

Access Control List Model
draft-bogdanovic-netmod-acl-model-01
IETF 90 Toronto

Lisa Huang, Dana Blair,
Kiran Koushik, Dean Bogdanovic

Agenda

- Motivation for new draft
- Design
- Next steps

Motivation

- Previous draft draft-huang-netmod-acl was complicated and the ACL structure is not obvious
- Create common base model that can be extended:
 - packet headers
 - vendor specific

Design

- ietf-acl
 - base model
 - ACL container
 - ACL oper data container
 - ACE List
 - » Match container
 - » Action container
- packet-fields
 - Used in ACE Match container
- newco-acl
 - vendor specific extensions of base model
 - augments the base model

Design cont'd

```
module: ietf-acl
  +--rw access-list
    +--rw acl-name
      +--rw acl-oper-data
      | ...
      | ...
    +--rw access-list-entries
      |
      | +--rw matches
      | | +--rw (ace-type)
      | | ...
      | | ...
      | +--rw actions
      | | ...
      | | ...
    +--rw default-actions
      +--rw deny? empty
```



Operation data:
counter, targets, etc



Matches container:
packet-header-fields
meta data filters



Actions container

Next steps

- Route filter
- Prefix-list filter
- Suggestions