AOS-CX 10.09 Ingress policy support for sub interfaces

Steve Bartlett
Technical Marketing Engineer CX Switching
6300, 6400, 8360 switch platforms
Agenda

1. Ingress policy support on specific platforms for sub interfaces
2. Ingress policy support on specific platform with PBR
Ingress policy support for sub interfaces
6300, 6400, 8360 switch platforms
Sub-interfaces summary

Overview – introduced in 10.08 but without policy support for sub-interfaces

▪ A sub-interface (also called child-interface) is a virtual interface created by dividing one parent interface (physical or LAG) into multiple logical interfaces that are tagged using different VLAN-IDs.

▪ Sub-interfaces use the parent physical interface for sending and receiving IP traffic.

▪ The feature is related to IP transport and not to Ethernet transport: consequently, sub-interfaces are available only for L3 interfaces. No sub-interface support for L2 interface.

▪ Multiple sub-interfaces (or child interfaces) can now be created below one parent interface.

▪ Parent interface can be a regular physical L3 interface including a split L3 port or a L3 LAG

```
interface 1/1/2
  no shutdown
interface 1/1/2.1
interface 1/1/2.2
interface 1/1/2.7
interface 1/1/2.9
interface 1/1/2.10
interface 1/1/2.11
interface 1/1/2.12
interface 1/1/2.13
interface 1/1/2.14
interface 1/1/2.15
interface 1/1/2.100

interface 1/1/35
  split
interface 1/1/35:1
  no shutdown
interface 1/1/35:1.1
interface 1/1/35:1.2
interface 1/1/35:2
  no shutdown
interface 1/1/35:2.1
interface 1/1/35:2.2
interface 1/1/35:2.3
interface 1/1/35:2.4
interface 1/1/35:2.5

interface lag 1
interface lag1
interface lag1.1
interface lag1.10
interface lag1.11
interface lag1.12
interface lag1.13
interface lag1.14
interface lag1.20
```
Policy Support inbound for sub-interfaces

Overview

- Policy support for inbound sub interfaces is now supported in 10-09
- Policy can only be applied ‘inbound’ on an interface – no egress policy support
- Application of policy must adhere to existing feature functional requirements of sub interfaces, example L3 only for sub interfaces on standard interfaces & L3 LAG. L2 sub-interfaces are not supported
  - sub-interfaces are referenced as a ‘child’ interface
  - the sub-interface parent must be up/routing
  - cannot configure IP addresses on parent
  - Parent must be ‘routing’ (not layer 2) and in the ‘no shut’ state
- Policy follows existing process of a ‘Classifier’ tied to ‘Policy’, as used for policy application with interfaces, and this leveraged for sub-interface policy support
- Policy support includes IPv4,IPv6 and mac classifying and policing within VLAN
Policy Support inbound for sub-interfaces

Overview continued

— Classifier

— A classifier policy allows an administrator to define sets of rules based on network traffic addressing or other content, and use these rules to match and restrict or alter the traffic passage through the switch by applying to a policy

— There are three type of rules for traffic classes, MAC, IPv4 & IPv6, which are focused on each frame/packet characteristics

— Policy

— Choosing the rule criteria is called classification and one rule or list of rules is called a policy which can leverage a single or multiple ‘actions’ matched by the traffic class

— A policy contains one or more entries listed based on priority by sequence number

— Policy actions are broadly classified as following:
  — Remark
  — Police actions
  — Other actions
Policy examples: Remark, Police, Drop, Mirror and other actions

- **Remark Policy inbound**: Remark to AF41 DSCP
- **Police Policy inbound**: subnet 10.1.0.0/24 CIR rate 10000 kbps
- **Drop Policy inbound**: Host(s) 10.1.1.1 drop
- **Mirror Policy inbound**: Host(s) 10.1.2.2 mirror
- **Other actions**: PBR, PCP (priority Code Point), local-priority

**Classifier(s for policy(s))**

```
class ip icmp-deny
  10 match icmp any 172.16.31.1 count

class ip remark_traffic
  10 match any 10.1.0.0/255.255.255.0 any
  20 match any 10.1.1.0/255.255.255.0 any
  30 match any 10.1.2.0/255.255.255.0 any

class ip traffic2
  10 match any 192.168.1.0/255.255.255.0
  192.168.2.0/255.255.255.0
  20 match ah 192.168.3.250 any
```
Policy examples: Remark, Police, Drop, Mirror and other actions

**Classifier(s for policy(s))**

- **Class ip remark_traffic**
  - 10 match any 10.1.0.0/255.255.255.0 any
  - 20 match any 10.1.1.0/255.255.255.0 any
  - 30 match any 10.1.2.0/255.255.255.0 any

- **Class ip traffic2**
  - 10 match any 192.168.1.0/255.255.255.0
  - 20 match any 192.168.2.0/255.255.255.0

**Classifier**

- **class ip remark_traffic**
  - 10 match any 10.1.0.0/255.255.255.0 any
  - 20 match any 10.1.1.0/255.255.255.0 any
  - 30 match any 10.1.2.0/255.255.255.0 any

**Policy name**

- **Remark Policy inbound**
- **Police Policy inbound**
- **Drop Policy inbound**
- **Mirror Policy inbound**
- **Other actions**
  - PBR, PCP (priority Code Point), local-priority

**Policy actions**

- **Config example**

  - **subint-policy1**
    - 10 remark_traffic ipv4
dscp AF41
cir kbps 1000000
cbs 500000
  exceed drop

- **traffic2 ipv4 dscp CS2**

- **icmp-drop ipv4**

**Policy actions for** remark_traffic class
- Remark traffic 10.1.0.0/24 to AF41
- Remark traffic 10.1.1.0/24 to AF41
- Remark traffic 10.1.2.0/24 to AF41

**Policy actions for** remark_traffic class
- CIR kbps 1000000
- CBS (kbps) 500000

**Policy actions for** traffic2 class
- Remark source traffic destined to subnet 192.168.1.0/24 to CS2

**Policy actions for** icmp-drop class
- Drop source ICMP traffic destined to ip address 172.16.31.1
Configuration summary example

Configure ‘class’ match

Create a policy and attach ‘classifiers’

Apply policy to sub-interface with ‘apply’ command

class ip remark_traffic
  10 match any 10.1.1.0/255.255.255.0 any

class ip traffic2
  10 match any 192.168.1.0/255.255.255.0
  192.168.2.0/255.255.255.0
  20 match ah 192.168.3.250 any

policy subint-policy1
  10 class ip remark_traffic action dscp AF41 action cir kbps 1000000 cbs 500000 exceed drop
  20 class ip traffic2 action dscp CS2

interface 1/3/48.10
  no shutdown
  apply policy subint-policy1 in
  ip address 172.16.31.1/31
  ip ospf 1 area 0.0.0.0
  no ip ospf passive
  ip ospf network point-to-point
  encapsulation dot1q 10
  exit
### Configuration verification -1

```
6405-BLDG03# sh policy subint-policy1
 Name
 Additional Policy Parameters
 Sequence Comment
 Class Type
 action

-------------------------------------------------------------------------------
subint-policy1
 10 remark_traffic ipv4
dscp AF41
cir kbps 1000000
cbs 500000
exceed drop

 20 traffic2 ipv4
dscp CS2

 30 icmp-deny ipv4
drop

-------------------------------------------------------------------------------
```

```
'sh policy [policy-name]'
```
Configuration verification - 2

6405-BLDG03# `sh running-config interface 1/3/48.10`
interface 1/3/48.10
no shutdown
  apply policy subint-policy1 routed-in
  ip address 172.16.31.1/31
  ip ospf 1 area 0.0.0.0
  no ip ospf passive
  ip ospf network point-to-point
  encapsulation dot1q 10
exit

6405-BLDG03# `sh policy hitcounts subint-policy1`
Statistics for Policy subint-policy1:

VRF default
interface 1/3/48.10 (routed-in):
  Matched Packets  Configuration
10 class ip remark_traffic action dscp AF41 action cir kbps 1000000 cbs 500000 exceed drop
  [ 0 kbps conform ]
  - 10 match any 10.1.1.0/255.255.255.0 any
20 class ip traffic2 action dscp CS2
  - 10 match any 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
     - 20 match ah 192.168.3.250 any
30 class ip icmp-deny action drop
  0 10 match icmp any 172.16.31.1 count

`sh policy hitcounts [policy-name]`
Configuration verification

Output is all switch policy configuration

```
6405-BLDG03# sh policy configuration
```

Output is specific interface policy

```
6405-BLDG03# sh policy interface 1/3/48.10
```

Output is policy commands applied on the switch (not ‘class’ configured definitions)

```
6405-BLDG03# sh policy commands
policy subint-policy1
    10 class ip remark_traffic action dscp AF41 action cir kbps 1000000 cbs 500000 exceed drop
    20 class ip traffic2 action dscp CS2
    30 class ip icmp deny action drop
interface 1/3/48.10
    apply policy subint-policy1 routed-in
```

Output is vsx-peer node configuration and commands

```
6405-BLDG03# sh policy vsx-peer
commands       Format output as CLI commands
configuration   Display user-specified configuration
```
Policy configuration notes

Detail

— Multiple ‘classifiers’ can be tied to a policy, classifiers can have multiple ‘classifications’

— A policy cannot be applied to the ‘parent’ interface of one or more sub-interfaces. This also means a sub-interface cannot be applied to an interface if there is a policy applied (at parent interface)

— If a policy contains any in class entry with the ‘count’ keyword and is applied to multiple sub-interfaces in the same direction:
  – The statistics will be aggregated
  – For ‘routed-in’ direction the statistics will aggregated only for sub-interfaces in the same vrf
  – Separate stats for different sub-interfaces can be obtained using another policy
  – Per-interface keyword is not available in the sub-interface context

— Sub-interface applications share lookups with ingress and egress VLANs

— no policy [policy name] removes the policy from the global configuration (even if applied within an interface sub context)
Policy configuration notes -2

Detail -2

— Note the usage of ‘in’ and routed-in cli syntax when applying policy to an interface, example with policy ‘subint-policy1’

  apply policy subint-policy1 routed-in
  or
  apply policy subint-policy1 in

<table>
<thead>
<tr>
<th>MAC Class(es)</th>
<th>PBR action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress sub-interface policy ‘in’</td>
<td>yes</td>
</tr>
<tr>
<td>routed-ingress sub-interface policy ‘routed-in’</td>
<td>no</td>
</tr>
</tbody>
</table>

— The direction option ‘in’ & ‘routed-in’ provides the option for administrators to decide between mac class policy and the PBR option for routed traffic. For routed traffic and for the option of using the PBR feature, use the routed-in option
Thank you

steve.bartlett@hpe.com