Description

This article describes how to customize TCAM (Ternary Content Addressable Memory) lookup for each feature which uses TCAM.

The lookup is composed of fields, in the packet header / forwarding chip pipeline decisions, that are of interest to a feature. Size of the lookup determines the number of banks to be used by a feature. Traditionally, any feature uses a predefined TCAM lookup. As TCAM is a scarce resource, features which use it may run out of hardware resources. Listed below are some of the reasons for TCAM exhaustion,

- Number of features using TCAM is high,
- One or more features are using too many TCAM entries,

One way to overcome TCAM exhaustion is by reducing TCAM lookup size. User-defined TCAM profile overrides the out-of-box predefined lookup by providing lookup keys that are in-line with the features configurations, like security ACL (Access Control List), policy QoS (Quality of Service). Example: if an IPv4 ACL applied on a port in egress direction is matching on source IP address and destination IP address, then the user can provide just these two fields for lookup. This helps in reducing the lookup size.

Platform compatibility

Platforms supported	First supported version
DCS-7050CX3-32S DCS-7050SX3-48C8 DCS-7050SX3-48YC8	4.26.0.F
DCS-7050SX3-48YC12 DCS-7050CX3M-32S DCS-7050TX3-48C8 DCS-7050SX3-96YC8 DCS-7060PX4-32 DCS-7060DX4-32 DCS-7060DX4-32-D CCS-720XP-24Y6 CCS-720XP-24ZY4 CCS-720XP-48Y6 CCS-720XP-48ZC2 CCS-720XP-96ZC2	4.26.1F
CCS-710P-12 CCS-710P-16P CCS-722XP-48Y6-F CCS-722XP-48ZY6-F DCS-7010TX-48-F	4.27.0F

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

DCS-7010TX-48-R DCS-7010TX-48-DC-F DCS-7010TX-48-DC-R	
DCS-7260CX3-64 DCS-7260CX3-64LQ DCS-7260CX3-64E	4.28.2F
7368X4-SC CCS-755-X3-SC CCS-758-X3-SC 7300X3-48YC4-LC 7300X3-32C-LC	4.29.0F
DCS-7050DX4-32S DCS-7050PX4-32S	4.30.0F

Configuration

TCAM profile CLI's configuration is under hardware tcam configuration mode.

```
switch(config)# hardware tcam
switch(config-hw-tcam)#
```

Profile Configuration

System profiles are predefined profiles in Arista EOS. Users can use a predefined system profile or create a TCAM profile to meet specific requirements.

There are two ways to create a TCAM profile:

- Create a new profile from the top.
- Create a new profile by copying an existing system profile.

The latter is the recommended way.

The "show hardware tcam profile <profilename>" command will display the features that are enabled in the system profile. Adding detail to the command "show hardware tcam profile <profilename> detail" will provide further information about the features key fields.

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

If a feature is not specified in a profile CLI configuration, then it will use the predefined lookup.

Note:
Due to the constant addition of new features and functionality, custom profiles that used to fit in an old release may no longer fit in a future release. Please work with customer support to ensure that any custom TCAM profile continues to work in future releases.

System profile	First supported	Description
default	4.26.0.F	This is the profile that is enabled by default. No configuration is necessary.

Profile Configuration - Copy existing profile

When creating a profile based on an existing one, all of the features configuration is copied to the new profile. Then it can be modified.

Although the default profile supports a wide variety of features, it is recommended to use a copyable profile with the closest features and key fields.

```
switch(config-hw-tcam)# profile <profilename> copy default
switch(config-hw-tcam-profile-<profilename>)#
```

Profile Configuration - New

When creating a profile from the top, all of the required features, and key fields have to be configured.

Note:
This method is not recommended.

```
switch(config-hw-tcam)# profile <profilename>
switch(config-hw-tcam-profile-<profile>)#
```

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

This command can also be used to update existing TCAM profiles.

Notes:
The predefined system profiles cannot be changed.
Only profiles that were created using the aforementioned methods can be modified.

Deleting TCAM Profiles

The following command is used to remove a profile

```
switch(config-hw-tcam)# no profile <profilename>
```

Note:
The predefined system profiles cannot be deleted.

Applying a Profile

The profile will be saved after exiting the profile config mode. The following command applies the profile to the system globally. For Modular Chassis, this command will apply profile to all the supported chips

```
switch(config-hw-tcam)# system profile <profile>
```

Applying a profile triggers a hitfull restart of the forwarding agent. This resets the forwarding chip. Look at the Syslog Messages section for more information on agent restart.

Feature Configuration

Each Feature can be added or deleted from the new profile.

```
switch(config-hw-tcam-profile-<profile>)# [no] feature <feature>
```

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
```

The features are described by hierarchical CLI keywords. See the Features section below for more details.

Feature copy

Adding a feature manually could be time consuming. Instead the feature can be copied from an existing profile. Then it can be used as is or modified. The command to copy the feature acl port mac ingress from the default profile template is described below.

```
switch(config)# hardware tcam
switch(config-hw-tcam)# profile newfeature
switch(config-hw-tcam-profile-
newfeature)# feature acl port mac ingress copy default
```

Note:
It is recommended to copy features from existing profiles or the profile template instead of configuring from scratch

Configuring Feature Key Fields

This command describes the TCAM key format for the feature. Command to add or delete fields that are used to build the key.

```
switch(config-hw-tcam-
profile-<profile>-feature-<feature>)# [no] key field <field>
```

Notes:
All supported key fields can be found with 'key field ?'.

See the Key Fields section below for more details.

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Show commands

The “show hardware tcam profile” lists the TCAM profile status on each line card. In case of successful programming it is as shown below.

```
switch(config)# show hardware tcam profile
                     Configuration            Status
FixedSystem          testprofile              testprofile


```

If the profile cannot be programmed, the “Status” column prints 'ERROR'. This status is usually seen when one or more qualifiers are not valid for a feature(s). Features that use TCAM functionality may not work properly when the profile is in the 'ERROR' state. Please, see Limitations section for more information.

```
switch(config)# show hardware tcam profile
                     Configuration            Status
FixedSystem          testprofile              ERROR

Detailed Programming Status:
FixedSystem
   [Error] qualifier  dst-
ipv6 is not supported by feature 'qos vlan ip'


```

The “show hardware tcam profile <profile>” command displays the features enabled in TCAM <profile>

```
switch(config-hw-tcam-profile-
myprofile)# show hardware tcam profile myprofile
Features enabled in TCAM profile myprofile: [ FixedSystem ]
 acl port ip egress
 acl port ip ingress
 acl port ipv6 egress
 acl port ipv6 ingress
 acl port ipv6 source-only egress
 acl port mac egress
 acl port mac ingress
 acl vlan ip egress
 acl vlan ip ingress
 acl vlan ipv6 egress
 acl vlan ipv6 ingress
```

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
 acl vlan ipv6 source-only egress
 qos port ip
 qos port ipv6
 qos vlan ip
 qos vlan ipv6
 pbr ip
 pbr ipv6
```

The “show hardware tcam profile <profile> detail” command displays further info about the TCAM profile features

```
switch(config-hw-tcam)# show hardware tcam profile myprofile detail
Profile myprofile [ FixedSystem ]
 Feature:              acl port ip egress
 Key size:             320
 Key Fields:           dscp, dst-ip, ip-frag, ip-protocol, l4-dst-port,
                       l4-src-port, src-ip

 Feature:              acl port ip ingress
 Key size:             320
 Key Fields:           dscp, dst-ip, ip-frag, ip-protocol, l4-dst-
port, l4-ops,
                       l4-src-port, src-ip, tcp-control, ttl

 Feature:              acl port ipv6 egress
 Key size:             320
 Key Fields:           dst-ipv6, ip-protocol, ipv6-next-header,
                       ipv6-traffic-class, l4-dst-port, l4-src-
port, src-ipv6,
                       tcp-control, ttl

 Feature:              acl port ipv6 ingress
 Key size:             320
 Key Fields:           dst-ipv6, ip-protocol, ipv6-next-header,
                       ipv6-traffic-class, l4-dst-port, l4-ops, l4-src-
port,
                       src-ipv6, tcp-control, ttl

 Feature:              acl port ipv6 source-only egress
 Key size:             320
 Key Fields:           ip-protocol, src-ipv6

 Feature:              acl port mac egress
 Key size:             320
```

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
 Key Fields:          dst-mac, ether-type, src-mac
...
```

Note:
The profile contains all the features that are untouched after copying from the base profile.

Examples

This example demonstrates how to create a new profile, 'matchvlan', to match on a outer-vlan-id field in IPv4 QoS applied to a port, by copying profile 'testprofile' which has the same feature but does not match on outer-vlan-id. The new 'matchvlan' profile inherits all of the features and key fields from 'testprofile'. Consequently, the only thing that has to be configured is adding the outer-vlan-id key field in the QoS feature.

```
switch(config-hw-tcam)# profile matchvlan copy testprofile
switch(config-hw-tcam-profile-matchvlan)# feature qos port ip
switch(config-hw-tcam-profile-matchvlan-feature-qos-port-
ip)# key field outer-vlan-id
switch(config-hw-tcam-profile-matchvlan-feature-qos-port-ip)# exit
switch(config-hw-tcam-profile-matchvlan)# exit
Saving new profile 'matchvlan'
switch(config-hw-tcam)# system profile matchvlan
```

Configurable Profile Attributes

Features

Security ACL Features

- acl port ip egress (Port ACL matching on IPv4 packets at egress)
    - This feature enables custom lookup for egress security acls on routed and bridged IPv4 packets. Enable this feature when egress IPv4 security acls are applied on a port.
- acl port ip ingress (Ingress Port ACL matching on IPv4 packets)
    - This feature enables custom lookup for ingress security acls on routed and bridged IPv4 packets. Enable this feature when ingress IPv4 security acls are applied on a port.
- acl port ipv6 egress (Egress Port ACL matching on IPv6 packets)

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

    - This feature enables custom lookup for egress security acls on routed and bridged IPv6 packets. Enable this feature when egress IPv6 security acls are applied on a port.
- acl port ipv6 ingress (Ingress Port ACL matching on IPv6 packets)
    - This feature enables custom lookup for ingress security acls on routed and bridged IPv6 packets. Enable this feature when ingress IPv6 security acls are applied on a port.
- acl port ipv6 source-only egress (Egress Port Source-Only ACL matching on IPv6 packets)
    - This feature enables custom lookup for egress standard security acls on routed and bridged IPv6 packets. Enable this feature when egress standard IPv6 security acls are applied on a port.
- acl port mac egress (Egress Port ACL matching on Ethernet packets)
    - This feature enables custom lookup for egress security acls on bridged and routed Ethernet frames. Enable this feature when egress Ethernet security acls are applied on a port.
- acl port mac ingress (Ingress Port ACL matching on Ethernet packets)
    - This feature enables custom lookup for ingress security acls on bridged and routed Ethernet frames. Enable this feature when ingress Ethernet security acls are applied on a port.
- acl vlan ip egress (Egress SVI ACL matching on IPv4 packets)
    - This feature enables custom lookup for egress IPv4 SVI security acls on routed packets. Enable this feature when egress IPv4 security acls are applied on an SVI.
- acl vlan ip ingress (Ingress SVI ACL matching on IPv4 packets)
    - This feature enables custom lookup for ingress IPv4 SVI security acls on routed packets. Enable this feature when ingress IPv4 security acls are applied on an SVI.
- acl vlan ipv6 egress (Egress SVI ACL matching on IPv6 packets)
    - This feature enables custom lookup for egress IPv6 SVI security acls on routed packets. Enable this feature when egress IPv6 security acls are applied on an SVI.
- acl vlan ipv6 ingress (Ingress SVI ACL matching on IPv6 packets)
    - This feature enables custom lookup for ingress IPv6 SVI security acls on routed packets. Enable this feature when ingress IPv6 security acls are applied on an SVI.
- acl vlan ipv6 source-only egress (SVI Source-Only ACL matching on IPv6 packets)

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

    - This feature enables custom lookup for egress IPv6 SVI standard security acls on routed packets. Enable this feature when egress IPv6 standard security acls are applied on an SVI.

Policy QoS Features

- qos port ip (Port QoS policy matching on IPv4 packets)
    - This feature enables custom lookup for ingress policy QoS on IPv4 packets. Enable this feature when IPv4 policy QoS is applied on a port.
- qos port ipv6 (Port QoS policy matching on IPv6 packets)
    - This feature enables custom lookup for ingress policy QoS on IPv6 packets. Enable this feature when IPv6 policy QoS is applied on a port.
- qos vlan ip (SVI QoS policy matching on IPv4 packets)
    - This feature enables custom lookup for ingress policy QoS on IPv4 packets. Enable this feature when IPv4 policy QoS is applied on a SVI.
- qos vlan ipv6 (SVI QoS policy matching on IPv6 packets)
    - This feature enables custom lookup for ingress policy QoS on IPv6 packets. Enable this feature when IPv6 policy QoS is applied on a SVI.

Policy Based Routing Features

- pbr ip (Policy Based Routing policy matching on IPv4 packets)
    - This feature enables custom lookup for ingress PBR policy on routed IPv4 packets. Enable this feature when IPv4 PBR policy is applied on routed ports.
- pbr ipv6 (Policy Based Routing policy matching on IPv6 packets)
    - This feature enables custom lookup for ingress PBR policy on routed IPv6 packets. Enable this feature when IPv6 PBR policy is applied on routed ports.

Key Fields

Ethernet Fields

- dst-mac
    - MAC destination address
    - Field size: 48bits
- ether-type
    - Ethertype protocol value

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

    - Field size: 16bits
- outer-vlan-id
    - Outer VLAN ID
    - Field size: 12bits
- src-mac
    - MAC source address
    - Field size: 48bits

Ethernet Internal Fields

- vlan
    - Forwarding VLAN ID (this field is available for ACL applied to SVI, remove this field to enforce strict ACL sharing mode on SVIs)
    - Field size: 12bits

IPv4 Fields

- dscp
    - IPv4 DSCP value
    - Field size: 8bits
- dst-ip
    - IPv4 destination address
    - Field size: 32bits
- ip-frag
    - Non-head packet fragment
    - Field size: 2bits
- ip-protocol
    - IP protocol number
    - Field size: 8bits
- src-ip
    - IPv4 source address
    - Field size: 32bits
- ttl
    - TTL (Time-To-Live) value
    - Field size: 8bits

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

IPv6 Fields

- dst-ipv6
    - IPv6 destination address
    - Field size: 128bits
- dst-ipv6-high
    - IPv6 destination address (upper 64 bits)
    - Field size: 64bits
- hop-limit
    - IPv6 hop limit
    - Field size: 8bits
- ipv6-next-header
    - IPv6 next header/IP protocol type
    - Field size: 8bits
- ipv6-traffic-class
    - IPv6 traffic class
    - Field size: 8bits
- src-ipv6
    - IPv6 source address
    - Field size: 128bits
- src-ipv6-high
    - IPv6 source address (upper 64 bits)
    - Field size: 64bits

Layer 4 Fields

- l4-dst-port
    - L4 destination port number
    - Field size: 16bits
- l4-ops
    - L4 port range
    - Field size: 32bits
- l4-src-port

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

    - L4 source port number
    - Field size: 16bits
- tcp-control

    - TCP control flags
    - Field size: 8bits

Tcam slice sharing

By default, each feature mentioned in Features list above will occupy a separate TCAM slice even if it doesn't need all of the tcam entries in a slice. Hence the number of slices available restricts the number of features that can be configured. It's possible to configure mutually exclusive features to share a TCAM slice between them using user defined TCAM profiles. Currently slice sharing is supported for the below pair of features.

Feature pair supported	First supported version
acl port ip ingress and acl port ipv6 ingress (only non vxlan groups)	4.30.2F
acl vlan ip ingress and acl vlan ipv6 ingress	4.30.2F
qos port ip and qos port ipv6	4.30.2F
qos vlan ip and qos vlan ipv6	4.30.2F
pbr ip and pbr ipv6	4.30.2F

To configure slice sharing for a pair of features, corresponding features configuration needs to be copied from one of the system TCAM profiles provided below. Each of these system profiles comes with a restriction on maximum lookup size (in terms of number of slices) used for feature programming. Feature configuration can be copied from the required system profile to user defined TCAM profile as per configurational needs.

system profile name	maximum lookup size (in terms of number of slices)
system-profile-160b-ip-type-tcam-slice-sharing-1	1
system-profile-320b-ip-type-tcam-slice-sharing-1	2
system-profile-480b-ip-type-tcam-slice-sharing-1	3

The commands to copy acl port ip ingress and acl port ipv6 ingress pair of features for slice

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

sharing configuration from system-profile-320b-ip-type-tcam-slice-sharing-1 is described below

```
switch(config)#hardware tcam
switch(config-tcam)#profile sliceSharing
switch(config-tcam-profile-sliceSharing)#feature acl port ip ingress c
opy system-profile-320b-ip-type-tcam-slice-sharing-1
switch(config-tcam-feature-acl-port-ip-ingress)#exit
switch(config-tcam-profile-sliceSharing)#feature acl port ipv6 ingress
 copy system-profile-320b-ip-type-tcam-slice-sharing-1
switch(config-tcam-feature-acl-port-ipv6-ingress)#exit
switch(config-tcam-profile-sliceSharing)#exit
```

After copying the features from a system profile, users may choose to replace some Key Fields as per the configurational needs. It is recommended to reach out to Arista for such changes. A pair of features that are configured to share slices will have the same Action priority and Key size value. Note that changing Action Priority and Key Size values might lead to erroneous TCAM profile and hence it’s highly discouraged.

“show hardware tcam profile <profilename> detail” command can be used to display the Slice sharing configured profile

```
switch(config-tcam)#show hardware tcam profile sliceSharing detail
Profile sliceSharing
 Feature:               acl port ip ingress
 Action priority:       63
 Key size:              320
 Key Fields:            dscp, dst-ip, ip-frag, ip-protocol, l4-dst-
port,
                        l4-ops, l4-src-port, src-ip, tcp-control, ttl

 Feature:               acl port ipv6 ingress
 Action priority:       63
 Key size:              320
 Key Fields:            dst-ipv6-high, hop-limit, ip-protocol,
                        ipv6-next-header, l4-dst-port, l4-src-port,
                        src-ipv6-high
```

Syslog messages

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Changing the TCAM profile will restart forwarding agent(s), and the following syslog message is expected:

```
%STRATA-6-EXPECTED_AGENT_EXIT: Slice agent will exit and restart becau
se TCAM profile changed.
```

WARNINGS

- Removing the “vlan” key field from the features “acl vlan ip ingress” and “acl vlan ipv6 ingress” forces ingress security ACL on SVIs to operate in strict sharing mode. This is an optimization to remove additional 12bits of VLAN id from lookup. If you are in this mode then the number of unique ACLs for SVI is reduced to 31 each for IPv4 and IPv6.
    - Example: if you configure 32nd unique IPv4 ACL on the switch after configuring 31 unique IPv4 ACLs which are applied to a set of SVIs then you would run into the following warning and syslogs,

```
switch(config-if-Vl32)# ip access-group acl32 in
% Error: Cannot apply ip ACL acl32 to Vlan32 (Too many ACLs
)

%ACL-3-HW_RESOURCE_FULL: Hardware resources are insufficien
t to program all ACLs (Linecard0/0)
%ACL-3-HW_RESOURCE_NORMAL: All ACLs are programmed in hardw
are (Linecard0/0)
```

- When configuring VxLAN you might see the following message in the forwarding agent(s) log. Please refer to the limitation section to get more information.

```
ERROR: VxLAN VFP entry invalid!! ( DstIp missing in group qset )
ERROR: VxLAN VFP entry invalid!! ( IpProtocol missing in group qs
et )
ERROR: VxLAN VFP entry invalid!! ( L4DstPort missing in group qse
t )
```

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Troubleshooting

In case “show hardware tcam profile” shows “ERROR” then it is likely that there are one or more errors in the applied profile.

- Comparing the applied profile with the “default” profile is a good starting point.
- You can use the following table to validate the profile manually.
- If the above steps do not resolve the issue contact Arista.

Feature	Valid key fields
acl port ip egress	dscp dst-ip ip-frag ip-protocol l4-dst-port l4-src-port src-ip tcp-control ttl
acl port ip ingress	dscp dst-ip ip-frag ip-protocol l4-dst-port l4-ops l4-src-port src-ip tcp-control ttl
acl port ipv6 egress	dst-ipv6 dst-ipv6-high hop-limit ip-protocol ipv6-next-header ipv6-traffic-class l4-dst-port l4-src-port src-ipv6 src-ipv6-high tcp-control
acl port ipv6 ingress	dscp dst-ipv6 dst-ipv6-high

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

	hop-limit ip-protocol ipv6-next-header ipv6-traffic-class l4-dst-port l4-ops l4-src-port src-ipv6 src-ipv6-high tcp-control
acl port ipv6 source-only egress	ip-protocol src-ipv6
acl port mac egress	dst-mac ether-type src-mac
acl port mac ingress	dst-mac ether-type src-mac
acl vlan ip egress	dscp dst-ip ip-frag ip-protocol l4-dst-port l4-src-port src-ip tcp-control ttl
acl vlan ip ingress	dscp dst-ip ip-frag ip-protocol l4-dst-port l4-ops l4-src-port outer-vlan-id src-ip tcp-control ttl vlan
acl vlan ipv6 egress	dst-ipv6 dst-ipv6-high hop-limit

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

	ip-protocol ipv6-next-header ipv6-traffic-class l4-dst-port l4-src-port src-ipv6 src-ipv6-high tcp-control
acl vlan ipv6 ingress	dst-ipv6 dst-ipv6-high hop-limit ip-protocol ipv6-next-header ipv6-traffic-class l4-dst-port l4-ops l4-src-port outer-vlan-id src-ipv6 src-ipv6-high tcp-control vlan
acl vlan ipv6 source-only egress	ip-protocol src-ipv6
qos port ip	dscp dst-ip ether-type ip-frag ip-protocol l4-dst-port l4-ops l4-src-port outer-vlan-id src-ip tcp-control ttl vlan
qos port ipv6	dscp dst-ipv6 dst-ipv6-high ether-type hop-limit ip-protocol ipv6-next-header

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

	ipv6-traffic-class l4-dst-port l4-ops l4-src-port outer-vlan-id src-ipv6 src-ipv6-high tcp-control vlan
qos vlan ip	dscp dst-ip ether-type ip-frag ip-protocol l4-dst-port l4-ops l4-src-port src-ip tcp-control ttl
qos vlan ipv6	dscp dst-ipv6 dst-ipv6-high ether-type hop-limit ip-protocol ipv6-next-header ipv6-traffic-class l4-dst-port l4-ops l4-src-port src-ipv6 src-ipv6-high tcp-control
pbr ip	dscp dst-ip ip-frag ip-protocol l4-dst-port l4-ops l4-src-port src-ip tcp-control ttl

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

	outerVlanId
pbr ipv6	dst-ipv6 hop-limit ip-protocol ipv6-next-header ipv6-traffic-class l4-dst-port l4-ops l4-src-port outer-vlan-id src-ipv6 tcp-control

FAQs

- **Do you need to use a TCAM profile to use features?**
  No, switches which support TCAM profiles are shipped with a “default” profile which provide similar lookup when compared to prior releases.
- **Can the default profile be edited?**
  No, this is a read-only profile.
- **Do all features need to be configured in profile?**
  No, if the profile does not specify a feature then predefined lookup is used. Profile provides a way to override predefined lookup.
- **Forwarding agent did not restart after a profile change. Is this expected?**
  If the profile has errors then it may fail validation checks. Validation failure will result in aborting of profile application and no agent restart will be seen. To verify if this is the issue run the “show hardware tcam profile” command and look for “ERROR” in output.
- **Security ACL, Policy QoS rules stopped working after a profile was applied. Can this be due to the newly applied profile?**
  There are a few possibilities here,
  - The feature lookup field configuration does not match ACL, Policy QoS rules,
  - The profile configuration is not valid therefore ACL, and Policy QoS will be using the last valid profile applied.

  In either case, read profile Arista.
- **Can profiles be configured using CLI sessions or configure replace?**
  Profiles can be configured using CLI session or configure replace but it is not recommended. CLI session / configure replace which has any configuration that changes TCAM layout can be impacted with a change in TCAM profile. Hence it is recommended not to combine TCAM profile change with other TCAM based configuration change.

Limitations

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

- Both security ACL and policy QoS program some implicit rules which may be impacted by missing key fields in TCAM profile features. Following is the list of implicit rules,
    - ICMPv6 Neighbor Discovery rules
    - IPv4 permit fragment rules
- Removing any of the fields listed below from the feature for IPv4 ingress security ACL on ports impacts VxLAN traffic (when both VxLAN and ingress IPv4 ACL is applied to ports). This is due to the sharing of lookup between VxLAN and “acl port ip ingress” feature.
    - dst-ip,
    - ip-protocol,
    - l4-dst-port,
- Predefined lookup and “default” profile lookup for a feature may differ. For certain features, using TCAM profile enables some optimizations in lookup which is not available with the predefined lookup. These optimizations are available with an out-of-the-box “default” profile itself.
- To use VLAN match criteria in policy QoS “vlan” key-field needs to be included in profile for policy QoS features.
- The “show hardware tcam profile” command does not display all errors in profile, instead it shows only the first error in profile. This makes profile rectification an iterative process. To check all errors please follow the steps given in the Troubleshooting section.
- Removing the “ip-proto” qualifier from ingress facing features may not remove IP protocol from lookup. This makes the rule match stricter. Ex: If ACL rule filters on TCP packets but TCAM profile does not have the “ip-proto” qualifier we still end up filtering on TCP packets instead of making IpProtocol match as DontCare.
- Policy Based Routing (PBR) policy configures some implicit rules on some platforms. These may impact PBR functionality if “dst-ip”/”dst-ip6” and “l4-ops” key fields are not selected in the TCAM profile feature. Following is the list of implicit rules:
    - Multicast Skip Rule
    - L3 MTU Skip Rule
- Slice sharing is supported only in IFP TCAM stage
- Qos policy maps that have class maps matching on dscp/ecn/mac or vlan will not work as expected if slice sharing is enabled on below pair of features
    - qos port ip and qos port ipv6
    - qos vlan ip and qos vlan ipv6
- Vni rate limiting will not filter properly for non-ip and ipv6 packets if slice sharing is configured for below pair of features
    - qos port ip and qos port ipv6
- Slice sharing with single slice lookup width configuration is not supported for the below pair of features.
    - pbr ip and pbr ipv6

Copyright 2023 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.