IETF90-PIM

Secure IGMP/MLD
Group Security Association Management

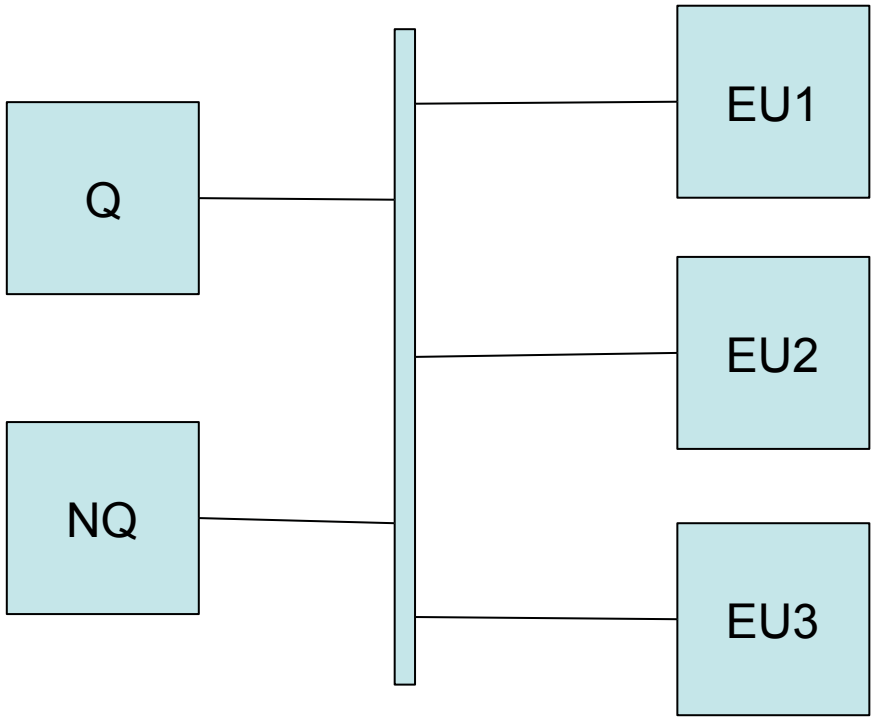
draft-atwood-pim-sigmp
draft-atwood-pim-gsam
draft-atwood-mboned-mrac-req
draft-atwood-mboned-mrac-arch

J. William Atwood
Bing Li
Concordia University, Montreal

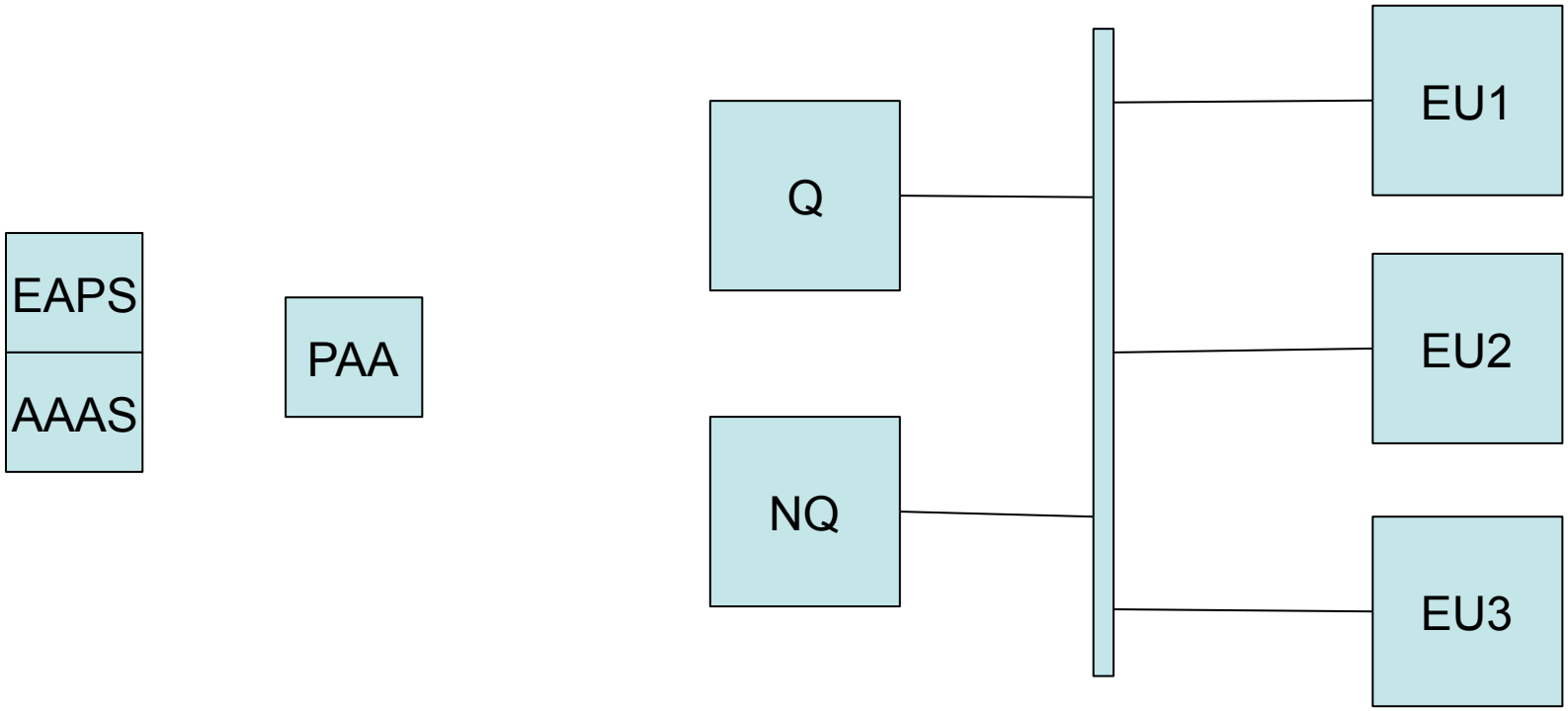
Overview

- Exploring the area of Receiver Access Control for IP Multicast
  - Subtitle: Making money using IP Multicast
  - MBONED: “application” level drafts
  - PIM: “network” level drafts
- Secure IGMP was presented at IETF 88
- This presentation is about key management for Secure IGMP
  - A new coordination protocol: GSAM

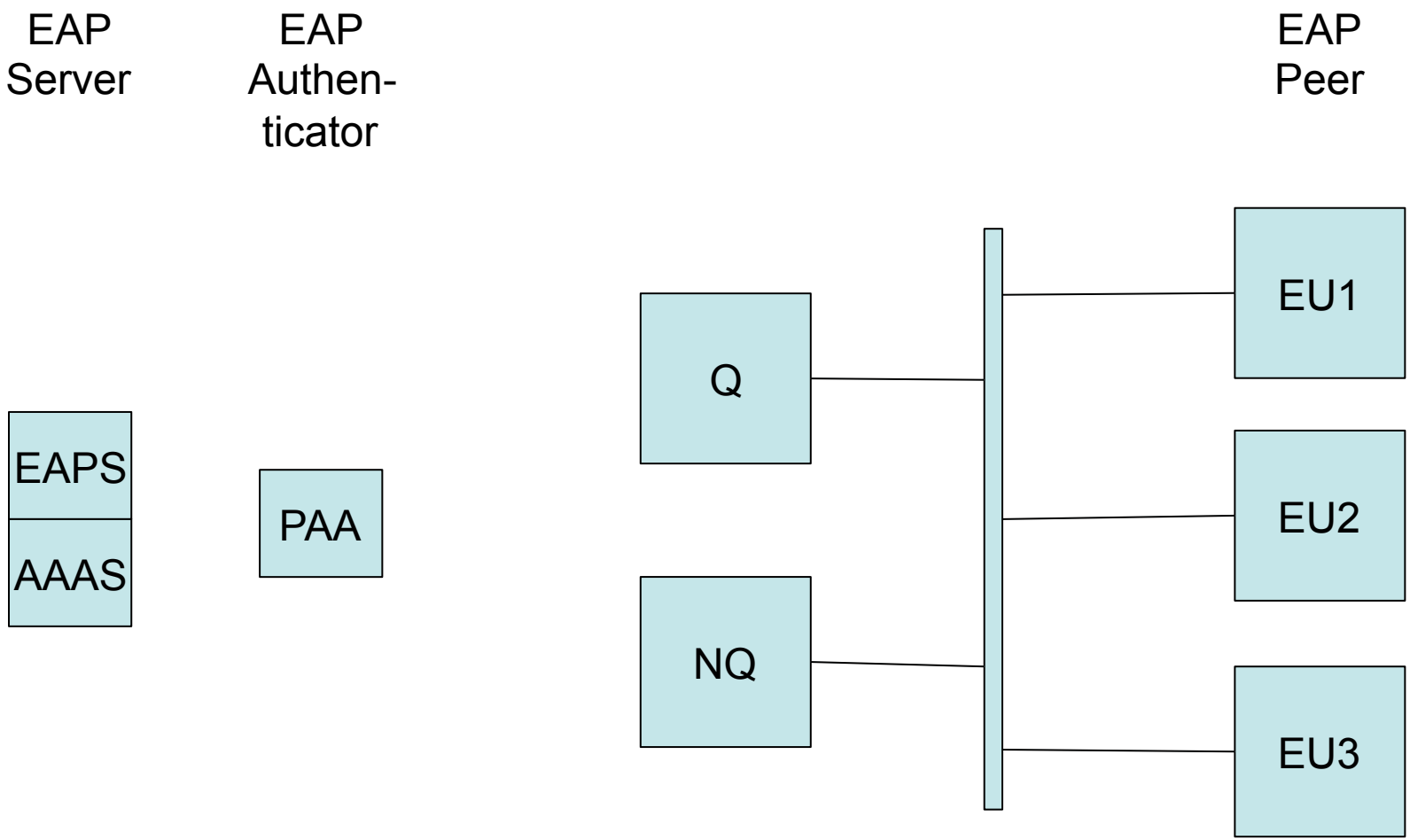
Environment: Network Segment for Multicast



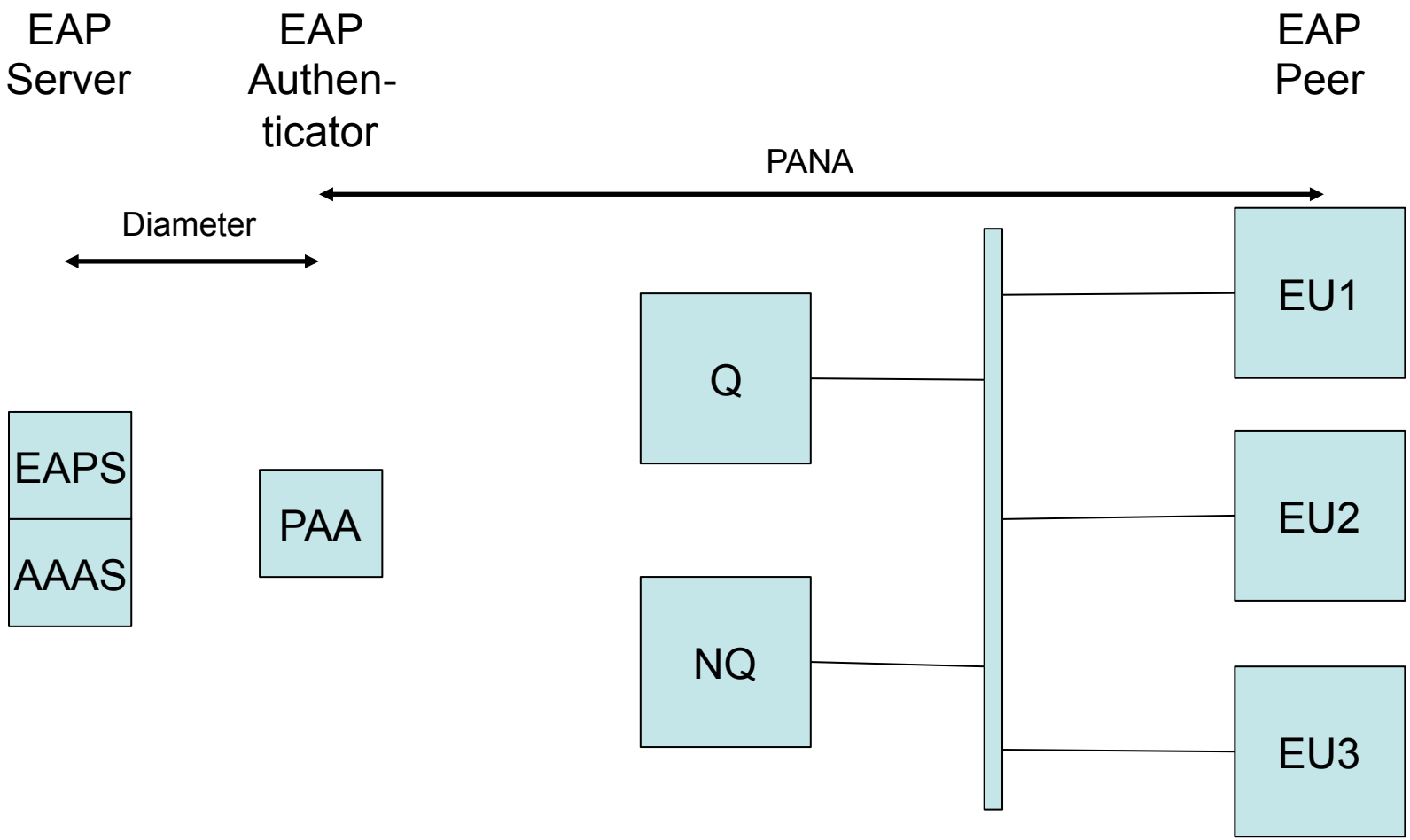
Environment: Add EAPS and PAA



Environment: Locate EAP participants



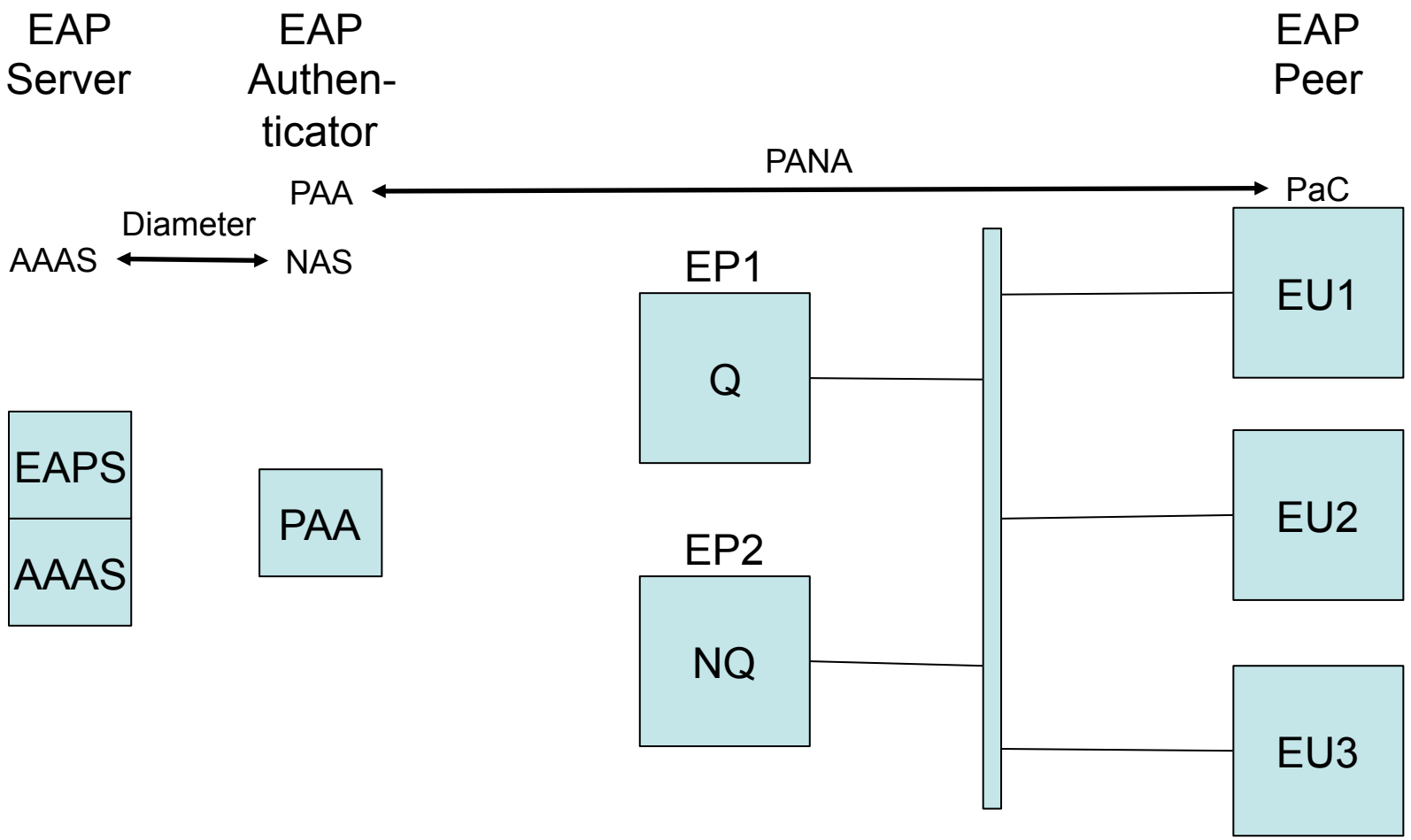
Environment: Show EAP Transport



Enforcement Points

- The PAA is the negotiator for one end of the PANA session
- In general, it 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.

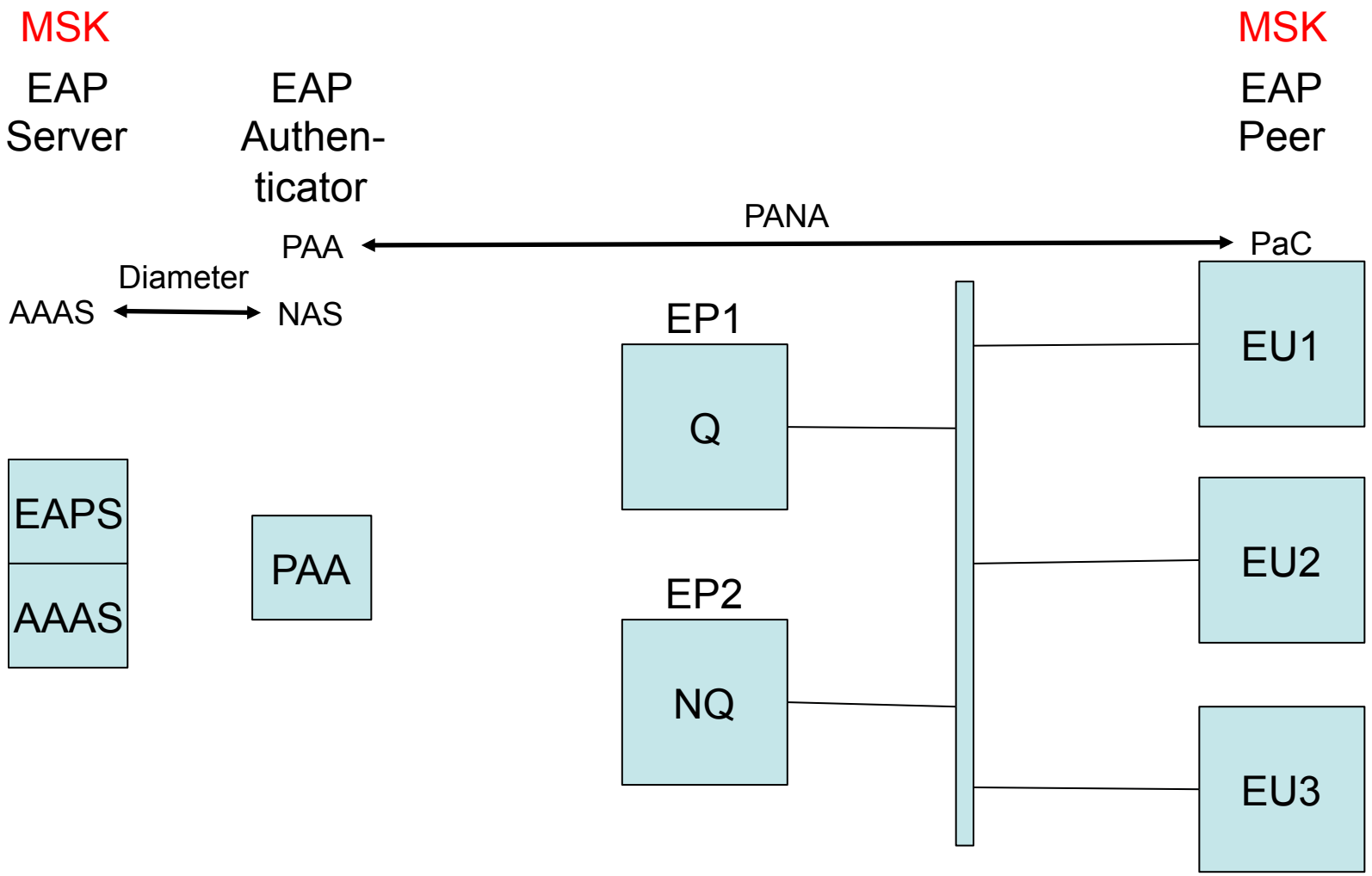
Environment: Show EPs



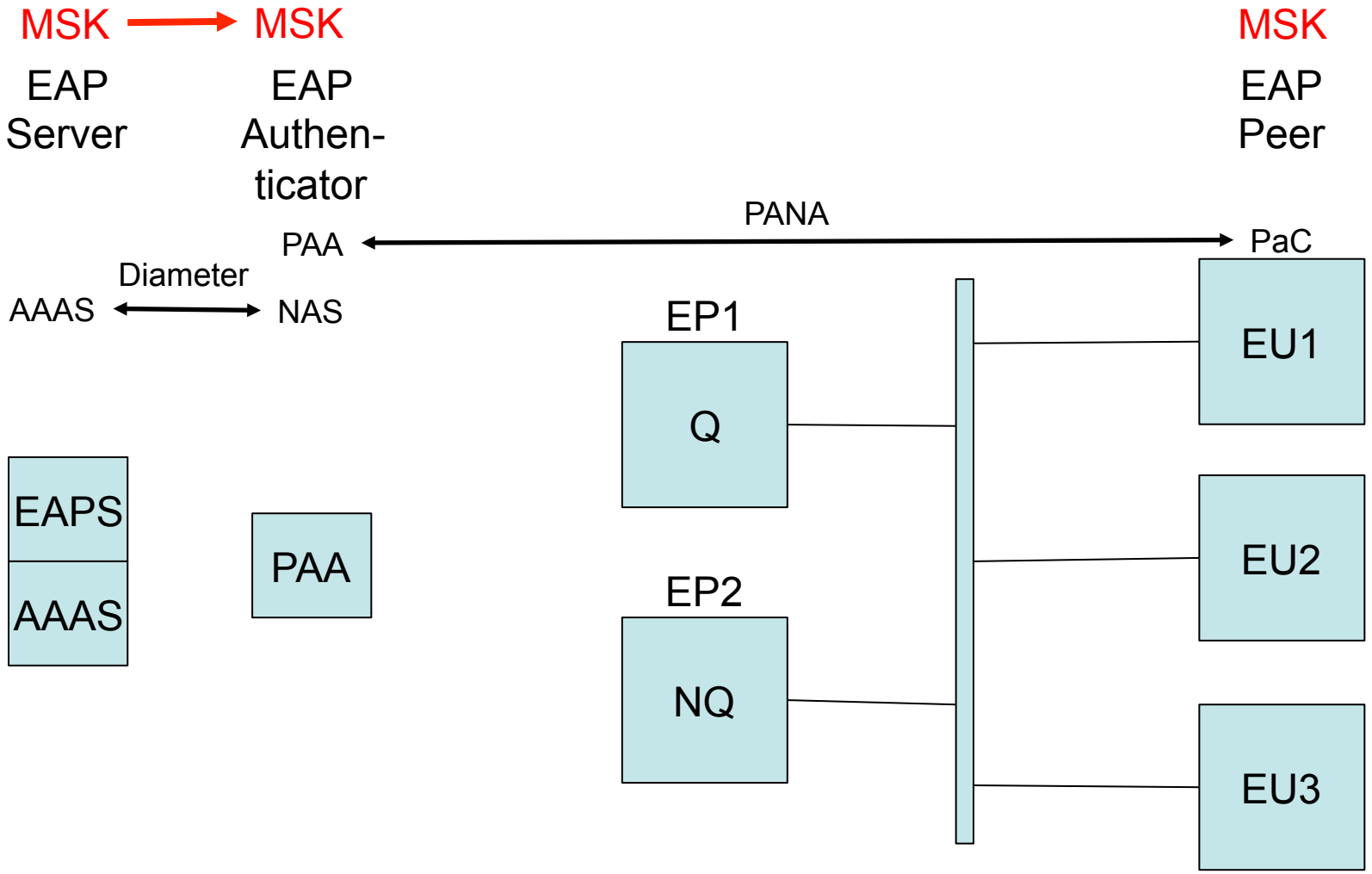
Master Session Key

- 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

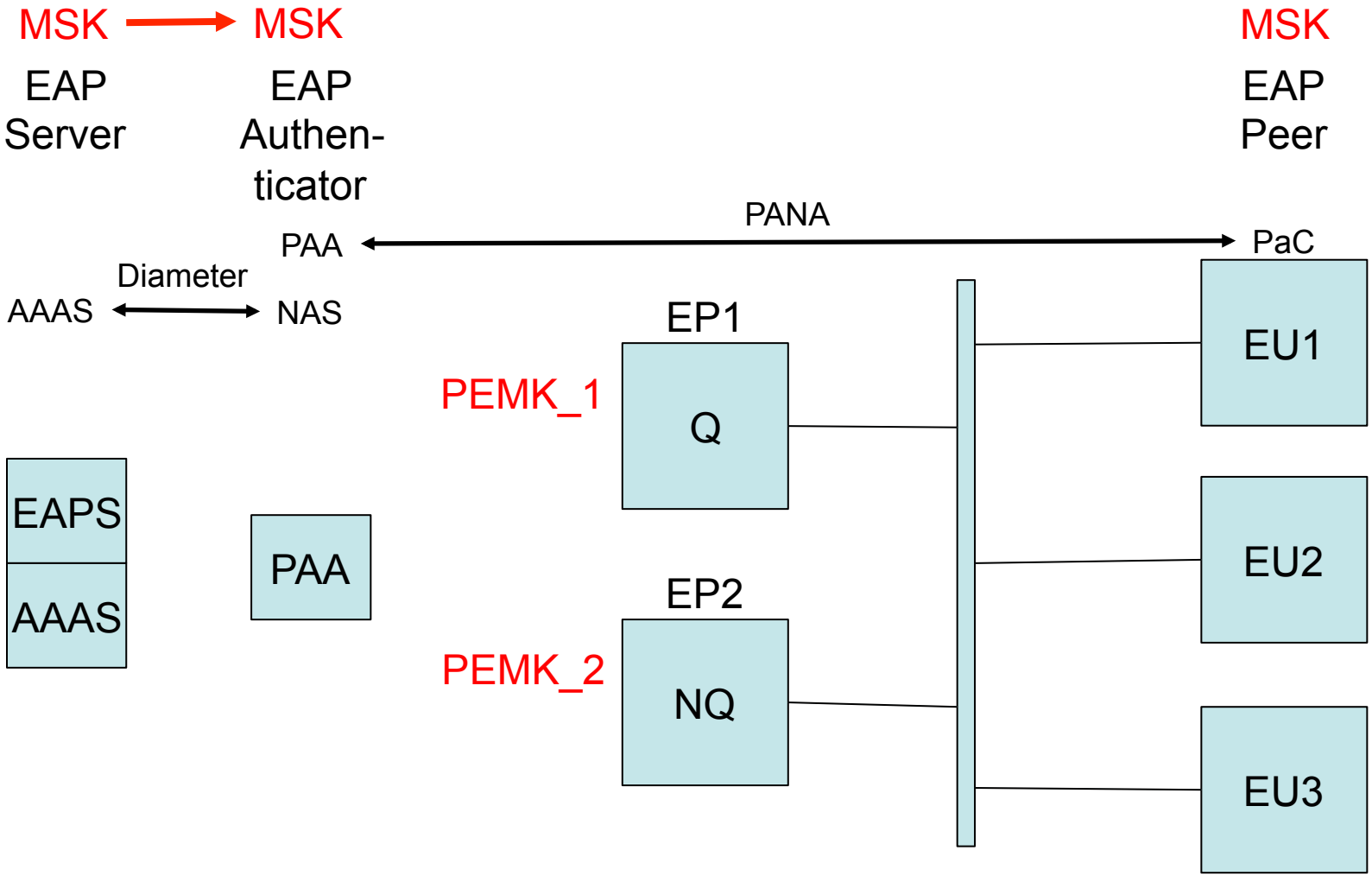
EAP: MSK copied to PAA



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.

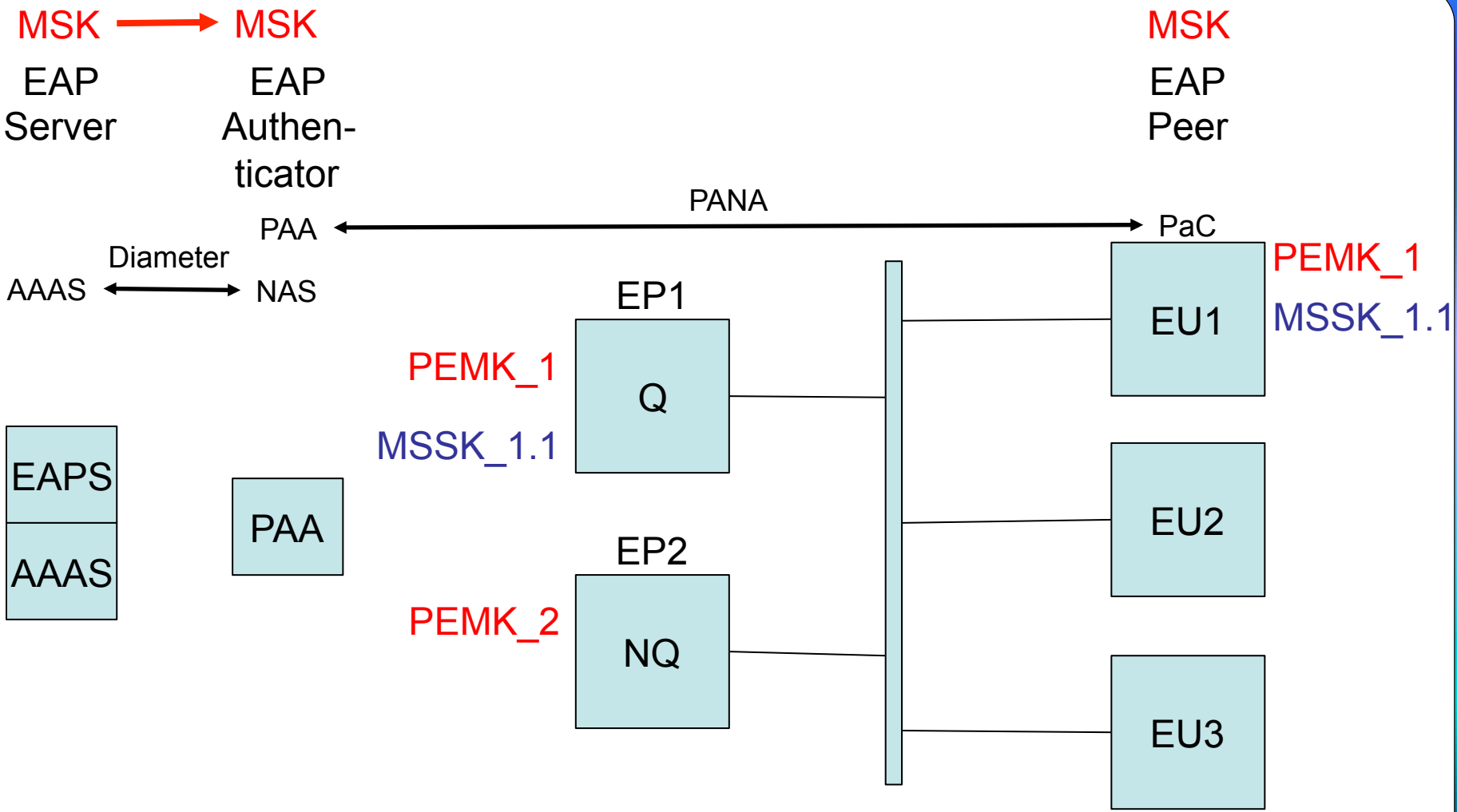
PAA sends PEMK to EPs



Multicast Session Specific 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).
- 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.

EPs compute MSSK; EUs compute PEMK and MSSK



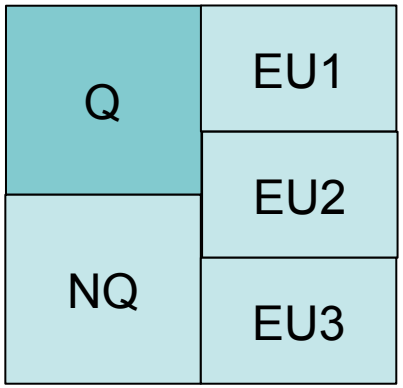
Open vs Secure Groups

- 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

Multicast Security Associations for Secure IGMP

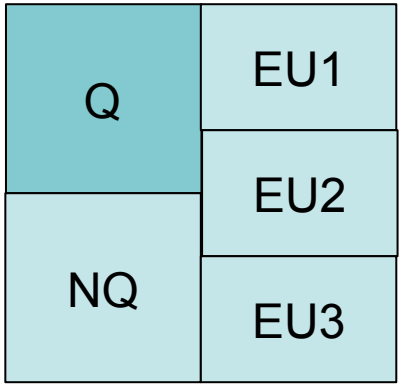
- Many distinct Multicast Security Associations are required on each network segment:
  - One with Q as the sender, and NQ plus the admitted members as receivers
  - One for each legitimate participant EU, with the EU as the sender, and NQ plus Q as the receivers
  - All are uni-directional, as defined in RFC5374

Unsecure Query



GQ V2, V3

224.0.0.1
No group



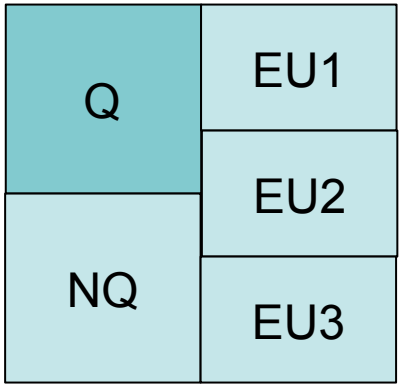
GSQ V2, V3
GSSQ V3

G_IP
Single group

Source

Destination

Secure Query



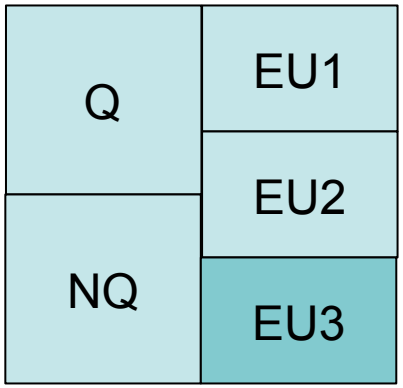
GSQ V2, V3
GSSQ V3
Secure

G_IP
Single group

IGMP v2/v3 Query

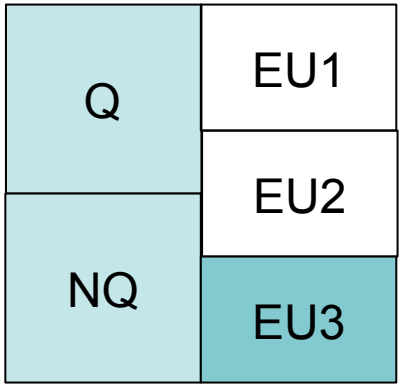
- The GQ is an “open” solicitation, for all groups, and so cannot be secured with information that is specific to one group. So, it has no “secure” form.
- The GSQ (v2 and v3) and GSSQ (v3 only) are specific to a group, and so can be secured with parameters that are specific to that group. No change is necessary to the packet format; we only need to protect the packet with IPsec.

Unsecure Report



R V2

Unsecure
Suppression
G_IP
Single group



R V3

Unsecure
NO suppression
224.0.0.22
Multiple groups

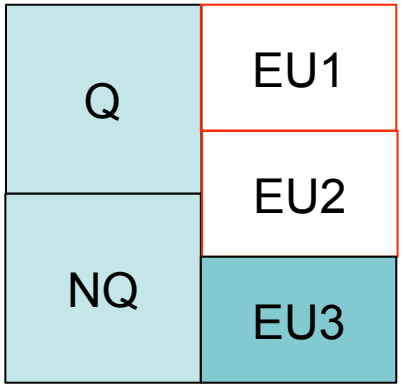
IGMP v2/v3 Report

- The details of the v2 report and the v3 report are quite different, because different design decisions were made on how to minimize traffic:
  - In v2, a Report contains only information about one group, but identical reports from other hosts should be suppressed.
  - In v3, multiple groups may be contained in a single Report, which is sent to a common address (224.0.0.22)

Secure IGMP v2/v3 Report

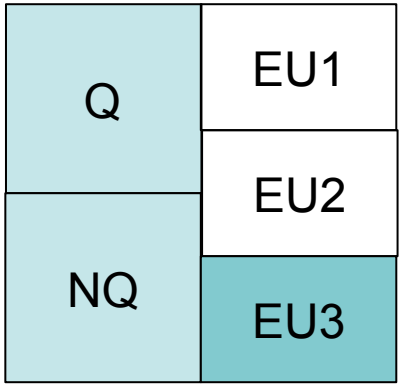
- Since the cryptographic protection must of necessity be specific to a group,
  - We cannot use address 224.0.0.22
  - We cannot have multiple groups in a Report message
- We are interested in minimum change to IGMP
  - Our solution requires no change to the packet format
- We are interested in maximum compatibility
  - Our solution does not change the semantics of IGMP for “open” groups

Secure Report



R V2

Secure
NO suppression
G_IP
Single group



R V3

Secure
NO suppression
G_IP
Single group

Three problems

- We need to solve three problems:
  - Determining the keys for these GSAs
  - Determining the Security Parameter Index to use
  - Distributing the keys and the SPIs to the participants who need them
- Group Security Association Management (GSAM) protocol
- It 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
  - Already shown

NQ registers with Q

- NQ has to establish a secure path to Q
  - QSAM_INIT (c.f. IKE_SA_INIT)
  - QSAM_AUTH (c.f. IKE_AUTH)
  - Based on the administratively-assigned authorization mechanism

EU registers with Q

- Before actually sending the first unsolicited report, the EU must negotiate the GSAs using GSAM.
- EU has to establish a secure path to Q
  - QSAM_INIT
  - QSAM_AUTH
  - Based on the MSSK shared with its EP (i.e., with Q)

Q creates a pair of GSAs

- GSA_q is for outgoing queries from Q
- GSA_r is for incoming reports from EU
- Q decides on the SPI to be used for each of these GSAs.
- Q distributes the two GSAs and the two SPIs to the EU, and to the NQ.
- If the incoming SPI on the EU would cause a conflict, the EU can reject the assignment and force a joint determination of the appropriate SPI

Another EU joins

- EU2 goes through the same steps
  - GSAM_INIT
  - GSAM_AUTH
- Q must re-do the establishment of GSA_q and GSA_r, and re-distribute the result to NQ, EU1, and EU2
- EU1 and EU2 must start using the new GSAs

Differences between GSAM and GDOI

- GDOI delivers only keys for a single Group Security Association
- GDOI assigns SPIs arbitrarily
- GSAM delivers computed keys and negotiated SPIs, for two related GSAs
- The GCKS in GDOI is administratively determined; in GSAM it is the Q
- The special needs of an NQ (if present) are accounted for
- GSAM is link-local, so it scales well

Documents: Issued

- MRAC Requirements
  - draft-atwood-mboned-mrac-req
- MRAC Architecture
  - draft-atwood-mboned-mrac-arch
- Secure IGMP
  - draft-atwood-pim-sigmp
- GSAM (coordination of Secure IGMP end points)
  - draft-atwood-pim-gsam

Documents: To Come

- Using PANA+EAP to achieve the MRAC
- Secure MLD

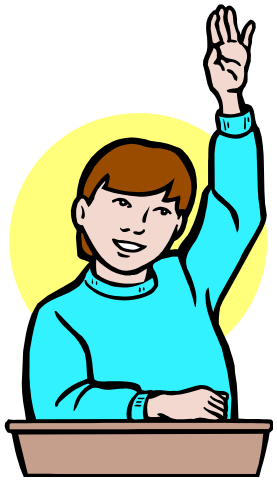
Acknowlegment

- Salekul Islam contributed significantly to mrac-req and mrac-arch

Next Steps

- Request for feedback (on the list or elsewhere)
- Eventual adoption of all three -pim documents as WG documents

Thank You!



Questions?