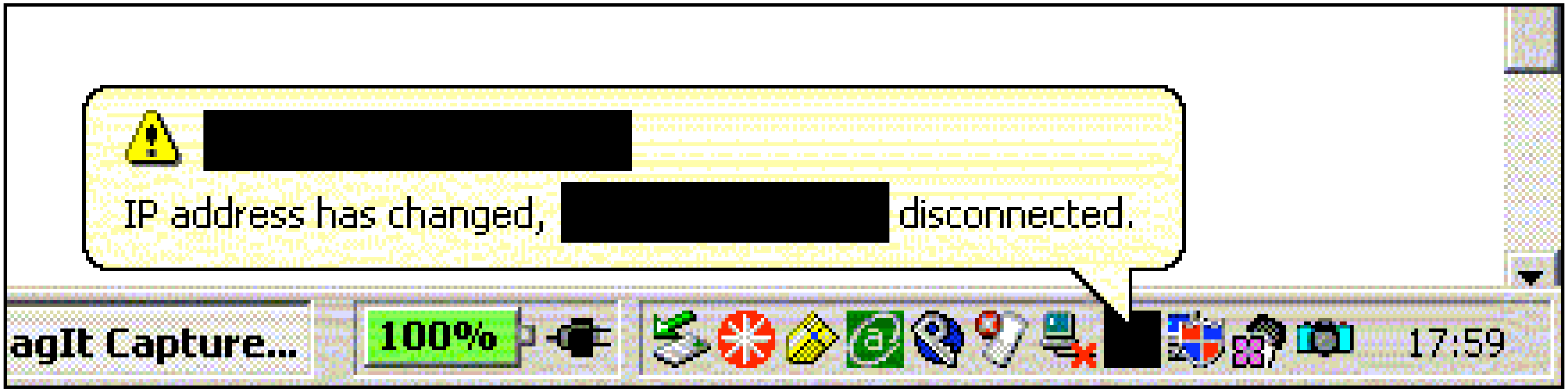
draft-ietf-mobike-protocol-01

Pasi Eronen
IETF63 MOBIKE WG
August 3, 2005

Why we're here

- Actual screen shot from a VPN client (product names deleted)



[redacted]

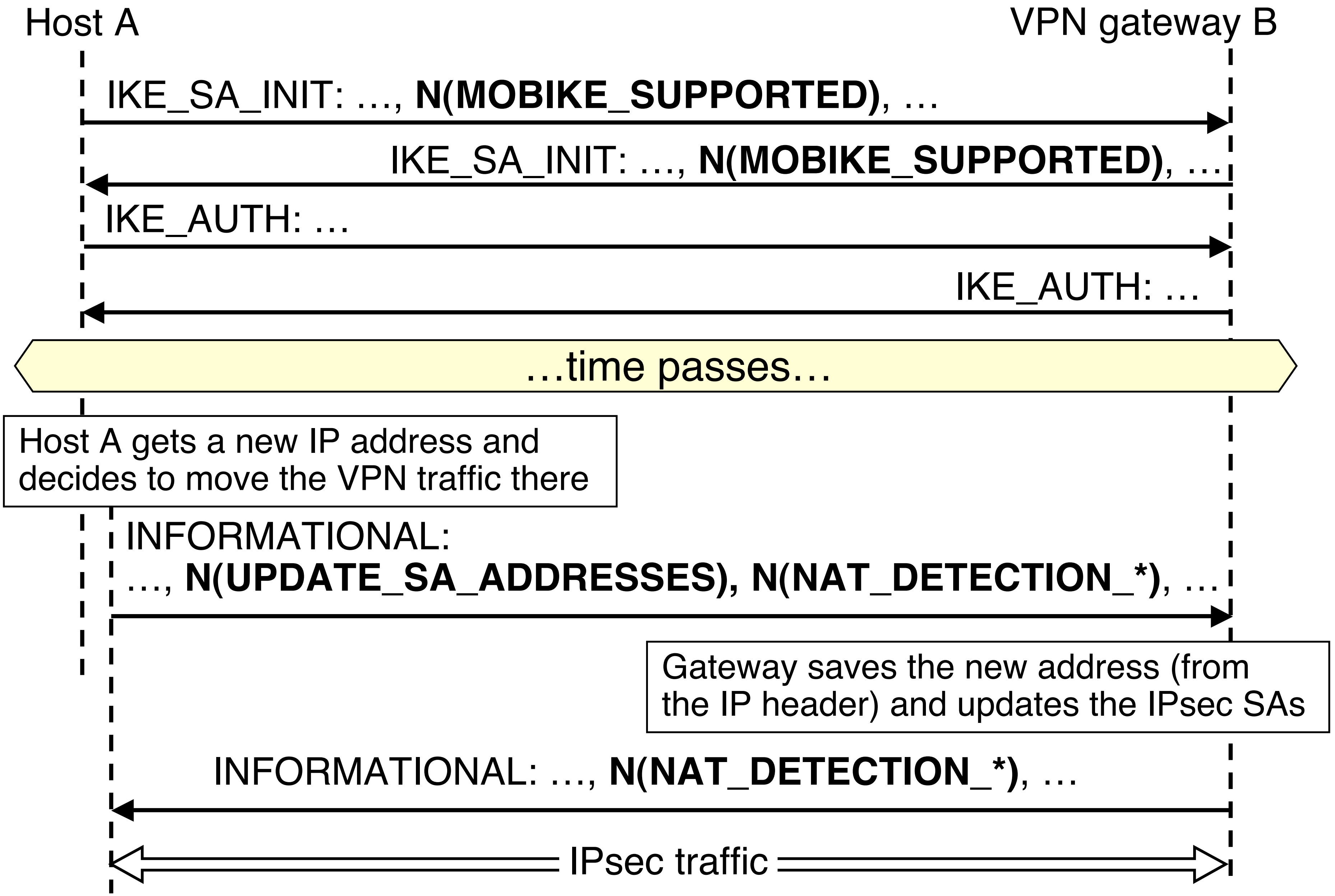
IP address has changed, [redacted] disconnected.

Document status

- New WG document
  - Version –00 out in late June
  - Small updates in –01 two weeks ago
- Obviously not ready yet
  - This presentation describes what is in –01
  - Next presentation is about what still needs to be worked on

One-slide summary: “Initiator decides”

- (Based on WG decision on issue 21)
- Responder sends a list of its addresses to the initiator
- Initiator decides which pair is used for IPsec SAs and tells the responder
  - “Update_SA_Addresses” message (previously called “Change_Path”)
  - If there is any reason to change the addresses (e.g., new interface, DPD failing, etc.) initiator handles it


Host A
VPN gateway B
IKE_SA_INIT: …, N(MOBIKE_SUPPORTED), …
IKE_SA_INIT: …, N(MOBIKE_SUPPORTED), …
IKE_AUTH: …
IKE_AUTH: …
…time passes…
Host A gets a new IP address and decides to move the VPN traffic there
INFORMATIONAL: …, N(UPDATE_SA_ADDRESSES), N(NAT_DETECTION_*), …
Gateway saves the new address (from the IP header) and updates the IPsec SAs
INFORMATIONAL: …, N(NAT_DETECTION_*), …
IPsec traffic

Additional details

- Interaction with NAT Traversal
- Responder address changes
- Path testing
- Return routability test
- Not working with NATs (“NAT prevention”)

Interaction with NAT Traversal

- Include NAT detection payloads in Update_SA_Addresses messages
- Enable/disable NAT Traversal according to detection results
  - Including “dynamic address updates” (if implemented) for handling changes in NAT mappings (issue 34 may change this)

Responder address changes

- If responder’s addresses change, it sends a new list to the initiator
- Does not fully work (and can’t be made to fully work) with NATs/stateful packet filters
  - Current approach: accept this limitation

Path testing

- Both initiator and responder can test if a path works
  - At any time, without possibility of disrupting anything else that might be going on
- Current approach: add separate Path_Test exchange
  - Not needed if we relax the “at any time” or “without disrupting” requirements
  - Or require support for larger window sizes
  - Issue 34 may change this

Return routability test

- Simple Informational exchange with additional “Cookie2” payload
- Can be done at any time according to local policies
  - Before/after updating IPsec SAs, never, …

Not working with NATs

- Currently called “NAT prevention”
  - A better name is probably needed
- Prevent the use of paths with NATs for IPsec SAs
  - If only paths with NAT are available, break connection rather than use them
  - Trade-off between DoS-ing yourself and religious beliefs

Next steps

- Get consensus on remaining technical issues
- Handle remaining editorial comments