監控Nexus 7000中EIGRP鄰接關係更改的SNMP陷阱

目錄

簡介

本檔案介紹用於監控Nexus 7000中增強型內部閘道路由通訊協定(EIGRP)鄰接關係的變更的簡易網路管理通訊協定(SNMP)陷阱。Nexus僅支援EIGRP-MIB的兩個陷阱（cEigrpAuthFailureEvent和cEigrpRouteStuckInActive），但不支援EIGRP鄰居的SNMP陷阱(cEigrpNbrDownEvent)。
生成SNMP陷阱以監控EIGRP鄰接關係更改的可行解決方法是配置兩個EEM指令碼 — 一個用於Neighbor Up，一個用於Neighbor Down — 基於系統日誌模式觸發。

範例

```
event manager applet EIGRP_TRAP_nbr_dwn
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*down"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Down"
event manager applet EIGRP_TRAP_nbr_up
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*up"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Up"
```

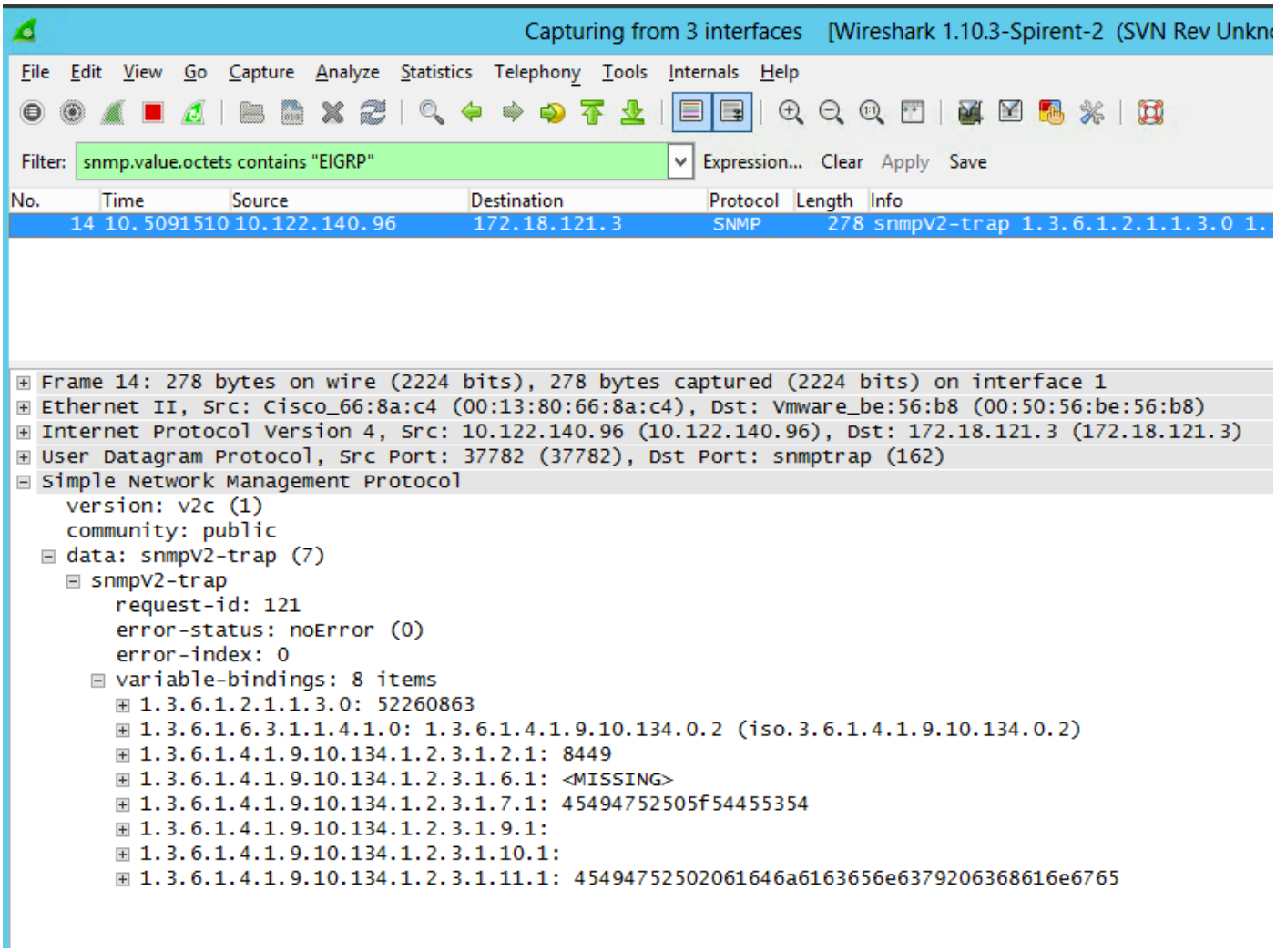
然後您可以通過擺動第3層介面進行測試(可以建立測試交換機虛擬介面(SVI)以驗證是否不中斷連線):

```
2017 Jul 12 15:51:06 N7K-AGG2 %EIGRP-5-NBRCHANGE_DUAL:  eigrp-10 [4049] (default-base) IP-
EIGRP(0) 10: Neighbor 10.10.10.84
(Vlan1064) is down: holding time expired 2017 Jul 12 15:51:10 N7K-AGG2 %EIGRP-5-NBRCHANGE_DUAL:
eigrp-10 [4049] (default-base) IP-EIGRP(0) 10: Neighbor 10.10.10.84
(Vlan1064) is up: new adjacency
```

確認Nexus正確發出這些命令並檢查您的SNMP監控工具 — 輸出可能略有不同，具體取決於使用的工具：

您還可以通過Wireshark捕獲檢查這些SNMP陷阱：

> **附註**：這取決於Wireshark的版本，字串不是人類可讀的文本，而是可以通過「snmp.value」進行過濾。八位元包含「EIGRP」。



您還可以驗證Nexus在通過Ethanalyzer觸發嵌入式事件管理器(EEM)時傳送這些消息。請參閱範例：

```
N7K-A-Admin# ethanalyzer local interface mgmt display-filter snmp limit-c 0

Capturing on mgmt0
2017-07-12 15:43:37.431067 10.122.140.96 -> 172.18.121.3 SNMP 278 snmpV2-trap 1.3.6.1.2.1.1.3.0
1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.1.9.10.134.1.2.3.1.2.1 1.3.6.1.4.1.9.10.134.1.2.3.1.6.1
1.3.6.1.4.1.
9.10.134.1.2.3.1.7.1 1.3.6.1.4.1.9.10.134.1.2.3.1.9.1 1.3.6.1.4.1.9.10.134.1.2.3.1.10.1
1.3.6.1.4.1.9.10.134.1.2.3.1.11.1
```

附註：NX-OS 7.x之前的版本不提供配置**snmp-server enable traps syslog**的選項，這反過來允許您監控整個日誌記錄日誌本身，然後過濾EIGRP消息。此功能在7.x及更新版本中新增。