IDR FSv2

IETF-120

IDR session 2: 7/26

FSv2 – Goals

Team 1: **Basic IP FSv2:**

Set minimal subset – V1 (actions + Filters) + User order

Team 2: **Add of New IP Filters + Filter Chains**

Filter Chain = dependency between filters

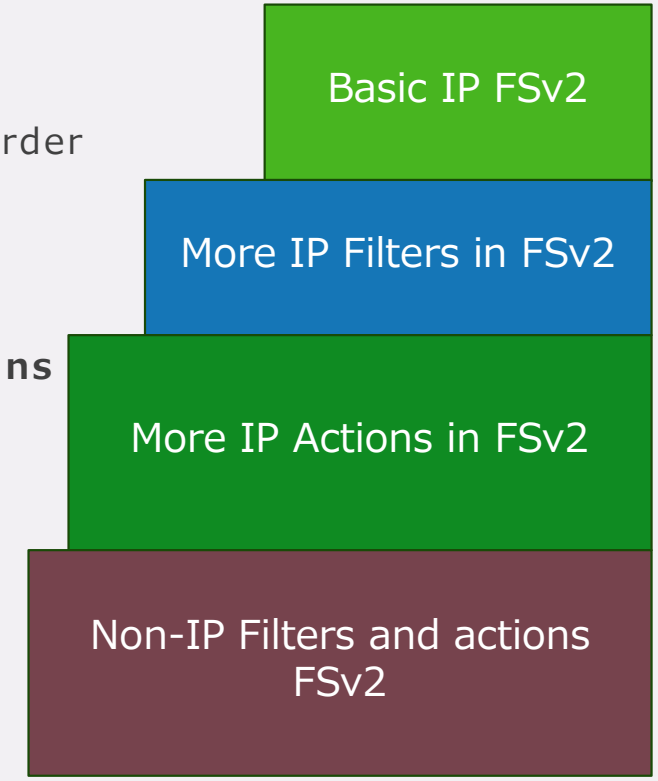
Team 3: New actions with User order + Action chains

- Form: Ext. Community + Wide Community

Action chain = dependency between Actions

Team 4: Non-IP filters and actions FSv2

- “Plug-in” for non-IP filters: L2, MPLS, SFC, Tunnel
- Filters + actions – User ordered + Chains



FSv2 Draft Split = goals

draft-ietf-idr-flowspec-v2 – remains WG document with summary

Split to:

- **draft-ietf-hares-fsv2-ip-basic** – minimal subset (FSv1+ filter ordering)
- **draft-ietf-hares-fsv2-more-ip-filters (team 2)**

  Extended IP filters TLV + filter chains + template for Individual Drafts
- **draft-ietf-hares-fsv2-more-ip-actions (team 3)**

  Format for Actions: Ext Community + Wide Community Action formats

  Description of Action chains (default + user ordered + failure issues)

  Template for specifying new actions in individual drafts
- **draft-ietf-hares-fsv2-non-IP-actions (team 4)**

  Any additional Common header requirements + Templates
- **Individual drafts (TTL, MPLS, SID) – will be generated as WG drafts**

What about I-Ds proposing Flow Specification (FSv2)

FSv1 WG drafts + IDs

- If deployed, need two drafts – FSv1 + FSv2
- If not deployed – use FSv2 templates and update draft
- FSv1 drafts deployments will be tracked on wiki

FSv2 IDs

- Use v2 templates – for filters + actions

Backlog of ID adoptions

- Plan to work templates and IDR I-D adoptions at same time (OK?)

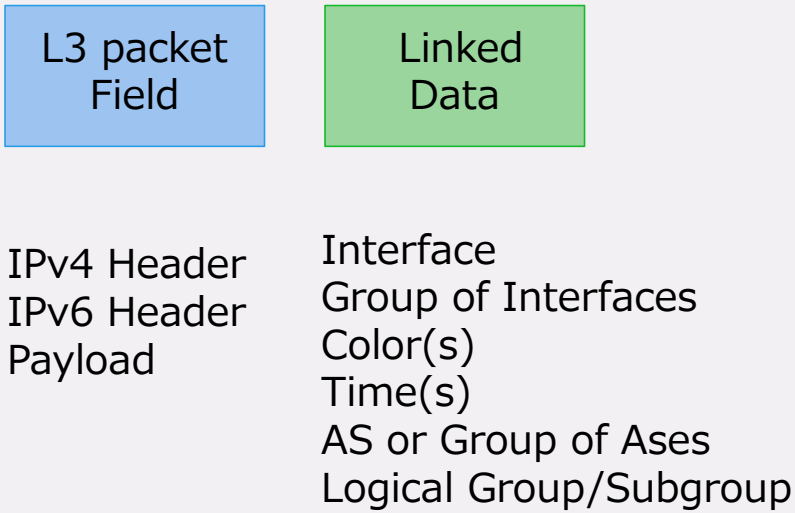
L3 Components as Firewall Rules

L3 Filters – L3 Packet field

- header IPv4 or IPv6
- Payload

Linked data

- smaller area in Firewalls
- Search packet + linked data



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

L3 Components (default order)

14 – TTL
15 – SID in IPv6 Routing header
16 – NRP in Hop-by-Hop IPv6 header
17 – CAT ID (IPv6 header (?))
30 – Payload

Linked data Components (151- 180)

151 interface or interface group
152 Color
153 Time (or times)
154 AS or Set of Ases
155 Group and Sub-group

MPLS Component Numbers [1-2 or 64-65)

01 (64) MPLS Label Match-1 (label)
02 (65) MPLS Label Match-2 (Exp bits)

L2 Component Numbers [1-15 or 81-98]

1 - Ethernet type
2 - Source MAC
3 - Destination MAC
4 – DSAP in LLC
5 – SSAP in LLC
6 – control field in LLC
7 – SNAP
8 – VPAN ID
9 – VLAN PCP
10 – Inner VLAN ID
11 – Inner VLAN PCP
12 - VLAN DEI
13 - Inner VLAN DEI
14 – Src Mac Special bits
15 – Dst Mac Special bits
16 – RSN Mac Data unit
17 – Det. Latency Info

Tunnel Component Numbers [1-11 or 131-142)

01 – VN ID
04 – Cookie
05 – Tunnel header flags
06 – L2TP control version
07 – L2TPv3 Control Connection ID
08 – L2TPv3 Ns
09 – L2TPv3 Nr
10 – Protocol type
11 – GRE Sequence

FSv2 for Basic IP Review

draft-hares-idr-fsv2-ip-basic-03

Sue Hares

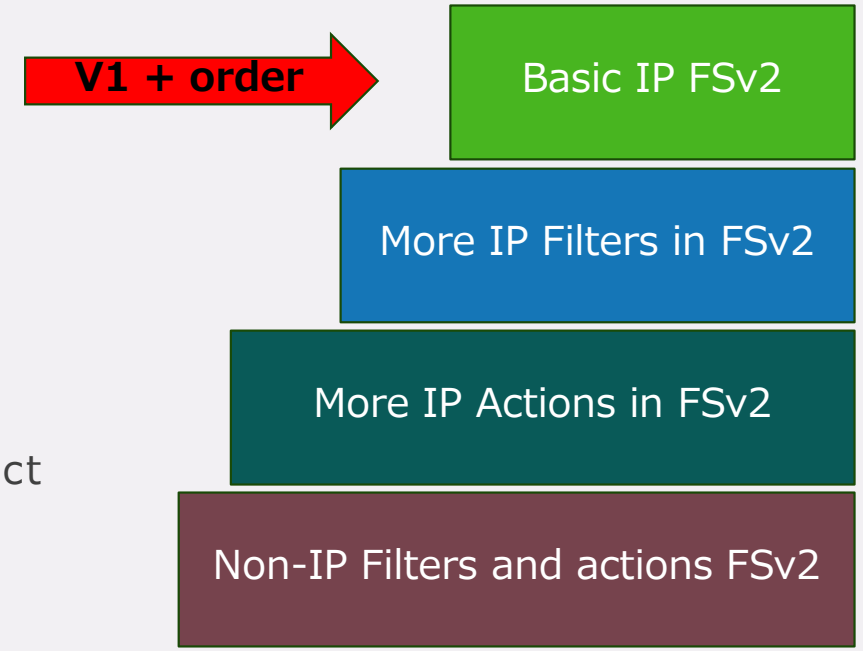
Goals of FSv2 Chunks: Simple + Complex

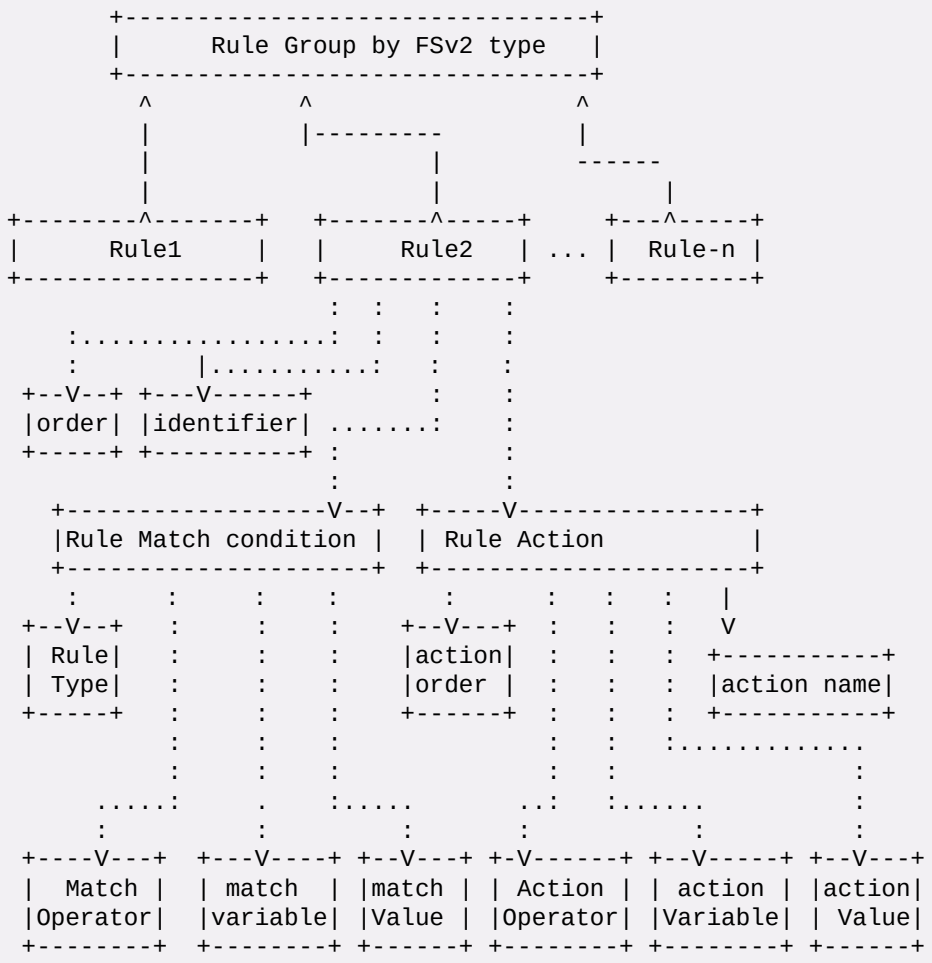
Simple DDOS Update

- User Ordering + FSv1 + Deterministic fixes

Platform for Complex Uses

- More Filters
- More Actions without conflict
- Non-IP Filters





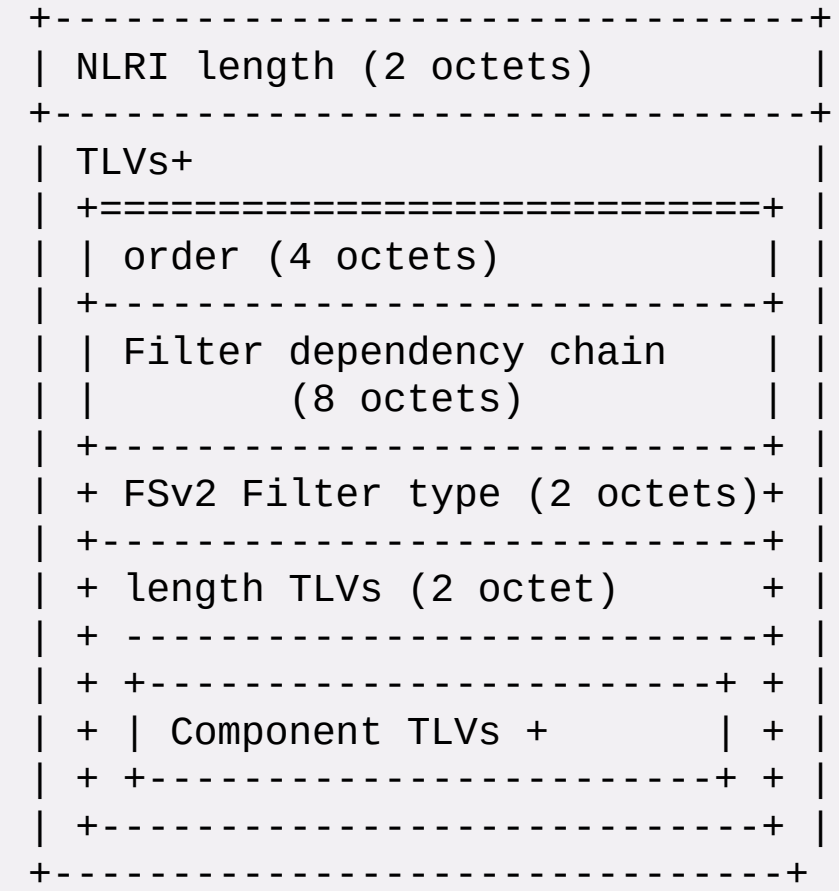
FSv2 Rules (see Rule 2) have

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

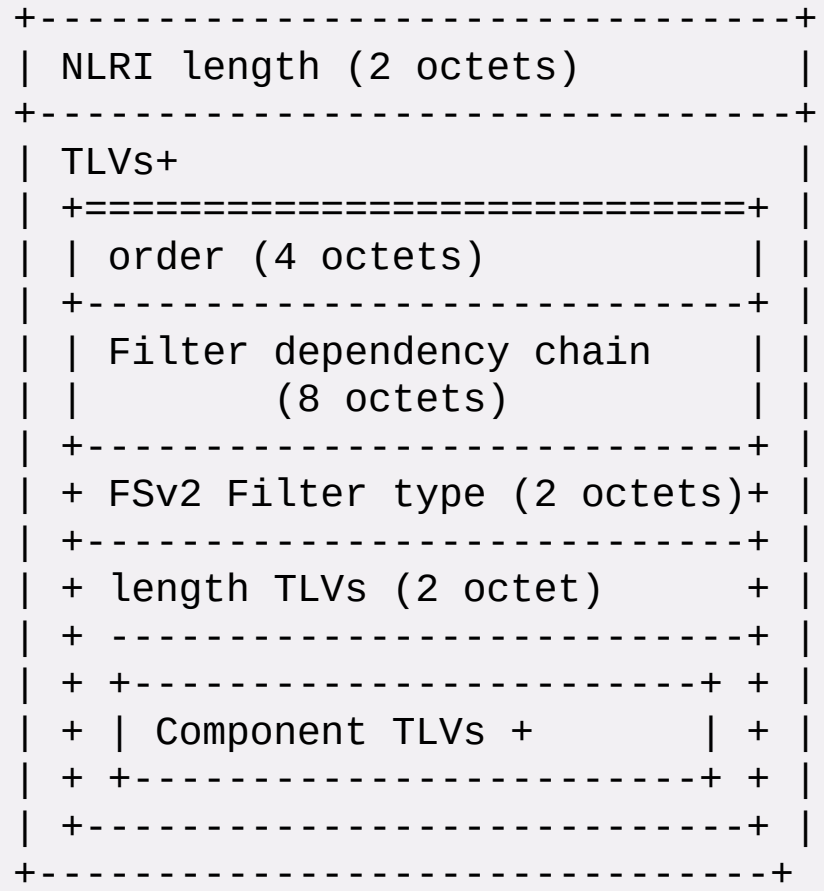
Rule 1-N – Filter traffic to take an action on.



NLRI format for Basic IP Filters

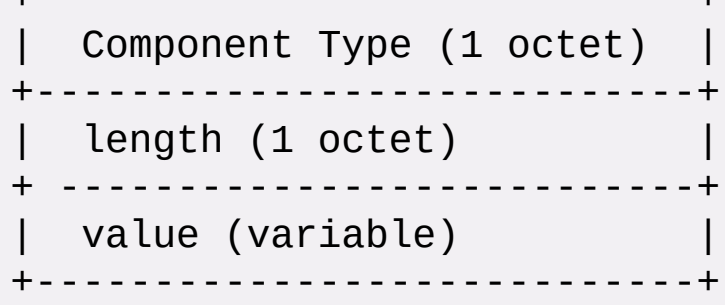
FSv2 Filter types
0 - reserved
1 - IP Basic Filter Rules
2 - Extended IP Filter rules
3 – MPLS traffic rules
4 – L2 Traffic rules
5 – SFC traffic rules
6 – Tunnel traffic rules

IP Basic only has FSv1 Filters



NLRI format for Basic IP Filters

Where the Component TLVs are:



FSv1 IP Component Numbers

0 - Reserved
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

Order of 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

Defaults

- If same user order number, then order by component number.
- If same user order number + same component number,

then order the multiple components (with same user order + same component type) by rules defined in a component.

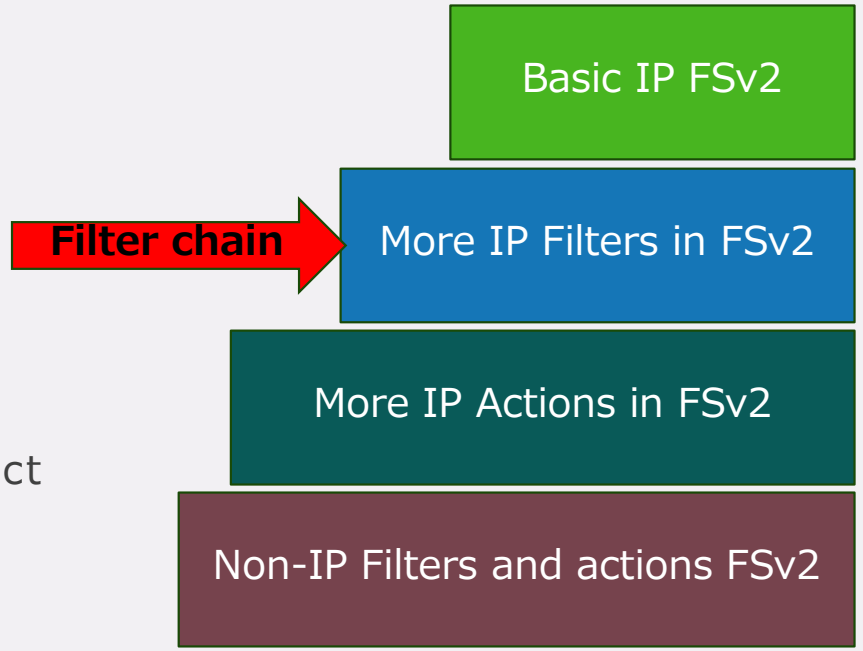
Goals of FSv2 Chunks: Simple + Complex

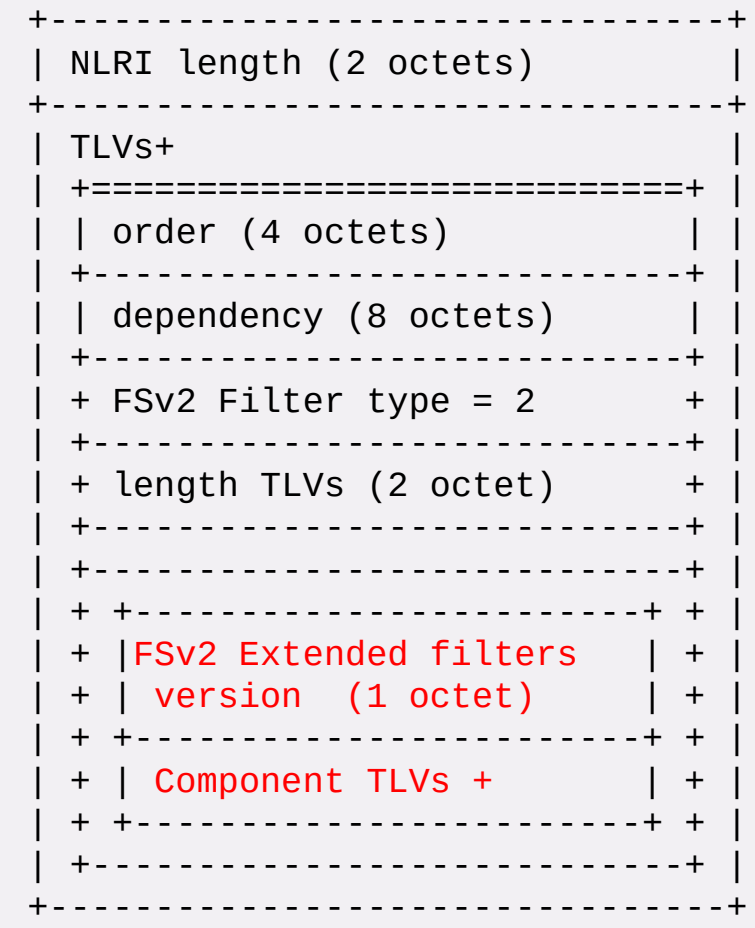
Simple DDOS Update

- User Ordering + FSv1 + Deterministic fixes

Platform for Complex Uses

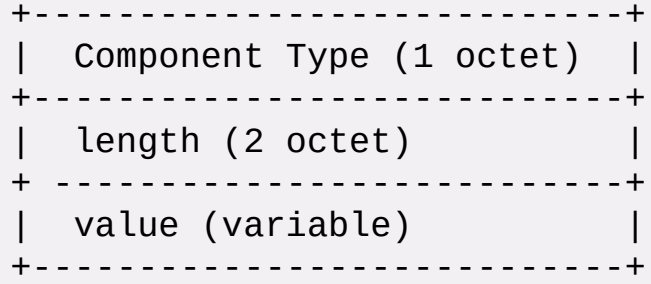
- More Filters
- More Actions without conflict
- Non-IP Filters





NLRI format for Extended IP Filters

Where the Component TLVs are:



- FSv2 Ext Filters Version – allows changed to Extended filter list
- Component length – 1 or 2 octets?

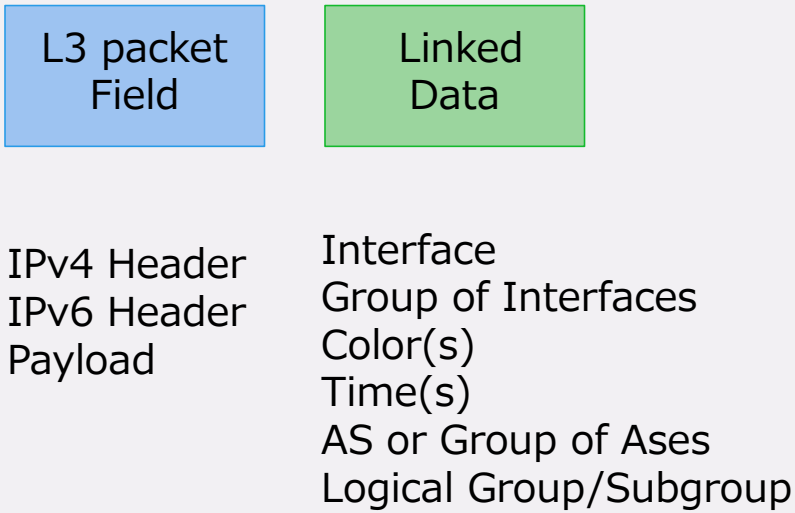
L3 Components as Firewall Rules

L3 Filters – L3 Packet field

- header IPv4 or IPv6
- Payload

Linked data

- smaller area in Firewalls
- Search packet + linked data



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

L3 Components (Unique to each type)

14 – TTL
15 – SID in IPv6 Routing header
16 – NRP in Hop-by-Hop IPv6 header
17 – CAT ID (IPv6 header (?))
18 - SAV ID (IPv6 header) (??)
…
30 – Payload

Linked data

151 interface or interface group
152 Color
153 Time (or times)
154 AS or Set of Ases
155 Group and Sub-group

Global Allocation of Component IDs (all standards action except FCFS)

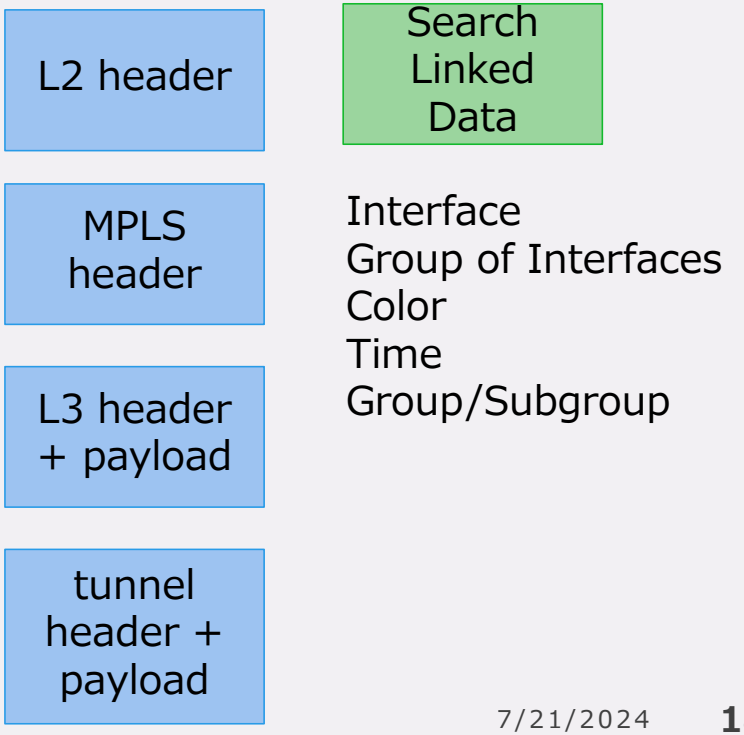
14 - 63 Reserved for IP Extensions
64 - 150 Reserved for Non-IP (MPLS, L2, tunnel)
151 - 180 Associated data (interface, interface group, AS, Time, Color)
181 – 191 Reserved
192 - 240 FCFS
241 - 255 Reserved

All Components as Firewall Rules

- **Default order of NLRI**
- L3, MPLS, L2, SFC, Tunnel
- Linked data linked to packet match

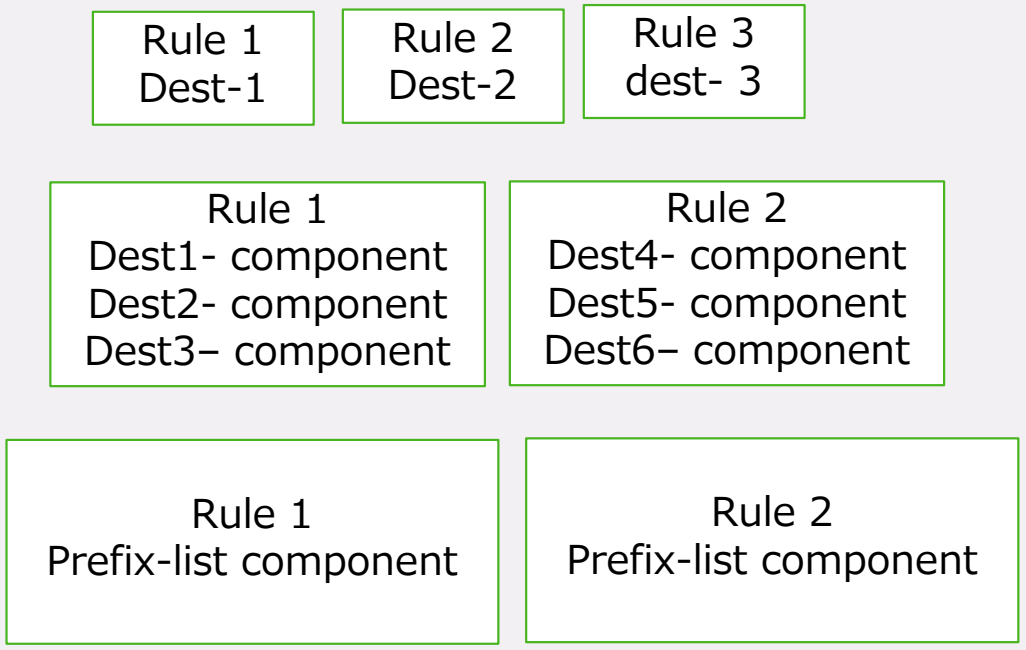
Global Allocation of Component IDs

14	- 63	Reserved for IP Extensions
64	- 80	MPLS (Std. Action)
81	- 120	L2
121	- 130	SFC
131	– 150	Tunnel
151	- 180	Linked data
181	– 191	Reserved
192	- 240	FCFS
241	- 255	Reserved



Prefix lists Implementation

1) User order (1..n) – with current TLVs (destination)
2) One User order with Multiple IP destinations ordered by Prefix
3) New Component – that has prefix lists in a different format



Component Number assignments

- Only per filter type (L3, MPLS, L2, SFC, tunnels) –

or

- Components assigned in global ranges

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

L2 Component Numbers [1-15 or 81-98]

1 - Ethernet type
2 - Source MAC
3 - Destination MAC
4 – DSAP in LLC
5 – SSAP in LLC
6 – control field in LLC
7 – SNAP
8 – VPAN ID
9 – VLAN PCP
10 – Inner VLAN ID
11 – Inner VLAN PCP
12 - VLAN DEI
13 - Inner VLAN DEI
14 – Src Mac Special bits
15 – Dst Mac Special bits
16 – RSN Mac Data unit
17 – Det. Latency Info

L3 Components (default order)

14 – TTL
15 – SID in IPv6 Routing header
16 – NRP in Hop-by-Hop IPv6 header
17 – CAT ID (IPv6 header (?))
30 – Payload

Linked data (151- 180)

151 interface or interface group
152 Color
153 Time (or times)
154 AS or Set of Ases
155 Group and Sub-group

MPLS Component Numbers [1-2 or 64-65)

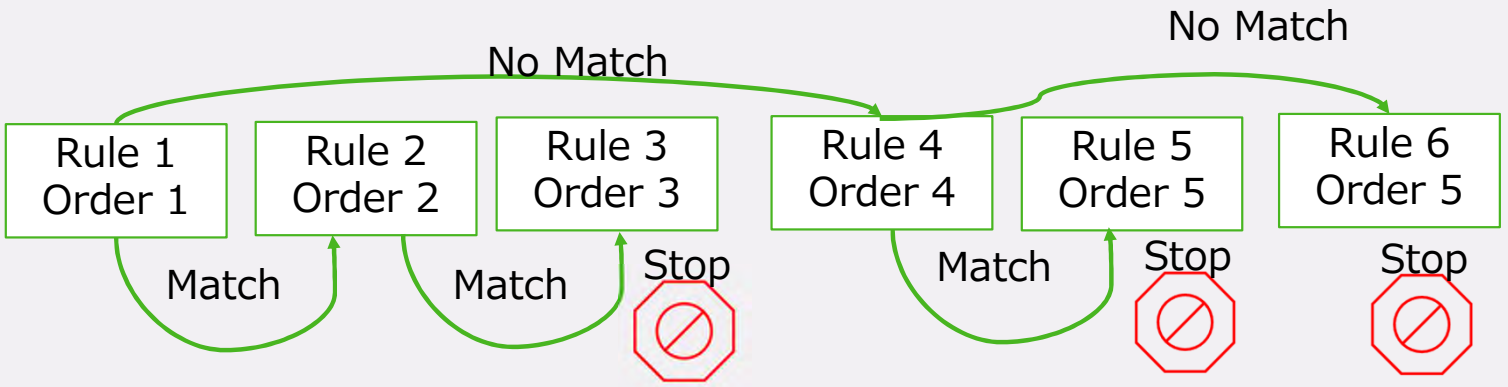
01 (64) MPLS Label Match-1 (label)
02 (65) MPLS Label Match-2 (Exp bits)

Tunnel Component Numbers [1-11 or 131-142)

01 – VN ID
04 – Cookie
05 – Tunnel header flags
06 – L2TP control version
07 – L2TPv3 Control Connection ID
08 – L2TPv3 Ns
09 – L2TPv3 Nr
10 – Protocol type
11 – GRE Sequence

Filter dependency chain logic

- Chain on Rule (User Order, simple)



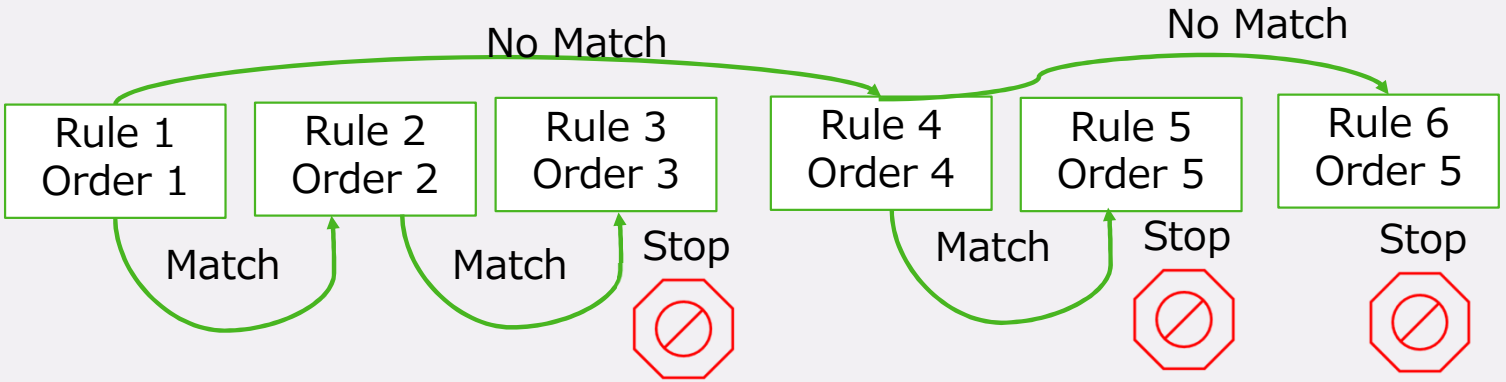
Complex rules: (wait until reason)

- User Order (chain) + Rule component chain (?)
- Conditional actions

Example 1: Packet rate limit (DDOS)

Rule 1: match Loc
Rule 2: match Destination Port 30
Rule 3: match Source Port 20
Action: Drop

Rule 4: match IP Dst-addr: 192.3.4/24
Rule 5: match Source Interfaces: if-2, if-3
Action: copy and drop
Rule 6: match IP Src-Addr: 192.5.2.1
Action: Drop



Example 2: Nat Kao's example of modifying packet

- A packet with DSCP 0 hits Rule 100.

  Rule 100 has actions <Set DSCP 4, GOTO Rule 400>.

  Rule 400 is matching against DSCP 4.

- Will that packet be considered a match for Rule 400?

  Rule 400 will match the modified packet, if we apply actions **after each rule**.

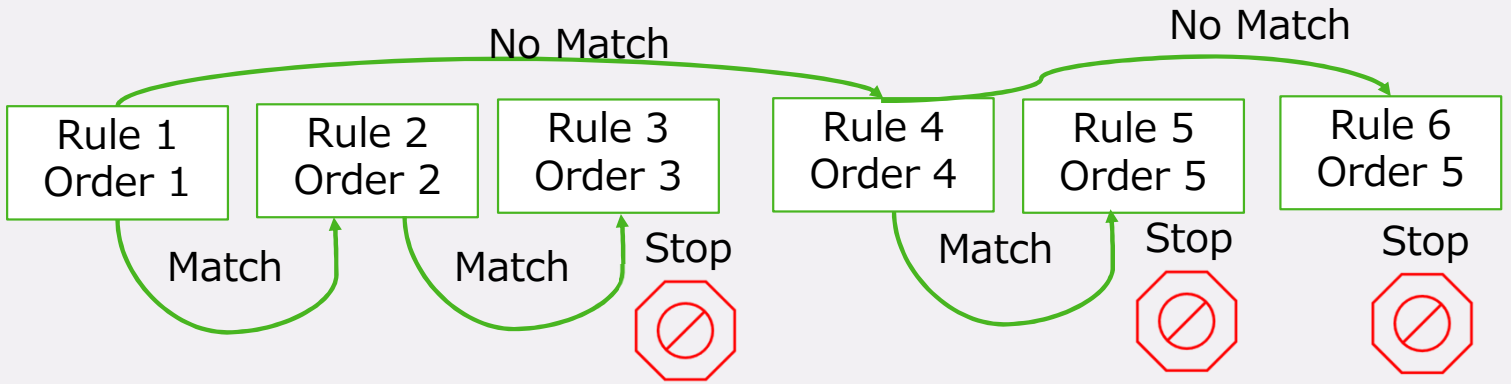
  Rule 400 will not match the unmodified packet, if we apply actions **after all rules**.

- Should we modify packets as soon as the match occurs?

Example 3: SR Header + NRP Example

Rule 1: Match Loc: SID1, FCN: End.X,
Arg: 128.2.1.1
Rule 2: match NRP-ID 10 in Hop by Hop
Rule 3: match Source Port 10
Action: Drop

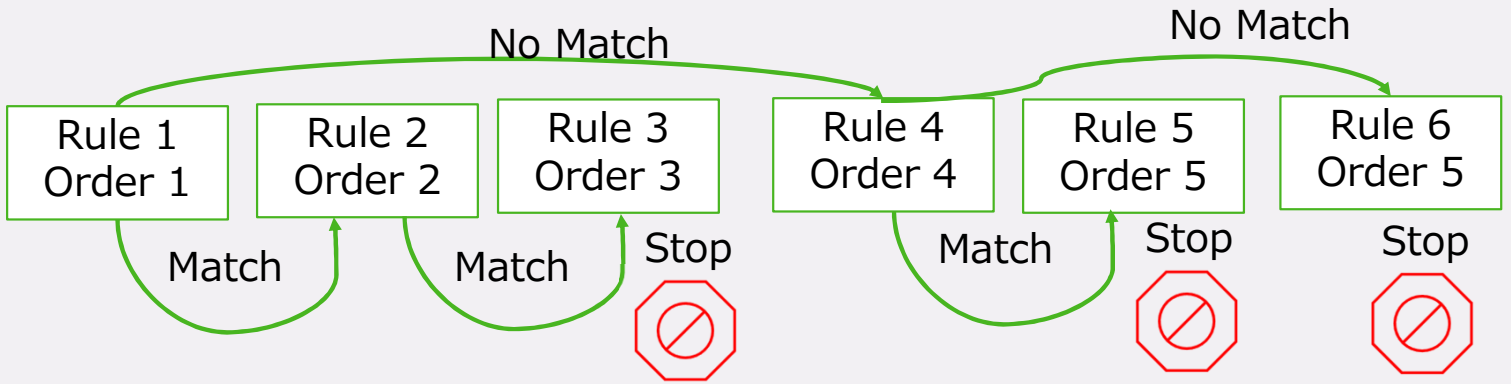
Rule 4: Match Loc: SID1, FCN: End.X,
Arg: 128.2.1.2
Rule 5: match NRP-ID 20 in Hop by Hop
Action: Copy and redirect to IP
Rule 6: Match IP Address 192.5.2.1
Action: drop



Example 4: Color + IP Prefix to place on Tunnel (SR or IP-sec)

Rule 1: Match Color: 20 (blue)
Rule 2: Match Dest Address: 128.2/16
Rule 3: Source Port 10
Action: redirect to 192.5.2.5

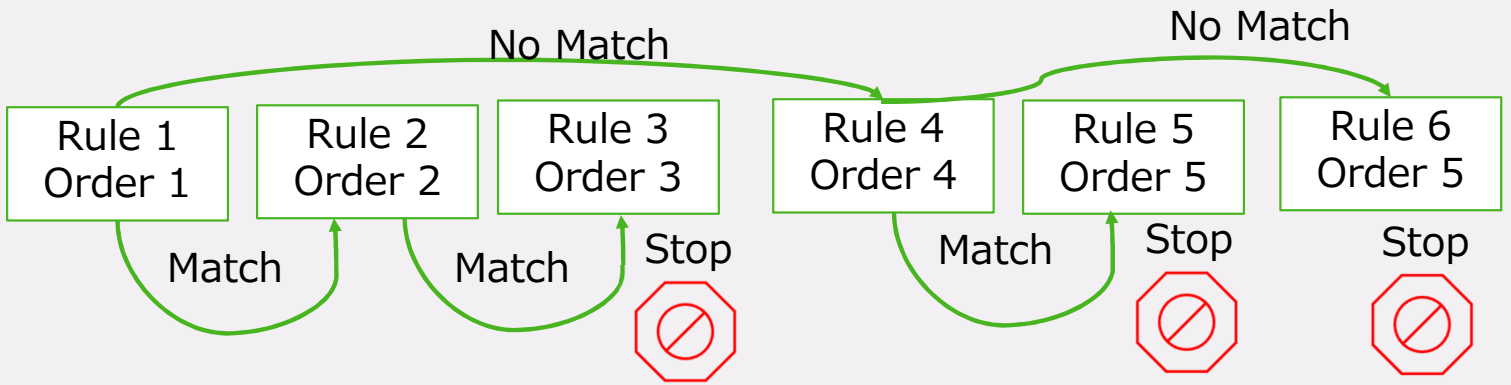
Rule 4: Match Color: 30 (gold)
Rule 5: Match Dest Address 129.4/16
Action: redirect to IP-sec tunnel
Rule 6: Match Color: 50 (red)
Action: drop



Example 5: Deep packet inspection

Rule 1: Match Destination Port (App-1)
Rule 2: Match Payload-1
Rule 3: Match Payload-2
  Action: copy and drop

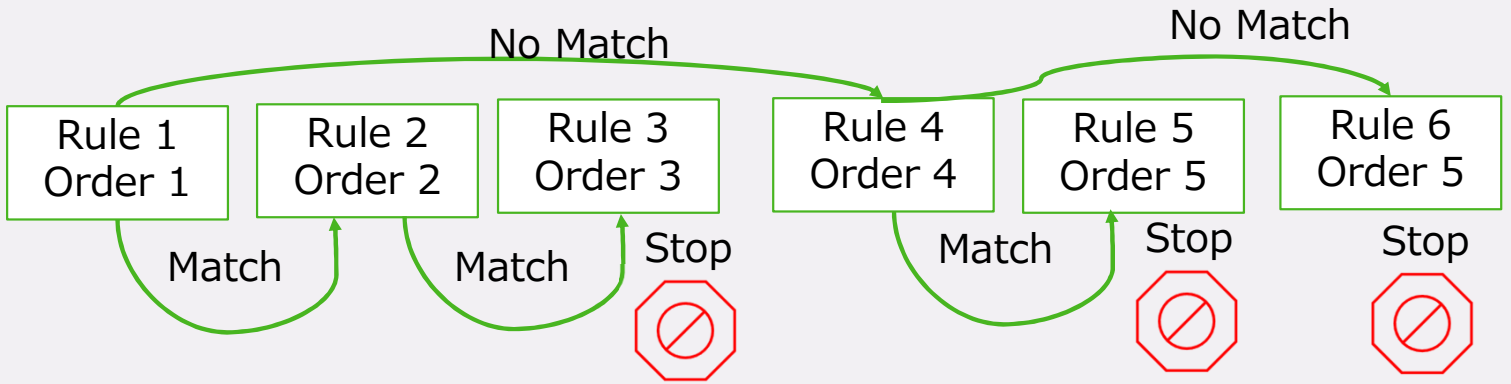
Rule 4: Match Source Port (attack-1)
  Action: rate limit
Rule 5: Match Payload-3
  Action: copy and drop
Rule 6: Match Source Port 2 (attack-2)
  Action: rate limit + forward



Example 6: Other data

Rule 1: Interface Group 1
Rule 2: AS 120
Rule 3: Mtach Prefix list
  Action: drop

Rule 4: Match Group-ID 1
Rule 5: Match Subgroups 1-3
Action: rate limit, mark NRP-10, redirect to SID1
Rule 6: Match Group-ID 2
Action: mark NRP-20, redirect to SID2



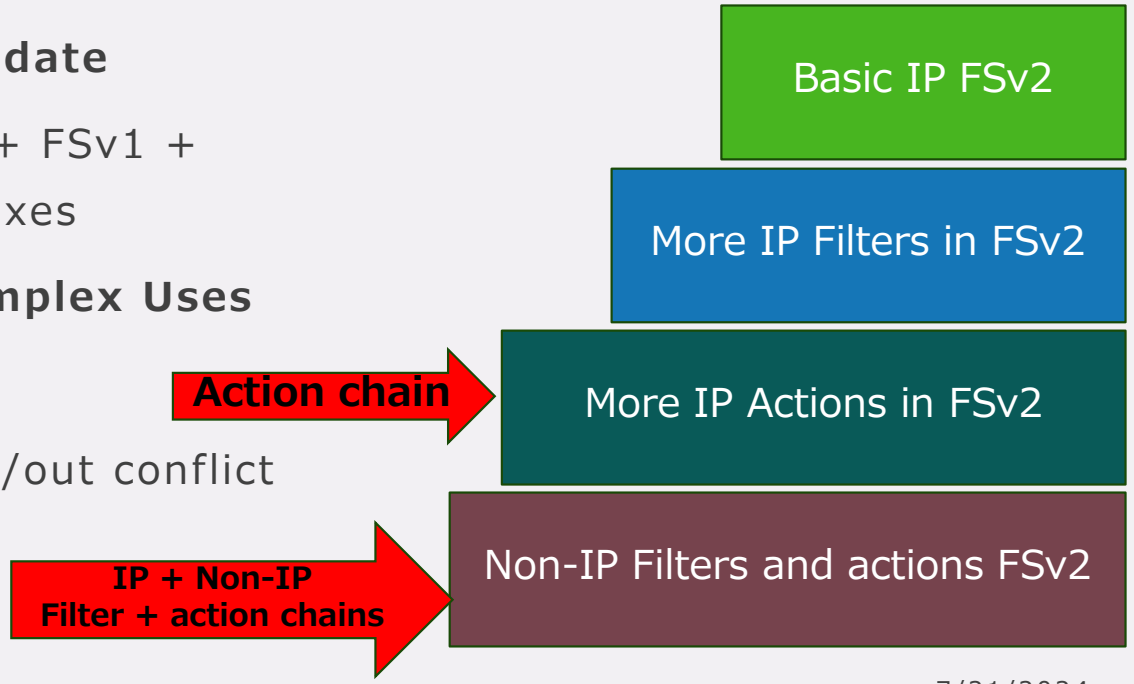
Goals of FSv2 Chunks: Simple + Complex

Simple DDOS Update

- User Ordering + FSv1 + Deterministic fixes

Platform for Complex Uses

- More Filters
- More Actions w/out conflict
- Non-IP Filters



Drafts on Actions

Draft	redirect	Seq	copy	mark	Pkt
draft-ietf-idr-flowspec-redirect-ip	IPv4/v6		X		
draft-ietf-idr-flowspec-path-redirect	V4 to GID	X	X		
draft-ietf0-idr-srv6-flowspec-path-redirect	V6 to GID	X	X		
draft-ietf-idr-ts-flowspec-srv6-policy	SID Tunnel				
draft-ietf-idr-flowspec-network-slice-ts				nrp-id	Encap
draft-dmc-idr-flowspec-tn-aware-mobility	IPSec tunnel			nrp-id	
draft-lin-idr-cats-flowspec-ts				cat-id	
draft-shen-idr-flowspec-traffic-compress-action					**Compress**
draft-peng-idr-apn-bgp-flowspec				apn-id	Sitch inherit

Encoding the Actions

Extended Communities (EC) – FSv2-EC Actions in

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

Community Attribute Actions – User Ordered Actions

- Community Attribute with a FSv2 Community type

Action Chain Ordering: Default + Failure of FSv2 Actions

Ordering of FSv2 Actions

- First: User-Ordered [Community Path Attribute]
- Second: Pre-defined Extended Community ordered by Type

Transitioning from FSv1 Extended Community

- Configuration knobs to Allow FSv1 Actions
- Configuration knobs must be consistent within AS or a Group of AS

What happens on Failure (Action Chain Ordering Action)

- 4 Cases in NETCONF Configuration – Stop (Terminate), Go on (Best effort), Conditional Go on, Rollback changes

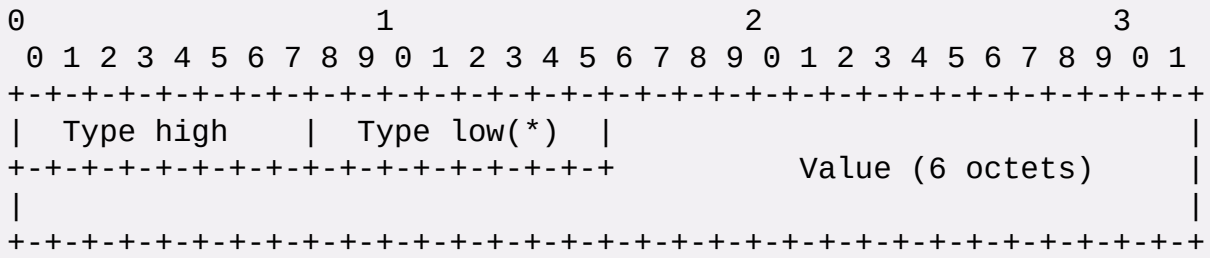


Figure 3-5 – Generic Transitive Extended Community

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**	[ip-basic]
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]

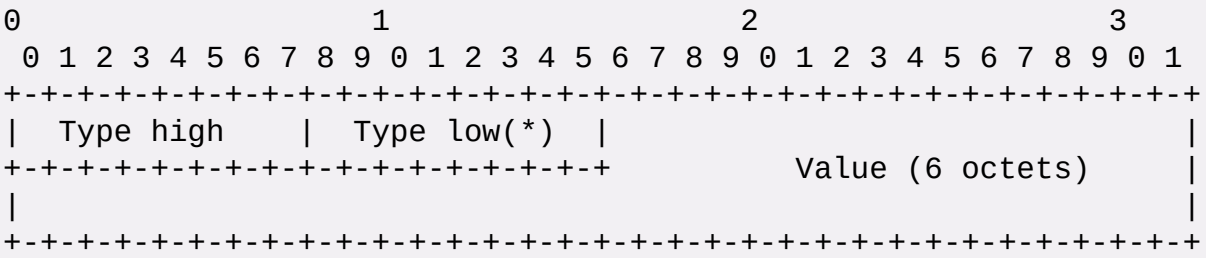


Figure 3-5 – Generic Transitive Extended Community

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

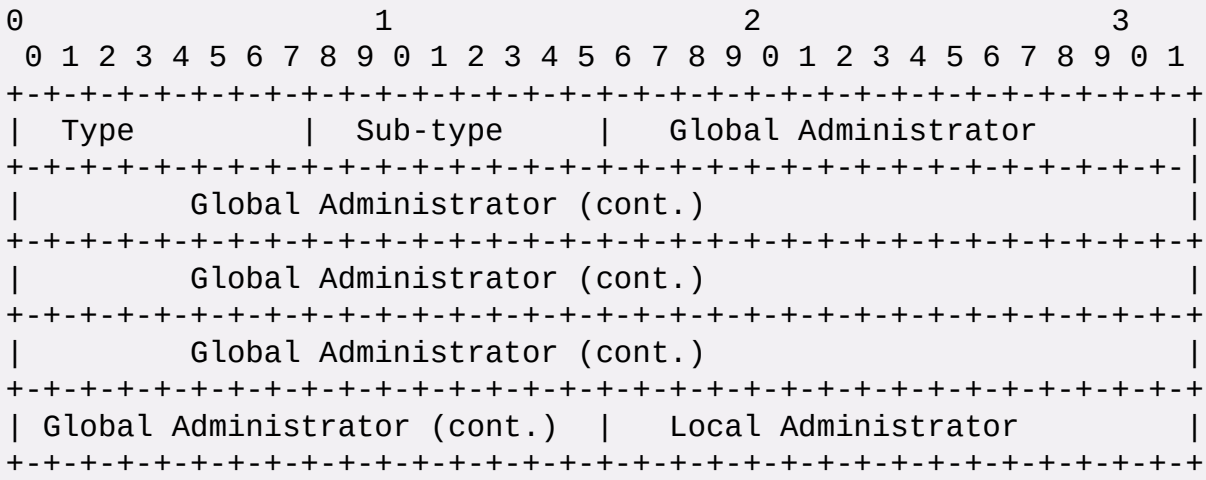


Figure 3-6 Transitive IPv6-Address-Specific-Actions

Table 3-8 Transitive IPv6-Address-Specific Actions

Value	Description	Name	
0x01	**Flow Spec Action Chain**	**ACO**	**[draft-ietf-hares-ip-basic]**
0x0C	Flow Spec redirect-v6-flag	RD6F	draft-ietf-idr-flowspec-redirect-ip
0x0D	Flow Spec rt-redirect IPv6 format IPv6 format	RDv6	RFC8956

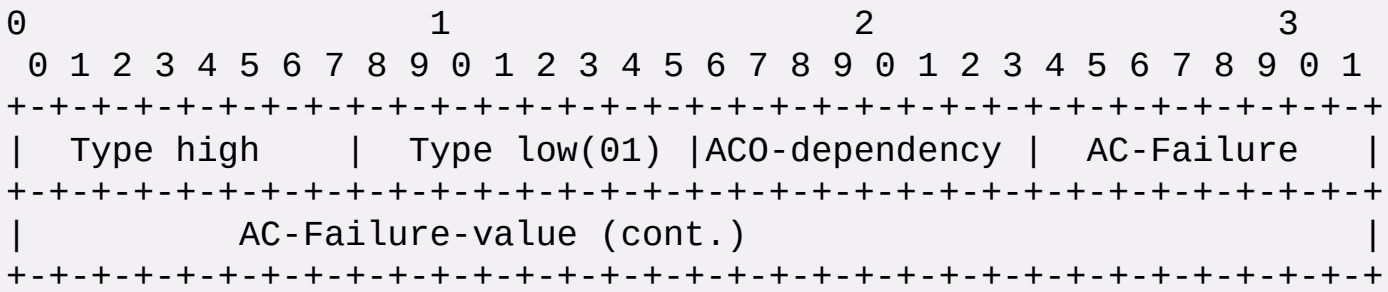


Figure 3-7

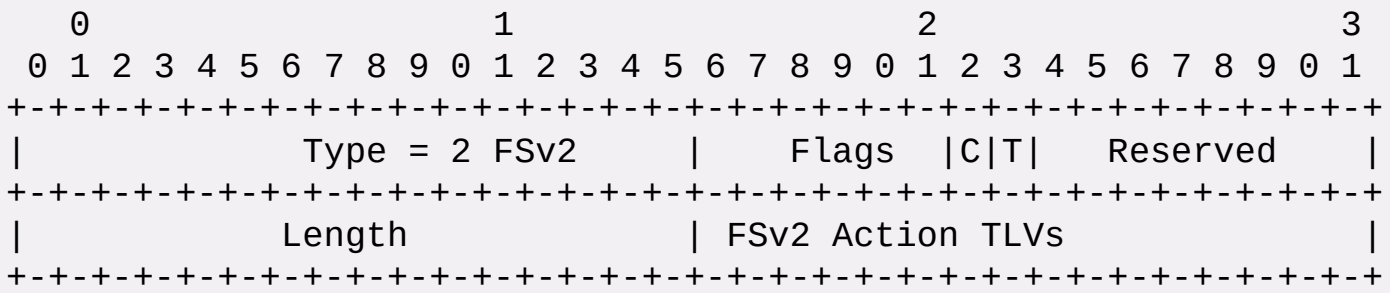
ACO Dependency - The order dependency within the Action chain.
where: 0 = default order and interactions (from this specification).
1 = Implementation specific ordering

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

Note: Yang configuration uses some of these modes on action failures.

FSv2 in Community Attribute header

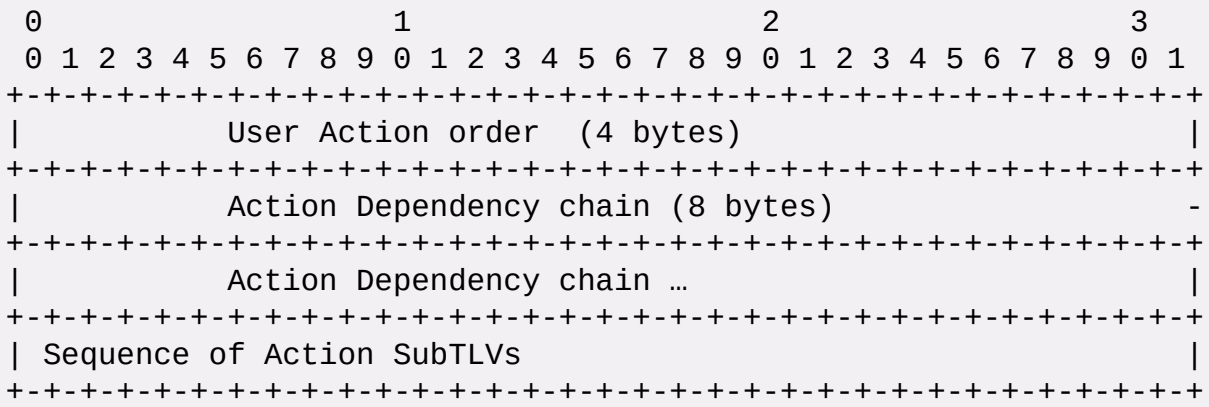
Community Path attribute common header (figure 2-3)



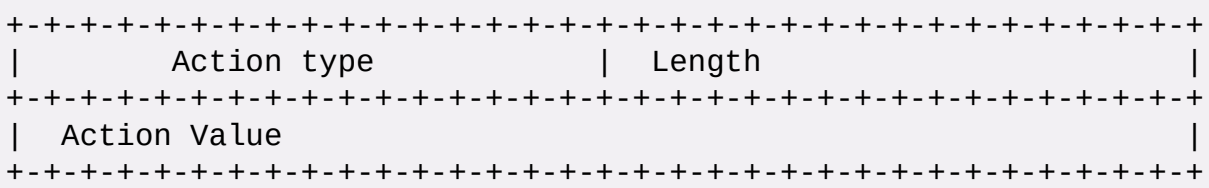
C = 1 - Transitive across Confederation boundaries
C = 0 - Non-transitive across Confederation boundaries
T = 1 – Transitive across AS boundaries
T = 0 – Non-Transitive across AS boundaries

Action TLV + SubTLV Format

Common Header for Action TLVs (figure 2-5)



Each Action SubTLV has the format:



Action TLVs for Community Path Attribute

Table 5-5 All Actions Proposed for FSv2 Community Path Attribute

act-id	Name	Description	Document
TBD	MatchSet	Match and Set attribute	[IDR-rpd] (type = 03)
TBD	MatchNoA	Match and No Advertise	[IDR-rpd] (type = 04)
TBD	DetLat	Deterministic Latency action	[PD-detnet-flowmap] (type = 37)
TBD	TSNMap	Map flow to TSN stream	[PD-detnet-flowmap] (type = 38)

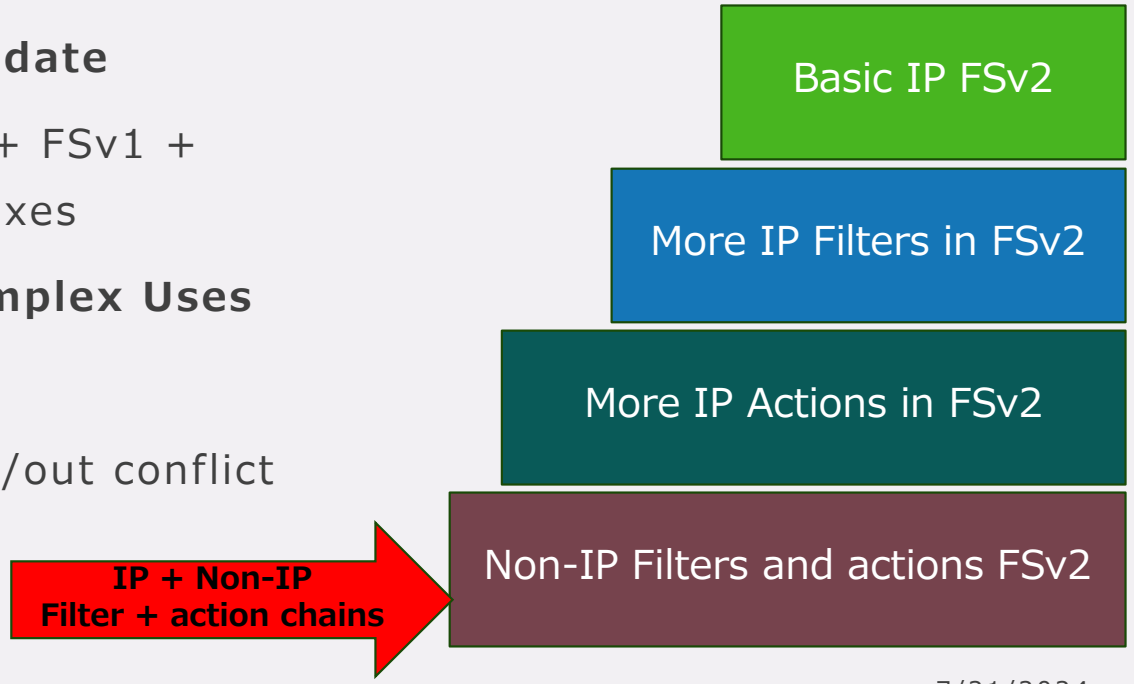
Goals of FSv2 Chunks: Simple + Complex

Simple DDOS Update

- User Ordering + FSv1 + Deterministic fixes

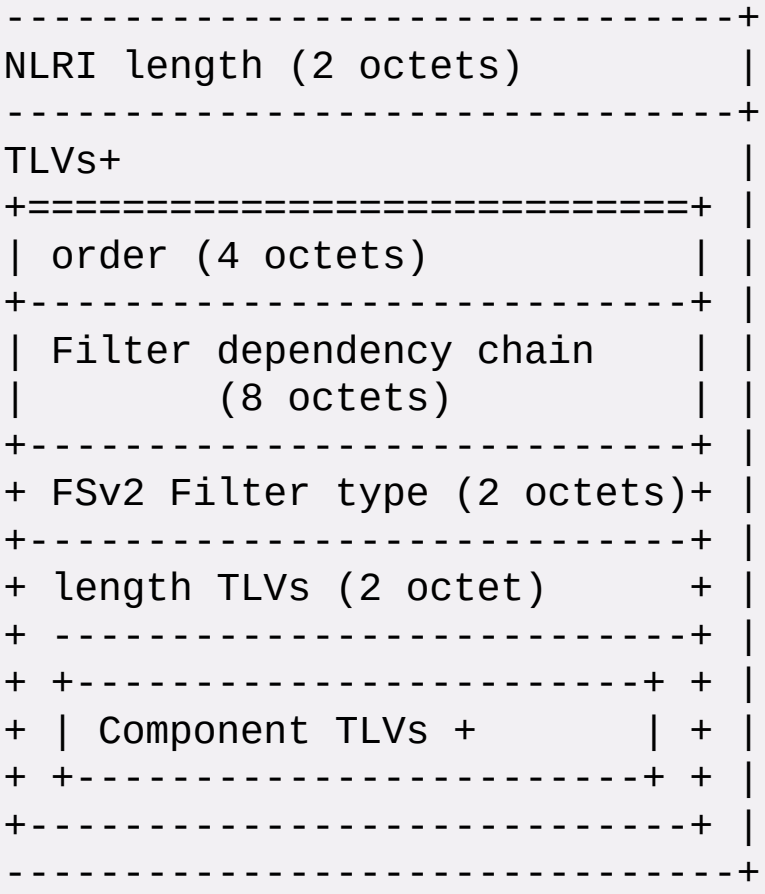
Platform for Complex Uses

- More Filters
- More Actions w/out conflict
- Non-IP Filters



Filters + Actions for Non-IP

Draft	Filter	mark	Actions
draft-ietf-idr-flowspec-v2	MPLS label EXP bits		Push/pop/ swap labels
RFC9015	IP		SFC classifier (SPI, SI, SPT)
draft-ietf-idr-flowspec-l2vpn	L2 header (15 items)	Rewrite VLAN ID (inner or outer)	Push/pop/ swap VLAN
			Ma TPID action
draft-ietf-idr-ts-flowspec-srv6-policy	SID Tunnel		SFC classifier (SPI, SI, SPT)
draft-ietf-idr-flowspec-nv03	VLAN, GRE, L2TP	DSCP (outer)	None
draft-xiong-idr-detnet-flow-mapping	MAC + TSN info	Set latency TSN / Profile	Map flow to TSN stream (L2)



NLRI format for Basic IP Filters

FSv2 Filter types
0 - reserved
1 - IP Basic Filter Rules
2 - Extended IP Filter rules
3 – MPLS traffic rules
4 – L2 Traffic rules
5 – SFC traffic rules
6 – Tunnel traffic rules
7-249 – TBD
250-end (Reserved)

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

L2 Component Numbers [1-15 or 81-98]

1 - Ethernet type
2 - Source MAC
3 - Destination MAC
4 – DSAP in LLC
5 – SSAP in LLC
6 – control field in LLC
7 – SNAP
8 – VPAN ID
9 – VLAN PCP
10 – Inner VLAN ID
11 – Inner VLAN PCP
12 - VLAN DEI
13 - Inner VLAN DEI
14 – Src Mac Special bits
15 – Dst Mac Special bits
16 – RSN Mac Data unit
17 – Det. Latency Info

L3 Components (default order)

14 – TTL
15 – SID in IPv6 Routing header
16 – NRP in Hop-by-Hop IPv6 header
17 – CAT ID (IPv6 header (?))
30 – Payload

Linked data (151- 180)

151 interface or interface group
152 Color
153 Time (or times)
154 AS or Set of Ases
155 Group and Sub-group

MPLS Component Numbers [1-2 or 64-65)

01 (64) MPLS Label Match-1 (label)
02 (65) MPLS Label Match-2 (Exp bits)

Tunnel Component Numbers [1-11 or 131-142)

01 – VN ID
04 – Cookie
05 – Tunnel header flags
06 – L2TP control version
07 – L2TPv3 Control Connection ID
08 – L2TPv3 Ns
09 – L2TPv3 Nr
10 – Protocol type
11 – GRE Sequence

Action TLVs for Community Path Attribute

Table 5-5 All Actions Proposed for FSv2 Community Path Attribute

act-id	Name	Description	Document
TBD	MatchSet	Match and Set attribute	[IDR-rpd] (type = 03)
TBD	MatchNoA	Match and No Advertise	[IDR-rpd] (type = 04)
TBD	DetLat	Deterministic Latency action	[PD-detnet-flowmap] (type = 37)
TBD	TSNMap	Map flow to TSN stream	[PD-detnet-flowmap] (type = 38)

Questions