IETF91-MBONED/PIM

IP Multicast Receiver Access Control

draft-atwood-mboned-mrac-pana
draft-atwood-pim-sigmp
draft-atwood-pim-gsam

J. William Atwood
Bing Li
Concordia University, Montreal
Salekul Islam
United International University, Dhaka

Overview

- Exploring the area of Receiver Access Control for IP Multicast
  - Subtitle: Making money using IP Multicast
  - Covers **some** of the same concerns as those of the "well-managed multicast" work that was presented in MBONED four years ago
  - **much** smaller scope of interest
  - MBONED: "application" level drafts
  - PIM: "network" level drafts

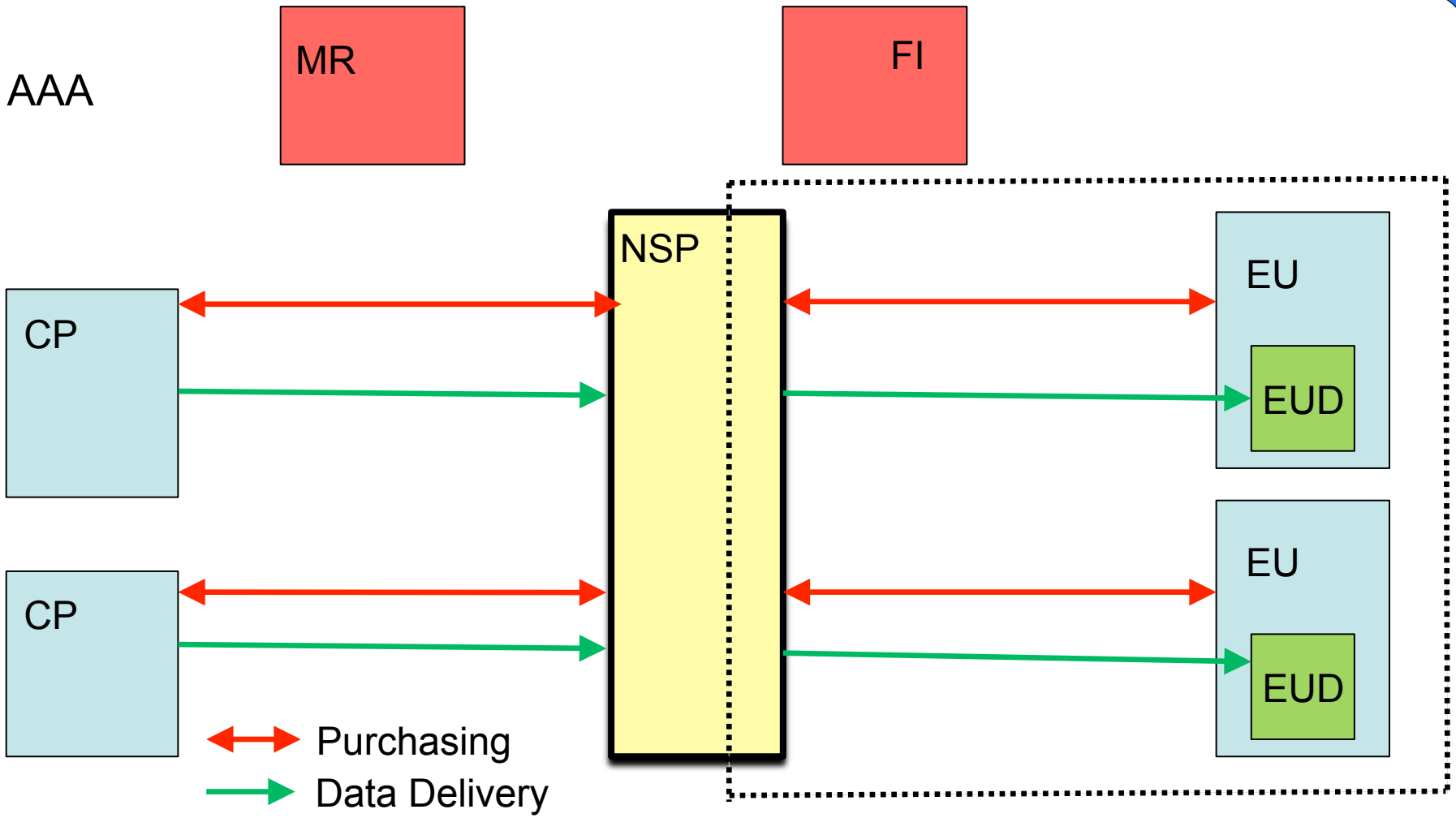
Two Assumptions

- The End User (EU) acquires a “ticket” from the Merchant (or anyone else) containing:
  - Session Descriptor
  - Secure End User authentication
  - Possibly, an encryption key for the data stream
- The “Network Representative” has information on how to validate a “ticket” or assess the authorization of the EU or EU Device
- This makes the discussion today independent of the business model in use by the NSP and/or CP
- It restricts the scope of the work

Open vs Secure Groups

- Open Group
  - No access controls
  - Operations will follow standard IP multicast rules (3376 or 3810)
- Secure Group
  - Access controls to prevent an unauthorized EU from accessing the group
  - Additional operations are needed
  - IGMP/MLD exchanges are protected with IPsec, using the derived keys → ***Secure*** IGMP/MLD
  - Key and SPI Management → **GSAM**

Overall Architecture

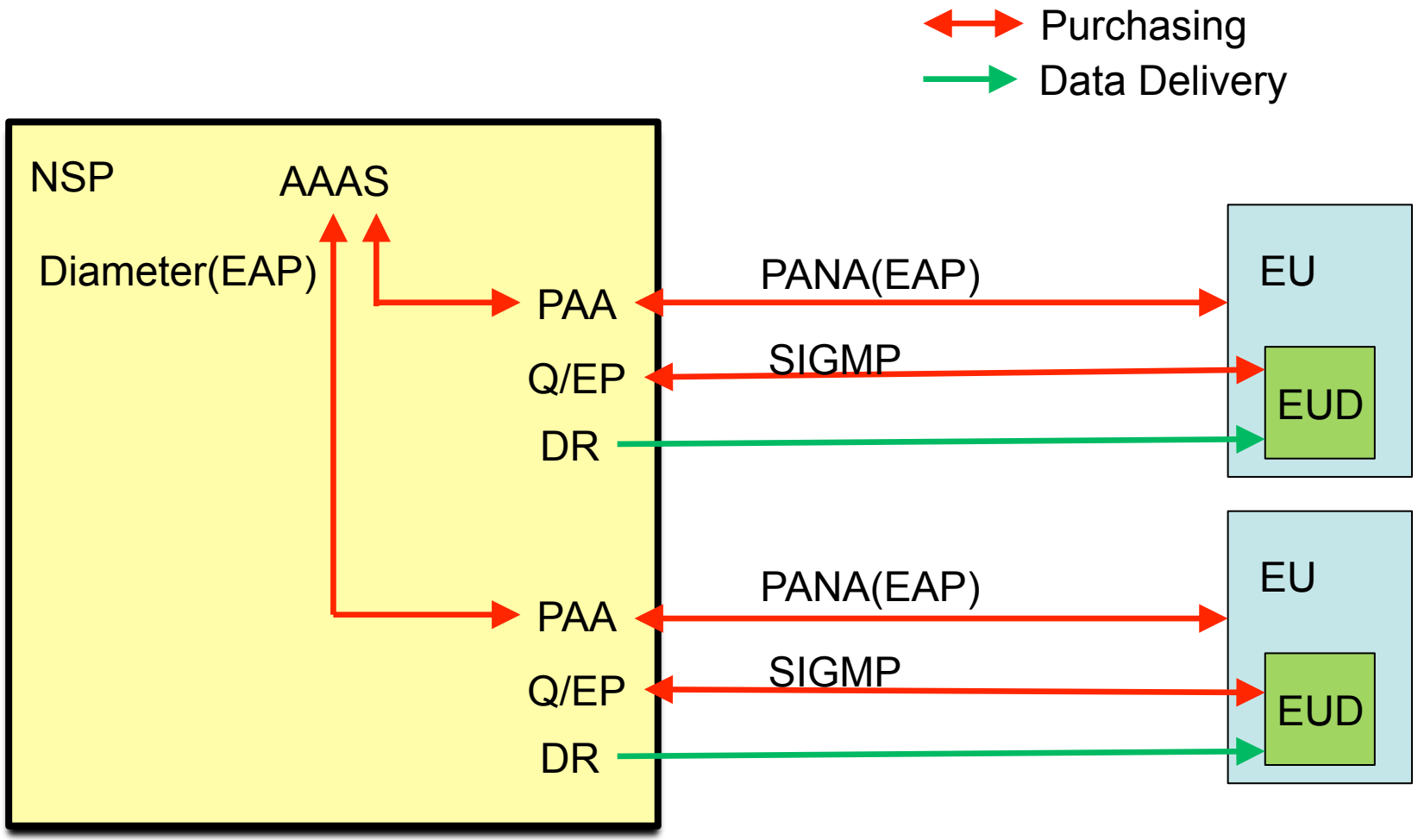


Two levels of interaction

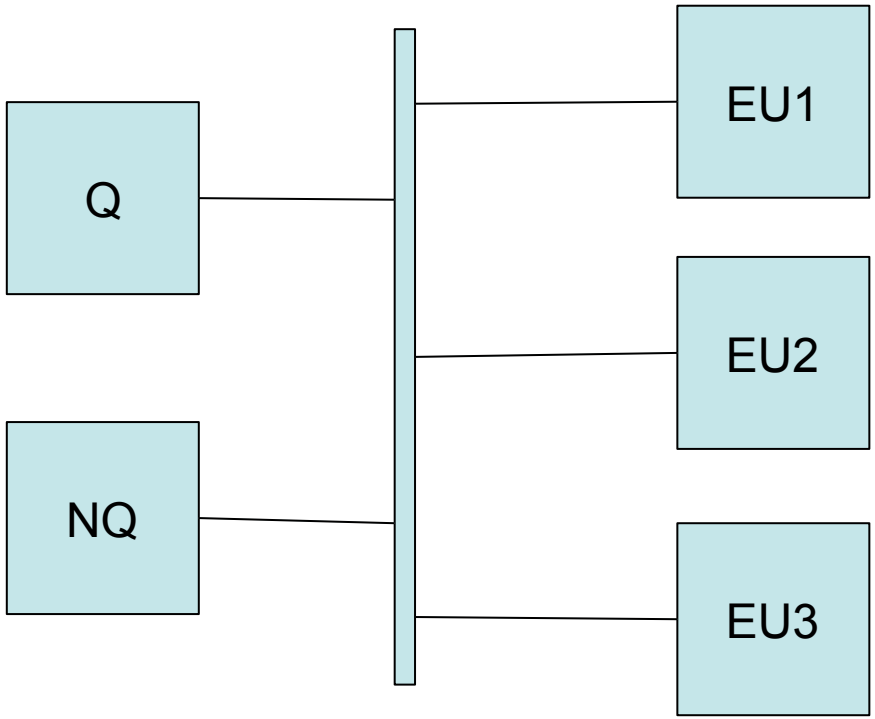
- Application Level
  - EU presents the “ticket”
  - Goal: Join the group
- Network Level
  - End User Device issues IGMP/MLD

- To ensure that only legitimate subscribers get access
  - MUST be secure at Application Level
  - MUST be secure at Network Level

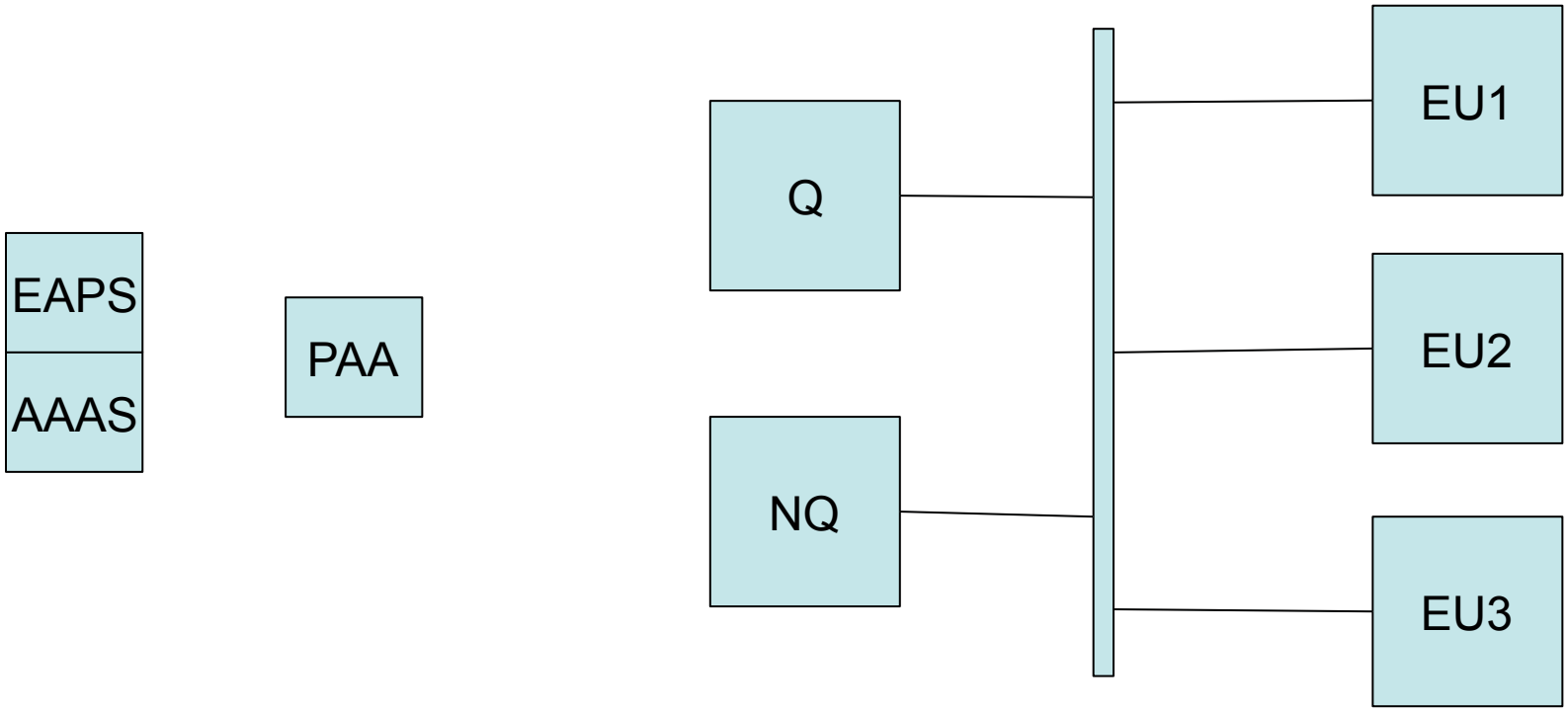
One network segment



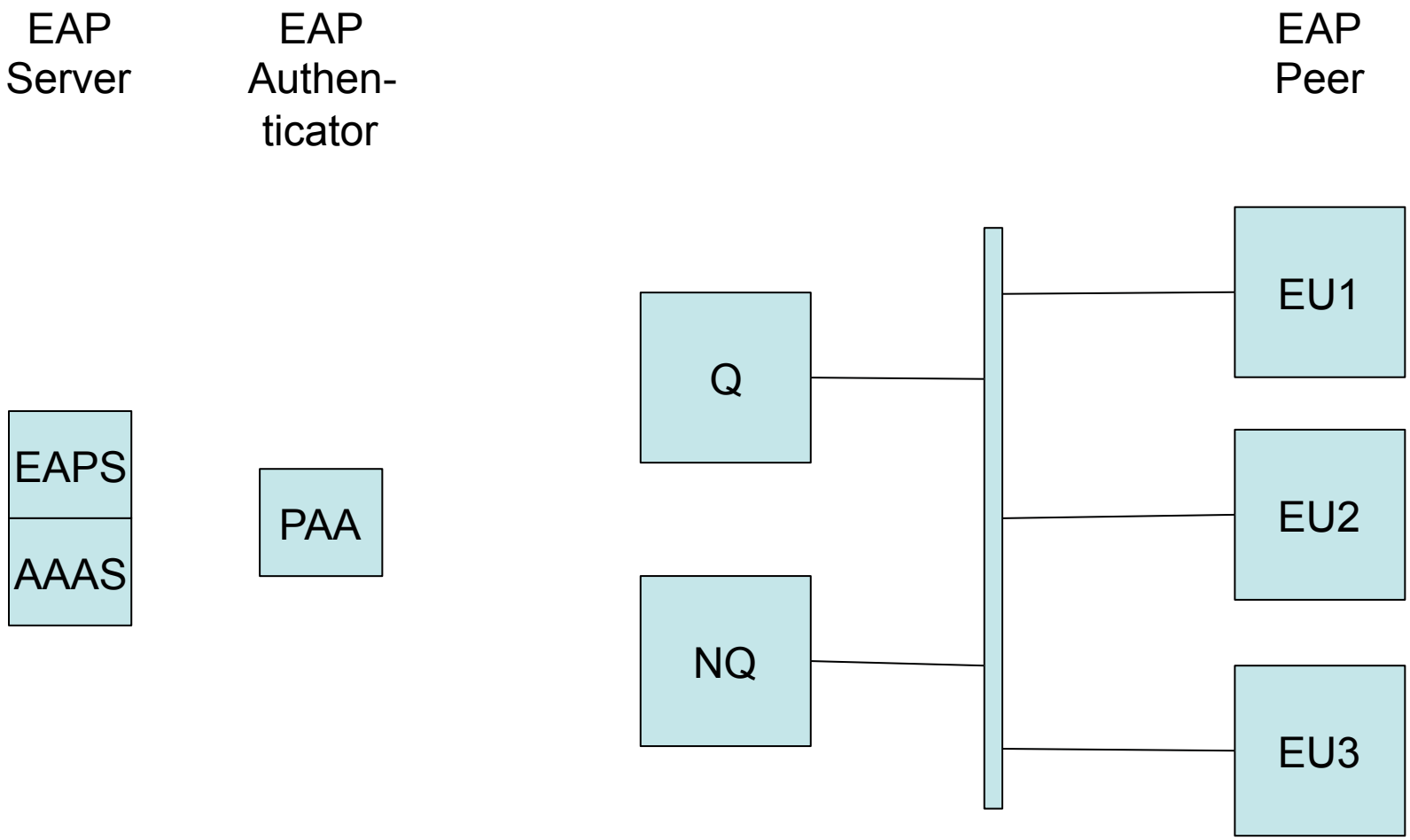
Environment: Network Segment for Multicast



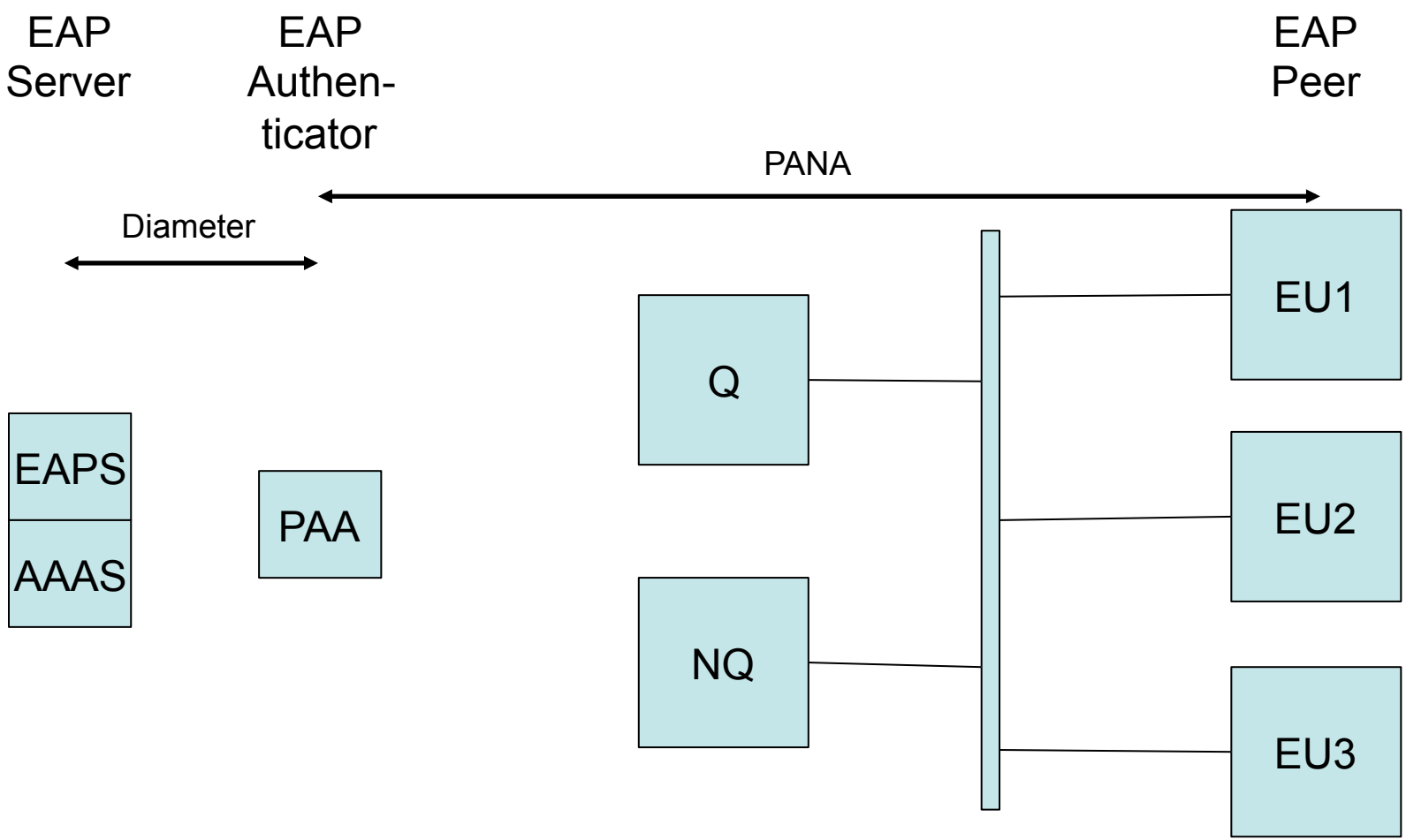
Environment: Add EAPS and PAA



Environment: Locate EAP participants



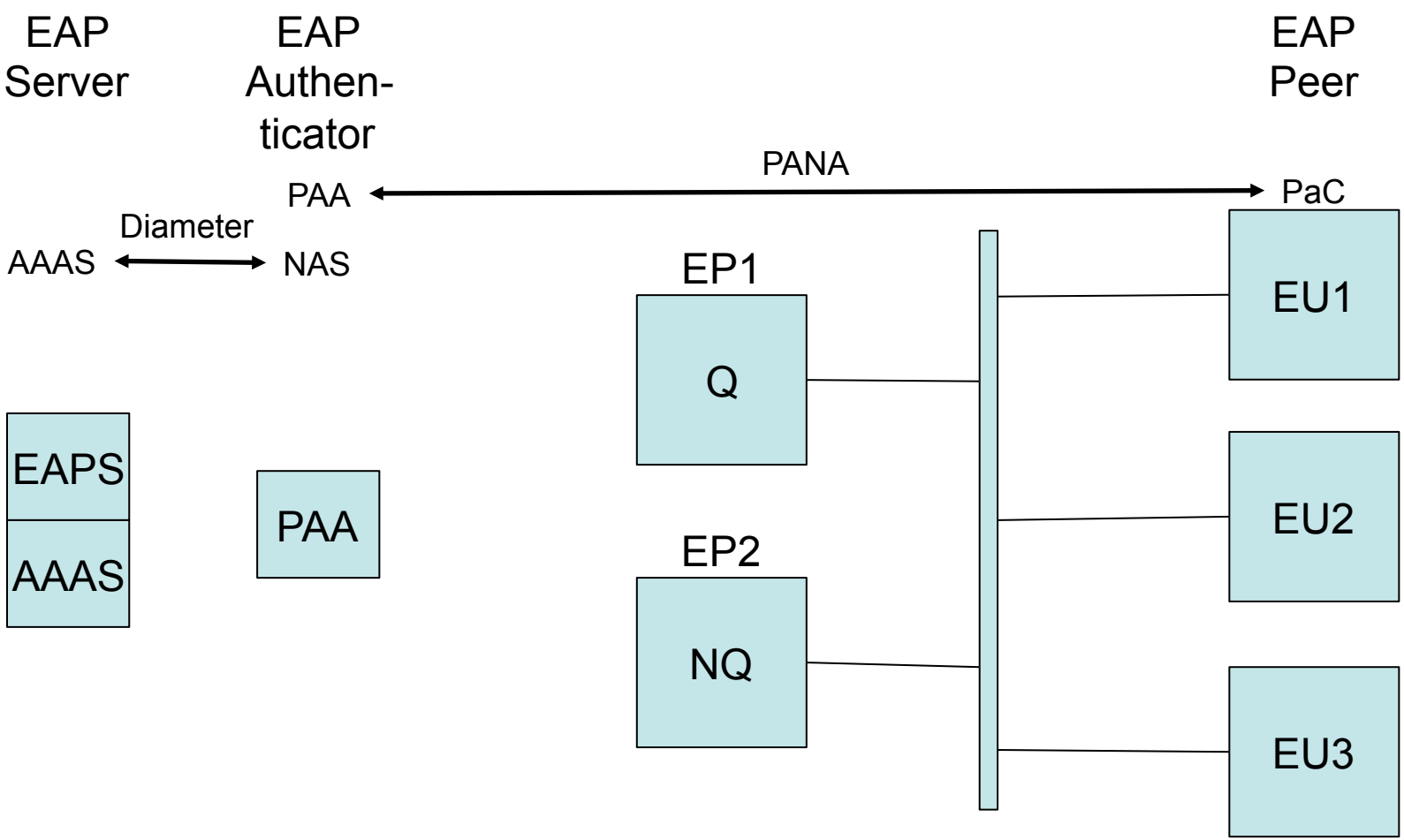
Environment: Show EAP Transport



PANA components: PAA, PaC, EP

- The PAA is the negotiator for the network end of the PANA session
- The PaC is the negotiator for the user end of the PANA session
- In general, the PAA will have one or more Enforcement Points (EP) under its control
  - For general network access control, the EP may well be a switch
  - For our application, the EP must be the Querier (Q) for that network segment. If a snooping IGMP switch is present, we may need to adjust this.

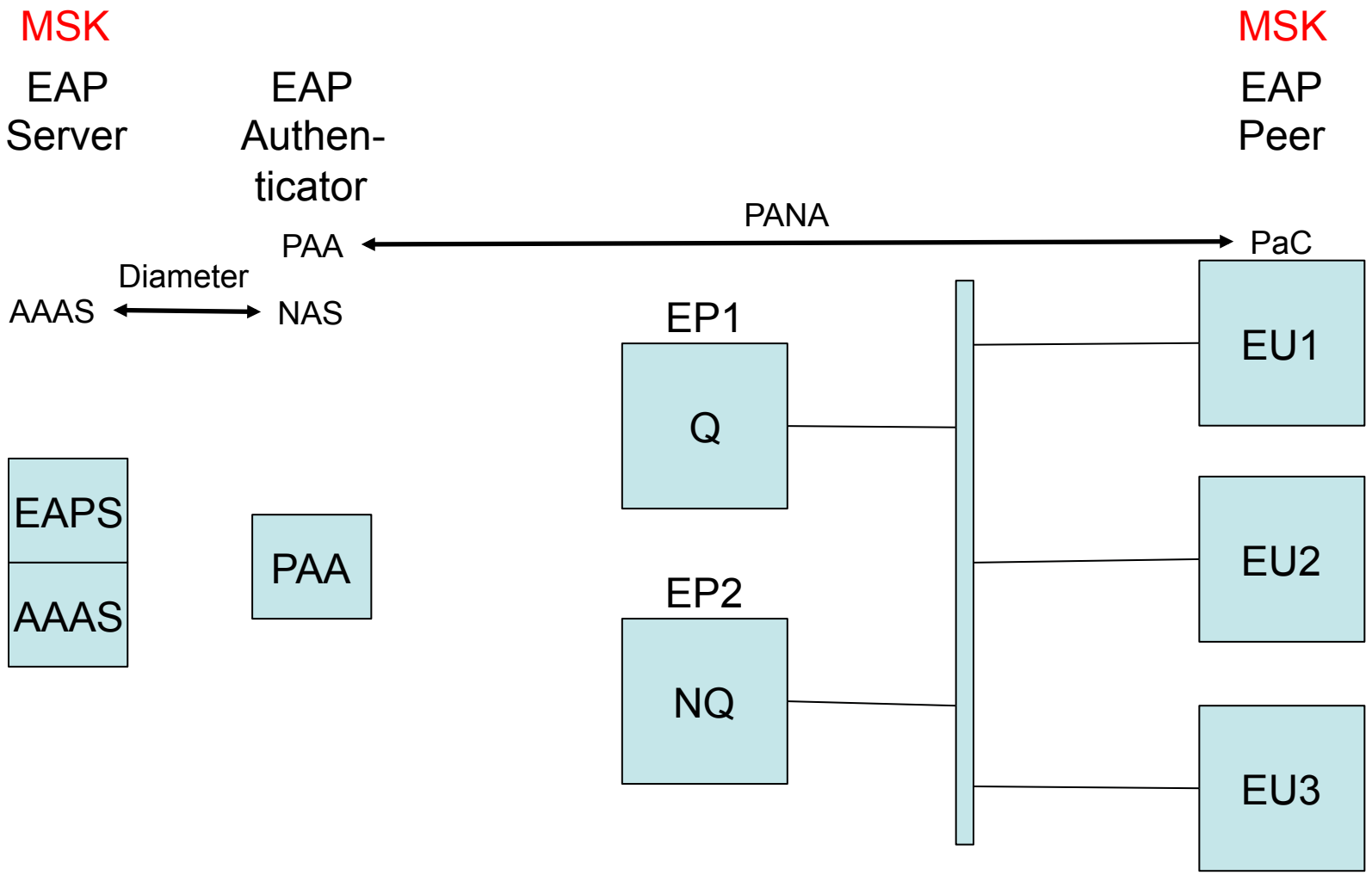
Environment: Show EPs



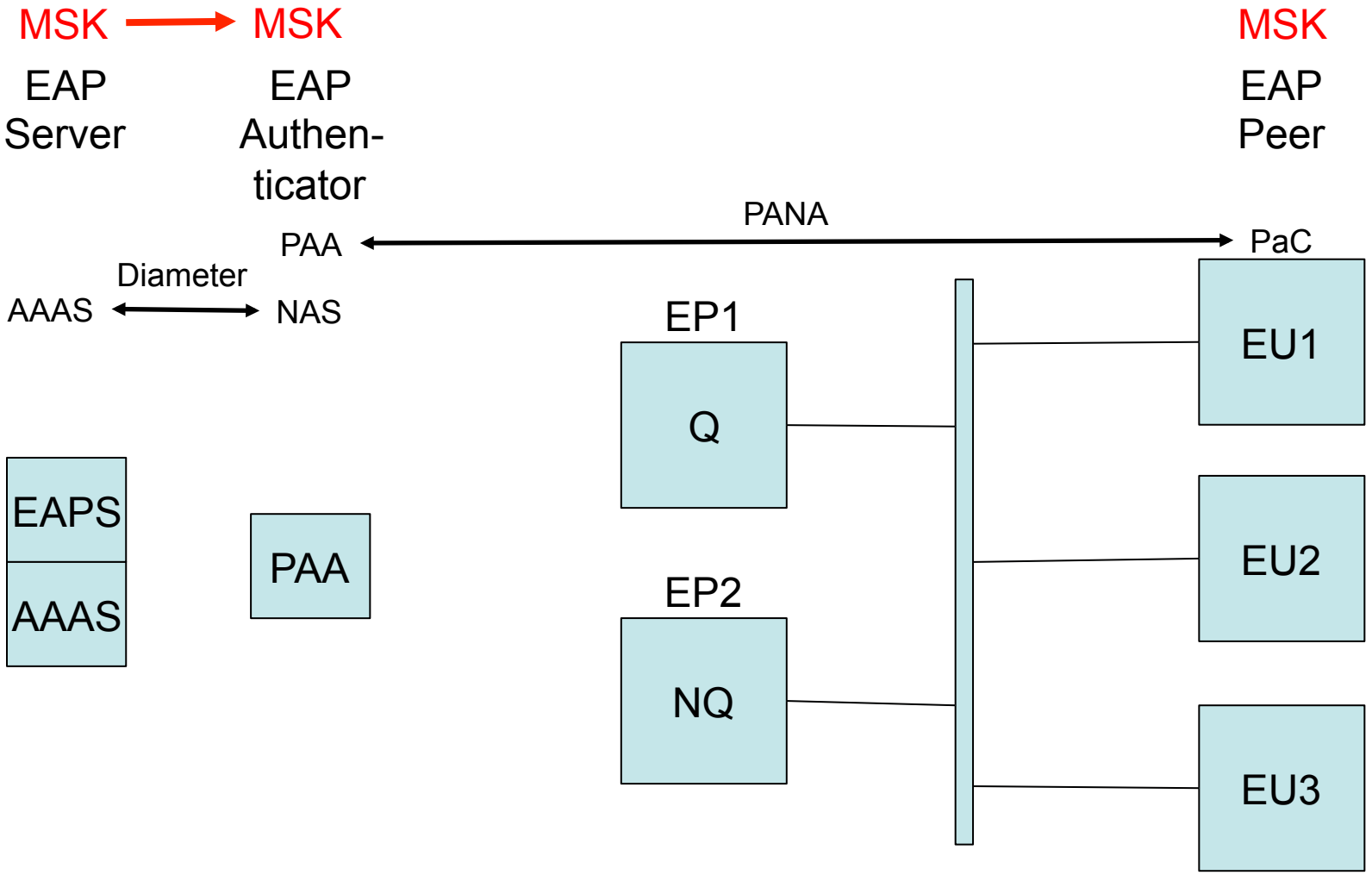
Master Session Key

- From EAP negotiation, a Master Session Key (MSK) becomes known to the EAPS and the EU.
- The EAPS forwards a copy to the PAA using Diameter.

EAP: MSK


MSK
EAP Server
EAP Authen-ticator
MSK
EAP Peer
PANA
PAA
PaC
Diameter
AAAS
NAS
EP1
Q
EU1
EAPS
AAAS
PAA
EP2
NQ
EU2
EU3

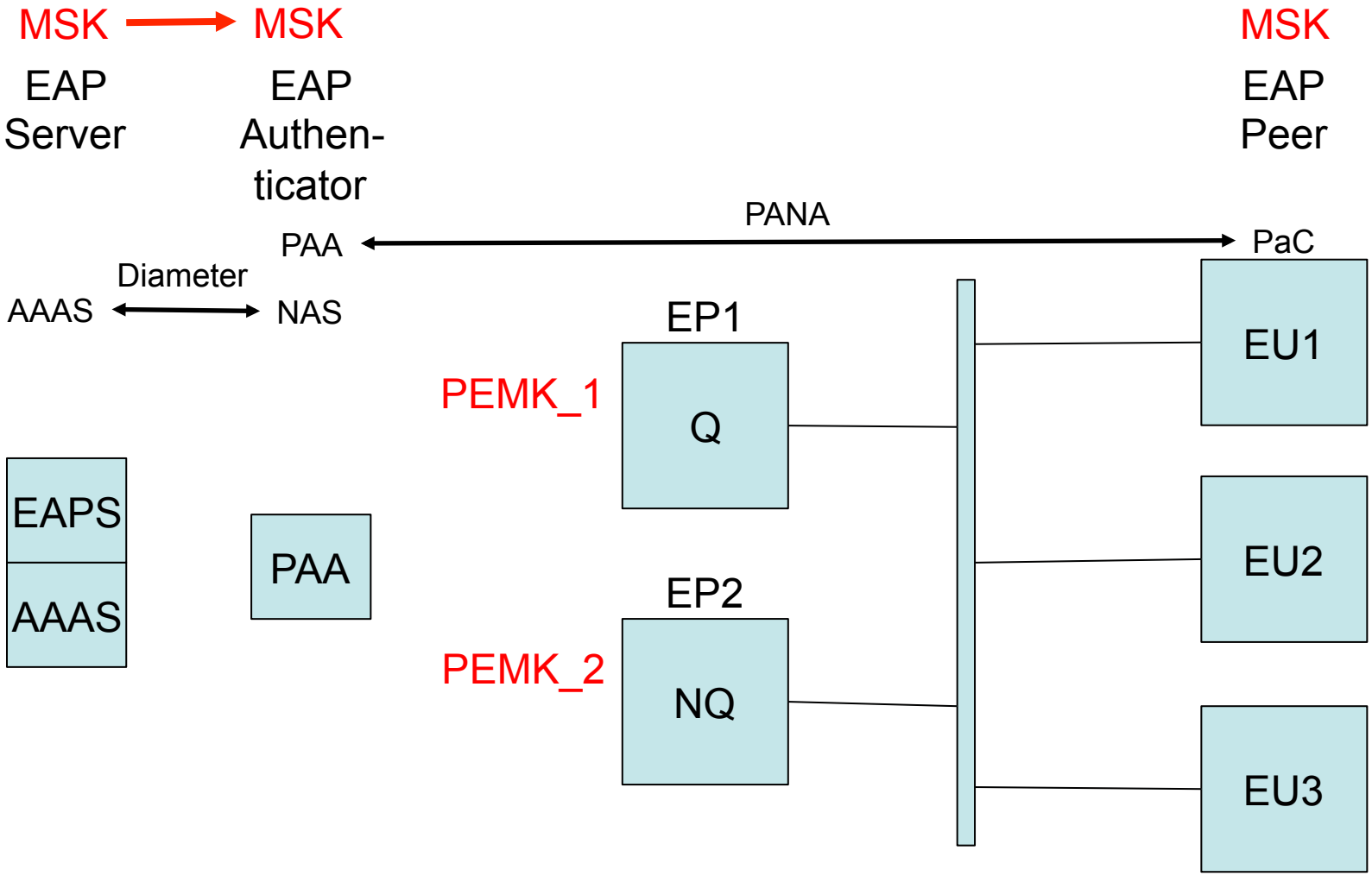
EAP: MSK copied to PAA



PaC-EP Master Key

- The PAA uses the MSK and EP-specific information to compute a PaC-EP Master Key (PEMK) for each EP.
- It sends the corresponding key to each of the EPs, along with information identifying the multicast group and the EU address.
- The rules for computing the PEMK are specified in RFC5807.

PAA sends PEMK to EPs



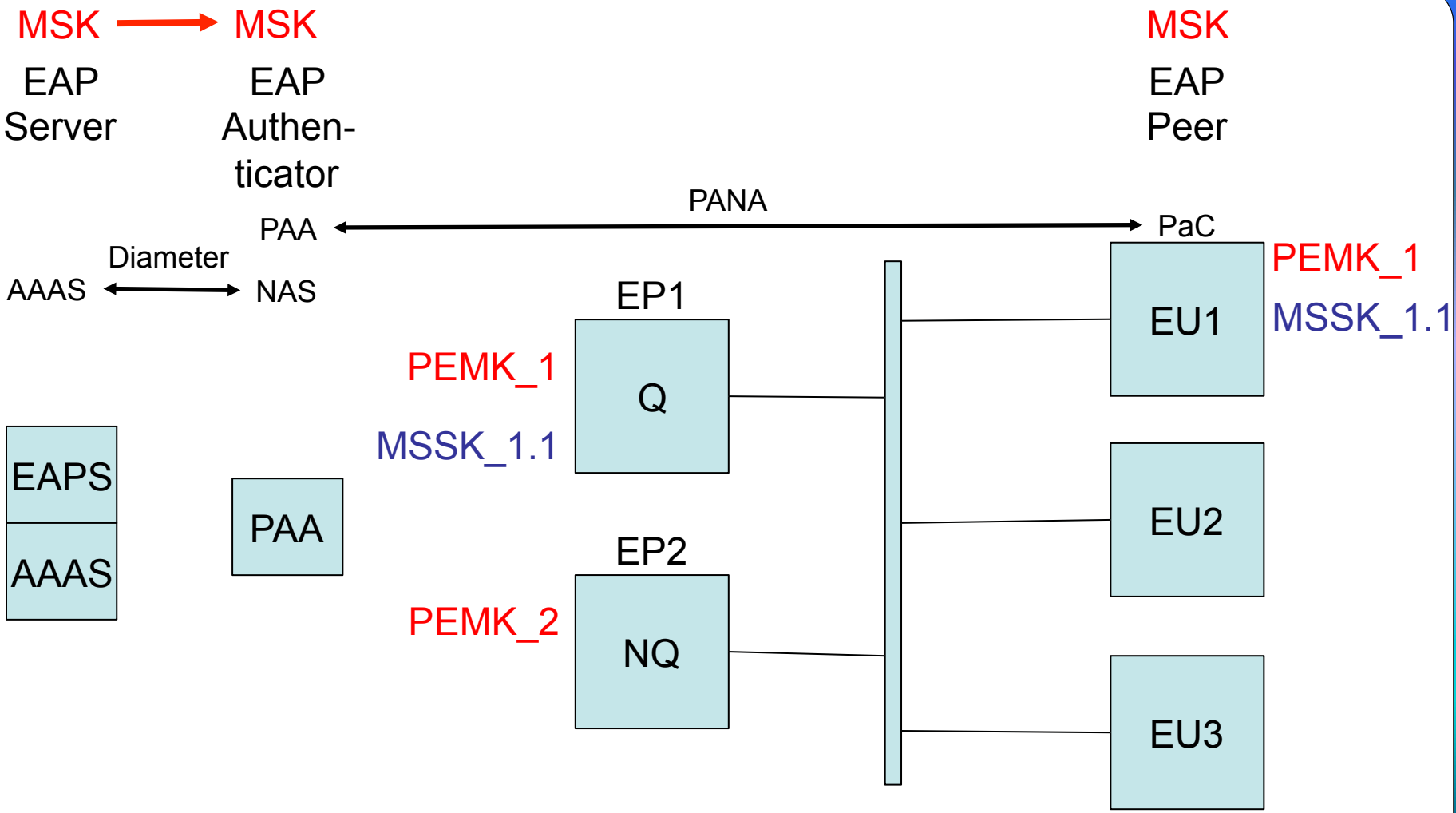
Multicast Session Specific Key - EP

- The two PEMKs are different, because the IP address of the two EPs is different.
- The MSK is ***not*** sent, so validation of an End User must use an additional derived key.
- Each EP combines its PEMK with information about the EU address and the specific multicast session, to produce a Multicast Session Specific Key (MSSK).
- This key is located, when needed, by indexing on the EU address.

Multicast Session Specific Key - EU

- At the EU, given that the EP is known to be Q, and given the MSK and the specific multicast group, the EU can calculate the same MSSK.
- The EP and the EU now have a shared key that they can use to establish the EU's right to join the multicast group.
- These calculations cannot be done at the time when the MSK becomes known to the EU, because the EAP software does not know the address of the Q. Therefore, they have to be done within GSAM.

EPs compute MSSK; EUs compute PEMK and MSSK



Another End User

- If End User EU2 joins the group, it will have a different MSK, say MSK_2.
- As a result, the PEMK computed by the PAA will be different, say PEMK_2.
- The MSSK will reflect this new PEMK, and the IP address of the EU2, so it will differ from the MSSK for EU1.
- The purpose of these MSSKs is to provide ***authorization*** for EU1 and EU2 to join the (network level) multicast group

Multicast Security Associations for Secure IGMP

- Many distinct Multicast Security Associations are required on each network segment:
  - One with Q as the sender, and NQ plus the admitted members as receivers
  - One for each legitimate participant EU, with the EU as the sender, and NQ plus Q as the receivers
  - All are uni-directional, as defined in RFC5374
- These are negotiated using GSAM, and used by Secure IGMP (SIGMP) for IPv4 (or Secure MLD, for IPv6)

GSAM

- Group Security Association Management (GSAM) protocol
- It solves three problems:
  - Determining the keys for the GSAs
  - Determining the Security Parameter Index to use
  - Distributing the keys and the SPIs to the participants who need them
- GSAM is triggered when an “Unsolicited Report” is sent for the first time from an EU towards Q

Assumptions

- The routers in a shared-medium LAN can authenticate and authorize each other.
  - Same administrator
- The participants can distinguish a secure group from an open group
  - Details are for future study
- There is a shared key between the EP and the EU
  - See next slide…

Shared Key

- The EP can compute the MSSK for a particular EU and group, immediately after it has received the PEMK from the PAA.
- The EU, once it has finished the EAP exchange, knows the MSK, but does not know the location of Q (i.e., the EP).
- EP stores MSSK in its GPAD as a credential.
- EU stores MSK in its GPAD as a credential.
- EU must rely on GSAM to compute the MSSK when it executes.

GSAM Operation

- Q accepts registrations from EUs using the MSSK as a credential.
- Q accepts registrations from NQs (if any exist) using administrator-defined credentials.
- Q determines the keys to be used and the SPIs.
- Q distributes the keys and the SPIs.
- If any of (EUs, NQs) objects to the SPI, all parties negotiate, and Q distributes the result.

Results

- Secure Authentication of the End User
- Authorization is then possible using standard AAA interactions within the NSP
- A shared key is generated, which can be used to derive the necessary keys for protecting the (secure) IGMP/MLD exchanges

Documents Issued (mboned)

- MRAC Requirements
  - draft-atwood-mboned-mrac-req
- MRAC Architecture
  - draft-atwood-mboned-mrac-arch
- Using PANA+EAP to achieve the MRAC
  - draft-atwood-mboned-pana

Documents Issued (pim)

- Secure IGMP
  - draft-atwood-pim-sigmp
- GSAM (coordination of Secure IGMP end points)
  - draft-atwood-pim-gsam

Documents: To Come

- Secure MLD
  - draft-atwood-pim-smld

Next Steps

- Request for feedback on the entire suite of documents
- On either the MBONED list or the PIM list, or off-list

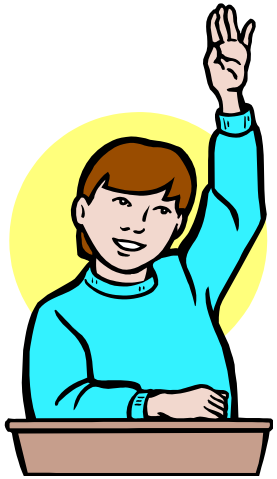
Implementation

- Based on OpenDiameter, which provides:
  - Diameter
  - PANA
  - EAP-TLS
  - We improved/updated this code.
  - We added EAP-FAST
- The code for GSAM is based on Racoon
- The code for SIGMP is based on the Linux Kernel implementation of IGMP, but is not yet complete.

Implementation

- The updating for OpenDiameter was recently uploaded to the SourceForge site, as version 1.0.7j.
- The improvements (EAP-FAST) were uploaded as version 1.0.8.

Thank You!



Questions?