

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Applied Mitigation Bulletins

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of Cisco Catalyst 6000, 6500, and Cisco 7600 Series MPLS Packet Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20070228-mpls.shtml>

## Revision 1.0

For Public Release 2007 February 28 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

[Cisco Response](#)  
[Device-Specific Mitigation and Identification](#)  
[Additional Information](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

## Cisco Response

### Vulnerability Characteristics

The Cisco Catalyst 6000 and 6500 series and Cisco 7600 Series Multiprotocol Label Switching (MPLS) packet vulnerability can be exploited from the local segment with no authentication, and no user interaction is necessary. The vulnerability may result in a denial of service (DoS) condition. The attack vector is via an MPLS frame (EtherType 0x8847 and 0x8848). This vulnerability is not designated by a CVE ID.

This document contains information to assist Cisco customers in identifying and mitigating attempts to exploit the Cisco Catalyst 6000 and 6500 series and Cisco 7600 Series MPLS packet vulnerability.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security

Advisory:

<http://www.cisco.com/warp/public/707/cisco-sa-20070228-mpls.shtml>

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the Cisco Catalyst 6000 and 6500 series and Cisco 7600 Series MPLS packet vulnerability. This document focuses on mitigation for vulnerable Cisco Catalyst 6000 and 6500 series and Cisco 7600 Series systems that are in core and distribution layers behind a switched access layer. The mitigation and identification techniques contained in this document are to be used on these access layer switches to filter frames that could be used to exploit this vulnerability.

The most preventive control provided by Cisco network devices is through the use of IOS VLAN maps.

Notice that the Cisco Catalyst 6000 and 6500 series and Cisco 7600 Series systems are not effective in filtering MPLS frames.

## Device-Specific Mitigation and Identification

Specific information on mitigation and identification is available for:

- [Cisco IOS Switches](#)

### Cisco IOS Switches



**Caution:** The effectiveness of any mitigation technique is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. As with any configuration change, evaluate the impact of this configuration prior to applying the change.

The following selected list of Catalyst IOS series switches were tested as screening devices in front of Cisco Catalyst 6000 and 6500 series and 7600 Series systems to mitigate the MPLS packet vulnerability:

- Cisco Catalyst 2960 Series
- Cisco Catalyst 3550 Series
- Cisco Catalyst 3750 Series
- Cisco Catalyst 4500 Series

### Cisco Catalyst 2960 Series Switches

#### Mitigation: MAC Access Groups

[MAC access groups](#) can be used to filter EtherType 0x8847 and EtherType 0x8848 frames from entering a port. For the mitigation to be effective, the MAC access group needs to be applied to all ports in the same broadcast domains as the vulnerable device. The Cisco Catalyst 2960 Series switches permit only the **mac access-group** to be applied on the input direction (**in** keyword)

```
mac access-list extended ACL-Deny-MPLS
```

```
!-- Filter MPLS frames
```

```
deny any any 0x8847 0x0
deny any any 0x8848 0x0
```

```
!-- Include other permit/deny MAC access list configuration commands
!-- according to security policy, might or not end in "permit any any"
```

```
permit any anyinterface FastEthernet0/10
switchport access vlan 200
mac access-group ACL-Deny-MPLS in
```

## Identification: MAC Access Groups

The Cisco Catalyst 2960 Series **show access-lists hardware counters** privileged EXEC mode command displays a single global counter for frames that have been dropped by all MAC access lists ("Drop: All frame count") and a single global counter for the total number of bytes in those dropped frames ("Drop: All bytes count")

```
Cat2960#show access-lists hardware counters
L2 ACL INPUT Statistics
Drop: All frame count: 165
Drop: All bytes count: 19684
Bridge Only: All frame count: 7886666
Bridge Only: All bytes count: 551148321
Forwarding To CPU: All frame count: 682046
Forwarding To CPU: All bytes count: 266514745
.
.
.
```

In the example, 165 frames were dropped by all MAC access groups in the switch, with a total of 19,684 bytes within those 165 dropped frames.

## Cisco Catalyst 3550 Series Switches

### Mitigation: VLAN Maps

[Catalyst 3550 Series VLAN maps](#) can be configured to filter MPLS frames in a VLAN. In the following example, vulnerable devices have interfaces in VLANs 162 and 200. Those VLANs are configured to drop incoming MPLS frames in the Cisco Catalyst 3550 Series switch that is serving as a shielding device:

```
mac access-list extended ACL-Match-MPLS
```

```
!-- Filter MPLS frames,
!-- will apply "action drop" to frames permitted in this MAC access-list
```

```
permit any any 0x8847 0x0
```

```
permit any any 0x8848 0x0
```

```
!-- Other permit/deny MAC access list configuration commands
!-- according to security policy
```

```
vlan access-map VMAP-Policy 10
  action drop
  match mac address ACL-Match-MPLS
vlan access-map VMAP-Policy 20
  action forward
vlan filter VMAP-Policy vlan-list 162,200
```

### Mitigation: MAC Access Groups

Catalyst 3550 Series MAC access groups can filter on any given EtherType value. They can be used to deny frames with EtherType 0x8847 or 0x8848. The access group needs to be applied to all ports in the broadcast domain of the vulnerable device. The Cisco Catalyst 3550 **mac access-group** can be applied only in the incoming direction (**in** keyword)

```
mac access-list extended ACL-Deny-MPLS
  deny any any 0x8847 0x0
  deny any any 0x8848 0x0
```

```
!-- Other permit/deny MAC access list configuration commands
!-- according to the security policy,
!-- might or might not end in "permit any any"
```

```
permit any any
```

```
interface FastEthernet0/1
  switchport access vlan 162
  switchport mode access
  mac access-group ACL-Deny-MPLS in
```

### Identification: MAC Access Groups and VLAN Maps

The Cisco Catalyst 3550 Series **show access-lists hardware counters** privileged EXEC mode command displays a single global counter for frames dropped by MAC access lists or VLAN maps. There is a separate counter for the total number of bytes dropped by both features. In the example below, 268 frames were dropped, which accounted for a total of 21,177 bytes.

```
Cat3550#show access-lists hardware counters
Input Drops:          268 matches (21177 bytes)
Output Drops:         0 matches (0 bytes)
Input Forwarded:     183663467 matches (14669769830 bytes)
Output Forwarded:    0 matches (0 bytes)
Input Bridge Only:   0 matches (0 bytes)
Bridge and Route in CPU: 0 matches (0 bytes)
Route in CPU:        460962054 matches (29596575890 bytes)
```

## Cisco Catalyst 3750 Series Switches

### Mitigation: VLAN Maps

[Catalyst 3750 Series VLAN maps](#) can be configured to filter MPLS frames in a VLAN. In the following example, a vulnerable device has one interface in VLAN 163. The Cisco 3750 that is serving as a screening device will drop incoming MPLS frames on VLAN 163.

```
mac access-list extended ACL-Match-MPLS

!-- MPLS EtherTypes to drop

permit any any 0x8847 0x0
permit any any 0x8848 0x0

!-- Include other permit/deny MAC access list configuration commands
!-- according to security policy.

vlan access-map VMAP-Policy 10
  action drop
  match mac address ACL-Match-MPLS
vlan access-map VMAP-Policy 20
  action forward

vlan filter VMAP-Policy vlan-list 163
```

### Mitigation: MAC Access Groups

[Catalyst 3750 Series MAC access groups](#) can filter on any given EtherType value, and can be used to deny frames with EtherType 0x8847 or 0x8848. The access group needs to be applied to all ports in the broadcast domain of the vulnerable device.

```
mac access-list extended ACL-Deny-MPLS
  deny any any 0x8847 0x0
  deny any any 0x8848 0x0

!-- Include other permit/deny MAC access list commands according to security p
!-- might or might not end in "permit any any"

permit any any

interface FastEthernet3/0/47
  switchport access vlan 163
  mac access-group ACL-Deny-MPLS in
```

### Identification: MAC Access Groups and VLAN Maps

The Cisco Catalyst 3750 Series **show access-lists hardware counters** privileged EXEC mode command displays a single global counter for frames dropped by all MAC access groups or VLAN

maps. There is a separate single global counter for the total number of bytes dropped by both features.

```
Cat3750#show access-lists hardware counters
L2 ACL INPUT Statistics
  Drop:                               All frame count: 18170
  Drop:                               All bytes count: 2999815
  Bridge Only:                         All frame count: 614950
  Bridge Only:                         All bytes count: 39483560
  Forwarding To CPU:                   All frame count: 0
  Forwarding To CPU:                   All bytes count: 0
.
.
.
```

In the previous output, 18,170 frames were dropped by MAC access groups or VLAN maps. The total byte count in the dropped frames was 2,999,815.

### Cisco Catalyst 4500 Series Switches

The proposed mitigation in the Cisco Catalyst 4500 Series is only possible if only IP frames are permitted by the Security Policy. The implementation of the **mac access-list** command allows only a predefined set of protocols to be filtered. The proposed mitigation for the Cisco Catalyst 6000 and 6500 series and Cisco 7600 Series MPLS packet vulnerability will drop AppleTalk and IPX frames, among others.

#### Mitigation: VLAN Maps

[Catalyst 4500 Series VLAN maps](#) provide the ability to filter according to a predefined list of protocol types. Mitigation of the Cisco Catalyst 6000 and 6500 and Cisco 7600 Series MPLS packet vulnerability can be accomplished by filtering all non-IP frames. In the following example VLAN 160 will drop all non-IP frames to protect a vulnerable device that has an interface in VLAN 160.

```
mac access-list extended ACL-Match-Non-IP
  permit any any

!-- Indicates ALL NON-IP frames flowing thru the switch will be dropped

vlan access-map VMAP-Policy 10
  action drop
  match mac address ACL-Match-Non-IP
!
vlan filter VMAP-Policy vlan-list 160
```

#### Mitigation: Port ACLs

[Catalyst 4500 Series port ACL \(PACL\)](#) can mitigate the Cisco Catalyst 6000 and 6500 series and Cisco 7600 Series MPLS packet vulnerability. The PACL in the Cisco Catalyst 4500 Series can be applied in the incoming or outgoing direction. The [access-group mode](#) interface configuration command can be used to control the interaction between the PACL, VLAN map, and router ACL that apply to the port.

```
mac access-list extended ACL-Deny-Non-IP
```

```

deny any any

!-- Drop all non-IP frames flowing through the switch

!
interface GigabitEthernet2/48
 switchport access vlan 160
 switchport mode access
 mac access-group ACL-Deny-Non-IP out
 access-group mode prefer port ! Default

```

Please note that the Cisco Catalyst 4500 Series VLAN maps and PACL features will not block IP protocol frames flowing through it (EtherTypes 0x0800 and 0x0806). Also, they will not block the following frames processed or generated by the switch itself:

- Spanning Tree 802.1d BPDU
- Cisco Shared Spanning Tree Protocol (SSTP)
- Cisco Discovery Protocol (CDP)
- Unidirectional Link Detection (UDLD)
- VLAN Trunking Protocol (VTP)

### Identification: VLAN Maps and PACL

The Catalyst 4500 Series implements counters per MAC Access Control Entry (ACE). Please note that the configuration required to mitigate the Cisco Catalyst 6000 and 6500 series and Cisco 7600 Series MPLS packet vulnerability would block loopback frames (EtherType 0x9000). There is no operational impact for the Catalyst 4500 Series to drop loopback frames of external stations. Due to the dropping of loopback frames, the **show access-lists** privileged EXEC mode command will constantly increment the number of matched frames. The default in Cisco IOS devices is to send a loopback frame every 10 seconds ( [keepalive](#) interface configuration command).

```

Cat4500#show access-lists
Extended MAC access list ACL-Deny-Non-IP
    deny any any (1151 matches)
Extended MAC access list ACL-Match-Non-IP
    permit any any (820 matches)

```

In the example output, 1151 frames were dropped by the MAC ACL used by the example PACL and 820 frames were dropped by the sample VLAN map configuration.

### Mitigation: {Insert content here}

- Cisco Catalyst 6000 and 6500 series VLAN Access Lists (VACLs) do *not* provide an effective mitigation. VACLs will not prevent MPLS frames from reaching the Route Processor nor they will filter those frames for upstream devices.
- Cisco Catalyst 2950 Series implementation of the MAC access group feature does not permit the ability to filter labeled packets independently of IP packets and cannot be used as a screening device for the Cisco Catalyst 6000 and 6500 series and Cisco 7600 Series MPLS packet vulnerability.

## Additional Information

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

## Revision History

|              |                  |                         |
|--------------|------------------|-------------------------|
| Revision 1.0 | 2007-February-28 | Initial public release. |
|--------------|------------------|-------------------------|

## Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

### Help us help you.

#### Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

#### This document solved my problem.

- Yes
- No
- Just browsing

#### Suggestions for improvement:

(256 character limit)

Send

|                      |                            |                       |                         |                          |                          |                      |
|----------------------|----------------------------|-----------------------|-------------------------|--------------------------|--------------------------|----------------------|
| <a href="#">Home</a> | <a href="#">How to Buy</a> | <a href="#">Login</a> | <a href="#">Profile</a> | <a href="#">Feedback</a> | <a href="#">Site Map</a> | <a href="#">Help</a> |
|----------------------|----------------------------|-----------------------|-------------------------|--------------------------|--------------------------|----------------------|

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)