draft-ietf-netmod-acl-03

IETF #93, IETF

Lisa Huang, Juniper Networks
Kiran Sreenivasa, Dana Blair, Cisco Systems
Dean Bogdanovic

changes since 02

- two open issues
- fixed according to discussions suggestions on the mailing list
- fixed container, leaf names for better clarity and abbreviation (previously was fully expanded)
  - access-list-entries-ip-version -> ace-ip-version
- extended abréviations in text
- added extended descriptions to the model
- fixed XML example
- added more explanation about Linux nftables model with example
- fixed typos, added some text for clarity

open issues #1

- presence vs non presence containers in port range definition

```
container source-port-range {
  presence “Enables source port range”;
  description “Inclusive …….”;
  leaf lower-port {
    type inet:port-number;
    mandatory true;
    description"Lower boundary for port.";
  }
  leaf upper-port {
    must ". >= ../lower-port”
    error-message"The upper-port must be greater than or
equal to lower-port";
        }
        type inet:port-number;
        description
          "Upper boundary for port . If existing, the upper
           port  must be greater or equal to lower-port.";
      }
    }
```

```
container source-port-range {
  description "Specification of source port …”;
  leaf lower-port {
    type inet:port-number;
    description "When set, …”;
  }
  leaf upper-port {
    type inet:port-number;
    description "When set, ….”;
    must ". > ../lower-port" {
      description "This expression is only true if
      lower-port exists and is less than this
      element.";
      error-message "Lower-port is required, and
      must be less than upper-port";
    }
  }
}
```

open issues #1

- generic ACL container vs ACL container per address family

```
container access-list{
   list acl {
      container access-list-entries {
         list ace {
            container matches {
               choice ace-type {
                  case ace-ip {
                     choice ace-ip-version {
                        case ip-v4
                        case ip-v6
                     }
                  case ace-eth {
                  }
               }
            }
         }
      }
   }
}
```

```
container access-list-v4{
   list acl-v4 {
      container access-list-entries-v4 {
         list ace-v4 {
            container matches {
               uses packet-fields:acl-ipv4-header-fields;
            }
         }
      }
   }
}
}
container access-list-v6{
list acl-v6 {
   container access-list-entries-v6 {
      list ace-v6 {
         container matches {
            uses packet-fields:acl-ipv6-header-fields;
         }
      }
   }
}
}
```

Question

- ready for last call?