Protocol for Carrying Authentication for Network Access (PANA) Requirements

Presentation for the Computer Science Elective

Internet Security

Lecturer: Prof. Dr. Trommler

University of Applied Sciences
GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

Agenda

- **Introduction to PANA and its requirements**
  - Nowadays situation
  - Motivation for a new protocol
  - The goal and solutions of PANA working group
  - What is NOT in the scope of PANA
- **Terminology and how PANA works**
  - Terminology and short cuts
  - The PANA usage model

- **Requirements of PANA**
  - Authentication
  - IP address assignment
  - PAA-to-EP Protocol
  - Network
  - Interaction with Other Protocols
  - Congestion Control and Performance
- **Conclusion**

Introduction to PANA and its requirements

- **Nowadays situation**

  - Modern devices – multi way network connectivity
  - Authentication methods for each kind of access
  - Restricted to certain access media
  - Restricted to specific network topologies
  - Inadequate technology with lack of security

• Motivation for a new protocol

- IP devices have to be authorized for network access
- Non-standard ad-hoc solutions are in use
- Clean solution: Network-layer protocol for authentication
- Meet expected authentication and security requirements
- Carrier for the authentication parameters between the client and the access network

Introduction to PANA and its requirements

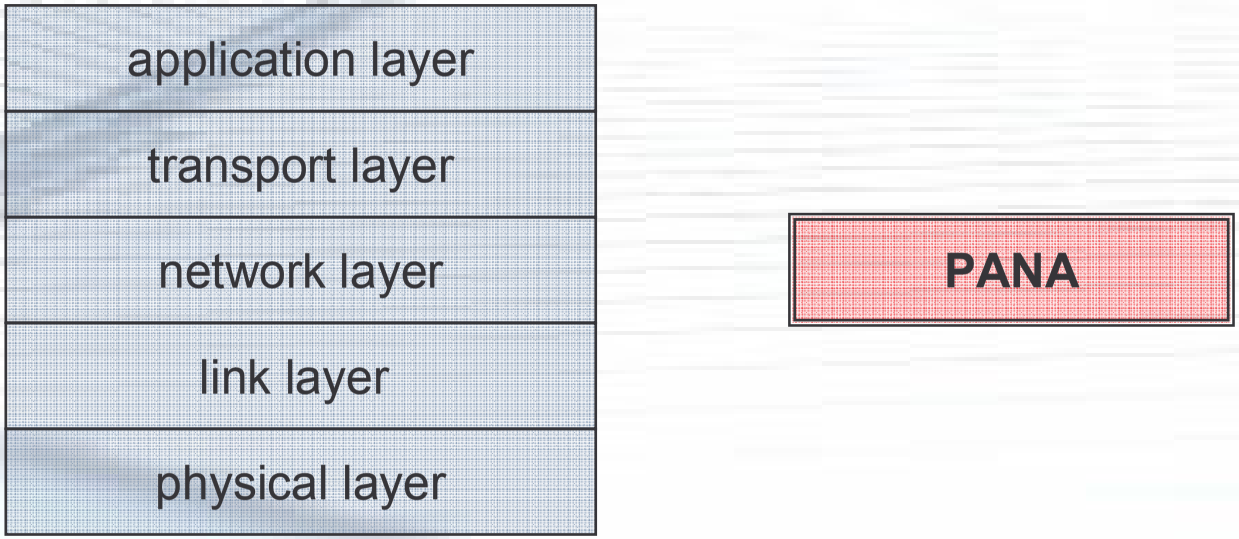
• Goal and solutions of PANA working group

- Defining a carrier for a certain payload
- Ideal payload: existing authentication protocol
- PANA: *A protocol for clients using IP protocols to authenticate themselves to an access network in order to be granted network access.*
- Supports multi-acces and point-to-point links
- Independent from kind of access and network topology
- Mutual authentication of host and network

Introduction to PANA and its requirements

• Goal and solutions of PANA workgroup

- Positioning PANA in the internet stack



• What is NOT in the scope of PANA

- Not the developement of a new security protocol
- No new authentication and authorization mechanisms
- But defining a transport for an existing security protocol
- And reuse its methods to achieve network access

Terminology and how PANA works

- Terminology and short cuts
- The PANA usage model

• Terminology and short cuts

- Components involved and required with PANA:

PaC PANA client. Has to prove its identity for network access authorization.

Hosted by a device which wants to get access to a network over the PAA.

PaCI PANA client identifier. Created by the PaC and sent to the PAA for authentication of the PaC.

• Terminology and short cuts (cont'd)

- Components involved and required with PANA:

DI Device identifier. A pointer to the client's device, used to control network access.

Contains IP address or switch port number or link layer address.

PAA PANA authentication agent. Verifies credentials of the PaC. Grants or denies network access.

• Terminology and short cuts (cont'd)

- Components involved and required with PANA:

EP Enforcement point. Provides per-packet filtering rules for network traffic of the PaC's device, using information of the DI provided by PaC.

- **The PANA usage model**

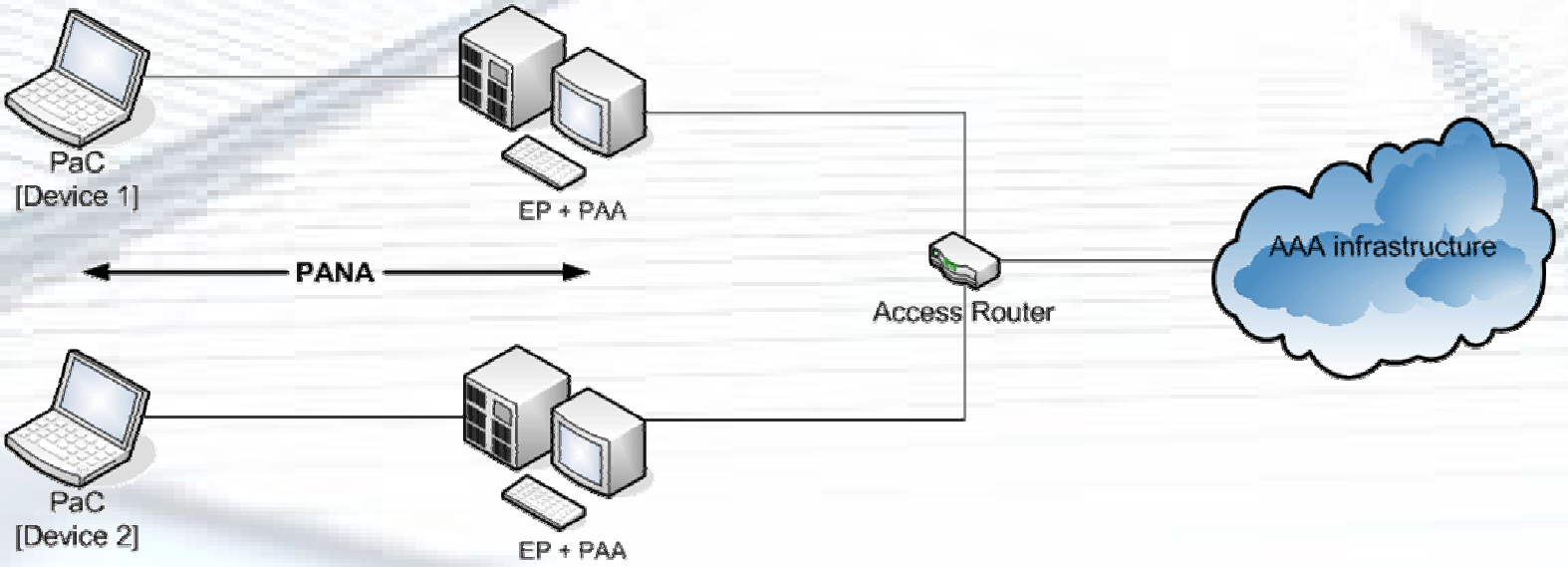
Four scenarios,
distinguished by location of components

- PAA co-located with EP but separated from AR
- PAA co-located with AR but separated from EP
- PAA co-located with EP and AR
- PAA separated from EP and AR

Terminology and how PANA works

• The PANA usage model

- PAA co-located with EP but separated from AR



- **The PANA usage model**

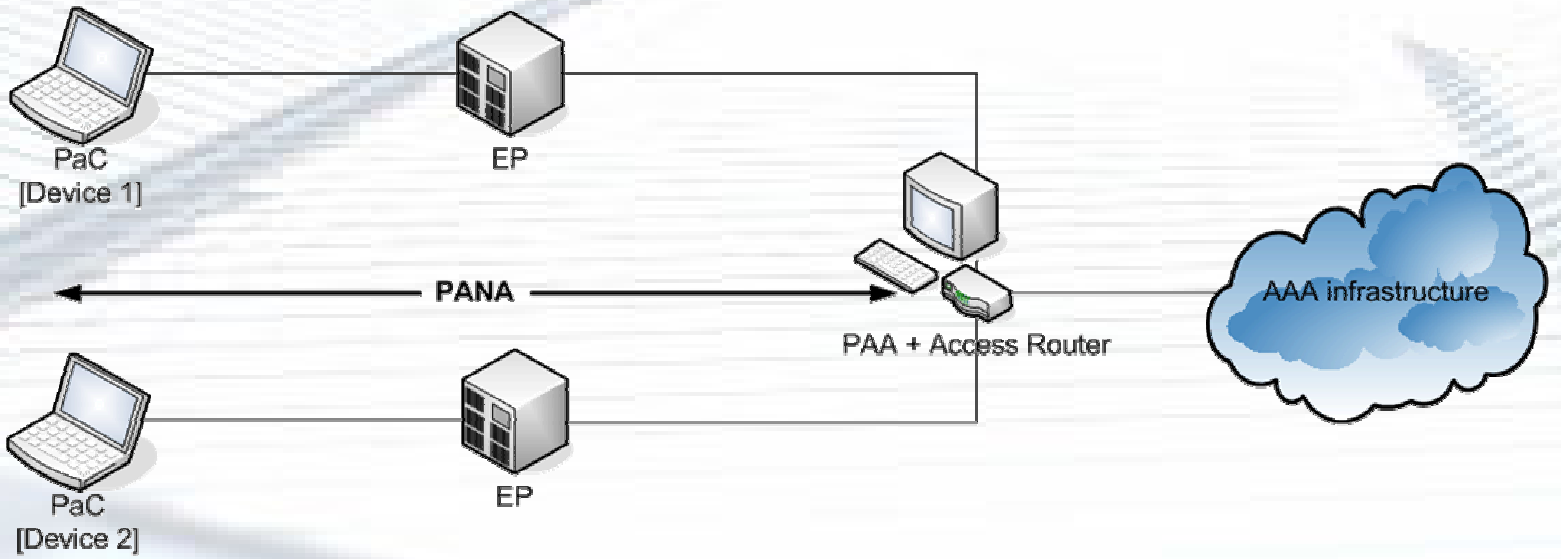
  - **PAA co-located with EP but separated from AR**

    - EP (controls access) and PAA located together
    - PaCs want to be authenticated by PAA
    - PANA has to carry authentication data from PaC to PAA
    - PAA grants or denies network access
    - PANA is only responsible for a secure transport of the credentials and methods, NOT for verification itself.

Terminology and how PANA works

• The PANA usage model

- PAA co-located with AR but separated from EP



- **The PANA usage model**

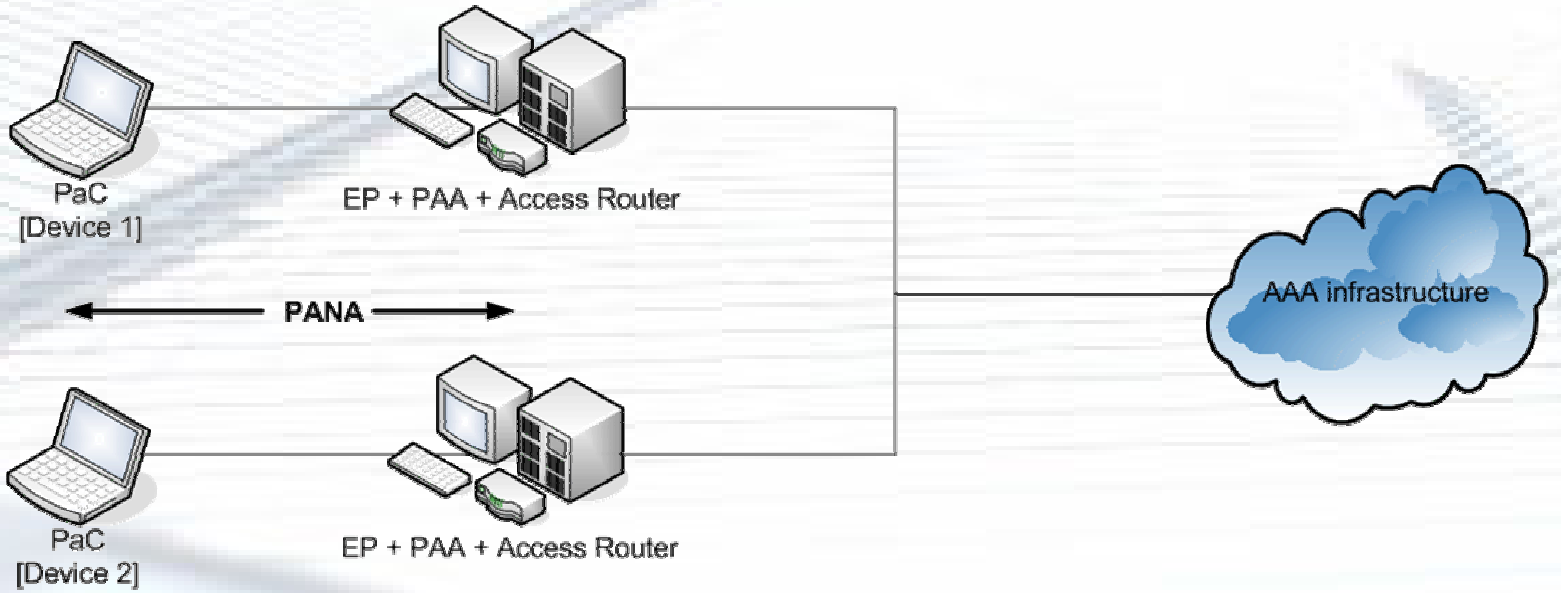
  - **PAA co-located with AR but separated from EP**

    - PAA and first hop access router located together
    - Same authentication data is sent from PaC to PAA
    - Parameters for access control have to be distributed to the corresponding EPs
    - Further protocol needed for PAA – EP transport !!

Terminology and how PANA works

• The PANA usage model

- PAA co-located with EP and AR



- **The PANA usage model**

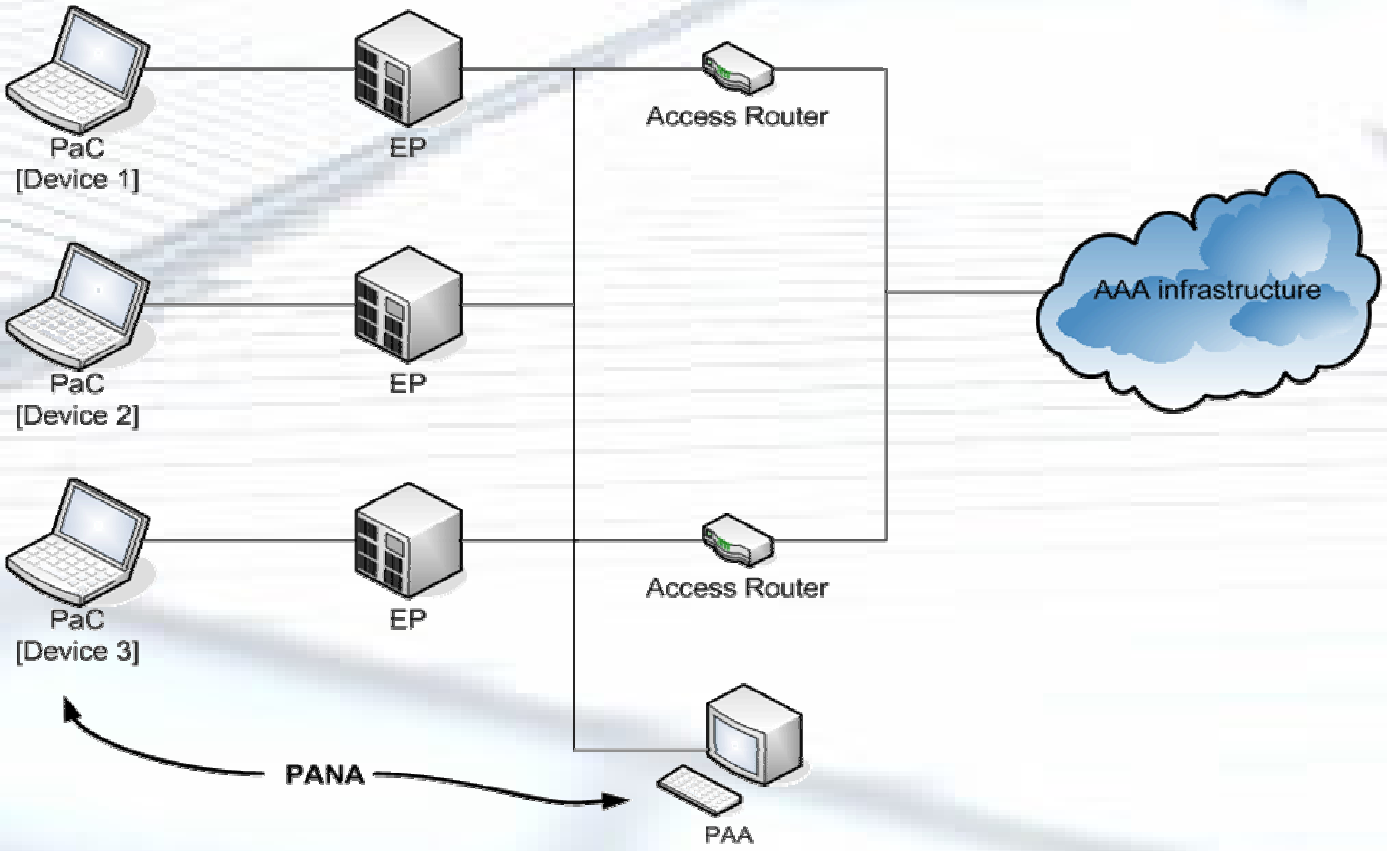
  - **PAA co-located with EP and AR**

    - PAA, EP and access router located together
    - Same authentication data is sent from PaC to PAA
    - No extra protocol needed for PAA – EP transport
    - Like before, PANA is only carrier

Terminology and how PANA works

• The PANA usage model

- PAA separated from EP and AR



- **The PANA usage model**

  - **PAA separated from EP and AR**

    - PAA, EP and access router are standalone instances
    - PAA has to be on the same IP range
    - Parameters for access control have to be distributed to the corresponding EPs
    - Further protocol needed for PAA – EP transport !!

Requirements of PANA

- Authentication
- IP address assignment
- PAA-to-EP Protocol
- Network
- Interaction with Other Protocols
- Congestion Control and Performance

Requirements of PANA

- **Authentication**

- PaC authenticated through its credentials

  Device identified by its DI (IP address, port number …)

  PaC, residing on device, identified by its PaCI

  → DI and PaCI together used for access control

Requirements of PANA

• Authentication (cont'd)

- PANA must not define new security protocols
  - Means of transport for an existing protocol
  - Candidate: EAP – Extensible Authentication Protocol
  - EAP provides key derivation and distribution
  - Requirements for EAP must be satisfied by PANA

Requirements of PANA

- **Authentication (cont'd)**

- PANA has to be independent from backend authentication technology, like an Authentication, Authorization and Accounting (AAA) infrastructure.
- Re-authentication PaC – PAA: *periodic* or *initiated*

Requirements of PANA

• Authentication (cont'd)

- PaC: Authorization after successful authentication to send and receive IP packets
- Hiding privacy of PaC from networks is not job of PANA

Requirements of PANA

• IP address assignment

- IP address configuration of PaC is not required

  - any other identifier could be used

  - increases complexity

  → Simply assigning an IP address to a not yet authenticated PaC would be a risk

  → Attacks: IP address depletion

Requirements of PANA

- **PAA-to-EP Protocol**

- Distributing access control parameters from PAA to EPs.

  Existing secure transport mechanism required.
- Control lists with filtering policies controlling network access of the PaC generated by PAA

  PAA-to-EP communication has to be secure

• PAA-to-EP Protocol (cont'd)

- Who is the initiator?

  → Push model: Communication initiated by PAA
  → Pull model: Communication initiated by EP

Requirements of PANA

- **Network**

- Pac: Multiple network interfaces
- Multiple routers in a network
- Multi-access links instead of point-to-point links
- One-hop distance between PaC and PAA offers possibility of multicast / anycast to the PaC to find the PAA

Requirements of PANA

- **Network (cont'd)**

- Disconnect indication (PaC)
  - PAA can free resources if disconnected PaC is indicated
  - Initiated by PaC: disconnect message
  - Initiated by PAA: regular authentication requests
  - Channel for disconnect message has to be secure!
- Unavailable network indication

Requirements of PANA

- **Network (cont'd)**

- Attack robustness
  - Communication PaC – PAA has to be secure
  - Avoiding attacks like eavesdropping and spoofing
  - Security has to be provided by PANA and must not be considered as existing!
  - EAP to achieve a secure channel

Requirements of PANA

• Interaction with Other Protocols

- Coexistence

  - To protocols like Mobile IPv4 (v6)

  - May not be obstructed / influenced by PANA

  - Work independently with IPv4 and IPv6

Requirements of PANA

• Congestion Control and Performance

- Same-time start-up problem

  - All PaCs request authentication at the same time

  - Mechanism to regulate verification traffic amount

  →Delayed initialization

- Performance and efficiency

Conclusion

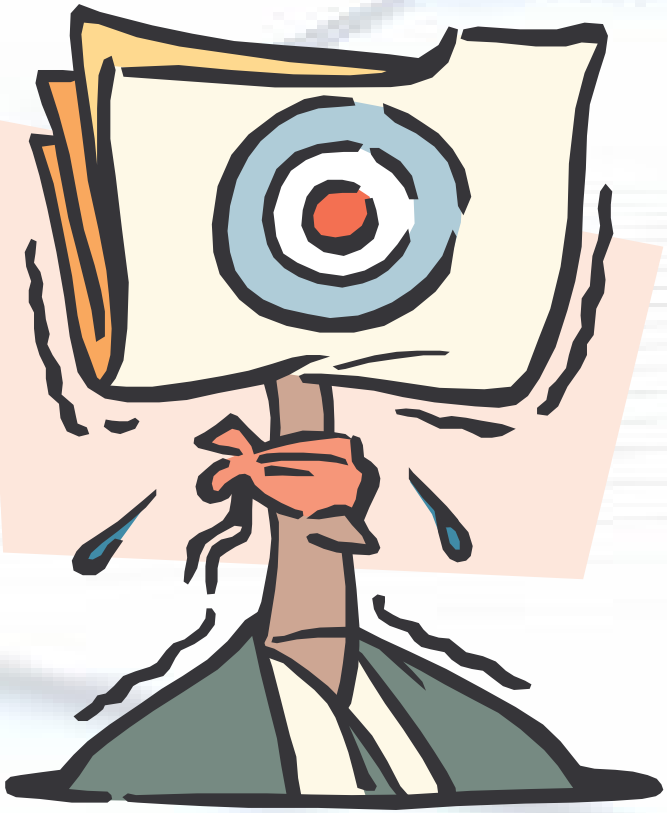
- Authentication of IP devices necessary.

  Link-layer possibilities not satisfying.

  Ad-hoc and inadequate non-standard solutions.

- PANA provides a clean solution on network-layer for secure network access.

…any questions?



Thank you!