HOW-TO

CONFIGURE MAC NOTIFICATION TRAPS ON EXTREME SWITCHES

DATE: 11.28.2018

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.

Extreme Switch Setup

Note: The command syntax may be dependent upon the Extreme OS. Refer to product documentation.

1. Enable MAC Tracking traps globally on the switch.
   enable snmp traps fdb mac-tracking

2. Enable MAC Tracking for specific ports (should only include access ports , NOT trunks, port channels, or uplinks).
   configure fdb mac-tracking add ports <PORT-LIST>

3. Display MAC Tracking configuration.
   show fdb mac-tracking configuration

   Example:
   # show fdb mac-tracking configuration
   MAC-Tracking enabled ports: 1:1-10
   SNMP trap notification : Enabled
   MAC address tracking table (0 entries):
   <No entries exist>

4. Remove linkUp and linkDown traps on ports Mac Tracking traps are added.
   disable snmp traps port-up-down ports <PORT-LIST>

5. Display link state traps configuration:

6. Configure the switch to send traps to FortiNAC (trapreceiver).
   configure snmp add trapreceiver [<eth0 ip_address of appliance>] community [<community_name>]

   FortiNAC managing switch using SNMP v3: Include the source IP address of the switch. If there are multiple addresses, use the IP address of the switch's model in Topology. **Note:** the below example may vary based on switch model and firmware.
   configure snmpv3 add target-addr "v1v2cNotifyTAddr1" param "v1v2cNotifyParam1" ipaddress < eth0 ip_address of appliance> transport-port 162 vr "VR-Default" tag-list "defaultNotify" from <switch-ip-addr>

7. Display trap receivers:
   show management

Example (only SNMP section displayed below for brevity):
show management
...

SNMP Traps : Enabled
SNMP v1/v2c TrapReceivers :
Destination Source IP Address Flags Timeout Retries
10.101.0.100 /162 32.1.0.2 2ET - -
...

Configuration Example: Mac Tracking traps configured for ports 1:1-1:10 and sending to FortiNAC IP 10.101.0.20 using community string "public."

enable snmp traps fdb mac-tracking
configure fdb mac-tracking add ports 1:1-1:10
disable snmp traps port-up-down ports 1:1-1:10
configure snmp add trapreceiver 10.101.0.20 community public

Other related commands:

Delete a trap receiver:

configure snmp delete trapreceiver [[<ip_address> | <ipv6_address>] {<port_number>} | all]

Example: Delete trap receiver 10.101.0.100 from the trap receiver list:

configure snmp delete trapreceiver 10.101.0.100

To verify FortiNAC is receiving the traps using the Administrative UI, see KB article Confirming Mac Notification Traps via Administrative UI.

