HOW-TO

CONFIGURE MAC NOTIFICATION TRAPS ON HP SWITCHES

DATE: 02.06.2018

Overview

For best performance, in an environment where FortiNAC manages a large number of devices and ports, the best practice is to use SNMP MAC Notification traps instead of the standard linkUp and linkDown traps.

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 (access port) 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.

Important: Do not enable MAC Notification traps on uplink ports (such as inter-switch links, trunks, port channels). Ports defined as uplinks in FortiNAC are not managed, and traps sent from such ports cause extra processing that is unnecessary.

HP Switch Setup

Note: The command syntax may be dependent upon the HP firmware. Refer to product documentation.

1. Enable MAC Notification traps globally on the switch with an interval of 2 seconds.
   snmp-server enable traps mac-notify trap-interval 2

2. Enable MAC Notification traps on the access ports.
   mac-notify traps <PORT-LIST> learned
   mac-notify traps <PORT-LIST> removed

3. Display MAC Notification Trap configuration:
   show mac-notify traps

4. Remove linkUp and linkDown traps on ports MAC Notification traps are added.
   no snmp-server enable traps link-change <PORT-LIST>

5. Display Link-Change traps configuration:
   show snmp-server traps

6. Configure each switch with the IP address of eth0 on the FortiNAC Server or Control Server as the destination for trap information (i.e., trap receiver).
   snmp-server host <community-name> <FortiNAC IP Address>

   Note: community name must be created in switch.

7. **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 trap-source <switch IP Address used in Topology>
   snmp-server response-source <switch IP Address used in Topology>

8. Display trap receivers:
   show snmp-server traps

Example: Mac Notification traps configured for ports 12-14 and sending to FortiNAC IP 15.255.133.236using community string “public.”

snmp-server enable traps mac-notify trap-interval 2
mac-notify traps 12-14 learned
mac-notify traps 12-14 removed
no snmp-server enable traps link-change 12-14
snmp-server community "public" Unrestricted
snmp-server host 15.255.133.236 "public"

To verify FortiNAC is receiving the traps using the Administrative UI, see “Verify Mac Notification Traps How To”.