S5130S-EI终端802.1x认证成功后很快下线经验案例

802.1X 曹圣琪 2023-08-31 发表

问题描述

现场在S5130S-EI设备上配置了802.1x认证，认证成功后终端很快被动下线

过程分析

1、确认现场配置的认证方式：

现场使用的是电脑自带的客户端软件而非Inode客户端，检查配置的认证方式为EAP中继方式，且服务器支持客户端采用的EAP认证方法。

报文交互方式	优势	局限性
EAP中继	· 支持多种EAP认证方法 · 设备端的配置和处理流程简单	一般来说需要RADIUS服务器支持EAP-Message和Message-Authenticator属性，以及客户端采用的EAP认证方法
EAP终结	对RADIUS服务器无特殊要求，支持PAP认证和CHAP认证即可	· 仅能支持MD5-Challenge类型的EAP认证以及iNode 802.1X客户端发起的“用户名+密码”方式的EAP认证 · 设备端处理相对复杂

2、Debug查看下线过程：

从debug来看，认证成功后连续发送两次EAP Request报文且未收到回应后导致的下线，缺省情况下在线用户握手功能是开启的，且设备向接入用户发送认证请求报文的最大次数缺省情况是2次（可通过dot1x retry命令修改），与现场现象匹配。握手功能存在以下限制，尤其是第3点需要与INODE客户端配合使用，现场未使用客户端，建议通过undo dot1x handshake命令将握手功能关闭再进行测试。

配置限制和指导

• 部分802.1X客户端不支持与设备进行握手报文的交互，因此建议在这种情况下，关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。

• 在线用户握手功能处于开启状态时，安全握手功能才会生效。

• 在线用户握手安全功能仅能在iNode客户端和iMC服务器配合使用的组网环境中生效。 • 只有当802.1X客户端需要收到在线握手成功报文时，才需要开启端口发送在线握手成功报文功能。

*Jan 30 05:17:40:586 2014 BGL-2F-RIGHT DOT1X/7/EVENT: Sending EAP packet: Identifier=17, type=1.

*Jan 30 05:17:40:586 2014 BGL-2F-RIGHT DOT1X/7/PACKET:

Transmitted a packet on interface GigabitEthernet1/0/3.

Destination Mac Address=28d2-4463-32dd

Source Mac Address=78aa-8204-edec

VLAN ID=123

Mac Frame Type=888e

Protocol Version ID=1

Packet Type=0

Packet Length=5

-----Packet Body-----

Code=1

Identifier=11

Length=1280

*Jan 30 05:17:46:314 2014 BGL-2F-RIGHT DOT1X/7/EVENT: EAP-Request/Identity packet multicasting timed out on GigabitEthernet1/0/3.

*Jan 30 05:17:46:314 2014 BGL-2F-RIGHT DOT1X/7/EVENT: Multicasted EAP-Request/Identity packets on interface GigabitEthernet1/0/3.

*Jan 30 05:17:55:586 2014 BGL-2F-RIGHT DOT1X/7/EVENT: Sending EAP packet: Identifier=17, type=1.

*Jan 30 05:17:55:586 2014 BGL-2F-RIGHT DOT1X/7/PACKET:

Transmitted a packet on interface GigabitEthernet1/0/3.

Destination Mac Address=28d2-4463-32dd

Source Mac Address=78aa-8204-edec

VLAN ID=123

Mac Frame Type=888e

Protocol Version ID=1

Packet Type=0

Packet Length=5

-----Packet Body-----

Code=1

Identifier=11

Length=1280

%Jan 30 05:17:59:987 2014 BGL-2F-RIGHT STP/6/STP_NOTIFIED_TC: Instance 0's port Ten-GigabitEthernet1/0/25 was notified a topology change.

%Jan 30 05:18:02:281 2014 BGL-2F-RIGHT STP/6/STP_NOTIFIED_TC: Instance 0's port Ten-GigabitEthernet1/0/25 was notified a topology change.

%Jan 30 05:18:05:224 2014 BGL-2F-RIGHT STP/6/STP_NOTIFIED_TC: Instance 0's port Ten-Giga

bitEthernet1/0/25 was notified a topology change.

%Jan 30 05:18:08:238 2014 BGL-2F-RIGHT STP/6/STP_NOTIFIED_TC: Instance 0's port Ten-Giga bitEthernet1/0/25 was notified a topology change.

解决方法

%Jan 30 05:18:10:586 2014 BGL-2F-RIGHT DOT1X/7/PACKET:

Transmitted a packet on interface GigabitEthernet1/0/3.

现场在接口视图下通过undo dot1x handshake命令将握手功能关闭后业务恢复正常。

Destination Mac Address=28d2-4463-32dd

Source Mac Address=78aa-8204-edec

VLAN ID=123

Mac Frame Type=888e

Protocol Version ID=1

Packet Type=0

Packet Length=4

-----Packet Body-----

Code=4

Identifier=11

Length=1024

*Jan 30 05:18:10:586 2014 BGL-2F-RIGHT DOT1X/7/EVENT: PAE is in Disconnect state: UserMAC =28d2-4463-32dd, VLANID=1, Interface=GigabitEthernet1/0/3.

*Jan 30 05:18:10:587 2014 BGL-2F-RIGHT DOT1X/7/EVENT: Interface GigabitEthernet1/0/3 receive d Set the port authorization status to unauthorized event.