN
    - Flood another host
  - Some allow
    - Hijacking
    - Eavesdropping
    - Man-in-the-middle
    - Impersonation attacks

# Forged Binding Updates



# Bogus BU between MN and HA

- May be sent by another legitimate MN
- MN has to show HoA “ownership”
- Main difference between BU with HA and CN
  - MN likely has on-going relationship with HA

# Bogus BU between MN and CN

- Redirect traffic between *any* pair of hosts
- Example:
  - Alice communicates with Bob
  - Eve sends Bob a BU that Alice's new Care-Of Address is Eve's address
    - Alice does not have to be mobile. Bob does not know.
    - May work when Alice and Bob communicate later
  - May be turned around as a DoS attack on Eve
- Prior relationship between MN and CN unlikely

# Prefix Propagation and HA Discovery

- ICMPv6 Mobile Prefix Solicitation (MPS) and Mobile Prefix Advertisement (MPA)
  - Spoofing MPA breaks HA-MN connectivity
  - Eavesdropping reveals addressing and topology information on home link
- ICMPv6 Home Agent Discovery and ICMPv6 Home Agent Reply
  - Discovery sent to the Home Agent anycast address on the home link
  - Unprotected

# Other Attacks

- Many denial of service “opportunities”
  - Inducing extra BUs
    - No satisfactory defense: route optimization is optional
    - Tradeoff is to risk non-optimal routing
    - Can be selective about route optimization
  - Preventing legitimate BU from completing while sending bogus BU to CN (attacker on same link as victim)
  - Reflection attacks
- Replaying old route optimization BUs
  - Handling crashes and sequence number rollover
- Bypassing firewall egress filtering with a forged Home Address Option

# Mobile IPv6 Security: Outline

1. Introduction to Mobile IPv6
2. Threats and Attacks against Mobile IPv6
3. **Security between Mobile Host and Home Agent**
  - Changes to IKE and IPsec
4. Security between Mobile Host and Correspondent Host
  - Type 2 Routing Header and Home Address Option
5. Summary and References

# 3. Securing MN to HA Communications

- Top priority is stopping a forged Binding Update (BU)
- Security Goal: use existing systems wherever practical
- IPsec is the logical choice
  - Working relationship between MN and HA naturally exists
  - IPsec is mandatory part of IPv6
- IPsec ESP in transport mode used for
  - BU            MN -> HA
  - BUA          HA -> MN
- MN Security Associations must use HoA in either
  - Source address,
  - Home Address destination option, or
  - Type 2 Routing Header
- Authentication transform mandatory
  - Replay detection advisable with dynamic keying

# Securing MN to HA Communications

## BU Message

- IPv6 Header
  - Source = CoA
  - Destination = HA
- Home Address Option
  - Address = HoA
- ESP header
  - Transport mode, authentication
- Mobility header
  - Alternate CoA Option = CoA

## BU Acknowledgement

- IPv6 Header
  - Source = HA
  - Destination = CoA
- Type 2 Routing Header
  - Address = HA
- ESP header
  - Transport mode, authentication
- Mobility header
  - BU Acknowledgement Option

# IPsec at the MN for BU and BUA with HA

## MN SPD

- SPD in: Use SA1 for
  - Source = HA
  - Destination = HoA
  - Protocol = Mobility Header
- SPD out: Use SA2 for
  - Source = HoA
  - Destination = HA
  - Protocol = Mobility Header

## MN SAD

- SA1 (IN, SPI, ESP, TRANSPORT):
  - Source = HA
  - Destination = HoA
  - Protocol = Mobility Header
- SA2 (OUT, SPI, ESP, TRANSPORT):
  - Source = HA
  - Destination = HoA
  - Protocol = Mobility Header

# IPsec at the HA for BU and BUA

## HA SPD

- SPD in: Use SA1 for
  - Source = HoA
  - Destination = HA
  - Protocol = Mobility Header
- SPD out: Use SA2 for
  - Source = HA
  - Destination = HoA
  - Protocol = Mobility Header

## HA SAD

- SA1 (IN, SPI, ESP, TRANSPORT):
  - Source = HoA
  - Destination = HA
  - Protocol = Mobility Header
- SA2 (OUT, SPI, ESP, TRANSPORT):
  - Source = HoA
  - Destination = HA
  - Protocol = Mobility Header

# Security Association Setup with IKEv1

MN

HA

Phase 1: ID = mobile1.home.net



Phase 1: ID = home.net



Phase 2: ID = ID\_IPV6\_ADDR HoA



Phase 2: ID = ID\_IPV6\_ADDR HA



# Security Association Setup with IKEv1

- Optional, but necessary for replay detection
- May use public keys or pre-shared secrets
- With pre-shared secrets, aggressive mode must be used in Phase 1
  - Cannot use the source address of the MN, which is the CoA, to select pre-shared secret
  - No identity hiding in this case
- Similarly, cannot use ID\_IPV6\_ADDR in Phase 1
- Use FQDN in Phase 1 and HoA in Phase 2
  - HA must verify relationship
  - HoA cannot be dynamically assigned
  - This area is a bit vague: DNSSEC? X.509? CGA?

# Mobile IPv6 Security: Outline

1. Introduction to Mobile IPv6
2. Threats and Attacks against Mobile IPv6
3. Security between Mobile Host and Home Agent
  - Changes to IKE and IPsec
4. Security between Mobile Host and Correspondent Host
  - Type 2 Routing Header and Home Address Option
5. Summary and References

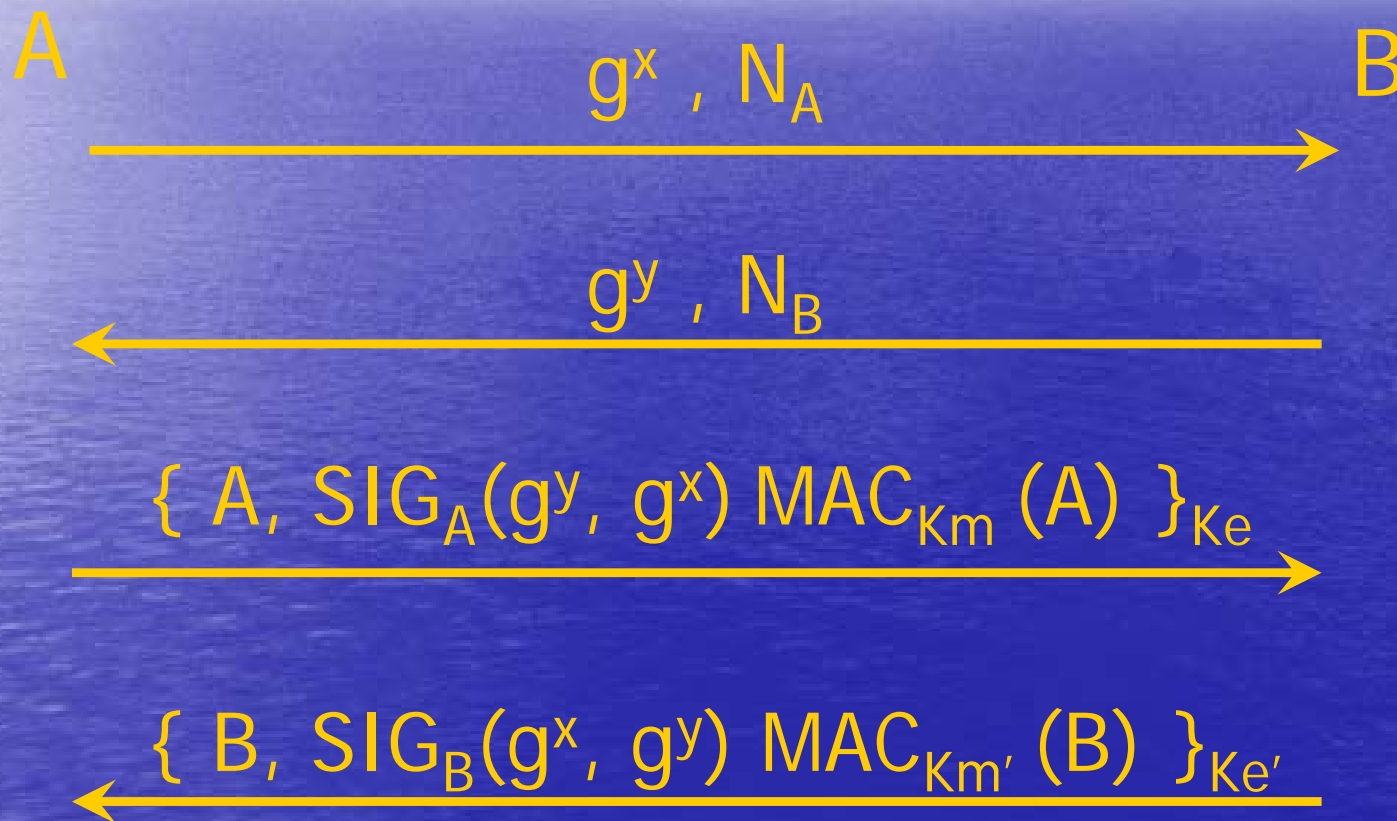
# IKE and IPsec: Current Revisions

- IKE v2
  - Problems fixed, much simpler, rarely used options dropped
  - Four-message sign-and-MAC protocol, formal security analysis
  - Cleaner design, better reliability
  - One document for protocol, one for the transforms
  - Still under discussion for IKEv2:
    - Mobility
    - PKI
- ESP, AH, and RFC2401bis
  - 64-bit (implicit) sequence numbers
  - Arbitrary padding
  - Dummy packets: Protocol 59
  - Virtual IDs to support VPNs
  - New processing model
- New algorithms and modes
  - Full support for AES-128 (encryption and MAC)
  - Two counter mode specifications



# IPsec: IKEv2 Key Exchange Protocol

IKEv2 adds directional protection, etc.



# Securing Other MN to HA Traffic

- Once we have IPsec for MN-HA BU & BUA, what else can we secure with it?
  - ICMPv6 between the Home Agent and Mobile Host
    - MPS and MPA prefix discovery
    - Dynamic Home Agent Address Discovery (DHAAD)
  - Return routability messages
    - “Home Test Init” and “Home Test”
  - User traffic
    - Anything else

# Security Associations at the MN

- Four sets of ESP SPD and SAD entries to and from the HA:
  - Transport mode for Mobility Headers for BU and BUA with the HA for authentication
  - Transport mode for ICMPv6 for home network prefix discovery for authentication
  - Tunnel mode for Mobility Headers for return routability messages to and from the CN for authentication and confidentiality
  - Optional tunnel mode for all other traffic for authentication and confidentiality

# A Few Words on Firewalls

- The model is changing
  - “Inside” and “outside” are harder to define
  - Change is consistent with IPv6 functionality
- IPv6 firewalls exist but are immature
  - Protocols are more firewall-friendly than with IPv4
- NAT is not much security
- Reasons for firewalls
  - There are bad things out there in the world
  - Accidents happen
  - Inside applications have inadequate security
    - These can be handled much as with IPv4 firewalls and VPNs
  - Insiders may do bad things
    - No complete technical solution
    - Need to make peace with IPsec
      - SSL is just as bad, right?

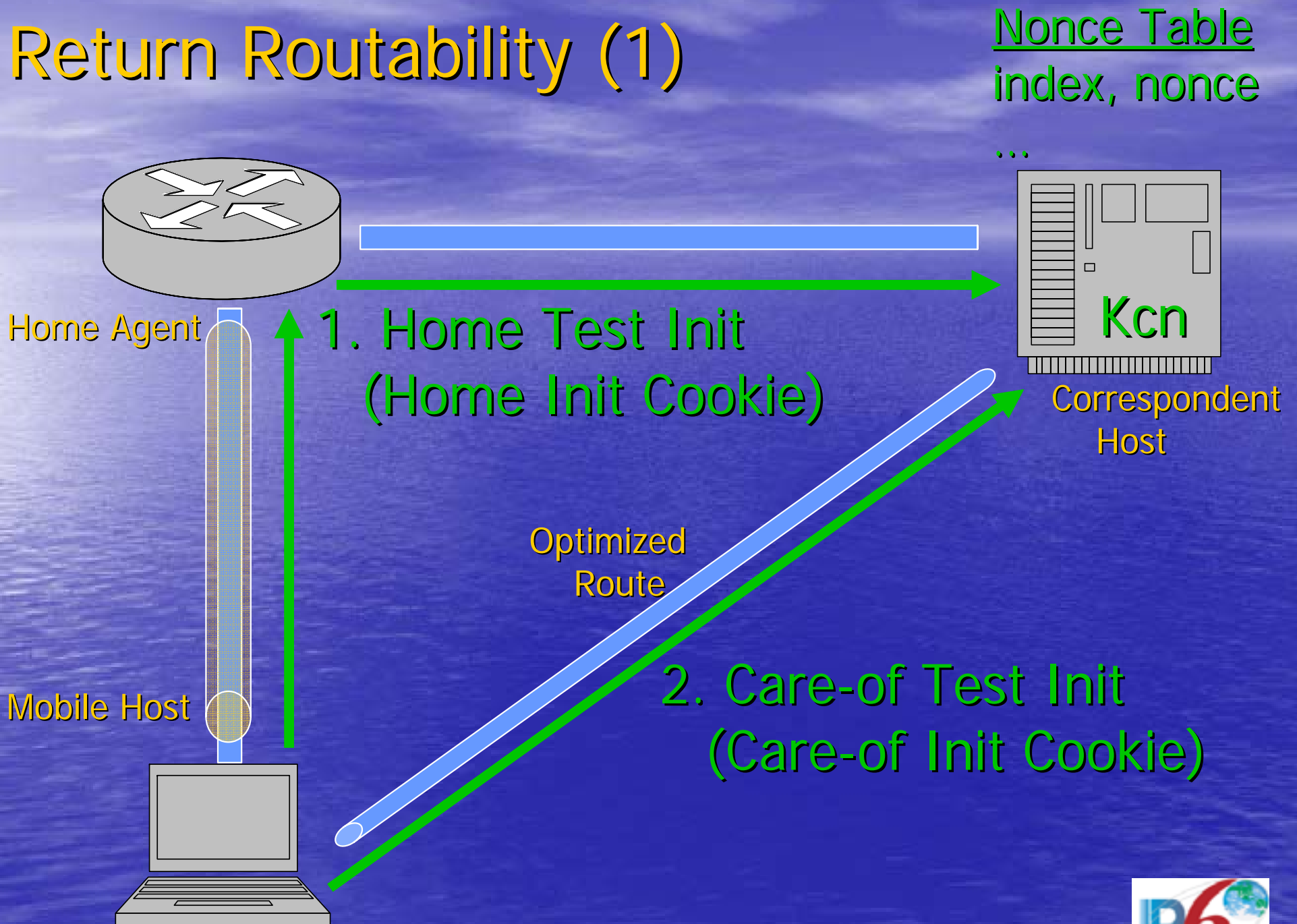
# Mobile IPv6 Security: Outline

1. Introduction to Mobile IPv6
2. Threats and Attacks against Mobile IPv6
3. Security between Mobile Host and Home Agent
  - Changes to IKE and IPsec
4. Security between Mobile Host and Correspondent Host
  - Type 2 Routing Header and Home Address Option
5. Summary and References

# 4. Securing MN to CN Communications

- Major threats:
  - CN gets a forged BU
    - CN MAY ignore BUs
  - CN processes a Home Address Option sent without authorization
- Original solution was IPsec
  - Rejected by the IESG based on deployability
  - Assume, however, a Security Association exists between MN and HA

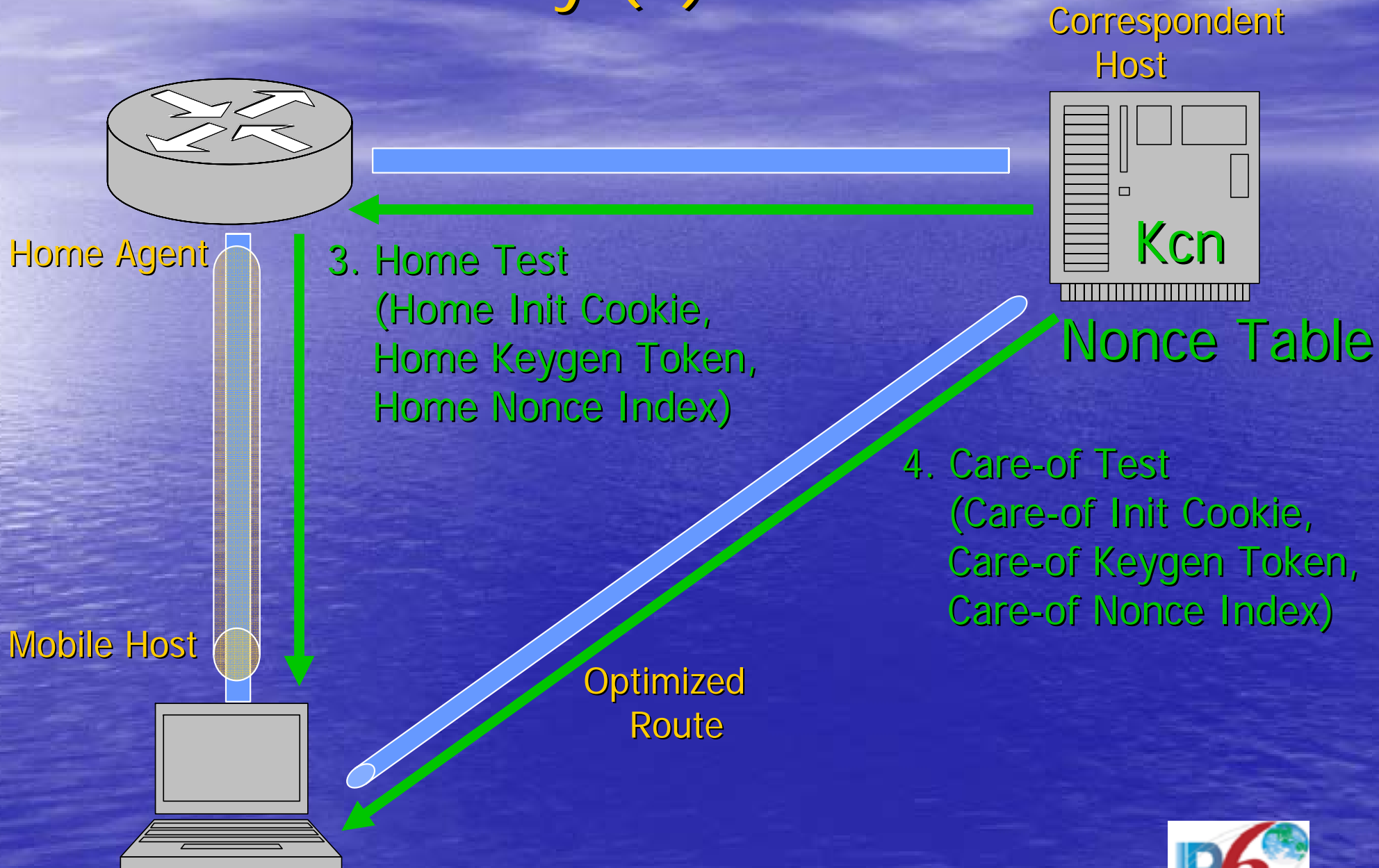
# Return Routability (1)



## Return Routability (2)

- CN computes:
  - Home Keygen Token =  
 $\text{First}(64, \text{HMAC\_SHA1}(K_{cn}, (\text{Home Address}, \text{HoA Nonce}, 0)))$
  - Care-of Keygen Token =  
 $\text{First}(64, \text{HMAC\_SHA1}(K_{cn}, (\text{Care-of Address}, \text{CoA Nonce}, 1)))$
- CN, later, when addresses and nonce indices are returned, can re-compute tokens and:
  - $K_{bm} = \text{SHA1}(\text{Home Keygen Token}, \text{Care-of Keygen Token})$
- CN does not allocate Binding Cache entry until authentication completes

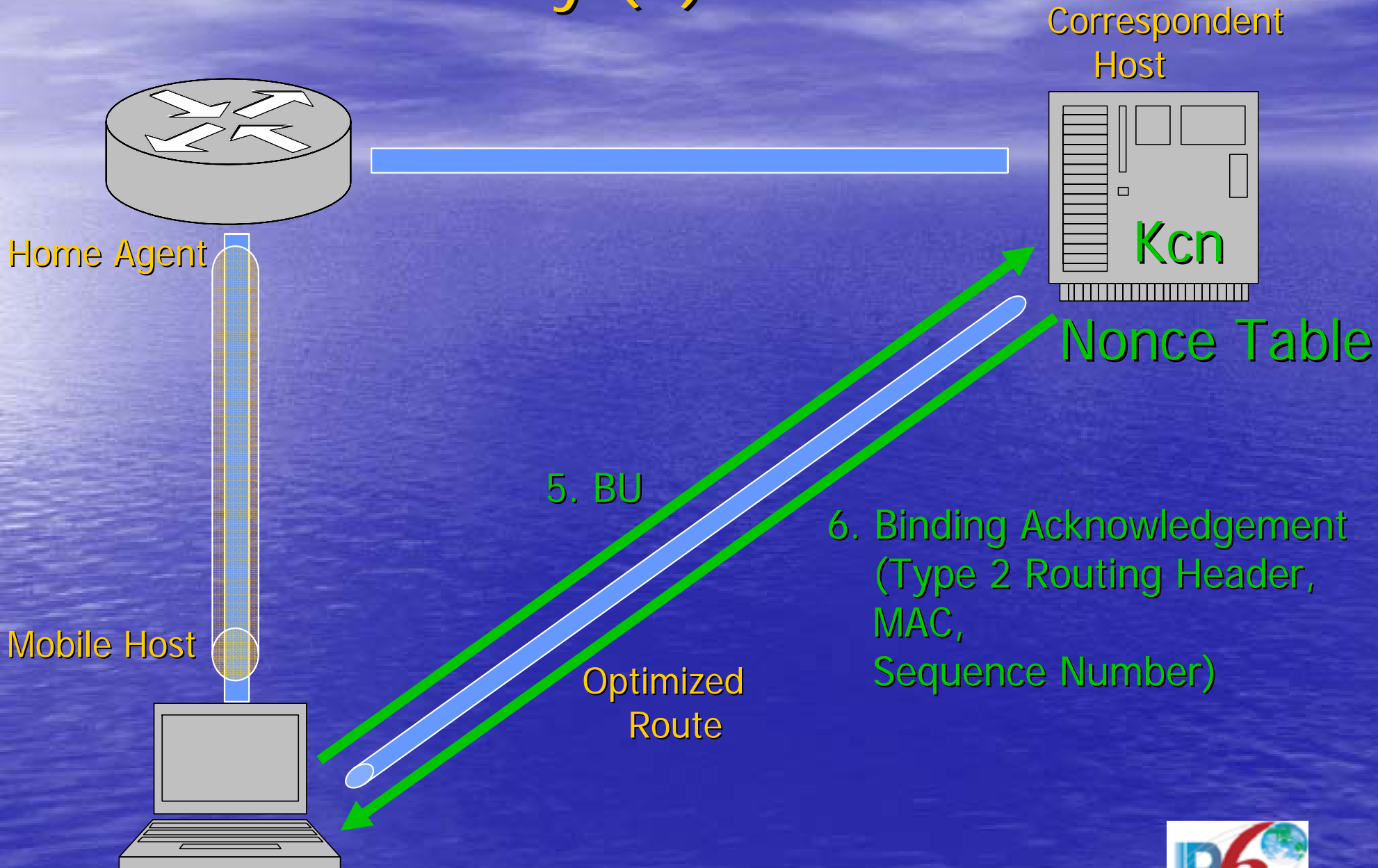
# Return Routability (3)



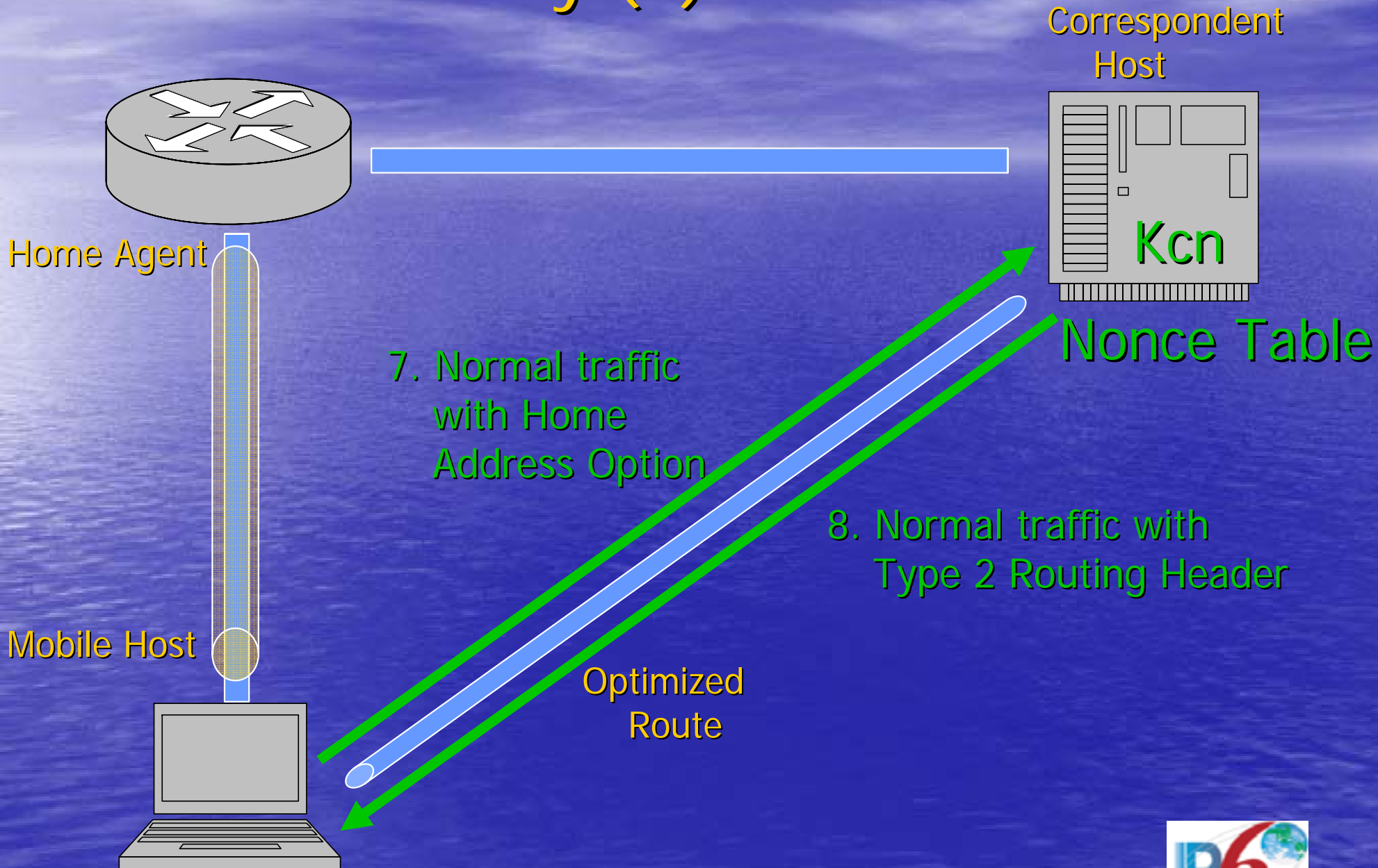
# Return Routability (4)

- MN computes:
  - $K_{bm} = \text{SHA1}(\text{Home Keygen Token}, \text{Care-of Keygen Token})$
  - Binding Update Message Authentication Code  
 $\text{BU MAC} = \text{First}(96, \text{HMAC-SHA1}(K_{bm}, (\text{Care-of Address} \mid \text{CN address} \mid \text{BU}^*)))$
  - Binding Update  
 $\text{BU} = (\text{Home Address Option}, \text{BU MAC}, \text{sequence number}, \text{Home Address Nonce Index}, \text{Care-of Address Nonce Index})$

# Return Routability (5)



# Return Routability (6)



# Mobile IPv6 Security: Outline

1. Introduction to Mobile IPv6
2. Threats and Attacks against Mobile IPv6
3. Security between Mobile Host and Home Agent
  - Changes to IKE and IPsec
4. Security between Mobile Host and Correspondent Host
  - **Type 2 Routing Header and Home Address Option**
5. Summary and References

# Restrictions on Home Address Option

- Only one per packet
- Must not be altered en route
- Must be unicast and routable address
- Must not cause changes in routing or binding cache
- If a BU at CN, must be authenticated with the Kbn established during return routability
- If a BU at HA, must be authenticated with transport mode ESP
- If not a BU, must correspond to an entry in the binding cache

# Restrictions on Type 2 Routing Header

- Only one Type 2 RH per packet
- Only one segment remaining
  - Must be within the end node receiving the RH
- HoA in Type 2 RH cannot have smaller scope than CoA in destination
- HoA must be routable and unicast
- HoA must be the correct one for the MN

# Security between MN and CN

- Summary

- Attacker has to intercept two messages sent along different paths to get  $K_{bm}$
- Greatest threat is in the MN's local link
  - Use IPsec with encryption to protect the Home Keygen Token in the Home Test (message 3)
- Similar threats exist against ICMPv6 and SEND on the local link
- We can imagine a variety of ways to strengthen this security model

# Mobile IPv6 Security: Outline

1. Introduction to Mobile IPv6
2. Threats and Attacks against Mobile IPv6
3. Security between Mobile Host and Home Agent
  - Changes to IKE and IPsec
4. Security between Mobile Host and Correspondent Host
  - Type 2 Routing Header and Home Address Option
5. Summary and References

## 5. Summary and Conclusions

- Mobile IPv6 security is based on a security goal and threat analysis
- Used IPsec where clearly practical
- Introduced return routability
- Opportunity to move to “IPsec v2”
- On-going work:
  - Mobike, PKI4Ipsec, EasyCert, BTNS

# References

- Kempf, J., J. Arrko, and P. Nikander, "Mobile IPv6 Security," *Wireless Personal Communications*, Vol. 29, pp. 389-414, 2004.
- Soliman, H., *Mobile IPv6*, Addison-Wesley, 2004.
- Johnson, D., C. Perkins, and J. Arrko, Mobility Support in IPv6, IETF RFC 3775, June 2004.
- Arrko, J., V. Devarapalli, and F. Dupont, Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, IETF RFC 3776, June 2004.
- Roe, M., Authentication of Mobile IPv6 Binding Updates and Acknowledgments, IETF work in progress, draft-roe-mobileip-updateauth-02.txt, expired August 2002.
- Aura, T., and J. Arrko, MIPv6 BU Attacks and Defenses, IETF work in progress, draft-aura-mipv6-bu-attacks-01.txt, expired August 2002.

