Autonomic IP Address to Access Control Groups Mapping

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

Presenter: Yujing Zhou

Yizhou Li, Li Shen, Yujing Zhou

ANIMA WG

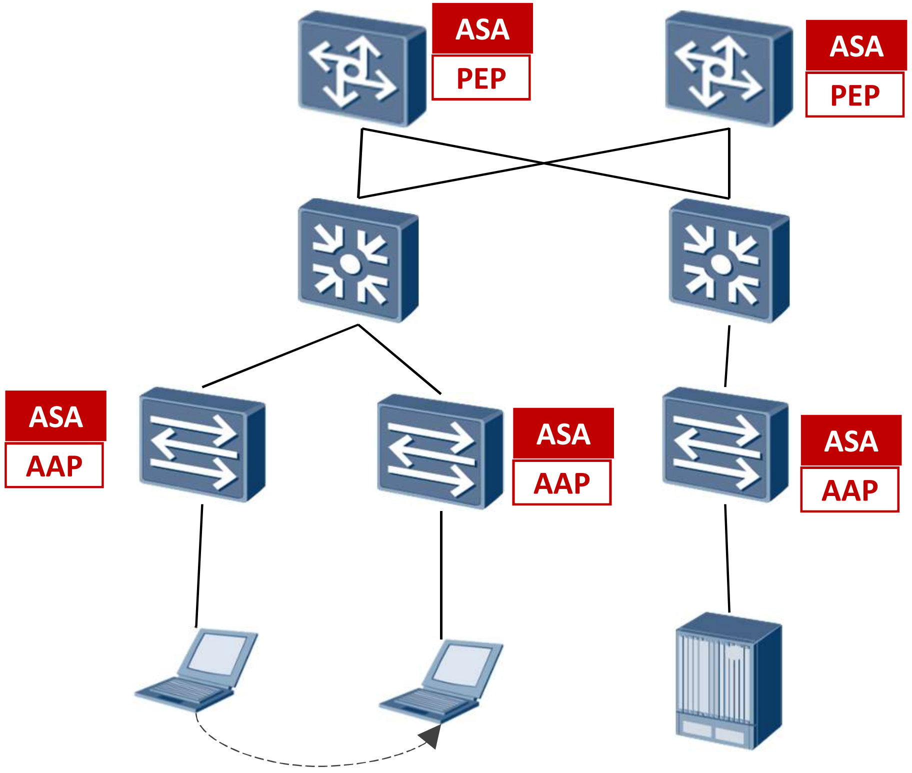
IETF-113 : March 2022, Online

Recap – basic idea

Terminology:

AAP: Access Authentication Point.

PEP: Policy Enforcement Point.



A user's laptop may change access point which is assigned a different IP. But user want to obtain the same network service.

- With the increasing deployment of wireless accessed users and more complicated and dynamic requirements of campus network policy, group based policy is becoming more commonly deployed.
- Group means a number of endpoints connecting to the network that share common network policies. So that users can obtain the same network access permission and QoS assurance wherever they access the campus network.
- This document defines the autonomic technical Objectives for IP address/prefix to access control group IDs mapping information.

Changes from last version

- Add a figure and example of AAP pushing mapping information to PEP for illustration purpose.
- Use two objective names instead of one to multiplex AAP and PEP roles during discovery phase.
- Change conveying message from unsolicited synchronization to normal Synchronization and Negotiation procedures to avoid long TCP connection.
- Editorial changes to make the text more organized.

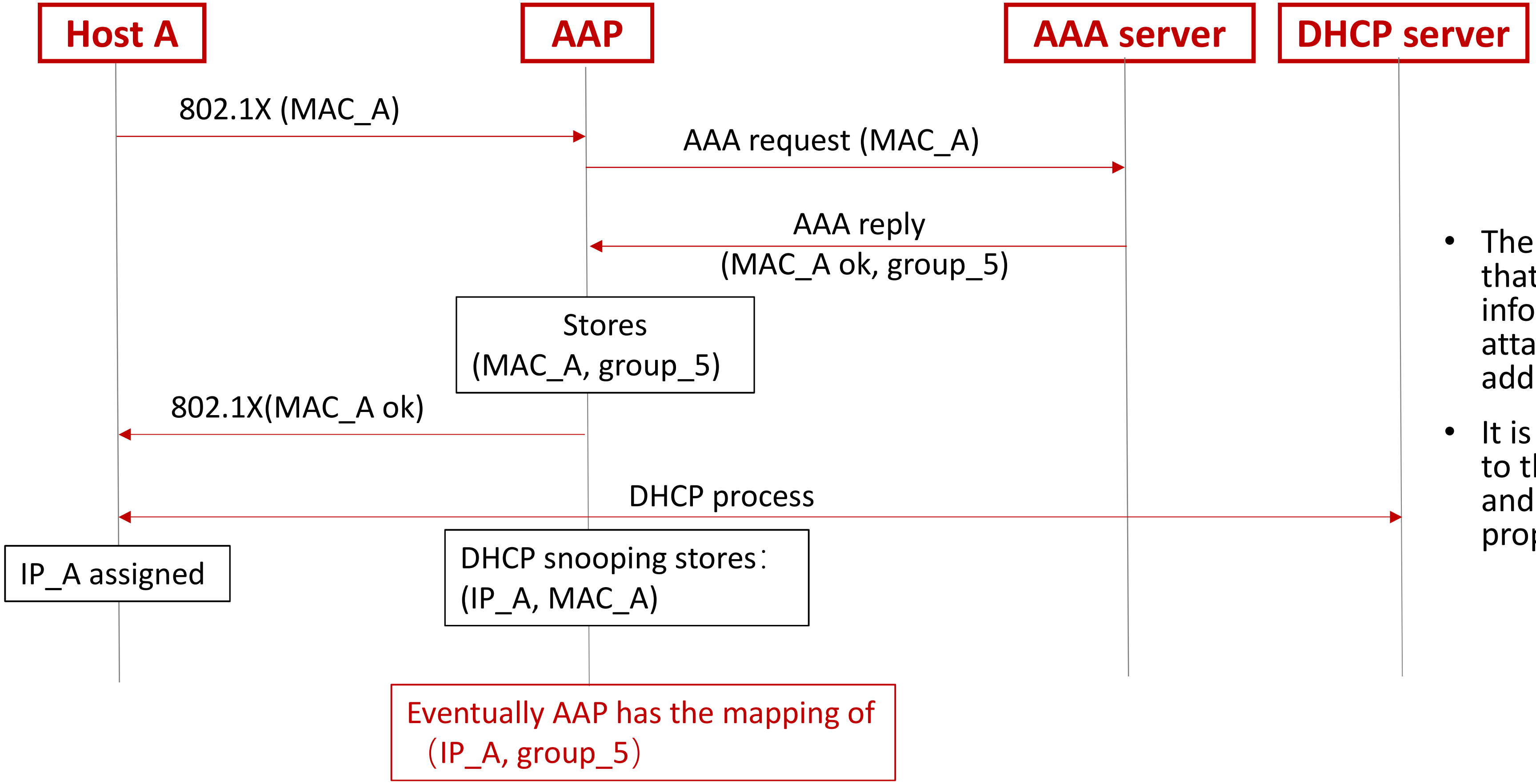
GRASP Objective

- Objective_AAP = ["IpToGroupId.AAP",objective-flags, loop-count,
  [ip-address-or-prefix, *group-id]]
- Objective_PEP = ["IpToGroupId.PEP",objective-flags, loop-count,
  [ip-address-or-prefix, *group-id]]

- group-id = uint
  - A common practice usually uses 16 bits to present a group ID. But the representation does not limit that. Zero group ID represents a NULL group value and is used for full retraction of a prefix or address.

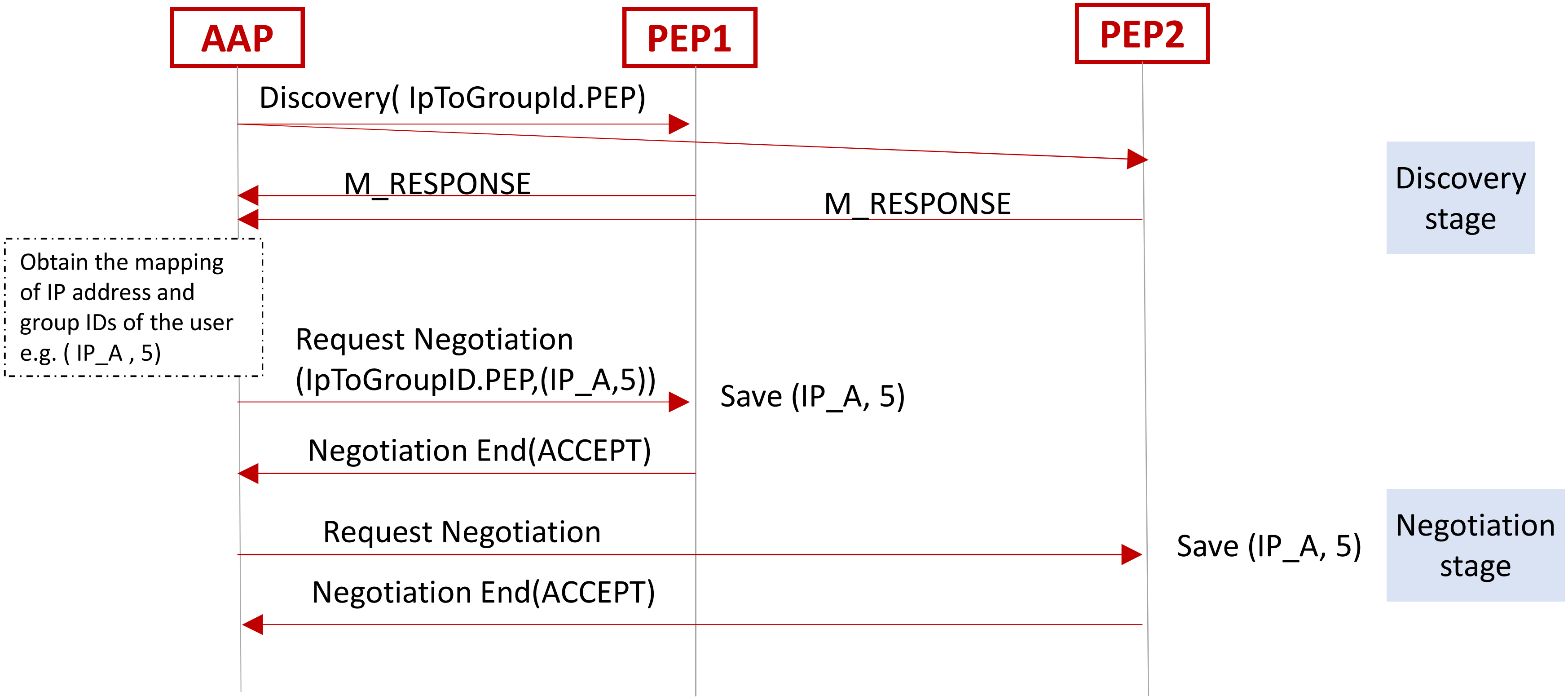
An example on how AAP obtains IP address and group ID mapping info for a host

(not to be standardized)



- There are various ways that an AAP obtains information for an attached host A’s IP address and group ID.
- It is the prior knowledge to the ANIMA objectives and procedures proposed in next page

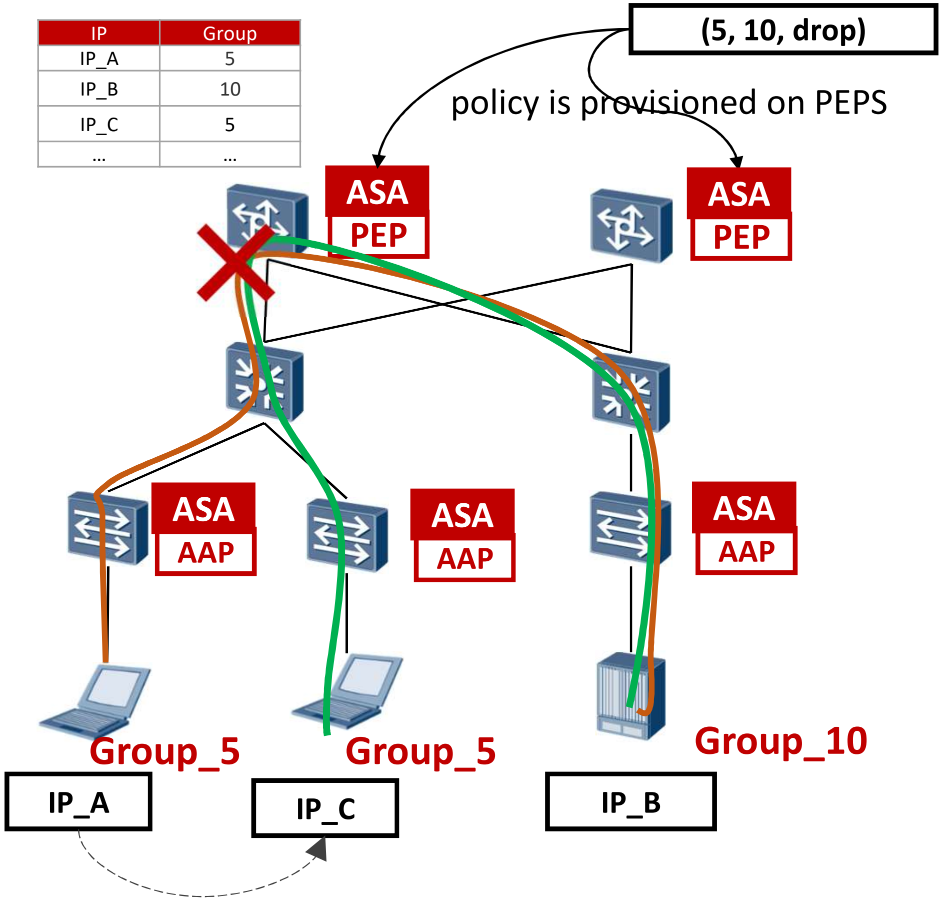
Example of Using the Defined Objective Options



This is an example of AAP pushing mapping information to PEPs.

Example of Using the Defined Objective Options

IP	Group
IP_A	5
IP_B	10
IP_C	5
…	…



(5, 10, drop)

policy is provisioned on PEPS

ASA PEP

ASA PEP

ASA AAP

ASA AAP

ASA AAP

Group_5

Group_5

Group_10

IP_A

IP_C

IP_B

Change the access point and get a different IP

- A data packet with source IP address IP_A and destination IP address IP_B is received by PEP.
- PEP checks its mapping table to get the group ID 5 for IP_A and group ID 10 for IP_B.
- The policy provisioned as (5, 10, drop) is enforcement.
- The data packet will be dropped at PEP.

User could change the access point but don’t change the group ID.

- If the laptop changes the access point and gets a different IP, user will map IP_C with group ID 5.
- So that the data packet should also follow the policy (5, 10, drop).
- The data packet will also be dropped at PEP.

Next Steps

- Suggestion are welcome to the mailing list
- Authors would like to call for adoption