H3C S5800交换机配合Windows XP SP3自带802.1X客户端做802.1X认证,通过后很快掉线

杨逢君 2009-12-28 发表

H3C S5800交换机配合Windows XP SP3的802.1X客户端认证，用户认证通过后很快掉线

一、 组网：

在某项目售前测试中，H3C S5800交换机作为接入层交换机，直接连接用户PC。

用户使用Windows XP自带802.1X客户端，RADIUS认证服务器为Windows Server 2003 IAS，认证方法为MD5-Chanllenge（该问题其实跟认证方法无关）。

H3C S5800交换机使能802.1X认证并透传EAP，相关802.1X认证配置均为缺省，即：

1）端口接入控制方式为macbased；

2）使能802.1X组播触发，时间间隔为30s；

3）使能802.1X握手，时间间隔为15s，最大重传次数为2；

4）关闭802.1X重认证。

二、 问题描述：

使用Windows XP SP3的用户可以通过802.1X认证，但上线后不到2分钟即掉线；而使用Windows XP SP2的用户可以始终在线。

三、 过程分析：

3.1 背景知识介绍：

1) 对于802.1X认证，IEEE曾于2001年和2004年发布两个正式版本，分别称之为802.1X-2001和802.1X-2004，目前仍处于继续修订状态；

2）针对在线用户的802.1X握手功能是H3C私有机制，具体为交换机周期性向在线用户发送EAP-Request/Identity报文，期待客户端回应EAP-Response/Identity报文，缺省情况下如果连续两次发送握手却没有收到回应，即认为该用户已离线，并发送EAP-Failure而结束802.1X认证；

3）IEEE 802.1X-2001和802.1X-2004两个版本均没有明确规定802.1X握手机制，但IEEE 802.1X-2001状态机描述了客户端在认证通过后收到EAP-Request/Identity如何进一步处理，而IEEE 802.1X-2004状态机则没有明确区分EAP-Request/Identity和其它类型EAP-Request的不同处理；

4）802.1X-2004引入了客户端后台状态机，并在某些状态机描述上与IEEE 802.1X-2001有重大变化，涉及本案例部分在下文分析中会有介绍；

5）Microsoft Windows产品对802.1X的支持从XP SP3起发生重大变化，具体为：

对于Windows 2000 SP3/SP4，XP及SP1/SP2，Server 2003及SP1/SP2产品，有线连接共享无线连接的802.1X模块，其服务为Wireless Zero Configuration，缺省设置为自动/已启动，相关配置保存在Registry中，基本遵循IEEE 802.1X-2001，但首次不能主动发送EAPoL-Start报文以发起802.1X认证；

而从Windows XP SP3起，包括Vista，Server 2008和Windows 7产品，有线连接的802.1X认证脱离于无线连接的802.1X模块，其独立服务为Wired AutoConfig，缺省设置为手动/已停止，相关配置保存在XML Profile中，基本遵循IEEE 802.1X-2004，可以主动发送EAPoL-Start报文以发起802.1X认证；

6）Microsoft Windows 802.1X认证已知问题ID303597：网络连接的属性中，必须选中“连接后在通知区域显示图标（W）”，否则始终不弹出“单击这儿以输入连接网络的用户名和密码”的通知图标。

3.2 案例详细分析：

3.2.1 Windows XP SP2自带802.1X客户端认证

Windows XP SP2自带802.1X客户端基本遵循IEEE 802.1X-2001，先来看看802.1X-2001客户端状态机，如下图所示：

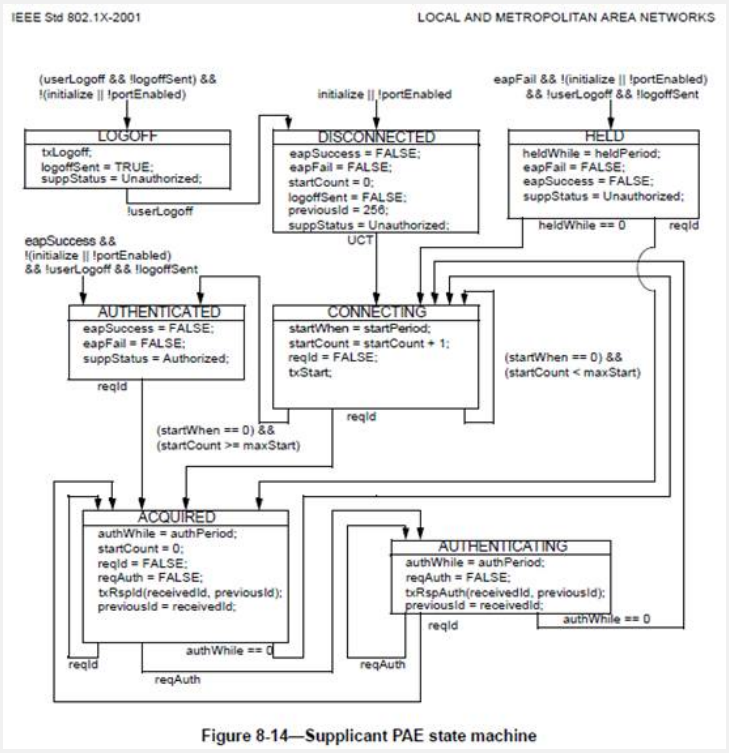
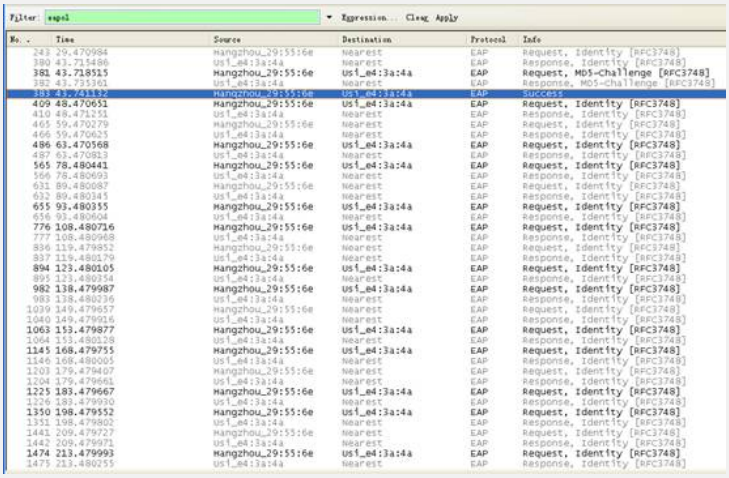


Figure 8-14—Supplicant PAE state machine

客户端通过802.1X认证后处于Authenticated状态，这时如收到EAP-Request/Identity，即转入Acquired状态。

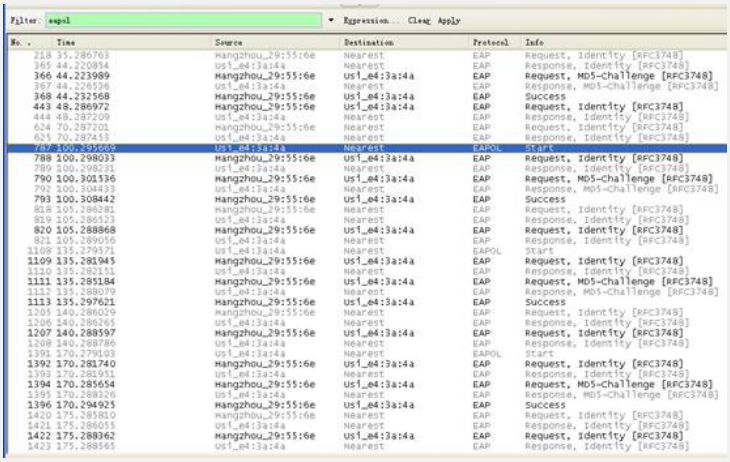
而在Acquired状态时，客户端即发送EAP-Response/Identity，并启动authWhile定时器（缺省为30s）以等待接收EAP-Request。其间如收到其它EAP-Request如EAP-Request/MD5-Challenge，则转入Authenticating状态；如仍收到EAP-Request/Identity，则回EAP-Response/Identity，并重置authWhile定时器。如果authWhile定时器超时，则转入Connecting状态。

Case 1：交换机802.1X默认配置-30s组播触发，15s握手：



客户端抓包如上图所示：XP SP2 802.1X客户端认证通过后，收到EAP-Request/Identity的时间间隔小于等于15s，即在authWhile定时器（30s）之内，按802.1X-2001描述，客户端由Authenticated状态转入并始终处在Acquired状态，即状态机变化为Authenticated->Acquired。对应网络连接的状态表现为“已连接上”，客户端可以正常通讯。

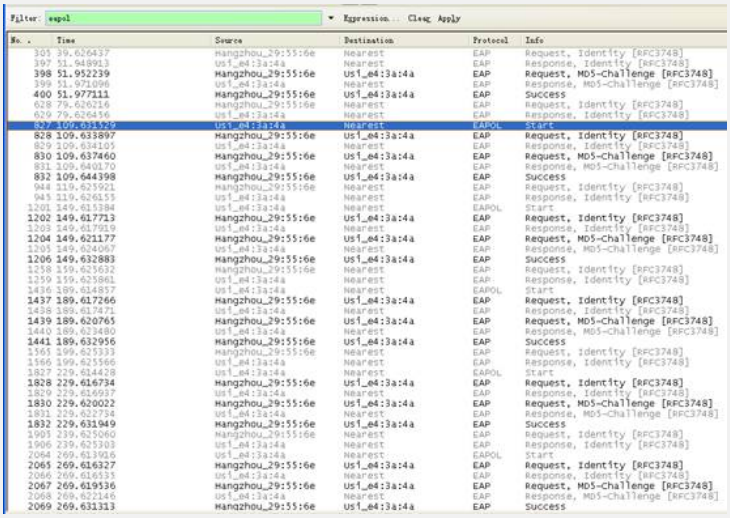
Case 2：交换机802.1X配置-35s组播触发，60s握手：



客户端抓包如上图所示：XP SP2 802.1X客户端认证通过后，5秒之内收到握手报文EAP-Request/Identity，按802.1X-2001描述，这时客户端由Authenticated状态转入Acquired状态，后来又收到组播触发报文EAP-Request/Identity，按交换机配置下一个EAP-Request/Identity无论是握手报文还是组播触发报文，都将30s之后，即时间间隔大于authWhile定时器（30s），按802.1X-2001描述，当authWhile定时器超时后客户端由Acquired状态转入Connecting状态，这时客户端主动发送EAPoL-Start发起类似802.1X重认证，结果又通过认证，如此反复。即状态机变化为Authenticated->Acquired->Connecting->Acquired ->Authenticating->Authenticated->Acquired……。对应网络连接的状态表现为“已连接上”->“尝试验证身份”->“已连接上”……，客户端可以正常通讯。

为更容易更明显观察，特配置交换机以取消握手，40s组播触发，见Case 3抓包。

Case 3：换机802.1X配置-40s组播触发，取消握手：



综上，Windows XP SP2自带802.1X客户端基本遵循IEEE 802.1X-2001，认证通过后始终能正常响应任意时间间隔的802.1X握手和周期性组播触发报文。

3.2.2 Windows XP SP3自带802.1X客户端认证

Windows XP SP3自带802.1X客户端基本遵循IEEE 802.1X-2004，先来看看802.1X-2004客户端状态机，如下两个图所示：

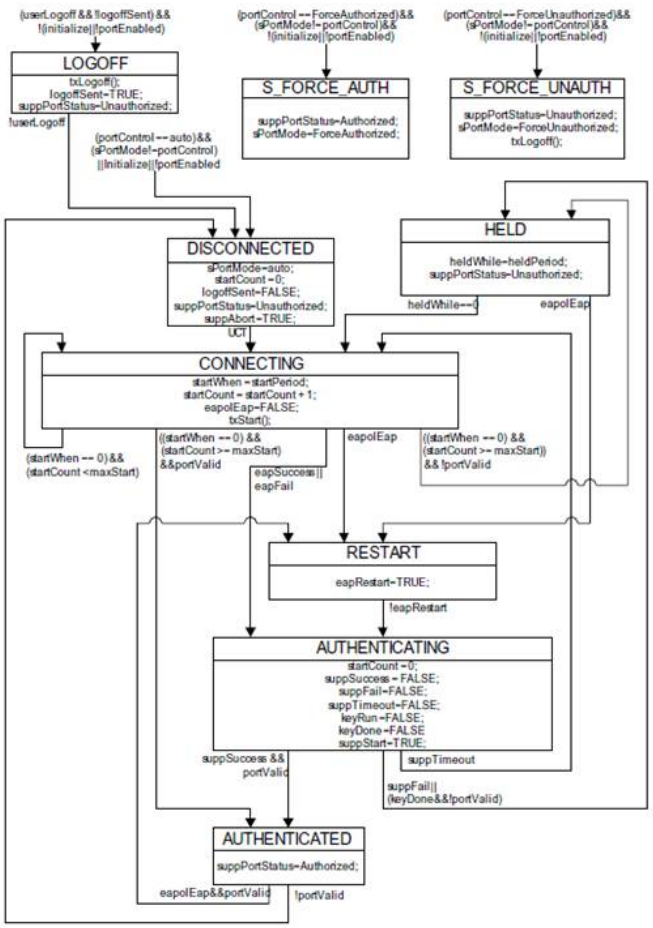


Figure 8-17—Supplicant PAE state machine

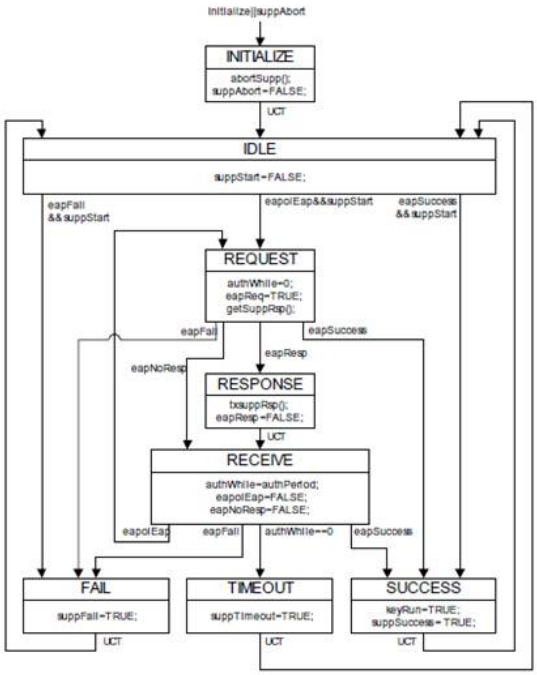


Figure 8-18—Supplicant Backend state machine

请注意！与IEEE 802.1X-2001客户端状态机相比，表面上看802.1X-2004客户端状态机只是将Acquired状态换成Restart状态。

其实不然，在IEEE 802.1X-2001中，上层协议EAP版本为RFC 2284，只考虑到PAP/CHAP/EAP MD5-Challenge/EAP OTP/EAP GTC，而这些认证方法都以EAP-Request/Identity开始，且802.1X认证实体PAE与EAP工作界面划分不是非常清晰，客户端PAE也因此没有划出后台处理模块。

而在IEEE 802.1X-2004中，上层协议EAP版本为RFC 3748，已考虑到其它EAP认证

方法，如EAP TLS等，并不都以EAP Request/Identity开始，故不再专门描述EAP-Request/Identity的处理，统一为EAP Request处理。且802.1X认证实体PAE与EAP工作界面划分非常清晰，由此客户端PAE也划出专门的后台处理模块。于是Restart状态萎缩为瞬态，主要用于PAE与EAP之间的状态同步，而Authenticating状态也是名同实异，该状态调用客户端后台处理模块具体处理认证事务并接受认证结果反馈（Success，Fail或Timeout）。

特别提到的是：客户端后台处理状态机中虽有authWhile定时器（缺省也是30s），但没有专门区分EAP-Request/Identity的处理。

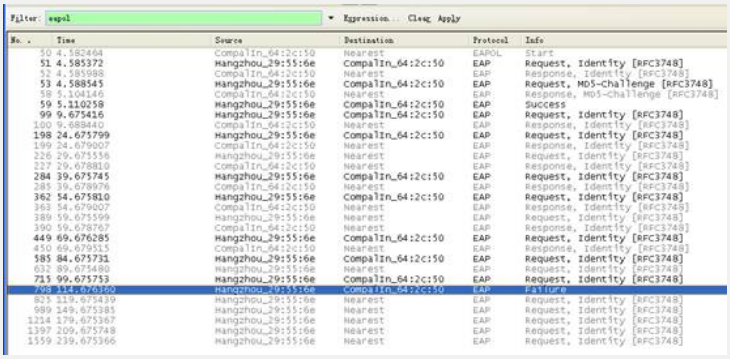
经过大量测试，可以推断Windows XP SP3的802.1X客户端在后台处理时有两个定时器，这里简单称之为T1和T2。

T1：含义同authWhile定时器，用于等待接收来自交换机（准确的俗语为Authenticator）的任何EAP Request，但其初始值不同于协议建议，约为18s。该定时器老化后报Timeout，客户端由Authenticating状态转入Connecting，发送EAPoL-Start以发起新一轮认证，类似802.1X重认证；

T2：按EAP认证方法的一轮处理流程，首次收到一个EAP Request，回EAP Response后，启动该定时器以等待下一个不同的EAP Request，其初始值约为60s。该定时器老化后报Fail，这时按照协议规定客户端应由Authenticating状态转入Held状态，不过Windows XP SP3的802.1X客户端这时报“身份验证失败”而彻底停止响应。

详见下面测试抓包：

Case 1：交换机802.1X默认配置-30s组播触发，15s握手：

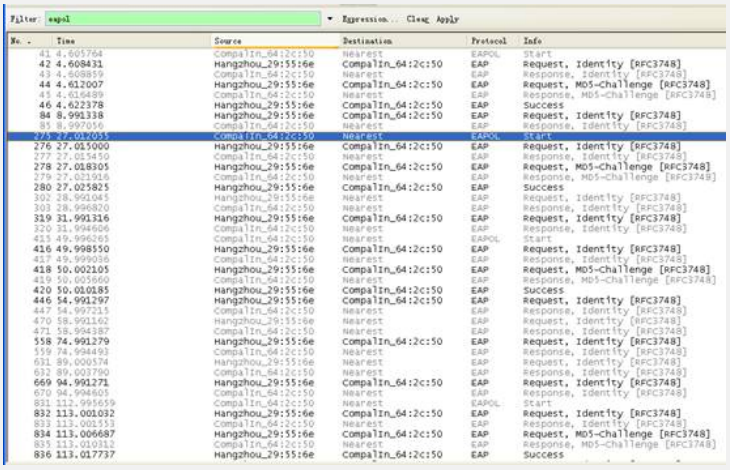


No.	Time	Source	Destination	Protocol	Info
50	4.583464	Compalin_64:2c:50	Nearest	EAPOL	Start
51	4.585372	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
52	4.585988	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
53	4.588545	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, MD5-Challenge [RFC3748]
58	5.104146	Compalin_64:2c:50	Nearest	EAP	Response, MD5-Challenge [RFC3748]
59	5.110258	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Success
99	9.675416	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
100	9.688440	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
198	24.675799	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
199	24.679607	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
226	29.675556	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]
227	29.678810	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
284	39.675745	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
285	39.678976	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
362	54.675810	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
363	54.679007	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
389	59.675599	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]
390	59.678767	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
449	69.676285	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
450	69.679515	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
585	84.675731	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
632	89.675490	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]
715	99.675753	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
798	114.676360	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Failure
835	119.675439	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]
989	149.675385	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]
1214	179.675367	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]
1397	209.675748	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]
1559	239.675366	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]

客户端抓包如上图所示：XP SP3 802.1X客户端认证通过后，5秒之内收到握手报文EAP-Request/Identity，按802.1X-2004描述，这时客户端由Authenticated状态转入Restart状态，随即进入Authenticating状态。随后收到EAP-Request/Identity的时间间隔小于等于15s，即在T1定时器（18s）之内，但客户端因只是收到EAP-Request/Identity，没有后续EAP-Request如EAP-Request/MD5-Challenge而停在Authenticating状态直至T2定时器（60s）超时进入Held状态。客户端状态机变化为Authenticated->Restart->Authenticating->Held。对应网络连接的状态表现为“已连接上”->“尝试验证身份”->“身份验证失败”。而后交换机连续两次发送握手却没有收到回应，即认为该用户已离线，并发送EAP-Failure而结束802.1X认证，这时客户端正常通讯失败！

用户在线时间为T2+3*握手时间间隔=60+3*15=105s

Case 2：交换机802.1X配置-30s组播触发，20s握手：

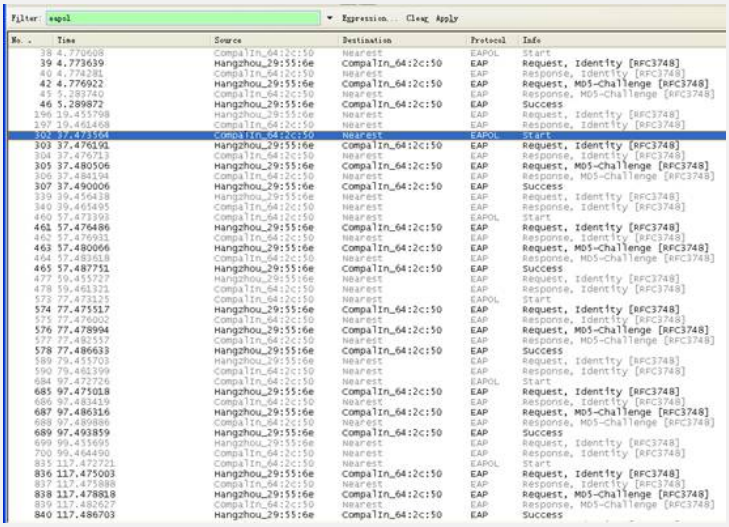


No.	Time	Source	Destination	Protocol	Info
41	4.605764	Compalin_64:2c:50	Nearest	EAPOL	Start
42	4.608431	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
43	4.608859	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
44	4.612007	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, MD5-Challenge [RFC3748]
45	4.616489	Compalin_64:2c:50	Nearest	EAP	Response, MD5-Challenge [RFC3748]
46	4.622378	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Success
84	8.991338	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
85	8.997056	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
275	27.012055	Compalin_64:2c:50	Nearest	EAPOL	Start
276	27.015000	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
277	27.015459	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
278	27.018305	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, MD5-Challenge [RFC3748]
279	27.021916	Compalin_64:2c:50	Nearest	EAP	Response, MD5-Challenge [RFC3748]
280	27.025825	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Success
302	28.991045	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]
303	28.996820	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
319	31.991316	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
320	31.994606	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
413	49.996265	Compalin_64:2c:50	Nearest	EAPOL	Start
416	49.998550	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
417	49.999036	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
418	50.002105	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, MD5-Challenge [RFC3748]
419	50.005660	Compalin_64:2c:50	Nearest	EAP	Response, MD5-Challenge [RFC3748]
420	50.010185	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Success
446	54.991297	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
447	54.997215	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
470	58.991162	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]
471	58.994387	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
558	74.991279	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
559	74.994493	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
631	89.000574	Hangzhou_29:55:6e	Nearest	EAP	Request, Identity [RFC3748]
632	89.003790	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
669	94.991271	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
670	94.994603	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
831	112.995659	Compalin_64:2c:50	Nearest	EAPOL	Start
832	113.001032	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, Identity [RFC3748]
833	113.001553	Compalin_64:2c:50	Nearest	EAP	Response, Identity [RFC3748]
834	113.006687	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Request, MD5-Challenge [RFC3748]
835	113.010312	Compalin_64:2c:50	Nearest	EAP	Response, MD5-Challenge [RFC3748]
836	113.017737	Hangzhou_29:55:6e	Compalin_64:2c:50	EAP	Success

客户端抓包如上图所示：XP SP3 802.1X客户端认证通过后，5秒之内收到握手报文EAP-Request/Identity，按802.1X-2004描述，这时客户端由Authenticated状态转入Restart状态，随即进入Authenticating状态。而后等待EAP-Request的时间间隔大于T1定时器（18s），导致T1超时而转入Connecting状态，这时客户端主动发送EAPoL-Start发起类似802.1X重认证，结果又通过认证，如此反复。即状态机变化为Authenticated-

>Restart->Authenticating ->Connecting->Restart->Authenticating->Authenticated->Restart->Authenticating……。对应网络连接的状态表现为“已连接上”->“尝试验证身份”->“已连接上”……，客户端可以正常通讯。
为更容易更明显观察，特配置交换机以取消握手，20s组播触发，见Case 3抓包。

Case 3：换机802.1X配置-20s组播触发，取消握手：



综上，Windows XP SP3自带802.1X客户端基本遵循IEEE 802.1X-2004，但因802.1X-2004没有专门区分EAP-Request/Identity的处理且又只定义一个authWhile定时器。于是Windows XP SP3自带802.1X客户端实现中定义两个定时器，见上文中T1和T2描述。如果交换机发送802.1X握手报文的时间间隔小于T1，则必然导致Windows XP SP3自带802.1X客户端在Authenticating状态因T2超时而报“身份验证失败”而停止响应包括802.1X握手的一切802.1X报文，最终交换机发送EAP-Failure而结束802.1X认证，客户端正常通讯失败！

四、 解决方法：

理解上述Windows XP SP2和SP3各自802.1X客户端的不同工作机制后，问题则迎刃而解：

H3C S5800交换机从版本CMW5.20-R1108起，802.1X模块增加对于未知MAC的单播触发，命令为以太网端口视图下配置：**dot1x unicast-trigger**

注意！该单播触发命令和组播触发各自独立，同一端口下可以共存。

于是解决方案如下：

1）如果不愿区分Windows XP SP2和SP3两类用户，可以在交换机上配置802.1X单播触发并取消组播触发，取消握手或握手时间间隔在18s以上；

2）如果交换机不是S5800，且最新版本尚不支持802.1X单播触发，则对于Windows XP SP3类用户，因其可以主动发送EAPoL-Start报文，可以在交换机相应端口下取消组播触发，取消握手或握手时间间隔在18s以上；

3）如果上述交换机端口不易区分Windows XP SP2和SP3类用户，则可以考虑在交换机上配置端口接入控制方式为portbased，这样该端口用户通过认证后，不再发送组播触发报文，同时配置取消握手或握手时间间隔在18s以上。