S5552P-EI-D-H3 交换机配置802.1X向Radius服务器请求未携带用户域问题

802.1X Radius 刘嘉炜 2019-03-29 发表

组网及说明

无

问题描述

现场测试802.1X结合Radius认证，测试发现只有客户端登录时用户名@域名后才能认证成功，在设备上将Radius方案中设置为with-domain并将默认域设置为huawei2.com时设备上送Radius报文并不会在用户名后面@域。

过程分析

现场配置：

interface GigabitEthernet1/0/1
port access vlan 201
stp edged-port
dot1x
dot1x mandatory-domain huawei2.com
#
dot1x authentication-method eap
#
radius scheme cams　　\\默认情况下为with-domain，因此配置中没有显示
primary authentication 10.0.15.10
primary accounting 10.0.15.10
secondary authentication 10.0.15.9
secondary accounting 10.0.15.9
accounting-on enable
key authentication cipher c3$/mnMmz+oz9cEBQUlBZ/gOpuGjte+zmE=
key accounting cipher c3$K8kd8frY06gd89O7o6mv8rxw2k4AtTA=
timer realtime-accounting 24
#
domain huawei2.com
authentication lan-access radius-scheme cams
authorization lan-access radius-scheme cams
accounting lan-access radius-scheme cams
#
domain default enable huawei2.com

客户端带域认证成功时debug信息：

*Jan 2 00:08:06:604 2013 S5552-XS33a-14.33 RADIUS/7/PACKET:
User-Name="\006\007OWI1Hh8OMSJ7SBdgJVx7K0zNclo= 28199@huawei2.com"
NAS-Identifier="S5552-XS33a-14.33"
EAP-Message=

客户端不带域认证失败时debug信息

*Jan 2 03:42:30:842 2013 S5552-XS33a-14.33 RADIUS/7/PACKET:
User-Name="\006\007OWA8SksHMyJ7Sh40cVV5KzpjQx0= 28199"
NAS-Identifier="S5552-XS33a-14.33"EAP-

正常情况下如果Radius方案中配置with-domain，那么在客户端认证时应该带上设备默认域，但是这台设备却不带导致认证失败。

查找对应命令手册：

1.4.58 user-name-format (RADIUS scheme view)

【使用指导】

接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为ISP域名，设备就是通过该域名来决定将用户归于哪个ISP域的。但是，有些较早期的RADIUS服务器不能接受携带有ISP域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给RADIUS服务器。因此，设备提供此命令以指定发送给RADIUS服务器的用户名是否携带有ISP域名。

如果指定某个RADIUS方案不允许用户名中携带有ISP域名，那么请不要在两个或两个以上的ISP域中同时设置使用该RADIUS方案。否则，会出现虽然实际用户不同（在不同的ISP域中），但RADIUS服务器认为用户相同（因为传送到它的用户名相同）的错误。

在802.1X用户采用EAP认证方式的情况下，RADIUS方案中配置的user-name-format命令无效，客户端传送给RADIUS服务器的用户名与用户输入的用户名保持一致。

若接入用户为需要漫游的无线用户，建议接入设备上将发送给RADIUS服务器的用户名格式配置为keep-original类型，否则可能导致这类用户认证失败。

解决方法

设置中删除dot1x authentication-method eap使用dot1x authentication-method chap/pap认证时客户端就不需要携带域名。