

A YANG Model for SAVNET

draft-li-savnet-sav-yang

@IETF 119 SAVNET WG

Dan Li (Tsinghua University)

Libin Liu (ZGC Lab)

Changwang Lin (New H3C)

Jianping Wu (Tsinghua University)

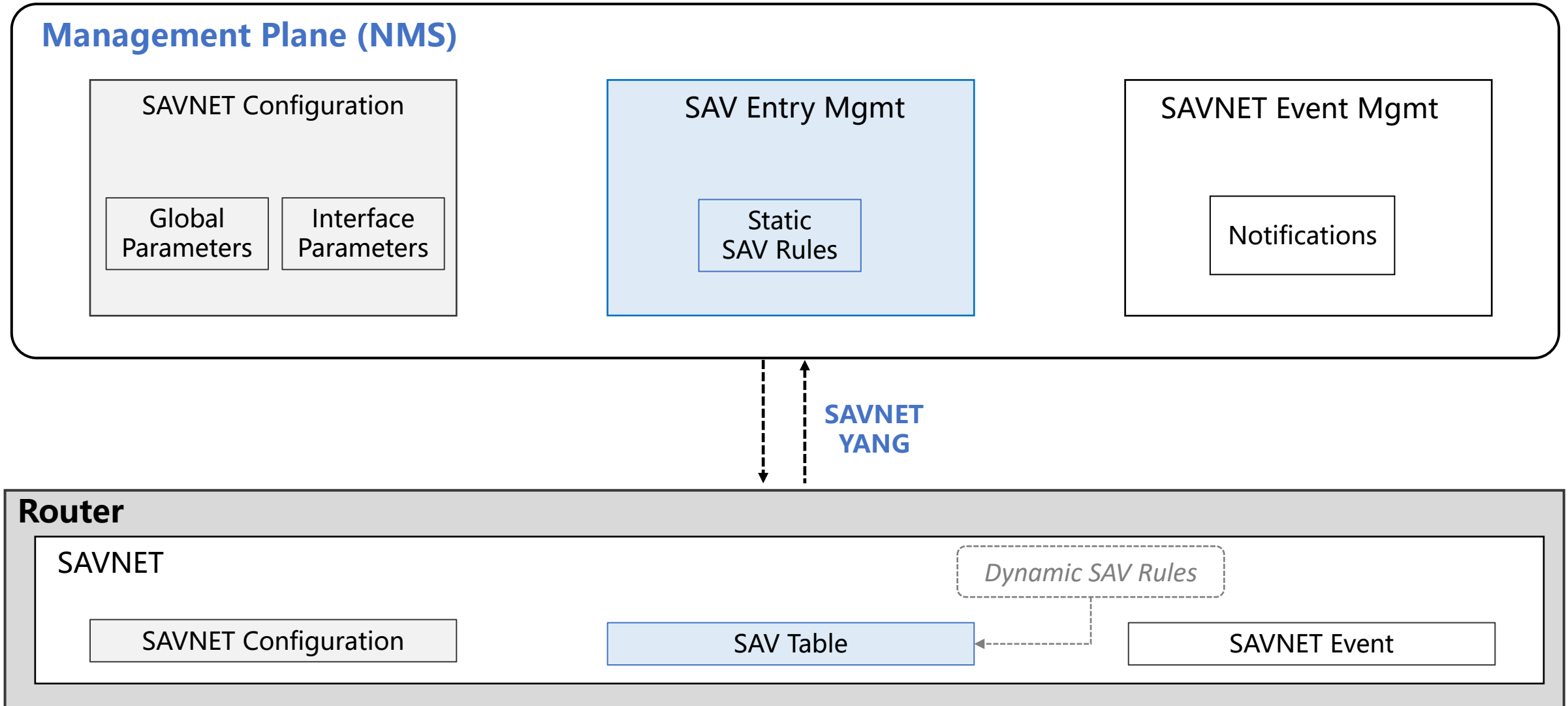
Tianhao Wu (Huawei)

Weiqiang Cheng (China Mobile)

SAVNET YANG

- ❑ This Yang model provides a base framework for configuring and managing an SAV subsystem, including SAV table and SAV rules. And it also specifies the model for the static SAV rules application.
- ❑ The data model is designed by referring to the SAVNET functions defined in related drafts. [[draft-li-savnet-intra-domain-architecture](#), [draft-wu-savnet-inter-domain-architecture](#), [draft-huang-savnet-sav-table](#)]

Operation of SAVNET Feature



Overview

SAVNET YANG

① SAVNET Global/Interface Configuration

② Static SAV-Rules Configuration

③ SAV Table

④ SAVNET Interface Information

⑤ SAVNET Notifications

Configuration

State

Event



```
module: ietf-sav
  +--rw sav
  |   +--rw router-id? yang:dotted-quad ①
  |   +--rw v4sav-entry-limits
  |   +--rw sav-controls
  |   ...
  +--rw /if:interfaces/if:interface: ①
  |   +--rw sav-control
  |   |   +--rw sav-enabled? boolean
  |   |   ...
  |   +--rw static-savs ②
  |   |   +--rw v4sav:ipv4
  |   |   |   ...
  |   |   +--rw v6sav:ipv6
  |   |   ...
  |   +--rw sav-tables ③
  |   |   +--rw sav-table* [name]
  |   |   |   +--ro sav-rules
  |   |   |   ...
  |   +--ro interfaces ④
  |   |   +--ro interface* [name]
  |   |   ...
  +--n sav-event ⑤
  |   +--ro router-id? yang:dotted-quad
  |   ...
```

Updates and Status

This Version-04 updates according to SAVNET deployment experience over the last 7 months.

- **Added**

- static SAV rules of “Blocklist” mode. (Configuration)
- notification of Top-N spoofing SAV rules . (Event and Configuration)
- support for showing flows information blocked by SAVNET. (State and Configuration)
- alarm threshold number of SAV-Rule capacity . (Configuration and Event)
- statistics of SAVNET total-packet. (State)

Updates-1: SASVNET General Configuration

Global configuration:

- ① Add entry threshold number for capacity alarm of entire SAV-Rules.
- ② Enable the function of reporting the top SAV-Rules hit by spoofing packets.
- ③ Enable the function of collecting the SAVNET blocking flow information.

```
+---rw sav
  +---rw router-id? yang:dotted-quad
  +---rw v4sav-entry-limits
    | +---rw number? uint32
    | +---rw threshold-percent? uint8
    ① | +---rw threshold-number? uint32
  +---rw v6sav-entry-limits
    | +---rw number? uint32
    | +---rw threshold-percent? uint8
    ① | +---rw threshold-number? uint32
  +---rw source-protocol-priorities
    | +---rw source-protocol-priority* [type]
    |   +---rw type identityref
    |   +---rw preference? rule-preference
  +---rw sav-controls
    | +---rw sav-enabled? boolean
    | +---rw sav-mode? identityref
    | +---x sav-interface-reset
    | | +---w input
    | |   +---w reset-statistics? boolean
    ② | +---rw sav-spoof-top
    |   +---rw enabled? boolean
    |   +---rw top-number? uint32
    ③ | +---rw sav-block-flow-report
    |   +---rw enabled? boolean
```

Updates-2: SASVNET Interface Configuration

Interface configuration:

- ① Enable the function of reporting the top SAV-Rules hit by spoofing packets on specific interface.
- ② Enable the function of collecting the SAVNET blocking flow information on specific interface.

```
augment /if:interfaces/if:interface:
  +--rw sav-control
  | +--rw sav-enabled? boolean
  | +--rw sav-mode? identityref
  | +---x sav-reset
  | | +---w input
  | | +---w reset-statistics? Boolean
  ① | +--rw sav-spoof-top
  |   +--rw enabled? boolean
  |   +--rw top-number? uint32
  ② | +--rw sav-block-flow-report
  |   +--rw enabled? boolean
```

Updates-3: Static SAV-Rules Configuration

Static SAV-rules configuration:

- ① Add threshold number for the alarm of static SAV-Rules capacity.
- ② Add the "Check-type" for supporting static SAV rules of "Blocklist" mode.

```
+---rw static-savs
+---rw v4sav:ipv4
| +---rw v4sav:sav-entry-limits
|   +---rw v4sav:number? uint32
|   +---rw v4sav:threshold-percent? uint8
|   ① +---rw v4sav:threshold-number? uint32
| +---rw v4sav:sav-rule* [source-prefix]
|   +---rw v4sav:source-prefix inet:ipv4-prefix
|   +---rw v4sav:description? string
|   +---rw v4sav:incoming-interfaces
|     +---rw v4sav:incoming-interface* [name]
|       +---rw v4sav:name if:interface-ref
|       ② | +---rw v4sav:check-type identityref
+---rw v6sav:ipv6
| +---rw v6sav:sav-entry-limits
|   +---rw v6sav:number? uint32
|   +---rw v6sav:threshold-percent? uint8
|   ① +---rw v6sav:threshold-number? uint32
| +---rw v6sav:sav-rule* [source-prefix]
|   +---rw v6sav:source-prefix inet:ipv6-prefix
|   +---rw v6sav:description? string
|   +---rw v6sav:incoming-interfaces
|     +---rw v6sav:incoming-interface* [name]
|       +---rw v6sav:name if:interface-ref
|       ② | +---rw v6sav:check-type identityref
```


Updates-4: SAV-Table State

```
+--rw sav-tables
| +--rw sav-table* [name]
|   +--ro name          string
|   +--ro address-family? identityref
|   +--ro description?  string
|   +--ro sav-rules
|     +--ro sav-rule*
|       +--ro rule-preference? rule-preference
|       +--ro incoming-interfaces
|       | +--ro incoming-interface* if:interface-ref
|       +--ro source-protocol  identityref
|       +--ro active?          empty
|       +--ro last-updated?    yang:date-and-time
|       +--ro v4sav:source-prefix? inet:ipv4-prefix
|       +--ro v6sav:source-prefix? inet:ipv6-prefix
|       +--ro total-packets?    uint64
|       +--ro total-bytes?      uint64
|       +--ro drop-packets?     uint64uint64
|       +--ro drop-bytes?       uint64uint64
|       +--ro sav-invalid-packets? uint64uint64
|       +--ro sav-invalid-bytes?  uint64uint64
|       +--ro sav-valid-packets?  uint64uint64
|       +--ro sav-valid-bytes?   Uint64uint64
```

①

```
.....
② +--ro sav-block-flow-infos
| +--ro sav-block-flow-info*
|   +--ro source-ip-address  inet:ip-address
|   +--ro source-port        uint16
|   +--ro destination-ip-address inet:ip-address
|   +--ro destination-port   uint16
|   +--ro arrival-time       yang:date-and-time
```

SAV-table state:

- ① Add the "total-packet" statistics for calculating pass-packet amount and trouble shooting
- ② Support for showing the flow information (5 tuples) of SAVNET blocking packets.

Updates-5: SAVNET Interface State

SAV-table state:

- ① Add "total-packets" statistics on specific interface for maintenance and trouble shooting.

```
+--ro interfaces
| +--ro interface* [name]
|   +--ro name      if:interface-ref
|   +--ro total-packets? uint64
|   +--ro total-bytes?  uint64
|   +--ro drop-packets? uint64
|   +--ro drop-bytes?   uint64
|   +--ro sav-invalid-packets? uint64
|   +--ro sav-invalid-bytes?  uint64
|   +--ro sav-valid-packets?  uint64
|   +--ro sav-valid-bytes?    uint64
```

Updates-6: SAVNET Event

SAVNET Event:

- ① Report the information of Top-N SAV-Rules hit by spoofing packets.

```
+---n sav-event
+---ro router-id?      yang:dotted-quad
+---ro address-family  identityref
+---ro sav-limit-reached? Boolean
① +---ro top-spoof-sav-rules
  | +---ro sav-rule*
  |   +---ro rule-preference?    rule-preference
  |   +---ro incoming-interfaces
  |   | +---ro incoming-interface* if:interface-ref
  |   +---ro source-protocol      identityref
  |   +---ro active?              empty
  |   +---ro last-updated?        yang:date-and-time
  |   +---ro v4sav:source-prefix?  inet:ipv4-prefix
  |   +---ro v6sav:source-prefix?  inet:ipv6-prefix
  |   +---ro total-packets?        uint64
  |   +---ro total-bytes?          uint64
  |   +---ro drop-packets?         uint64
  |   +---ro drop-bytes?           uint64
  |   +---ro sav-invalid-packets?  uint64
  |   +---ro sav-invalid-bytes?    uint64
  |   +---ro sav-valid-packets?    uint64
  |   +---ro sav-valid-bytes?      uint64
```

Next Steps

- ❑ Request more review and comments.
- ❑ Add an example of Jason format.
- ❑ Add the choice of “action-mode” for SAVNET execution.
- ❑ Support SAV rules from more types of control-plane-protocol.
[SAVNET architecture updates]

Thanks!