# Nexus 7000 Series Switch ACL Capture Example

**Document ID: 116044**

Contributed by Rajesh Gatti, Geovany Gonzalez, and Andy Gossett,
Cisco TAC Engineers.
Apr 29, 2013

## Contents



## Introduction

Access Control List (ACL) capture provides you the ability to selectively capture traffic on an interface or virtual local area network (VLAN) When you enable the capture option for an ACL rule, packets that match this rule are either forwarded or dropped based on the specified permit or deny action and can also be copied to an alternate destination port for further analysis. An ACL rule with the capture option can be applied:

1. In a VLAN,
2. In the ingress direction on all interfaces,
3. In the egress direction on all Layer 3 interfaces.

This feature is supported from Nexus 7000 NX−OS Release 5.2 and later. This document provides an example as a quick reference guide on how to configure this feature.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- Nexus 7000 with Release 5.2.x and later.
- M1 series line card.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to Cisco Technical Tips Conventions for information on document conventions.

# ACL Configuration Example

Here is an example configuration of ACL capture applied to a VLAN, also known as virtual LAN Access Control List (VACL) capture. Ten gigabit snifers designated may not be feasible for all scenerios. Selective traffic capture can be very useful in such scenerios especially during troubleshooting when traffic volumes are high.

```
!! Global command required to enable ACL-capture feature (on default VDC)
hardware access-list capture

             monitor session 1 type acl-capture
             destination interface ethernet 2/1
             no shut
             exit
!!
ip access-list TEST_ACL
  10 permit ip 216.113.153.0/27 any capture session 1
  20 permit ip 198.113.153.0/24 any capture session 1
  30 permit ip 47.113.0.0/16 any capture session 1
  40 permit ip any any
!!
!! Note: Capture session ID matches with the monitor session ID
!!
vlan access-map VACL_TEST 10
        match ip address TEST_ACL
        action forward
        statistics per-entry
!!
vlan filter VACL_TEST vlan-list 500
```

You can also check the ternary content addressable memory (TCAM) programming of the access list. This output is for the VLAN 500 for Module 1.

```
N7k2-VPC1# show system internal access-list vlan 500 input statistics

slot  1
=======

INSTANCE 0x0
---------------

  Tcam 1 resource usage:
  ----------------------
  Label_b = 0x802
   Bank 0
   ------
     IPv4 Class
       Policies: VACL(VACL_TEST)
       Netflow profile: 0
       Netflow deny profile: 0
       Entries:
         [Index] Entry [Stats]
         ---------------------
  [0006:0005:0005] permit ip 216.113.153.0/27 0.0.0.0/0  capture [0]
  [0009:0008:0008] permit ip 198.113.153.0/24 0.0.0.0/0  capture [0]
  [000b:000a:000a] permit ip 47.113.0.0/16 0.0.0.0/0  capture [0]
  [000c:000b:000b] permit ip 0.0.0.0/0 0.0.0.0/0   [0]
  [000d:000c:000c] deny ip 0.0.0.0/0 0.0.0.0/0   [0]
```

## Caveats

1. Only one ACL capture session can be active at any given time in the system across virtual device contexts (VDCs).
2. Nexus 7000 F1 Series modules do not support ACL capture.
3. Nexus 7000 F2 Series modules do not currently support ACL capture, but this might be in the roadmap.
4. ACL capture on Nexus 7000 M2−Series modules is supported with Cisco NX−OS Release 6.1(1) and later.
5. ACL capture on Nexus 7000 M1−Series modules is supported with Cisco NX−OS Release 5.2(1) and later.
6. ACL capture is not compatible with ACL logging.  Therefore, if you have ACLs with a ***log*** keyword, these do not work after you have globally entered ***hardware access−list capture***.
7. Because of bug CSCug20139, the example in this document is documented with a ***capture session*** per ACE instead of per ACL, until the bug is resolved.

# Related Information

- ***Cisco Nexus 7000 Series NX−OS Security Configuration Guide, Release 6.x, Configuration Examples for IP ACLs***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Apr 29, 2013 Document ID: 116044