HOW-TO

# CONFIGURE MAC NOTIFICATION TRAPS ON CISCO SWITCHES

*Applicable Versions: FortiNAC 8*

*03/15/2018*

Rev: D

# Contents



 

# *Overview*

## Introduction

In an environment where FortiNAC manages a large number of devices and ports, the best practice on switches that support SNMP MAC notification traps is to use these traps, instead of the standard linkUp and linkDown traps, to increase performance.

When MAC Notification traps are implemented, FortiNAC does not have to read the forwarding tables of the switches each time a host connects or disconnects from the network. This is because the MAC Notification traps contain MAC and connection data embedded in the traps. Networks using switches in the following situations may benefit from using MAC notification traps:

- An excessive number of switch ports, where performance would improve by changing the trap configuration, or

- Host connection and disconnection from the network do not generate linkUp and linkDown traps, such as, VoIP: where clients connect to the network behind IP Phones or Access Point Management (HUBs).

Set up each connection point to generate MAC Notification traps when a MAC address is added or removed from the network. This is done through the switch CLI interface. The coldStart and warmStart traps are not affected by this configuration change.

## Requirements

- Switches sending traps must be modeled in FortiNAC. Switches are added in Topology using the “Start Discovery” or “Add Device” option. See Online Help topics “Discover Devices” and “Add/Modify a Device” for instructions.

- This solution applies only to access ports – *do not enable MAC Notification traps on trunks, port channels, or uplinks.*

- **Only SNMP v1 traps are supported for inbound SNMP trap processing** (i.e. linkUp and linkDown traps, MAC Notification traps, cold start and warm start traps). SNMP v1 or v3 read and write are supported for communication between FortiNAC and the Cisco switch. For a list of traps and supported SNMP versions, see Online Help Topic "FortiNAC SNMP Traps Support."

 

- FortiNAC handles Mac Notification traps from IP Phones based on an attribute set on the server. The default is to ignore these traps in order to alleviate excessive traffic. However, trap handling for IP phones can be re-enabled manually at any time. See Solution 1753 in the Customer Portal or contact Support for assistance.

## Procedure

1. Configure SNMP MAC Notification traps on all access ports (do not include uplinks).
   **Important:** Only SNMP v1 traps are supported for inbound SNMP trap processing.

2. Remove linkUp and linkDown traps on ports where Mac Notification traps are added.

3. Configure SNMP and enable MAC Notification traps pointed to the IP address of the eth0 on FortiNAC Control Server or Control Server.

4. Configure MAC address table notifications globally.

5. Configure Context settings in switch for reading Mib-2 information. **Note:** This step only applies to devices managed using SNMP v3.

The following pages provide configuration examples for two different Cisco models.

**Note:** Based on switch model or IOS version, some of the commands may vary. It is recommended to review any associated Cisco product documentation.

## *Configuration Example 1: Cisco 3560 (IOS 12.2)*

1. Configure SNMP MAC Notification traps on all access ports (do not include uplinks). Remove linkUp and linkDown traps on ports where Mac Notification traps are added.

   interface fastEthernet 0/23
   **snmp trap mac-notification change added**
   **snmp trap mac-notification change removed**

   Example of an interface range setup: (ports 1 - 23):
   **interface range fastEthernet 0/1-23**
   **snmp trap mac-notification added**
   **snmp trap mac-notification removed**

2. Configure SNMP and enable MAC Notification traps pointed to the IP address of the eth0 on FortiNAC Control Server or Control Server (xxx.xxx.xxx.xxx).
   **snmp-server community public RO**
   **snmp-server community private RW**
   **snmp-server enable traps snmp coldstart warmstart**
   **snmp-server enable traps mac-notification change move threshold**
   **snmp-server host <xxx.xxx.xxx.xxx> public mac-notification snmp**

   **Important:** Only SNMP v1 traps are supported for inbound SNMP trap processing.

3. Configure MAC address table notifications globally.
   **mac address-table notification change**
   **mac address-table notification mac-move**
   **mac address-table notification threshold**

4. **L3 switches:** specify the IP address from which to source the traps and respond to SNMP requests. If SNMP traffic is sourced from an IP other than the one used to model the switch in Topology, FortiNAC will not process the traffic:
   **snmp-server source-interface traps <vlan>**

5. (SNMP v3 managed devices only) Configure Context settings correctly for reading Mib-2 information. See Appendix A.

6. When setup is complete, run the following command to save the configuration:
   **write memory**

To verify FortiNAC is receiving the traps using the Administrative UI, see Appendix B.

 

## *Configuration Example 2: Cisco cat4500e*

1. Configure SNMP MAC Notification traps on all access ports (do not include uplinks).

   interface fastEthernet 0/23
   **snmp trap mac-notification added**
   **snmp trap mac-notification removed**

   Example of an interface range setup: (ports 1 - 23):
   **interface range fastEthernet 0/1-23**
   **snmp trap mac-notification added**
   **snmp trap mac-notification removed**

2. Remove linkUp and linkDown traps on ports where Mac Notification traps are added.
   **no snmp-server enable traps snmp linkup**
   **no snmp-server enable traps snmp linkdown**

3. Configure SNMP and enable MAC Notification traps pointed to the IP address of the eth0 on FortiNAC Control Server or Control Server (xxx.xxx.xxx.xxx).
   **snmp-server community public RO**
   **snmp-server community private RW**
   **snmp-server enable traps MAC-Notification**
   **snmp-server host <xxx.xxx.xxx.xxx> public**

   **Important:** SNMP v1 traps are supported for inbound SNMP trap processing.

4. Configure MAC address table notifications globally.
   **mac-address-table notification**

5. (SNMP v3 managed devices only) Configure Context settings correctly for reading Mib-2 information. See Appendix A.

6. When setup is complete, run the following command to save the configuration:
   **write memory**

To verify FortiNAC is receiving the traps using the Administrative UI, see Appendix B.

 

## *Appendix A: Configure Context Settings for Mib-2 Information*

When using SNMP v3 to manage your Cisco device, you must configure your Context settings correctly for reading Mib-2 information. When FortiNAC processes MAC Notification traps, the dot1dbridge mib must be read. This mib is accessed via SNMP v3 using SNMP context values. The Cisco switch must be configured to allow access to these context values for the SNMP User/View created for access by FortiNAC. Specifically, each VLAN defined on the device is used as a context and a configuration setting allowing access to that VLAN/Context there is needed. See the example below:

**snmp-server group mygroup v3 auth read myview**
**snmp-server group mygroup v3 auth context vlan-35 read myview snmp-server group mygroup v3 auth context vlan-60 read myview**

This is where you create a group and provide the group with access to a particular view. You need to specify read access for each VLAN context. The example shows this was done for vlan-35 and vlan-60. You must add a line for each VLAN defined on the switch.

## *Appendix B: Confirming Mac Notification Traps*

Enable events:

1. Navigate to **Logs > Event Management**
2. Enable MAC Learned and MAC Removed events. Right click on each event and select **Log Internal**.

Once enabled, any MAC Notification traps processed will generate an event.

To view these events:

1. Navigate to **Logs > Events**.
2. From Add Filter drop-down menu, select **Event**.
3. From Event drop-down menu, select the either **MAC Learned** or **MAC Removed**.

Set any additional desired filters (such as date and time), then click **Update**.

Once troubleshooting is complete, disable the event:

1. Navigate to **Logs > Event Management**
2. Disable MAC Learned and MAC Removed events. Right click on each event and select **Disable**.