S5130S-28P-EI The AccessVLANID & the AuthorizationVLANID is not the same in the radius massage.

Switches 蒋笑添 2020-08-09 Published

Network Topology

Null

Problem Description

About dot.1x dynamic vlan assignment.

User auth and dynamic vlan assignment are all ok. Except only the log sent to the radius is not correct. So dynamic vlan assignment operation is correct but the vlan info sent to the radius is wrong.

Example:
User authenticated+ dynamic vlan 160 assigned + accounting info sent to radius says vlan 150 assigned.
Log has to say vlan 160 not vlan 150...

So all operations are correct, but only log information sent to the radius is wrong, it always informs vlan 2 assigned which is port default vlan(pvid).

Process Analysis

We can clearly see the log about the authorization vlan from Radius server on the device as following:
%Jan 1 01:52:28:313 2013 H3C DOT1X/6/DOT1X_LOGIN_SUCC: -IfName=GigabitEthernet1/0/2-MACAddr=28d2-4491-4e77-**AccessVLANID=150-AuthorizatiOnVLANID=160**-Username=MAYCYBER\h3c1; User passed 802.1X authentication and came online.

And according to the packets capture from the device to the server:

```
AVP: t=NAS-Port-Id(87) l=36 val=slot=1;subslot=0;port=2;vlanid=150
```

We know the device feedback Radius with the accessVlanID which is the vlan of access clients before authentication, while without the AuthorizationVlanID.

So even the server authorize the vlan itself, it can only receive the access vlan anyway. The requirements from customer is receiving the **AuthorizationVLANID**, which not support at the current software version.

Solution

Modified feature of version Release 6317
Information included in RADIUS accounting request packets
Feature change description:
As from this version, the device supports including the User-VLAN-ID attribute in RADIUS accounting request packets sent to the RADIUS server. This attribute is used to carry authorization VLAN information for 802.1X and MAC authentication users. The modification ensures that the logs output by the RADIUS server can include user authorization VLAN information.
If the RADIUS server assigns a VLAN ID or VLAN name as the authorization VLAN to a user, the device includes the server-assigned authorization VLAN in the User-VLAN-ID attribute.
If the RADIUS server assigns a group of VLANs in the authorization VLAN information to a user, the device includes a VLAN in the User-VLAN-ID attribute as described in Table 1.
Table 1 Including a VLAN in the User-VLAN-ID attribute of RADIUS accounting packets

VLAN information	VLAN included in the User-VLAN-ID attribute
VLANs by IDs VLANs by names VLAN group name Combination of VLAN IDs and VLAN names	• If the device has selected an authorization VLAN when it starts accounting for the user, it includes the selected VLAN in the User-VLAN-ID attribute. The VLAN will be included in start-accounting, real-time accounting, and stop-accounting request packets. • If the device has not selected an authorization VLAN when it starts accounting for the user, it includes the user's initial VLAN in the User-VLAN-ID attribute in start-accounting request packets. When sending real-time accounting or stop-accounting request packets, the device will include the authorization VLAN in the User-VLAN-ID attribute.
VLAN IDs with suffixes	The device includes the untagged authorization VLAN in the User-VLAN-ID attribute in RADIUS accounting request packets. If no untagged authorization VLAN is available, the device includes the user's initial VLAN in the User-VLAN-ID attribute in RADIUS accounting request packets.