ERICSSON

Network Access Developments at the IETF

Jari.Arkko@nomadiclab.com

Ericsson Research NomadicLab

Goals & Outline

Goals

- Learn about the evolution of network access protocols
- Understand the limitations of the protocols

Outline

- Current market place & environment
- Basic protocol components
- Ongoing work
- Future challenges

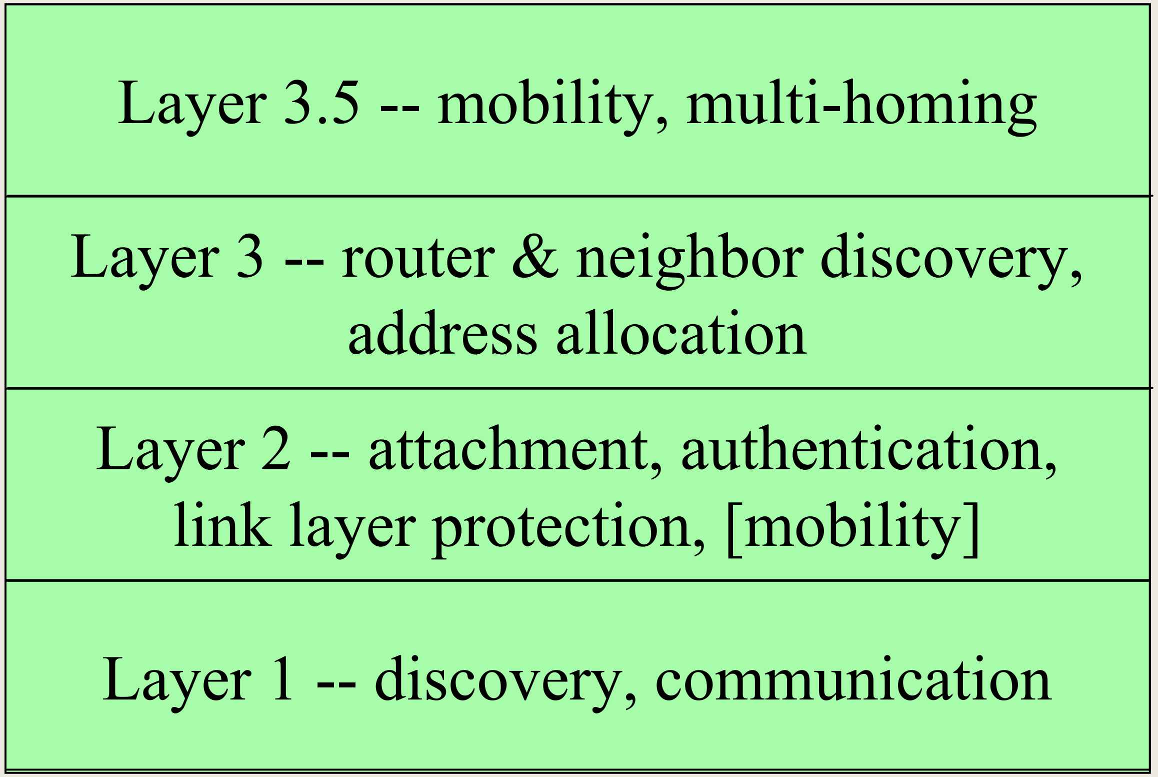
Current Market Place & Environment

Some Trends in the Environment...

- Dial-in => wireless (many kinds)
- One connection => moving around
- Low speed => high speed
- One provider, one technology => one subscription, many technologies
- PPP => Ethernet, cellular encapsulations
- Same service & configuration => differentiated
- Relatively secure media => open wireless
- Plaintext passwords are a good idea => more clue today
- Use weakest possible ciphers => more clue today

Basic Protocol Components

The Network Access Stack



Layer 3.5 -- mobility, multi-homing

Layer 3 -- router & neighbor discovery, address allocation

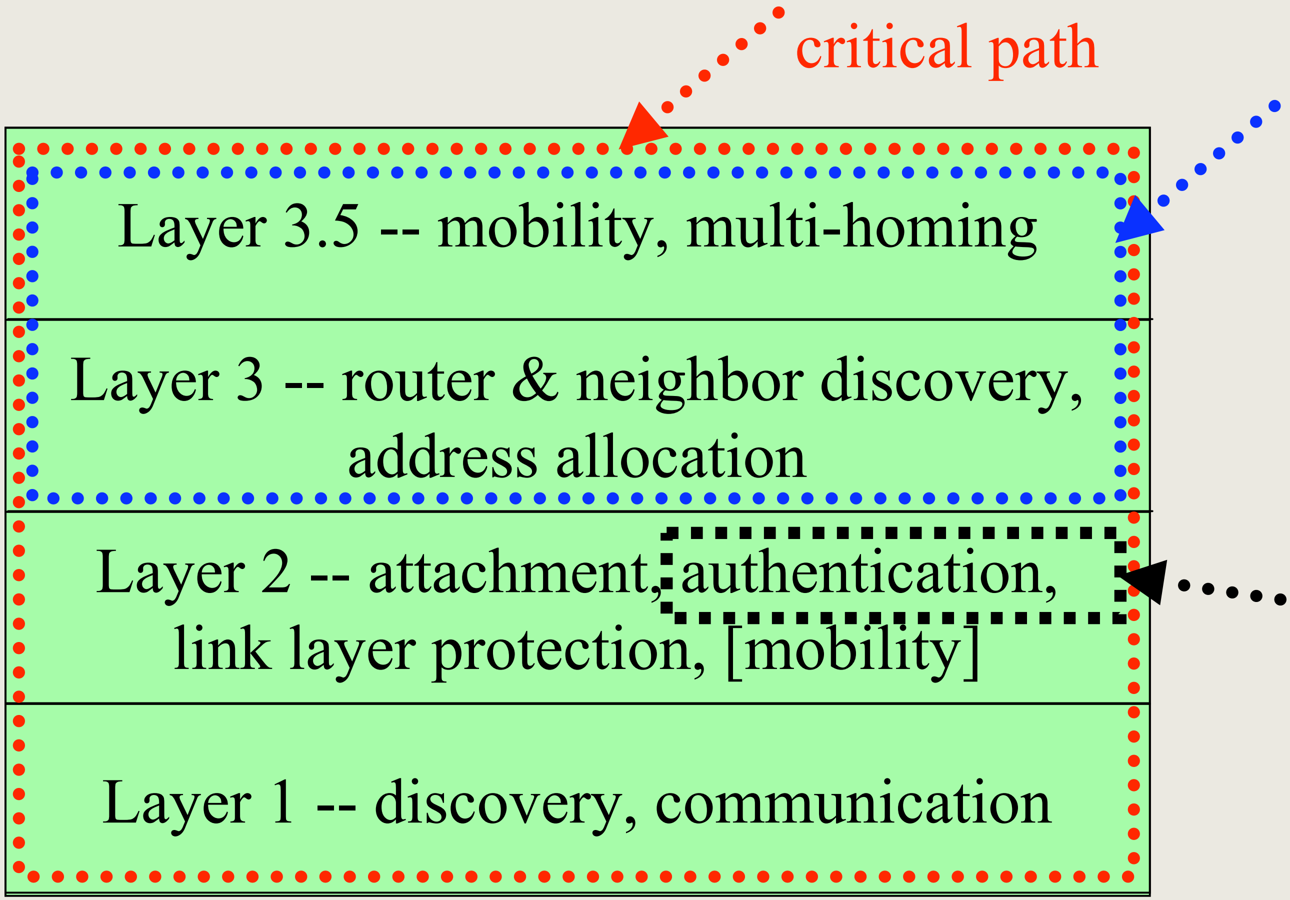
Layer 2 -- attachment, authentication, link layer protection, [mobility]

Layer 1 -- discovery, communication

Some Interesting Discussion Items...

- Efficiency
  - Overhead
  - Latency
  - ...
- Network architecture
  - What happens on the link vs. in the network
- Protocols

Initial & Movement Latencies



Layer 3.5 -- mobility, multi-homing

Layer 3 -- router & neighbor discovery, address allocation

Layer 2 -- attachment, authentication, link layer protection, [mobility]

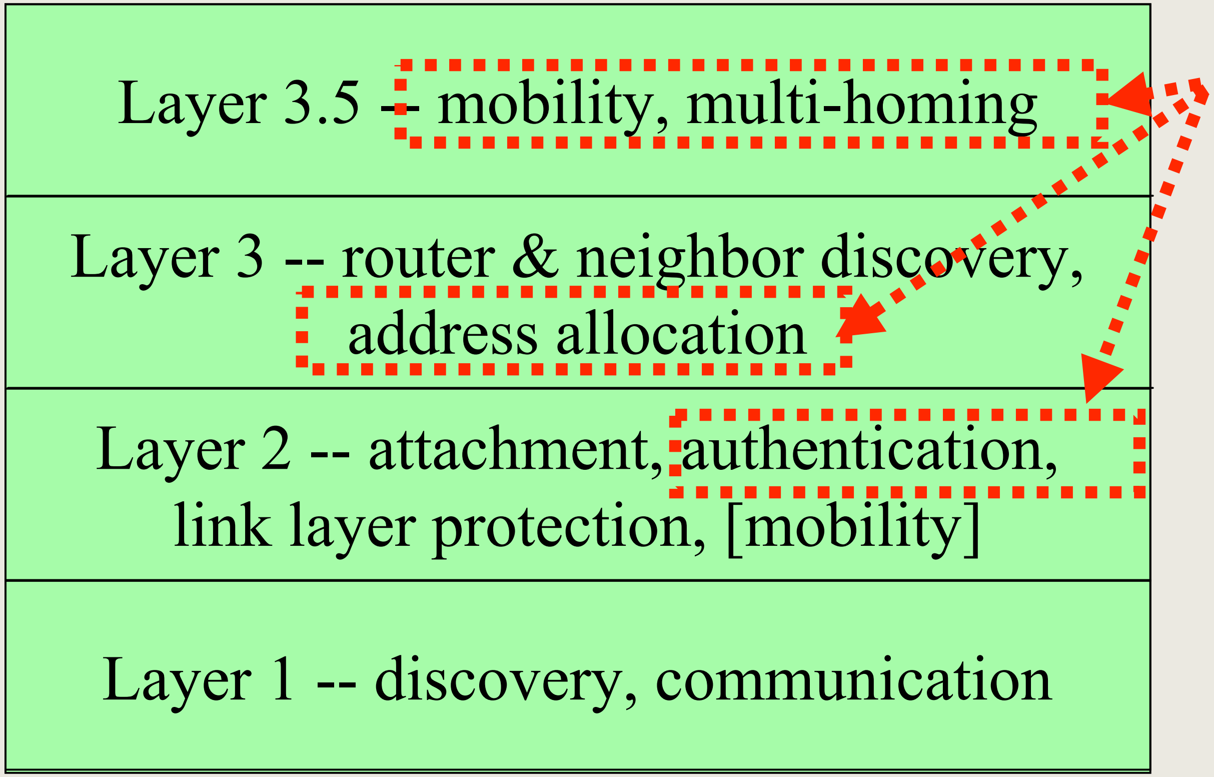
Layer 1 -- discovery, communication

All of this is on the critical path

Not on c.p. unless there is subnet change - but how do you know?

Might be reused

Local and End-to-End Communications



Layer 3.5 -- mobility, multi-homing

Layer 3 -- router & neighbor discovery, address allocation

Layer 2 -- attachment, authentication, link layer protection, [mobility]

Layer 1 -- discovery, communication

May involve nodes beyond the access network device(s)

Layer 1 and 2 Protocols

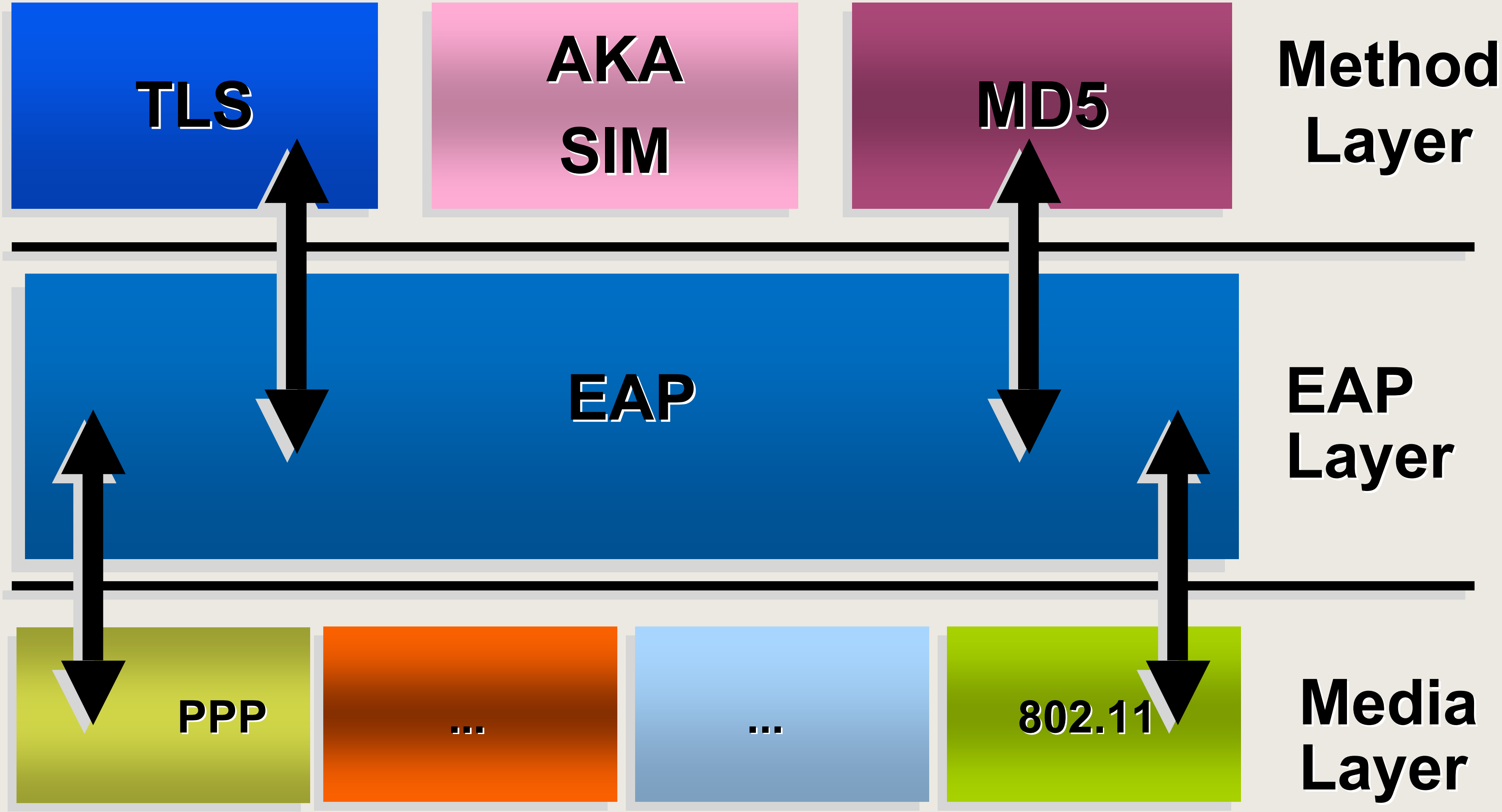
- GPRS
- UMTS
- Wireless LANs

- Generic L2 components
  - 802.1X, PANA
  - Extensible Authentication Protocol, EAP
  - AAA

What is EAP?

- The Extensible Authentication Protocol
- Originally defined in RFC 2284, now in RFC 3748
  - Provides a flexible link layer security framework
  - Simple encapsulation protocol
    - No dependency on IP
    - ACK/NAK, no windowing
    - No fragmentation support
  - Few link layer assumptions

EAP Architecture



EAP, Continued

Protocols Using EAP

- PPP
- 802.1X and 802.11i
- PANA (= IP-based 802.1X/11i)

Issues in EAP

- Only a few standard authentication methods -- many vendor specific ones
- Has Denial-of-Service & data transport efficiency issues

AAA Protocols

- RADIUS, Remote Access Dial In User Service
- Diameter ~ RADIUS v2
- Support authentication, authorization, and accounting for network access
- Allows centralized administration and accounting
- Issues
  - Many of the recent RADIUS extensions are not standardized
  - RADIUS transport (UDP) is being stretched
  - Diameter is not widely used, except in 3G networks

Layer 3 Protocols

- IPv6 control mechanisms
  - Router discovery
  - Neighbor discovery
  - DHCP or address autoconfiguration
  - Duplicate address detection
- IPv4 control mechanisms
  - Similar as in IPv6 (but a bit simpler)
- Issues
  - Not optimized for wireless usage

Layer 3.5 Protocols

- IP layer mobility mechanisms
  - Mobile IP
  - HIP
  - MOBIKE
- Tunneling
- Layer 3.5 vs. layer 2 vs. application layer mobility

Ongoing Work

Ongoing Work

- EAP -- Cleaning up…
- AAA -- Diameter for network access
- RADEXT -- Accommodating new link layers
- DNA, IPV6, DHC -- Optimizations
- Other -- Mobility, secure ND, enrollment, ...

Ongoing Work

- EAP -- Cleaning up…
- AAA -- Diameter for network access
- RADEXT -- Accommodating new link layers
- ENROLL -- How does one get the keys to access?
- DNA, IPV6, DHC -- Optimizations
- PANA -- Alternative to 802.1X
- SEND -- Security
- MIP*, HIP, … -- Mobility

EAP

- Cleanup: Going from RFC 2284 (15 pages) to RFC 3748 (67 pages) + state machine (30 pages)
  - You have got to wonder how it worked before…
- Some EAP methods work
- System-level security analysis -- the EAP (Bermuda?) triangle:

```
                       EAP peer
                          /\
                         /  \
 Protocol: EAP          /    \    Protocol: Secure Association
 Auth: Mutual          /      \   Auth: Mutual
Unique keys: MK,      /        \  Unique keys: TSKs
  TEKs,EMSK          /          \
                    /            \
  Auth. server +--------------+ Authenticator
                    Protocol: AAA
                    Auth: Mutual
              Unique key: AAA session key
```

AAA, RADEXT

- Revised version of EAP over RADIUS & defining EAP over Diameter
- New functionality related to network access
  - Control of specific link layer parameters, e.g., WLAN
  - Accommodating new requirements, e.g., controlling filtering and redirection
  - Prepaid
- Revised version of Network Access Identifiers (NAIs)
  - Privacy, international user names, ...

ENROLL

- How do you establish a shared secret between you and your network provider?
- One of the deployment barriers
- Maybe different sets of requirements for
  - Corporate network
  - Operator network
  - Home

DNA, IPV6, DHC

- Some IP layer tasks are on the critical path in movements
  - Attachment delays are at least 16 messages in IPv6 for full functionality
  - Many request-response pairs, mandatory delay periods
  - Security at many layers
  - A large part of the signaling goes to the home network
- Work ongoing in multiple places to address the bottlenecks:
  - IPv6 & DAD: potential to eliminate 1 second delay period
  - DNA: how to detect reliably & fast that you have or have not moved IP-subnet wise?
  - DHC: same as in DNA, but for IPv4

Future Challenges -

Functionality, Efficiency, and Security

Functionality, Efficiency

- L2 specific designs do not extend to heterogeneous networks
- Duplication and conflicting work in different link layers
  - E.g. fast handoffs do not work across link types
- Attachment delays
  - Will individual optimizations be sufficient?
- Optimized handoffs needed
- Bottlenecks in information transfer
  - Information transfer, discovery
  - Link layers are incapable of efficient & secure broadcast
  - EAP not suitable for large scale information transfer

Security

- Completely open network model insufficient for wireless
- AAA, EAP, WLAN, PANA security model provides only “one of the trusted nodes” assurances, not individual node authentication
- Denial-of-service issues
  - Separation of attachment procedures and security leads to significant Denial-of-Service issues in Wireless LANs

Conclusions

Conclusions

- We have come a long way since PAP & PPP
- Security is still not perfect (denial-of-service etc)
- Efficiency issues starting to dominate discussion
- Seems like many legacy protocols are carried on from past networks (EAP, RADIUS, .1X, …) to new ones