FSv2 Revision

Susan Hares and Jeff Haas

draft-ietf-idr-fsv2-ip-basic-10

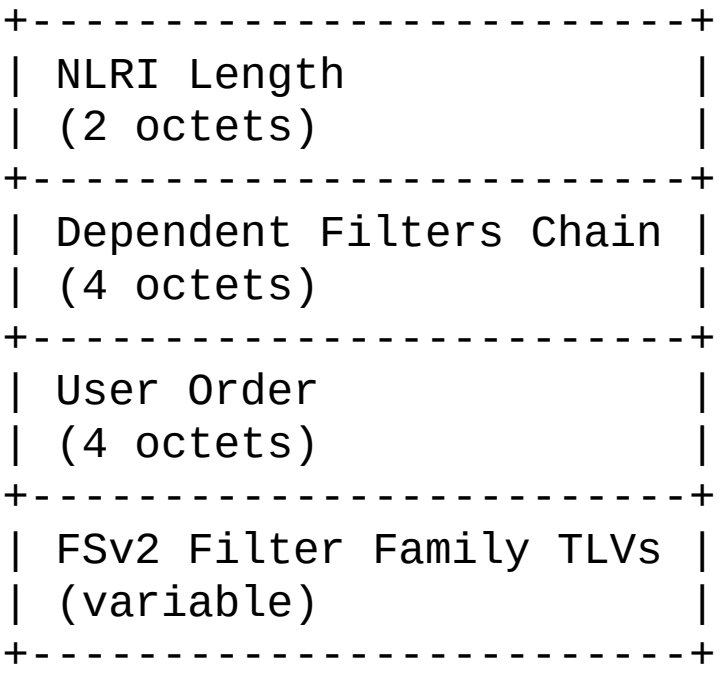
IETF 126

Topics

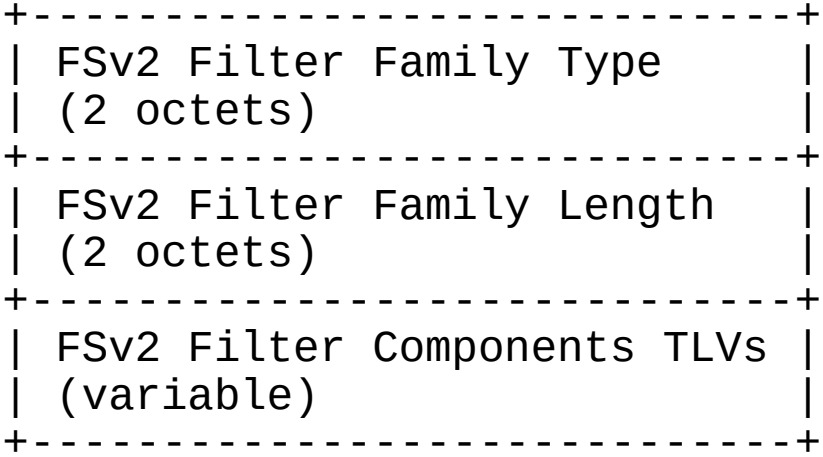
- **FSv2 NLRI**
- **Open capabilities (new)**
- **IP Basic Filter Family Components**
- **Partial Deployments**
- **Actions**
- **Validation Rules**
- **Next Steps**

2 SAFIs – Unicast, VPN
FSv2 – NLRI
FSv2 ordering:
User-order, Filter-Family, Component, Component values

FSv2 header



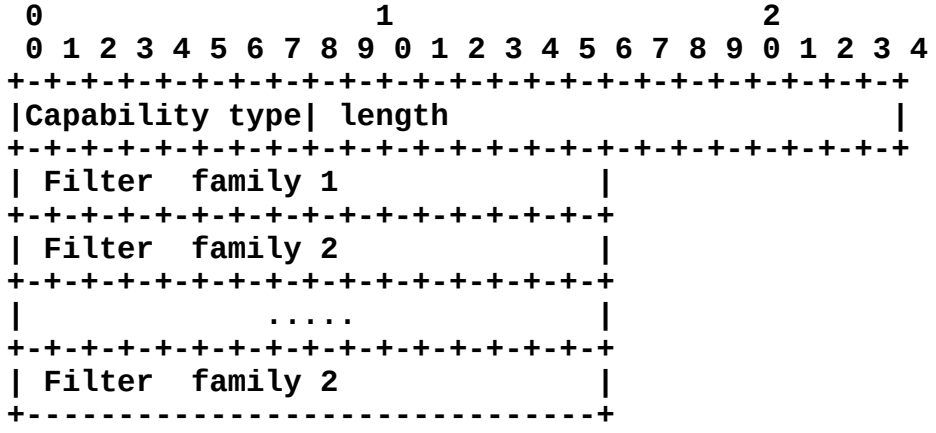
FSv2 Filter Family TLVs



Juniper Business Use Only

Open Capability – Signals filter families

New In -10



Filter Family ordering

- FSv2 implementations MUST pass valid filter Family TLVs even if the implementation does not understand them.
- All Filter Family TLVs within the FSv2 NLRI MUST be ordered in a strictly increasing fashion.
- FSv2 filter types and FSv2 filter-type-specific component types for a given component MUST NOT occur more than once.

FSv2 ordering:

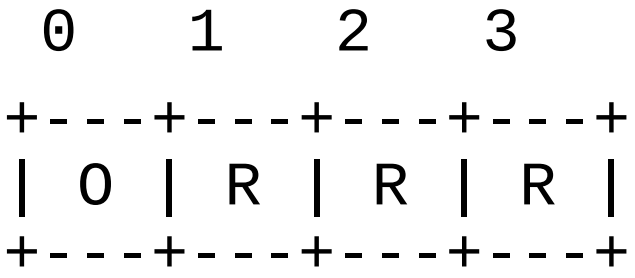
- User-order, Filter-Family, Component, Component values

Dependencies

Dependency Filter Chain (DFC) is a number (4 octets)

- If DFC is a zero (0), then no consideration is given for dependencies
- If DFC is non-zero (n), then FSv2 Filters that share the dependency number share fate
- If a filter with DFC value (n) is invalid, then all filters with DFC value of n are invalid.

Filter Component Flags



O – Optional

R – Reserved

- **Optional flag** signals that a component, if it can't be installed, can be safely ignored for the filter term covered by the NLRI.
  - The default (zero) is "**mandatory**"
- When a mandatory component can't be installed, the entire filter term for the flow specification is NOT installed.

Juniper Business Use Only

DSCP Example

rule 1. match dst=10.1.1.1/24 tcp port=25 then dscp=AF1 and permit

rule 2. match dst=10.0.0.0/8 tcp port=25 then drop

If the router firewall cannot install rule 1, then all packets are dropped.

If rule 1 and rule 2 have a dependency number (10), then if rule 1 is invalid – both rule 1 and rule 2 are ignored.

Filter Families

0 – Reserved
200 – Time
300 – Interface
400 – L2 traffic rules
500 – MPLS traffic rules
600 – SFC Traffic Rules
700 - Queued Pair
800 – Tunneled traffic
1000 – IPv4 Basic
1100 – IPv6 Basic
1200 – CATs
1400 – Routing

Drafts can propose new filter families:
AFI/SAFIs that validate
Components valid for the filter family

Current assignments are at

https://wiki.ietf.org/group/idr/FSv2-Alloc

The goal is to leave space to add new components or filter families at a later date and have them able to be inserted in the natural sort order.

IPv4/IPv6 Basic Components

Component ID

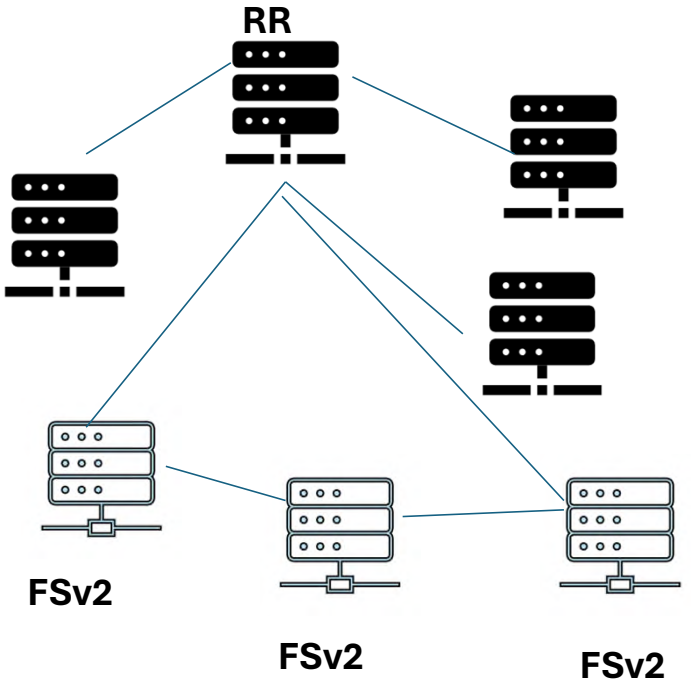
0 – Reserved
100 – Destination QP
300 – Some parts of SRHv6
500 – NRP ID SR Next Hop Header
800 - Bitwise IPv4 Destination
810 – Bitwise IPv6 Destination
1000 – IPv4 Destination
1010 – IPv6 Destination
1100 – Bitwise Source Filter IPv4
1110 – Bitwise Source Filter IPv6
1200 – IPv4 Source Prefix
1210 – IPv6 Source Prefix
1300 – IPv4 Protocol

Component ID

1310 – IPv6 UL Protocol
1400 – Port
1500 – Destination Port
Connection ID
1600 - Source Port
Connection ID
1700 – ICMPv4 Type
1710 – ICMPv6 Type
1800 – ICMPv4 Code
1810 – ICMPv6 Code
1900 – TCP (v4) Flags
1910 – TCP (v6) Flags
2000 - Packet length
2100 – DSCP
2200 – Fragment
2300 – Flow Labe

3000- Packet Content
3100 – Quic Dest.
3110 - Quic Source
3120 – Quic header flags

Partial Deployment



- Reason 1: Only a portion of nodes (white) support FSv2 filter type
  - RR and other BGP only check syntax and not meaning.
- Reason 2: During upgrades only a portion of nodes know about new filter type.

Actions proposed in FSv1 or FS

Types of Actions

- Further constraint of matches – Grouping
- Apply Traffic shaping
- Change IP packet
- Redirect
- Flag traffic for sampling
- Terminate

- If FS (v1 or V2) Filters have multiple actions of a single type of action, then problems can occur in Extended Communities
- If FSv2 actions are passed in BGP Community Container, then order and dependencies can be indicated.

Failures of FS-EC action

Open issue

3 options

1. Stop processing
2. Continue process
3. Decide between 1 and 2

Unknown actions

Example: 3 actions

1. Set DSCP
2. Request sampling
3. Redirect to VRF

If router cannot set DSCP,

Option 1: No further action

Option 2: Request sampling

Option 3: Something else

Minimal FSv2

Minimal FSv2 Compliant:

- 1 AFI/SAFI (FSv2/Unicast) + FSv2 Extended Communities
- Filter Family: Recognize all, support 1
- Filter Family components: support mandatory
- Extended Communities for actions

Validation

- FSv2 NLRI - Syntactic and semantic checks
- Validate FSv2 route properties
- Validate FSv2 Route actions

FSv2 NLRI Checks

- Length > 20
- 1 non-empty FSv2 Filter Family
- 1 possibly-empty – FSv2 Filter component
- All TLVs and sub-TLVs are wholly contained within their parent.

Failure mode: Session reset!

Filter Family validations

FSv2 NLRI	Filter Families	AFI/SAFI to Validate
AFI: FSv2 SAFI: Unicast	Time, Interface, QP, IPv4 Basic, CATs, Routing	AFI=1/SAFI=1
AFI: FSv2 SAFI-VPN	MPLS (v4), Tunneled (v4)	AFI=1/SAFI=128
AFI: FSv2 SAFI: Unicast	IPv6 Basic	AFI=2/SAFI=2
AFI: FSv2 SAFI: VPN	MPLS (v6), Tunneled (v6)	AFI=2/SAFI=128
AFI: FSv2 SAFI: Unicast	SFC	AFI=31/SAFI=1
AFI: FSv2 SAFI: Unicast	L2 components	AFI=2/SAFI=1
AFI: FSv2 SAFI: VPN	? L2 VPNs (should this be added?)	AFI=6/SAFI=128

Syntax limits

- Multiple Filter Family TLVs with distinct types (value x) per NLRI – ordered ascending
- Multiple Filter Family Component TLVs with distinct types per Filter Family TLV –ordered ascending
- If understood by implementation, length and TLV values must be well-formed. (Discussion: What if they're not understood?!)
- Sort order
  1. Filter family type
  2. Component Type
  3. Component Values

Failure mode: Treat-as-withdraw

BGP Route Validation

Validate FSv2 NLRI using Unicast Routes

- Best match unicast or
- AS path is empty or just AS-Confed statement

Failure mode: Flow specification is not valid for traffic filtering and is not installed.

Next Steps

Filter drafts:
WG drafts - revised, implementation, WG LC [7 new fsv2 filter drafts]
Additional FSv2 filter adoption calls after IETF-127

Extended Community actions:
Adopted 3 new drafts (by IETF-127)
Deployed – Revise and send to RFC

Community container actions
draft-hares-idr-more-ip-actions – proposes format, need feedback
Individual drafts – Adoptions starting after IETF-127



Questions?

