

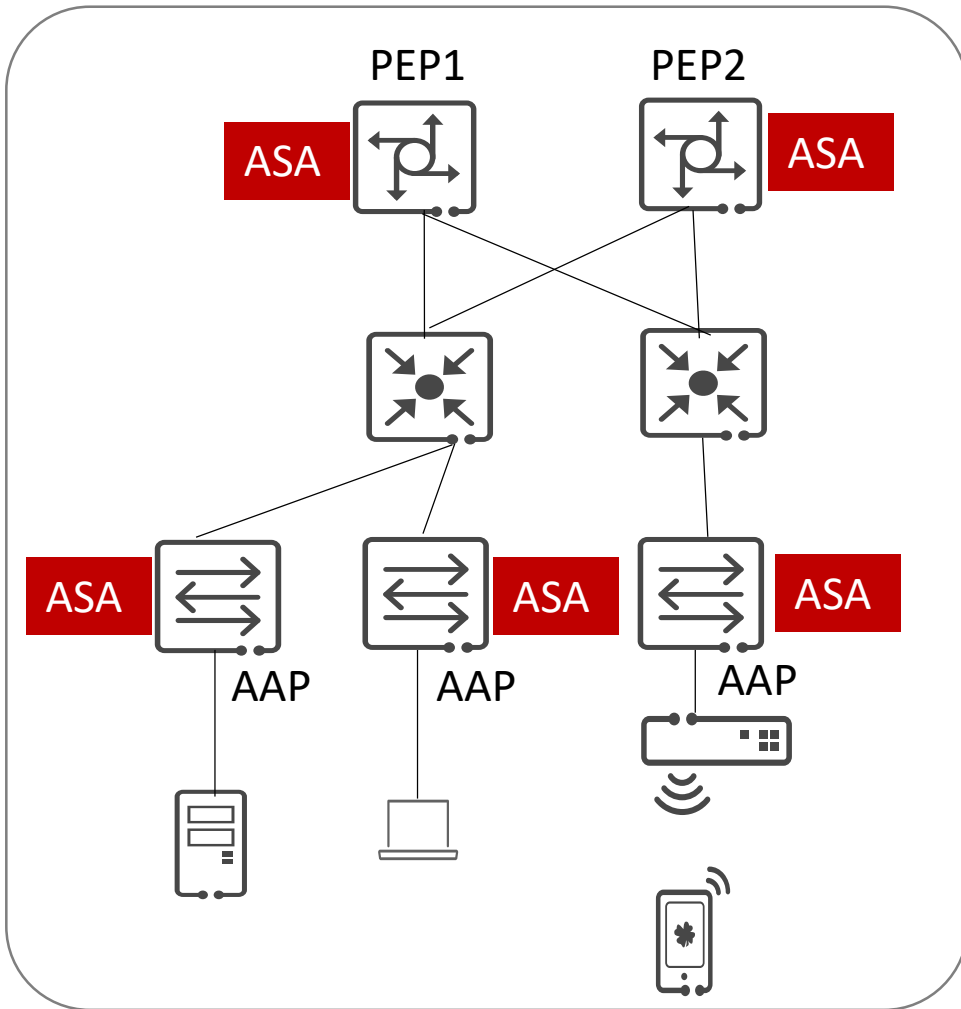
# Autonomic IP Address to Access Control Groups Mapping

draft-yizhou-anima-ip-to-access-control-groups

Presenter: Yizhou Li

IETF112

# Recap –basic idea



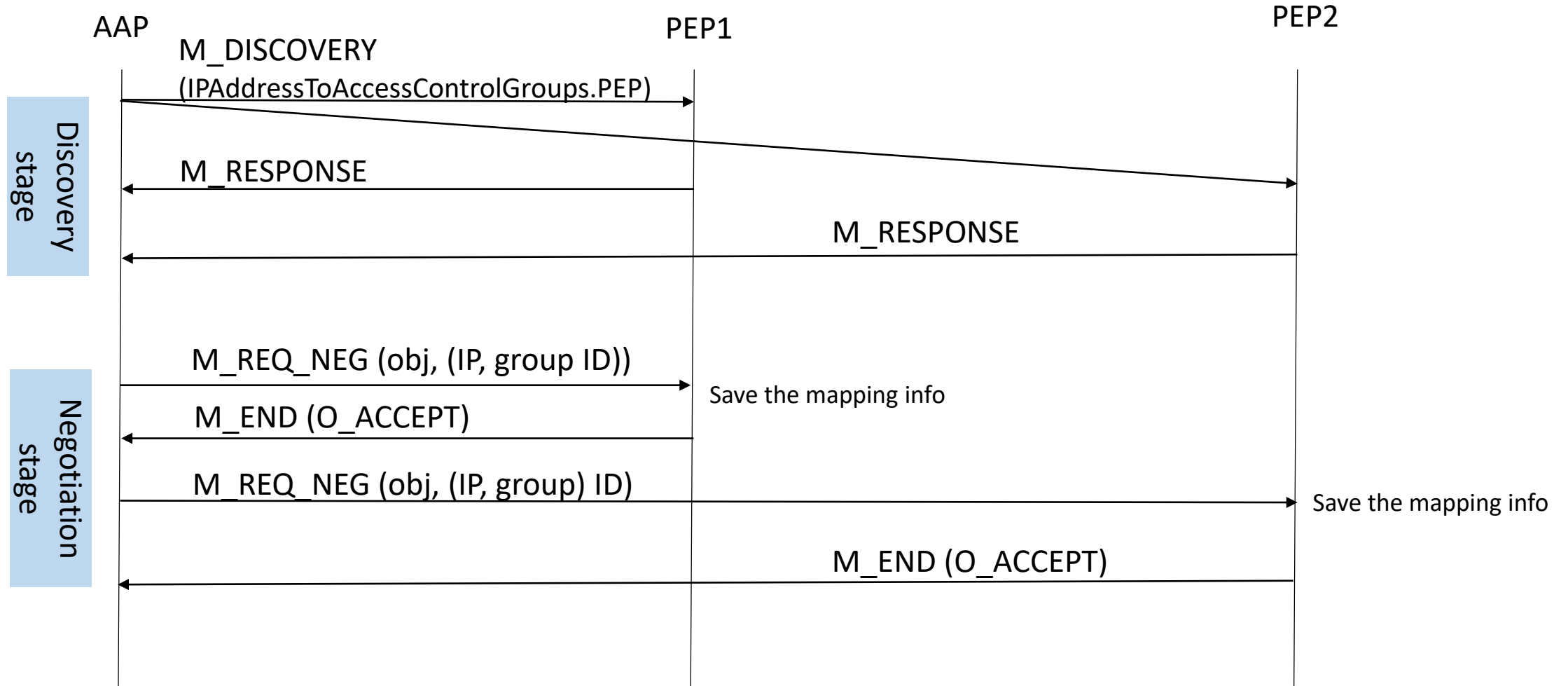
- Group based policy is becoming more commonly deployed.
- IP address to Group ID mapping information needs to be passed to access authentication point (AAP) to policy enforcement points (PEP).
- New GRASP objective "IPAddressToAccessControlGroups" is defined to carry this information
- This objective is used by ASA called IPAddressToAccessControlGroups.

# Changes from last version

- Give a name to the ASA which uses the new defined objective so that the text is easier to understand
- Clarified the terms PEP and AAP. Basically PEP and AAP are different “roles”.
- Clarified that PEP node can be the info provider to other PEP because in such case it is equivalent to a conceptual AAP to the requesting PEP.
- Other editorial changes

# AAP provides the mapping info to PEP

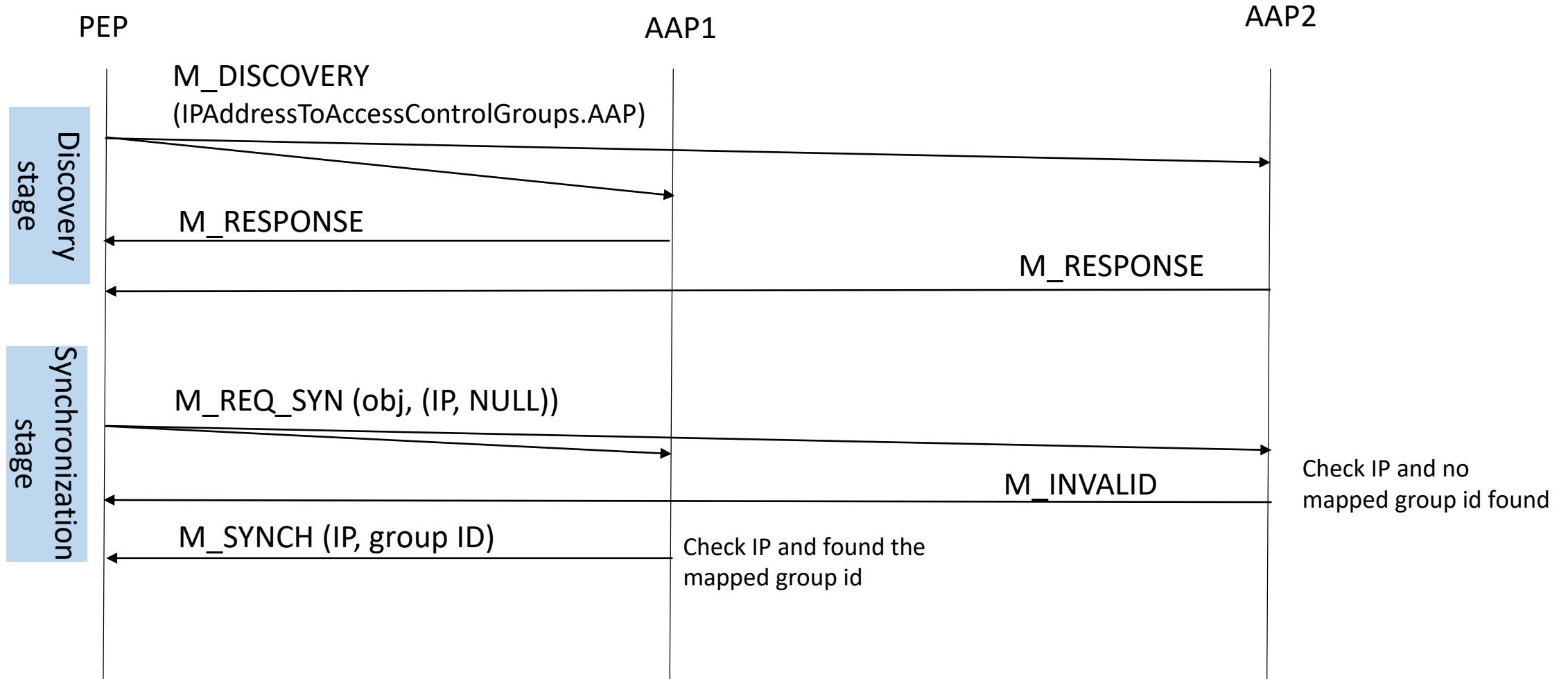
obj is short for  
"IPAddressToAccessControlGroups.PEP"  
Objective



This is the regular case that an AAP pushes the mapping information to PEPs.

# PEP asks for the mapping info from AAP

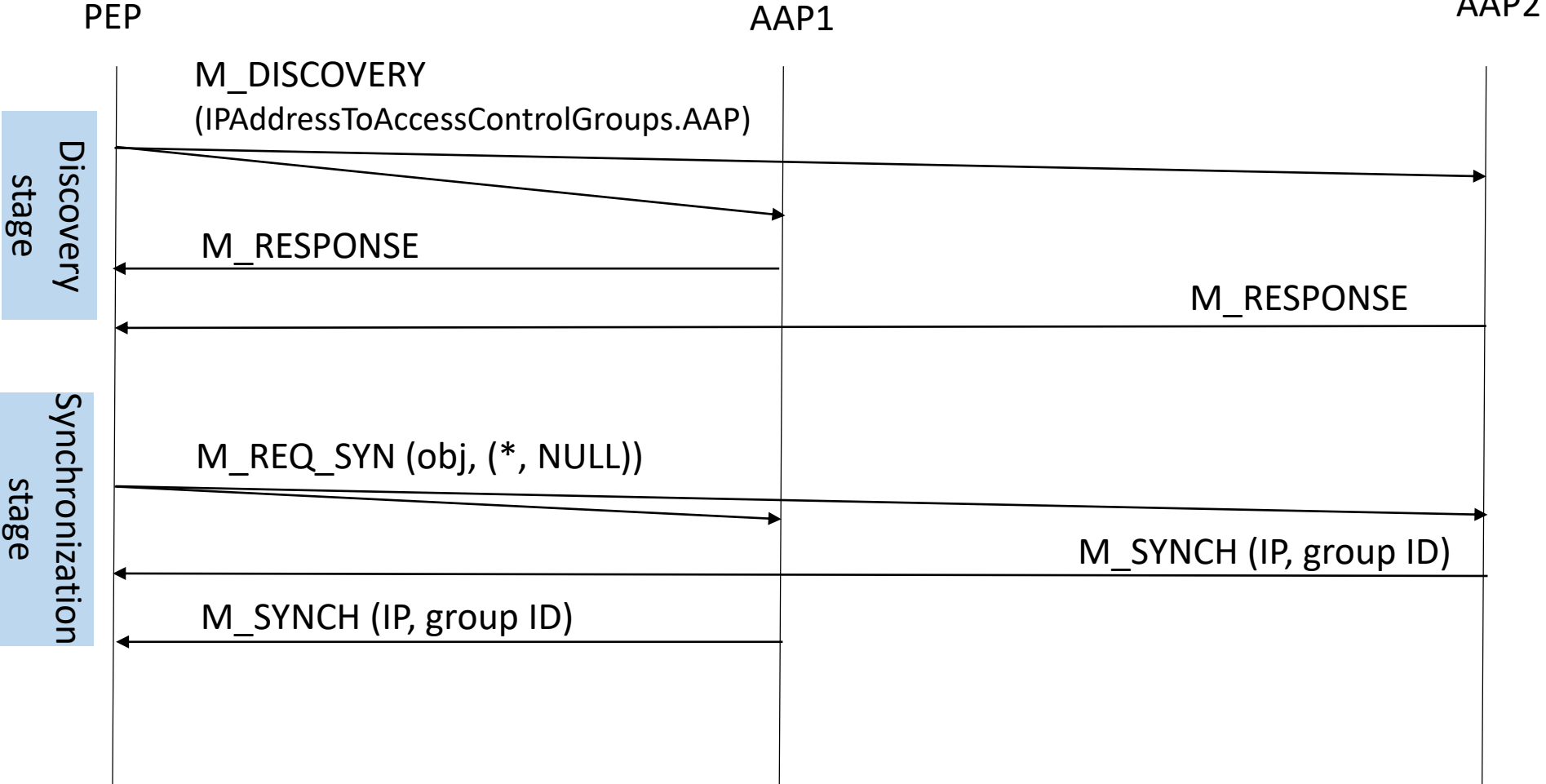
obj is short for  
"IPAddressToAccessControlGroups.AAP"  
Objective



This is the not-so-common case that an PEP asks for the mapping info, say when the mapped group info is not pre-stored upon receiving a pkt.

# A new PEP joins

obj is short for  
"IPAddressToAccessControlGroups.AAP"  
Objective



A new PEP gets the mapped info from AAPs.

# Comments from and off the list to be incorporated to draft

- Change the conveying message from the Unsolicited Synchronization to Negotiation to allow the AAP pushes the mapping info to PEPs
  - To avoid TCP long connection problem
- Allow the discovery message in rapid mode to accelerate the procedures
- “Role” to be used so that the ASA can better decide the counterparts to communicate. The “role” is for the purpose of multiplexing the objective name, i.e. “IPAddressToAccessControlGroups.AAP” and “IPAddressToAccessControlGroups.PEP”

# Next Steps

- Revise the draft accordingly and upload the draft when channel re-opens
- Authors would like to call for adoption on next revision