A YANG Data Model and RADIUS Extension for Policy-based Network Access Control

draft-ietf-opsawg-ucl-acl-03

Qiufang Ma (Huawei) **Presenter**
Qin Wu (Huawei)
Mohamed Boucadair (Orange)
Daniel King (Lancaster University)

Document Updates Since IETF 118

- Emphasize what hardware ramifications might exist and what operational tradeoffs one would consider (issue #14)
  - Add a new section for implementation considerations:
    - The group-based ACL model can be implemented in different ways
    - Dedicated hardware/software support might be needed if the PEP needs to act upon the endpoint group identifier
    - Implementations need to evaluate the operational tradeoff (flexibility brought to the network vs. complexity of implementation) carefully
- Add rationale for endpoint group id defined as a string (issue #33)
  - To accommodate deployments which require some identification hierarchy; such a hierarchy is meant to ease coordination within a domain
- Clarify mapping of endpoint group string to encapsulation ID is out of scope (issue #25)

Document Updates Since IETF 118 (cont.)

- Define application group as another endpoint group type (issue #42)
  - A collection of applications that shares common access control policies.
- List endpoint-groups under ACLs (issue #66)
  - Endpoint group should be independent of a given ACL
- Define endpoint group type as “identityref” for extensibility
- Reflect the recent updates of schedule YANG data model
  - Separated from this I-D because of wide applicability

The Current Model design

```
module: ietf-ucl-acl

  augment /acl:acls:
   +--rw endpoint-groups
     +--rw endpoint-group* [group-id]
       +--rw group-id      string
       +--rw group-type?   identityref
  augment /acl:acls/acl:acl/acl:aces/acl:ace/acl:matches:
   +--rw endpoint-group {match-on-group}?
     +--rw source-group-id?       group-id-reference
     +--rw destination-group-id?  group-id-reference
  augment /acl:acls/acl:acl/acl:aces/acl:ace:
   +--rw effective-schedule
     +--rw (schedule-type)?
       +--:(period)
       |  +---u schedule:period-of-time
       +--:(recurrence) {schedule:icalendar-recurrence-supported}?
         +---u schedule:icalendar-recurrence
```

endpoint group definition

Allow group identifier as one of matching criteria

Allow each ACE to be activated based on a scheduled time

reuse groupings in I-D.ma-opsawg-schedule-yang

Next Steps

- Request the WG to review the document updates and provide feedback
- Line up with the schedule YANG data model in I-D.ma-opsawg-schedule-yang
- Working group last call?