H3C S5500-SI和iNode 配合做Radius认证异常下线问题处理实例

赵国卫 2008-06-23 发表

H3C S5500-SI和iNode 配合做Radius认证异常下线问题处理实例

一、 组网:

无

二、 问题描述:

H3C S5500-SI交换机在和iNode配合做Radius认证时，发现客户端经常性出现异常下线，在iNode客户端出现如下提示信息:

2008-04-10 13:30:39 连接网络...
2008-04-10 13:30:39 开始进行身份验证... [nb-gw]
2008-04-10 13:30:39 正在验证用户密码...
2008-04-10 13:30:40 您的身份验证成功
2008-04-10 20:18:39 连接中断
2008-04-10 20:18:40 收到服务器下线请求
2008-04-10 20:18:43 连接已断开
2008-04-10 20:30:43 连接网络...
2008-04-10 20:30:56 开始进行身份验证... [nb-gw]
2008-04-10 20:30:57 正在验证用户密码...
2008-04-10 20:30:57 您的身份验证成功
2008-04-11 10:51:52 连接中断
2008-04-11 10:51:53 收到服务器下线请求
2008-04-11 10:51:53 连接已断开
2008-04-11 12:10:59 连接网络...

从iNode信息的输出可以看到，客户端每个几个小时就出现下线的情况，且时间并不是固定的，而且从全网来看，下线的客户端也呈现随机性，并无规律可循。

三、 过程分析:

对于此类问题，首先要弄清楚客户端下线的原因，在交换机上开启debug radius packet来查看Radius报文的交互过程，在打印出来的debug日志中，发现如下信息:

[1 User-name] [7] [nb-gw]
[32 NAS-Identifier] [5] [H3C]
[5 NAS-Port] [6] [16871425]
[61 NAS-Port-Type] [6] [15]
[31 Caller-ID] [16] [303031622D666361622D64633833]
[40 Acct-Status-Type] [6] [2]
*Apr 29 21:32:04:938 2008 H3C RDS/7/DEBUG:
[45 Acct-Authentic] [6] [1]
[44 Acct-Session-Id] [16] [10803291801119]
[4 NAS-IP-Address] [6] [192.168.1.2]
[55 Event-Timestamp] [6] [1209504724]
[25 Class] [32]
[638D07610000013700001C0A801FA01C8A75434FA49EE0000000000000299]
[46 Acct-Session-Time] [6] [12647]
*Apr 29 21:32:05:442 2008 H3C RDS/7/DEBUG:
[41 Acct-Delay-Time] [6] [0]
[42 Acct-Input-Octets] [6] [3640034185]
[47 Acct-Input-Packets] [6] [4218463]
[43 Acct-Output-Octets] [6] [2863649036]
[48 Acct-Output-Packets] [6] [3900283]
[52 Acct_Input_Gigawords] [6] [0]
*Apr 29 21:32:05:865 2008 H3C RDS/7/DEBUG:
[53 Acct_Output_Gigawords] [6] [0]
[49 Terminate-Cause] [6] [2]

从信息中可以看到，用户的下线原因为2，根据Radius字典中的定义可以查到2对应的下线原因为Lost-Carrier。 这通常是因为网络拥塞导致交换机和客户端之间握手报文丢导致。默认情况下，交换机以15s为间隔周期向客户端发送握手请求报文，如果连续两次没有收到客户端响应报文，就会将用户置为下线状态。

四、 解决方法:

首先建议排查网络内是否存在攻击，导致网络内发生拥塞情况，也可以通过调整握手参数来处理此类问题，可以在交换机上做如下配置来调整握手参数:

dot1x timer handshake-period 60

> dot1x retry 10
> 上述参数将以60s为周期发送握手请求，连续10次没有收到客户端握手响应报文，才会将客户端下线。