“Quick NAP” - Secure and Efficient Network Access Protocol

Jari Arkko
Ericsson Research NomadicLab

Pasi Eronen
Nokia Research Center

Hannes Tschofenig
Siemens

Seppo Heikkinen
Tampere University of Technology

Anand Prasad
DoCoMo Euro-Labs

This presentation has been produced partially in the context of the Ambient Networks Project. The Ambient Networks Project is part of the European Community's Sixth Framework Program for research and is as such funded by the European Commission. All information in this document is provided ``as is'' and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors view

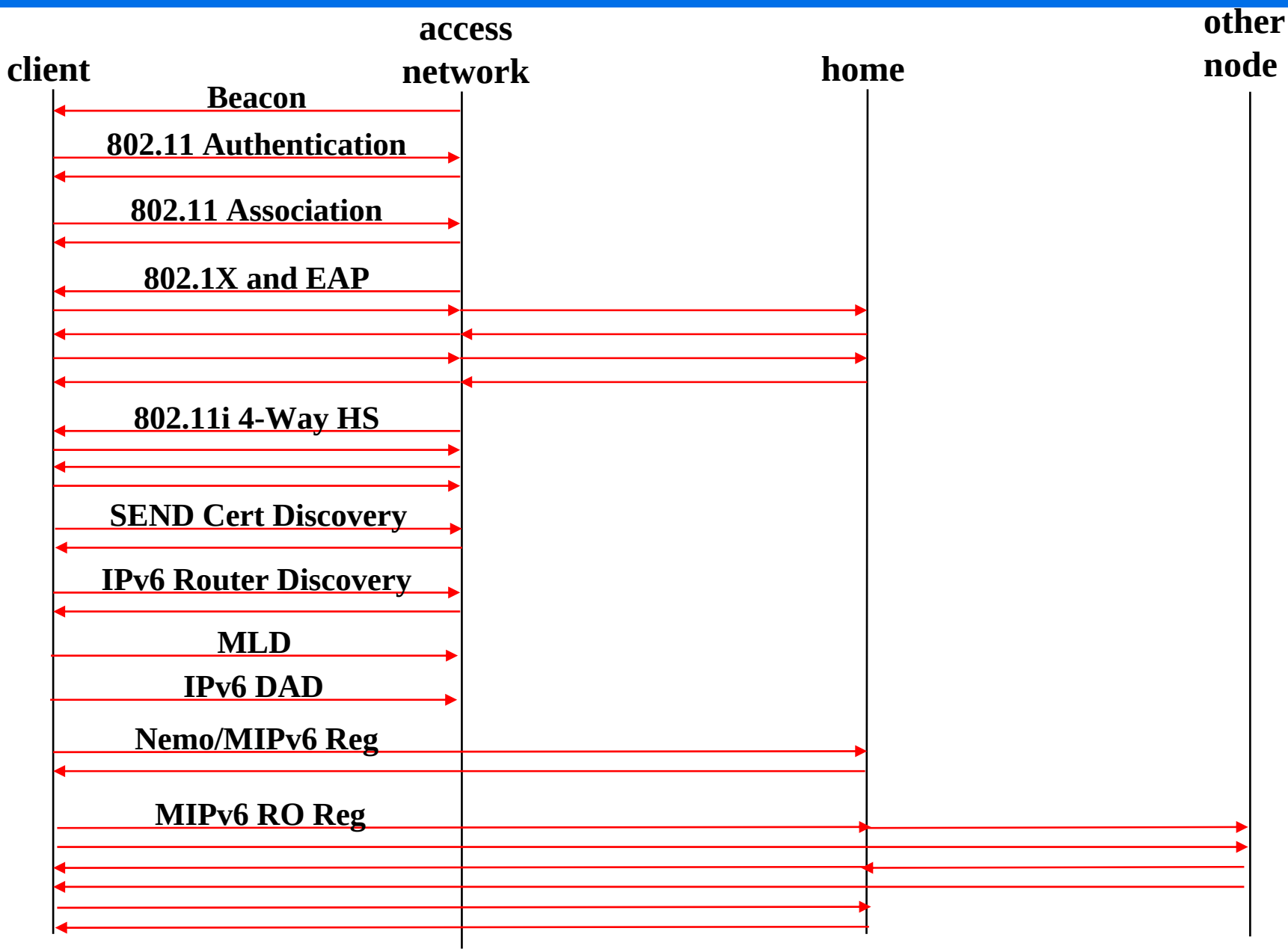
Presentation Outline

- The Problem
- Basis for a new design
- Tentative protocol proposal
- Evaluation and next steps

The Problem

Performance in Network Access (1/2)

- The attachment/movement performance of current protocol stacks is not all that great
- Attachments involve a large number of messages
- Over 50% of this is due to security
- Request/Response style, even across the Internet
- Multiple mandatory waiting periods
- New features lead to a worse situation?


client
access network
home
other node
Beacon
802.11 Authentication
802.11 Association
802.1X and EAP
802.11i 4-Way HS
SEND Cert Discovery
IPv6 Router Discovery
MLD
IPv6 DAD
Nemo/MIPv6 Reg
MIPv6 RO Reg

Performance in Network Access (2/2)

- Much of the excess baggage is due to developing everything in separate SDOs and groups
- L2 fast handoff mechanisms exist, but do not help in all scenarios
- People are developing optimizations to, I believe, all individual parts of the shown flow
  - Will this be sufficient or do we have to collapse several functions into the same mechanisms?

Security in Network Access (1/2)

- Many known specific problems (e.g. algorithms)
  - Solvable
- Privacy protection is non-existent or incomplete
  - MAC addresses
  - Most exchanges are in the clear
  - Limitations in identity privacy support in the protocols
- Denial-of-Service problems
  - Use of cryptographic keys very late in the process
  - Attacks that create/leave state to network side elements
  - Insecure lower-layer “detach” messages

Security in Network Access (2/2)

- No security at all for the open model
- No security for related functions
  - E..g, DHCP security is not deployed
  - No security for control of firewall functions or QoS
  - Secure Neighbor Discovery could be deployed, but attacks remain
  - Why? Deploying new security credentials for these would be extremely expensive
  - Barrier for deploying new functions (e.g. FMIP)

Functionality in Network Access

- Manual processes
  - Web-logins break applications and can't be handled automatically by software
- Configuration and discovery support
  - What are the IP parameters that I can get from this access point?
  - Is my home operator available via this access point?
- Security models do not fit all types of deployment
  - Credit card payments

Ongoing Work

Ongoing Work to Address the Problems...

There is ongoing work for most of the problems:

- IP mobility
  - Optimized mobility mechanisms, e.g., new faster signaling schemes for route optimization
- Address autoconfiguration
  - IPv6 addressing speedups, e.g., Optimistic DAD
  - DHCP and SEND security
- DNA
  - Faster algorithms for detecting whether or not movement has occurred

Ongoing Work, Continued

- Link layer
  - Pre-authentication and proactive key distribution
  - Better protection of payload packets (AES etc)
  - Better information channels from the network to the clients (e.g., 802.21)
  - Bigger subnets (less IP layer work after attachment)
  - ...

Ongoing work

- Everything on previous slides is being addressed
  - People care about this and there are a lot of results!
- Most work focused on a particular “slice” of the problem
- No good understanding of what the impact of individual improvement is for effiency
  - E.g., “I can’t afford 1 RTT in Mobile IP”
- Not enough system-level understanding of the security issues

Basis for a New Design

Approach

- Attempting to solve some of the security, functional, and performance issues
- Focus on the problem as a whole!
  - There are multiple parties involved -- not just two
  - Who needs to communicate with who?
  - How are the parties identified?
  - What is the optimal order of messages?
  - What system security properties are needed?
  - Are there bulk information transfer needs? How can they best be addressed?

Potential Solution Ingredients (1/3)

Security:

- Denial-of-Service protection
  - No separation to “attachment” and “secure attachment”
  - Stateless design on the network side
- Privacy protection
  - Build the protocols for non-static identifiers and addresses
  - Protect communications from the start, not at the end
- Uses hashes of public keys as addresses (a la CGA)
  - Avoid address stealing and functionality to bind addresses to credentials
  - Nodes can generate their addresses and keys on their own, without infrastructure -- works for ad hoc mode too!

Potential Solution Ingredients (2/3)

Protocol construction

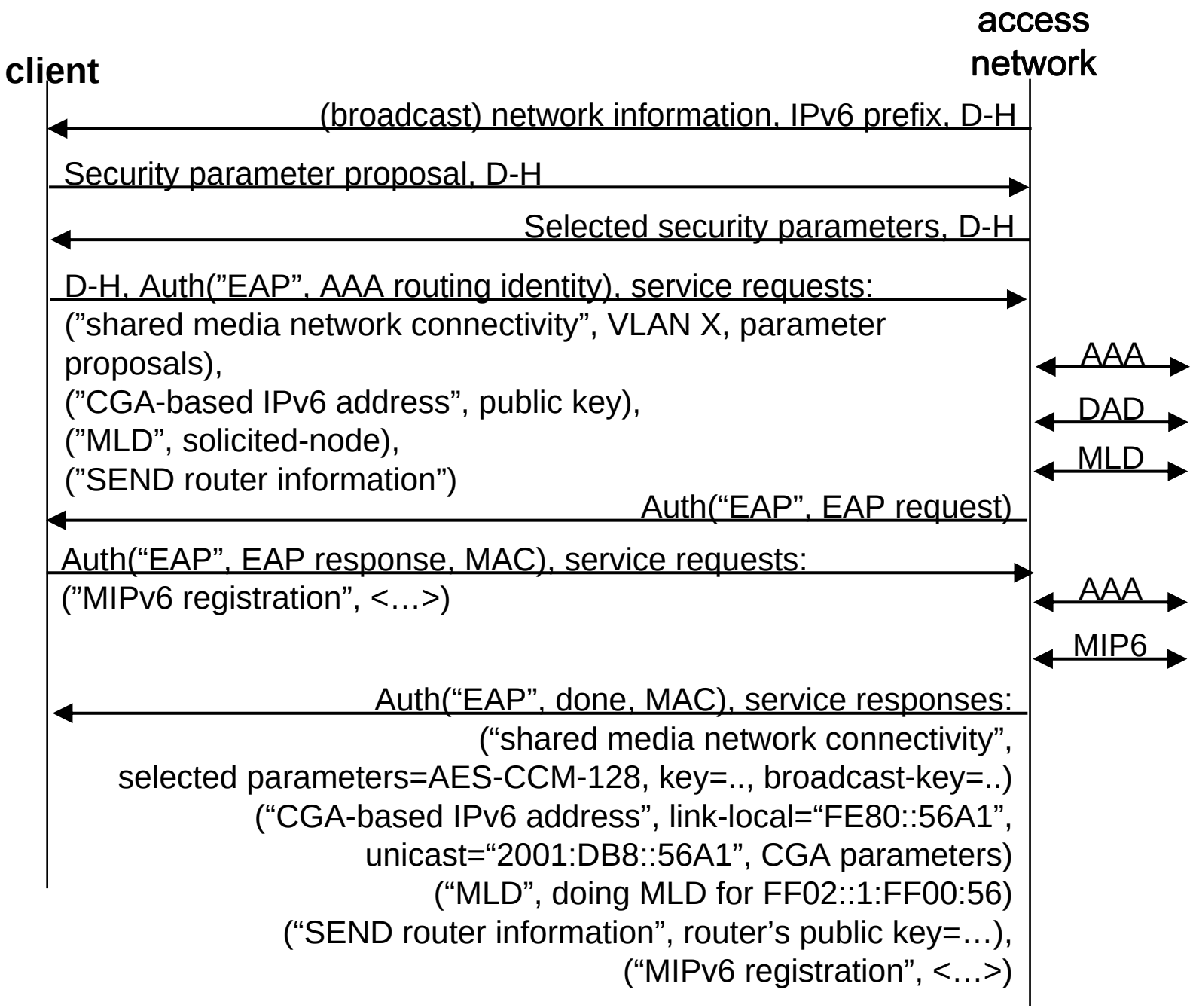
- Message order
  - Find out what information the whole problem involves, and how many messages need to carry it and re-think message order
  - Example: If the client's IP address was known earlier, the authentication process with the home network could handle mobility-related registrations as well
- Information transfer capabilities should not be restricted to the initial authentication exchange

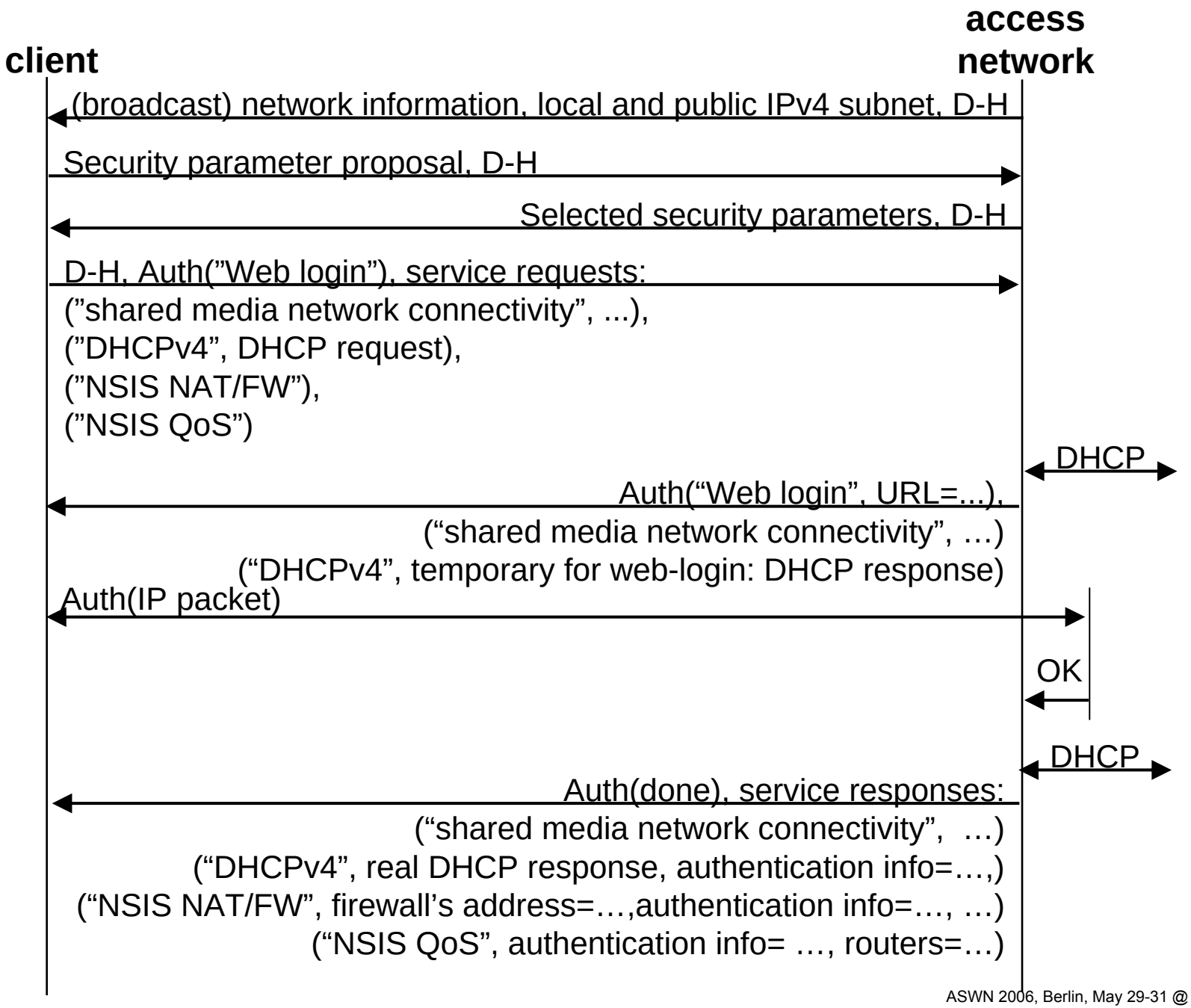
Potential Solution Ingredients (3/3)

Miscellaneous

- Delegation
  - Does the client have to be involved in tasks?
  - Can some tasks be delegated to the access point/router?
  - For instance, router based address assignment and DAD
  - Even a mobility related registration could be delegated

Tentative Protocol Design


client
access network
(broadcast) network information, IPv6 prefix, D-H
Security parameter proposal, D-H
Selected security parameters, D-H
D-H, Auth(”EAP”, AAA routing identity), service requests:
(”shared media network connectivity”, VLAN X, parameter proposals),
(”CGA-based IPv6 address”, public key),
(”MLD”, solicited-node),
(”SEND router information”)
AAA
DAD
MLD
Auth(“EAP”, EAP request)
Auth(“EAP”, EAP response, MAC), service requests:
(”MIPv6 registration”, <…>)
AAA
MIP6
Auth(“EAP”, done, MAC), service responses:
(“shared media network connectivity”,
selected parameters=AES-CCM-128, key=.., broadcast-key=..)
(“CGA-based IPv6 address”, link-local=“FE80::56A1”,
unicast=“2001:DB8::56A1”, CGA parameters)
(“MLD”, doing MLD for FF02::1:FF00:56)
(“SEND router information”, router’s public key=…),
(“MIPv6 registration”, <…>)


client
access network
(broadcast) network information, local and public IPv4 subnet, D-H
Security parameter proposal, D-H
Selected security parameters, D-H
D-H, Auth(”Web login”), service requests:
(”shared media network connectivity”, ...),
(”DHCPv4”, DHCP request),
(”NSIS NAT/FW”),
(”NSIS QoS”)
DHCP
Auth(“Web login”, URL=...),
(“shared media network connectivity”, …)
(“DHCPv4”, temporary for web-login: DHCP response)
Auth(IP packet)
OK
DHCP
Auth(done), service responses:
(“shared media network connectivity”, …)
(“DHCPv4”, real DHCP response, authentication info=…,)
(“NSIS NAT/FW”, firewall’s address=…,authentication info=…, …)
(“NSIS QoS”, authentication info= …, routers=…)

Evalution and Next Steps

Evaluation 1/2

- Significant reduction in number of messages
- No waiting periods
- Better privacy and DoS defense support
- Can be used to secure open models
- Can be used to secure other services (e.g. DHCP)
- Eliminates user intervention

Evaluation 2/2

- This may not be compatible with current protocols; likely possible only in new link layers
- Deployment needs new client - AP protocol set
  - But not AP - AAA set
  - And no new credentials
- Access devices become involved in layer 3 operations
  - But we note that this is optional
- Layer-purists might object to our views

Next Steps

- Prototyping this and variations in the Ambient Networks EU project
- Continuing with detailed protocol design
- Get measurements on benefits
- Get experience on implementation feasibility
- Feedback ideas to new link layer designs

Questions?