

知 S5820V2-54QS-GE 结合第三方radius服务器做MAC地址认证需要携带NAS-PORT-ID属性字段

MAC地址认证 蔡洋 2019-04-28 发表

问题描述

设备版本: V7 Alpha7571

客户需求NAS设备发送radius报文中携带NAS-PORT-ID属性字段, 客户第三方服务器没有此字段, 如下没有显示NAS-PORT-ID字段

Ready to process requests.

```
rad_recv: Access-Request packet from host 172.0.254.20 port 1024, id=106, length=137
User-Name = "c0-56-e3-dc-5b-e5"
User-Password = "c0-56-e3-dc-5b-e5"
NAS-IP-Address = 172.0.254.20
NAS-Identifier = "4F_WW_ZXJF_S5120"
NAS-Port = 16797908
NAS-Port-Type = Ethernet
Service-Type = Framed-User
Framed-Protocol = PPP
Calling-Station-Id = "c056-e3dc-5be5"
# Executing section authorize from file /etc/freeradius/hlcsites/default
+group authorize {
++[preprocess] = ok
++[chap] = noop
++[mschap] = noop
[realm_suffix] No '$' in User-Name = "c0-56-e3-dc-5b-e5", looking up realm NULL
[realm_suffix] Found realm "NULL"
```

怎么配置端口属性格式
比如: 1/0/3 这样的

解决方法

radius方案视图下配置87号属性字段值实现

```
radius scheme rad1
primary authentication 192.168.0.204 key cipher $c$3$45LLnxRZHAi3JZ6ArUr3itQaWJcD1M4=
primary accounting 192.168.0.204 key cipher $c$3$vm9K9t5vUUmKpJmwNPCLDHnH4kFw/nc=
timer response-timeout 1
user-name-format without-domain
nas-ip 192.168.0.130
attribute 87 format custom slot / subslot / port
radius scheme rad2
user-name-format without-domain
nas-ip 192.168.0.130
```

attribute 87 format命令用来配置RADIUS Attribute 87的格式。

undo attribute 87 format命令用来恢复缺省情况。

【命令】

```
attribute 87 format { custom { c-vid [ delimiter ] | interface-type [ delimiter ] | port [ delimiter ] | s-vid [ delimiter ] | slot [ delimiter ] | string string [ delimiter ] | subslot [ delimiter ] | vxlan-id [ delimiter ] } * | vendor vendor-id }
```

undo attribute 87 format

【缺省情况】

未配置RADIUS Attribute 87的格式, 直接采用接入模块定义的RADIUS Attribute 87格式, 具体为:

- 对于Portal: SlotID00ifNOVlanID, 其中SlotID占用2个字符、00为固定字符、ifNO占用3个字符、VlanID占用9个字符;
- 对于IPoE、PPP、802.1X、MAC地址认证: slot=xx;subslot=xx;port=xx;vlanid=xx;vlanid2=xx;
- 对于Login: 不填充任何内容。

【视图】

RADIUS方案视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

custom: 表示采用自定义的属性格式。

c-vid: 用户报文的内层VLAN ID。

interface-type: 用户接入的接口类型。

port: 用户接入的端口号。

s-vid: 用户报文的外层VLAN ID。

slot: 用户接入单板所在槽位号。

string string: 自定义的属性字符串, 其中string为1~63个字符的字符串, 区分大小写。

subslot: 用户接入单板所在子槽位号。

vxlan-id: 用户所属的VXLAN ID。

delimiter: 本属性字段与下一个属性字段之间的分隔符, 为除问号之外的任意可输入字符。若不指定该参数, 则表示不使用分隔符。

vendor vendor-id: 表示采用指定设备厂商的属性格式, 其中vendor-id厂商标识号码, 取值范围目前仅为9 (Cisco) 和2636 (Juniper) 。

【使用指导】

RADIUS Attribute 87为NAS-Port-ID属性。不同的RADIUS服务器对NAS-Port-ID属性的解析格式要求不同, 为了保证RADIUS报文的正常交互, 设备发送给服务器的NAS-Port-ID属性的格式必须与服务器的要求保持一致。

可通过本命令修改设备发送的RADIUS NAS-Port-ID属性的格式, 具体情况如下:

- 如果采用指定设备厂商的属性格式, 则NAS-Port-ID属性内容完全按照厂商要求填充。
- 如果采用自定义属性格式, 则NAS-Port-ID属性中可携带哪些属性字段、各字段之间使用的分隔符以及各字段的排列顺序, 由配置决定。其中, 各字段的填充先后顺序, 与本命令中对应关键字的配置顺序一致。

配置自定义属性格式时, 请综合考虑用户的实际组网环境以及设备形态, 避免指定无效的属性字段, 例如非QinQ组网中, 不需要指定报文外层VLAN ID。

【举例】

在RADIUS方案rad中, 配置使用Cisco的RADIUS Attribute 87格式。

```
<Sysname> system-view
```

```
[Sysname] radius scheme rad
```

```
[Sysname-radius-rad] attribute 87 format vendor 9
```

在RADIUS方案rad2中, 配置使用自定义的RADIUS Attribute 87格式, 属性中依次携带用户报文的内层VLAN ID和接口类型, 属性分隔符为; 。

```
<Sysname> system-view
```

```
[Sysname] radius scheme rad2
```

```
[Sysname-radius-rad2] attribute 87 format custom c-vid ; interface-type ;
```