YANG Data Model for Stateless Packet Filter Configuration draft-huang-netmod-acl-03

Lisa Huang, yihuan@cisco.com

Alexander Clemm, alex@cisco.com

Andy Bierman, andy@yumaworks.com

11/04/2013

SPF Summery

- SPF: Stateless Packet Filter, aka ACL, Access Control Lists
  - Used to filter traffic (“Firewall Rules”); major part of device configurations
  - No configuration complete without ACLs
- Why a YANG data model?
  - Netconf and YANG are intended for network device configuration
  - Make SPF more accessible to automated applications, examples:
    - I2RS, Open Daylight, Dynamic Intrusion Protection Systems
    - Dynamic setup/configuration of services, e.g. temporary firewall rule adjustments for video conferences
- Covered popular SPFs and incorporated a rich set of filters
  - IP SPF, MAC SPF, ARP SPF as initial SPF types
  - More than 50 filter leaves in models.
  - Extensible + modular framework

Revision History

- Main changes in revision 02
  - Expounded how to extend the current SPF to support SPF chain. Gave an example for ipv4. Same pattern can apply to ipv6, mac, and arp PFEs if needed.
  - Multivendor SPF follow up and result.
  - DMTF's (Desktop management Task Force) CIM (Common Information Model) vendor specific follow up and result.
  - Can map 1-to-1 to AAA protocol IP filters.
- Main changes in revision 03
  - Renamed all ACL to SPF, ACE (Access Control Entry) to PFE(Packet Filter Entry) .
  - Explained the relationship between SPF and ACL
- http://www.ietf.org/id/draft-huang-netmod-acl-03.txt

Proposal

- Request to adapt SPF model as standards-track working group item
  - SPFs are an important part of device configurations
  - Needed both by administrators and by applications
  - Enabler for many applications, generally related to security, widely used in policy
  - Will clearly benefit from standardization
- Rev 03 of draft has already been posted
  - Addressed all issues raised in two previous rounds of WG discussions
  - Extendable structure
  - Includes support for 3 different types of SPF, more can be added
  - Covers comprehensive set of parameters;
feature statements allow for customization and device adaptation

Q & A

Thank You

SPF concept

- SPF: Stateless Packet Filter
  - Also know as ACL: Access Control List
  - An ordered set of rules used to filter traffic on a networking device
- Packet Filter Entry (PFE) : a representation of a rule
  - Left hand side: the matching criteria, or "filter"
  - Right hand side : the action to take – permit/deny a packet
  - Note: can generalize SPF with further actions: packet capture, audit logging, ...
- First rule that matches is applied
  - Most specific rules first to avoid rule shadowing
- SPFs are applied against interfaces
  - Interface refers to SPF (SPF specified independent of interface)
  - Different interfaces can use different SPFs, or use the same

ACL Types covered in the data model

- IP SPFs
  - Filter traffic based on IP information in the Layer 3 header of packets.
- MAC SPFs
  - Filter traffic using the information in the Layer 2 header of each packet.
- ARP SPFs
  - Filter IP- and non-IP-based traffic by checking the Ethernet type code field in the Layer 2 header.

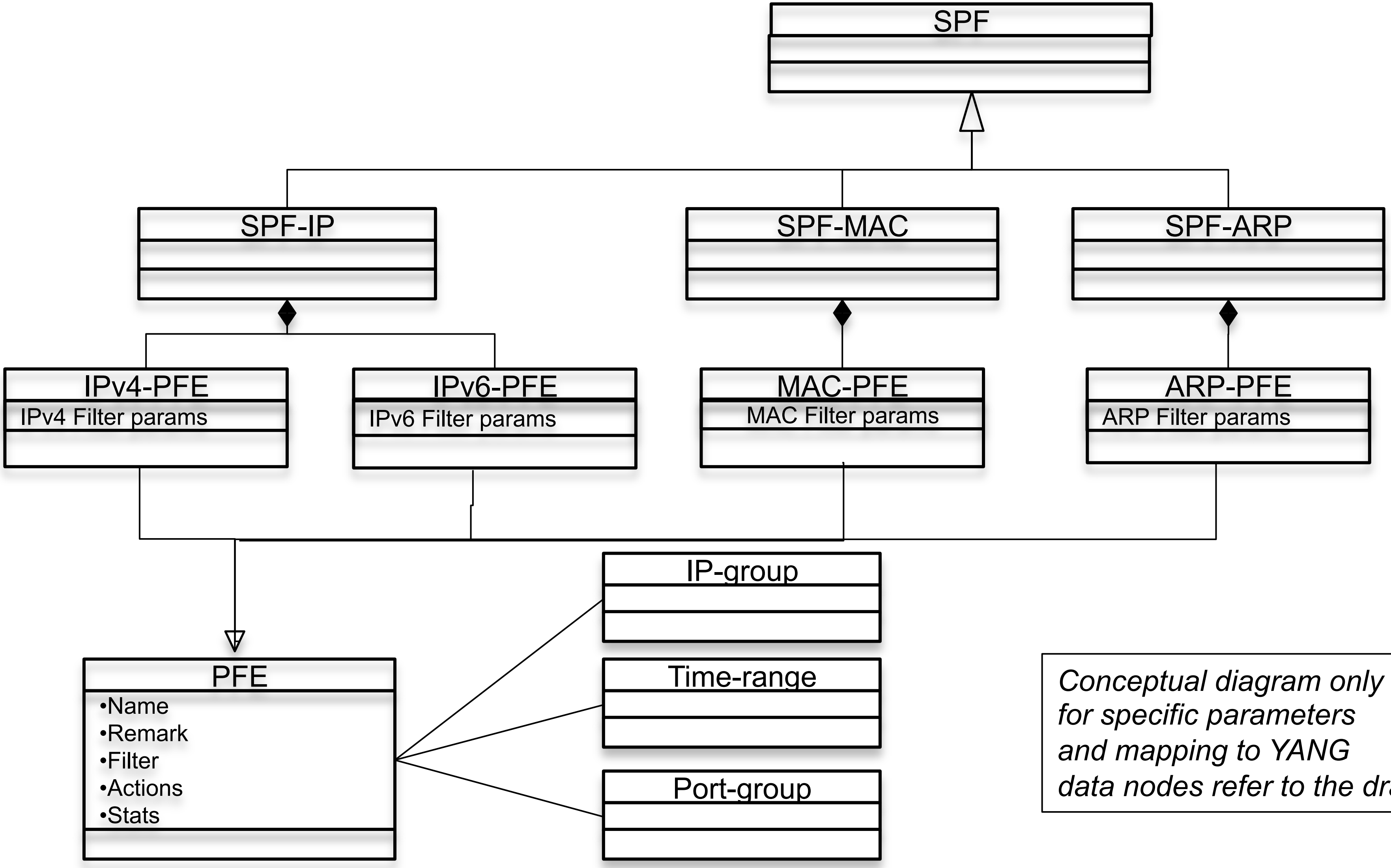
Each SPF includes only PFEs of its type (no mix and match)

Framework can be extended with additional SPF types

Augment stateless-pf YANG module

Follow design pattern of other SPF types, leverage common SPF data types

SPF module overview



Conceptual diagram only – for specific parameters and mapping to YANG data nodes refer to the draft

Example

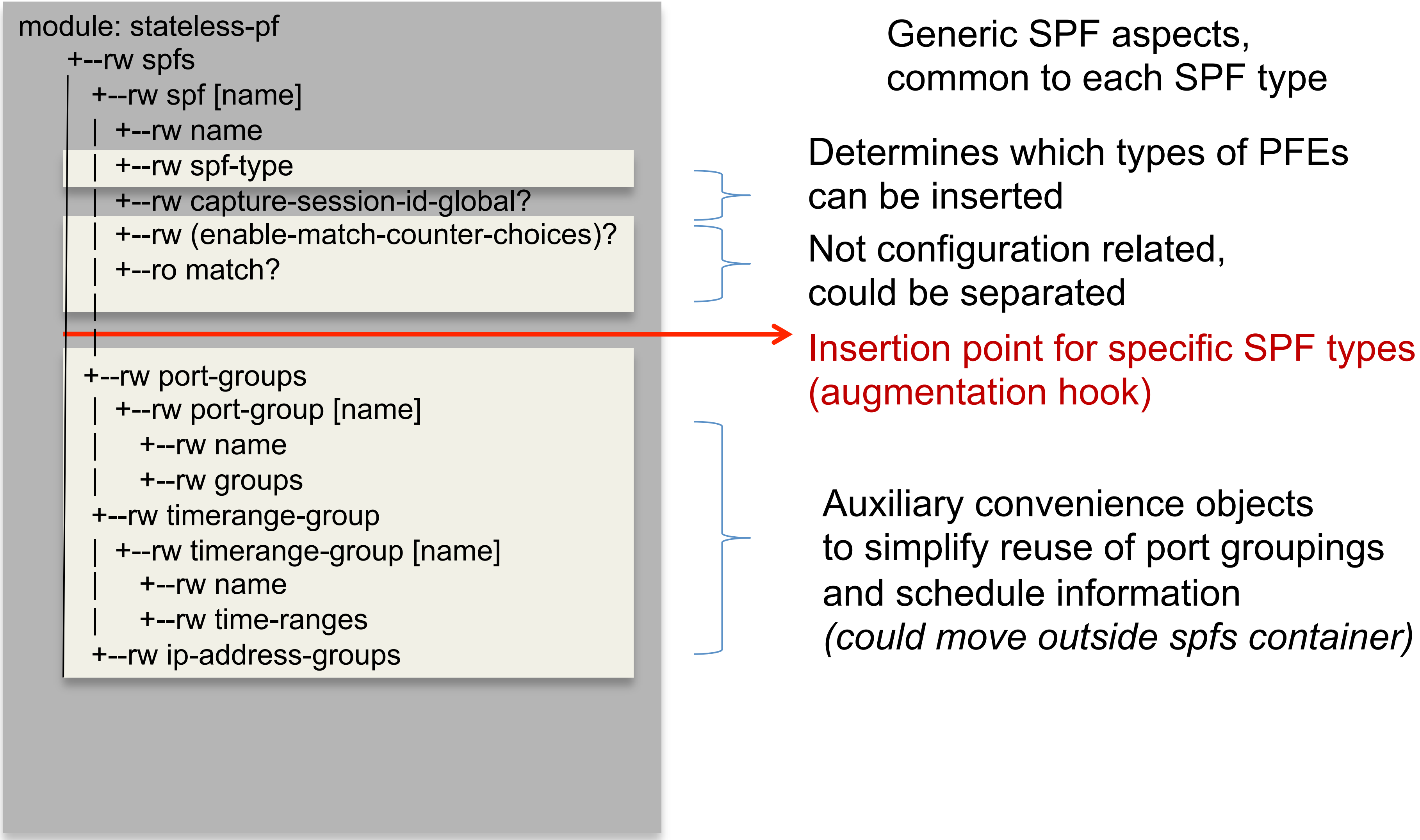
- **SPF Example:**

  Denies TELNET traffic from 14.3.6.234 bound for host 6.5.4.1 from leaving.
  Denies all TFTP traffic bound for TFTP servers.
  Permits all other IP traffic.

- **SPF CLI:**

```
access-list ip iacl
  deny tcp 14.3.6.234 0.0.0.0 host 6.5.4.1 eq 23
  deny udp any any eq tftp
  permit ip any any
```

YANG Module Structure



```
module: stateless-pf
   +--rw spfs
      +--rw spf [name]
      |  +--rw name
      |  +--rw spf-type
      |  +--rw capture-session-id-global?
      |  +--rw (enable-match-counter-choices)?
      |  +--ro match?
      |
      |
     +--rw port-groups
      |  +--rw port-group [name]
      |     +--rw name
      |     +--rw groups
      +--rw timerange-group
      |  +--rw timerange-group [name]
      |     +--rw name
      |     +--rw time-ranges
      +--rw ip-address-groups
```

Generic SPF aspects, common to each SPF type

Determines which types of PFEs can be inserted

Not configuration related, could be separated

Insertion point for specific SPF types (augmentation hook)

Auxiliary convenience objects to simplify reuse of port groupings and schedule information *(could move outside spfs container)*

YANG module structure (contd.)

```
module: stateless-pf
    +--rw spfs
      +--rw spf [name]
      |  +--rw spf-ip:afi
      |  +--rw spf-ip:ipv6-pfes
      |  |  +--rw spf-ip:ipv6-pfe [name]
      |  |     +--rw spf-ip:name
      |  |     +--rw (remark-or-ipv6-case)?
      |  |        +--:(remark)
      |  |        |  +--rw spf-ip:spf-remark
      |  |        +--:(ipv6-pfe)
      |  |        |  +--rw spf-ip:filters
      |  |        |     +-- filter parameters
      |  |        |  +--rw spf-ip:actions
      |  |        |     +-- action parameters
      |  |        +-- ro spf-ip:match
```

Indicates IP address type

SPFs can include “comment lines” for human/admin consumption
Included in YANG module to maintain consistency with CLI

“left hand side”

“right hand side”

Not configuration related, could be separated

Generic design pattern that is reflected in every SPF type
All SPF type specifics are in the filter parameters and in the actions

YANG module structure (contd.)

```
module: stateless-pf
    +--rw spfs
      +--rw spf [name]
        |  +--rw spf-ip:afi
        |  +--rw spf-ip:ipv4-pfes
        |  |  +--rw spf-ip:ipv4-pfe [name]
        |  |     +--rw spf-ip:name
        |  |     +--rw (remark-or-ipv4-case)?
        |  |        +--:(remark)
        |  |        |   +--rw spf-ip:spf-remark
        |  |        +--:(ipv4-pfe)
        |  |        |   +--rw spf-ip:filters
        |  |        |      +-- filter parameters
        |  |        |   +--rw spf-ip:actions
        |  |        |      +-- action parameters
        |  |        +-- ro spf-ip:match
```

IPv4

(IPv4 and IPv6 specified
in same submodule)

Indicates IP address type

SPFs can include “comment lines” for human/admin consumption
Included in YANG module to maintain consistency with CLI

“left hand side”

“right hand side”

Not configuration related, could be separated

Generic design pattern that is reflected in every SPF type
All SPF type specifics are in the filter parameters and in the actions

YANG module structure (contd.)

```
module: stateless-pf
    +--rw spfs
      +--rw spf [name]
        |  +--rw spf-mac:mac-pfes
        |  |  +--rw spf-mac:mac-pfe [name]
        |  |     +--rw spf-mac:name
        |  |     +--rw (remark-or-mac-case)?
        |  |        +--:(remark)
        |  |        |   +--rw spf-mac:remark
        |  |        +--:(mac-pfe)
        |  |        |   +--rw spf-mac:filters
        |  |        |       +-- filter parameters
        |  |        |   +--rw spf-mac:actions
        |  |        |       +-- action parameters
        |  |        +-- ro spf-mac:match
```

MAC

(separate module)

Generic design pattern that is reflected in every SPF type
All SPF type specifics are in the filter parameters and in the actions

YANG module structure (contd.)

```
module: stateless-pf
    +--rw spfs
      +--rw spf [name]
        |  +--rw spf-arp:arp-pfes
        |  |  +--rw spf-arp:arp-pfe [name]
        |  |     +--rw spf-arp:name
        |  |     +--rw (remark-or-arp-case)?
        |  |        +--:(remark)
        |  |        |   +--rw spf-arp:remark
        |  |        +--:(arp-pfe)
        |  |        |   +--rw spf-arp:filters
        |  |        |       +-- filter parameters
        |  |        |   +--rw spf-arp:actions
        |  |        |       +-- action parameters
        |  |        +-- ro spf-arp:match
```

ARP

(separate module)

Generic design pattern that is reflected in every SPF type
All SPF type specifics are in the filter parameters and in the actions

YANG module structure (contd.)

```
module: stateless-pf
    +--rw spfs
      +--rw spf [name]
      |  +--rw spf-ip:ipv6-pfes
      |  |  +--rw spf-ip:ipv6-pfe [name]
      |  |     +--rw spf-ip:name
      |  |     +--rw (remark-or-ipv6-case)?
      |  |        +--:(ipv6-pfe)
      |  |        |  +--rw spf-ip:filters
      |  |        |     +-- rw (source-address-host-group)?
      |  |        |     +-- rw (dest-address-host-goup)?
      |  |        |     +-- rw spf-ip:protocol?
      |  |        |     +-- rw spf-ip:capture-session-id?
      |  |        |     +-- rw spf-ip:fragments?
      |  |        |     +-- rw spf-ip:time-range?
      |  |        |     +-- rw spf-ip:src-ports?
      |  |        |     +-- rw spf-ip:dest-ports?
      |  |        |     +-- ...
      |  |        |  +--rw spf-ip: actions
      |  |        |     +-- rw spf-ip:action
      |  |        |     +-- rw spf-ip:log?
```

IPv6-specific parameters, but could add IP-v6 Specific filters

Insertion point for specific filters (augmentation hook)

Common actions but could add IP-specific actions later, such as copy, chain

Insertion point for additional actions

SPF Chain ipv4 Example

```
augment "/spf:spfs/spf:spf/spf-ip:ipv4-pfes" +
      "/spf-ip:ipv4-pfe/spf-ip:actions" {
      leaf chain {
          type spf-ref ;
          description "Reference to another SPF name to chain the PFEs";
      }
  }
```