IETF ACL YANG Enhancements

Sonal Agarwal
Mahesh Jethanandani

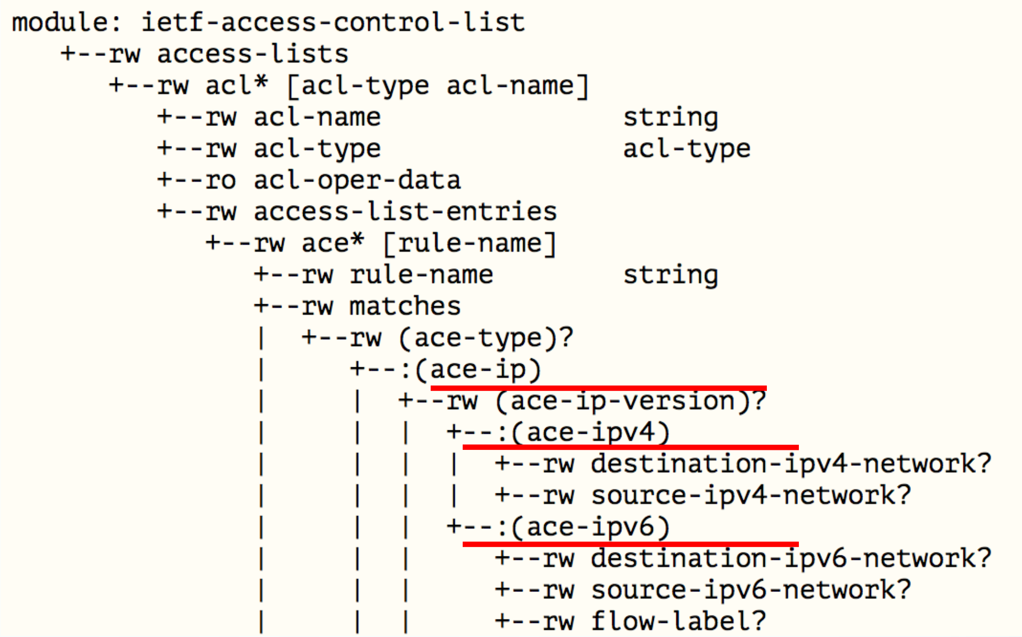
Agenda

- Support for combinations of ACL address family types
- Inclusion of match & action parameters
- Open Issues found on further review

Support for combinations of ACL address family types

What's in the current model?

Draft 10 allowed different types of ACEs (IPv4, IPv6, L2) to be configured within a single ACL



```
module: ietf-access-control-list
   +--rw access-lists
      +--rw acl* [acl-type acl-name]
         +--rw acl-name                 string
         +--rw acl-type                 acl-type
         +--ro acl-oper-data
         +--rw access-list-entries
            +--rw ace* [rule-name]
               +--rw rule-name          string
               +--rw matches
               |  +--rw (ace-type)?
               |     +--:(ace-ip)
               |     |  +--rw (ace-ip-version)?
               |     |  |  +--:(ace-ipv4)
               |     |  |  |  +--rw destination-ipv4-network?
               |     |  |  |  +--rw source-ipv4-network?
               |     |  |  +--:(ace-ipv6)
               |     |  |     +--rw destination-ipv6-network?
               |     |  |     +--rw source-ipv6-network?
               |     |  |     +--rw flow-label?
```

What is the problem with that?

- Model is error prone because it does not perform strict type checks of the ACL
- Extending the model to include additional types would modify the main model
- Lacks flexibility as it supported only IPv4, IPv6 & L2

Support for combinations of ACL address family types

What is the enhancement in Draft 11?

- Identified all possible L2 & L3 ACL combinations
- Added identity/feature/container statements for the above types

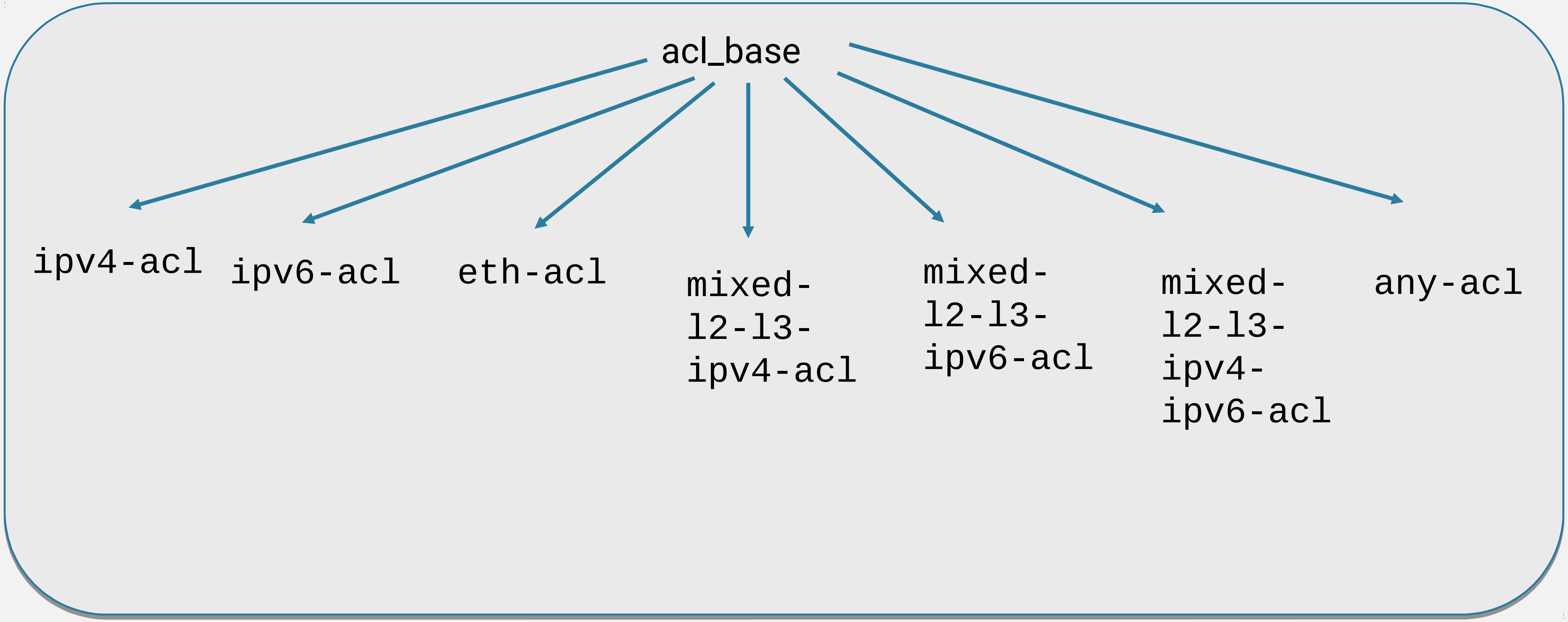
```
identity ipv4-acl {
base acl:acl-base;
}

feature ipv4-acl {
description "Layer 3 IPv4 ACL supported";
}

container ipv4-acl {
if-feature ipv4-acl; must "../../../../acl-type =
'ipv4-acl'";
uses packet-fields:acl-ip-header-fields;
uses packet-fields:acl-ipv4-header-fields;
description "Rule set that supports IPv4
headers."; }
```

What are the benefits of this enhancement?

- Stricter ACL type checks
- Only supports parts of the model identified by the feature and removes all other parts of model
- Easy to extend ACL types by adding new identity, feature and container statements

Support for combinations of ACL address family types

What are the different ACL types supported in draft 11?



Inclusion of more match & action parameters

```
feature tcp-acl {}

container tcp-acl {
  if-feature tcp-acl;
  uses packet-fields:
       acl-tcp-header-fields;
}
```

```
feature udp-acl {}

container udp-acl {
  if-feature udp-acl;
  uses packet-fields:
       acl-udp-header-fields;
}
```

```
feature icmp-acl {}

container icmp-acl {
  if-feature icmp-acl;
  uses packet-fields:
       acl-icmp-header-fields;
}
```

```
leaf logging {type boolean;}
```

Open issues

https://github.com/netmod-wg/acl-model/issues