How to save TCAM resources

**Labels: ArubaOS-CX Switches**

**Requirement:**

For some switch designs, TCAM resources doesn't scale well and there is no way to re-use same TCAM resource again and again.

This is exactly the case with AOS-CX 8325.

If we have an ACL and this ACL needs to be applied to many SVIs. Each time ACL is applied additional TCAM resources are consumed.

As example about sharing TCAM resources; In Comware, TCAM resources allocated in ASIC for below mentioned ACL could be re-used when applied to more SVIs by using *share-mode* command extension.

[Sysname] *interface Vlan-interface 8*

[Sysname-Vlan-interface8] *packet-filter 2001 inbound share-mode*

In 8325

Command : ***show resources***

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Command : show resources  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Resource Usage:

Mod  Description  
         Resource                          Width    Used Reserved   **Free**  
-------------------------------------------------------------------------  
1/1  Routed Ingress IPv4 VLAN Policy  
         Ingress TCAM Entries                  3       6     2304   
     Ingress Control Plane Policing  
         Ingress TCAM Entries                  3     318     2304   
     Egress Control Plane Policing  
         Egress TCAM Entries                   2      86     1024   
     Routed Ingress IPv4 VLAN ACL  
         Ingress TCAM Entries                  3    4245     4608   
     Total  
         Ingress TCAM Entries                       4569     9216      **0**  
         Egress TCAM Entries                          86     1024    1024  
         Policers                                      0             6144  
         Ingress L4 Port Ranges                        2               30

Above output shows 0 TCAM entries are left after using same ACL across multple SVIs.

**Solution:**

Better solution is to use a hardware which scales well for TCAM resources.

Answer is 8360 which has

To give an idea about TCAM resources in 8325 and 8360.

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$  8360 $$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

 Without any explicit resources being used.

router(config)# sh resources

Resource Usage:

Mod  Description  
         Resource                                   Used Reserved   **Free**  
-------------------------------------------------------------------------  
1/1  Total  
         Ingress TCAM Entries                          0        0   **65536**                      
         Egress TCAM Entries                           0        0    8192  
         Ingress Lookups                               0                9  
         Ingress Flex Lookups                          0                1  
         Egress Lookups                                0                4  
         Ingress Policers                              0             8191  
         Egress Policers                               0             4095

########################  8325 #####################      
 Without any explicit resources being used.

8325# sh resources

Resource Usage:

Mod  Description  
         Resource                          Width    Used Reserved    **Free**  
-------------------------------------------------------------------------  
1/1  Ingress Control Plane Policing  
         Ingress TCAM Entries                  3     309     2304  
     Egress Control Plane Policing  
         Egress TCAM Entries                   2      86     1024  
     Total  
         Ingress TCAM Entries                        309     2304    **6912**  
         Egress TCAM Entries                          86     1024    1024  
         Policers                                      0             6144  
         Ingress L4 Port Ranges                        0               32

Other answer is to use TCAM optimization in such a way that less TCAM entries are consumed.

One method is to use object-group in ACE(Access list entry) carefully, because number of entries in an object-group multiplies with other object-group in the same ACE.

**Configuration:**

In short, if object-group is being used to denote  L4 ports in an ACL, then,

Below is better than:

8325(config)# sh object-group  
Type       Name  
  Sequence L4 Port(s)/Address  
-------------------------------------------------------------------------------  
IPv4       testip  
        10 10.10.10.1  
        30 10.10.10.3  
-------------------------------------------------------------------------------  
**Port       test-ports  
        10    4010 -  4011**

this:

8325(config)# sh object-group  
Type       Name  
  Sequence L4 Port(s)/Address  
-------------------------------------------------------------------------------  
IPv4       testip  
        10 10.10.10.1  
        30 10.10.10.3  
-------------------------------------------------------------------------------  
**Port       test-ports  
        10 =  4010  
        20 =  4011**

**Verification:**

Please have some patience and go through below outputs to understand how it works.

TCAM resource for an acl is calculated by adding (ACE entries multiplied by TCAM resource width)

Lets take a quick example, **test1** acl is applied to SVI **vlan10**

interface vlan10  
    apply access-list ip test1 routed-in                            << TCAM resource width =3

access-list ip test1  
    10 permit tcp 10.10.10.2 testip group test-ports2                                    (((2\*2)+1)\*3) =15

that 1 in above expression is ACL's implicit deny, which also consumes resource.

Below shows the definiton of object-groups(testip and test-ports2) used above

8325(config)# sh object-group  
Type       Name  
  Sequence L4 Port(s)/Address  
-------------------------------------------------------------------------------  
IPv4       testip  
        10 10.10.10.1  
        30 10.10.10.3                                                                                         ................ 2 ACE  
-------------------------------------------------------------------------------  
Port       test-ports2  
        10 =  4010  
        20 =  4011                                                                                              ................ 2 ACE

######################## 2. After applying a single ACE ACL to interface vlan 10

8325(config)# sh access-list commands configuration  
access-list ip test1  
    10 permit any 10.10.10.2/255.255.255.0 10.10.10.1/255.255.255.0  
interface vlan10  
    apply access-list ip test1 routed-in  
8325(config)# sh resources

Resource Usage:

Mod  Description  
         Resource                          Width    Used Reserved    Free  
-------------------------------------------------------------------------  
1/1  Ingress Control Plane Policing  
         Ingress TCAM Entries                  3     309     2304  
     Egress Control Plane Policing  
         Egress TCAM Entries                   2      86     1024  
     Routed Ingress IPv4 VLAN ACL  
         Ingress TCAM Entries                  3       6     2304  
     Total  
         Ingress TCAM Entries                        315     4608    4608  
         Egress TCAM Entries                          86     1024    1024  
         Policers                                      0             6144  
         Ingress L4 Port Ranges                        0               32  
           
           
######################## 3. with object-group, only one address in object-group

8325(config)# sh object-group  
Type       Name  
  Sequence L4 Port(s)/Address  
-------------------------------------------------------------------------------  
IPv4       testip  
        10 10.10.10.1  
8325(config)# sh access-list commands  
access-list ip test1  
    10 permit any 10.10.10.2/255.255.255.0 testip                     ((1+1)\*3) =6  
interface vlan10  
    apply access-list ip test1 routed-in  
8325(config)# sh resources

Resource Usage:

Mod  Description  
         Resource                          Width    Used Reserved    Free  
-------------------------------------------------------------------------  
1/1  Ingress Control Plane Policing  
         Ingress TCAM Entries                  3     309     2304  
     Egress Control Plane Policing  
         Egress TCAM Entries                   2      86     1024  
     Routed Ingress IPv4 VLAN ACL  
         Ingress TCAM Entries                  3       **6**    2304                                            
     Total  
         Ingress TCAM Entries                        315     4608    4608  
         Egress TCAM Entries                          86     1024    1024  
         Policers                                      0             6144  
         Ingress L4 Port Ranges                        0               32

######################## 4. with two addresses in a object-group

8325(config)# sh access-list commands  
access-list ip test1  
    10 permit any 10.10.10.2/255.255.255.0 testip                     ((2+1)\*3) =6  
interface vlan10  
    apply access-list ip test1 routed-in  
8325(config)# sh object-group  
Type       Name  
  Sequence L4 Port(s)/Address  
-------------------------------------------------------------------------------  
IPv4       testip  
        10 10.10.10.1  
        30 10.10.10.3  
8325(config)# sh resources

Resource Usage:

Mod  Description  
         Resource                          Width    Used Reserved    Free  
-------------------------------------------------------------------------  
1/1  Ingress Control Plane Policing  
         Ingress TCAM Entries                  3     309     2304  
     Egress Control Plane Policing  
         Egress TCAM Entries                   2      86     1024  
     Routed Ingress IPv4 VLAN ACL  
         Ingress TCAM Entries                  3     **9**    2304                          <<   one triple width entry(+3) is added  
     Total  
         Ingress TCAM Entries                        318     4608    4608  
         Egress TCAM Entries                          86     1024    1024  
         Policers                                      0             6144  
         Ingress L4 Port Ranges                        0               32  
8325(config)#

######################## 5. Using range keyword in ACE for ports instead of object-group

8325(config)# sh object-group  
Type       Name  
  Sequence L4 Port(s)/Address  
-------------------------------------------------------------------------------  
IPv4       testip  
        10 10.10.10.1  
        30 10.10.10.3  
8325(config)# sh access-list ip commands  
access-list ip test1  
    10 permit tcp 10.10.10.2 testip range 4010 4011                            ((2+1)\*3) =9  
interface vlan10  
    apply access-list ip test1 routed-in  
8325(config)# sh resources

Resource Usage:

Mod  Description  
         Resource                          Width    Used Reserved    Free  
-------------------------------------------------------------------------  
1/1  Ingress Control Plane Policing  
         Ingress TCAM Entries                  3     309     2304  
     Egress Control Plane Policing  
         Egress TCAM Entries                   2      86     1024  
     Routed Ingress IPv4 VLAN ACL  
         Ingress TCAM Entries                  3      **9**   2304                                  << no change from last  
     Total  
         Ingress TCAM Entries                        318     4608    4608  
         Egress TCAM Entries                          86     1024    1024  
         Policers                                      0             6144  
         Ingress L4 Port Ranges                        0               32  
8325(config)#

######################## 6. Using range of ports defined in a single entry in object-group

8325(config)# sh object-group  
Type       Name  
  Sequence L4 Port(s)/Address  
-------------------------------------------------------------------------------  
IPv4       testip  
        10 10.10.10.1  
        30 10.10.10.3  
-------------------------------------------------------------------------------  
Port       test-ports  
        10    4010 -  4011  
8325(config)# sh access-list commands  
access-list ip test1  
    10 permit tcp 10.10.10.2 testip group test-ports  
interface vlan10  
    apply access-list ip test1 routed-in  
8325(config)# sh resources

Resource Usage:

Mod  Description  
         Resource                          Width    Used Reserved    Free  
-------------------------------------------------------------------------  
1/1  Ingress Control Plane Policing  
         Ingress TCAM Entries                  3     309     2304  
     Egress Control Plane Policing  
         Egress TCAM Entries                   2      86     1024  
     Routed Ingress IPv4 VLAN ACL  
         Ingress TCAM Entries                  3       9     2304                                   << no change from last  
     Total  
         Ingress TCAM Entries                        318     4608    4608  
         Egress TCAM Entries                          86     1024    1024  
         Policers                                      0             6144  
         Ingress L4 Port Ranges                        0               32  
8325(config)#

######################### 7. Using ports defined in separate entries in object-group

8325(config)# sh object-group  
Type       Name  
  Sequence L4 Port(s)/Address  
-------------------------------------------------------------------------------  
IPv4       testip  
        10 10.10.10.1  
        30 10.10.10.3  
-------------------------------------------------------------------------------  
Port       test-ports  
        10    4010 -  4011  
-------------------------------------------------------------------------------  
Port       test-ports2  
        10 =  4010  
        20 =  4011  
8325(config)# sh access-list commands  
access-list ip test1  
    10 permit tcp 10.10.10.2 testip group test-ports2                                    (((2\*2)+1)\*3) =15  
interface vlan10  
    apply access-list ip test1 routed-in  
8325(config)# sh resources

Resource Usage:

Mod  Description  
         Resource                          Width    Used Reserved    Free  
-------------------------------------------------------------------------  
1/1  Ingress Control Plane Policing  
         Ingress TCAM Entries                  3     309     2304  
     Egress Control Plane Policing  
         Egress TCAM Entries                   2      86     1024  
     Routed Ingress IPv4 VLAN ACL  
         Ingress TCAM Entries                  3      **15**    2304                                   << two triple width entry(+6) are added  
     Total  
         Ingress TCAM Entries                        324     4608    4608  
         Egress TCAM Entries                          86     1024    1024  
         Policers                                      0             6144  
         Ingress L4 Port Ranges                        0               32

Tags: ArubaOS-CX Switches, 10.01.0040, #8325, tcam, #acl, object-group