FortiNAC

Cisco MAC Notification Trap Configuration

Version: 8.x

Date: 02/28/2019

Rev: F

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM
http://www.fortinet.com/support-and-trainingt/training.html

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

Thursday, February 28, 2019

Contents

Overview

The information in this document provides guidance for configuring the Cisco device for MAC Notification traps. This document details the items that must be configured.

Note: As much information as possible about the integration of this device with FortiNAC is provided. However, the hardware vendor may have made modifications to the device's firmware that invalidate portions of this document. If having problems configuring the device, contact the vendor for additional support.

What it Does

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.

How it Works

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.*
- As of version 8.2.1, FortiNAC supports SNMP versions 1, 2 and 3 for MAC Notification traps. Refer to FortiNAC SNMP Trap Support in the Document Library.

- 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 and improve server performance. However, trap handling for IP phones can be re-enabled by navigating to **System > Settings > Network Device** in the FortiNAC Administration UI.

Procedure

General Steps

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

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

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 Contexts for VLANs.

   Context settings must be configured 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.

   For details and examples, see KB article Configure and validate Cisco SNMPv3.

6. Run the following command to save the configuration:
   write memory

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

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

5. (SNMP v3 managed devices only) Configure Contexts for VLANs.

   Context settings must be configured 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.

   For details and examples, see KB article Configure and validate Cisco SNMPv3.

6. Run the following command to save the configuration:
   write memory

Validate

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**.
4. 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**.

Troubleshooting

Possible causes for events not generating:

- NAC is not receiving the traps.
    - Verify the sending switch is configured properly. Traps should be sent to the eth0 IP address of the NAC Server/Control Server.
    - Run a packet capture to confirm whether or not the traps are reaching NAC. The tcpdump tool can be used in the NAC Server/Control Server CLI to run a packet capture. Alternatively, run a packet capture on the switch port the eth0 NAC Server/Control Server connects.

- Traps are received but not getting processed.
    - If SNMPv3, verify context values for every VLAN created in the switch are defined. See KB article Configure and validate Cisco SNMPv3.
    - Contact Support for troubleshooting assistance.