

anima
Internet-Draft
Intended status: Standards Track
Expires: May 19, 2022

Y. Li
L. Shen
Y. Zhou
Huawei Technologies
November 15, 2021

**Autonomic IP Address To Access Control Group ID Mapping
draft-yizhou-anima-ip-to-access-control-groups-02**

Abstract

This document defines the autonomic technical Objectives for IP address/prefix to access control group IDs mapping information. The Objectives defined can be used in Generic Autonomic Signaling Protocol (GRASP) to make the policy enforcement point receive IP address and its tied access control groups information directly from the access authentication points and facilitate the group based policy enforcement.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 19, 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminologies	3
3.	Problems	3
4.	Autonomic IP Address to Access Control Groups ID Mapping Procedures	7
4.1.	Behaviours of IP to Group Mapping Information Providing Nodes	8
4.2.	Behaviours of IP to Group Mapping Information Receiving or Requesting Nodes	8
5.	Autonomic IP Address to Access Control Groups Objectives . .	10
5.1.	IpToGroupId.AAP and IpToGroupId.PEP Objective Option . .	10
5.2.	Example of Using the Defined Objective Options	12
6.	Security Considerations	14
7.	IANA Considerations	14
8.	Acknowledgements	14
9.	References	14
9.1.	Normative References	14
9.2.	Informative References	15
Appendix A.	Objective Examples	16
Authors' Addresses	16

[1.](#) Introduction

Ubiquitous group based policy management makes sure that the users can obtain the same network access permission and QoS assurance wherever they access the campus network. That is, the permission and QoS assurance are tied to user role, rather than access points and/or IP address assigned.

Group means a number of endpoints connecting to the network that share common network policies. It facilitates the easy design and provision of policy. A user's role is usually a group indicated by a group ID. Group based policy management has been replacing the traditional IP address and/or port number based policy widely.

The policy enforcement point (PEP) requires the IP address/prefix and access control group ID mapping information of user in order to execute the group based policy. This mapping information is usually available at the access authentication point (AAP) during the procedures of user access and authentication/authorization. However PEP may not be the access authentication point. Therefore IP and access control group ID mappings has to be passed to PEP.

This document defines the autonomic technical Objectives for IP address/prefix and access control group ID mapping. In this document, group is also used for short to refer to the access control group. The Generic Autonomic Signaling Protocol (GRASP) [[RFC8990](#)] can make use of these technical Objectives as the basic building blocks of a ubiquitous group based policy management solution, especially for a campus network.

Autonomic Networking Infrastructure (ANI) is designed to provide the elementary functions and services to be further integrated and used by Autonomic Service Agents (ASA) on nodes. A campus policy management system can integrate the function introduced in this document when necessary. Such an Autonomic Service Agent (ASA) performing the function of IP address/prefix to access control group ID mapping is called IPAddressToAccessControlGroups ASA in this document.

2. Terminologies

This document uses terminology defined in [[RFC7575](#)].

PEP: Policy Enforcement Point. A logical entity that enforces policy decisions [[RFC3198](#)]. The policy decisions are group based policies in this document.

AAP: Access Authentication Point. A logical entity that obtains the information of the attaching clients' assigned IP address/prefix and their access control group IDs. AAP may get the information from one or different resources, for example, DHCP [[RFC2131](#)] [[RFC8415](#)] server and/or RADIUS [[RFC2865](#)] server.

3. Problems

The traditional policy in a campus network is normally presented as IP prefix/address based, for example, "Deny the traffic from IP prefix X to IP prefix Y". Each of the access port of the switches is assigned a subnet prefix and each subnet implies a group. It works well when the end hosts are static. With the increasing deployment of wireless accessed users and more complicated and dynamic requirements of campus network policy, such an assumption no longer holds. For instance, a user from the engineering department may bring the laptop to access the campus network via a WiFi access point. Then it will be assigned an IP address from a different subnet prefix from the other fixed end hosts in the same engineering department. It is hard and tedious to provision the consistent policy with the other hosts in the same group for this specific IP address. Another example is a user can belong to more than one group, say group of department A and also VIP group. Group

assignment is much more flexible than subnet defined IP address assignment.

Therefore group based policy is used in such cases. No matter what IP address is assigned to the user, its belonging access control groups have no change and the group based policies have no change either. For example, the policy can be "Allow the traffic from group engineering whose group ID is 3 to group testing whose group ID is 15", or "assign the traffic destined to VIP group whose group ID is 1 the highest priority". In order to make group based policy work, the IP address and its group mapping information has to be stored on PEP so that IP addresses carried in data packet can be extracted and then mapped to the group ID. For instance, when a packet with source address X and destination address Y is received by PEP, PEP checks its mapping table to get that source address X maps to group ID 3 and destination address Y maps to group ID 15. It checks its policy table to see what kind of policy, such as "allow" or "drop", should be enforced on packet from group ID 3 to group ID 15. Then PEP executes the group based policy. The mapping table is short for IP address to access control group ID mapping table. For the information in the mapping table, we call it IP and group mapping information in this document.

IP and group mapping information is usually first available at the access authentication point (AAP). AAP may serve as the DHCP relay which remembers the IP address assigned to the client during DHCP address assignment and at the same time it talks to AAA server to get the client's group ID information based on client's identity using AAA protocol such as RADIUS [[RFC2865](#)]. AAP then obtains the IP and group mapping information. Figure 1 show a typical campus network. The policy enforcement point (PEP) can be core switches, while the access authentication point (AAP) is the access switch in the figure. The problem to be solved by Autonomic Networking Infrastructure(ANI) here is how to make IP address and access control group ID mapping information passing from AAP to PEPs using IPAddressToAccessControlGroups ASA.

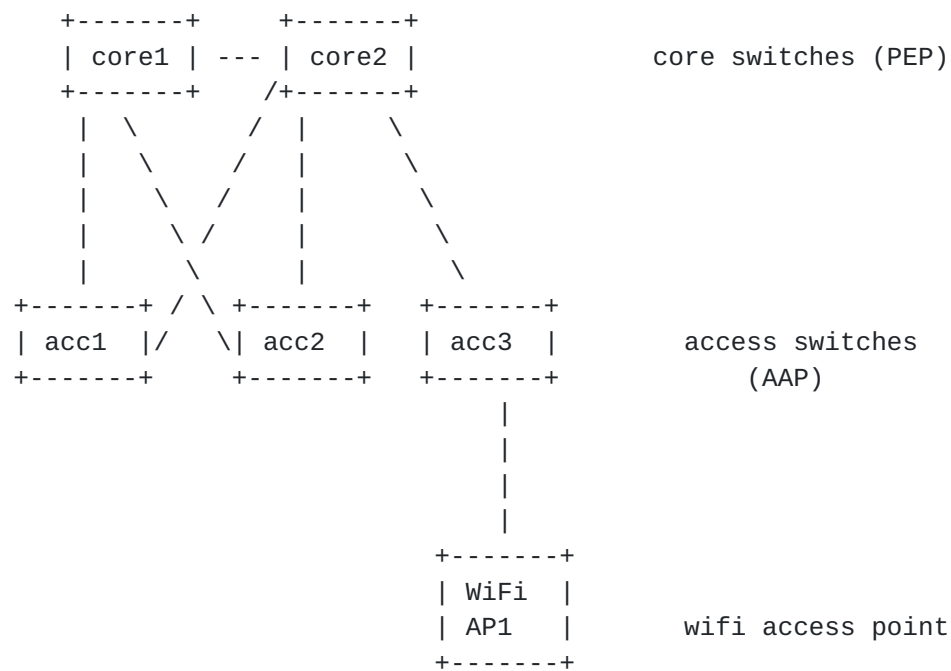


Figure 1: Hierarchical Campus Network

A more complex campus network is shown in Figure 2. There are 4 PEPs are deployed at the key positions for different types of traffic. The AAPs obtaining a user's IP and group ID mapping information are access switches which are the access nodes for the attaching clients.

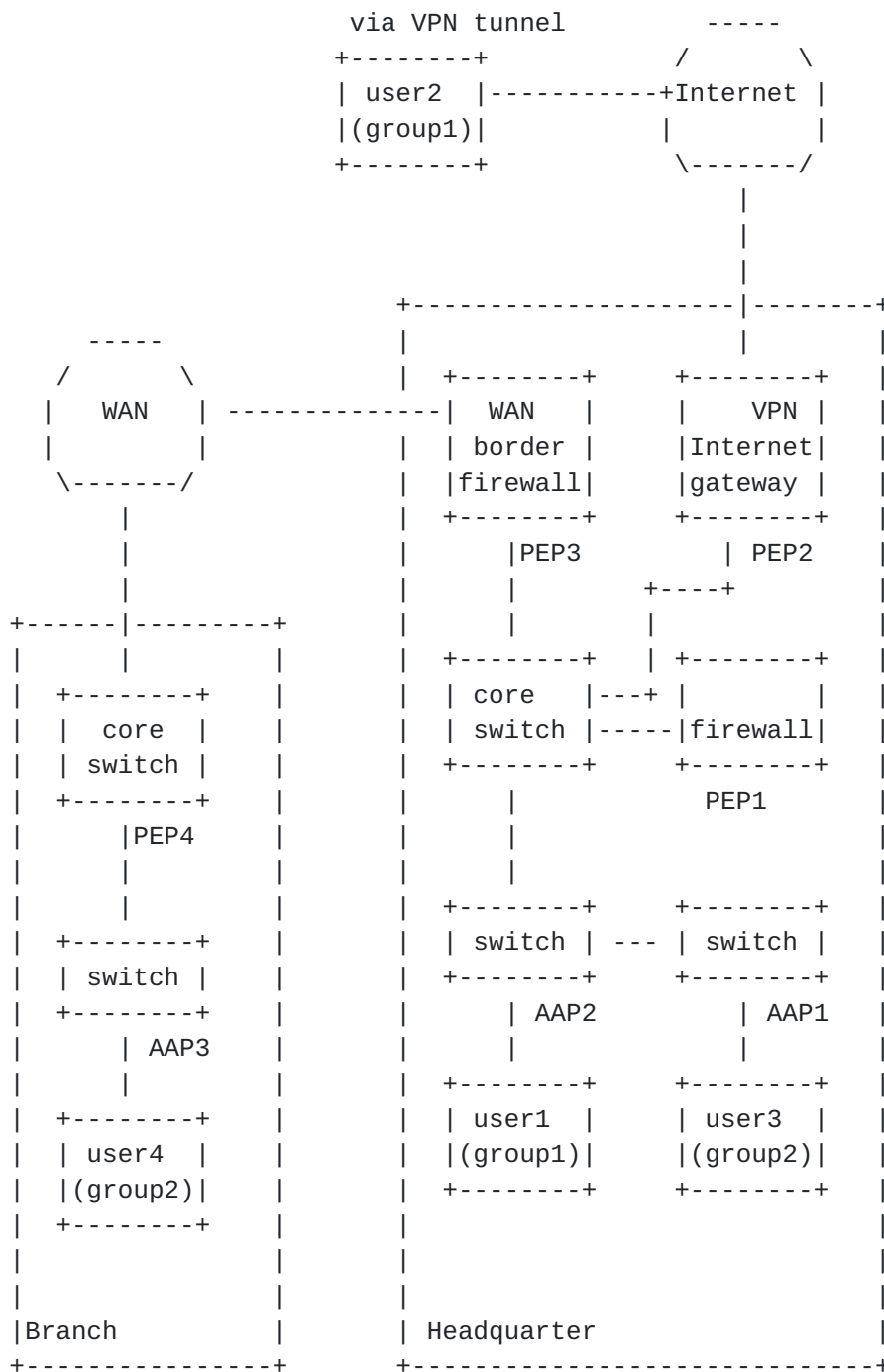


Figure 2: Campus Networks with remote access

Some deployment uses a centralized controller to distribute IP and group ID mapping information. Every single AAP reports its IP and group ID mapping information to the controller. Controller pushes the information regularly to all the PEPs. In addition, when a PEP receives a data packet without pre-stored mapped group ID information

of the corresponding IP addresses, it queries the controller for the group IDs of the source and/or destination IP addresses and then enforce the group based policy. This approach requires an explicit controller able to talk to each and every AAP and PEP. In the deployment where the headquarter and branch campus networks are far apart, it will require controllers for each site to exchange information or have another super-controller to help exchange the information among sites. It introduces the complexity and interoperability issues.

Autonomic Networking (AN) puts the intelligence at the node level, to minimize dependency on human administrators and central management such as a controller. The Autonomic Networking approach discussed in this document is based on the assumption that there is a generic discovery and negotiation protocol that enables direct negotiation and/or synchronization between the routers or switches. GRASP [[RFC8990](#)] is intended to be such a protocol which can make use of the technical Objectives defined in the following sections as the basic building blocks of a ubiquitous group based policy management solution, especially for a campus network. The ultimate goal is self-management of campus networks which can expand over multiple sites and share the same set of policies, including self-configuration, self-optimization, self-healing and self-protection (sometimes collectively called self-X).

4. Autonomic IP Address to Access Control Groups ID Mapping Procedures

IPAddressToAccessControlGroups ASA carries out the the function of IP address/prefix to access control groups ID mapping in this document. The procedures is illustrated below. As noted in [Section 3](#), a network node with IPAddressToAccessControlGroups ASA deployed usually has a role of either AAP or PEP. Therefore two new GRASP Objectives are defined and used for Objective name based multiplexing. They are IpToGroupId.PEP and IpToGroupId.AAP respectively. [Section 5](#) gives more details of the format of them.

The basic procedures are AAP provides the mapping information to PEPs whenever it obtains new or updated or withdrawn mapping information. PEPs will then store the information for future policy enforcement usage. A rare case is that a PEP requests the group ID for a specific IP address when it finds that information is required but not locally stored. AAP possessing such mapping information will reply to this request.

4.1. Behaviours of IP to Group Mapping Information Providing Nodes

IPAddressToAccessControlGroups ASA with mapping information providing feature is usually an AAP supporting IpToGroupId.AAP Objective option. If a PEP would like to provide mapping information as well to the other PEPs, it is logically an AAP in that procedure. Then such PEPs should support both IpToGroupId.PEP and IpToGroupId.AAP Objective options in its IPAddressToAccessControlGroups ASA.

AAP obtains the mapping of IP address and group IDs of a user in various ways. For instance, use RADIUS [[RFC2865](#)] or CAPWAP [[RFC5415](#)] to get the user's access control group IDs during authentication phase and use DHCP snooping to get the user's assigned IP address. Therefore the IP and group ID mapping information of a user can be obtained by AAP at the very early stage when the user connects to the network. Sometimes such mapping information can be statically provisioned based on port or VLAN. Mapping information obtained in such ways is stored locally on AAP. AAP discovers the IPAddressToAccessControlGroups ASA supporting IpToGroupId.PEP first. Then AAP sends Request Negotiation message to those PEPs with the mapping information it has. Whenever there is a change or withdrawn of the mapping information, AAP has to send Request Negotiation again to PEPs for updating.

The providing nodes of mapping information are usually at the network edges. The requesting or receiving nodes of the mapping information are normally aggregation or core nodes with more storage and capability to enforce the policy. There are normally only a few of them, for instance two in a campus network. Therefore the number of mapping information receiving nodes is usually much less than the number of providing nodes. Hence it is quite efficient that the information providing AAP nodes proactively send the mapping information to the receiving PEP nodes. It is the most common case how the mapping information is distributed.

In some rare cases that an AAP receives the Request Synchronization with specific IP address and NULL (represented by zero) group ID, it should reply with Synchronization message with the mapped group ID of the specific IP address. If an AAP has no such mapped information available locally, it can reply with an Invalid message.

4.2. Behaviours of IP to Group Mapping Information Receiving or Requesting Nodes

IPAddressToAccessControlGroups ASA with mapping information requesting or receiving feature is usually a PEP supporting IpToGroupId.PEP Objective option. PEPs need to map the IP address/

prefix of the received data packets to one or more group IDs in order to enforce the group based policy.

PEPs deployed IPAddressToAccessControlGroups ASA supporting IpToGroupId.PEP Objective option will receive the Request Negotiation GRASP message with the mapping information from the information providing AAP nodes as shown in [Section 4.1](#). It should save the mapping information locally. And reply with an Negotiation End GRASP message with an Accept option.

It makes the mapping information of the specific IP addresses received and pre-stored in most cases by PEP before the data packet with those addresses as source or destination is received.

However there are cases that the mapped group ID information of the IP address is not pre-stored when a data packet with that IP address arrives, for example due to timeout or unintentional withdrawn of the mapping information. Then PEPs will send the Request Synchronization with the specific IP address and NULL group ID to ask AAPs for the mapping information.

The request can be triggered by the first data packet of a flow. Group based policy requires both the source and destination group IDs which are mapped from source and destination IP addresses respectively. If any of such mapping is not locally available, the requesting node needs to ask for it. In some implementation, data packet encapsulation includes the source group ID directly such as in the reserved field in VXLAN [[RFC7348](#)]. Therefore it is up to the requesting node to determine if both source and destination group IDs or only one of them should be requested. If the requesting node is a tunnel endpoint, usually the inner rather than outer IP addresses should be used to request for the corresponding group id.

The request can also be sent periodically or voluntarily. It can be sent when a newly booted requesting node wants to get the whole set of mapping information or when a requesting node would like have an explicit refreshment on some specific information.

The requesting PEP should send out a GRASP Discovery message containing IpToGroupId.AAP Objective option in order to discover AAPs. It then acts as a GRASP synchronization initiator by sending the Request Synchronization with IP address and NULL group ID as the Objective values to ask for the mapping information. This starts a GRASP synchronization process.

5. Autonomic IP Address to Access Control Groups Objectives

This section defines two GRASP technical Objective options IpToGroupId.AAP and IpToGroupId.PEP that can be used by IPAddressToAccessControlGroups ASA to support autonomic IP address/prefix to access control group ID mapping information distribution.

5.1. IpToGroupId.AAP and IpToGroupId.PEP Objective Option

Both IpToGroupId.AAP and IpToGroupId.PEP Objective option are GRASP Objective options conforming to [[RFC8990](#)]. They share the same Objective option value format defined in this section. Normally IpToGroupId.AAP Objective option should be supported by IPAddressToAccessControlGroups ASA deployed on AAP nodes to provide the mapping information and IpToGroupId.PEP Objective option should be supported by IPAddressToAccessControlGroups ASA deployed on PEP nodes to request or receive the mapping information .

The Objective carries the IP prefix/address and its mapping access control group IDs. The format of them in CBOR (Concise Binary Object Representation [[RFC8949](#)]) is show in Concise data definition language (CDDL) [[RFC8610](#)] as follows. Tags for general IPv4 and IPv6 addresses and prefixes defined in [[I-D.ietf-cbor-network-addresses](#)] are used.


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

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

```
group-id = uint
```

```
; copied from draft-ietf-cbor-network-addresses, RFC YYYY TBD:
```

```
ip-address-or-prefix = ipv6-address-or-prefix/ipv4-address-or-prefix
```

```
ipv6-address-or-prefix = #6.54(ipv6-address / ipv6-prefix)
```

```
ipv4-address-or-prefix = #6.52(ipv4-address / ipv4-prefix)
```

```
ipv6-prefix = [ipv6-prefix-length, ipv6-prefix-bytes]
```

```
ipv4-prefix = [ipv4-prefix-length, ipv4-prefix-bytes]
```

```
ipv6-prefix-length = 0..128
```

```
ipv4-prefix-length = 0..32
```

```
ipv6-prefix-bytes = bytes .size (uint .le 16)
```

```
ipv4-prefix-bytes = bytes .size (uint .le 4)
```

```
ipv6-address = bytes .size 16
```

```
ipv4-address = bytes .size 4
```

```
; copied from the GRASP specification, RFC 8990:
```

```
objective-flags = uint .bits objective-flag
```

```
objective-flag = &(
    F_DISC: 0      ; valid for discovery
    F_NEG: 1      ; valid for negotiation
    F_SYNCH: 2    ; valid for synchronization
    F_NEG_DRY: 3   ; negotiation is a dry run
)
```

```
loop-count = 0..255
```

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.

5.2. Example of Using the Defined Objective Options

Figure 1 shows a typical campus network of with three access switches which are AAPs and two core switches which are PEPs. We assume that the policy in this campus is `outsource_group` (which has group ID 5) is not allowed to access `accounting_group` (which has group ID 10). The policy (5, 10, drop) expressed in the form of (source group ID, destination group ID, action) is provisioned on the PEPs which are core switches in the figure.

When a user gets connected, the access switch which is an AAP snoops the DHCP address assignment exchange to obtain the IP address `IP_A`. The user provides a user ID to get authenticated via 802.1x and RADIUS protocol. Thus the access switch obtains the user's group ID which is 5 in this example in authentication procedures. So the access switch has the mapping information (`IP_A`, 5) in the form of (IP address, access control group ID). The mapping information is then passed from the access switch to the core switches which are PEPs using GRASP Objective defined in this document. Figure 3 shows an example of the procedures. Only the key values of the Objective is shown for simplicity.

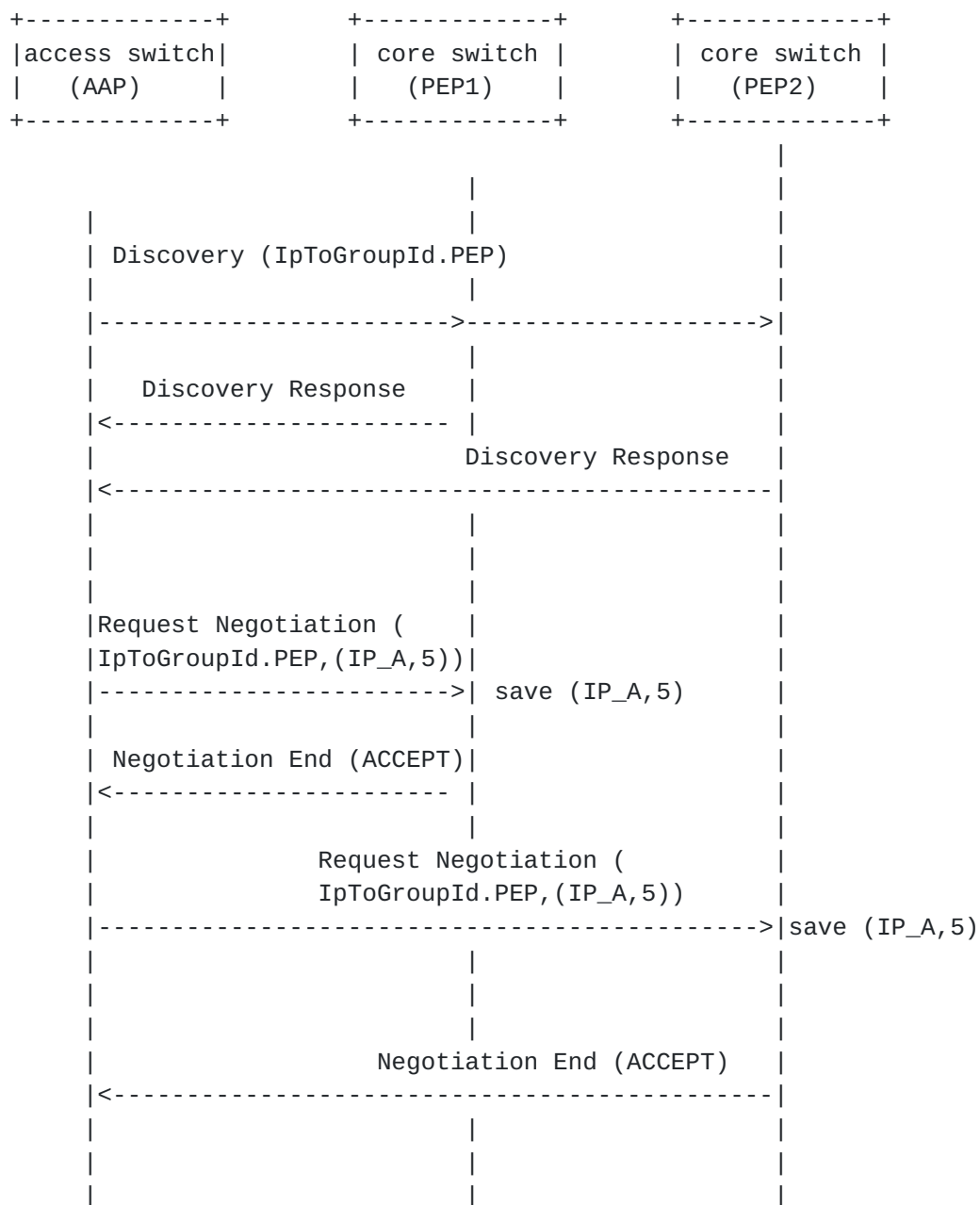


Figure 3: Example of AAP pushing mapping information to PEPs

After the core switches get this mapping information, they save it for future policy enforcement. For example, when a data packet with source IP address IP_A and destination IP address IP_B is received, the PEP checks its mapping table to get the group ID 5 for IP_A and group ID 10 for IP_B. Then the policy provisioned as (5, 10, drop) is enforcement. So the data packet will be dropped. It facilitates the group based policy execution.

6. Security Considerations

Security consideration for GRASP [RFC8990] applies in this document. The preferred security model is that devices are trusted following the secure bootstrap procedure [RFC8995] and that a secure Autonomic Control Plane (ACP) [RFC8994] is in place.

7. IANA Considerations

This document defines two new GRASP Objective option names: "IpToGroupId.AAP" and "IpToGroupId.PEP". The IANA is requested to add them to the "GRASP Objective Names" subregistry defined by [RFC8990].

8. Acknowledgements

Thanks to Carsten Bormann, Brian Carpenter and Michael Richardson for useful suggestions and revising CDDL representations.

9. References

9.1. Normative References

- [RFC7575] Behringer, M., Pritikin, M., Bjarnason, S., Clemm, A., Carpenter, B., Jiang, S., and L. Ciavaglia, "Autonomic Networking: Definitions and Design Goals", [RFC 7575](#), DOI 10.17487/RFC7575, June 2015, <<https://www.rfc-editor.org/info/rfc7575>>.
- [RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", [RFC 8610](#), DOI 10.17487/RFC8610, June 2019, <<https://www.rfc-editor.org/info/rfc8610>>.
- [RFC8990] Bormann, C., Carpenter, B., Ed., and B. Liu, Ed., "GeneRic Autonomic Signaling Protocol (GRASP)", [RFC 8990](#), DOI 10.17487/RFC8990, May 2021, <<https://www.rfc-editor.org/info/rfc8990>>.
- [I-D.ietf-cbor-network-addresses] Richardson, M. and C. Bormann, "CBOR tags for IPv4 and IPv6 addresses and prefixes", [draft-ietf-cbor-network-addresses-13](#) (work in progress), October 2021.

9.2. Informative References

- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), DOI 10.17487/RFC2131, March 1997, <<https://www.rfc-editor.org/info/rfc2131>>.
- [RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), DOI 10.17487/RFC2865, June 2000, <<https://www.rfc-editor.org/info/rfc2865>>.
- [RFC3198] Westerinen, A., Schnizlein, J., Strassner, J., Scherling, M., Quinn, B., Herzog, S., Huynh, A., Carlson, M., Perry, J., and S. Waldbusser, "Terminology for Policy-Based Management", [RFC 3198](#), DOI 10.17487/RFC3198, November 2001, <<https://www.rfc-editor.org/info/rfc3198>>.
- [RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", [RFC 5415](#), DOI 10.17487/RFC5415, March 2009, <<https://www.rfc-editor.org/info/rfc5415>>.
- [RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", [RFC 7348](#), DOI 10.17487/RFC7348, August 2014, <<https://www.rfc-editor.org/info/rfc7348>>.
- [RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 8415](#), DOI 10.17487/RFC8415, November 2018, <<https://www.rfc-editor.org/info/rfc8415>>.
- [RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, [RFC 8949](#), DOI 10.17487/RFC8949, December 2020, <<https://www.rfc-editor.org/info/rfc8949>>.
- [RFC8994] Eckert, T., Ed., Behringer, M., Ed., and S. Bjarnason, "An Autonomic Control Plane (ACP)", [RFC 8994](#), DOI 10.17487/RFC8994, May 2021, <<https://www.rfc-editor.org/info/rfc8994>>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", [RFC 8995](#), DOI 10.17487/RFC8995, May 2021, <<https://www.rfc-editor.org/info/rfc8995>>.

Appendix A. Objective Examples

This appendix shows a number of examples of Objective defined in this document conforming to the CDDL syntax given in [Section 5.1](#).

```
["IpToGroupId.PEP", 15, 101,  
  [54([4, h'A50386A78BA56FA4BBC734281C51']), 3506, 2698, 4562]]
```

```
["IpToGroupId.PEP", 5, 73, [52(h'9946B8A3'), 2881,  
  2265, 1720, 2450]]
```

```
["IpToGroupId.PEP", 15, 161,  
  [54(h'39F3045B641AD291B057CD1857A7314A')]]
```

```
["IpToGroupId.PEP", 15, 2, [52(h'98A1CE4F')]]
```

```
["IpToGroupId.PEP", 15, 66, [52(h'69A16BFE'), 2601,  
  1851, 3876, 1405]]
```

```
["IpToGroupId.AAP", 15, 254,  
  [54(h'38AB303B8895DC95068CE00248D2FE91'), 4019, 1166, 3113]]
```

```
["IpToGroupId.AAP", 15, 63, [52([4, h'0B48']), 3035,  
  1181]]
```

```
["IpToGroupId.AAP", 15, 44, [52(h'01F1D8FF'), 3099,  
  1577, 1138, 1670]]
```

```
["IpToGroupId.AAP", 15, 181,  
  [54(h'2C74719F9355BA4E3BDE5689D1FE4CB0')]]
```

```
["IpToGroupId.PEP", 15, 129, [52(h'A2EF97C7'), 3149,  
  2728]]
```

Authors' Addresses

Yizhou Li
Huawei Technologies

Email: liyizhou@huawei.com

Li Shen

Huawei Technologies

Email: kevin.shenli@huawei.com

Yujing Zhou

Huawei Technologies

Email: zhouyujing3@huawei.com