S5130S-HI series switch wired 802.1X using windows self-client authentication abnormality experience cases

Switches 蒋笑添 2020-09-27 Published

Network Topology

null

Problem Description

We use S5130S-HI series switch, combined with a third-party RADIUS server, for 802.1X certification of the terminal computer, the computer is directly connected to the switch for certification, but found t hat the computer can't access the Internet normally after the certification, the computer is using the w indows client to authenticate.

Process Analysis

First of all, we check the 802.1X configuration on the device side, we can see that the device is in EA P relay mode, but there is no obvious problem in the configuration, and the switch can communicate with the RADIUS server by pinging each other. Collect debugging dot1x all and debugging radius all i nformation, check the debug information, and observe if the server's problem causes the authentication failure.

#

dot1x

dot1x authentication-method eap

#

radius scheme sensetimeradius

primary authentication 10.151.1.248

primary accounting 10.151.1.248

key authentication cipher c3$VlUaBXvVhtV5Nna57g9popb7m+8SQ4MhU4Kxp8hnsQ==.

key accounting cipher c3$DhTobwxPpFz1WP1ZPkMr5nrNt0XxWRUD64W0P+edAQ===

user-name-format without-domain

#

domain sensetimeradius

authentication lan-access radius-scheme sensetimeradius

authorization lan-access radius-scheme sensetimeradius

accounting lan-access radius-scheme sensetimeradius

#

interface GigabitEthernet1/0/6

stp edged-port

dot1x

dot1x mandatory-domain sensetimeradius

dot1x port-method portbased

#

Looking at the debug message, we can see that the switch has sent EAP messages and has received a response from the terminal.

*Aug 19 16:58:09:617 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF DOT1X/7/EVENT: Sending EAP packet: Identifier=2, type=1.

*Aug 19 16:58:09:618 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF DOT1X/7/PACKET:

Transmitted a packet on interface GigabitEthernet1/0/6.

Destination Mac Address=c8f7-503f-f1be

Source Mac Address=743a-208a-f02f

VLAN ID=1

Mac Frame Type=888e

Protocol Version ID=1

Packet Type=0

Packet Length=5.

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

Code=1

Identifier=2

Length=5.

*The following table shows the number of packets that have been received on the interface GigabitEthernet:

Received a packet on interface GigabitEthernet1/0/6.

Destination Mac Address=0180-c200-0003

Source Mac Address=c8f7-503f-f1be

Mac Frame Type=888e

Protocol Version ID=1

Packet Type=0

Packet Length=15.

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

Code=2

Identifier=2

Length=15.

Review the RADIUS and switch interaction process and find that the switch successfully send authentication request messages to the RADIUS server.

*Aug 19 16:58:17:173 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/PACKET:

User-Name="zhangyibin"

NAS-Identifier="ASCNHZTR-AS-S5130S-29FA-02-IRF"

EAP-Message=0x0202000f017a68616e67796962696e

Message -Authenticator=0x00000000000000000000000000000000000000000000000000

Framed-MTU=1450

Framed-Protocol=PPP

Called-Station-

NAS-Port-Type=Ethernet

H3c-Ip-Host-Addr="0.0.0.0 c8:f7:50:3f:f1:be"

Calling-Station-

H3C-NAS-Port-Name="GigabitEthernet1/0/6"

NAS-Port=16801793

NAS-Port-

H3c-AVPair="nas:ifindex=6"

Acct-Session-

Service-Type=Framed-User

NAS-IP-Address=10.156.1.5

H3c-Product-

H3c-Nas-Startup-Timestamp=1597820936

*Aug 19 16:58:17:175 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF DOT1X/7/EVENT: AAA processe d authentication request: Result=Processing, UserMAC=c8f7-503f-f1be, VLANID=1, Interface=GigabitEthernet1/0/6.

*Aug 19 16:58:17:175 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Sent request packet successfully.

Then devices have successfully received response packets from the RADIUS server.

*Aug 19 16:58:17:177 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Sent request packet and create request context RADIUS/7/EVENT: Added request context to global table successf ully.

*Aug 19 16:58:17:177 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Added reques t context to global table successfully.

*Aug 19 16:58:17:177 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Processing A AA request data.

*Aug 19 16:58:17:211 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Reply Socket Fd recieved EPOLLIN event.

*Aug 19 16:58:17:212 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Received repl y packet succuessfully.

*Aug 19 16:58:17:212 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Found request context, dstIP: 10.151.1.248, dstPort: 1812 , VPN instance: --(public), socketFd: 77, pktID: 127.

*Aug 19 16:58:17:212 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: The reply packet is valid.

*Aug 19 16:58:17:213 2020 ASCNHZTR-AS-S5130S-29FA-02-IRF RADIUS/7/EVENT: Decoded reply packet successfully.

So far, we found no obvious the error message in debug information, combined with the customer On-site test feedback, the use of inode client can be normal authentication, and the terminal has been able to access Internet normally, so we can conclude that is not configuration problems, but the windows client caused.

Solution

When the device is configured with 802.1X authentication, the online user handshake feature is enabled by default. When the online user handshake feature is enabled on the device, the device periodically (at intervals set by the command dot1x timer handshake-period) sends handshake-request messages (EAP-Request/ Identity) to periodically check the user's online status. If the device does not receive an answer message (EAP-Response/Identity) from the client multiple times in a row (set with the dot1x retry command), the user will be taken offline.

After undoing the dot1x handshake , the feedback from the customer on site is that the windows client can be authenticated normally and the customer does not go offline rapidly. This is because some 802.1X clients do not support handshake message interaction with the device, so it is recommended to disable the online user handshake in this case to avoid forcing the online user offline for not responding to the handshake message.