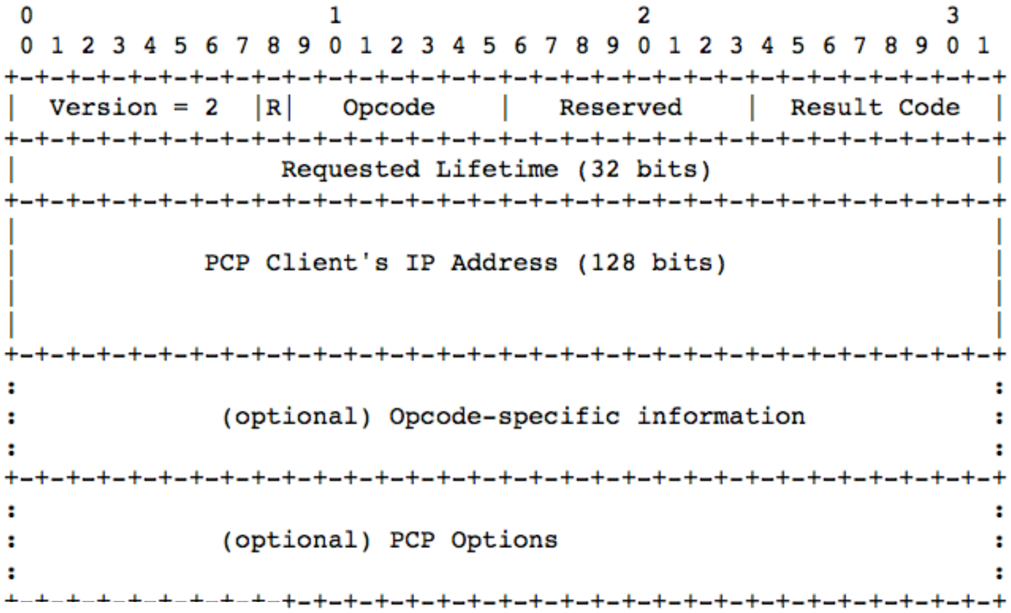
Port Control Protocol (PCP) Authentication Mechanism

draft-ietf-pcp-authentication-02

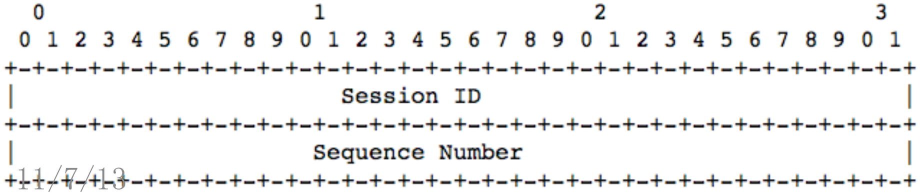
Margaret Wasserman
Sam Hartman
Dacheng Zhang

PCP Authentication (PCP Auth) messages

- An authentication Opcode, a set of Options are defined in order to perform authentication using EAP.
- A PCP message with an Authentication OpCode is referred to as a PCP Auth message.
- Result codes are defined to specify the types of messages



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Version = 2  |R|   Opcode    |   Reserved    |  Result Code  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Requested Lifetime (32 bits)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|            PCP Client's IP Address (128 bits)                 |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                                                               :
:             (optional) Opcode-specific information            :
:                                                               :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                                                               :
:             (optional) PCP Options                            :
:                                                               :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Session ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

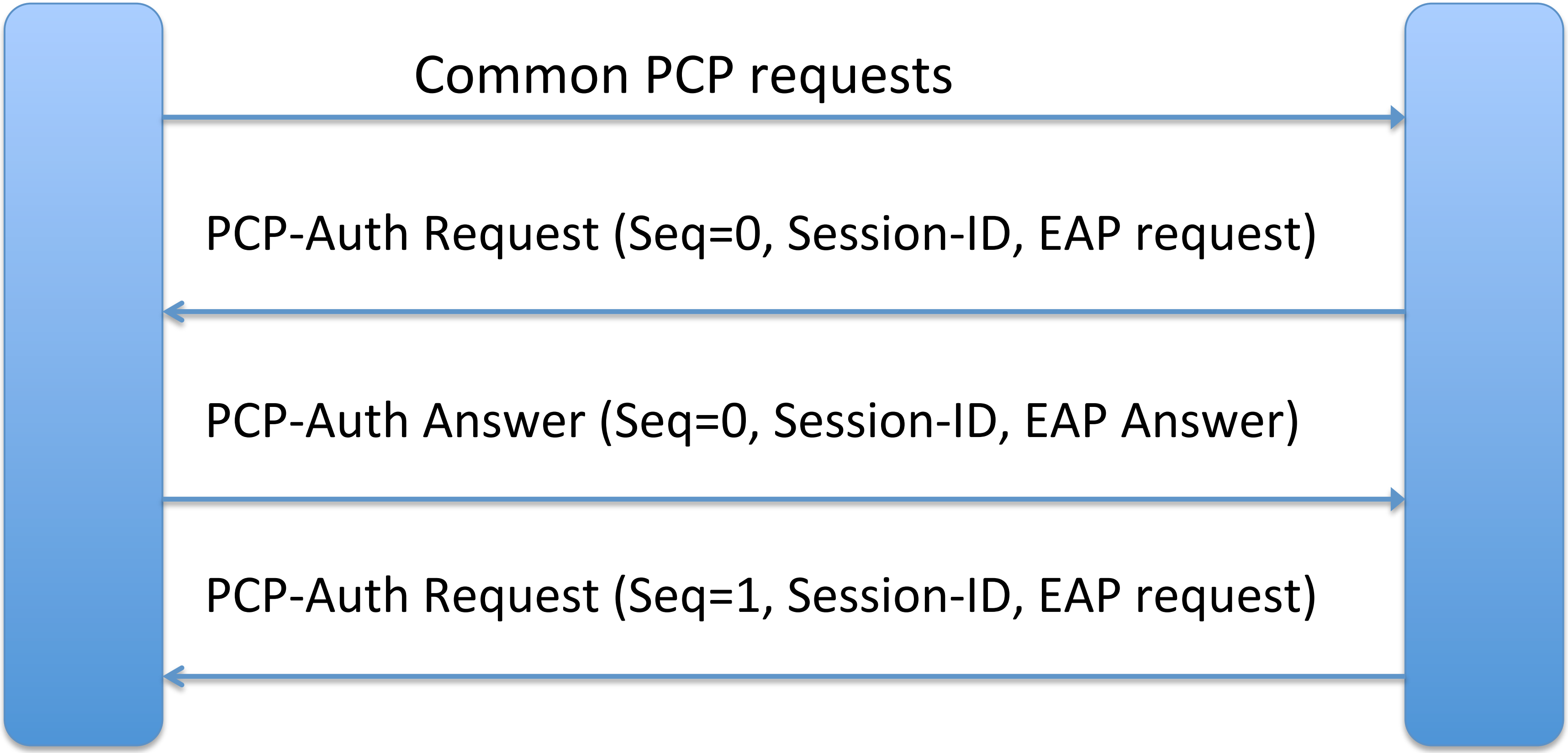
PCP-Auth-Requests and Answers

- A PCP Auth message sent from a PCP server to a PCP client is referred to as a PCP-Auth-Request. A PCP-Auth-Request is actually a PCP response message specified [RFC6887]
- A PCP Auth message sent from a PCP client to a PCP server is referred to as a PCP-Auth-Answer. A PCP-Auth- Answer is a PCP request message.

Result Codes

- Results codes are used specified for different types of PCP-Auth messages
  - INITIATION
  - AUTHENTICATION-REQUIRED
  - AUTHENTICATION-FAILED
  - AUTHENTICATION-SUCCEED
  - AUTHORIZATION-FAILED
  - SESSION-TERMINATION
  - PACKET-RECEIVED-ACK

Session Initiation—Scenario 1



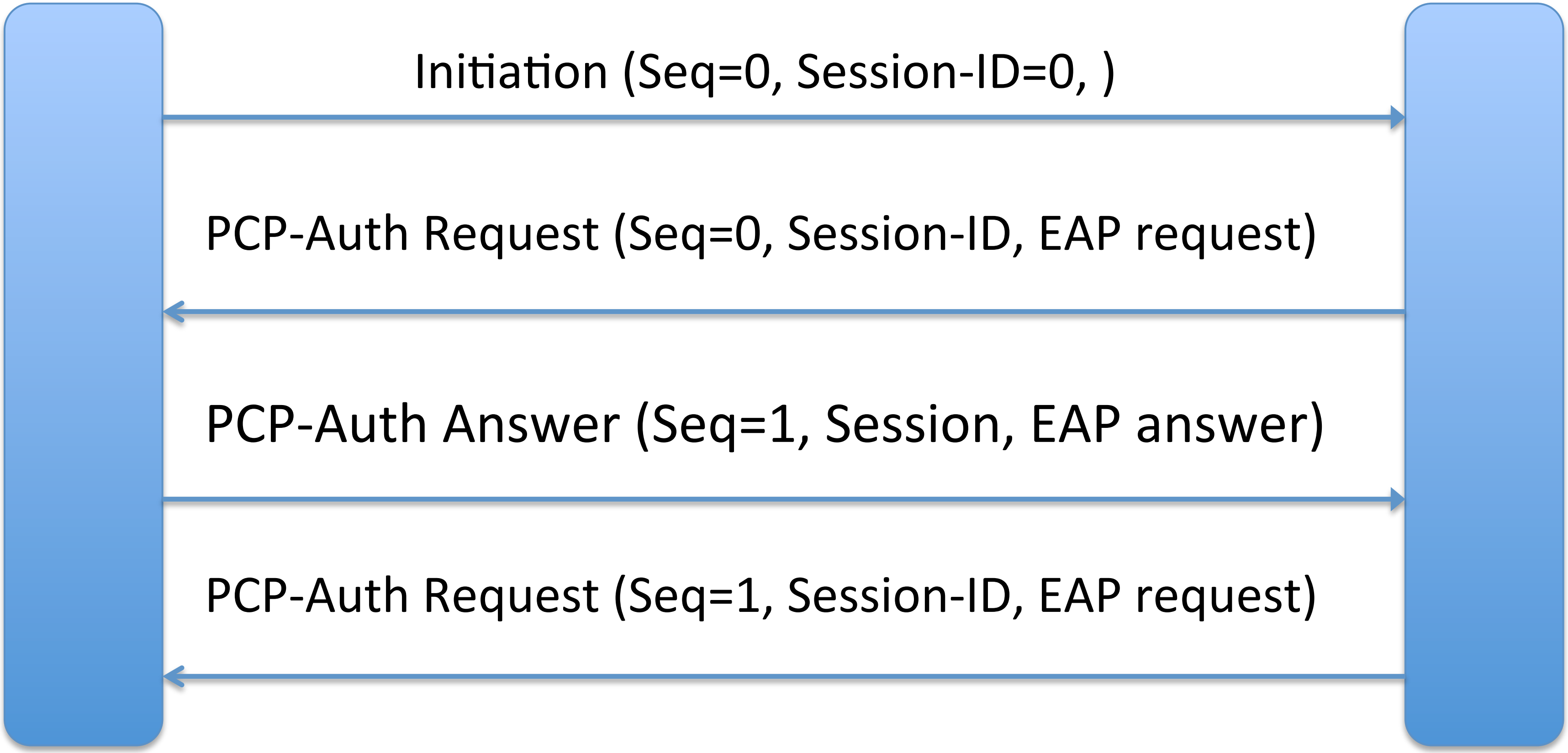
Common PCP requests

PCP-Auth Request (Seq=0, Session-ID, EAP request)

PCP-Auth Answer (Seq=0, Session-ID, EAP Answer)

PCP-Auth Request (Seq=1, Session-ID, EAP request)

Session Initiation—Scenario 2



Initiation (Seq=0, Session-ID=0,)

PCP-Auth Request (Seq=0, Session-ID, EAP request)

PCP-Auth Answer (Seq=1, Session, EAP answer)

PCP-Auth Request (Seq=1, Session-ID, EAP request)

Session Termination

- A PCP Auth session can be explicitly terminated by sending a termination-indicating PCP Auth message (a PCP Auth message with a result code "SESSION-TERMINATION") from either session partner.
- After receiving a termination-indicating message from the session partner, a PCP device MUST respond with a termination-indicating PCP Auth message and remove the PCP Auth SA immediately.

Session Re-Authentication

- When the PCP server initiates re-authentication, it sends a PCP-Auth-Request message containing the EAP message for re-authentication to the PCP client with the result code ”RE-AUTHENTICATION”
- The PCP client send an PCP-Auth-Answer message containing the EAP message for re-authentication to the PCP server, The result code is set to "RE-AUTHENTICATION".
- Before the new SA is generated, the old SA is used to protect the PCP-Auth packets

Nonce

- In order to prevent an attacker from interrupting the authentication process by sending off-line generated PCP-Auth-Request messages, the PCP client needs to generate a random number as nonce in the PCP- Auth-Initiation message ／ the first PCP-Auth-Answer message.
- If the subsequent PCP-Auth-Request message from the server does not carry the correct nonce, the message will be discarded.
- If nonce is transported during a session, it will be used in the generation of traffic keys.

Algorithm Negotiation

- The PCP server needs to append the initial PCP-Auth-Request message with a set of PRF Options and MAC Algorithm Options.
- Each PRF Option contains a PRF that the PCP server supports, and each MAC Algorithm Option contains a MAC algorithm that the PCP server supports.
- After receiving the request, the PCP client selects a PRF and a MAC algorithm which it would like to use, and sends back a PCP-Auth-Answer with a PRF Option and a MAC Algorithm Option for the selected algorithm.

Reliable Packet Delivery

- In the base PCP protocol, PCP clients are responsible for reliable delivery of PCP request messages
- In this document, both PCP clients and PCP servers need to provide reliable delivery of PCP Auth messages.
- When a PCP device cannot generate a response within a pre-specified period, the PCP device MUST reply with a PCP-Auth-Acknowledge message (a PCP-Auth message with the result code "PACKET-RECEIVED-ACK") to notify the packet has been received.

Sequence Member (1)

- A PCP device needs to maintain two sequence numbers, one for incoming packets and one for outgoing packets.
- When generating an outgoing PCP packet, the device attaches the outgoing sequence number to the packet and increments the sequence number maintained in the SA by 1.
- When receiving a PCP packet from its session partner, the device will not accept it if the sequence number carried in the packet does not match the incoming sequence number the device maintains.
- After confirming that the received packet is valid, the device increments the incoming sequence number maintained in the SA by 1.

Sequence Member (2)

- An exception is PCP-Auth-Acknowledgement messages which is not required to be reliably delivered.
- When receiving or sending out a PCP-Auth-Acknowledgement message, the device MUST not increase the corresponding sequence number stored in the SA.

Sequence Member (3)

- Another exception is packet re-transmission.
- The duplicate messages and the original message MUST use the identical sequence number.
- The maintained incoming and outgoing sequence numbers will not be affected by the message retransmission.

Thank you for your time!