S10508 SSH不能正常登陆设备

SSH　zhiliao_my0Dx6　2022-02-28 发表

组网及说明

核心（聚合组1/1/0/1和2/1/0/1)----（聚合组1xge1/0/47和48)汇聚交换机（1/0/6）----接入交换机
设备都配置了SSH，汇聚交换机在对应端口放通了VLAN，核心和接入设备位于同一网段

问题描述

问题是核心不能SSH到接入设备，但是能ping通接入设备，汇聚可以SSH到接入设备，接入设备可以SSH到核心。

核心在SSH登录接入设备是提示网络不可达。

核心SSH接入时，在汇聚设备进行流统测试，可以看到核心设备发出的包，接入没有回，但是其他设备可以SSH接入设备

过程分析

1、看了下核心上的debug信息，刚刚获取本地initialization并发给对端，但是对端接入却没有收到，导致接入设备校验失败，并报版本不一致

核心上debug，本地的initialization都正常：

*Dec 30 16:08:51:289 2021 ZKGY_CORE_S10508 SSHC/7/EVENT: -MDC=1; PAM initialization result: 0.

*Dec 30 16:08:51:290 2021 ZKGY_CORE_S10508 SSHC/7/EVENT: -MDC=1; PAM: Sent a start-accounting request. Result: 4.

*Dec 30 16:08:51:295 2021 ZKGY_CORE_S10508 SSHC/7/EVENT: -MDC=1; PAM: Resources released.

*Dec 30 16:08:51:295 2021 ZKGY_CORE_S10508 SSHC/7/EVENT: -MDC=1; Remote protocol version 2.0, remote software version Comware-7.1.070

*Dec 30 16:08:51:295 2021 ZKGY_CORE_S10508 SSHC/7/EVENT: -MDC=1; Enabling compatibility mode for protocol 2.0

*Dec 30 16:08:51:297 2021 ZKGY_CORE_S10508 SSHC/7/EVENT: -MDC=1; Get self version string Comware-7.1.070

%Dec 30 16:08:51:297 2021 ZKGY_CORE_S10508 SSHC/6/SSHC_DISCONNECT: -MDC=1; The SSH client was disconnected from the SSH server because the network was not available.

接入设备上：

*Jan 27 00:59:11:004 2013 NW-S5130-1F-5#-01 SSHS/7/EVENT: Start new child 119088.

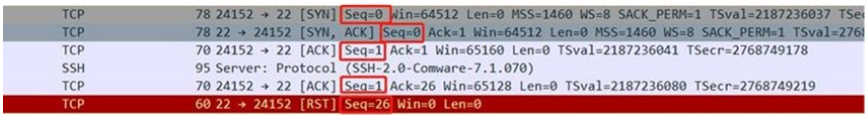
*Jan 27 00:59:11:029 2013 NW-S5130-1F-5#-01 SSHS/7/EVENT: Connection from X.X.X.X port 27313

*Jan 27 00:59:11:035 2013 NW-S5130-1F-5#-01 SSHS/7/ERROR: Did not receive identification string from X.X.X.X.

%Jan 27 00:59:11:036 2013 NW-S5130-1F-5#-01 SSHS/6/SSHS_VERSION_MISMATCH: SSH client X.X.X.X failed to log in because of version mismatch.

2、在设备进行抓包，查看抓包信息

根据设备CPU上debug rxtx打印出来解析的报文，两台设备一开始的tcp连接建立是正常的。而正常TCP连接的报文序号seq都是连续递增的，但是现场核心设备和接入设备建立tcp连接后，会突然收到一个序号seq=26的rst报文（reset，会重置TCP连接），导致tcp连接中断，ssh登陆异常



解决方法

现场反馈核心上有一台网络准入设备，准入设备占用了镜像资源，现场将镜像删掉之后SSH就通了
大概率是流量被镜像到准入设备了，准入设备会回应交换机发出的ssh报文，远程查看时发现会有序列号不同的tcp rst ack，导致连接直接中断
现网都是本地端口镜像，镜像的目的口g1/8/0/17也有极少量的入方向流量，可以确认下是否现场的准入设备对ssh交互产生干扰：

```
#
interface Ten-GigabitEthernet1/1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 300
mirroring-group 2 mirroring-port both
mirroring-group 3 mirroring-port both
port link-aggregation group 1
#
interface GigabitEthernet1/8/0/17
port link-mode bridge
description ===to_zhunru(zhu)_ETH1===
mirroring-group 2 monitor-port
#
GigabitEthernet1/8/0/17
Current state: UP
Line protocol state: UP
Last 300 seconds input: 0 packets/sec 89 bytes/sec 0%
Last 300 seconds output: 6051 packets/sec 1957563 bytes/sec 2%
```

基于以上以及现场取消镜像后故障恢复，建议确认下准入设备的机制，避免收到tcp rst ack断开tcp连接。