# IDR FSv2 Interim Design Team 2

5/6/2024

Time: 10-11:30am

# Agenda for Design Team 2 (DT2)
# FSv2 for Basic IP (60 minutes)

---

**3) Extended IP Filters - proposal and design team questions**

draft-hares-idr-fsv2-more-ip-filters [10 minutes] [Sue Hares]

**4) IP Application layer - UDP and Payload [10 minutes]**

4a) draft-dmc-idr-flowspec-tn-awaqre-mobility - UDP filter [TBD]

4b) draft-cui-idr-content-filter-flowspec-00: Payload filter [Yong Cui + Yujia Gao]

**5) FSv1 Group by Extended Community Action**

draft-ietf-idr-flowspec-interfaceset- [Hares and Haas]

# Agenda for Design Team 2 (DT2)
# FSv2 for Basic IP

---

**6) Emerging filters by Groups [15 minutes]**

6a) CATS [5 minutes] [TBD]

[draft-lin-idr-cats-flowspec-ts]

6b) SAVnet [5 minutes] [Nan Geng]

[draft-geng-idr-flowspec-sav-03

6c) APN – [5 minutes] [TBD]

[draft-spend-idr-apn-bgp-flowspec-00]

7) **Design Team 2 – 6 questions** [15 minutes]

8) **Action items – 5 minutes**

# FSv2 – IDR Interims operating as Open Parallel design teams to break FSv2 into “chunks”

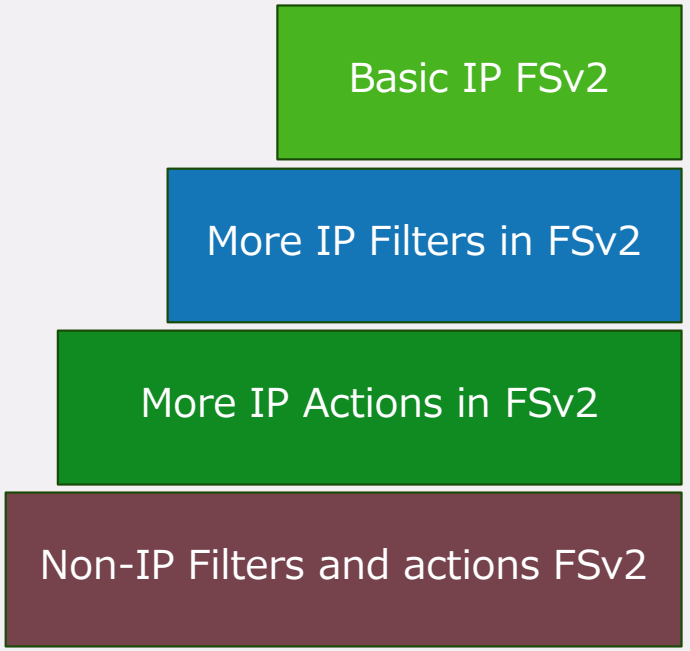
**Team 1**: Basic IP FSv2: Current IPv4/v6 filters + current actions + order

**Team 2**: More IP Filters FSv2 - Defining more IP filters to add to IP

**Team 3**: More IP actions FSv2 – Defining more actions + action sequences to add to

Team 4: Non-IP filters and actions FSv2

**Just ask to join a team!**



# Interims for FSv2 Open Design Teams

**Phase 1 – May - Start our work**

- 4/29 – Design Team 1
- 5/06 – Design Team 1 + 2
- 5/13 – Design 3+ 4 – IP Action Design + Non-IP Filters/Actions

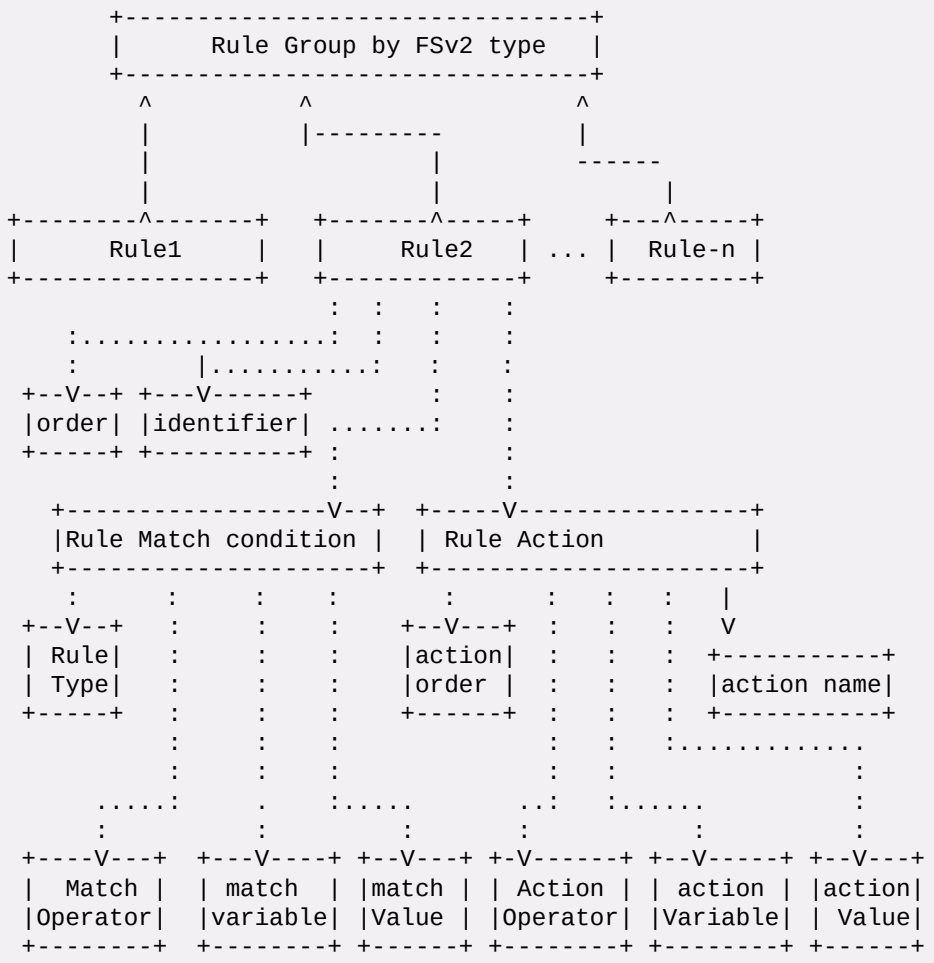
**Phase 2 – June – Getting ready for IETF-120**

- 6/03 – Design Team 1 – Review of FSv2 Basic IP
- 6/10 – Design Team 1 + 2 – Review of FSv2 - More IP Filters
- 6/17 – Design Team 3 + 4 – Review of IP Actions

# FSv2 –More IP filters

## draft-hares-idr-fsv2-more-ip-filters

Sue Hares




**FSv2 Rules (see Rule 2) have**

1. User Order – User assigned number
2. Identifier – logging identifier
3. Rule type
   - match operator
   - match variables
   - match value

Possible to have multiple filter conditions before an action

Order

Rule – 0 = permit all traffic
no actions

Rule 1-N – Filter traffic to take an action on.

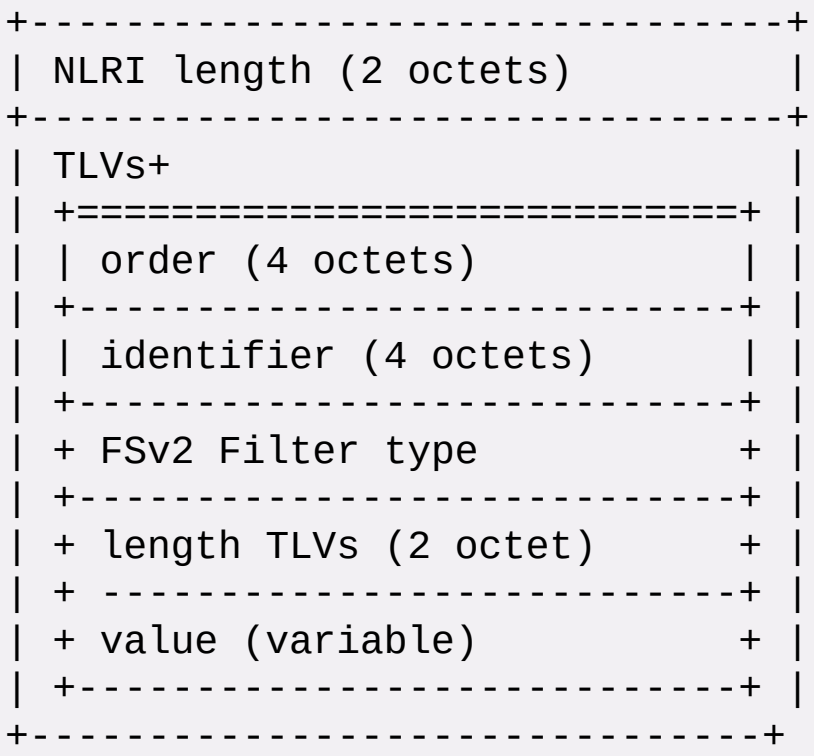
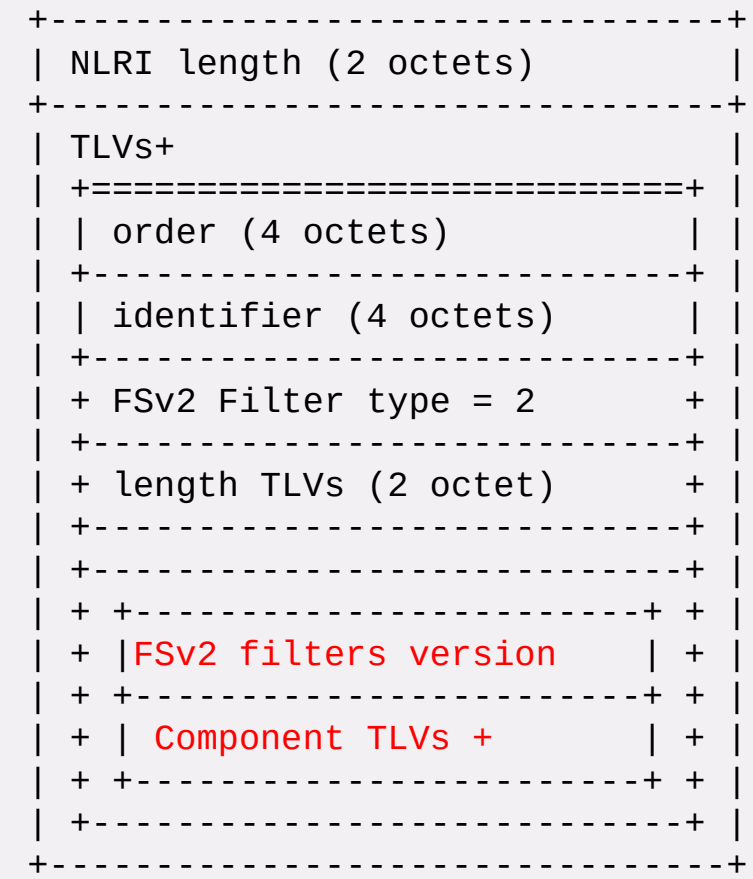


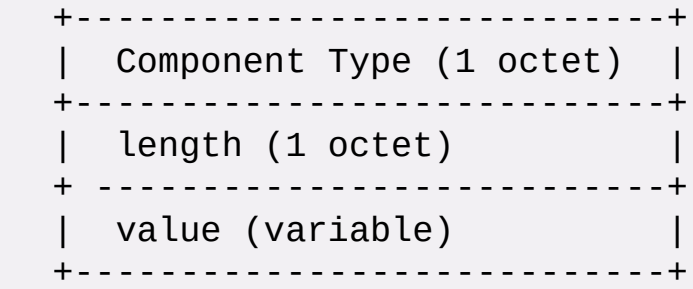

Figure 3-1 - NLRI format for FSv2

FSv2 Filter types
0 - reserved,
1 - IP Basic Filter Rules
2 - Extended IP Filter rules
3- L2 traffic rules<
4- SFC Traffic rules
5- SFC VPN Traffic rules <
6 - BGP/MPLS VPN IP Traffic Rules
7 - BGP/MPLS VPN L2 Traffic Rules
8 - Tunneled traffic




NLRI format for Extended IP Filters

Where the Component TLVs are:




Should the component length be More than 1 octet?

**IP Component Numbers**

1 - IP Destination prefix
2 - IP Source prefix
3 – IPv4 Protocol / IPv6 Upper Layer Protocol
4 – Port
5 – Destination Port
6 – Source Port
7 – ICMPv4 type / ICMPv6 type
8 – ICMPv4 code / ICPv6 code
9 – TCP Flags
10 – Packet length
11 – DSCP
12 – Fragment
13 – Flow Label

**IP Component numbers (IDR WG drafts)**

0 – TTL (option 2)
14 – TTL (option 1)

16 – SID in IPv6 Routing header
17 – NRP in Hop-by-Hop IPv6 header

**Proposed New Component Types**

18 – Payload Match
19 – Group ID

**Allocation of Component IDs**

15-63 Reserved for IP Extensions (standards action)
64-127 Reserved for Non-IP Filters (standard action)
128-191 Reserved for Standard Action
192-249 FCFS
250-255 Reserved

# FSv2 filters + FSv1 filters

- FSv2 and FSv1 are Ships in the night (two NLRIs)
- Ordering

  Rule 0 – permit all

  Rule 1 to Rule N-1 – FSv2 with user order.

  Rule N to end - FSv1 rules at a single-user order
- If same user order, then component number order.
- If same user order + component number, then the order of multiple components of the same component - use rules defined in the component.

# Design Team 2 Questions

# Q1. Does the FSv2 Extend version help deployments?

Feedback from implementers stated that:

- Only Addition for FSv2 is the user order
- FSv2 adheres to this for the IP Filters (type =1)
- *Only Components are the FSv1 components*
- IP Extended Filters – uses a FSv2 Filter version
- *Filters version – allows more Filters to be added per FSv2 filter version*

# Q2. What Filters do we need for IPv6

**FSv1 IP Component Numbers**

1 - IP Destination prefix
2 - IP Source prefix
3 – IPv4 Protocol / IPv6 Upper Layer Protocol
4 – Port
5 – Destination Port
6 – Source Port
7 – ICMPv4 type / ICMPv6 type
8 – ICMPv4 code / ICPv6 code
9 – TCP Flags
10 – Packet length
11 – DSCP
12 – Fragment
13 – Flow Label

**FSv2 – Component numbers – WG drafts**

0 – TTL (option 2)
14 – TTL (option 1)
15 - UDP Port Range
16 – SID in IPv6 Routing header
17 – NRP in Hop-by-Hop IPv6 header

**FSv2 Proposed New Component - ID**

15 - UDP Port Range
18 – Payload Match
19 – Group ID

# 3. What IP Payload filters should we add?

FSv2 currently orders filters with the same user order by FSv1 component types (using FSv1 component logic)

- Should Component types be common in IPv4 and IPv6?
- How should we order component types for upper layers?
- Does this scheme break down?

# 4. Does the NLRI format for user-ordering allow for additions?

- Can New IP Filters for payload be added?
- Can Non-IP Filters (such as L2 + Time) be added?
- How can dependency between filters be expressed?

  If filter-1 matches, can we skip to filter-2.
- Can we handle creating group tags and then testing?
- Can we handle groups + interfaces?
- Can we handle quick addition of new filters (DDOS)?

# 4. What happens if errors are detected in the parsing of the filters?

- If a filter format is broken, how does it impact past filters?

  IDR RFC7606 has a concept of “treat as withdraw”
- What types of errors are possible with user-ordered filters?

# 5. What happens if errors are detected when filters are used?

- What happens if the BGP parsing and validation for a filter is correct, but the filter fails to install on an IP firewall portion of a machine?
- What might cause this problem?
- Should BGP FSv2 flag this problem?

# 6. Are the Validity Checks from FSv1 sufficient

FSv1 – RFC8955 (IPv4), RFC8956, and RFC9117 focused on check that the FSv1 filters were valid.

- Are these validity checks enough for this work?

# Drafts to read for FSv2 on 5/13

## Design team 3 (FSv2 Actions) AND
## Design team 4  (Non-IP filters + Actions)

**FSv2 for Basic IP**

- draft-hares-idr-fsv2-ip-basic
- draft-hares-idr-fsv2-more-ip-filters
- draft-hares-idr-fs-v2-more-ip-actions (5/6/2024)

**Drafts on Actions**

- draft-ietf-idr-flowspec-path-redirect-12
- draft-ietf0-idr-srv6-flowspec-path-redirect-11
- draft-ietf-idr-flowspec-interfaceset-05
- draft-lin-idr-cats-flowspec-ts-00
- draft-peng-idr-apn-bgp-flowspec-00
- draft-shen-idr-flowspec-traffic-compress-action-01

**Non-IP**

- draft-ietf-idr-flowspec-l2vpn
- draft-ietf-idr-flowspec-nv03
- RFC9015
- draft-xiong-idr-detnet-flow-mapping-05
- draft-xiong-idr-detnet-flow-mapping-05

# Thanks for all your work!

# Backup slides

# Two types of Actions

**Extended Communities (EC) – FSv2-EC Actions in**

- Generic transitive EC
- IPv4 Transitive Extended Communities
- Transitive IPv6-Address-Specific Actions

**Community Attribute Actions**

- Community Attribute with a FSv2 Community type

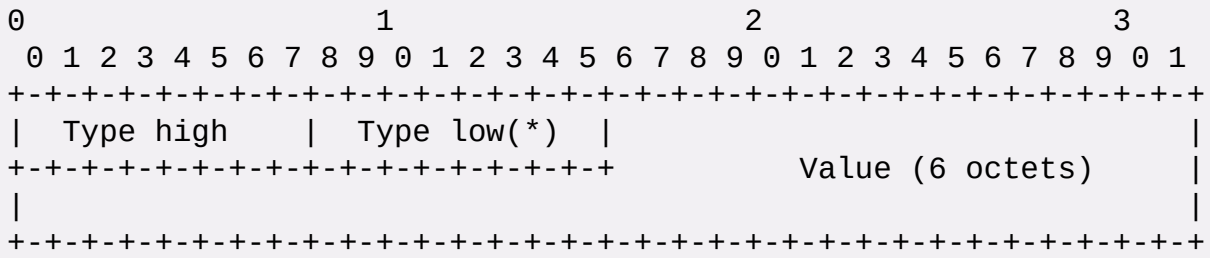



Figure 3-5 – Generic Transitive Extended Community

Table 3-3 Generic Transitive Extended Community
Part 1 - (0x80)

IPv4 Extended Communities (Type 0x80)

| Value | Description | Name | Reference |
|---|---|---|---|
| **0x01** | **FSv2 Action Chain Ordering** | **ACO** | [This document] |
| 0x06 | FSv2 traffic-rate-byte | TRB | [RFC8955] |
| 0x07 | Flow spec traffic-action | TAIS | [RFC8955] |
| 0x08 | Flow spec rt-redirect AS-2 octet format | RDIP | [RFC8955] |
| 0x09 | Flow spec Remark DSCP | TMDS | [RFC8955] |
| 0x0C | Flow Spec Traffic-rate-packets | TRP | [RFC8955] |
| 0xOD | Flow Spec for SFC classifiers | SFCC | [RFC9015] |

Table 3-4 Generic Transitive Extended Community
Part 2 (0x81)

IPv4 Extended Communities FSv2 action (Type 0x81)

| Value | Description | Name | Reference |
|---|---|---|---|
| 0x08 | Flow spec rt-redirect | RDIP | [RFC8955] |

Table 3-5 Generic Transitive Extended Community
Part 3 (Type 0x82)

| Value | Description | Name | Reference |
|---|---|---|---|
| 0x08 | Flow spec rt-redirect AS-4 octet format | RDIP | [RFC8955] |

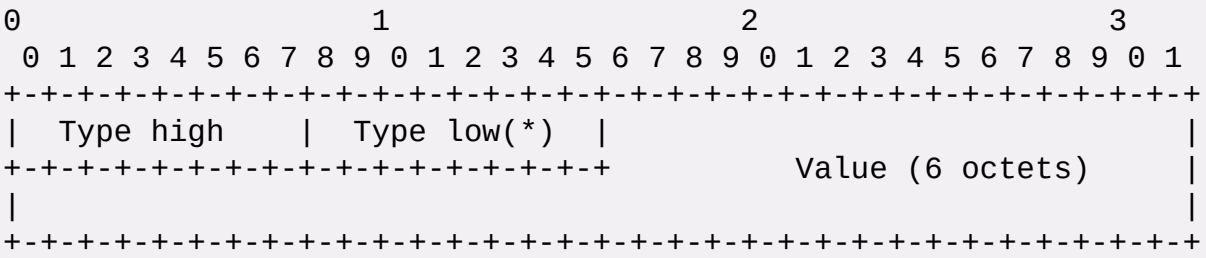



Figure 3-5 – Generic Transitive Extended Community

Table 3-7 Transitive Extended Community types (T-EC-types)

| sub-type | FSv1 Description | Name | Reference |
|---|---|---|---|
| 0x07 | FS Interface set | Ifset | draft-ietf-idr-flowspec-interfaceset |
| 0x08 | FS Redirect/Mirror | RIPv4 | draft-ietf-idr-flowspec-redirect-ip |
| 0x09 | FS Redirect to Indirection ID | RGID | draft-ietf-idr-flowspec-path-redirect |

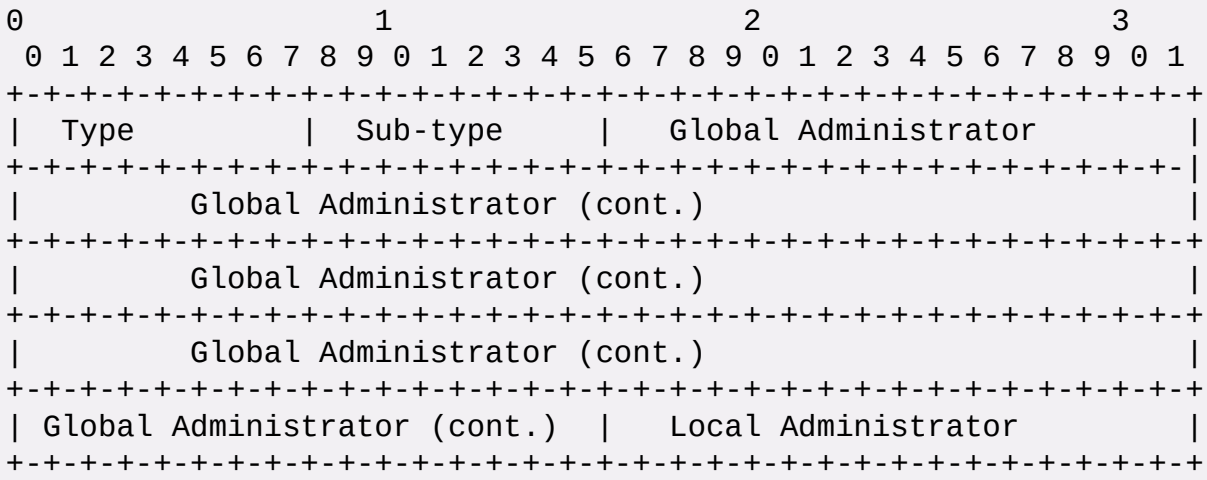



Figure 3-6 Transitive IPv6-Address-Specific-Actions

Table 3-8 Transitive IPv6-Address-Specific Actions

| Value | Description | Name | |
|---|---|---|---|
| **0x01** | **Flow Spec Action Chain** | **ACO** | **This document t** |
| 0x0C | Flow Spec redirect-v6-flag | RD6F | draft-ietf-idr-flowspec-redirect-ip |
| 0x0D | Flow Spec rt-redirect IPv6 format IPv6 format | RDv6 | RFC8956 |

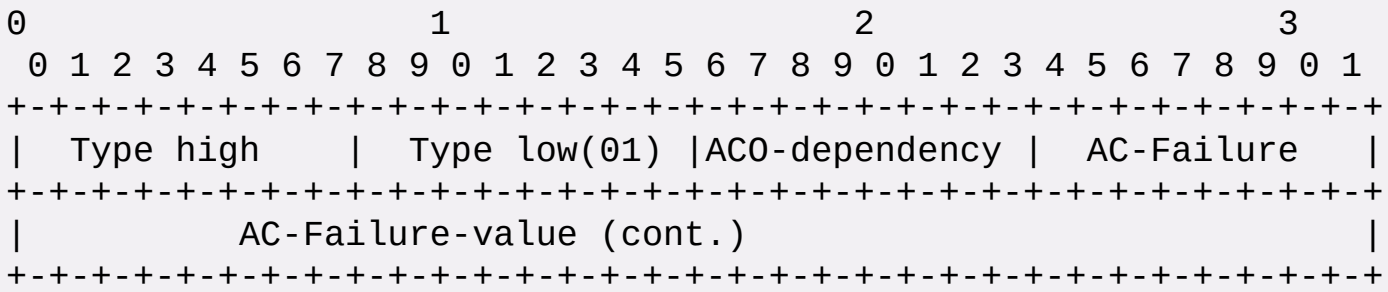



Figure 3-7

**ACO Dependency** - The order dependency within the Action chain.
where: 0 = default order and interactions (from this specification).
1 = Implementation specific ordering

**AC Failure:** Action chain action when an individual action fails
0x00 – default – stop on failure
0x01 – continue on failure (best effort on actions)
0x02 – conditional stop on failure – depending on AC-Failure-value
0x03 – rollback – do all or nothing - depending on AC-Failure-value

Yang configuration uses some of these modes on action failure.

# Questions?