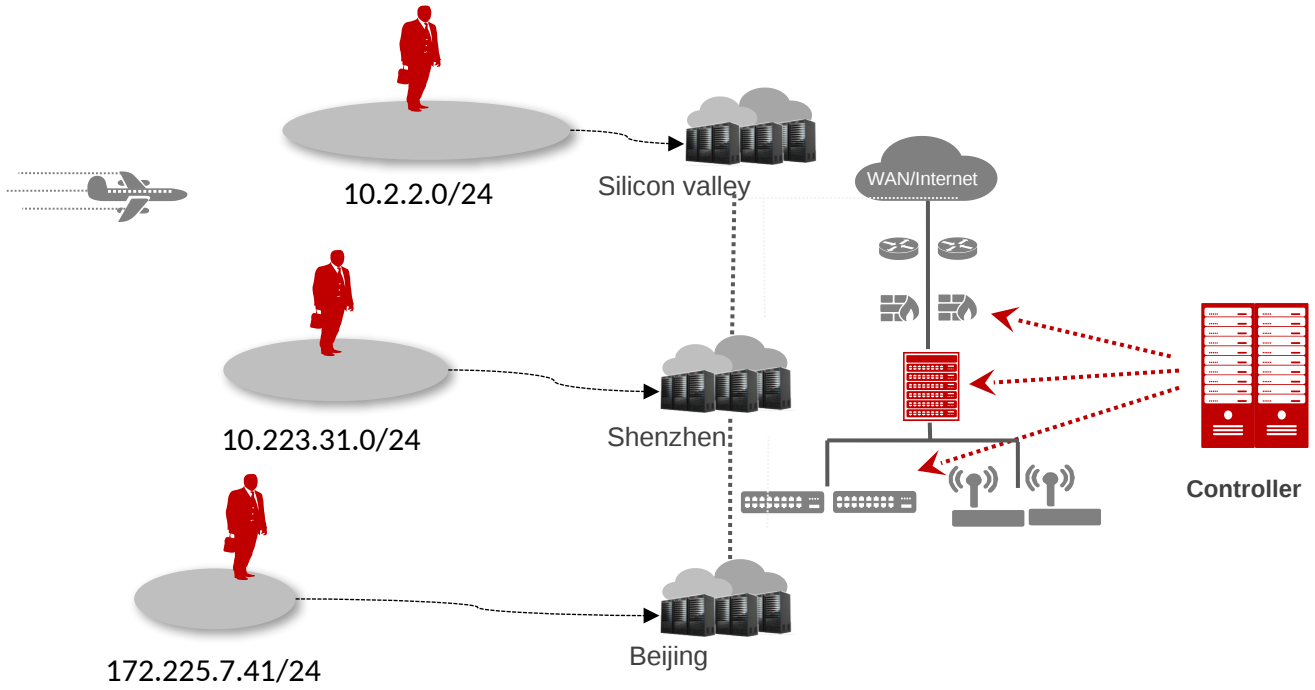
A Policy-based Network Access Control

draft-ma-opsawg-ucl-acl-00

Qiufang Ma (Huawei)
Qin Wu (Huawei)
Mohamed Boucadair (Orange)
Daniel King (Old Dog Consulting)

Problem Statement



During 8am-5pm every workday:

- Deny source IP 10.2.2.0/24 to destination youtube.com
- Deny source IP 10.223.31.0/24 to destination youtube.com
- Deny source IP 172.225.7.41/32 to destination youtube.com

During off-hours and weekends:

- Permit source IP 10.2.2.0/24 to destination youtube.com
- Permit source IP 10.223.31.0/24 to destination youtube.com
- Permit source IP 172.225.7.41/32 to destination youtube.com

The address and/or ports based access control list (ACL) are often insufficient in the expression of real-world network access

- Mobile office makes the **IP addresses** of employees **change frequently**.
- **different** security policies need to be applied to the same set of users **under different circumstances**(e.g., users' location, users' role, time-of-day, type of network device used)

Solution Overview

- Ensure enforcement of access control policies based on user-group identity:

  During 8am-5pm every workday:
  - Deny **source group ID sales** to destination youtube.com **workday**

  During off-hours and weekends:
  - Permit **source group ID sales** to destination youtube.com **non-workday**

- What's a user-group?
  - An identifier that represents the collective identity of a **group of users**
    - The ones who access the network and consumes specific network services/resources.

UCL Extension to the ACL model

src dst	Finance group	Sales group	10.1.1.0/24
Sales group	permit	permit	deny
Visitor group	deny	permit	deny
10.1.1.1/24	permit	deny	permit

User-group based ACL example

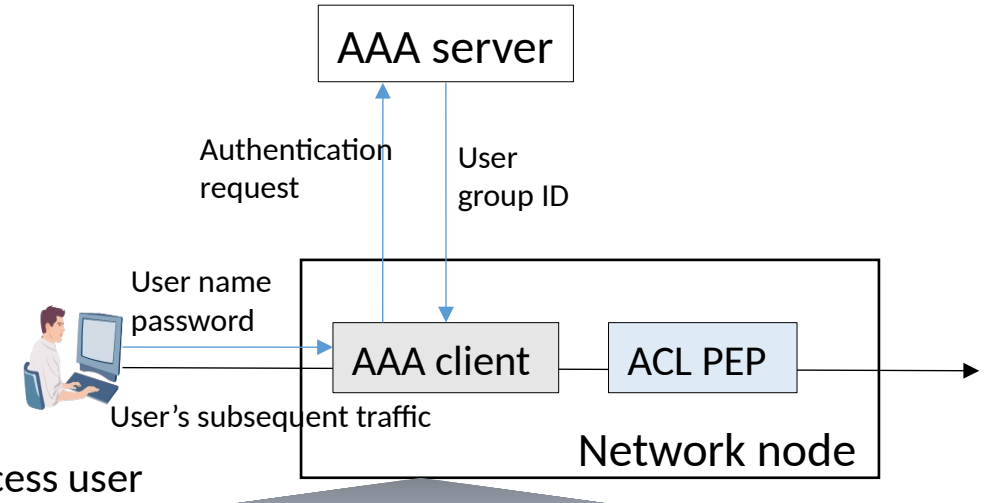
To cover the following types of access control:

- U2U: user-group to user-group access
- N2N: IP address prefix to IP prefix access
- U2N: user-group to IP prefix access.
- N2U: IP prefix to user-group access.

to realize time variant access policies, e.g., restrict access to specific websites during 8am~5pm, every workday

```
module: ietf-ucl-acl
  augment /acl:acls/acl:acl/acl:aces/acl:ace/acl:matches:
    +--rw (user-control-groups)?
       +--:(source-match)
       |  +--rw source-match
       |     +--rw (destination-match)?
       |        +--:(user-group) {match-on-user-group}?
       |        |  +--rw user-group-name?   string
       |        +--:(IP-address)
       |           +--rw ipv4-network?      inet:ipv4-prefix
       |           +--rw ipv6-network?      inet:ipv6-prefix
       +--:(destination-match)
          +--rw destination-match
             +--rw (destination-match)?
                +--:(user-group) {match-on-user-group}?
                |  +--rw user-group-name?   string
                +--:(IP-address)
                   +--rw ipv4-network?      inet:ipv4-prefix
                   +--rw ipv6-network?      inet:ipv6-prefix
  augment /acl:acls/acl:acl/acl:aces/acl:ace:
    +--rw time-range
       +--rw (time-range-type)?
          +--:(periodic-range)
          |  +--rw month*          lmap:month-or-all
          |  +--rw day-of-month*   lmap:day-of-months-or-all
          |  +--rw day-of-week*    lmap:weekday-or-all
          |  +--rw hour*           lmap:hour-or-all
          +--:(absolute-range)
             +--rw start-time?     yang:date-and-time
             +--rw end-time?       yang:date-and-time
```

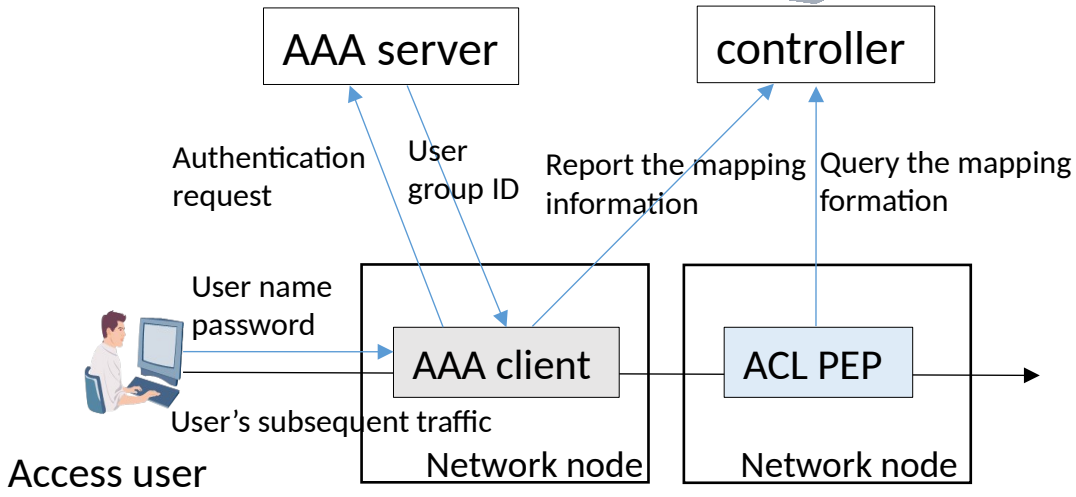
Alternatives to realize group ID to address mapping



Group ID	User name	IP address	Login time
1	Alice	10.223.32.96/32	…
	Bob	10.223.32.64/32	…
2	Cindy	10.223.32.144/32	…

If PEP is also the user authentication device, it already maintains the mapping information

Group ID	User name	IP address	Login time
1	Alice	10.223.32.96/32	…
	Bob	10.223.32.64/32	…
2	Cindy	10.223.32.144/32	…



If PEP has no user group ID information, it queries the mapping from the controller side

Comments, Questions, Concerns?