某金融局点S7506E不停报802.1X认证成功日志问题处理经验案例

张玺 2016-01-26 发表

某金融局点使用S7506E设备做802.1X认证，认证功能正常，业务正常。但客户发现，设备的logbuffer里存在大量802.1X认证日志，如下所示：

%Dec 24 10:41:17:522 2015 JS1_MN_AS_31 PORTSEC/6/PORTSEC_DOT1X_LOGIN_SUCC: -Slot=4; -IfName=GigabitEthernet4/0/22-MACAddr=C0:3F:D5:30:D0:91-VlanId=206-UserName=SSA(C0-3F-D5-30-D0-91); The user passed 802.1X authentication and got online successfully.

%Dec 24 10:41:17:621 2015 JS1_MN_AS_31 PORTSEC/6/PORTSEC_DOT1X_LOGIN_SUCC: -Slot=4; -IfName=GigabitEthernet4/0/12-MACAddr=C0:3F:D5:30:CE:00-VlanId=206-UserName=SSA(C0-3F-D5-30-CE-00); The user passed 802.1X authentication and got online successfully.

%Dec 24 10:41:17:631 2015 JS1_MN_AS_31 PORTSEC/6/PORTSEC_DOT1X_LOGIN_SUCC: -Slot=4; -IfName=GigabitEthernet4/0/41-MACAddr=C0:3F:D5:30:2C:C0-VlanId=206-UserName=SSA(C0-3F-D5-30-2C-C0); The user passed 802.1X authentication and got online successfully.

大量的802.1X认证日志发送给客户的日志服务器，导致客户的日志服务器空间不足，将更重要的其他日志覆盖掉了。客户希望我们彻底定位该问题。

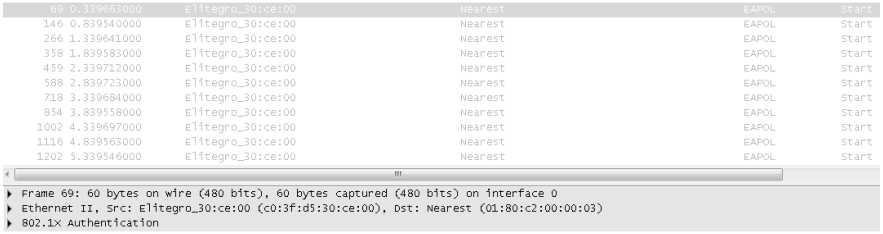
设备在终端802.1X认证成功后，产生上述日志是正常的。但频繁的产生大量的该日志就不正常了。经过统计，对于每个终端，设备每0.5秒就会产生一条802.1X认证成功日志：

%Dec 24 10:41:17:621 2015 JS1_MN_AS_31 PORTSEC/6/PORTSEC_DOT1X_LOGIN_SUCC: -Slot=4; -IfName=GigabitEthernet4/0/12-MACAddr=C0:3F:D5:30:CE:00-VlanId=206-UserName=SSA(C0-3F-D5-30-CE-00); The user passed 802.1X authentication and got online successfully.

%Dec 24 10:41:18:120 2015 JS1_MN_AS_31 PORTSEC/6/PORTSEC_DOT1X_LOGIN_SUCC: -Slot=4; -IfName=GigabitEthernet4/0/12-MACAddr=C0:3F:D5:30:CE:00-VlanId=206-UserName=SSA(C0-3F-D5-30-CE-00); The user passed 802.1X authentication and got online successfully.

我们进一步了解客户终端的情况，得知客户终端使用了趋势、赛门铁克等软件，这些软件会做802.1X认证。

那么，我们就在MAC地址为C0：3F：D5：30：CE：00的终端上开启抓包，观察一下终端是否有异常报文。抓包如下图所示，可以看到，终端每隔0.5秒就会发送一个802.1X EAPOL报文给设备。



联系交换机研发确认，S7506E在终端认证成功后，如果再次收到该终端发来的eapol-start报文，就会再次打印802.1X 认证成功日志信息。

从上述分析可见，导致该问题的原因就是终端在认证成功后，仍然频繁发送eapol-start报文，导致设备产生大量日志。

如需解决该问题，根本情况是联系终端侧，了解为何会频繁发送eapol-start报文（这显然是不正常的）。

如果终端侧无法定位，可以通过设备的信息中心功能，使该日志不显示在logbuffer，且不发送给loghost日志主机。

无