监控Nexus 7000中EIGRP邻接关系更改的SNMP陷阱

目录

简介

本文档介绍用于监控Nexus 7000中增强型内部网关路 由协议(EIGRP)邻接更改的简单网络管理协议(SNMP)陷阱。Nexus仅支持EIGRP-MIB的两个陷阱cEigrpAuthFailureEvent和cEigrpRouteStuckInActive，但不支持EIGRP邻居的SNMP陷阱up/down(cEigrpNbrDownEvent)。生成SNMP陷阱以监控EIGRP邻接关系更改的可行解决方法是配置两个EEM脚本（一个用于邻居启动，一个用于邻居关闭），根据系统日志模式触发。

示例

```
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"
```

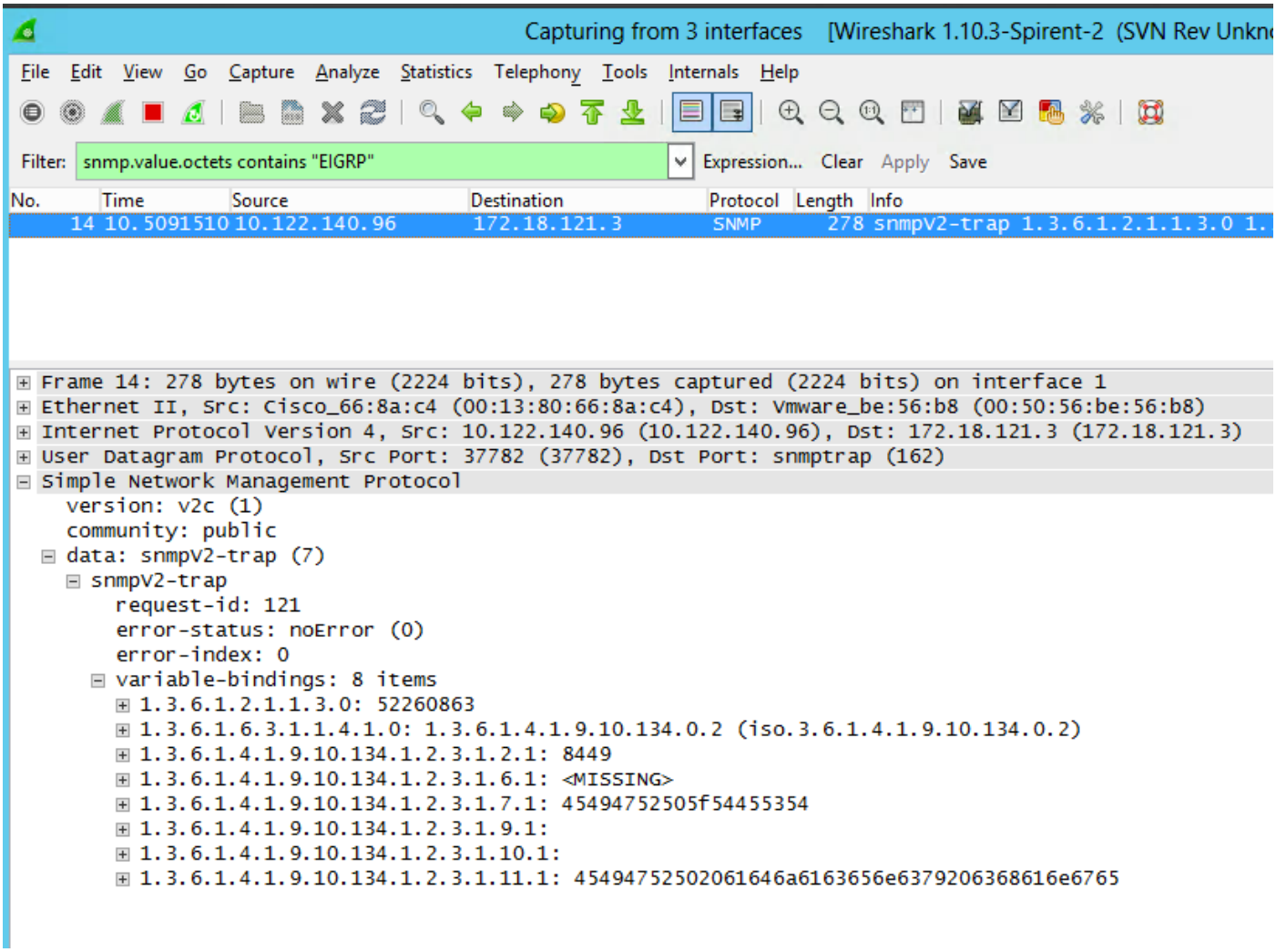
然后，可以通过摆动第3层接口进行测试(可以创建测试交 换机虚拟接口(SVI)以验证是否不中断连接):

```
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
```

确认Nexus正确发送这些信息并检查您的SNMP监控工具 — 输出可能稍有不同，具体取决于使用的工具：

您还可以通过Wireshark捕获查看以下SNMP陷阱：

> **注意**：它取决于Wireshark的版本，该字符串不会以人类可读的文本形式显示，但可以通过“snmp.value.octets包含“EIGRP”进行过滤。



您还可以验证Nexus是否在嵌入式事件管理器(EEM)触发时通过Ethanalyzer发送这些消息。有关“等待”状态的解释，请参阅示例：

```
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
```

注意：在NX-OS 7.x之前，我们不提供配置**snmp-server enable traps syslog**的选项，这反过来又允许您监控整个日志记录日志本身，然后过滤EIGRP消息。此功能已在7.x及更高版本中添加。