如何在思科基于Unix的统一通信平台中抓包

目录

软件版本

目前常见的思科统一通信平台产品，例如CUCM(6.0以上版本),UCCX(8.0以上版本)，CUPS（6.0以上版本）等，都是基于Unix平台的应用服务器

技术领域

Cisco 统一通信平台

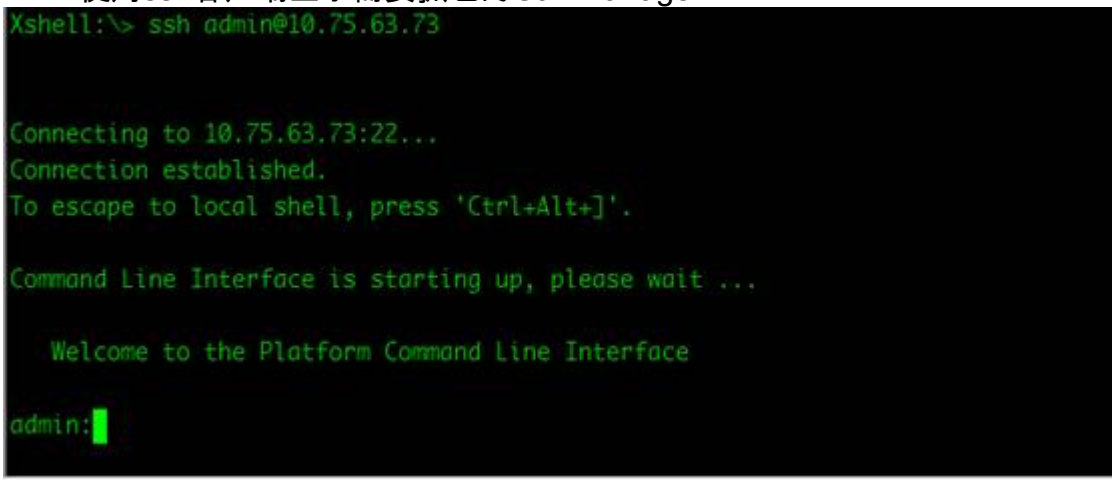
问题描述

在处理CUCM等统一通信平台的问题时，遇到网络问题导致的行为不正常，比如电话在莫名其妙的情况下失去了与CUCM的连接而注册到了SRST。类似的情况经常出现在跨广域网使用VoIP，而这种情况无法从Call Manager或者电话的配置以及trace判断出问题所在，这个时候往往就需要在这类的应用服务器中抓包。

抓包方法

这里以Call Manager 8.6版本为例

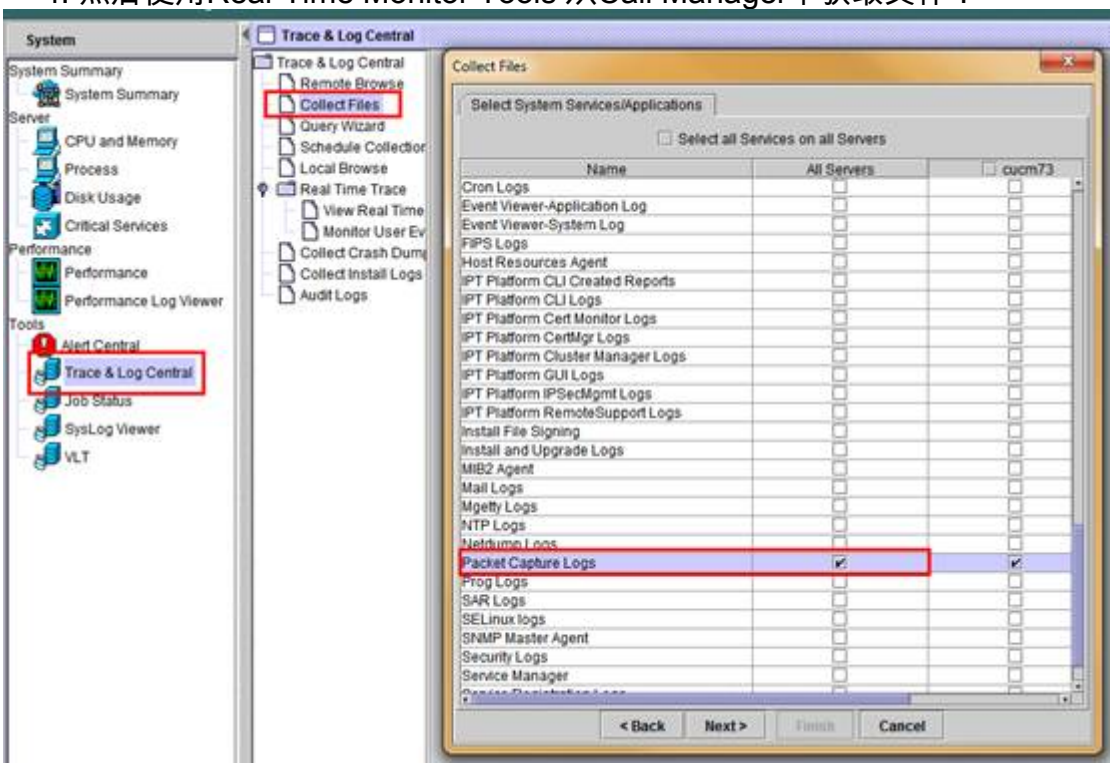
1. 使用ssh客户端登录需要抓包的Call Manage：



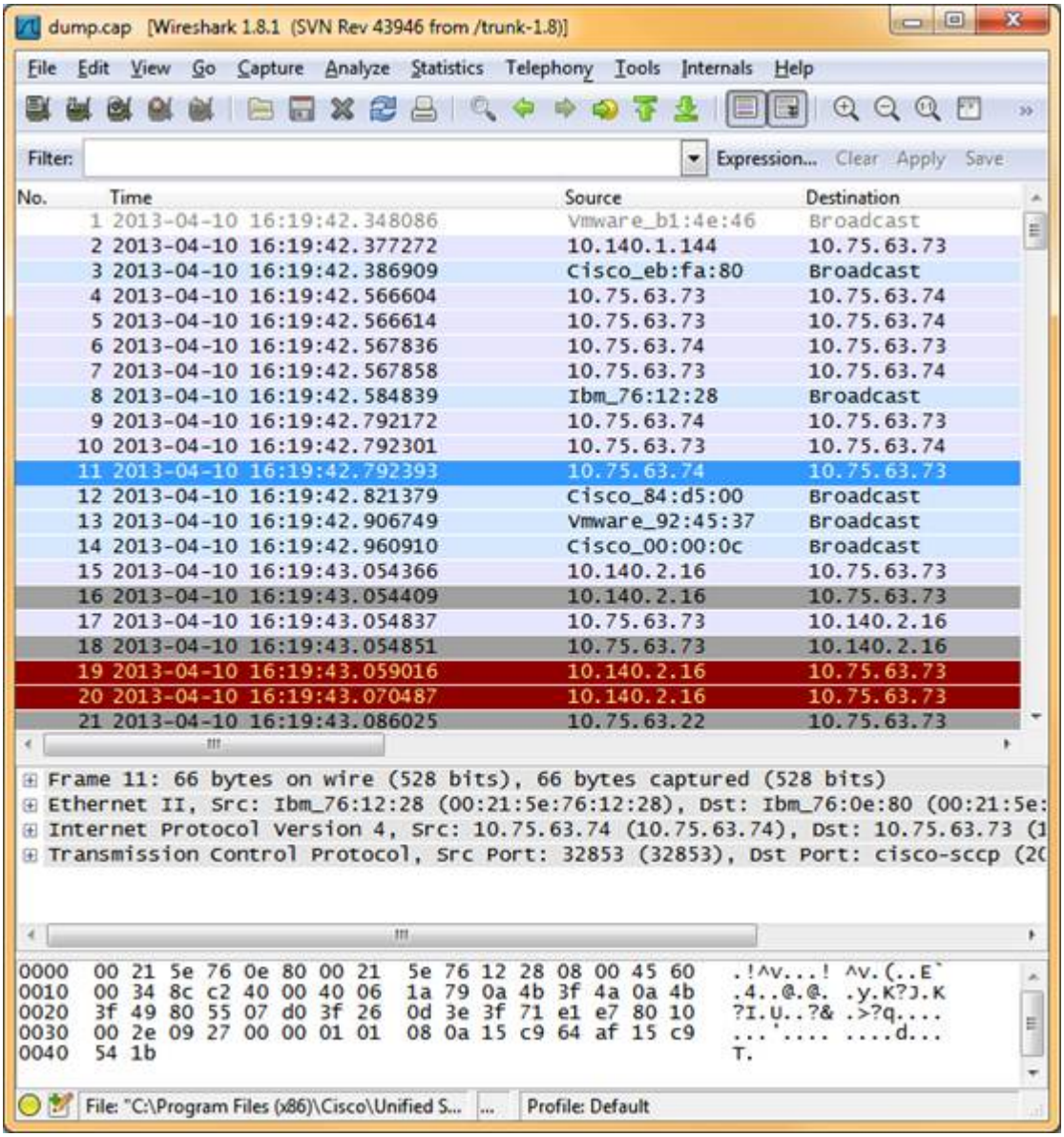
2. 使用命令utils network capture file [file name] [count]来启动抓包，这里的file name是存储抓包的文件名，count是总共抓取的包的数量：

```
admin:utils network capture file dump 10000
Warning: existing dump.cap was renamed dump_7.cap
Executing command with options:
 size=128              count=1000              interface=eth0
 src=                  dest=                   port=
 ip=

Control-C pressed

admin:
```

3. 停止抓包的方式有两种，一种是使用Ctrl+C，另外一种则是等待抓取包的数量达到设定的上限自动停止。
4. 然后使用Real-Time Monitor Tools 从Call Manager中获取文件：



5. 获取的文件是pcap文件，可以直接使用wireshark等工具打开查看：



关于抓包的一点说明：
Cisco的统一通信平台在整合之后，都是基于Unix，抓包实际使用的工具其实就是tcpdump

引用

1. Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 8.6(1)
2. Cisco Unified Real-Time Monitoring Tool Administration Guide Version 8.6(1)
3. Tcpdump