<draft-ietf-pana-usage-scenarios-01.txt>

Basavaraj Patil
Yoshihiro Ohba
Subir Das
Hesham Soliman

Draft objectives

- Problem Statement:
  - Highlight what's missing in today in network authentication, in users' devices and network elements.
    - Not all L2s have built-in authentication mechanisms
    - Not all L2 authentication schemes have re-authentication
    - One L2 authentication scheme is not re-usable across different L2s, especially when the identities are attached to a particular L2
    - IP address configuration and version independence
- Usage scenarios:
  - Highlight where the above problems may arise by showing use cases and how an upper layer authentication protocol would help in these scenarios

Problem1: Need for authentication over unauthenticated L2 links

- Not all L2 links implement L2 authentication mechanism
  - Authentication is an optional feature for most L2 protocols (e.g., IEEE 802)
  - Higher layer authentication is clearly needed for the network that does not implement L2 authentication

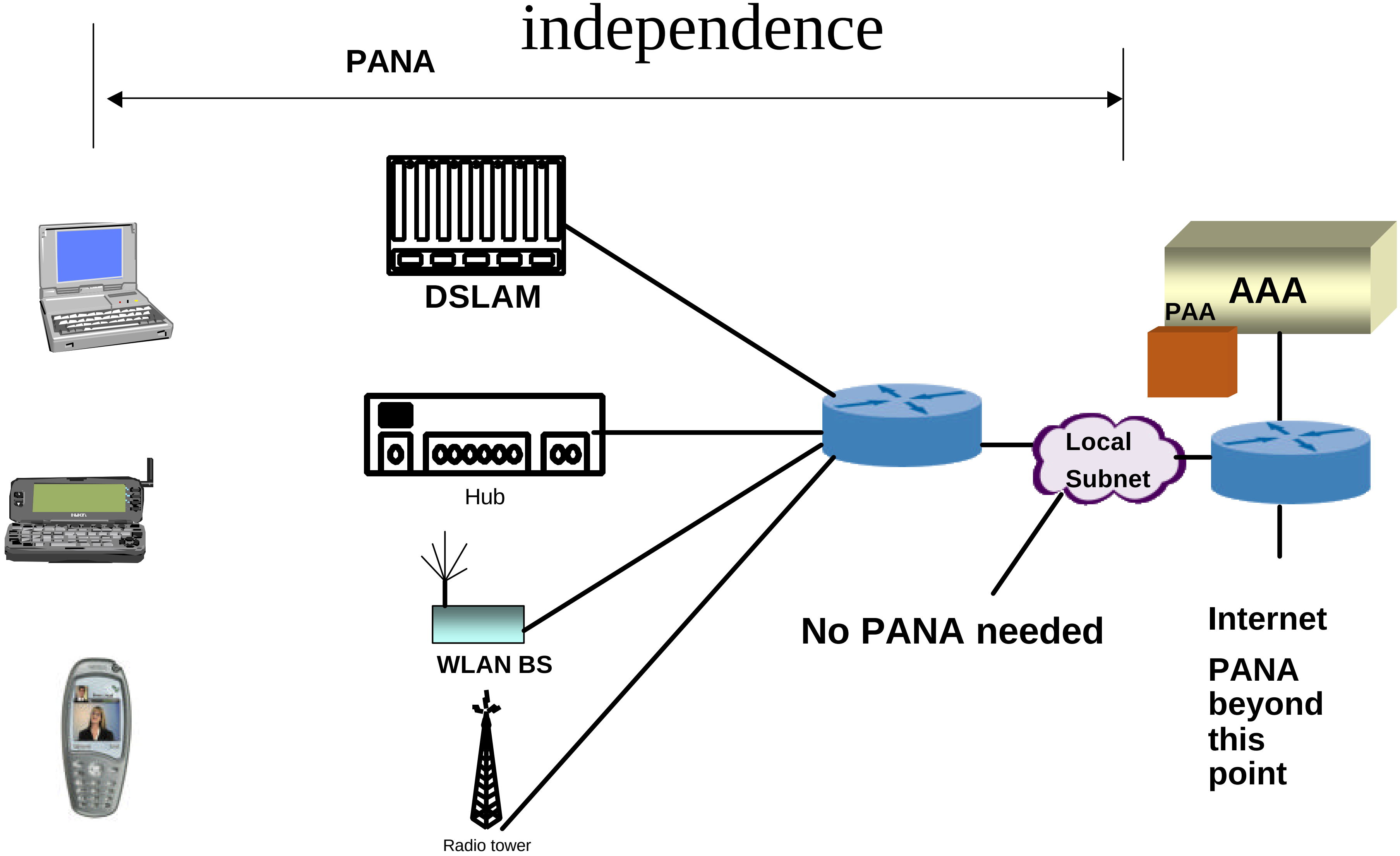
Problem2: Need for local re-authentication

- Re-authentication is required at least when:
  - Authorisation lifetime needs to be extended (could be done locally only, or using backend AAA as well)
  - Authorisation parameters (such as MAC address and IP address) needs to be changed
  - Detect connectivity/reachability
- Local re-authentication between client and PAA is desired

Problem3: IP address configuration independence

- “IP address configuration” means
  - configuration of an IP address (beyond link-local scope) that needs to be authorised for network access
- Timing independence
  - Authentication/Authorisation must be able to occur both before and after IP address configuration
- IP version independence
  - The authentication/authorisation should not be tied to an IP address type/configuration method/IP version.

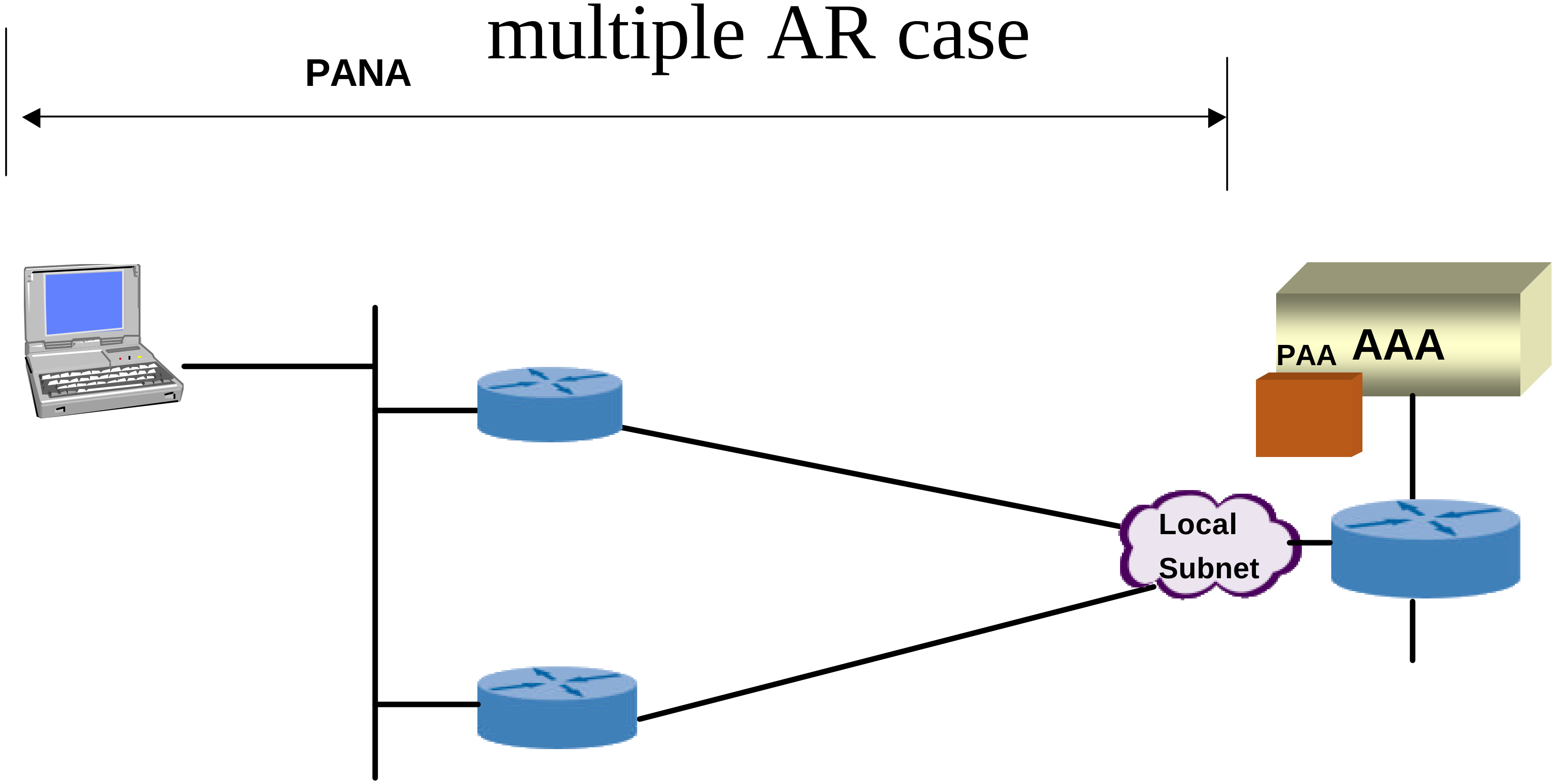
Scenario: IP address configuration independence



Problem4: Multiple ARs, e.g., for multi-access networks

- In most deployment scenarios NASs are in first hop only today
- This would cause a problem if multiple ARs are used and traffic diverges (outbound AND inbound)

Scenario: How PANA can help with the multiple AR case

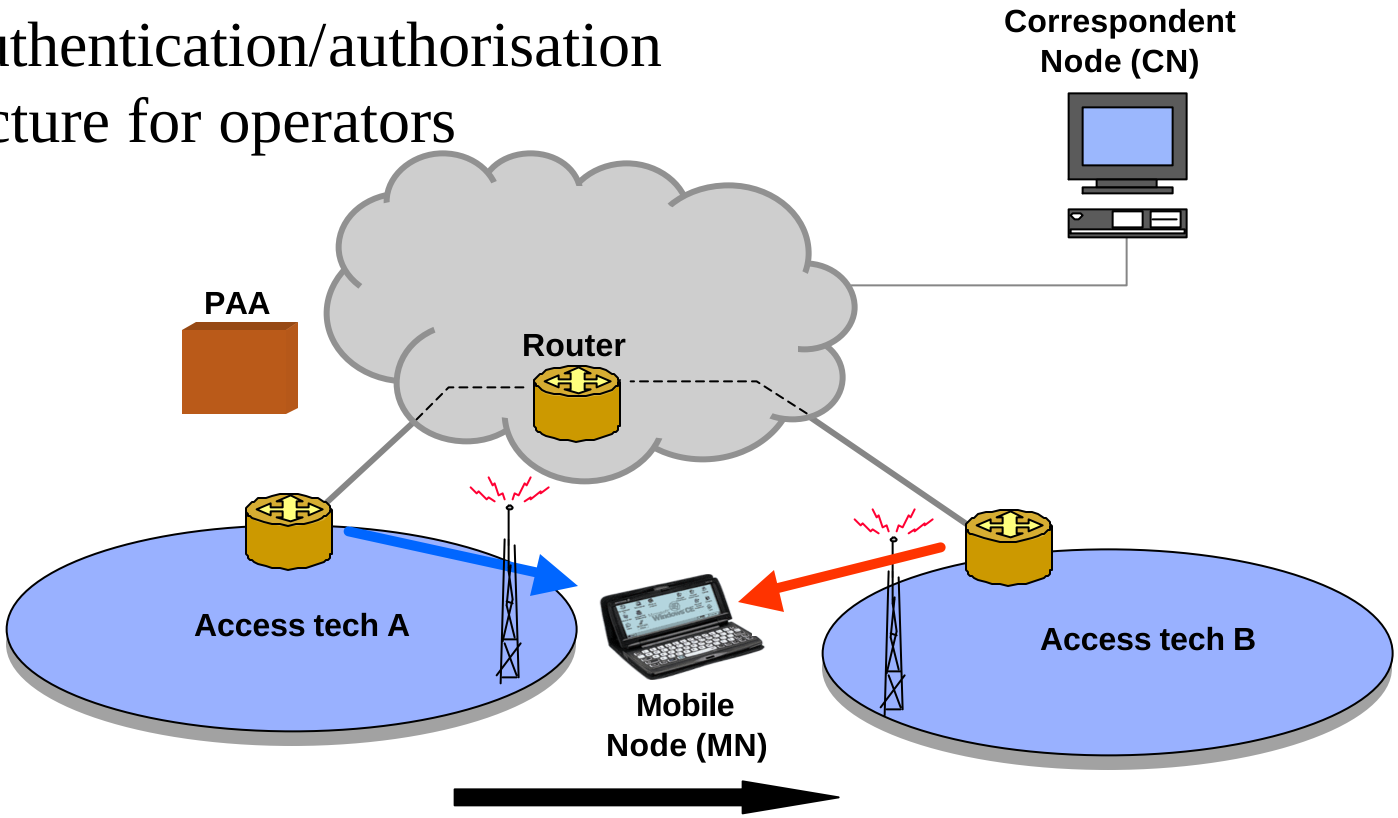


Problem5: Handover between different access technologies within one admin domain

- L2-specific authentication/authorisation mechanisms are not applicable when performing an IP layer handover between 2 interfaces
- Context transfer does not help if the identities used are L2-specific
- Unnecessary Re-authentication to the new network is required
- Multiple AAA infrastructures, or translator between one AAA system and the other would be needed.

Scenario: Handover between different access technologies for multi-homed hosts

- Single authentication/authorisation infrastructure for operators



Conclusions

- To be able to solve the problems presented, in an architecturally clean way, we need:
  - Access independent authentication/authorisation schemes
  - Access independent identities to be used
  - IP version independence (important for dual stack hosts)
  - Flexibility in placement of NAS
  - Flexible service models

Open issues

- The draft contains requirements language
- Need to elaborate more on the scenarios