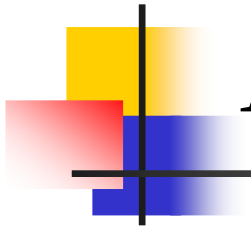
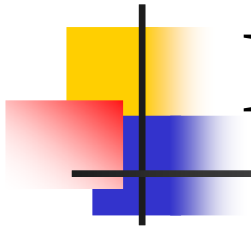
Threat Analysis and Security Requirements

Stefan Hertel



Agenda

- Introduction
- PANA usage Scenarios
- Threat Scenarios

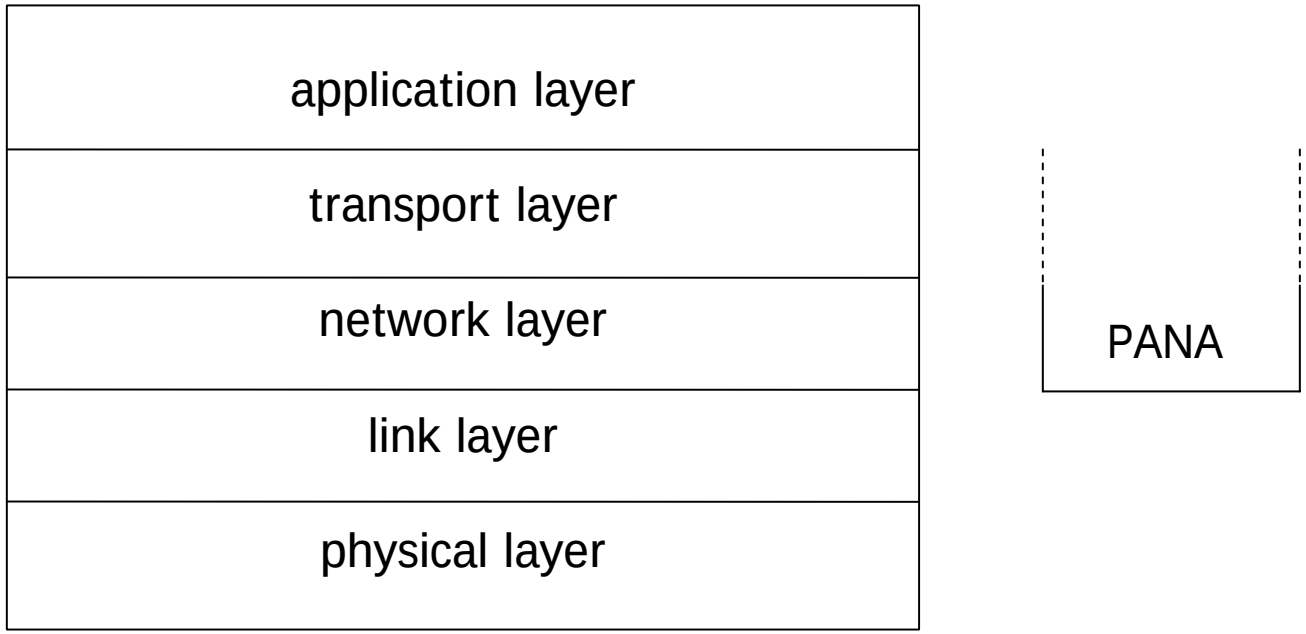


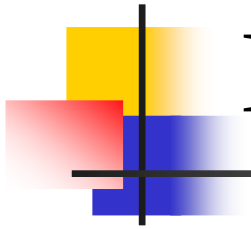
Introduction

- PANA WG
- Relation of the Draft to PANA WG
- Contents of the Draft

Introduction

- Internet Layer





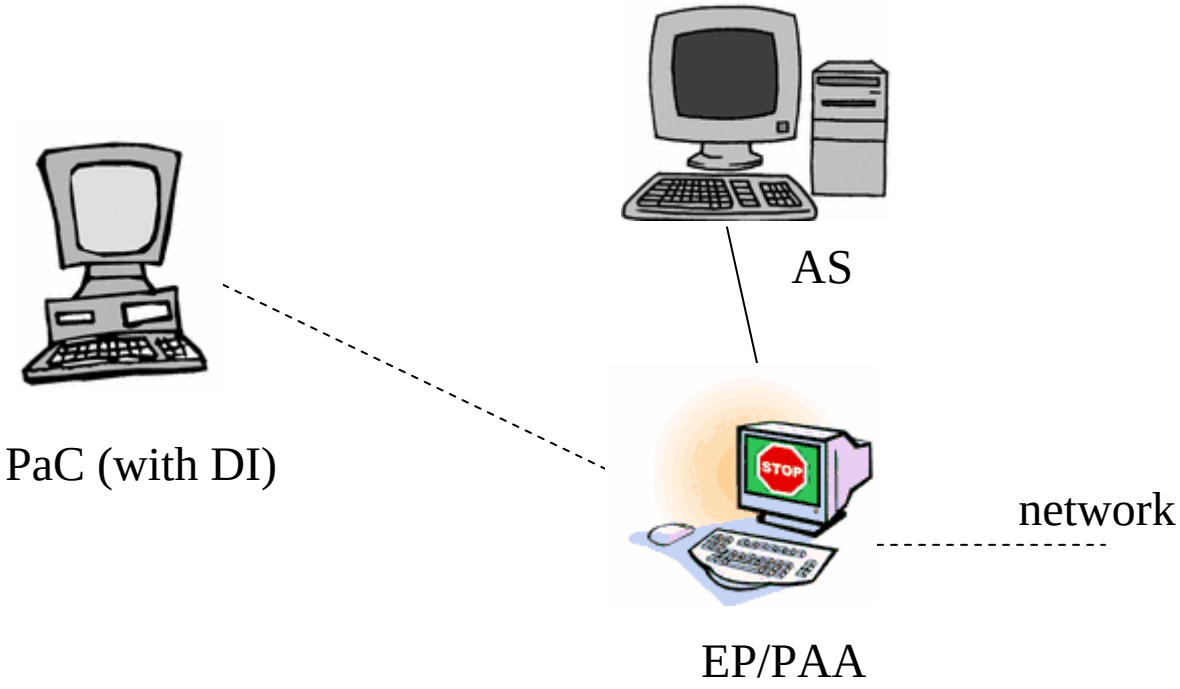
Introduction

Acronyms:

- AS
- DI
- EP
- PAA
- PaC

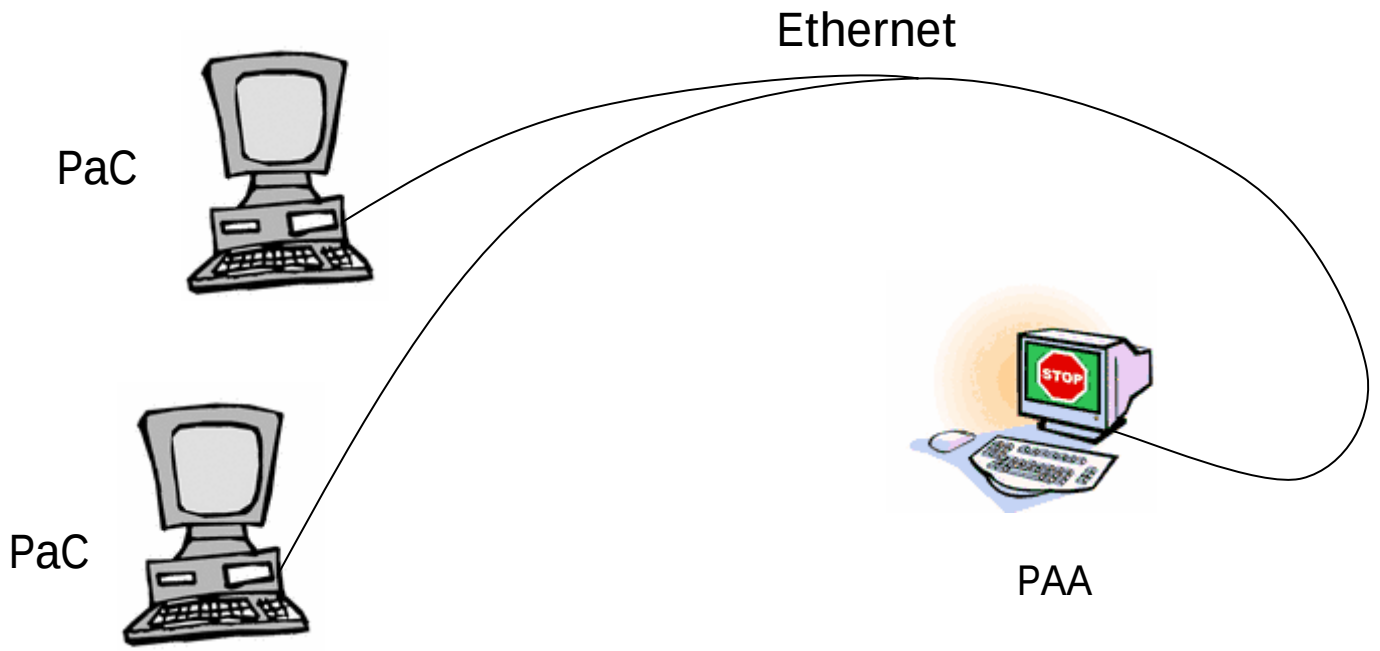
Introduction

Network Structure



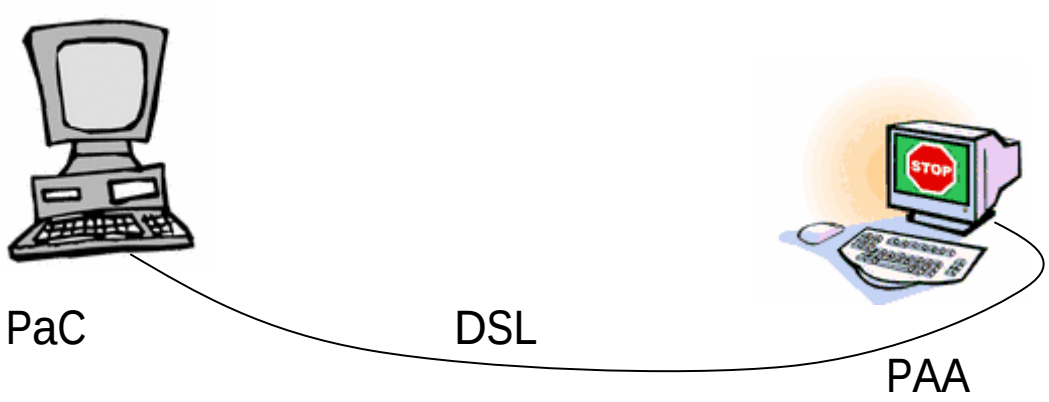
PANA Usage Scenarios

PaC and PAA linked by a shared medium



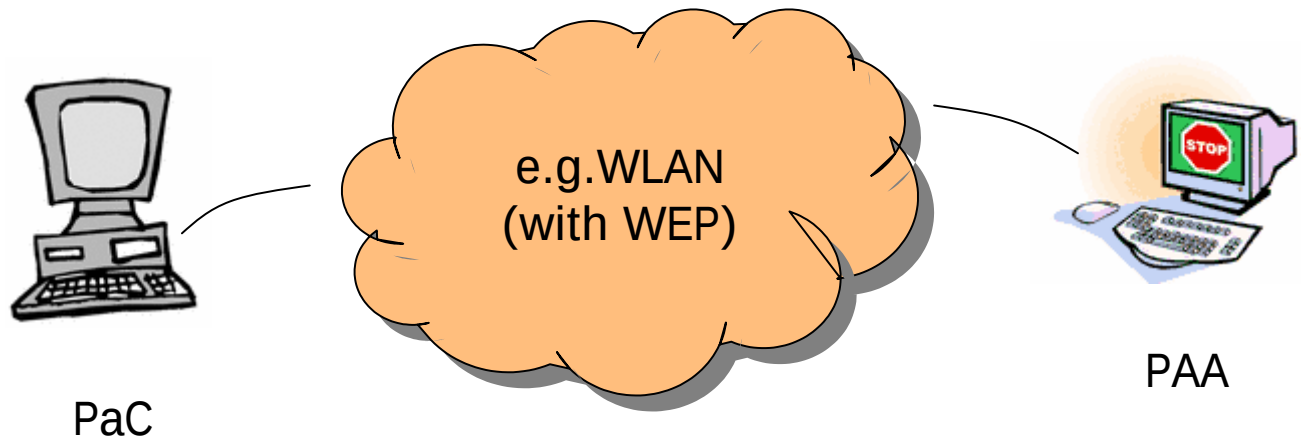
PANA Usage Scenarios

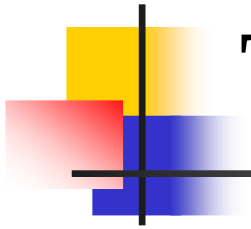
- PaC and PAA linked by a non shared medium



PANA Usage Scenarios

- PaC and PAA linked at Layer2 sharing a security association





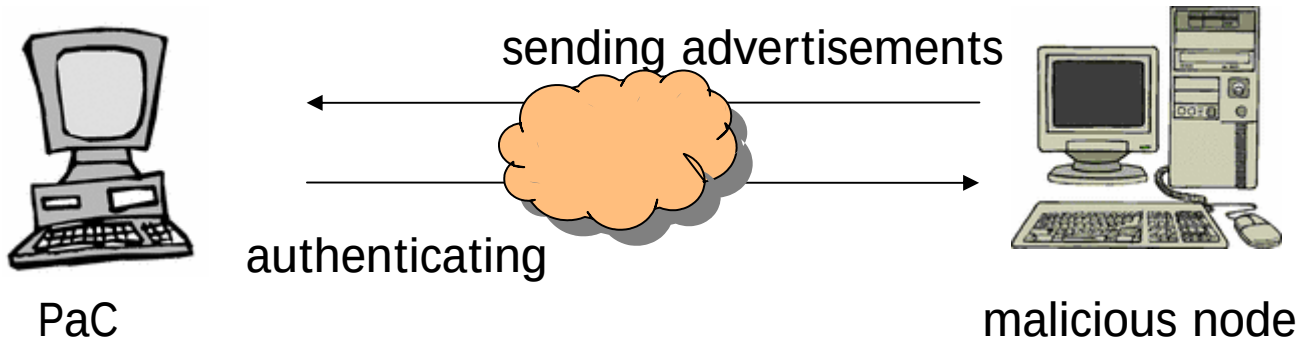
Threat Scenarios

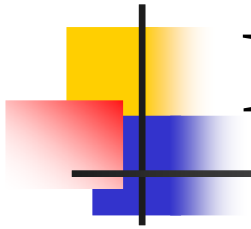
- PAA Discovery
- Authentication
- Pac leaving the Network
- Service Theft
- PAA-EP Communication
- Miscellaneous Attacks

PAA Discovery

- State
- Threat Scenario:
  - malicious node pretends being PAA

    (present only at shared mediums)

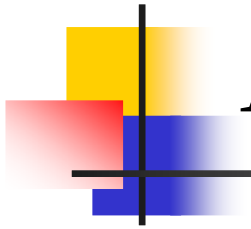




PAA Discovery

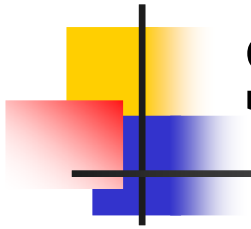
Security Requirements:

- PANA MUST not assume that the discovery process is protected
- security-critical information exchange SHOULD be limited



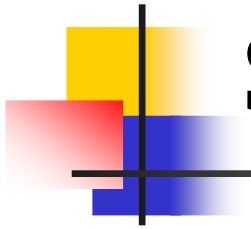
Authentication

- Success or Failure Indication
- Man in the Middle Attack
- Replay Attack
- Device Identifier Attack



Success or Failure Indication

- Present only at Shared Links
- Attacker can deny Service for PaC
  - by sending false failure messages
  - by sending false success messages



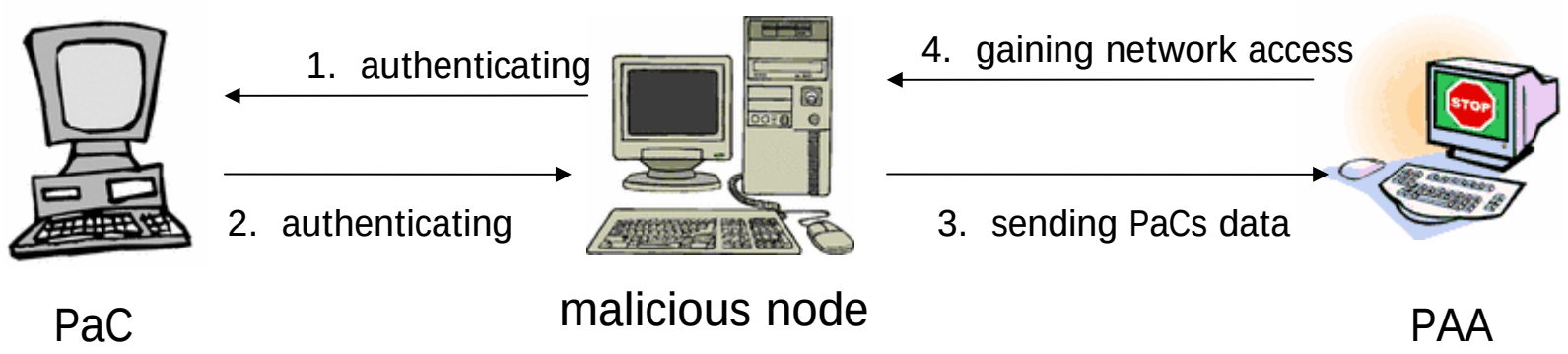
Success or Failure Indication

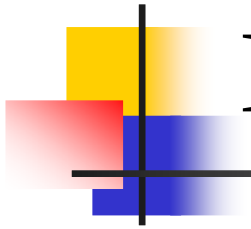
Security Requirements:

- PANA MUST be able to mutually authenticate PaC and PAA
- PANA MUST be able to protect the PANA messages.

Man in the Middle Attack

- Present only at Shared Links
- Possible when using Compound Authentication Methods

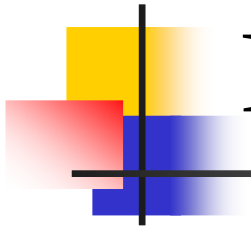




Man in the Middle Attack

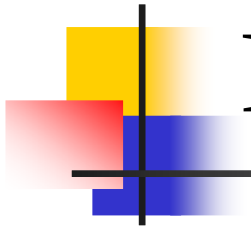
Security Requirement:

- Compound authentication methods used in PANA MUST be cryptographically bound



Replay Attack

- Present only at Shared Links
- Malicious Node replays Messages to:
  - gain access to the network
  - deny service to PaC
- Threat is present even if Layer 2 provides Replay Protection

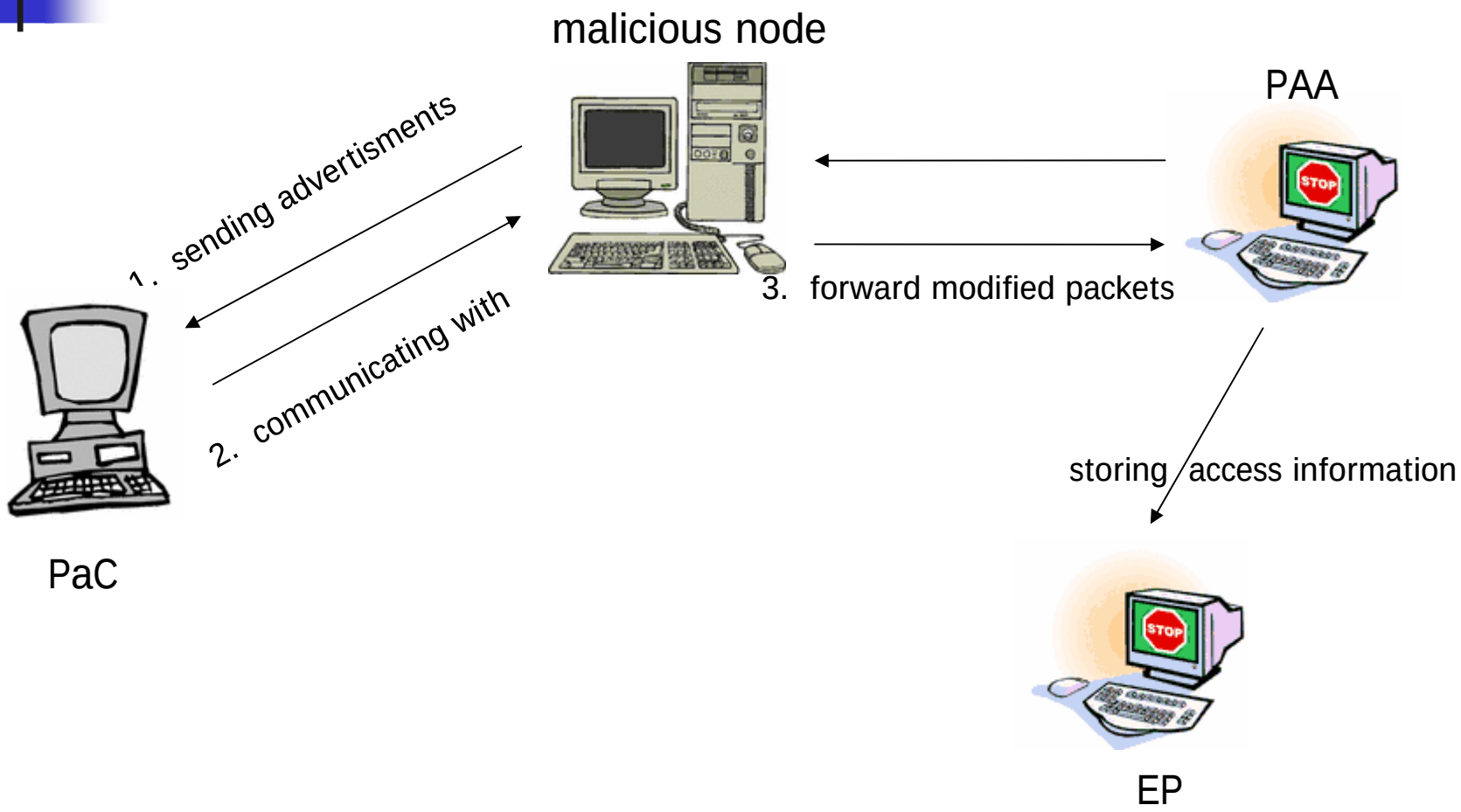


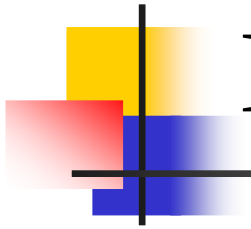
Replay Attack

Security Requirement:

- PANA MUST be able to protect itself against replay attacks

Device Identifier Attack

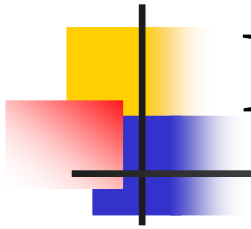




Device Identifier Attack

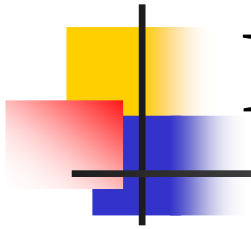
Security Requirement:

- PANA MUST be able to protect the device identifier against spoofing



PaC leaving the Network

- Malicious Node pretends to be PAA
- Malicious Node pretends to be PaC
- PaC leaves Network without notifying PAA or EP

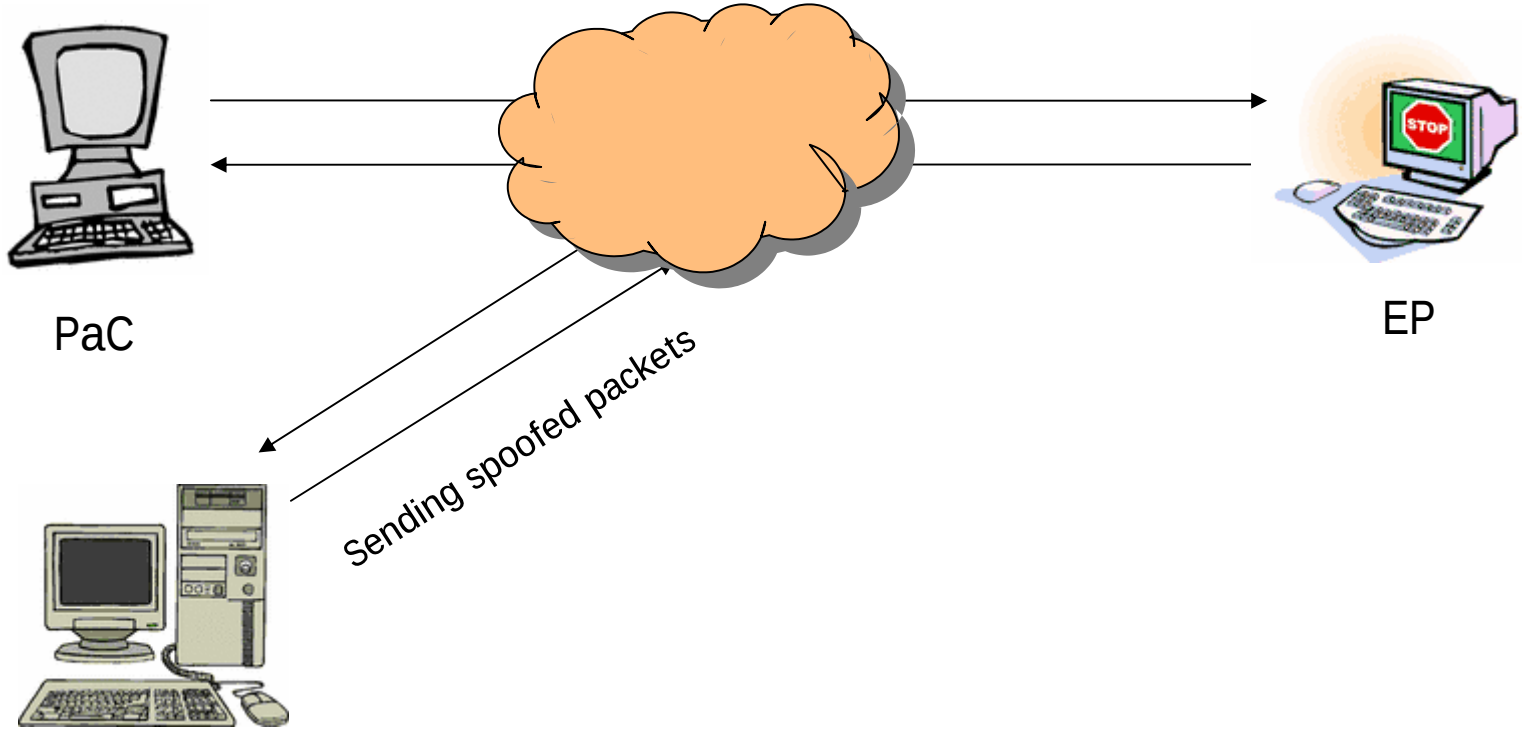


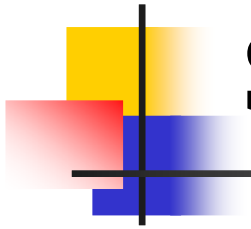
PaC leaving the Network

Security Requirements:

- PANA MUST be able to protect disconnect and revocation messages
- PANA MUST NOT depend on PaC sending a disconnect message

Service Theft

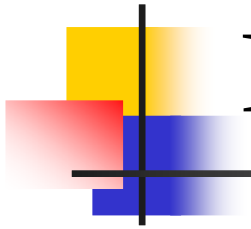




Service Theft

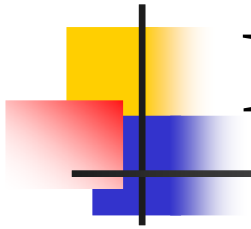
Security Requirements:

- PANA MUST securely bind the authenticated session to the device identifier of the client
- PANA MUST be able to bootstrap a shared secret between the PaC and PAA



PAA-EP Communication

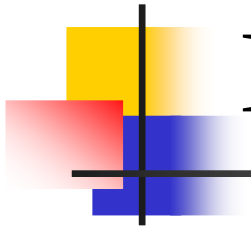
- Threat Scenarios:
  - Attacker can eavesdrop Communication between PAA and EP
  - Attacker can pretend to be PAA
- Threats are absent if Communication between PAA and EP is protected



PAA-EP Communication

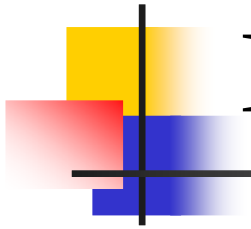
Security Requirement:

- Communication between PAA and EP MUST be protected



Miscellaneous Attacks

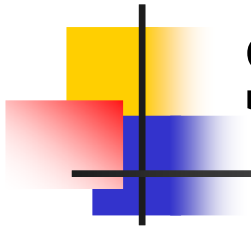
- Bombard PAA with Authentication Requests
- Force PAA or AS to do computationally intensive Operations
- Address Depletion Attack



Miscellaneous Attacks

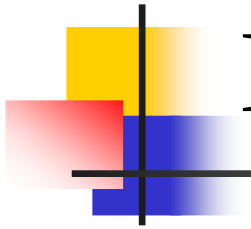
Security Requirement:

- PANA SHOULD not assume that the PaC has acquired an IP address



Sources

- draft-ietf-pana-threats-eval-04
- draft-ietf-pana-requirements-07
- draft-puthenkulam-eap-binding-02



End of Presentation

Thank you for your Attention