如何使用 ES 网络通二代检测 802.1x 安全认证过程及进行故障诊断

网络的接入控制对网络管理者来说是非常重要的。网络管理员和网络用户关心网络访问权限和安全性。网络管理员希望确保请求访问网络的客户端确实是其本身——是已授权用户而非冒名顶替的用户。类似的，网络用户希望确保当无线笔记本电脑连接到网络时，他确实连接到了自己的网络——而不是由黑客匆匆建成，用于收集用户信息的假冒网络。

目前 ES 网络通二代支持对有线和无线网络的 802.1x 安全认证检测。

802.1x 协议是标准化的一个符合 IEEE 802 协议集的局域网接入控制协议，其全称为基于端口的访问控制协议。它能够在利用 IEEE 802 局域网优势的基础上提供一种对连接到局域网的用户进行认证和授权的手段，达到了接受合法用户接入，保护网络安全的目的。

802.1x 协议与 LAN 是无缝融合的。802.1x 利用了交换 LAN 架构的物理特性，实现了 LAN 端口上的设备认证。在认证过程中，LAN 端口要么充当认证者，要么扮演请求者。在作为认证者时，LAN 端口在需要用户通过该端口接入相应的服务之前，首先进行认证，如若认证失败则不允许接入；在作为请求者时，LAN 端口则负责向认证服务器提交接入服务申请。基于端口的 MAC 锁定只允许信任的 MAC 地址向网络中发送数据。来自任何“不信任”的设备的数据流会被自动丢弃，从而确保最大限度的安全性。

在 802.1x 协议中，只有具备了以下三个元素才能够完成基于端口的访问控制的用户认证和授权。

1.客户端。一般安装在用户的工作站上，当用户有上网需求时，激活客户端程序，输入必要的用户名和口令，客户端程序将会送出连接请求。

2.认证系统。在以太网系统中认证交换机，其主要作用是完成用户认证信息的上传、下达工作，并根据认证的结果打开或关闭端口。

3.认证服务器。通过检验客户端发送来的身份标识（用户名和口令）来判别用户是否有权使用网络系统提供的网络服务，并根据认证结果向交换机发出打开或保持端口关闭的状态。

请求者　　认证者　　认证服务器

802.1x 是基于 IEEE 标准的网络认证访问框架，可以选择它管理负责保护网络畅通的密钥。它不仅限于无线网络，事实上，它还在顶级供应商的高端有线 LAN 设备上使用。802.1x 依赖于 RADIUS（远程身份验证拨入用户服务）网络身份验证和授权服务来验证网络客户端的凭据。802.1x 使用 EAP 来打包解决方案不同组件间的身份验证会话，并生成保护客户端与网络访问硬件畅通的密钥。EAP 是执行身份验证的网络工程任务小组（IETF）标准。它可用于多种基于密码、公钥许可证或其他凭据的不同身份验证方法。

EAP-TLS 通过基于证书的传输层安全（TLS）在采用强加密方法的无线客户端和 RADIUS 服务器间进行相互身份验证，并生成了保护无线传输的加密密钥。这是使用 802.1x 最受欢迎、最安全的 EAP 方法之一。它要求在客户端和 RADIUS 服务器上有公钥证书。

802.1 x 认证的突出优点就是实现简单、认证效率高、安全可靠。无需多业务网管设备，就能保证 IP 网络的无逢相连。同时消除了网络认证计费瓶颈和单点故障。解决了采用多业务网关，不便于视频业务开展的难题。在二层网络上实现用户认证，大大降低了整个网络的建网成本。

ES 支持对 802.1x 安全性进行配置。所支持的认证类型包括：

- EAP TLS
- EAP GTC
- EAP MD5
- EAP MSCHAPV2
- PEAP GTC
- PEAP MD5
- PEAP MSCHAPV2
- PEAP TLS
- TTLS PAP
- TTLS CHAP
- TTLS MSCHAP
- TTLS MSCHAP-V2
- TTLS EAP-MD5
- TTLS EAP GTC
- TTLS EAP MSCHAP-V2
- TTLS EAP-TLS

TLS 认证类型（也称为 SmartCard）允许导入由 IT 管理员提供的用户证书，并可在加密时使用其它标识号.