Nexus 7000 TCAM Bank Limitations and Bank Chain Configuration

Document ID: 116151

Contributed by Jane Zizhen Gao, Cisco TAC Engineer.
Jun 18, 2013

Contents

Introduction

This document describes the default programming for the Access Control List-based (ACL) features for Nexus 7000 Ternary Content Addressable Memory (TCAM) banks and how to pool resources using the bank chaining feature.

Problem

With the initial implementation, ACL features are not programmed across different TCAM banks. This limits the available entries for each feature to 16,000. For those customers who have large ACLs, this becomes a problem. Use of the bank chain feature solves this problem with the removal of the bank restriction. When the bank chain is enabled, ACL-based features can be programmed across banks.

Examples of errors messages:

```
ACLQOS-SLOT3-4-ACLQOS_OVER_THRESHOLD
Tcam 0 Bank 0's usage has reached its threshold

ACLMGR-3-ACLMGR_VERIFY_FAIL  Verify failed: client 8200016E,
Sufficient free entries are not available in TCAM bank
```

Solution

- When the bank chain is enabled, it only affects future configurations. The current TCAM entries are not reprogrammed. When a new ACL is applied to an interface, that new ACL is programmed across multiple banks.
- When the bank chain is enabled, the ACL is programmed across banks (except Tunnel Decap and Control Plane Protection (CoPP)). (Refer to the Restrictions section.) If there are enough entries in two TCAM Bank 0's, the ACL is split and programmed into those two banks.
- If the two TCAM Bank 0s do not have enough free entries, the ACL rule is programmed across all four banks.
- When the bank chain feature is enabled, even if the ACL has a smaller number of rules than one single bank's free entries, it is programmed across the two TCAM Bank 0s.

- When the bank chain is disabled, the current TCAM entries are reprogrammed. If the current ACL does not fit into one bank, an error message is returned and the bank chain cannot be disabled.
- During the In-Service Software Upgrade (ISSU) downgrade, the bank chain must be disabled; otherwise, the ISSU downgrade will fail.

Restrictions

- When the bank chain feature is enabled, the policies applied to one interface and one directory are mergable. Any one of the policies which have statistics enabled cannot be merged. When the bank chain is enabled, the feature with statistics enabled cannot co-exist with other features on the same interface, at the same direction.

  Example: When statistics are enabled on ingress Router Access Control List (RACL) at Ethernet2/1, Policy Based Routing (PBR) cannot be configured under that interface.

- Any two policies, whose result types are different, cannot be merged. There are three result types: ACL, Accounting, and Quality of Service (QoS). These three result types cannot be merged.
    1. Features under the ACL result type: Port Access Control List (PACL), RACL, VLAN Access Control List (VACL), PBR, DHCP, Address Resolution Protocol (ARP), Netflow
    2. Features under the Accounting result type: Netflow simple
    3. Features under the QoS result type: QoS

  Example: RACL and QoS cannot co-exist on the same direction under one interface with the bank chain enabled.

- Tunnel Decap and CoPP are programmed under one Logical Interface (LIF) and cannot be merged because their result types are different. In order to avoid the restriction in which they cannot co-exist, they are kept in one bank, even when the bank chain is enabled. When the Role-Based Access Control List (RBACL) is enabled, the Source Security Group Tag/Destination Security Group Tag (SGT/DGT) will be used in order to create the TCAM look-up key. The RBACL cannot merge with other egress policies, since the label is programmed to pick up SGT/DGT instead of IPv4 source destination addresses. When the bank chain is enabled, the following rules apply:

    1. If the RBACL is enabled under Virtual Routing and Forwarding (VRF), no other egress policies can be configured under those interfaces on that VRF.
    2. If the RBACL is enabled under VLAN, no VLAN egress policy can be configured.

- Port + Vlan policy: In hardware (HW), port policy and VLAN policy labels are programmed under one Information Lifecycle Management (ILM) entry. It can only have one label for port policy and one label for VLAN policy. When the bank chain is enabled, Port + VLAN policies cannot be supported:
    1. When a port policy is configured, no policy can be configured under the VLAN/SVI that the port belongs to.
    2. When a VLAN/SVI policy is configured, no policy can be configured on the port that belongs to the VLAN.

Example of an error message:

```
ERROR: Resource-pooling is not supported with certain feature combinations
```

Configuration

config t
hardware access-list resource pooling !can only be issued from the default VDC

show hardware access-list resource pooling
show system internal access-list status

```
SITE1-AGG1(config)# hardware access-list resource pooling mod ?
  <1-9>  Specify module number
SITE1-AGG1(config)# hardware access-list resource pooling mod 3
SITE1-AGG1(config)# show hardware access-list resource pooling
   Module 3 enabled
SITE1-AGG1# show system internal access-list status
Atomic ACL updates Enabled.
TCAM Default Result is Deny.
ACL Logging enabled.
Current LOU resource threshold: 5
```

Related Information

- **Technical Support & Documentation - Cisco Systems**

Updated: Jun 18, 2013 Document ID: 116151