工业互联网产业联盟
Alliance of Industrial Internet

工业互联网
园区终端接入自动化
技术白皮书

（2021 年）

工业互联网产业联盟（AII）

2021 年 9 月

声　　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

编写说明

园区作为工业互联网企业集聚区，部署了大量基础设施，为企业用户提供了众多的公共服务。随着物联网和 5G 通信技术的发展，工业园区的终端数量将会呈现爆发式增长，海量终端的接入自动化就显得尤为重要。同时，终端设备的增多，也使得企业园区变得更加复杂，未经授权的非法终端接入，会给整个园区网络带来安全威胁。因而，园区终端接入和安全自动化是企业数字化转型的关键环节。

在此形势下，工业互联网产业联盟（以下简称“联盟/AII”）组织多家企业联合撰写了《工业互联网园区终端接入自动化技术白皮书》。本白皮书首先分析了园区终端接入的现状和园区网络面临的挑战，接着介绍了业界现有的网络技术和标准，给出了园区终端接入自动化的解决方案，并详细阐述了其中的关键技术，最后对终端接入自动化进行了总结和展望。

本白皮书编写过程中，得到了 AII 联盟成员及国内外众多技术专家的大力支持，为白皮书的观点形成与编写提供了有力支撑。后续我们将根据业界的实践情况和各界的反馈意见，在持续深入研究的基础上适时修订和发布的新版本。

牵头编写单位：华为技术有限公司

参与编写单位：中国信息通信研究院，广东九联科技股份有限公司，北京研华电子兴业电子科技有限公司

编写组成员：（排名不分先后）

华为技术有限公司	杨杰、侯方明
中国信息通信研究院	张恒升、陈洁
广东九联科技股份有限公司	何云华、戴林皓
北京研华电子兴业电子科技有限公司	耿琪之

目 录

一、园区终端接入现状

（一）园区终端发展趋势

IoT 已经成为当今世界的焦点，基于智能终端的万物互联，已经成为技术发展和产业应用的必然趋势。随着我国对工业 4.0、智慧城市、制造强国和数字中国战略的大力推进，智能终端正在加速渗透到制造、交通、安防、环境、电力、能源、医疗等相关行业和领域。

IoT 时代将有数量庞大的、种类繁多的智能终端接入企业网络，例如智联网联汽车、网络摄像头、机器人、无人机等，并覆盖制造、安保、能源、物流等众多应用领域。当前，企业智能终端数量正处于高速增长阶段，根据 IoT Analytics 的预测报告，2021 年全球活跃的 IoT 终端设备数量会达到 117 亿台，到 2025 年将达到 309 亿台，年复合增长率达 13%，如下图 1 所示:

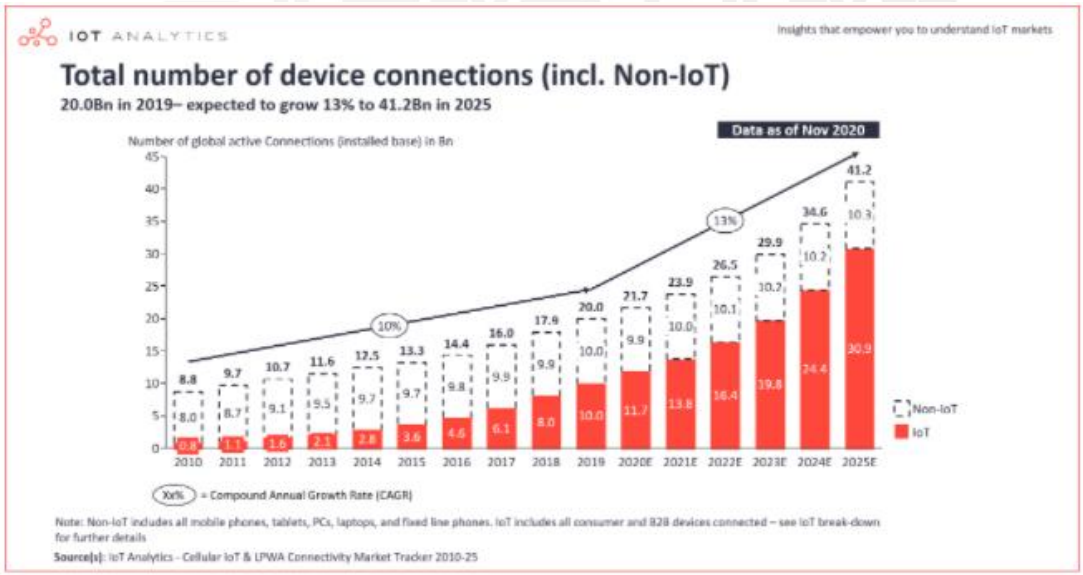


图 1 IoT Analytics 全球活跃的 IoT 终端设备数量预测

同时，根据 Gartner 发布的 IoT 标准与协议成熟度曲线 2020，如下图 2 所示：

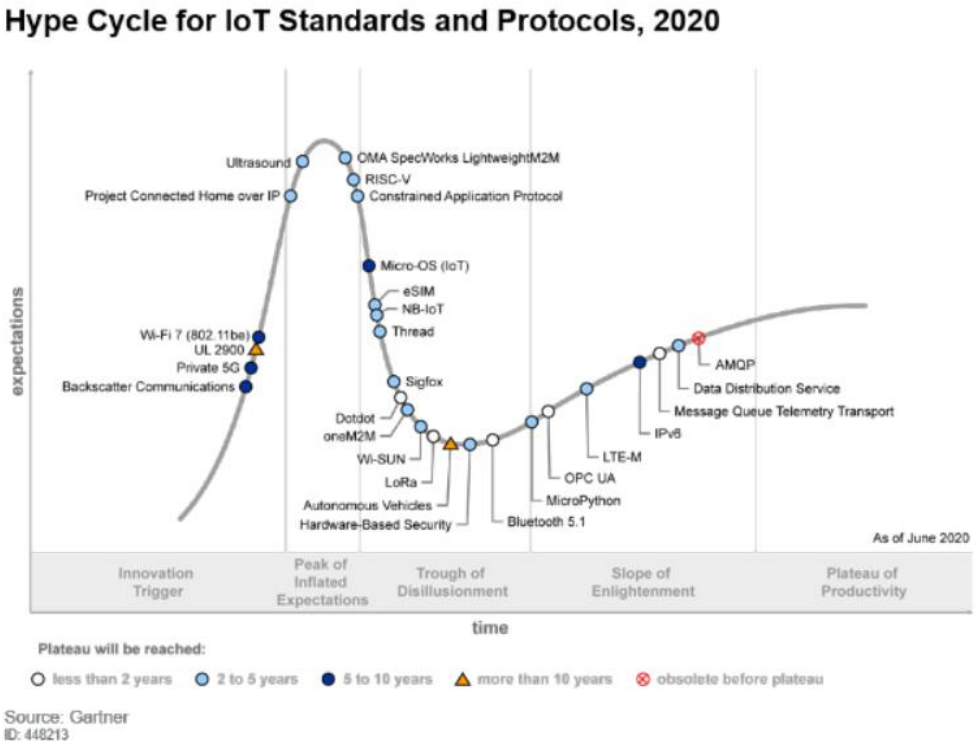


图 2 Gartner IoT 标准和协议成熟度曲线-2020

从上图中，我们可以得出 IoT 领域的标准和技术，存在如下趋势：

- 终端 IPv6 化，将进入成熟部署阶段
- 各种无线连接技术，包括 Wi-Fi、5G、NB-IOT、LoRa、Bluetooth 等，已成为终端连接的热点技术
- 基于平台的设备自动发现和认证标准，包括 oneM2M、LwM2M 等，已进入技术验证阶段
- 终端接入安全变得至关重要，Gartner 建议 IoT 厂商遵循 UL2900 中定义的安全指导原则，并通过测试认证

面向未来的物联网，需要以适应“数字化、智能化“为发展方向，通过云化、网络 IP 化、无线化、AI 化等技术应用，彻底消除“信息

孤岛”和“数据碎片化”，实现数字信息的泛在互联、高效通信，从而驱动产业升级，提高生产效率、降低管理成本、重构商业模式，提升用户体验，开启“数字经济”新时代。

（二）园区终端给网络带来的挑战

园区网络，实现了企业内部不同业务、终端之间的连接和通信。工业互联网园区网络，主要由工业生产网、企业信息网、园区公共服务网以及云基础设施组成，其网络架构如下图 3 所示:

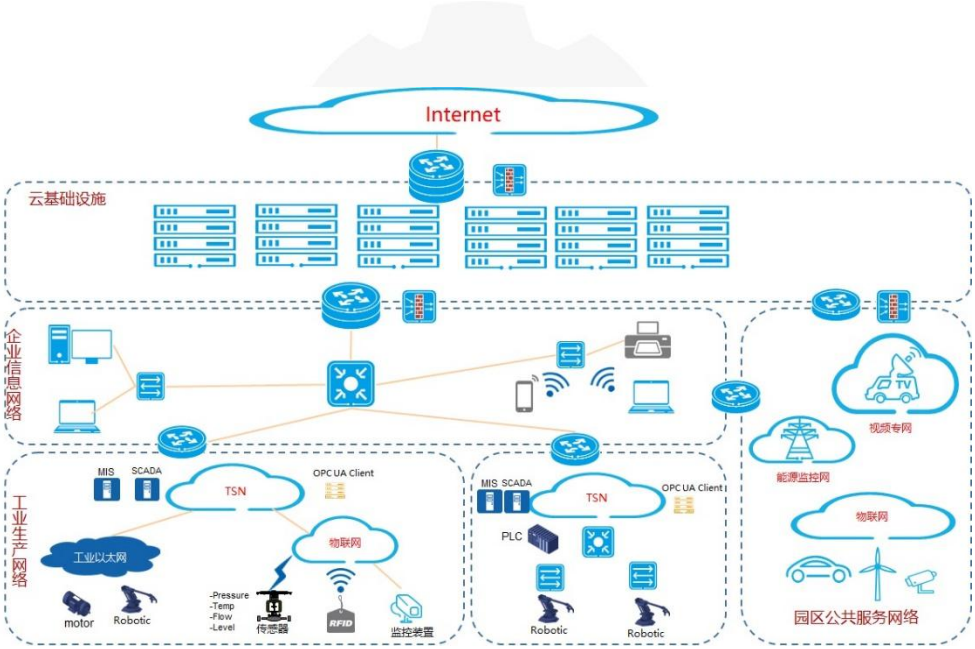


图 3 工业互联网园区网络架构图

以工业生产网络为例，它主要连接工厂内部的各种要素，包括人员（如生产人员、设计人员、外部人员）、机器（如生产装备）、材料（如原材料、过程件、制成品）、环境（如仪表、监测设备）等，包含多种不同的生产终端。典型的工业生产网络架构，如下图 4 所示:

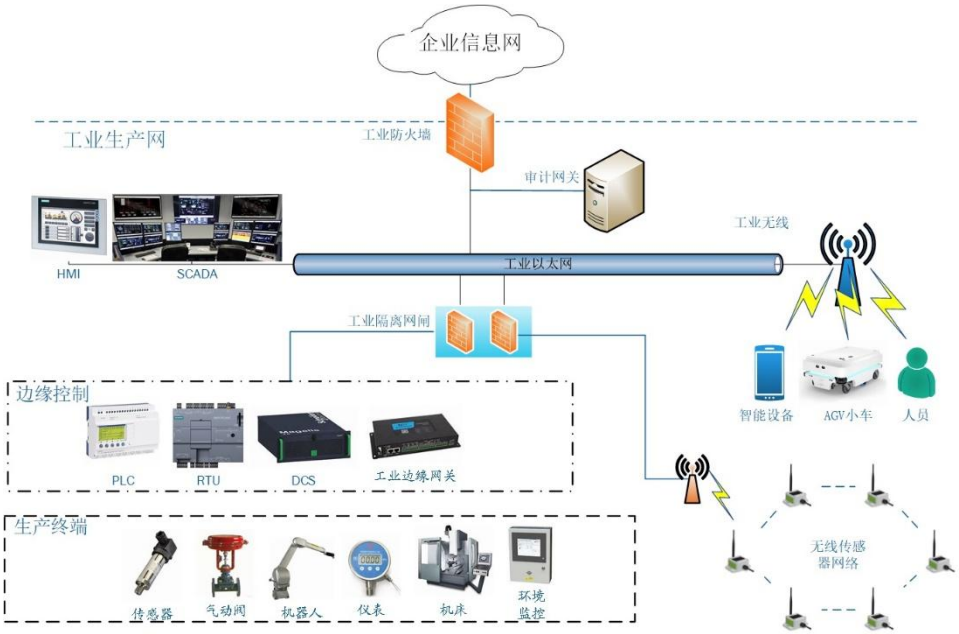


图 4 工业生产网络架构图

随着网络规模的不断增大，园区网络终端接入存在如下难点和挑战：

1) **设备数量庞大**：随着技术提高，越来越多的设备可以接入网络，对整个园区来说是海量设备、海量布线。依靠人工对每一个设备进行识别管理、制定规则，工作量大效率低，甚至出现故障后用户无感知，解决故障恢复时间长；

2) **设备种类多**：除了智能手机、Pad 等终端设备，还有打印机、传感器等哑终端，以及各种各样的园区终端设备，采用不同的终端接入协议。传统封闭的“七国八制”终端接入协议，没有统一的标准，使得企业园区的管理和运维更加复杂；

3) **设备识别困难**：不同的设备具有不同的能力，访问网络的行为也不同。在企业园区中部署大数量、多种类的终端，就需要更自动、更精准的设备识别技术，否则后续无法正确管理设备；

4）**接入安全管理复杂**：非法终端接入、网络隔离措施、智能终端安全防护等，依赖于人工参与，无法及时阻止病毒和网络攻击。同时，当发生入侵攻击、恶意破坏、误操作等事件发生时，用户无法及时定位和有效溯源。当接入设备的安全状态发送变化、出现安全事件时，需要自动及时响应；

近年来，出现过安全漏洞问题的企业不在少数，设想针对自动化制造环境部署的工业互联网，如果出现了安全漏洞将会导致怎样的混乱，生产停机和设备损坏又可能造成怎样的财务损失？下图 5 展示了企业网络被攻击的场景：

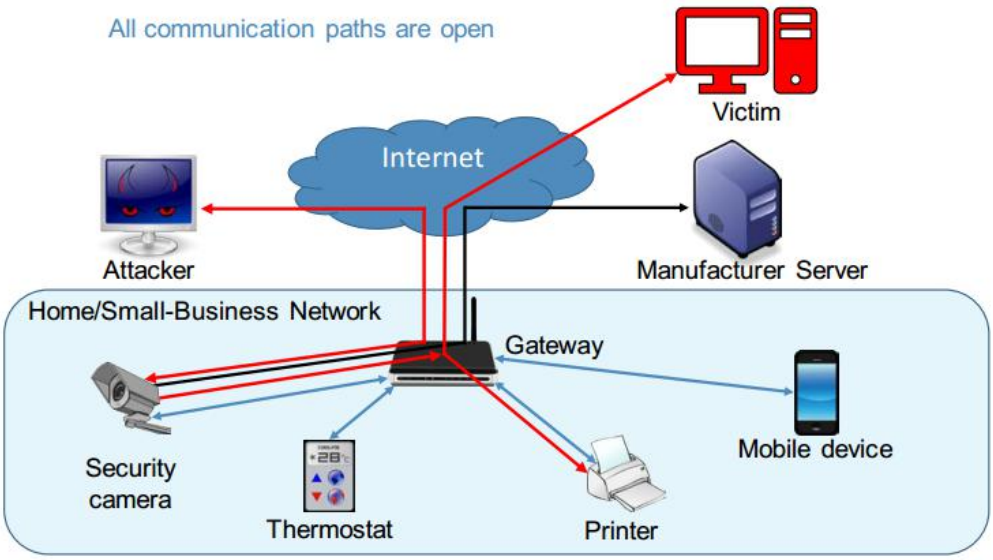


图 5 企业网络终端被攻击的一个案例

其中，企业网络中存在安全摄像头、温控计、打印机和移动设备，所有的通信路径都是开放的，它们可能会被互联网上的攻击者进行端口扫描（或者被劫持）。比如，本地网络中的安全摄像头被黑客攻击了，则黑客会利用该摄像头对本地和远程目标发起额外的攻击，造成更大的事故。因此，现代化的企业生产网，对于所有接

入的工业生产设备，都必须实现接入控制，进行接入认证和访问授权。

（三）园区终端接入自动化的发展路线

终端设备在企业园区的大规模部署，首先需要解决其接入自动化，即终端设备的即插即用、安全接入认证和可视可管。当前，业界有两条创新路线，分别是以云平台为锚点和以网络基础设施为锚点。

1. 以云平台为锚点

Case 1： 云服务商 AWS

首先，AWS 为 IoT 终端设备提供 SDK，由设备预安装。终端设备上线时通过 MQTT、HTTP 或 WebSockets 协议，接入到 AWS 的 IoT 系统，无缝安全地与 AWS IoT 系统提供的设备网关和设备影子协作，自动化的完成认证&鉴权。如下图 6 所示：

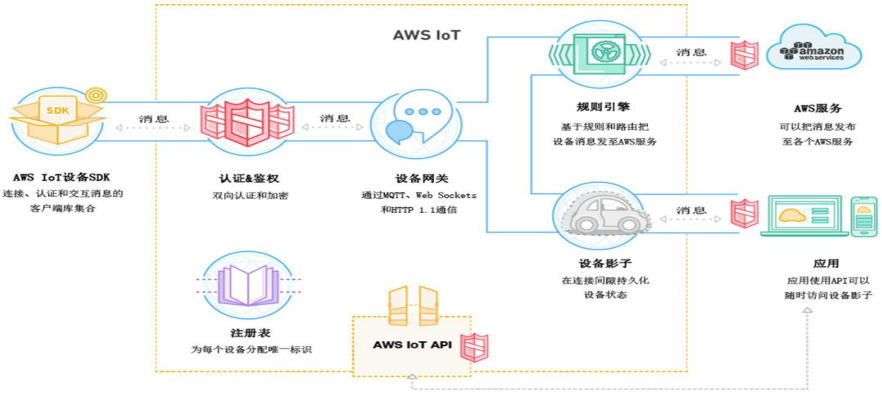


图 6 云服务商 AWS IoT 终端接入自动化解决方案

Case 2： 云服务商阿里云

与 AWS 的终端接入自动化方案类似，阿里云 Link ID²将密钥分发中心和认证中心作为两个服务，以 SDK 的方式提供给终端设备预安装。其中，分发中心采用硬件加密机和安全存储技术，确保密钥云端生成和存储的安全，与合作伙伴的安全产线对接，确保密钥安全烧录到各种安全等级的载体上。客户将安全载体集成到园区终端设备，基于设备端和云端的 SDK，调用 ID²认证中心提供的设备认证、信息加密等接口，建立安全通道，保障业务数据的不可抵赖性、完整性和保密性。如下图 7 所示:

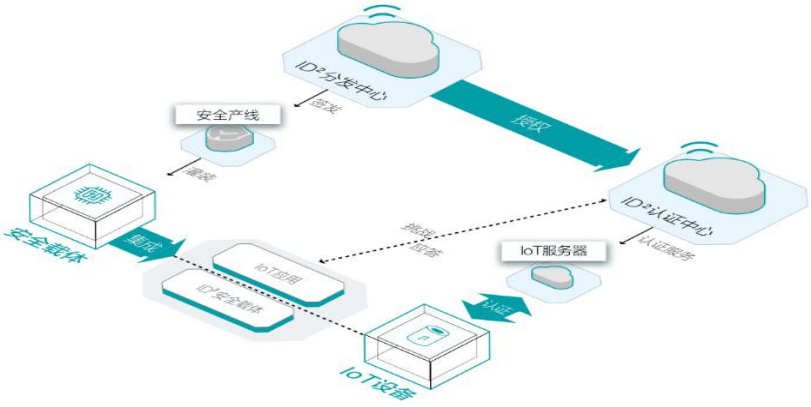


图 7 云服务商阿里云 IoT 终端接入自动化解决方案

2. 以网络基础设施为锚点

Case 1: 网络设备商 Cisco

Cisco 终端接入自动化解决方案基于 IETF MUD。首先，IoT 终端设备制造商通过定义 MUD File，完成对 IoT 终端的描述（如设备类型等）及其网络权限的定义。当 MUD-Capable 的终端设备上线时，设备通过内置的 MUD URL，向厂家的 MUD File Server 获取设备的描述信息和接入策略，自动化实现设备的即插即用。如下图 8 所示:

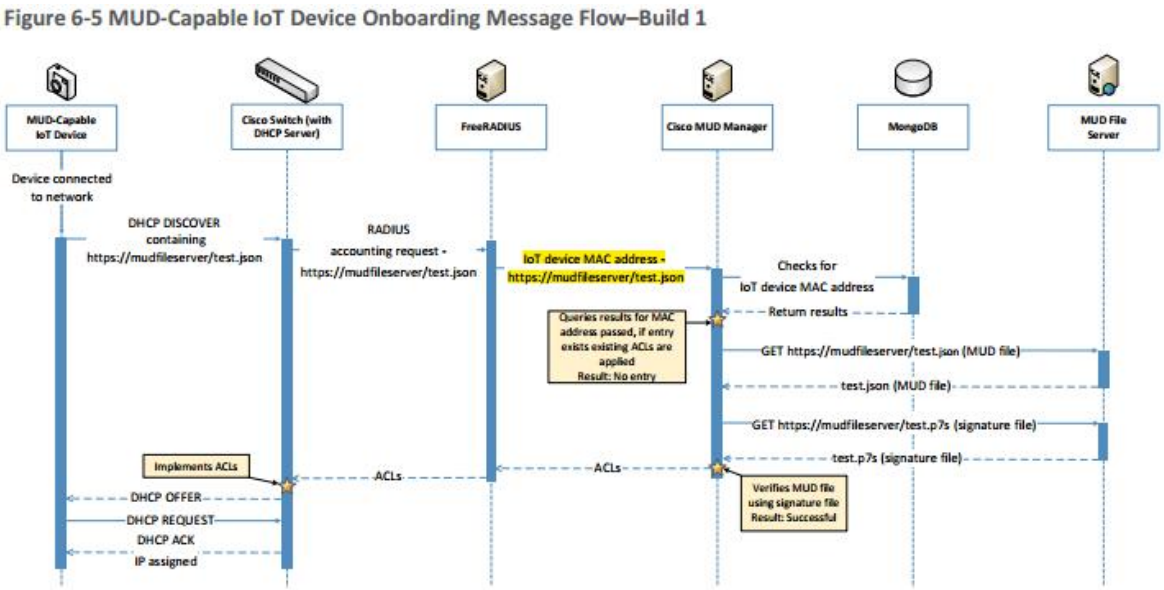


图 8 网络设备商 Cisco IoT 终端接入自动化解决方案

Case 2: 设备商 ForeScout

ForeScout 终端接入自动化解决方案基于终端指纹库，提供可视化平台，包括 ForeScout Device Cloud 和 ForeScout Research。其中，ForeScout Device Cloud 基于来自 10 多个行业的 500 多家企业客户的设备分类，建立丰富的分类标准，可以根据设备的类型和功能、操作系统和版本、制造商和型号对设备进行自动分类。ForeScout Research 利用云中超过 300 万个现实世界设备的情报，周期性发布这些新配置文件，以帮助提高分类效果和覆盖。其解决方案如下图 9 所示:

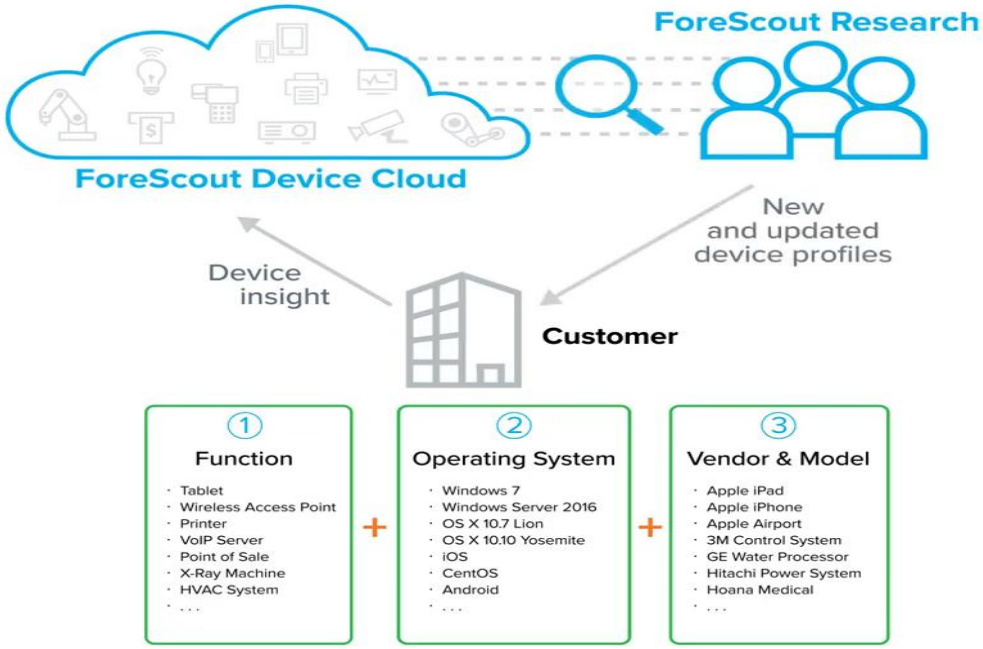


图 9 网络设备商 ForeScout IoT 终端接入自动化解决方案

以上两条业界终端接入自动化的创新路线，虽然实现方式不同：

- 以云平台为锚点的终端接入自动化解决方案，需要在 IoT 终端设备预置云服务商的 SDK;
- 以网络基础设施为锚点的终端接入自动化解决方案，需要对现有终端进行 MUD-Capable 改造，或者依赖终端指纹库;

但核心理念是一致的，即：IoT 终端设备接入园区网络，从原有的单设备认证和策略授权，发展到基于生态链集成的自动化认证和策略授权，实现终端设备的即插即用、安全接入。

二、园区终端接入自动化技术标准概述

终端接入园区网络，包含设备与链路发现、接入认证、策略管控三个阶段。下面，分别介绍这三个阶段中业界现有的技术与标准。

（一）设备与链路发现

1.LLDP 协议

网络设备种类繁多且各种配置错综复杂，为了使不同厂商的设备能够在网络中相互发现并交互各自的系统、配置信息，需要有一个标准的信息交流平台。LLDP 就是在这样的背景下产生的。

LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的链路层协议。它提供了一种标准的链路层发现方式，可以将本端设备的的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发送给直连的邻居，邻居收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

通过采用 LLDP 技术，在网络规模迅速扩大时，网管系统可以快速掌握二层网络拓扑信息和拓扑变化信息。LLDP 不会配置也不会控制网络元素或流量，它只是报告第二层的配置。

2.DHCP 协议

随着网络规模的扩大和网络复杂度的提高，网络配置变的越来越复杂，再加上计算机数量剧增且位置不固定（如移动便携机或无线网络），引发了 IP 地址变化频繁以及 IP 地址不足的问题。为了实现网络可以动态合理地分配 IP 地址给主机使用，需要用到动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）。

DHCP 协议是在 BOOTP（Bootstrap Protocol）协议基础上发展而来，但 BOOTP 运行在相对静态（每台主机都有固定的网络连接）的环境中，管理员为每台主机配置专门的 BOOTP 参数文件，该文件会在相当长的时间内保持不变。而 DHCP 从两方面对 BOOTP 进行了扩展:

- DHCP 实现了 IP 地址及网络配置参数的自动分配的功能。
- DHCP 允许计算机快速、动态地获取 IP 地址，而不是静态为每台主机指定地址。

DHCP 技术实现了 IP 地址的合理分配，提高了 IP 地址的使用率，避免了 IP 地址的浪费。

3. Beacon 技术

从无线制式方面，将 IoT 的无线联网技术归为三类:

- 2G/3G/4G/5G 插 SIM 卡上网，无需配网;
- WiFi 连路由器上网，需要配置 SSID（Service Set Identifier，服务组合识别码）和 Password;
- BlueTooth/Zigbee 等通过网关代理上网，需要与网关配对;

其中，第 1 类，无需配网；第 3 类，多采用协议规定的配网方式，多为 PBC 触发配对方式。

针对第 2 类（WiFi 连路由器）的方式，其首次使用时的网络配置，通常有如下三种方式:

- 配有 MMI I/O 设备的，可以直接人机交互配网。
- 配备有 NFC、USB 等的，可以通过 Out-of-Band 的方式，辅助 APP 配网。

- 除此之外，只能通过 In-Band 方式配网。技术上包括以下方案:

a) SoftAP 方式

IoT 设备工作于 AP 模式，手机直连 IoT 设备，将目标路由器的 SSID/Password 传过去。该方式是最传统的配网方式，不考虑终端兼容性问题，配网成功率 100%。缺点是用户操作复杂：用户需要下载 APP，连接 IoT 设备，手动输入 SSID/Password。同时，APP 也需要开发团队自己开发。

b) WPS 方式

WPS 方式，需要在 IoT 设备端和路由器端按下 WPS 按钮，一键配对。但该方式要求路由器和 IoT 同时支持 WPS，目前部分路由器已经取消 WPS 功能，IoT 增加按键也有诸多不便。

c) Broadcast/Sniffer 方式

APP 控制通过 UDP 广播或者组播方式向空中广播 SSID/Password，IoT 设备工作于混杂模式，抓包得到目标路由器的 SSID/Password。因为空口通信被加密，通常会利用帧长度编码，效率低、易受干扰。该方案是一种 hack 类型的方案，未在 802.11 协议内规定，兼容性不能保证。尤其双频下面，路由器隔离了 2.4G 和 5G 的情况下，大概率会配网失败。该方式下用户操作也很复杂，相对 SoftAP 方式，只是少了连接 IoT 设备的过程，仍然需要下载 APP，SSID/Password 仍需手动输入。

d) Beacon/Probe Vender-specific 方式

Beacon/Probe Vender-specific 方式，通过自定义 beacon/probe 帧的 vender-specific 字段，可以使 IoT 设

备和路由器在建立连接之间，进行简单通信，从而实现高级的配网功能。该方案是路由器和 IoT 设备直接通信，路由器是知道自己的 SSID/Password 的，所以，极限情况下，甚至可以上电即入网、免人工干预，已经成为 WIFI & IoT 领域设备发现的优选技术。

（二）接入认证技术

认证作为信息技术领域重要的安全控制技术，主要作用是在系统中确认每一个成员的身份。当前的接入认证技术，包括 MAC 认证、Web 认证、802.1x 认证。下面我们介绍下接入认证相关的标准与技术。

1.MAC 认证

MAC 认证是以终端的 MAC 地址作为身份凭据的认证技术。当终端接入网络时，准入设备获取终端的 MAC 地址，并将该 MAC 地址作为用户名和密码进行认证。

由于 MAC 地址很容易被仿冒， MAC 认证方式的安全性较低，另外，需要在准入服务器上登记 MAC 地址，管理较复杂。对某些特殊情况，终端用户不想或不能通过输入用户账号信息的方式进行认证时，可以采用此认证技术。例如，某些特权终端希望能“免认证”直接访问网络；终端为某些无法输入用户账号信息的哑终端，如打印机、 IP 电话等设备。

2.Web 认证

随着互联网和 Web 应用的快速发展，人们对信息的传输速率以及网络访问安全性等方面提出了更高的要求，同时网络需要对接入的各类终端的合法性进行验证而又不想通过安装复杂的认证软件进行认证，因而产生了一种基于端口的接入控制方式，即 Web 认证。

Web 认证是一种对用户身份以及网络访问权限进行校验的身份认证方式，这种认证方式不需要接入终端安装较为复杂的接入认证软件，仅仅依靠浏览器在应用层对终端 HTTP 请求进行拦截，校验终端设备提供的用户名以及密码等认证信息，从而完成接入认证操作。当未经认证的终端访问网络时，其会被强制重定向到特定的指定的服务器（即 Web 认证服务器，通常也称为 Portal 服务器）进行认证，只有身份认证通过之后，终端才能接入到网络中，才能访问网络中的资源。

3.802.1x 认证

IEEE 802.1x 是由 IEEE 于 2004 年所提出，旨在制定与规范用户接入网络的认证标准，全称是“基于端口的网络接入控制”，即在局域网接入设备的接口这一级，对所接入的用户设备通过认证来控制对网络资源的访问。

802.1x 认证系统是典型的 C/S 结构，包括三个实体：客户端、设备端和认证服务器：

- **客户端**：客户端是位于局域网链路一端的实体，由该链路另一端的设备端对其进行认证。客户端通常是支持 802.1x 认

证的用户终端设备，用户通过启动客户端软件发起 802.1x 认证。

- **设备端**：对连接到局域网链路对端的客户端进行认证。设备端通常为支持 802.1x 协议的网络设备，它为客户端提供接入局域网的接口。
- **认证服务器**：为客户端提供认证服务的实体。认证服务器用于对用户进行认证、授权和计费，通常为 RADIUS 服务器。

802.1x 认证系统结构如下图 10 所示：

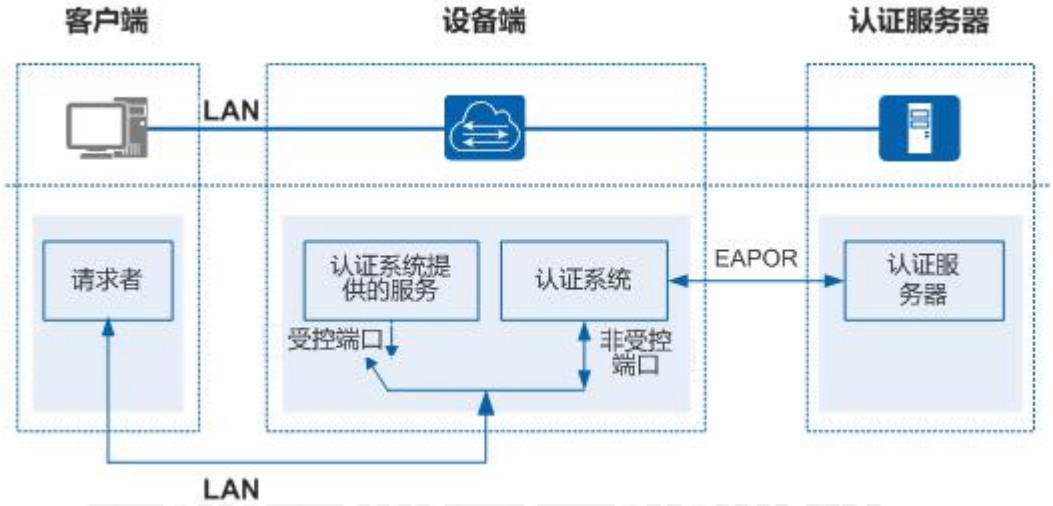


图 10 802.1x 认证系统示意图

802.1x 认证系统通过在设备端端口上进行配置，对端口上接入的用户终端进行身份认证与访问拦截从而控制用户终端对网络资源的访问，保证网络安全。在 802.1x 认证系统中客户端设备必须支持局域网可扩展认证协议(Extensible Authentication Protocol over LAN, EAPOL)，通过该协议来封装传输客户端与设备端的 EAP（Extensible Authentication Protocol）认证报文。设备端与认证服务器端通过将 EAP 认证报文封装在 RADIUS(Remote

Authentication Dial In User Service)报文中完成认证消息交互，如下图 11 所示:

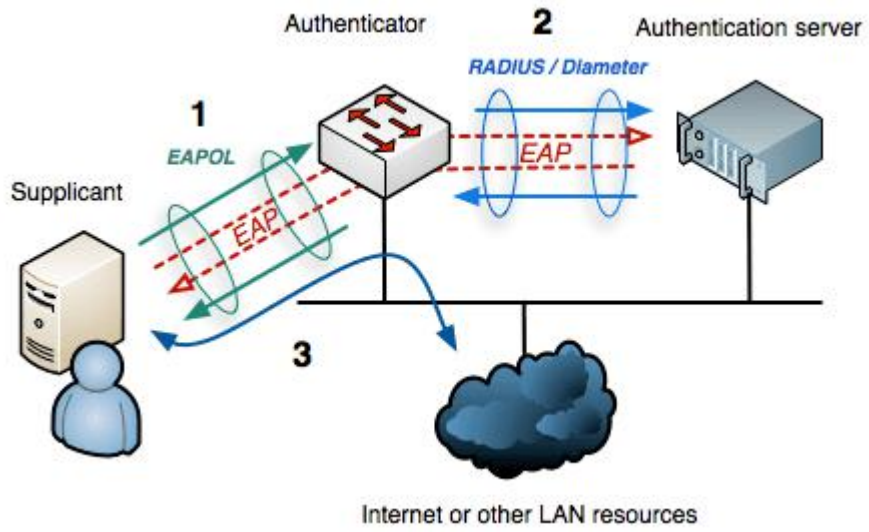


图 11 EAP 认证消息交互流程图

4. X.509 标准与证书

X.509 是国际电信联盟-电信（ITU-T）部分标准和国际标准化组织（ISO）的证书格式标准。作为 ITU-ISO 目录服务系列标准的一部分，X.509 是定义了公钥证书结构的基本标准。1988 年首次发布，1993 年和 1996 年两次修订。当前使用的版本是 X.509 V3，它加入了扩展字段支持，这极大地增进了证书的灵活性。X.509 V3 证书包括一组按预定义顺序排列的强制字段，还有可选扩展字段，即使在强制字段中，X.509 证书也允许很大的灵活性，因为它为大多数字段提供了多种编码方案。

X.509 证书广泛地被应用于加密（Encryption）和数字签名（Digital Signature），以提供认证的实现和确保数据的一致性（Integrity）和机密性（Confidentiality）。常见的加密/解密算

法有：PKI(public-key cryptography)公钥密码体制、对称加密算法、非对称加密算法、RSA 密码算法。

5.数字签名

数字签名（Digital Signature）技术是不对称加密算法（RSA）的典型应用。数字签名就是电子签章，用于确认数据的完整性和数据来源，建立在数字指纹和公共密钥体制基础上。数字指纹就是对一段消息进行数学变换，计算出一个指定长度的唯一特征码，用来唯一标识原文信息。

数字签名具体做法是:

① 将报文按双方约定的 Hash 算法计算得到一个固定位数的报文摘要。在数学上保证：只要改动报文中任何一位，重新计算出的报文摘要值就会与原先的值不相符。这样就保证了报文的不可更改性。

② 将该报文摘要值用发送者的私人密钥加密，形成数字签名，然后连同原报文一起发送给接收者。

③ 接收方收到报文后，用同样的 Hash 算法对报文计算摘要值，然后用发送者的公开密钥对数字签名进行解密得到的另一个摘要值，如果两者相等则说明报文确实来自发送方，且没有经过任何篡改。

采用数字签名，能够确认以下两点:

① 保证信息是由签名者自己签名发送的，签名者不能抵赖，他人不能伪造，在公证人面前能够验证真伪;

② 保证信息自签发后到收到为止未曾作过任何修改，签发的文件是真实文件。

通过“IE/internet 选项”对话框的“内容”页面，可以查看计算机中的证书信息（包括证书中的签名信息）。如下所示的 Internet 选项数字证书信息图 12，数字证书使用了 sha1 算法来生成证书的报文摘要（左图），摘要共 160 比特（中图），CA（证书授权中心）使用 sha1RSA 算法对证书进行了数字签名（右图）：

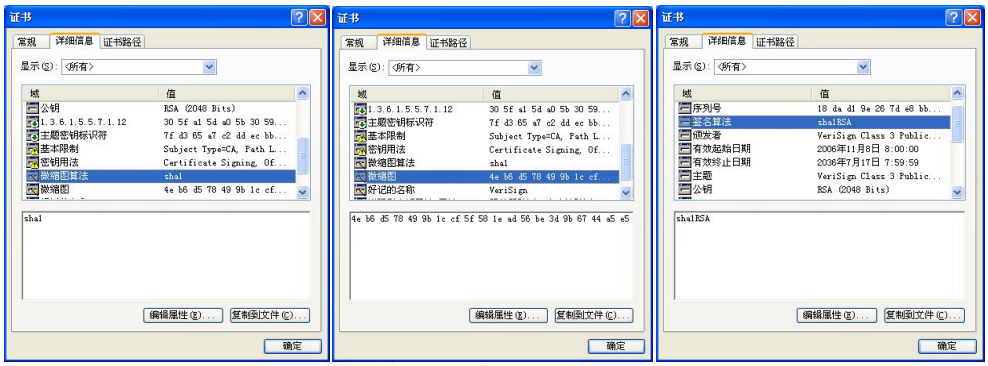


图 12 Internet 选项数字证书信息图

6. EAP 协议

EAP(Extensible Authentication Protocol)可扩展认证协议，是一种在无线网络中普遍使用的认证框架，由 IETF RFC 3748 定义，之后 RFC 5247 对其内容有所更新。EAP 协议非常简单，它可以运行在各种底层，包括数据链路层和上层协议[如 UDP（User Datagram Protocol，用户数据报协议）、TCP（Transmission Control Protocol，传输控制协议）等]，而不需要 IP 地址，因此使用 EAP 的 802.1X 认证具有良好的灵活性。EAP 协议的架构如下图 13 所示:

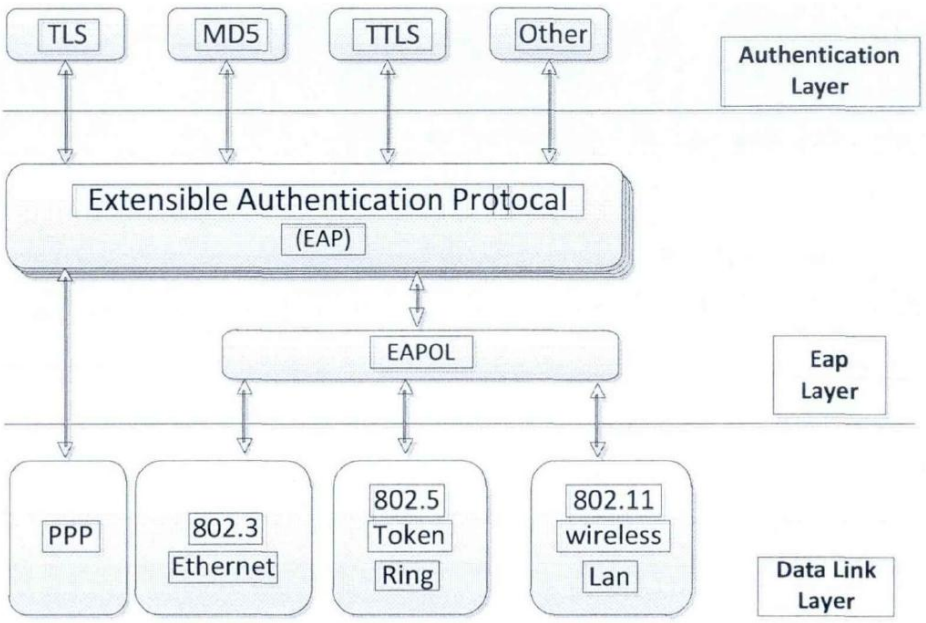


图 13 EAP 协议架构图

7. EAP-TLS

EAP-TLS 是目前最受欢迎，又是最安全的 EAP 认证方法之一，大型企业由于对安全性有较高的需求，往往使用 EAP-TLS 认证方式。

EAP-TLS 是在 EAP 框架上使用 TLS（Transport Layer Security）承载实现鉴权、密钥协商和证书交换，是 IETF 推荐的 WLAN 接入认证方法，由 RFC 5216 定义。EAP-TLS 通过在客户端与服务器上同时部署数字证书，使用强加密方法对客户端和服务器间进行双向的身份验证，然后进行密钥协商产生会话的加密密钥。如下图 14 所示:

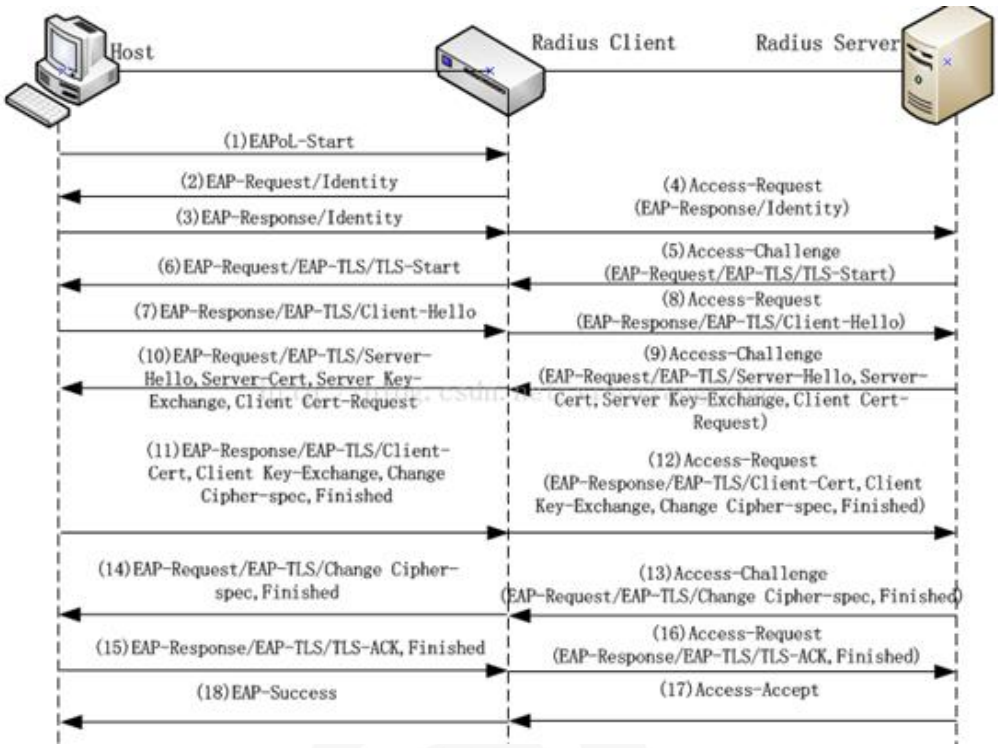


图 14 EAP-TLS 认证流程图

通常，终端接入园区网络时，不仅要对通信数据进行加密，还需要完成通信双方的双向身份认证。也就是说，网络必须对用户（或终端）进行身份验证，用户（或终端）也必须能够来认证网络的身份。智能终端与园区网络之间相互认证身份，才能保证通信双方身份的合法性和真实性，这是通信安全中最基本的安全需求。

（三）策略管控技术

终端设备的策略管控，通常的技术方案有三种：本地配置静态 ACL（Access Control List，访问控制列表）策略、通过准入服务器动态授权策略、IETF MUD 基于终端设备描述信息。

1.本地配置静态 ACL 策略

本地配置静态 ACL 策略，是指在准入设备上定义基于 ACL 的用户策略，实现对用户的策略控制。

ACL 是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源 IP 地址、目的 IP 地址、端口号等。 ACL 本质上是一种报文过滤器，规则则是过滤器的滤芯。

准入设备基于这些 ACL 规则进行报文匹配，可以过滤出特定的报文。然后根据应用 ACL 的业务模块的处理策略来执行策略动作，常见的策略动作有网络资源的访问权限（如是否允许某用户访问某服务器资源）、限制用户的接入带宽（如限制某类用户的接入带宽）、区分优先级的服务（如 VIP 用户的权限比普通用户更高）等。通过 ACL，网络管理员可以精确控制每一个终端所具备的网络访问权限，从而达到终端管控的目的。

静态 ACL 策略授权，如下图 15 所示:

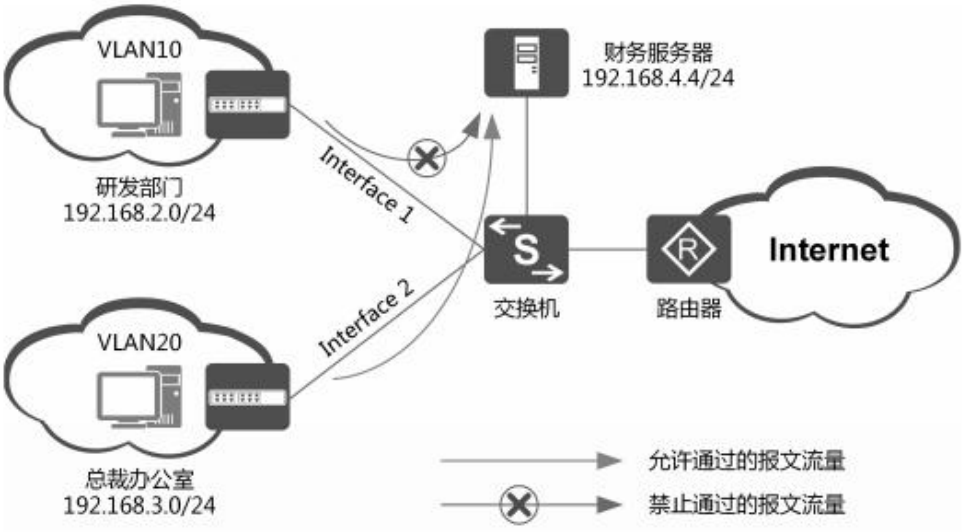


图 15 ACL 策略授权示例

其中，企业为保证财务数据安全，禁止研发部门的用户访问财务服务器，但总裁办公室不受限制。可以通过在 Interface 1 的入方向上部署 ACL，禁止研发部门访问财务服务器的报文通过。Interface 2 上无须部署 ACL，总裁办公室访问财务服务器的报文默认允许通过。

常见的 ACL 结构组成，如下图 16 所示:

图 16 ACL 的结构组成

本地配置静态 ACL 策略，本质是把用户的策略权限映射到用户使用的 IP 地址，然后基于 IP 地址规划 ACL 规则，实现对用户权限的管控。在用户网络较小、用户终端位置固定、用户策略诉求简单、IP 和终端物理位置强绑定的场景下，适合选择本地配置静态 ACL 策略。它的优点是配置简单，无须跟准入服务器配合，但随着网络规模的增加，策略诉求也会更加复杂，其配置将会变得复杂并且难以维护。

2.通过准入服务器动态授权策略

通过准入服务器授权 ACL 策略，是指在准入服务器上定义用户的策略，然后把授权策略下发给准入设备，由准入设备对用户执行

策略动作。在企业园区网络解决方案中，通常将 SDN Controller 作为准入服务器，实现对用户的身份认证和策略授权。

常见的授权信息有基于 VLAN 和基于 ACL 的策略授权。以基于动态 ACL 的策略授权为例，根据不同用户的策略需求，直接在 SDN Controller（即准入服务器）上配置授权策略（ACL 编号、ACL 匹配规则及策略）。终端访问网络时到准入设备进行身份认证，准入设备将用户身份凭证发送给准入服务器。准入服务器认证校验通过后，根据先前配好的授权策略，对准入设备返回策略结果，准入设备根据准入服务器下发的策略执行相应的策略动作。基于动态 ACL 的策略授权，如下图 17 所示:

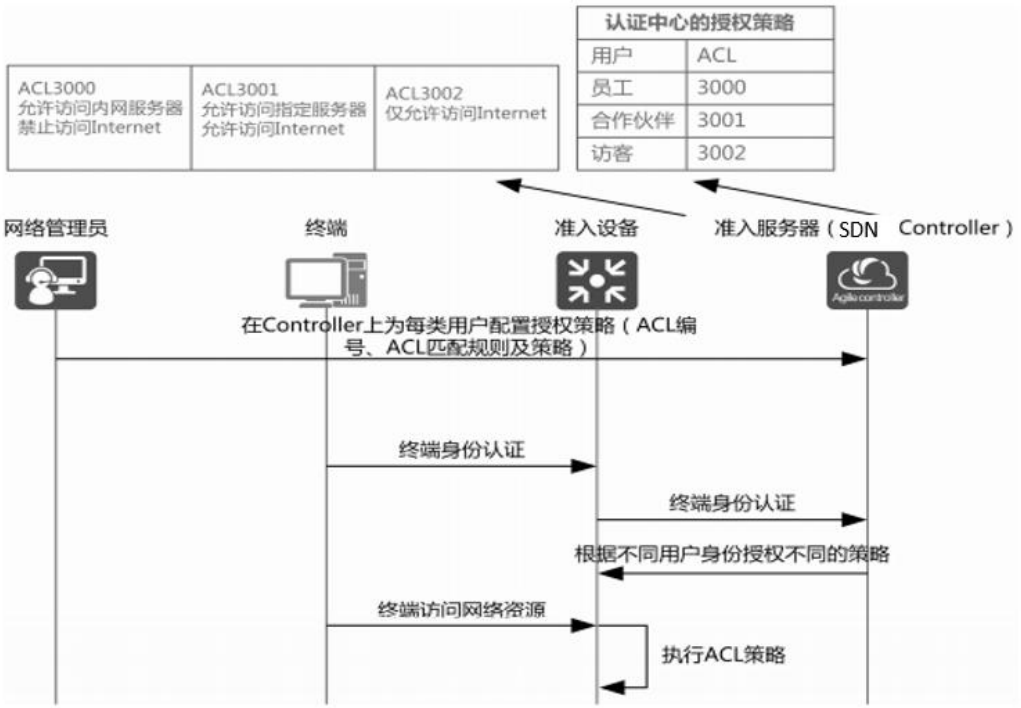


图 17 动态 ACL 策略授权原理示意图

通过准入服务器授权 ACL 策略，本质是根据用户身份授权不同的 ACL 策略，一定程度上做到了终端用户权限和 IP 地址以及物理位置的解耦，依赖网络规划将具有相同权限的用户划分成相同的网段，

然后在设备上配置基于用户网段的 ACL，实现基于用户身份的策略管控。

通过准入服务器授权的 ACL 策略，不需要在准入设备上配置，但需要提前在准入服务器上统一规划。当用户规模较大时，特别是接入的终端有移动诉求，难以做到提前在准入服务器上进行统一的预配置。

3.MUD（厂家使用说明）

IETF RFC 8520 构建了一套基于 MUD（Manufacturer Usage Description，厂家使用说明）文件为核心的协议框架。首先由终端设备厂商在 MUD 文件中，完成对终端的描述（如设备类型等）以及其网络权限的定义，然后基于 MUD 文件实现通过控制器或者 AAA 服务器完成终端设备厂商的权限定义到网络设备中的网络策略的自动映射。MUD 协议架构如下图 18 所示:

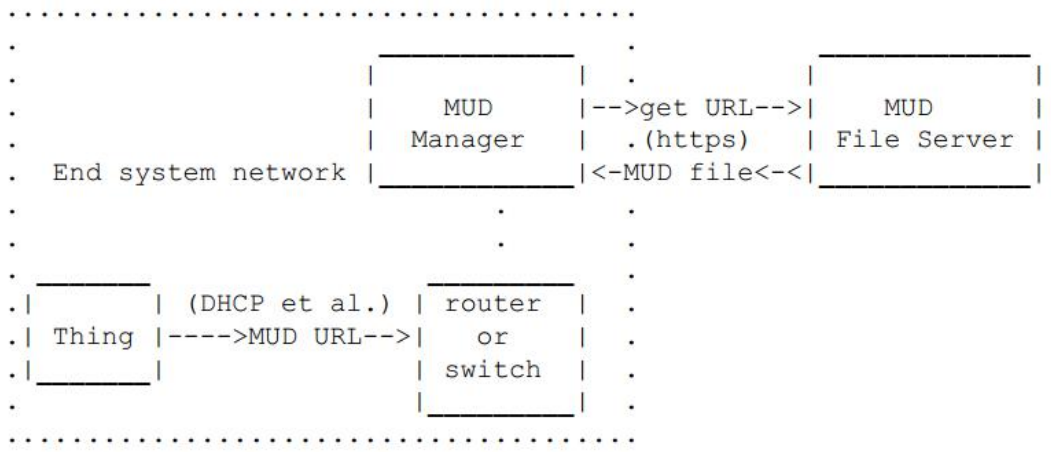


Figure 1: MUD Architecture

图 18 IETF MUD(RFC 8520)协议架构

为了更好的理解 MUD 通信机制的工作原理以及策略自动化配置过程，下面给出 MUD 标准中所定义的相关关键术语:

- Thing：发出 MUD URL 的 IoT 终端
- MUD URL：MUD 控制器接收 MUD 文件的 URL
- MUD 控制器：向 MUD 文件服务器请求/获取 MUD file 的系统，完成 MUD 文件处理后，将策略下发给对应的网络设备
- MUD 文件：包含基于 YANG 的 JSON 文件，描述 IoT 终端属性及其关联的特定网络行为
- MUD 文件服务器：承载 MUD 文件的 Web 服务器。
- 制造商：在 MUD 文件中，配置 Things 发出 MUD URL 的实体。制造商可能并不总是 IoT 设备的制造实体，例如，它可以是一个系统集成商，甚至是一个组件提供商。

MUD 协议的部署架构，如下图 19 所示：

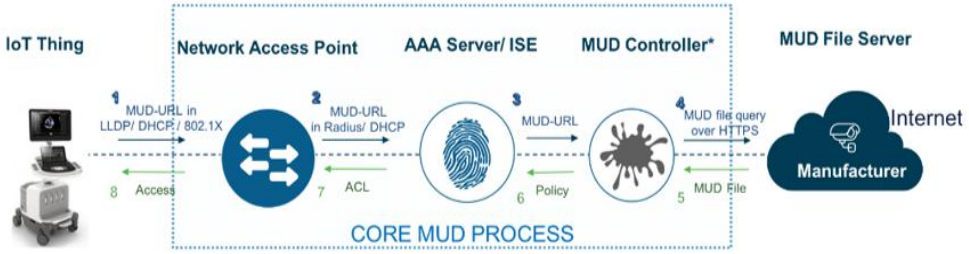


图 19 MUD(RFC 8520)协议的部署架构

其处理流程如下：

① IoT 设备首次连接到网络时，将 MUD URL 嵌入在发送的 LLDP，DHCP 或 802.1X 请求中；

② 网络接入设备提取 URL，将其封装在 Radius 数据包中，然后将其发送到 AAA 服务器；

③ AAA 服务器再将该 URL 传递到 MUD 控制器上；

④ MUD 控制器通过 HTTPS 与该 URL 指向的制造商的 MUD 文件服务器联系；

⑤ 在确认设备制造商生产了 MUD 文件后，将与该设备相对应的 MUD 文件发送到 MUD 控制器。该文件中包含有关 IoT 设备的抽象通信意图;

⑥ MUD 控制器将此抽象意图转换为特定于上下文的策略，并传递到 AAA 服务器;

⑦ AAA 服务器以基于端口的访问控制列表（ACL）的形式将策略强制应用到网络接入设备上，以约束 IoT 设备的网络行为。

假定企业网络中存在安全摄像头、温控计、打印机和移动设备都支持 MUD 特性（为简化描述，图中省略了 MUD 管理器、MUD 文件服务器等 MUD 部署的组件），如下图 20 所示。每个支持 MUD 的 IoT 设备，在 MUD 文件列出了允许它能访问的所有外部服务域，不能访问的外部服务域，以及允许基于厂商或型号等特征的本地设备通信关系。这样，支持 MUD 的 IoT 设备，不向 MUD 文件中未明确允许的外部目标发送流量，不从 MUD 文件中未明确允许的外部站点接收流量。如果本地网络的一台设备试图攻击另一台设备，但对应的 MUD 中未允许它们互通，则丢弃该攻击流量，避免更大的威胁攻击。

如图 20 所示，在打印机的 MUD 文件中，未定义安全摄像头与打印机的通信关系，则打印机将丢弃来自摄像头的攻击:

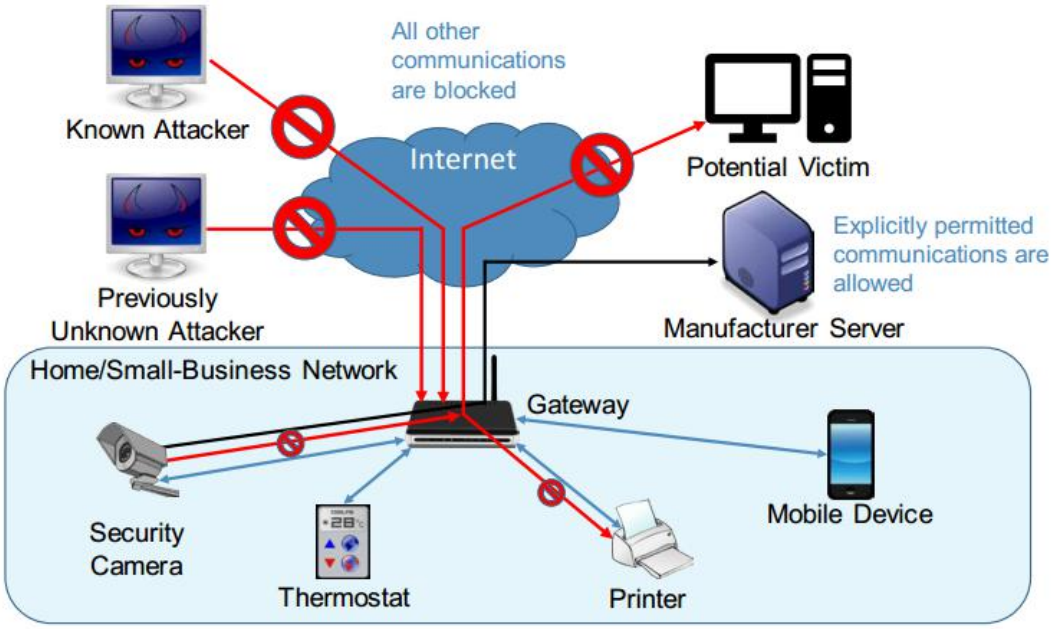


图 20 支持 MUD 特性的企业网络被攻击的一个案例

MUD 可用于自动允许设备发送和接收的流量，执行在 MUD file 中描述的预期功能。但 MUD file 本身的安全性，比如：是否被篡改了，就需要对 MUD 提供者（MUD Server）和使用者（网络管理员）都进行合法性校验。此时，推荐终端接入园区网络时，首次在本地局域网中基于电子身份规约进行业务识别和本地认证，再由 SDN 控制器基于识别的终端业务申请数字证书，并引导园区终端二次入网，保障终端与网络的双向安全接入。

三、园区终端接入自动化解决方案

针对企业园区终端接入面临的一系列挑战，需要有一种极简、智能、安全的园区网络终端接入自动化解决方案，实现终端设备的即插即用、安全可信、可视可管等。下面基于园区终端接入自动化解决方案总体架构，介绍园区终端接入自动化的关键技术。

（一）总体架构

园区终端接入自动化解决方案总体架构，如下图 20 所示:

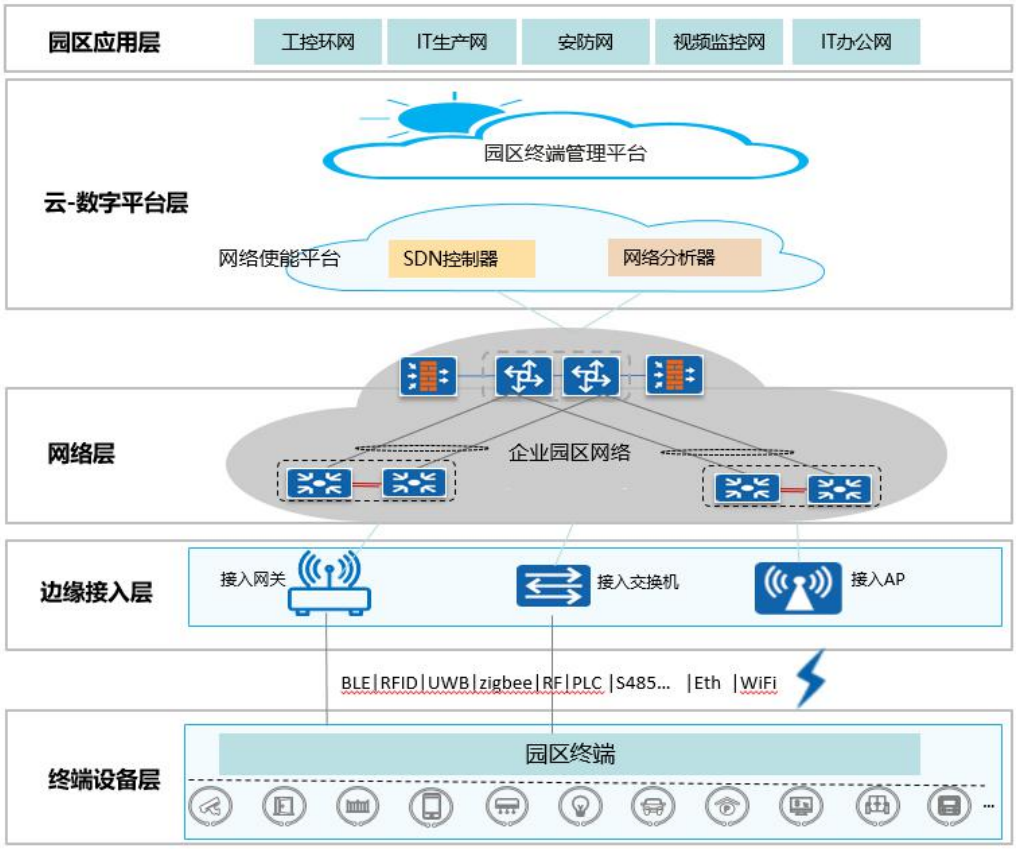


图 21 园区终端接入自动化解决方案总体架构图

园区终端接入自动化解决方案，总体架构由端、边、管、云四层组成。以下分别介绍每一层的功能，以及园区终端接入自动化解决方案相关的关键技术:

- **终端设备层**

  终端设备层是园区网络的“神经末梢”，联接着物理世界和数字世界。这些终端根据行业不同部署在不同环境中，有室内也有室外，有固定的也有移动的，根据场景不同需要选择合适的网络联接方式。

- **边缘接入层**

  边缘接入层实现终端设备的接入网络构建，以及边缘数据采集，协议的转换和适配，以及满足本地业务存活需求具备的本地容器能力，或本地数据分析与处理能力。边缘接入层的也被看作园区终端接入网络的“边缘神经”。

- **网络层**

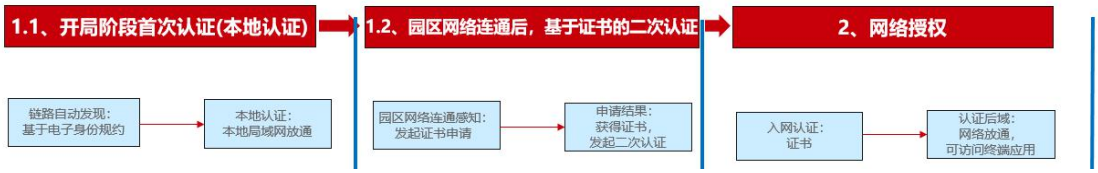
  网络层是园区终端接入网络的“神经网络”，主要是保障终端设备数据高效，可靠，安全的传输。不同的行业按需选择广域网络建设、园区网络、或运营商网络，实现终端设备数据的回传。

- **云-数字平台层**

  数字平台层是整张园区终端接入网络的“神经中枢”，分为网络使能平台，以及终端管理平台等。其中网络使能平台是园区终端端网管理的核心，实现对终端、边缘网关、企业网络的整网管理与运维。

（二）终端设备即插即用

1. 终端设备入网过程



终端设备即插即用，主要体现在终端设备自动发现、业务识别、入网引导、接入认证、获得业务证书进行二次认证，以及配网自动化，无需传统开局方式的复杂网络设备配置、复杂的终端接入配置，

只需要终端设备能够连入网络，就可以自动做到终端设备接入、认证和上网，具体步骤如下:

① 开局首次认证

开局阶段首次认证，包括链路自动发现，和本地认证过程。主要实现终端设备的自动发现，终端设备自动识别，对于终端设备的本地接入认证过程。完成首次认证后，设备接入网络，但只获得有限的本地网络访问权限，无法访问终端设备业务。终端设备需在 PKI 上申请合法的 PKI 证书，用于访问业务的二次认证过程。

② 二次认证

完成本地认证的终端设备，仍然没有访问业务的权限，只能具备访问网络中的部分区域的网络设备的能力，因此只有有限的部分访问权限。此时终端设备和业务网络之间访问是隔离的，这样可以避免终端仿冒设备会对网络构成安全威胁。终端设备访问相应的业务则需要再进行数据证书二次认证。建议由 SDN 控制器引导终端设备，到 PKI 服务器上申请数字证书，基于电子身份规约的业务识别能力，发放业务（比如：便捷通行）对应的 PKI 证书给终端设备，并重新引导网络策略，完成终端设备的二次接入认证。

③ 网络授权

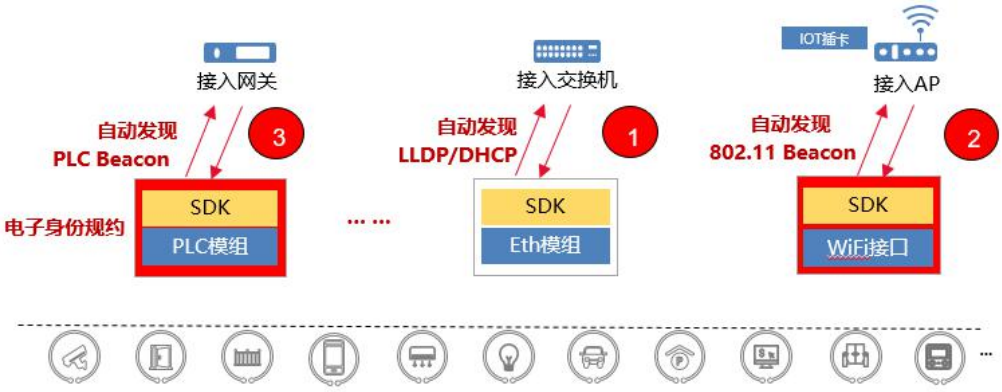
终端设备证书采用 PKI 数字证书进行二次接入认证，AAA 服务器校验证书合法性后，决定准许访问业务。SDN 控制器在发放终端设备的二次认证数字证书时，也会发放新的网络接入点（比如：指定引导到新 AP 或者 SSID），终端设备即可访问新的 AP 或者 SSID。

2. 终端设备电子身份规约

园区终端接入自动化基于终端设备的电子身份规约。其中，电子身份规约标识，包含：设备版本号、厂家信息、产品名称、终端类型、SN、标识符、安全启动、加密算法、传输加密及 option 字段。通过生态集成，构建终端和网络设备的电子身份规约的标记和识别能力。电子身份规约的携带，可以通过以下几种报文：

- 设备发现类的报文，比如：LLDP，DHCP；
- 设备认证类的报文，比如：EAP；
- WLAN，IoT 链路协商报文，比如：Beacon 帧；

3. 自动引导&终端识别



即插即用过程中，园区终端设备通过自动发现，基于电子身份规约，完成终端识别、自动引导入网。具体方式如下：

- 有线园区终端：在设备上线后，通过设备发现协议（比如 DHCP,LLDP 等）中携带的电子身份规约，终端设备响应报文中也携带电子身份规约，设备对接后彼此完成终端设备类型识别；

- WIFI 园区终端：在 WIFI 终端上线后，通过在 WLAN 802.11 帧中扩展字段携带的电子身份规约， WIFI 终端响应报文中也携带电子身份规约，设备对接后彼此完成终端设备类型识别；
- IoT 园区终端：在 IoT 终端上线后，通过在入网消息的扩展字段携带的电子身份规约，园区 IoT 终端响应报文中也携带电子身份规约，设备对接后彼此完成终端设备类型识别；
- 企业园区接入设备和园区终端设备完成设备发现，和终端身份识别后，根据各自的认证策略，完成园区终端设备的入网认证。

4. 园区终端认证方式

通常，园区终端入网认证方式有两种：管理员审批入网和管理员免审批入网。前者在园区终端首次认证时，会将终端信息上报给管理员，管理员通过手动方式选择终端是否可以审批通过。后者免认证方式，则需要管理员通过描述终端上二维码信息，将终端的身份信息录入平台白名单，设备在认证时，完成白名单审核，即可认证通过。无论哪种方式，相对于传统 PC 终端需要安装下载数字证书等方式，园区终端的认证过程结合园区终端数量多、配置麻烦的特征，实现更加简易，基本实现无需在终端上的人工配置，就可以完成接入认证。

- **管理员审批入网流程如下：**

① 在数字平台上，先调用 SDN 控制器接口导入园区终端设备的白名单和对应的终端组；

② 在 SDN 控制器界面上，配置哪些终端组需要审批准入，此处可以选择数字平台自定义的终端组，也可以选择未识别的终端组;

③ 终端接入网络，设备发现和认证报文中携带电子身份规约，认证点提取电子身份证书到 Radius 私有属性中触发 MAC 认证;

④ SDN 控制器识别 MAC 地址需要进行审批准入，则加入待审批列表并呈现终端的电子身份（MAC、接入位置、厂商、产品名称、终端类型、SN），然后通知给数字平台审批;

⑤ 管理员在数字平台上核对终端电子身份的正确性后审批准入，并通知 SDN 控制器审批结果;

⑥ SDN 控制器上将终端从待审批列表中加入到已审批列表中，后续终端 MAC 重认证就会成功;

- **管理员免审批入网:**

SDN 控制器免审批方案,原理是通过定制的 APP 扫描园区终端上的二维码，将终端的身份信息录入到数字平台，数字平台继而将终端白名单同步给 SDN 控制器。终端关联引导 SSID 后触发认证，由于之前数字平台已经将终端白名单同步给 SDN 控制器，终端直接认证成功。管理员可以在终端列表页面查看到已经认证成功上线的终端信息。

SDN 控制器免审批方案相比于需要管理员审批的方案，省去了客户在 SDN 控制器界面的操作，但是增加了客户扫码录入园区终端资产的工作。从安全性角度看，免审批的方案更安全。

（三）终端设备二次认证

对于园区终端设备，园区终端接入解决方案建议采用二次认证，最终自动化的实现端到端的网络业务发放。首次认证让园区终端接入企业局域网，实现基于终端身份识别的认证通道打开，申请合法的入网数字证书，并对合法终端进行二次引导入网，基于申请的合法数字证书重新接入业务网络，获得与园区终端业务匹配的网络权限和 QoS 权限，与应用之间网络打通。

这种二次认证方式，给园区终端用户，在安全方面带来如下价值:

① 园区终端设备由于采用首次认证+二次认证过程，让园区终端更加难以被设备仿冒，杜绝网络侧劫持问题;

② 二次认证后，园区终端根据子系统业务类型，重新引导进入新的一张业务网，各个业务网络之间数据隔离，最大程度降低了子系统终端被攻破后对整体网络安全性威胁;

③ 终端在整个认证过程流量传输加密，采用防窃取、防篡改机制，保证通信高安全性，降低数据被窃取仿冒的风险。

园区终端接入企业园区网络的二次认证过程，如下图 22 所示:

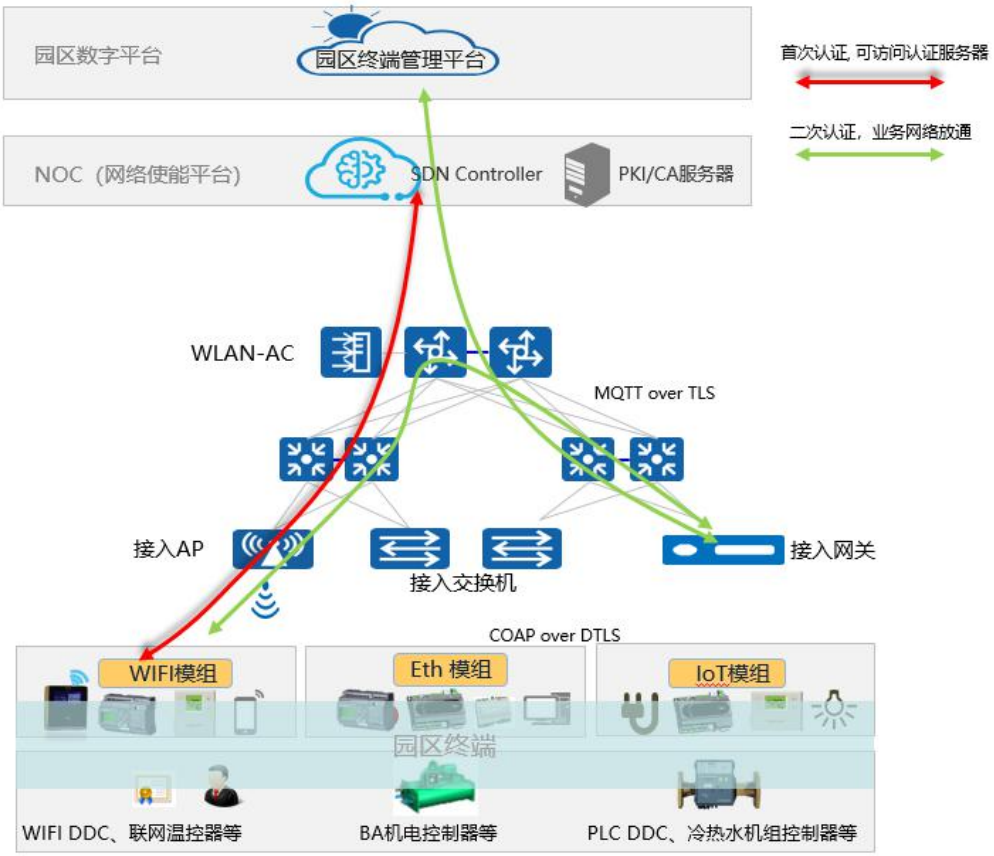


图 22 终端接入企业园区网络的二次认证流程图

如上图 22 所示:

① 终端上线后，通过引导入网后，在 SDN 控制器上，完成对电子身份规约的审核，完成本地认证，从而获得本地网络访问权限。

② 获得本地网络访问权限的终端，仍然没有访问业务的权限。SDN 控制器会根据终端的电子身份规约，到 PKI 服务器中，根据终端类型、业务、访问意图，为其申请对应业务网络的 CA 证书，并发放给终端;

③ 由于业务网络是隔离的，比如园区终端视频监控网，和工厂生产内网之间，建议通过 VxLAN 实现虚拟隔离。所以视频类业务终端，可以在报文中携带申请到的 CA 证书，重新联网

认证，并被引导到新的网络接入点上，比如新的 SSID，进行数字证书认证，这个过程称之为二次认证;

④ 二次认证通过后的终端，就可以连入业务网络，比如与接入网关之间通过 CoAP 协议进行业务交互，并通过接入网关的 MQTT 代理协议转换，访问云端的园区终端管理平台等行为。

（四）终端设备可视可管

园区网络建设后，在园区终端的管理运维上，带来如下新问题和挑战:

① **管理难**：园区终端运维管理平台维护业务状态，不显示联接。网络平台仅能看到网络状态，看不见终端状态；终端拓扑需要手工表格维护。端到端管理依然靠人工串起来维护;

② **问题定位定界难**：终端业务一旦中断，当前故障分析引擎，无从定位到底是网络问题还是园区终端问题;

③ **效率低**：采用人工报障，手工定位方式，手工查 IP，查位置，查通路，效率低。

在 3.1 节园区终端接入解决方案总体架构图 21 中，园区网络的网络使能平台包括如下部件:

- **园区网络控制器平台**

  是面向园区解决方案的 SDN 控制器管理控制系统，可以对园区网络和设备进行集中管控，支持网络业务管理、网络安全管理、用户准入管理、网络监控、网络质量分析、网络应用分析、告警和报表等特性，提供大数据分析的能力，同时提供开放的接口、支持与其他平台集成;

- **园区网络智能分析平台**

是网络的智能分析引擎，将人工智能应用于运维领域，为用户网络提供智能运维服务，辅助客户及时发现网络问题，改善用户体验。

因此，针对园区终端运维管理难的问题，可基于企业现有的园区网络运维管理平台，集成网络使能平台和园区终端运维管理平台。如下图 23 所示：

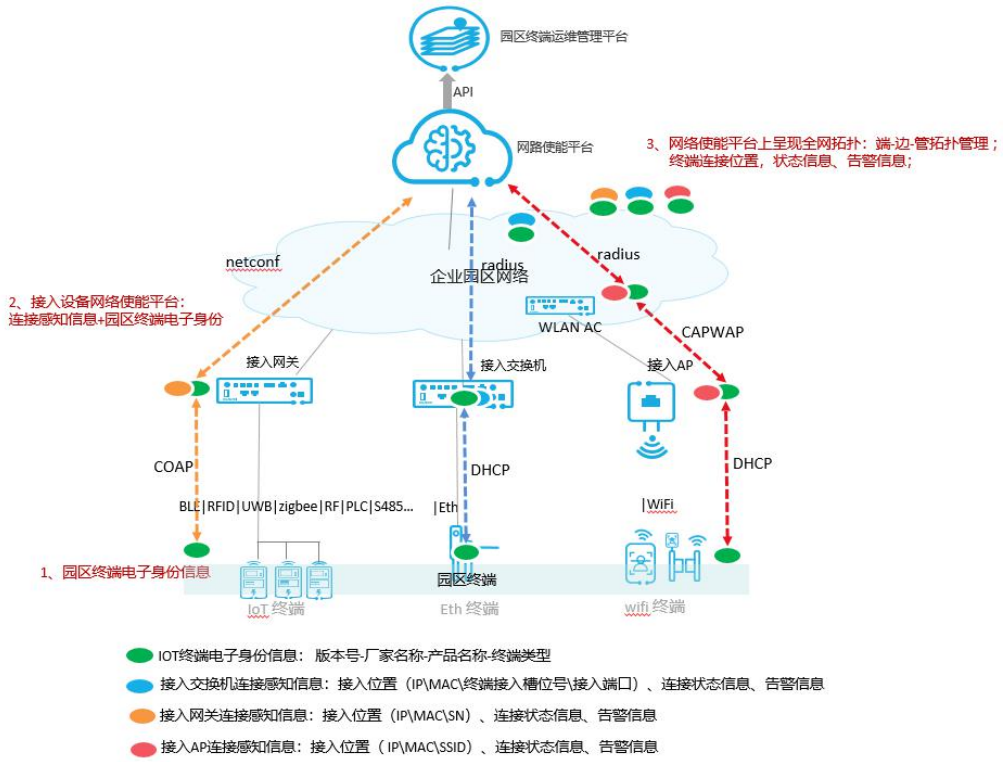


图 23 园区终端可视可管流程图

进一步将以“网络设备管理”为中心转变为以“业务可用性保障”为中心，打造为园区终端业务的运维支撑平台。

四、园区终端接入自动化总结与展望

随着物联网和 5G 通信技术的发展，园区终端数量将会呈现爆发式增长，海量终端的接入自动化就显得尤为重要。同时，随着终端

数量的增多，园区网络会变得越来越复杂，需要有一种极简、智能、安全的园区网络终端接入自动化解决方案，实现终端设备的即插即用、安全可信、可视可管等网络带来安全威胁。

同时，随着企业园区的大规模建设，终端接入自动化方案的研究、规范、部署，需要增强易集成、更安全、业务多样化、配网及运维自动化等核心能力。为进一步适应工业互联网产业园区快速发展，需要在终端接入自动化领域进行创新研究和标准制定。建议园区终端接入自动化分三步走:

① 发布技术白皮书，为园区终端产业提供有用参考

② 联合联盟行业力量，形成园区终端接入自动化最佳实践

③ 标准组织联合（国内通信行业标准、国际 IETF 等），推动产业链协同创新

（一）发布技术白皮书

着眼于工业互联网未来发展，建议先发布园区终端接入自动化技术白皮书，引导研发机构、企业重视在园区终端接入安全自动化领域的技术研究和标准制定，通过关键共性技术、前沿技术，加快园区终端的电子身份规约定义、即插即用、新入网设备和网络的安全认证、授权自动化、轻量级数字证书和协议等新技术新应用的研究和探索，为园区产业提供有用参考。

（二）打造业界最佳实践

园区终端产业具有高度融合、应用多样、发展迅速等特点，其生态覆盖传感器元器件制造、设备集成生产、网络服务提供、软件服务提供、系统集成开发及销售等环节，接入安全问题更是涉及传

感器、芯片、硬件，通信技术、网络服务以及相关行业领域应用等方面，因此构建开放、合作、共赢的园区终端接入安全生态圈是产业发展的必然趋势和要求。

着眼打造园区终端接入自动化和安全生态，建议基于工业互联网联盟平台，在工业互联网的重点行业内开展园区终端接入自动化的测试床应用与创新实践，孵化 UseCase，形成园区终端产业链协同创新的局面，提升我国园区终端安全入网的核心竞争力。

（三）推动产业链协同创新

园区终端接入自动化和安全，是企业园区、终端设备、安全等多个产业发展的重要方向，需要基于产业链进行协同创新。标准化是产业化持续发展的基础，建议由国内工业互联网联盟对接国内行业组织、国际联盟和行业标准组织，比如：中国通信标准化协会 CCSA、互联网工程任务组 IETF、美国国家标准和技术委员会 NIST、欧盟网络和信息安全局 ENISA 等，进一步推动国内园区终端接入自动化的标准化和产业影响力出海。

五、参考文献

[1]全国信息安全标准化技术委员会通信安全标准工作组. 物联网安全标准化白皮书[D], 2019.

[2]中国信息通信研究院. 物联网安全白皮书[D], 2018.

[3]中国信息通信研究院. 工业互联网园区网络白皮书[D], 2020.

[4]中国电子标准化研究院,交通运输部科学研究院,交通运输网络安全技术行业研发中心. 物联网智能终端信息安全白皮书[D], 2019.

[5]上海市经济和信息化委员会,中国信息通信研究院. 5G+智能制造白皮书[D], 2019.

[6]RFC8576. Internet of Things (IoT) Security: State of the Art and Challenges[J], 2019.

[7]RFC8520. Manufacturer Usage Description Specification[J], 2019.

[8]RFC8366. A Voucher Artifact for Bootstrapping Protocols[J], 2018.

[9]RFC3748. Extensible Authentication Protocol (EAP) [J], 2004.

[10] RFC2284. PPP Extensible Authentication Protocol (EAP) [J], 1998.

[11] RFC4388. Dynamic Host Configuration Protocol (DHCP) Leasequery[J]. 2006.

[12] IETF ANIMA WG. Bootstrapping Remote Secure Key Infrastructures (BRSKI) [J], 2020.

[13] IEEE Standard for Local and metropolitan area networks[D], 2005.

[14] Gartner Research. Hype Cycle for IoT Standards and Protocols[J], 2020.

[15] Gartner Research. Magic Quadrant for the Wired and Wireless LAN Access Infrastructure[J], 2019.

[16] IoT Analytics. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

[17] NIST SPECIAL PUBLICATION 1800-15A, Securing Small-Business and Home Internet of Things (IoT) Devices[D], 2019.

[18] European Union Agency For Network And Information Security. Baseline Security Recommendations for IoT[J], 2017.

[19] 物联网智库，挚物 AIoT 产业研究院. 2020 中国物联网产业全景图谱报告[J]，2020.

[20] 中商产业研究院. 2019 年中国工业物联网市场前景研究报告[J]，2019.

[21] 中国产业信息网. 2019-2025 年中国工业物联网行业市场评估及投资前景评估报告[J]，2019.

[22] 沈宁国，于斌。智简网络：园区网络架构与技术[D]，北京：人民邮电大学出版社，2019.

[23] 徐召杰. 物联网中基于双向认证的安全通信协议的研究与实现[D]. 北京邮电大学硕士学位论文，2018.

[24] 李威. 自治网络安全自启动通信机制研究与实现[D]. 重庆邮电大学硕士学位论文，2019.

[25] 韩琪. 云环境下的身份认证与数据安全技术研究[D]. 西安电子科技大学博士学位论文，2018.

[26] 叶墩辉. 基于可信模块视频监控系统的安全双向认证架构设计[D].广东工业大学硕士学位论文, 2016.

[27] 付韬. 基于 EAP 的接入认证协议的设计与分析[D]. 哈尔滨工程大学工学硕士学位论文, 2014.

[28] 林兆鹏,邹起辰. 可信设备接入网络认证协议设计及安全分析[J]. 计算机仿真, 2018.

[29] Dell Inc. IOT SECURITY: CHALLENGES,SOLUTIONS & FUTURE PROSPECTS[J], 2018.

[30] IEC. IoT 2020: Smart and secure IoT platform[J]. http://www.iec.ch/whitepaper/iotplatform.

[31] J. Kanniappan and B. Rajendiran. Privacy in the Internet of Things[D], 2017.

[32] Shancang Li, Li Da Xu. Securing the Internet of Things[J]. 2017.

[33] Miao Yu,Jianwei Zhuge,Ming Cao,Zhiwei Shi,Lin Jiang. Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices[J], 2020.

[34] Anca D Jurcut,Pasika S Ranaweera,Lina Xu. Introduction to IoT Security[J], 2019.

[35] Hany F. Atlam and Gary B. Wills. IoT Security, Privacy, Safety and Ethics[J], 2019.