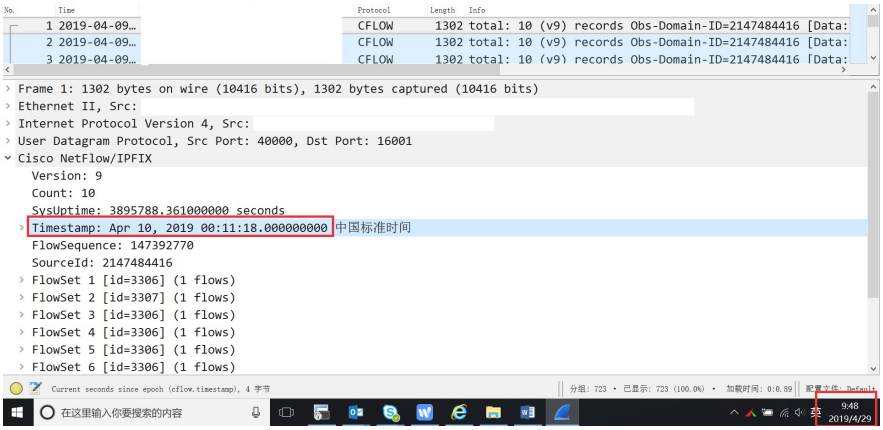
CR16008-X netstream报文时间戳异常问题经验案例

NetStream　郭昊　2019-04-29 发表

组网及说明

网管通过netstream监测CR16K-X接口流量

问题描述



网管显示流量大小正确，但netstream报文携带的时间戳比实际时间快8小时。例如下图，wireshark显示的时间戳是4月10日00:11:18，抓包PC的时间是4月9日16:11:18。

过程分析

该问题实际上与设备配置的时区、抓包电脑的时区有关系。

查看现网设备配置，是手动配置时钟，且没有加时区。

#

clock protocol none

#

<XXX>dis time-range all

Current time is 16:13:06 4/9/2019 Tuesday

设备发送netstream报文给服务器时，所写的时间戳是0时区时间。网管服务器接受到这个报文后，再根据服务器本地时间所在时区，加减对应小时数，最后显示成wireshark抓包上的时间。

对现网设备来说，手动配置时钟没有加东八区，这样相当于0时区时间为16:11:18 4/9/2019。设备发给服务器时也是带着这个时间戳。之后网管根据自己所在的东八区，再加8小时，就成了截图显示的4月10号这个结果。

解决方法

可以调整一下设备时钟，改成标准时间+东八区。例如现在东八区时间是17:05 2019/04/09，对应设备配置就是，

[H3C]clock timezone bj add 8

[H3C]quit

<H3C>clock datetime 17:05:00 2019/04/09

这样设备本地时间为

<H3C>dis clock

17:05:01 bj Tue 04/09/2019

Time Zone : bj add 08:00:00

这样设备发出去的netstream报文应该携带的时间戳是09:05:00 2019/04/09，网管再加8小时，得出正确时间。