IPCN 2001

From Address Orientation to Host Orientation

Pekka Nikander

`http://www.nomadiclab.com/~pnr/homeless/`

Chief Scientist
Ericsson Research NomadicLab

Adjunct Professor
Helsinki University of Technology

Presentation content

- Introduction
- Different approaches
  - SCTP
  - HIP
  - Homeless Mobile IPv6
- Security Issues
  - An attack example: “Future” stealing
  - The Address Ownership Problem
  - Solution ingredients
- Summary
- Conclusions

Introduction

- In the early days of the Internet, each host had a single persistent well-known address and there was no NAT
  - Thus, in practise, **Address** $\cong$ **Host**
  - May people still seem to have this view
- Today, a host typically has a single dynamic address that is mangled with multiple NAT / NAT-PT boxes
- Tomorrow, a typical host will have multiple dynamic addresses which it may use at the same time
  - Thus, in practise, **Address** $\in$ **host** at a given time

- Summary: IPv6, multi-homing and mobility will profoundly change the way we should think

Different approaches

- Invariants that were held in the early days of Internet
  - An address received was the address sent
  - Addresses were *stationary* (non-mobile)
  - Source and destination were *reversible*
  - All hosts *omnisciently* knew to which address they should send packets to reach the wanted host
- These assumptions still largely hold in the APIs

- Different approaches to the problems
  - SCTP (RFC 2960)
  - HIP (IETF WG, Robert Moskowitz)
  - Homeless Mobile IPv6 (our research)

SCTP

- Stream Control Transport Protocol, RFC 2960
- General purpose transport protocol
  - Provides services similar to TCP and UDP
- Originally developed to transport signalling protocols over IP based networks
  - The result is applicable as a generic transport
- Lots of properties that we do not consider here
- Supports multi-homing at the transport level
  - Each SCTP socket is associated with several addresses at both ends
  - An I-D proposes how to change the address sets dynamically

HIP

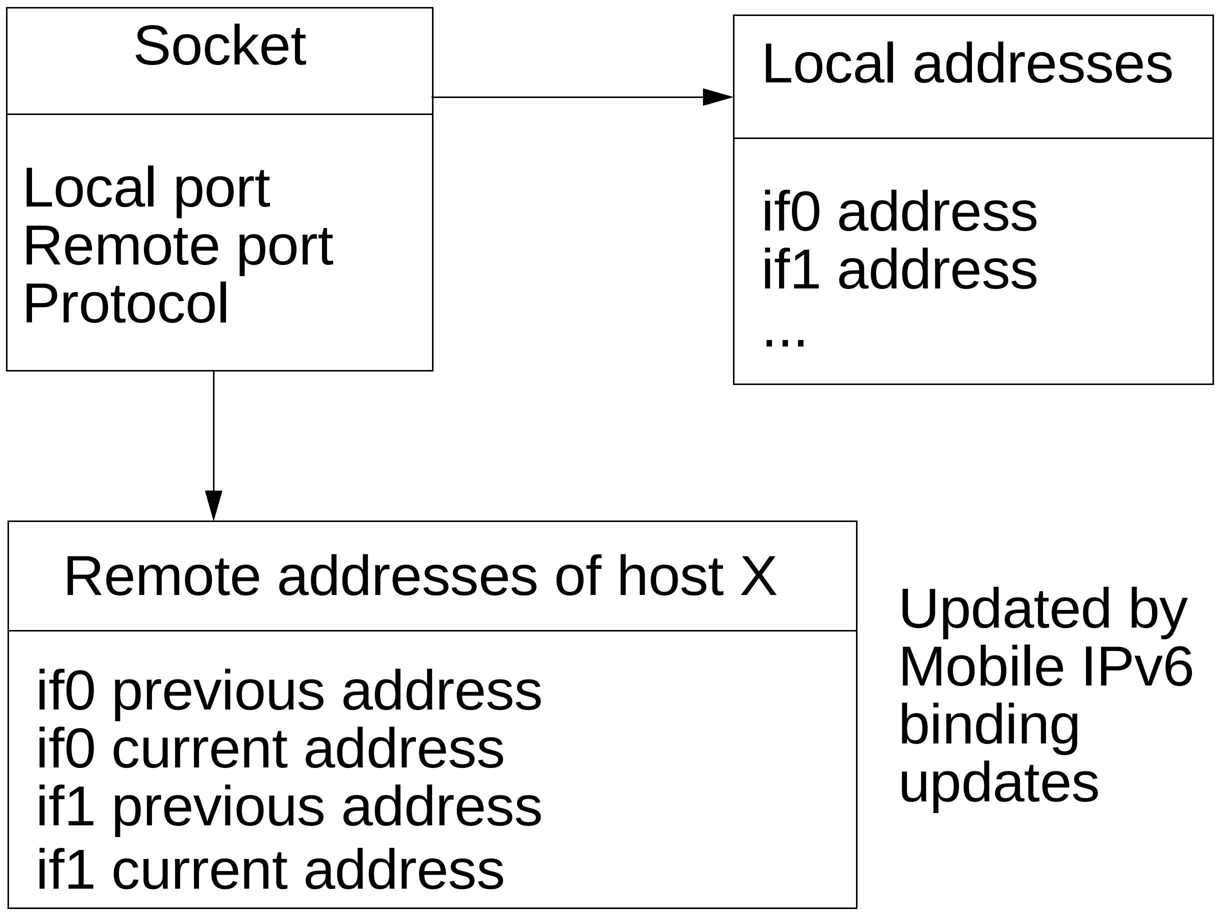
- Host Identity Protocol
- New IETF WG, three drafts by Robert Moskowitz
- Introduces a new Host Identity layer between the IP layer and the upper layers
- The upper layer sockets are bound to Host Identities, not any more to IP addresses
  - A typical HI is a public cryptographic key, and it is represented via its 128 bit has (HIT) or 32 bit LSI
- Binding of Host Identities to addresses is dynamic
  - However, there is only one address per identity
  - I.e. simultaneous multi-homing is not supported
- Current focus on the protocol

Homeless Mobile IPv6

- Ericsson/HUT Research project, one Internet Draft
- A variation of Mobile IPv6, mobility being the default
- Changes the way addresses are used
  - *Semantic* change, or way how addresses are *used*
  - Removes the difference between the home address and the care-of-address(es)
  - Allows easy use of multiple simultaneous home and care-of-addresses
  - Does not require home addresses or home agents any more, but allows them to be used
- Does not change any other aspects of Mobile IPv6
  - E.g. hierarchical routing or micro mobility solutions may still be used

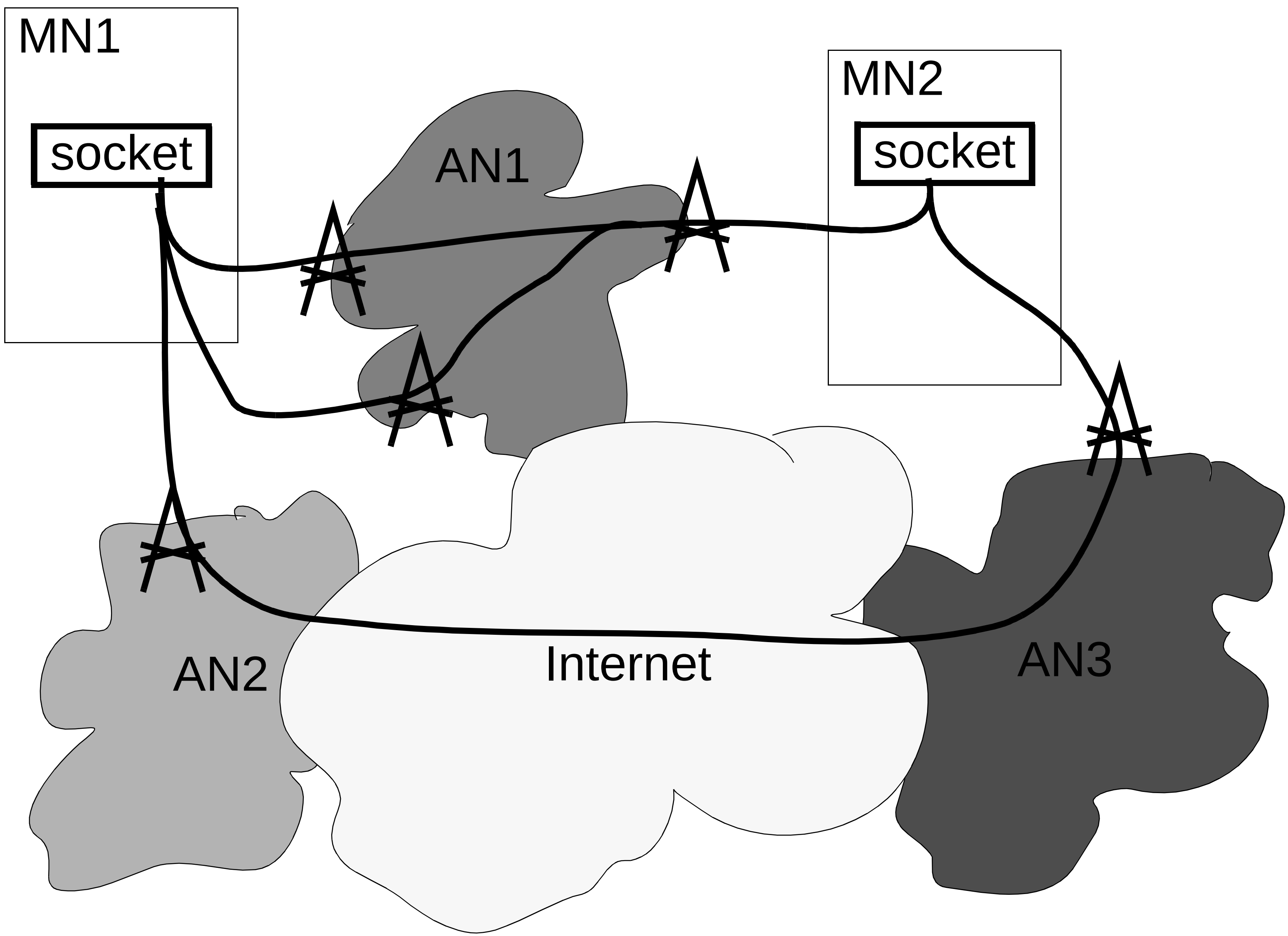
Basic Homeless Approach

- Bind sockets to address sets, not single addresses



- Home addresses are not needed (hence the name)
  - Home agents may still be used as points-of-contact

Basic Homeless Approach (cont.)



Main benefits

- Smaller average IP header size
  - Home Address Destination Options not needed
  - Routing Extension Headers not needed
  - Mobile-to-Mobile IP header size: 92 -> 40 bytes
- Enhances basic fixed end-to-end multi-homing
  - Comparable to the SCTP approach
- Easy to handle router renumbering
  - Receive new prefixes, send them in Binding Updates
- Supports mobile multi-homing / multi-access
  - Destination address MAY be selected for each packet
  - Outgoing interface may differ from packet to packet

  $\rightarrow$ Hand-over between interfaces is seamless

Security Issues

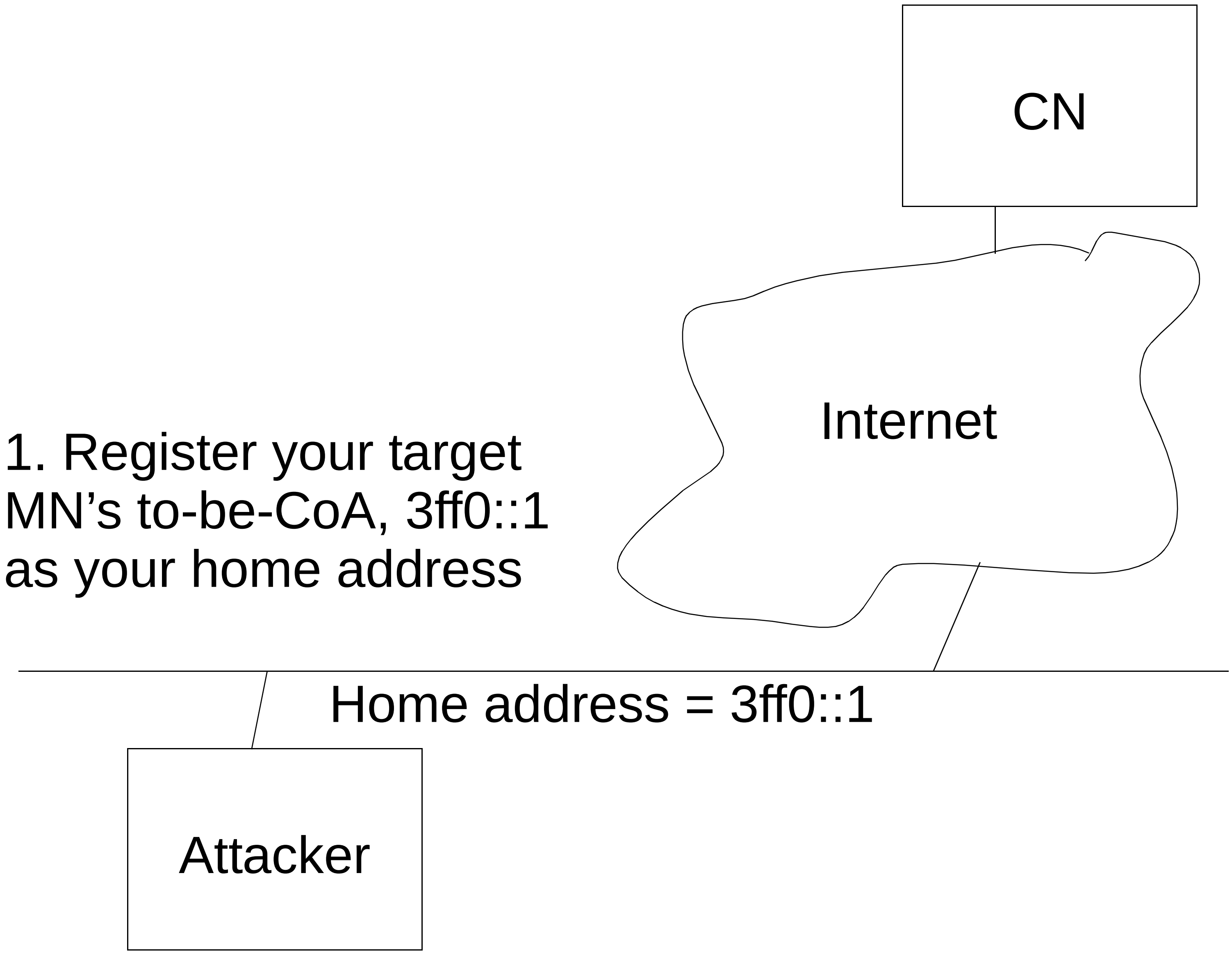
- Security problems emerge when you change addresses
- Problems are more severe if you
  - perform address mappings at the IP layer
  - bind several addresses together (multi-homing)
- Focus here on the IP layer approach
  - Each address is assumed to belong to a single host

  $\rightarrow$ IP layer approach is architecturally better
- An attack example: “Future” stealing
- The Address Ownership Problem
  - Single vs. multiple addresses
  - Hardest case: Mobile Networks
  - Solution ingredients

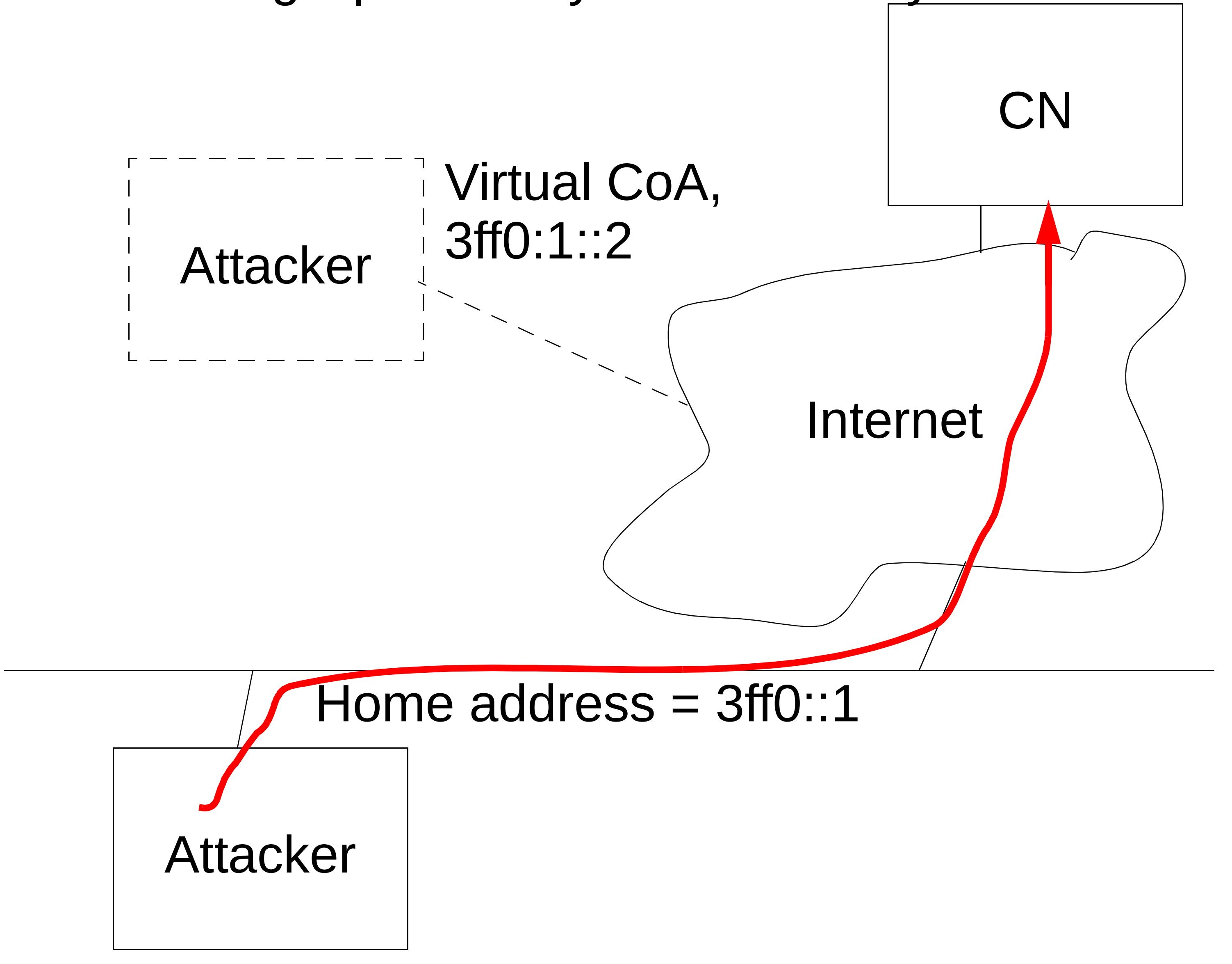
An attack example: “Future” stealing

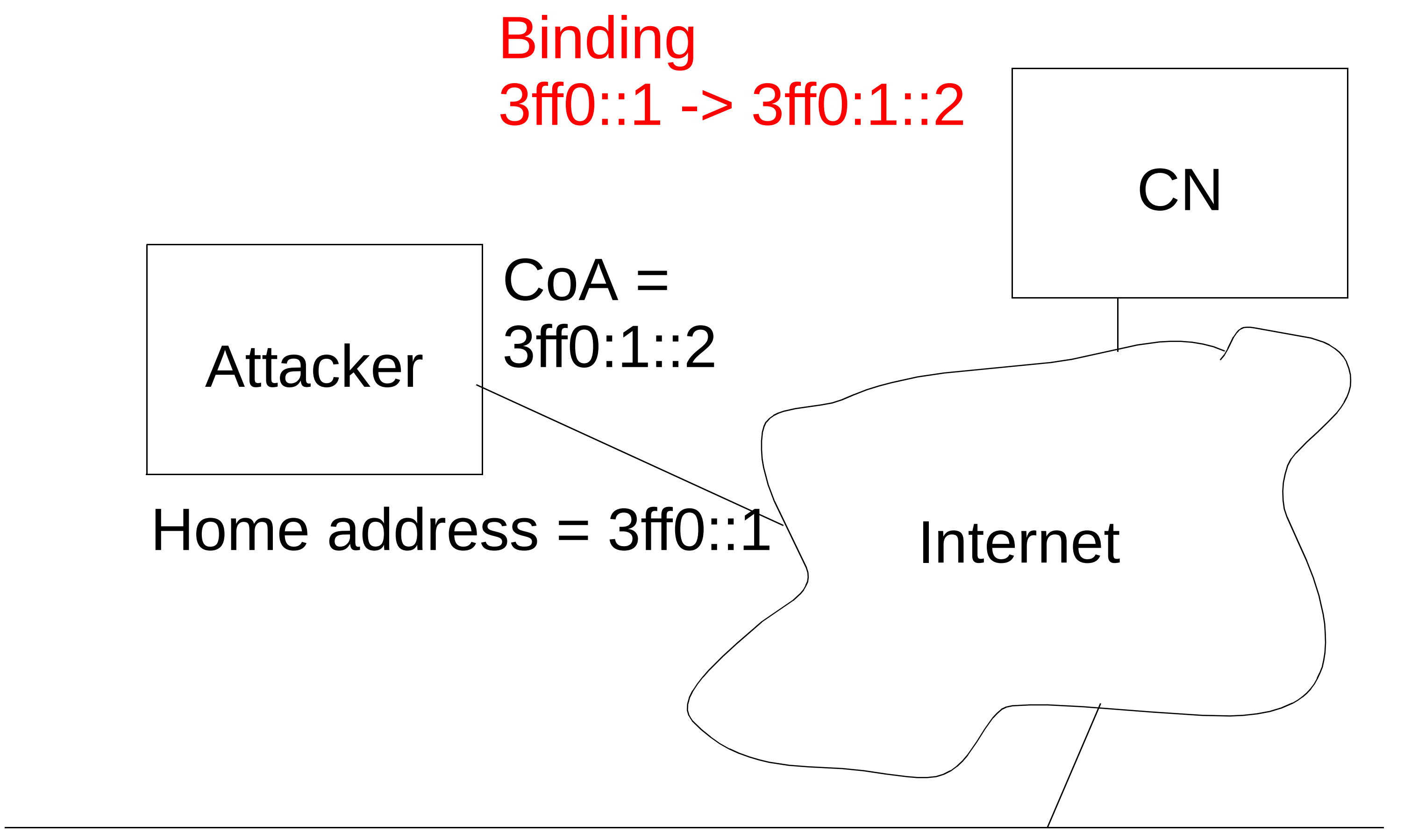
- One specific possible attack
  - This is just an example
  - There are other “similar” attacks
- Represented here in terms of Mobile IPv6
  - Variant also for Homeless Mobile IPv6
  - HIP may also be vulnerable (more analysis needed)

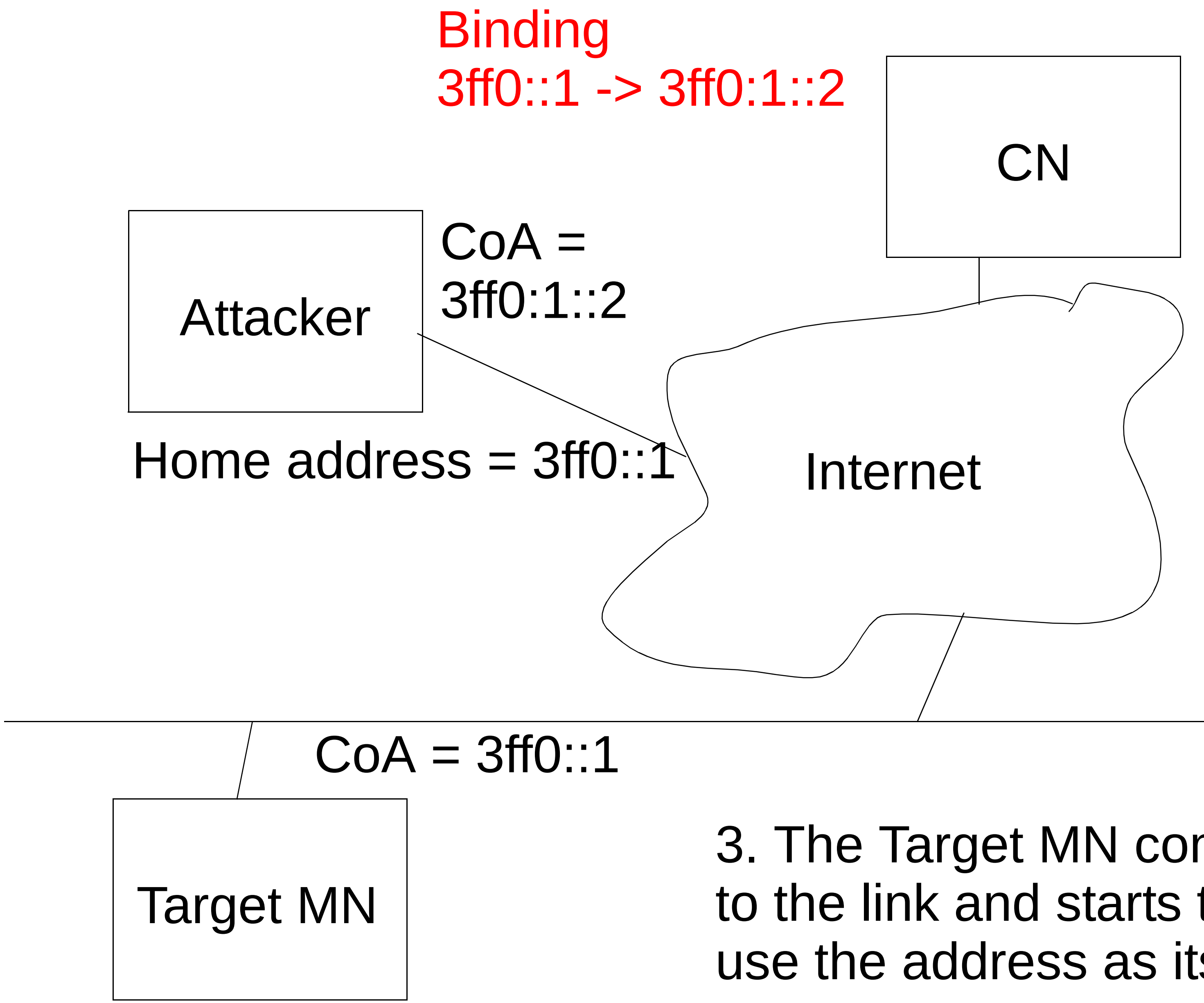
- Redirect traffic sent to an address that you anticipate that your target will be using in the future
- A hypothetical example: divert Mobile IPv6 by creating a Binding for a CoA that your target is likely to use


CN
Internet
1. Register your target
MN’s to-be-CoA, 3ff0::1
as your home address
Home address = 3ff0::1
Attacker

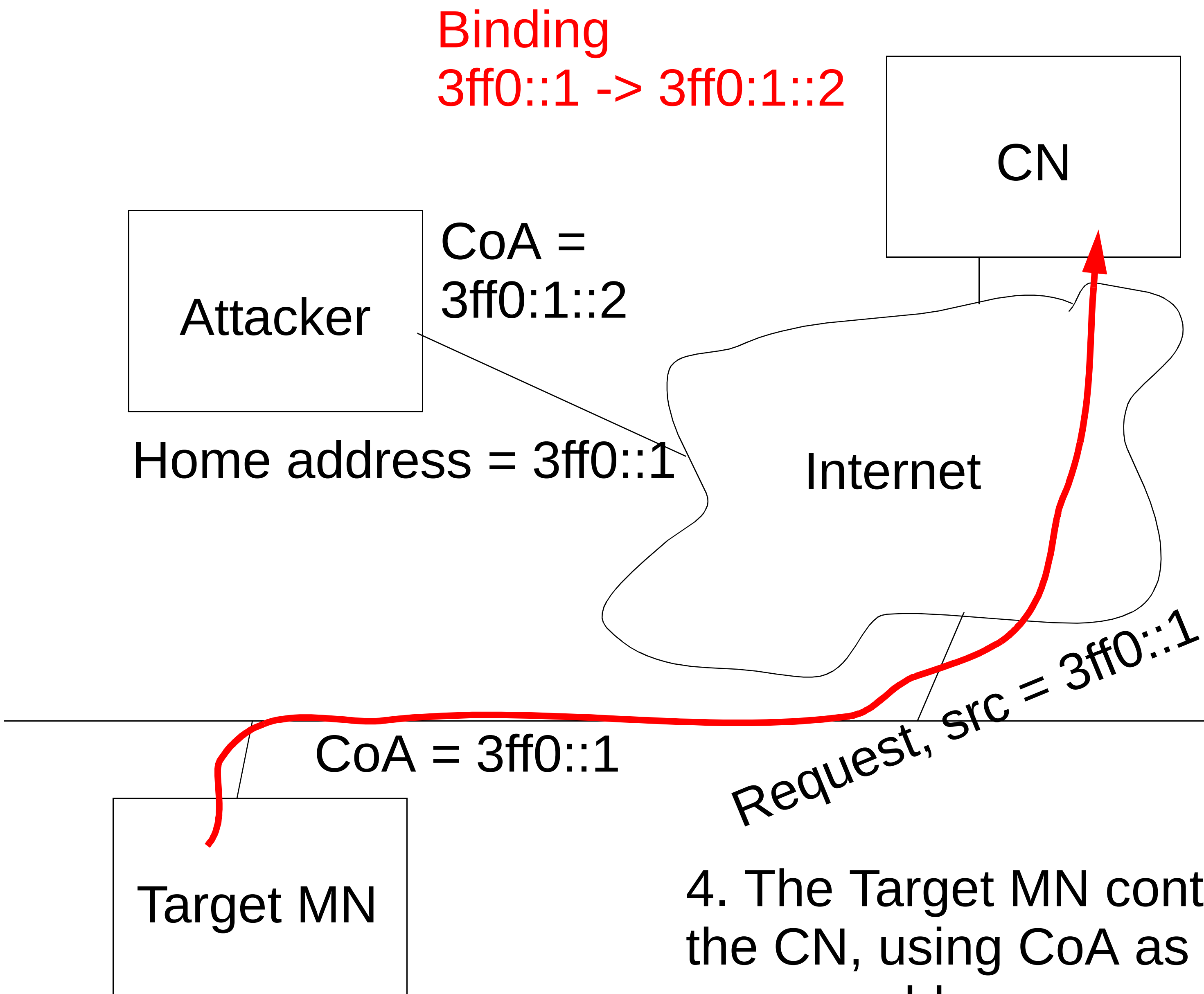
2. Send Binding Update as you move away



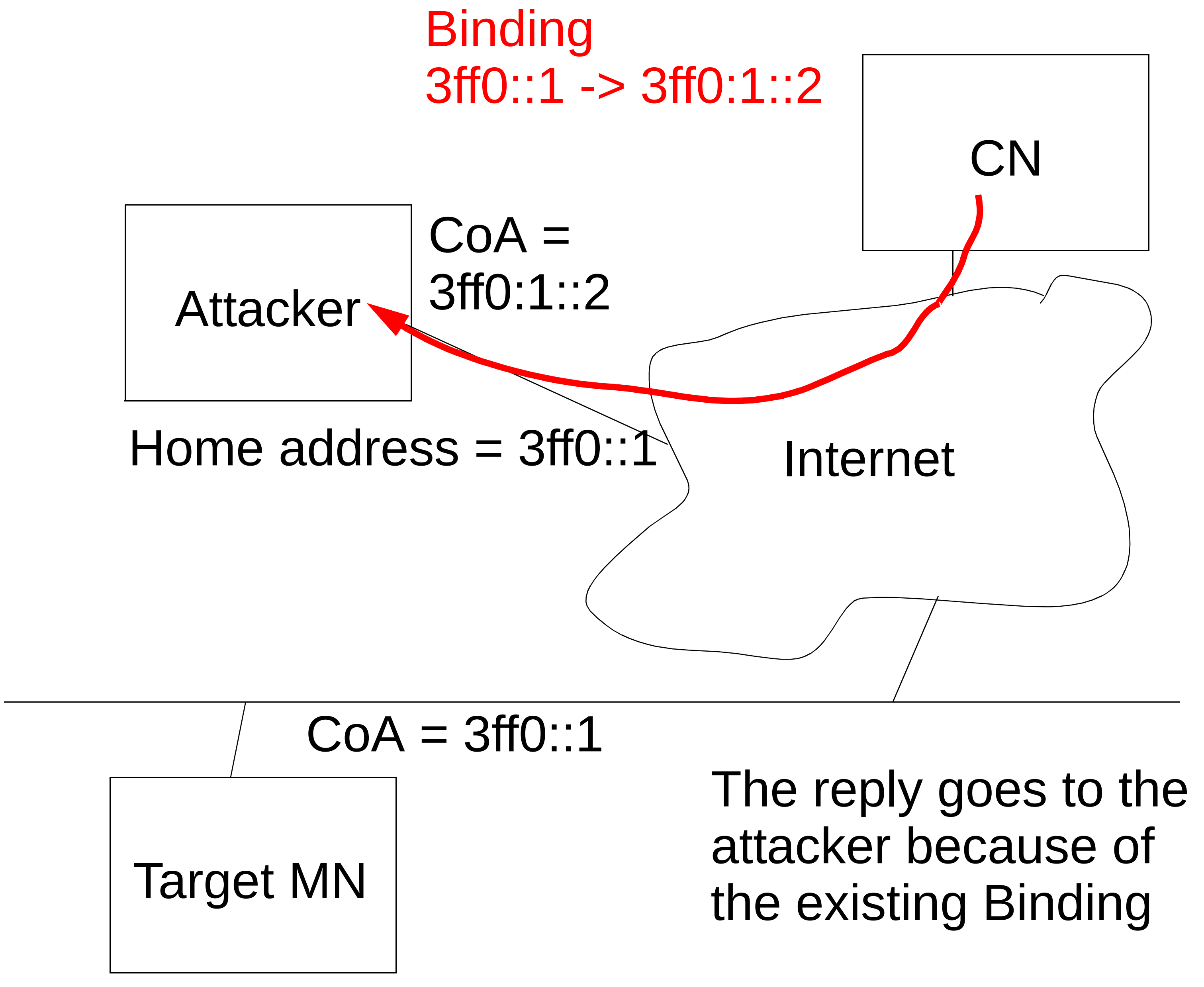

Binding
3ff0::1 -> 3ff0:1::2
CN
CoA =
3ff0:1::2
Attacker
Home address = 3ff0::1
Internet



3. The Target MN comes to the link and starts to use the address as its CoA



4. The Target MN contacts the CN, using CoA as the source address


Binding
3ff0::1 -> 3ff0:1::2
CN
Attacker
CoA =
3ff0:1::2
Home address = 3ff0::1
Internet
CoA = 3ff0::1
Target MN
The reply goes to the
attacker because of
the existing Binding

The Address Ownership Problem

- Who is *authorized* to change routing information for a specified IP address or address prefix?
  - Focus: temporary changes e.g. for mobility
  - Scope: any address/host in the Internet
- Answer: whoever “owns” or “controls” the address
    * (Yes, this is a tautology, but restating a problem often helps)
- Restated problem:
  How do you *show* that you “own” an IP address?
  - More specifically: that you “own” it now and in the (near) *future* as well
- NOTE! Authentication (as per IPsec) is not sufficiently alone; having an IPsec association with a host is *not* a proof that the host is fully honest and competent

Single vs. multiple addresses

- If you use only one address at the time, the scope of the problem is limited
  - E.g. dynamically rebinding a TCP end-point
  - Since you alter only your connections (and not the routing info for the “old” address), you cannot so easily “steal” addresses
- If you use more than one addresses, the problem starts to become more serious
  - Mobile IPv6 Binding Updates (because of home addr)
  - SCTP end-points (especially if going dynamic)
  - Single host multi-homing (e.g. a la Homeless MIPv6)
- Real problems begin once you consider *mobile networks*

Hardest case: Mobile Networks

- Address ownership for single addresses may be workable (a proposed solution to follow)
  - You can challenge the “owner” of the address to show that it really controls the address right now
- Address ownership for mobile subnets seems much harder
  - Problem 1: How do you challenge the router to show that it owns all of the subnet it claims to own?
  - Problem 2: What are the security implications to the hosts that move along with the mobile subnet?

Solution ingredients

- Check that you can reach the “owner”
  - Send a challenge to the address
  - OK only if you get a corresponding reply
- Use random addresses against future address stealing
  - If the attacker cannot anticipate your address, it has much harder time to establish a binding before you
- Protect the random addresses using an OTP like mech.
  - Generate the random part of the address through a series of hashes, and reveal them in reverse order
- In the process, bind a temporary public key to the address, using the address as a crypto token

Summary

- In the future, a host will have a transient set of dynamically allocated addresses
  - Some of these addresses may be used at the same time due to mobility and multi-homing
  - Transport level connections must persist
- Most application still assume stationary addresses
  - Should we fix applications or hide address changes?
- Issues to consider
  - Effects on applications
  - Effects on overall architecture
  - Signalling overhead
  - Security

Summary of solution proposals

- Transport layer solution (SCTP)
  - Incompatible with old applications
  - Requires heavy signalling (separate per connection)
  - Security proposals heavy
- New layer solution (HIT)
  - Some applications may break
  - Changes the architecture
  - Security promising but requires more work
- Network layer solution (Homeless Mobile IPv6)
  - Some applications will break (non RFC 1958 compl)
  - Architecturally most natural (IMHO)
  - Address ownership problem must be solved

Conclusions

- The structure of the Internet is changing
- Old assumptions do not hold any more
- Host and addresses will no more be equal
- New solutions bring forth new problems
  - Signalling overhead
  - Architectural changes
  - Security problems
- There are at least three different approaches
  - Transport layer approach
  - New layer approach
  - Network layer approach