Problem Statement
And Usage Scenarios for PANA

Andreas Blinzler

Agenda

- Introduction
- Problem Statement
  - What is PANA?
  - Network Access Provider / Internet Service Provider
  - Extensible Authentication Protocol
  - Client authentication with PANA
  - Ad-hoc mechanisms
- Usage Scenarios
  - PANA with physical layer security
  - PANA with link-layer security
  - PANA in the absence of any lower-layer security
  - Mobile IP
  - Personal area networks
  - Limited free access

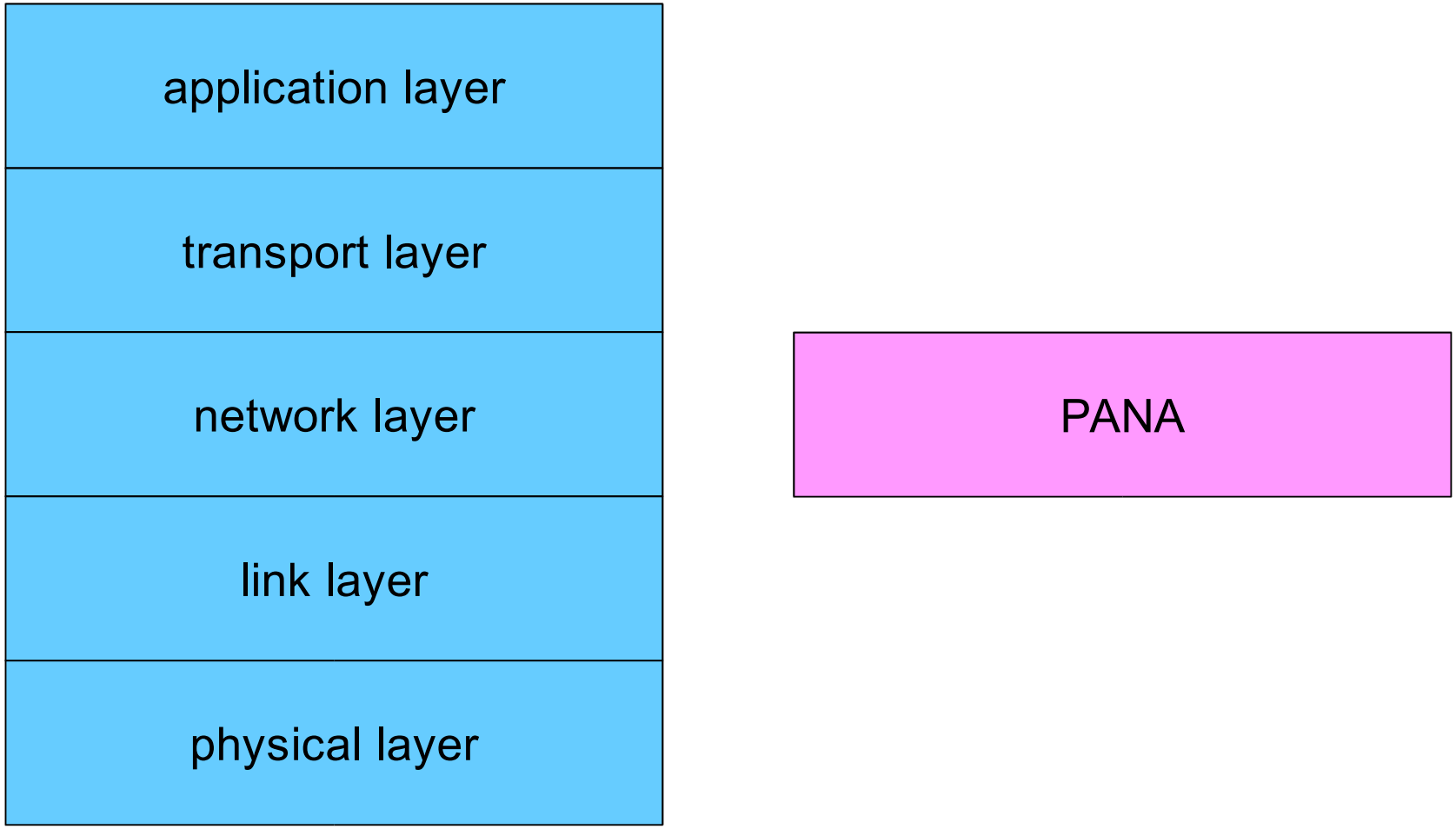
Introduction

Introduction

- Source: draft-ietf-pana-usage-scenarios-06.txt
- PANA = Protocol for carrying Authentication for Network Access
- Network access authentication
  - Physical security
  - Link-layer security
  - Network- or higher-layer security
- Status quo
  - No Standard protocol to perform network access authentication above the link-layer
  - Instead some ad-hoc solutions are being used
  - PANA will be developed to fill this gap

Introduction

- Internet Layer



Problem Statement

Problem Statement

- A protocol for authentication and authorization
- This protocol must execute one or more authentication methods (e.g. PAP, CHAP, TLS, SIM, etc.)
- The authentication methods need not to be tied to the underlying link-layer (e.g. GPRS, IEEE 802.11, DSL, etc.)
- The authentication protocol must be able to support various authentication methods

Problem Statement

- Seperation
  - NAP provides physical and link-layer connectivity for an access network
  - ISP provides internet connectivity for the NAP
- Important aspect of network access
  - Ability to enable dynamic ISP selection during the initial connection process
  - Example: Network Access Identifier [RFC2486]

Problem Statement

- Single authentication
  - Generally sufficient for both NAP and ISP access by relying on the pre-established trust relation between the NAP and the ISP
- Multi-layer authentication
  - NAP authentication is realized with a link-layer mechanism
  - ISP authentication can be left to network layer mechanisms
  - Example:
    - Cdma2000 networks
    - GSM

Problem Statement

- EAP = Extensible Authentication Protocol [RFC2284]
- Only IEEE 802 can carry EAP on the link-layer (IEEE 802.1X)
- Other link-layers resort to using PPP/PPPoE [RFC1661, RFC2516], with consequences
  - Additional round trips
  - Overhead of PPP processing
  - “Point-to-point network model”
- Greater applicability if EAP could be carried directly over IP

Problem Statement

- „Authenticate a client to a server for network access“
- Client authentication needs to be bound to subsequent traffic to prevent spoofing of data packets
- Realization
  - Secure physical or link-layer channel
  - Cryptographic keying material
- Keying material can be used with link-layer ciphers or IPSec

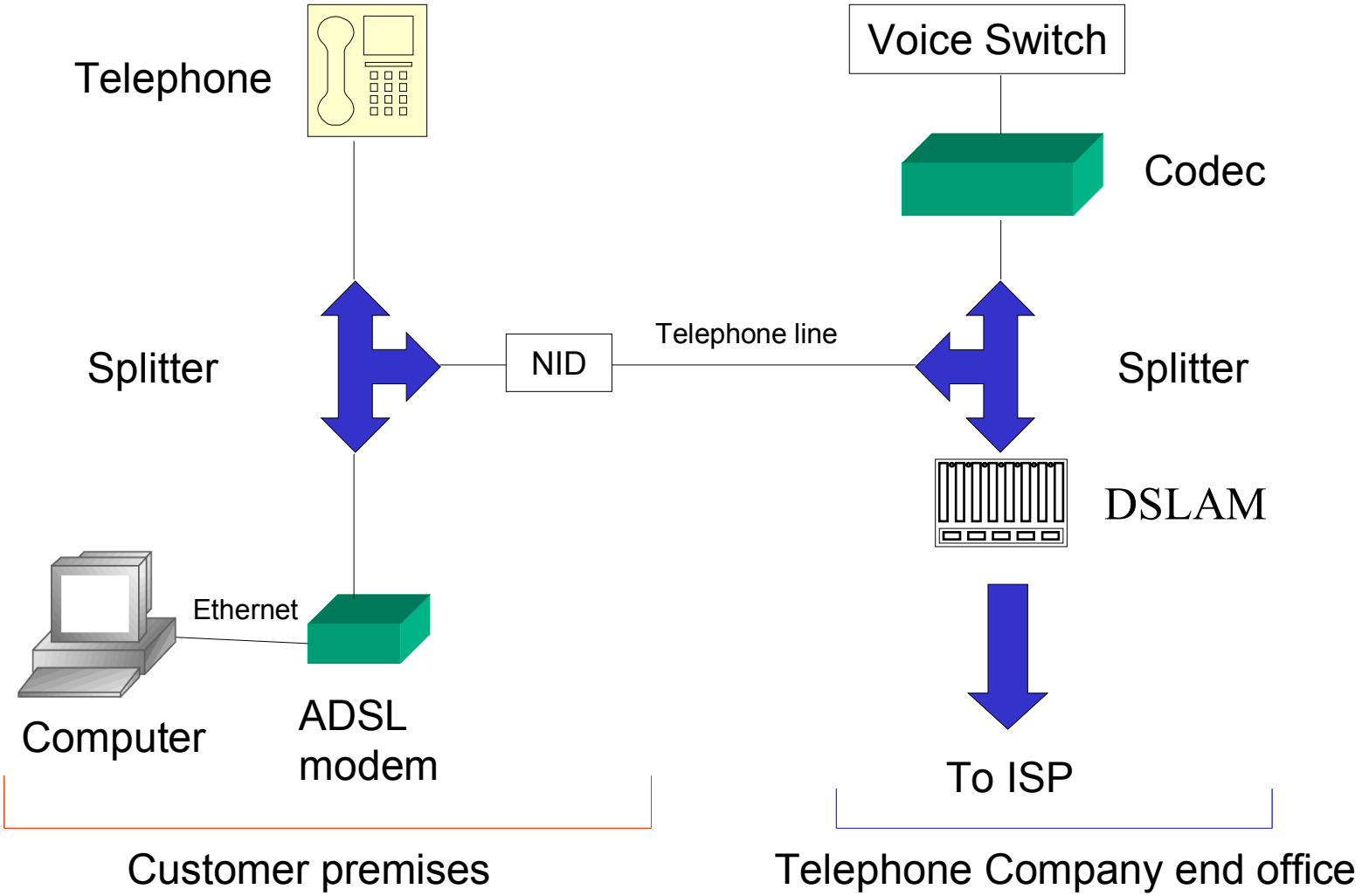
Problem Statement

- Application-layer authentication method
  - HTTP redirect and web-based login
- Overload of an existing network layer protocol
  - Example: Mobile IPv4 [RFC3344]

Usage Scenarios

Usage Scenarios

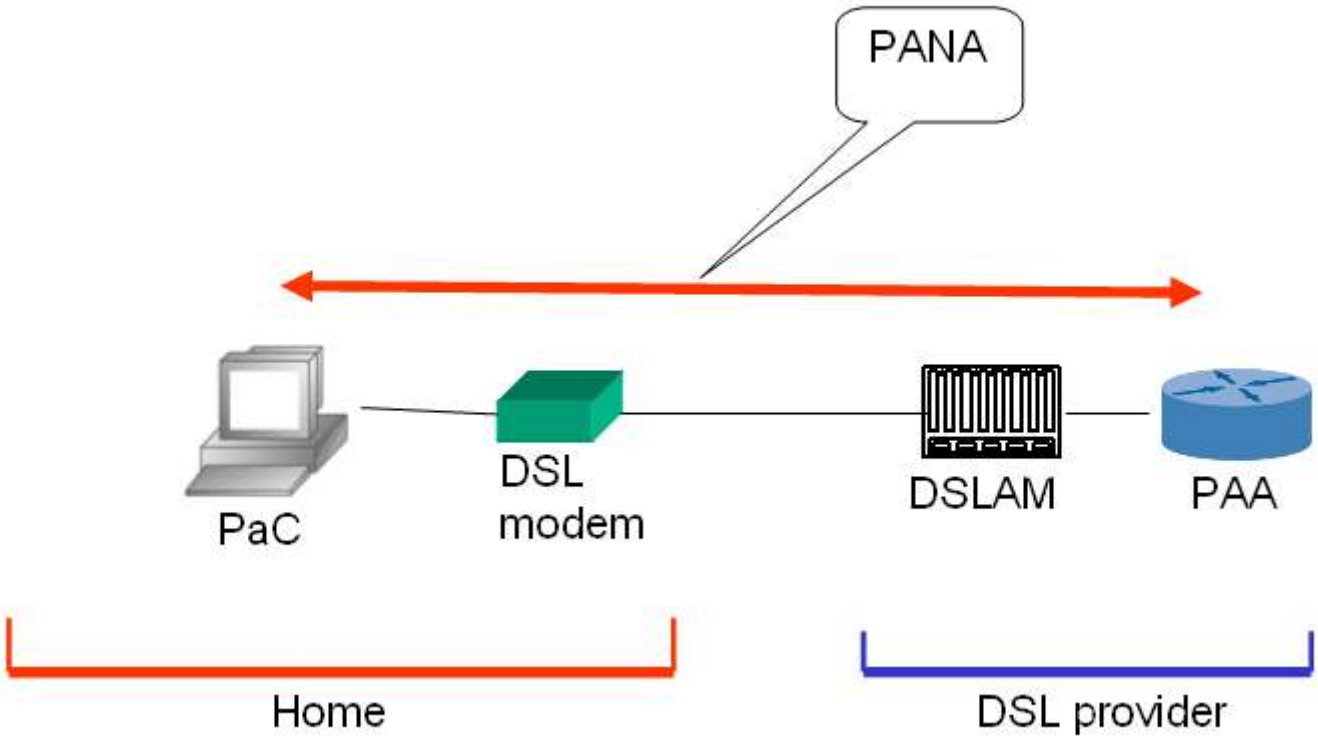
- Example: DSL network



Usage Scenarios

- Single network access authentication solution would be an improvement for DSL
- PANA with point-to-point lines (DSL)
  - PANA can be used for client authentication
  - PANA build the basis for an appropriate access control mechanism

Usage Scenarios

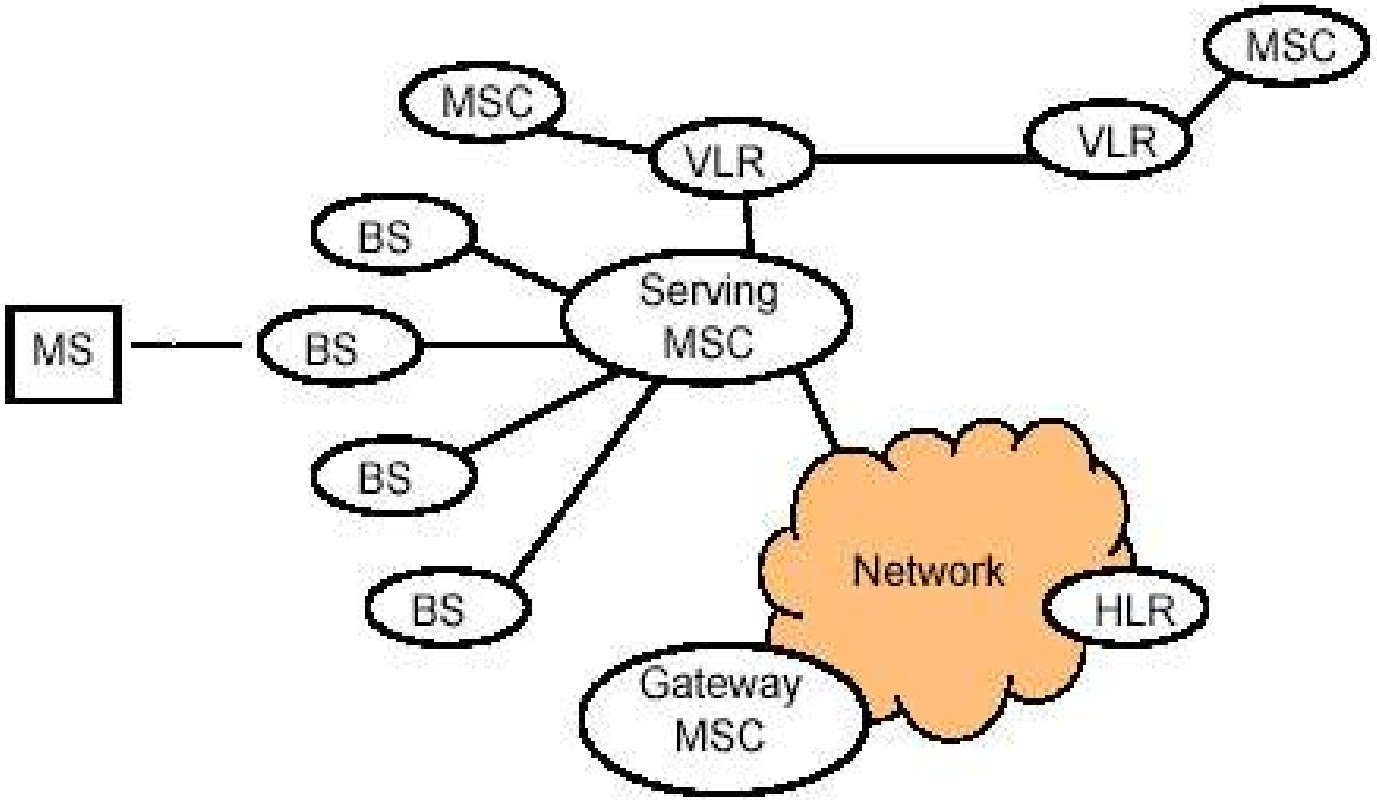


Usage Scenarios

- Certain cellular link-layers provide their own authentication mechanisms
- Technology specific authentication enables authorization for link access by the NAP
- Multi-layered authentication for network access
  - Accessing the Internet via an ISP another layer of authentication is needed

Usage Scenarios

- Example: Cellular Telecommunication

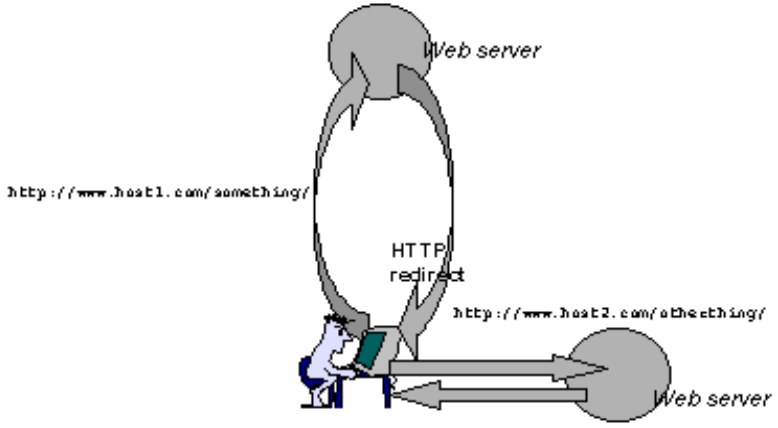


Usage Scenarios

- Example: Cdma2000
  - Authentication with the MSC / VLR is required
  - Has its own authentication mechanism (uses CAVE)
  - Modes of operation
    - Simple IP (CHAP via PPP)
    - Mobile IP (C/R protocol)
  - PANA could be used as a single unifying network layer authentication mechanism

Usage Scenarios

- Scenarios where neither physical nor link-layer access control is available
  - Due to the lack of adequate client authentication
  - Due to the difficulty of deployment
- Many providers use today a higher-layer security
  - HTTP-redirect, commonly known as web-based login

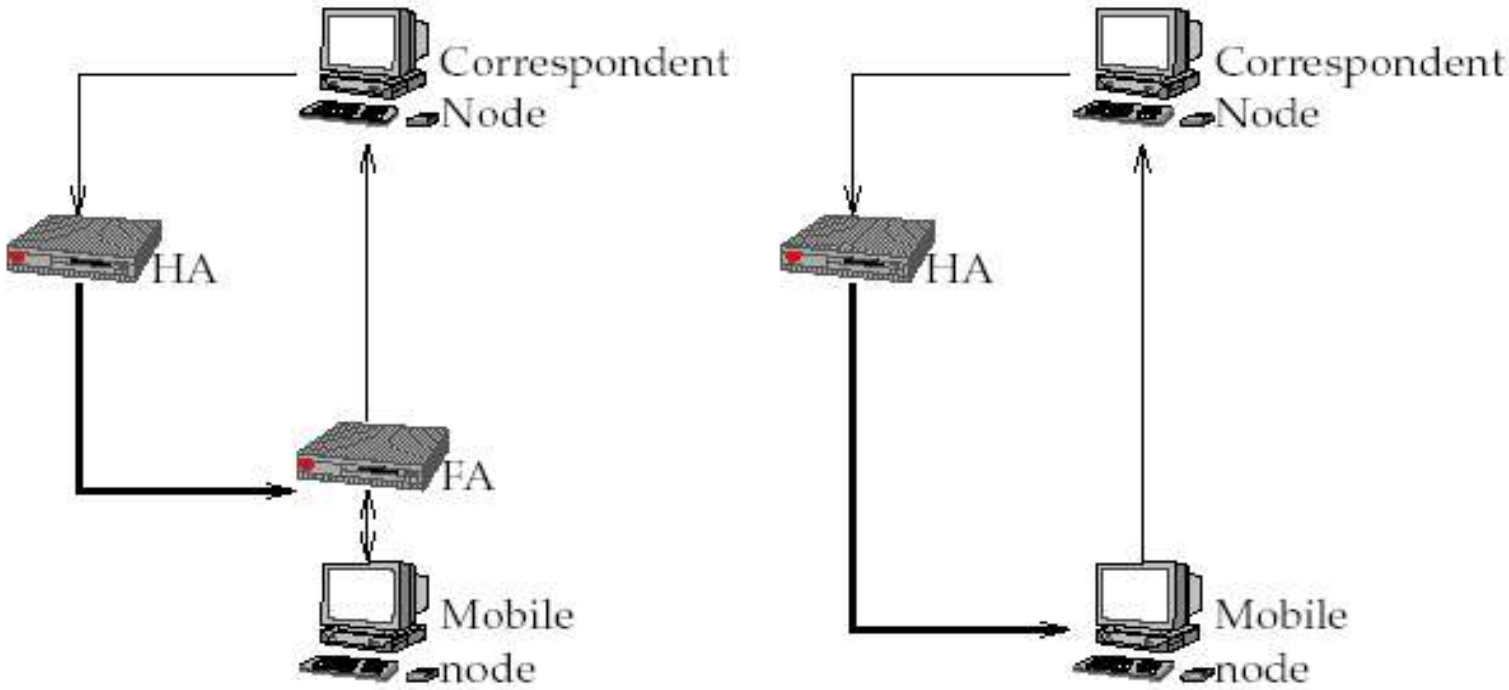


Usage Scenarios

- Standard solution is need: PANA
- Specified authentication methods must be able to derive and distribute keys for
  - Authentication
  - Integrity
  - Confidentiality
- Successful PANA authentication can result in a secured network environment
- Providers will have the advantage using a single framework across multiple environments

Usage Scenarios

- Mobile nodes authenticate at the foreign and home agents
- Mode of operation
  - Co-located care-of-address-mode



Usage Scenarios

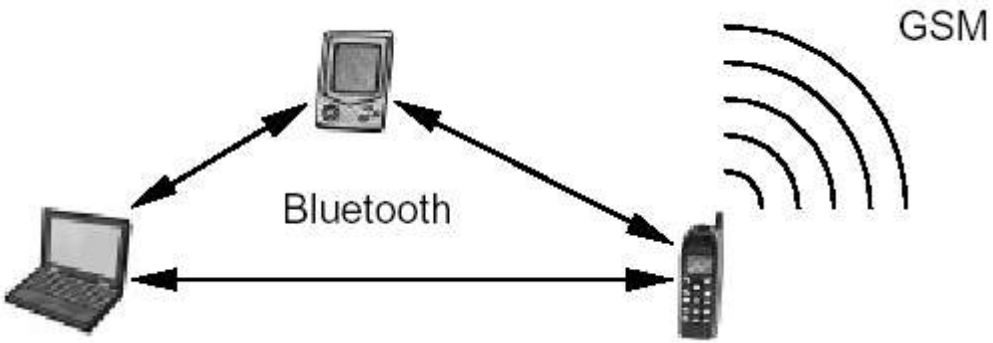
- Access networks requirement
  - Authenticate mobile nodes before allowing access
  - Mobile Nodes are forced to send their registration requests via the foreign agent

Usage Scenarios

- PANA with Mobile IP:
  - Can be used with any client
  - Can support various authentication methods
  - Can be used with IPv6 clients or dual-stack client

Usage Scenarios

- PAN = Personal Area Network
- Definition
  - *A PAN is the interconnection of devices within the range of an individual person.*
- Functionality



Usage Scenarios

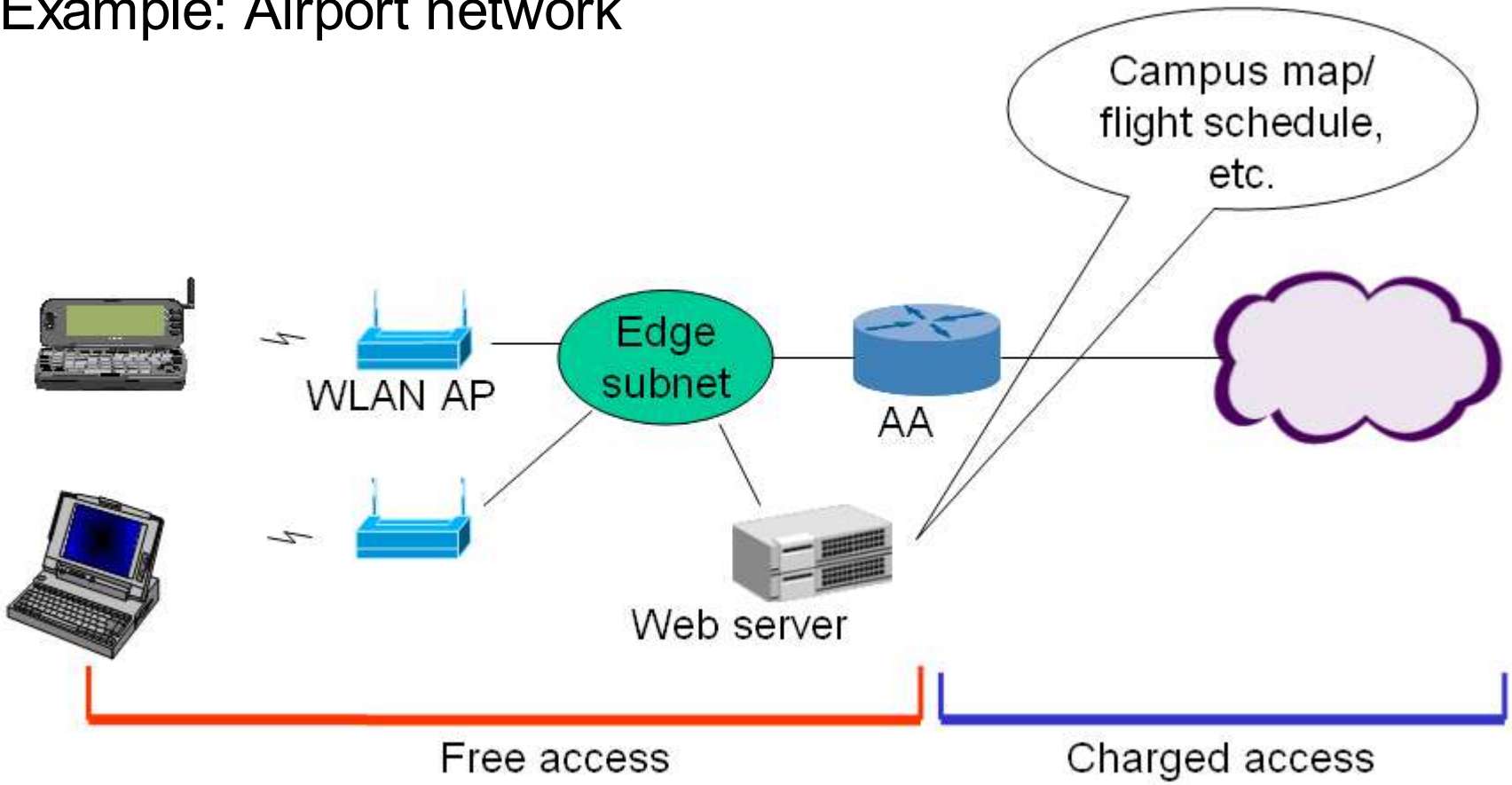
- PANA with PAN
  - Authentication is independent on the underlying link-layer (different nodes might be using different link-layers)
  - PAN have a small scale
    - No need to support roaming
    - Authentication process does not necessarily require a managed backend AAA infrastructure for verification

Usage Scenarios

- Example: 3GPP architecture [RFC3314]
  - Separation: MT and TE
  - TE can connect to the internet via MT using PPP
  - One or more TEs can be connected to a MT to form a PAN
  - Status quo of the architecture
    - No direct connection between the TEs
    - Connected through the cellular interface of the MT
  - Solution
    - Using shared links (ethernet) between TE and MT
    - Using PANA for authenticating PAN nodes when using shared links

Usage Scenarios

- Example: Airport network

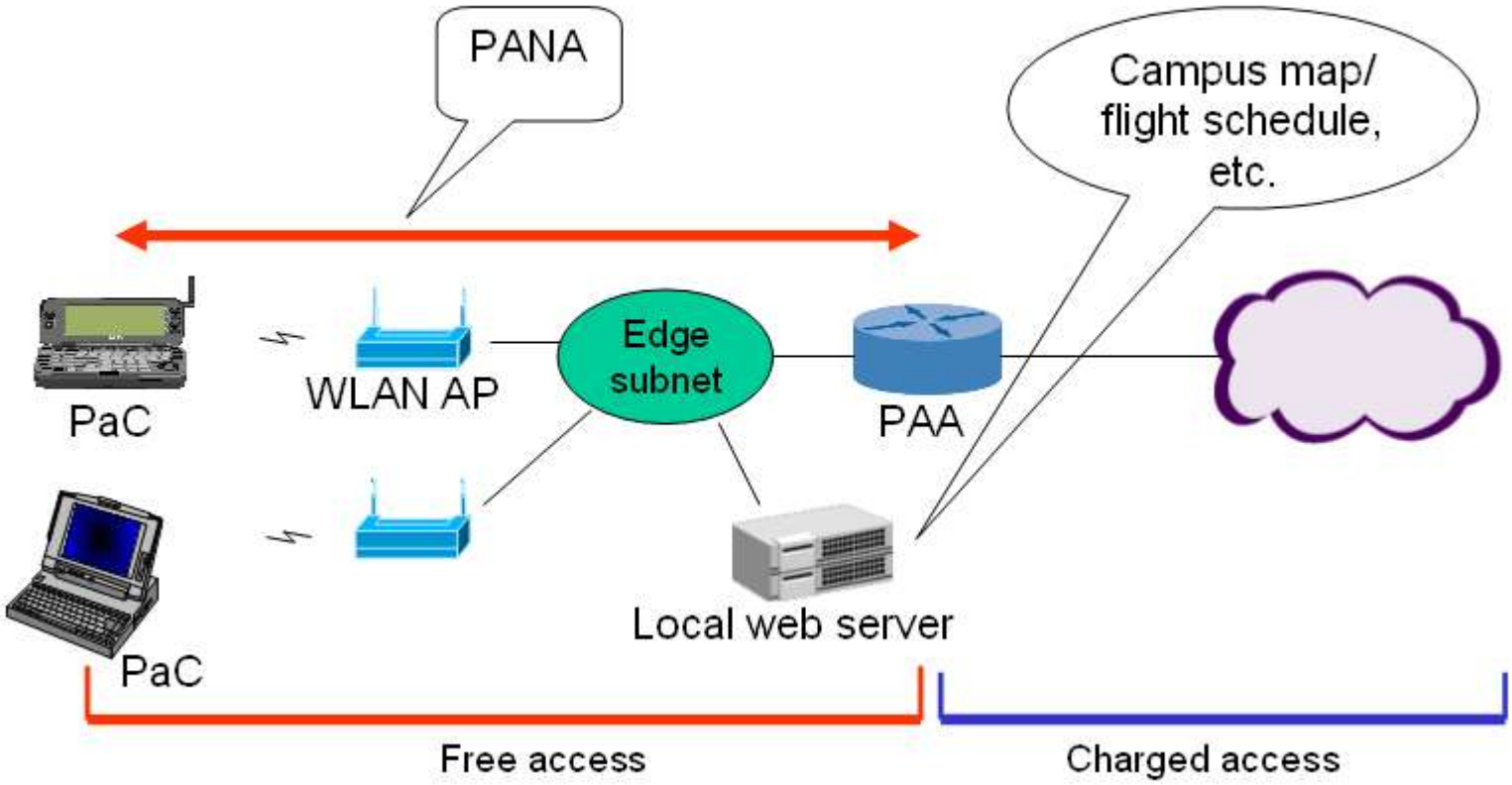


Limited free access

Usage Scenarios

- Network will only offer link-layer connectivity and limited network layer access to users
- Users have to perform a authentication to be allowed to go beyond the free access zone
- PANA can be an enabler to such limited free access scenarios

Usage Scenarios



Limited free access

Conclusion

Conclusion

- Need for network access authentication at higher layer when L2 does not have an authentication mechanism
  - Not all L2 technologies support carrying EAP
  - Assuming every L2 to carry EAP is not realistic
  - Using PPP authentication for shared media is inefficient
- Need for higher layer authentication on top of L2 authentication
  - Multi-layer authentication is widely used and common higher layer authentication carrier protocol needs to be standardized
  - Web-based authentication that is widely used in hot-spot network access is known to be proprietary hack

Thank you