FortiNAC

Configuring Traps for MAC Notification

Version: 8.x, 9.x

Date: December 27, 2022

Rev: L

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

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

FORTINET KNOWLEDGE BASE
https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase

FORTINET BLOG
http://blog.fortinet.com

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

FORTINET COOKBOOK
http://cookbook.fortinet.com

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

Contents

Overview

The information in this document provides guidance for configuring MAC Notification traps for supported 3rd party devices.

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.

Customers have also found this document helpful:
https://packetfence.org/doc/PacketFence_Network_Devices_Configuration_Guide.html#_about_this_guide

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.

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).

How it Works

MAC Notification traps trigger under the following conditions:
Add - Device generates traffic for the first time
Remove - MAC is removed from the address table. The time it takes for this to occur depends upon how the device is connected.

- Directly connected devices: MAC entry is removed immediately
- Devices behind an IP Phone, non-managed switch or hub: MAC entry must age out of the switch's MAC address table. This is based on the age time configured within the switch (typically minutes).

Change - device whose MAC is already learned on a port moves and connects to another port and generates traffic

Events logged in FortiNAC can be used to verify whether or not MAC Notification traps are being processed.

Each connection point must be configured 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

- FortiNAC supports SNMP versions 1, 2 and 3 for MAC Notification traps. For a list of supported traps by vendor, see FortiNAC SNMP Trap Support in the Document Library.

- Some switches in this document do not support MAC Notification traps. If this capability has been added in newer switch firmware, see KB article Requesting SNMP Trap Support to submit a request for support.

- 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.

- Traps should be configured on the following port types:
  - Access ports (ports for endpoint connections or IP Phones)
  - Ports connecting to Access Points (ensures NAC is notified of an endpoint connection if the AP is replaced with an endpoint device)

- For best performance, do not enable traps on the following:
  - Ports connecting to network infrastructure (e.g. switches, firewalls, controllers)
  - Aggregate ports
  - Any port with a Connection State of "User Defined Uplink" in FortiNAC Topology

  Traps sent from these ports cause unnecessary processing in FortiNAC and will generate events.

- 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 changing the **Ignore MAC Notification Traps for IP Phones** option setting in the Administration UI. For details see section **Network device** of the 8.x or 9.x Administration Guide.

Procedure

General Steps

1. Configure SNMP MAC Notification traps on all access ports (see requirements above).
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 FortiNAC eth0 IP address.
4. Configure MAC address table notifications globally.
5. Configure Context settings in switch for reading Mib-2 information. **Note:** This step only applies to certain devices managed using SNMP v3.

The following pages provide configuration examples for supported switches:

Alcatel
Cisco cat4500e
Cisco 3560
Dell
Extreme
HP
H3C / HPE
Juniper
Ruckus Brocade

Note: Based on switch model or version, some of the commands may vary. It is recommended to review any associated vendor 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 MAC address table notifications globally.
   mac address-table notification change
   mac address-table notification mac-move
   mac address-table notification threshold

   snmp-server enable traps snmp coldstart warmstart
   snmp-server enable traps mac-notification change move threshold

3. Configure to send traps to the IP address of the eth0 on FortiNAC Control Server or Control Server. SNMP Traps are independent of the SNMP Discover protocols. Example: if switch was modeled SNMP v3, traps can be sent with either SNMP v1/2c or v3.

   Option1: Send SNMP v1/2c traps
   snmp-server host <eth0 FNAC IP> <RO or RW community> mac-notification snmp

   Option 2: Send SNMP v3 traps
   snmp-server host <eth0 FNAC IP> traps version 3 <auth or priv> <user name> mac-notification

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.

   snmp-server community public RO
   snmp-server community private RW
   snmp-server enable traps MAC-Notification
   snmp-server host <eth0 FNAC IP> <RO or RW community>

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

Extreme

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. 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.

   Configuration variation 1:
   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>

   Configuration variation 2:
   configure snmpv3 add target-params “v1v2cNotifyParam1" user "snmpv3-username” mp-model snmpv3 sec-model usm sec-level priv

6. 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

H3C / HPE

(H3C 1950 example)

1. 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).
   Note: If target host is defined without specifying traps, all traps are enabled.

   Example (SNMP V3)
   system-view
   snmp-agent sys-info version v3
   snmp-agent sys-info contact <sys-contact>
   snmp-agent sys-info location <sys-location>
   snmp-agent group v3 SNMPV3_Group privacy write-view ViewDefault notify-view ViewDefault
   snmp-agent target-host trap address udp-domain xxx.xxx.xxx.xxx params securityname V3
   snmp-agent usm-user v3 snmpv3usr SNMPV3_Group cipher authentication-mode sha SecretKey*** Comment only**
   snmp-agent trap enable mac-address

   Note:
   - The securityname value is required by the switch in order to enter the command. However, it is not used by FortiNAC when processing traps.
   - If the mac-address option is not available, the following command enables all traps: **snmp-agent trap enable**

   Example (V1/V2)
   system-view
   snmp-agent sys-info version v1 v2c
   snmp-agent community read public
   snmp-agent community write private
   snmp-agent sys-info contact <sys-contact>
   snmp-agent sys-info location <sys-location>
   snmp-agent target-host trap address udp-domain xxx.xxx.xxx.xxx params securityname public v1
   snmp-agent trap enable mac-address

   Note: if the mac-address option is not available, the following command enables all traps: **snmp-agent trap enable**

2. Enable MAC address table notifications globally.
   mac-address information enable

3. Configure SNMP MAC Notification traps and disable link traps on all access ports (do not include uplinks).
   disable snmp trap updown
   mac-address information enable added
   mac-address information enable deleted

HP

SNMP v1/2

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

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 <FortiNAC IP Address> community <community-name>

   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 15.255.133.236 using 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"

SNMP v3

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

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).
   snmpv3 enable
   snmpv3 only
   snmpv3 restricted-access
   snmpv3 group managerauth user "<username>" sec-model ver3
   snmpv3 notify "<name>" tagvalue "<tag value>"
   snmpv3 targetaddress "<target name>" params "<parameter name>" < FortiNAC IP Address> taglist "<tag value>"
   snmpv3 params "<parameter name>" user "<username>" sec-model ver3 message-processing ver3 auth
   snmpv3 user "<username>" auth sha " < Authentication password> "

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
- Sending to FortiNAC Primary IP 15.42.133.236 and Secondary IP 15.42.150.236 (High Availability configuration)

snmp-server enable traps mac-notify trap-interval 2
snmp-server enable traps mac-notify
snmp-server enable traps mac-notify mac-move
mac-notify traps 12-14 learned
mac-notify traps 12-14 removed
no snmp-server enable traps link-change 12-14
snmpv3 enable
snmpv3 only
snmpv3 restricted-access
snmpv3 group managerauth user "nactrapsnmp" sec-model ver3
snmpv3 notify "FortiNAC" tagvalue "FortiNAC_tag"
snmpv3 targetaddress "CT_FortiNAC" params "FortiNAC_params" 15.255.133.236 taglist "FortiNAC_tag"
snmpv3 targetaddress "EG_FortiNAC" params "FortiNAC_params" 15.255.150.236 taglist "FortiNAC_tag"
snmpv3 params "FortiNAC_params" user "nactrapsnmp" sec-model ver3 message-processing ver3 auth
snmpv3 user "nactrapsnmp" auth sha "AUTHENTICATION_PASSWORD"

Juniper

Reference URL:
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/mac-notification.html

Enable MAC Notification with an interval of 5 seconds:
set mac-notification notification-interval 5

To verify settings:
show ethernet-switching mac-notification

To disable MAC Notification on uplink ports
set interface <uplink interface> no-mac-notification

Example
set interface ge-0/0/3 no-mac-notification

Alcatel

As of this writing, MAC Notification traps are not available for Alcatel.

The following syntax is used to set up SNMP with linkUp and linkDown traps for an Alcatel switch. The commands listed below are known to work on the following switches:
Alcatel-Lucent 6250 24 PORT COPPER FE 6.6.2.249.R01
Alcatel-Lucent OS6850-U24X 6.4.3.640.R01
Alcatel-Lucent OS6850-24X 6.4.3.640.R01

Enable link up and link down traps on an entire slot or specific port:
trap <slot> port link enable
trap <slot/port> port link enable

Configure SNMP v1 or SNMPv3:

SNMP v1
user <the_username> read-write all password <the_password> no auth
snmp security no security
snmp community map <snmp_community> user <the_username> enable
snmp station <ip_snmp_server> <the_username> v1 enable

SNMP v3
snmp security authentication all
snmp security privacy all

// Note for this example auth protocol is SHA, encryption protocol is DES. Other options Exist for: MD5, MD5+DES, SHA:
user <the_username> sha+des password <the_password> read-write all

snmp station <ip_snmp_server> <the_username> v3 enable

Ruckus Brocade

Reference:
https://docs.commscope.com/bundle/fastiron-08030-adminguide/page/GUID-04EE9011-98EE-41E2-AA7F-292D4C778A8A.html

SNMP V3

```
device(config)#snmp-server view internet internet included
device(config)#snmp-server view system system included
device(config)#snmp-server community ..... ro
device(config)#snmp-server community ..... rw
device(config)#snmp-server contact isc-operations
device(config)#snmp-server location sdh-pillbox
device(config)#snmp-server host <FortiNAC eth0 ip_address> .....
device(config)#snmp-server group ops v3 priv read internet write system
device(config)#snmp-server group admin v3 priv read internet write internet
device(config)#snmp-server group restricted v3 priv read internet
device(config)#snmp-server user ops ops v3 encrypted auth md5
ab8e9cd6d46e7a270b8c9549d92a069 priv encrypted des 0e1b153303b6188089411447dbc32de
device(config)#snmp-server user admin admin v3 encrypted auth md5
0d8a2123f91bfbd8695fef16a6f4207b priv encrypted des 18e0cf359fce4fcd60df19c2b6515448
device(config)#snmp-server user restricted restricted v3 encrypted auth md5
261fd8f56a3ad51c8bcec1e4609f54dc priv encrypted des d32e66152f89de9b2e0cb17a65595f43
```

Note:

- MAC Change messages are sent by the switch for connections and disconnections.
- Upon disconnect, the trap sent by the switch contains all zero's for the MAC address (00:00:00:00:00:00). If the VLAN in the trap matches the current VLAN on the port, FortiNAC treats it like a link down and updates the port status accordingly.

Dell

Reference:
https://gzhls.at/blob/ldb/9/7/6/6/3c335e115e332a2cad08f62d1642c793b9b6.pdf

As of this writing, MAC Notification traps are not available for Dell. Enable link traps (Note: command may not display in the running configuration).

snmp-server enable traps link
snmp-server community <community name> ro ipaddress <FortiNAC eth0 ip_address>
snmp-server host <FortiNAC eth0 ip_address> <community name>

SNMP V3

```
snmp-server engineid local 800002a203f48e384f616f
no snmp-server enable traps snmp authentication
snmp-server group <group name> v3 priv notify DefaultSuper read DefaultSuper
write DefaultSuper
snmp-server user <username> <groupname> auth-md5 ***** priv-des *****
snmp-server community <community name> ro ipaddress <FortiNAC eth0 ip_address>
snmp-server host <FortiNAC eth0 ip_address> <community name>
no snmp-server enable traps auto-copy-sw
no snmp-server enable traps dot1q
no snmp-server enable traps port-security
no snmp-server enable traps buffers
no snmp-server enable traps cpu threshold
no snmp-server enable traps multiple-users
no snmp-server enable traps spanning-tree
no snmp-server enable traps poe
no snmp-server enable traps vrrp
no snmp-server enable traps acl
exit
```

Validate

Verify FortiNAC updates the database as devices connect to the switch.

1. In the Administration UI, navigate to the Ports view of the switch.
   Version 8.x: **Network Device > Topology**
   Version 9.x: **Network > Inventory**

2. Select the model of the switch to be tested and click the **Ports** tab.
3. Connect the computer to the desired switch port.
4. Verify on the switch the link is up and the computer's MAC address is listed in the switch's MAC address table.
5. After a few moments, the Ports view should update with the computer's MAC address on the expected port. If not, click the refresh button  in the upper right hand corner.

Troubleshooting

Related KB articles

Confirming MAC Notification traps via Administration UI
Mac Change on Uplink events
Confirming Link State traps via Administration UI

Debugging

Use the following KB article to gather the appropriate logs using the debugs below.
Gather logs for debugging and troubleshooting

Note: Debugs disable automatically upon restart of FortiNAC control and management processes.

Function	Syntax	Log File
L2 related activity	`nacdebug -name BridgeManager true`	/bsc/logs/output.master
SNMP activity	`nacdebug -name SnmpV1 true`	/bsc/logs/output.master
Device Interface	`nacdebug -name DeviceInterface true`	/bsc/logs/output.master
Notification Trap debug	`DumpBridgePerformance -enableMacNotifyDebug`	/bsc/logs/output.master
Disable Notification Trap debug (**important:** disabled when not troubleshooting)	`DumpBridgePerformance -disableMacNotifyDebug`	N/A
Disable debug	`nacdebug -name <debug name> false`	N/A