Introduction to Network Access Control

网络准入控制概论

聂元铭　董建锋　周小平　著

科学出版社

(TP-6006.0101)

网络准入控制概论

www.sciencep.com

ISBN 978-7-03-035257-6

9 787030 352576 >

定 价：48.00 元

网络准入控制概论

聂元铭　董建锋　周小平　著

科学出版社

内 容 简 介

本书系统研究了网络准入控制技术（NAC）的基本原理、主要技术手段、体系架构和解决方案，探讨了下一代网络准入控制技术的发展方向，提出了建设NAC项目的实施方法和关键要素，给出了颇具代表性的实际应用案例。

本书适合信息网络安全技术研发和应用人员使用，亦可供信息网络安全管理和维护人员学习参考，并可作为大学相关专业教材。

图书在版编目(CIP)数据

网络准入控制概论/聂元铭，董建锋，周小平著. —北京：科学出版社，2012

ISBN 978-7-03-035257-6

Ⅰ.①网… Ⅱ.①聂…②董…③周… Ⅲ.①计算机网络-安全技术-研究 Ⅳ.①TP393.08

中国版本图书馆CIP数据核字（2012）第182812号

责任编辑：王淑兰/责任校对：王万红

责任印制：吕春珉/封面设计：耕者设计工作室

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2012年8月第 一 版 开本：B5（720×1000）

2012年8月第一次印刷 印张：14 1/2

字数：285 000

定价：48.00元

（如有印装质量问题，我社负责调换〈双青〉）

销售部电话 010-62136131 编辑部电话 010-62130750

前　言

伴随着社会信息化步伐的不断提速，网络正全方位地改变着我们的工作、生活以及娱乐方式。发展初期的网络注重设备的互通性、链路的可靠性，从而达到信息共享的通畅。经过多年的应用与发展，伴随着人们对网络软硬件技术认识的深入，网络安全已经超过人们对网络可靠性、交换能力和服务质量的需求，而网络的可信接入更成为网络安全的最重要环节，因此研究网络安全准入控制技术具有非常重要的现实意义。

在内网中，新的安全威胁不断涌现，任何一台终端的安全状态，都将直接影响到整个网络的安全。不符合企业安全策略的终端，如防病毒库版本低、补丁未升级、非法终端接入和违规外联等情况，最终的结果可能是全网瘫痪，所有终端都无法正常工作。如何确保网络中的终端安全状态符合企业安全策略，防止内部网络系统遭受非法入侵，防止终端身份伪造，成为构建可信网络的一大难题。通过网络准入控制系统对内网终端边界进行防护，可实现“身份认证—安全检查—隔离修复—访问授权”的一体化终端入网流程管理，对接入网络的终端实现安全准入控制，使每个入网终端均满足安全管理的基准线是网络准入控制技术的重要作用。

本书共有 7 章。从基本概念、技术原理和运行机制等方面，阐述了网络准入控制技术所涵盖的内容，并深入研究分析了网络准入控制技术的主要手段、技术架构、解决方案和网络准入控制项目的建设实践，旨在使读者了解网络准入控制技术的内涵与外延，掌握网络安全准入控制实用技术，解决网络安全管理问题，提高信息网络安全的效益和效率。

本书技术数据在盈高科技网络准入控制实验室通过验证，并在第 7 章列举了盈高科技实施的工程案例。本书写作过程中，得到了孙桂芝、常明、叶启平、翟寅川、杨军、罗治华、张婧、张优扬、汪丽娟、刘璇、韩金龙的大力支持，特别是参与本书部分章节资料整理和文字校对工作的李力、何俊、龙杨、袁宏宇、张明、王建鑫、赵思成等人为完成书稿做出了突出贡献，在此表示真诚的感谢。

由于作者水平所限，书中错误和疏漏在所难免，诚请读者予以指正。

作　者

2012 年 8 月

目　录

第 1 章　网络准入控制技术基础

网络准入控制（Network Access Control，NAC）是目前一种新型的安全防御技术，它通过对终端实施安全防护，可以有效地解决因不安全终端接入网络而引起的安全威胁，将病毒、蠕虫等各类攻击拒绝于网络之外，从而真正保障网络的安全。目前，对网络准入控制还没有一个权威、统一的定义，甚至其名称也有各种叫法，如网络接入控制、终端准入控制、终端安全接入、安全接入控制，等等。专业人员普遍认为，网络准入控制是一套可用于定义在节点访问网络之前，如何保障网络及节点安全的协议集合。该技术的核心概念是从网络终端的安全控制入手，通过消除终端的不安全因素或将其减少到最小，从而保护网络和终端的安全。

网络准入控制的主要思路是：终端接入网络之前应根据预定安全策略对其进行检查，只允许符合安全策略的终端接入网络，而将不安全的终端隔离于网络之外，自动拒绝不安全的主机接入受保护网络，直到这些主机符合网络内的安全策略为止。

具体来说，网络准入控制技术是通过使用用户身份认证手段，对用户的接入设备进行状态评估，实现对用户属性、在线状态、流量限制的全面管理与掌握。在企业、机构网络环境中，由于缺乏有效的管理与控制，网络安全形势日趋严峻，即使部署了防火墙、漏洞扫描系统、入侵检测系统和防病毒软件等安全防线，攻击网络的现象仍然层出不穷，网络的可用性难以保证。在众多的网络安全事件背后，普遍存在的事实是管理者不能及时掌握用户属性、在线状态、流量使用情况等，网络用户若没有及时安装系统补丁和升级病毒库，每个网络用户都可能成为网络攻击的发起者，同时也是受害者。因此，只有采用网络准入控制技术，通过用户身份认证手段，对用户的接入设备进行安全状态评估，使每个接入点都具有较高的可信身份和基本的安全条件，才能达到高效、安全、全方位地保护内部网络安全的目的。

1.1　网络准入控制技术背景

随着 IT 技术的不断进步，信息一体化带给人们的双刃剑效应也越来越明显，人们在体验到信息高速公路的便捷高效的同时，也会遭受到各种各样的威胁和风险带来的损失，信息安全问题越来越显得突出。据 CSI/FBI 安全报告称，虽然安全技术多年来一直在发展，且安全技术的实施更是耗资数百万美元，但病毒、蠕虫、间谍软件和其他形式的恶意软件仍然是各机构现在面临的主要问题。每年遭

遇的大量安全事故造成系统中断、收入损失、数据损坏或毁坏以及生产率降低等问题，给企业和机构带来了巨大的经济影响。

在当今这个多样化的、动态的全球网络环境中，对于试图接入企事业单位网络的可管理或不可管理的设备，网络管理员根本无法在其接入网络前知晓它们的来源。面对手段高明、资金雄厚的黑客，用户设备很可能在不知不觉间已经感染致命的恶意软件。随后，用户设备就作为一种传输媒介，在网络上传播病毒、间谍软件、广告软件、特洛伊木马、蠕虫、木马后门、bots、rootkits 和其他形式的恶意应用，或将它们直接传染给不设防的其他用户设备。感染任何此类恶意应用都将威胁到企事业单位的信息资产安全，使企业付出惨重的代价。

与此同时，随着 Internet 的快速发展，在电子政务和电子商务应用快速发展的今天，Intranet 作为 Internet 技术运用于单位、部门和企业专用网的产物，也得到迅速普及发展。这些单位、部门和企业的办公和生产对信息化的依赖程度越来越高，对信息网络安全要求也越来越高。众所周知，Intranet 并非是地域上的概念，而是在信息空间上的虚拟网络概念，如一个国家外交系统的内域网用户可能分布全球。它在原有专用网的基础上增加了服务器、服务器软件、Web 内容制作工具和浏览器，与 Internet 连通，从而使内域网充满了生机和活力。随着信息网络的迅速发展，企业的信息网络规模越来越庞大，信息接入点就越来越多。内域网为公司和单位信息的散播和利用提供了极为便利的条件。浏览器为网上用户提供信息，服务器对网络进行管理、组织和存储信息，并提供必要的安全服务。通常情况下，Intranet 中存有大量的单位内部的敏感信息，具有极高的商务、政治和军事价值。

因此，Intranet 应该说是一种半封闭甚至是全封闭的集中式可控网，所以其安全保密是至关重要的。要保证内域网不被非法入侵和破坏，网中的敏感信息不被非法窃取和篡改，同时还要保证网内用户和网外用户之间正常连通，并向他们提供应有的服务。但是从当前的实际情况来看，内网中技术手段和有效的安全机制相对落后或缺乏，这必然造成难以杜绝不符合安全规范的终端接入网络中情况的发生，这些终端都将成为传播病毒的源头和被病毒感染的对象，影响内部信息网络和终端的可利用率。

目前，大部分网络的安全管理重点是放在了防范来自外部的攻击上面，主要依赖于防火墙、入侵检测、防病毒软件等。事实证明，企事业单位内部的不安全因素远比外部危害更恐怖。据权威统计显示，83%的信息安全事故是由内部人员和内外人员勾结所为，80%以上的企事业单位内部网络曾遭受过病毒的肆虐，60%以上的企事业网站受过黑客的攻击，从这一些数字足见内部网络安全管理问题的重要性。可以说，网络内部漏洞给重要资源造成的威胁远远大于从互联网穿越防火墙造成的入侵，而传统的防护技术，如防火墙、IDS 等均无法有效地对内部漏洞进行防范。显然，如果不能相信所有的用户都能正确、合法地使用网络，这就有必要进行适当的访问控制，最基本的要求就是采用确定的机制对通信实体

和网络用户进行可靠的认证和控制。这些安全业务都需要建立健全一个完善的网络准入控制机制。

正如上面所说，对于政府机关、金融机构、各种企事业单位，虽然其内部网络基本上与互联网隔开，但仍会受到病毒、黑客等网络危害的影响，而且一旦其信息系统受到破坏，产生的经济以及社会影响相当巨大，甚至会波及到每个人的切身利益。对于这种网络覆盖面广、应用复杂、计算机终端数量众多的内网来说，很大一部分安全隐患来自内部。网络安全管理上往往面临以下这些问题。

1. 单位资产，员工私产——资产管理失控

网络中终端用户随意增减调换，每个终端硬件配备（CPU、硬盘、内存等）肆意组装拆卸、操作系统随意更换、各类应用软件胡乱安装卸载，各种外设（软驱、光驱、U 盘、打印机、Modem 等）无节制使用。

2. 网络无限，自由无限——网络资源滥用

IP 地址滥用，流量滥用，甚至工作时间聊天、游戏、赌博、疯狂下载、登录色情反动网站等行为影响工作效率，影响网络正常使用。

3. 蠕虫泛滥，业务瘫痪——病毒蠕虫入侵

由于补丁不及时，网络滥用，非法接入等因素导致网络内病毒蠕虫泛滥、网络阻塞、数据损坏丢失，而且无法快速查找定位和隔离感染病毒或表现异常的计算机终端，无法找到灾难的源头以迅速采取隔离等处理措施，导致处理病毒和异常事件效率不高，从而为正常业务带来灾难性的、持续性的影响。

4. 脆弱防线，外强中干——终端安全隐患

内部网用户计算机终端的安全补丁和杀毒软件病毒库更新缺乏有效的检查和管理手段，无法有效地防范病毒入侵内部网；每个终端漏洞密布、口令简陋且经年不改，管理员无法时刻检查、提醒或强制解决，为蠕虫、泄密等灾难埋下了各种隐患。

5. 门户大开，长驱直入——外部非法接入

移动设备（笔记本电脑等）和新增设备未经过安全检查和处理违规接入或者入侵内部网络，带来病毒传播、黑客入侵等不安全因素；对用户计算机终端接入内部网缺乏有效的管理和控制，致使外来笔记本等不安全设备可随意接入内部网，对内部网的安全造成威胁。

6. 外贼好治，家贼难防——内部非法外联

内部网络用户计算机终端通过调制解调器、双网卡、无线网卡等设备进行在

线违规拨号上网、违规离线上网等，将企业内部网与外部不安全的网络系统（如互联网）联在一起，可能会使黑客进入到内部网，并使计算机感染病毒；或违反规定将专网专用计算机带出内网进入到其他网络。

7. 网络无界，一损俱损——重要信息泄密

因系统漏洞、病毒入侵、非法接入、非法外联、网络滥用、外设滥用等各种原因与管理不善导致组织内部重要信息泄露或毁灭，造成不可弥补的重大损失。

8. 千里之堤，毁于蚁穴——补丁管理混乱

终端用户不了解系统补丁状态，不及时打补丁，也没有办法统一进行补丁的下载、分析、测试和分发，从而为蠕虫与黑客入侵保留了通道。

因此，大家应该看到，网络中连接的各个用户终端设备已成为影响当前网络安全的重要因素。这一点在国内的网络安全行业中同样十分明显，从以下的几点安全动态中就可见一斑。

1.1.1 安全动态

1. 安全动态之一

上海某上市企业（全球500强合资公司），生产基地包括4个工厂，网络内有超过1000台终端设备，经常发生网内ARP攻击事件，导致业务系统中断。后查明是机器不受管控的随意接入，其自身由于感染ARP病毒，影响和攻击到了全网内正常工作的机器，造成重大安全事故。

2. 安全动态之二

国家电网某省分支机构，购买了某品牌的终端管理软件，并从单位层面规定必须安装此软件后入网。但由于各种原因（用户私自卸载、重装系统、与其他软件冲突等）导致全网的软件部署率极低，并曾由于此系统与某安全软件冲突而无法运行，导致大部分用户无法入网。

3. 安全动态之三

2010年3月，微软IE浏览器出现“零日漏洞”——KB981374，该漏洞被大量挂马网站利用，漏洞影响范围包括IE6、IE7。未安装相关安全补丁的用户电脑一旦被攻击成功，将会感染木马下载器、黑客后门，使得电脑无法正常工作，并导致个人账号密码等隐私信息被窃取。

4. 安全动态之四

2011年2月，某省厅级单位有效阻断**木马病毒风险百余次，阻断入侵攻击**

1700 余次。

1.1.2　风险分析

上述的安全事件表明，对于各机构的内网而言，现在存在的十分常见（或应该引起重视的）的网络安全风险点包括以下几个方面。

1. 入网设备及人员控制（参见安全动态之一）

如果对于单位的网络接入无法进行控制，非法机器插上网线后能随意接入网络，就会**造成进入网络窃取机密信息的危险，这将对网络中的涉密信息造成严重威胁**；另外，如果非法机器带毒入网，极有可能成为木马或蠕虫病毒威胁内网的跳板并造成重大安全事件。

2. 入网规范性控制（参见安全动态之二）

许多单位已经制定了一套内部网络管理规范，如禁止私自修改 IP 地址，禁止安装游戏或非业务软件，禁止随意保存或修改某些涉密文档等，但规范无法真正落到实处，许多用户依然我行我素，网络管理员无法对接入计算机的使用和软件安装情况进行整体管理，网络中的各类违规行为增加了管理的难度，甚至有可能造成涉密的安全风险。

3. 补丁、杀毒软件等漏洞控制（参见安全动态之三、四）

由于机构分散，部分员工整体安全意识不足又无法及时得到培训和管理，接入终端不及时升级系统补丁、不安装杀毒软件或杀毒软件不及时升级病毒库的现象普遍存在，无法对这些安全规范进行统一强制管理，这种情况下，安全性低下的单台终端同样容易成为影响全网的威胁来源和跳板（如 ARP 病毒攻击），或无法对入侵及病毒威胁进行有效的抵御，从而带来潜在的安全风险。

另外，员工计算机水平参差不齐，许多人面对计算机出现的故障无法进行及时修复。由于网点数多、范围分散，计算机出现问题后管理员需要频繁奔赴现场进行维护，工作效率低下。

4. 全网安全性审计——报告及审计需要

如果无法对入网设备进行安全性的整体评估，网络管理者就无法整体了解内网的安全性。由于无法确定设备安全性，造成无法确定和定位网络中的风险点，在安全事故发生时就无法明确相应的责任人，网络管理及维护者往往成为普通用户计算机安全漏洞的责任承担者。

由计算机安全协会（Computer Security Institute）与美国联邦调查局（FBI）联合进行的计算机安全报告显示，目前内网遭遇的主要威胁有病毒、蠕虫、间谍软件和其他形式的恶意软件，而这些威胁大都由不安全终端接入所引起。终端安

全接入是目前一种新型的安全防御技术，它通过对终端实施安全防护，可以有效地解决因不安全终端接入网络而引起的安全威胁事件，将病毒、蠕虫等各类攻击拒绝于网络之外，从而真正保障网络的安全。

在国内，直到近几年上述问题才逐渐引起管理者的重视，作为网络安全防范的源头，如何阻止非法用户接入网络，如何限制用户的安全行为，如何加强内部用户的网络接入控制已成为各个部门建立信息网络安全防御体系必须重点考虑的问题。目前，解决这一问题的有效方法就是利用交换机自身带有的功能，通过一定的配置，将网络准入控制应用到网络中，从而达到控制效果。解决这一类内网安全问题的方法被称为网络准入控制（Network Access Control，NAC）。

1.1.3 实施意义

网络准入控制体现了病毒防治、补丁修复、系统维护等终端安全防护措施与接入控制、身份认证、权限控制等网络准入控制手段的结合，体现了主动防御、整体安全的理念。网络准入控制解决方案可提供广泛而深入的功能，因此不仅涉及整个内网，而且还适用于内部组织机构和职能部门。网络准入控制技术的部署从桌面系统管理到桌面系统安全性、从网络基础设施到网络管理，几乎跨越整个IT 领域。实施网络准入控制需要部署网络接入控制机制，网络策略通常基于用户身份、设备标识、设备运行状况以及设备位置等的制订。

实施网络准入控制不仅可同时确保用户和设备以适当方式通过适当连接接入适当网络，还可确保用户满足验证策略的要求、用户设备满足验证和安全策略的要求，以及用户和设备同时满足企事业单位制订的任何其他策略的要求。最直接的一个实施效果就是通过对接入企业局域网用户的认证，可以有效地拒绝不合法用户进入局域网内。例如，当有外来人员来到该企业后打算上网，他直接用网线链接网口将无法连接网络，即使他参照上网的计算机设置 IP 地址，由于得不到认证也不能连接网络。他必须向网管员申请后，由网管员对该计算机进行接入认证后，才能连接网络，同时也对分配的账户设置了限制权限，实现了控制源头和接入管理，从而能够更好地保障企事业网络的信息安全。

网络安全事件的源头产生于内网的情况越来越多，保障内网安全的前提和基础是网络准入控制技术。这里通过一个实例来说明网络准入控制系统都能够解决哪些具体问题。图 1-1 所示的是一个典型的中型企业内网的拓扑结构。

通过图 1-1 可以看出，该企业内网划分为多个 VLAN，各 VLAN 的终端主机通过接入交换机接入网络，各 VLAN 之间通过三层交换机互连。同时，用户内网通过防火墙与广域网互联，实现外网与内网的逻辑隔离与访问控制。这样典型的网络结构虽然具有一定程度的安全性，但对于来自于内网的威胁没有很好的防范措施。

针对以上典型网络，网络准入控制解决方案可以解决用户的如下需求。

（1）防止有安全隐患的电脑或者非法电脑直接访问内部网络，发现并限制非

图 1-1　典型中型企业内网拓扑结构图

法外来主机接入内部网络，以免对内部网络造成危害。

（2）自行定义多种准入控制策略，加强内网接入设备的管理，合法主机的注册与审批入网，提供审批流程。

（3）内网 IP 地址管理，IP 与 MAC 地址的绑定，可依据 IP/MAC/主机名以及资产的配置对接入设备快速定位，以及防止地址冲突、网络扫描、ARP 欺骗等攻击对内网的危害。

（4）对合法主机的身份认证，以及接入后的访问控制，防止对网络资源的非授权访问和滥用。

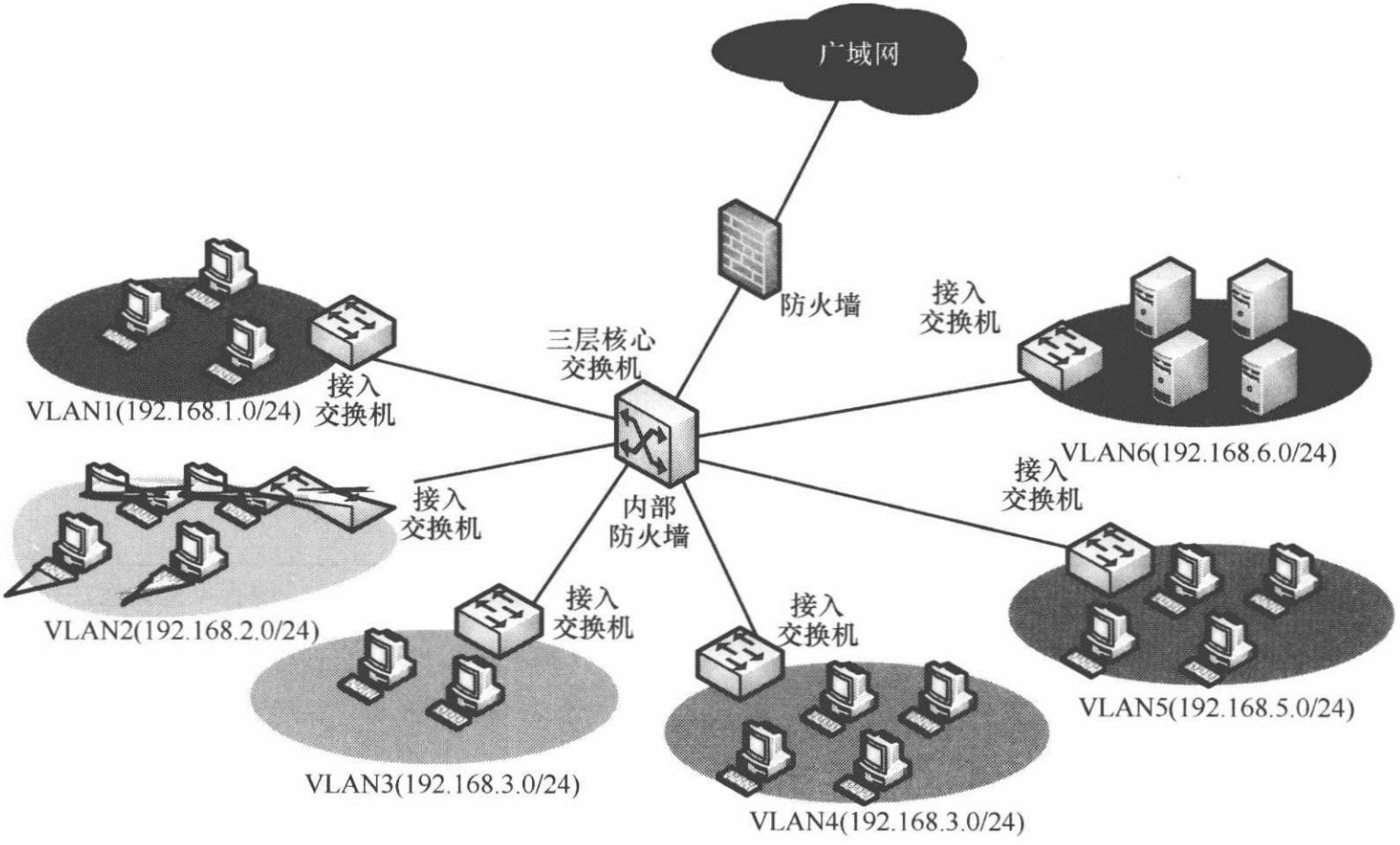
（5）自动发现网络上的所有接入设备，对合法主机安全状态实时检测，如果发现主机存在安全风险或者用户进行了违规操作，可以隔离违规主机。

（6）检查桌面 PC 是否安装了非法软件，不允许禁止运行非法进程等；对 Modem 拨号、同时使用内外网卡等非法操作的监控、审计和禁止使用。

（7）及时发现安全设置不完善或存在安全隐患的 PC 机，对被存在风险的被隔离主机提供补丁漏洞自动修复、操作系统补丁和 MS 应用软件补丁自动更新和针对登录口令强度、Guest 账户、屏幕保护检测，加固主机安全性等必要的加固措施等。并能够形成报表，用于提示系统管理员和用户要采取的弥补措施。

总体而言，网络准入控制作为内网网络边界的第一道防线，为构建可信、安全、高效的内部网络环境提供了必要的基础支撑。

随着对网络安全问题的日益重视，网络准入控制采用的技术手段正在不断发展和更新，安全防范理念也在不断完善。目前，实现网络准入有多种方法，从这


广域网
防火墙
三层核心
交换机
内部
防火墙
接入
交换机
VLAN1(192.168.1.0/24)
VLAN2(192.168.2.0/24)
VLAN3(192.168.3.0/24)
VLAN4(192.168.3.0/24)
VLAN5(192.168.5.0/24)
VLAN6(192.168.6.0/24)

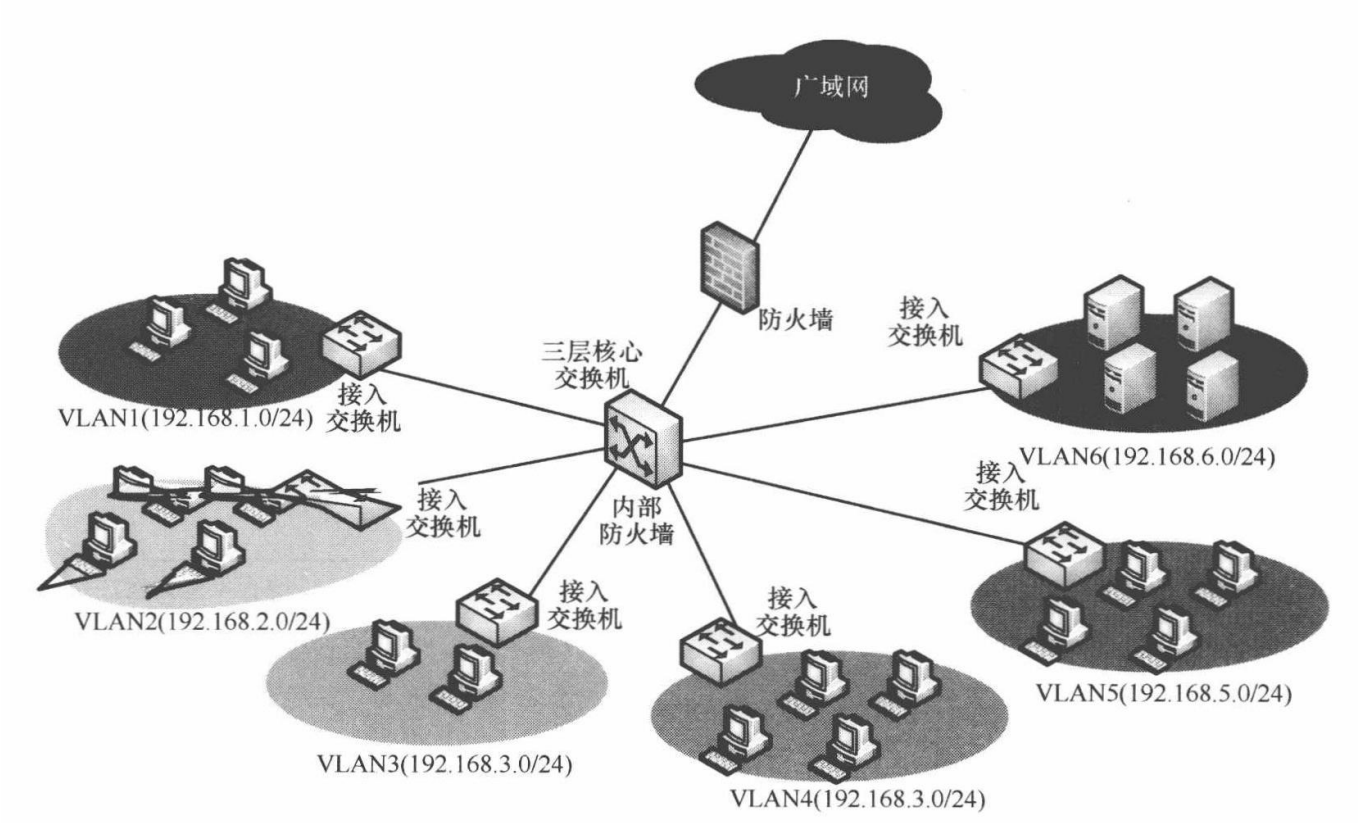


图 1-1　典型中型企业内网拓扑结构图

法外来主机接入内部网络，以免对内部网络造成危害。

（2）自行定义多种准入控制策略，加强内网接入设备的管理，合法主机的注册与审批入网，提供审批流程。

（3）内网 IP 地址管理，IP 与 MAC 地址的绑定，可依据 IP/MAC/主机名以及资产的配置对接入设备快速定位，以及防止地址冲突、网络扫描、ARP 欺骗等攻击对内网的危害。

（4）对合法主机的身份认证，以及接入后的访问控制，防止对网络资源的非授权访问和滥用。

（5）自动发现网络上的所有接入设备，对合法主机安全状态实时检测，如果发现主机存在安全风险或者用户进行了违规操作，可以隔离违规主机。

（6）检查桌面 PC 是否安装了非法软件，不允许禁止运行非法进程等；对 Modem 拨号、同时使用内外网卡等非法操作的监控、审计和禁止使用。

（7）及时发现安全设置不完善或存在安全隐患的 PC 机，对被存在风险的被隔离主机提供补丁漏洞自动修复、操作系统补丁和 MS 应用软件补丁自动更新和针对登录口令强度、Guest 账户、屏幕保护检测，加固主机安全性等必要的加固措施等。并能够形成报表，用于提示系统管理员和用户要采取的弥补措施。

总体而言，网络准入控制作为内网网络边界的第一道防线，为构建可信、安全、高效的内部网络环境提供了必要的基础支撑。

随着对网络安全问题的日益重视，网络准入控制采用的技术手段正在不断发展和更新，安全防范理念也在不断完善。目前，实现网络准入有多种方法，从这

些方法出发，不同的IT厂商各自推出了不同的实现方案。这些方法与方案还在不断完善中。网络准入控制技术今后的发展方向将是适应各种不同的复杂的网络环境，以及在准入过程中结合其他的网络管理要求，实现灵活的网络安全控制策略。研究新型终端安全接入技术对于新一代可信网络设备的研制，可信网络软件的设计，以及新一代网络安全防护技术的研发都具有重要的意义。

1.1.4 技术特点

网络准入控制技术主要解决网络终端合规性控制及其可信接入问题，与其他传统网络安全产品对比详见表1-1。

表1-1 NAC系统与传统安全产品对比表

对比项目	网络准入控制系统	防火墙	入侵防御	桌面安全管理
简介	为解决内网中，各种类型的设备入网身份认证、安全状态检测、修复而建设的系统平台。 网络准入控制系统提供了一整套覆盖全网端点的安全管理平台，从设备入网、安全检查、隔离、修复等整个周期进行安全管理	防火墙英文名称为FireWall，是指位于计算机和它所连接的网络之间的硬件或软件，也可以位于两个或多个网络之间，比如局域网和互联网之间，网络之间的所有数据流都经过防火墙。通过防火墙可以对网络之间的通信进行扫描，关闭不安全的端口，阻止外来的DoS攻击，封锁特洛伊木马等，以保证网络和计算机的安全	网络入侵防御系统作为一种在线部署的产品，提供主动的、实时的防护，其设计目标旨在准确监测网络异常流量，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断，而不是简单地在监测到恶意流量的同时或之后才发出告警	为解决桌面安全管理而设立的一套软件系统（硬件很少）。 桌面安全管理功能点很多，主要从资产管理、软件和补丁分发、应用软件管理、网络行为管理、行为审计等多个功能模块组成
定位	随着政策法规的要求，以及内网中各种安全事件的不断增加，在政府、电力、金融、电信及大型企事业单位日益成为迫切建设平台	作为网络安全建设的重要组成部分，防火墙系统是必须要建设的。 然而防火墙只能解决网关级的特定需求，网络安全建设决不仅仅是买几台防火墙	已成为网络安全建设的重要组成部分，在政府及高端行业以成为普遍配备的系统	作为终端安全管理的重要手段之一，桌面安全管理已越来越重要，但由于研发门槛不高，导致产品品牌众多，产品质量良莠不齐，因此，选择一款真正稳定、可靠的产品是最重要的
性能要求	主要从控制容量：200、500、1500、3000、5000等每分钟上线率等来考虑，对可靠性、稳定性要求很高。 高端产品一般采用硬件级解决方案，在多协议支持、双机热备、无单点故障、大容量支撑上有重点解决	主要从安全性、网络性能：百兆、千兆等两方面来考虑，对可靠性、稳定性要求很高。	主要从安全性、网络性能：百兆、千兆等两方面来考虑，对可靠性、稳定性要求很高	主要从服务器承载终端数进行考量，还有客户端的性能。 由于桌面安全产品尚无相应的标准，一般采用纯软件形式，并且客户端所处的环境千差万别，各个厂商的研发实力差别很大，因此，相对而言，该系列产品的稳定性、可靠性要较弱

续表

对比项目	网络准入控制系统	防火墙	入侵防御	桌面安全管理
功能要求	解决网络层面上，所有入网设备的身份认证，安全状态的检查、隔离，以及不安全设备的修复等功能	重点解决内外网交换数据上的端口控制、访问控制等功能，实现如：地址转换、IP/MAC 绑定、静态和动态路由、源地址路由、代理、透明代理、ADSL 拨号、VPN 接入等功能	重点实现内外网交换数据上的入侵行为检测、防护，提供应用层的防护，以及对于内容级的管理，如阻断间谍软件、木马、P2P 下载等	桌面安全管理实现的功能非常多，基本上跟桌面相关的功能，都可以归入该系统，由此带来另一个问题，即功能很难达到精细、专业的标准。如资产管理很难和一套专业的资产管理平台相比，上网行为审计很难和专业的审计平台相比，甚至桌面管理平台还带有桌面准入、桌面防火墙、桌面 IPS 等功能，但其功能、性能不能和专业设备相比
发展趋势	随着等级保护、SOX 法案及内网安全管理需求的日益提升，网络安全准入控制系统已成为网络安全建设的重要组成部分，且为内网安全系统建设最为迫切的要求	防火墙已是一个成熟的市场，正常发展	IPS 市场是一个快速发展中的市场	市场需求虽然不断增加，但是桌面产品普遍功能模块太多，总体可靠性和专业性不高，和准入控制、防火墙、IPS 等专业性产品差距较大

1.2　网络准入控制技术发展

近年来，在网络安全管理实践中人们发现，安全事件的源头产生于网络内部的情况越来越多。比如，不明身份计算机的随意接入网络导致关键数据的外泄，一台染有 ARP 欺骗类病毒的计算机造成整个局域网的瘫痪，移动存储造成病毒的传播等。因此，如何确保网络内部的安全已经越来越受到人们的重视。作为内网安全保障的前提和基础，网络准入技术成为研究、应用与实践的热点。

随着对网络安全问题的日益重视，用户接入控制采用的技术手段在不断发展和更新，安全防范理念也在不断完善，市场上实现准入控制的技术方法很多，从这些技术方法出发，各 IT 厂商研发了很多各具特色的方案。这些技术方法与应用方案各适合于不同的网络环境和应用要求，还没有哪一种处于绝对领先的状态。从国外的 NAC 技术发展分析，以思科为主导的 NAC 领导产商，提出了更先进的技术框架与实现模型。目前，从控制层次的角度来分析网络准入控制技术主要分为两类：基于网络层的用户控制和基于应用的综合接入控制。总的来说，

随着网络应用技术的不断发展，企业用户正在逐步加强各自的信息网络安全建设，用户接入控制作为信息网络安全防范的源头，随着信息安全理念和技术的日益深入，其实施方法已经从原先的简单基于网络层的接入控制向基于应用的综合接入控制转变，实施手段从原来的单一的安全手段向一套整体的网络安全防御体系解决方案转变，在网络安全体系建设中起到越来越重要的作用。

而在网络准入控制发展的过程中，由于各家厂商利用标准的或私有的各种准入控制协议（标准的如 ARP 技术、DHCP 技术，私有的如 Cisco 的 EOU 技术），并且在整个准入控制的框架中利用了多种组成成分（如交换机、路由器、客户端、各种功能定位的服务器），因此整个网络准入控制行业的阵营逐渐得到了划分。

国际权威的评测机构 Forrester 对整个 NAC 行业按照核心技术的选择划分为 3 大阵营。

（1）Software-Based NAC（基于端点 Endpoint 技术协议的 NAC 系统架构）。

（2）Infrastructure-Based NAC（基于基础网络设备的 NAC 系统架构）。

（3）Appliance-Based NAC（基于应用设备理念的 NAC 系统架构）。

在 2008 年第三季度的独立调查报告“The Forrester Wave：Network Access Control，Q3 2008”中，Appliance NAC 解决方案被评价成网络访问控制领域的领跑者。Forrester 重点集中在不同的访问控制场景中进行评估，总共在 12 个不同场景中评估了各个供应商的解决方案，同时还在技术、战略和市场表现方面进行了对比。

Forrester Wave 的版权属于 Forrester Research Inc.。Forrester 和 Forrester Wave 是 Forrester Research Inc. 的商标。Forrester Wave 是 Forrester 的一个关于某一市场的图示分析，其中通过详细的电子表格列出了评分、权重和注释。Forrester 并不会为任何在 Forrester Wave 中描述到的供应商、产品或服务做宣传或广告。信息都来自于最容易获取的资源。其中的观点是当时的判断，可能随时间的发展而发生变化。图 1-2 是 Forrester 对国外主流 NAC 产商从技术框架、产品战略和市场表现等方面做的集中对比分析。

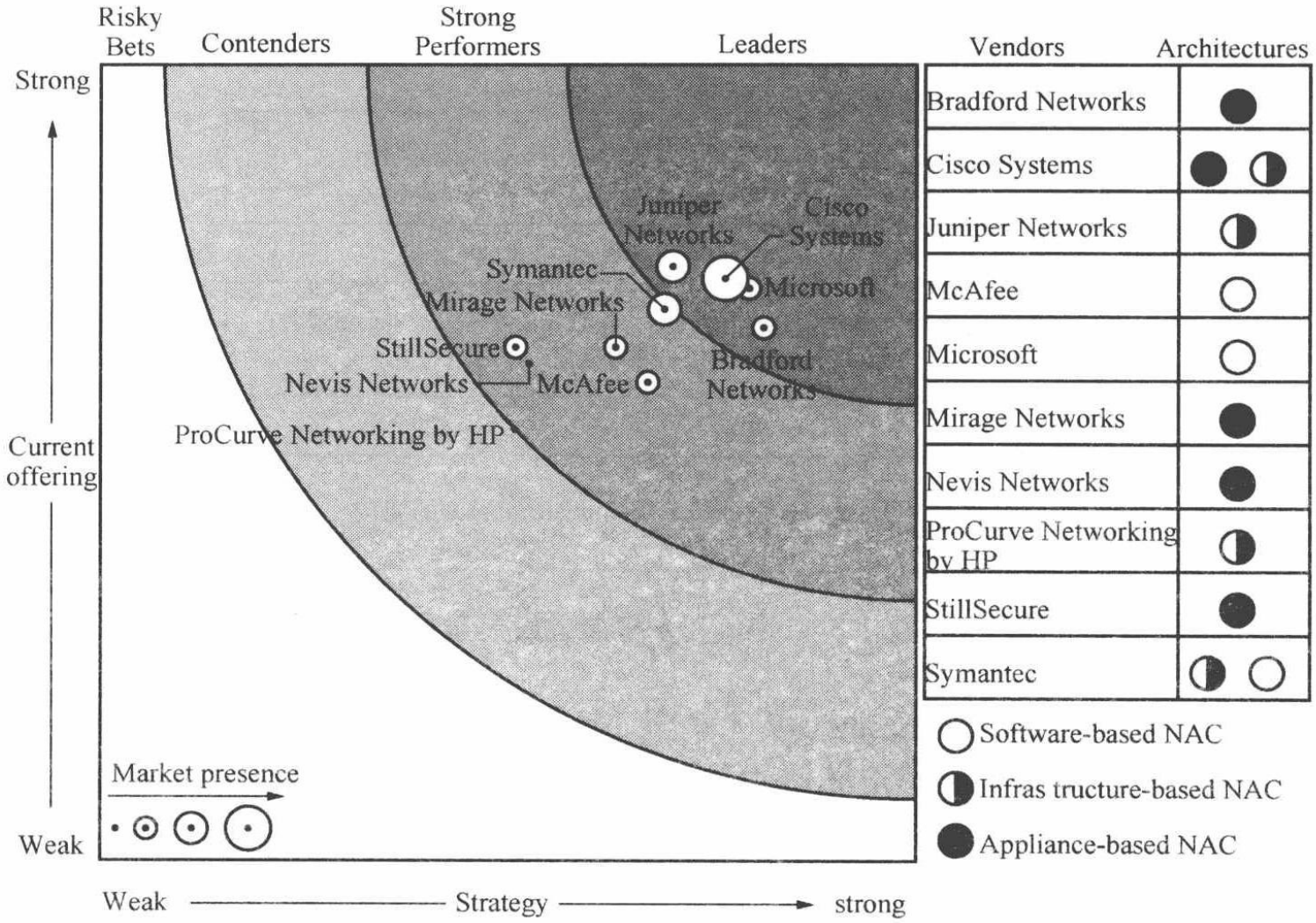
总体上看，Software-Based NAC 属于利用网络中的接入终端自行实施控制的准入架构，符合此类技术架构比较常见的是 ARP 欺骗技术；Infrastructure-Based NAC 是较为传统，也是应用范围最广的准入架构，其经典的实现方式就是 802.1x；而 Appliance-Based NAC 则属于行业领导厂商掌握的技术架构，其核心理念是用单台设备完成 90%以上的 NAC 所具备的功能，这种前沿性技术带来的益处十分明显，包括大大缩短部署时间、降低维护成本、增强对接入用户的友好性等。

图 1-2　集中对比分析示意图

1.2.1　三代技术框架的发展

网络准入控制技术也是随时网络技术的发展，信息安全技术的发展，经历了几代技术框架的变迁。如图 1-3 所示。从早期的完全基于 Agent-Based 框架的 NAC，主要采用类似 ARP 欺骗技术、主机防火墙（TDI、NDIS）技术、DNS 协议拦截技术等，这种基于 Software-based 的 NAC 相对来说最具有伸缩性，也是最低廉的方案。但是对于如果无法安装 Agent 的网络设备就无法控制，并且如果不安装Agent也很容易绕开 NAC 的控制接入网络，同时不能很好地给用户提供友好的体验，无法对来宾做管理。

随着网络技术的发展，很多网络交换厂商为了让他们提供的基础网络方案增值，发展了基于网络交换设备的网络准入控制技术框架（Infrastructure-based NAC)。此方案主要是网络设备（交换机、路由器或者防火墙）联动，整合 Radius 服务，设备启用相关协议由设备进行控制。具有代表性的是 802.1x，EOU（EAP over UDP 的简称，是 Cisco 的专有协议），像 802.1x 技术安全性还不错并且也可以分范围部署，但是部署复杂，部署周期也比较长，并且日常维护也十分的麻烦。由于目前这种方案相对而言还算较成熟，所以有很多客户选择以这种技术框架建设 NAC 系统。


Risky Bets
Contenders
Strong Performers
Leaders
Strong
Current offering
Weak
Juniper Networks
Cisco Systems
Symantec
Microsoft
Mirage Networks
StillSecure
Nevis Networks
McAfee
Bradford Networks
ProCurve Networking by HP
Market presence
Weak
Strategy
strong
Vendors
Architectures
Bradford Networks
Cisco Systems
Juniper Networks
McAfee
Microsoft
Mirage Networks
Nevis Networks
ProCurve Networking by HP
StillSecure
Symantec
Software-based NAC
Infras tructure-based NAC
Appliance-based NAC

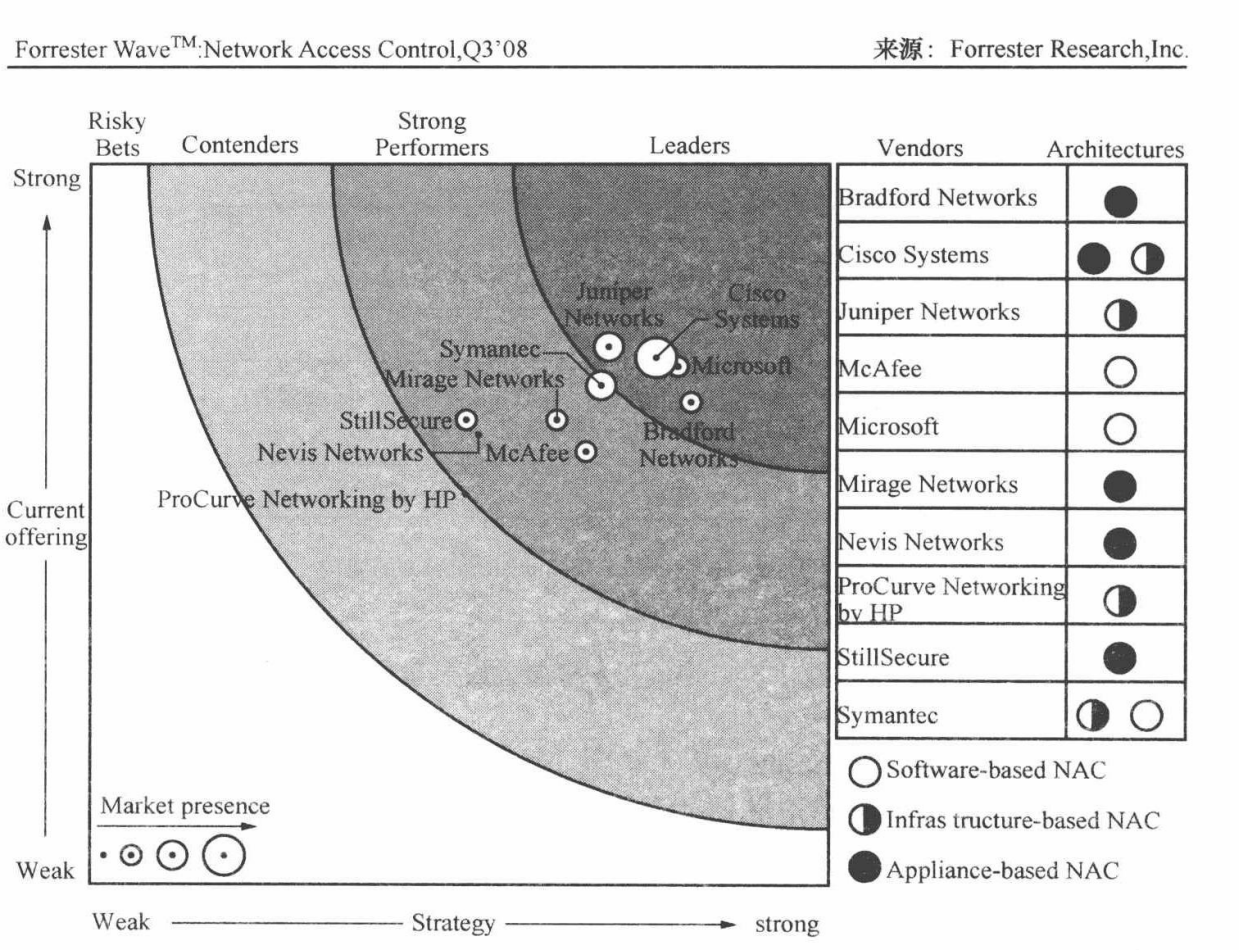


图 1-2　集中对比分析示意图

1.2.1　三代技术框架的发展

网络准入控制技术也是随时网络技术的发展，信息安全技术的发展，经历了几代技术框架的变迁。如图 1-3 所示。从早期的完全基于 Agent-Based 框架的 NAC，主要采用类似 ARP 欺骗技术、主机防火墙（TDI、NDIS）技术、DNS 协议拦截技术等，这种基于 Software-based 的 NAC 相对来说最具有伸缩性，也是最低廉的方案。但是对于如果无法安装 Agent 的网络设备就无法控制，并且如果不安装Agent也很容易绕开 NAC 的控制接入网络，同时不能很好地给用户提供友好的体验，无法对来宾做管理。

随着网络技术的发展，很多网络交换厂商为了让他们提供的基础网络方案增值，发展了基于网络交换设备的网络准入控制技术框架（Infrastructure-based NAC)。此方案主要是网络设备（交换机、路由器或者防火墙）联动，整合 Radius 服务，设备启用相关协议由设备进行控制。具有代表性的是 802.1x，EOU（EAP over UDP 的简称，是 Cisco 的专有协议），像 802.1x 技术安全性还不错并且也可以分范围部署，但是部署复杂，部署周期也比较长，并且日常维护也十分的麻烦。由于目前这种方案相对而言还算较成熟，所以有很多客户选择以这种技术框架建设 NAC 系统。

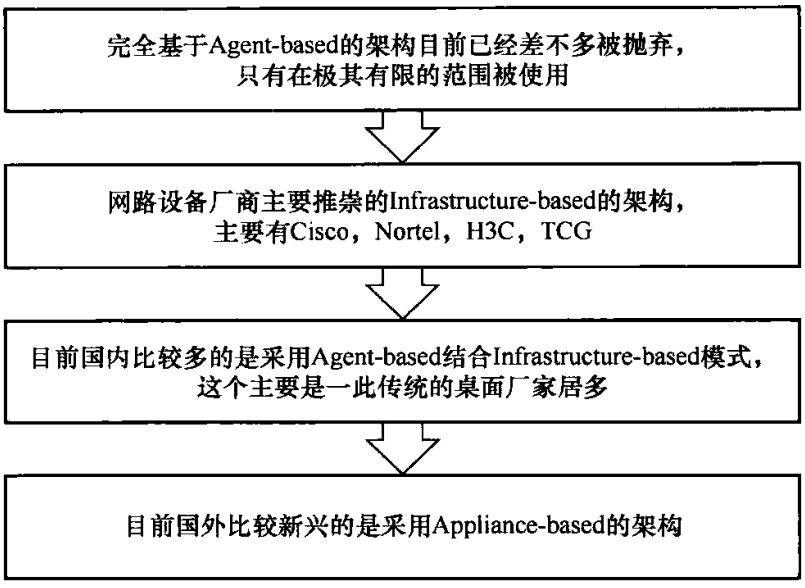


图 1-3 NAC 技术框架的发展阶段

思科在提出 NAC Framework（框架 NAC，代表技术 802.1x 与 EOU）之后，在 NAC 实践的过程中也同样存在很多的实际问题。在上述的基础上，思科提出了 NAC Appliance（设备 NAC，代表技术有 L2-OOB-VG、策略路由、透明网桥等）。NAC 系统本身就是一个网络设备，是对现有网路的补充，如果 NAC 设备接入到网络中可以起到准入控制的作用，如果将 NAC 设备从网络环境中拿走也不会影响正常的网络使用，并且不用对网络设备做更改。这是目前最先进的 NAC 技术发展方向，对网络环境的要求低，尽可能少地改动网络。通常采用带外模式，不会影响正常的业务流量。基于网络层的控制技术，可以做到 Agentless 的健康检查体验效果。

如前文所述，国际知名评测机构 Gartner 和 Forrester 对 NAC 技术的分析中，将其按技术种类和先进性从低到高分为三代标准。

1. 第一代：Software-based NAC

这是纯软件或协议方式的准入架构，比较初级。情况如下：

1）架构简介

基于端点的客户端进行准入控制，通过在端点安装 Agent，进行互相访问的控制，采用的技术一般有主机防火墙、ARP 干扰（或 ARP 欺骗）等。

2）优点

最具有伸缩性的部署方案，价格最便宜的准入控制，可以时时刻刻监控终端的合法性和安全性。

3）缺点

技术比较落后。对于没有安装 Agent 的设备控制较弱，对安装有 ARP 防火墙等软件的计算机不起作用。对于来宾设备的友好性欠缺。采用 ARP 欺骗和

ARP 病毒没什么区别，产生大量 ARP 包将造成网络拥塞，网络规模越大影响越严重，同时影响防毒系统对 ARP 病毒的检测。

4）相关厂商

北信源、极地银河。

2. 第二代：Infrastructure-based NAC

这是依托现有网络交换设备协议框架实现准入控制。情况如下：

1）架构简介

利用现有的网络设备（交换机、路由器和防火墙等）自身协议框架，采用与他们进行联动，需要网络设备支持相应的协议，并且在网络设备上配置或者启用相应的协议，实际的准入控制由网络设备完成。具有代表性的网络准入控制强制技术主要有 802.1x、Cisco 的 EOU、H3C 的 PORTAL \ PORTAL+等，且必须配合客户端进行安全检查和修复。

2）优点

该架构相对成熟、可靠。

3）缺点

（1）准入自身安全性较差，如果认证服务器故障，全网中断，且局域网之间也无法实现互访，后果极为严重。逃生机制可操作性较差，风险较高。

（2）对交换机型号、软件版本要求较高，且需在交换机上配置大量的命令，实现复杂。对厂商的方案设计能力、实施能力，以及自身产品适应网络的能力提出了很高的要求。

（3）需单独搭建认证服务器，必须安装庞大的客户端（20M 以上）。加载很多底层驱动，造成不必要的软件冲突。

（4）部署麻烦，实施工作量相当大。后期维护成本较高。无 URL 重定向引导机制，用户体验较差。

（5）无法完全解决 HUB 环境的颗粒度准入问题。

4）相关厂商

H3C、天融信、锐捷、联软。

3. 第三代：Appliance-based NAC

这是独立作为一个应用的 NAC 产品，具有框架无关性，代表了 NAC 技术发展的趋势。情况如下：

1）架构简介

本身就是一个网络设备，不使用 802.1x 的方式，也不需要交换机是否支持 EOU 协议或者是否支持 H3C 的 PORTAL 协议，对网络环境要求很低，一般只需要简单要求接入层交换机以 Trunk 方式接入汇聚层即可，主要通过网络层的检测来实现终端接入网络的控制，具有代表性的有虚拟网关（L2-OOB-VG）、网

关、策略路由等技术。一般会采用带内技术与带外技术相结合的方式实现。

2）优点

对网络设备要求较低，不需要在网络设备上配置或启用相应协议；可以达到较高的安全性，同时用户体验可以很友好；系统逃生方案比较完善可靠；能实现对 HUB 环境的颗粒度准入；项目实施与后期维护十分方便，工作量很少。

3）缺点

要求接入层交换机以 Trunk 方式接入汇聚层。

4）相关厂商

Cisco、Juniper、盈高科技。

1.2.2 基于应用层实现的准入控制技术

随着信息网络安全意识的逐步深入，对于一些政府机关、金融机构、大型企事业单位来说，由于网络庞大——可能涉及全国范围，用户众多——可能涉及几千台用户设备，安全运行要求高——可能要求系统 7 * 24 小时运行，这种大型网络已不能满足仅限于网络层的单一接入控制，往往需要考虑的安全因素更多，诸如防病毒、防黑客、防非法外联等，需要建立的是一套整体网络安全防御体系。针对这种情况，各个大型信息安全公司都提出了一些整体解决方案，其中很重要的一点就是更加严格了客户端的管理，加强了用户的接入控制，相比基于网络层的用户接入控制，其控制的内容更广泛，可以称为基于应用的综合接入控制。虽然由于各个软件开发商以及企业用户各不相同，这些解决方案各有特点，但基本上都有以下 5 个共同点。

（1）这是一整套基于软件的解决方案，需要在用户客户端安装代理程序。

（2）可以通过 SNMP 读写等方式与交换机形成联动。

（3）能够通过侦听或者扫描网络的方法了解客户端的接入情况，并且当没有安装代理程序的客户端接入网络时，会对用户提示要求注册下载软件，在监控管理中心形成告警，并且可以自动或者手动的方式对设备进行阻断（关闭交换机端口）。

（4）对于已安装代理的客户端，控制中心核对客户端的各种用户信息，并且根据这些信息以及用户的操作判断是否允许用户正常接入网络。如计算机的病毒库没有更新；内网用户有私自连接互联网以及其他未经允许的网络；或存在任何危害网络安全的行为，代理程序都会向监控管理中心发出告警，并且能够通过关闭交换机端口或者设备网卡（利用代理程序）的方式自动关闭网络连接。

（5）可以与其他用户接入控制系统（如 802.1x 认证）、客户端监控系统以及防病毒系统相结合，形成一个整体的安全防御体系。

此种方式进行的网络安全接入控制，要远比单纯的基于设备 MAC 地址或者用户名/密码方式等更加复杂、功能更加强大、安全系数也更高，它已经不仅限于网络层的接入控制，而是从设备以及用户信息、设备状态、用户的网络行为等

多个方面考虑接入控制安全，能够利用网络智能，根据客户端的安全状况提供访问权限，完全是基于应用的接入控制方式，而且它还可以与防病毒、防黑客、用户端管理等多个方面结合起来，形成一整套的网络安全防御体系。具有优点如下：

① 适应所有连接方式的统一解决方案，不管有线、无线、还是拨号接入都可以通过此种方法进行安全控制。

② 能够验证所有主机。

③ 可以实现与客户端防病毒解决方案全面融合。

④ 自动的隔离、恢复服务和连接。

⑤ 网络部署具有可扩展性，适合于各种大小规模的网络。

⑥ 易于形成统一的网络安全监控、防范、管理平台。

目前一些大型的网络和信息安全公司都在推广此类型的网络安全解决方案，比如思科的网络安全自防御系统（SDN）和准入控制（NAC），冠群的 eTrust 网络安全解决方案。而此类方案也得到相当一批大型政府机关、企事业单位的青睐，相比以前的网络层的接入控制，此种方法实施的难度也较大，往往需要根据各个企业不同的安全需求来订制整个系统，项目的投资也较大。

1.2.3　基于网络层实现的准入控制技术

基于网络层的用户接入控制是指利用网络设备（接入交换机）的某些安全功能，仅在交换机上采用一系列配置方法来实现网络用户接入控制的手段，对于用户或者接入网络的设备来说则是完全透明的。它在早期的网络安全防范中起到了重要作用，主要有以下 3 种方法。

1. MAC 地址绑定

安全端口过滤是大部分以太网交换机上的一项安全访问功能，可以用来阻止非授权的工作站/微机接入网络，它是通过将允许接入设备的 MAC 地址与交换机端口绑定来实现控制用户接入的。现有的一些高级的三层交换机（如 Catalyst 3550 EMI 和 Alcatel 5024 等）还可以实现设备 MAC 地址、IP 地址、端口号三者之间的绑定。

当试图访问端口的设备 MAC 地址与该端口所指定的 MAC 地址不同时，安全端口过滤功能将会阻止该设备的网络连通。

MAC 地址绑定通过交换机本身的安全机制来实现用户接入的控制，实施方法简单，管理严格，通过限定接入设备的 MAC 地址，杜绝了不安全的机器接入局域网，能够较大程度上保证接入安全。但该方法手段比较死板，设备移机或更换都需要更改交换机配置，日常维护工作量较大，仅适合小型局域网。

2. 动态接入控制

动态接入控制又称为动态分配 VLAN 的方式，即交换机根据接入设备的

MAC 地址自动将交换机端口分配到不同的 VLAN，一方面可以阻断外来非法设备的接入，另一方面对于合法的网络用户还可以根据不同的现场和部门划分不同的 VLAN，加强网络安全管理。现行的一些主流的交换机基本上都支持动态分配 VLAN 的方式，Cisco 网络设备是通过 VMPS 的方式来实现动态的接入控制，下面就以此为例作以介绍。

VMPS（VLAN MembershIP Policy Server）技术，简单来说就是针对局域网接入交换机的每个端口采用动态分配 VLAN 方式。它有 3 个要素：TFTP Server、VMPS、VMPS Client。

TFTP Server（Trivial File Transfer Protocol）：使用一般的网管服务器或微机即可（开启 TFTP 服务或运行相关 TFTP Server 软件）；

VMPS：只有 Catalyst 5000 系列、Catalyst 6500 系列交换机支持；

VMPS Client：Catalyst 2900 以上的大多数 Cisco 交换机都支持。工作原理如下所述。

（1）在 TFPT Server 上按照一定格式建立一个数据库文件，包含接入微机 MAC 地址与 VLAN Name 对应表、VMPS Client 的 IP 地址与其参与动态分配 VLAN 的端口对应表、其他的相应策略等信息。

（2）VMPS（交换机）通过 TFTP 的方式将上述建立好的数据库文件导入到自己的内存中。

（3）现场交换机（VMPS Client）的端口上设置为动态分配 VLAN，当有设备接入时，交换机将向 VMPS 发起相关请求，VMPS 则根据 Client 的 IP 地址，以及其提供的接入设备的 MAC 地址、接入端口与内存中的数据库作比对，返回给 VMPS Client 相应的信息。

（4）现场交换机（VMPS Client）根据得到的 VLAN name 信息，将该端口分配到相应的 VLAN 中；如果得到的是 access deny 的信息，该设备将不能与网络中其他设备相通，如果设置在安全模式下，该端口将被 shutdown。

3. 802.1x 认证

802.1x 认证是在 2004 年后才被广泛使用的基于用户的接入控制，它是通过认证用户名和密码来实现网络的接入控制，对于接入端微机或服务器来说，Windows XP 以上操作系统自动支持 802.1x 协议。控制原理如下：

（1）当接入交换机的端口被设置成 802.1x 认证方式时，端口只允许接入设备的认证信息（EAPoL，Extensible Authentication Protocol over LAN）和生成树协议（STP）的信息通过。

（2）用户接入网络时，点击网络连接会跳出窗口要求用户输入用户名和密码。

（3）用户信息经交换机传输到后方认证服务器（RADIUS），认证通过后，服务器赋予接入交换机相关信息（如 VLAN 信息）后，相应端口被打开，客户

端设备才被允许正常传输数据，否则端口将被封闭。交换机和认证服务器只要可路由即可，无需限于同一地点、同一局域网，而且 RADIUS 服务器还可以与其他外部服务器（如域服务器等）或数据库进行协同认证。同样，此种认证方式也被广泛应用于一些无线局域网的接入控制。

前面介绍的 3 种用户接入控制方式，共同点都是基于网络层的控制，即对于用户和接入设备来说是透明的，无需或者很少做任何更改，只需要在后方的网络设备和管理服务器上进行相应配置。不同点是前两种接入控制是面向接入设备的控制（针对设备的 MAC 地址），802.1x 认证则是面向用户的控制，只要是允许的用户，对于接入设备没有相应要求。3 种控制方式的应用的网络范围也是逐步扩大，MAC 绑定的方式只适合中小型的网络，后两种适用的范围则较广，从有线到无线网络接入都可以使用。

1.3　网络准入控制行业发展

为了解决网络安全问题，安全专家相继提出了新的理念。20 世纪 90 年代以来，国内外提出了主动防御、可信计算等概念，认为安全应该回归终端，以终端安全为核心来解决信息系统的安全问题。同时，很多安全产品生产厂家相继提出了新的安全构想，如 Cisco 的自防御网络（Self-Defending Network，SDN）和华为 3COM 的安全渗透网络（Safe Pervasive Network，SPN）等，这些蓝图是上述理念的具体体现，而在 SDN、SPN 等新型安全构想中不约而同地将准入控制技术作为重要的组成部件或解决方案。

前面提到，目前对网络准入控制还没有一个权威、统一的定义。但普遍认同的是：网络准入控制是目前一种新型的安全防御技术，它通过对终端实施安全防护，可以有效地解决因不安全终端接入网络而引起的安全威胁，将病毒、蠕虫等各类攻击拒绝于网络之外，从而真正保障网络的安全。

NAC 自诞生之日起就争议不断，其中一个十分重要的因素就是对网络中接入点的管控过强，同时实施和维护工作量相比于防火墙等网关型的安全产品要高出一个数量级，因此在行业发展中期历经过数年平淡的市场表现。而在 2012 年，各机构对于部署 NAC 的需求将在“BYOD”浪潮的驱动下重新激发起来。

同时，我们也看到，NAC 方案中的安全策略随着时间的推移在不断的变化。在 NAC 应用的第一波浪潮（2003～2006 年）中，主要的 NAC 管理策略是针对终端的系统配置（如 Windows 系统补丁是否更新、杀毒软件是否安装等）。在 2007 年，NAC 应用进入了第二波浪潮，焦点变为了对来宾设备提供简便易行的基于认证的控制，从而搭建出灵活的访客网络环境。在 2011 年——NAC 技术的第三波浪潮中，除了对来宾提供简易的接入服务外，还提出了对员工的个人设备提供“有限访问区”的控制要求。国际权威评测机构 Gartner 认为，这次的第三波 NAC 应用浪潮将是有史以来最为强劲的一次，并且通过周期性的宣传，能够

驱动 NAC行业达到真正的生产力成熟期和稳定期。

为了避免 BYOD 所引发的威胁，机构们都开始创建自己的有限访问区，从而控制个人移动设备与网络中的重要区域实现隔离。“BYOD”们只能够获得Internet的访问权，以及只能够访问公司业务的一个特定的子集。而由于这些终端设备都是私人所有，因此 IT 部门往往很难对其强制部署策略、安全客户端或生命周期管理工具。而另一方面，将这些私人终端隔离到有限访问区内则能够对保障网络的安全起到有益的作用。要建立起完善的有限访问区，一个十分重要的元素就是在终端（例如 IPad、Android 设备、IP 电话、打印机以及 PC）接入网络时能够对其进行发现并识别出相关信息，这也被称为“显影”（profiling）。一旦一台终端设备得到了识别，自然就立即能够被放置于合适的网络区域（机构生产网、来宾访客网、或有限访问区等）中，在这些不同的网络区域中，NAC 能够执行不同的接入控制策略。

2011 年年底，Gartner 对 NAC 市场的销售收入进行了总结，NAC 市场销售额在 2011 年全年保持在 2.06 亿美元（主要是国外市场）左右，相比 2010 年增长约 3%。Gartner 预计 2012 年的整个市场将进一步增长 10%左右。

Forrester 和 Gartner 都对 2011 年前两个季度北美 NAC 市场进行了半年的盘点，其中的一些评判标准很值得我们思考，同时国内的 NAC 市场发展了近 4 年，涌现出了许多独立于国际市场的个性化需求，这也是业界和用户都不可回避的话题。

在 Forrester 对 NAC 厂商的排名中，看到顶尖的 NAC 产品关键词中赫然列出了以下 5 条标准：

（1）Unified management（整合管理）。

（2）Integration（集成度，或兼容性）。

（3）Clientless（Agentless）mode（无客户端模式）。

（4）Hardware（appliance）（硬件应用）。

（5）Heavy focus on IT consumerization，mobile device control and data center virtualization（关注前端、移动端和虚拟化）。

国内的准入控制标准因为多方利益的博弈迟迟未能出台，甚至在各国家级评测机构的产品类别中都难以找到。NAC（中国）只能躲在角落里看着同为“访问控制类”产品的防火墙们穿着“西装革履”满大街都是，看看自己周围，却是“桌面管理”或“上网行为管理”等一干人等在沿街叫卖。皇帝的新衣都是一样，却没有一颗 NAC 的心。

其实国内早有厂商在 NAC 的标准化或评优参数上做出了积极有效的工作，硬件化、无客户端化、兼容度这些标准并不是 Forrester 第一个想出的，整合管理也是很适应国内内网安全架构的折中解决办法，至于前端和移动端，国内的桌面管理产品已经给 NAC 好好上过一课了。

总体来说，NAC 行业在多年的发展中形成了包括以下几个类型的组成。

1. 网络基础设施类

大多数的商用级网络交换机厂商都能够提供 NAC 的解决方案，而这些方案中有 90%都是基于公用标准 802.1x 协议的，因此必须依赖于厂商自身网络交换机的支持。而 BYOD 浪潮为此带来了不小的难题，因为此时的策略必须开始分别针对有线网络和无线网络，具有讽刺意味的是，大部分的交换机制造商并没有较强的无线产品实力。总体来看，在 WLAN 上支持 NAC 策略的能力将在 BYOD 新纪元下变得越来越重要，另外，有线和无线网络基础设施厂商在异构网络中或其竞争对手的基础网络中均很难将自己的 NAC 体系部署上去，这是一个不可避免的硬伤——兼容性问题。此类厂商典型的有 Cisco、Juniper、华为、H3C。

2. 网络安全及终端安全类

包括 IPS、防火墙、VPN 等厂商均能够提供部分的 NAC 功能。因为上述的这些产品在网络中都已经作为一个策略强制点存在了，因此能够变相地作为一个附加的 NAC 控制点。典型的如 CheckPoint、Symantec、LeagView、趋势科技等。

3. 纯 NAC 独立第三方类

BYOD 浪潮为第三方的纯 NAC 厂商创造了新的契机，纯 NAC 厂商也成为了新趋势下引导 NAC 市场增长的主力军。在今天的多元化终端环境下很多时候均需要各种特定的策略来进行部署和管理，因此第三方的纯 NAC 厂商优秀的兼容性和专业度就成为了大规模及复杂网络环境下用户的首选参考。此类厂商比较突出的代表如：Infogo（盈高科技）、Bradford 等。

综上所述，目前，国内外有代表性的终端准入控制技术有以下几种：思科的网络准入控制（Cisco Network Admission Control，C-NAC），微软的网络接入保护（Network Access Protection，NAP），JunIPer 的统一接入控制（Uniform Access Control，UAC），可信计算组织 TCG 的可信网络连接（Trusted Network Connect，TNC），H3C 的端点准入防御（Endpoint Admission Defense，EAD），Infogo 的入网规范管理（Admission Standard Management，ASM）等。

其他如赛门铁克、北信源、锐捷、启明星辰等大大小小国内外厂商也不约而同地基于自身特色提出了准入控制的解决方案。这也从一个方面反映出终端准入控制技术的重要性以及广阔的发展前景。

第 2 章　网络准入控制基本原理

网络准入控制（Network Access Control，NAC），最早是一项由 Cisco 发起、多家厂商参加的计划，其宗旨是防止病毒和蠕虫等新兴黑客技术对企业安全造成危害。对于各机构的网络管理者而言，虽然大多从业者都会使用身份管理及验证、授权和计费（AAA）机制来验证用户并为其分配网络访问权限，但这些对验证用户终端设备的安全状况几乎不起任何作用。如果不通过准确方法来评估设备“状况”，即便是最值得信赖的用户也有可能在无意间通过受感染的设备或未得到适当保护的设备，将网络中所有用户暴露在巨大风险之中。借助 NAC，网络管理员可以只允许合法的、值得信任的端点设备（例如 PC、服务器、PDA）接入网络，而不允许其他不符合要求（未通过认证、安全性不符合要求等）的设备接入。在初始阶段，当端点设备进入网络时，NAC 能够帮助其所联动的网络设备（如交换机）对终端或用户实施（通过 ACL 变换、VLAN 切换、端口开关等）访问权限控制，权限控制决策的内容可以根据端点设备的信息制定，例如设备的当前防病毒状况、操作系统补丁、弱口令、软件安装情况等。

2.1　网络准入控制技术特点

从 Cisco 在 2003 年提出 NAC 的概念以来，到目前为止，网络准入控制仍然缺少一个单一的标准，并且被证明它比第一次出现时更难实施，现在如果说 NAC 不是至关重要的但也仍然是一项非常有价值的安全技术。确实如此，Forrester 研究公司已经在最近的一份报告中预测，今后的 NAC 将会日益重要，这个“看门狗”技术将会迅速变成网络基础设施中必不可少的一部分，它也会是促使企业安全策略倡议更加有效的组成部分。Gartner 公司的研究主管 Lawrence Orans 认为，NAC 是“一个可以添加到自己网络中的有价值的防御”，并表示，“我们给出的建议是，现在就可以实施 NAC。”

1. 安全管理规范落实的问题

目前各个政府单位及各行各业都建立了较为完整的网络安全管理规范，但很多时候落实情况不尽如人意，究其原因是缺乏行之有效的管理手段。

随着信息化的发展，企业或者单位自己已经制定了详细的安全规范和标准，但现状依然是“病毒”、“蠕虫”、“木马”在个人电脑上，甚至在整个网络中肆虐横行。这是为什么呢？最根本的原因就是，现有的安全规范制度，无法落实下去，造成“安全规范没有从抽屉里走入到电脑”的局面。

安全规范制度的落实，一直是令各单位信息部门头痛的难题。安全规范的实

施前期，依靠行政发文通告的方式强制实施下去；但到后期，总是由于这样那样的原因，安全规范实施的热度降下去，变成一纸空文，被束之高阁。

2. 接入用户及设备的实名制

随着信息化建设越来越普遍，人们越来越依赖于网络办公。网络服务给单位和企业带来方便性和高效率的同时，也带来了诸多的网络安全问题，例如，如何确认使用网络服务的用户身份？身份可信的用户所使用的设备是否同样可信？

电子政务网涉及国家重要数据信息，因此，必须要求对使用者进行实名认证，以确保对使用行为承担责任；另一方面，必须对使用者入网办公所使用的设备进行可信认证，以有效降低各类设备所引起的风险。

3. 人机对应管理机制落实的问题

很多政府、事业单位目前每位工作人员都配置相应的一台或两台工作当中使用的计算机。而大多用户对 IP 资源管理通常的做法是，将 IP 提前分配到部门和个人。问题是，很难知道谁正在使用这台设备访问网络，发生网络安全事故后，也很难追踪到个人。

正是由于大多数单位没有建立用户身份管理机制，通常一台机器是谁使用的，管理员一般会认为某个 IP 的机器就是对应使用者负责的。所以需要一套能够落实这个实效的“人机对应”管理机制。

4. 快速发现设备隐患及智能修复的问题

目前终端设备为数众多，不知道哪些计算机未安装杀毒软件，或安装了没有及时更新病毒库，或是没有加入 AD 域，或是未打好系统补丁等；信息管理人员如何及时发现计算机的安全漏洞，提供使用者打上系统补丁，安装杀毒软件，更新病毒库等，同时修复工作又要轻松化、傻瓜化、便捷化？

5. 安全检查规则库不能更新升级的问题

每个行业的安全要求都有差异，终端设备使用规范都不一样。即使在同一个单位随着管理需求的变化，随着网络威胁、漏洞和补丁的不断更新，对设备的安全检查要求也越来越高，如果使用的准入产品都是固定的检查项，不能方便支持安全检查库扩展升级的话，将很难适应安全管理的不断升级的需求。例如银监会对商业银行的要求不断变化，要求检查的软件安装情况又时有增加，信息部门的处理措施也肯定需要随之调整。

6. 网络结构复杂、新老设备兼容的问题

用户经过多年的网络建设，逐步已形成了一个完整的网络，但网络中存在着各种各样的新老网络设备，存在各种复杂的网络结构，像 HUB、多种品牌的交换机等。目前，大多数厂家的网络准入控制方案都无法兼容新老设备。

大部分厂家的方案都要求用户将已有的网络设备进行升级，如：交换机、VPN、无线 AP 等，然后才能实现网络准入的控制。

如 Cisco 和 H3C 的 NAC 解决方案就要求用户将网络交换机升级，更换为能够支持 802.1x 协议的交换机。对这类网络设备厂商来说，升级可以增加网络设备的销售额，达到明修栈道暗渡陈仓的效果。但对用户来讲，需要对网络设备进行再投入，造成了不必要的浪费。

当用户网络形成后，由于资金、操作难度、设备正常更新周期等原因，用户很难一次性的将所有设备全部进行更新。如果采用这类的网络准入控制方案的话，就会造成已更新的网络接入设备可以实现接入控制，而未更新的网络设备无法实现网络准入控制的局面。

7. 内网分角色分区域访问控制的问题

目前，虽然各个用户内部在行政意义上都划分多个部门区域，但在内部网络访问层面上却无角色或区域的划分，任何入网员工及来宾用户都是“平等”的，可以访问内网的所有资源。如此，内部资源安全性保障成了严重问题。

8. 日益增多的移动办公与特殊情况处理的问题

随着 VPN、无线网络等多种接入技术的应用，移动办公已成为用户一大业务特色。然而，丰富的接入技术带来的不只是日益提高的办公效率，同时也将原本单一、可控、安全的网络环境，变成复杂、难以控制，加大了内部网络管理的成本与风险。

9. 用户来宾的访问控制与管理问题

一台 PC，一根网线，再加一个内部 IP 地址，来宾就能轻松接入企业内部网络，犹如内部员工般畅通无阻地访问内部资源，传播病毒。然而，网络管理员却对来宾的一切行为全然无知也无从管理。

10. 单点防御及分散管理的问题

对病毒的重复、交叉感染目前的解决方式，更多的是在单点防范，当网络中有机器始终没有解决病毒问题而又能无限制上网时，网络就会始终处于被感染、被攻击状态。

只有从用户的接入终端进行安全控制，才能够从源头上防御威胁；但是，分散管理的终端难以保证其安全状态符合用户的安全策略，无法有效地从网络接入点进行安全防范。在分散管理的安全体系中，新的补丁发布了却无人理会，新的病毒出现了却不及时升级病毒库的现象普遍存在。

11. 实名入网安检日志审计问题

实名入网安检日志审计虽说只是“事后诸葛”，无法避免网络威胁行为的发生，但它记录威胁行为的源头，是追究责任的有力证据。某些系统尽管提供了详细的日

志审计信息（用户上网过程、病毒查杀事件等），但美中不足的是无法根据实名入网设备的信息来进行日志记录，也无法查看接入设备安全检查结果的日志信息。

12. 保证网络边界完整的问题

由于笔记本、上网本、手机终端等设备的兴起，同时由于 ADSL，WiFi 和 3G 等网络接入手段的不断出现，用户可以很容易地在任何时间、任何地点实现跨网络连接。正是由于这种原因，信息内网已无法按照传统的网线和交换机端口来保证网络边界的完整。

网络边界很有可能因为 ADSL，WiFi，3G 的外联，造成网络边界的被破坏，造成有不明终端穿越网络边界接入。网络边界的防护不能仅限于网络出口的保护，而是应该是所有网络边界的防护。

2.2　网络准入控制运行机制

新型终端安全接入技术的主要思路是：终端接入网络之前应根据预定安全策略对其进行检查，只允许符合安全策略的终端接入网络，将不安全的终端隔离于网络之外，自动拒绝不安全的主机接入保护网络，直到这些主机符合网络内的安全策略为止。

网络准入控制作为一种主动式网络安全管理技术，很好地体现了主动防御的理念，能有效增强网络的安全性。网络准入控制系统的运行机制始终围绕着终端安全状态检测展开，终端在接入网络之前，必须先接受身份认证和完整性度量，只有可信并且符合安全策略的终端才获准访问网络，拒绝不符合安全策略的设备接入，或将其放入隔离区加以修复，或仅允许其访问限定资源。其周期可以用图 2-1 来描述。具体请参考附录 B。

图 2-1　“检测—决策—执行”周期

检测包含准入前检测（Pre-Admission Assessment）和准入后检测（Post-Admission Assessment）。准入前检测在终端获得网络访问权限之前进行，准入后检测与其相反。准入后检测可以周期性地检测终端安全状态，保证其不会在网络访问过程中引入安全威胁。终端一旦连接到网络就要接受检测，系统之后依据检测结果和管理者制定的策略作出准入决策，最后执行该决策，整个过程周期性地循环。另外，当终端的安全状态发生改变时，也将激发这个过程。

2.3　网络准入控制工作流程

NAC 能确保等待接入网络的系统符合一定级别的安全标准，它会检测病毒防


执行
Enforcement
检测
Assessment
决策
Decision

志审计信息（用户上网过程、病毒查杀事件等），但美中不足的是无法根据实名入网设备的信息来进行日志记录，也无法查看接入设备安全检查结果的日志信息。

12. 保证网络边界完整的问题

由于笔记本、上网本、手机终端等设备的兴起，同时由于 ADSL，WiFi 和 3G 等网络接入手段的不断出现，用户可以很容易地在任何时间、任何地点实现跨网络连接。正是由于这种原因，信息内网已无法按照传统的网线和交换机端口来保证网络边界的完整。

网络边界很有可能因为 ADSL，WiFi，3G 的外联，造成网络边界的被破坏，造成有不明终端穿越网络边界接入。网络边界的防护不能仅限于网络出口的保护，而是应该是所有网络边界的防护。

2.2　网络准入控制运行机制

新型终端安全接入技术的主要思路是：终端接入网络之前应根据预定安全策略对其进行检查，只允许符合安全策略的终端接入网络，将不安全的终端隔离于网络之外，自动拒绝不安全的主机接入保护网络，直到这些主机符合网络内的安全策略为止。

网络准入控制作为一种主动式网络安全管理技术，很好地体现了主动防御的理念，能有效增强网络的安全性。网络准入控制系统的运行机制始终围绕着终端安全状态检测展开，终端在接入网络之前，必须先接受身份认证和完整性度量，只有可信并且符合安全策略的终端才获准访问网络，拒绝不符合安全策略的设备接入，或将其放入隔离区加以修复，或仅允许其访问限定资源。其周期可以用图 2-1 来描述。具体请参考附录 B。

图 2-1　“检测—决策—执行”周期

检测包含准入前检测（Pre-Admission Assessment）和准入后检测（Post-Admission Assessment）。准入前检测在终端获得网络访问权限之前进行，准入后检测与其相反。准入后检测可以周期性地检测终端安全状态，保证其不会在网络访问过程中引入安全威胁。终端一旦连接到网络就要接受检测，系统之后依据检测结果和管理者制定的策略作出准入决策，最后执行该决策，整个过程周期性地循环。另外，当终端的安全状态发生改变时，也将激发这个过程。

2.3　网络准入控制工作流程

NAC 能确保等待接入网络的系统符合一定级别的安全标准，它会检测病毒防

护软件的升级版本、当前可用补丁、浏览器设置限定，以及有效的个人安全相关配置等，在首先检测系统是否符合上述要求后，平台能够决定是否准允其接入网络。

通过运行 NAC，只要终端设备试图连接网络，网络访问设备（LAN，WAN，无线或远程访问设备）都将自动申请已安装的客户端或评估工具提供终端设备的安全资料。随后将这些资料信息与网络安全策略进行比较，并根据设备对这个策略的符合水平来决定如何处理网络访问请求。网络可以简单地允许或拒绝访问，也可通过将设备重新定向到某个网段来限制网络访问，从而避免暴露给潜在的安全漏洞。此外，NAC 还能对设备进行隔离，它将不符合策略的设备重新定向到修补服务器中，以便通过组件更新使设备达到符合安全策略水平。

NAC 执行的某些安全策略符合检查包括：

（1）判断设备是否运行操作系统的授权版本。

（2）通过检查来查看操作系统是否安装了适当补丁，或完成了最新的热修复。

（3）判断设备是否安装了防病毒软件以及是否带有最新的系列签名文件。

（4）确保已打开并正在运行防病毒技术。

（5）判断是否已安装并正确配置了个人防火墙、入侵防御或其他桌面系统安全软件。

NAC 随后能够根据上述问题的答案作出基于策略的明智的网络准入决策。

由上可见，一个标准完善的 NAC 系统事实上实现了如图 2-2所示的控制流程。

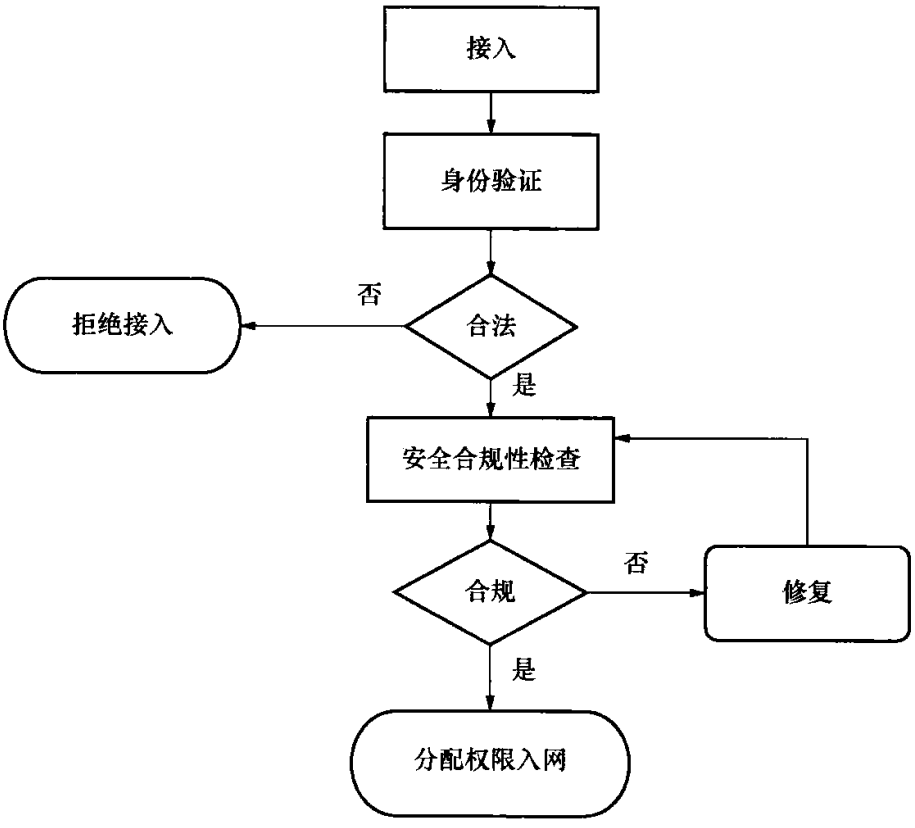


图 2-2 NAC 系统基本控制流程

2.4　网络准入控制实施准则

在任何一个 NAC 部署实施项目中，技术选型的确定是非常重要的。有 5 条关键准则可以帮助区分不同的准入方式，并能够确认到底哪一种是最适合现有具体网络的。这 5 条准则是：安全性（security）；灵活性（flexibility）；风险性（risk）；可伸缩性（scalability）；开销（cost）。

1. 安全性

NAC 首先是一种安全服务，因此选取 NAC 准入方式最重要的标准就是强制技术的安全性。更高的安全性带来的是强制认证、限制认证前的网络接入，并且与设备的认证会话紧密绑定。

2. 灵活性

每个安全设计师都会要求所选择部署的产品有着最高的灵活性。被单一的功能套牢是非常危险的，并且会限制对突发事件和企业长远发展的响应能力。具有更高灵活性的 NAC 强制技术是更具吸引力的，尤其是那些与不断发展的安全技术相关的。

3. 风险

以务实、Step-by-Step 的方式来部署 NAC 绝对会提高成功率。最好能够以细件（small pieces）的方式来部署 NAC，再将这些细件与网络纯净地融合（merge it cleanly），在实施方案具有足够的稳定性和可靠性后再逐步提高安全等级。

4. 可伸缩性

对 NAC 来说，无法提供可伸缩性会造成潜在的危险。如果 NAC 停止工作，想象一下对公司的所有员工会造成什么影响。这就要求当网络调整的时候，NAC 也应该顺利地做出相应的调整。

5. 开销

NAC 应该撬动出那些已存在设备的价值。举例来说，NAC 应该利用好那些已安装设备中的存在特性，比如 802.1x 认证、VLAN 功能等。另外一点则需要依靠网络设备厂商的力量，很多网络厂商都会积极地提高他们产品的安全性。

对于不同的用户来说，可以根据自身的实际网络情况，结合以上 5 点准则，计算出一个 NAC 方案对于自身的适用度，根据不同的用户，每一项准则在选购的时候所占的比例可能不尽相同。

第 3 章　网络准入控制技术架构

首先分析研究网络准入控制系统中应用到的一些主要技术手段，基于不同的技术手段也往往造就了不同的 NAC 框架。

3.1　网络准入控制基本技术手段

3.1.1　IP-MAC 绑定

相对于 IP 地址可轻易更改，MAC 地址则固化在网卡的 EEPROM 中，它由 IEEE 统一分配，一次性写入，不能随意改动。因此，IP-MAC 绑定的思想就是：将合法终端的 IP 地址与 MAC 地址写入交换机的访问控制列表中。终端访问网络时，只有其 IP，MAC 地址均与访问控制列表匹配，才认为其是合法终端，允许其访问网络。

但是，网卡驱动在发送 Ethernet 报文时，并不从 EEPROM 中读取 MAC 地址，而是在内存中来建立一块缓存区，每次从缓冲区中读取 MAC 地址。根据这个原理，可以修改实际发送的 Ethernet 报文中的源 MAC 地址。这样的修改工具很容易找到，甚至很多操作系统本身也具备这个功能。既然 MAC 地址可以修改，那么 MAC 地址与 IP 地址绑定的准入控制效果就大打折扣。IP-MAC 绑定还有操作不方便等问题，一般适用于小型局域网，不适合大型网络的统一管理。

3.1.2　DHCP Snooping

DHCP Snooping 技术起初是在 DHCP 网络中，通过过滤来自不信任端口的非法 DHCP 服务器的 DHCP Offer、DHCP Ack 等消息，来防止非法 DHCP 服务器影响网络的问题。目前，通过将 DHCP Snooping Binding 数据库供给 IP Source Guard 使用，可以实现准入控制等功能。

IP Source Guard 保护功能是实现准入控制的关键，应用在交换机的不信任的二层端口。当启用该功能后，在终端获取 IP 地址之前，该端口只允许 DHCP 包通过，该端口只能接收来自与静态或 DHCP Snooping binding 数据库相应条目的 IP 产生的数据包。杜绝了用户随意设置 IP 地址，从而干扰其他用户上网。IP Source Guard 不但可以配置成对 IP 地址或者 MAC 地址的过滤，也可以配置成对 IP-MAC 地址的过滤，以及对交换机 PORT-MAC-IP 三者的过滤。

通过 DHCP Snooping 技术实现准入控制，可以实现更多的过滤组合，控制得更精细。而且 DHCP 网络中终端不用配置 IP，减少了维护工作量；通过 DHCP Snooping Binding 数据库，可以在一定程度上实现终端的固定 IP 分配。但

是，需要在网络中额外配置 DHCP 服务器，因此，通过 DHCP Snooping 技术实现的准入控制更适合于大型网络。

3.1.3　ARP 欺骗

ARP（Address Resolution Protocol，地址解析协议），是一种将 IP 地址转化成物理地址的协议。从 IP 地址到物理地址的映射有两种方式：表格方式和非表格方式。ARP 具体来说就是将网络层（IP 层，也就是相当于 OSI 的第三层）地址解析为数据连接层（MAC 层，也就是相当于 OSI 的第二层）。简单说，IP 地址与 MAC 地址之间就必须存在一种对应关系，而 ARP 协议就是用来确定这种对应关系的协议。

在同一个 IP 子网内，数据包根据目标机器的 MAC 地址进行寻址，而目标机器的 MAC 地址是通过 ARP 协议由目标机器的 IP 地址获得的。每台主机（包括网关）都有一个 ARP 缓存表，在正常情况下这个缓存表能够有效维护 IP 地址对 MAC 地址的一对一对应关系。但是在 ARP 缓存表的实现机制和 ARP 请求应答的机制中存在一些不完善的地方，容易造成 ARP 欺骗的情况发生。

ARP 欺骗本来是一种网络上的攻击方法，它利用了 ARP 协议对于 ARP 包是否被伪造缺少检查，对 ARP 高速缓存的更新不严密的缺陷，可以干扰局域网上其他计算机的正常通信。有些网络管理软件正是利用了 ARP 欺骗的这一特点，将它作为准入技术，来控制其他计算机访问网络。

但是，针对 ARP 欺骗的防护软件也很多，比如各种 ARP 防火墙等。当非法终端安装了这类软件，ARP 欺骗的准入效果就大打折扣。而且启用 ARP 欺骗后，对网络会造成较大的流量负担，影响合法终端的通信。

3.1.4　IEEE802.1x

2001 年 6 月 14 日，IEEE 标准协会发布了以“基于端口的网络访问控制”命名的 IEEE802.1x（以下简称 802.1x）标准。标准发布的初衷旨在提升局域网或无线局域网以计费为目的的用户接入认证的安全性。目前，标准更多地应用于网络中的准入控制。标准中的角色组件及其功能如图 3-1 所示。

在图 3-1 中可以看到 802.1x 标准由三种角色组成。其中，申请者（Supplicant）的是位于点到点局域网段的一个端点，它向连接到局域网段另一端点的认证者提出请求，以便实施认证；认证者（Authenticator）是位于点到点局域网段的一个端点，它接收来自连接到局域网段另一端点的实体的认证请求，并对其进行认证；认证服务器（Authentication Server）则是为认证者提供认证服务的实体。用来检测申请者提供的认证信息。

与其他接入认证方式相比，802.1x 具有在二层认证、认证流与数据流分离等优点。链路层认证的优势主要表现为快速简单、成本低廉和安全可靠。认证流与数据流分离则较好地平衡了网络的可管理性与效率间的矛盾。

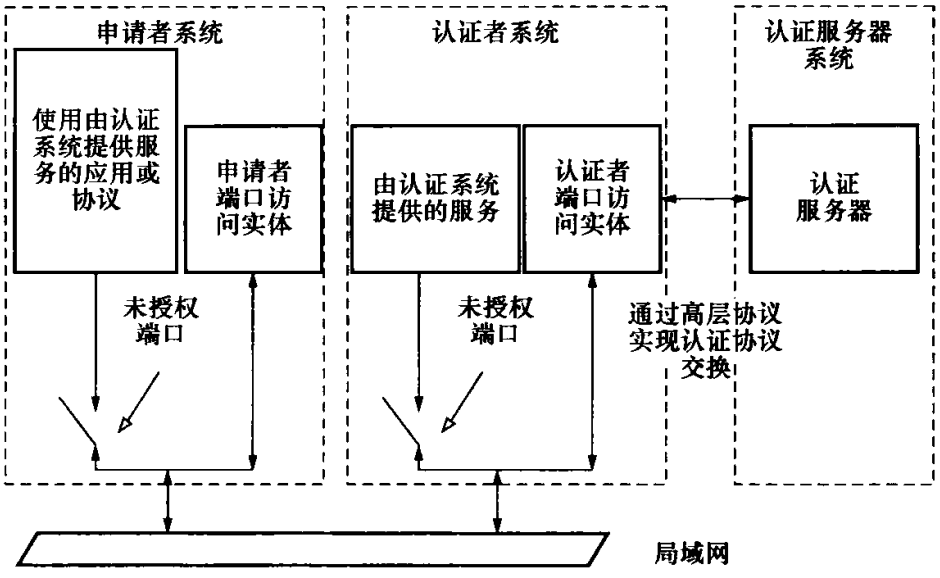


图 3-1 申请者、认证者与认证服务器角色

在实际应用中，802.1x 并没有像最初人们期望的那样迅速得到普及。经分析认为其原因包括网络设备对标准的支持，以及新的网管方式可实施性等。为此，人们提出了各种改进办法，比如为了适应在大型网络中的部署，采用网桥应用模式与混合应用模式等。

3.1.5 可信计算

“可信计算”是基于这样一种思想：要做到网络真正的可信可控，必须从信息安全的源头着手，内外共防来构造安全的计算环境。1999 年，由 Intel，IBM，HP 等公司发起成立了可信计算组织（Trusted Computing Group，TCG），支持厂家达到一百多家。TCG 采用广义的工业标准，配合可信平台模块（Trusted Platform Module，TPM），将网络与端点设备进行整合。

TPM 是 TCG 的核心，它通过在计算机系统中嵌入一个可抵制篡改的独立计算引擎，使非法用户无法对其内部数据进行更改，从而确保了身份认证和数据加密的安全性。它并不像一般安全软件那样只能被动地抵抗病毒和黑客，而是在检测到系统数据被非法篡改后即自动恢复，以保证平台的完整性。这种办法从本质上提高了计算机自身的免疫力，弥补了计算机的先天不足，从而主动做到预防多种病毒的攻击。

3.1.6 Web/Portal

Web/Portal 准入控制的实现过程是：客户机在认证通过前只能访问特定的 IP 地址，这个地址通常是门户服务器（Portal Server）的 IP 地址。输入用户名和密码，认证通过后，才会被允许访问网络。Web/Portal 服务器通常串接于网络的准入控制点中。基于这种准入控制技术，很多网络设备公司开发了各具特色的产品。

Web/Portal 认证技术存在的主要问题有：Web 承载在第七层协议上，对于设备的要求较高，网络建设成本高；用户在访问网络之前，不管是 TELNET、FTP 还是其他业务，均须使用浏览器进行 Web 认证，易用性不够好；还有就是认证前后业务流和数据流无法区分等。

3.1.7　PPPoE

以太网上的点对点协议（Point to Point Protocol over Ethernet，PPPoE）于 1998 年后期问世，PPPoE 协议定义了在以太网中传输 PPP 协议帧的方法，它既利用了以太网的便利性又实现了 PPP 协议的点对点特性。其主要目的是希望把比较经济的 LAN 技术与以太网和 PPP 协议的可扩展性及管理控制功能结合在一起，由于 PPPoE 协议在用户管理、用户认证和计费等方面具有较大的优势，使互联网服务提供商在提供宽带接入服务时更加简便易行，所以很多宽带接入网采用基于 PPPoE 技术的解决方案。目前，该准入控制方式已经被大量应用于 ADSL 接入，它是传统 PSTN 窄带拨号接入技术在宽带接入时代的延伸，适应目前电信运营商的运维和管理体制。

PPPoE 工作流程：主机广播一个发起分组（PADI），一个或多个接入服务器发送响应分组（PADO），主机从（PADO）中挑选一个合适的接入服务器并发送单播会话请求分组（PADR），被选择的接入服务器发送一个确认分组（PADS）。当主机接收到确认分组，它可以开始进行 PPP 会话阶段。当接入服务器发送出确认分组，它可以开始进行 PPP 会话阶段。当主机在指定的时间内没有接收到 PADO，它应该重新发送它的 PADI 分组，并且加倍等待时间。在重试指定的次数后，主机应该重新发送 PADI 分组。PPPoE 还有一个 PADT 分组，它可以在会话建立后的任何时候发送，来终止 PPPoE 会话。它可以由主机或者接入服务器发送。当接收到一个 PADT，不再允许使用这个会话来发送 PPP 业务。

PPPoE 方式主要的缺陷是局端接入设备的开销相当大，很容易形成瓶颈。由于 PPPoE 协议的第一阶段是发现阶段，广播只能在二层网络才能发现 BRAS。因此，用户主机和 BRAS 之间，不能有路由器或三层交换机。另外，由于 PPPoE 的点对点的本质，在用户主机和 BRAS 之间限制了多播协议的使用。这样就会影响多种业务的开展。

3.1.8　策略路由

策略路由（Policy-Based-Route）是一种依据用户制定的策略进行路由选择的机制。与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由基于到达报文的源地址等信息灵活地进行路由选择。

传统上，路由器根据目的地址查找路由表获得下一跳，来进行报文的转发，路由表条目由网络管理者静态指定或由路由协议通过路由算法动态产生。而在现实应用中经常有这样的需求：进行路由选择时不仅仅根据数据包的目的地址，而

且根据数据包的其他一些特性如：源地址、IP 协议、传输层端口，甚至是数据包的负载部分内容，这种类型的路由选择被称作基于策略的路由。

基于策略的路由比传统路由功能更强，使用更灵活，它使网络管理者不仅能够根据目的地址，而且能够根据报文应用（TCP/UDP 端口号）或源 IP 地址来选择转发路径。

在报文转发控制方面，基于策略的路由比传统路由控制能力更强。策略路由可以在一定程度上实现流量工程，使不同服务质量的流或不同性质的数据（如语音和 FTP）走不同的路径。人们对网络性能的要求越来越高，按业务或用户类别差异来选择不同的数据包转发路径是很有必要的。

3.1.9 透明网桥

透明网桥（Transparent Bridging）用于连接物理介质类型相同的局域网，它主要应用在以太网环境中。透明网桥通常都保存一张网桥表，该网桥表记录目的 MAC 地址与接口之间的对应关系。常见透明网桥类型有 ATM 透明网桥、PPP 透明网桥、MP 透明网桥、帧中继透明网桥、X.25 透明网桥、HDLC 透明网桥以及 VLAN 透明网桥。

概括来说，网桥实现最重要的两点：

（1）MAC 学习。学习 MAC 地址，起初，网桥是没有任何地址与端口的对应关系的，它发送数据，还是得像 HUB 一样，但是每发送一个数据，它都会关心数据包的来源 MAC 是从自己的哪个端口来的，由于学习，建立地址-端口的对照表（CAM 表）。

（2）报文转发。每发送一个数据包，网桥都会提取其目的 MAC 地址，从自己的地址-端口对照表（CAM 表）中查找由哪个端口把数据包发送出去。

3.1.10 DHCP+

DHCP+认证技术是一种基于 DHCP 协议控制终端用户的 IP 地址分配，实现控制用户接入上网的认证鉴权技术。DHCP+的认证过程如下：DHCP 用户通过广播找到 DHCP 服务器，从回应的多个 DHCP 服务器中选一个提出申请，该服务器接受之后，通过认证用户的有关信息，确认是合法用户之后，就把相关参数，如 IP 地址、DNS 服务器、子网掩码、网关的地址等传送给用户。用户得到这些参数之后，就能直接进入网络进行通信，而所有的通信数据流无需经过 DHCP 服务器。

DHCP+具备传统的 DHCP 功能，如 IP 地址租用的申请、提供、选择和确认，以及 IP 更新租用、释放 IP 地址租用等。DHCP+认证技术主要是通过对 DHCP 协议进行扩展。目前，发展出的技术包括 DHCP+Web 认证和 DHCP+Client 认证两种方式。

3.1.11　网络探针

网络探针是对接入网络的计算机终端进行接入控制的一种程序，它由网络探针服务器和网络探针客户端两部分组成。它能够监测到同一子网内没有安装运行指定程序或没有进行入网授权的计算机，并采取措施自动将其引导至指定服务器下载指定程序或申请入网授权，也可以直接阻断这些计算机的网络通信。

3.1.12　EAPoU

EAPoU（Extensible Authentication Protocol over UDP）技术实际上网络准入的概念是 Cisco 普及的，Cisco 的 NAC 除了包含前面讨论的 EAPoL，还有 EAPoU（EAP over UDP）。与 EAPoL 是国际标准的协议不同，EAPoU 基本上是 Cisco 的专有协议或独家技术。EAPoU 是 Cisco NAC 技术的第一个实现版本，最早是 2003 年在 Cisco 的路由器上实现，后来在 Cisco 的 3 层交换机上也实现了 EAPoU。EAPoL 是在网络的接入层进行准入控制，而 EAPoU 是在网络的汇聚层或核心层进行准入控制。

EAPoU 的工作原理是当支持 EAPoU 的汇聚层设备接收到终端设备发来的数据包时，汇聚层 EAPoU 设备将要求终端设备进行 EAP 认证。EAP 认证包封装在 UDP 包内，在 EAP 认证的内容中，身份认证其实并不重要，重要的是安全状态认证。如果安全状态不符合企业策略，汇聚层 EAPoU 设备将从策略服务器上下载 ACL，限制不安全的客户端的网络访问，并对其进行修复。

EAPoU 技术的优点是它对网络接入设备要求不高，因而覆盖面较高；而且汇聚层设备一般明显少于接入层设备，因此部署相对要容易一些。EAPoU 有一个显著的缺点，即 EAP 协议要求数据包按顺序到达，而协议本身没有机制保证包的到达顺序，以前承载 EAP 包的底层协议比如 PPP、802.1x 都能保证数据包的顺序，而 UDP 不能保证数据包的顺序（在 IP 分片的情况下更严重），在大用户量的情况下，可能会产生显著的认证失败的问题，因此在 EAP 新的 RFC 标准文档里（RFC3748），已经明确写上了不建议采用 EAPoU 的语句。所以 EAPoU 没有成为一个国际标准，在潮流转向 EAPoL 的情况下，EAPoU 得不到更多的厂商支持，只有 Cisco 独家支持。EAPoU 的其他缺点包括控制强制性不如 EAPoL，因为 EAPoU 的控制点在汇聚层，而不是接入层，离终端越远，控制力越弱。如果终端不受管理，即使其不符合安全策略，它只是不能访问汇聚层以后的网络，而可以照常访问其所在的接入层的网络。

3.1.13　L2-OOB-VG 虚拟网关

Cisco 最早提出 L2-OOB-VG（VG：虚拟网关，OOB：Out-Of-Band，VG：Virtual Gateway）技术，但只适合采用 Cisco 网络交换机的大型局域网。原理是通过 VG 设备管理 Cisco 的交换机，并在交换机上划分可信 VLAN 和不可信

VLAN，如果入网设备没安装客户端软件或没有进行入网注册，则通过下发命令将对应端口划入不可信 VLAN 进行重定向安装客户端，安装完成后再下发命令将对应端口划入可信 VLAN 批准入网，通过客户端对入网设备进行安全检查，如果符合要求则批准访问网络资源，如果不符合则禁止访问网络资源。

优点：不使用 802.1x，但能够实现比 802.1x 更强的管理效果。

采用对交换机端口接入设备的检测，然后通过真实 VLAN 与虚拟 VLAN（没有接口地址的 VLAN）端口所属 VLAN 切换，同时实现了对网络内部相同子网不同 VLAN 之间报文通信进行控制和实现。

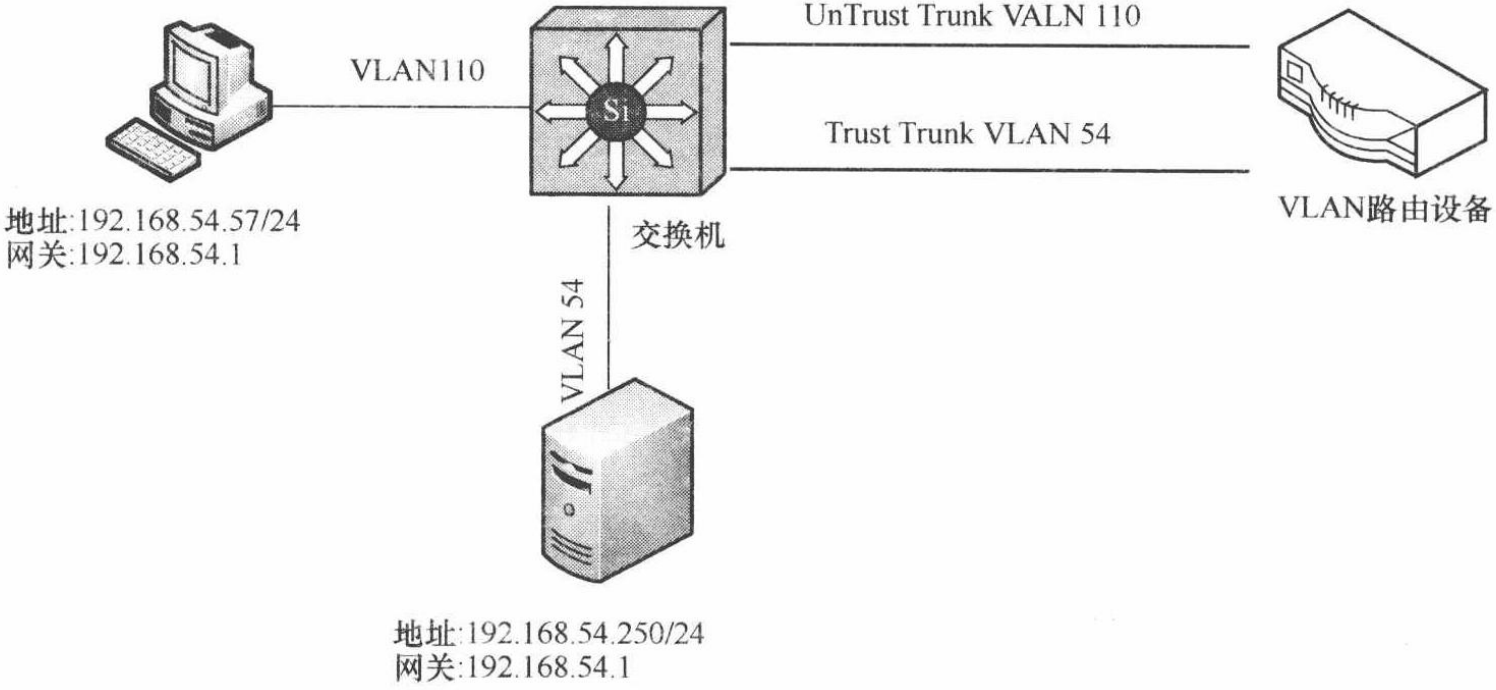
具体方法主要是，由于和交换机的连接方式是 Trunk 连接，且设置报文的封包格式为 802.1Q（通过 switchport trunk encapsulation dot1q 命令），交换机在将报文发送过来的时候会附带 802.1Q 的 TAG，VLAN 路由设备根据系统设置的 VLAN 路由信息或者其他配置的一些安全策略等相关信息，进行相应报文 TAG 的修改，并通过 TRUNK 连接发回给交换机，完成 VLAN 之间路由通信的工作。如在图 3-2 中所说明的，当终端电脑 54.57 希望和 54.250 通信时候，由于设备处于认证 VLAN，交换机发送过来的 VLAN ID 为 110，VLAN 路由设备根据配置的路由映射关系，将 110 的 VLAN ID 修改为 54，然后通过 Trust 的接口发送回交换机，即可实现 54.57 对 54.250 的访问，即完成设备即使处于 110VLAN 子网为 54 仍然可以和 VLAN 54 中子网 54 的设备通信功能。

图 3-2 实际应用示例

在报文经过 VLAN 路由之后，使得具有以下有效效果。

（1）经过 VLAN 路由之后，使得不同 VLAN 之间的报文在两层时候即可进行通信，解决了相同子网在不同 VLAN 之间无法通信的问题，这个对于静态地址下面的 802.1X 来宾访问或者认证访问的意义重大。

（2）由于可以在外部进行报文的 VLAN 路由，可以根据各种认证要求，安全要求或者管理要求等方式对报文进行路由判读和控制，扩充了交换机的功能，


UnTrust Trunk VALN 110
VLAN110
Trust Trunk VLAN 54
S1
地址:192.168.54.57/24
网关:192.168.54.1
交换机
VLAN路由设备
VLAN 54
地址:192.168.54.250/24
网关:192.168.54.1

VLAN，如果入网设备没安装客户端软件或没有进行入网注册，则通过下发命令将对应端口划入不可信 VLAN 进行重定向安装客户端，安装完成后再下发命令将对应端口划入可信 VLAN 批准入网，通过客户端对入网设备进行安全检查，如果符合要求则批准访问网络资源，如果不符合则禁止访问网络资源。

优点：不使用 802.1x，但能够实现比 802.1x 更强的管理效果。

采用对交换机端口接入设备的检测，然后通过真实 VLAN 与虚拟 VLAN（没有接口地址的 VLAN）端口所属 VLAN 切换，同时实现了对网络内部相同子网不同 VLAN 之间报文通信进行控制和实现。

具体方法主要是，由于和交换机的连接方式是 Trunk 连接，且设置报文的封包格式为 802.1Q（通过 switchport trunk encapsulation dot1q 命令），交换机在将报文发送过来的时候会附带 802.1Q 的 TAG，VLAN 路由设备根据系统设置的 VLAN 路由信息或者其他配置的一些安全策略等相关信息，进行相应报文 TAG 的修改，并通过 TRUNK 连接发回给交换机，完成 VLAN 之间路由通信的工作。如在图 3-2 中所说明的，当终端电脑 54.57 希望和 54.250 通信时候，由于设备处于认证 VLAN，交换机发送过来的 VLAN ID 为 110，VLAN 路由设备根据配置的路由映射关系，将 110 的 VLAN ID 修改为 54，然后通过 Trust 的接口发送回交换机，即可实现 54.57 对 54.250 的访问，即完成设备即使处于 110VLAN 子网为 54 仍然可以和 VLAN 54 中子网 54 的设备通信功能。

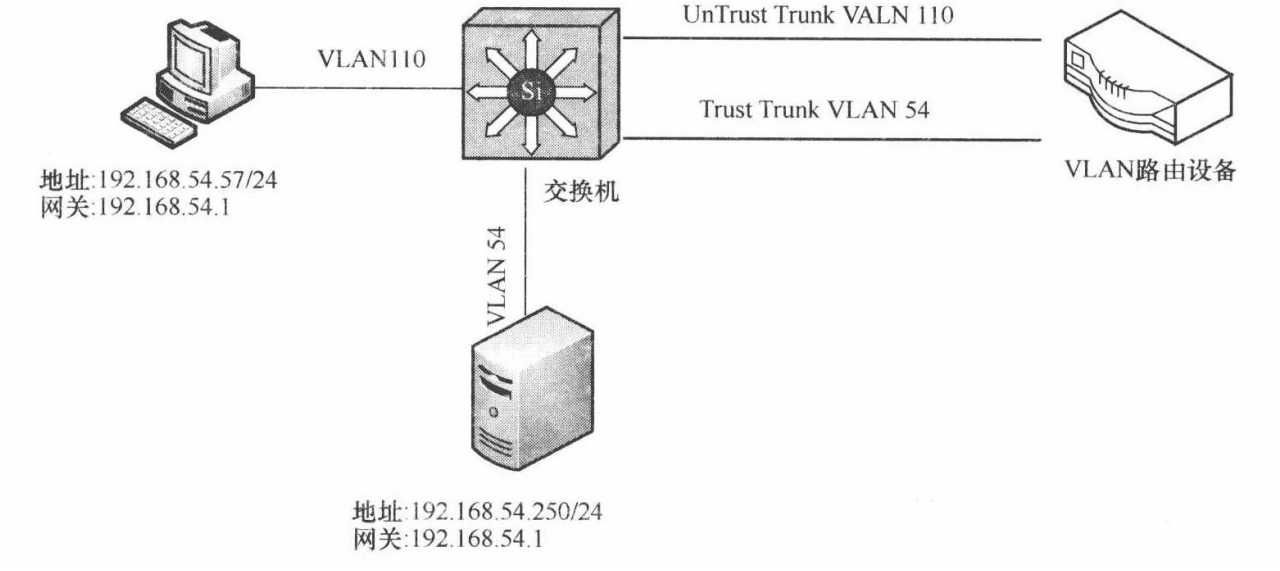


图 3-2 实际应用示例

在报文经过 VLAN 路由之后，使得具有以下有效效果。

（1）经过 VLAN 路由之后，使得不同 VLAN 之间的报文在两层时候即可进行通信，解决了相同子网在不同 VLAN 之间无法通信的问题，这个对于静态地址下面的 802.1X 来宾访问或者认证访问的意义重大。

（2）由于可以在外部进行报文的 VLAN 路由，可以根据各种认证要求，安全要求或者管理要求等方式对报文进行路由判读和控制，扩充了交换机的功能，

提高了企业内部网络的安全性，可以根据企业的业务需要开发出不同的安全系统。

（3）对于子网数目或者IP资源紧张的企业，通过将不同的VLAN共用一个子网，可以极大地节省IP地址资源。

3.1.14　终端主机防火墙

主要技术原理是通过终端防火墙（基于TDI、NDIS网络协议技术），根据终端安全状况，控制终端是否允许访问网络。甚至可以控制终端的哪些应用（程序）访问网络，通过安装了终端防火墙软件的客户端拒绝让未安装客户端的终端访问。但是务必要求终端安装有具有防火墙功能的客户端软件，如果没有安装客户端软件就无法实现准入的功能。另外，客户端软件也需要具有防止终端用户删除，停止程序运行。

在安全接入管理系统中，把所有的终端划分成了非法主机、合法主机和超级主机3个类别。

非法主机就是没有在系统中经过任何形式认证的主机，其网络通信会收到最多的限制：只能和超级主机通信，不能和其他的非法主机和合法主机通信。

合法主机就是在系统中经过认证的主机，主要包括两种：第一种是装过客户端的主机，会自动成为合法主机；第二种是管理员通过控制台手工添加的信任主机。合法主机的网络通信收到的限制很少，除了与非法主机不能通信外，其余的通信都不受影响。合法主机应该是网络中存在最多的主机类型。

超级主机是一种特别的合法主机，只能由管理员通过控制台手工设定。超级主机的通信是不受任何限制的，它既可以和其他超级主机、信任主机通信，也可以和任何非法主机进行正常通信。超级主机主要用于需要向非法主机开放访问时使用，比如非法主机也可以访问某个服务器完成客户端安装功能，那么这台服务器就需要被指定为超级主机。安全接入管理服务器自身默认会成为超级主机。

对于以上3种类别主机之间的通信许可，可以表示如下：

非法主机<——>非法主机，禁止通信；

非法主机<——>合法主机，禁止通信；

非法主机<——>超级主机，允许通信；

合法主机<——>合法主机，允许通信；

合法主机<——>超级主机，允许通信；

超级主机<——>超级主机，允许通信。

指定信任主机和超级主机的方法主要是通过输入要指定主机的IP地址和MAC地址，两种地址可以单独输入，也可以同时输入。如果只输入一个，则另外一个是任意值都可以正确识别，如果两个都输入，则必须IP和MAC都与输入值相匹配才能被正确识别。

在实际使用环境中，可以根据需要手工指定合法主机和超级主机，以实现相

应的功能，举例如下：

① 如果网关和内部的一些服务器不能或不希望安装客户端，而希望其他合法主机能够访问的话，可以手工将其指定为合法主机；

② 对于非法主机，不希望其使用内部网络资源，但是希望其可以访问互联网的话，可以手工将网关设定为超级主机；

③ 对于指定的服务器，如防病毒管理服务器，终端安全管理服务器等，希望任何主机都可以访问的话，可以手工将其指定为超级主机。

3.1.15 DNS 重定向

DNS 是计算机域名系统（Domain Name System 或 Domain Name Service）的缩写，它是由解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应 IP 地址，并具有将域名转换为 IP 地址功能的服务器。其中域名必须对应一个 IP 地址，而 IP 地址不一定有域名。域名系统采用类似目录树的等级结构。域名服务器为客户机/服务器模式中的服务器方，它主要有两种形式：主服务器和转发服务器。在 Internet 上域名与 IP 地址之间是一对一（或者多对一）的，也可采用 DNS 轮循实现一对多，域名虽然便于人们记忆，但机器之间只认 IP 地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。DNS 命名用于 Internet 的 TCP/IP 网络中，通过用户友好的名称查找计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与之相关的其他信息，如 IP 地址。因为，你在上网时输入的网址，是通过域名解析系统解析找到了相对应的 IP 地址，这样才能上网。其实，域名的最终指向是 IP。

在 IPv4 中 IP 是由 32 位二进制数组成的，将这 32 位二进制数分成 4 组每组 8 个二进制数，将这 8 个二进制数转化成十进制数，就是我们看到的 IP 地址，其范围是在 0～255 之间。因为，8 个二进制数转化为十进制数的最大范围就是 0～255。现在已开始试运行、将来必将代替 IPv4 的 IPv6 中，将以 128 位二进制数表示一个 IP 地址。

DNS 域名管理系统域名是由圆点分开一串单词或缩写组成的，每一个域名都对应一个唯一的 IP 地址，这一命名的方法或这样管理域名的系统叫做域名管理系统。

大家在上网的时候，通常输入的是网址，其实这就是一个域名，而网络上的计算机彼此之间只能用 IP 地址才能相互识别。再如，客户到 Web 服务器中请求一 Web 页面，可以在浏览器中输入网址或者是相应的 IP 地址，例如客户要上新浪网，就可以在 IE 的地址栏中输入网址，也可输入 IP 地址，但是这样子的 IP 地址很难记住，所以有了域名的说法，这样的域名会让客户容易的记住。

申请了 DNS 后，客户可以自己为域名作解析，或增设子域名。客户申请 DNS 时，建议客户一次性申请两个。

DNS 服务器在域名解析过程中的查询顺序为：本地缓存记录、区域记录、转发域名服务器、根域名服务器。

目前也有些技术是利用 DNS 劫持的原理，修改注册信息、劫持解析结果。在 DNS 重定向机制中，将终端的所有 DNS 解析请求（不管其请求解析的是什么域名），全部指定到一个固定的服务器 IP 地址。这种技术类似于 DHCP 管理和 ARP spoofing，适用于任何使用 DNS 协议的网络，易于安装和部署。可以支持 Web Portal 页面，可以通过 DNS 重定向，将终端的 HTML 请求重定向到 Web 认证和安全检查页面。

3.1.16　NAP

如果网络设备不支持网络准入，或不想花费太多的部署和管理时间，还可以利用基于主机的准入控制。在此处的主机是指网络中除网络设备外的电脑主机，包括服务器和电脑终端。基于主机的准入控制（NAP）最大特点就是容易部署。

系统及应用准入是在服务器的操作系统上安装准入控制软件，当电脑终端访问服务器时，准入控制软件会检查对方的安全状态，如果符合策略则允许访问，如果不符合将拒绝对方的访问，并给出相关提示。而客户端准入控制是终端相互之间访问时，安装在终端上的软件也会检查对方的安全状态。基于主机的准入控制点一般安装在代理服务器、邮件服务器、内网 Web 服务器、DNS 服务器上或 DHCP 服务器上。这些服务器是企业内部员工最常访问的服务器，因此准入效果较好，覆盖面广。实际部署时，一般只需在 1～2 个服务器上部署控制点即可做到对全局的控制。

基于主机的准入控制优点首先是容易部署，一般网络准入配置起来都较复杂，不同型号的设备的配置都各不相同，如果网络规模较大，配置的工作量极其巨大，而基于主机的准入控制只需要在对应的主机上安装一个软件，相对而言容易得多。第二是适应性好、覆盖面广、不依赖任何网络设备的支持，可有效保护企业已有的投资。第三是对网络性能没有影响，基于网络的准入控制在运行时会根据客户端的认证状态和安全状态改变自己的状态，比如 VLAN 切换和动态 ACL 加载，这或多或少都将影响设备或网络的性能，特别是在大规模网络环境下，这一点不能忽视。基于主机的准入控制将其控制分散到每个终端和主机上，终端的状态变化对网络没有任何影响。第四是其访问控制功能是所有方案中最强的，基于主机的准入控制能够做到基于进程的访问控制，以及基于进程的带宽管理，因此对蠕虫、木马的防治就能更加积极主动。基于主机的准入控制的缺点主要是控制强度较弱，系统及应用准入控制点处于内网的核心，远离终端，而客户端准入依赖于网络中已经广泛部署的客户端。

3.2　基于端点的网络准入控制架构

第 1 章中曾经提到 Forrester 对 NAC 技术框架的划分，对于绝大多数 NAC

制造商而言，网络准入控制架构（Software-Based NAC）都是最容易实现的一种技术架构，这也成为了 NAC 入门的一种廉价方案。在国内，绝大多数的终端管理软件厂商都实现过或正在采用这种成本低且有一定适用性的 NAC 方案。

但是，Software-Based NAC 方案的缺点也是显而易见的，其最致命之处就是稳定性不足，因此 100%的大型网络（1000 点以上）机构都不会将这类技术架构的方案列入其 NAC 的采购名单中，Software-Based NAC 架构最常见的存在方式往往见于那些规模较小（100 点以下）或预算不高的机构网络中。

3.2.1 ARP 网络准入控制技术分析

ARP 准入控制技术，顾名思义就是利用 RFC 826 中定义的 ARP 协议所实现的对终端接入进行控制的技术。由于 ARP 欺骗的阻断方式技术实现较简单，故被国内大部分厂商所采用，特别是针对未注册阻断、非法访问的阻断等，往往都采用 ARP 欺骗的阻断方式。

如上所述，以前大多数内网安全产品在防止非法接入时主要使用 ARP 欺骗的阻断方式。事实上这种技术在 NAC 之外的领域往往被归类为一种安全威胁，也即是 ARP 欺骗。因此，作为廉价 NAC 实现的 ARP 准入控制技术从一开始就名声不好，这也决定了 ARP 在大部分具有正规网络安全素养的管理员眼中是一种不入流的准入控制技术。所以，ARP 欺骗阻断对于内网安全产品而言，需要科学合理运用才能发挥最大的功效。

可以用一句话来总结应用代理准入控制的特点：应用网关的软件防火墙控制技术。基于 ARP 的网络准入控制技术最大的优点就是无需安装代理，易用、部署简单，但通过 ARP 欺骗阻断存在很多不足：正是由于没有代理，因此 ARP 网络准入控制只是提供网络安全防护，不能提供主机安全防护功能，而且安全性没有 802.1x 方式高。即便如此，通过分析 ARP 网络准入控制技术仍然可以帮助我们从基本层面了解 NAC 的基本实现目的。

1. 技术实现原理

1）ARP 概述

在以太网协议中规定，同一局域网中的一台主机要和另一台主机进行直接通信，必须要知道目标主机的 MAC 地址。而在 TCP/IP 协议栈中，网络层和传输层只关心目标主机的 IP 地址。这就导致在以太网中使用 IP 协议时，数据链路层的以太网协议接到上层 IP 协议提供的数据中，只包含目的主机的 IP 地址。于是需要一种方法，根据目的主机的 IP 地址，获得其 MAC 地址。这就是 ARP 协议要做的事情。所谓地址解析（address resolution）就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。

2）ARP 工作原理

在每台安装有 TCP/IP 协议的电脑里都有一个 ARP 缓存表，图 3-3 中所示的 IP 地址与 MAC 地址是一一对应的。

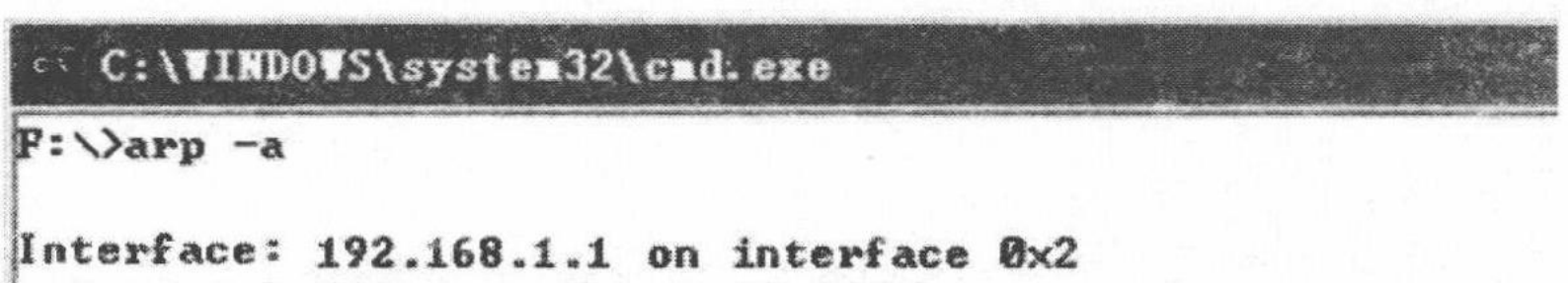
IP 地址	MAC 地址
192.168.1.1	00－aa－00－62－c6－09
192.168.1.2	00－aa－00－62－c5－03
192.168.1.3	03－aa－01－75－c3－06
……	……

图 3-3　AEP 缓存表示意图

以主机 A（192.168.1.5）向主机 B（192.168.1.1）发送数据为例。当发送数据时，主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址。如果找到了，也就知道了目标 MAC 地址，直接把目标 MAC 地址写入帧里面发送就可以了；如果在 ARP 缓存表中没有找到目标 IP 地址，主机 A 就会在网络上发送一个广播，A 主机 MAC 地址是“主机 A 的 MAC 地址”，这表示向同一网段内的所有主机发出这样的询问：“我是 192.168.1.5，我的硬件地址是主机 A 的 MAC 地址，请问 IP 地址为 192.168.1.1 的 MAC 地址是什么?”网络上其他主机并不响应 ARP 询问，只有主机 B 接收到这个帧时，才向主机 A 做出这样的回应：“192.168.1.1 的 MAC 地址是 00-aa-00-62-c6-09”。这样，主机 A 就知道了主机 B 的 MAC 地址，它就可以向主机 B 发送信息了。同时 A 和 B 还同时都更新了自己的 ARP 缓存表（因为 A 在询问的时候把自己的 IP 和 MAC 地址一起告诉了 B），下次 A 再向主机 B 或者 B 向 A 发送信息时，直接从各自的 ARP 缓存表里查找就可以了。ARP 缓存表采用了老化机制（即设置了生存时间 TTL），如果在一段时间内（一般 15～20min）表中的某一行没有使用，就会被删除，这样可以大大减少 ARP 缓存表的长度，加快查询速度。

3）ARP 准入原理

如前所述，由于局域网的网络流通不是根据 IP 地址进行，而是按照 MAC 地址进行传输，所以，那个伪造出来的 MAC 地址在 A 上被改变成一个不存在的 MAC 地址，这样就会造成网络不通，导致 A 不能 Ping 通 C。这就是一个简单的 ARP 欺骗过程。


C:\WINDOWS\system32\cmd.exe
F:\>arp -a
Interface: 192.168.1.1 on interface 0x2
Internet Address Physical Address Type
192.168.1.1 00-aa-00-62-c6-09 static
F:\>

2）ARP 工作原理

在每台安装有 TCP/IP 协议的电脑里都有一个 ARP 缓存表，图 3-3 中所示的 IP 地址与 MAC 地址是一一对应的。

IP 地址	MAC 地址
192.168.1.1	00－aa－00－62－c6－09
192.168.1.2	00－aa－00－62－c5－03
192.168.1.3	03－aa－01－75－c3－06
……	……

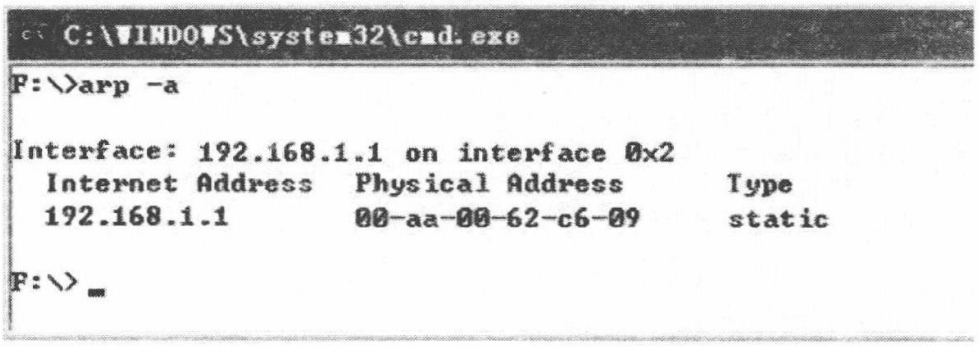


图 3-3　AEP 缓存表示意图

以主机 A（192.168.1.5）向主机 B（192.168.1.1）发送数据为例。当发送数据时，主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址。如果找到了，也就知道了目标 MAC 地址，直接把目标 MAC 地址写入帧里面发送就可以了；如果在 ARP 缓存表中没有找到目标 IP 地址，主机 A 就会在网络上发送一个广播，A 主机 MAC 地址是“主机 A 的 MAC 地址”，这表示向同一网段内的所有主机发出这样的询问：“我是 192.168.1.5，我的硬件地址是主机 A 的 MAC 地址，请问 IP 地址为 192.168.1.1 的 MAC 地址是什么?”网络上其他主机并不响应 ARP 询问，只有主机 B 接收到这个帧时，才向主机 A 做出这样的回应：“192.168.1.1 的 MAC 地址是 00-aa-00-62-c6-09”。这样，主机 A 就知道了主机 B 的 MAC 地址，它就可以向主机 B 发送信息了。同时 A 和 B 还同时都更新了自己的 ARP 缓存表（因为 A 在询问的时候把自己的 IP 和 MAC 地址一起告诉了 B），下次 A 再向主机 B 或者 B 向 A 发送信息时，直接从各自的 ARP 缓存表里查找就可以了。ARP 缓存表采用了老化机制（即设置了生存时间 TTL），如果在一段时间内（一般 15～20min）表中的某一行没有使用，就会被删除，这样可以大大减少 ARP 缓存表的长度，加快查询速度。

3）ARP 准入原理

如前所述，由于局域网的网络流通不是根据 IP 地址进行，而是按照 MAC 地址进行传输，所以，那个伪造出来的 MAC 地址在 A 上被改变成一个不存在的 MAC 地址，这样就会造成网络不通，导致 A 不能 Ping 通 C。这就是一个简单的 ARP 欺骗过程。

ARP 准入就是利用 ARP 协议在局域网中传播不需要验证身份，可以随意被篡改目的 MAC 地址的漏洞，由授权主机向网络中发出大量的 ARP 欺骗报文，从而达到阻断非授权主机进入网络的目的。

从技术原理上看，ARP 准入的实现方式分为两类：一类是对交换机 ARP 表的欺骗；另一类是对内网 PC 的网关的欺骗。第一类 ARP 准入的原理是——影响交换机对于数据的转发，所有非授权主机去往目的地的数据帧都将被交换机转发到错误的地址上，这样就实现了拒绝其访问目的地的目的。

在实现的过程中，授权发送欺骗包的主机将通知交换机一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在交换机中，结果交换机的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。第二种 ARP 准入的原理是——将自身伪造成网关。所有非授权主机的跨网段访问数据都将被交换机转发到发送欺骗包的主机上，而不是通过正常的路由器途径上网，这样也实现了阻断连接的目的。

2. 工作过程

可以通过一个实例来分析 ARP 准入的工作过程，假设在模拟网络环境中有 3 台主机，分别为主机 A，B，C。主机详细信息如下描述：

A 的 IP 地址为 192.168.10.1，MAC 地址 AA-AA-AA-AA-AA-AA

B 的 IP 地址为 192.168.10.2，MAC 地址 BB-BB-BB-BB-BB-BB

C 的 IP 地址为 192.168.10.3，MAC 地址 CC-CC-CC-CC-CC-CC

我们指定主机 B 为网络中授权实现 ARP 准入的客户机，一般情况下会在这台主机 B 上安装一个发送 ARP 欺骗包的客户端软件。在正常情况下，A 和 C 之间进行通信，但是此时 B 通过 ARP 准入控制客户端软件向 A 发送一个自己伪造的 ARP 应答，在应答中发送方 IP 地址是主机 C 的 IP 地址，但 MAC 地址被伪造成主机 B 的 MAC 地址 BB-BB-BB-BB-BB-BB。当主机 A 接收到主机 B 伪造的 ARP 应答数据后，就会更新主机 A 的 ARP 缓存，这时 B 就伪装成 C 了，这样所有从 A 发往主机 C 的数据包都会到达主机 B，并且由于 A 未经过授权，因此数据包会被 B 丢弃，从而实现了拒绝 A 连接 C 的目的。

另外一个可选的实现是，在 B 欺骗 A 的同时，B 同样向 C 发送一个 ARP 应答，应答包中发送方 IP 地址四 192.168.10.1（A 的 IP 地址），MAC 地址是 BB-BB-BB-BB-BB-BB（A 的 MAC 地址本来应该是 AA-AA-AA-AA-AA-AA），当 C 收到 B 伪造的 ARP 应答，也会更新本地 ARP 缓存（C 也被欺骗了）。

3. 主要特点

ARP 网络准入控制技术无需安装代理、易用、部署简单，但是由于这种控制技术是基于 ARP 欺骗的原理，所以，在很多情况下容易被恶意接入者通过各种反 ARP 欺骗手段绕过，从而攻破 ARP 准入系统。具体来讲，通过 ARP 欺骗

实现 NAC 阻断主要存在以下不足。

1）采用 ARP 欺骗阻断方式对网络的负荷影响很大

ARP 工作时，首先请求主机会发送出一个含有所希望到达的 IP 地址的以太网广播数据包，然后目标 IP 的所有者会以一个含有 IP 和 MAC 地址的数据包应答请求主机。在 ARP 欺骗阻断的实现中，一个 ARP 请求可能会收到数十个、甚至数百个 ARP 应答，有些 ARP 欺骗阻断程序还通过主动发 ARP 请求实现欺骗，因此，在网络中采用大量发 ARP 包的动作对于网络资源的占用是十分巨大的，可能导致网络设备性能下降，影响用户正常的业务。

2）ARP 欺骗阻断方式准入效果不可靠

ARP 欺骗并不能 100%保证有效，比如目标机器的 ARP 应答包和欺骗包都能正确达到 ARP 请求者，请求者是否被欺骗还存在一定的机率，譬如请求者的客户端安装了防 ARP 欺骗的软件，所以，如果采用 ARP 欺骗包来实现终端设备的准入控制，效果就可想而知，其自身的缺陷，使得准入的可靠性大为降低。

3）ARP 欺骗阻断和真正的 ARP 欺骗难以区分

在一个网络内如果启用了 ARP 欺骗阻断，当真的发生 ARP 欺骗时，后果将是灾难性的。用户将不能区分主动的 ARP 欺骗阻断和真正的 ARP 欺骗，这会给用户的故障排除带来极大的困难，严重影响用户业务。另一方面，在大多数 ARP 欺骗阻断的技术实现中，往往是子网内的所有电脑同时对目标电脑进行欺骗，如果目标电脑无需再受欺骗阻断，要求所有电脑停止对其进行欺骗，而此时如果个别电脑没有收到停止欺骗的指令，将导致目标电脑不能正常访问网络，导致用户运维事故。

ARP 准入控制技术由于需要准入客户端向网络内发送大量的欺骗数据包，这种处理过程很容易造成正常的授权入网机器也被欺骗并导致断网，同时，大大增加了网络中数据传输的负担，而且在每台机器上安装准入客户端的做法也会给管理员带来巨大的实施和维护工作量。所以，从系统自身安全性、稳定性和维护度的角度看，ARP 准入都是最低端的一种准入控制技术。

4. 部署与配置方法

图 3-4 描述了基于 ARP 的准入控制系统的部署方式，与 802.1x 的 Guest VLAN 区不同，ARP 隔离区和工作区在同一个 VLAN 中，通过 ARP 屏蔽隔离区主机和正常主机之间的数据通信。管控服务器通过合法主机检测和网络风险检测对接入主机进行干扰。

“安全管控服务器”的接口接入方式有两种，一种是服务器配置多个网卡，每个网卡接入一个 VLAN；另外一种是交换机配置 Truck 口，服务器的管理口和 Truck 口连接。第一种部署简单，无需配置交换机，但是对于 VLAN 比较多的情况不太适合；第二种适合 VLAN 个数多于服务器接口数的情况，需要为交换机配置一个 Truck 口，并把需要管控的 VLAN 都与该 Truck 口绑定。

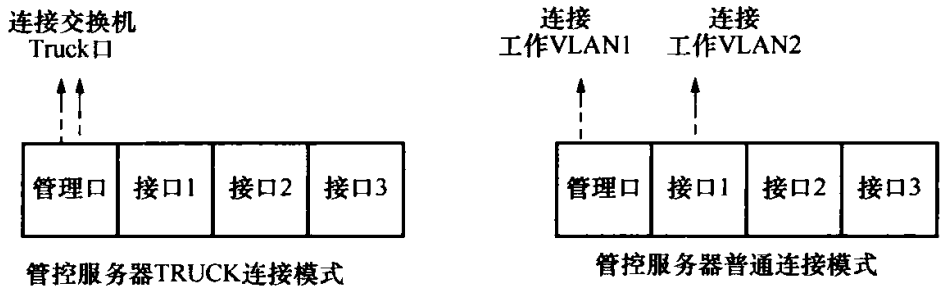


图 3-4 基于 ARP 管理的网络准入控制部署示意图

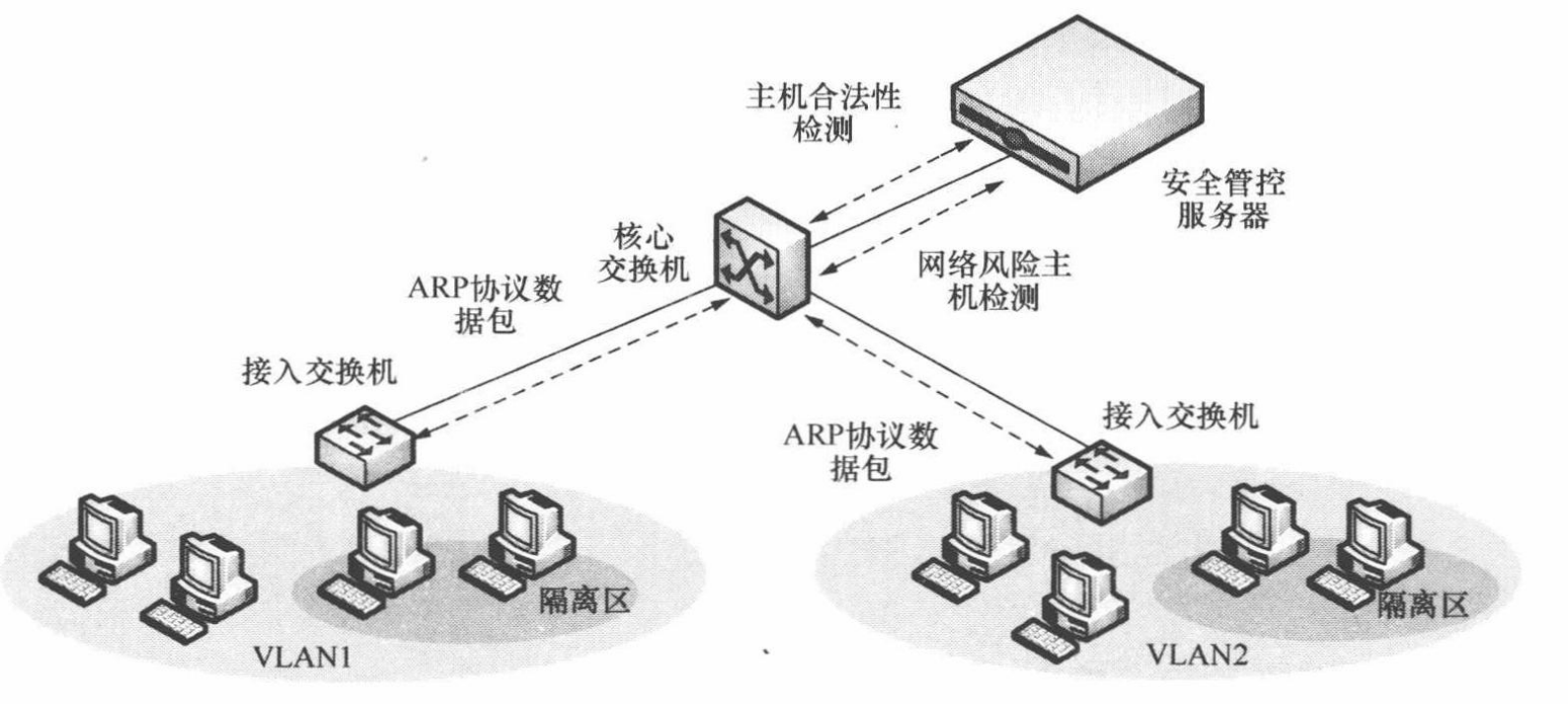
ARP 准入控制技术就是利用 ARP 协议在局域网中由授权主机向网络中发出大量的 ARP 欺骗报文，从而达到阻断非授权主机进入网络的目的。

ARP 准入技术一般不需要在交换机上配置任何命令，只需要网内所有授权接入的机器都安装一个证明其合法性的准入客户端即可，同时管理员需要在系统后台指定一台机器探测新接入的非授权机器，并向其发送 ARP 欺骗数据包。

3.2.2 应用代理网络准入控制技术分析

应用代理准入控制技术或者说网络探针接入控制技术是比 ARP 准入控制技术更为原始的一种架构，是一种无需依赖于网络交换设备的接入控制技术，其本质上就是利用已有的代理服务器进行端口、服务、可访问地址的一种限制，在某种意义上可以看作利用一台网关型的防火墙来实现访问控制，从而达到 NAC 最基本的功能之一。

现代企业或单位，出于保密目的可能会要求接入单位内部网络的办公计算机终端安装指定的程序，或者通过一定的程序或网络安全技术进行计算机终端网络准入授权。在这个前提下，作为网络管理人员来说，就要做到了解掌握哪些计算机终端没有进行网络准入授权或没有安装指定程序，同时能够做到严格控制这些计算机终端使其无法接入网络。要实现以上技术，通常情况下需要结合网络交换设备一同使用，但是在网络交换设备无法达到以上技术要求的情况下，就需要采


主机合法性
检测
安全管控
服务器
核心
交换机
网络风险主
机检测
ARP协议数
据包
接入交换机
ARP协议数
据包
接入交换机
隔离区
VLAN1
隔离区
VLAN2

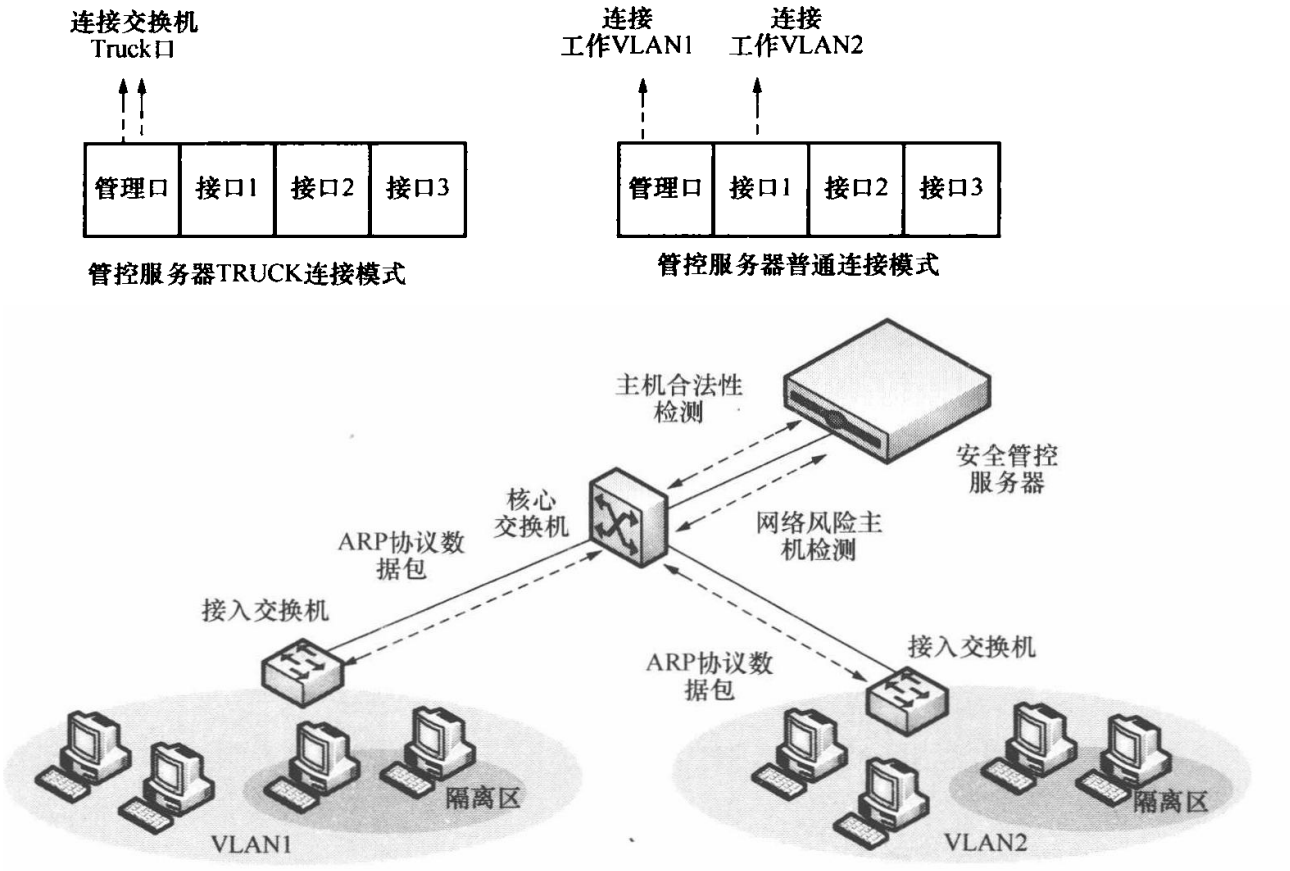


图 3-4 基于 ARP 管理的网络准入控制部署示意图

ARP 准入控制技术就是利用 ARP 协议在局域网中由授权主机向网络中发出大量的 ARP 欺骗报文，从而达到阻断非授权主机进入网络的目的。

ARP 准入技术一般不需要在交换机上配置任何命令，只需要网内所有授权接入的机器都安装一个证明其合法性的准入客户端即可，同时管理员需要在系统后台指定一台机器探测新接入的非授权机器，并向其发送 ARP 欺骗数据包。

3.2.2 应用代理网络准入控制技术分析

应用代理准入控制技术或者说网络探针接入控制技术是比 ARP 准入控制技术更为原始的一种架构，是一种无需依赖于网络交换设备的接入控制技术，其本质上就是利用已有的代理服务器进行端口、服务、可访问地址的一种限制，在某种意义上可以看作利用一台网关型的防火墙来实现访问控制，从而达到 NAC 最基本的功能之一。

现代企业或单位，出于保密目的可能会要求接入单位内部网络的办公计算机终端安装指定的程序，或者通过一定的程序或网络安全技术进行计算机终端网络准入授权。在这个前提下，作为网络管理人员来说，就要做到了解掌握哪些计算机终端没有进行网络准入授权或没有安装指定程序，同时能够做到严格控制这些计算机终端使其无法接入网络。要实现以上技术，通常情况下需要结合网络交换设备一同使用，但是在网络交换设备无法达到以上技术要求的情况下，就需要采

取其他方法来达到对计算机终端进行入网接入控制的要求。网络探针技术就是其中一个很好的选择。

网络探针是对接入网络的计算机终端进行接入控制的一种程序，网络探针角色是网络探针服务器在安装有网络探针客户端的计算机终端中自动指定的，网络探针有限制计算机访问服务器工作模式和阻断计算机访问网络工作模式。网络探针对于网络交换设备没有依赖性，不会对网络带宽产生影响。通过网络探针，能够实现全网接入集中式管理控制。

在前些年大家还是比较着重网络基础环境的建设，并且网络基础环境的建设都比较简单，而随着网络交换等基础技术的快速发展，当时又需要实现很多的网络安全管理，信息安全的要求。在当时的环境条件下，采用应用代理网络探针技术来实现终端接入。因此，采用应用代理准入控制的机构大多数是网络建设较早，基础设备陈旧，且不愿意另外购买准入产品的用户。在这种情况下，网络管理员为实现基本的准入控制效果，就在网络中已有的代理服务器上进行相关的配置，从而分角色进行访问权限的控制。在国内，应用代理准入控制基本上已经被其他标准的准入控制架构所代替。

1. 技术实现原理

应用代理准入控制，主要是在机构已搭建好的代理服务器（一般是 Linux 系统）上进行规则的设置，用类似于 ACL 的方式来对通过代理服务器进行访问的接入主机进行权限的限制。而应用代理中 ACL 的控制在 Linux 系统下主要是通过 IP tables 工具来实现的，一般的实现规则是没有明确定义的就进行拒绝（deny），只有明确授权（permit）的数据包才会被转发给目的端口。

网络探针是对接入网络的计算机终端进行接入控制的一种程序，它由网络探针服务器和网络探针客户端两部分组成。它能够监测到同一子网内没有安装运行指定程序或没有进行入网授权的计算机，并采取措施自动将其引导至指定服务器下载指定程序或申请入网授权，也可以直接阻断这些计算机的网络通信。

1）网络探针的轮询功能

由哪台计算机终端担任网络探针角色是网络探针服务器在安装有网络探针客户端的计算机终端中自动指定的，不需要网络管理员的特别指定，这样就杜绝了指定计算机终端没有开机，无法运行网络探针客户端的可能性。

网络探针轮询功能的优点是只要同一子网内的计算机终端有一台运行网络探针客户端，就可以保证网络探针对整个网络探测子网生效。当指定计算机终端关机或断开网络后，网络探针服务器会自动将网络探针角色赋予另一台运行了网络探针客户端的计算机终端，并同时保证在同一时间，同一子网内只有一台安装有网络探针客户端的计算机终端具有网络探针功能，担任网络探针角色。

2）网络探针限制计算机访问服务器工作模式

当网络探针发现没有安装指定程序或授权的计算机终端试图通过 HTTP、

FTP、SMTP 等协议访问网络域名时，将自动截断其访问网络的 DNS 请求，将要访问域名对应的 IP 地址转换为指定服务器的 IP 地址，这样计算机终端得到的是假的域名解析结果，访问路径会跳转至指定服务器，下载并安装指定程序或进行授权认证。

3）网络探针阻断计算机终端访问网络工作模式

网络探针可以利用 ARP 重定向技术阻断网络探针检测到的没有安装指定程序或授权的计算机终端试图访问网络的行为。例如，当这些计算机终端试图通过网关访问外部网络时，网络探针会告知网关设备这些计算机终端的 IP 地址和与 IP 地址对应的错误的 MAC 地址，这样网关设备就不能将数据包转发至这些计算机终端，同理，网络探针也会告知这些计算机终端网关设备的 IP 地址和一个与网关 IP 对应的错误 MAC 地址，这样，计算机终端就不能将数据包发送至网关。

同理，在网络探针的阻断计算机终端访问网络工作模式下，没有安装指定程序或授权的计算机也是无法和内网中的其他计算机终端进行通信的。

2. 工作过程

以 Linux 下最为流行的代理服务器软件 Squid 为例，在代理服务器中存在 Forward 链、Input 链和 Output 链，当一个数据包被代理服务器收到时，将经过如下的处理流程：

Step1：如果数据包的目的地址是本机，则系统将数据包送往 Input 链。如果通过规则检查，则该包被发给相应的本地进程处理；如果没有通过规则检查，系统就会将这个包丢掉。

Step2：如果数据包的目的地址不是本机，也就是说，这个包将被转发，则系统将数据包送往 Forward 链。如果通过规则检查，则该包被发给相应的本地进程处理；如果没有通过规则检查，系统就会将这个包丢掉。

Step3：如果数据包是由本地系统进程产生的，则系统将其送往 Output 链。如果通过规则检查，则该包被发给相应的本地进程处理；如果没有通过规则检查，系统就会将这个包丢掉。

在上述的 Step2 中，管理员可以自定义访问规则，从而对非授权的数据包进行过滤，最终实现接入控制的目的。

3. 部署与配置方法

网络探针对于网络交换设备没有依赖性，网络探针服务器无需接入网络主干链路，而是以旁路方式接入网络，因此网络探针产生的网络流量不会对网络带宽产生影响。通过网络探针服务器管理网络探针，可以实现对所有计算机终端的全网接入集中式管理控制。

网络探针在部署初期，可采用网络探针的限制工作模式，因为此时网络中可能存在大量没有安装指定程序或授权的计算机终端，可以让它们跳转到指定服务

器进行授权或下载指定程序，部署一段时间后，网内可能仅剩少部分计算机终端没有安装指定程序或授权，这时可转用网络探针的阻断工作模式，拒绝这些不符合相关标准和要求的计算机终端进行网络活动。

常见配置以 Squid 代理服务器的设置为例，如果要对某台主机禁止使用本地代理，则找到 squid. conf 文件中的“http _ access deny all”并改为“http _ access deny ip-add”令使用该 IP 地址的主机无法通过代理服务器访问互联网资源即可。

另外还可以采用 IP Tables 一步一步地来建立包过滤防火墙，需要说明的是，在这个例子中，主要是对内部的各种服务器提供保护。另外，由于服务器/客户机交互是双向的，所以不仅仅要设置数据包出去的规则，还要设置数据包返回的规则，设置针对来自 Internet 数据包的如下的过滤规则。

Step1：首先禁止转发任何包，然后再一步步设置允许通过的包。

Step2：先允许源为内网的所有端口的 TCP 包。

Step3：再允许目的为内部网（192. 168. X. X/24）的 FTP 数据包。

Step4：允许目的为内网的来自 Internet 的非连接请求 TCP 包。

3. 2. 3　DHCP 网络准入控制技术分析

DHCP 提供了一套架构用来在 TCP/IP 网上传递配置信息到主机，是 BOOTP 的扩展，增加了自动分配网络地址，重用释放的网络地址的功能，以及引进安全机制的附加信息。DHCP 主要用来动态提供配置参数给 Internet 上的主机，一方面从 DHCP 服务器传送主机特定的协议配置参数到主机，同时自动分配网络地址给主机。DHCP 支持 3 种 IP 地址分配方式：自动分配，即分配永久的 IP 地址给用户；动态分配，即分配有一定时限的 IP 地址给用户，若超时则释放；手动分配，即由网络管理员手工分配。通常网络可采用 3 种分配方式的任意组合，由网络管理员根据网络特点和策略自行决定。

在国外，绝大多数的机构都是采用 DHCP 系统来管理网络的地址，因此针对 DHCP 管理的安全性和规范性产生了大量的技术方案。DHCP 准入架构就是综合了多种 DHCP 管理技术而诞生的适用于准入控制的一种有效快速的解决方案。

正如其名称，DHCP 准入控制技术必须运行在 DHCP 环境下，而这个方案在国内最大的劲敌就是大量机构正在使用的静态 IP 环境，不幸的是，改动现有网络架构正是 NAC 实施的大忌。

如前所述，在国外使用较为普遍的 DHCP 准入控制架构在国内的大环境下并没有发挥其应有的效果，在后面阐述的技术分析中还将从技术细节角度继续对此作出探讨。

1. 技术实现原理

DHCP 准入的实现原理依靠的是改变接入终端的 IP 地址和相对应的网关。

由于基于 DHCP 环境，因此所有的 IP 地址分配决定权被 NAC Appliance 控制，终端所获得的 IP 地址组决定了其状态和所获得的访问权限。因此一般的 DHCP 架构都会依据接入状态的不同定义 2～3 组 IP 地址池。

① 正常 IP 地址池。接入终端通过认证和安检后获得的 IP 地址组。此时的网关为网络中的正常网关，因此所有数据流量不通过 NAC Appliance，实现了正常入网。

② 访客 IP 地址池。如果接入终端所选角色为 guest，那么将被分配到这个 IP 地址组，网关被指定为 NAC Appliance，因此所有去往正常 IP 地址段的访问都会经过 NAC Appliance，并接受管理，NAC Appliance 可以选择放通去往某些限定区域的流量。

③ 隔离 IP 地址池。接入终端未通过认证或安检不通过，所获得的 IP 地址组。网关依然被指定为 NAC Appliance，因此流量依然会受到准入设备的控制，可以设置在这个地址组中的接入计算机只能够访问隔离修复区。

DHCP 是客户（Client）-服务器（Server）模式，服务器端提供网络地址和配置参数给请求的主机也就是客户端，客户端根据服务器送来的配置参数和网络地址进行初始化。当给客户端分配一个新的网络地址时，DHCP 服务器与客户间的协议交互如下：

① 客户在本地子网广播 DHCP Discover 消息，若 DHCP 服务器与客户端不在一个子网，则由 DHCP 中继代理（relay agent）传递消息到服务器。

② 服务器端在收到 DHCP Discover 后，以带有客户请求的网络地址的 DHCP Offer 响应，假如服务器发现 DHCP Discover 来自 relay agent，则将 DHCP Offer 直接单播送至 relay agent，由其单播送至客户，反之，则在本地子网广播。

③ 客户从一个或多个服务器接收到一个或多个 DHCP Offer 后选择其中一个获得配置参数，并将带有标识选中服务器的 DHCP Request 在本地子网广播经由 relay agent 转发。若客户在规定时间内未收到 DHCP Offer，则重发 DHCP Discover。

④ 所有服务器将接收到 DHCP Request 消息，根据 DHCP Request 内的服务器标识，被选用的服务器根据客户的硬件地址唯一确认客户后，发送 DHCP Ack 至客户端。若服务器不能满足客户在 DHCP Request 内的配置请求，则响应 DHCP Nak。若服务器在一定时间未从客户接收到 DHCP Request，则直接回复 DHCP Ack。

⑤ 客户从服务器接收 DHCP Ack 后，首先核对消息内的配置参数（如 ARP，租用时间等），若不一致，则发 DHCP Decline 至服务器，如一致则进行配置，之后客户与服务器间可以直接交互。当客户从服务器处接收 DHCP Nak，则重新启动配置过程。一旦客户在规定时间内未收到服务器的响应，重传 DHCP Request 消息，若 10 次重传后，仍未收到服务器的响应，则通知用户并回到配置初始化阶段重新开始。当客户想释放由服务器提供的网络地址，可发送标识客户硬件地址和网络地址的 DHCP Release。

2. 工作过程

DHCP 工作过程示意见图 3-5，具体步骤如下。

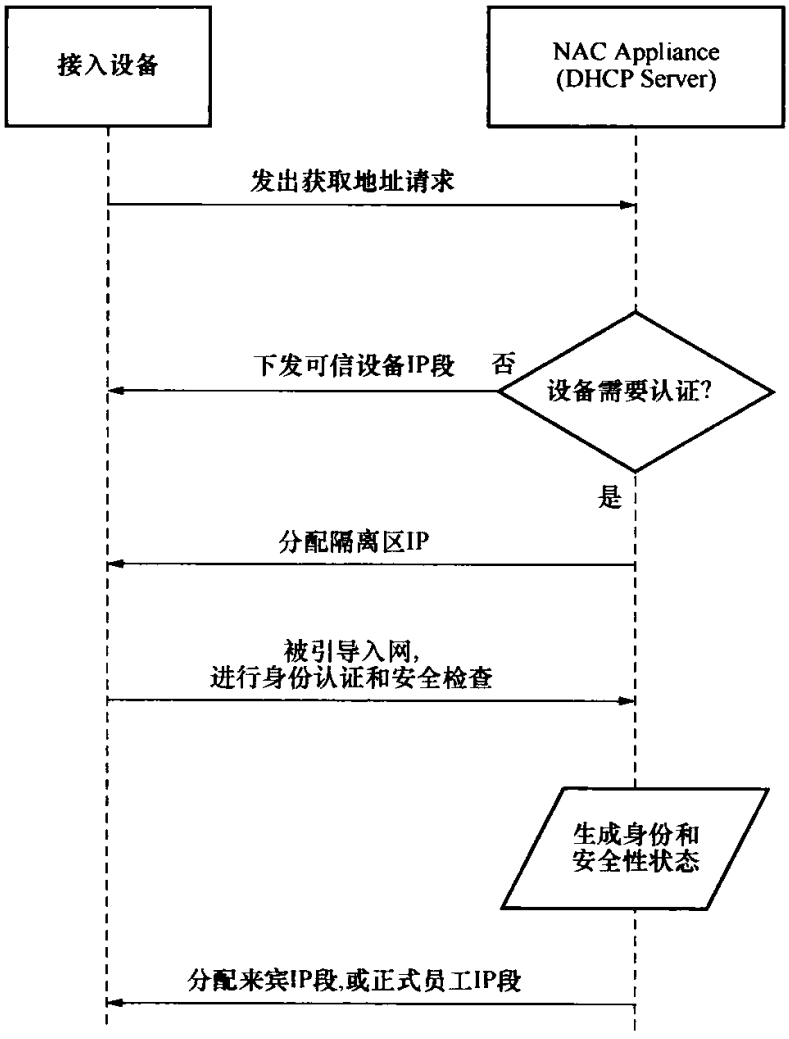


图 3-5　DHCP 工作过程示意图

1）新入网终端

Step1：终端发出 DHCP 请求，NAC Appliance 响应此请求并分配 IP 地址、掩码、网关和 DNS 给新入网设备，其中网关为 NAC Appliance 自己的地址，子网掩码控制终端安检前的访问区域。

Step2：新终端获得 IP 地址后，如果需要访问内网资源，必定需要经过 NAC Appliance 设备（此时为网关），因此会被强制重定向到身份认证和安检模块，此时终端就受到 NAC Appliance 的控制进行身份验证和安全性检查。

Step3：新终端可以选择“来宾方式”入网，这样可以收发邮件（由 NAC APPliance 进行转发）但无法访问内网资源（由于没有经过身份验证和安检，所有访问内网的数据包都被丢弃）。

Step4：新终端也选择内部合法用户或正式员工入网，此时需要验证使用人的身份，并进行安全性检查，对于两者都通过的设备，NAC Appliance 将分配原

网络中的正常网关给入网终端；如果出现不合规的情况，则设备的网关依然是NAC Appliance，所有数据都必须通过NAC Appliance的检查。

2）入网后终端

符合规定的设备在通过身份验证和安全检查后，被分配到了网络中的正常网关，此时所有数据流量都不受到NAC Appliance的控制，符合规定的设备可以正常使用网络直到下一次DHCP请求发出（如重启机器或强行修复）。

3. 主要特点

DHCP网络准入控制技术主要特点如表3-1所示。

表3-1 DHCP网络准入控制主要特点

NAC体系	对应参数	备注
架构组成	Agent（可选） + Switch + NAC Appliance （DHCP Server）	客户端模式是可选的，如果用户需要较完善的安全检查和控制功能，可以加装客户端
支持环境	支持DAI的交换机	Cisco2960以上（IOS要求12.2（50））
旁路部署	视接入终端状态	只有接入终端完全符合要求才转变为旁路，来宾模式或隔离模式下均为带内控制
无客户端支持	√	
交换机配置量	较多	所有接入层交换机（如果支持的话）均进行DHCP Snooping及DAI的配置
接入层端口级控制	视环境而定	在接入层交换机支持DAI的情况下能够实现
Hub接入控制	√	
http快捷性	√	由于是基于3层的准入控制技术，因此可以进行Web重定向引导
系统资源（内存）占用	小	在无客户端环境下占用小
来宾管理	好	能够进行Web引导，因此十分友好
稳定性	好	在支持DAI的环境下表现良好。可以依赖交换机及服务器来确保稳定性； 如果在不支持DAI的环境下，则架构存在重大缺陷。（参见配置方法中的介绍）
兼容性	一般	支持DAI的交换环境
防单点故障	×	失去DHCP Server的严重性是人尽皆知的

4. 配置方法

DHCP 架构本身只需要接入终端配置为 DHCP 模式，服务器端建设好 IP 地址池即可，但是正如在主要特点中我们所讨论到的那样，没有 DAI 支持的 DHCP 架构就是一个空架子。因为如果恶意闯入者能够私设静态 IP 和网关，那么完全可以绕过 NAC Appliance 的控制，从而让整个 NAC 体系形同虚设。而 DAI 技术（Dynamic ARP Inspection，动态 ARP 检测）就是为了防止这种私设静态 IP 行为而在交换机平台上做出的维护。

因此在搭建 DHCP 准入环境时，最大的部署工作量是在所有的接入层交换机上都部署 DAI，从而堵住私设静态 IP 的所有通道。

在 DAI 技术中，能够做到防御的基础是使用 DHCP Snooping 来创建合法的 DHCP 数据库，在合法数据库基础上，DAI 能够判断出非法的静态 IP 行为并加以阻断。

1）DHCP Snooping 的配置方法

DHCP Snooping 技术是 DHCP 的安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息，这些信息是指来自不信任区域的 DHCP 信息。DHCP Snooping 绑定表包含不信任区域的用户 MAC 地址、IP 地址、租用期、VLAN-ID 接口等信息。

当交换机开启了 DHCP Snooping 后，会对 DHCP 报文进行侦听，并可以从接收到的 DHCP Request 或 DHCP Ack 报文中提取并记录 IP 地址和 MAC 地址信息。另外，DHCP Snooping 允许将某个物理端口设置为信任端口或不信任端口。信任端口可以正常接收并转发 DHCP Offer 报文，而不信任端口会将接收到的 DHCP Offer 报文丢弃。这样，可以完成交换机对假冒 DHCP Server 的屏蔽作用，确保客户端从合法的 DHCP Server 获取 IP 地址。

（1）DHCP Snooping 主要作用。DHCP Snooping 的主要作用就是隔绝非法的 DHCP Server，这一点可以通过配置非信任端口来实现。建立和维护一张 DHCP Snooping 的绑定表，这张表可以通过 DHCP Ack 包中的 IP 和 MAC 地址生成，也可以通过手工来进行指定。这张表是后续 DAI 和 IP Source Guard 的基础。这两种类似的技术，是通过这张表来判定 IP 或者 MAC 地址是否合法，来限制用户连接到网络的。

（2）基本配置方法。

```
switch（config）#ip dhcp snooping
switch（config）#ip dhcp snooping vlan 10
switch（config-if）#ip dhcp snooping limit rate 10
//dhcp 包的转发速率，超过就接口就 shutdown，默认不限制
switch（config-if）#ip dhcp snooping trust
//这样，这个端口就变成了信任端口，信任端口可以正常接收并转发 DHCP
```

Offer 报文，不记录 IP 和 MAC 地址的绑定，默认是非信任端口

switch#ip dhcp snooping binding 0009.3452.3ea4 vlan 7 192.168.10.5 interface gi1/0/10

//这样可以静态 IP 和 MAC 一个绑定

switch（config）#ip dhcp snooping database tftp：//10.1.1.1/dhcp_table

//因为掉电后，这张绑定表就消失了，所以要选择一个保存的地方，ftp，tftp，flash 皆可。本例中的 dhcp_table 是文件名，而不是文件夹，同时文件名要手工创建一个

2）DAI 的配置方法

如前所述，DAI 就是以 DHCP Snooping 的绑定表为基础来检查 MAC 地址和 IP 地址的合法性。其基本配置方法如下：

switch（config）#ip dhcp snooping vlan 7

switch（config）#ip dhcp snooping information option

switch（config）#ip dhcp snooping

switch（config）#ip arp inspection vlan 7

//定义对哪些 VLAN 进行 ARP 报文检测

switch（config）#ip arp inspection validate src-mac dst-mac IP

//对源，目 MAC 和 IP 地址进行检查

switch（config-if）#ip dhcp snooping limit rate 10

switch（config-if）#ip arp inspection limit rate 15

//定义接口每秒 ARP 报文数量

switch（config-if）#ip arp inspection trust

//信任的接口不检查 ARP 报文，默认是检测

5. 注意点

对于前面 DHCP Snooping 的绑定表中关于端口部分，是不做检测的。同时对于已存在于绑定表中的 MAC 和 IP 对于关系的主机，不管是 DHCP 获得，还是静态指定，只要符合这个表就可以了，如果表中没有就阻塞相应流量。

在开始应用 DAI（Dynamic ARP Inspection）时，交换机会记录大量的数据包，当端口通过的数据包过多时，交换机会认为遭受 DoS 攻击，从而将端口自动 errdisable，造成通信中断。为了解决这个问题，需要加入命令 errdisable recovery cause arp-inspection。

6. 总结

虽然 DHCP Snooping 是用来防止非法的 DHCP Server 接入的，但是它一个重要作用是一旦客户端获得一个合法的 DHCP Offer，启用 DHCP Snooping 设备会在相应的接口下面记录所获得 IP 地址和客户端的 MAC 地址，这是后面另外

一个技术 ARP Inspection 进行检测的一个依据。ARP Inspection 是用来检测 ARP 请求并防止非法 ARP 请求的。认为是否合法的标准是前面 DHCP Snooping 时建立的那张表。

在本小节开头的应用现状中，笔者曾提及 DHCP 技术在国内应用所遇到的阻碍，除开已有静态地址环境的制约外，事实上通过上文的分析所了解到的 DAI 支持的重要性，国内网络的不规范导致的交换机环境不支持 DAI 则是影响 DHCP 准入架构无法普及的第二大重要原因。

3.3　基于基础网络设备的网络准入控制架构

由于 802.1x 技术的采用以及众多准入技术对于 Radius 服务器的依赖性，基于基础网络设备的网络准入控制（Infrastructure-Based NAC）架构目前拥有世界上最多的准入用户。在本章将阐述可以真正实现 NAC 标准流程（而不是像 ARP 准入或应用代理那样只是简单的阻断）的各种准入技术，并领悟 NAC 与交换设备联动的博大精深。帮助读者树立 NAC 并不是一个单一的产品，而是一套整体的解决方案的关键概念。

3.3.1　802.1x 网络准入控制技术分析

20 世纪 90 年代后期，802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1x 协议。后来，802.1x 协议作为局域网端口的一个普通接入控制机制用在以太网中，主要解决以太网内认证和安全方面的问题。比较而言，基于 802.1x 的网络准入控制安全性最强，功能最全面的准入控制机制。如今，几乎所有的网络设备厂商都能够支持 802.1x 架构的准入控制方案。主流网络设备厂商也都提供了解决方案，其支持的标准也最为普遍，包括 Cisco 的 C-NAC、微软的 NAP 以及国际可信计算组织的 TNC。但是它们也有如下一些不足之处：需要安装代理，需要接入交换机支持接入认证协议，配置管理较为复杂，如果认证服务器瘫痪容易引发单点故障，因此一般需要进行热备，成本较高，等等。

802.1x 确实足够优秀了，这也是它为什么能够成为 IEEE 委员会的国际标准的理由。对于一个在 20 世纪 90 年代就已经提出的安全框架协议来说，能够在 21 世纪还继续使用数十年，并且仍然还有大量厂商在不断推陈出新地在其框架基础上进行扩展支持的，简直可以说是一个奇迹。很难想象如今还有多少安全架构能够在提出之际就考虑到 20 年后的需求，但是 802.1x 在即将迈入其成人之际，依然是一个在 TCP/IP 第 2 层中很少有破绽的架构。虽然有众多评论针对其稳定性和友好性提出了质疑，但理论派们也不得不向这位安全界的老前辈脱帽致敬。

2001 年，IEEE 工作组发布了名为基于端口的网络访问控制（Port-based Network Access Control，PBNAC）的 802.1x 标准，其初衷是提升无线局域网中认证的安全性以及实现以计费为目的的用户认证。但在目前的多数应用中，人

们更多地将 PBNAC 应用于如下经典场景：网络管理员根据对终端安全状态的审计结果，阻止不符合内部网络预定安全策略的终端对网络资源的访问，从而更好地保证内部网络的安全。基于上述典型应用范式，802.1x 标准一直广受关注。人们认为 PBNAC 是解决网络安全问题的一项重要支撑技术，通过它可以杜绝网络安全问题的死角。

在国内的实际应用中，几乎所有能够实现 ARP 准入控制的厂商，在其第二步的准入策略中都不约而同地选择了 802.1x。因为所有主流交换机设备的制造商都会在其产品中加入对 802.1x 的支持，这就决定了 802.1x 架构优秀的兼容性，能够在各种交换环境中进行搭建，并且由于其基于网络 2 层的特点，控制力度也比其他的 3 层准入技术更强。

当然，由于必须安装认证客户端的局限性，802.1x 必将逐渐退出人们的视野，让位给使用无客户端技术的其他准入架构，但至少我们可以自豪地说，没有 802.1x，就没有无客户端准入的投入和研发，而且由于大型跨路由网络中广泛地采用了 802.1x 安全准入技术，完全过渡到无客户端技术架构（Agentless）的过程也将持续 1～2 年。

在本节将对 802.1x 技术的原理进行详细的分析，由于 802.1x 协议的通用性和国际标准性，笔者将在厂商的环境下进行细节性的数据包分析，使得读者从底层能够对这个 NAC 的鼻祖架构得到真正全面的理解。

1. 技术实现原理

802.1x 又名为基于端口的网络访问控制协议，所谓端口：在 802.1x 标准中，端口的含义不是通常所指的 TCP 端口或 UDP 端口，且不限于交换机上的物理端口，而是“网络访问端口”的简称。802.1x 标准将“网络访问端口”定义为“系统连接到局域网的一个点”。因此，它可以是一个具体的物理端口（如一个物理局域网段上的单一 MAC），或是一个虚拟的逻辑端口（如无线局域网中工作站到访问点（Access Point，AP）的一个连接）。

1）802.1x 协议概况

802.1x 源于 802.11 无线以太网（EAPOW）。该协议的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能，从而可以实现认证与业务的分离，保证了网络传输的效率。该协议的核心内容如图 3-6 所示。

靠近用户一侧的以太网交换机上放置一个 EAP（Extensible Authentication Protocol）代理，用户 PC 机运行 EAPoE（EAP over Ethernet）的客户端软件与交换机通信。其主要控制原理为：

初始状态下，在靠近用户一侧的以太网交换机上的所有端口均处于关闭状态，只有 EAPoL（EAP over LAN）数据流才能通过，而另外任何类型的网络数据流，如动态主机配置协议、超文本传输协议（HTTP）、文件传输协议（FTP）、简单邮件传输协议（SMTP）和邮局协议（POP3）等都被禁止传输。

图 3-6　802.1x 协议的核心内容

此时，交换机上将具有一个标准或非标准的 EAP（Extensible Authentication Protocol）代理，用户 PC 机运行一个能够生成 EAPoL 报文的客户端与交换机通信。当用户通过 EAPoE 登录交换机时，用户 PC 机发出携带用户名和口令的 EAPoL 报文，交换机将用户同时提供的用户名口令传送到后台的 RADIUS 认证服务器上。如果用户名及口令通过了验证，则相应的以太网端口打开，允许用户访问。

2）802.1x 协议的体系结构

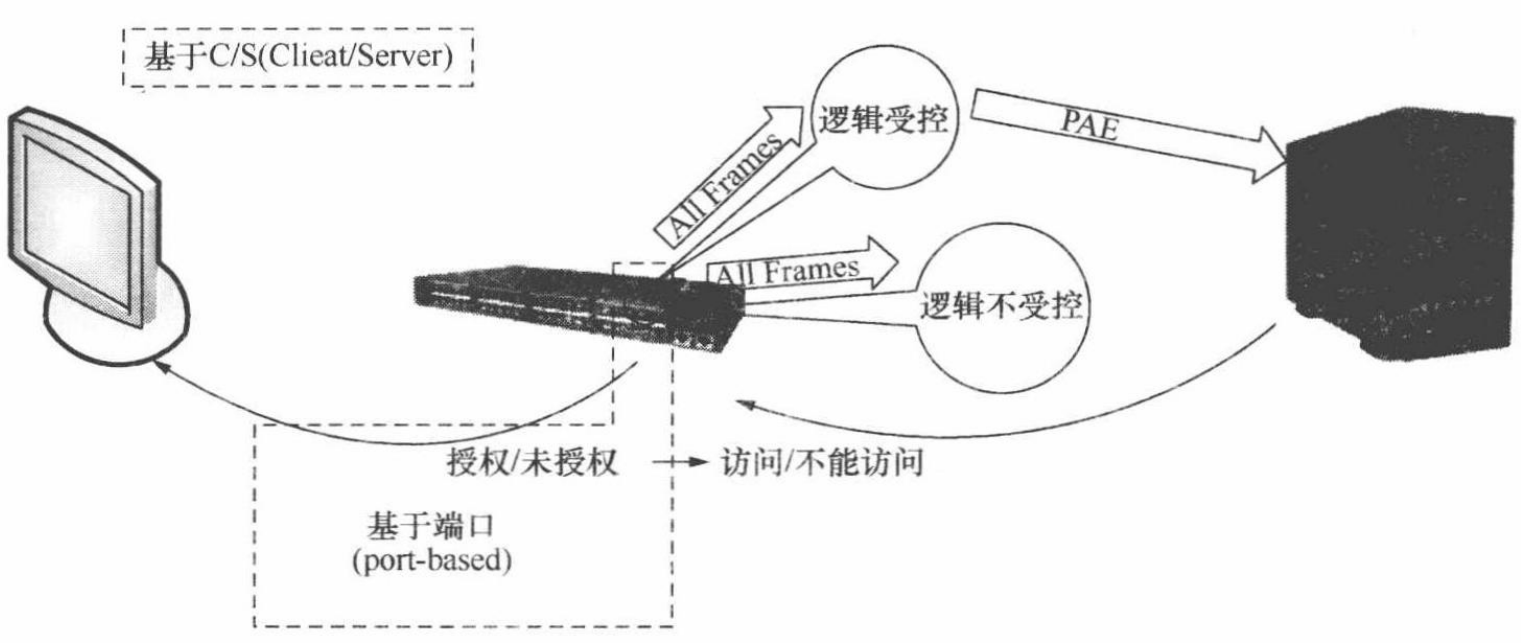
传统的以太网具有开放的特性，用户只要连接到交换机上，就可以通过交换机进入任何网络服务。802.1x 标准在 802 网络结构的基础上，定义了一种基于工作站/服务器模式的输入控制机制和认证协议，约束网络服务只向那些允许进行访问的用户提供，克服传统交换机的安全性弱点。

802.1x 协议的体系结构包括 3 个重要的部分：客户端（Supplicant System）、认证者（Authenticator System）、认证服务器（Authentication Server System），图 3-7 描述了三者之间的关系以及互相之间的通信过程。

下面对 802.1x 协议的体系结构的各个组成部分进行具体介绍。

（1）客户端系统（Supplicant System）。一般为用户终端系统，该终端系统通常要安装一个客户端软件，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。为支持基于端口的接入控制，客户端系统需支持 EAPoL（Extensible Authentication Protocol over LAN）协议。

（2）认证系统（Authenticator System）。通常为支持 802.1x 协议的网络设备，其端口分成两个逻辑端口：受控端口（Controlled Port）和不受控端口（Uncontrolled Port）。该设备对应于不同用户的端口（可以是物理端口，也可以是用户设备的 MAC 地址、VLAN、IP 等）。认证系统的端口访问实体通过不受控端口与客户端端口访问实体进行通信，二者之间运行 EAPoL 协议。认证者的端口访问实体与认证服务器之间运行 EAP 协议。EAP 协议并不是认证者和认证服务器通信的唯一方式，其他的通信通道也可以使用。例如，如果认证系统和认


基于C/S(Clieat/Server)
All Frames
逻辑受控
PAE
All Frames
逻辑不受控
授权/未授权
访问/不能访问
基于端口
(port-based)

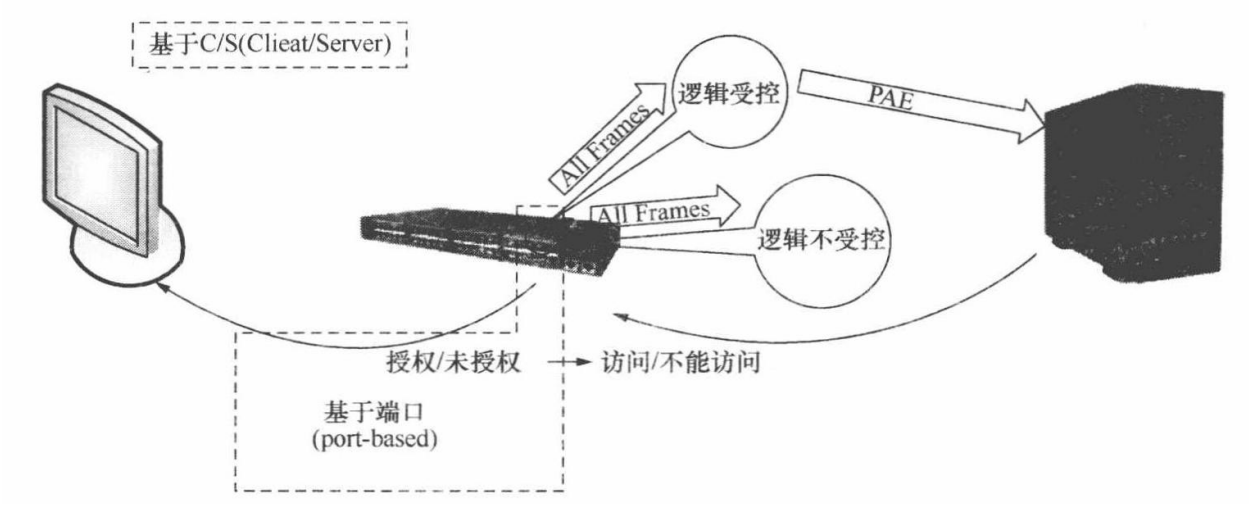


图 3-6　802.1x 协议的核心内容

此时，交换机上将具有一个标准或非标准的 EAP（Extensible Authentication Protocol）代理，用户 PC 机运行一个能够生成 EAPoL 报文的客户端与交换机通信。当用户通过 EAPoE 登录交换机时，用户 PC 机发出携带用户名和口令的 EAPoL 报文，交换机将用户同时提供的用户名口令传送到后台的 RADIUS 认证服务器上。如果用户名及口令通过了验证，则相应的以太网端口打开，允许用户访问。

2）802.1x 协议的体系结构

传统的以太网具有开放的特性，用户只要连接到交换机上，就可以通过交换机进入任何网络服务。802.1x 标准在 802 网络结构的基础上，定义了一种基于工作站/服务器模式的输入控制机制和认证协议，约束网络服务只向那些允许进行访问的用户提供，克服传统交换机的安全性弱点。

802.1x 协议的体系结构包括 3 个重要的部分：客户端（Supplicant System）、认证者（Authenticator System）、认证服务器（Authentication Server System），图 3-7 描述了三者之间的关系以及互相之间的通信过程。

下面对 802.1x 协议的体系结构的各个组成部分进行具体介绍。

（1）客户端系统（Supplicant System）。一般为用户终端系统，该终端系统通常要安装一个客户端软件，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。为支持基于端口的接入控制，客户端系统需支持 EAPoL（Extensible Authentication Protocol over LAN）协议。

（2）认证系统（Authenticator System）。通常为支持 802.1x 协议的网络设备，其端口分成两个逻辑端口：受控端口（Controlled Port）和不受控端口（Uncontrolled Port）。该设备对应于不同用户的端口（可以是物理端口，也可以是用户设备的 MAC 地址、VLAN、IP 等）。认证系统的端口访问实体通过不受控端口与客户端端口访问实体进行通信，二者之间运行 EAPoL 协议。认证者的端口访问实体与认证服务器之间运行 EAP 协议。EAP 协议并不是认证者和认证服务器通信的唯一方式，其他的通信通道也可以使用。例如，如果认证系统和认

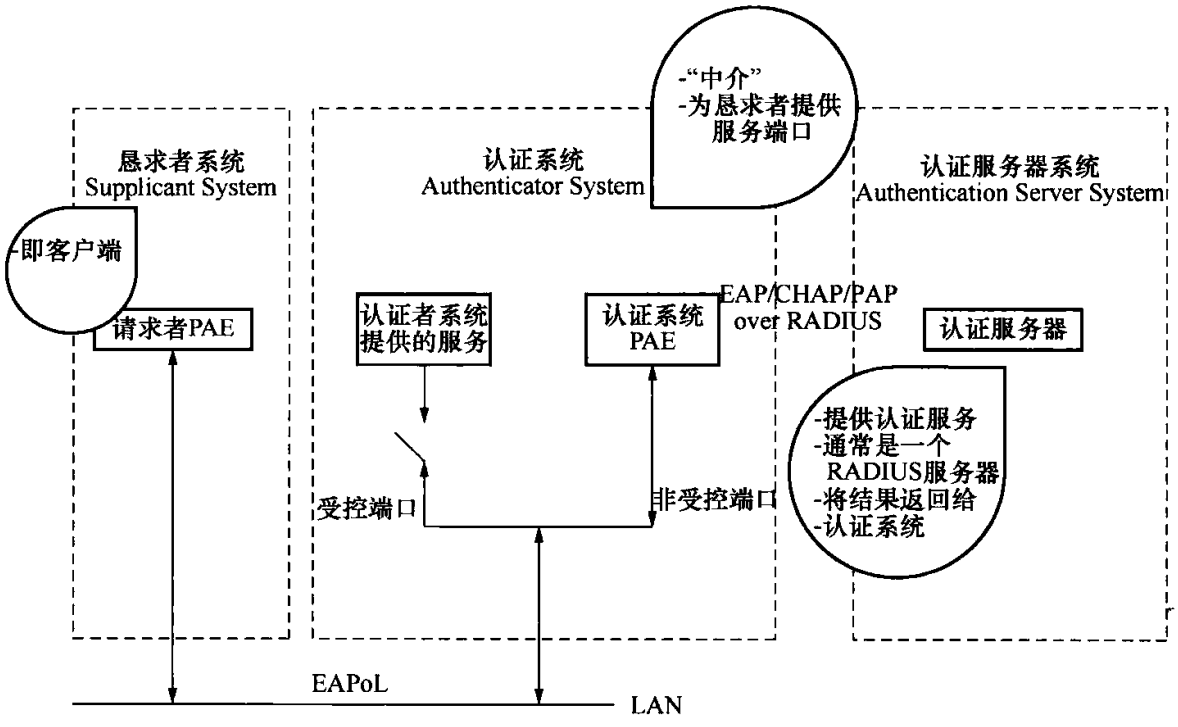


图 3-7 802.1x 协议体系结构的组成部分

证服务器系统集成在一起，两个实体之间的通信就可以不采用 EAP 协议。

① 受控端口（Controlled Port）：受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。可配置为双向受控和仅输入受控两种方式，以适应不同的应用环境。如果用户未通过认证，则受控端口处于未认证状态，则用户无法访问认证系统提供的服务。

② 不受控端口（Uncontrolled Port）：不受控端口始终处于双向连通状态，主要用来传递 EAPoL 协议帧，保证客户端始终可以发出或接受认证。

③ 认证控制方式：不受控端口只能传送认证的协议报文，而不管此时受控端口的状态是已认证状态（Authorized）还是未认证状态（Unauthorized）。受控端口传送业务报文。如果用户通过认证，则受控端口的状态为已认证状态，可以传送业务报文。如果用户未通过认证，则受控端口的状态为未认证状态，不能传送业务报文。它的认证计费方式就是通过认证前后“打开/关闭”受控端口来实现对用户接入的控制，从而实现对用户的物理端口的认证和控制。

（3）认证服务器系统（Authentication Server System）：通常为 RADIUS 服务器，该服务器可以存储有关用户的信息。例如，用户的账号、密码以及用户所属的 VLAN、CAR 参数，优先级，用户的访问控制列表等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证者，由认证者构建动态的访问控制列表，用户的后续流量将接受上述参数的监管。认证服务器和 RADIUS 服务器之间通过 EAP 协议进行通信。

2. 工作过程

1）802.1x 协议认证角色

802.1x 协议认证有 3 个角色，分别为恳请者、认证者、认证服务器，如图 3-8所示。

图 3-8　802.1x 认证角色组成

各角色具体说明如下：

（1）恳请者（Supplicant）。恳请者即 802.1x 标准描述中的 Supplicant，是最终用户所扮演的角色。它请求对网络服务的访问，并对认证者的协议请求报文进行应答。

恳请者是必须运行符合 802.1x 客户端标准的软件，目前最典型的就是 Windows XP 操作系统自带的 802.1x 客户端支持。

（2）认证者（Authenticator）。认证者控制恳请者对网络服务的访问。它实际在认证过程中只是一个认证信息交换的途径，负责与恳请者通信，将恳请者的认证请求发往认证服务器，而后根据认证服务器的指示执行对恳请者的授权。

（3）认证服务器（Authentication Server）。认证服务器是最终用户的认证服务的实际提供者。它负责认证用户的身份并将认证结果通知认证者。

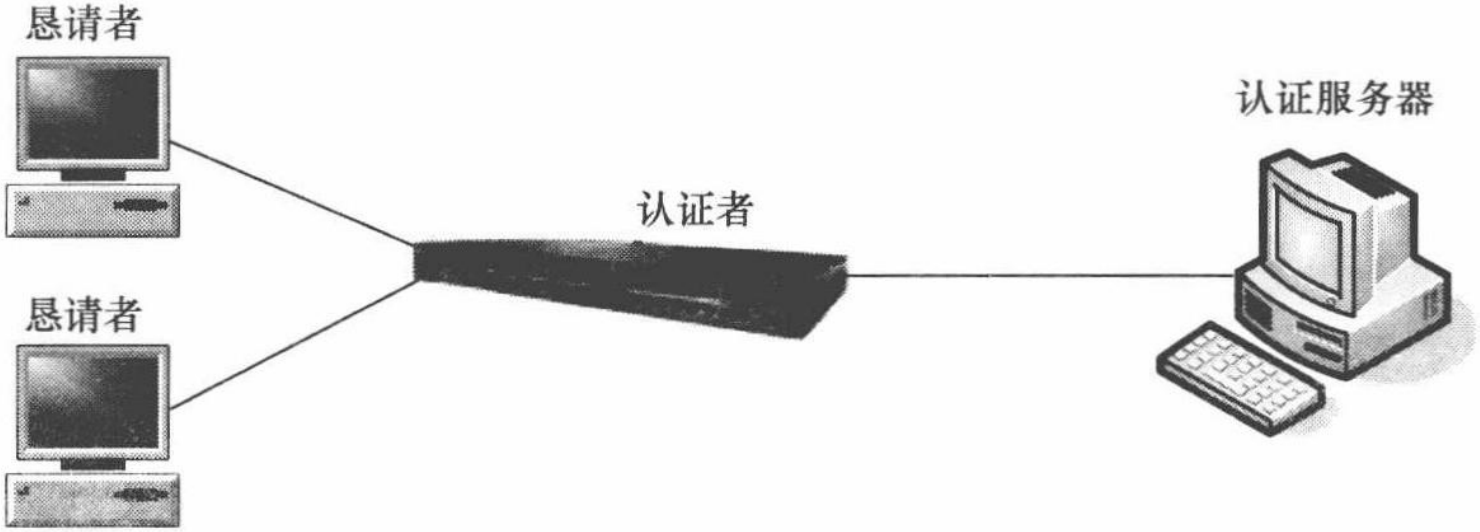
服务器必须是支持扩展 EAP（Extensible Authentication Protocol）协议或 CHAP 认证的 RADIUS（Remote Authentication Dial-In User Service）安全系统。典型的服务器软件如 Windows 2000 Server 操作系统自带的 IAS（Internet Access Server）服务。

认证服务器通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用户所属的 VLAN、优先级、用户的访问控制列表等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量就将接受上述参数的监管。认证服务器和 RADIUS 服务器之间通过 EAP 协议进行通信。以下为其认证过程。

Step1：用户通过 802.1x 客户端软件发起认证（EAPoL 报文）。

Step2：交换机截获 EAPoA 报文并向认证服务器转发 EAP 报文。

Step3：认证通过。


恳请者
恳请者
认证者
认证服务器

2. 工作过程

1）802.1x 协议认证角色

802.1x 协议认证有 3 个角色，分别为恳请者、认证者、认证服务器，如图 3-8所示。

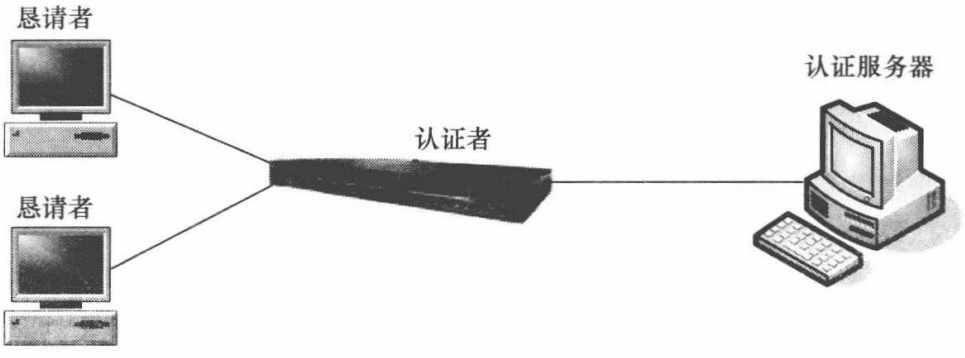


图 3-8　802.1x 认证角色组成

各角色具体说明如下：

（1）恳请者（Supplicant）。恳请者即 802.1x 标准描述中的 Supplicant，是最终用户所扮演的角色。它请求对网络服务的访问，并对认证者的协议请求报文进行应答。

恳请者是必须运行符合 802.1x 客户端标准的软件，目前最典型的就是 Windows XP 操作系统自带的 802.1x 客户端支持。

（2）认证者（Authenticator）。认证者控制恳请者对网络服务的访问。它实际在认证过程中只是一个认证信息交换的途径，负责与恳请者通信，将恳请者的认证请求发往认证服务器，而后根据认证服务器的指示执行对恳请者的授权。

（3）认证服务器（Authentication Server）。认证服务器是最终用户的认证服务的实际提供者。它负责认证用户的身份并将认证结果通知认证者。

服务器必须是支持扩展 EAP（Extensible Authentication Protocol）协议或 CHAP 认证的 RADIUS（Remote Authentication Dial-In User Service）安全系统。典型的服务器软件如 Windows 2000 Server 操作系统自带的 IAS（Internet Access Server）服务。

认证服务器通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用户所属的 VLAN、优先级、用户的访问控制列表等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量就将接受上述参数的监管。认证服务器和 RADIUS 服务器之间通过 EAP 协议进行通信。以下为其认证过程。

Step1：用户通过 802.1x 客户端软件发起认证（EAPoL 报文）。

Step2：交换机截获 EAPoA 报文并向认证服务器转发 EAP 报文。

Step3：认证通过。

Step4：DHCP 服务器分配 IP 地址。

Step5：受控端口打开。

Step6：正常通信。

由此可以看出，802.1x 认证仅仅在认证阶段进行 EAP 封装，通信过程中采用 TCP/IP 协议。

2）802.1x 协议认证原理

802.1x 协议认证的发起可以由用户主动发起，也可以由认证者发起。当认证者探测到未经过认证的用户使用网络，就会主动发起认证；用户端则可以通过客户端软件向认证者发送 EAPoL-Start 开始报文发起认证。由客户端发送 EAPoL 退出报文，主动下线，退出已认证状态的直接结果就是导致用户下线，如果用户要继续上网则要再发起一个认证过程。

为了保证用户和认证者之间的链路处于激活状态，而不因为用户端设备发生故障造成异常死机，从而影响对用户计费的准确性，认证者可以定期发起重新认证过程，该过程对于用户是透明的，即用户无需再次输入用户名/密码。重新认证由认证者发起，时间从最近一次成功认证后算起。重新认证时间默认值为 3600s，而且默认重新认证是关闭的。

对于认证者和客户端之间通信的 EAPoL 报文，如果发生丢失，由认证者负责进行报文的重传。在设定重传的时间时，考虑网络的实际环境，通常会认为认证者和客户端之间报文丢失的概率比较低以及传送延迟短，因此，一般通过一个超时计数器来设定，默认重传时间为 30s。

对于有些报文的丢失重传比较特殊，如 EAPoL-Start 报文的丢失，由客户端负责重传；而对于 EAP 失败和 EAP 成功报文，由于客户端无法识别，认证者不会重传。由于对用户身份合法性的认证最终由认证服务器执行，认证者和认证服务器之间的报文丢失重传也很重要。另外，对于用户的认证，在执行 802.1x 认证时，只有认证通过后，才有 DHCP 发起和 IP 分配的过程。由于客户终端配置了 DHCP 自动获取，则可能在未启动 802.1x 客户端之前，就发起了 DHCP 的请求，而此时认证者处于禁止通行状态，这样认证者会丢掉初始化的 DHCP 帧，同时会触发认证者发起对用户的认证。

由于 DHCP 请求超时过程为 64s，所以，如果 802.1x 认证过程能在这 64s 内完成，则 DHCP 请求不会超时，能顺利完成地址请求；如果终端软件支持认证后再执行一次 DHCP，就不用考虑 64s 的超时限制。

3）802.1x 协议的认证步骤

802.1x 协议认证过程是用户与服务器交互的过程，如图 3-9 所示，以下为其认证步骤。

Step1：用户开机后，通过 802.1x 客户端软件发起请求，查询网络上能处理 EAPoL 数据包的设备。如果某台验证设备能处理 EAPoL 数据包，就会向客户端发送响应包，并要求用户提供合法的身份标识，如用户名及其密码。

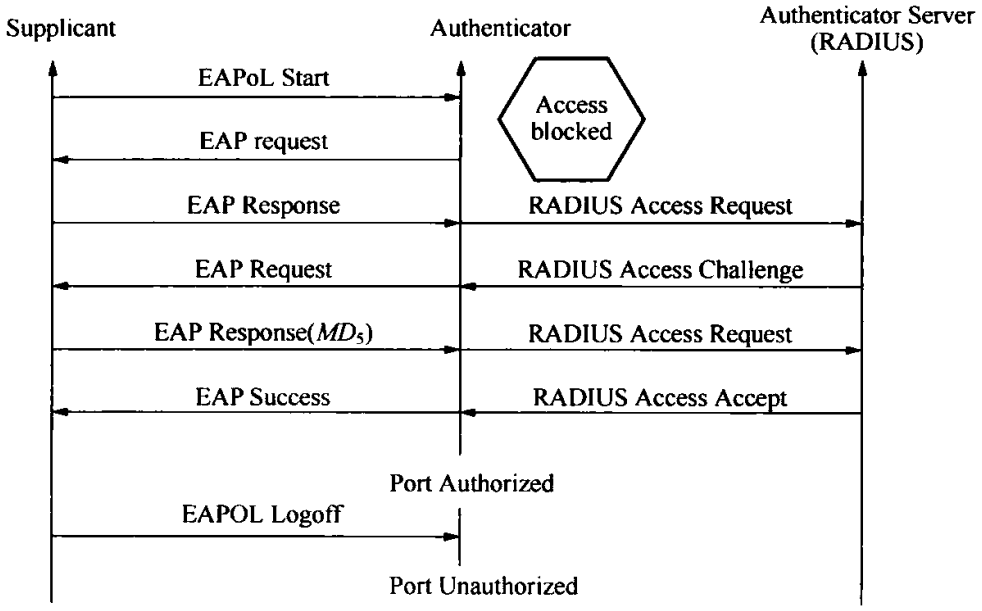


图 3-9　IEEE802.1x 协议的认证步骤示意图

Step2：客户端收到验证设备的响应后，提供身份标识给验证设备。由于此时客户端还未经过验证，因此认证流只能从验证设备的未受控的逻辑端口经过。验证设备通过 EAP 协议将认证流转发到 AAA 服务器，进行认证。

Step3：如果认证通过，则认证者的受控逻辑端口打开。

Step4：客户端软件发起 DHCP 请求，经认证设备转发到 DHCP Server。

Step5：DHCP Server 为用户分配 IP 地址。

Step6：DHCP Server 分配的地址信息返回给认证者，认证者记录用户的相关信息，如 MAC，IP 地址等信息，并建立动态的 ACL 访问列表，以限制用户的权限。

Step7：当认证设备检测到用户的上网流量，就会向认证服务器发送信息。

Step8：如果用户退出网络，可以通过客户端软件发起退出过程，认证设备检测到该数据包后，会删除用户的相关信息（如物理地址和 IP 地址），受控逻辑端口关闭；用户进入再认证状态。

Step9：验证设备通过定期的检测保证链路的激活。如果用户异常死机，则验证设备在发起多次检测后，自动认为用户已经下线，于是向认证服务器发送终止信息。

3. 主要特点

首先，目前所有的 802.1x 平台都要求入网用户必须安装进行认证的 EAPoL 客户端，这种情况存在许多缺陷：其一新入网设备如果未安装客户端，将无法通过认证进入网络，而此时没有任何提示信息，所有与网络中资源的联系均被切断，用户自身无法进行任何操作，如果依靠管理员手工安装 EAPoL 客户端，工作量将十分繁重；其二网络中的许多非桌面型 IP 设备（如网络打印机）在无法

安装客户端的情况下将被隔离出网络。

其次，大部分的 802.1x 认证都是基于端口的，认证通过后端口完全放开，无法根据入网用户身份角色的不同进行动态的权限控制，在入网用户权限无法规范的情况下，很容易导致内部重要资源的泄密。

而对于大部分交换机而言，标准的 802.1x 协议也无法解决端口下挂 Hub 的情况。802.1x 协议是基于端口的，那么在端口下挂 Hub 时，有某一台设备通过认证打开交换机端口后，同一 Hub 下广播域内的所有设备均无需认证就直接入网，这是 Hub 环境下的控制漏洞。

最后，大部分的 802.1x 架构中 EAP 包的响应和处理都是基于软件方式的，在通用的某台服务器上，基于 Windows 系统安装 RADIUS 程序后进行处理和控制，其响应速度和处理效率都受到整体硬件环境和操作系统的制约，无法应用于大规模、高性能要求的网络环境中。

这里，笔者以表格的形式明确基于 802.1x 协议的准入技术在标准 NAC 体系中的元素比重，通过量化的评估能够帮助读者更明确 802.1x 协议的技术侧重点和平衡性。如表 3-2 所示。

表 3-2 基于 802.1x 的网络准入控制技术主要特点

NAC 体系	对应参数	备注
架构组成	Supplicant +Authenticators +Radius Server	大部分厂商的 802.1x 架构都需要安装自有客户端，而不是使用操作系统自带的 802.1x 认证配置
支持环境	主流交换机厂商的 2 层可网管交换机	
旁路部署	√	完全旁路部署
无客户端支持	×	虽然有用户声称采用 Windows 自带的 802.1x 认证配置搭建了 NAC 体系，但绝大多数的机构还是购买了第三方的 802.1x 产品，并给每台机器都安装了第三方的客户端，因为第三方客户端能够提供更多的准入特性
交换机配置量	大	所有接入层交换机均进行大量配置
接入层端口级控制	√	基于端口的特性在这里体现出了优势
Hub 接入控制	×	在大部分交换机环境下都不支持 Hub 接入的准入管理
http 快捷性	×	部分厂商的交换机环境能够支持入网时页面转向，从而提供自助安装认证客户端的功能；但是大部分交换机厂商不提供这种功能，而是需要由管理员手工逐台安装客户端。 这就体现了 802.1x 体系架构无法支持友好快速的 Web 管理，而需要花费大量时间在客户端上做众多的配置，这也导致了大部分的 802.1x 方案都遭到接入用户的反感

续表

NAC 体系	对应参数	备注
系统资源（内存）占用	大	大部分厂商的 802.1x 认证客户端占用内存在 30M 以上，部分杀毒软件集成的 802.1x 客户端需要占用 100M 以上的内存
来宾管理	不好	DHCP + Guest VLAN 下才能够支持
稳定性	不好	客户端加载在系统底层驱动，因此容易受兼容性影响，一旦出现问题很容易导致认证不通过而引发断网
兼容性	分组成而定	在交换机层面，802.1x 的兼容性非常优秀，但由于需要安装客户端，非 Windows 系统的接入终端将遇到很大的问题
防单点故障	×	一旦 radius 宕机，则所有接入终端均无法通过认证

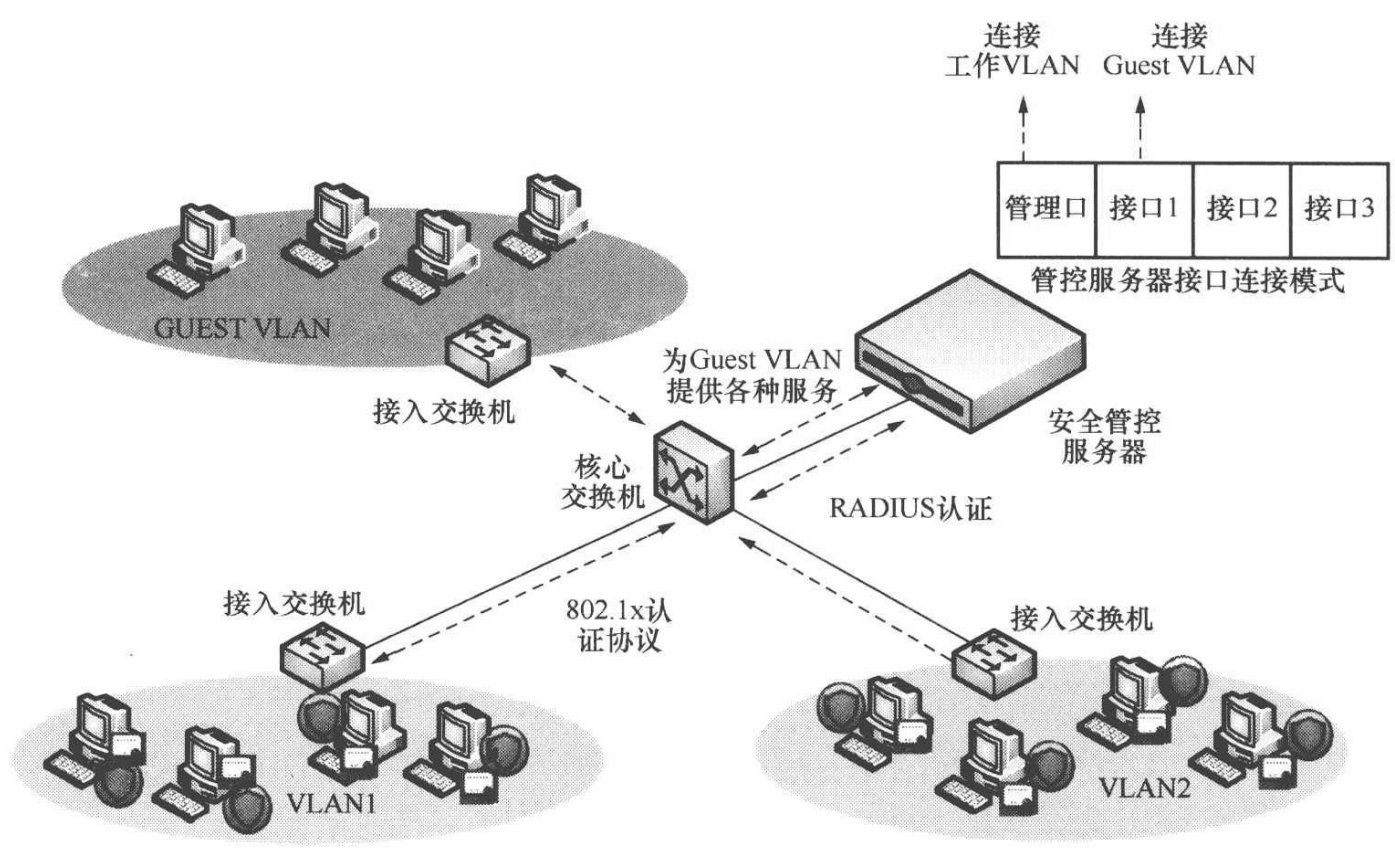
由表 3-2 可以看出，基于 802.1x 协议的准入控制方案存在使用上的极大不便，无法在端口打开后根据用户身份进行权限控制，另外在大部分环境下对 Hub 的支持不足。

4. 部署与配置方法

图 3-10 描述了基于 802.1x 准入控制系统的部署，整个内部网络被划分为 Guest VLAN 和工作 VLAN（含 VLAN 1 与 VLAN 2）两大部分，没有通过认证的计算机被隔离于 Guest VLAN 中。

图 3-10　基于 802.1x 准入控制系统的部署方式

“安全管控服务器”的接口 1 需要连接交换机的 Guest VLAN 口，通过接


连接
工作VLAN
连接
Guest VLAN
管理口
接口1
接口2
接口3
管控服务器接口连接模式
GUEST VLAN
接入交换机
为Guest VLAN
提供各种服务
安全管控
服务器
核心
交换机
RADIUS认证
接入交换机
802.1x认
证协议
接入交换机
VLAN1
VLAN2

续表

NAC 体系	对应参数	备注
系统资源（内存）占用	大	大部分厂商的 802.1x 认证客户端占用内存在 30M 以上，部分杀毒软件集成的 802.1x 客户端需要占用 100M 以上的内存
来宾管理	不好	DHCP + Guest VLAN 下才能够支持
稳定性	不好	客户端加载在系统底层驱动，因此容易受兼容性影响，一旦出现问题很容易导致认证不通过而引发断网
兼容性	分组成而定	在交换机层面，802.1x 的兼容性非常优秀，但由于需要安装客户端，非 Windows 系统的接入终端将遇到很大的问题
防单点故障	×	一旦 radius 宕机，则所有接入终端均无法通过认证

由表 3-2 可以看出，基于 802.1x 协议的准入控制方案存在使用上的极大不便，无法在端口打开后根据用户身份进行权限控制，另外在大部分环境下对 Hub 的支持不足。

4. 部署与配置方法

图 3-10 描述了基于 802.1x 准入控制系统的部署，整个内部网络被划分为 Guest VLAN 和工作 VLAN（含 VLAN 1 与 VLAN 2）两大部分，没有通过认证的计算机被隔离于 Guest VLAN 中。

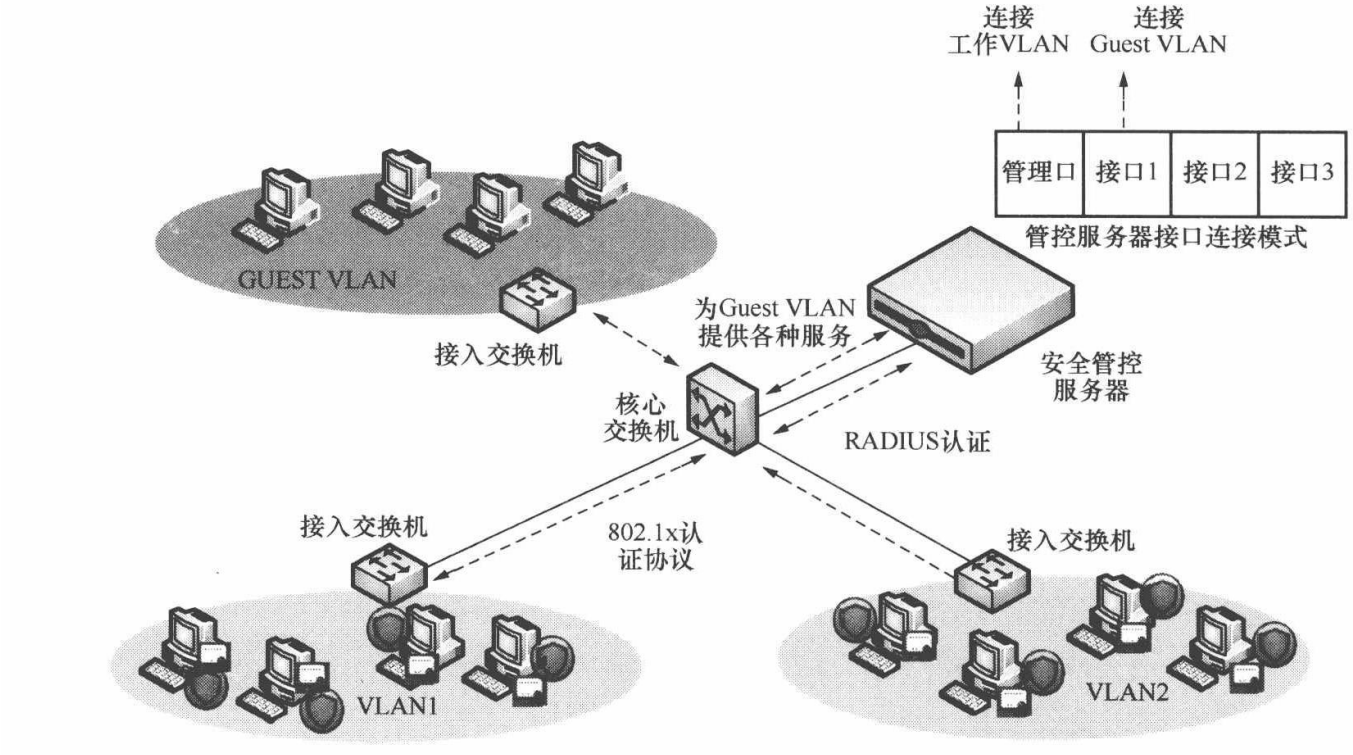


图 3-10　基于 802.1x 准入控制系统的部署方式

“安全管控服务器”的接口 1 需要连接交换机的 Guest VLAN 口，通过接

口 1，Guest VLAN 中的主机可以访问“管控服务器”提供的重定向服务并完成身份注册。

“安全管控服务器”管理口需要连接交换机的工作 VLAN 口（VLAN 1 或者 VLAN 2），通过管理口“管控服务器”为工作 VLAN 中的合法主机提供各种安全管控服务。

根据 802.1x 的工作机制，整个 802.1x 的准入控制工作是由 802.1x 客户端，接入层交换机，认证服务器 3 部分组件来配合完成的。因此，准入控制的配置需要分成 3 个部分的配置来完成。

1）客户端配置

基于 802.1x 的网络准入控制系统的代理内置有 802.1x 的客户端模块，用来完成身份认证的监听，发送身份认证信息和接收认证结果的工作。因此，要配置 802.1x，首先必须配置接入计算机支持 802.1x。关于 802.1x 在 Windows 下的配置网络上已经有很多详细的介绍，本文中不再赘述。

如果用户端是采用的第三方厂商的 802.1x 认证客户端，那么可以参考厂商的 802.1x 配置手册。

2）接入层交换机配置

在 802.1x 准入控制机制中，第二个组件就是接入层交换机。交换机充当的角色主要是在端口上启用 802.1x，发起认证，划分 VLAN 来将网络资源分为不同的区域（如访客区，修复区等），指定 RADIUS 服务器信息以及根据认证结果控制端口等。以下以 Cisco 交换机为例来说明交换机上的 802.1x 相关配置。

Step 1：配置交换机对 RADIUS 服务器的支持。

```
#启用 AAA
aaa new-model
#创建缺省的登录认证方法列表，采用 line password 认证（可选）如果用 default-list，list 中要有 none，防止 line con 0 下没有 passwd 导致 Console 登录时无法正常登录
aaa authentication login default line none
#创建 802.1x 认证方法列表，group radius 表示使用 Radius 服务进行认证
aaa authentication dot1x default group radius
aaa authorization network default group radius
#指定 Radius 服务器 IP 地址和安全字，可以配置多个做备份
radius-server host 192.168.0.1 auth-port 1812 acct-port 1813 key test
radius-server host 192.168.1.205 auth-port 1812 acct-port 1813 key test
#指定网络交换机向 radius 服务器的重传次数
radius-server retransmit 3
#指定交换机发送 Radius 包时加上 Cisco 自己的扩展（以便解析接入端口名）
```

radius-server vsa send authentication

Step2：配置某个端口对 802.1x 的支持，下面以配置端口 FastEthernet0/23 为例说明：

#进入到 FastEthernet0/23 的接口配置模式进行配置

interface fastethernet 0/23

dot1x port-control auto

Step 3：全局开启 802.1x

#在全局模式下，启用 802.1x

dot1x system-auth-control

5. 底层分析

这里以 H3C 的产品为例。相比 Cisco 而言，H3C 的 802.1x 是国内交换机设备市场的另一个代表，下面我们将在 H3C 的 802.1x 环境下进一步对整个 802.1x 架构深入到数据包底层进行解析。

1）基本配置

dot1x　//全局开启 802.1x

dot1x　authentication-method　eap

//缺省的认证协议是 CHAP，可以按需更改为 EAP

dot1x timer quiet-period 10

//当对 802.1x 用户认证失败以后，Authenticator 设备需要静默一段时间（该时间由静默定时器设置）后再重新发起认证。

dot1x timer 109 up-timeout 10

//请求超时定时器。若在该定时器设置的时长内，Supplicant 设备未成功响应，Authenticator 设备将重发认证请求报文。

dot1x timer handshake-period 900

//与客户的握手报文时间间隔

radius　scheme　msac

//设置一个认证方案

[h3c-radius-msac] primary authentication 10.1.254.129

//H3C 3600 上缺省端口号是 1812，不用像 Cisco 那样显式指明

[h3c-radius-msac] accounting optional

//在于第三方 RADIUS 服务器进行联动的时候，这个配置可以按需进行调整

[h3c-radius-msac]　key authentication msackey

//交换机与 radius 服务器交互时加密报文的密钥

domain domain _ name

//建立一个认证域

[H3C-isp-joyoung] scheme radius-scheme msac

//这个域下采用的 RADIUS 方案是 msac

domain default enable domain _ name

//默认采用这个认证域（可能有些 H3C 设备上建立了多个认证域）

interface eth1/0/2

dot1x

//进入某个端口下开启 802.1x

2）配置技巧

（1）dot1x interface Ethernet [port number] to Ethernet [port number]。配置一个端口范围的 dot1x 开启，如图 3-11 所示。

```
[H3C-3600]dot1x interface Ethernet 1/0/23 ?
  Ethernet          Ethernet interface
  GigabitEthernet   GigabitEthernet interface
  to                To
  <cr>
```

图 3-11 端口开启 dot1x

在全局视图下直接指定某个端口的 802.1x，后面的 to 参数表明可以进行一个端口范围的 802.1x 指定，相当于 Cisco 中 interface range fa0/1 - 24 这样的配置。

（2）交换机的主动 EAP 请求。默认情况下，交换机每隔 30s 会发起一次 Identity 的请求，（参见下一节定时器中的 eap-request-ID）这个报文的目的是为了发现网络中那些没有发起会话能力（不能发送 EAPoL-Start 包）的接入设备。

可以参考图 3-12 的 No.1 和 No.8，交换机 EAP 广播 Request 的间隔是 30s。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Hangzhou_65:0a:c5	Nearest	EAP	Request, Identity [RFC3748]
2	1.068679	Hangzhou_07:f2:e0	Spanning-tree-(for-br	0x88a7	Ethernet II
3	1.172355	Wistron_e8:78:87	Nearest	EAP	Response, Identity [RFC3748]
4	8.028557	Hangzhou_65:0a:c5	Wistron_e8:78:87	EAP	Request, Identity [RFC3748]
5	8.439746	Wistron_e8:78:87	Nearest	EAP	Response, Identity [RFC3748]
6	18.441823	Wistron_e8:78:87	Nearest	EAP	Response, Identity [RFC3748]
7	28.444105	Wistron_e8:78:87	Nearest	EAP	Response, Identity [RFC3748]
8	30.004883	Hangzhou_65:0a:c5	Nearest	EAP	Request, Identity [RFC3748]

图 3-12 交换机 EAP 广播

如果接入设备 a 已经认证成功，此时客户端默认仍然会进行 Response-Identity 的响应，但交换机的认证列表中已经有了此设备的地址，所以不会去询问 Radius Server，因此 md5-challenge 不会产生。所以图 3-12 中不会看到对于客户端的 md5-challenge，而是一直进行 Request 和 Response 的交替循环。

3）802.1x 中的定时器

（1）Timer of Eap-Request-ID。交换机会周期性地向端口下发出 eap-request-ID 报文，此周期决定于 tx-period。如图 3-13 和图 3-14 所示。

```
[H3C-3600]dot1x timer ?
  acl-timeout       The time limit of ACL being valid
  handshake-period  Value of handshake interval with 8021x supplicant
  quiet-period      Interval following failed authentication
  reauth-period     Reauthenticate period
  server-timeout    Value of server timeout
  supp-timeout      Value of supplicant timeout
  tx-period         Interval between identity requests
  ver-period        Interval between version requests
```

图 3-13　tx-period 参数示意图

```
[H3C-3600]dot1x timer tx-period ?
  INTEGER<1-120>  Value of parameter (unit: second)
```

图 3-14　tx-period 设置命令

图 3-15 是设置为 2s 后的效果。

```
15:48:33.250  LcAgent.exe  2772  3220  UserAuth...  ParseE...  461  收到 Eap-Request-ID = 1
15:48:35.500  LcAgent.exe  2772  3220  UserAuth...  ParseE...  461  收到 Eap-Request-ID = 1
```

图 3-15　tx-period 设置为 2s

图 3-16 设置为 10s 后的效果。

```
15:56:38.765  LcAgent.exe  2772  3220  UserAuth...  ParseE...  461  收到 Eap-Request-ID = 1
15:56:47.281  LcAgent.exe  2772  3220  UserAuth...  Respon...  121  ResponseIdentity 发送身份信息
15:56:48.281  LcAgent.exe  2772  3220  UserAuth...  ParseE...  461  收到 Eap-Request-ID = 1
```

图 3-16　tx-period 设置为 10s

在 dot1x 全局参数里对应的项是 transmit period，如图 3-17 所示。

```
[H3C-3600]dot1x timer tx-period 1
[H3C-3600]dis dot1x
 Global 802.1X protocol is enabled
 EAP authentication is enabled
 DHCP-launch is disabled
 Handshake is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD Quick Deploy is enabled

 Configuration: Transmit Period      1 s,  Handshake Period       15 s
                ReAuth Period     3600 s,  ReAuth MaxTimes        2
                Quiet Period        60 s,  Quiet Period Timer is disabled
                Supp Timeout        30 s,  Server Timeout         100 s
                Interval between version requests is 30s
                Maximal request times for version information is 3
                The maximal retransmitting times          2
```

图 3-17　tx-period 与 transmit period

设置效果如图 3-18 所示。

（2）supp-timeout。这个定时器是用于客户端没有响应 Request 包或 MD5 包的情况下在多少时间后进行重传的参数，如图 3-19、图 3-20 所示。

同理可知 server-timeout 的作用。

```
15:27:45.734  LcAgent.exe  3848  3816  UserAuth...  ParseE...  461  收到Eap-Request-ID = 1
15:27:45.734  LcAgent.exe  3848  3816  UserAuth...  Respon...  121  ResponseIdentity 发送身份信息
15:27:46.734  LcAgent.exe  3848  3816  UserAuth...  ParseE...  461  收到Eap-Request-ID = 1
15:27:46.734  LcAgent.exe  3848  3816  UserAuth...  Respon...  121  ResponseIdentity 发送身份信息
15:27:47.734  LcAgent.exe  3848  3816  UserAuth...  ParseE...  461  收到Eap-Request-ID = 1
15:27:47.750  LcAgent.exe  3848  3816  UserAuth...  Respon...  121  ResponseIdentity 发送身份信息
15:27:48.750  LcAgent.exe  3848  3816  UserAuth...  ParseE...  461  收到Eap-Request-ID = 1
```

图 3-18　transmit period 设置效果

```
[H3C-3600]dot1x timer ?
  acl-timeout        The time limit of ACL being valid
  handshake-period   Value of handshake interval with 8
  quiet-period       Interval following failed authenti
  reauth-period      Reauthenticate period
  server-timeout     Value of server timeout
  supp-timeout       Value of supplicant timeout
  tx-period          Interval between identity requests
  ver-period         Interval between version requests
```

图 3-19　supp-timeout 参数示意图

```
[H3C-3600]dot1x timer supp-timeout ?
  INTEGER<1-120>  Value of parameter (unit: second)
```

图 3-20　supp-timeout 设置命令

（3）server-timeout。用于 RADIUS 服务器没有响应询问的情况下多少时间后进行超时重传，如图 3-21 所示。

```
[H3C-3600]dot1x timer ?
  acl-timeout        The time limit of ACL being valid
  handshake-period   Value of handshake interval with 8021x supplicant
  quiet-period       Interval following failed authentication
  reauth-period      Reauthenticate period
  server-timeout     Value of server timeout
  supp-timeout       Value of supplicant timeout
  tx-period          Interval between identity requests
  ver-period         Interval between version requests
```

图 3-21　server-timeout 参数示意图

（4）Re-authenticate timer。在接入设备认证成功的情况下，交换机可以主动向接入者发起认证请求，客户端需要再次发送用户名和密码以便验证自己是否仍然可信，这是 802.1x 防止非法人员利用认证通过设备入网的身份验证机制。此即重认证时间参数。（EOU 中也有此功能，利用重认证确认接入设备的合法性，这也应该是所有准入技术必备的功能点。）

默认情况下，H3C 是关闭重认证功能的。人们需要手动开启重认证，如图 3-22所示。

开启重认证后，交换机会立即向开启了此功能的端口发起重认证，此时如果有非法客户端或认证时 Radius Server 无响应（会收到 eap-failure）则接入设备会立即下线。

重认证定时器参数如图 3-23 所示。

```
[H3C-3600]dot1x re-authenticate
 Re-authentication is enabled on port Ethernet1/0/1
 Re-authentication is enabled on port Ethernet1/0/2
 Re-authentication is enabled on port Ethernet1/0/3
 Re-authentication is enabled on port Ethernet1/0/4
 Re-authentication is enabled on port Ethernet1/0/5
 Re-authentication is enabled on port Ethernet1/0/6
 Re-authentication is enabled on port Ethernet1/0/7
 Re-authentication is enabled on port Ethernet1/0/8
 Re-authentication is enabled on port Ethernet1/0/9
 Re-authentication is enabled on port Ethernet1/0/10
 Re-authentication is enabled on port Ethernet1/0/11
 Re-authentication is enabled on port Ethernet1/0/12
 Re-authentication is enabled on port Ethernet1/0/13
 Re-authentication is enabled on port Ethernet1/0/14
 Re-authentication is enabled on port Ethernet1/0/15
 Re-authentication is enabled on port Ethernet1/0/16
 Re-authentication is enabled on port Ethernet1/0/17
 Re-authentication is enabled on port Ethernet1/0/18
 Re-authentication is enabled on port Ethernet1/0/19
 Re-authentication is enabled on port Ethernet1/0/20
 Re-authentication is enabled on port Ethernet1/0/21
 Re-authentication is enabled on port Ethernet1/0/22
 Re-authentication is enabled on port Ethernet1/0/23
 Re-authentication is enabled on port Ethernet1/0/24
```

图 3-22　重认证功能开启

```
[H3C-3600]dot1x timer ?
  acl-timeout        The time limit of ACL being valid
  handshake-period   Value of handshake interval with 8021x supplicant
  quiet-period       Interval following failed authentication
  reauth-period      Reauthenticate period
  server-timeout     Value of server timeout
  supp-timeout       Value of supplicant timeout
  tx-period          Interval between identity requests
  ver-period         Interval between version requests
[H3C-3600]dot1x timer reau
[H3C-3600]dot1x timer reauth-period ?
  INTEGER<60-7200>   Value of parameter (unit: second), the default is 3600
                     seconds
```

图 3-23　Re-authenticate timer 参数示意图

可以看到，默认情况下重认证间隔是 1h。将重认证间隔设为 60s 后，如图 3-24所示。这时，会有如图 3-25～图 3-27 所示的日志输出。

```
[H3C-3600]dis dot1x
 Global 802.1X protocol is enabled
 EAP authentication is enabled
 DHCP-launch is disabled
 Handshake is disabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD Quick Deploy is enabled

 Configuration: Transmit Period     120 s,  Handshake Period      1024
                ReAuth Period        60 s,  ReAuth MaxTimes         10
                Quiet Period         60 s,  Quiet Period Timer is disa
                Supp Timeout          2 s,  Server Timeout           100
                Interval between version requests is 30s
```

图 3-24　Re-authenticate timer 参数设置为 60s

18:40:36.031	LcAgent.exe	5248	4360	UserAuth...	ParseE...	461	收到 Eap-Request-ID =19
18:40:36.031	LcAgent.exe	5248	4360	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
18:40:36.078	AsmAssista...	5860	1556	..\AsmAs...	GetSelf...	362	GetSelfPath 取到自身存放路径 C:\Documents and Sett
18:40:36.093	AsmAssista...	5860	1556	MsacAss...	Workin...	900	发送心跳报文
18:40:36.125	AsmAssista...	5860	1556	MsacAss...	SendPa...	505	Send UDP packet: TradeCode: HeartTest Serial: 7166 Ty
18:40:36.359	AsmAssista...	5860	1556	MsacAss...	RecvPa...	585	Get UDP packet: TradeCode: HeartTest Serial: 7166 Typ
18:40:36.406	AsmAssista...	5860	1556	..\AsmAs...	GetSelf...	362	GetSelfPath 取到自身存放路径 C:\Documents and Sett
18:40:37.031	LcAgent.exe	5248	4360	UserAuth...	ParseE...	498	收到 Eap-Request-MD5
18:40:37.046	LcAgent.exe	5248	4360	UserAuth...	Respon...	267	ResponseMd5Challenge 分析认证结果并返回 Token
18:40:38.046	LcAgent.exe	5248	4360	UserAuth...	ParseE...	540	收到 Eap-Success

图 3-25 Re-authenticate timer 参数设置为 60s 效果 1

18:41:37.515	LcAgent.exe	5248	4360	UserAuth...	ParseE...	461	收到 Eap-Request-ID =21
18:41:37.515	LcAgent.exe	5248	4360	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
18:41:38.515	LcAgent.exe	5248	4360	UserAuth...	ParseE...	498	收到 Eap-Request-MD5
18:41:38.515	LcAgent.exe	5248	4360	UserAuth...	Respon...	267	ResponseMd5Challenge 分析认证结果并返回 Token
18:41:39.515	LcAgent.exe	5248	4360	UserAuth...	ParseE...	540	收到 Eap-Success

图 3-26 Re-authenticate timer 参数设置为 60s 效果 2

18:42:38.984	LcAgent.exe	5248	4360	UserAuth...	ParseE...	461	收到 Eap-Request-ID =23
18:42:38.984	LcAgent.exe	5248	4360	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
18:42:39.828	LcAgent.exe	5248	5552	Base_Net...	SendPa...	699	Send Online packet: TradeCode: HeartTest Serial: 1637
18:42:39.984	LcAgent.exe	5248	4360	UserAuth...	ParseE...	498	收到 Eap-Request-MD5
18:42:39.984	LcAgent.exe	5248	4360	UserAuth...	Respon...	267	ResponseMd5Challenge 分析认证结果并返回 Token
18:42:40.062	LcAgent.exe	5248	2808	Base_Net...	RecvPa...	772	Get packet: TradeCode: HeartTest Serial: 16377880 Ty
18:42:40.984	LcAgent.exe	5248	4360	UserAuth...	ParseE...	540	收到 Eap-Success

图 3-27 Re-authenticate timer 参数设置为 60s 效果 3

人们可以看到每次的 eap-request-ID 序列号都发生了递增（类似于 handshake period 而不同于 transmit period），而且每次客户端产生响应后交换机都完成了完整的认证过程（不同于响应 transmit period 的那个 request，交换机并没有进行处理），因此这可以真正确认客户端是否合法。

4）实例分析

（1）实例 1。在图 3-28 中可以看到 eap-request-ID=1 的包是每 2s 收到一个，这个包的特点是所有的序列号都是 1；而 eap-request-ID=4X 的包则是每 15s 收到一个，这个包的特点是序列号会递增。

通过在交换机中使用 dis dot1x 命令查看 802.1x 环境参数：

从图 3-29 中可以看到，序列号全部都为“1”的 Request 包是由“tx-period”所决定的，也可以发现利用递增的数字来记录数据包序列的 Request 包，则是由“handshake period”所决定的。

不断递增的 handshake 数据包，如图 3-30 所示。

全部 eap-request-ID=1 的数据包的时间间隔是一定的，只由 transmit period 决定。而 eap-request-ID=？的递增数据包的时间间隔则不规则，可以参照下面的实例分析 2（transmit period 为 120s）。

（2）实例 2。实例分析如图 3-31 所示。

在这个实例中，由于 transmit period 时间为 2min，可以看到很长时间都不见 eap-request-ID=1 的数据包出现，而 handshake period 却出现了不规则的变

2010-08-04	15:36:02.171	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 43
2010-08-04	15:36:02.187	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:07.046	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:07.062	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:09.359	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:09.359	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:11.656	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:11.671	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:13.953	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:13.953	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:14.968	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:15.000	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:17.312	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:17.312	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 44
2010-08-04	15:36:17.328	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:19.656	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:19.656	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:21.953	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:21.953	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:23.062	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:23.062	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:25.328	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:25.359	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:27.640	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:27.656	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:28.062	LcfSecurity.dll	3848	440	Se_IpMa...	SeIpMa...	93	没有取到 IP/MAC 策略
2010-08-04	15:36:29.968	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:29.984	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:30.984	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
2010-08-04	15:36:31.000	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
2010-08-04	15:36:32.046	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 45

图 3-28　实例分析 1

```
[H3C-3600]dis dot1x
 Global 802.1X protocol is enabled
 EAP authentication is enabled
 DHCP-launch is disabled
 Handshake is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD Quick Deploy is enabled

 Configuration: Transmit Period      2 s,  Handshake Period       15 s
                ReAuth Period     3600 s,  ReAuth MaxTimes         2
                Quiet Period        60 s,  Quiet Period Timer is disabled
                Supp Timeout        30 s,  Server Timeout          100 s
                Interval between version requests is 30s
                Maximal request times for version information is 3
                The maximal retransmitting times          2
```

图 3-29　dis dot1x 命令示例

15:46:27.859	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 64
15:46:27.859	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
15:46:28.265	LcfSecurity.dll	3848	440	Se_IpMa...	SeIpMa...	93	没有取到 IP/MAC 策略
15:46:32.656	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
15:46:32.671	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
15:46:37.546	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
15:46:37.546	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
15:46:42.531	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 1
15:46:42.531	LcAgent.exe	3848	3816	UserAuth...	Respon...	121	ResponseIdentity 发送身份信息
15:46:43.625	LcAgent.exe	3848	3816	UserAuth...	ParseE...	461	收到 Eap-Request-ID = 65

图 3-30　handshake 数据包示例

15:50:18.812	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 97
15:50:18.812	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:50:28.296	LcfSecurity.dll	3848	440	Se_IpMa...	SeIpMacBindThread	93	没有取到 IP/MAC 策略
15:50:29.078	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	889	等待请求超时，重发 EAP_Package_ID
15:50:29.078	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:50:39.296	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	889	等待请求超时，重发 EAP_Package_ID
15:50:39.296	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:50:49.531	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	889	等待请求超时，重发 EAP_Package_ID
15:50:49.531	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:50:54.015	LcfVirusSof...	3848	212	LcfDealVi...	LcfDealVirusLog_...	217	检测杀毒软件日志。。。。。
15:50:54.015	LcfVirusSof...	3848	212	LcfDealVi...	GetNewestPolicyI...	151	最新策略创建时间：(null)
15:50:54.015	LcfVirusSof...	3848	212	LcfDealVi...	LcfDealVirusLog_...	446	检测杀毒软件日志 完成
15:50:59.734	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	851	等待新认证请求。。。
15:51:04.546	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 98
15:51:04.562	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:51:14.890	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	889	等待请求超时，重发 EAP_Package_ID
15:51:14.937	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:51:25.078	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	889	等待请求超时，重发 EAP_Package_ID
15:51:25.078	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:51:28.343	LcfSecurity.dll	3848	440	Se_IpMa...	SeIpMacBindThread	93	没有取到 IP/MAC 策略
15:51:28.593	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 1
15:51:28.593	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:51:38.875	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	889	等待请求超时，重发 EAP_Package_ID
15:51:38.875	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:51:39.937	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 99
15:51:39.937	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:51:50.140	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	889	等待请求超时，重发 EAP_Package_ID
15:51:50.140	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:51:54.031	LcfVirusSof...	3848	212	LcfDealVi...	LcfDealVirusLog_...	217	检测杀毒软件日志。。。。。
15:51:54.046	LcfVirusSof...	3848	212	LcfDealVi...	GetNewestPolicyI...	151	最新策略创建时间：(null)
15:51:54.046	LcfVirusSof...	3848	212	LcfDealVi...	LcfDealVirusLog_...	446	检测杀毒软件日志 完成
15:52:00.453	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	889	等待请求超时，重发 EAP_Package_ID
15:52:00.453	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:52:10.609	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	889	等待请求超时，重发 EAP_Package_ID
15:52:10.625	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
15:52:20.703	LcAgent.exe	3848	3816	UserAuth...	ListeningProc	851	等待新认证请求。。。
15:52:25.656	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 100

图 3-31 实例分析 2

化，即 45s～35s～45s。如果把 handshake period 调小其他不变，如图 3-32 所示，则可以看到又恢复规则的变化，如图 3-33 所示。

```
[H3C-3600]dis dot1x
 Global 802.1X protocol is enabled
 EAP authentication is enabled
 DHCP-launch is disabled
 Handshake is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD Quick Deploy is enabled

 Configuration: Transmit Period     120 s,  Handshake Period        (5 s)
                ReAuth Period      3600 s,  ReAuth MaxTimes          2
                Quiet Period         60 s,  Quiet Period Timer is disabled
                Supp Timeout         30 s,  Server Timeout           100 s
                Interval between version requests is 30s
                Maximal request times for version information is 3
                The maximal retransmitting times          2
```

图 3-32 handshake 调小示例

这个实验的最后，看到 handshake period 数据包归零的现象，如图 3-34 所示。

由此我们知道 H3C 的序列号字段为 8 bit。

16:07:17.359	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 127
16:07:17.359	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:07:23.359	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 128
16:07:23.375	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:07:28.500	LcfSecurity.dll	3848	440	Se_IpMa...	SeIpMacBindThread	93	没有取到 IP/MAC 策略
16:07:29.390	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 129
16:07:29.390	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:07:30.390	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 1
16:07:30.390	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:07:35.171	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 130
16:07:35.171	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:07:41.218	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 131

图 3-33　handshake 示例效果

16:18:58.234	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 249
16:18:58.250	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:03.156	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 250
16:19:03.203	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:08.125	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 251
16:19:08.156	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:13.062	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 252
16:19:13.125	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:18.062	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 253
16:19:18.062	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:24.312	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 254
16:19:24.328	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:29.265	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 255
16:19:29.359	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:29.687	LcfSecurity.dll	3848	440	Se_IpMa...	SeIpMacBindThread	93	没有取到 IP/MAC 策略
16:19:33.078	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 1
16:19:33.078	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:34.140	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 0
16:19:34.140	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:40.296	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 2
16:19:40.359	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:45.328	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 3
16:19:45.328	LcAgent.exe	3848	3816	UserAuth...	ResponseIdentity	121	ResponseIdentity 发送身份信息
16:19:50.250	LcAgent.exe	3848	3816	UserAuth...	ParseEAPOL	461	收到 Eap-Request-ID = 4

图 3-34　handshake period 数据包归零

再将 handshake period 调大，其他不变，如 3-35 图所示。

```
[H3C-3600]dis dot1x
 Global 802.1X protocol is enabled
 EAP authentication is enabled
 DHCP-launch is disabled
 Handshake is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD Quick Deploy is enabled

 Configuration: Transmit Period     61 s,  Handshake Period       35 s
                ReAuth Period     3600 s,  ReAuth MaxTimes        2
                Quiet Period        60 s,  Quiet Period Timer is disabled
                Supp Timeout        30 s,  Server Timeout         100 s
                Interval between version requests is 30s
                Maximal request times for version information is 3
                The maximal retransmitting times          2
```

图 3-35　handshake 调大示例

在此情况下，则可以发现 handshake period 又呈现出 66s～56s～66s 的变化规律。

若我们将实例改成如下时间环境（supp-timeout 改为 2s），如图 3-36 所示。

```
[H3C-3600]dis dot1x
 Global 802.1X protocol is enabled
 EAP authentication is enabled
 DHCP-launch is disabled
 Handshake is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD Quick Deploy is enabled

 Configuration: Transmit Period     61 s,  Handshake Period       35 s
                ReAuth Period     3600 s,  ReAuth MaxTimes        2
                Quiet Period        60 s,  Quiet Period Timer is disabled
                Supp Timeout         2 s,  Server Timeout         100 s
                Interval between version requests is 30s
                Maximal request times for version information is 3
                The maximal retransmitting times          2
```

图 3-36　handshake 调大且 supp-timeout 改为 2s 示例

此时会发现：supp-timeout 对 handshake period 并没有产生影响。由此可知 supp-timeout 的作用。

5）调试 802.1x

（1）查看 802.1x 整体环境参数。

dis dot1x

//如图 3-37 所示

从图 3-37 可以看到全局下的 802.1x 运行环境和运行参数（如握手时间、静默时间等）。并且可以看到端口下的配置情况，如图 3-38 所示。

```
<H3C-3600>dis dot1x
 Global 802.1X protocol is enabled
 EAP authentication is enabled
 DHCP-launch is disabled
 Handshake is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD Quick Deplcy is disabled

 Configuration: Transmit Period     30 s,  Handshake Period       15 s
                ReAuth Period     3600 s,  ReAuth MaxTimes        2
                Quiet Period        60 s,  Quiet Period Timer is disabled
                Supp Timeout        30 s,  Server Timeout         100 s
                Interval between version requests is 30s
                Maximal request times for version information is 3
                The maximal retransmitting times          2
 EAD Quick Deploy configuration:
                Acl-timeout:   30 m

 Total maximum 802.1x user resource number is 1024
 Total current used 802.1x resource number is 1
```

图 3-37　dis dot1x 命令

由图 3-38 可见，默认的 802.1x 端口下配置是 mac-based，authentication 模式也是 auto。

```
Ethernet1/0/21  is link-down
  802.1X protocol is enabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Check is disabled
  The port is an authenticator
  Authentication Mode is Auto
  Port Control Type is Mac-based
  ReAuthenticate is disabled
  Max number of on-line users is 256

  Authentication Success: 3, Failed: 3
  EAPOL Packets: Tx 595, Rx 1142
  Sent EAP Request/Identity Packets : 587
       EAP Request/Challenge Packets: 0
  Received EAPOL Start Packets : 3
           EAPOL LogOff Packets: 0
           EAP Response/Identity Packets : 1131
           EAP Response/Challenge Packets: 3
           Error Packets: 0

  Controlled User(s) amount to 0
```

图 3-38　端口配置情况

(2) 查看 802.1x 会话参数。

dis dot1x sessions

//如图 3-39 所示

```
[H3C-3600]dis dot1x sessions
 Global 802.1X protocol is enabled
 EAP authentication is enabled
 EAD Quick Deploy configuration:
               Acl-timeout:   30 m

 Total maximum 802.1x user resource number is 1024
 Total current used 802.1x resource number is 0
```

图 3-39　dis dot1x sessions 命令

此命令主要用于查看认证方式（eap、chap 等）及是否开启了 EAD 的快速部署。另外还可以看到端口下的 802.1x 配置情况和认证用户（MAC 地址），如图 3-40所示。

(3) 查看 eap 包统计信息。

dis dot1x statistics

//如图 3-41 所示，从图中可以查看各种 eap 包的收发

(4) 查看端口下是否有设备认证通过。

dis dot1x interface Ethernet【port number】

//如图 3-42 所示

从图 3-43 中可以看到获取到 23 口下一台设备的 MAC 地址，且未认证。认

```
Ethernet1/0/23  is link-up
  802.1X protocol is enabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Cneck is disabled
1. Authenticated user : MAC address: 0016-d3e8-7887

  Controlled User(s) amount to 1

Ethernet1/0/24  is link-up
  802.1X protocol is disabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Check is disabled

  Controlled User(s) amount to 0
```

图 3-40　端口的 802.1x 配置情况

```
  Ethernet1/0/23  is link-up
    802.1X protocol is enabled
    Proxy trap checker is disabled
    Proxy logoff checker is disabled
    Version-Check is disabled

    Authentication Success: 2, Failed: 41
    EAPOL Packets: Tx 682, Rx 453
    Sent EAP Request/Identity Packets : 639
         EAP Request/Challenge Packets: 0
    Received EAPOL Start Packets : 3
             EAPOL LogOff Packets: 0
             EAP Response/Identity Packets : 445
             EAP Response/Challenge Packets: 2
             Error Packets: 0

    Controlled User(s) amount to 1
```

图 3-41　端口配置情况

图 3-42　dis dot1x interface 命令

证过后的状态，如图 3-44 所示。

(5) 查看 RADIUS 方案及 RADIUS 服务器。

dis radius scheme【name of scheme】

//如图 3-45 所示

这是查看 RADIUS 服务器（amc）状态很重要的一条命令，可以看到连通性——state=active/block，目前使用的端口号，会话密钥 key、accouting 方式、username-format 等。

```
[H3C-3600]dis dot1x interface Ethernet 1/0/23
```

```
Ethernet1/0/23  is link-up
  802.1X protocol is enabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Cneck is disabled
1. Authenticated user : MAC address: 0016-d3e8-7887

  Controlled User(s) amount to 1

Ethernet1/0/24  is link-up
  802.1X protocol is disabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Check is disabled

  Controlled User(s) amount to 0
```

图 3-40　端口的 802.1x 配置情况

```
Ethernet1/0/23  is link-up
  802.1X protocol is enabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Check is disabled

  Authentication Success: 2, Failed: 41
  EAPOL Packets: Tx 682, Rx 453
  Sent EAP Request/Identity Packets : 639
       EAP Request/Challenge Packets: 0
  Received EAPOL Start Packets : 3
           EAPOL LogOff Packets: 0
           EAP Response/Identity Packets : 445
           EAP Response/Challenge Packets: 2
           Error Packets: 0

  Controlled User(s) amount to 1
```

图 3-41　端口配置情况

```
[H3C-3600]dis dot1x interface Ethernet 1/0/23
```

图 3-42　dis dot1x interface 命令

证过后的状态，如图 3-44 所示。

(5) 查看 RADIUS 方案及 RADIUS 服务器。

dis radius scheme【name of scheme】

//如图 3-45 所示

这是查看 RADIUS 服务器（amc）状态很重要的一条命令，可以看到连通性——state=active/block，目前使用的端口号，会话密钥 key、accouting 方式、username-format 等。

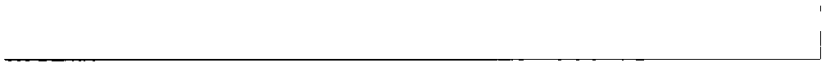


图 3-43　端口下设备未通过认证

图 3-44　端口下设备通过认证

```
[H3C-3600]dis radius scheme my_scheme
SchemeName  =my_scheme                          Index=1    Type=standard
Primary Auth IP  =192.168.54.200   Port=1812
Primary Acct IP  =N/A              Port=1813
Auth Server Encryption Key= msackey
Acct Server Encryption Key= Not configured
Accounting method = optional
Accounting-On packet disable, send times = 15 , interval = 3s
TimeOutValue(in second)=3 RetryTimes=3 RealtimeACCT(in minute)=12
Permitted send realtime PKT failed counts       =5
Retry sending times of noresponse acct-stop-PKT =500
nas-ip:Source-IP-address                        =N/A
Quiet-interval(min)                             =5
Username format                                 =with-domain
Data flow unit                                  =Byte
Packet unit                                     =1
calling_station_id format                       =XXXX-XXXX-XXXX in lowercase
Primary Auth IP  =192.168.54.200
  State(unit)=A(1)  (A:Acitve/B:Block)
Primary Acct IP  =N/A
  State(unit)=B(1)
```

图 3-45　dis radius scheme 命令

```
Ethernet1/0/23  is link-up
  802.1X protocol is enabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Check is enabled
  The port is an authenticator
  Authentication Mode is Auto
  Port Control Type is Mac-based
  ReAuthenticate is disabled
  Max number of on-line users is 256

  Authentication Success: 1, Failed: 373
  EAPOL Packets: Tx 675, Rx 488
  Sent EAP Request/Identity Packets : 283
       EAP Request/Challenge Packets: 0
  Received EAPOL Start Packets : 23
           EAPOL LogOff Packets: 0
           EAP Response/Identity Packets : 455
           EAP Response/Challenge Packets: 1
           Error Packets: 0
1. Unauthenticated user : MAC address: 0016-d3e8-7887
```

```
Ethernet1/0/23  is link up
  802.1X protocol is enabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Check is enabled
  The port is an authenticator
  Authentication Mode is Auto
  Port Control Type is Mac-based
  ReAuthenticate is disabled
  Max number of on-line users is 256

  Authentication Success: 2, Failed: 373
  EAPOL Packets: Tx 698, Rx 521
  Sent EAP Request/Identity Packets : 303
       EAP Request/Challenge Packets: 0
  Received EAPOL Start Packets : 23
           EAPOL LogOff Packets: 0
           EAP Response/Identity Packets : 487
           EAP Response/Challenge Packets: 2
           Error Packets: 0
1. Authenticated user : MAC address: 0016-d3e8-7887
```

```
Ethernet1/0/23  is link-up
  802.1X protocol is enabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Check is enabled
  The port is an authenticator
  Authentication Mode is Auto
  Port Control Type is Mac-based
  ReAuthenticate is disabled
  Max number of on-line users is 256

  Authentication Success: 1, Failed: 373
  EAPOL Packets: Tx 675, Rx 488
  Sent EAP Request/Identity Packets : 283
       EAP Request/Challenge Packets: 0
  Received EAPOL Start Packets : 23
           EAPOL LogOff Packets: 0
           EAP Response/Identity Packets : 455
           EAP Response/Challenge Packets: 1
           Error Packets: 0
1. Unauthenticated user : MAC address: 0016-d3e8-7887
```

图 3-43　端口下设备未通过认证

```
Ethernet1/0/23  is link-up
  802.1X protocol is enabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Check is enabled
  The port is an authenticator
  Authentication Mode is Auto
  Port Control Type is Mac-based
  ReAuthenticate is disabled
  Max number of on-line users is 256

  Authentication Success: 2, Failed: 373
  EAPOL Packets: Tx 698, Rx 521
  Sent EAP Request/Identity Packets : 303
       EAP Request/Challenge Packets: 0
  Received EAPOL Start Packets : 23
           EAPOL LogOff Packets: 0
           EAP Response/Identity Packets : 487
           EAP Response/Challenge Packets: 2
           Error Packets: 0
1. Authenticated user : MAC address: 0016-d3e8-7887
```

图 3-44　端口下设备通过认证

```
[H3C-3600]dis radius scheme my_scheme
SchemeName   =my_scheme                          Index=1    Type=standard
Primary Auth IP   =192.168.54.200   Port=1812
Primary Acct IP   =N/A              Port=1813
Auth Server Encryption Key= msackey
Acct Server Encryption Key= Not configured
Accounting method = optional
Accounting-On packet disable, send times = 15 , interval = 3s
TimeOutValue(in second)=3 RetryTimes=3 RealtimeACCT(in minute)=12
Permitted send realtime PKT failed counts       =5
Retry sending times of noresponse acct-stop-PKT =500
nas-ip:Source-IP-address                        =N/A
Quiet-interval(min)                             =5
Username format                                 =with-domain
Data flow unit                                  =Byte
Packet unit                                     =1
calling_station_id format                       =XXXX-XXXX-XXXX in lowercase
Primary Auth IP   =192.168.54.200
  State(unit)=A(1)  (A:Acitve/B:Block)
Primary Acct IP   =N/A
  State(unit)=B(1)
```

图 3-45　dis radius scheme 命令

6. 技术对比

可以通过 ARP 准入和 802.1x 准入两种架构的比较来进一步理清 Software-Based NAC 与 Infrastructure-Based NAC 架构的区别。

通过 ARP 干扰的网络准入控制方案分为两个部分。

(1) 通过一个预先安装好的探测器模块监测本网段有哪些机器、哪些机器是安装了客户端代理、哪些机器没有安装客户端代理，通过 ARP 欺骗包来限制或者禁止没有安装客户端代理的桌面 PC 机访问服务器资源。

(2) 通过强制在主机上安装客户端软件，检查客户端用户身份和是否满足安全策略。对于 Guest 身份的用户，客户端软件限制他们只能访问访客区的服务器资源；对于不满足安全策略要求的内部用户，客户端软件限制他们只能访问修复区的服务器资源。

虽然通过 ARP 干扰的网络准入控制方案好像也能够达到 802.1x 网络准入控制方案的效果，但这两者是有本质不同的：通过 ARP 干扰的网络准入控制方案是通过客户端代理软件来控制客户机可以访问的 IP 资源，由于操作系统兼容性的问题，这种软件方式存在很严重的稳定性影响；而 802.1x 网络准入控制方案是通过网络交换机控制客户机可以访问的网络资源（所属 VLAN），由于交换机作为网络设备的稳定性要求，802.1x 方案的稳定性要远远高于 ARP 欺骗方式。

802.1x 过时了吗？谈到 802.1x，前沿的 NAC 人员恐怕都有些嗤之以鼻，而那些体验过 802.1x 威力的企业雇员们也是谈虎色变。2011 是 Agentless 应用“大跳草裙舞”的年份，而这确实和 802.1x 沾不到边。

与潮流相反，人们看到在某运营商的 NAC 案例中，管理者们力挺 802.1x 的异军突起之势。其实，抛开 802.1x 对于接入用户的友好性和管理者的工作量不谈，这种前辈级（在 IT 界，10 年弹指一挥，可以算是一辈了）的安全技术在控制力度、out-of-band 典型性、管理流程、跨厂商兼容性以及边界定义能力上确实可以作为 NAC 技术后起之秀们的表率。在国内众多新兴 NAC 技术如雨后春笋般冒出的时候，大部分却都存在一个致命的弱点——在路由边界上，管理被终结。而 802.1x 却能够穿越层层路由，向冰岛的 Radius 认证站传输来自火地岛的接入信息，这在运营商的复杂网络中不啻是一股福音。而人们惊喜地看见了运营商对老技术新用的创新敏感度，提出在 802.1x 认证流中结合短信验证码来识别用户身份，毕竟短信网关在运营商网络中实在是“白菜”一般了。这也给众多的 802.1x Fans 们提供了旧瓶新酒的灵感。如果你不讨厌客户端，那么好吧，这个组合还是有点陈年佳酿的厚重味感的。

3.3.2 EOU 网络准入控制技术分析

网络设备制造商的私有准入协议必定是只能够适用于其自身的网络环境，因此 EOU 和下一节要分析的 PORTAL/PORTAL+，这两种准入控制技术很符合

Infrastructure-Based NAC 的特征，就是各有其特定的网络基础架构作为平台，在这个平台（Infrastructure）之上来展开所有的准入实现。

分别来看，不管是 Cisco 的 EOU 还是 H3C 的 PORTAL/PORTAL+都对网络环境的要求较高，Cisco 的 EOU 要求接入层交换机采用 Catalyst 3560 或以上，并且对 IOS 的版本也有一定的限制；而 H3C 的 PORTAL/PORTAL+则基本是路由器层面的技术，要求至少达到 S5500 EI 以上的交换机或基本的企业级路由器进行支持。

鉴于以上特点，以上两种技术在国内基本只能够局限于基础网络较为规范，且配置较高的行业性大客户中，这就决定了相比 802.1x 这样的大众技术，具有厂商特性的准入架构在国内更像是一种小众概念，虽然架构本身够完善，但其理论研究价值可能更大于在实际行业中的应用价值。

1. 技术实现原理

EOU 架构的核心在于动态 ACL 的切换，因此必须基于三层交换机环境，其基本原理的示意图如图 3-46 所示。

图 3-46　EOU 架构基本原理示意图

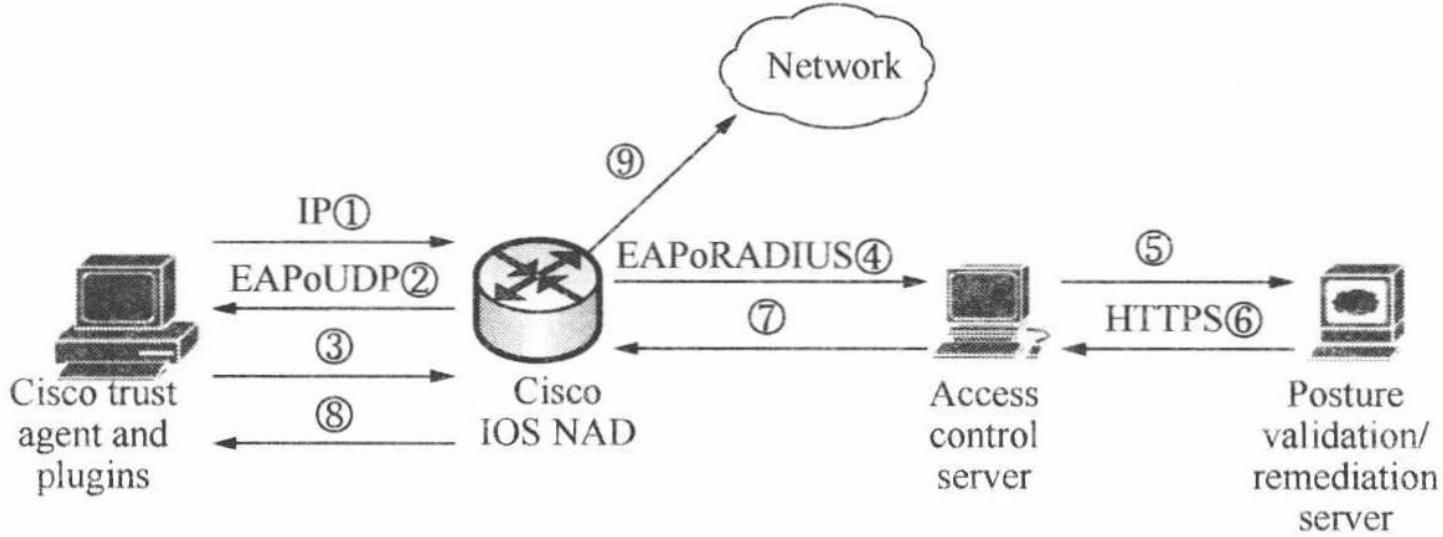
在整个 EOU 架构中，基本的控制数据流都是基于标准的 eap 报文，但与 802.1x 的 eap 报文根本上的区别如下：

802.1x 的 eap 是承载在 2 层帧上的，因此又被称为 EAPoL（EAP over LAN），因此入网终端与认证设备（交换机）的交互是去 IP 地址的，这样也就无法进行基于 http 的 Web 页面交互。

EOU 又被称作 EAPoU（EAP over UDP），从名称中可以看出这个架构是承载在 UDP 报文之上的，因此是一个 3 层架构，这样就可以进行基于 http 的 Web 页面引导，故 EOU 对于入网用户的友好型和交互性要远远高于 802.1x 架构。

EOU 架构有 3 个基本的组成，包括用户端的 Client、作为认证控制和信息中继的交换设备（如 Cisco 3560）以及一台 Cisco RADIUS 服务器，在 Cisco 架构中一般会额外再提供一台 Posture Server 以及其他第三方厂商融合在架构中的联动设备。

对于入网用户来说，可以利用预先安装好的 CAA（Cisco Access Agent）发


Network
⑨
IP①
EAPoUDP②
③
⑧
EAPoRADIUS④
⑦
⑤
HTTPS⑥
Cisco trust agent and plugins
Cisco IOS NAD
Access control server
Posture validation/ remediation server

Infrastructure-Based NAC 的特征，就是各有其特定的网络基础架构作为平台，在这个平台（Infrastructure）之上来展开所有的准入实现。

分别来看，不管是 Cisco 的 EOU 还是 H3C 的 PORTAL/PORTAL+都对网络环境的要求较高，Cisco 的 EOU 要求接入层交换机采用 Catalyst 3560 或以上，并且对 IOS 的版本也有一定的限制；而 H3C 的 PORTAL/PORTAL+则基本是路由器层面的技术，要求至少达到 S5500 EI 以上的交换机或基本的企业级路由器进行支持。

鉴于以上特点，以上两种技术在国内基本只能够局限于基础网络较为规范，且配置较高的行业性大客户中，这就决定了相比 802.1x 这样的大众技术，具有厂商特性的准入架构在国内更像是一种小众概念，虽然架构本身够完善，但其理论研究价值可能更大于在实际行业中的应用价值。

1. 技术实现原理

EOU 架构的核心在于动态 ACL 的切换，因此必须基于三层交换机环境，其基本原理的示意图如图 3-46 所示。

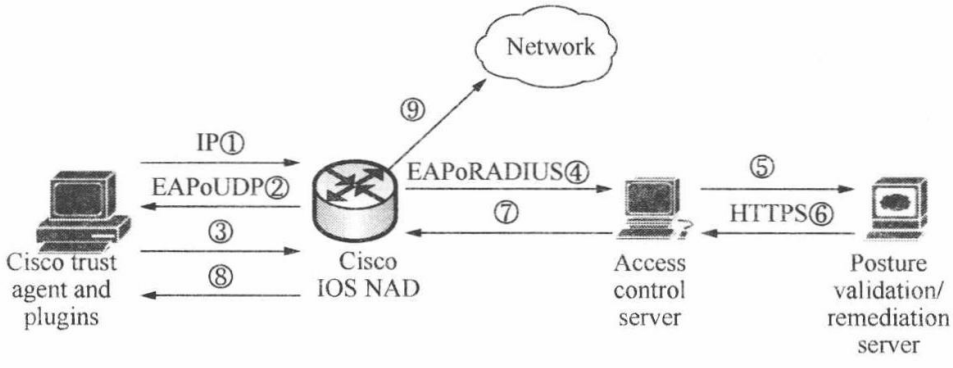


图 3-46　EOU 架构基本原理示意图

在整个 EOU 架构中，基本的控制数据流都是基于标准的 eap 报文，但与 802.1x 的 eap 报文根本上的区别如下：

802.1x 的 eap 是承载在 2 层帧上的，因此又被称为 EAPoL（EAP over LAN），因此入网终端与认证设备（交换机）的交互是去 IP 地址的，这样也就无法进行基于 http 的 Web 页面交互。

EOU 又被称作 EAPoU（EAP over UDP），从名称中可以看出这个架构是承载在 UDP 报文之上的，因此是一个 3 层架构，这样就可以进行基于 http 的 Web 页面引导，故 EOU 对于入网用户的友好型和交互性要远远高于 802.1x 架构。

EOU 架构有 3 个基本的组成，包括用户端的 Client、作为认证控制和信息中继的交换设备（如 Cisco 3560）以及一台 Cisco RADIUS 服务器，在 Cisco 架构中一般会额外再提供一台 Posture Server 以及其他第三方厂商融合在架构中的联动设备。

对于入网用户来说，可以利用预先安装好的 CAA（Cisco Access Agent）发

起 EAP 认证过程，Cisco 的交换设备将判断接入终端的状态，在 EOU 框架中存在如下 3 种基本的终端状态。

① Healthy：代表终端完全符合要求，一般是认证和安检都通过的终端；

② Quarantine：代表终端不符合安全要求，比如未完成认证，或未通过安检；

③ Static：处于这种状态下的终端一般是网络中的例外设备，比如无法进行认证的打印机等。

Cisco 的 Posture Server 将依据不同的状态通知 Radius Server，并向交换设备下发与状态匹配的 ACL，交换设备（如 Cisco 3560）能够在接入层通过 ACL 的控制来实现 Web 重定向、权限控制等 NAC 功能。

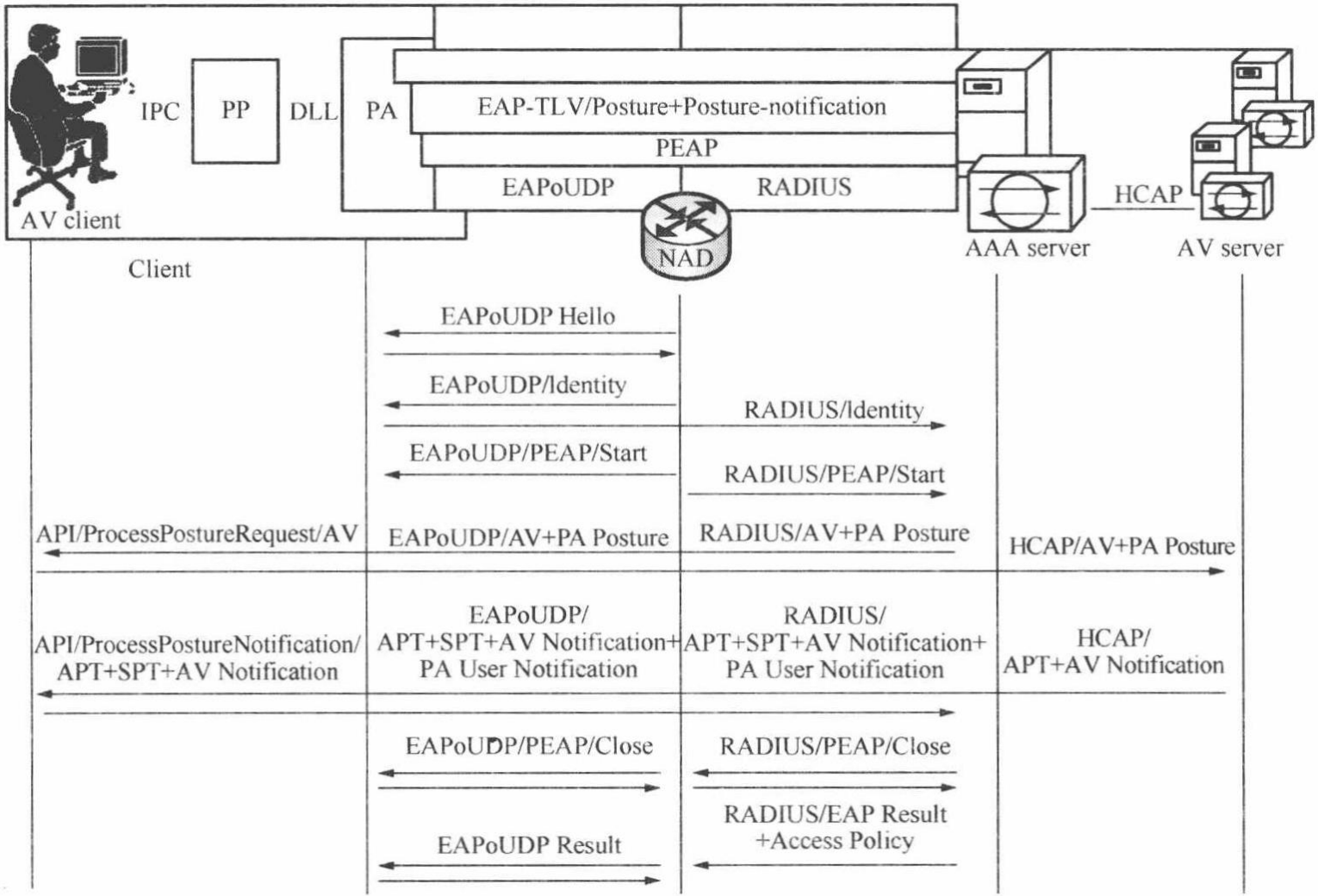
2. 工作过程

一个完整的 EOU 工作过程如图 3-47 所示，需要注意的是，如下的流程是在安装了 Cisco 的 CAA 客户端环境下实现的，因此能够在用户端就发出涵盖 identity 和 posture 的 EAP 数据包。

图 3-47 EOU 架构工作过程

3. 主要特点

EOU 网络准入控制技术主要特点如表 3-3 所示。


IPC
PP
DLL
PA
EAP-TLV/Posture+Posture-notification
PEAP
EAPoUDP
RADIUS
AV client
NAD
HCAP
AAA server
AV server
Client
EAPoUDP Hello
EAPoUDP/Identity
RADIUS/Identity
EAPoUDP/PEAP/Start
RADIUS/PEAP/Start
API/ProcessPostureRequest/AV
EAPoUDP/AV+PA Posture
RADIUS/AV+PA Posture
HCAP/AV+PA Posture
API/ProcessPostureNotification/
APT+SPT+AV Notification
EAPoUDP/
APT+SPT+AV Notification+
PA User Notification
RADIUS/
APT+SPT+AV Notification+
PA User Notification
HCAP/
APT+AV Notification
EAPoUDP/PEAP/Close
RADIUS/PEAP/Close
RADIUS/EAP Result
+Access Policy
EAPoUDP Result

起 EAP 认证过程，Cisco 的交换设备将判断接入终端的状态，在 EOU 框架中存在如下 3 种基本的终端状态。

① Healthy：代表终端完全符合要求，一般是认证和安检都通过的终端；

② Quarantine：代表终端不符合安全要求，比如未完成认证，或未通过安检；

③ Static：处于这种状态下的终端一般是网络中的例外设备，比如无法进行认证的打印机等。

Cisco 的 Posture Server 将依据不同的状态通知 Radius Server，并向交换设备下发与状态匹配的 ACL，交换设备（如 Cisco 3560）能够在接入层通过 ACL 的控制来实现 Web 重定向、权限控制等 NAC 功能。

2. 工作过程

一个完整的 EOU 工作过程如图 3-47 所示，需要注意的是，如下的流程是在安装了 Cisco 的 CAA 客户端环境下实现的，因此能够在用户端就发出涵盖 identity 和 posture 的 EAP 数据包。

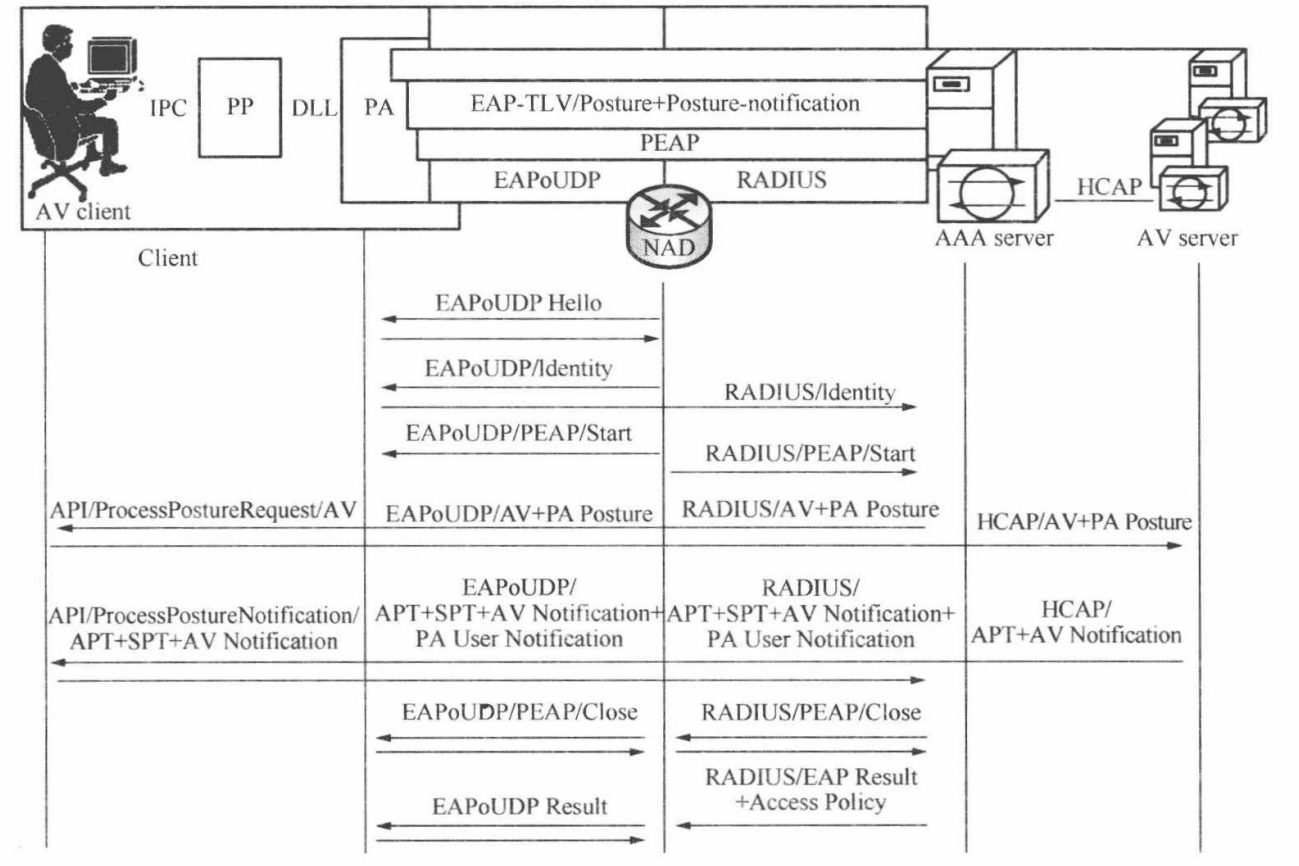


图 3-47 EOU 架构工作过程

3. 主要特点

EOU 网络准入控制技术主要特点如表 3-3 所示。

表 3-3　EOU 网络准入控制技术主要特点

NAC 体系	对应参数	备注
架构组成	CAA（Cisco Access Agent） + Cisco Switch + CAS + Posture Server	也能够支持无客户端模式，但在国内只有少数第三方 NAC 厂商能够支持
支持环境	Cisco 3 层交换机	Cisco3550 以上（IOS 有要求）
旁路部署	√	只传输控制流，完全旁路
无客户端支持	√	
交换机配置量	极大	所有接入层交换机均进行配置，且配置复杂
接入层端口级控制	√	能够精细到端口下的单台电脑，比 802.1x 控制力度更精细
Hub 接入控制	√	
http 快捷性	√	由于可以选择放通部分流量，因此能够兼容 DHCP 环境，可以进行 Web 重定向引导
系统资源（内存）占用	小	在无客户端环境下占用小
来宾管理	好	能够进行 Web 引导，因此十分友好
稳定性	好	在无客户端环境下可以依赖交换机及服务器来确保稳定性； 但在某些 IOS 环境下会发生误判
兼容性	×	只能运行在 Cisco 自有环境
防单点故障	√	EOU 协议本身支持对 RADIUS 服务器存活状态的监测，一旦发现宕机，交换机能够立即解除 EOU 控制，放通网络

4. 配置方法

1）配置认证服务器

```
aaa new-model
aaa group server radius ASMEOU
server-private 192.168.56.4 auth-port 1812 acct-port 1813 key msackey
server-private 192.168.56.5 auth-port 1812 acct-port 1813 key msackey
```

2）配置认证

```
aaa authorization network default local
```

aaa accounting network default none

aaa authentication login default line

//此处可参考 802.1x 的 AAA 认证配置

radius-server attribute 8 include-in-access-req

radius-server vsa send authentication

radius-server deadtime 720

radius-server dead-criteria tries 3

3）配置所有都放开的 ACL

IP access-list extended ASMEouAllAcl

permit IP any any

4）配置 URL 重定向的 ACL

IP access-list extended ASMEouUrlAcl

deny tcp any host 192.168.56.14 eq www

permit tcp any any eq www

5）配置缺省的 ACL

IP access-list extended ASMEouDefaultAcl

remark allow DHCP

permit udp any any eq bootps

remark allow DNS

permit udp any any eq domain

remark allow to the server

permit ip any host 192.168.56.14

remark deny other

deny ip any any

6）配置 AAA 的 fail-open 策略

identity policy AaaDown

access-group ASMEouAllAcl

7）配置例外设备的策略

identity profile eapoudp

device authorize ip-address 192.168.56.128 policy AaaDown

8）开启全局的 EOU 配置

aaa authentication eou default group ASMEOU

ip admission name ASMEouNac eapoudp bypass event timeout aaa policy identity AaaDown

eou allow clientless

ip device tracking

9）开启端口的 EOU 配置

```
interface range fa0/13 -24
switchport mode access
ip access-group ASMEouDefaultAcl in
#spanning-tree portfast
ip admission ASMEouNac
```

在上述配置中，我们看到，整个 EOU 架构在交换设备上的搭建需要众多命令的组合，因此平台体系较为庞大，对于一个维护大型网络的管理员而言是不小的考验，加之众多 ACL 的配置，稍有不慎就有可能导致断网，因此，人工管理的风险是购买时必须考虑的因素。

3.3.3　PORTAL/PORTAL＋网络准入控制技术分析

PORTAL 本是华为公司在 21 世纪初推出的针对宽带接入的控制架构，因此在设计之初主要是考虑用于路由器体系中作为网关型的访问控制。

在华为公司将交换机业务剥离给 H3C 后，H3C 在华为公司原 PORTAL 协议的基础上推出了 PORTAL＋，升级版的 PORTAL＋加入了对部分企业级 3 层交换设备的支持，因此可以在购买了支持 PORTAL 协议的交换机后在网关级别部署整个准入控制体系。

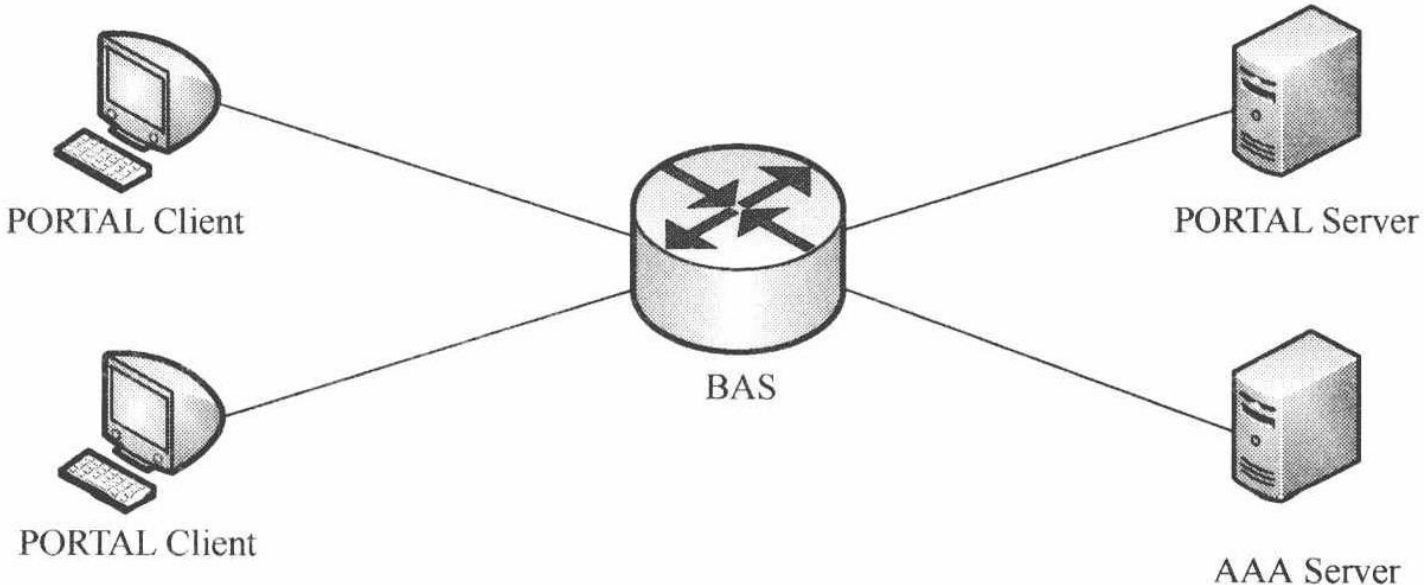
1. 技术实现原理

PORTAL 在英语中是入口的意思。PORTAL 认证通常也被称为 Web 认证，一般将 PORTAL 认证的网站称为门户网站。未认证用户上网时，搭建了 PORTAL 环境的设备将强制用户登录到特定站点，用户将在此特定站点上完成认证和其他安全规范要求，只有通过后才可以使用互联网资源。

1）基本要素

如图 3-48 所示，PORTAL 认证过程涉及到了认证客户端（PORTAL Client），PORTAL 服务器（PORTAL Server），BAS 和 AAA 服务器四个基本要素。

图 3-48　PORTAL 认证组成要素


PORTAL Client
PORTAL Client
BAS
PORTAL Server
AAA Server

9）开启端口的 EOU 配置

```
interface range fa0/13 -24
switchport mode access
ip access-group ASMEouDefaultAcl in
#spanning-tree portfast
ip admission ASMEouNac
```

在上述配置中，我们看到，整个 EOU 架构在交换设备上的搭建需要众多命令的组合，因此平台体系较为庞大，对于一个维护大型网络的管理员而言是不小的考验，加之众多 ACL 的配置，稍有不慎就有可能导致断网，因此，人工管理的风险是购买时必须考虑的因素。

3.3.3　PORTAL/PORTAL＋网络准入控制技术分析

PORTAL 本是华为公司在 21 世纪初推出的针对宽带接入的控制架构，因此在设计之初主要是考虑用于路由器体系中作为网关型的访问控制。

在华为公司将交换机业务剥离给 H3C 后，H3C 在华为公司原 PORTAL 协议的基础上推出了 PORTAL＋，升级版的 PORTAL＋加入了对部分企业级 3 层交换设备的支持，因此可以在购买了支持 PORTAL 协议的交换机后在网关级别部署整个准入控制体系。

1. 技术实现原理

PORTAL 在英语中是入口的意思。PORTAL 认证通常也被称为 Web 认证，一般将 PORTAL 认证的网站称为门户网站。未认证用户上网时，搭建了 PORTAL 环境的设备将强制用户登录到特定站点，用户将在此特定站点上完成认证和其他安全规范要求，只有通过后才可以使用互联网资源。

1）基本要素

如图 3-48 所示，PORTAL 认证过程涉及到了认证客户端（PORTAL Client），PORTAL 服务器（PORTAL Server），BAS 和 AAA 服务器四个基本要素。

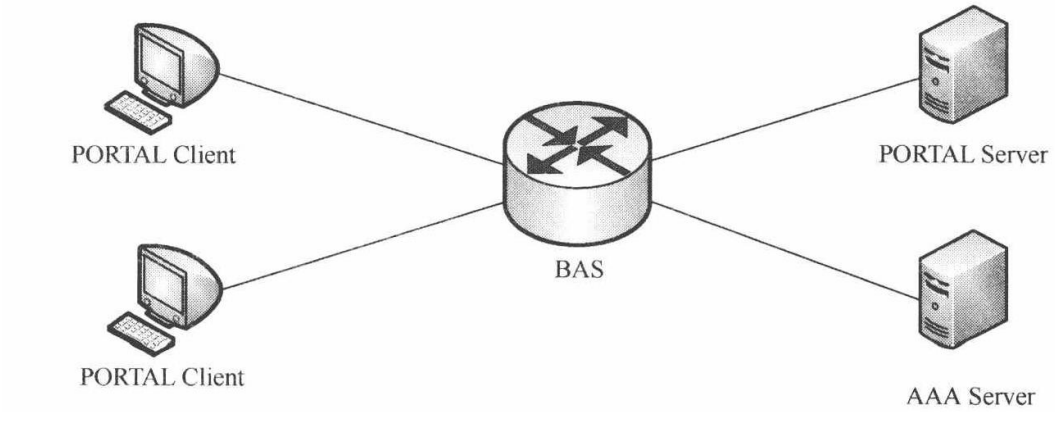


图 3-48　PORTAL 认证组成要素

（1）PORTAL Client。PORTAL 组网中发起认证请求的客户端系统，为运行 HTTP 协议的浏览器；

（2）PORTAL Server。PORTAL 组网中接受客户端认证请求的服务端系统，提供免费门户服务和基于 Web 认证的界面，与 BAS 设备交互认证客户端的身份信息；

（3）BAS。宽带接入服务器，用于向 PORTAL Server 重定向 HTTP 认证请求，并且与 PORTAL Server、AAA 服务器交互完成用户的认证/授权/计费功能；

（4）AAA 服务器：认证/授权/计费服务器，与 BAS 进行交互，对用户进行认证/授权/计费。

2）交互过程

以上四个基本要素的交互过程为：

① 未认证用户访问网络时，在 IE 地址栏中输入一个跨网段的访问地址，那么此 HTTP 请求在经过 BAS 设备时会被重定向到 PORTAL Server 的 Web 认证主页上；

② 用户在认证主页/认证对话框中输入认证信息后提交，PORTAL Server 会将用户的认证信息传递给 BAS；

③ BAS 与 AAA 服务器通信进行用户认证和计费；

④ 认证通过后，BAS 会打开用户与资源区域的通路，允许用户访问资源。

3）协议框架

PORTAL 协议包括 PORTAL 接入和 PORTAL 认证两部分，协议框架如图 3-49 所示。

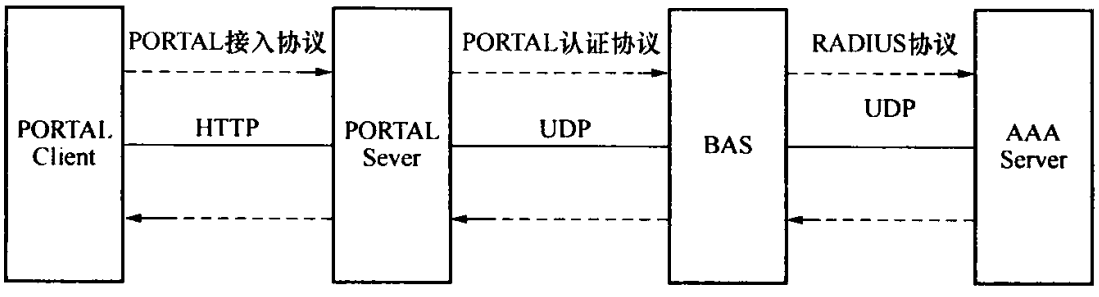


图 3-49 PORTAL 协议框架

PORTAL 接入协议描述了 PORTAL Client 和 PORTAL Server 之间的协议交互，主要内容包括：

① PORTAL Client 通过 HTTP 协议向 PORTAL Server 提交认证信息；

② PORTAL Server 通过 HTTP 协议向 PORTAL Client 推出认证成功或者认证失败页面；

③ PORTAL Server 与 PORTAL Client 间通过握手检测用户是否在线；

PORTAL 认证协议描述了 PORTAL Server 和 BAS 之间的协议交互，主要

内容包括：

① PORTAL 认证协议采用了非严格意义上的 Client/Server 结构，大部分消息采用 Request/Response 进行交互。同时还定义了一种 Notify 报文，提供 PORTAL Server 和 BAS 设备之间的消息通道；

② PORTAL 认证协议承载在 UDP 报文上；

③ PORTAL Server 使用本地的特定 UDP 端口监听 BAS 设备发送的非响应类报文，并向 BAS 设备特定的端口发送所有报文。BAS 使用本地的特定的 UDP 端口监听 PORTAL Server 发送的所有报文，并向 PORTAL Server 的特定端口发送非响应类报文。响应类报文的目的端口号使用对应的请求报文的源端口号。

2. 工作过程

PORTAL 认证有两种认证方式：二层认证方式和三层认证方式。

1）二层认证方式

二层认证方式又包括直接认证方式和二次地址方式。

二次认证方式下，PORTAL Client 与 BAS 直连，或它们之间只有二层设备存在；

直接认证方式下，用户通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在认证通过之前，只能访问 PORTAL 服务器以及设定的免费访问地址，认证通过后可使用此 IP 地址访问外部网络。

二者比较，直接认证流程简单，但由于限制了 PORTAL Client 只能与 BAS 通过二层交换设备互连，降低了组网的灵活性；二次地址方式下，用户通过 DHCP 获取一个私网 IP 地址进行认证，在认证通过之前，只能访问 PORTAL 服务器以及设定的免费访问地址，认证通过后，释放原有私网 IP 地址，使用重新分配的公网 IP 地址访问外部网络，二次地址方式流程较为复杂，认证通过之前用户可使用私网 IP 地址，节省了公网 IP 地址，但组网方式不灵活。

2）三层认证方式

这种认证方式允许 PORTAL Client 和 BAS 之间跨接三层转发设备，组网方式灵活。

因为三层认证流程与直接认证方式相同，下面将仅对直接认证方式的认证流程和二次地址方式的认证流程做详细描述。

直接认证方式的认证流程如图 3-50 所示。

二次地址方式的认证流程如图 3-51 所示。

3. 主要特点

PORTAL/PORTAL＋网络准入控制技术主要特点如表 3-4 所示。

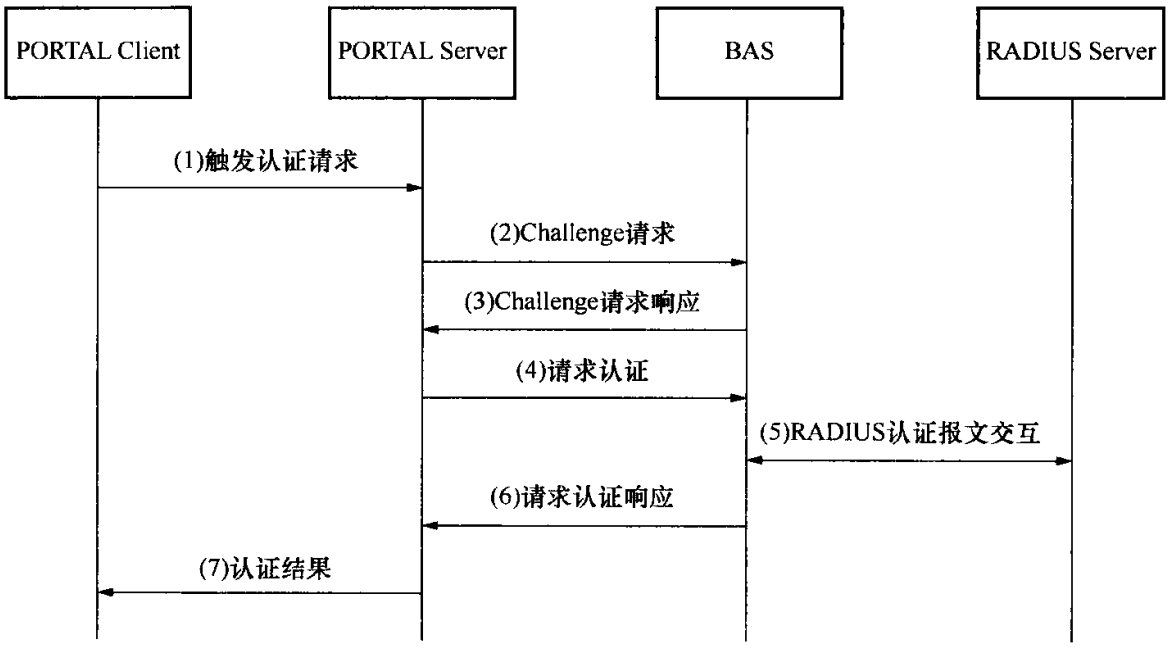


图 3-50 PORTAL 直接认证方式认证流程图

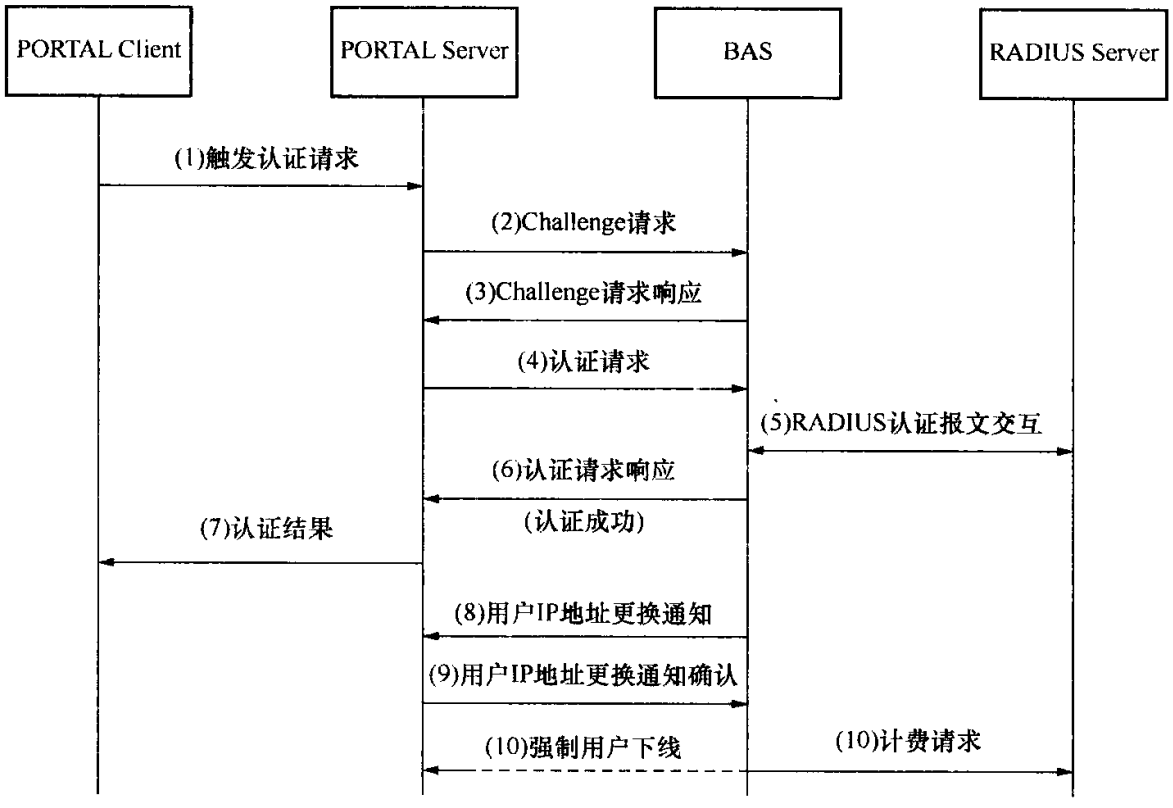


图 3-51 PORTAL 二次地址方式认证流程图

表 3-4　基于 H3C PORTAL/PORTAL＋的准入控制技术主要特点

NAC 体系	对应参数	备注
架构组成	认证客户端（PORTAL Client） ＋ PORTAL 服务器（PORTAL Server） ＋ BAS ＋ AAA 服务器	也能够支持无客户端模式，但在国内只有少数第三方 NAC 厂商能够支持
支持环境	H3C MSR 系列路由器 S5500 EI 及以上的交换机	
旁路部署	√	只传输控制流，完全旁路
无客户端支持	√	
交换机配置量	较少	只需要在网络干道上的网关或路由器上进行配置
接入层端口级控制	×	控制力度较弱，只能在网络出口上进行管理
Hub 接入控制	√	
http 快捷性	√	由于可以选择放通部分流量，因此能够兼容 DHCP 环境，可以进行 Web 重定向引导
系统资源（内存）占用	大	在第三方厂商的无客户端环境下占用较小
来宾管理	好	能够进行 Web 引导
稳定性	好	在无客户端环境下可以依赖交换机及服务器来确保稳定性
兼容性	×	只能运行在 H3C 自有环境或部分华为路由器环境
防单点故障	√	PORTAL 协议本身支持对 radius 服务器存活状态的监测，一旦发现宕机，交换机能够立即解除控制，放通网络

4. 配置方法

1）配置 RADIUS 方案

创建名字为 AmcScheme 的 RADIUS 方案并进入该方案视图

<Router> system-view

[Router] radius scheme AmcScheme

配置 RADIUS 方案的服务器类型为 extended

[Router-radius-AmcScheme] server-type extended

配置 RADIUS 方案的主认证服务器及其通信密钥

[Router-radius-AmcScheme] primary authentication 192.168.56.227

[Router-radius-AmcScheme] key authentication NAC _ key

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名

[Router-radius-AmcScheme] user-name-format without-domain

[Router-radius-AmcScheme] quit

2）配置认证域

创建并进入名字为 AmcDomain 的 ISP 域

[Router] domain AmcDomain

配置 ISP 域的 RADIUS 方案 AmcScheme

[Router-isp-AmcDomain] authentication portal radius-scheme AmcScheme

[Router-isp-AmcDomain] authorization portal radius-scheme AmcScheme

[Router-isp-AmcDomain] accounting portal none

[Router-isp-AmcDomain] quit

3）配置 全局 PORTAL 认证

配置 PORTAL 服务器：包括名称、IP 地址、密钥、端口、URL。

[Router] portal server AmcPORTAL IP 192.168.56.222 key msackey port 50100 url http：//192.168.56.4：8080

4）配置例外网段

对 56 网段不认证。

[Sysname] portal free-rule 15 source IP 192.168.56.0 mask 24 destination IP any

[Sysname] portal free-rule 15 source IP any destination IP 192.168.56.0 mask 24

5）开启指定接口 PORTAL 认证。

[Router] interface Vlan-interface 1

[Router-Vlan-interface1] portal server AmcPORTAL method layer3

[Router-Vlan-interface1] quit

6）关闭指定接口 PORTAL 认证

[Router] interface Vlan-interface 1

[Router-Vlan-interface1] undo portal

[Router-Vlan-interface1] quit

3.4 基于应用设备的网络准入控制架构

在 NAC 发展的历程中，由于 802.1x 架构在使用上的诸多不灵活性，从而引

发各厂商积极探索适合自身架构的快捷入网管理技术，但各厂商的封闭特性加之需要配合联动的组件过多（从上一章的阐述中看到，私有架构至少都有 4 个组件需要部署），导致 NAC 在发展到第二波浪潮的时候受到了各机构不同程度上的抵触，管理员维护工作量过大，系统稳定性不高，配置工作过于繁杂，技术要求过高，仿佛一瞬间所有的因素都在朝着不利于 NAC 的方向发展。

在这个背景下，简化配置、简化架构、简化维护量的呼声开始出现，基于应用设备的网络准入控制（Appliance-Based NAC）架构就是基于上述思路的第三代 NAC 架构体系，“One box，One day”是 Appliance-Based NAC 解决 Infrastructure-Based NAC 难用、复杂、庞大的理念和宣言。

3.4.1　Cisco 虚拟网关准入控制技术分析

大部分的网关型安全产品都能够或多或少地实现一些准入的功能，比如防火墙、比如流控，常见的方式是与网络中已有的 RADIUS 服务器进行联动，对所有需要穿越网关的数据进行身份验证，从而可以实现与 802.1x 类似的开/关效果。

但是，人们要认清的一点是，普通网关型设备的控制都是发生在终端已经接入内网后，试图向外进行互联网访问时所触发的，此时整个内网的安全状况完全没有得到有效的管理，因此又有人把这类的控制架构称作“准出”，以示区别于标准的 NAC“准入”。本章要介绍的是有别于传统网关型准入控制技术的另一种基于接入层交换机的架构——VG（Virtual Gateway，虚拟网关）准入架构。

VG 是 Appliance-based NAC 框架实现准入控制技术之一。VG 技术虽然是由 Cisco 提出的，但其技术实现原理可以适用于大部分的基础网络架构，在国内，已经有第三方的 NAC 制造商实现了这种准入技术架构，并扩展了 VG 的兼容性，在 5000 点左右的大规模内网中得到了应用。但其与交换网络环境依赖性太大、基于软件协议的准入强度不够、部署维护太复杂等的现实问题限制了此类 NAC 产品的成熟度与市场的推广。通过对 Cisco 自身 VG 原理的分析，能够帮助理解这种超越了 802.1x 的 2 层准入架构，并为理解下一节介绍的 MVG 技术打下基础。

1. 技术实现原理

VG 准入架构模型如图 3-52 所示。

图 3-52 中，CAS 和 CAM 都是 VG 架构中配套的 Cisco 管理设备。

在 VG 架构中，实现的关键是 VLAN 切换，但不同于 802.1x 中的 guest VLAN 切换，在 VG 架构中切换的隔离 VLAN 和管理服务器（CAS）是能够进行通信的，此时所有的报文都会通过 CAS 进行转发，相当于 CAS 成为了接入终端的网关；而在终端认证及安检通过后，将切换回原始的正常 VLAN，数据流量不经过 CAS，此时的 CAS 就成为了一台完全旁路的设备。

未认证前

图 3-52 VG 虚拟网关准入架构

由于 VG 架构中的管理服务器 CAS 会根据接入终端状态的不同进行或网关，或旁路的位置转换，因此被称为虚拟网关。

在上述的分析中我们看到，VG 的架构一定会存在两种 VLAN 类型，从认证前到认证后 VLAN ID 是会变化的：

① Authentication VLAN：当新主机接入到 switch 时，就会被先划入到 authentication vlan 里，此时主机的所有流量将被强制转发到 CAS，Client 的 authentication，assessment，remediation 都将在这个 VLAN 中进行。

② access VLAN：当主机完成 authentication 和 certification 后，主机将被划入到 access VLAN，进入这个 VLAN 后就和 NAC 没有关系了，流量不会再经过 CAS 了，直接转发走了。

管理服务器 CAS 的作用在于 CAS 有两个接口，一边是 untrust 的 VLAN (authentitaion VLAN)，另一边是 trust VLAN（access VLAN），有点类似于 firewall，untrust 到 trust 默认只允许 DHCP 和 DNS 过，其他都过不了。

2. 工作过程

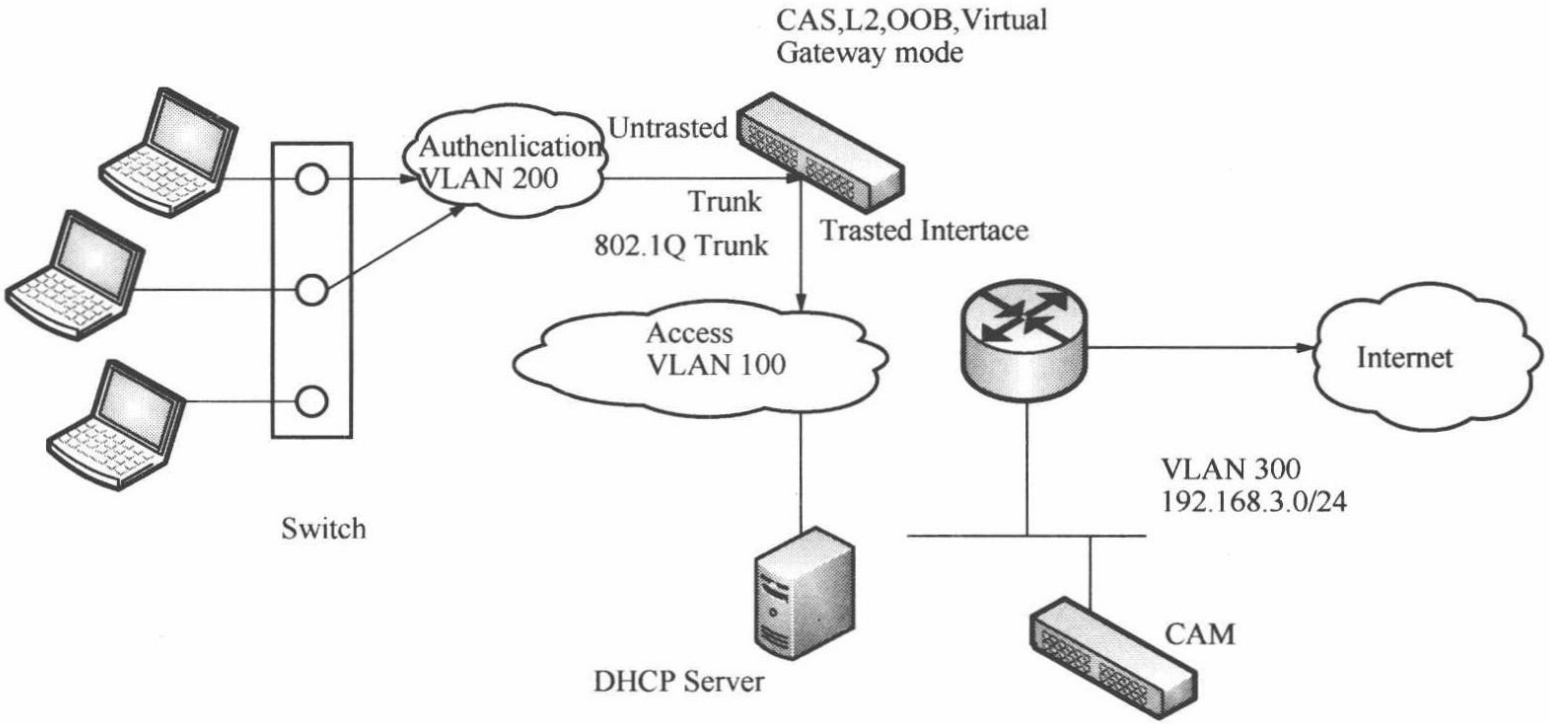
下面以一个实例来说明 VG 准入控制的工作过程，并两个 VLAN 为例进行分析。

authe vlan = VLAN 200

access vlan（normal vlan）= VLAN 100

整个的 VG 准入管理流程在底层的数据报流上不同于正常的数据传输过程，因此交互步骤远远多于 802.1x 架构，以下为具体的工作过程。

Step1：Client 接入 Switch 的 port 3/1 接口，Switch 会立即发送 linkup 和


CAS,L2,OOB,Virtual
Gateway mode
Authenlication
VLAN 200
Untrasted
Trunk
802.1Q Trunk
Trasted Intertace
Access
VLAN 100
Internet
VLAN 300
192.168.3.0/24
Switch
DHCP Server
CAM

未认证前

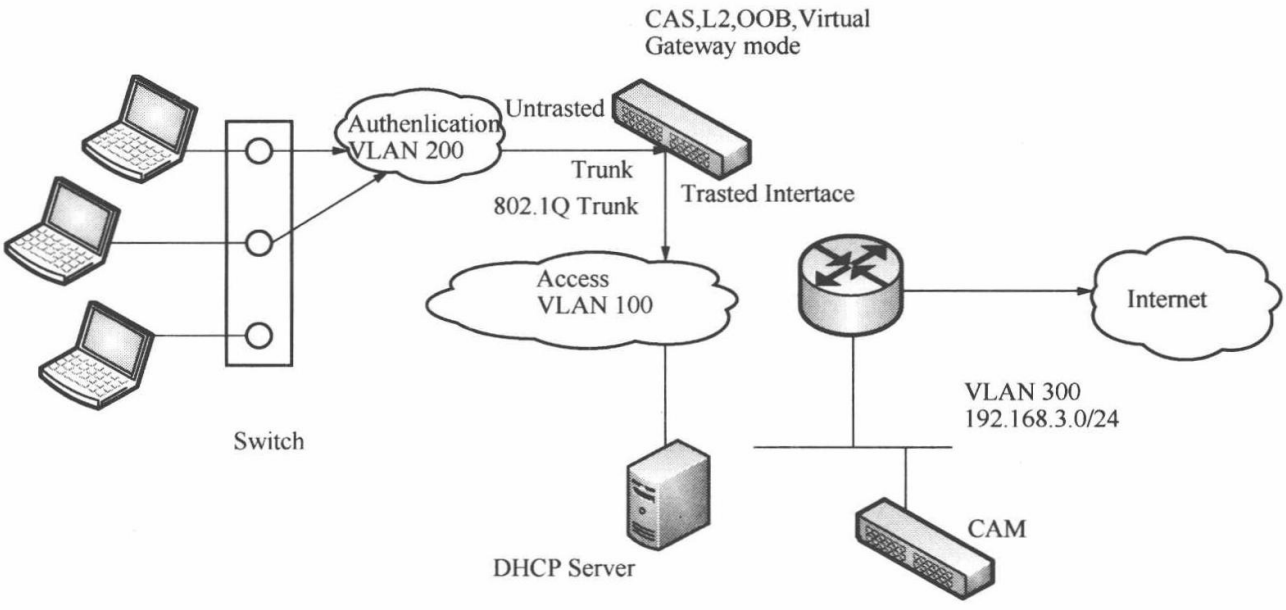


图 3-52 VG 虚拟网关准入架构

由于 VG 架构中的管理服务器 CAS 会根据接入终端状态的不同进行或网关，或旁路的位置转换，因此被称为虚拟网关。

在上述的分析中我们看到，VG 的架构一定会存在两种 VLAN 类型，从认证前到认证后 VLAN ID 是会变化的：

① Authentication VLAN：当新主机接入到 switch 时，就会被先划入到 authentication vlan 里，此时主机的所有流量将被强制转发到 CAS，Client 的 authentication，assessment，remediation 都将在这个 VLAN 中进行。

② access VLAN：当主机完成 authentication 和 certification 后，主机将被划入到 access VLAN，进入这个 VLAN 后就和 NAC 没有关系了，流量不会再经过 CAS 了，直接转发走了。

管理服务器 CAS 的作用在于 CAS 有两个接口，一边是 untrust 的 VLAN (authentitaion VLAN)，另一边是 trust VLAN (access VLAN)，有点类似于 firewall，untrust 到 trust 默认只允许 DHCP 和 DNS 过，其他都过不了。

2. 工作过程

下面以一个实例来说明 VG 准入控制的工作过程，并两个 VLAN 为例进行分析。

authe vlan = VLAN 200

access vlan (normal vlan) = VLAN 100

整个的 VG 准入管理流程在底层的数据报流上不同于正常的数据传输过程，因此交互步骤远远多于 802.1x 架构，以下为具体的工作过程。

Step1：Client 接入 Switch 的 port 3/1 接口，Switch 会立即发送 linkup 和

MAC-notification 的 SNMP trap 给 CAM，这个 trap 信息里包括 Client 的 MAC 地址和端口号（交换机是通过 SNMP 和 CAM 沟通的），trap 有三种：linkup，linkdown，MAC-notification。

Step2：在 CAM 检查看到了 trap 后，会检查 MAC 地址是否在 certified devices list 里有记录（就是说这个 MAC 地址之前已经登录过，然后再 logout 出去的），如果是 logout 出去的话，可以有以下 2 种操作（需要说明的是：certified devices list 里包含认证机器的 MAC 和 IP 地址，这些操作须在改 MAC 地址并在 certified devices list 里没超时之前有效）。

① 直接把端口划入到 VLAN 100 进入正常通信 VLAN，什么都不检查；

② 重新分配到 authe VLAN，但是此时仅仅是验证用户名和密码，不进行 posture 的检测，因为 Client 仍然在 certified list 里。

Step3：Client 的 MAC 不在认证列表里，则 CAM 会发送一个 SNMP write trap 给 Switch（这个 trap 的作用是更改交换机的端口到一个 auth VLAN），这个 SNMP write trap 告诉 Switch 划分 3/1 这个接口到 auth VLAN（VLAN 200），这个认证 VLAN 号是由 Switch 上的 port profile 决定的。

Step4：CAM 会添加这台设备的 MAC 地址进 out-of-band discovery client list，这里可以看到所有通过 MAC-notification 和 linkup 或者 Linkdown 发现的设备 Client，主要包含了 MAC 地址以及这个 MAC 是来自交换机上的那个端口（可以看到交换机发送的 2 中的 trap 信息）。

Step5：此时 Client 已经在 VLAN 200 里了，这个 VLAN 在 CAS 的 untrust 一边，此时 Client 的所有流量被强制发送到 CAS，CAS 可以被配置为仅允许认证流量通过到 trust 一边，CAS 默认不会让任何流量过的，但是有 2 种流量可以过：DHCP 和 DNS，这些流量可以定义的，定义哪些流量第一次可以穿越 CAS（建议允许用户先登录域）。

Step6：在 DHCP 环境下，Client 可以通过 CAS 向 DHCP Server 申请一个地址，具体的步骤是：Client 发送 DHCP request 给 CAS，CAS 看到这个 request 来自 VLAN200 的 untrust 接口，然后 CAS 会对这个 request 进行 retag VLAN ID。这里就是会把 request 信息里的 VLAN 200 的 tag 改成 VLAN 100，并转发到 trust 接口，然后这个 DHCP Request 消息会继续发向 DHCP Server。这个 VLAN retag 的配置是在 CAM 上的 VLAN mapping table 里配置的。

当 DHCP Server 收到来自 VLAN 100 的 request 后，它会回应 Client 一个 VLAN 100 里的 IP 地址，CAS 从 trust 接口收到 DHCP Reply 后，它还是会 Retag DHCP Reply 里的 tag，把 VLAN 100 改成 VLAN 200，然后再转发 DHCP Reply 给 Client。此时 Client 已经在 VLAN 200 里获得了一个 IP 地址，但其实这个地址是属于 VLAN 100 里的地址。

当 Client 获得 IP 地址的时候，同时 CAM 已经为这个 Client 分配了一个 unauthentication role，默认这种 role 的 Client 还是不允许任何流量过，除了 DHCP

和 DNS。

Step7：当 Client 有了地址，则开始发送对外的数据包，此时 CAS 将收到该数据包，由于该 Client 没有经过认证和安检，则 CAS 会返回一个重定向提示，引导接入终端进入 CAS 的认证和安检 Web 页面。

Step8：如果 Client 通过验证，会被分配到 normal role 里，用户 pass 后，CAM 根据接入终端的源 MAC 地址和之前 MAC-notification 里的 MAC 地址做比对，然后可以根据 MAC 找到相应的 Switch 端口号，那么 CAM 会再次发送 SNMP write trap 给 CAS，然后 CAS 给 Switch，将端口划到 VLAN 100 里，这时候用户地址不用改变，就可以正常通信了（这里的 access VLAN ID 也是在 Switch 的 port profile 里定义的）。

因此，在主机正常入网后，最后实际的流量是不经过 CAS 的。

还有另外一种情况，如果主机的认证或检测没有通过时。即

Step9：如果检测失败，CAM 会命令 CAS 回送给用户一个 remediation（补救）对话框，去下载一些补丁，CAM 会分配给用户从一个 authentication role 转换到 temporary role，在这里，仅允许补救流量通过 CAS，CAS 会 retag 这些流量的 VLAN ID，在用户打上这些补丁后，主机需要重新被检测，检测通过后，才被允许访问内网。

3. 主要特点

VG 准入控制技术最重要的特点是具有 Cisco 自身的厂商属性，基本上需要依靠 Cisco 环境（如 Cisco 2950）来搭建整个架构。其主要特点如表 3-5 所示。

表 3-5 VG 准入控制技术主要特点

NAC 体系	对应参数	备注
架构组成	CAA（Cisco Access Agent） + Cisco Switch + CAS/CAM	VG 支持无客户端模式
支持环境	Cisco 2 层交换机	Cisco 2950 以上
旁路部署	视接入终端状态	在终端通过检测后完全旁路
无客户端支持	√	
交换机配置量	一般	所有接入层交换机均进行配置
接入层端口级控制	√	
Hub 接入控制	√	
http 快捷性	√	由于可以选择放通部分流量，因此能够兼容 DHCP 环境，可以进行 Web 重定向引导

续表

NAC 体系	对应参数	备注
系统资源（内存）占用	小	无客户端的优势在这里体现出来了
来宾管理	好	能够进行 Web 引导，因此十分友好
稳定性	好	不依赖客户端，交换机及服务器能够确保稳定性
兼容性	×	基本只能运行在 Cisco 自有环境
防单点故障	√	终端正常认证后，CAS 是旁路模式，不影响流量； 但如果在终端认证过程中 CAS 宕机，则有可能引发无法入网

4. 配置方法

下面以一个实际环境为例，进一步介绍 VG 的配置步骤和命令。

1）网络环境

某网络目前采用二层架构进行组网，核心为一台 Cisco 的 4507 交换机，终端电脑通过 4 台 Cisco 的 2960 接入交换机进行互连。内部服务器直接与核心交换机相连提供全网的业务访问。拓扑结构如图 3-53 所示。

2）准入组网

准入控制设备使用 2 个网口（纯 2 层，不配置 IP 地址）与核心 4507 交换机的 2 个 Trunk 口相连，另外 1 个网卡作为管理口，配置一个全网可达的 IP 地址。设备连线示意图如图 3-54 所示。

3）接入交换机配置

从图 3-53 中可以看出，在此网络中共有 4 台 2960 接入交换机，其具体配置步骤如下：

Step1：创建认证前 VLAN。

```
Cisco-2960 >enable
Cisco-2960 #Configure t
Cisco-2960 (config) #vlan 50
```

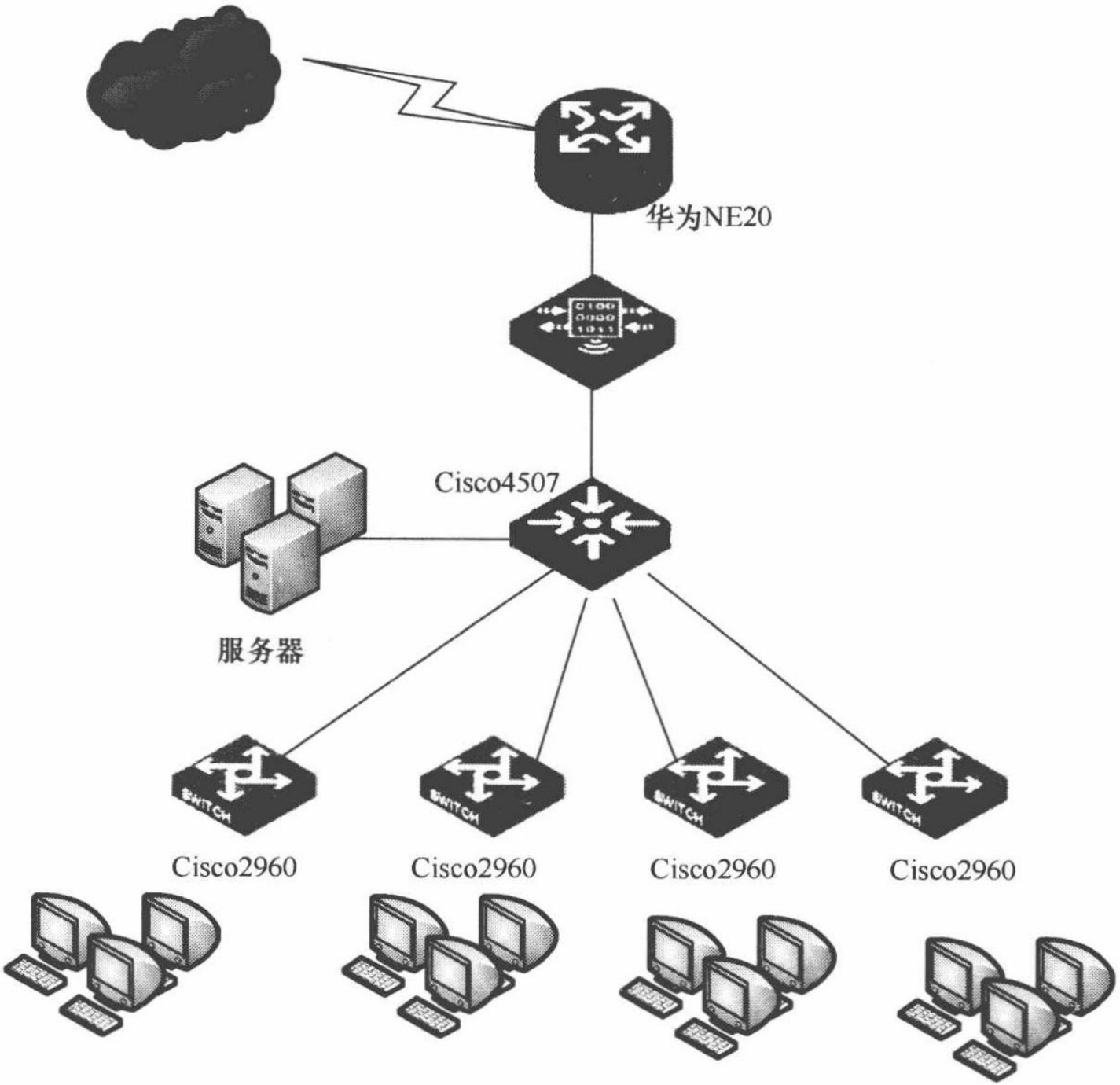
Step2：配置 snmp-server。

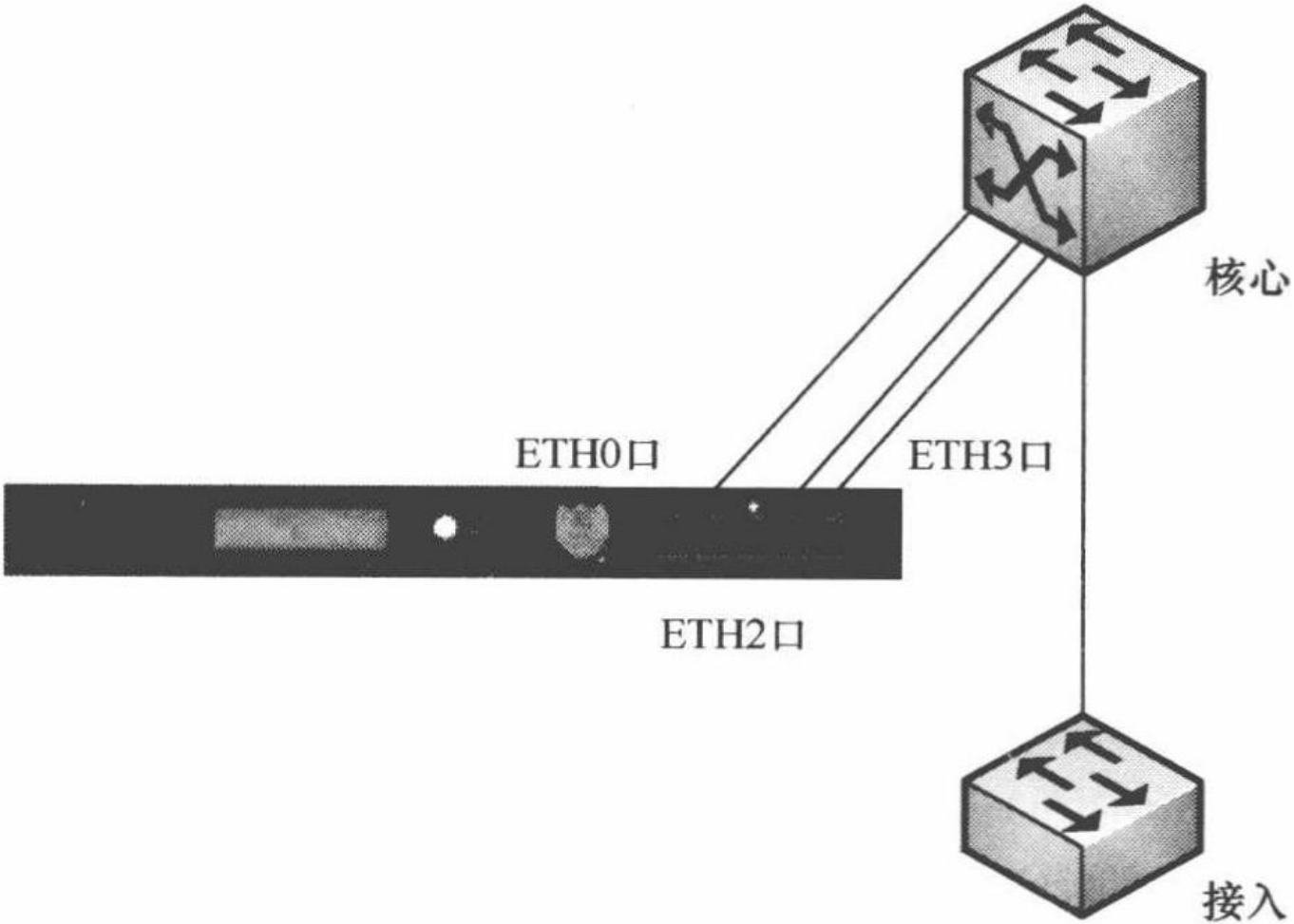
```
Cisco-2960 >enable
Cisco-2960 #Configure t
//配置用于通过 SNMP 查询交换机信息的共同体
Cisco-2960 (config) #snmp-server community NAC Appliancepublic ro
//配置用于通过 snmp 设置交机信息的共同体
```

图 3-53 某二层架构网络拓扑图

图 3-54 设备连接示意图

```
Cisco-2960（config）＃snmp-server community NAC Applianceprivate rw
//启用 linkdown trap
Cisco-2960（config）＃snmp-server enable traps snmp linkdown
//启用 MAC address 通知 Trap
```


华为NE20
Cisco4507
服务器
Cisco2960
Cisco2960
Cisco2960
Cisco2960


核心
ETH0口
ETH3口
ETH2口
接入

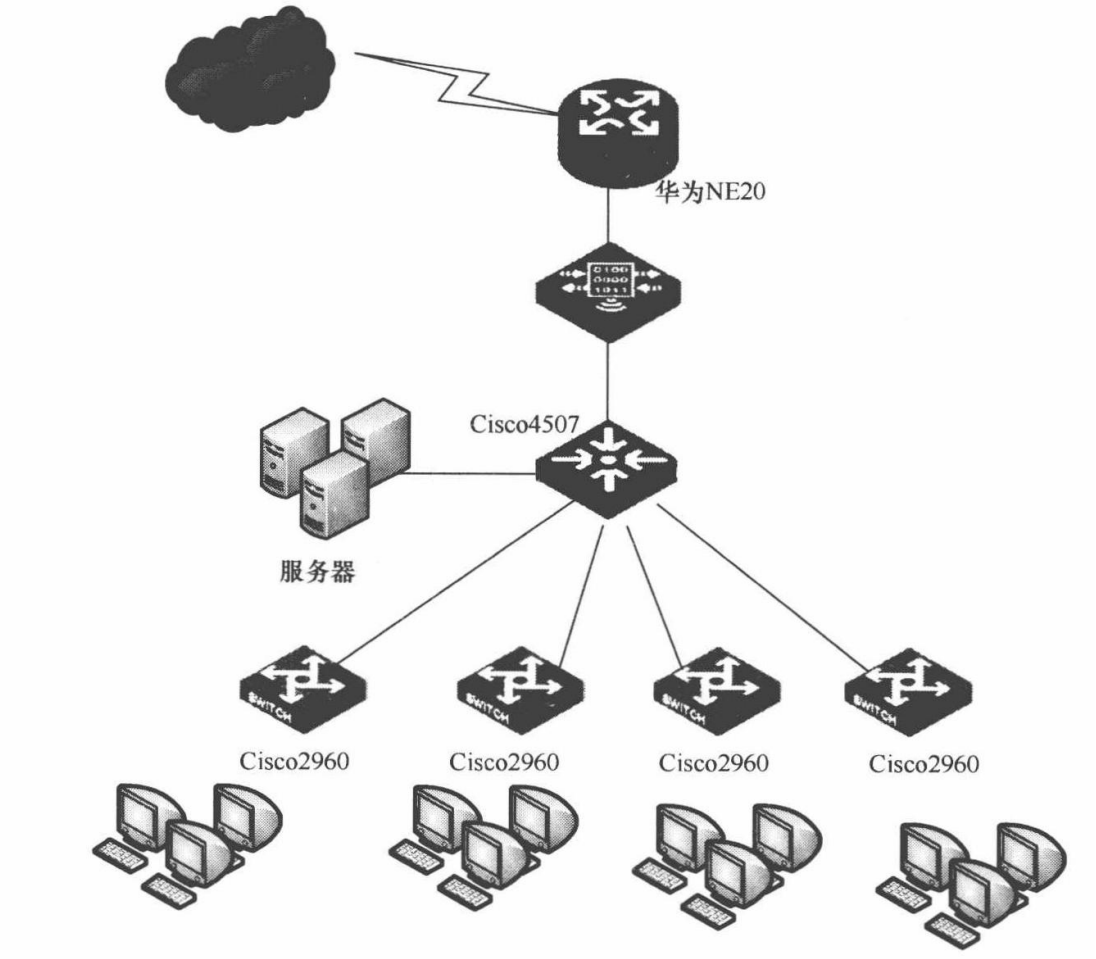


图 3-53 某二层架构网络拓扑图

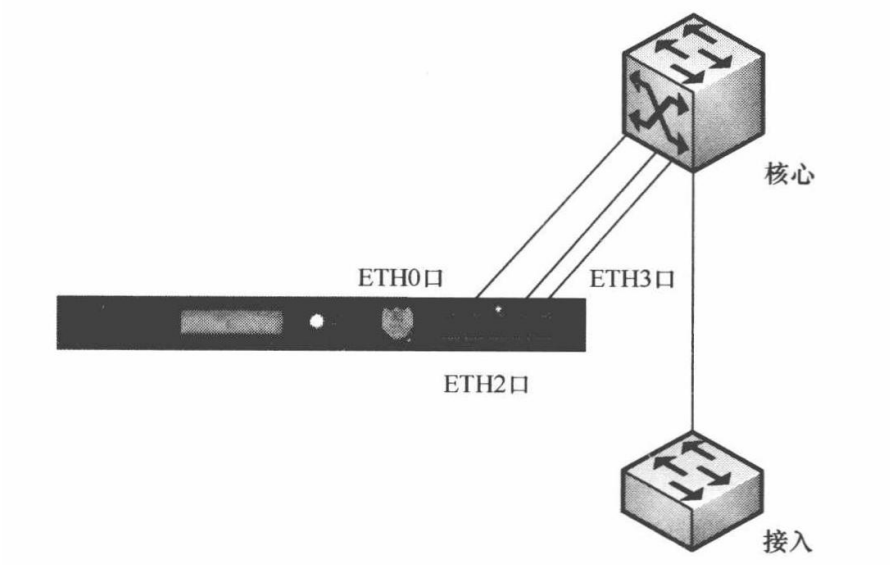


图 3-54 设备连接示意图

Cisco-2960（config）#snmp-server community NAC Applianceprivate rw

//启用 linkdown trap

Cisco-2960（config）#snmp-server enable traps snmp linkdown

//启用 MAC address 通知 Trap

Cisco-2960（config）＃snmp-server enable traps mac-notification

//指定将 Trap 报文发给 CAS（203.155.176.232）

Cisco-2960（config）＃snmp-server host 203.155.176.232 version 2c NAC Appliancetrap

Cisco-2960（config）＃mac address-table notification

在顺利完成上述步骤后，可登录 CAS 管理平台，进行相关参数设置。

3.4.2 Infogo Multi-VG 准入控制技术分析

上一节提及过 Cisco 自有的 VG 准入架构，但是由于其偏向于 Cisco 自身的交换设备体系，因此影响了其普及和运用。国内的第三方准入厂商敏锐地察觉到了这一点，并研发出了更适应大众交换环境的多厂商 VG（Multi-VG，MVG）架构，在沿袭了 VG 架构控制和灵活性原有优势的情况下，MVG 扩展了其网络兼容性，从而达到了一种较为完美的 NAC 平衡。

MVG 在 2011 年的 NAC 准入市场中异军突起，在大规模网络中得到了广泛的运用，也成为了 Appliance-Based NAC 体系中的首选技术。目前 VG 虚拟网关的应用比较少，只是在国外很多独立的 NAC 产商在应用与实践（如 Bradford networks、Forescout），国内的有 Infogo 盈高科技公司。主要由于采用 SNMP 或 CLI 方式等方式，目前在国内还不是很被认可，但从实践经验看这种技术已经被市场所肯定的，技术上是确实可行的。可以兼容国内外主流的网络交换设备厂商，像 Cisco、Juniper、北电、华为、H3C、锐捷、迈普、中兴、神码，等等。随着各种网络环境的不一样，可以实现对无线网络环境以及 Lay3 层的 VG 准入技术的实现。

1. 技术实现原理

在介绍 MVG 的技术原理之前，首先介绍两个关键概念：VLAN 和 NP。

1）VLAN

VLAN 是英文 Virtual Local Area Network 的缩写，中文名为“虚拟局域网”，VLAN 是一种将局域网（LAN）设备从逻辑上划分成一个个网段（或者子网），从而实现虚拟工作组（单元）的数据交换技术。

VLAN 技术的出现，使得管理员根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

正是由于 VLAN 的隔离广播特性，使得不同 VLAN 之间如果要进行访问则必须进行三层的路由，这个在各个 VLAN 具有不同子网的时候可以正常通信。但是当出现两个 VLAN 具有相同子网的时候，由于子网相同，这个时候将不会

进行 3 层的路由，进而导致无法进行通信。

下面举例一个实际的例子进行说明。在网络准入控制技术中，802.1x 是一个非常普遍和安全的技术。802.1x 进行认证的时候为了方便终端设备的使用，提供了来宾访问的 guest-VLAN 功能，对于无法进行认证的终端设备可以进行接入端口 VLAN 的切换，这个对于动态地址（DHCP）环境可以很好地工作，但是对于静态地址环境则会存在问题，具体的流程如下：

假设接入交换机的一个接入端口属于 VLAN 2，该 VLAN 的子网为 192.168.54.0/24，子网网关为 192.168.54.1。进行来宾认证时候的 guest-VLAN 为 VLAN 110，该 VLAN 的子网为 192.168.110.0/24，子网网关为 192.168.110.1。现在一台 IP 地址固定为 192.168.54.57 的终端电脑接入到该端口，由于该终端电脑不能成功进行 802.1x 的认证，认证服务器根据 802.1x 的认证要求将：

Tunnel-Medium-Type = IEEE-802

Tunnel-Pvt-Group-ID = 110

Tunnel-Type = VLAN

属性发送给交换机，通知交换机进行来宾 VLAN 切换，使得交换机端口切换到 VLAN 110。按照 802.1x 当初的设计，这个时候终端电脑应该通过 DHCP 方式获取到 100 网段的地址，进而进行网络的通信。但是在这个案例中，由于终端电脑已经配置了静态的地址，导致终端电脑不会获取新的地址而继续使用原有地址。这个时候终端电脑和其他设备进行通信时候由于其子网和 VLAN 的子网不一致导致网络无法访问。

另外，对于通用的 CPU 来说，由于企业的网络带宽极具增大普通的软件解决方案或者 X86 解决方案已经无法满足带宽的要求，盈高科技公司按照集成电路中 NP 设计的思想，设计出了高性能的硬件处理模块来提高路由的处理速度。

2）NP

NP 即网络处理器，是专门为处理数据包而设计的可编程处理器，能够直接完成网络数据处理的一般性任务。硬件体系结构大多采用高速的接口技术和总线规范，具有较高的 I/O 能力，包处理能力得到了很大提升。网络处理器一般具有以下特点。

（1）并行处理器。采用多内核并行处理器结构。片内处理器按任务大致分为核心处理器和转发引擎。

（2）专用硬件协处理器。对要求高速处理的通用功能模块采用专用硬件实现以提高系统性能。

（3）专用指令集。转发引擎通常采用专用的精简指令集，并针对网络协议处理特点优化。

（4）分级存储器组织。NP 存储器一般包含多种不同性能的存储结构，对数据进行分类存储以适应不同的应用目的。

（5）高速 I/O 接口。NP 具有丰富的高速 I/O 接口，包括物理链路接口、交换接口、存储器接口、PCI 总线接口等。通过内部高速总线连接在一起，提供很强的硬件并行处理能力。

（6）可扩展性。多个 NP 之间还可以互连，构成网络处理器簇，以支持更为大型高速的网络处理。

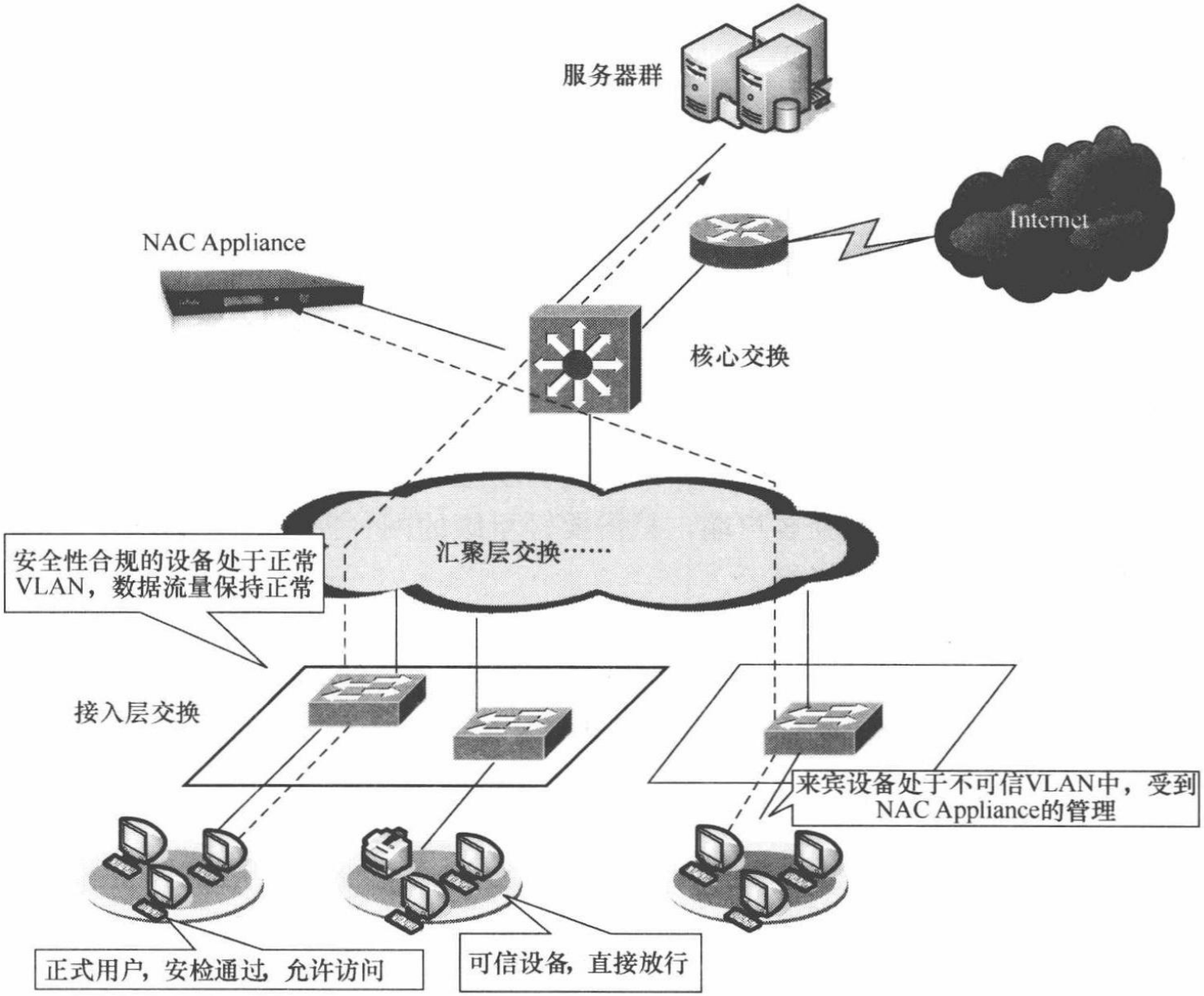
MVG 的技术原理图如图 3-55 所示，在基于 MVG 架构的准入控制平台下，准入控制设备采用旁路方式连接核心交换机，整体准入技术的关键是 VLAN 切换，以下为其基本原理描述。

图 3-55　MVG 技术原理示意图

在每个接入层交换机上将构建准入控制的 VLAN 对，每个 VLAN 对中，一个是网络中原有的正常 VLAN，被称为可信 VLAN；另一个是在准入部署中新增加的 VLAN，这是针对来宾设备或违规设备的 VLAN，被称为不可信 VLAN。

在 MVG 体系中，整个的数据流程基本遵循了 VG 架构的优势，但为了更好地支持 Cisco 外的交换机，故而扩展了原 SNMP 的控制方案，加以兼容 cli 命令行方式的控制，这样就能够实现左右逢源，并给了终端用户更为灵活的选择。

在 cli 方式下，利用高性能的网络处理器模块，MVG 能够更轻松地控制所有


服务器群
Internet
NAC Appliance
核心交换
汇聚层交换……
安全性合规的设备处于正常VLAN，数据流量保持正常
接入层交换
来宾设备处于不可信VLAN中，受到NAC Appliance的管理
正式用户，安检通过，允许访问
可信设备，直接放行

（5）高速 I/O 接口。NP 具有丰富的高速 I/O 接口，包括物理链路接口、交换接口、存储器接口、PCI 总线接口等。通过内部高速总线连接在一起，提供很强的硬件并行处理能力。

（6）可扩展性。多个 NP 之间还可以互连，构成网络处理器簇，以支持更为大型高速的网络处理。

MVG 的技术原理图如图 3-55 所示，在基于 MVG 架构的准入控制平台下，准入控制设备采用旁路方式连接核心交换机，整体准入技术的关键是 VLAN 切换，以下为其基本原理描述。

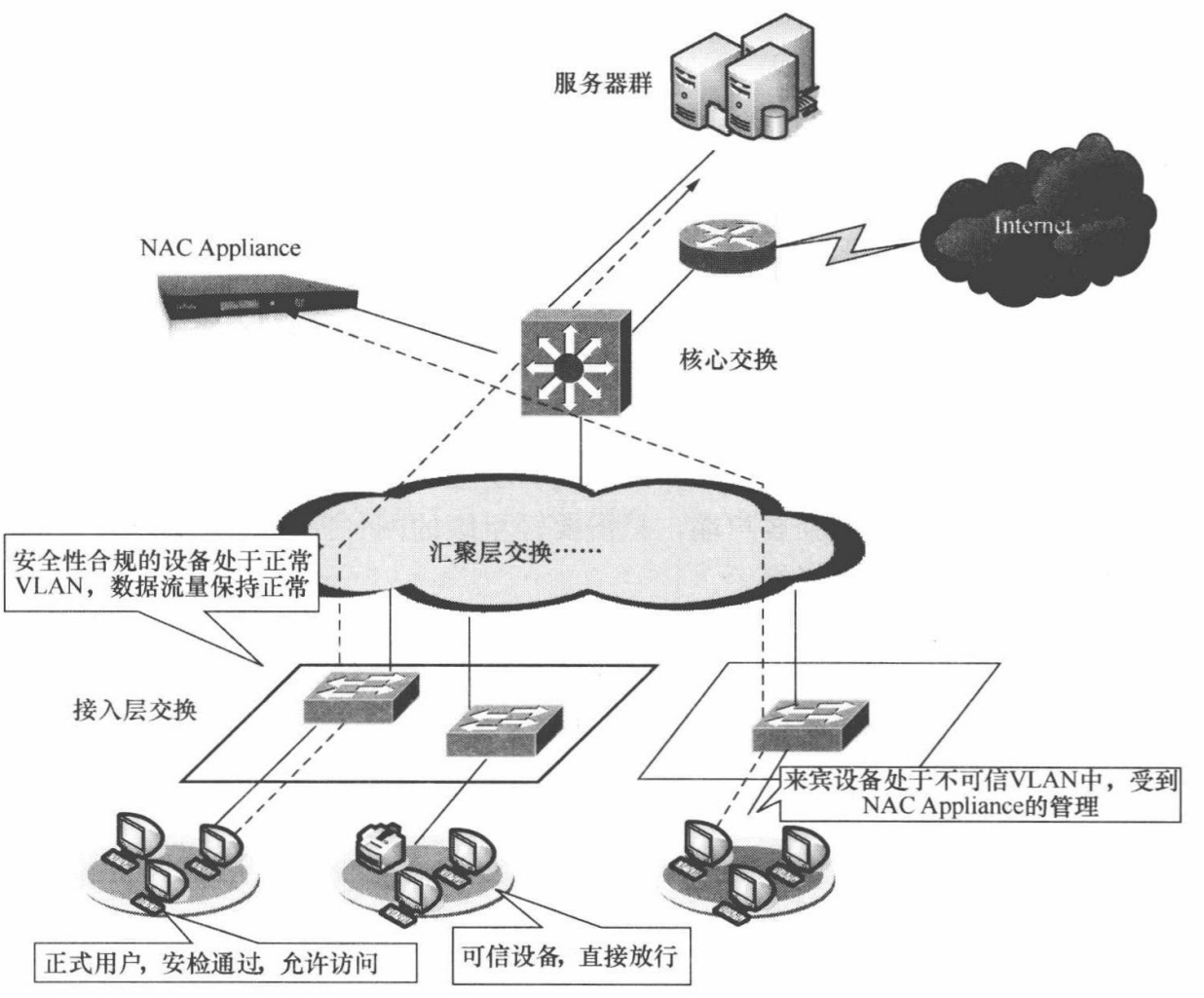


图 3-55　MVG 技术原理示意图

在每个接入层交换机上将构建准入控制的 VLAN 对，每个 VLAN 对中，一个是网络中原有的正常 VLAN，被称为可信 VLAN；另一个是在准入部署中新增加的 VLAN，这是针对来宾设备或违规设备的 VLAN，被称为不可信 VLAN。

在 MVG 体系中，整个的数据流程基本遵循了 VG 架构的优势，但为了更好地支持 Cisco 外的交换机，故而扩展了原 SNMP 的控制方案，加以兼容 cli 命令行方式的控制，这样就能够实现左右逢源，并给了终端用户更为灵活的选择。

在 cli 方式下，利用高性能的网络处理器模块，MVG 能够更轻松地控制所有

可网管的交换设备，通过命令方式的 VLAN 切换来实现原有 VG 架构下 SNMP 的工作，实现 VLAN 之间的互相访问控制，这在国内众多不规范网络或陈旧网络中不啻是一剂良药。

2. 工作过程

通过一个实例来说明 MVG 准入控制的工作过程，假定某接入层交换机某端口的原有正常 VLAN 为 VLAN 3，对应的不可信 VLAN 为 VLAN 300，则新设备入网流程如下：

Step1：设备插上网线后，MCG 设备能够及时从可网管交换机上探测到设备的 MAC 地址与所属端口号。

Step2：NAC Appliance 查询相应信息，如果发现是新设备，则通知交换机切换端口到隔离 VLAN 300，此时入网设备无法获得网络中的任何资源。

进入隔离 VLAN（VLAN 300）的设备所有数据流量都只能经过 NAC Appliance。

Step3：设备在通过管理员审核并检查合规后将切换回正常的工作 VLAN（VLAN 2），从而得以正常访问内部资源；未知设备、不合规设备、未通过审核设备均将停留在不可信 VLAN（VLAN 300）中，只有受限的访问权限（如只能访问隔离修复区服务器）。

由于 MVG 技术不需要接入计算机发送驱动层的认证数据包，因此可以不需要在接入计算机上安装常驻客户端，只需要轻量级的网页控件即可实现设备的身份认证、安全检查及隔离修复。

3. 主要特点

MVG 网络准入控制技术主要特点如表 3-6 所示。

表 3-6 MVG 网络准入控制技术主要特点

NAC 体系	对应参数	备注
架构组成	Agent（可选） + Switch + NAC Appliance	客户端模式是可选的，如果用户需要较完善的安全检查和控制功能，可以加装客户端或控件
支持环境	可网管交换机	
旁路部署	视接入终端状态	在终端通过检测后完全旁路
无客户端支持	√	
交换机配置量	小	网络内只需要配置与正常 VLAN 相对应的隔离 VLAN 号即可
接入层端口级控制	√	

续表

NAC 体系	对应参数	备注
Hub 接入控制	√	
http 快捷性	√	由于可以选择放通部分流量，因此能够兼容 DHCP 环境，可以进行 Web 重定向引导
系统资源（内存）占用	小	无客户端的优势在这里体现出来了
来宾管理	好	能够进行 Web 引导，因此十分友好
稳定性	好	不依赖客户端，交换机及服务器能够确保稳定性
兼容性	好	去品牌化，兼容所有可网管交换机
防单点故障	√	终端正常认证后，NAC Appliance 是旁路模式，不影响流量； 但如果在终端认证过程中 NAC Appliance 宕机，则有可能引发无法入网

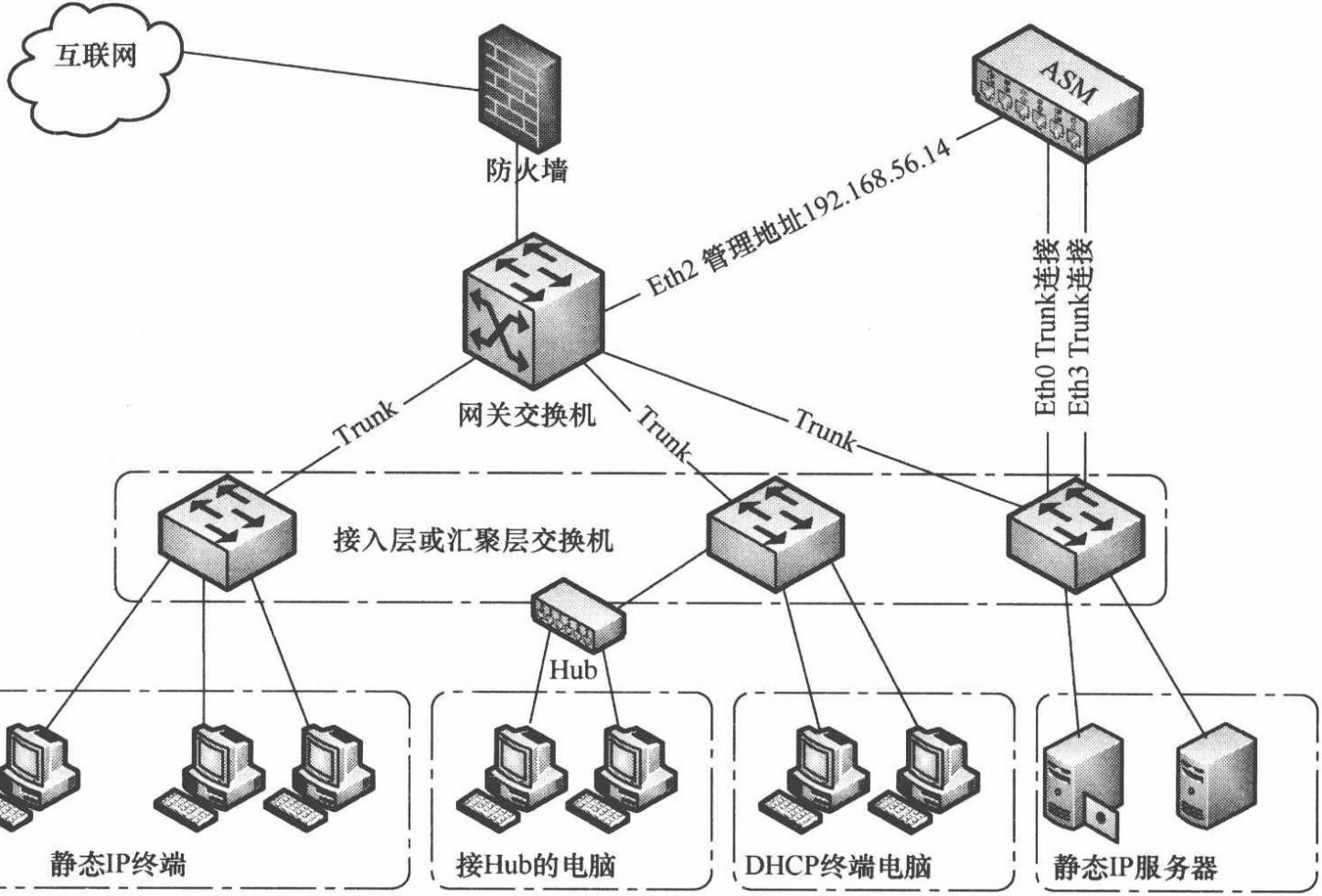
4. 配置方法

下面以一个实际环境为例，对 MVG 的配置步骤和命令进行简单说明。

1）网络连接拓扑

某网络采用静态 IP 地址和二层架构进行组网，一台 Cisco 交换机作为网关交换，终端电脑通过两台 Cisco 接入交换机进行互连。内部服务器通过一台 Cisco 接入交换机直接与核心交换机相连提供全网的业务访问。拓扑结构如图 3-56 所示。

图 3-56　某静态地址网络拓扑结构


互联网
防火墙
ASM
Eth2 管理地址192.168.56.14
Eth0 Trunk连接
Eth3 Trunk连接
网关交换机
Trunk
Trunk
Trunk
接入层或汇聚层交换机
Hub
静态IP终端
接Hub的电脑
DHCP终端电脑
静态IP服务器

续表

NAC 体系	对应参数	备注
Hub 接入控制	√	
http 快捷性	√	由于可以选择放通部分流量，因此能够兼容 DHCP 环境，可以进行 Web 重定向引导
系统资源（内存）占用	小	无客户端的优势在这里体现出来了
来宾管理	好	能够进行 Web 引导，因此十分友好
稳定性	好	不依赖客户端，交换机及服务器能够确保稳定性
兼容性	好	去品牌化，兼容所有可网管交换机
防单点故障	√	终端正常认证后，NAC Appliance 是旁路模式，不影响流量； 但如果在终端认证过程中 NAC Appliance 宕机，则有可能引发无法入网

4. 配置方法

下面以一个实际环境为例，对 MVG 的配置步骤和命令进行简单说明。

1）网络连接拓扑

某网络采用静态 IP 地址和二层架构进行组网，一台 Cisco 交换机作为网关交换，终端电脑通过两台 Cisco 接入交换机进行互连。内部服务器通过一台 Cisco 接入交换机直接与核心交换机相连提供全网的业务访问。拓扑结构如图 3-56 所示。

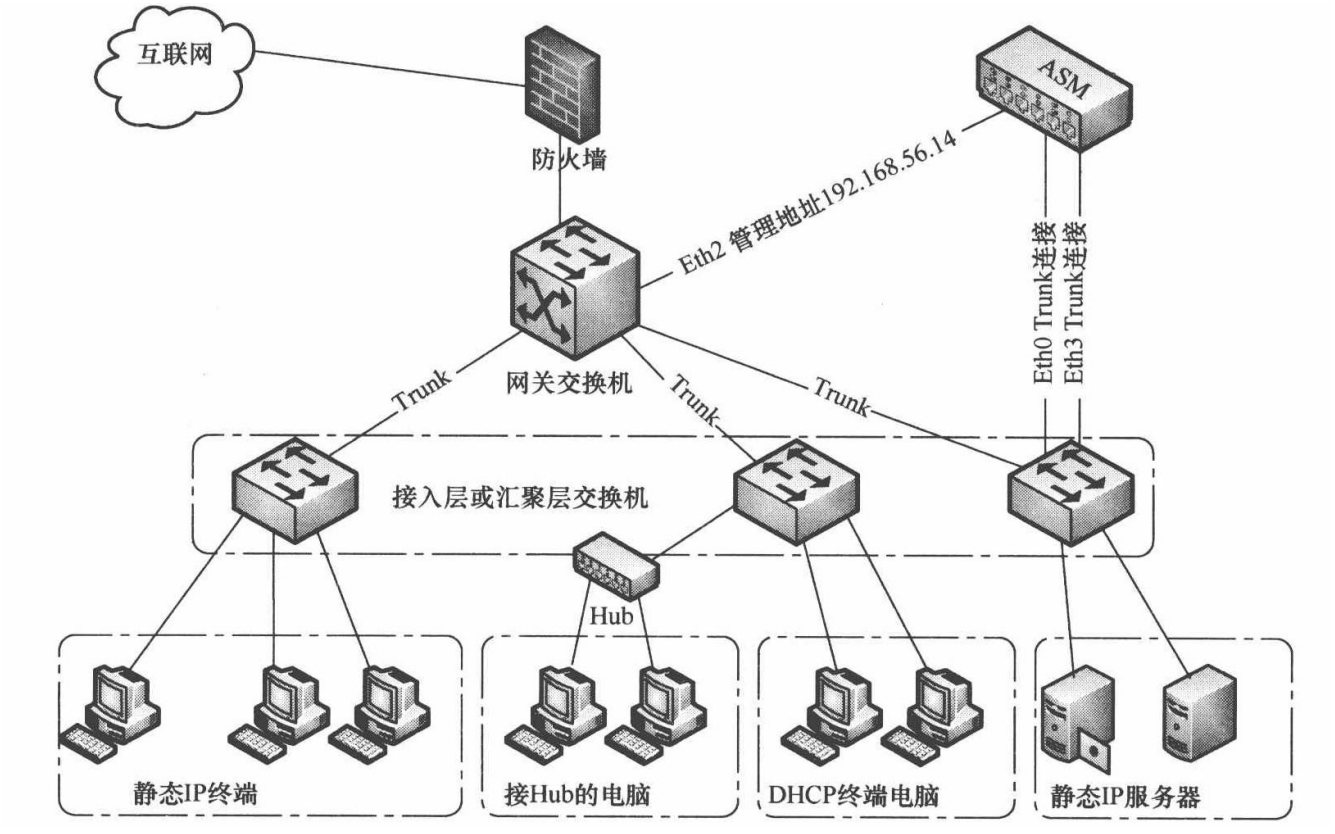


图 3-56　某静态地址网络拓扑结构

2）虚拟网关的配置方法

以图 3-56 所示 Cisco 交换机为例。

Step1：将与 MVG 准入控制设备相连的交换机端口配置为 Trunk 模式：

Switch（config-if）＃switchport mode trunk

Step2：在交换机上为每个 VLAN 建立一个对应的隔离 VLAN（此 VLAN 无需进行其他操作），如 VLAN10 对应 VLAN 100，配置命令为：

Switch（config）＃vlan 100

Step3：所有 VLAN10 中的终端接入网络时，MVG 准入控制设备会将交换机端口切换到 VLAN100，此时只能和 MVG 准入控制设备（和例外服务器）。

由于 MVG 技术只需要在交换机上添加与正常 VLAN 所对应的隔离 VLAN 号，因此 MVG 准入控制设备的配置方法不在此赘述。

3.4.3 策略路由网络准入控制技术分析

在多种旁路技术之后，将进入 NAC 的另一个领域——在线型（in-line）准入控制技术。

对于旁路型准入控制技术来说，核心因素在于控制流的处理，包括 Client—Switch 的控制交互、Switch—NAC Appliance 的控制交互，大部分的旁路准入架构都能够控制到接入层，但是这也带来了一个问题，就是在网络规模较大的情况下，由于接入层交换机数量较多而带来的部署困难和维护压力，另一个问题是：人们真的需要把准入控制推进到网络的最边缘吗？在线型准入控制技术给网络管理者提供了另一个选择，能够在保证部署和维护工作量较小的情况下，也实现另一个层面的准入，那就是对重点区域的保护。而基于策略路由的网络准入控制技术正是这样一种在线型的准入控制技术。

策略路由（PBR）准入技术是一种半在线型的准入控制技术，如图 3-57 所示。通过控制上行流量，能够做到既保证对网络影响较小，同时实现旁路部署和较高强度准入控制的双重平衡，另外由于其协议的特性还能够做到单机逃生，部署工作量也远远小于旁路式准入架构，因此受到了许多用户的青睐。在许多大型网络中都能够看到策略路由准入技术的身影，当然，前提是核心交换机能够支持策略路由的配置。

1. 技术实现原理

策略路由（Policy Based Route，PBR）位于 IP 层，在做 IP 转发前，如果报文命中某个策略路由对应的规则，则要进行相应的策略路由的动作（重定向到指定下一跳），然后根据重定向的下一跳代替报文的目的 IP 去查 FIB 表（转发信息表），做 IP 转发技术。

基于策略路由 PBR 的准入方案是通过在核心交换机上利用 ACL 捕获所有访问核心业务服务器的数据流量，并通过策略路由将捕获的流量发 NAC Appli-

图 3-57　策略路由准入控制技术示意图

ance，这样就由 NAC Appliance 控制了所有访问核心区域的数据流量，从而达到保护核心资源，对入网访问终端进行准入控制的安全目标。

PBR 在使用中有以下 3 个好处：

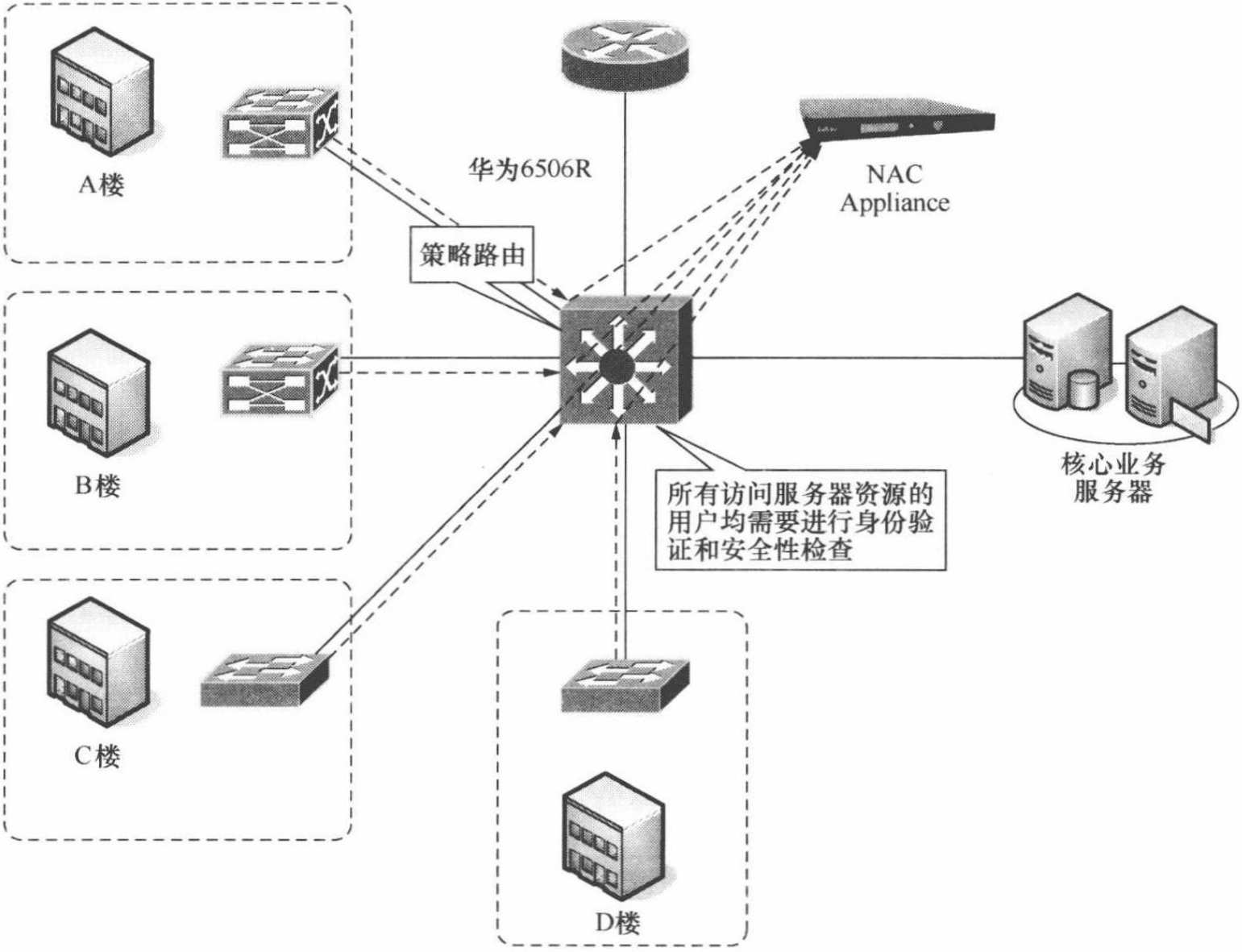
① 能够通过 ACL 来灵活的控制哪些终端是需要受管理，哪些终端是可以例外的。

② 只管理上行流量，只要终端通过了验证和安检，则下行流量可以走正常的路径，由于上行流量的数据大小一般远远小于下行流量，从而较好地解决了在线型架构影响正常访问速度的问题。

③ 在部署阶段，PBR 架构是物理旁路部署，因此不会改动网络的拓扑结构，同时也更方便小范围的测试。

2. 工作过程

在策略路由准入架构下，能够基于网关将跨网段访问的数据流量发送至已经配置好的下一跳地址，这个地址一般是 NAC Appliance 的管理口。因此被管控计算机的所有上行流量都将经过 NAC Appliance 并接收安全准入管理，计算机顺利入网后，其上行数据路由为：核心网关→NAC Appliance→核心→目标资源。其工作过程如图 3-58 所示。


A楼
B楼
C楼
D楼
华为6506R
NAC
Appliance
策略路由
核心业务
服务器
所有访问服务器资源的
用户均需要进行身份验
证和安全性检查

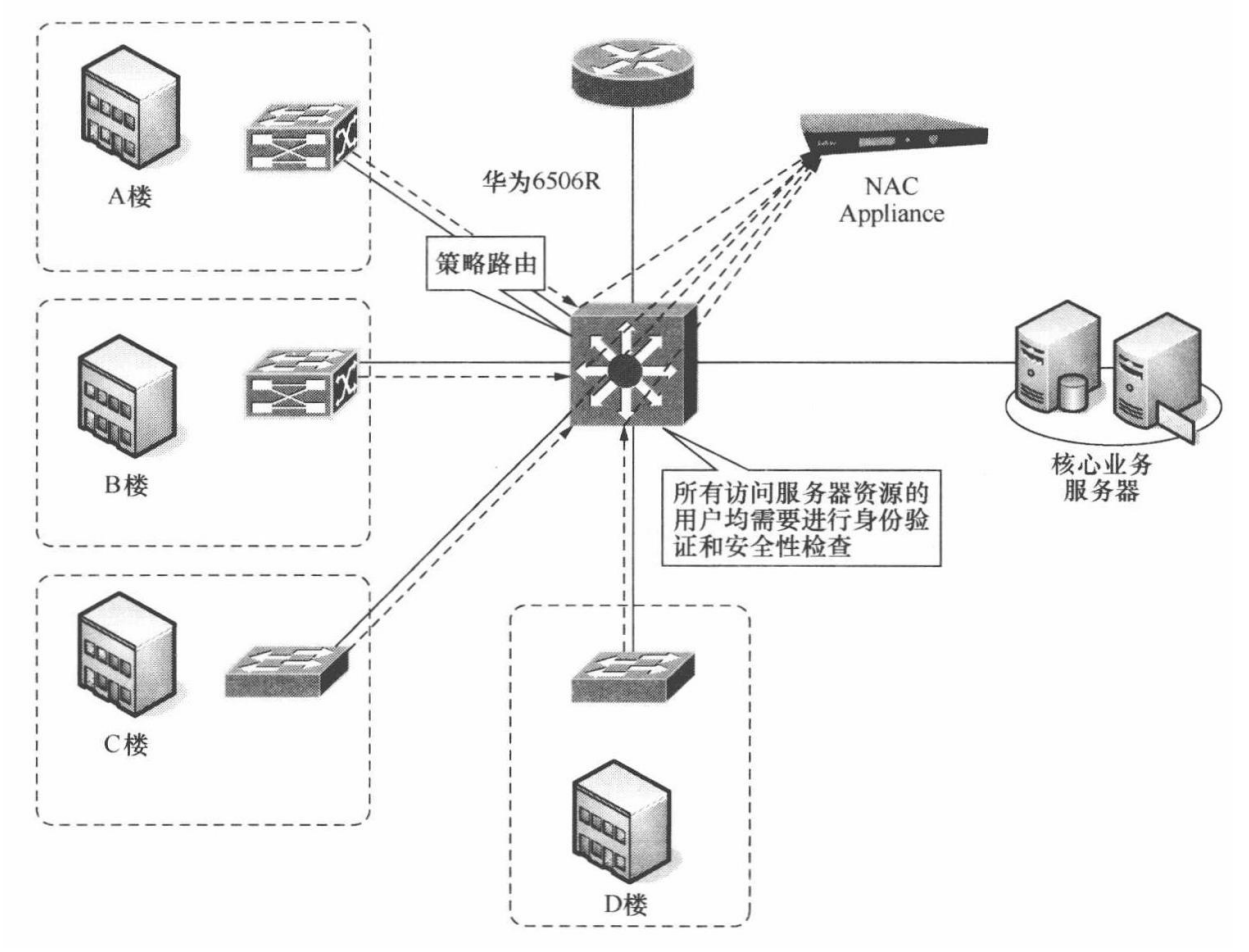


图 3-57　策略路由准入控制技术示意图

ance，这样就由 NAC Appliance 控制了所有访问核心区域的数据流量，从而达到保护核心资源，对入网访问终端进行准入控制的安全目标。

PBR 在使用中有以下 3 个好处：

① 能够通过 ACL 来灵活的控制哪些终端是需要受管理，哪些终端是可以例外的。

② 只管理上行流量，只要终端通过了验证和安检，则下行流量可以走正常的路径，由于上行流量的数据大小一般远远小于下行流量，从而较好地解决了在线型架构影响正常访问速度的问题。

③ 在部署阶段，PBR 架构是物理旁路部署，因此不会改动网络的拓扑结构，同时也更方便小范围的测试。

2. 工作过程

在策略路由准入架构下，能够基于网关将跨网段访问的数据流量发送至已经配置好的下一跳地址，这个地址一般是 NAC Appliance 的管理口。因此被管控计算机的所有上行流量都将经过 NAC Appliance 并接收安全准入管理，计算机顺利入网后，其上行数据路由为：核心网关→NAC Appliance→核心→目标资源。其工作过程如图 3-58 所示。

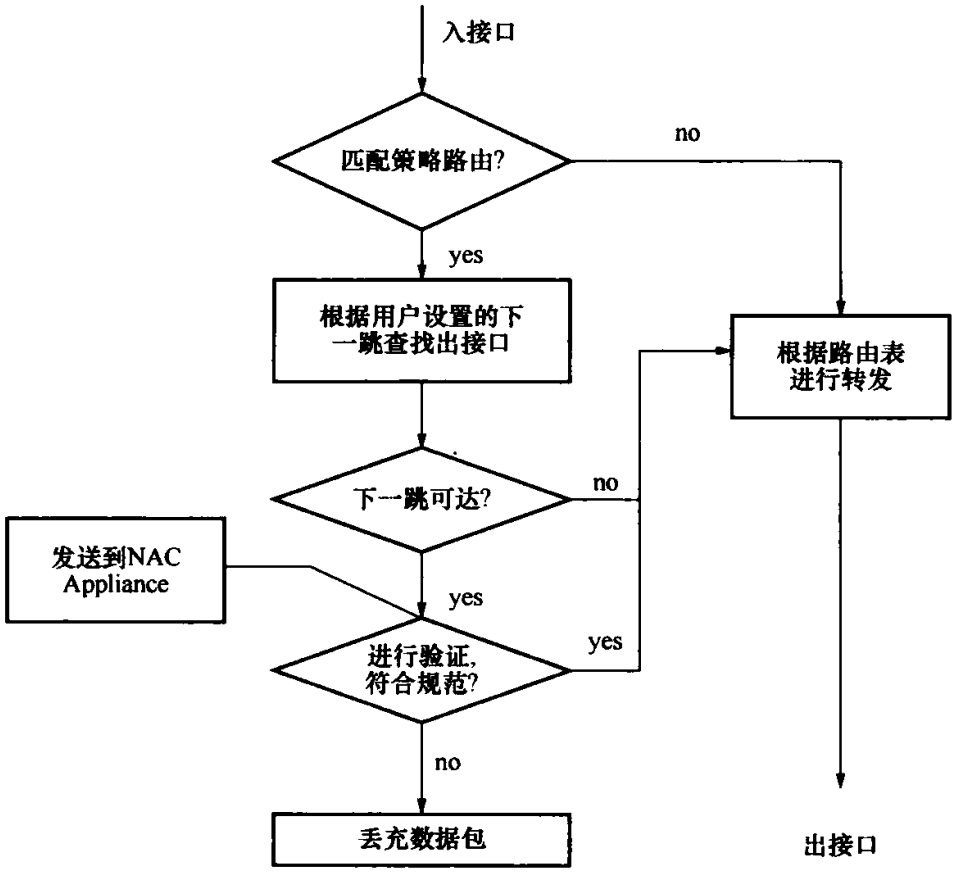


图 3-58 策略路由准入架构工作流程

1）交换机

交换机上使用重定向功能实现策略路由。重定向是指根据流分类对具有某种特征的数据报文的转发作出重新决策，改变报文的输出方向，将其输出到指定的端口、CPU 或下一跳 IP 地址。将数据报文重定向到下一跳 IP 地址，可用于实现策略路由。

2）路由器

策略路由的配置分为两大部分：定义策略和在接口上应用策略。策略路由的 Route-map 有 match 匹配条件和 set 动作。策略路由 Route-map 中的 match 匹配条件只有访问控制列表的方式，set 动作只有强制指定下一跳 IP 和下一跳接口两种。定义策略只是完成了策略路由的一步，只有在接口上应用了定义的策略，策略路由才能真正生效。

在路由器上，网络管理者可以用 match 和 set 语句定义不同的 Route-map，然后将 Route-map 应用在接收报文接口上，实现路径的选择。

每个 Route-map 都有一系列 sequence，每个 sequence 中含有多个 match 和 set 从句。match 从句定义了匹配的条件，当入报文满足该条件时进行策略路由；set 从句规定了当 match 条件被满足时将要进行的路由动作。当一个 sequence 中的 match 条件未被满足时，继续尝试匹配下一个 sequence。

对于路由器收到的报文，首先判断入接口是否绑定了策略路由，如果没有绑

定，按照正常的根据目的地址查找路由表进行转发；如果绑定了策略路由，则按照 Route-map 的 sequence 依次进行处理，以下为具体过程。

Step1：首先用报文去匹配第一个 sequence 中配置的 ACL，若匹配失败，则接着匹配下一个 sequence 中配置的 ACL，依次类推；若匹配成功，则判断所属 sequence 的属性。

Step2：若 sequence 的属性为 deny，则走正常路由；若 sequence 的属性为 permit，则根据该 sequence 中的 set 项进行转发。

Step3：判断是否存在有效的 set ip next-hop 项（为直连下一跳）。当有多个 set ip next-hop 项时，按照设置顺序选择第一个有效的下一跳，若存在，则将报文送往设定的下一跳。

Step4：若未设置 set ip next-hop 或不存在有效的 set ip next-hop，则需要进一步查看是否存在有效的出接口（该接口存在且状态为 UP）。当有多个 set interface 项时，按照设置顺序选择第一个有效的出接口，若存在，则报文从该接口直接发出，否则走正常路由。

Step5：走正常路由时，若在转发表中查到相应的路由，则按此路由进行报文转发，否则按照策略路由中设定的有效的 set ip default next-hop 项（为直连下一跳）进行转发。当有多个 set ip default next-hop 项时，按照设置顺序选择第一个有效的默认下一跳。

Step6：若未设定 set ip default next-hop 或不存在有效的 set ip default next-hop，则按照策略路由中设定的有效 set default interface 项进行转发。当有多个 set default interface 项时，按照设置顺序选择第一个有效的默认出接口。

Step7：若未设定 set default interface 或不存在有效的 set default interface，则按照默认路由转发。

Step8：若系统未设置默认路由，则将报文丢弃。

3. 主要特点

策略路由网络准入控制技术主要特点如表 3-7 所示。

表 3-7　策略路由网络准入控制技术主要特点

NAC 体系	对应参数	备注
架构组成	Agent（可选） + Switch（Router） + NAC Appliance	客户端模式是可选的，如果用户需要较完善的安全检查和控制功能，可以加装客户端或控件
支持环境	支持 PBR 的交换机	
旁路部署	半旁路	对上行流量 in-line，下行流量旁路
无客户端支持	√	

续表

NAC 体系	对应参数	备注
交换机配置量	小	只需在网关上搭建 PBR 环境
接入层端口级控制	×	只能基于网关进行跨网段访问时的 3 层控制
Hub 接入控制	√	
http 快捷性	√	由于可以选择放通部分流量，因此能够兼容 DHCP 环境，可以进行 Web 重定向引导
系统资源（内存）占用	小	无客户端的优势在这里体现出来了
来宾管理	好	能够进行 Web 引导，因此十分友好
稳定性	好	不依赖客户端，交换机及服务器能够确保稳定性
兼容性	好	去品牌化，主流核心交换机一般均能支持 PBR
防单点故障	√	PBR 本身支持下一跳不可达即可恢复默认路由

4. 配置方法

1）Cisco 与 H3C 环境配置方法

（1）Cisco 环境配置方法。

//利用 ACL 对需要管控的计算机地址进行过滤

access-list 199 permit ip 192. 167. 10. 0 0. 0. 0. 255 any

//建立一个 Route-map，将管控计算机的流量下一跳指向 NAC Appliance

route-map pbr permit 10

match ip address 199

set ip next-hop x. x. x. x

//在接口（可以是物理接口也可以是 VLAN 虚接口）下应用这条 Route-map

interface vlan2

ip address 192. 167. 10. 1 255. 255. 255. 0

ip policy route-map pbr

注意：Cisco 35 系列的交换机要求在 sdm 中开启路由功能后才能使策略路由配置生效。

sdm prefer routing

exit

reload

（2）H3C 环境配置方法。

//配置 ACL 策略，圈定准入管理范围

[H3C7506E] acl number 3040

[H3C7506E-acl-adv-3040] rule 10 permit ip source 203.133.129.16 0 dest any

[H3C7506E-acl-adv-3040] quit

//配置匹配 ACL 的流分类 1

[H3C7506E] traffic classifier 1

[H3C7506E-classifier-1] if-match acl 3040

[H3C7506E-classifier-1] quit

//配置刚才定义的流分类 1 的行为，定义如果匹配就下一跳至 NAC Appliance

[H3C7506E] traffic behavior 1

[H3C7506E-behavior-1] redirect next-hop 203.133.131.200

[H3C7506E-behavior-1] quit

//将刚才设置的流分类及行为应用至 QOS 策略中，定义 policy 1

[H3C7506E] qos policy 1

[H3C7506E-qospolicy-1] classifier 1

[H3C7506E-qospolicy-1] behavior 1

[H3C7506E-qospolicy-1] quit

//在接口上应用定义的 QOS 策略 policy 1

[H3C7506E] interface GigabitEthernet 2/0/11

[H3C7506E-GigabitEthernet2/0/11] qos apply policy 1 inbound

[H3C7506E-GigabitEthernet2/0/11] quit

2）交换机策略路由配置实例（中兴环境）

这里以中兴设备为例，介绍一下交换机策略路由的具体配置方法。

（1）网络拓扑。如图 3-59 所示，核心交换机通过不同的接口接入两个子网的用户，而且有两个 ISP 出口可供使用。默认情况下，两个子网的用户业务使用 ISP1 出口。为了业务的开展，需要将 IP 地址属于 10.10.0.0/24 子网的用户业务使用 ISP2 出口。

（2）配置步骤。具体配置步骤如下：

ZXR10（config）#interface fei_1/1

ZXR10（config-if）#description to User1

ZXR10（config-if）#ip address 10.10.0.1 255.255.255.0

ZXR10（config-if）#exit

//配置接口 IP 地址，作为 10.10.0.0/24 网段用户的网关

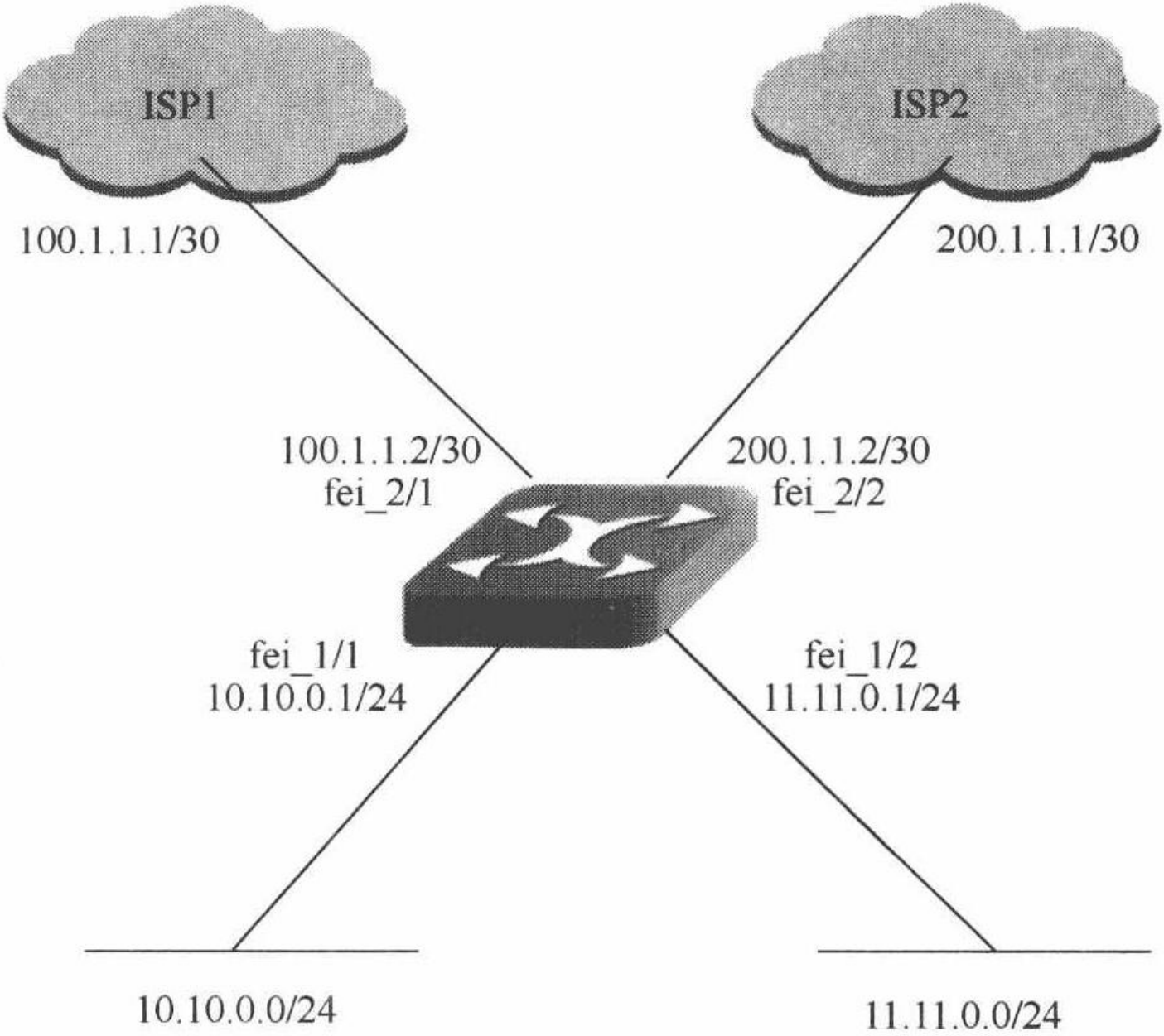
ZXR10（config）#interface fei_1/2

ZXR10（config-if）#description to User2

ZXR10（config-if）#ip address 11.11.0.1 255.255.255.0

图 3-59 策略路由组网实例（交换机）

```
ZXR10（config-if）#exit
//配置接口 IP 地址，作为 11.11.0.0/24 网段用户的网关
ZXR10（config）#interface fei_2/1
ZXR10（config-if）#description to ISP1
ZXR10（config-if）#ip address 100.1.1.2 255.255.255.252
ZXR10（config-if）#exit
//配置与 ISP1 对接 IP 地址
ZXR10（config）#interface fei_2/2
ZXR10（config-if）#description to ISP2
ZXR10（config-if）#ip address  200.1.1.2 255.255.255.252
ZXR10（config-if）#exit
//配置与 ISP2 对接 IP 地址
ZXR10（config）#ip route 0.0.0.0 0.0.0.0 100.1.1.1
//配置默认路由，指向 ISP1
ZXR10（config）#acl standard number 10
ZXR10（config-std-acl）#rule 1 permit 10.10.0.0 0.0.0.255
ZXR10（config-std-acl）#exit
//定义一个 ACL，描述 10.10.0.0/24 网段的用户
ZXR10（config）#redirect in 10 rule-id 1 next-hop 200.1.1.1
//配置 QoS 的策略路由，把 10.10.0.0/24 网段的用户策略路由到 ISP2
ZXR10（config）#interface fei_1/1
ZXR10（config-if）#ip access-group 10 in
```


ISP1
ISP2
100.1.1.1/30
200.1.1.1/30
100.1.1.2/30
fei_2/1
200.1.1.2/30
fei_2/2
fei_1/1
10.10.0.1/24
fei_1/2
11.11.0.1/24
10.10.0.0/24
11.11.0.0/24

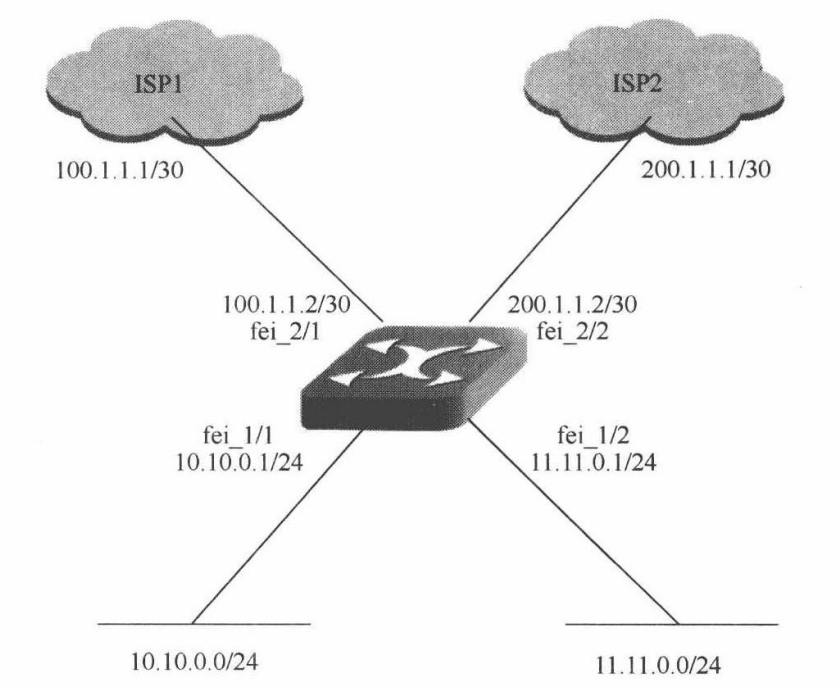


图 3-59 策略路由组网实例（交换机）

ZXR10（config-if）#exit
//配置接口 IP 地址，作为 11.11.0.0/24 网段用户的网关
ZXR10（config）#interface fei _ 2/1
ZXR10（config-if）#description to ISP1
ZXR10（config-if）#ip address 100.1.1.2 255.255.255.252
ZXR10（config-if）#exit
//配置与 ISP1 对接 IP 地址
ZXR10（config）#interface fei _ 2/2
ZXR10（config-if）#description to ISP2
ZXR10（config-if）#ip address 200.1.1.2 255.255.255.252
ZXR10（config-if）#exit
//配置与 ISP2 对接 IP 地址
ZXR10（config）#ip route 0.0.0.0 0.0.0.0 100.1.1.1
//配置默认路由，指向 ISP1
ZXR10（config）#acl standard number 10
ZXR10（config-std-acl）#rule 1 permit 10.10.0.0 0.0.0.255
ZXR10（config-std-acl）#exit
//定义一个 ACL，描述 10.10.0.0/24 网段的用户
ZXR10（config）#redirect in 10 rule-id 1 next-hop 200.1.1.1
//配置 QoS 的策略路由，把 10.10.0.0/24 网段的用户策略路由到 ISP2
ZXR10（config）#interface fei _ 1/1
ZXR10（config-if）#ip access-group 10 in

ZXR10（config-if）#exit

//在相应的端口上应用 ACL

3）路由器策略路由配置实例

这里仍以中兴环境的设备为例。中兴环境的路由器与交换机策略路由的配置略有不同，当网络中存在多个互联网服务提供商（ISP）出口时，可以在出口路由器上通过策略路由为不同组别的用户选择不同的 ISP 出口，也可以基于服务的种类来选择不同的 ISP 出口。

（1）路由器策略路由配置实例一。

① 网络拓扑。如图 3-60 所示，路由器通过不同的接口接入两个子网的用户，而且有两个 ISP 出口可供使用，要求根据用户的 IP 地址选择不同的出口，IP 地址属于 10.10.0.0/24 子网的用户业务使用 ISP1 出口，而 IP 地址属于 11.11.0.0/24 子网的用户业务使用 ISP2 出口。

图 3-60　策略路由组网实例（路由器）1

② 配置步骤。具体配置步骤如下：

ZXR10（config）#interface fei _ 1/1

ZXR10（config-if）#description to User1

ZXR10（config-if）#ip address　10.10.0.1 255.255.255.0

ZXR10（config-if）#exit

//配置接口 IP 地址，作为 10.10.0.0/24 网段用户的网关

ZXR10（config）#interface fei _ 1/2

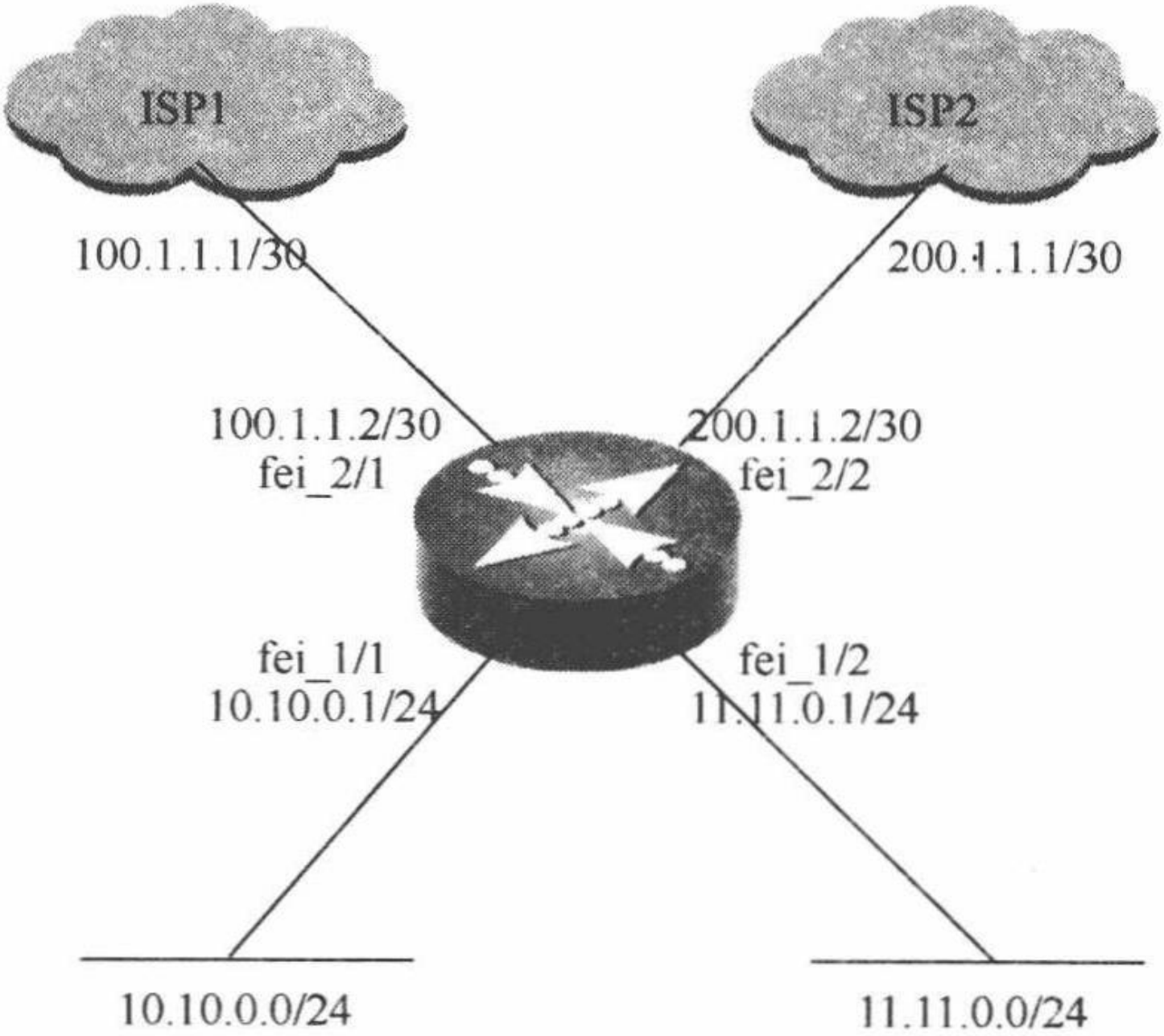
ZXR10（config-if）#description to User1

ZXR10（config-if）#ip address　11.11.0.1 255.255.255.0

ZXR10（config-if）#exit

//配置接口 IP 地址，作为 10.10.0.0/24 网段用户的网关

ZXR10（config）#interface fei _ 2/1


ISP1
ISP2
100.1.1.1/30
200.1.1.1/30
100.1.1.2/30
fei_2/1
200.1.1.2/30
fei_2/2
fei_1/1
10.10.0.1/24
fei_1/2
11.11.0.1/24
10.10.0.0/24
11.11.0.0/24

ZXR10（config-if）＃exit

//在相应的端口上应用 ACL

3）路由器策略路由配置实例

这里仍以中兴环境的设备为例。中兴环境的路由器与交换机策略路由的配置略有不同，当网络中存在多个互联网服务提供商（ISP）出口时，可以在出口路由器上通过策略路由为不同组别的用户选择不同的 ISP 出口，也可以基于服务的种类来选择不同的 ISP 出口。

（1）路由器策略路由配置实例一。

① 网络拓扑。如图 3-60 所示，路由器通过不同的接口接入两个子网的用户，而且有两个 ISP 出口可供使用，要求根据用户的 IP 地址选择不同的出口，IP 地址属于 10.10.0.0/24 子网的用户业务使用 ISP1 出口，而 IP 地址属于 11.11.0.0/24 子网的用户业务使用 ISP2 出口。

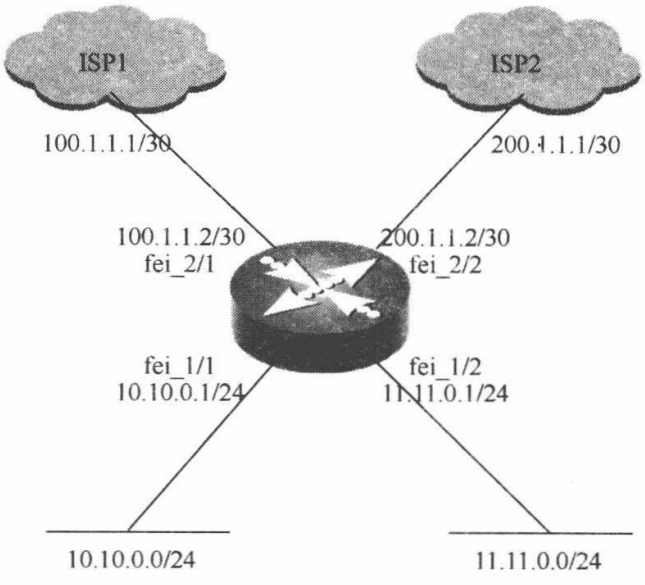


图 3-60　策略路由组网实例（路由器）1

② 配置步骤。具体配置步骤如下：

ZXR10（config）＃interface fei _ 1/1

ZXR10（config-if）＃description to User1

ZXR10（config-if）＃ip address　10.10.0.1 255.255.255.0

ZXR10（config-if）＃exit

//配置接口 IP 地址，作为 10.10.0.0/24 网段用户的网关

ZXR10（config）＃interface fei _ 1/2

ZXR10（config-if）＃description to User1

ZXR10（config-if）＃ip address　11.11.0.1 255.255.255.0

ZXR10（config-if）＃exit

//配置接口 IP 地址，作为 10.10.0.0/24 网段用户的网关

ZXR10（config）＃interface fei _ 2/1

```
ZXR10（config-if）#description to ISP1
ZXR10（config-if）#ip address 100.1.1.2 255.255.255.252
ZXR10（config-if）#exit
//配置与 ISP1 对接 IP 地址
ZXR10（config）#interface fei_2/2
ZXR10（config-if）#description to ISP2
ZXR10（config-if）#ip address  200.1.1.2 255.255.255.252
ZXR10（config-if）#exit
//配置与 ISP2 对接 IP 地址
ZXR10（config）#ip route 0.0.0.0 0.0.0.0 100.1.1.1
//配置默认路由，指向 ISP1
ZXR10（config）#acl standard number 10
ZXR10（config-std-acl）#rule 1 permit 10.10.0.0 0.0.0.255
ZXR10（config-std-acl）#exit
//定义一个 ACL，描述 10.10.0.0/24 网段的用户
ZXR10（config）#acl standard number 20
ZXR10（config-std-acl）#rule 1 permit 11.11.0.0 0.0.0.255
ZXR10（config-std-acl）#exit
//定义一个 ACL，描述 11.11.0.0/24 网段的用户
ZXR10（config）#route-map source-ip permit 10
ZXR10（config-route-map）#match ip address 10
ZXR10（config-route-map）#set ip next-hop 100.1.1.1
ZXR10（config-route-map）#exit
//配置策略路由，将与 ACL 10 匹配的报文转发到 100.1.1.1
ZXR10（config）#route-map source-ip permit 20
ZXR10（config-route-map）#match ip address 20
ZXR10（config-route-map）#set ip next-hop 200.1.1.1
ZXR10（config-route-map）#exit
//配置策略路由，将与 ACL 20 匹配的报文转发到 200.1.1.1
ZXR10（config）#interface fei_1/1
ZXR10（config-if）#ip policy route-map source-ip
ZXR10（config-if）#exit
//在用户接口 fei_1/1 上运用策略路由
ZXR10（config）#interface fei_1/2
ZXR10（config-if）#ip policy route-map source-ip
ZXR10（config-if）#exit
//在用户接口 fei_1/2 上运用策略路由
```

在本实例中，会出现以下 3 种情况：

① 当 ISP1 和 ISP2 出口均正常时，10.10.0.0/24 和 11.11.0.0/24 子网的用户业务分别走 ISP1、ISP2 出口。

② 当 ISP1 正常、ISP2 出口异常时，两个子网的用户业务都走 ISP1 出口，此时 11.11.0.0/24 子网的用户业务利用的是默认路由。

③ 当 ISP1 异常、ISP2 出口正常时，11.11.0.0/24 子网的用户业务正常，而 10.10.0.0/24 子网的用户业务中断。

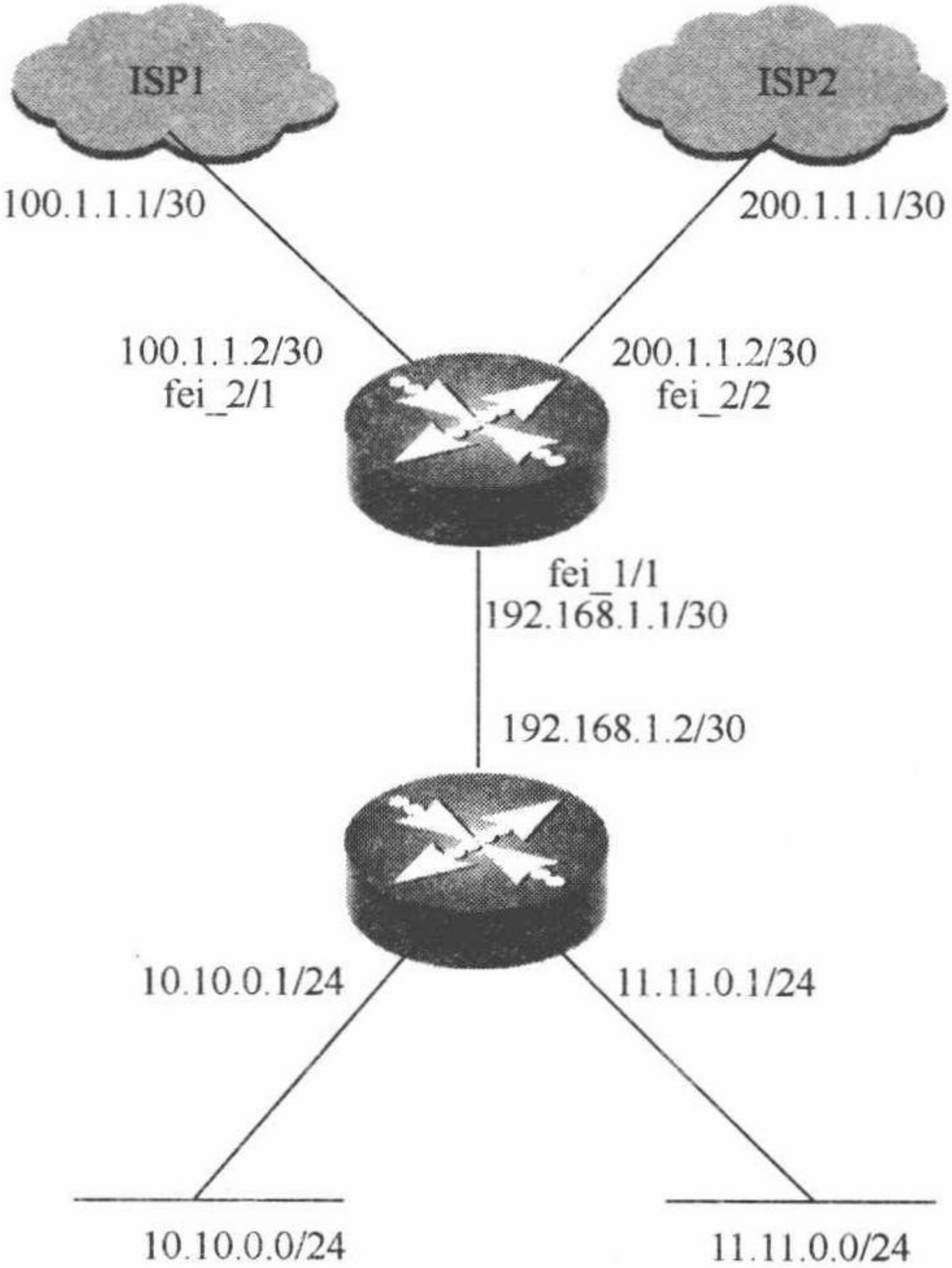
（2）路由器策略路由配置实例二。

① 网络拓扑。如图 3-61 所示，当不同子网的用户通过路由器的同一个接口接入时，策略路由器的配置要做相应的变化。

图 3-61　策略路由组网实例（路由器）2

② 配置步骤。具体配置步骤如下：

```
ZXR10（config）#interface fei_1/1
ZXR10（config-if）#description to User
ZXR10（config-if）#ip address  192.168.1.1 255.255.255.252
ZXR10（config-if）#exit
//定义与用户路由器对接接口 IP 地址
ZXR10（config）#interface fei_2/1
ZXR10（config-if）#description to ISP1
ZXR10（config-if）#ip address  100.1.1.2 255.255.255.252
ZXR10（config-if）#exit
```


ISP1
ISP2
100.1.1.1/30
200.1.1.1/30
100.1.1.2/30
fei_2/1
200.1.1.2/30
fei_2/2
fei_1/1
192.168.1.1/30
192.168.1.2/30
10.10.0.1/24
11.11.0.1/24
10.10.0.0/24
11.11.0.0/24

在本实例中，会出现以下 3 种情况：

① 当 ISP1 和 ISP2 出口均正常时，10.10.0.0/24 和 11.11.0.0/24 子网的用户业务分别走 ISP1、ISP2 出口。

② 当 ISP1 正常、ISP2 出口异常时，两个子网的用户业务都走 ISP1 出口，此时 11.11.0.0/24 子网的用户业务利用的是默认路由。

③ 当 ISP1 异常、ISP2 出口正常时，11.11.0.0/24 子网的用户业务正常，而 10.10.0.0/24 子网的用户业务中断。

（2）路由器策略路由配置实例二。

① 网络拓扑。如图 3-61 所示，当不同子网的用户通过路由器的同一个接口接入时，策略路由器的配置要做相应的变化。

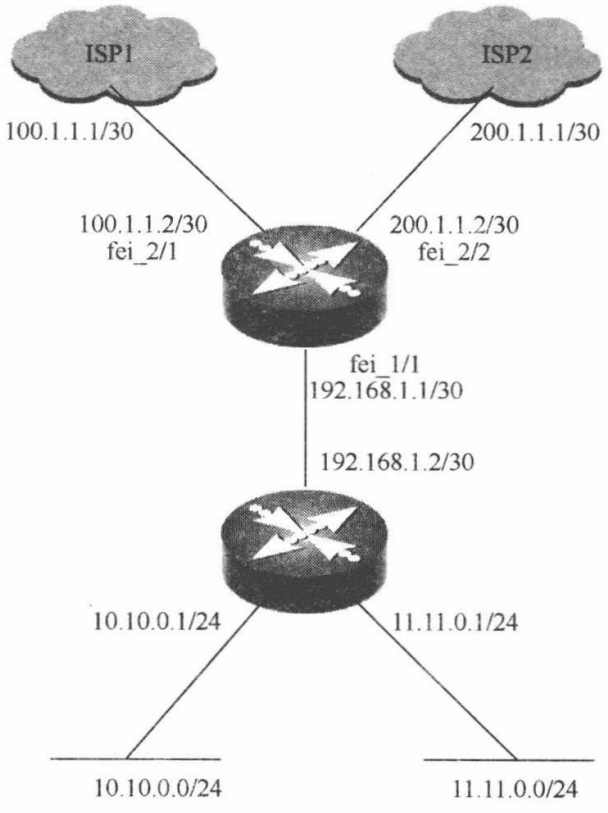


图 3-61　策略路由组网实例（路由器）2

② 配置步骤。具体配置步骤如下：

```
ZXR10（config）＃interface fei _ 1/1
ZXR10（config-if）＃description to User
ZXR10（config-if）＃ip address  192.168.1.1 255.255.255.252
ZXR10（config-if）＃exit
//定义与用户路由器对接接口 IP 地址
ZXR10（config）＃interface fei _ 2/1
ZXR10（config-if）＃description to ISP1
ZXR10（config-if）＃ip address  100.1.1.2 255.255.255.252
ZXR10（config-if）＃exit
```

```
//配置与 ISP1 对接 IP 地址
ZXR10（config）#interface fei _ 2/2
ZXR10（config-if）#description to ISP2
ZXR10（config-if）# ip address  200.1.1.2 255.255.255.252
ZXR10（config-if）#exit
//配置与 ISP2 对接 IP 地址
ZXR10（config）# ip route 10.10.0.0 255.255.255.0 192.168.1.2
ZXR10（config）# ip route 11.11.0.0 255.255.255.0 192.168.1.2
//配置回指用户 IP 网段地址的静态路由
ZXR10（config）#acl standard number 10
ZXR10（config-std-acl）#rule 1 permit 10.10.0.0 0.0.0.255
ZXR10（config-std-acl）#exit
//定义一个 ACL，描述 10.10.0.0/24 网段的用户
ZXR10（config）#acl standard number 20
ZXR10（config-std-acl）#rule 1 permit 11.11.0.0 0.0.0.255
ZXR10（config-std-acl）#exit
//定义一个 ACL，描述 11.11.0.0/24 网段的用户
ZXR10（config）#route-map source-ip permit 10
ZXR10（config-route-map）#match ip address 10
ZXR10（config-route-map）#set ip next-hop 100.1.1.1 200.1.1.1
ZXR10（config-route-map）#exit
//将与 ACL 10 匹配的报文转发到 100.1.1.1，200.1.1.1 作为备用出口
ZXR10（config）#route-map source-ip permit 20
ZXR10（config-route-map）#match ip address 20
ZXR10（config-route-map）#set ip next-hop 200.1.1.1 100.1.1.1
ZXR10（config-route-map）#exit
//将与 ACL 20 匹配的报文转发到 200.1.1.1，100.1.1.1 作为备用出口
ZXR10（config）#interface fei _ 1/1
ZXR10（config-if）# ip policy route-map source-ip
ZXR10（config-if）#exit
//在用户接口 fei _ 1/1 上运用策略路由
```

在本实例中，两个 ISP 出口互为备用，会出现以下两种情况。

① 当 ISP1 和 ISP2 出口均正常时，10.10.0.0/24 和 11.11.0.0/24 子网的用户业务分别走 ISP1、ISP2 出口。

② 当其中一个出口故障时，相应子网的用户业务将走备用出口。所以只要两个出口不同时出现异常，业务将不会中断。

3.4.4　透明网桥准入控制技术分析

透明网桥准入控制技术又被称为网关型的墙准入强制技术，由于透明网桥技术在传统的安全技术中广为应用，像防火墙、UTM、病毒墙、VPN、流量控制等都是属于网关型的基本应用。与策略路由架构不同的是，网桥准入控制是一种 total in-line 架构，采用类似防火墙的部署模式，对网络出口处的所有流量进行相关的管理。

由于企业内部网络十分复杂，涉及到很多种不同的交换网络，而如果用户的网络设备不支持网络准入，或不想花费太多的部署和管理时间，那么可以选择透明网桥准入控制技术来实现 NAC。一般透明网桥设备的部署位置本身即位于安全域边界（互联网出口、服务器出口及办公网出口等），从安全理论的角度讲，对某个用户进行控制（包括访问控制、准入控制、业务控制）。网关配合内网管理系统实现准入控制，与基于 802.1x/EOU 等协议相比，业务实现流程相对清晰可靠、环节少，用户只需要购买少量网关准入设备，采用透明方式部署至网络关键节点处，即可实现准入控制，且对用户原有的业务流程不造成任何影响。只有数据流量通过网关准入设备时，才会起到准入控制的强制作用，由于网桥部署的完全不需要与其他设备联动的特性，因此，透明网桥准入架构是所有准入控制架构中上线最快的方案。

1. 技术实现原理

透明网桥架构采用了防火墙的部署模式，直接桥接在网络出口处，由于所有上下行流量都会流经 NAC Appliance，因此能够很方便地实现准入管理，但正如之前我们曾经提到的那样，由于控制的层次太过远离入网边界，甚至已经到达出口的位置了，这种方案也被人称为“准出”。但是，由于完全节省了旁路 NAC 模式下的大量实施成本，也有用户将网桥架构的 NAC 用于保护特定的区域，作为内部网络和特定区域入口处的一道安全控制闸门。

简单来说，桥接就是把一台机器上的若干个网络接口“连接”起来。其结果是，其中一个网口收到的报文会被复制给其他网口并发送出去。以使得网口之间的报文能够互相转发。交换机就是这样一个设备，它有若干个网口，并且这些网口是桥接起来的。于是，与交换机相连的若干主机就能够通过交换机的报文转发而互相通信。

如图 3-62 所示，主机 A 发送的报文被送到交换机 S1 的 eth0 口，由于 eth0 与 eth1、eth2 桥接在一起，故而报文被复制到 eth1 和 eth2，并且发送出去，然后被主机 B 和交换机 S2 接收到，S2 又会将报文转发给主机 C、D。

交换机在报文转发的过程中并不会篡改报文数据，只是做原样复制。然而桥接却并不是在物理层实现的，而是在数据链路层。交换机能够理解数据链路层的报文，所以实际上桥接却又不是单纯的报文转发。

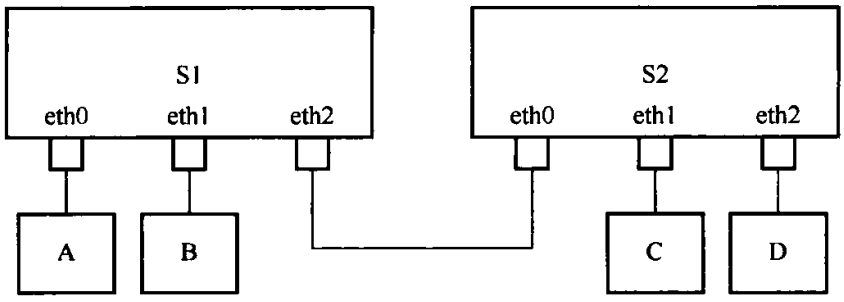


图 3-62 桥接连接示意图

交换机会关心填写在报文的数据链路层头部中的 Mac 地址信息（包括源地址和目的地址），以便了解每个 Mac 地址所代表的主机都在什么位置（与本交换机的哪个网口相连）。在报文转发时，交换机就只需要向特定的网口转发即可，从而避免不必要的网络交互。这个就是交换机的“地址学习”。但是如果交换机遇到一个自己未学习到的地址，就不会知道这个报文应该从哪个网口转发，则只好将报文转发给所有网口（接收报文的那个网口除外）。

比如，主机 C 向主机 A 发送一个报文，报文来到了交换机 S1 的 eth2 网口上。假设 S1 刚刚启动，还没有学习到任何地址，则它会将报文转发给 eth0 和 eth1。同时，S1 会根据报文的源 MAC 地址，记录下“主机 C 是通过 eth2 网口接入的”。于是当主机 A 向 C 发送报文时，S1 只需要将报文转发到 eth2 网口即可。而当主机 D 向 C 发送报文时，假设交换机 S2 将报文转发到了 S1 的 eth2 网口（实际上 S2 也多半会因为地址学习而不这么做），则 S1 会直接将报文丢弃而不做转发（因为主机 C 就是从 eth2 接入的）。

然而，网络拓扑不可能是永不改变的。假设我们将主机 B 和主机 C 换个位置，当主机 C 发出报文时（不管发给谁），交换机 S1 的 eth1 口收到报文，于是交换机 S1 会更新其学习到的地址，将原来的“主机 C 是通过 eth2 网口接入的”改为“主机 C 是通过 eth1 网口接入的”。

但是如果主机 C 一直不发送报文呢？此时，S1 将一直认为“主机 C 是通过 eth2 网口接入的”，于是将其他主机发送给 C 的报文都从 eth2 转发出去，结果报文就发丢了。所以交换机的地址学习需要有超时策略。对于交换机 S1 来说，如果距离最后一次收到主机 C 的报文已经过去一定时间了（默认为 5min），则 S1 需要忘记“主机 C 是通过 eth2 网口接入的”这件事情。这样一来，发往主机 C 的报文又会被转发到所有网口上去，而其中从 eth1 转发出去的报文将被主机 C 收到。

那么，在 Linux 环境下的桥接是如何实现的呢？Linux 内核支持网口的桥接（目前只支持以太网接口）。但是与单纯的交换机不同，交换机只是一个二层设备，对于接收到的报文，要么转发、要么丢弃。小型的交换机里面只需要一块交换芯片即可，并不需要 CPU。而运行着 Linux 内核的机器本身就是一台主机，有可能就是网络报文的目的地。其收到的报文除了转发和丢弃，还可能被送到网

络协议栈的上层（网络层），从而被自己消化。

Linux 内核是通过一个虚拟的网桥设备来实现桥接的。这个虚拟设备可以绑定若干个以太网接口设备，从而将它们桥接起来。如图 3-63 所示。

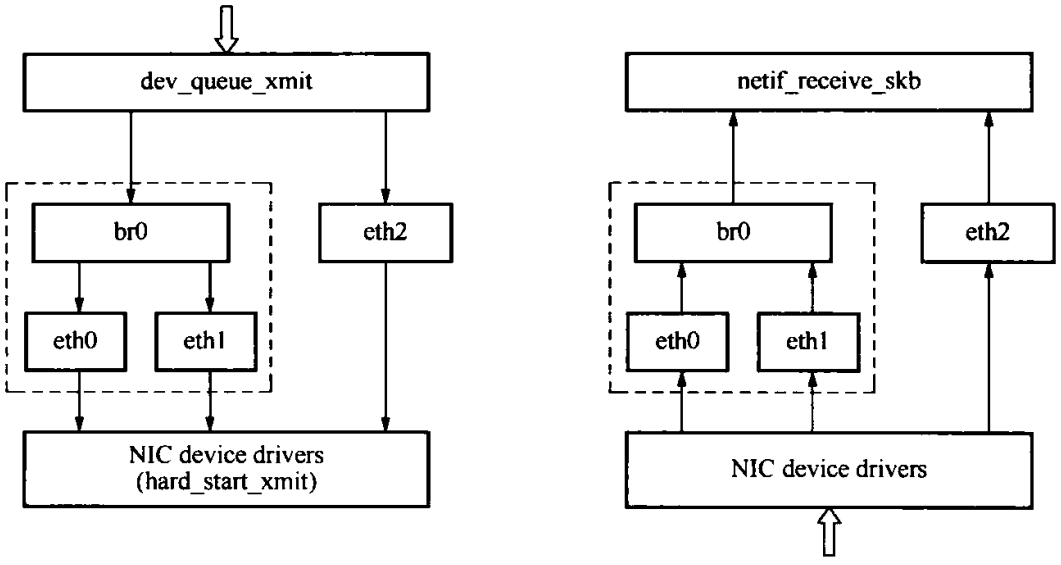


图 3-63　Linux 环境桥接示意图

网桥设备 br0 绑定了 eth0 和 eth1。对于网络协议栈的上层来说，只看得到 br0，因为桥接是在数据链路层实现的，上层不需要关心桥接的细节。于是协议栈上层需要发送的报文被送到 br0，网桥设备的处理代码再来判断报文该被转发到 eth0 或是 eth1，或者两者皆是；反过来，从 eth0 或从 eth1 接收到的报文被提交给网桥的处理代码，在这里会判断报文该转发、丢弃、或提交到协议栈上层。

而有时候 eth0、eth1 也可能会作为报文的源地址或目的地址，直接参与报文的发送与接收（从而绕过网桥）。

2. 工作过程

透明网桥架构准入技术工作过程如下。

1）获取地址表

透明网桥依据网桥表进行转发，网桥表由 MAC 地址和接口两部分组成。网桥与物理网段相连时，会监测该物理网段上的所有以太网帧，一旦监测到某个接口上节点发来的以太网帧，就提取出该帧的源 MAC 地址，并将该 MAC 地址与接收该帧的接口之间的对应关系加入到网桥地址表中。

如图 3-64 所示，Host A、Host B、Host C 和 Host D 4 个 PC 分布在两个局域网中，以 Ethernet 1 与网桥接口 1 相连，以 Ethernet 2 与网桥接口 2 相连。某一时刻，当 Host A 向 Host B 发送以太网帧时，网桥接口 1 和 Host B 都将收到这个帧。

网桥收到这个以太网帧后，就知道 Host A 是与网桥接口 1 相连的（因为从接口 1 收到了该帧），于是 Host A 的 MAC 地址与网桥接口 1 之间的对应关系就被加入到网桥表中。如图 3-65 所示。

图 3-65 网桥得知 Host A 与网桥接口 1 相连

当 Host B 对 Host A 的以太网帧做出响应后，网桥也能监测到 Host B 回应的以太网帧，并知道 Host B 也是与网桥接口 1 相连的（因为从接口 1 收到了该帧），于是 Host B 的 MAC 地址与网桥接口 1 之间的对应关系也被加入到网桥表中，如图 3-66 所示。

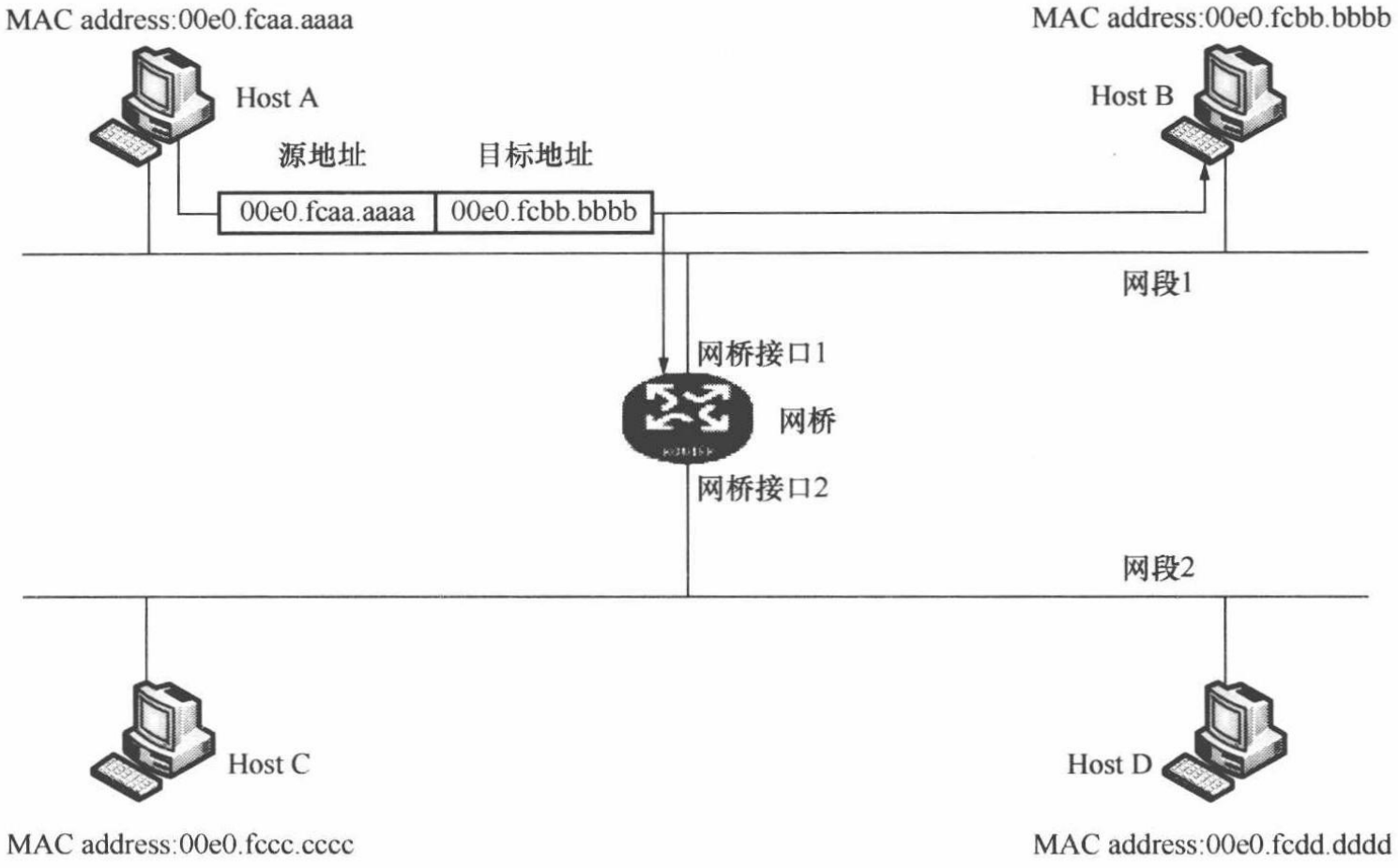
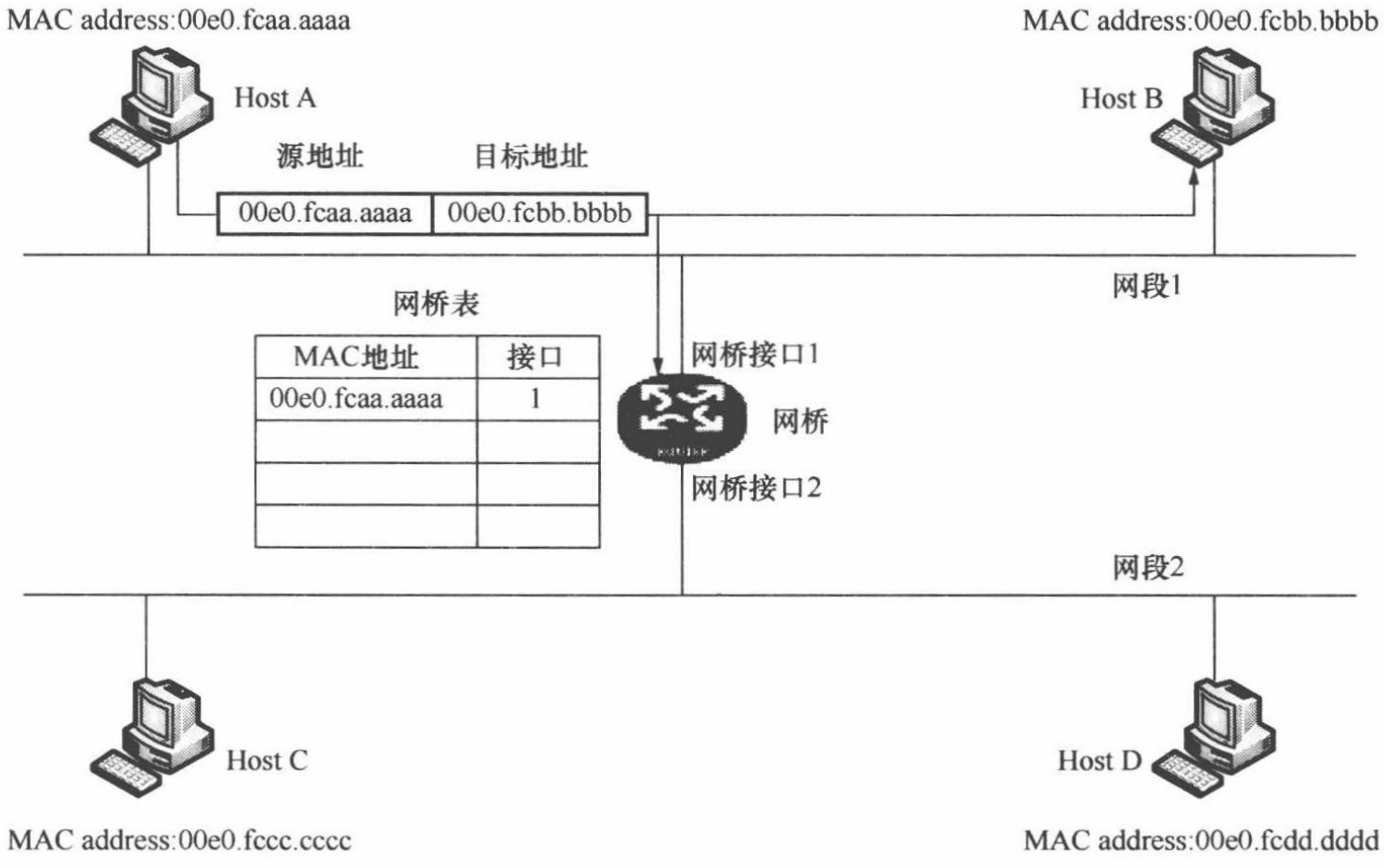


图 3-64　Host A 将信息传递至网段 1 上的 Host B



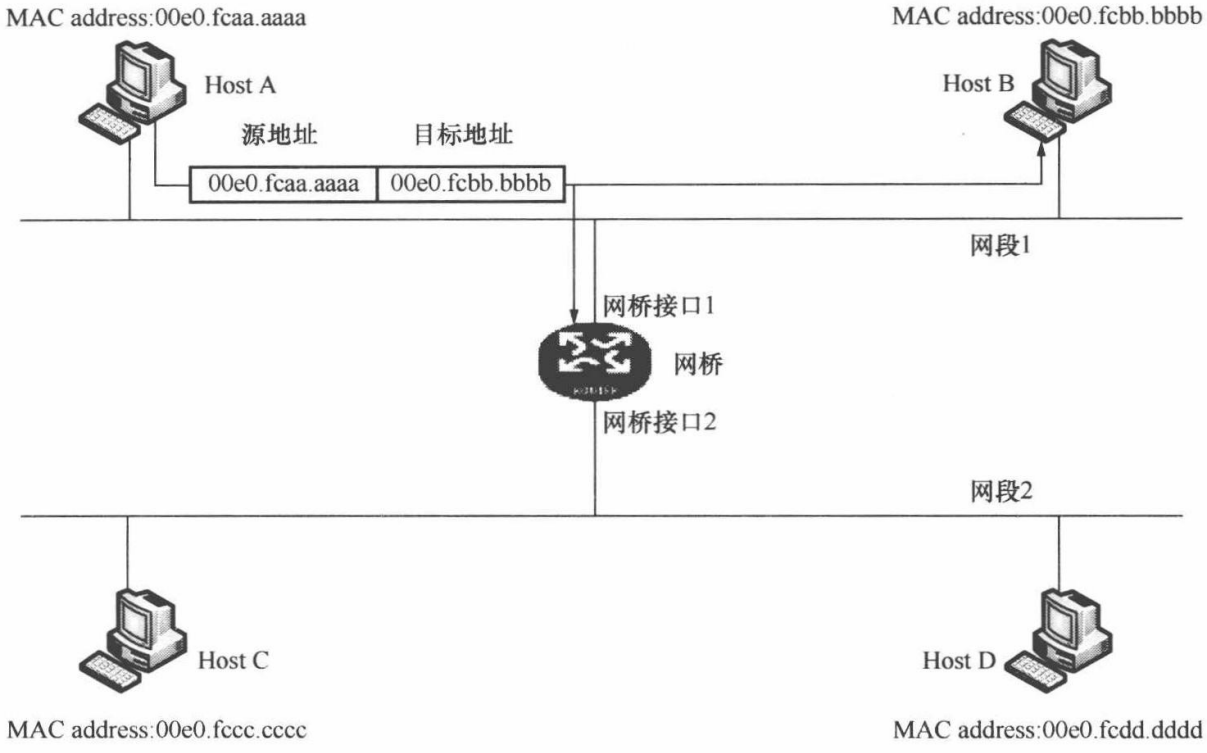


图 3-64　Host A 将信息传递至网段 1 上的 Host B

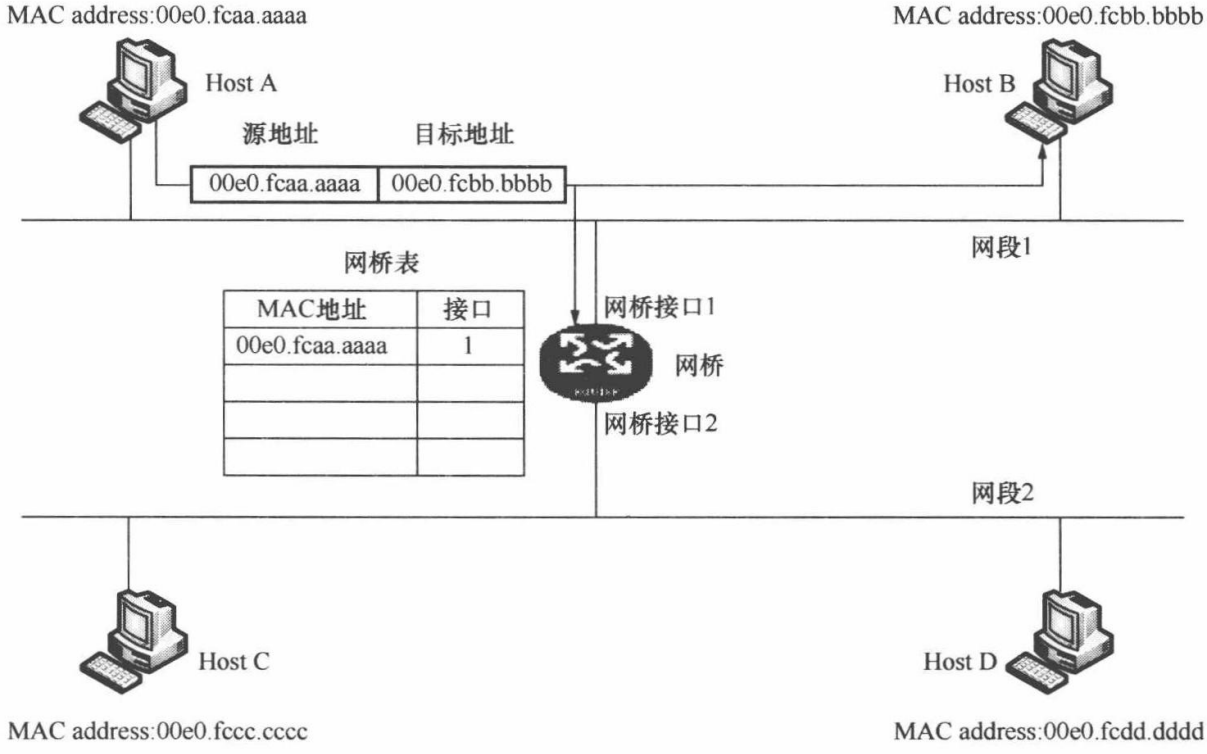


图 3-65　网桥得知 Host A 与网桥接口 1 相连

当 Host B 对 Host A 的以太网帧做出响应后，网桥也能监测到 Host B 回应的以太网帧，并知道 Host B 也是与网桥接口 1 相连的（因为从接口 1 收到了该帧），于是 Host B 的 MAC 地址与网桥接口 1 之间的对应关系也被加入到网桥表中，如图 3-66 所示。

图 3-67　最后网桥中的地址表

2）转发和过滤

网桥将根据下列 3 种情况对数据帧做出转发或不转发（即过滤）帧的决定：

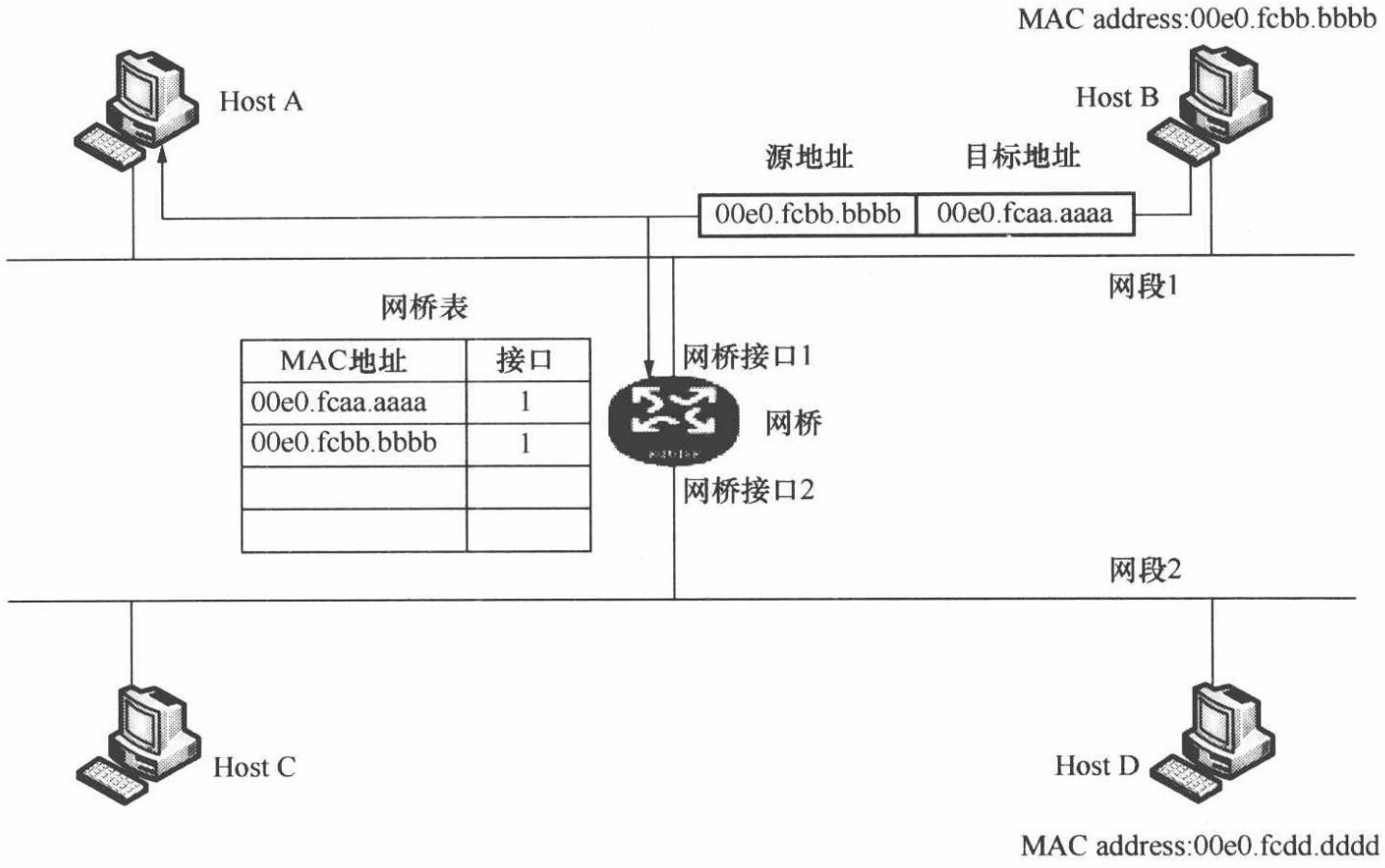
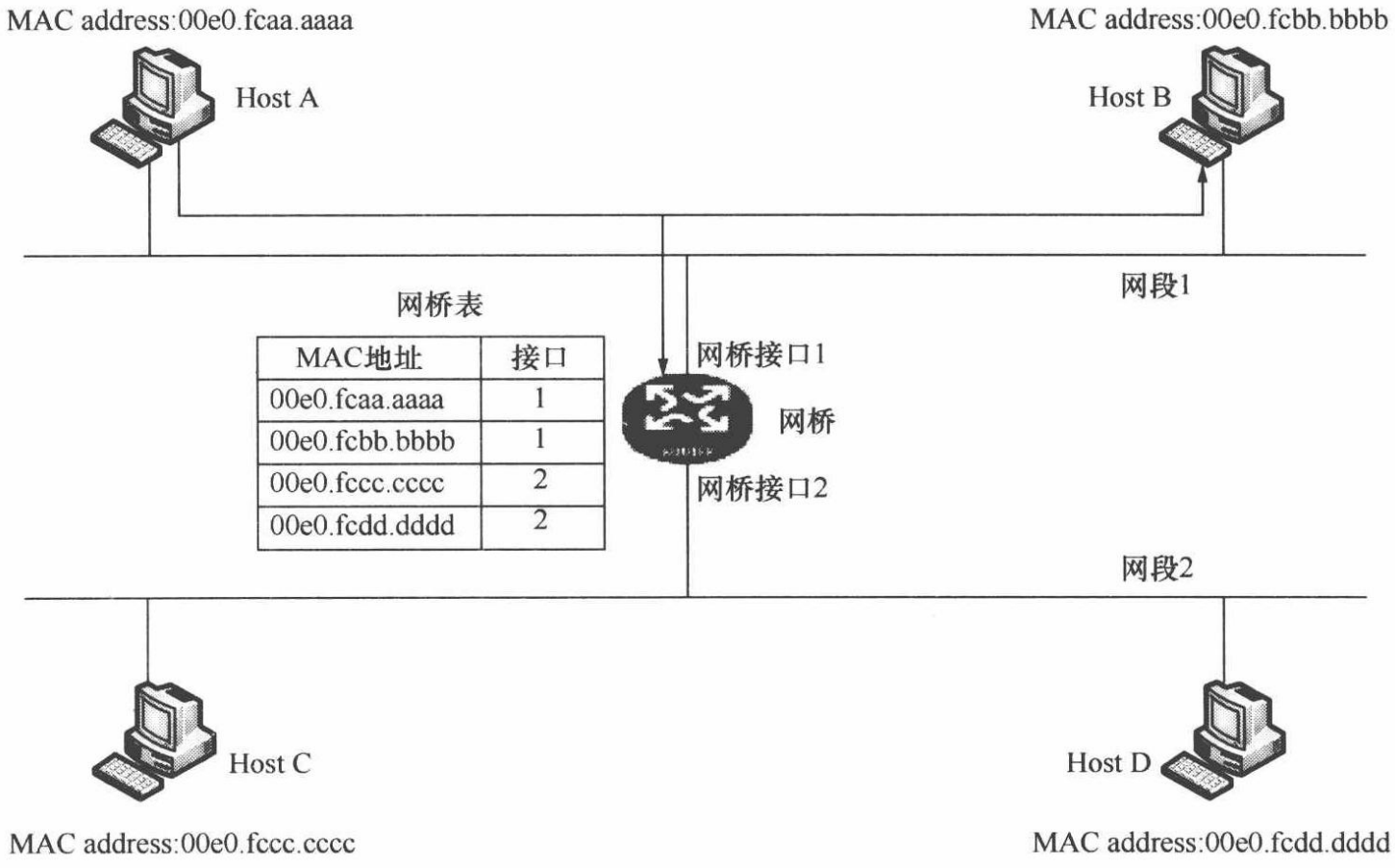


图 3-66　网桥得知 Host B 也与接口 1 相连

最后，所有 MAC 地址与网桥接口的对应关系都会被网桥获取（假设所有的 Host 都在使用中），如图 3-67 所示。



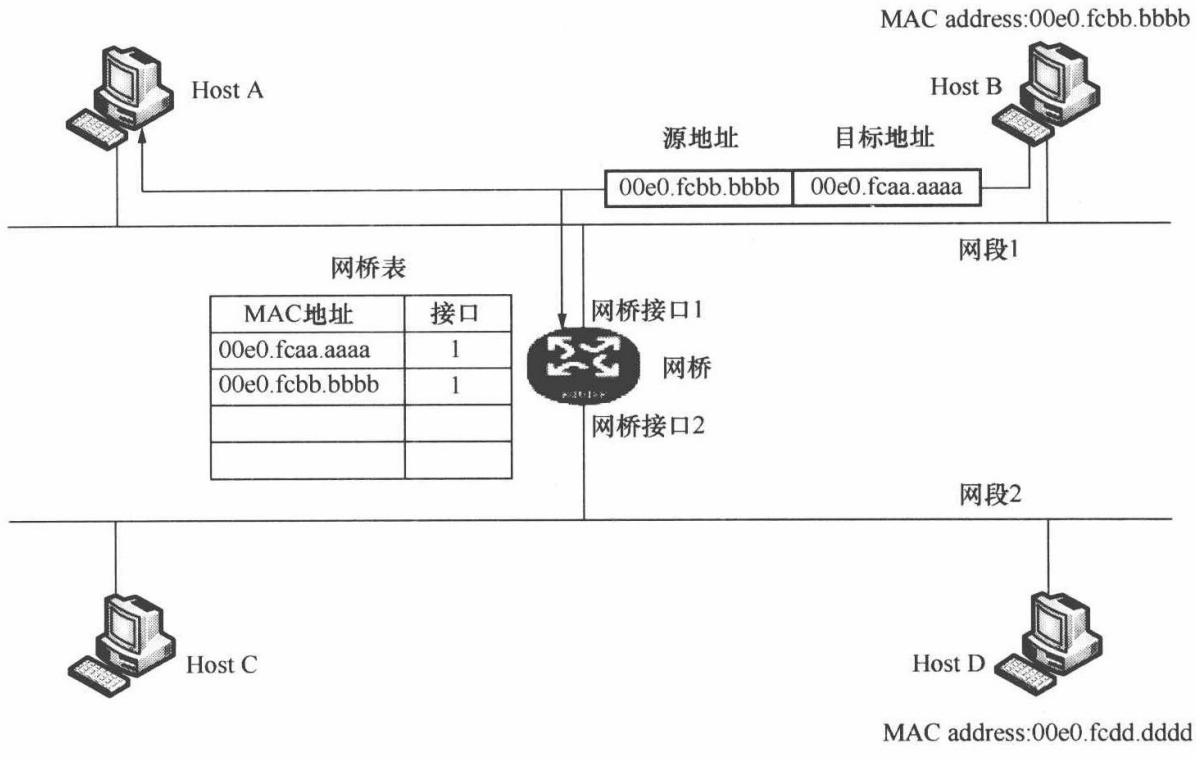


图 3-66　网桥得知 Host B 也与接口 1 相连

最后，所有 MAC 地址与网桥接口的对应关系都会被网桥获取（假设所有的 Host 都在使用中），如图 3-67 所示。

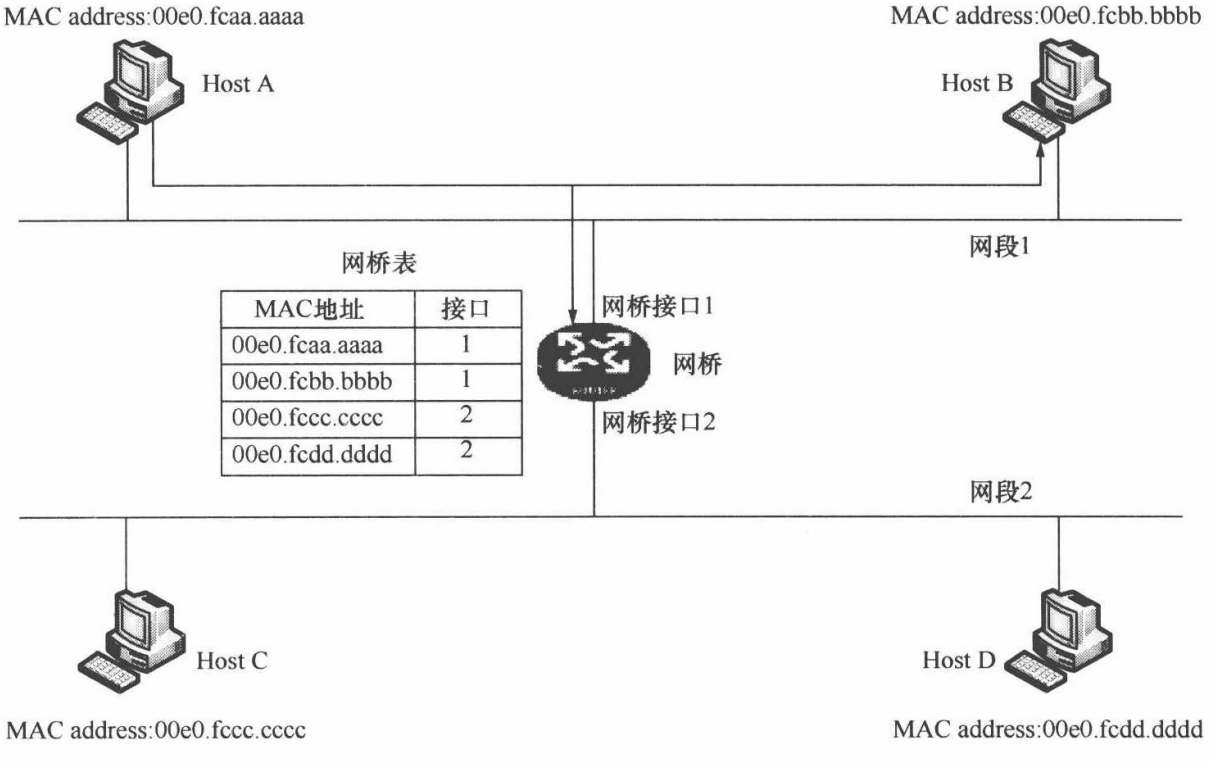


图 3-67　最后网桥中的地址表

2）转发和过滤

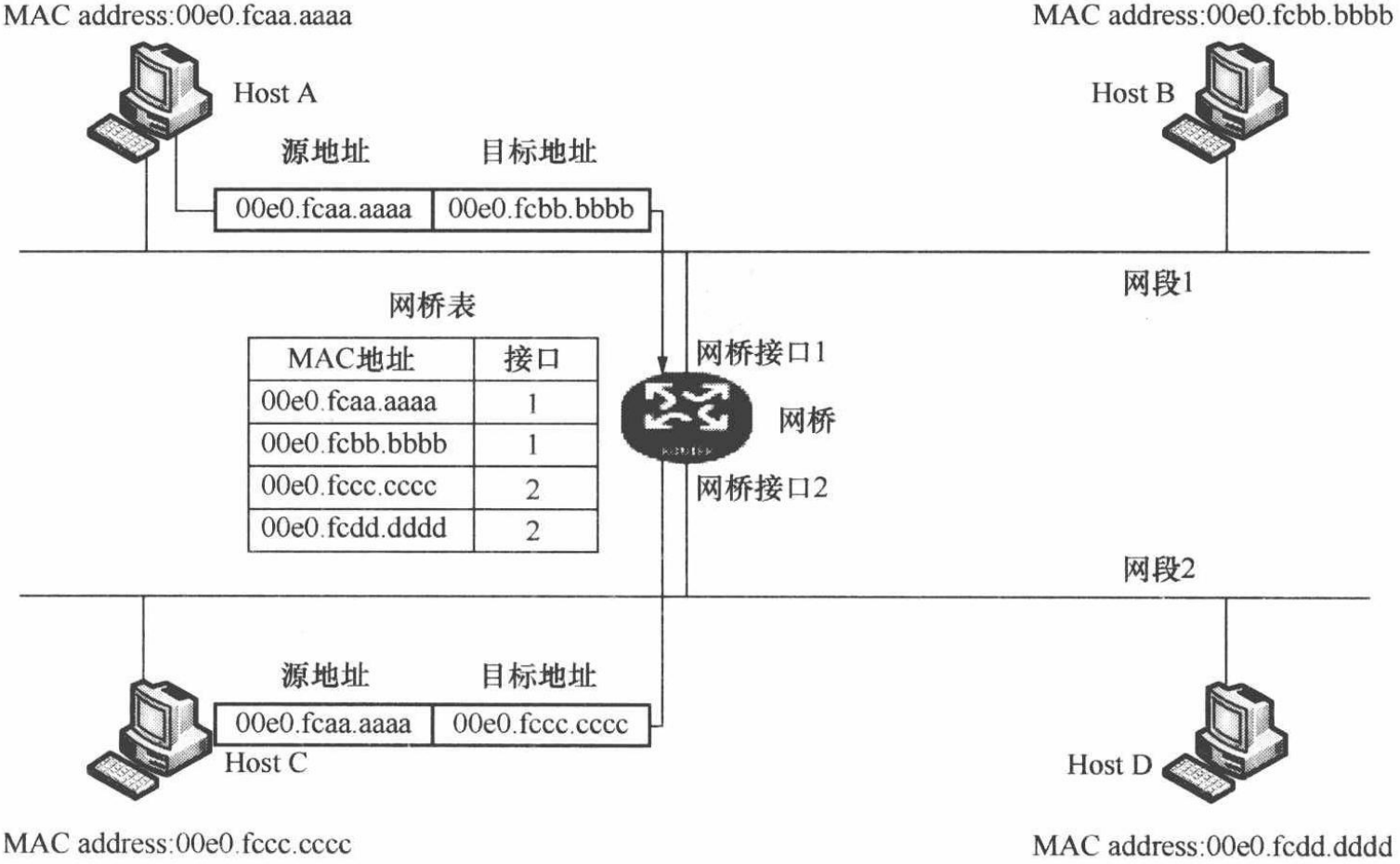
网桥将根据下列 3 种情况对数据帧做出转发或不转发（即过滤）帧的决定：

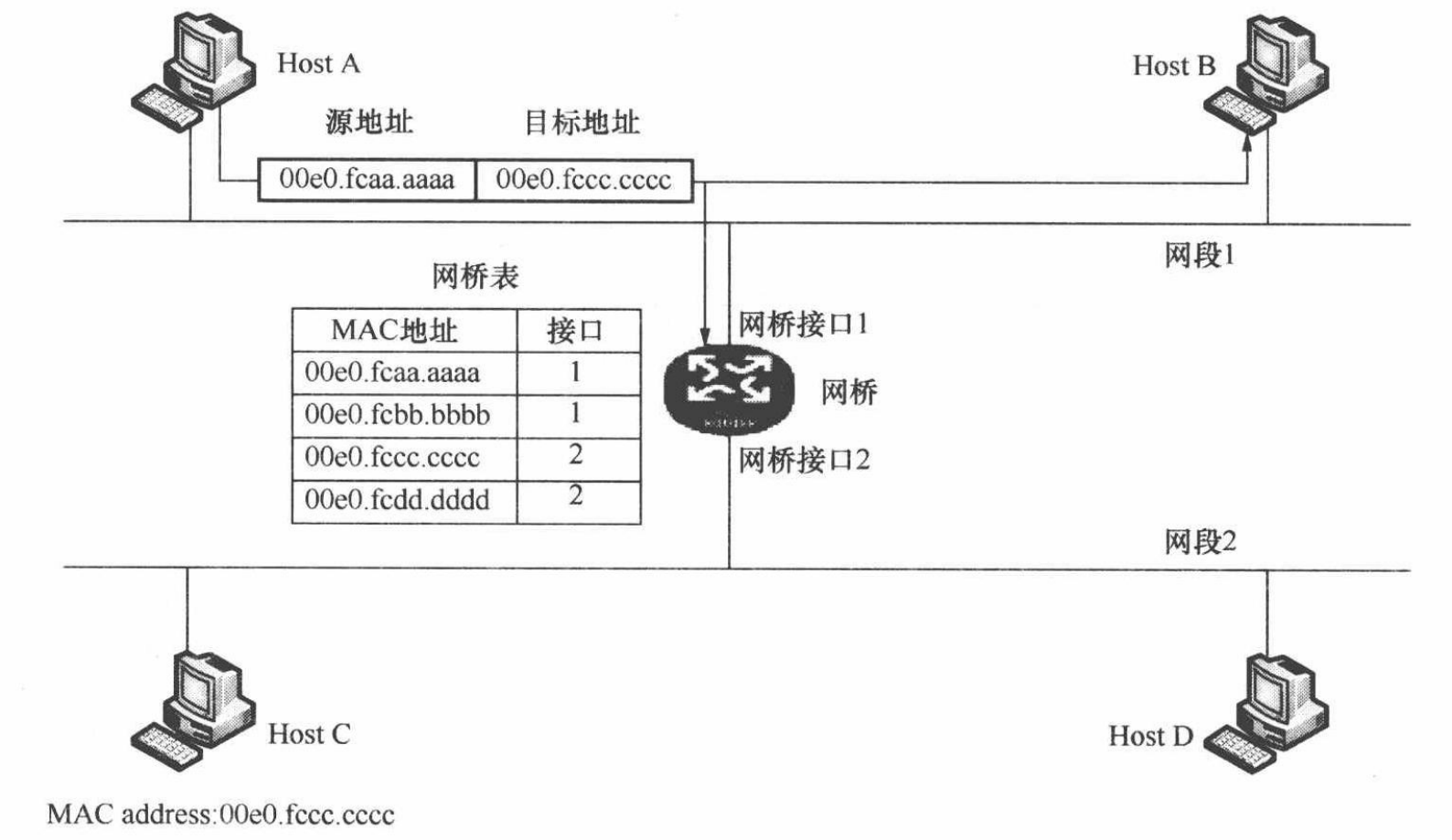
若 Host A 向 Host C 发送以太网帧，网桥通过查找网桥表知道 Host C 与网桥接口 2 对应，就将该帧从接口 2 转发，如图 3-68 所示。

图 3-68 转发

若 Host A 向 Host B 发送以太网帧，因 Host B 与 Host A 在同一个物理网段上，网桥对此帧进行过滤，不转发该帧，如图 3-69 所示。

图 3-69 过滤（不转发）


MAC address:00e0.fcaa.aaaa
MAC address:00e0.fcbb.bbbb
Host A
Host B
源地址
目标地址
00e0.fcaa.aaaa
00e0.fcbb.bbbb
网段1
网桥表
MAC地址
接口
00e0.fcaa.aaaa
1
00e0.fcbb.bbbb
1
00e0.fccc.cccc
2
00e0.fcdd.dddd
2
网桥接口1
网桥
网桥接口2
网段2
源地址
目标地址
00e0.fcaa.aaaa
00e0.fccc.cccc
Host C
Host D
MAC address:00e0.fccc.cccc
MAC address:00e0.fcdd.dddd


Host A
Host B
源地址
目标地址
00e0.fcaa.aaaa
00e0.fccc.cccc
网段1
网桥表
MAC地址
接口
00e0.fcaa.aaaa
1
00e0.fcbb.bbbb
1
00e0.fccc.cccc
2
00e0.fcdd.dddd
2
网桥接口1
网桥
网桥接口2
网段2
Host C
Host D
MAC address:00e0.fccc.cccc

若 Host A 向 Host C 发送以太网帧，网桥通过查找网桥表知道 Host C 与网桥接口 2 对应，就将该帧从接口 2 转发，如图 3-68 所示。

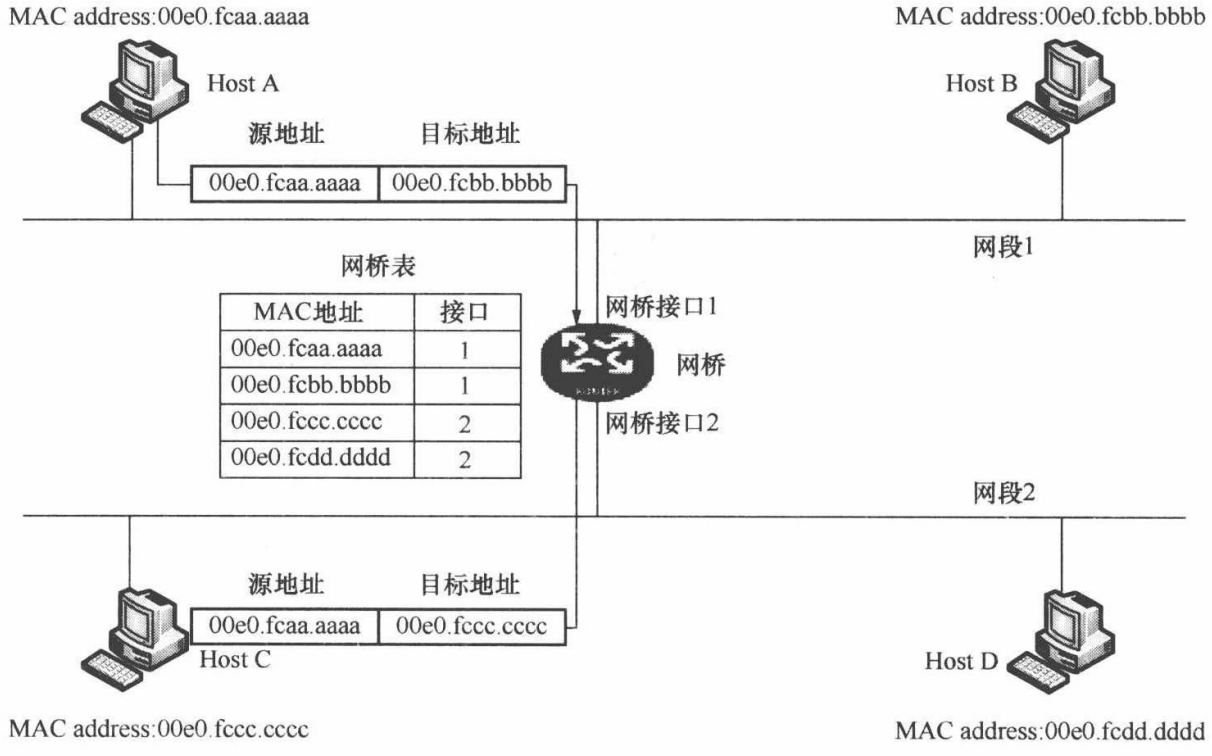


图 3-68 转发

若 Host A 向 Host B 发送以太网帧，因 Host B 与 Host A 在同一个物理网段上，网桥对此帧进行过滤，不转发该帧，如图 3-69 所示。

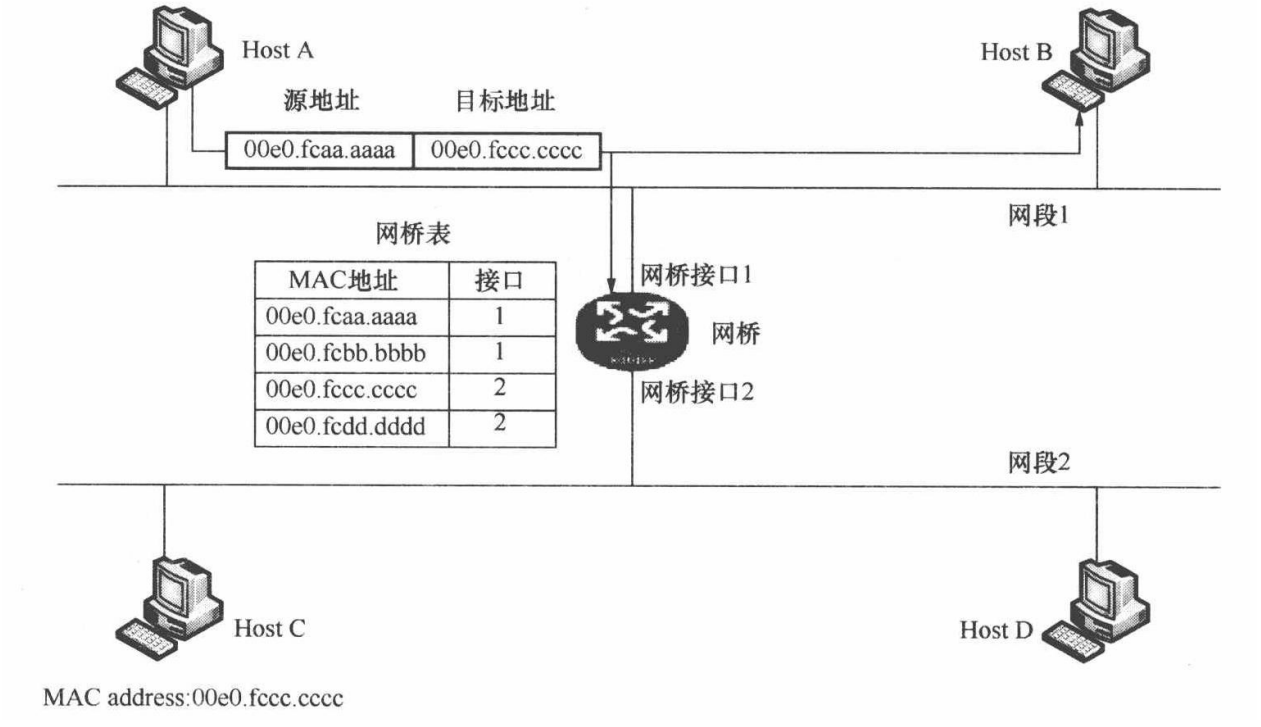


图 3-69 过滤（不转发）

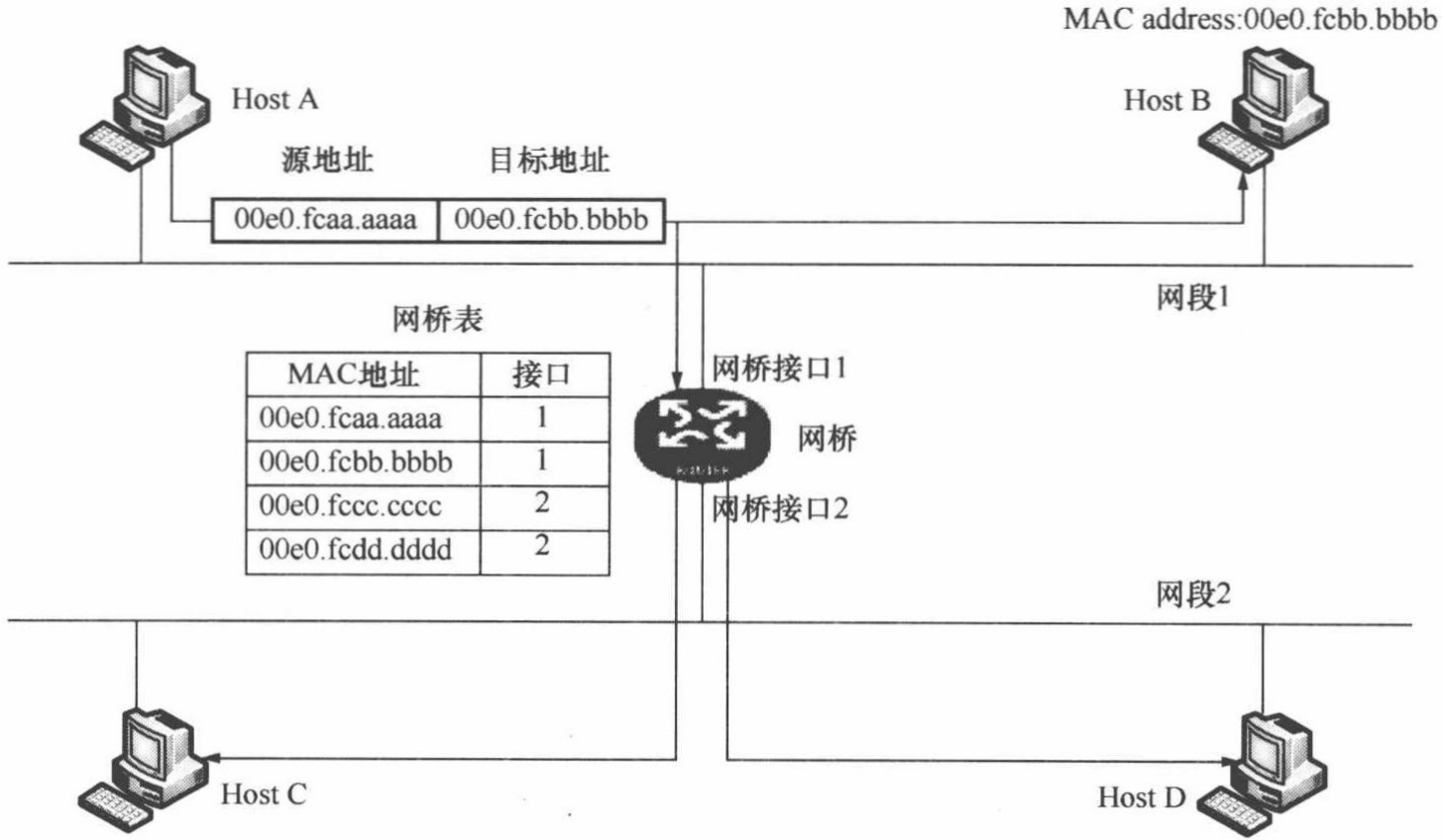
若 Host A 向 Host C 发送以太网帧，而在网桥地址表中未找到关于 Host C 的 MAC 地址与接口的对应关系，网桥就会向除接收该帧的接口以外的其他接口进行转发，如图 3-70 所示。

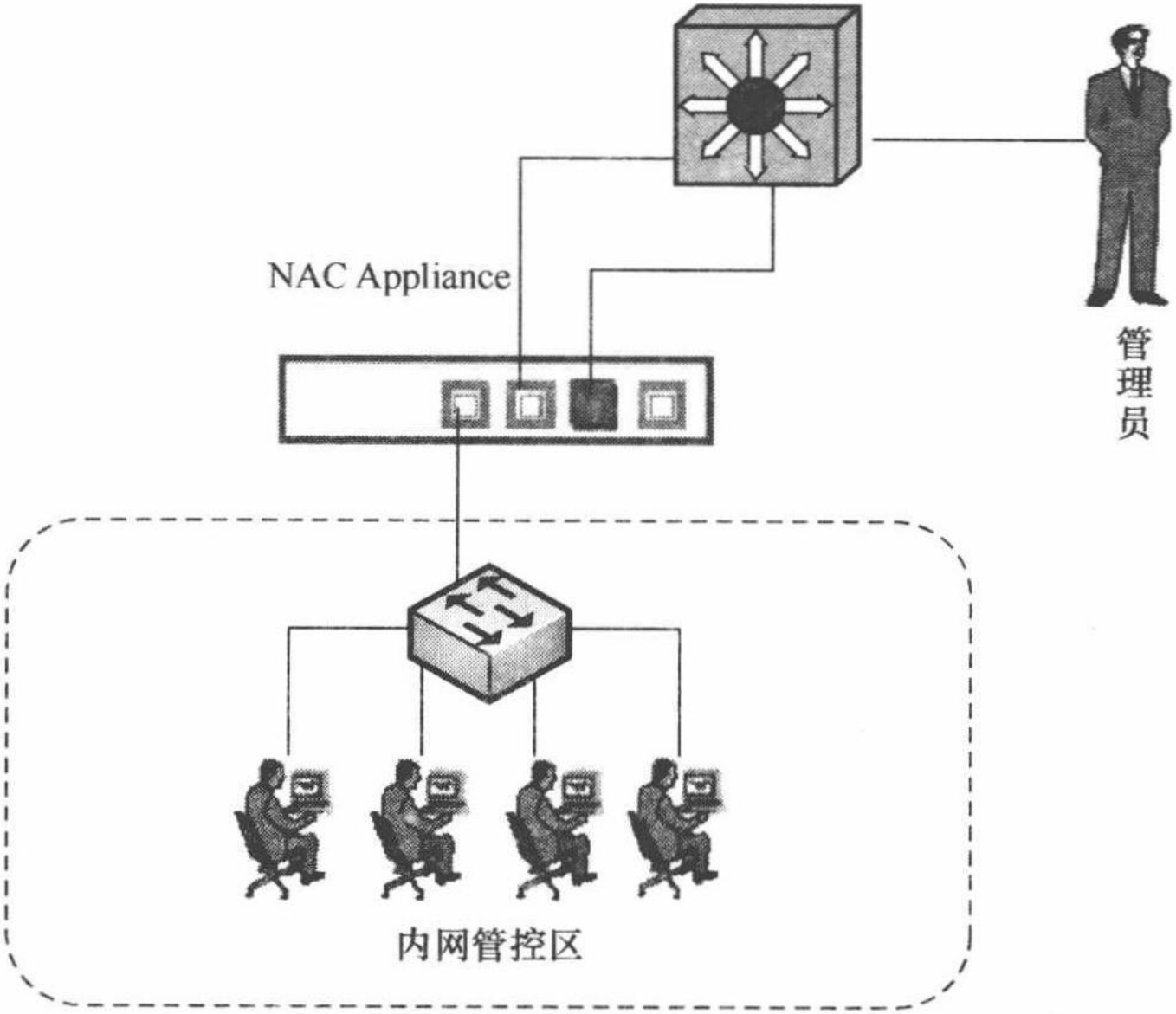
图 3-70　网桥表中未找到匹配 MAC 地址的情况

3. 实例分析

现在以实际环境中比较典型的一种接线方式来描述透明网桥准入架构的实现过程，如图 3-71 所示。

图 3-71　透明网桥准入架构应用实例


MAC address:00e0.fcbb.bbbb
Host A
Host B
源地址
目标地址
00e0.fcaa.aaaa
00e0.fcbb.bbbb
网段1
网桥表
MAC地址
接口
00e0.fcaa.aaaa
1
00e0.fcbb.bbbb
1
00e0.fccc.cccc
2
00e0.fcdd.dddd
2
网桥接口1
网桥
网桥接口2
网段2
Host C
Host D
MAC address:00e0.fcdd.dddd


NAC Appliance
管理员
内网管控区

若 Host A 向 Host C 发送以太网帧，而在网桥地址表中未找到关于 Host C 的 MAC 地址与接口的对应关系，网桥就会向除接收该帧的接口以外的其他接口进行转发，如图 3-70 所示。

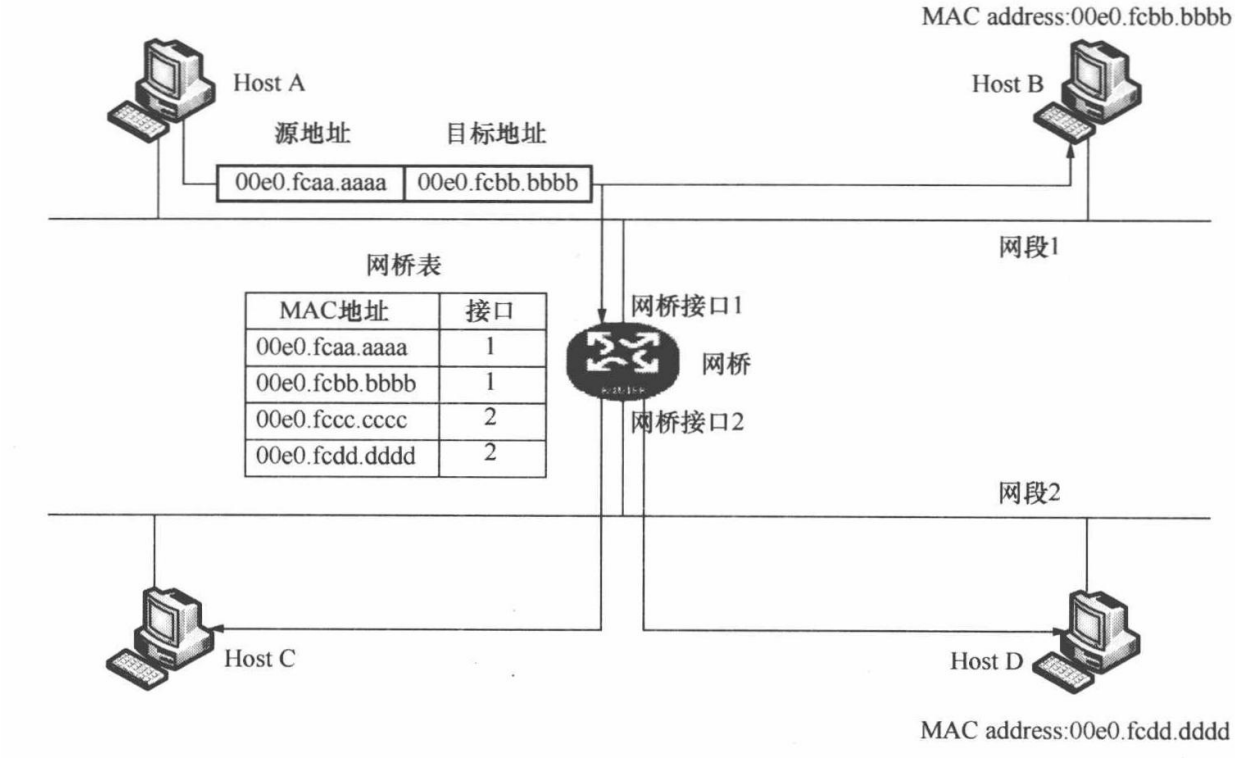


图 3-70　网桥表中未找到匹配 MAC 地址的情况

3. 实例分析

现在以实际环境中比较典型的一种接线方式来描述透明网桥准入架构的实现过程，如图 3-71 所示。

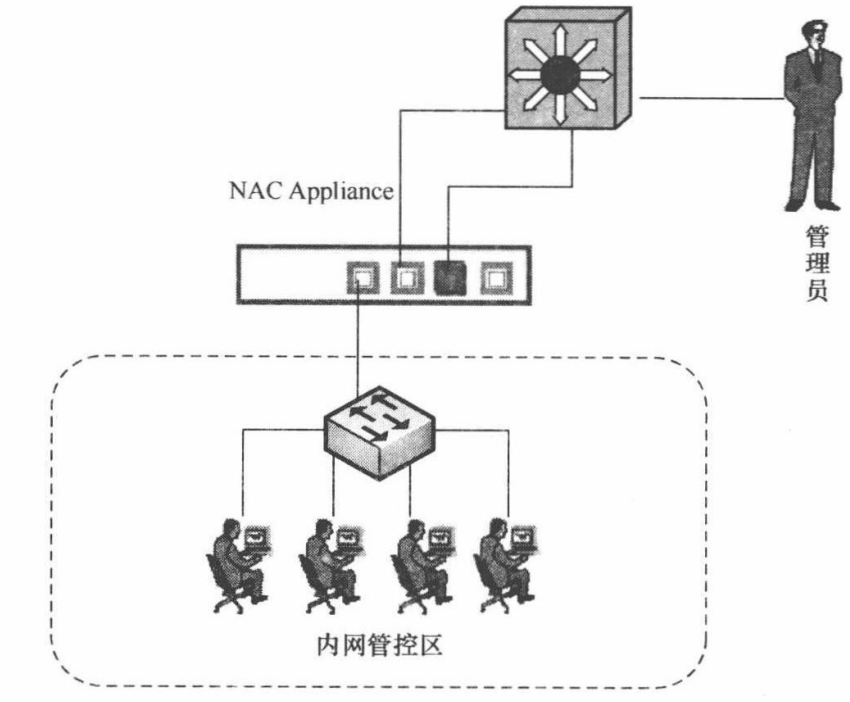


图 3-71　透明网桥准入架构应用实例

1）内部的 ACL

在 NAC Appliance 的内部默认放开了 4 种流量。

① DHCP 请求，所有设备首先是肯定能够拿到 IP 地址的。

② ARP 广播（2 层数据包，不会被过滤），设备首先会掌握到网络中的整体 IP 情况。

③ DNS 请求，所有设备都被允许进行 DNS 查询。

④ 访问 NAC Appliance 认证及安检地址端口的所有流量都会被放过。

2）数据走向

所有非访问安检页面的流量分两类进行处理。

① 非 HTTP 请求数据——直接丢弃（但首先遵循内部的 ACL）。

② HTTP 请求数据：被重定向往安检页面，从 0 口入，从 1 口出，通过核心交换最后到达安检页面进行安检。

4. 主要特点

透明网桥网络准入技术主要特点如表 3-8 所示。

表 3-8 透明网桥网络准入技术主要特点

NAC 体系	对应参数	备注
架构组成	Agent（可选） + NAC Appliance	客户端模式是可选的，如果用户需要较完善的安全检查和控制功能，可以加装客户端或控件； 这是唯一一个不需要交换设备或路由设备做联动的 NAC 方案
支持环境	任意环境	
旁路部署	×	Total in-line
无客户端支持	√	
交换机配置量	无	
接入层端口级控制	×	保护特定区域的控制
Hub 接入控制	√	
http 快捷性	√	由于可以选择放通部分流量，因此能够兼容 DHCP 环境，可以进行 Web 重定向引导
系统资源（内存）占用	小	无客户端的优势在这里体现出来了
来宾管理	好	能够进行 Web 引导，因此十分友好
稳定性	依据 NAC Appliance 而定	不同厂商的网桥设备稳定性不一样
兼容性	好	完全不依赖网络环境
防单点故障	视设备本身硬件架构而定	能够利用硬件设备本身的特性实现逃生。例如 bypass、watchdog 等

5. 配置方法

这里以 H3C 设备为例，介绍一下透明网桥的基本配置方法。

1）配置网桥地址表

一般情况下，网桥地址表根据该透明网桥获取的 MAC 地址和接口的对应关系动态生成，但管理员也可以手工配置一些静态地址表项，并且永远不会老化，配置网桥地址表命令如图 3-72 所示。

操作	命令	说明
进入系统视图	**system-view**	-
打开动态地址学习功能	**bridge** *bridge-set* **learning**	可选 缺省情况下，动态地址学习功能打开，允许所有网桥组向地址表中添加动态地址表项
配置静态地址表项	**bridge** *bridge-set* **mac-address** *mac-address* { **deny** | **permit** } [**disw** | **interface** *interface-type interface-number*]	可选 缺省情况下，没有配置静态地址表项
配置动态地址表的老化时间	**bridge aging-time** *seconds*	可选 缺省情况下，动态地址表的老化时间为 300 s

图 3-72　配置网桥地址表命令

动态地址表的老化时间是指该表项从地址表中删除之前的生存时间，动态地址表项在地址表中保持的时间超过老化时间后，系统就将该表项从网桥地址表中删除。

2）配置网桥路由功能

网桥路由功能提供了一种结合路由和桥接的转发方法。对于指定的协议数据，如果是在网桥端口之间进行通信，则进行桥接转发；如果是需要与非网桥组内的网络进行通信，则可以进行网络协议的路由转发。当集成的路由和桥接功能没有激活时，所有的协议数据只能够进行桥接处理。当集成的路由和桥接功能被激活后，就可以指定某种协议的报文既可以做桥接，又可以进行路由处理，通过命令配置进行灵活的切换，如图 3-73 所示。

bridge-template 接口是一个虚拟的选路接口，可以配置各种网络层的属性。对于每个网桥组来说，只能有一个 bridge-template 接口。bridge-template 接口的编号是它所代表的网桥组的编号。缺省情况下，如果已经有以太网接口加入 bridge-template 接口对应的网桥组，bridge-template 接口将借用网桥组中任意以太网接口的 MAC 地址。如果没有以太网接口加入 bridge-template 接口对应的网桥组，bridge-template 接口将使用系统默认的 MAC 地址（前 5 字节由设备决定，以设备的实际情况为准；后 1 字节为接口对应的网桥组号）。

当在两台或两台以上设备上启用网桥组号相同的网桥组，并创建相应的 bridge-template 接口，且均没有以太网接口加入网桥组，则这些 bridge-template

操作	命令	说明
进入系统视图	**system-view**	-
使能网桥路由功能	**bridge routing-enable**	必选 缺省情况下，禁用网桥的路由功能
创建 bridge-template 接口，并进入 bridge-template 接口视图，将指定的网桥组连接到路由的网络中	**interface bridge-template** *bridge-set*	必选 缺省情况下，未配置 bridge-template 接口
配置 bridge-template 接口的 MAC 地址	**mac-address** *mac-address*	可选
退回系统视图	**quit**	-
配置网桥组对网络层协议的路由或桥接功能	**bridge** *bridge-set* **routing** { **ip** | **ipx** }	可选 缺省情况下，使能所有协议的桥接功能
	bridge *bridge-set* **bridging** { **ip** | **ipx** | **others** }	

图 3-73 配置网桥路由功能

接口将使用完全相同的默认 MAC 地址。造成 MAC 地址冲突，此时可以在不同 bridge-template 接口上配置不同的 MAC 地址。

3）网桥显示和维护

在完成上述配置后，在任意视图下执行 display 命令可以显示网桥配置后的运行情况，通过查看显示信息验证配置的效果。在用户视图下，执行 reset 命令可以清除相关信息。相关命令如图 3-74 所示。

操作	命令
显示网桥组信息	**display bridge information** [**bridge-set** *bridge-set*]
显示 bridge-template 虚拟接口	**display interface bridge-template** [*interface-number*]
显示 MAC 地址转发表的信息	**display bridge address-table** [**bridge-set** *bridge-set* | **dlsw** | **interface** *interface-type interface-number* | **mac** *mac-address*] [**dynamic** | **static**]
显示网桥组中接口上的流量统计数据	**display bridge traffic** [**bridge-set** *bridge-set* / **dlsw** / **interface** *interface-type interface-number*]
清除 MAC 地址转发表	**reset bridge address-table** [**bridge-set** *bridge-set* | **dlsw** | **interface** *interface-type interface-number*]
清除网桥组中接口上的流量统计数据	**reset bridge traffic** [**bridge-set** *bridge-set* / **dlsw** / **interface** *interface-type interface-number*]

图 3-74 网桥显示和调试

4）VLAN 透明网桥配置方法

如图 3-75 所示，Router A 和 Router B 之间用一条网线连接，这两台路由器分别配置透明网桥功能，通过子接口上使用网桥功能，使得用路由器搭建的两个网桥都能相互访问。

具体配置方法如下：

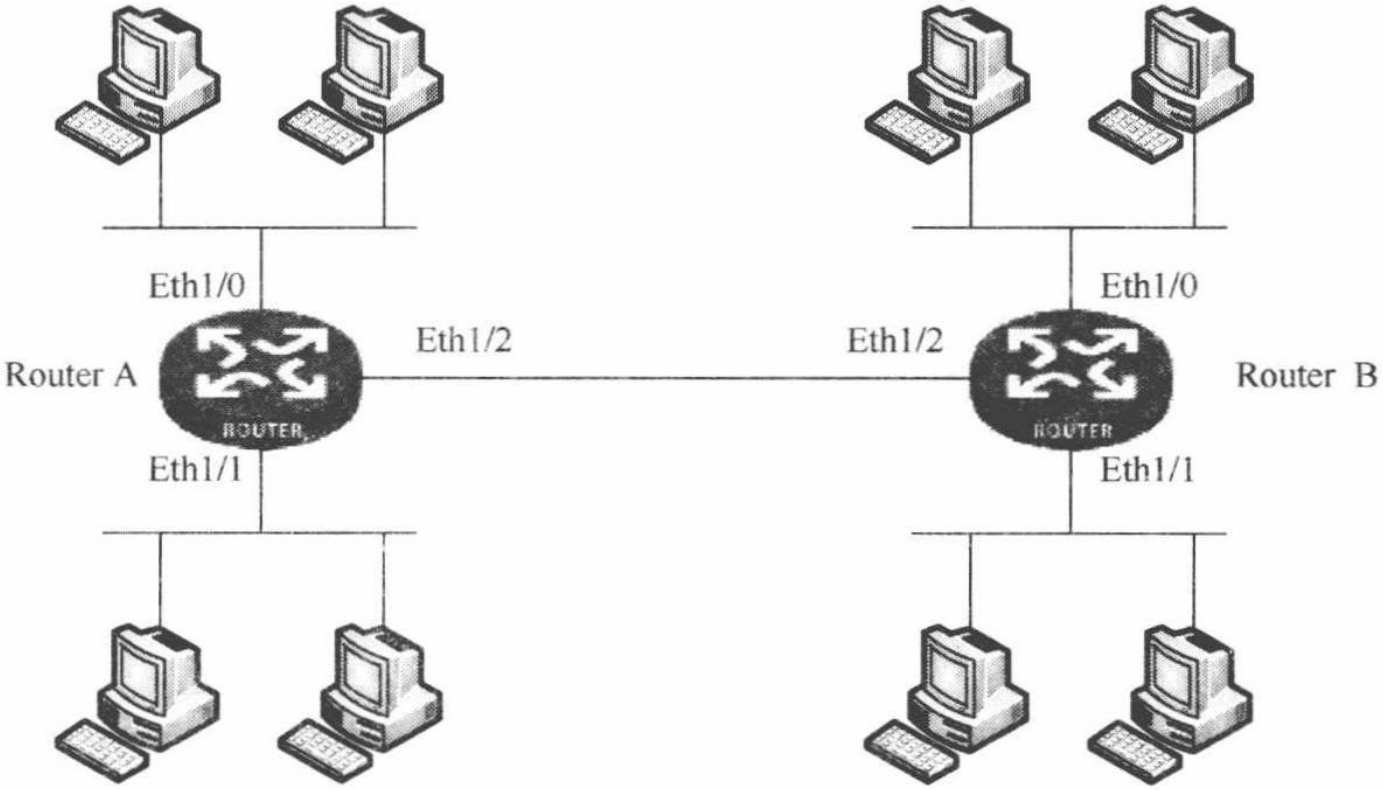
图 3-75　配置 VLAN 透明网桥组网图

(1) 配置 Router A。

<RouterA> system-view
[RouterA] bridge enable
[RouterA] bridge 1 enable
[RouterA] bridge 2 enable
[RouterA] interface ethernet 1/0
[RouterA-Ethernet1/0] bridge-set 1
[RouterA-Ethernet1/0] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] bridge-set 2
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2.1
[RouterA-Ethernet1/2.1] VLAN-type dot1q vid 1
[RouterA-Ethernet1/2.1] bridge-set 1
[RouterA-Ethernet1/2.1] quit
[RouterA] interface ethernet 1/2.2
[RouterA-Ethernet1/2.2] VLAN-type dot1q vid 2
[RouterA-Ethernet1/2.2] bridge-set 2

(2) 配置 Router B。

<RouterB> system-view
[RouterB] bridge enable
[RouterB] bridge 1 enable
[RouterB] bridge 2 enable
[RouterB] interface ethernet 1/0


Eth1/0
Router A
Eth1/2
Eth1/2
Eth1/0
Router B
Eth1/1
Eth1/1

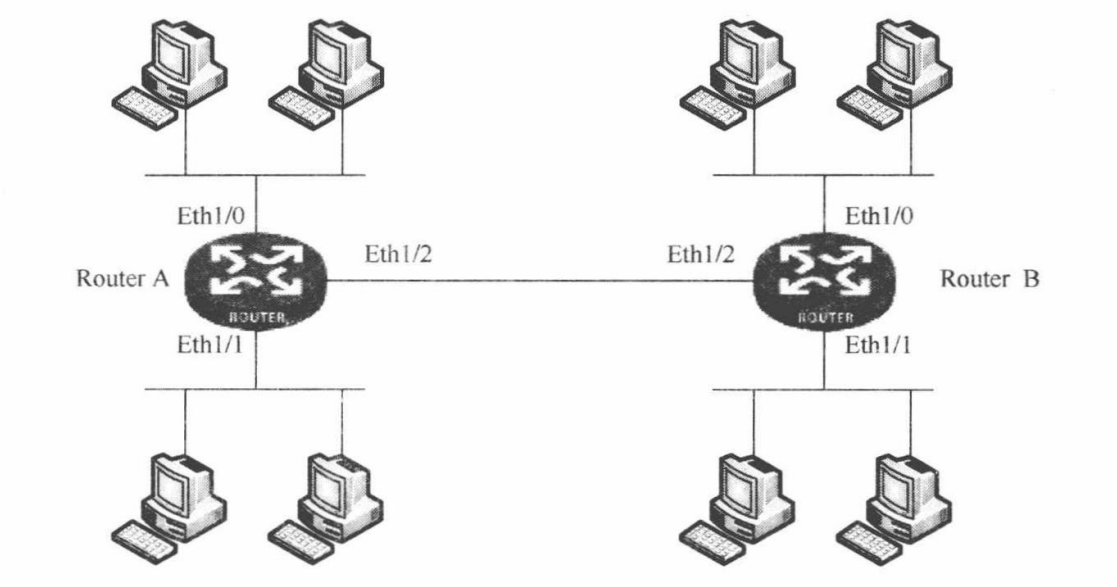


图 3-75　配置 VLAN 透明网桥组网图

(1) 配置 Router A。

<RouterA> system-view
[RouterA] bridge enable
[RouterA] bridge 1 enable
[RouterA] bridge 2 enable
[RouterA] interface ethernet 1/0
[RouterA-Ethernet1/0] bridge-set 1
[RouterA-Ethernet1/0] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] bridge-set 2
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2.1
[RouterA-Ethernet1/2.1] VLAN-type dot1q vid 1
[RouterA-Ethernet1/2.1] bridge-set 1
[RouterA-Ethernet1/2.1] quit
[RouterA] interface ethernet 1/2.2
[RouterA-Ethernet1/2.2] VLAN-type dot1q vid 2
[RouterA-Ethernet1/2.2] bridge-set 2

(2) 配置 Router B。

<RouterB> system-view
[RouterB] bridge enable
[RouterB] bridge 1 enable
[RouterB] bridge 2 enable
[RouterB] interface ethernet 1/0

[RouterB-Ethernet1/0] bridge-set 1
[RouterB-Ethernet1/0] quit
[RouterB] interface ethernet 1/1
[RouterB-Ethernet1/1] bridge-set 2
[RouterB-Ethernet1/1] quit
[RouterB] interface ethernet 1/2.1
[RouterB-Ethernet1/2.1] VLAN-type dot1q vid 1
[RouterB-Ethernet1/2.1] bridge-set 1
[RouterB-Ethernet1/2.1] quit
[RouterB] interface ethernet 1/2.2
[RouterB-Ethernet1/2.2] VLAN-type dot1q vid 2
[RouterB-Ethernet1/2.2] bridge-set 2

第 4 章　网络准入控制技术解决方案

目前，从厂商方面来看，有代表性的新型终端安全接入技术解决方案主要有以下几种：由主流网络设备厂商 Cisco 提出的网络准入控制（Cisco Network Admission Control，C-NAC）技术，以及 H3C 提出的准入技术方案端点准入防御（Endpoint Admission Defense，EAD）技术；由操作系统厂商微软提出的网络接入保护（Network Access Protection，NAP）技术；由安全厂商可信计算组织（Trusted Computing Group，TCG）提出的可信网络连接（Trusted Network Connect，TNC）技术和赛门铁克提出的赛门铁克端点防护（Symantec Endpoint Protection，SEP）技术和独立第三方 NAC 软件厂商盈高科技提出来的基于 L2-OOB-MVG（Layer2 Out-Of-Band Multi-Virtual Gateway）框架的 ASM（Admission Standard Management）技术等。上述终端安全接入技术都会在终端接入网络之前对其进行身份认证和完整性度量，只有终端可信并且遵循访问策略时才允许其接入网络。

4.1　C-NAC 技术解决方案

Cisco 的网络安全准入控制（Cisco Network Access Control，C-NAC）由 Cisco 在 2004 年开始推向市场。C-NAC 的设计目标是要防止病毒和蠕虫等新兴黑客技术对企业安全造成危害。在主机接入网络之前，C-NAC 能够检查它是否符合企业最新制定的防病毒和操作系统补丁策略，有问题的主机将被隔离或限制网络接入范围，直到修复为止。Cisco 在设计 C-NAC 标准时，充分发挥其在网络设备方面的专业技术和强大实力，各个功能都与 Cisco 的路由器及交换机等网络设备进行了紧密融合。

4.1.1　C-NAC 架构

C-NAC 解决方案中系统组件通常被设计的主要包括：客户端软件、网络准入控制设备、认证与策略服务器。它们的作用分别如下：

（1）客户端软件。主要负责对接入的终端进行 802.1x 接入认证与健康检查。

（2）网络准入控制设备。可以是路由器、交换机、无线接入点和安全网关，这些设备接受终端委托，然后将信息传送到策略服务器，并实施由策略服务器传回来的相应的准入控制决策：允许、拒绝、隔离或限制。

（3）认证与策略服务器。认证服务器对终端进行用户认证，策略服务器负责评估终端安全信息，并决定应该使用哪种接入策略。

根据准入控制点位置的不同，网络安全准入控制主要分为两大类：一类是在网络接入设备处进行控制，另一类是在网关处进行控制。网关型准入控制的优点是对网络接入设备没有品牌限制，通用性强；缺点是只对网络出口进行了控制，没有对接入层进行控制，使得病毒、蠕虫仍然可以进入内部网络；同时，控制网关是网络的性能瓶颈。

C-NAC 的实现架构如图 4-1 所示，它主要由 3 部分组成：网络接入设备（Host Attempting Net-work Access）、网络访问设备（Network Access Device，NAD）和 Cisco 策略服务器（Cisco Policy Server，CPS）。

图 4-1 C-NAC 架构示意图

各部分的具体功能如下。

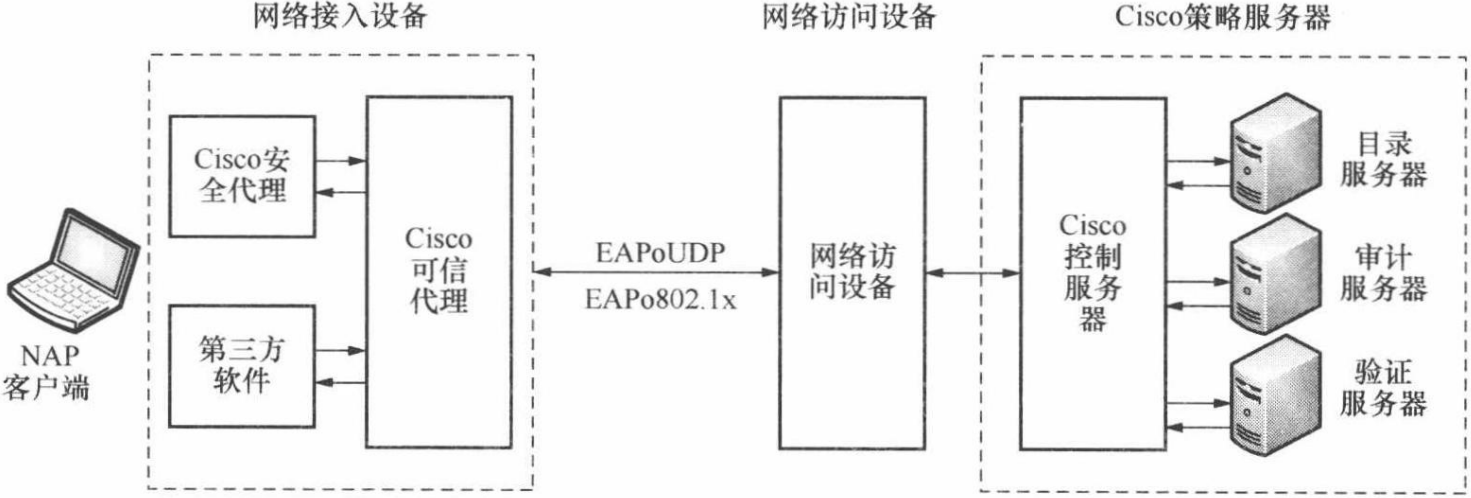
1）网络接入设备

负责从终端的安全解决方案中收集终端的操作系统补丁、病毒库版本等安全状态信息，并通过 802.1x 上的可扩展认证协议（Extensible Authentication Protocol，EAP）或 EAPoUDP（EAP over UDP）协议将安全状态信息传递到网络访问设备。它包含下列组件。

① Cisco 安全代理（Cisco Security Agent，CSA）。集合了如主机入侵防护、分布式防火墙、操作系统完整性等安全功能来为终端提供安全保护，并与 Cisco 可信代理共同加强对终端的保护。

② 支持 NAC 的应用（NAC Enabled Application）。支持 NAC 的第三方软件。

③ Cisco 可信代理（Cisco Trust Agent，CTA）。负责发起网络接入请求，收集 CSA 和第三方软件报告的安全状态信息，并提交给网络访问设备。CTA 维护由开发商和应用类型标识的已注册的记录，每个开发商和应用类型对应一个 PP。CTA 分解网络与 PP 间的状态证书请求与状态通知。它同时能够判断 PP 的中状态是否变化，使用多种 EAP 传输机制通知网络访问设备。CTA 不翻译网络和 PP 间传递的状态证书和通知。CTA 只是对 PP 与网络之间的请求和响应进行分解和组装。PP 传递的状态可以包括主机操作系统、防病毒、防火墙、入侵检测系统等应用的状态，具体状态信息可以包括某厂商的防病毒应用，某扫描引擎


网络接入设备
网络访问设备
Cisco策略服务器
Cisco安全代理
第三方软件
Cisco可信代理
NAP客户端
EAPoUDP
EAPo802.1x
网络访问设备
Cisco控制服务器
目录服务器
审计服务器
验证服务器

根据准入控制点位置的不同，网络安全准入控制主要分为两大类：一类是在网络接入设备处进行控制，另一类是在网关处进行控制。网关型准入控制的优点是对网络接入设备没有品牌限制，通用性强；缺点是只对网络出口进行了控制，没有对接入层进行控制，使得病毒、蠕虫仍然可以进入内部网络；同时，控制网关是网络的性能瓶颈。

C-NAC 的实现架构如图 4-1 所示，它主要由 3 部分组成：网络接入设备（Host Attempting Net-work Access）、网络访问设备（Network Access Device，NAD）和 Cisco 策略服务器（Cisco Policy Server，CPS）。

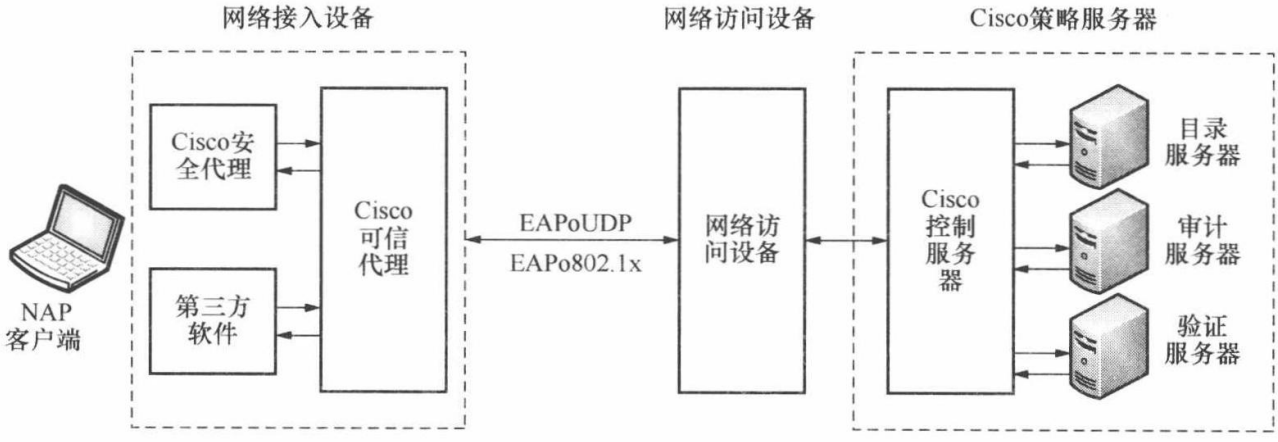


图 4-1 C-NAC 架构示意图

各部分的具体功能如下。

1）网络接入设备

负责从终端的安全解决方案中收集终端的操作系统补丁、病毒库版本等安全状态信息，并通过 802.1x 上的可扩展认证协议（Extensible Authentication Protocol，EAP）或 EAPoUDP（EAP over UDP）协议将安全状态信息传递到网络访问设备。它包含下列组件。

① Cisco 安全代理（Cisco Security Agent，CSA）。集合了如主机入侵防护、分布式防火墙、操作系统完整性等安全功能来为终端提供安全保护，并与 Cisco 可信代理共同加强对终端的保护。

② 支持 NAC 的应用（NAC Enabled Application）。支持 NAC 的第三方软件。

③ Cisco 可信代理（Cisco Trust Agent，CTA）。负责发起网络接入请求，收集 CSA 和第三方软件报告的安全状态信息，并提交给网络访问设备。CTA 维护由开发商和应用类型标识的已注册的记录，每个开发商和应用类型对应一个 PP。CTA 分解网络与 PP 间的状态证书请求与状态通知。它同时能够判断 PP 的中状态是否变化，使用多种 EAP 传输机制通知网络访问设备。CTA 不翻译网络和 PP 间传递的状态证书和通知。CTA 只是对 PP 与网络之间的请求和响应进行分解和组装。PP 传递的状态可以包括主机操作系统、防病毒、防火墙、入侵检测系统等应用的状态，具体状态信息可以包括某厂商的防病毒应用，某扫描引擎

版本被激活，某版本的签名文件。

2）网络访问设备

负责将 CTA 收集的终端安全状态信息传递给策略服务器，以供其做出访问控制决策，并从策略服务器获得访问控制决策。

3）Cisco 策略服务器

由 Cisco 安全访问控制服务器（Cisco Secure Access Control Server，ACS）和策略服务器决定点（Policy Server Decision Points）两部分构成。

① 控制服务器 ACS。根据客户端认证信息、安全健康状态信息，决定是否允许计算机进入网络，并根据预先设定的策略，向网络访问设备发出访问控制决策，这一过程需要依靠策略服务器决定点的建议。ACS 也就是 AAA 服务器，ACS 除了进行身份认证外，还对主机的状态证书进行授权，它将策略映射为网络访问规则，供 NAD 执行。ACS 能够将授权决定权转交给外部状态验证服务器执行。PVS 从 AAA 或其他 PVS 接收状态证书验证请求，将状态证书与安全策略比较或将状态证书传递给其他的 PVS，将状态验证的结果返回给 AAA。修补服务器中包含更新的操作系统、安全包、宿主代理软件和其他软件组件。当宿主机不符合安全策略规则时，通过 URL 重定向，用户被链接到修补服务器。审计服务器主要执行脆弱性评估（VA）。VA 技术包括由 802.1x 或 CTA 提供的网络扫描技术、远程注册技术和基于浏览器的代理技术。当审计服务器完成审计过程，它向 ACS 报告宿主机状态，同时 ACS 也周期性地从审计服务器抽取审计决定。

② 策略服务器决定点。配合 ACS 对客户端提交的不同信息分别进行认证。

4.1.2　C-NAC 的工作流程

以下为 C-NAC 的工作流程。

Step1：首先由终端主机提出网络接入请求，NAD 收到请求后在 CTA 和 ACS 之间建立一条通信通道。

Step2：ACS 要求终端提交安全状态信息。

Step3：CTA 收集 CSA 和第三方软件提交的安全状态信息后，通过 NAD 传递给 ACS。

Step4：ACS 在策略决策服务点的配合下对这些信息进行验证，并决定是否授予终端网络访问权。

Step5：NAD 根据策略决策点的访问策略对终端实施控制，允许或拒绝终端接入网络。

C-NAC 作为一套完整的准入控制技术标准，虽具备其先进性，但也同样存在局限。主要体现在不支持非 Cisco 网络设备上。由于 Cisco 的行业背景，其 NAC 标准基于自己的网络设备实现。对于已采用其他厂商网络设备的环境，无法良好的部署 C-NAC。另外由于支持 C-NAC 的网络设备往往属于高端设备，这使得系统部署成本及其高昂。同时，Cisco 在操作系统层级的安全评估与微软还

存在一些差距，目前的评估主要包括防病毒客户端的状态。

4.2 NAP 技术解决方案

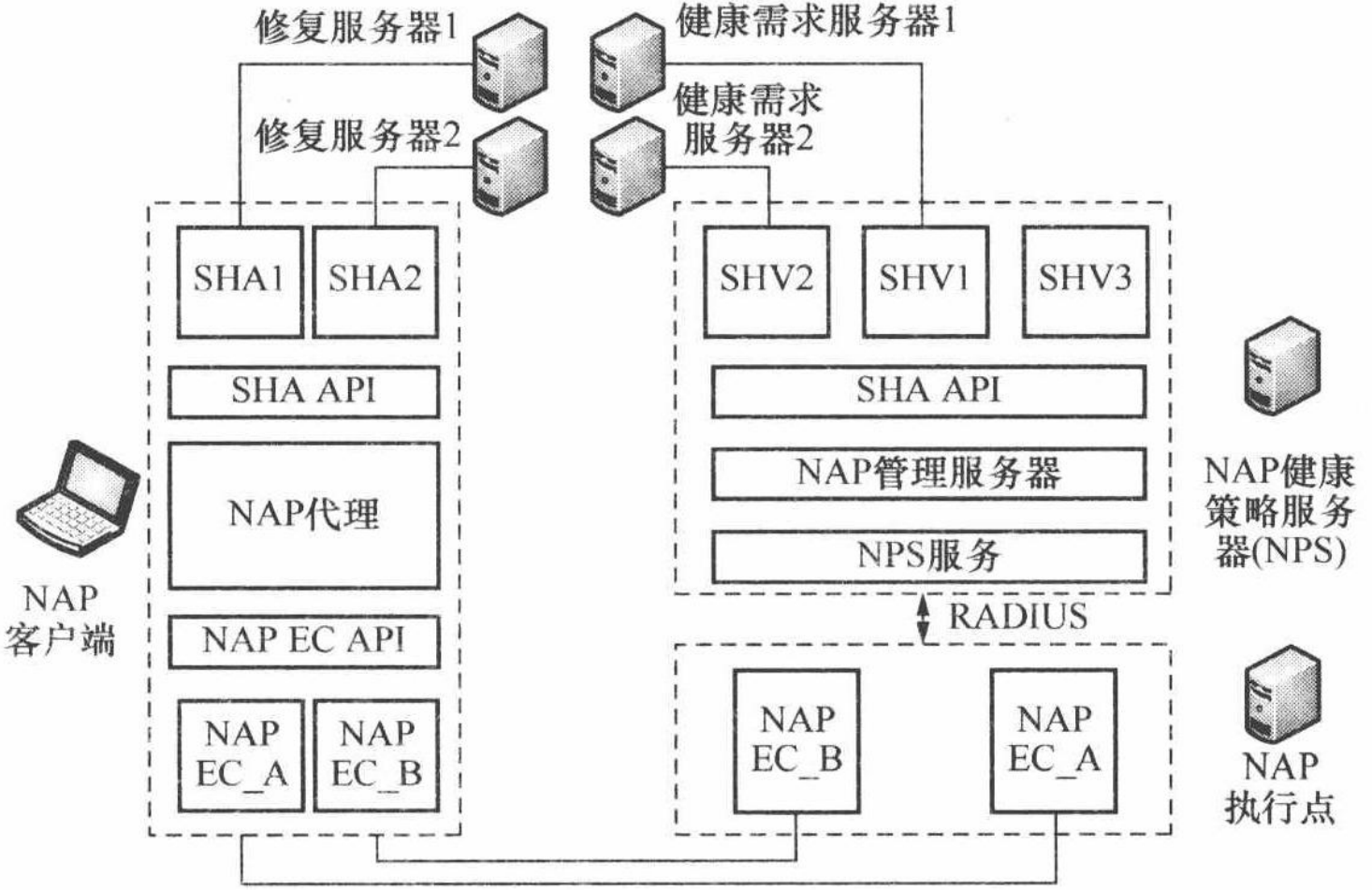
NAP 于 2006 年年底，随着微软的 Microsoft Windows Server “Longhorn” 和 Windows Vista 操作系统一起推向市场。NAP 是微软为其目前的主流操作系统 Windows Vista、Windows7、Windows Server 2008 设计的新的一套操作系统组件，它充分发挥了微软在操作系统领域的优势，它是内置于 Windows Vista 及 Windows Server 2008 操作系统中的安全机制，可以在终端计算机访问网络时提供系统平台健康校验。其目标是让管理者可以监视任何试图接入网络的计算机的安全状态，并确保接入的计算机都具有符合健康策略的安全防范措施。不符合健康策略的电脑，将被接入到一个受限的网络环境，管理者可以在这个网络环境中存储一些安全软件，帮助这些安全性较差的计算机提高到符合要求的安全水平。

NAP 平台是一套提供了策略认证、网络访问控制、自动补救以及动态适应等功能的架构。NAP 平台提供了一套完整性校验的方法，来判断接入网络的终端计算机的健康状态，对不符合健康策略需求的终端限制其网络访问权限。为了预防不符合企业安全策略的计算机接入网络，NAP 可以通过批准连接与否而加以控制，这些不符合安全策略的状态包括：未启动自动更新、未启用个人防火墙、反病毒软件定义码超过期限而未更新等。

4.2.1 NAP 架构

NAP 的架构如图 4-2 所示，它由 3 个实体构成，分别为：NAP 客户端（NAP Clients）、NAP 执行点（NAP enforcement points）和 NAP 健康策略服务器（NAP health policy server）。

图 4-2 NAP 架构示意图


修复服务器1
健康需求服务器1
修复服务器2
健康需求
服务器2
SHA1
SHA2
SHA API
NAP代理
NAP EC API
NAP
EC_A
NAP
EC_B
SHV2
SHV1
SHV3
SHA API
NAP管理服务器
NPS服务
RADIUS
NAP
EC_B
NAP
EC_A
NAP
客户端
NAP健康
策略服务
器(NPS)
NAP
执行点

存在一些差距，目前的评估主要包括防病毒客户端的状态。

4.2 NAP 技术解决方案

NAP 于 2006 年年底，随着微软的 Microsoft Windows Server “Longhorn” 和 Windows Vista 操作系统一起推向市场。NAP 是微软为其目前的主流操作系统 Windows Vista、Windows7、Windows Server 2008 设计的新的一套操作系统组件，它充分发挥了微软在操作系统领域的优势，它是内置于 Windows Vista 及 Windows Server 2008 操作系统中的安全机制，可以在终端计算机访问网络时提供系统平台健康校验。其目标是让管理者可以监视任何试图接入网络的计算机的安全状态，并确保接入的计算机都具有符合健康策略的安全防范措施。不符合健康策略的电脑，将被接入到一个受限的网络环境，管理者可以在这个网络环境中存储一些安全软件，帮助这些安全性较差的计算机提高到符合要求的安全水平。

NAP 平台是一套提供了策略认证、网络访问控制、自动补救以及动态适应等功能的架构。NAP 平台提供了一套完整性校验的方法，来判断接入网络的终端计算机的健康状态，对不符合健康策略需求的终端限制其网络访问权限。为了预防不符合企业安全策略的计算机接入网络，NAP 可以通过批准连接与否而加以控制，这些不符合安全策略的状态包括：未启动自动更新、未启用个人防火墙、反病毒软件定义码超过期限而未更新等。

4.2.1 NAP 架构

NAP 的架构如图 4-2 所示，它由 3 个实体构成，分别为：NAP 客户端（NAP Clients）、NAP 执行点（NAP enforcement points）和 NAP 健康策略服务器（NAP health policy server）。

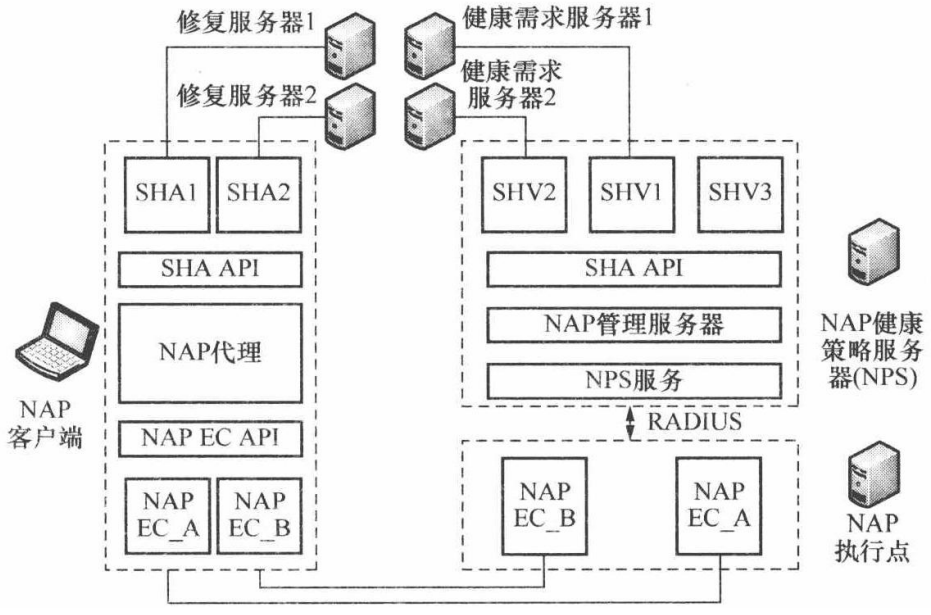


图 4-2 NAP 架构示意图

各个实体的功能如下。

1）NAC 客户端

该实体为支持 NAP 平台的计算机。NAC 客户端自下而上包含 3 个组件。

（1）NAP 执行客户端（NAP Enforcement Clients，NAP EC）：相当于网络访问请求者，不同的 NAP EC 对应于不同类型的执行点。NAP 客户执行组件请求对网络的访问，传递系统当前健康状态给 NAP 服务器，为 NAP 客户端体系结构中的其他组件指示 NAP 客户的受限或非受限网络访问状态。在 Windows 中内嵌的客户组件包括 IPSec NAP EC、EAPHost NAP、VPN NAP EC 以及 DHCP NAP EC。

（2）NAP 代理（NAP Agent）：负责维护 NAP 客户端当前的健康信息，并使 NAPEC 和 SHA 之间的通信变得更加方便。主要完成以下功能：①从每个系统健康代理收集健康列表。②在需要时向执行组件提供健康列表。③当受限的网络访问状态改变时，通知健康代理组件。④存储系统健康状态，从每个系统健康代理收集状态信息。⑤将系统健康响应传递给相应的健康代理。

（3）系统健康代理（System Health Agents，SHA）：负责收集客户端的安全信息。

2）NAP 执行点

该实体处于 NAP 架构中的服务器端，它根据 NAP 健康策略服务器的决策，对请求接入的 NAP 客户端执行控制策略，准予、限制或拒绝其接入网络。基于 Windows 的 NAP 执行点包含 NAP 执行服务器（NAP Enforcement Server，NAP ES）组件。

3）NAP 健康策略服务器

该部件处于 NAP 架构中的服务器端。NAP 健康策略服务器自下而上由以下组件构成。

① NPS 服务（NPS service），负责接收认证服务器的认证请求消息，并将提取出的健康状况等信息传递给 NAP 管理服务器。

② NAP 管理服务器（NAP Administration Server），负责 NPS 服务和 SHV 之间的通信。

③ 系统健康状态验证器（System Health Validator，SHV），负责接收来自客户端 SHA 的健康状态，并为 NAP 管理服务器提供回复，每个 SHV 都和一个相对应的 SHA 匹配。

NPS 接收 RADIUS 访问请求消息，抽取健康列表，将它们传递给 NAP 管理服务组件。NAP 管理服务协调 NPS 和 SHV 间的通信。系统健康验证（SHV）组件层从 NAP 管理服务接收系统健康列表并且验证表中的系统健康状态信息与需要的系统健康状态是否一致。通过 SHV API 允许 SHVs 注册到 NAP 管理服务组件，从 NAP 管理服务组件接收系统健康列表。

4.2.2 NAP 的工作流程

以下为 NAP 的工作流程。

Step1：NAP 客户端请求接入网络，该请求通过 NAP 执行点转发给 NPS。

Step2：NPS 请求 NAP 客户端的身份信息和健康状态。

Step3：NAP 将收集的身份信息和健康状态通过 NAP 执行点传递给 NPS。

Step4：NPS 根据一定的安全策略对 NAP 客户端的身份和健康状态进行认证后，对其访问请求做出决策。

Step5：NAP 策略执行点根据 NPS 的决策，对请求接入的 NAP 客户端执行控制策略，准予、限制或拒绝其接入网络。

作为微软的产品，NAP 的优势在于与操作系统的兼容性良好、与 Windows 内置的各种安全检测机制（如补丁扫描、Windows 防火墙）配合紧密。但 NAP 也存在以下的不足。

首先，NAP 不是完善的安全评估和状态检测机制。它不能检测系统内其他安全系统，如漏洞扫描、IDS 等。NAP 的作用暂时还只是用来检查接入网络的电脑是否具有完备的补丁，是否有安全配置方面的错误等。当然也就更不可能根据 IDS、漏洞扫描等安全设施提供的报告进行检测评估。

其次，NAP 不能适应多样化的终端操作系统。微软公司出于产品换代方面的考虑，要求 NAP 服务器必须运行 Windows 2008，客户端必须运行 Windows Vista、Windows XP SP2 或 Windows Server 2008。这使得运行 Windows 2000 或者 Windows Server 2003 的终端无法利用 NAP 实现准入控制。

另外需要说明的是，由 NAC 和 NPC 的系统组成可以看出，C-NAC 和 NPC 是与 Cisco 与 Microsoft 的技术背景有着密切的联系。Cisco 是接入设备厂商，因此 C-NAC 中的接入设备占了很大的比例。NAP 则偏重在客户端代理以及接入服务（DHCP、802.1x、VPN 和 IPSee 组件）上。而且 C-NAC 与 NAP 作为技术标准，其具体实现都具有大而全的特点，通常需要多家不同供应商的软件或硬件才能构建完整解决方案，这往往导致复杂程度显著提高。由于上面提到的某些局限性，往往又不能适合实际需求。Cisco 与 Microsoft 自己也意识到了各自的不足，因此这两家公司在 2010 年波士顿举办的安全标准大会上共同发布了一份技术白皮书，宣布 C-NAC 与 NAP 将实现互操作，以实施安全策略和进行状态评估，即网络接入设备上采用 Cisco 的 C-NAC 技术，而主机客户端上则采用 Microsoft 的 NAP 技术，这样 C-NAC 与 NAP 结为同盟，从而达到两者互补的局面。

4.3 TNC 技术解决方案

2004 年 5 月，TCG 组织提出了可信网络 TNC 方案，目标是解决可信接入问

题。TNC 是通过行为可信（即计算机可信）、行为和系统完整性可信（即平台可信），结合可信计算的免疫特性，构建一个可信可控的网络平台。TNC 的特点是只制定详细规范，技术细节公开，提供一个弹性的安全架构，由于技术开放，各个厂家都可以自行设计开发兼容 TNC 的产品，并可以兼容安全芯片技术，借助于安装在客户端主机的硬件设施来确认是否发生问题，并根据硬件来监控或执行客户端安全的政策。

除此之外，基于可信计算机的方案还有可信认证网关解决方案（Trusted Authentication Gateway System，TAGS）等。总体来说，这些方案对网络终端的硬件环境要求较高，因而，其推广进程受到一定限制。而 TNC 的优势之一就是，TNC 是开放标准，TCG 组织的成员都可以对其提出自己的意见，符合标准的任何厂商产品之间可以互相调用或提供操作接口。

4.3.1　TNC 架构

TNC 标准提出的网络准入控制体系架构如图 4-3 所示，从纵向看，该架构中的 3 列代表 3 个实体，分别为：访问请求者（Access Requestor，AR）、策略执行点（Policy Enforcement Point，PEP）和策略决定点（Policy Decision Point，PDP）；从横向看，该架构中的 3 行代表 3 个抽象层次，分别为：网络访问层（Network Access Layer）、完整性评估层（Integrity Evaluation）和完整性度量层（Integrity Measurement Layer）。

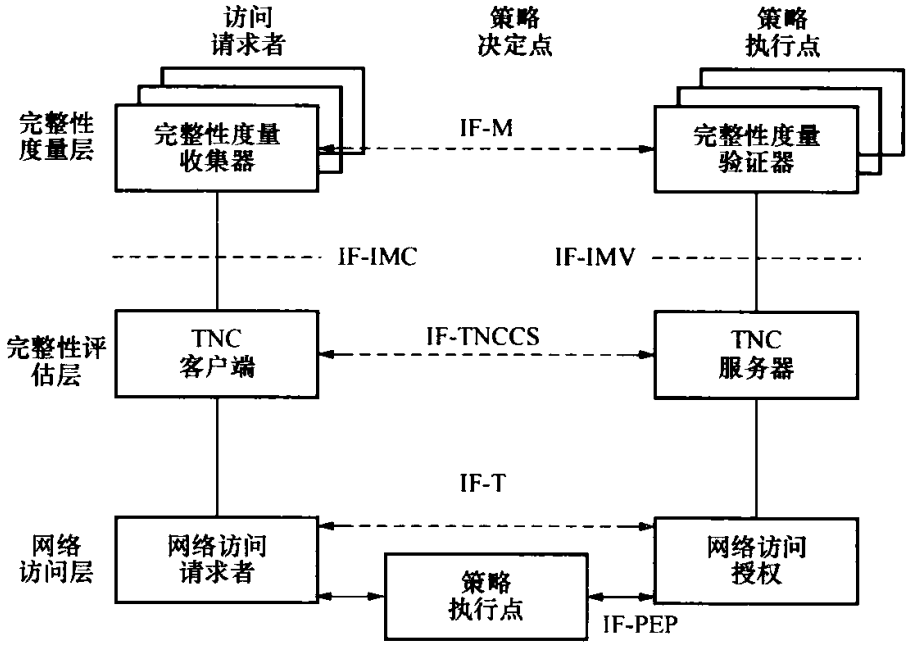


图 4-3　TNC 架构示意图

下面将介绍各个实体的具体功能。

1. 访问请求者

请求访问受保护网络的实体，其自底向上包含如下组件。

（1）网络访问请求者（Network Access Request，NAR）。运行在 AR 上的一个软件，负责协商和建立网络连接。为建立不同的网络连接，一个 AR 上可以同时拥有几个 NAR。TNC 访问请求者由以下几部分组成。

① 可信平台模块（TPM）：TPM 执行受保护能力、受保护空间以及其他功能。

② TCG 软件栈（TSS）：TSS 是一中间件堆栈，应用与 TPM 支持的功能进行通信使用更高一层的界面，包括不限制的密钥存储，密钥缓存和更高界面的抽象。

③ 平台可信服务（PTS）：向 TNC 组件开放平台可信能力。PTS 包括受保护密钥存储、非对称加密、随机数、平台身份、平台配置报告和完整性状态跟踪。

（2）TNC 客户端 TNCC（TNC Client）。收集来自 IMC 的完整性度量值，并将本地平台报告的完整性度量值和 IMC 的完整性度量值组合。

（3）完整性度量收集器（Integrity Measurement Collector，IMC）。运行在 AR 上的一个软件，负责度量 AR 的完整性属性。

2. 策略执行点

执行 PDP 所作的网络访问授权决策的实体，包含 PEP 组件。PEP 组件负责控制对受保护网络的访问，PEP 检测到 AR 的请求后，传递 AR 请求到 PDP，并通过 AE 与 PDP 协商安全通道来决定网络访问权是否应该被授予，PEP 扮演中断代理角色。PDP 授权完成后，向 PEP 发送访问规则，决定是否允许 AR 接入网络。

3. 策略决定点

根据访问策略以及 AR 的状态，决定是否允许其接入网络的实体，其自底向上包含的组件为：

（1）网络访问授权（Network Access Authority，NAA）。决定是否授予 AR 访问权的组件。NAA 通过与 TNCS 协商，以判定 AR 的完整性度量值是否和 PDP 的安全策略一致。

（2）TNC 服务器（TNC Server，TNCS）。管理 IMV 和 IMC 之间的信息流，收集和总结来自 IMV 的行为建议，并将其传递给 NAA。

（3）完整性度量验证器（Integrity Measurement Verifier，IMV）。该组件根据来自 IMC 的完整性度量值或其他数据对 AR 某一方面的完整性进行校验。

4.3.2 TNC 的工作流程

以下为 TNC 的工作流程。

Step1：AR 请求访问受保护的网络。

Step2：PEP 将网络访问请求传递给 PDP。

Step3：PDP 要求终端提供用户身份信息、平台身份信息和平台完整性信息。

Step4：PEP 将这些信息传递给 PDP；PDP 根据预定的网络访问策略对这些信息进行验证，并决定是否授予终端网络访问权。

Step5：PEP 执行 PDP 的决策，允许或拒绝终端的接入请求，或对终端进行隔离。

4.4　EAD 技术解决方案

EAD 系统是 H3C 公司为了解决现有网络安全管理中存在的不足，应对网络安全威胁而提出的一套解决方案。该方案从网络用户终端准入控制入手，整合网络接入控制与终端安全产品，通过安全客户端、安全策略服务器、网络设备以及防病毒软件产品对接入网络的用户终端强制实施安全策略，控制终端用户的网络使用行为，可以加强网络用户终端的主动防御能力，提高网络自身安全，防止“危险”、“易感”终端接入网络。这种端到端的安全防护体系，可以在网络接入层帮助网络管理员统一实施企业安全策略，大幅度提高网络的整体安全。

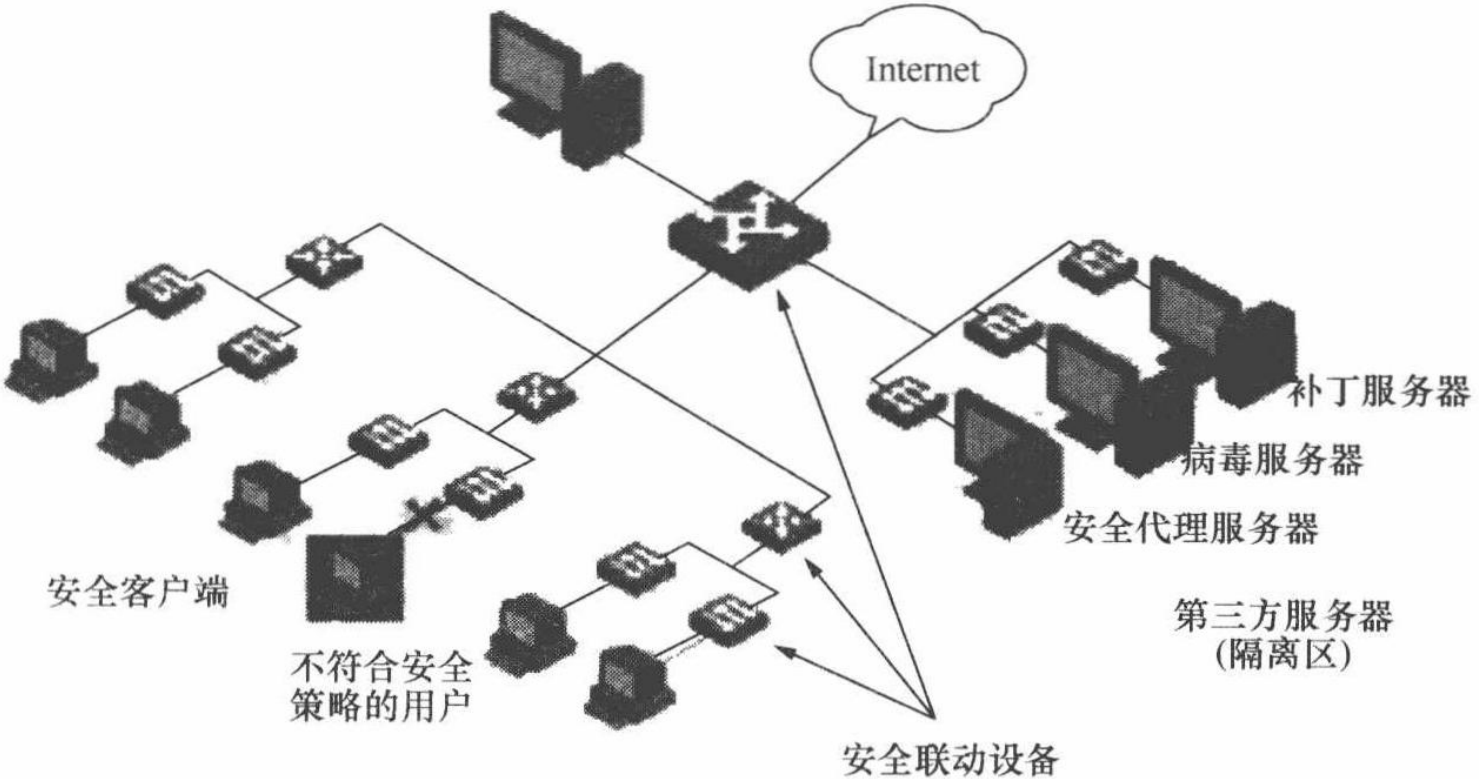
4.4.1　EAD 架构

EAD 解决方案提出的网络准入控制体系架构如图 4-4 所示，其基本部件包括 EAD 安全策略服务器（CAMS 服务器）、防病毒服务器、补丁服务器等修复服务器、安全联动设备和 H3C 安全客户端，各部件由安全策略中心协调，共同完成对网络接入终端的安全准入控制。

EAD安全策略服务器

图 4-4　EAD 架构示意图

下面介绍各个部件的具体功能。


Internet
补丁服务器
病毒服务器
安全代理服务器
第三方服务器
(隔离区)
安全客户端
不符合安全
策略的用户
安全联动设备

Step2：PEP 将网络访问请求传递给 PDP。

Step3：PDP 要求终端提供用户身份信息、平台身份信息和平台完整性信息。

Step4：PEP 将这些信息传递给 PDP；PDP 根据预定的网络访问策略对这些信息进行验证，并决定是否授予终端网络访问权。

Step5：PEP 执行 PDP 的决策，允许或拒绝终端的接入请求，或对终端进行隔离。

4.4　EAD 技术解决方案

EAD 系统是 H3C 公司为了解决现有网络安全管理中存在的不足，应对网络安全威胁而提出的一套解决方案。该方案从网络用户终端准入控制入手，整合网络接入控制与终端安全产品，通过安全客户端、安全策略服务器、网络设备以及防病毒软件产品对接入网络的用户终端强制实施安全策略，控制终端用户的网络使用行为，可以加强网络用户终端的主动防御能力，提高网络自身安全，防止“危险”、“易感”终端接入网络。这种端到端的安全防护体系，可以在网络接入层帮助网络管理员统一实施企业安全策略，大幅度提高网络的整体安全。

4.4.1　EAD 架构

EAD 解决方案提出的网络准入控制体系架构如图 4-4 所示，其基本部件包括 EAD 安全策略服务器（CAMS 服务器）、防病毒服务器、补丁服务器等修复服务器、安全联动设备和 H3C 安全客户端，各部件由安全策略中心协调，共同完成对网络接入终端的安全准入控制。

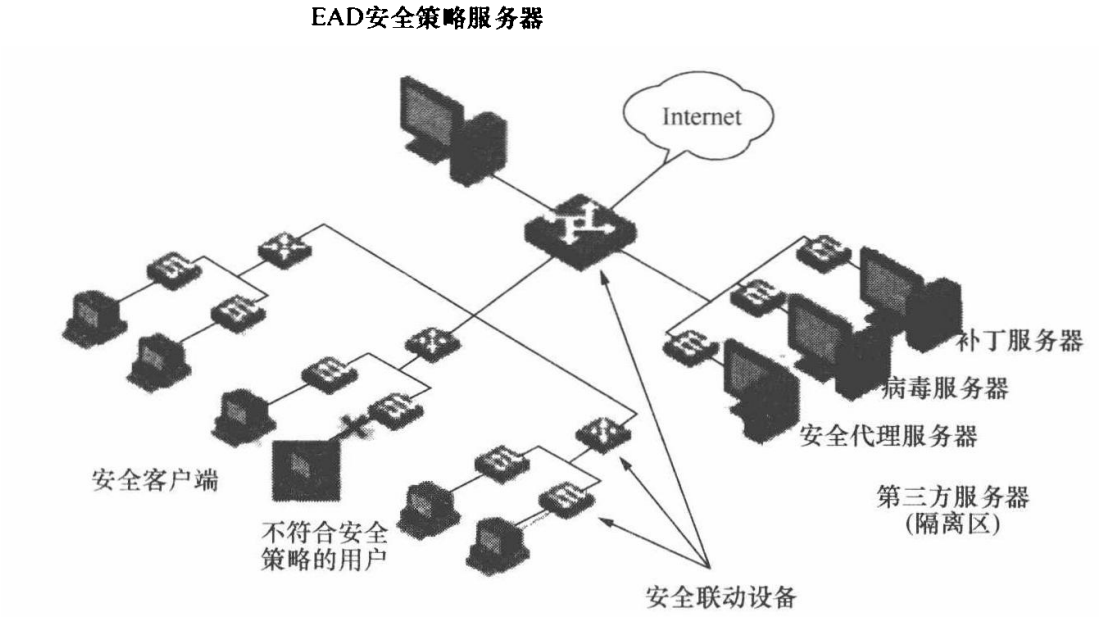


图 4-4　EAD 架构示意图

下面介绍各个部件的具体功能。

1. 安全客户端

安全客户端是指安装了 H3C iNode 智能客户端的用户接入终端，负责身份认证的发起和安全策略的检查。安全客户端可按照企业安全策略的要求，集成第三方厂商的安全产品插件，提供丰富的身份认证方式、实施基于角色的安全策略。

安全客户端是安装在用户终端系统上的软件，是对用户终端进行身份认证、安全状态评估以及安全策略实施的代理主体，其主要功能包括：

① 提供 802.1x、PORTAL、VPN 等多种认证方式，可以与交换机、路由器、VPN 网关配合实现接入层、汇聚层及 VPN 的终端准入控制。

② 收集用户终端的安全状态，包括操作系统版本、系统补丁等信息；同时提供与防病毒客户端联动的接口，实现与第三方防病毒客户端的联动，检查用户终端的防病毒软件版本、病毒库版本、病毒查杀信息。这些信息将被传递到安全策略服务器，执行终端准入的判断与控制。

③ 安全策略实施，接收安全策略服务器下发的安全策略并强制用户终端执行，包括设置安全策略（是否监控邮件、注册表）、系统修复通知与实施（自动或手工升级补丁和病毒库）等功能。不按要求实施安全策略的用户终端将被限制在隔离区。

④ 实时监控系统安全状态，包括是否更改安全设置、是否发现新病毒等，并将安全事件定时上报到安全策略服务器，用于事后进行安全审计。

2. 安全联动设备

安全联动设备是指用户网络中的交换机、路由器、VPN 网关等设备。EAD 提供了灵活多样的组网方案，安全联动设备可以根据需要灵活部署在各层，比如网络接入层和汇聚层。

安全联动设备是网络中安全策略的实施点，起到强制用户准入认证、隔离不合格终端、为合法用户提供网络服务的作用。根据应用场合的不同，智能联动设备可以是交换机、路由器或 VPN 安全网关，分别实现不同认证方式（如 802.1x、VPN 和 Portal 等）的终端准入控制。不论是哪种接入设备或采用哪种认证方式，智能联动设备均具有以下功能。

① 强制网络接入终端进行身份认证和安全状态评估。

② 隔离不符合安全策略的用户终端。联动设备接收到安全策略服务器下发的隔离指令后，可以通过 VLAN 或 ACL 方式限制用户的访问权限；同样，收到解除用户隔离的指令后也可以在线解除对用户终端的隔离。

③ 提供基于身份的网络服务。智能联动设备可以根据安全策略服务器下发的策略，为用户提供个性化的网络服务，如提供不同的 QOS、ACL、VLAN 等。

3. CAMS 安全策略服务器

它要求和安全联动设备路由可达。负责给客户端下发安全策略、接收客户端安全策略检查结果并进行审核，向安全联动设备发送网络访问的授权指令。

EAD 方案的核心是整合与联动，而安全策略服务器是 EAD 方案中的管理与控制中心，兼具用户管理、安全策略管理、安全状态评估、安全联动控制以及安全事件审计等功能。

（1）安全策略管理。安全策略服务器定义了对用户终端进行准入控制的一系列策略，包括用户终端安全状态评估配置、补丁检查项配置、安全策略配置、终端修复配置以及对终端用户的隔离方式配置等。

（2）用户管理。网络中，不同的用户、不同类型的接入终端可能要求不同级别的安全检查和控制。安全策略服务器可以为不同用户提供基于身份的个性化安全配置和网络服务等级，方便管理员对网络用户制定差异化的安全策略。

（3）安全联动控制。安全策略服务器负责评估智能客户端上报的安全状态，控制智能联动设备对用户的隔离与开放，下发用户终端的修复方式与安全策略。通过安全策略服务器的控制，智能客户端、智能联动设备与防病毒服务器才可以协同工作，配合完成端到端的安全准入控制。

（4）日志审计。安全策略服务器收集由智能客户端上报的安全事件，并形成安全日志，可以为管理员追踪和监控网络的整个网络的安全状态提供依据。

4. 第三方服务器

在 EAD 方案中，第三方服务器是指处于隔离区中，用于终端进行自我修复的防病毒服务器、补丁服务器和安全代理服务器等。当用户通过身份认证但安全认证失败时，将被隔离到隔离区，此时用户能且仅能访问隔离区中的服务器，通过第三方服务器进行自身安全修复，直到满足安全策略要求。网络版的防病毒服务器提供病毒库升级服务，允许防病毒客户端进行在线升级；补丁服务器则提供系统补丁升级服务，当用户终端的系统补丁不能满足安全要求时，可以通过补丁服务器进行补丁下载和升级。

EAD 不仅支持 802.1x 标准，还支持 PORTAL 认证方式。在网络均支持 802.1x 交换机的情况下，通常使用 802.1x 认证方式；认证过程中网络设备和用户终端采用 802.1x 认证方式，网络设备和 IMC（相当于 Cisco 的 CAM）之间用 RADIUS。分支网络设备如果都是 H3C 的就可以直接下发端口 ACL，控制力度比较细腻；如果分支网络设备不是 H3C 设备的话，则可以实现用 RADIUS 端口 VLAN 划分方式。

华为网络设备在 802.1x 标准的实现中，不仅支持标准所规定的端口接入认证方式，还对其进行了扩展与优化，可以支持一个物理端口下挂接多个用户的应用场合。当采用基于 MAC 方式时，该物理端口下的所有接入用户均需要单独认

证，当某个用户下线时，也只有该用户无法访问网络；当采用基于交换机的物理端口方式时，只要该物理端口下的第一个用户认证成功后，其他接入用户无需认证就可访问网络资源，但是当第一个用户下线后，其他用户也会被拒绝访问网络。

PORTAL 认证是一种 Web 方式的认证。Web 认证同 802.1x 认证相比，具有应用简单的优势。但是，在 EAD 解决方案中，需要使用客户端进行终端的安全状态检测和控制，因此在 Web 认证的基础上，扩展了 PORTAL 协议，使之不仅能够处理 Http 协议，还可以控制其他协议的数据流，使 EAD 解决方案也支持 PORTAL 认证方式下的端点准入控制。这种方式和 NAC 系统的 NAC Appliance 基本类似。

4.4.2 EAD 的工作流程

如上所述，EAD 准入控制系统，通过安全客户端、安全策略服务器、网络设备以及第三方安全系统的协同，对接入网络的用户终端实施安全策略管理。以下为实现终端安全准入的流程。

Step1：用户终端试图接入网络时，终端计算机首先通过安全客户端上传用户信息至安全策略服务器进行身份认证，非法用户将被拒绝接入网络。

Step2：合法用户将被要求进行安全状态认证，由安全策略服务器验证用户终端安全状态是否符合基于用户账号预定义的安全策略，包括补丁版本、病毒库版本是否合格，软件安装允许是否合格、是否使用代理服务器等信息，不合格用户将被智能联动设备隔离到隔离区。

Step3：进入隔离区的用户可以根据安全策略，通过第三方服务器进行安装系统补丁、升级病毒库、检查终端系统信息、卸载非法程序、取消代理设置等操作，直到接入终端符合安全策略。

Step4：安全状态合格的用户将实施由安全策略服务器根据不同用户的角色下发不同的安全设置，并由安全联动设备提供基于身份的网络服务。

从 EAD 的主要工作流程和基本原理可以看出，EAD 将终端防病毒、补丁修复等终端安全措施与网络接入控制、访问权限控制等网络安全措施整合为一个联动的安全体系，通过对网络接入终端的检查、隔离、修复、管理和监控，使整个网络变被动防御为主动防御；变单点防御为全面防御；变分散管理为集中策略管理，提升了网络对病毒、蠕虫等新兴安全威胁的整体防御能力。

4.4.3 EAD 的主要特点

以下阐述 EAD 系统的主要特点。

1. 严格的身份认证

除基于用户名和密码的身份认证外，EAD 还支持身份与接入终端的 MAC 地

址、IP 地址、所在 VLAN、接入设备 IP、接入设备端口号等信息进行绑定，支持智能卡、数字证书认证，增强身份认证的安全性。

2. 完备的安全状态评估

根据管理员配置的安全策略，用户可以进行的安全认证检查包括终端病毒库版本检查、终端补丁检查、终端安装的应用软件检查、是否有代理、拨号配置等；为了更好地满足客户的需求，EAD 客户端支持和微软 SMS、LANDesk、BigFix 等业界桌面安全产品的配合使用，支持和瑞星、江民、金山、Symantec、MacAfee、Trend Micro、Ahn 等国内外主流病毒厂商联动。例如 EAD 可充分利用微软成熟的桌面管理工具，由 SMS 实现各种 Windows 环境下用户的桌面管理需求：资产管理、补丁管理、软件分发和安装等。

3. 基于角色的网络授权

在用户终端通过病毒、补丁等安全信息检查后，EAD 可基于终端用户的角色，向安全联动设备下发事先配置的接入控制策略，按照用户角色权限规范用户的网络使用行为。终端用户的所属 VLAN、ACL 访问策略、是否禁止使用代理、是否禁止使用双网卡等安全措施均可由管理员统一配置实施。

4. 扩展开放的解决方案

EAD 解决方案为客户提供了一个扩展、开放的结构框架，最大限度地保护了用户已有的投资。EAD 广泛、深入地与国内外开发生产防病毒、操作系统、桌面安全等产品的厂商展开合作，融合各家所长；EAD 与第三方认证服务器、安全联动设备等之间的交互基于标准、开放的协议架构和规范，易于互联互通。

5. 灵活方便的部署方式

EAD 方案部署灵活，维护方便。EAD 按照网络管理员配置的安全策略区别对待不同身份的用户，定制不同的安全检查和处理模式，包括监控模式、提醒模式、隔离模式和下线模式；此外，EAD 还支持灵活的旧网改造方案和客户端静默安装等特性。

EAD 系统同样存在一定的不足：一是认证过程存在一定隐患。例如在系统中采用用户名加口令登录，而且信息传输安全性不高。虽然能够实现客户端与服务器强相互身份认证，但存在被绕过而受到中间人攻击、会话劫持攻击的风险。因此要想进一步增强端点准入防御机制的安全功能，势必要加强客户端与服务器端之间信息。二是 EAD 系统对安全客户端软件进行检测的过程比较简单，非法的兼容客户端软件通过接收版本检查请求帧，然后将合法安全客户端发出的应答帧信息封装到版本检查应答帧中发送给联动设备，就可以规避系统检查，躲避版本检测。同时，EAD 系统对指定软件的检查还只能简单的针对软件名称进行，

安全性不够高。

4.5 ASM 技术解决方案

来自国内第三方 NAC 供应商盈高科技的 ASM 技术解决方案是国内唯一的采用开放式平台的准入架构体系。ASM 针对国内的各种不规范网络、混合品牌复杂网络、大型网络及分布式网络等环境提供了一个厂商无关性的纯准入构架平台。整个 ASM 平台能够支持包括开放性 802.1x、DHCP，厂商专有的 EOU、Portal、VG 以及跨平台的 MVG 自主技术等多达 8 种网络级的准入控制架构，能够迅速地在各种环境下有效上线，满足从重点区域布防到接入边界管理的各级别准入控制要求。

由于在设计之初就考虑了 Gartner 所提出的第三代准入控制架构（Appliance-based NAC）的技术要求，ASM 能够实现“One box，One day”的准入平台快速上线理念，真正达到了 Appliance＝NAC 的技术层级。ASM 架构在 2009 年就提出了“不改变网络、不装客户端”的业内领先的 NAC 实践标准，是目前主流准入框架中组成架构最具开放性，实践应用性最强的一种模式。

也正是由于 ASM 遵循了 Appliance＝NAC 的实践方案，因此 ASM 就具有不同于其他所有架构的简捷性，在架构设计上独特地从管理流程上提出了更为清晰的功能性架构组成。ASM 在实现准入的过程中采用了自顶向下的管理方式，独特的“SOPE”安全管理模型让人眼前一亮，“SOPE”各字母含义如下：

（1）S（shaping infrastructure）——基础架构生成。智能获取用户网络的整体构成信息（包括交换设备、入网终端、IP 资源等），从而帮助各大型网络的负责人更明晰地形成网络视图。

（2）O（obsevation）——观测。ASM 上线后，能够在线观测所有上下网行为并生成统计报告，同时对入网计算机精确地定位到边界交换机端口，从而为 IT 人员提供管理网络接入的数据依据。

（3）P（policy implement）——策略实施。ASM 能够在前期大量安全视图的基础上，帮助用户更容易做出管理网络接入的各项策略，并有效规避传统准入控制的各种风险。对于外来计算机的接入管理和员工计算机的接入管理，ASM 提供的丰富技术策略包括入网规范学习、入网身份认证、入网权限控制、入网安全及规范性评估、入网安全加固、入网异常阻断、网络基础架构规范（Hub、NAT 管理等）、及其他各类风险漏洞分析和预防策略。

（4）E（evaluation & management）——评估与管理。ASM 丰富的技术手段与风险漏洞发现修复能力为众多客户的等级保护测评工作提供了重要支持，同时 ASM 的宏观网络安全视图及丰富的统计数据也在各种安全管理汇报中起到了十分重要的作用。

4.5.1　ASM 架构

ASM 提出的网络准入控制体系架构如图 4-5 所示，从横向看，该架构中的 3 行代表 3 个体系层次，分别为：接入体系、网络基础框架体系和应用体系。

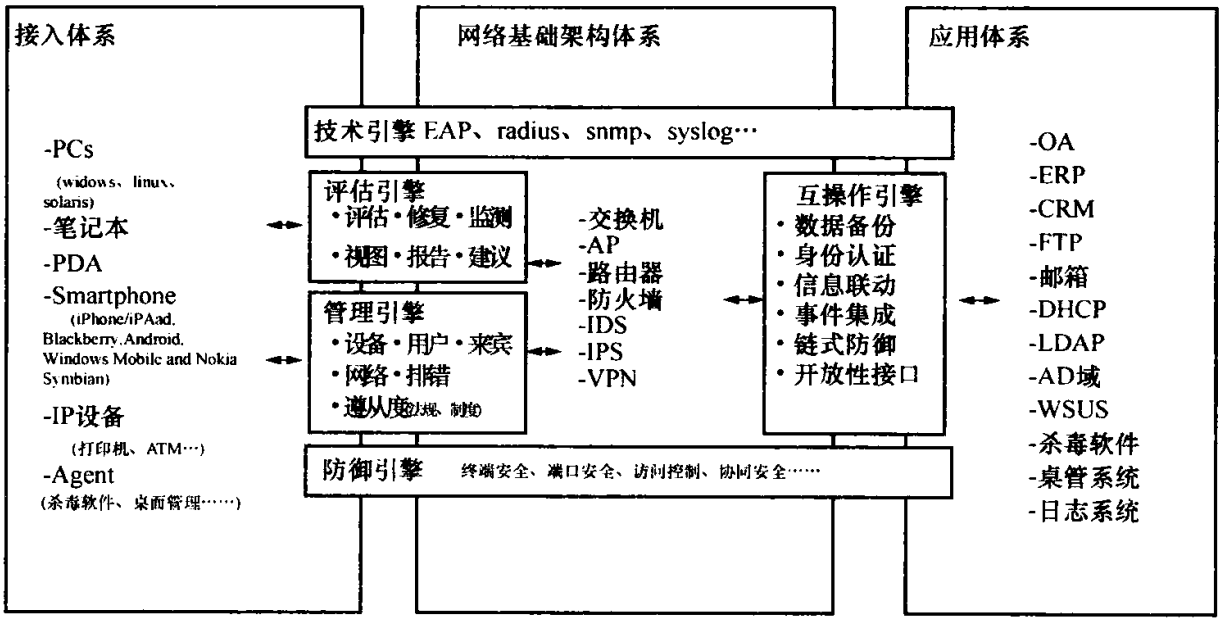


图 4-5　ASM 架构示意图

下面具体介绍 ASM 架构中各个体系内涵。

1. 接入体系

ASM 将各类终端体系都纳入到了平台的管理范畴，这个理念完全不同于前几个准入框架所规定的必须安装客户端的狭义化的接入管理。

在必须安装客户端的情况下，对网络接入的管理很有可能因为不同操作系统、不同硬件架构、不同设备类型的制约而大打折扣，这也就决定了目前大部分准入框架的管理范围都相当有限，无法作为一个开放性的平台提供给普遍的组织或机构用户使用。而采用了 Agentless 设计思路的 ASM 框架则能够提供给用户更为开放的选择权，更适应 BYOD 浪潮下的管理需要。

在用户需要了解接入体系基本信息或安全状况的情况下，ASM 可以通过标准的各种协议，如 snmp、netbios，或从用户网络中已有的应用体系中获取的方式来监测整个网络的基本运行情况。在这个运行体系下，ASM 即使不安装客户端也能够得到一些客户端类 NAC 架构所无法获取到的详细安全信息。

在云计算平台下，瘦客户端的接入将完全抹除客户端类 NAC 架构的存在可能，这样的环境更适合 ASM 的无客户端架构体系，因此 ASM 也是进入云计算的十分合适的一种安全准入架构。

2. 网络基础架构体系

Appliance-based NAC 的一大特点就是兼容并蓄的容纳力。在采用单一硬件 Appliance 的情况下，却能够监测或管理到网络中绝大部分的基础设施，并利用这些基础设施中已经集成的安全特性施行准入管理，这样才能够真正做到无需改变用户网络就完成准入控制的高级 NAC 特性。

在接入层交换机的位置，ASM 可以兼容各厂商的 802.1x 协议，或利用 snmp、cli 等基于 VLAN、ACL、端口来进行十分严格的控制；在核心或汇聚层交换机，ASM 则集成了前面所提到的各厂商的专有框架，支持 EOU、PORTAL、PBR 等各种控制级别的准入架构；另外，ASM 能够联动已有的网络安全产品，如桌管系统 EPP、防火墙、Anti-virus、AD 环境等对攻击和违规行为进行综合防范。

可以设想一次恶意的攻击将经过从 EPP、AP VLAN 控制、交换机端口安全、IPS、防火墙、日志审计等链式的防线，这样的整体防御体系是任何单个的安全产品都无法做到的。但是在 ASM NAC 方案的整体控制下，用户的已有安全资产被挖掘出了最大的潜力。

3. 应用体系

管理和安全从来都是不分家的。同理，应用体系也被整合到了 ASM 的准入平台下，能够从身份认证（如 LDAP）、健康度取样（桌面管理系统、日志系统）、交互式管理（OA）、合规修复（WSUS）等多个维度让整个准入平台的功能更为丰富充实。

另外，从逻辑结构上分析，ASM 系统分为网络适配层、应用支撑层、业务功能层、行业解决方案层以及系统保障管理模块等“四层一模块”。网络适配层主要兼容所有的交换网络环境、支持类似于 Cisco 的 C-NAC、H3C 的 PORTAL/PORTAL+、PBR 策略路由、DHCP Snooping 强制、L2-OOB-VG 虚拟网关、透明网桥等技术。业务支撑层包括可扩展的 Radius 服务、固化的 Web 服务、SQL 数据库服务、集成 SMTP、Syslog 与短信网关等服务；并且可以支持数据管理平台与网络准入控制器分离，数据管理平台采用级联分级分域管理模式。

由于支持的应用体系众多，ASM 在许多用户的环境中已经大大超越了传统 NAC 框架所局限的安全功能，而进一步融合到了用户的日常管理流程中。用户在部署好基本的安全策略后，可以从 ASM 体系获得十分详尽的包括资源、用户、事件、管理、时间的 5 个维度的评估报表，可以反馈给日志系统，也可以影响管理者的后续决策，或提供给其他应用系统进行相关的管理衔接。

从平台的组成看，ASM 提供了十分广阔的开放性组成空间，能够迅速地粘合用户的已有网络基础设施，形成多层级、多区域的整体安全防御体系，这也被

称之为统一安全（自防御）与评估方案（Universal Security（Self-Defense）& evaluation Solution，UseS）。在以上介绍的三个体系的构建下，ASM 实现了统一全网已有资产的安全属性，对恶意攻击或违规行为进行自动智能化的链式防御反应，并利用应用系统进行合理化评估，为管理者的决策和控制提供数据来源。这就是 ASM 提供的统一安全（自防御）与评估方案名称的来源。

4.5.2　ASM 的工作流程

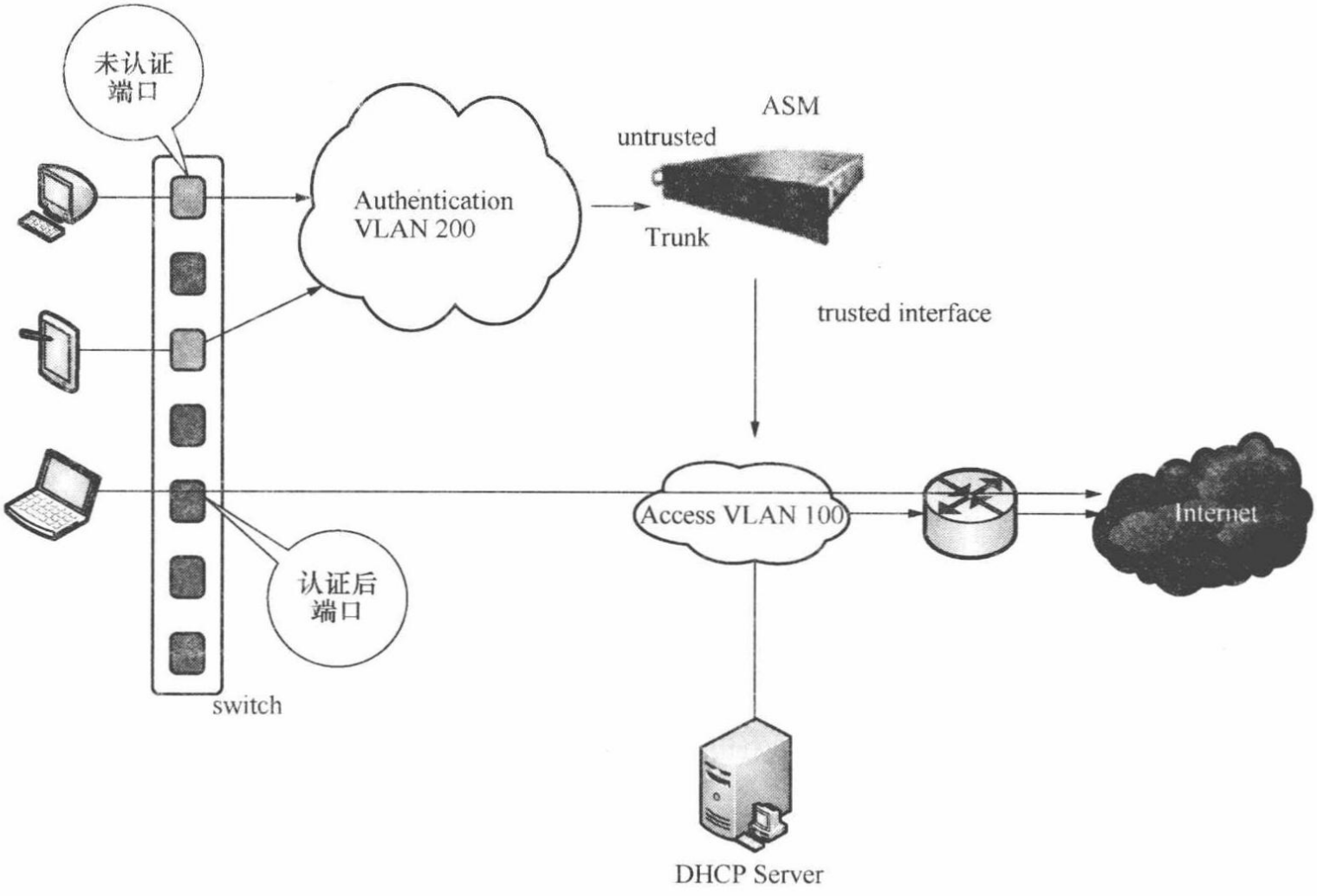
ASM 可以支持多种网络接入强制技术，比如：802.1x、EOU、策略路由、L2-OOB-VG 等技术。重点采用基于 Appliance-Based 的 L2-OOB-VG 的技术，通过旁路部署方式接入网络环境中。其中主要准入控制技术（L2-OOB-VG 技术）在部署过程中需要在核心交换机上配置相应的策略以及认证 VLAN，最终通过 ASM 与交换机作联动控制，对接入的终端用户自动下发相应的强制控制策略，限定非法用户不能随意接入到办公网络，系统部署示意图如图 4-6 所示。

图 4-6　ASM 系统部署示意图

在部署了 ASM 的业务承载网络中，在未通过认证的情况下，用户不能获得访问中心应用系统的权限。以下为实现接入控制的具体流程。

Step1：用户登录网络，进行身份的验证和完整性检查。用户通过 Web 申请引导页面中输入用户名、静态口令（或者动态口令）进行认证，同时安全管理插件会检查用户终端系统的完整性信息。

Step2：安全管理插件将用户的身份认证信息和终端完整性信息发送


未认证
端口
Authentication
VLAN 200
ASM
untrusted
Trunk
trusted interface
Access VLAN 100
Internet
认证后
端口
switch
DHCP Server

称之为统一安全（自防御）与评估方案（Universal Security（Self-Defense）& evaluation Solution，UseS）。在以上介绍的三个体系的构建下，ASM 实现了统一全网已有资产的安全属性，对恶意攻击或违规行为进行自动智能化的链式防御反应，并利用应用系统进行合理化评估，为管理者的决策和控制提供数据来源。这就是 ASM 提供的统一安全（自防御）与评估方案名称的来源。

4.5.2　ASM 的工作流程

ASM 可以支持多种网络接入强制技术，比如：802.1x、EOU、策略路由、L2-OOB-VG 等技术。重点采用基于 Appliance-Based 的 L2-OOB-VG 的技术，通过旁路部署方式接入网络环境中。其中主要准入控制技术（L2-OOB-VG 技术）在部署过程中需要在核心交换机上配置相应的策略以及认证 VLAN，最终通过 ASM 与交换机作联动控制，对接入的终端用户自动下发相应的强制控制策略，限定非法用户不能随意接入到办公网络，系统部署示意图如图 4-6 所示。

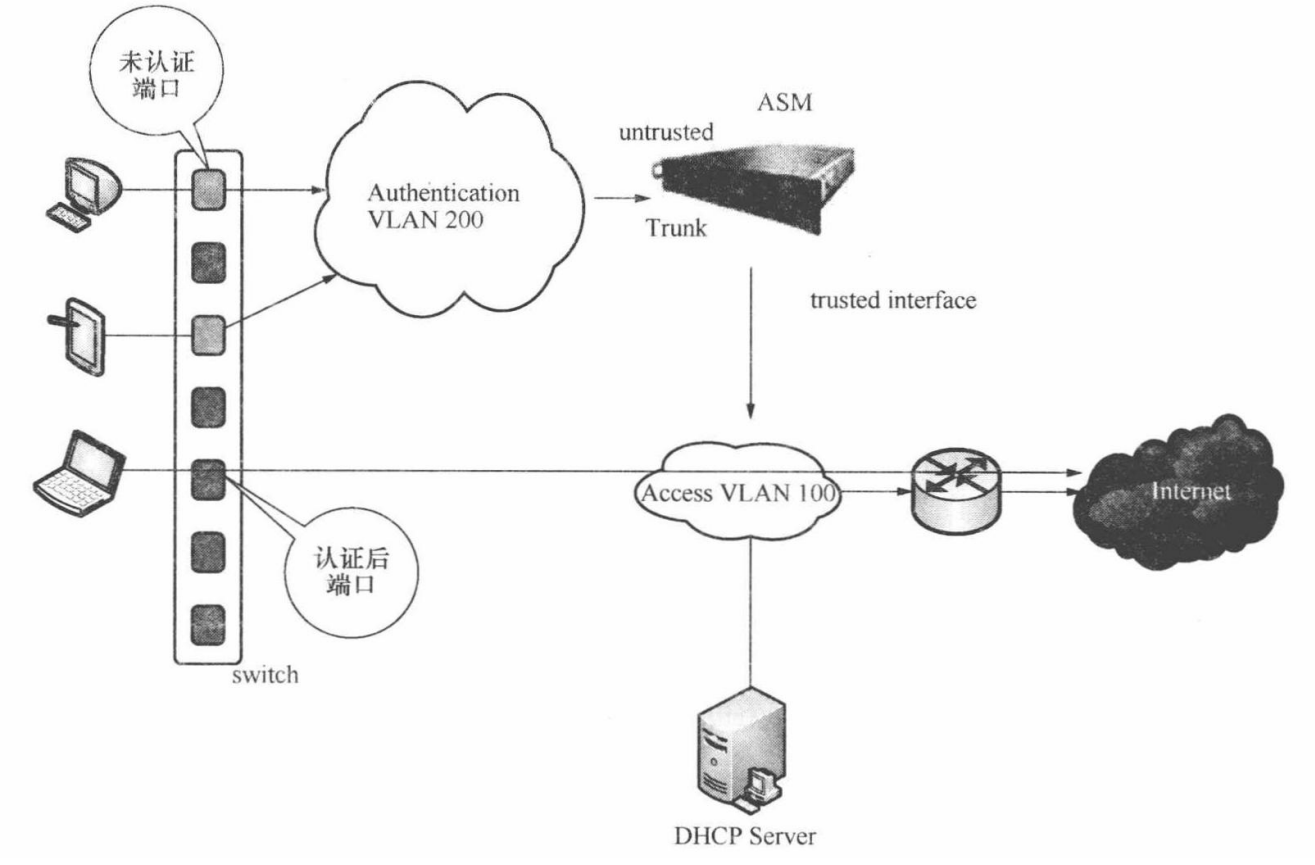


图 4-6　ASM 系统部署示意图

在部署了 ASM 的业务承载网络中，在未通过认证的情况下，用户不能获得访问中心应用系统的权限。以下为实现接入控制的具体流程。

Step1：用户登录网络，进行身份的验证和完整性检查。用户通过 Web 申请引导页面中输入用户名、静态口令（或者动态口令）进行认证，同时安全管理插件会检查用户终端系统的完整性信息。

Step2：安全管理插件将用户的身份认证信息和终端完整性信息发送

到 ASM。

Step3：ASM 将用户的身份认证信息和终端完整性信息应用全网统一的准入控制策略，对用户身份和终端完整性进行认证和管理。

Step4：身份认证不通过的用户将被拒绝接入或置于隔离区；身份认证通过而且终端完整性信息符合要求的用户，ASM 将根据用户的服务类别，为不同类型的用户分配对应的 IP 地址，并实现对应的访问控制策略，确保用户只能访问某些特定的应用；对于身份认证通过而终端完整性信息不符合要求的用户，ASM 将为这些用户分配相应的 IP 地址和特定的访问控制策略，用户将只能获得访问安全中心服务器的权限，进行补丁的升级或漏洞的防护，避免这样的用户接入网络后对应用系统、承载网络以及其他用户造成影响；用户的补丁升级或漏洞防护完成后，重新进行认证，将获得正常的访问权限。用户的登录信息将被记录，提供日后的查询和审计。

4.5.3 ASM 的主要特点

ASM 是依据第三代 NAC 准入技术架构对用户网络进行入网管理的平台，是目前唯一由国内厂商自主提出的准入框架。由于充分考虑到了国内网络的复杂性和普遍的不规范性，因此更能够适应国内大部分机构的准入部署需要。

同时 ASM 不同于其他框架十分重要的一点是，ASM 并不仅仅拘泥于技术实现，而是一开始就从整体的管理角度来构建整个平台，这也决定了 ASM 的 NAC 框架更适合被称作是一套管理类的安全平台，而不是普通的单个技术实现产品。在这个平台上，由于其开放性和扩展性，可以不断的添加进来新的安全组件，而不是像传统安全产品那样具有排他性。因此 ASM 在整体性管理、资产价值深度挖掘、提供不断延展的功能区块等技术类产品所不注重的模块上都做得十分优秀。从这个角度上看，ASM 为整个 NAC 行业都提供了一个很好的新思路。而由于 ASM 第三方厂商的特性，这样的设计理念也相信更容易被广大的机构及用户所认可，也更符合 BYOD 浪潮下的多元化环境发展要求。

从技术层面分析，ASM 具有下面的几个特点。

（1）唯一支持 L2-OOB-MVG 技术。Cisco 的 VG 技术的升级版能够兼容多个厂家的网络设备（包括 Cisco、华为、H3C、中兴、锐捷、神码、迈普等品牌）。

（2）将网络改动减小到最低，支持多厂家网络设备，对于交换机的功能需求较低，无需在交换机配置大量命令，部署方便、快捷。

（3）基于 Agentless 控件模式，不装常驻客户端程序。大幅度地减轻售中实施工作量和管理的维护成本。（Agent 和 Agentless 的区别：Agent 为客户端软件，大小一般 20M 以上，需要常驻内存，加载底层驱动，占用后台资源，属于程序，可在操作系统程序管理器中看到，如果想卸载需要管理员权限。Agentless 不是真正意义的无客户端，因为如果要做安全检查，就必须有客户端，而这

种客户端是以控件形式存在，大小一般 1M 左右，类似网银的控件，只在 IE 中加载，不影响底层驱动，后台资源占用很少，属于 ActiveX 控件，在操作系统程序管理器中看不到）。

（4）友好的 Web 引导界面，终端用户安检体检并提供一键式修复。

（5）支持对私接交换机、Hub 细粒化管理，认证通过正常入网，认证不通过则隔离与修复。

（6）控制到接入层交换机，保障了网络边界。严格有效地遏制了局域网之间的互相访问，共享文件资料外泄等。

（7）有交换机 UI 管理界面，能够实时掌握端口的使用情况，终端的在线状态等。

主要不足是，ASM 基于二层准入控制，无法跨路由实现接入层的控制，对于大型局域网比较适合，小型局域网成本较高。

应该说 ASM 是专注于身份验证—安全评估—智能修复—权限控制的完整 NAC 架构产品，是业内唯一的纯 NAC 硬件架构产品，也是国内第一个无客户端大规模部署（2000 点以上）案例的缔造者，从平台角度看，ASM 具有如下的优势。

1. 能够对人员和设备提供双实名认证

对入网设备进行人员和设备的双实名认证，能够提供多样化的人员身份认证方式（如用户名密码、USB-KEY、邮箱认证、手机短信等），在保障接入网络人员合法性的同时还能够支持对设备的实名认证，保障接入人员合法性和接入网络终端设备的合法性，从而加强内部网络的保密可控性，方便管理员对网络的统一管理。

2. 提供来宾管理功能

ASM 提供“来宾模式”和“员工模式”，对访客和员工分角色进行相应的访问控制，从而确保内网的保密安全等级。随着各项业务的开展，访客来往公司会十分的频繁，对来宾访客的安全规划和有效管理十分重要。ASM 准入平台能够提供“我是来宾”选择访问模式，管理员可以事先配置来宾可以访问的资源，比如只能上互联网、收发邮件等。并且来宾在不知道具体员工身份认证的方式，没有办法获取内部员工的访问模式与权限，只能选择“来宾模式”。这样基于应用控制来宾访问权限，可以很好地解决既满足业务需要，又很好地保护好用户内网资源。

3. 提供用户与设备的“人机对应”负责制

ASM 准入平台能够实现非常灵活的设备分组、分级分域管理，对所有设备建立责任人对应管理制度；依据入网设备的 MAC 和硬盘 ID 对设备进行识别，

建立 IP 设备与用户 ID 对应列表，属于内部计算机的将通过管理员审核后入网，其他机器不允许入网或只允许以来宾身份入网。这样将 IP 设备与用户 ID 建立对应关系，便于对设备和人员行为进行审计，并有效防止账号泄密后的非法入网。对日常管理、事中责任明确以及事后规范行为审计等有十分重要的意义。同时可以实现灵活的设备分组、分级分域管理，根据不同组别的资产，可以采取不同的安全检查规范。

4. 多种杀毒软件厂商支持，快速补丁扫描与修复

鉴于杀毒软件与系统补丁对于内网安全的重要性，ASM 准入平台能够支持检查市面上主流的所有杀毒软件产品（多达 12 种），并且准入平台自身提供补丁服务器功能，能够及时与微软官方的补丁更新同步，并且提供补丁的分级管理（如严重、重要、中等）和分级修复，在对终端进行安全检查时为了不影响公司员工的日常工作，补丁扫描时间将控制在 8s 以内，支持系统补丁的自动修复。

5. 提供用户所在机构特色的安全检查规范库

NAC 准入平台能够针对机构内的具体网络情况提供个性化的规范模版；并以此模版为依据，通过系统落实在管理手段上。结合优化的高效检查引擎——“基于安全策略可配置引擎”（国家科技部创新基金编号-09C26223301274），进行安全检查修复，支持多达 24 项的安全漏洞扫描参数，并且可持续在线升级引擎及规范库，充分获取网络内的保密机器安全性相关数据

6. 对漏洞设备进行“一键式”智能修复

由于接入终端数量多、配置差异大，人员计算机水平参差不齐，ASM 准入平台能够对存在安全隐患的设备提供智能、快速的“一键式”修复功能，通过与杀毒软件服务器和补丁服务器等安全设备的联动整合提供内网保密的最大安全性，建立保密的主动防御体系。解决终端用户面对漏洞而无从下手导致不能及时恢复正常业务的问题，从而减少安全隐患修复的复杂性和专业性，同时也大大减少管理员的工作量。

7. 基于人员角色进行动态授权

ASM 准入平台能够基于终端用户的角色分配网络访问权限，通过权限规范用户的网络使用行为。可以事先做好安全管理规划，根据需要划分多个安全域，并且由管理员自定义配置安全域的 IP 地址段。基于终端用户的角色，向安全联动设备下发事先配置的接入控制策略，按照用户角色权限规范用户的网络使用行为，按照角色限定用户的入网权限和入网时间。这样就可以在内网中做好区域访问部署控制。

8. 安全检查引擎及规则库能够保持定期更新

ASM 准入平台的安全检查规范作为准入控制系统对接入设备审核安全性的依据，具有丰富性、扩充性、行业性，包含了内网安全所必需的补丁检查、杀毒软件检查、IP/MAC 地址绑定检查等常规安全检查项，也需要包含了桌面客户端运行状态检查、域用户检查、必须/禁止安装软件检查等个性化安全检查项，还可以根据用户的实际需求进行扩充。

9. 能够支持无客户端 Agentless 的准入部署模式

考虑到网络对于日常运行的关键性，ASM 准入设备在部署时将基于无客户端 Agentless 部署模式，这样可以充分防止客户端的兼容性和稳定性问题对于网络准入平台的不良影响，将整个平台的防单点故障能力提升到更高的等级。

10. IP-Mac 绑定与智能探测

对入网设备的 IP-Mac 对进行绑定从而有效地进行 IP 管理，能够智能探测网络中的 IP 地址私自更改行为并产生报警，对非法 IP 地址更改行为自动进行入网阻断，从而加强涉密网络中的地址规范性和可控性。

11. 能够提供实名制日志审计报表

平台可以收集接入设备的相关信息，提供新入网设备、来宾设备、待审核设备的多项入网报表统计，提供 IP 上下线情况统计，提供安全趋势图、违规设备、修复设备、安全检查统计报表，并提供每日、每周及每月的综合报表。对各检查项数据进行统计分析并提供报表便于查看，报表能够以邮件形式自动通知管理员，方便管理员能一目了然地掌控全网的安全状态。

12. 能够提供及时的报警响应

能够将新入网设备、待审核设备、统计报表及网络中的异常情况以邮件、手机短信等形式及时报告给网络管理员，让管理员随时掌握网络边界安全动态。

13. 分级补丁部署

自带补丁服务器组件，通过内部严格测试的分级补丁系统对入网端点进行自动智能化补丁升级，确保涉密内网系统补丁的即时更新。

应该说，一个准入框架是否优秀，技术和开放性是同等重要的，在特定厂商环境下运行的 Vendor-Specific 准入平台在技术实现上各具特点，也互有长短，但从整个 NAC 行业发展的角度看，第三方厂商或组织的开放性架构更有长期性优势，更容易成为整个行业的整体化标准，更符合 NAC 是一个平台的终极思路。

4.6 网络准入控制解决方案对比分析

4.6.1 传统准入控制解决方案对比分析

传统网络准入控制的核心概念是从网络终端的安全控制入手，结合身份认证，安全策略执行和网络设备联动，以及第三方软件系统（信息服务系统、杀毒软件和系统补丁服务器等）的应用，完成对终端的强制认证和安全策略实施，从而达到保障整个网络安全的目的。因此，从这个角度讲，当前应用方案的目的和技术架框事实上基本相似。

首先，它们的目标都是保证主机的安全接入。当 PC 或笔记本接入本地网络时，通过特殊的协议对其进行校验，除了验证用户名密码、用户证书等用户身份信息外，还验证终端是否符合管理员制定好的安全策略，如：操作系统补丁、病毒库版本等信息。并根据各自制定的自己的隔离策略，通过接入设备（防火墙、交换机、路由器等），强制将不符合要求的终端设备隔离在一个指定区域，只允许其访问补丁服务器进行下载更新。在验证终端主机没有安全问题后，再允许其接入被保护的网络。其次，这几种技术和技术框架也比较相似。基本上都划分为接入端、策略服务以及接入控制 3 个主要层次组件。

下面主要从技术开放性、技术侧重点和所采用的标准等方面对几种网络准入控制技术进行一下对比分析。

1. C-NAC、NAP 和 TNC

表 4-1 对 C-NAC、NAP 和 TNC 技术进行了对比与分析，给出了它们的相似性与不同性。

表 4-1 三种接入控制技术对比分析

名称	倡导者	相同点	不同点		
			开放性	技术侧重点	采用标准
C-NAC	Cisco	目标、原理和架构相似	专有技术	围绕 Cisco 网络设备设计	EAP、RADIUS 等
NAP	微软		专有技术	侧重于代理和接入服务的开发	DHCP、RADIUS 等
TNC	TCG		开放标准	可以与可信平台模块绑定	802.1x、IPSec 等

1）相似性

C-NAC、NAP 和 TNC 技术的目标和实现技术在以下方面具有很大相似性。

① 它们的目标相同，都是为了保证终端的安全接入。

② 它们的实现原理相同，都是在终端接入网络之前验证用户和平台身份信息，此外还要检查终端安全策略是否符合要求，只有验证通过的终端才允许接入

网络，未通过验证的终端被送入隔离网络进行修复，直到满足安全策略后才允许接入网络。

③ 它们在技术实现的体系架构上基本相似，都由 3 个逻辑部件构成，分别为接入端、接入控制和安全策略服务组件。

④ C-NAC、NAP 和 TNC 中涉及到接入端、接入控制和安全策略服务 3 个主要组件，其相应的安全通信协议包括接入端与接入控制端的通信协议、接入控制与安全策略服务的通信协议以及接入端与安全策略服务之间安全认证通道协议的建立。扩展认证协议（EAP）是 3 种接入系统普遍采用的安全认证通道协议。远程认证拨号用户服务（RADIUS）协议是 3 种系统中接入控制与安全策略服务普遍采用的通信协议。

2）不同性

由于 C-NAC、NAP 和 TNC 3 种技术的发布者的技术背景各不相同，因此它们之间又存在以下几方面明显的区别。

① 开放性不同。C-NAC 和 NAP 是厂商的专有技术，而 TNC 是一个开放标准，任何厂商产品都可以调用或提供操作接口。

② 技术侧重点不同。

C-NAC 由于是 Cisco 发布的，所以其构架中接入设备的位置占了很大的比例，或者说 C-NAC 自身就是围绕着 Cisco 的设备而设计的。Cisco 的 C-NAC 方案着重在网络架构及策略规划与管理能力，侧重于网络层接入控制。当然，前提是企业内大多采用 Cisco 设备，并且想由 Cisco 设备与其安全方案来保护客户端。

NAP 主要侧重于应用层的接入控制，偏重在终端 Agent 以及接入服务（VPN、DHCP、802.1x、IPSec 组件）的开发。这与微软自身的技术背景也有很大的关联。前提是服务器或桌上型计算机采用的是微软操作系统，而且希望这些主机都能安全地运作。

TNC 将网络层和应用层接入控制都纳入了其标准范围以内，技术重点放在与 TPM 绑定的主机身份认证与主机完整性验证，或者说 TNC 的目的是给 TCG 发布的 TPM 提供一种应用支持。相比 C-NAC 和 NAP 技术，其最大优势在于 TNC 可以和可信平台模块（Trusted Platform Module，TPM）绑定，通过 TPM 的硬件密码保护，能够保证接入端的平台身份、平台完整性状态信息不被假冒不被篡改，实现终端的可信接入，能够建立从客户端到网络的完整可信路径。

③ 采用标准不同。C-NAC 采用 EAP、RADIUS 等协议；NAP 采用 DHCP、RADIUS 等协议；TNC 采用 802.1x、IPSec、L2-OOB-VG 等协议。

目前 C-NAC 和 NAP 之间、NAP 和 TNC 之间已实现互操作。实现互操作带来的好处有：

① 用户在架构和产品方面有了更多的选择，他们可以选择最适合自己的一种解决方案，而不必担心兼容性问题。

② 简化了网络访问控制框架和协议。

③ 用户在实施方案时，不会因为选择了某一方案而替换原有设备，避免了资源浪费。

④ 保护了网络访问控制产品生产厂商的利益。

2. H3C 的 EAD

很明显，这又是一个厂商专用的解决方案，但与上述几个框架不同的是，H3C 提出的 EAD 是沿袭了其公司前身华为数通部门的 PORTAL 框架，因此 EAD 可以看作是传统 NAC 框架中唯一具有一定国产血统的平台。

总的来说，EAD 是一个可扩展的安全解决方案，对现有网络设备和组网方式改造较小。在现有网络中，只需对网络设备和第三方软件进行简单升级，即可实现接入控制和防病毒的联动，达到端点准入控制的目的，有效保护用户的网络投资。在 2007 年前后，国内资本占控股权的 H3C 迅速铺开了一大批的交换机和路由器用户，这也为其 EAD 平台的有效扩张打下了十分坚实的基础。EAD 最初也是基于 802.1x 为主的一个平台，并作为 H3C 内网的一个服务组件赠送给大批量购买了其交换设备的用户。但与 H3C 的推广初衷违背的是，这些客户的网络规模都比较庞大，在部署 802.1x 技术的时候遇到了相当多的问题，包括客户端的资源占用率、客户端部署工作量、客户端兼容性和稳定性、单点故障等。因此 H3C 的 EAD 平台在实际采用 802.1x 的情况下，很少有用户到现在还在持续使用，往往是维护到第二个年头甚至是刚刚部署完毕就因为各种问题而匆忙下线。这并不是 H3C 本身的问题，而是所有 802.1x 平台的通病。

EAD 的比较高级的框架是采用 PORTAL＋协议，这是 H3C 沿袭华为公司 PORTAL框架的一个扩展协议。PORTAL/PORTAL＋运行的环境要求要远远高于 802.1x，一般是运行在 H3C 的企业级路由器上，或是运行在较高系统版本的核心交换机上，如 H3C S5500-EI。PORTAL/PORTAL＋能够在跨路由网络访问时实现身份验证、策略下发和计费等功能，这实际上十分近似于运营商的 PPPoE，但由于运行在 3 层网络中，控制力度远远弱于 802.1x 的 2 层端口级控制，其最大的优势在于可以对 VPN 接入的远程用户实施策略强制。

在 EAD 系统中，安全策略服务器与网络设备的交互，与第三方服务器的交互都基于开放，标准的协议实现。在防病毒方面，目前 EAD 系统已与瑞星、金山、江民等多家主流防病毒厂商的产品实现联动，但相对于 NAC 系统来说，EAD 系统和国外防病毒厂商的交互比较少。EAD 管理界面中文操作简便、设置简单，但规则制定一般是直接定义策略，可共享的资源不多。

3. SEP

赛门铁克公司的准入实现方案 SEP 中，主要由 SEP 管理器（Symantec Endpoint Protection Manager，SEPM），SEP 客户端，SNAC（Symantec Network

Access Control）客户端，Symantec Enforcer 等组成。SEPM 主要用于安全策略的制定和终端用户的管理，SNAC 客户端与 SEP 客户端配合，向 Symantec Enforcer 报告其主机完整性遵从状态。Symantec Enforcer 是一种硬件设备，可限制非法终端对网络的访问。相比其他厂商的解决方案，SEP 可以实现根据灵活的安全策略实施准入的功能。比如 SEP 的客户端软件还具有桌面防火墙、基于主机的入侵防御等功能，能更好的保护终端的安全，其具体策略可以通过管理平台进行管理与设置。

Symantec 的病毒厂商优势也自然集成到了其准入方案中，SEP 中就可以集成 Anti-virus 组件，这样就无需配备第三方的防病毒服务器，这是其他任何一个准入框架都不具有的独特优势。但剑有双刃，SEP 也不例外，相当多的用户都在诟病其 Agent 的庞大和难以维护，加入了包括防病毒、桌面防火墙、主机入侵防御等一系列功能的 Symantec 客户端，光安装包就超过 100M，安装好后的系统空间超过 500M，一个安全类产品的运行成本居然比用户 90%的业务还要高，这是很难让人接受的，而之前中提到的 802.1x 方案的各种弊病也同样存在于 Symantec 的 SEP 平台下。相对于 Symantec 品牌的国际知名度而言，SEP 在国内的口碑并不那么理想。

4.6.2　新老准入控制解决方案对比分析

传统的准入控制架构设计的重点在于功能实现，往往是 3～5 个组件联手实现一个庞大的功能体系，用户在必须购买这多个组件的情况下，实际有效使用到的功能却不到 50%。而更为严重的情况是，在基础设施厂商 NAC 框架的引导下，非常多的用户在开始选型 NAC 时就不得不面对必须更换已有网络设备的难题，这让运营和维护人员苦不堪言。综合来看，传统 NAC 框架的组件过多、维护复杂、购买成本高、运营风险无法控制，实际收益与投入比例十分低下。

NAC 从 2003 年提出，到 2012 年经过了大概 3 个阶段的发展，在第二阶段发展浪潮（2009 年前后）中，众多的用户就已经对传统 NAC 框架提出了严厉的质疑，在那个时期 NAC 整个行业都陷入到了发展的低谷，NAC 的框架也进入到了一个修正和创新的阶段。在国外有众多的第三方 NAC 厂商开始了开放性平台的研究，而在国内则是以 ASM 为首的第三方 NAC 框架异军突起，以“开放性”、“适应性”、“单一硬件设备”、“无客户端”、“快速上线”等为其设计理念，并且不仅仅局限于在“接入”层面进行控制了，而是将管理的视角延展到了接入后也就是“post-connect”的层面，这就重新打开了 NAC 的管理视角。而无客户端化的宣言则更符合 BYOD 浪潮和云计算的发展需要。

下面通过具体的对比表格对传统 NAC 架构和新兴 NAC 架构进行分析探讨，如表 4-2 所示。

表 4-2 传统 NAC 架构和新兴 NAC 架构对比

对比项目	传统 NAC 框架（C-NAC、EAD 等为代表）	新兴 NAC 框架（ASM 为代表）
实现目标	侧重功能堆叠	侧重管理实现、友好度和适应性
技术原理	厂商专用协议	开放式协议，如 snmp、EAP，也支持厂商专用协议
框架组成	3～4 个组件，包括 2～3 台管理服务器、接入客户端、厂商专用交换设备	1～2 个组件，包括一台专用硬件，和一个可选的客户端
开放性	低，很少的架构如 TCG 具有开放性	高，以开放性为设计理念，可以提供众多接口
接入体系	局限于 Windows 系统的接入设备	支持各种移动设备和智能手机
云计算扩展	未考虑	无客户端模式能够与云计算配合
综合成本	较高	低

1. 实现目标

在前面就已经提到传统 NAC 框架的设计目标在于向用户提供可实现的 NAC 功能，因为在任何一个行业发展的前期，功能有无都是首要的考虑目标，这也体现出了 NAC 发展前期的技术手段匮乏、标准不统一、实践经验不丰富等特点。而在越过了技术发展探索期后，整个行业往往会趋向于提供更人性化、更简便易用、更符合管理思维的高级框架，这就是目前新兴 NAC 框架所处的地位。

2. 技术原理

传统 NAC 由于处在技术探索期，因此功能的实现与否往往能够决定一个产品的成败，这就导致了网络基础设施厂商纷纷发展各自为政的技术体系来屏蔽对手。事实证明，开放性平台更适合国内的网络环境，如 ASM 诞生于第三方厂商，在博采众长的优势下提供了更通用的技术解决方式，并且由于专一从事 NAC 开发，整个平台在移植外来技术上能够获得更为有效的投入力度，这样就能够集传统 NAC 框架各门派之大成，成为一个真正的“平台”。

3. 框架组成

传统 NAC 框架依靠众多复杂的组件提供给用户纷繁的功能特性，但大部分无法在管理环境中得到有效使用，同时加剧了运营和维护的成本和运行风险。以 ASM 为代表的新兴 NAC 框架剔除了诸多难用冗余的功能，而保留了关键、实用、高效的 NAC 核心框架，同时提供给用户极其简洁的平台构成，用户可以在这个平台上依据需要扩展其他组件或第三方产品，真正体现了 Appliance-based NAC 的精髓，这是新老 NAC 框架一个最为关键的区别。

4. 开放性

传统 NAC 框架大部分是厂商专用框架，因此开放性的高低不言而喻。而 TCG 组织的 TNC 框架更像是一个理论模型，最终也没能够得到实际推广，只能停留在 NAC 第一波浪潮的印象中供人瞻仰。新兴的 NAC 框架中提供了众多友好的扩展接口，无论是接入体系、网络基础设施体系或是应用体系均能够得到友好的支撑。

5. 接入体系

在采用客户端作为必选组件的情况下，操作系统支持的局限性就是必然的了，尤其是 Microsoft 自家的 NAP 平台则更容易被埋葬在 BYOD 的浪潮中。传统 NAC 框架已经有不少厂商在考虑或已经实现对非 Windows 系统的支持了，但是，如果不改变客户端模式的框架，那么在云计算时代，就又会变成一个短命的设计实现。新兴 NAC 框架所提供的可选的无客户端模式或客户端模式则成为了过渡到云计算的一个十分合适的方案。

6. 云计算扩展

准入控制 NAC 本来就是在一台“标准计算机”接入的背景下诞生的，在桌面虚拟化、服务虚拟化、一切都虚拟化后，准入控制将何去何从？这将是摆在整个 NAC 行业面前一个十分严峻的问题。这方面的详细分析可以参见本书的第 5 章。

7. 综合成本

如果需要部署一大堆组件，改动网络组成，每天面对复杂的操作，下班前祈祷明天上班时不要断网，这样的成本放在任何一个管理者面前都是不可承受的。简化后的新兴 NAC 框架在上述的 4 个方面都表现得十分可靠，当你发现部署 NAC 就像部署防火墙一样快速简便时，这样的方案是任何人都无法拒绝的。新兴 NAC 框架将成为整个行业大幅度降低成本的表率。

8. 小结

传统的 NAC 框架在厂商专用的环境中能够得到比其他框架更多的功能特性，但部署复杂度和排他性也让很多用户在购买前产生了不小的顾虑，相信任何机构都不愿意让自己的信息系统永远被某一家单一厂商所劫持。而从 NAC 行业的发展趋势和长远影响来看，第三方 NAC 厂商的新兴开放式 NAC 框架更具前沿性和生命力，尤其是在 BYOD 和云计算的背景下得到了整个市场更全面的接受，也更具有成为行业标准的潜力。相信只有在这种开放与易用并重的理念下，NAC 才能够成为与“云”并驾齐驱的安全体系。

第5章　下一代网络准入控制技术

5.1　云计算及其发展趋势

2012年，在IT消费化和工作地点转移的大趋势之下，企业的移动办公需求将变得比以往任何时候都更加迫切——员工希望随时随地使用他们所心仪的设备进行工作；企业将工作地点转移至各种有利资源所在之处，如位于其他地区的员工（在家办公/远程办公）、承包商、顾问、临时工、合作伙伴和外包厂商等。

在这样一个多变的时代，企业不断寻求新的解决方案来应对内部移动员工的需求，同时将目光转向了云服务。全球前五大SaaS服务供应商Citrix预计，2012年内将有更多亚洲及中国企业采纳云服务，并从“总拥有成本”的传统思路转向“真实拥有价值”，最终认识到灵活的云基础设施所实现的运营成果，即更高的生产率和更灵活的业务运转。

在技术和商业模式创新的驱动之下，一些关键技术将在2012年影响企业的运营方式，首当其冲的便是云计算、信息安全和桌面虚拟化。对CIO们而言，这“三大件”在2012年将从“最好拥有”变成“必须拥有”。

云计算（Cloud Computing）是一种互联网上的资源利用新方式，可为大众用户依托互联网上异构、自治的服务进行按需即取的计算，云计算的资源是动态易扩展而且虚拟化的，通过互联网提供。云计算让现在的IT环境更具生产力，将实现资源调度按需分配，环境部署自动化，降低人工运营和维护成本，提高生产效率。随着云计算的成熟，虚拟桌面或者说“桌面云”将成为未来终端管理和桌面系统建设的主要趋势。

根据IBM云计算智能商务桌面（IBM Smart Business Desktop Cloud）中的定义，桌面虚拟化（桌面云）指的是可以通过瘦客户端或者其他任何与网络相连的设备来访问跨平台的应用程序，以及整个客户桌面。

5.1.1　云计算

云计算是目前工业界和学术界的热点概念，IBM公司在2007年的技术白皮书中第一次提到云计算，此后IT领域广泛开展了对云计算的讨论。云计算的理念是计算机资源公共化的商业实现，为信息管理和服务提供了全新的思路。作为一项正在兴起中的技术，云计算以开放的标准和服务为基础，以互联网为中心，让互联网上的各种计算资源协同工作，共同组成数个庞大的数据中心和计算中心，为各类用户提供安全、快速、便捷的数据存储和网络计算等特定服务。

有关云计算的定义没有统一的标准，不同的企业和个人对云计算的理解不尽

相同，但云计算的基本原理可以概括如下：在“云”中，所有数据处理任务都由大量的分布式计算机来进行，终端用户可以根据需求通过网络访问计算机和存储系统，由企业级数据中心负责处理客户电脑上的数据，这样就可以通过一个数据中心向使用多种不同设备的用户提供数据服务，从而使得任何拥有合适的互联网连接设备的人都可以访问云应用。对企业用户而言，云计算带来的服务整合与按需供给极大地提高了计算资源的利用率，降低了能耗，与传统方式相比，其优势通过表 5-1 得以体现。

表 5-1　传统方式与云计算方式对比表

对比项目	传　统　方　式	云　计　算
实现模式	采购设备，开发系统	购买外部服务
商业模式	支付设备和劳动力费用	所用即所付，按需服务
技术模式	用户单一	多用户，有弹性
计算能力	特定模式	超大规模
可扩展性	不可扩展	可扩展，可以动态伸缩
运行成本	高	极其廉价

5.1.2　桌面云

桌面云，简而言之就是基于云计算的虚拟桌面，在本地具备输入输出设备的硬件环境，而运行环境由云端资源虚拟实现，同时，相关的应用、数据、运算都部署于云端。桌面云是云计算的重要应用领域之一，也是最具特点的应用之一。相对于传统本地桌面，桌面云具有数据安全、节能减排、易于管理、灵活访问、稳定可靠、易于备份的特点。在云计算架构中，桌面云是一种实现计算、存储、网络等资源的集中化、共享化的平台方案，能够将单台 PC 的处理能力（包括 CPU 和硬盘）集中到数据中心，办公个人终端变成 TC（Terminal Client），从而不需要强的处理能力和存储能力就能够搭建好整个业务平台，并兼具计算高效性和数据保密安全性。

处于后台的云数据中心将负责给每个办公终端提供虚拟化的“计算机”实现，每个终端所使用的资源都是共享的，通过云数据中心的统一调度和管理，实现对资源的“按需分配”管理。

1. 桌面云组成架构

这里以 IBM 云计算智能商务桌面为例展示桌面云的一个基本架构。如图 5-1 所示，桌面云主要由以下几个部分组成。

（1）瘦客户端。瘦客户端是使用桌面云的设备，一般是一个内嵌了独立的嵌入式操作系统，可以通过各种协议连接到运行在服务器上的桌面的设备。

（2）瘦客户端和服务器的网络。桌面云提供了各种接入方式供用户连接。用

图 5-1 桌面云的基本架构

户可以通过有线或者无线网络连接，这些网络既可以是局域网，也可以是广域网。

（3）身份认证。一个企业级应用解决方案，必须有用户的认证和授权。在桌面云中一般通过 Active Directory 或者 LDAP 等产品来进行用户的认证和授权，这些产品可以很方便地对用户进行添加、删除、配置密码、设定角色等操作，还可以赋予不同的角色不同的权限，修改用户权限等。

（4）操作系统或应用程序。桌面云架构通过共享服务的方式来提供标准桌面和应用，这样可以在特定的服务器上提供更多的服务。

（5）应用服务器。应用服务器把各种应用分发到虚拟桌面，这样客户只需要连到一个桌面就可以使用所有的应用，就好像这些应用安装在桌面上一样。

另外，桌面云架构中还可能有存放文件和数据的存储服务器。

2. 桌面云的平台搭建

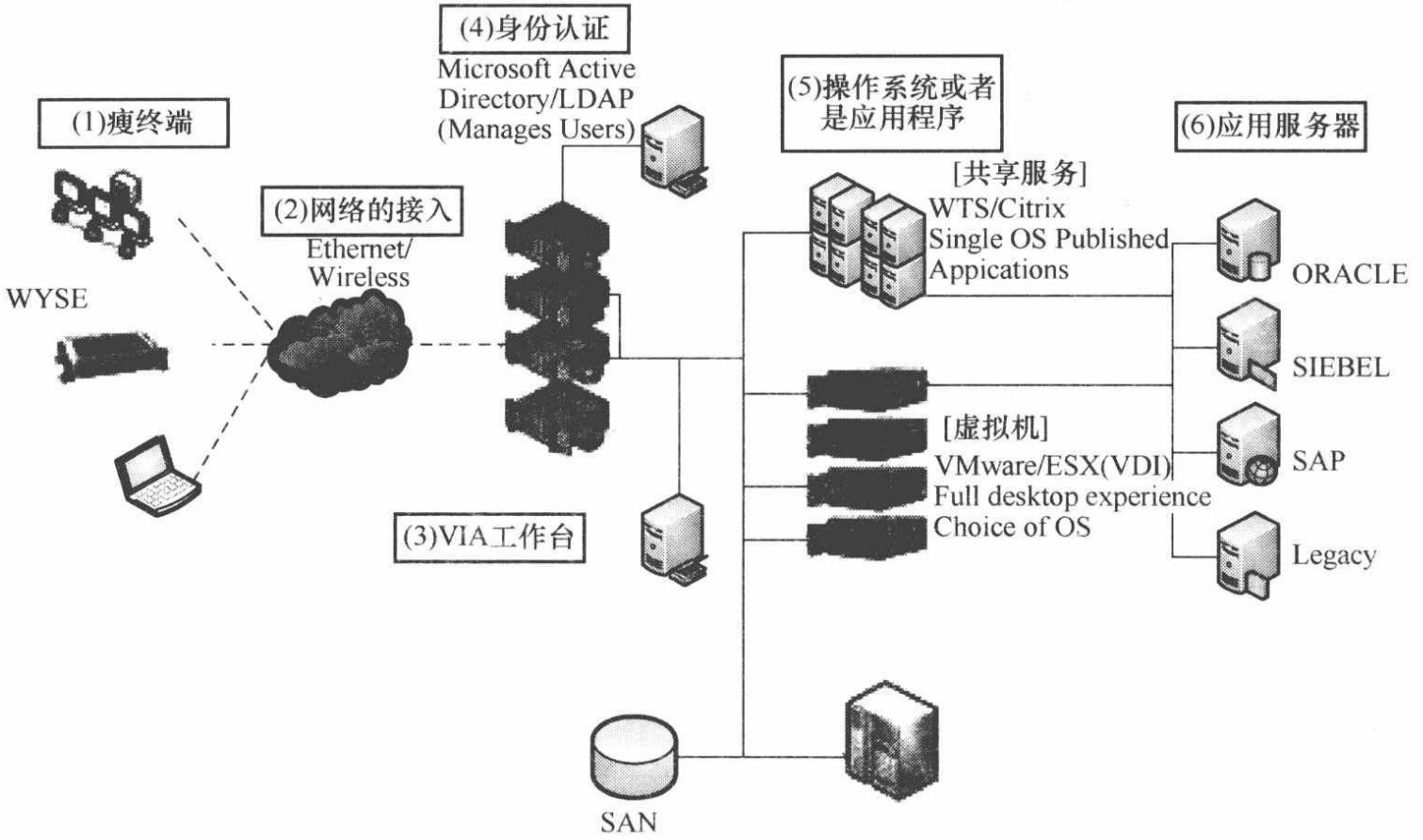
总体来看，桌面云的平台搭建分为前端和后端，如图 5-2 所示。

1）桌面云前端建设

Step1：建设桌面云的前端虚拟交付平台。

Step2：在桌面云的后端服务器上安装 Windows 桌面系统，并安装用户的各类应用系统（如 CRM、收费系统及其他核心业务）的对应客户端，并将这些应用客户端发布到前端的虚拟交付平台。

在建设好前端之后，终端用户的体验即可生成，使用者只需要登录到虚拟交付平台上来使用后端服务器上的 Windows 资源以及利用后端客户端访问相应的


(4)身份认证
Microsoft Active
Directory/LDAP
(Manages Users)
(5)操作系统或者
是应用程序
(6)应用服务器
(1)瘦终端
[共享服务]
WTS/Citrix
Single OS Published
Appications
(2)网络的接入
Ethernet/
Wireless
WYSE
ORACLE
SIEBEL
[虚拟机]
VMware/ESX(VDI)
Full desktop experience
Choice of OS
SAP
Legacy
(3)VIA工作台
SAN

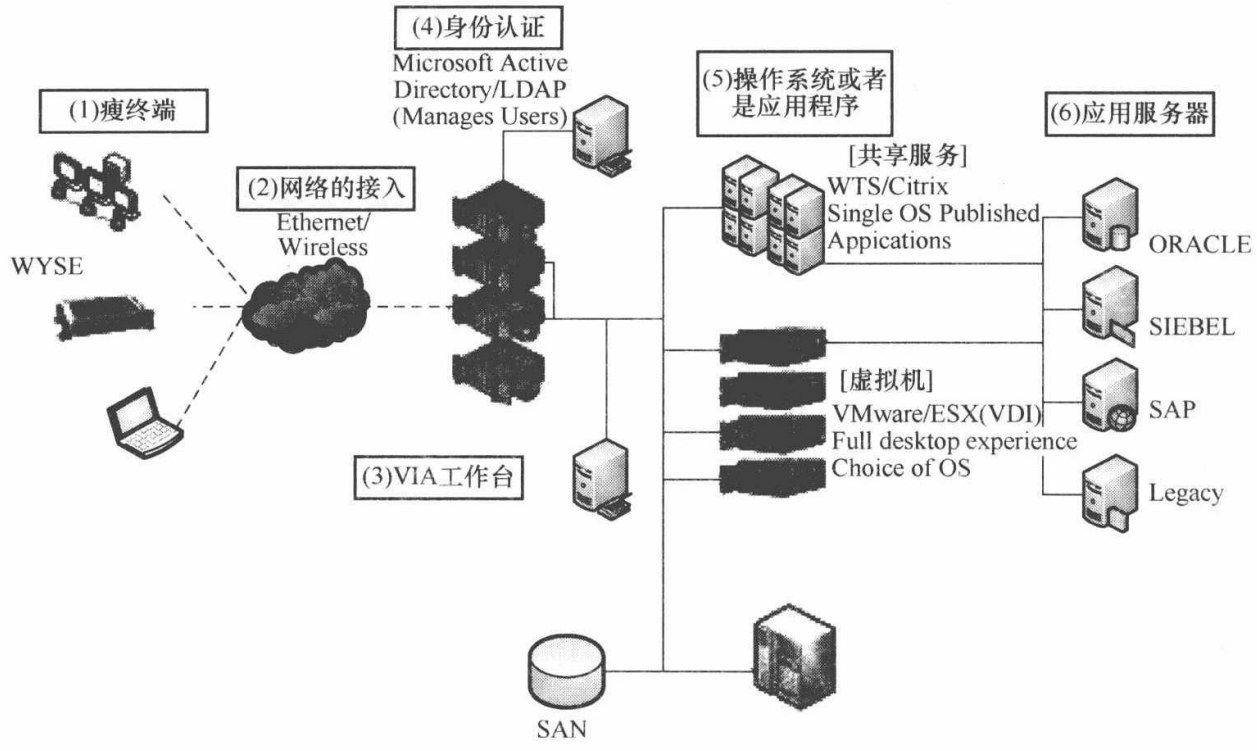


图 5-1 桌面云的基本架构

户可以通过有线或者无线网络连接，这些网络既可以是局域网，也可以是广域网。

（3）身份认证。一个企业级应用解决方案，必须有用户的认证和授权。在桌面云中一般通过 Active Directory 或者 LDAP 等产品来进行用户的认证和授权，这些产品可以很方便地对用户进行添加、删除、配置密码、设定角色等操作，还可以赋予不同的角色不同的权限，修改用户权限等。

（4）操作系统或应用程序。桌面云架构通过共享服务的方式来提供标准桌面和应用，这样可以在特定的服务器上提供更多的服务。

（5）应用服务器。应用服务器把各种应用分发到虚拟桌面，这样客户只需要连到一个桌面就可以使用所有的应用，就好像这些应用安装在桌面上一样。

另外，桌面云架构中还可能有存放文件和数据的存储服务器。

2. 桌面云的平台搭建

总体来看，桌面云的平台搭建分为前端和后端，如图 5-2 所示。

1）桌面云前端建设

Step1：建设桌面云的前端虚拟交付平台。

Step2：在桌面云的后端服务器上安装 Windows 桌面系统，并安装用户的各类应用系统（如 CRM、收费系统及其他核心业务）的对应客户端，并将这些应用客户端发布到前端的虚拟交付平台。

在建设好前端之后，终端用户的体验即可生成，使用者只需要登录到虚拟交付平台上来使用后端服务器上的 Windows 资源以及利用后端客户端访问相应的

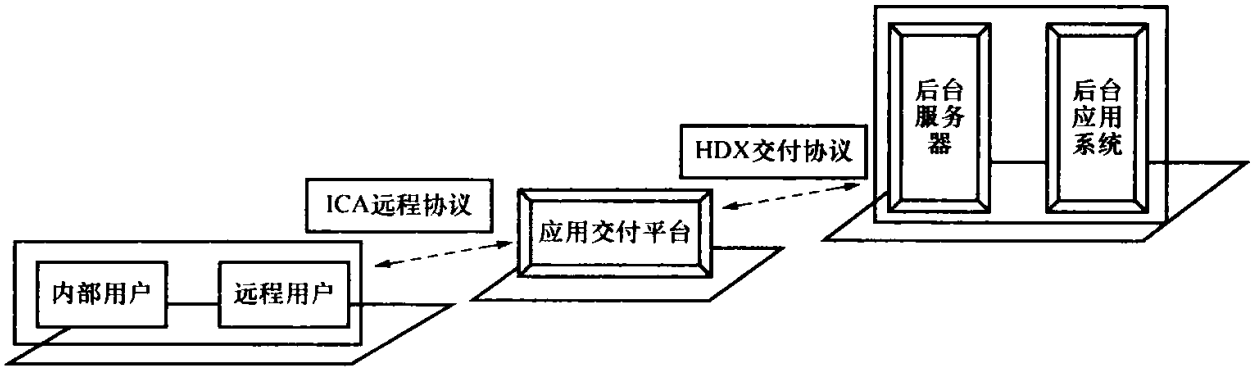


图 5-2　桌面云平台物理架构

应用服务即可，此时的操作系统及应用系统客户端均运行在后端服务器，而不是运行在用户的本地终端，从而实现数据、协议、操作均控制在“云”范围内的效果，大大提高了计算速度和安全性。

2）桌面云后端建设

对于运维管理者而言，在云后端则需要组建集中化的、高性能的云计算数据中心，包括：

① 计算设备。基于各类后台操作系统（如 Unix）对提交上来的业务数据进行计算处理，并将处理结果写入存储设备。

② 存储设备。存储用户内部的重要业务应用系统及各类重要数据资源、各类日志等。

③ 网络设备。支撑云后端体系的通信工作。

④ 机柜系统。放置上述的硬件设备。

⑤ UPS 电源系统。为全套硬件系统提供能源保障。

⑥ 软件系统。VM 虚拟化平台、业务平台、操作系统、数据库平台等。

3. 桌面云的安全性

桌面云系统本质上也是一个分布式的网络系统，和其他分布式系统一样，需要考虑信息安全问题，根据维基百科的定义，一般来说信息安全包括以下 3 个方面：

① 机密性（confidentiality）是指个人或团体的信息不为其他不应获得者获得。

② 完整性（integrity）指在传输、存储信息或数据的过程中，确保信息或数据不被未授权的篡改或在篡改后能够被迅速发现。

③ 可用性（availability）是指信息在需要时能够及时获得以满足业务需求。

桌面云系统也是从这三个方面来考虑安全问题的，它通过数据的加密和数据访问的认证和授权来保证数据的机密性，通过各种安全传输协议来保证数据传输的机密性，通过为桌面云各组件配置冗余组件来保证负载均衡和高可用性。但是由于桌面云系统复杂性，需要从端到端来保证系统整体的安全性。

1）桌面云提供的天生安全性

桌面云之所以吸引企业，除了因为它总体拥有成本较低以外，最主要的一个原因是它天生的安全性。桌面云的建设目标就在于实现高效能的计算和集中化管理的数据安全，在“云”中，用户能够充分享受到传统分散式桌面计算所无法保证的高度的数据安全性。它提供的安全性包括了以下几个方面：

（1）桌面云系统终端用户数据的安全性。由于所有计算和数据的存储都是在云端，客户端不保存用户的数据，在瘦客户端和（后台）云端通信时，传输的仅仅是位图的变化，并没有实际用户的数据传递到客户端，所以不需要担心服务器端传递过来的数据被窃取。

换句话说就是，桌面云的用户桌面环境都是托管在后端的数据中心，本地终端只是一个显示设备而已。因此，即便用户在桌面系统中保存了数据，实质上也是存储在后端的数据中心，而没有在接入“云”的终端设备上保存任何副本。通过这样的数据隔离措施，管理者能够有效地保证数据不被违规带出，从而实现了数据安全。

（2）桌面云系统终端用户访问控制的安全性。桌面云可以提供细粒度的访问控制，用户可以通过安全策略开放或者关闭 USB 端口、打印机端口等。这些 USB 端口还可以分等级控制，保证连接在上面的扫描仪、智能卡等设备可以正常使用，但是大容量存储盘被禁止使用，这样既确保敏感数据不会通过 U 盘泄露出去，又保证了业务的正常进行。同时，由于瘦客户端没有硬盘，也不需要担心别有用心的用户把敏感数据复制到本地硬盘再通过其他路径窃取出去。

（3）存储容灾。桌面云采用集中部署所有托管桌面的方式，所有桌面数据都集中存储在数据中心，因此，用户能够轻松地实现在不同站点间的数据复制，桌面系统可以融入到整体 IT 容灾体系中，构成一个完整的容灾体系。当灾难发生的时候，可以迅速恢复所有托管桌面，保证完全恢复业务的处理能力。

2）桌面云中的安全问题以及解决方法

可以想象一下，在未来的某一天，随着桌面云解决方案的成熟，许多 IT 企业纷纷构建自己内部的桌面云系统或者公共的桌面云系统。大家使用桌面系统的方式也发生了很大的变化：只要一台显示器和一台可以连接网络的设备，插上网线，无需安装软件，无需配置，就可以得到一个桌面云服务提供商给你的桌面，所有的应用都可以从网络上选择使用。另外，你无需支付购买传统 PC 的费用，只要按照你所用的时间和桌面的配置来按月、按使用付费，就像每个月付电话费一样（前面提到过：IBM 其实已经提供了这种服务，只是现在还只是面向企业，没有面向个人，IBM 称之为 Smart Business Desktop on the IBM Cloud，SBDIC，也即在 IBM 云计算智能商务桌面）。这样的场景或许会让人感到很高兴，因为初期购买的花费、安装软件、复杂的配置、经常需要打补丁、安装杀毒软件，等等烦恼都没有了。或许用户心中还有一丝不安：桌面云后端是怎么保证安全的？我的桌面安全吗？我的数据会被人窃取吗？我可以随时使用我的桌面吗？我的数据

都保存在一个集中的地方会不会有很大的风险？其实这和人们通常把存款或者一些贵重的东西存在银行而不是放在家里的道理一样，因为相对于个人的住所而言，银行是一个更专业、更安全、更保险的场所。所以数据放在云端相对于分散在个人电脑上而言更安全，所担心的问题可以在下面找到详细的答案。

下面从整个系统的角度来端到端看桌面云系统的安全性，其中既有硬件，也有软件，忽略整个系统任何一个小的方面，都可能导致整个系统的不安全。

（1）瘦客户端。现在任何一个瘦客户端都可以访问自己在云端的桌面，这对于一般情况下是没有问题的，而且还获得了移动性的好处。但是在某些场景下，这却是一个安全弱点，例如，在一些对安全要求极高的单位。以前在使用传统桌面的时候，由于物理上的隔离，其他人无法进入这个安全区域来窃取资料；而在使用桌面云时，窃密者却可以非法获取别人的用户名和密码，或者使用自己合法的用户名密码，在安全区域外通过任何一台瘦客户端来访问。为了防范这种情况的出现，我们除了登录使用用户名和密码外，要通过添加另外一种认证方式来确保没有非法访问。这种另外的认证方式可以是限制瘦客户端的 MAC 地址、限定某一范围内的 MAC 地址可以访问、配置智能卡认证等。

（2）瘦客户端和服务器的网络。客户端和服务器之间的通信由于是通过网络上传播，所以有可能被人窃听、破解，破坏数据的完整性。为了防范这种情况的出现，一种方法是采用私有云方案，保护网络中的客户都是可信任客户；另一种方式是对通信的数据进行加密。在桌面云方案中一般对于公司防火墙外的非信任用户提供安全连接点，外部用户通过这个安全连接点连接到防火墙内的服务器，这种安全连接点的原理类似于 SSL VPN。对于公司防火墙内部的用户和服务器之间的连接，一般是通过 SSL 协议进行加密传输。通过这两种方式，桌面云方案有效地保证了数据传输的安全性。

（3）服务器的安全。和通常的数据中心的服务器一样，桌面云方案中的服务器也必须遵循企业一般的安全策略，例如，关闭所有的不需要的端口，安装必需的防火墙以及升级到最新的安全补丁，每天进行备份，部署监控软件等。但是和一般服务器相比较特殊的一点是，由于有些桌面云解决方案软件模块之间通信的要求，用户必须以 root 用户登录进行操作，这是非常危险的一方面，目前除了加强安全教育和加强审计之外，没有其他办法对 root 用户操作造成的危险进行规避。希望不远的将来所有的云桌面解决方案杜绝使用 root 用户，对用户权限进行分层。

（4）存储的安全。桌面云中的存储的安全要求和企业中的其他存储安全基本上是一样的。在桌面云系统中从性能出发，一般使用 FC（Fiber Channel）存储，但是 FC 协议本身不是一个安全的协议，服务器可以看到后台 Storage Area Network（SAN）上面所有的设备。最常用的存储安全方式是在 FC 的路由器做分区（zoning）和逻辑单元数掩码（LUN masking）。考虑到高可用性，桌面云中的存储需要考虑备份方案，这样在发生灾难的时候就可以及时回复用户的数据，保证

服务的 SLA。

在传统桌面中，用户数据都是保存在本地的硬盘当中，非授权用户未经许可，难以获取用户数据。但是在云桌面方案中，用户数据都是保存在服务器存储中，云桌面管理员可以比较容易的获取这些数据，这就要求对用户数据加密，防止未经授权的获取用户数据，同时对管理员的密码和访问都需要做出严格的限制，防止用户数据的泄密。

（5）桌面镜像的安全。桌面云中，如果桌面配置成非持久方式，而且用户又没有的存储文件的话，要恢复一个受到病毒侵袭的桌面是非常容易的。只需要重启桌面，桌面就自动恢复到以前未受感染时的状态，而用户数据保存在云端，没有受到病毒的影响。但是如果用户有私有文件的话，由于这些文件是可写的，所以病毒就可能常驻在这些文件里面，需要运行反病毒软件来清理病毒，所以防病毒软件必不可少。所以，必须给桌面云中的桌面安装防火墙和防病毒软件，就像传统桌面一样。和传统桌面相比，这种安装是非常快的，因为一般只需要在几个基础镜像上进行安装就可以了。

（6）软件架构组件的安全。在桌面云的一个安全架构中，通常许多组件都有冗余配置，关键组件甚至可以有多个冗余配置，这样就保证了系统的高可用性以及在大量负载下的负载均衡。在有大量用户访问的情况下，一般在系统的最前端就有一个负载均衡器，把用户的连接请求发送给不同的服务器去处理，根据系统的大小，可能会有一个或者多个负载均衡器在前端处理客户的请求。根据需要，还可以在最前端的负载均衡器上加上安全访问控制组件，保证连接的用户都是经过认证和安全的，防止分布式拒绝服务（DDOS）攻击。例如，在系统前端的防火墙后，可以设置一个安全网关，负责用户的鉴权、授权，并加密所有在客户端和服务器之间的通信。

（7）管理权限的安全。桌面云系统中所有的管理都集中到云端进行，不小心的误操作或者黑客获得管理权限之后的有意操作会造成很大的影响。影响的大小取决于操作的类型和总的用户的数量。所以在桌面云系统中采取以下两种措施来消除这种影响。

① 定义不同的管理角色。例如分为维护用户，升级用户和管理用户。这里只是一个示例，可以根据实际需要来进行更细粒度的划分。

② 审计。对每个涉及到系统变更的操作都需要做好审计工作，这样在事故发生以后可以追溯系统中的变化，及时作出回退操作。审计也能有理由识别出恶意操作，及时发现系统的漏洞。

4. 桌面云面临的威胁

许多企业在考虑把自己的传统桌面替换成桌面云，但是桌面云的安全问题一直困扰他们，成为主要考虑的问题之一。在实施桌面云架构过程中必须要着重考虑安全问题。

在云提供了很多供个人和企业等机构使用的服务的同时，它的出现也对隐私、信任体系和身份产生了新的挑战。具体来说，云计算应用有很多优点，但仍然面临如下安全威胁。

(1) 服务可用性威胁。用户的数据和业务应用处于云计算系统中，其业务流程将依赖于云计算服务提供商所提供的服务，这对服务商的云平台服务连续性、SLA 和 IT 流程、安全策略、事件处理和分析等提出了挑战。另外当发生系统故障时，如何保证用户数据的快速恢复也成为一个重要问题。

(2) 云计算用户信息滥用与泄露风险。用户的资料存储、处理、网络传输等都与云计算系统有关，如果发生关键或隐私信息丢失、窃取，对用户来说无疑是致命的。如何保证云服务提供商内部的安全管理和访问控制机制符合客户的安全需求；如何实施有效的安全审计，对数据操作进行安全监控；如何避免云计算环境中多用户共存带来的潜在风险都成为云计算环境下所面临的安全挑战。

(3) 拒绝服务攻击威胁。云计算应用由于其用户、信息资源的高度集中，容易成为黑客攻击的目标，同时由拒绝服务攻击造成的后果和破坏性将会明显超过传统的企业网应用环境。

从上面阐述的桌面云的安全问题和面临的威胁中不难看出，桌面云涉及前端、网络、服务器、存储、软件架构、内部和外部等各个方面。同时，桌面云支持多种接入方式，包括移动方式的接入，如 iOS 和 Android 的智能手机、平板电脑等，在这种情况下，对于用户认证和接入控制不严格，会导致整个系统的不安全。因此网络准入控制技术在桌面云日益推广发展“云时代”将会发挥出越来越重要的作用。

5.2　云计算的网络准入控制技术分析

在《中国云计算产业发展白皮书》2011 版中，反映我国的大部分“云”都高高在上地飘着，供人瞻仰。椰子也总有掉下来的时候，可是“人云亦云”什么时候能够真正落地让管理者和用户摸着它纯洁柔软的外衣？

不可否认的是，“云”确实是计算发展的一个美好归宿。Forrester 预言 Standalone 型 NAC 产品需要慢慢融合扩展到其他各类安全应用或框架中，不妨理解为：NAC 也需要有向“云”靠拢的气度，如何在虚拟化的基础上发挥 NAC 认证和控制的优势？或者，为什么不也建立一个“NAC 云”？“云”的诱惑很大，NAC 的蛋糕也不小。

5.2.1　技术需求定位

随着云计算的不断深入，越来越多的企业业务系统由传统的 C/S（Client/Server）架构向 B/S（Browser/Server）架构迁移，以往访问后台数据需要安装专用软件，IT 部门控制客户端软件的许可发放，就能够大致控制访问用户的范

围。而在B/S架构中，用户只需要一个Web浏览器即可登录系统，加上智能手机、智能平板和WiFi的流行，以往的限制条件消失了，任何人手中的设备都成了可能访问后台数据库的平台。在虚拟化越来越深入的云时代，IT部门突然一下子失去了对局面的控制，因此，对网络的准入控制被重新提上日程。只有合法的用户才能够接入网络，通过对接入用户的控制，IT部门开始试图重新夺回对数据访问的控制权。

1. 对云设施进行细粒度控制

云计算已经成为很多企业正在评估和采纳的战略优先事项。2012年，企业将寻求对自有云设施进行日益细粒度的控制，其重点是引导数据在公共或私有云设施上的分布。由此，企业将能更自信地利用可以获得的各种好处和资源。

但传统安全的设计方式并非用于管理内网以外的信息，限制了企业充分利用云计算优势的能力。IT部门必须考虑如何在确保信息安全的同时，对云计算加以战略性利用，让云设施更加可控。

2. 平衡移动办公与安全

IT消费化和移动办公为员工和雇主带来了双赢局面：一方面，移动办公可以帮助企业提高灵活性、生产力、成本效益和运营连续性；另一方面，员工有权选择自己喜欢的硬件/设备、工作地点和工作时间。与此同时，企业IT部门也面临一个挑战性与日俱增的问题——如何控制访问和维护安全，对于分布式企业而言，这是个极其复杂的管理过程。这意味着IT部门不仅要确保日益繁多的终端设备安全性，同时还要为各色操作平台交付企业信息。

传统应对方法是限制用户的体验，如仅允许在企业局域网内的指定位置工作，或将所有数据保留在端点上却导致它们容易丢失或被盗。为了支持工作地点转移所带来的更高的企业生产力，必须采纳更加现代化的安全机制，以及制定合理的自带设备（BYO，Bring Your Own）政策。

可以看到，上述两个趋势将有助于提高业务敏捷性，提升工作场所和劳动力的灵活性，而它们能否落地的关键因素都在于安全。由于数据随处可见，员工可能出现在任何地方——在家、在路上、在项目现场、在客户那里、在工厂车间、在仓库等，他们的身份状态也各不相同——兼职、全职、承包商、顾问、临时工、合伙人等，并且使用着种类繁多的硬件设备，而且其中不少设备为员工自己所有，因此传统安全战略恐怕已经不能再提供完整、有效的信息安全保护。

对于企业面临愈发严重的信息安全威胁、日趋沉重的法规遵从合规要求，以及日益复杂的信息环境，IT人员需要更好的方式来控制应用程序、数据和知识产权，同时又不能限制企业自身的生产力、敏捷性和业务增长。对此，云时代的网络准入控制技术应当秉承“为云安全而设计”的宗旨谋求进一步的发展。通过

途径来帮助IT部门重新获得控制权。它将是一种现代信息安全方式，以桌面虚拟化为基础，从设计伊始就以“安全”为主导，其内容包括：

① 通过实施细粒度访问控制政策，可实现针对任何一名员工的安全访问与区域隔离。

② 支持任何为企业提供或员工所拥有的设备，并以安全的方式进行接入管控。

③ 提供全面的监控、活动记录和报告制度，以保护数据，确保终端安全，满足企业的合规性要求。

5.2.2　技术发展方向

在“云”安全中，还有十分重要和关键的一环，就是接入“云”用户的身份认证。传统的“云”认证一般都是采用Windows AD域或加装第三方LDAP服务器的方式来实现的，但许多用户反映要建设一个具有整体性且功能完善的AD域十分复杂，实现及维护工作量巨大，而AD域最大的缺陷在于，对于需要对员工进行入网规范的企业客户来说，当员工逃避管理，不访问“云”资源的时候，则完全可以逃避AD域的约束。此时管理者将面临两难的局面：在辛辛苦苦建设好AD域后，突然发现真正需要与“云”安全结合的其实是一套对“云”用户及所有入网用户结合为一体来进行身份认证和安全控制的准入控制系统；而在AD域的建设上又投入了大量的时间、精力和成本，最终可用性不高。这样的重复投资和重复性维护工作对于投资者将是一个极大的难题。

在传统“云”安全中使用的LDAP服务器则由于安全控制功能太弱，只能完全沦为一个纯身份信息数据库的单一化节点，定位为对已有强安全系统的一个便利型的补充。而在没有强入网控制系统的情况下，这没有任何意义。

对于“云”的建设者而言，“云”架构本身的安全性就在于应用（本质是数据）安全，属于控制层次较高的安全范畴，这对于用户的业务型安全需求是基本符合的。但正因为控制层次太高，在基本IP层或MAC层的控制力度就形同虚设，基本的通信级的接入控制近乎为零，从国际通用的安全标准考虑，忽视底层的安全将带来大量的渗透风险（当然由于应用层的强力控制，这其中可能只有少部分渗透能够威胁到核心数据），但这样门户洞开对于黑客或攻击者的诱惑是相当大的，试想一个每日被不断物理侵入的“云”网络，其虚拟交付平台将承受多大的攻击风险？

换句话说，如果在基本的IP或MAC层就进行接入控制，绝大部分的攻击将在交换机端口级别就得到有效的限制，从而大大减轻云前端虚拟交付台的抗风险攻击压力。这也标志着在用户“云”时代，NAC准入控制系统依然将发挥着至关重要的接入控制功用，通过NAC的底层控制和“云”自身的高层控制，共同打造用户网络的整体安全架构。

5.3 基于云计算的网络准入控制技术

5.3.1 前景展望

通过详细的分析后，对2012年后的网络准入控制市场的发展趋势作出如下预测。

1. 趋势一：将无客户端化进行到底

2012年是国内市场提出无客户端准入的第三个年头，越来越多的机构开始投入无客户端准入的用户阵营。鉴于隐私、实施便捷性、维护度、故障点等多方面的原因，高端客户或对准入有深入了解的客户也更倾向于只需要一台硬件化的设备就能够帮助自己解决绝大多数的问题，One box，One day已经成为了无客户端准入产品的主打宣传词。对于意欲实施NAC的各行业，尤其是在政府行业，无客户端化的准入产品已经成为了必需的配置——鉴于前几个年头桌面产品风风火火的进入及其在2011年中的黯然退出，在信息化建设较为先进的沿海各省份政府机构中，准入选型中的无客户端化已经成为了最基本的要求。当然，必须能够提供可选的客户端配置，尤其对于企业用户来说，NAC所附加的功能（如交互式提醒、虚拟防火墙、准入环境下的软件监测等）是一个增加管理权和控制力度的有效砝码。

2. 趋势二：市场趋于稳定，品牌效应显现

2011年是国内准入市场的第二波浪潮，NAC在各机构中的扩散度堪比iPhone在个人电子消费领域的影响程度，各行业均有众多用户把准入控制列入到年度网络安全建设的预算范围内，甚至有高端用户在几年前已经部署的软件准入系统之基础上，停用原架构而改投硬件准入的阵营——有相当多的802.1x用户中止了原系统的运行。在2011年技术发展的日新月异驱动了许多准入系统的重建设和二次投入。但是繁荣的市场背后却是鱼龙混杂，借安全趋势而投机者大有人在，这正是国内安全市场多年来的发展痼疾：各类产品和厂家都想借时局的东风分一杯羹，但真正在技术领域有深层次积累和专业化投入的纯准入团队却屈指可数。

在2012年后，国内NAC市场将趋于稳定和冷静，因此一大批浅尝辄止的公司将淡出NAC市场而转投其他门槛较低但利润值更高的新概念安全产品，准入控制市场将最终由最具技术性和积累度的原创型品牌担纲领衔。历经了3年的涅槃，准入市场的凤凰将破壁而出，品牌效应将在2012年真正开始显现。

3. 趋势三：第三方无线准入产品面市

无线接入作为数通技术发展的前沿领域已经是一个不争的事实，这一点尤其

在企业中表现得最为明显，2011年已经有高端企业在整个生产区域都实现了无线接入的全部覆盖。对于大部分还在考虑办公大楼无线化的用户而言，这个建设方案实在太前卫了，投入产出比如何还值得考究。

不管无线与有线之争的结局如何，起码欣喜地看到了国内用户对于新兴技术的关注度和投入热情。但在从基础无线部署迁移到大规模覆盖之后，大量的无线通道该怎样建设，以及需要建设到怎样的安全水准也是管理者无法回避的一个问题。目前大部分的无线安全均仅仅停留在2层的控制上，也就是在接入SSID时进行安全认证，比如WPA或WPA2，或常见的802.1x（这又回到了客户端的老调上），但是对于需要在接入层全部覆盖NAC的用户而言，不得不再次强调一个谈论了多年的原则：身份认证≠准入控制。这里可以回到之前所提到的那个大规模无线部署案例，在大规模铺设了专业的WLC、lightweight AP等设备后，该机构中具有前瞻性的管理者已经着手制定了合理的WLAN NAC方案，这里就囊括了基本的3层认证、安全性判别、漏洞修复、虚拟防火墙等整套NAC架构，全部方案基于无客户端模式，而需要强调的是，不同于传统NAC在网关层面所做的工作，WLAN NAC方案的合格要求应该是在接入AP层就实施准入管理，在这样的要求下，目前大部分技术白皮书中以网关技术来“支持”无线AP均只是隔靴搔痒。

对于WLAN NAC方案，国外厂商中也仅有少数网络巨头有整体的设计和产品，例如Cisco，在WLC中直接集成了NAC属性，但要真正用起来，其高昂的费用就不是国内用户所能够承担的了，附加的NAC套件可能比搭建整个WLAN体系的费用还要贵不止一倍。因此对于大部分国内用户来说，要搭建一个比较可行的WLAN NAC方案只能去考虑第三方NAC厂商，况且在兼容性上第三方厂商做的更为优秀。

基于以上背景，在2012年后，国内的NAC大厂将会跟进技术前沿的需求，推出第三方的无线NAC产品。可以预计的是，从2012年中期到今后的2～3年间，WLAN NAC将逐渐成为网络准入行业的主流方案，其所蕴含的高技术含量也将建立起网络准入行业自身的准入门槛。

4. *趋势四：云计算与准入坐拥两大安全体系*

谁也不可否认，2011年不管是在基础运营界还是网络安全界，云的浪潮已经势不可挡。作为资源集中化的最佳解决方案，“云”同样在安全领域带来了摧枯拉朽的效果，可是在大家一阵风似的跪拜在“云”脚下的时候，里面到底是团棉花还是空气就真的不得而知了。对于2012年，甚至5年之内的安全界一个最大胆的预测是——NAC将与“云”共同组成用户内网的两大安全体系。在做好数据集中化与区域安全的同时，准入控制系统则能够对分散的接入点进行充分的安全保障。对于用户而言，由于“私有云”的长期存在，数据的保护和资源的配比将得到有效的控制和管理；而NAC则将从网络层面保护整个云的接入体系和

“端”到“云”的数据传输体系安全。巧合的是，没有任何一个单一的产品能够承担整个“云”体系，也没有任何一个单一的产品能够承担整个 NAC 体系，二者在诞生之时就已经不谋而合，NAC 与“云”的握手必将火星四溅。

趋势仅仅代表着方向，2012 年后的网络准入控制技术和 NAC 市场还会有什么新的奇迹发生？大家拭目以待吧。

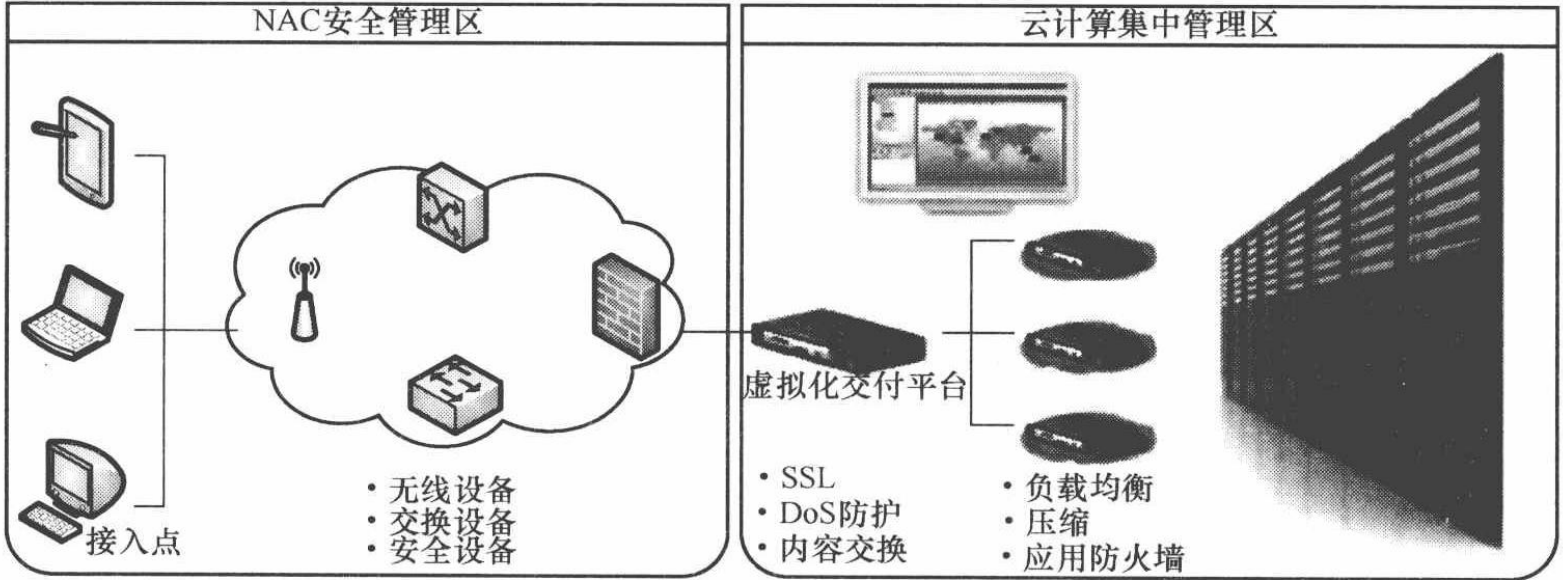
5.3.2 桌面云与网络准入控制技术的结合

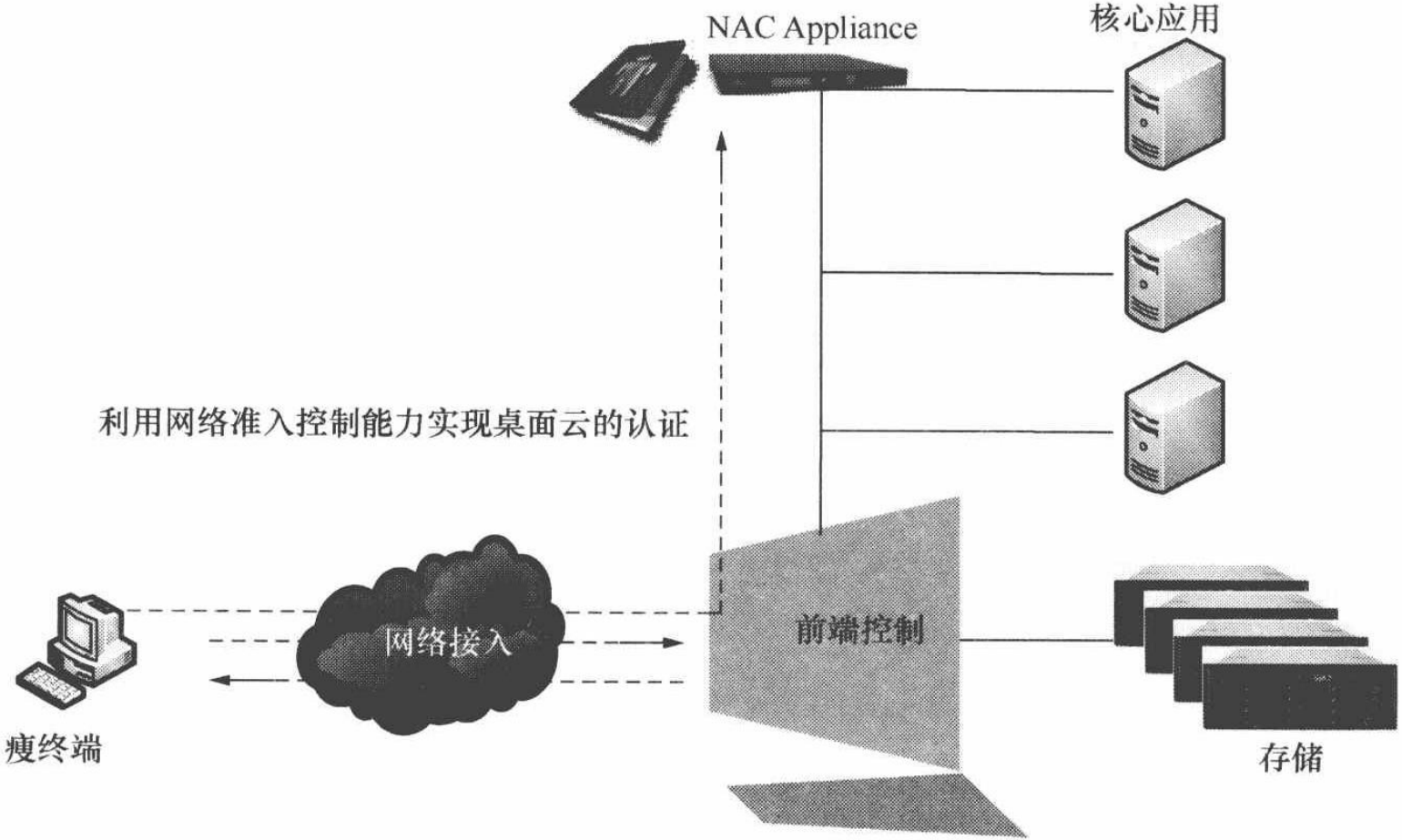
NAC 与云计算的结合点从本质上看就是数据与传输的结合，由云来保证数据安全，NAC 来保障传输安全，如图 5-3 所示。从另一个角度说，NAC 甚至可以参与到传输协议安全标准的制定中，这也符合 NAC 本身博大精深的特性。

图 5-3 NAC 与“云”的握手

以下是一个典型的云计算与准入控制技术结合的应用场景，如图 5-4 所示。

图 5-4 云计算与准入控制技术结合应用


NAC安全管理区
云计算集中管理区
接入点
• 无线设备
• 交换设备
• 安全设备
虚拟化交付平台
• SSL
• DoS防护
• 内容交换
• 负载均衡
• 压缩
• 应用防火墙


NAC Appliance
核心应用
利用网络准入控制能力实现桌面云的认证
网络接入
前端控制
瘦终端
存储

“端”到“云”的数据传输体系安全。巧合的是，没有任何一个单一的产品能够承担整个“云”体系，也没有任何一个单一的产品能够承担整个 NAC 体系，二者在诞生之时就已经不谋而合，NAC 与“云”的握手必将火星四溅。

趋势仅仅代表着方向，2012 年后的网络准入控制技术和 NAC 市场还会有什么新的奇迹发生？大家拭目以待吧。

5.3.2 桌面云与网络准入控制技术的结合

NAC 与云计算的结合点从本质上看就是数据与传输的结合，由云来保证数据安全，NAC 来保障传输安全，如图 5-3 所示。从另一个角度说，NAC 甚至可以参与到传输协议安全标准的制定中，这也符合 NAC 本身博大精深的特性。

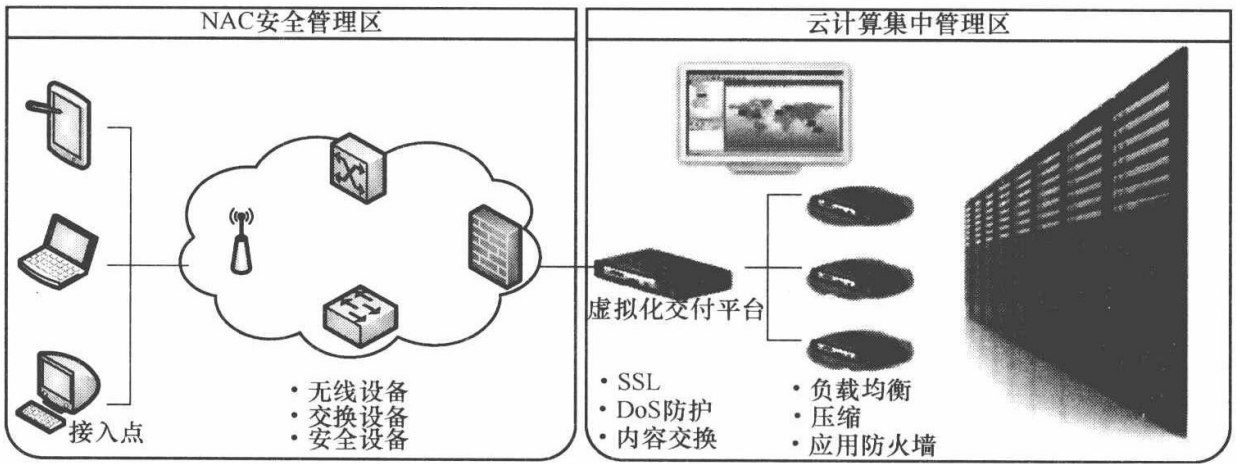


图 5-3 NAC 与“云”的握手

以下是一个典型的云计算与准入控制技术结合的应用场景，如图 5-4 所示。

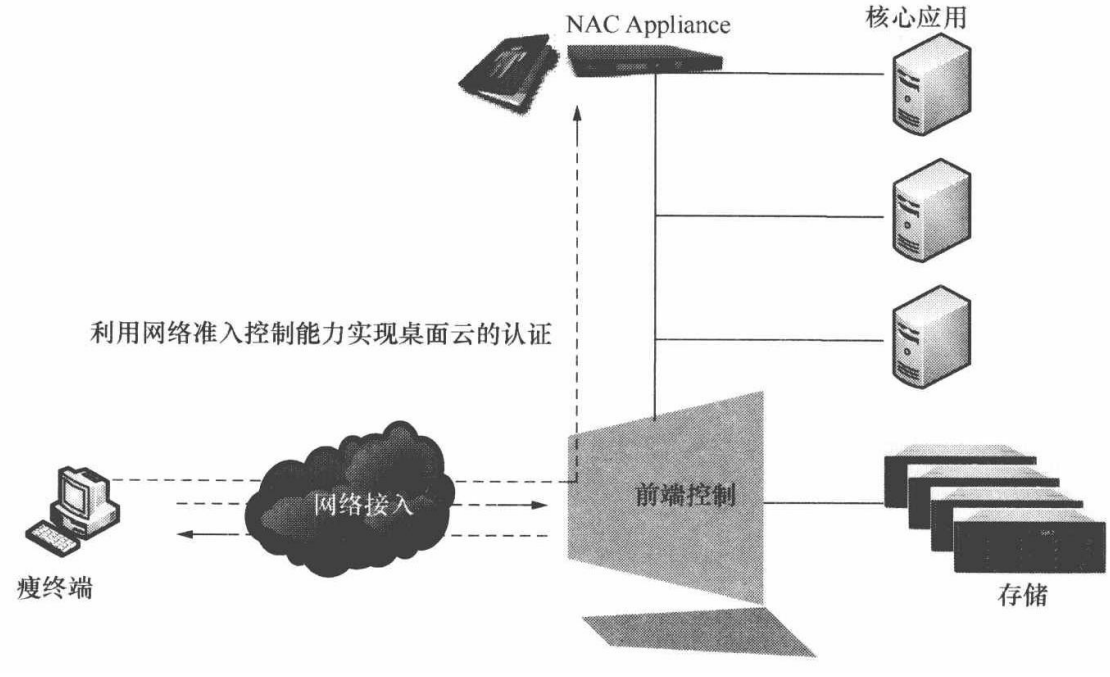


图 5-4 云计算与准入控制技术结合应用

在云保护了核心区域的应用、数据之后，所有需要接入网络（狭义上的物理网络）的终端都必须通过 NAC 的身份认证和安全检查，否则连接入物理网络的权限都没有。

这样的强保护就实现了在核心数据得到管理的同时，另外的非法接入设备也无法对网络内的其他正常访问设备造成威胁，例如蠕虫病毒、ARP 攻击、MITM 攻击等，这样就从数据访问对象和访问源两个角度确保了网络的可信、可靠和高效。

NAC 还是终端安全？这是个问题。不得不承认，NAC 侧重的是入网这一段短途旅行，入网后的计算机管理与审计往往被划归到终端安全层面。在许多用户的基础网络架构还是 Hub＋Hub＋Hub 的情况下，人们不能奢求管理者理清“网”的概念，对于他们能意识到有工具能够帮助管理好终端就足够了，但正如有人说的，没有终端，网就没有了价值，信息也没有了终结点，这正好能解释国内大多数的 NAC 厂商是从桌面终端管理起家的，他们更了解网络的使用者，他们也不会把 NAC 做成像防火墙一样让终端用户到达管理必须穿越层层部门最后到达机房最热辐射最高的地方。但青出于蓝，能否胜于蓝？这是个问题。

夏威夷群岛上的活火山每隔若干年就喷发一次，因为地底需要积蓄能量。NAC 也是一样，当它能够足够适应用户需求的时候，当它的评价标准形成的时候，人们会看到整个行业的力量喷发。让我们对 NAC 的未来说：“Aloha!”。

第 6 章　NAC 项目建设应用实施方法

6.1　NAC 项目建设前期关键要素

作为 NAC 项目的建设，对于项目的提出方和建设方来说都是要求或愿景比较高的，想要做一个成功的 NAC 建设项目，选择一个好的系统方案就至关重要了，通常可以通过以下几点进行综合考虑。

1）功能需求

对于新系统的设计要经过前期调研或需求分析，并将所需功能进行归纳，所选产品应该满足功能需求，即需求分析。

2）前期成本

NAC 系统建设项目一次性投入的费用。

3）中后期成本

项目实施过程中以及项目实施后的后期维护将造成的实施及维护成本。

4）安全性

新系统本身对现有系统的影响，不能因为安全系统让原有系统更不安全。

5）用户体验

新系统的使用者包括系统功能的使用者和系统本身的维护者，应该考虑两者的体验及使用满意度。

6）服务能力

对于新系统需要厂家对系统进行定期和不定期的维护与支持，需要评估其响应速度和服务质量。对于服务能力需在后期实际维护中才能评判。

而对于一个好的 NAC 系统来说，如何真正做到以上几点，需求分析是第一个关键步骤。

6.1.1　NAC 系统建设需求分析确定

项目需求分析是一个项目的开端，也是项目建设的基石。在以往建设失败的项目中，80%是由于需求分析的不明确而造成的。因此一个项目成功的关键因素之一，就是对需求分析的把握程度，进行需求定位。

需求分析定位，是一个项目建设双方相互沟通的过程，一方是项目使用者，一方是项目的设计者，在项目建设过程中，只有双方相互配合，共同对系统进行设计才能最后达到使用的需求。用户方是业务上的熟悉者，对业务流程有非常清晰的了解，但是对于需求方面的描述不甚了解，所能提供的只是他们最终要达到的功能，这其中包含的业务流程、系统流程又是非常复杂的。如何让需求真正合

理地得到解决，必须进行严密的需求分析，而在需求分析阶段解决问题的代价是最小的，越往后就成指数级递增，因此，要建设一个成功的项目，冷静的分析才是最关键的。

同样在进行 NAC 的项目建设中，实际需求定位是一项非常重要的工作，也是最困难的工作，需求是项目建设存在的意义所在，而需求的变化会让项目建设双方头痛不已，明确的需求定位能够给 NAC 项目建设带来极大的帮助。

因此，在投入时间和金钱之前，先问自己如下几个问题，只有这样你才能更好地定义自己的目标。

（1）需要保障安全的是什么对象？

（2）我们在什么地方缺乏安全性，NAC 如何帮助我们解决？

（3）实施一个 NAC 解决方案的总体影响是什么？

（4）除了保障 PC（或其他的任何目标）的安全，对工作人员、终端用户、在外的销售人员、远程访问用户会有什么影响？

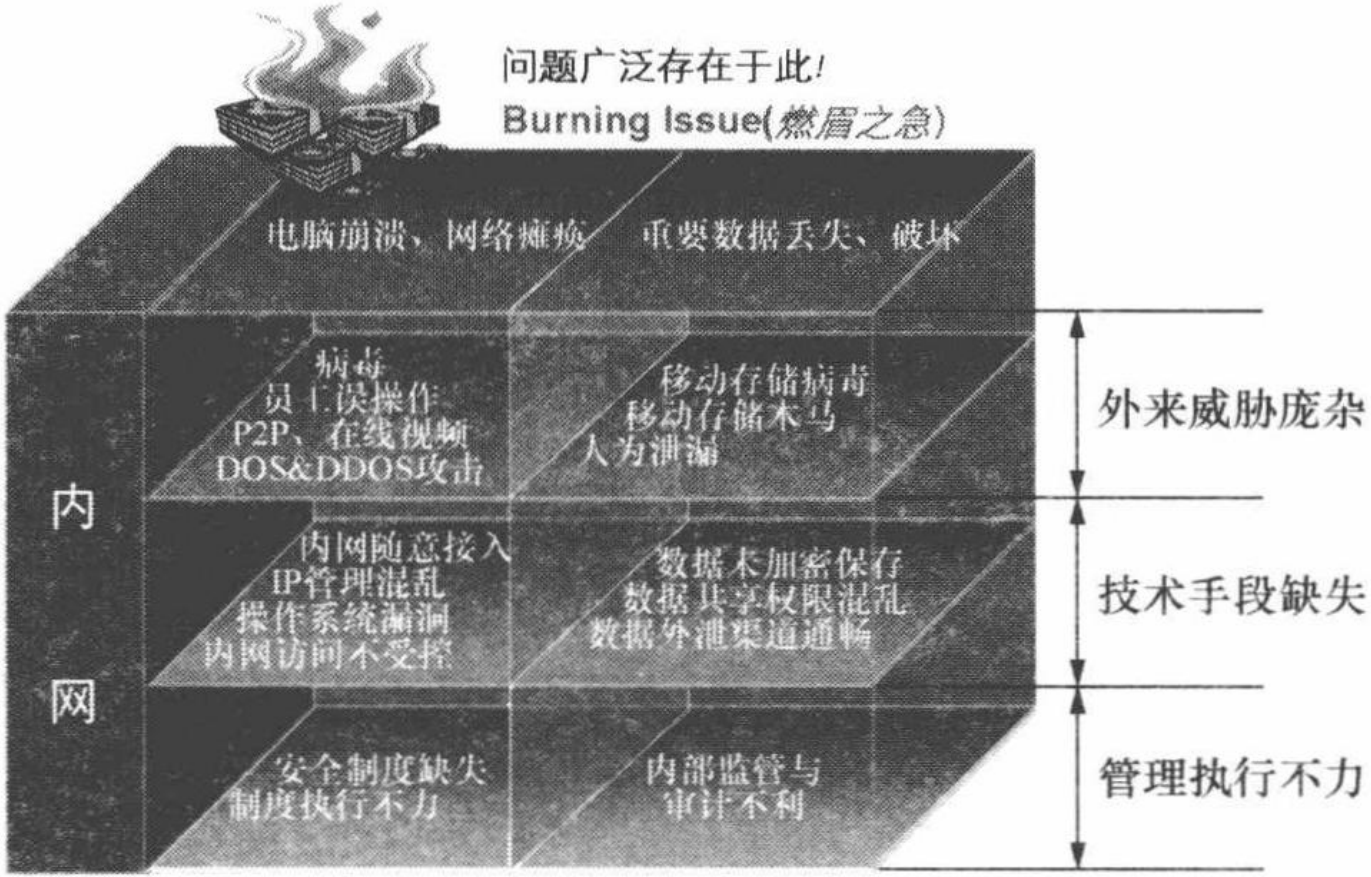
（5）实施 NAC 方案的收益与由此引起的影响孰轻孰重？

（6）在这个时点上你真的需要采用 NAC 吗？

随着各类网络规模不断扩大，企业内网面临的问题越来越多，所在的办公网络是否经常遇到网络瘫痪、计算机终端操作系统崩溃的情况？或者是保存在核心服务器或计算机终端中的重要数据遭到破坏、丢失？这些问题爆发的表现形式看似简单，究其根源，却往往包含了管理执行、技术手段、外来威胁等多个层面的原因，如图 6-1 所示。

图 6-1　内网问题来源

由于缺乏技术和管理手段结合，许多管理规定仅仅是一张纸，难以执行到位。例如：未安装指定的防病毒软件、桌面管理软件，不及时更新系统补丁，在个人使用的计算机内安装 BT 下载软件，私自更改电脑的安全设置，将内部网络的电脑连接到互联网等行为。这些行为违反了单位的管理规定，也影响的计算机网络的安全性，如果情况严重可能会导致网络瘫痪。


问题广泛存在于此!
Burning Issue(燃眉之急)
电脑崩溃、网络瘫痪
重要数据丢失、破坏
病毒
员工误操作
P2P、在线视频
DOS&DDOS攻击
移动存储病毒
移动存储木马
人为泄漏
内网随意接入
IP管理混乱
操作系统漏洞
内网访问不受控
数据未加密保存
数据共享权限混乱
数据外泄渠道通畅
安全制度缺失
制度执行不力
内部监管与
审计不利
内网
外来威胁庞杂
技术手段缺失
管理执行不力

理地得到解决，必须进行严密的需求分析，而在需求分析阶段解决问题的代价是最小的，越往后就成指数级递增，因此，要建设一个成功的项目，冷静的分析才是最关键的。

同样在进行 NAC 的项目建设中，实际需求定位是一项非常重要的工作，也是最困难的工作，需求是项目建设存在的意义所在，而需求的变化会让项目建设双方头痛不已，明确的需求定位能够给 NAC 项目建设带来极大的帮助。

因此，在投入时间和金钱之前，先问自己如下几个问题，只有这样你才能更好地定义自己的目标。

（1）需要保障安全的是什么对象？

（2）我们在什么地方缺乏安全性，NAC 如何帮助我们解决？

（3）实施一个 NAC 解决方案的总体影响是什么？

（4）除了保障 PC（或其他的任何目标）的安全，对工作人员、终端用户、在外的销售人员、远程访问用户会有什么影响？

（5）实施 NAC 方案的收益与由此引起的影响孰轻孰重？

（6）在这个时点上你真的需要采用 NAC 吗？

随着各类网络规模不断扩大，企业内网面临的问题越来越多，所在的办公网络是否经常遇到网络瘫痪、计算机终端操作系统崩溃的情况？或者是保存在核心服务器或计算机终端中的重要数据遭到破坏、丢失？这些问题爆发的表现形式看似简单，究其根源，却往往包含了管理执行、技术手段、外来威胁等多个层面的原因，如图 6-1 所示。

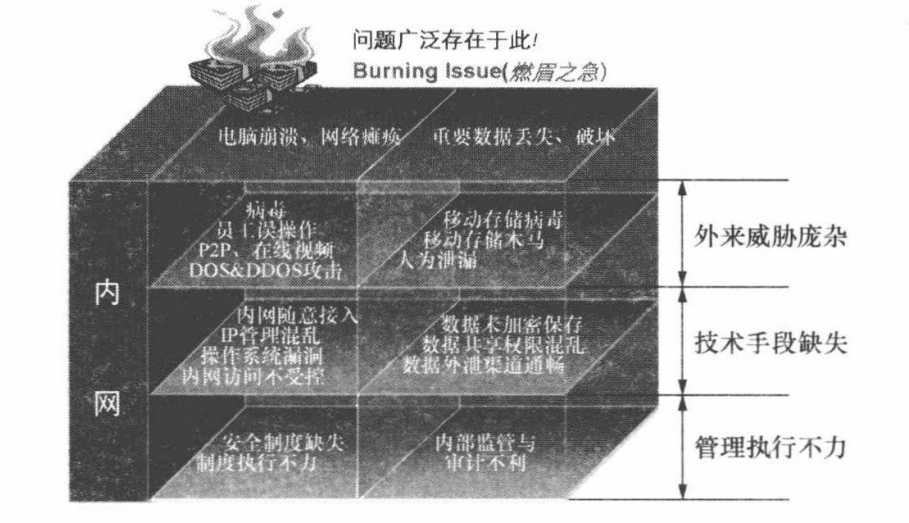


图 6-1　内网问题来源

由于缺乏技术和管理手段结合，许多管理规定仅仅是一张纸，难以执行到位。例如：未安装指定的防病毒软件、桌面管理软件，不及时更新系统补丁，在个人使用的计算机内安装 BT 下载软件，私自更改电脑的安全设置，将内部网络的电脑连接到互联网等行为。这些行为违反了单位的管理规定，也影响的计算机网络的安全性，如果情况严重可能会导致网络瘫痪。

单位内部有大量的机密文件，对于终端接入网络的方式纪委灵活，直接威胁各类信息的机密性，例如私接 Hub、无线 Wifi 等。由于移动终端的便利性，为人们的日常工作中提供了很多方便，但容易形成网络管理盲点，带来了前所未有的安全威胁，因为它已经成为了网络终端管理的最大难点。

此外，由于桌面计算机的数量非常多，地理位置分散，给日常的管理维护带来了很大的困难，这些困难包括：难以对计算机的资产、配置进行统计；由于补丁、漏洞、升级等问题频繁，维护工作量很大；计算机的使用人员技能不一，有些很小的问题都需要维护人员现场解决，降低了维护的效率；无法对计算机进行批量维护，例如：批量安装软件、批量打补丁、批量设置计算机的安全设置。

信息安全等级保护办法对于二级信息系统的要求中，对于网络准入有相应的管理与技术要求。通过网络准入控制系统的部署，提供统一的、集成化管理平台。向 IT 系统管理员提供一个统一的登录入口，有整体的终端安全视图，呈现整个计算机网络系统中所有终端设备的安全运行状况。管理员不仅可以看到终端安全的运行状况，终端的安全设置，也能够看到终端的软件配置、硬件配置、终端的物理位置等信息。

在实际管理中，大部分的网络都是逐步建设起来的，规模庞大，结构复杂，每个阶段都具有当时的技术特点，有本地管理网络，也存在远程移动办公接入，有 Hub 接入方式，也存在无线 Wifi 网络模式，不具备统一性、标准性，管理员面对如此复杂的网络情况，以及多种多样的准入控制管理方式，是要做到接入层精确控制，还是针对重点区域进行可信安全接入，成为方案选择中需要进行取舍权衡的。

通过统一的集成化的管理平台，管理员可以完成所有与终端安全管理维护相关的各种任务，具体包括：网络准入控制管理；设备快速定位；存储设备注册管理；终端安全补丁管理；终端基本信息管理；终端的软件推送；终端安全策略加固，包括：主机安全漏洞策略、防病毒安全策略、非法外联策略等的设置。

6.1.2 NAC 系统建设技术方案选型

端点安全是近年来信息安全领域的一个热门话题，这并不奇怪。不管你多么努力地防御网络边界，漫游的笔记本电脑和设备总是必然会把蠕虫、病毒和间谍软件带入到你的网络上。

配置了无线适配器的大众化笔记本电脑具有的移动功能解放了大批员工，他们可以在任何地方办公，无论在办公室、在家里，还是在路上。咨询顾问和厂商可能连接到你的网络使用一小时或者一天——你如何防范他们可能带来的潜在危害呢？

网络基础设施和操作系统软件领域的巨头：Cisco、H3C 和微软各自都启动了这方面的计划，确保端点设备只有符合安全策略，才可以访问内网。并不奇怪的是，Cisco 的网络准入控制（C-NAC）依赖 Cisco 的交换基础设施，H3C 的终

端准入控制（EAD）亦以自身的网络产品为平台；而微软的网络访问保护（NAP）通过 Windows 操作系统发挥作用。除了这些普遍但专有的方案外，可信计算组织（TCG）正在开发基于标准的可信网络连接（TNC），同时还存在一部分提供准入安全解决方案的第三方厂商，如盈高科技等，他们提供的是自身的准入安全解决方案，由于是与 Cisco、H3C 或 TCG 方案相结合的，也更具扩展性的通用性解决方案。

那么问题又出现了：如果让你来选择，该选择哪个方案来保护端点安全，让本地网络避免终端机器的安全漏洞影响呢？

面对需要立即引起注意的安全问题，你应当寻求这样的解决方案：可以定义细粒度策略、检测连接到网络上的每个设备、评估遵从策略的级别、执行访问策略，以及补救未遵从策略的机器。

这对任何一个安全系统来说都是过高要求，积极采用端点安全并非易事。之前反复提到过的三大架构：C-NAC、NAP 和 TCN 都不完整，实施成本也很高，而且很复杂，不易理解。它们都从不同方面来处理端点安全问题，所以彼此并非相互排斥也就不足为怪了。

（1）Cisco 的 C-NAC 专注于网络基础设施和策略定义及管理。当然，它假定你会使用许多 Cisco 路由器，采用 Cisco 的安全解决方案；而且在将来牢牢保护端点时，希望继续使用 Cisco 的系列产品。

（2）微软的 NAP 偏重于健康评估和补救方案。它假定你从微软服务器和桌面系统开始着手，并且假定你主要关注的是确保它们安全运行。

（3）可信计算组织的 TNC 采用了粗略的架构方案。它假定每个桌面系统都含有一种专门的硬件，负责验证端点的安全未遭到破坏，并且依靠这个硬件来监控及执行端点策略。

不妨看一下这些方案，看看它们声称具有的功能以及各自存在的不足。

1. Cisco 的 C-NAC

C-NAC 处于领先位置，这归功于同时出现了支持它的架构和产品。C-NAC 旨在通过实施在路由器和交换机以及 Windows 和 Linux 客户端中的可信模块来保护网络访问。

现有众多厂商支持 C-NAC，理由很充足：你需要其中几家厂商来组建一套完整的解决方案，以便满足端点安全需求的所有 5 个方面。你至少需要在端点上运行两个代理，才能处理比较复杂的策略以及检查遵从 SSL VPN 的情况。

C-NAC 使用的客户软件 Cisco 可信代理（Cisco Trusted Agent）负责收集设备信息，并使用 802.1x 机制，把信息传送到 Cisco 的远程验证拨入用户服务（RADIUS）服务器：安全访问控制服务器（ACS）。而 ACS 与第三方策略服务器（反病毒和补丁）进行通信，确定遵从情况，并通过交换基础设施执行网络访问。

有些分析师认为，C-NAC 需要部署太多的部件；实施起来可能有难度，因为要管理所有的互联网操作系统（IOS）更新工作，以便各部分协同工作；而且基础设施出现变化时，需要维护。

C-NAC 的问题在于：它自身会带来全孤岛；依赖 Cisco 的 RADIUS 服务器作为唯一的验证机制；而且 Cisco 交换机需要最新版本的固件。此外，C-NAC 不一定与 Cisco 的早期基础设施协同工作，除非早期设施更新到最新固件。

英国电信 Radianz 公司是一家面向金融服务行业的知名 IT 服务商，公司副总裁兼首席安全官 Lloyd Hession 说："C-NAC 问题的一方面在于，你必须升级 IOS 版本。我的网络上共有 4 万个路由器，对它们进行更新可不是容易的事情。" Hession 改而选择了 ConSentry 公司，那样他不需要对网络进行 MAC 层过滤和访问控制。ConSentry 销售的嵌入式安全设备能够自动评估及执行端点安全策略，确保遵从策略。

另外，C-NAC 架构缺少补救功能——它在管理端点本身的补丁级别方面不尽如人意。另外，设备经过评估后，采取什么措施方面缺乏很强的灵活性。只有这两种情况：要么通过评估，允许连接到网络上；要么未通过评估，被转移到访问权限有限的某个虚拟局域网（VLAN）上。

Altiris 公司的产品经理 Rich Lacey 负责处理本公司的 C-NAC 兼容产品，这种产品提供了通过桌面管理和复制来补救的解决方案。他说："通过补救机制，让客户端摆脱隔离区域，这确实是一门技艺，这也是我们现在所做的。"

Cisco 得到了迈克菲、趋势科技和赛门铁克等反病毒产品的支持，另外还得到了几家软硬件厂商的支持。

Hession 并不觉得把代理安装到所有端点上特别吸引人。他说："代理存在的问题在于，你最终不得不安装多个代理，以便支持你想要处理的所有事情，比如反病毒和访问控制。Cisco 的 C-NAC 迫使我往代理这个方向走，但我不想走这条路。"

Cisco 公司安全技术部门的产品经理主管 Russell Rice 说："我们目前支持代理。但我们也会开发无代理的解决方案，那样就能主动扫描及评估其他非 Windows 设备。"

C-NAC 正在把支持范围扩大到代理以外的领域，而 Qualys（其产品 QualysGuard 支持 C-NAC）等厂商正在提供这种服务：可支持无代理监控无法使用代理的网络设备，比如打印机及其他嵌入设备。

2. 微软的 NAP

NAP 还没有实施在任何产品中，不过这项方案得到了 60 多家厂商的支持，其中许多厂商为了保险起见，同时支持 C-NAC。

NAP 把安全策略管理和执行功能集成到了 Windows Server 中——自活动目录的早期以来，Windows Server 就多少缺乏这种功能。

微软公司负责 NAP 的 Windows Server 事业部的集团产品经理 Mike Schutz 说："NAP 将会提供通过各种机制来执行策略的功能，使用验证主机的 IPSec、802.1x，或者通过 VPN 或 DHCP。"

与 C-NAC 一样，NAP 也使用客户软件：隔离代理（Quarantine Agent），把信息传送到微软的网络策略服务器；与 Cisco 的 ACS 一样，网络策略服务器也与第三方服务器一起检查遵从策略的情况。NAP 承诺会提供多种执行选项，包括 DHCP、IPSec VPN 和 802.1x。

NAP 最初将单单支持 Windows XP SP2、Longhorn Server 和 Windows Vista，需要在每个设备上安装 NAP 更新。这将给使用旧版本 Windows 的公司带来问题，而且需要使用新的操作系统，还要测试及管理 Windows XP 升级。另外，验证和执行服务器即 DHCP 和 RADIUS 服务器将需要 Longhorn，这就需要进一步升级，NAP 的专有性因而更明显了。

Schutz 说："我们并不认为 C-NAC 和 NAP 是两者择一的情况。我们已宣布，我们将开展互操作性解决方案方面的合作，那样客户就可以选择满足自身需求的最佳方案。"不过，微软和 Cisco 目前都还没有与 TCN 解决方案兼容，眼下也没有这方面的计划。

佐治亚州富尔顿县政府已经在试用 NAP，使用早期版本的微软服务器和 Windows Vista 桌面电脑及笔记本电脑。

负责管理该县 IT 部门部署 NAP 的 Keith Dickie 说："一切都仍处于测试中。不过我们的几名 IT 员工正在生产环境的机器上使用 NAP，没有任何问题，包括把赛门铁克的诺顿反病毒软件与微软的 SMS 和 Windows 服务器集成起来。"

该县在使用 IPSec 验证，部署的 NAP 可以检查一系列健康要求，包括确保诺顿反病毒软件的版本最新。

3. 可信计算组织的 TNC

TNC 由支持一批开放标准的几十家业界重量级公司（Cisco 除外）组成。好消息就是，标准或多或少符合之前提到的网络访问控制安全的 5 个要求：策略定义、检测、评估、执行及补救。坏消息是，不是所有标准都已经得到了定义；糟糕的是，也没有多少产品支持真正实施解决方案所需要的大部分标准。

TNC 的关键要素是支持 RADIUS 和 802.1x 验证服务器和协议的功能，另外还有端点上的可信硬件芯片和软件。

TNC 的联合主席、Juniper Networks 公司的产品经理 Steve Hanna 说："这可不是需要全面改动的叉车式升级（forklift upgrade）。"它与 Cisco 采用的方案有着尤其明显的区别，后者使用 Cisco 的 ACS 验证服务器。

名为可信平台模块（TPM）的一种公钥基础设施（PKI）芯片增强了验证功能，有助于通过硬件实现方案来防止软件遭到潜在破坏，从而保护笔记本电脑的安全，远离未授权用户，比如窃贼或者仅仅捡到丢失笔记本电脑的人。

Hanna 说："如今你根本没法信任软件，因为 PC 可能遭到了零日漏洞（Zero-Day vulnerability）或者用户通过互联网下载的东西的破坏。要发现这个问题，唯一的办法就是借助可信硬件。"许多笔记本电脑厂商已经把可信硬件模块添加到了各自的产品线当中，包括戴尔、富士通、惠普和联想。

一旦验证检查获得通过，可信硬件里面的程序就会把控制权交给第三方软件代理，由代理检查设备遵从策略的情况，与负责处理网络验证和登录访问的 TNC 架构协同工作。作为一项开放标准，TNC 有望使用任何一种执行机制。

Cisco 的竞争对手 Juniper 已经在提供符合 TNC 的产品，这不足为怪。Juniper 之前收购了开发 RADIUS 服务器产品的 Funk 软件公司。

4. SSL VPN 支持是软肋

上面介绍的这三款解决方案都缺少了支持 SSL VPN 有功能。TNC 的 Hanna 说："谁都没有支持 SSL VPN 的任何产品，我们还无法支持它。不过我们预计很快就会出现这样的功能。"

SSL VPN 方面要走很长的一段路。没多少厂商提供支持众多反病毒扫描器的功能，许多只支持 Windows/IE 组合，或者在网络登录之前扫描网络连接。问题的一方面在于，大多数 VPN 厂商在完成开发了第一批产品之后才添加了支持端点安全的功能。举例说，北电网络（Nortel）和 Aventail 在各自的 VPN 产品中有两套不同的访问控制——一个支持端点安全，而另一个不支持。许多 SSL VPN 厂商正与第三方端点安全厂商合作——提供 C-NAC、NAP 和 TNC 之外选择的市场在日渐壮大。

虽然 Cisco、微软和可信计算组织之间的营销大战日渐升温，但企业在寻求这样的解决方案：眼下管用，又可能支持 C-NAC、NAP 和 TNC，以便将来升级。有几家厂商现在交付的产品至少能够满足保护网络访问的部分要求。

这些产品提供众多检查及执行选项，以控制得到管理及没有得到管理的设备，并且为客户提供了很大的灵活性。许多产品提供基于登录、代理、ActiveX 或者 Java 的扫描方法，确定端点遵从策略的情况；可以根据自身的要求，对这些扫描方法进行混合搭配。另外，这些产品日益提供 DHCP、802.1x、基于代理的、嵌入式设备或者 C-NAC 等选择，而不是单一的执行机制，所以企业确实可以选择与自己的环境一致的方案。

实际上，Cisco 拥有与自己的 NAC 架构并不完全相符的第二种方案，名为"干净客户机访问"（Clean Client Access），这是它收购 Perfigo 公司的成果。它能够实现基于代理的端点评估、客户机与策略管理以及补救等服务。

5. 选型过程中应重点考虑的问题

事实上，没有哪家厂商拥有完整的解决方案可以保护用户的所有端点确保资源安全。要找到一款产品来处理不同的安全策略，从而保护那些漫游笔记本电脑

和关键的网络资产。另外，除非你有一个完全同类的网络，全部由运行 IE 的 Windows XP 用户组成，否则就需要支持其他操作系统和浏览器。尽管厂商的说法都很动人，但没有哪家厂商即将提供可与代理技术和无代理技术一起使用的通用的端点解决方案。

如果你坚持使用 Windows XP/IE 环境，如果所有用户都使用管理员权限来访问系统，如果你不介意他们通过浏览器下载某种 Java 或者 ActiveX 应用程序，那么你使用其中一种第三方设备产品，或者使用 Juniper 和 Aventail 等公司提供的 VPN 解决方案，差不多就能如愿以偿。

如果微软的 NAP 远景与你的远景相一致，不妨使用 Windows ISA Server 运行 VPN 隔离机制，以此获得先机。而如果你把所有 Cisco 路由器更新到最新版本，而且继续一律使用 Cisco 的产品，那么 Cisco 及合作伙伴的其中一款 NAC 解决方案可能适合你。

但如果上述场景不符合你的情况，你就要安排好工作，实施最佳的端点安全解决方案。与所有信息安全项目一样，最可靠的忠告就是，全面了解企业和业务需求，要弄清楚以下的问题。

（1）移动员工有哪些？他们使用哪些操作系统和安全应用软件？他们又如何连接到网络上？

（2）顾问和厂商经常访问网络吗？

（3）你的网络基础设施是什么？它支持哪些执行/补救机制？它是同构网络吗？它是比较新、使用最新版本的固件吗？有没有无法支持基于网络的解决方案的遗留路由器和交换机？

因此，在 NAC 方案的选择过程中，NAC 方案与现有网络架构的契合度，准入技术的成熟度、系统部署的灵活性、准入系统的高可靠性、以及良好的可扩展性等方面，成为 NAC 系统建设方案选择的重要关键点。你要自行决定如何保护访问网络的端点。要选择这样的解决方案：至少应该满足那些最关键的需求，而且一定要与将来的计划相一致。

6.1.3　NAC 系统建设关键要素总结

NAC 系统的建设，按照第一章提到的 5 条关键准则，结合自身的实际情况，还应着重考虑以下几个关键要素。

1. 具有很好的网络环境适应性，不需要大幅调整网络结构

一般考虑到要上准入控制系统的单位，信息化建设已经达到一定高度了，网络环境已经建设好，存在多种复杂网络设备。作为网络准入控制系统的选择，一定要考虑产品是否支持多种入网强制技术，以适应各种网络环境的复杂性。

所以选择的产品必须能够适应用户多种多样的接入环境，尽量避免改造用户网络，要求产品支持多种入网强制技术，能够适应各种网络设备及环境。像

Cisco设备、H3C设备、华为设备、中兴设备等，另外像VPN接入网络，Hub网络、无线网络等。

2. 选择成熟的、先进的网络准入控制技术方案

现在各种厂家介绍了很多种网络准入控制的技术解决方案，那么我们先要了解一下现行的网络准入控制框架都有哪些？他们分别有什么优缺点？网络准入控制未来的发展趋势是怎么样的？

如前所述，根据美国著名调研机构Gartner研究，他们把所有的NAC厂家、技术统一做了归类与分析，提出了3个NAC技术框架的理论。

（1）基于端点系统的架构——Software-base NAC；主要是桌面厂商的产品，采用ARP干扰、终端代理软件的软件防火墙等技术，像北信源、LanSecs等。

（2）基于基础网络设备联动的架构——Infrastructure-base NAC；主要是采用802.1x技术的产品。

（3）基于应用设备的架构——Appliance-base NAC；主要是专业准入控制厂商，如盈高科技公司的入网规范管理系统。

综观这3种框架的进化与发展，现在完全基于Software-base的架构，范围及控制力度有限，目前已不被用户接纳；而大多数网络设备厂商现在主要推崇Infrastructure-base的架构，可以促进他们网络设备的市场销售，但存在互相设置壁垒的问题；现在国外比较新兴的是采用Appliance-base架构的NAC设备，在部署应用方面有优势。

目前市场认可度比较好的NAC方案，是集成了成熟的第二代Infrastructure-base架构以及第三代Appliance-base NAC架构，融合两者优点的方案。

3. 能够支持快速部署的，良好的用户体验

一个好的准入控制产品一定要能够让各类用户接受，能够快速部署，并且在部署时具有友好的Web引导界面；让终端用户一目了然，可以减少管理员很多工作。用户上准入控制系统的目的，就是要将之前经常出问题的网络从源头上保护起来，但是安全性与易用性需要一个平衡的，如果一味地追求安全性，而给已经超负荷的管理员增加很多额外的工作，会对系统的建设、运营都将带来非常严重的阻碍。

所以在选择产品时要看，是否支持快速部署，是否提供友好的Web引导界面，终端最好不要安装客户端。

4. 具有高可靠性，一定要有很好的逃生方案

用户一旦建成网络准入控制系统后，就意味着所有终端每天进入网络，都依赖于这套网络准入控制系统的解决方案。现在市面上的网络准入控制方案有纯软件、有纯硬件也有软硬件结合等多种。建议用户一定要选择具有高可靠性的、系

统集成度高的成熟方案，不要因为先期的低廉带来后期高额的维护成本；另外选择无论哪种方案，一定要求有完善的逃生方案，具备“Fail-Open”模式，不存在单点故障。绝对不能因为网络准入控制系统的建设影响业务连续性，影响正常办公业务开展。

5. 具有较好的可扩展性，能够提供不断更新的安全检查引擎和规则库升级

在选择网络准入控制产品时，应该要考虑产品是否具有很好的可扩展性，在产品的架构上是否可以很好地实现扩展，方便升级，可以满足企业未来几年的发展。尤其是像安全检查规范库、补丁漏洞库、支持联动的防病毒软件、支持联动的终端安全管理软件以及入网强制技术适配器等。

6.2　NAC 项目建设中期关键要素

6.2.1　NAC 项目建设实施策略

NAC 项目建设是一个复杂的系统工程，涉及到网络架构、应用系统以及大量的用户。因此，为了实现既定的总体目标，必须制定明确的项目实施策略。

1. 总体规划、分步实施

“总体规划、分步实施”的策略是 NAC 系统顺利实施的重要策略之一。NAC 系统项目作为信息安全的重要应用项目之一，要按照总体信息安全架构统一部署。在总体规划的同时，将系统的建设目标分解为若干可操作控制的项目目标，分步实施，保证实施一个部分，整体进程推进一步，收获一份成果。同时在整个项目推进过程中，必须紧紧抓住主线、突出重点。系统建设重点除完成信息化安全设施的部署之外，还要重点关注相配合的安全管理制度，以确保系统的顺利实施。

2. 先试点、后推广

在实施的过程中，笔者认为采用先进行项目试点，后全面推广的原则比较适合 NAC 项目建设。在组织架构内，需要选择合适的试点部门或下属单位。选择过程中，笔者认为应该依据如下一些指导原则。

（1）广泛调研，集中试点，即在调研的过程中通过多样本调研，充分了解不同部门的信息安全需求，反映各单位和部门的安全需求的多样性；在调研单位的基础上，进一步筛选能够集中体现不同类型安全需求的 2～3 个部门或下属单位作为试点单位。

（2）充分考虑对 NAC 系统建设的迫切程度和部门领导对 NAC 项目的支持，试点部门应选择对 NAC 系统有迫切需求且部门领导对项目非常支持的单位。

（3）考虑实施的人员条件，尽量选择有对信息化和信息安全有足够认识的部

门参与试点工作。

(4) 考虑管理水平，应选择具备相当的管理水平，以便能够快速适应 NAC 系统上线后的安全管理工作的要求。

(5) 要考虑具有集中的代表性，所选的试点部门应能够集中体现组织中各部门的大多数共性条件。

3. 加强安全理念宣传贯彻与系统培训

NAC 系统实施的关键环节中还包括安全理念的宣传贯彻与系统的培训。NAC 系统的建设并不仅仅是一个安全产品的部署过程，同时也是一个信息安全理念的宣传贯彻和培训的过程。因此，在系统建设的同时，就要及时安排相关的讲座及培训。

对于参与项目的信息部门及试点部门的关键用户要带动他们在项目进行过程中边干边学，在项目进行中培养相关能力。要发挥骨干人员的以点带面的作用，使得他们对信息安全理念、应用、操作等方面得到全面培训，将他们从业务专家培养成信息安全应用的专家，并使这些骨干到各单位后能够进行安全知识的内部培训，成为信息安全知识传播的力量，为 NAC 项目的全面铺开上线奠定人员基础。同时，要加强宣传贯彻和培训的统一管理。通过建立统一的培训支持体系，培训讲师可以及时反馈情况、获得有力的支持，进一步加强培训能力。另外，还要针对不同层面的用户采用有针对性培训。将针对管理层、操作层、用户层等不同培训对象，提供与之相适应的培训内容。

6.2.2 NAC 项目管理制度制定

进行 NAC 项目建设本身就是对网内终端的要求是安全的，更为安全的终端才能打造出安全的网络环境，任何一台终端设备存在漏洞就代表整个网络存在漏洞，安全威胁时刻存在的网络中，只有主动地去检测威胁、分析威胁和阻断威胁才能更好地防患于未然。但针对大型单位来说，行政手段上的执行力度并不如想象中的那么优秀，一些网络安全措施在推广到每个员工时并不能很好地得到执行，员工计算机水平的参差不齐也是其中的主要原因。如何才能更好地推广网络安全措施，更为强制地、主动地去执行，满足单位对网络安全的要求，成为单位信息化成长过程将要考虑的问题。

用户在制定入网规范方面可以遵循单位自身的安全管理制度和实际情况进行灵活制定。规范的应用可以分为以下几个部分。

1. 常规性检查项

常规性检查项如防病毒软件及病毒库更新检查、补丁安装检查等，均为网络安全的基础门槛，这对于大多数用户来说都是比较看中的需求点，特别是补丁服务器，需要定期提供微软相关补丁信息，为网络的补丁安全提供保障。

2. 加固性检查项

加固性检查项主要是在常规要求基础上对安全的提升，旨在进一步加固每个终端的安全性，如软件安装检查、Guset 来宾账户检查、弱口令账户检查、运行进程检查等。

3. 自身特点检查项

自身特点检查项在基础安全门槛的基础上，就自身网络需求，基于现有应用、业务系统特点，与准入系统结合，做到统一管理，实现整体升值，包括桌面管理系统客户端检查、域用户检查、计算机名称检查、屏幕保护设置检查、违规外联检查等。

根据上述情况，以常规性检查为主，辅以加固性检查项，结合自身特点，以单位安全管理制度为基准，制订符合单位网络特色的安全检查规范，在实际应用中，分身份、分部门等情况，制订不同的安全检查要求，做到酌情考虑。如本单位内部员工需要安装统一的杀毒软件、安装桌面管理系统客户端、加入 AD 域等要求，符合要求后能够访问内部资源；而来宾用户要求有所不同，只需要安装了防病毒软件，没有系统漏洞等，无需安装桌面管理客户端，入网以后只能访问有限的网络资源等，这样单位的安全制度能够得到保障，又能做到区别对待。

6.2.3　NAC 项目实施风险管理

在系统建设中另外一项重要的成功因素就是风险管理。因此在项目的实施前就应充分考虑到所面临的风险，并提前准备相应的应对措施。以下将主要分析 NAC 项目建设的主要风险及解决方案。

1. 技术风险

前文已经充分讨论了 NAC 系统目前所采用的种种技术方案，并分析了各种方案的利弊及适合的条件。因此，综上所述，在规避技术风险的时候，我们将采用如下应对措施。

（1）充分了解项目目标及用户需求，在需求清晰的基础上选择合适的技术路线和方案，降低技术路线选型风险。

（2）选择能够提供更完善技术支持的平台和开发工具的提供商。借助厂商方面的技术力量和服务，可以减少系统实施部署和运维的难度，降低此方面的风险。

（3）加强人员培训。要充分考虑并针对各类安全服务与运维人员及最终用户制定明确详细的培训计划，以使他们尽快掌握新的平台与技术，为系统提供更好的支持。

2. 产品风险

在NAC项目建设中的核心产品的选择上，应尽量选择基于优秀的产品架构、灵活的可定制性和完善的功能的产品。然而NAC系统在技术上的最大风险就在于产品与系统需求间匹配性上的差异性。这种差异如果过大将导致系统实施的难度增加，并引起用户对系统的认可度下降。

对此我们将采用如下应对措施。

（1）进行细致全面的需求调研。确保最大限度地涵盖用户需求的各个方面，降低NAC系统实施的风险。

（2）仔细选择实施策略。针对产品不同功能模块与客户需求差异度，可以要求供应商采用部分定制的策略，并针对用户使用习惯进行调整，以增加用户对系统认可度，降低实施风险。

3. 组织风险

项目实施的组织风险主要包括人类资源投入不足、实施人员能力有限、用户不能明确表述需求以及实施范围扩大所带来的项目延迟等风险。

为避免类似风险可按下列方法实施。

（1）加强项目的管理力度。

（2）强化项目中的成果管理和知识积累管理。

（3）从人力资源规划方面，储备备用人力资源。提前进行人员的储备和培养。

（4）完善培训机制和手段。

（5）利用试点单位的实施过程，充分培养后继人才。

（6）系统供应商在其他类似项目上的设计和经验的再利用。

（7）系统供应商在项目实施过程中，将技能传授给项目小组和用户方。

（8）控制实施范围的变化——形成书面文档、陈述更改原因，待高层管理部门批准后方可实施更改。

（9）建立当项目实施出现问题时进行汇报和解决的标准工作流程。

6.3 NAC项目建设后期关键要素

为了真正实现NAC管理，把系统上线是远远不够的，这仅仅证明有了这套东西，然而在新一代攻击手段面前依然十分脆弱，仍然会有新的问题产生。如何才能将网络安全防线真正从网络边缘扩展落实到所有网络终端节点上呢？从广大承建方及使用方看来，后续跟进的合理化使用管理能帮助用户实现这一点。

但是，如果在网络运维过程中，不能正确处理制度和技术的关系，片面夸大制度的重要性，试图希望建立完善的制度，依赖用户自觉自愿地遵守制度，杜绝

问题的发生，也无疑是幻想。历史证明，问题或冲突最终能够得到有效解决，战略（制度）和战术（技术）都很重要，只是看待问题的不同角度和问题解决的不同阶段，制度和技术的优先级和权重是存在差异的，因此，要做到“制度和技术产品同样重要”，都不能忽视。

当系统上线以后，要做到全网无盲点 NAC 管理，都不是一步到位的，需要将管理制度和流程通过循序渐进的过程逐步建立起来，并进行不断的完善优化。

6.3.1　NAC 系统运行初期

1. 系统初始化运行

网络准入控制解决方案一般都会提供广泛而深入的功能，因此不仅涉及到整个网络，而且还关系到内部组织机构和职能部门。网络准入控制技术的部署几乎跨越整个 IT 领域，从桌面系统管理到桌面系统安全性，从网络基础设施到网络管理。此外，鉴于网络准入控制解决方案能够帮助企业成功满足行业和政府规章制度的要求，因此，还可能涉及到与制度遵从相关的个人与资源。鉴于网络准入控制的决策流程牵扯到众多部门，因此，将有大量的用户设备以及网络基础设施硬件、软件和固件组件受到决策的影响。

网络准入控制的涉及面非常广泛，从直接受其影响的大量用户设备和基础设施组件直到参与决策流程的众多组织机构，因此，进行大规模应用之前有必要在部分网络中进行试运行使用。

利用初始化试运行，通过系统的运行状态和抽检情况，掌握网络准入控制系统的特性，了解准入控制系统的安全行、稳定性、先进性及可扩展性等。

2. 与现有系统结合

无缝衔接网络准入控制系统，网络准入控制系统不是一个单独的系统，是为网络管理者量身定做的准入控制管理平台，目的在于提升 IT 服务部门的工作效率，解决大部分手工操作工作，对终端安全要求做规范并管理，避免网络准入控制系统和业务管理流程脱离，成为管理孤岛，不利于长远应用。

网络准入系统所具备的功能不仅仅是准入，还包含身份认证识别，接入终端安全统计，日志信息，均关系到对终端进行管理的各个方面，而对于管理者而言，每个系统都会有各自的信息，而相互之间并未建立联系，在安全管理中，一旦出现安全事故，往往会出现由于网络规模过于庞大，导致无法及时定位到具体的人、具体终端，给后续的补救工作带来阻碍。

因此在网络准入系统运行的初期很有必要与现有相关业务、应用系统进行结合，构建一个以准入为基础，相关管理系统结合的，多平台、多功能管理平台。

3. 全网部署逐步展开

做好了前期的准备工作，掌握了网络准入系统的整体特性，并做好系统结合

准备工作后，对网络准入系统有了全面的了解，接下来的重点就转移到了进行全网部署管控过程中。对于一般的网络来说机构众多，终端数量庞大是普遍存在的特点，如果没有一个合理的、完善的计划进行配合，将会给部署工作带来不利影响。因此，正如前面提到的实施策略之一："总体规划、分步实施"将是需要重点考虑的问题，只有通过循序渐进的方式，才能够保障整个项目部署顺利进行。以下为部署步骤。

Step1：培训工作开展。网络准入系统的全网部署，涉及到单位各个部门，范围广、影响大，难免会出现不协调的声音，如何减少这样的不和谐，同时让每一个终端用户理解网络准入控制，真正配合管理部门开展工作，以及如何正确使用网络准入控制系统等，做好培训工作将会带来事半功倍的效果。

Step2：全网信息采集。准入系统的部署正是一个对全网进行具体了解的大好时机，利用其对功能收集全网相关信息，涉及包括终端数量、地址使用情况、网络设备、打印机、扫描仪等专用设备统计等，建立一套全网的信息管理体系结构，为准入策略的开启做好准备，同时也是一个让终端用户实际接触、了解网络准入系统的最好时期。

Step3：准入策略开启。接下来的工作就是准入控制功能的开启，这一点是整个项目的重点，也是里程碑式的步骤，因此为了实现平滑过渡，降低这一过程的问题，功能的开启更需要循序渐进，把全网分成若干个不同的组成部分，再依据时间计划分步进行，完成一部分推进一部分，提高成功效率。

Step4：安全策略制订。安全策略的启用直接影响到准入系统的相关运用，对终端用户来说从原来的放纵自如，到规范遵循，在使用习惯上有了变化，如何实现平滑过渡，需要一套科学的策略支撑，可以考虑由少至多、由简至繁、由松至严的原则，逐步增加策略以及要求力度。

Step5：优化管理流程。优化就是改善、进步、提高。流程优化实现的不是正确的事情，而是如何正确地做事情。新的系统上线，利用系统中的信息，佐证决策，辅助决策，支持决策，进而帮助企业在正确的时间、方向上，正确地做事，对管理者来说真正的好产品，不仅仅由产品自身决定，管理使用的流程也是很大的因素，因此有必要形成一套简化而必需的管理流程。

6.3.2 NAC 系统管理流程

建设一套合格的 NAC 系统，不仅仅是从安全技术角度寻求完善的技术产品，另一方面还需要一个完整的系统运行管理流程，因此在项目建设的后期，必须充分考虑所面临的管理要求，并制订合理的管理流程，使准入系统的使用更合理化。下面阐述就 NAC 系统建设后对管理流程上的要求。

1. 系统管理团队建设

建立一个有权威的、有技术能力、效率高的管理团队。该团队一般由单位领

导牵头，以信息安全管理部门人员为主体，辅以与终端准入相关人员组成，系统运行的管理、操作、审计等权限明确，做到三权分立。

1）安全管理人员

安全管理人员负责协调各个职能部门，分解目标，优化终端准入管理流程，制定便于终端管理的规章制度，比如定期汇报，报表统计、入网流程、安全管理等。

2）安全操作人员

安全操作人员负责对 NAC 系统进行日常管理及操作，定期整理当前工作情况，并提出下阶段工作目标。

3）安全审计人员

安全审计人员负责评估整个系统的运行情况，判断管理工作的合理性、合规性，做到系统运行更符合实现具体目标。

2. 终端入网流程管理

终端接入是 NAC 入网管理的首要环节，作为准入管理者来说面对的将是全网所有终端，区域分散、数量大、涉及面广，因此在提供网络准入的过程中仅仅依靠安全技术是不够的，通过管理制度建立标准化的终端入网流程，真正做到管理与技术手段相结合，将为终端入网准入控制工作带来事半功倍的效果。具体流程如图 6-2所示。

3. 网络边界可视管理

在网络规模不断增大的现状，建设 NAC 系统其目的就是在接入流程管理的前提下，掌握接入终端的安全情况，并进行统一规范，解决由内网边界安全带来的安全隐患，在这里除了终端本身而言，网络边界情况的了解也将给管理工作带来便利条件，如交换机端口的使用情况，IP 地址的分配情况、终端在线情况、有无违规使用 Hub、NAT 设备的现象等。具体流程如图 6-3 所示。

4. 运行报表统计管理

报表是系统管理的基本措施和途径，是准入系统使用的基本要求。报表可以帮助操作人员了解全网终端安全风险，并把数据信息以可靠和安全的方式呈现给管理者，有针对性制订终端安全管理解决方案，便于进行安全事件全面分析及定位。具体流程如图 6-4 所示。

5. 系统应急预案管理

NAC 系统建设好后，就意味着所有的终端进入网络都依赖于这套网络准入控制系统，是全网终端接入网络的“门禁系统”。一旦系统运行出现问题，将直接影响到终端正常接入网络，导致业务工作无法正常开展，因此一定要建立完善

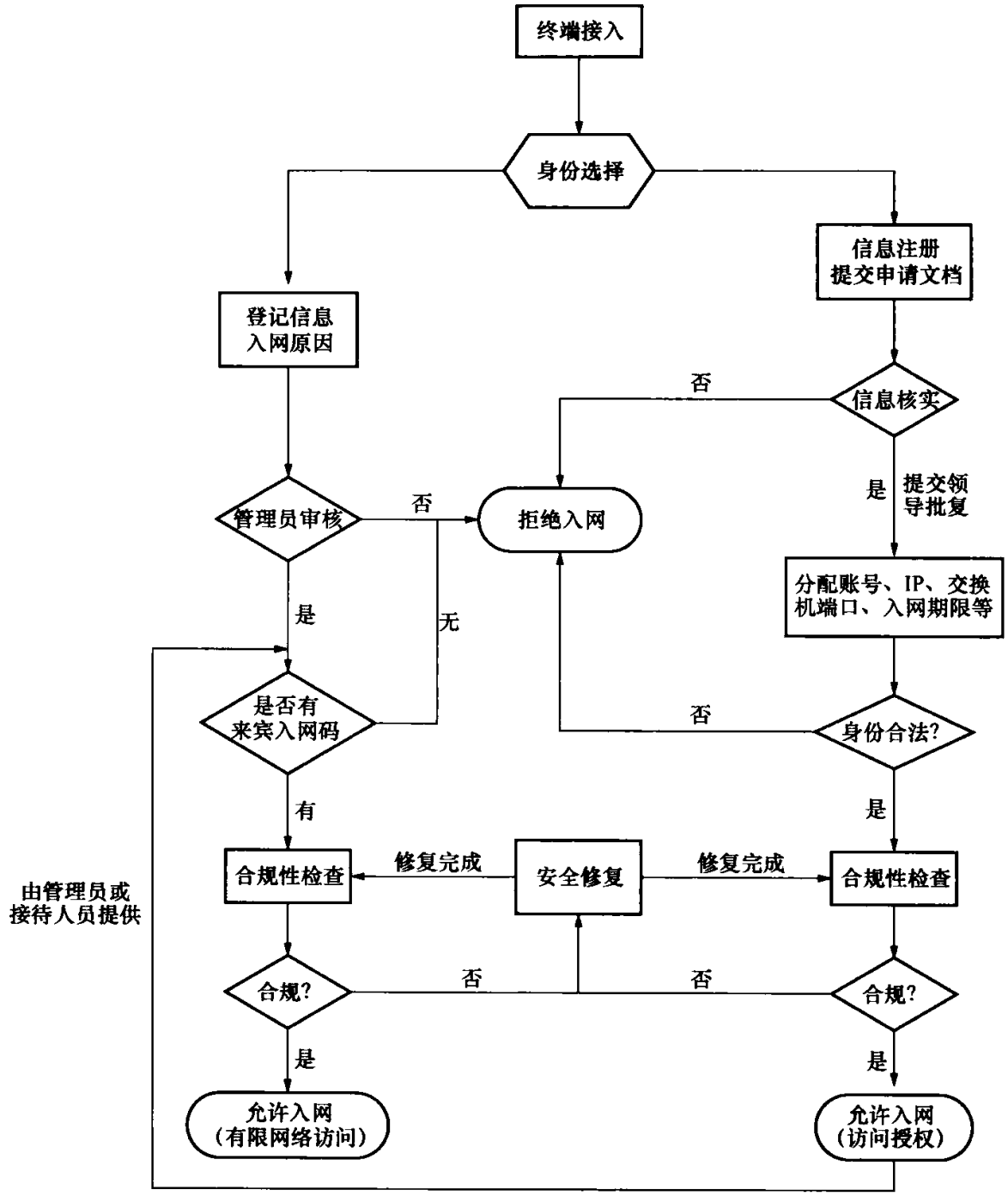


图 6-2 终端入网管理流程

的高可靠性应急方案，具备“Fail-Open”机制，不存在单点故障绝对不能因为网络准入控制系统而影响业务连续性，影响正常办公业务开展。具体流程如图 6-5所示。

6.3.3 NAC 系统日常管理

根据各终端在全网系统中的业务要求和安全需求，制定与业务相符合的终端准入管理规范和需要遵循的安全策略，并在实际管理中严格遵循。具体可以根据终端业务类型的不同制定不同的安全管理策略或规范，包括：终端用户入网行为

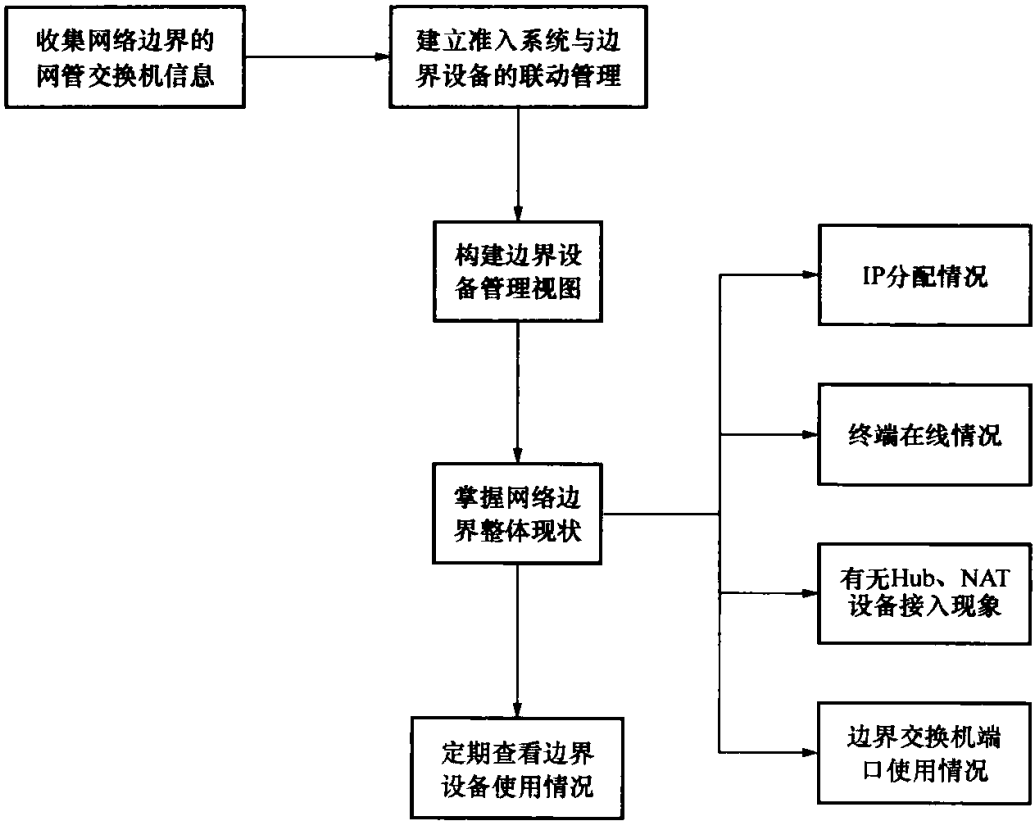


图 6-3　网络边界可视管理流程

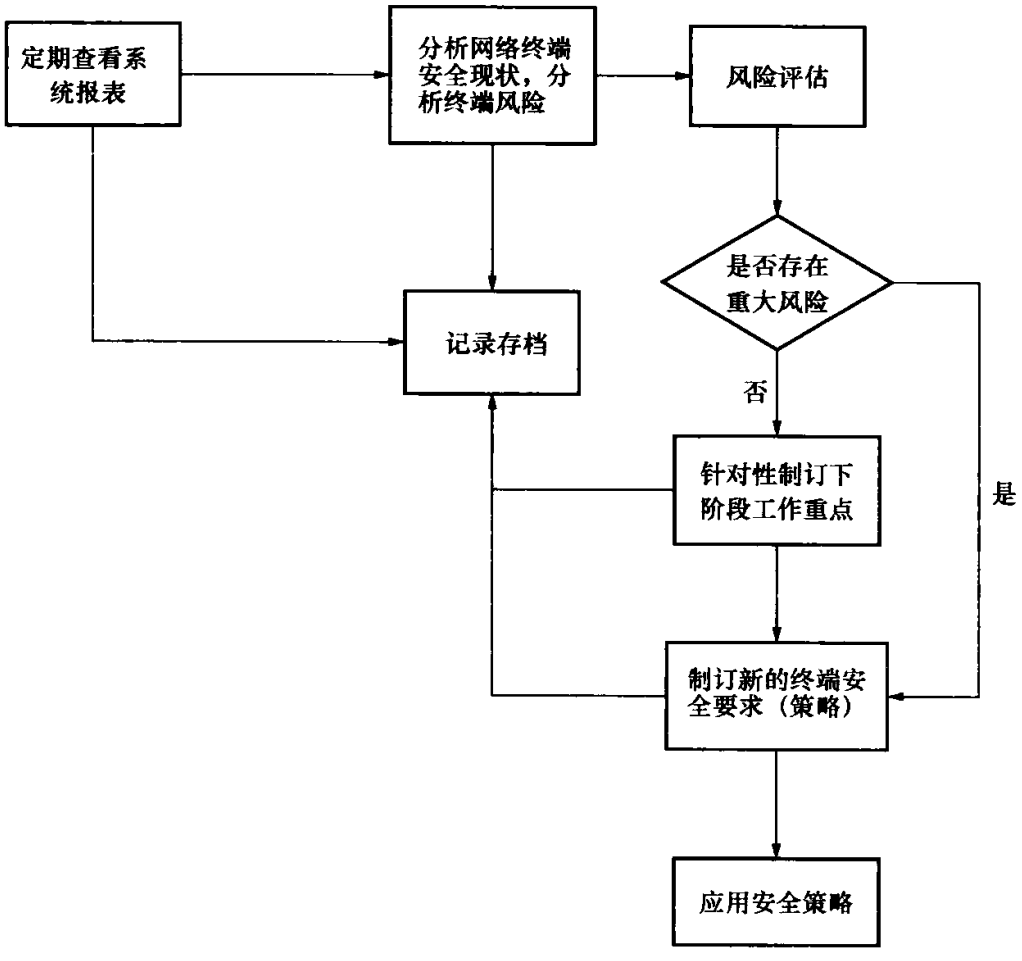


图 6-4　运行报表统计管理流程

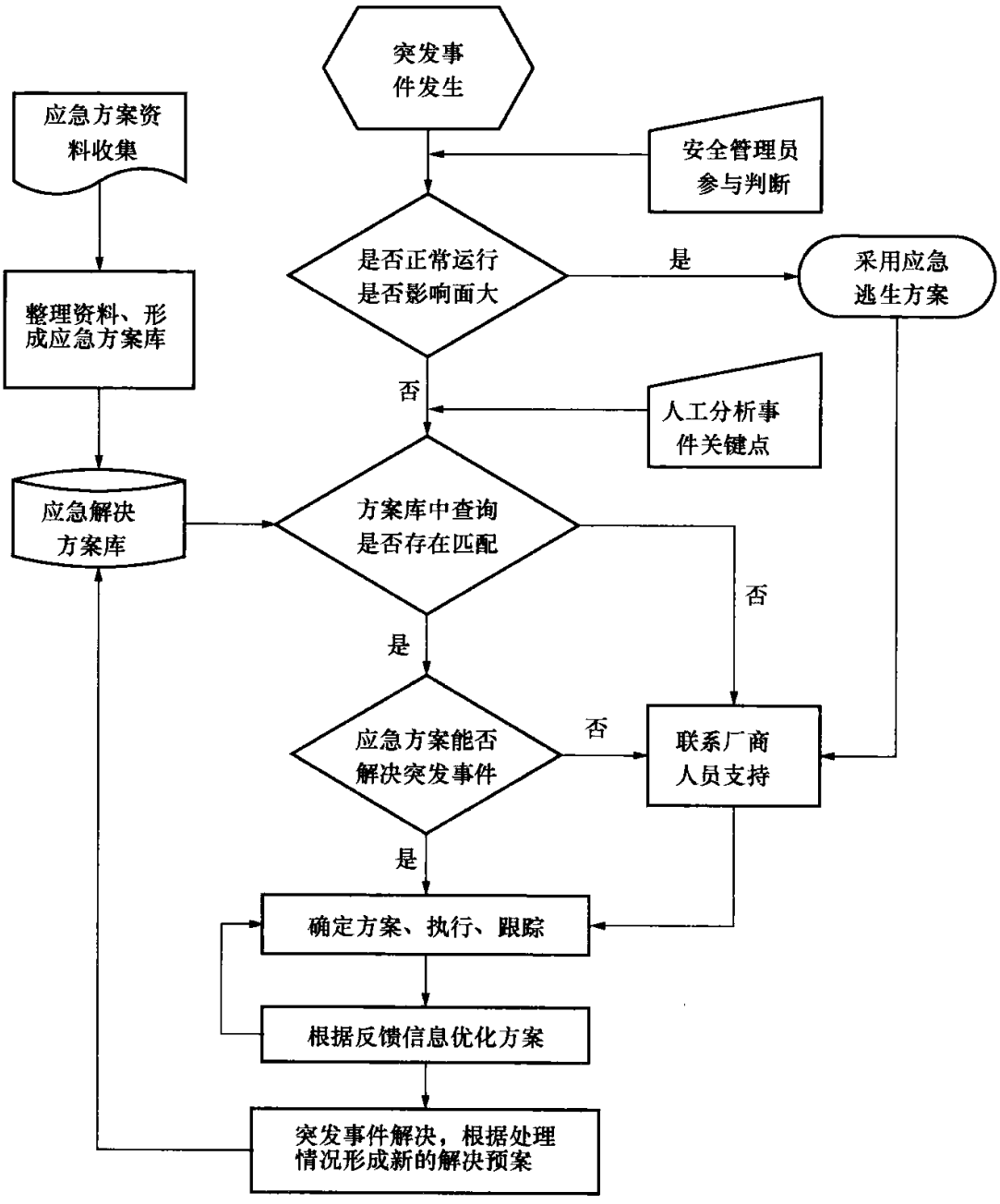


图 6-5 系统应急预案管理流程

规范、局域网使用规范、外联管理规范等不同的安全策略。

1. 入网终端配置规范管理

(1) 所有接入网络的办公用户必须按照网络终端标准入网流程进行每日的入网操作，由使用者的操作不当引起的故障和损失由使用者承担。具体流程如图 6-6 所示。

(2) 所有网络用户确保规定必须安装的杀毒软件及时更新及随时运行的义务。当用户收到入网系统页面中显示的有关杀毒软件未安装、病毒库未更新或未运行的告警通知时，必须立即按照页面中的有关引导进行安全修复，不依据本规范进行及时修复的用户将在页面上被告知并立即隔离出网，直到修复合格。

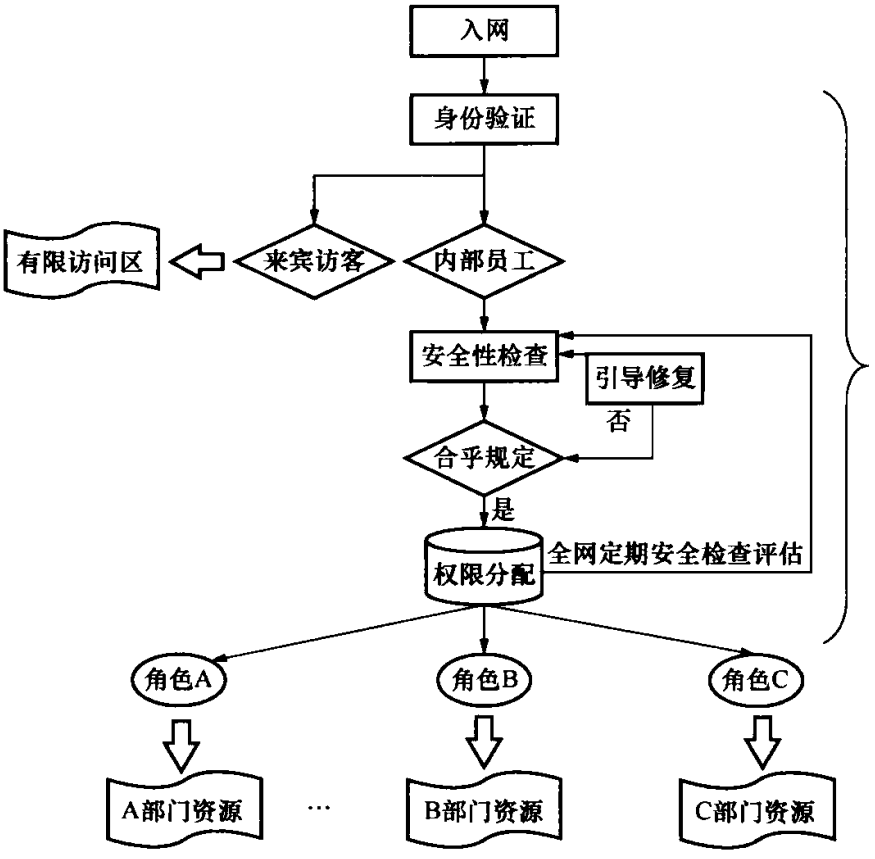


图 6-6　网络终端标准入网流程

（3）所有网络用户有依据规定必须及时更新操作系统补丁的义务。当用户收到入网系统页面中显示的补丁未更新告警通知时，必须立即按照页面中的有关引导进行安全修复，不依据本规范进行及时修复的用户将在页面上被告知并立即隔离出网，直到修复合格。

（4）未经网管员许可不得在个人计算机上安装与工作无关或影响网络使用的各类软件，如腾迅 QQ、BT、emule 等，更不得安装各种黑客软件用以故意破坏局域网的正常运行或超越应具有的权限。信息安全管理部门将定期对用户的安装软件进行规范性检查，如果在管理员规定的修改时限后，准入管理系统检查中依然发现用户有私自安装使用违规软件行为的，将追究相关人员的责任。

（5）未经网管员许可不得擅自修改计算机已分配的动态、静态 IP 地址及 DNS 等网络设置。信息安全管理部门将定期对用户的 IP 地址进行规范性检查，如果在管理员规定的施行时限后，准入管理系统检查中依然发现用户有私自更改 IP 地址等网络设置行为的，将追究相关人员的责任。

（6）用户有责任设置具有一定强度的系统口令，并设置相应的屏保属性，确保非正式用户不能通过非授权开机或正式用户离开间隙进入其终端系统。用户必须保护好其系统口令，不得将个人口令打印，在线储存或泄露给别人。

2. 入网用户行为规范管理

（1）网络终端使用者有义务维护网络的完整性和可用性，正确合理地使用局

域网设备，不得破坏、私自拆卸、挪用或盗窃局域网设备。当用户发现局域网中存在隐患或故障时，应及时告知网管员，以便能及早检查避免故障范围扩大，尽快使危害程度降到最低。

（2）未经网管员许可不得更改终端计算机的硬件配置（包括网络电缆、共享设备如打印机、传真机等）。

（3）因工作或业务上的相关需要（如建立软件或硬件上的模拟环境），要求更改局域网中的技术参数（如终端 IP 地址）或硬件布局结构等，需事先向网管员提出口头或书面的申请，经网管员确认在不影响公司正常工作的范围下方可实施。如改动的范围较大可能影响到局域网的运行效率或安全时，需经主管批准后与网管员共同实施。

（4）在入网终端计算机出现影响运行的故障并且网络仍然可用的情况下，可以向网管员申请协助，在得到用户许可后，网管员将对用户计算机进行处理，从而帮助用户迅速恢复计算机的正常运行。

（5）网管员在发现网络中出现系统、终端计算机或其他方面有异常情况时，将向相关入网用户发送通知，用户必须遵从收到的通知进行相应操作，未按照通知进行操作的用户，产生的一切责任后果由用户自身承担。

3. 终端违规联网规范管理

（1）单位的网络及其与 Internet 的连接只能用于与单位业务相关的目的，不得作个人目的使用。严禁非授权进入内网及互联网。公司将对所有内部计算机及由外入内的计算机纳入安全准入体系，新入网计算机必须向管理员提出申请，在网管员审核通过后入网。

（2）Internet 上的信息应被视为非机密的，除非信息加密，否则信息的机密性可能会在沿途任一节点受到威胁。非工作业务需要严禁向 Internet 上发送涉及机密、敏感或其他与公司业务相关的信息。

（3）除非事先得到批准，用户不得建立那些可能让未经授权者访问公司系统和信息的 Internet 或其他外部网络连接，这些连接包括但不限于：建立 VPN、无线路由、代理、3G 拨号等其他所有形式的向外主机连接。

（4）单位将严格控制外设的使用权限，防止内部数据通过各类外设非法流出造成危害。对于常用的 USB 移动存储设备，在没有得到管理员许可的情况下信息安全管理部门将通过技术手段禁止一切外来 U 盘接入，需要在单位内部使用的 U 盘由用户统一向管理申请使用权限并进行相关的注册和加密，内部 U 盘一律禁止外带。对于部分涉及重要数据的计算机将控制到其各类外设接口的使用，包括但不限于 USB 口、蓝牙、红外、1394 接口、串并口、光驱、软驱等。

以上几点作为在 NAC 系统日常使用管理的建议，基于严密合理的规范管理要求，实现对于 NAC 系统的有效应用，将日常的工作流程化、制度化、规范化。

第 7 章　网络准入控制案例研究

7.1　某银行网络准入控制案例

7.1.1　基本情况

某省银行成立于 20 世纪 90 年代，是一家具有一级法人资格的地方性股份制商业银行。截止 2009 年末，股本金 198365.5 万元，资产规模 634 亿元，职工 3800 余人，内设 12 个管理部门，下辖 135 个营业网点。涉及支付系统、办公系统、财务系统、管理系统等 15 个银行日常运行维护软件，累积终端设备达 7000 个。

7.1.2　需求分析

该银行在不断推出新的金融产品和业务以满足客户需求的同时，也在进一步提升信息化应用水平以满足业务需求。构建高可靠性和高安全性的信息化网络系统是银行、证券等金融企业业务运营的前提保障，因此，在加速开展信息化应用的同时加强信息系统安全建设，保障应用与业务的稳定运行，成为该银行信息化建设中的重中之重。

具体来看，以下几方面是该银行内网安全建设的基本需求。

1. 身份认证

银行合作伙伴多，进行的业务洽谈和人员往来多，外来人员经常需要接入到单位网络，如果非授权人员随意将外来笔记本电脑接入内网的某个网络端口，容易产生占用网络带宽，带来有意无意的攻击等，影响单位内部网络的正常运行。因此银行需要建立一套适合于内网的身份认证体系，防止外网人员随意接入。

2. 终端安全隔离和修复

该银行内部所属的近 7000 台接入终端在网络中的安全性始终没有可靠的保证，规定的杀毒软件没有安装，规定的补丁没有及时更新，终端的安全策略不到位，Windows 组策略过于简单，都是威胁其内网安全的重要因素，因此建立一套合理的安全隔离和修复的系统，可以极大地保障防病毒软件和补丁软件的安装率从根本上降低内网风险。

3. 违规外联管理

因为工作业务需要，有部分密级比较高的计算机是不能够访问互联网的，但

是仍然有终端员工通过 3G 网卡来连接外网，一旦进行了违规的外网访问，那么当再次接回到银行内网的时候就很容易带入木马及病毒，造成内网信息的泄密甚至严重泄密。因此，该银行需要建立一套完整的违规外联控制系统，以达到外联管理的目的。

4. 移动介质管理

由于信息化办公的需要，该银行内网文件传输和复制一般采用移动介质拷贝的方法，然而由于外来 U 盘的管理不善，将大量外部病毒带入内网，并且由于人员流动性大，无法确保内部资料的保密性，因此急需一套移动介质管理系统来解决此类问题。

7.1.3 网络拓扑

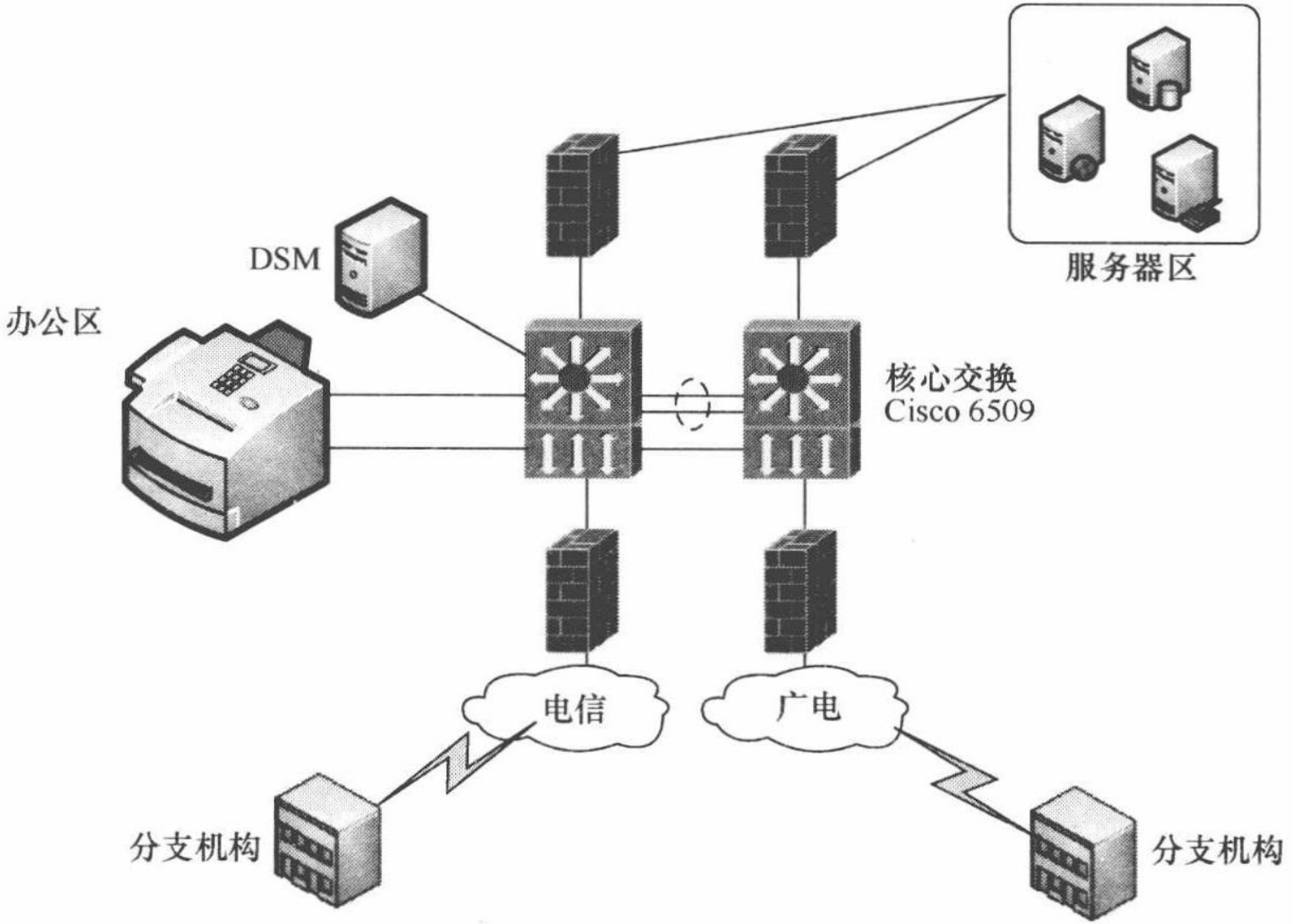
该银行网络在接入层交换机（楼层交换机）这一平台上普遍采用了 Cisco 2960 或华为 3100 交换机，全网都是可网管的交换机，因此构成了一个可实现 MVG 的环境，如图 7-1 所示。

图 7-1 某银行网络拓扑结构

7.1.4 解决方案

最终的方案采用某公司的一体化准入管理平台，在该银行总部所属办公大楼机房的两台核心交换机上分别部署准入控制设备，整个方案基于 MVG 准入控制技术，如图 7-2 所示。

通过一系列标准简单的协议来控制终端接入交换机，将交换机端口来回切换


服务器区
DSM
办公区
核心交换
Cisco 6509
电信
广电
分支机构
分支机构

是仍然有终端员工通过 3G 网卡来连接外网，一旦进行了违规的外网访问，那么当再次接回到银行内网的时候就很容易带入木马及病毒，造成内网信息的泄密甚至严重泄密。因此，该银行需要建立一套完整的违规外联控制系统，以达到外联管理的目的。

4. 移动介质管理

由于信息化办公的需要，该银行内网文件传输和复制一般采用移动介质拷贝的方法，然而由于外来 U 盘的管理不善，将大量外部病毒带入内网，并且由于人员流动性大，无法确保内部资料的保密性，因此急需一套移动介质管理系统来解决此类问题。

7.1.3 网络拓扑

该银行网络在接入层交换机（楼层交换机）这一平台上普遍采用了 Cisco 2960 或华为 3100 交换机，全网都是可网管的交换机，因此构成了一个可实现 MVG 的环境，如图 7-1 所示。

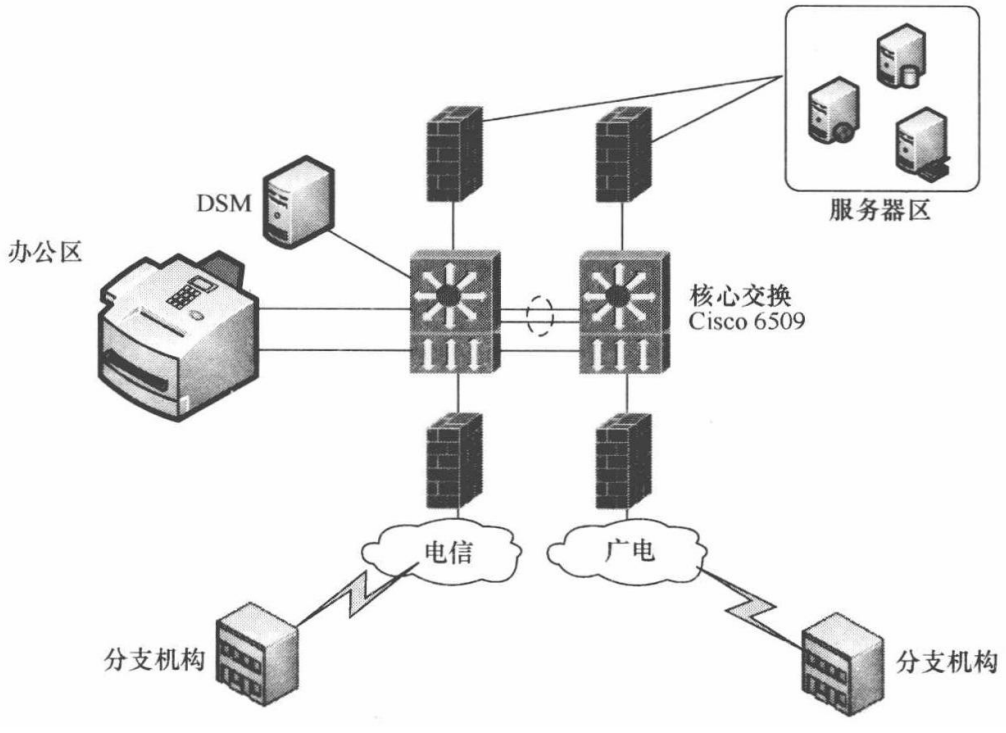


图 7-1 某银行网络拓扑结构

7.1.4 解决方案

最终的方案采用某公司的一体化准入管理平台，在该银行总部所属办公大楼机房的两台核心交换机上分别部署准入控制设备，整个方案基于 MVG 准入控制技术，如图 7-2 所示。

通过一系列标准简单的协议来控制终端接入交换机，将交换机端口来回切换

图 7-2　MVG 解决方案部署示意图

与正常 VLAN 和隔离 VLAN 的方式来进行准入。

入网设备经过身份认证和安全检查后方可入网进行正常访问，如果是安全检查不合格的设备，需要安全修复才能入网。外来设备只有经过管理员审核批准后才能够接入网络。整个网络边界明确，入网流程清晰，终端使用规范安全。

7.2　卫生行业网络准入控制案例

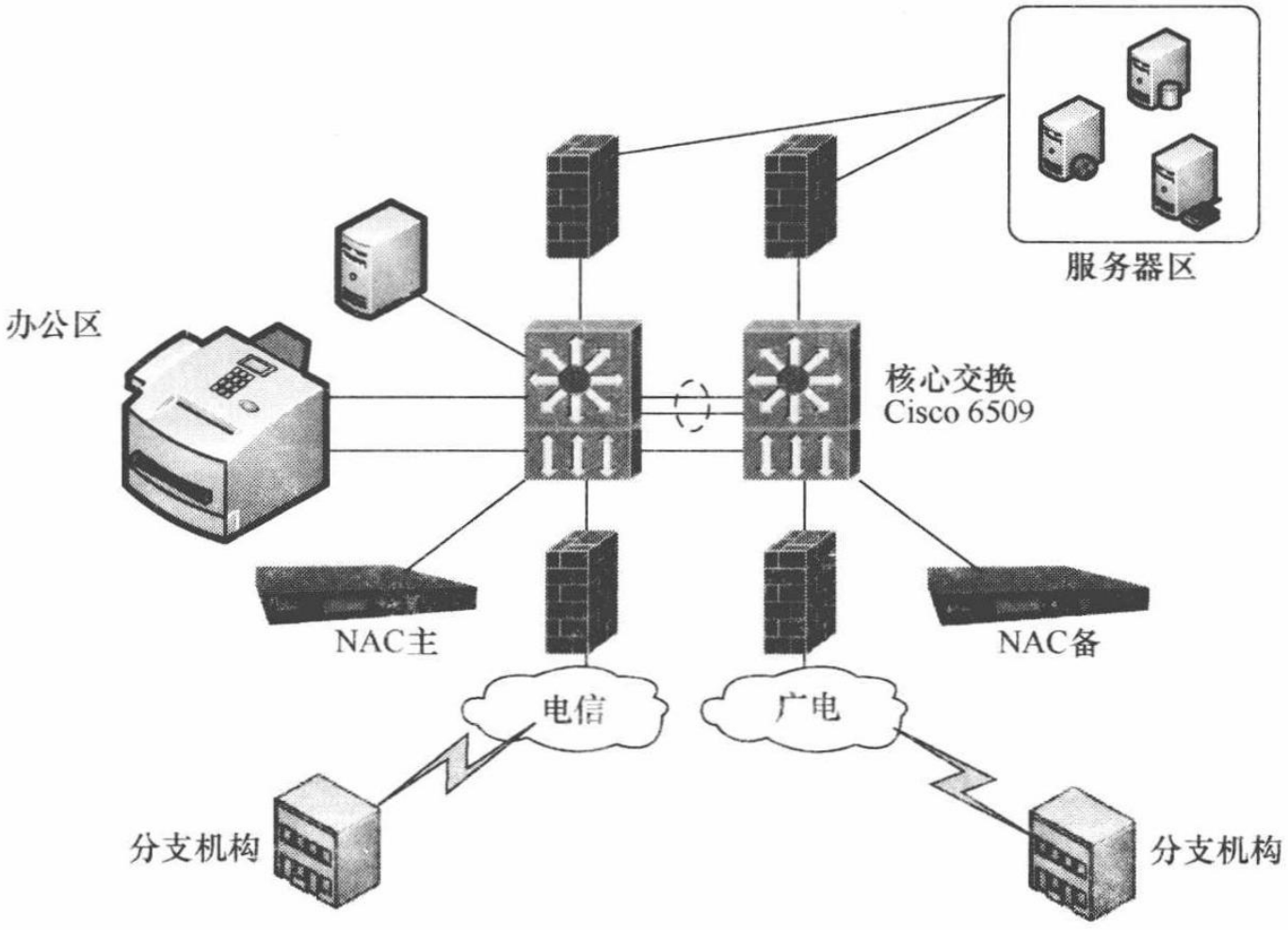
7.2.1　基本情况

某省肿瘤医院成立于 1963 年 10 月，是国内最早的 4 家肿瘤医院之一。医院现有职工近 1522 人，高级职称 186 人，中级职称 299 人。开放床位 1393 张，设有 19 个病区。据 1963～2007 年 12 月底资料统计，医院总门诊量已达 22 608 631 人次，住院 218 232 人次，手术 90 159 人次，44 年收治患者逾 200 万人。

该医院有 7 栋综合类病院楼，下属各科室、十几个病区，包括院内住院部、门诊部的 5 幢大楼，2500 多台医院内部计算机，应用系统为 HIS 系统、LIS 系统、医生工作站系统和电子病历 4 个软件架构，主要受控终端为进入 HIS 系统的台式机、医生工作站、移动设备和部分打印机。

7.2.2　安全现状

在多年信息化建设中，该医院内部已建立起了完善的临床、医技、财务、管理等部门的内部信息安全网，以及连接各医保中心、Internet 互联网的外部网络体系，信息交换、信息共享的模式日趋成形。但是在从信息系统获取便捷的同


服务器区
办公区
核心交换
Cisco 6509
NAC主
NAC备
电信
广电
分支机构
分支机构

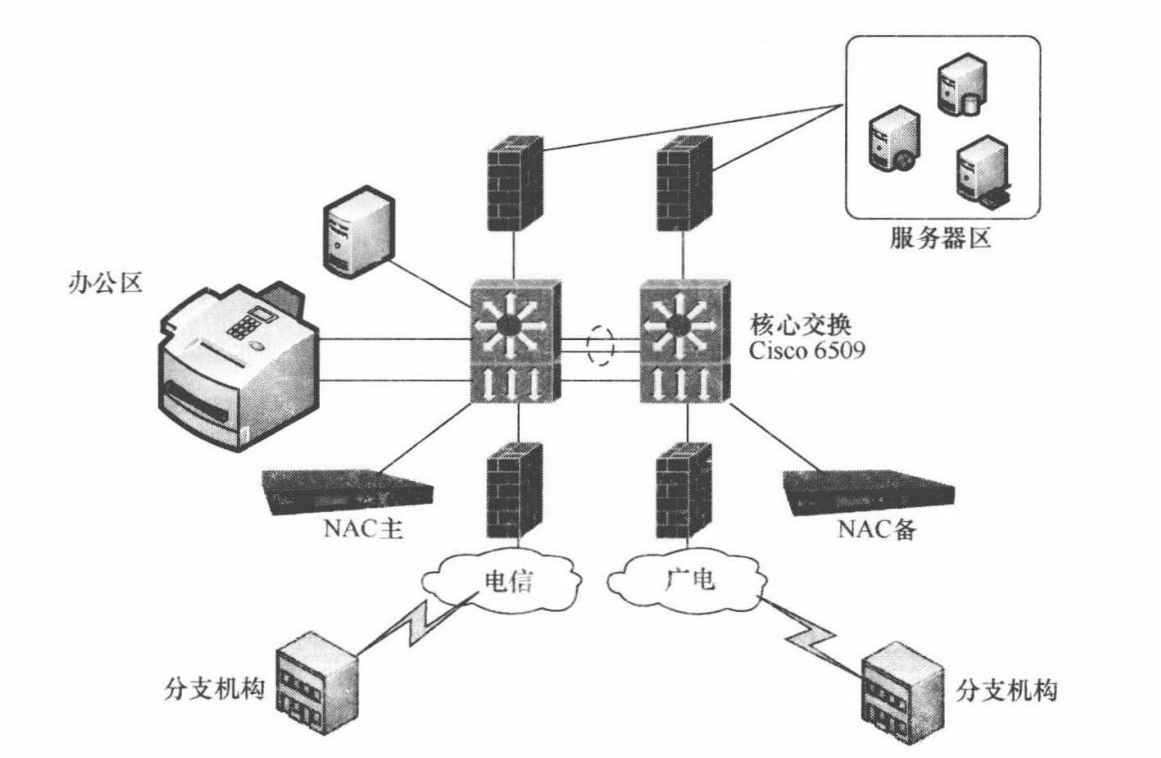


图 7-2　MVG 解决方案部署示意图

与正常 VLAN 和隔离 VLAN 的方式来进行准入。

入网设备经过身份认证和安全检查后方可入网进行正常访问，如果是安全检查不合格的设备，需要安全修复才能入网。外来设备只有经过管理员审核批准后才能够接入网络。整个网络边界明确，入网流程清晰，终端使用规范安全。

7.2　卫生行业网络准入控制案例

7.2.1　基本情况

某省肿瘤医院成立于 1963 年 10 月，是国内最早的 4 家肿瘤医院之一。医院现有职工近 1522 人，高级职称 186 人，中级职称 299 人。开放床位 1393 张，设有 19 个病区。据 1963～2007 年 12 月底资料统计，医院总门诊量已达 22 608 631 人次，住院 218 232 人次，手术 90 159 人次，44 年收治患者逾 200 万人。

该医院有 7 栋综合类病院楼，下属各科室、十几个病区，包括院内住院部、门诊部的 5 幢大楼，2500 多台医院内部计算机，应用系统为 HIS 系统、LIS 系统、医生工作站系统和电子病历 4 个软件架构，主要受控终端为进入 HIS 系统的台式机、医生工作站、移动设备和部分打印机。

7.2.2　安全现状

在多年信息化建设中，该医院内部已建立起了完善的临床、医技、财务、管理等部门的内部信息安全网，以及连接各医保中心、Internet 互联网的外部网络体系，信息交换、信息共享的模式日趋成形。但是在从信息系统获取便捷的同

时，各种应用系统被破坏后带来的危害和损失也提高到一个十分严峻的位置。如何保证医疗信息系统的 7×24 小时不间断运行，保证内网设备的安全使用，这是医院内的信息中心管理者面对的新问题。

该医院内网安全现状有以下几方面问题。

1. 非法接入

在医院内外网隔离的情况下，内网由于欠缺安全防护手段，在医生或患者的笔记本电脑随意接入时存在极大的安全风险和管理隐患，甚至有可能成为非法“统方”行为的工具。

2. U 盘随意使用

内外网物理隔离，计算机专机专用，的确会给内部办公带来了很多便捷，也会给个人使用计算机带来一些“不便”。于是，U 盘成为信息存储的工具，人们私自使用 U 盘进行娱乐资源的传输成为管理员极其头疼的问题，因为，稍有不慎即有可能通过 U 盘产生全网的病毒感染。

3. 终端未打齐补丁

内部员工整体安全意识不足，接入设备不及时升级系统补丁的现象普遍存在，无法对这些安全规范进行统一强制管理，这种情况下安全性低下的单台终端极易成为影响全网的威胁来源和跳板（如 ARP 病毒攻击，中木马病毒后威胁网络安全等），造成重大安全事件的发生，带来巨大的安全风险。

4. 终端故障分析困难

员工计算机水平参差不齐，许多人面对计算机问题无法进行及时修复，由于点数多，范围分散，出现问题后管理员需要频繁奔赴现场进行维护，工作效率极低。而且很多次现场维护都发现问题不大或者根本没有问题，本来可以通过远程电话解决的问题也需要现场奔波一次，大量地浪费了人力和物力。

7.2.3 网络拓扑和需求

该医院网络拓扑结构如图 7-3 所示。

综合分析后，发现该医院的总体需求为以下几点。

1. 接入可控

针对网络进行准入控制，并且做到来宾入网可控可管理，对入网终端先进行性身份选择，本单位员工需要进行身份认证才能入网，外来人员需要一个已入网员工为其提供来宾码才能入网。

图 7-3　某医院网络拓扑结构图

2. U 盘管理

针对信息办公点的移动介质，该医院需要一套移动介质管理系统来解决 U 盘乱插，移动介质泄密等问题。

3. 补丁分发

该医院需要一套完整的强制补丁分发系统，分发时需要终端用户更新补丁后才能入网，做到能够及时的高强度的分发补丁和堵住计算机漏洞，防止终端电脑被黑客利用漏洞而入侵，导致内网被攻击的现象。

4. 终端安全性统一管理

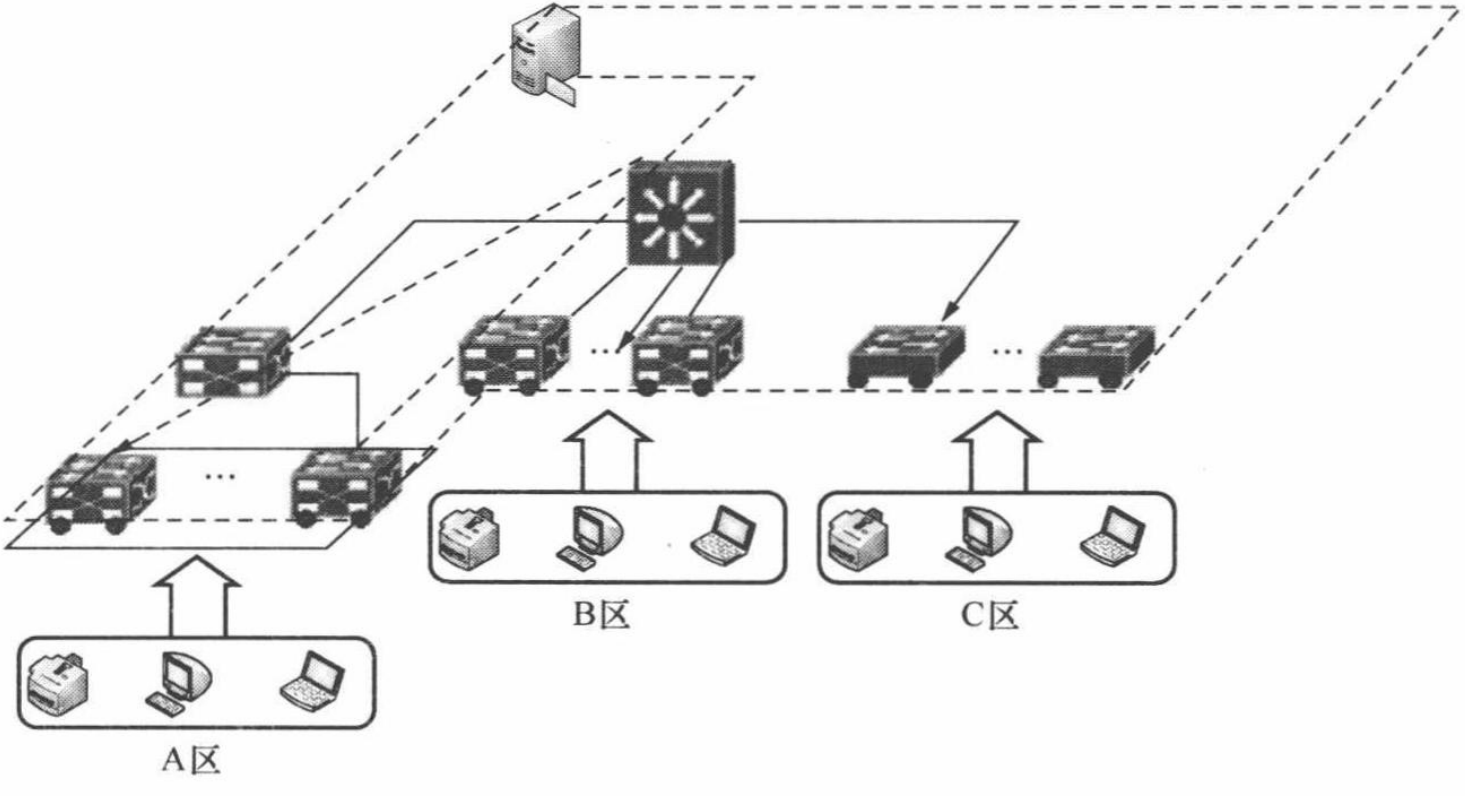
该医院需要一套终端安全性统一分析和管理的系统，以便于帮助其维护、解决终端常见故障分析，帮助该医院的网管人员减少维护量，加快维护速度。

7.2.4　解决方案

最终的方案采用某公司的纯硬件独立准入控制管理平台，在该医院行政管理大楼机房的核心交换机上部署硬件准入控制设备，整个方案基于策略路由准入控制技术，如图 7-4 所示。

通过一系列高级路由协议来控制入网终端，将终端流量进行旁路引流的方式来进行准入。

入网设备设备经过身份认证和安全检查后方可入网进行正常访问，如果是安全检查不合格的设备，需要安全修复才能入网。如果是来宾入网，则需要正式员工入网后为其申请一个来宾码的方式才能入网。所有设备由准入设备统一安全规划。整个网络边界明确，入网流程清晰，终端使用规范安全。


B区
C区
A区

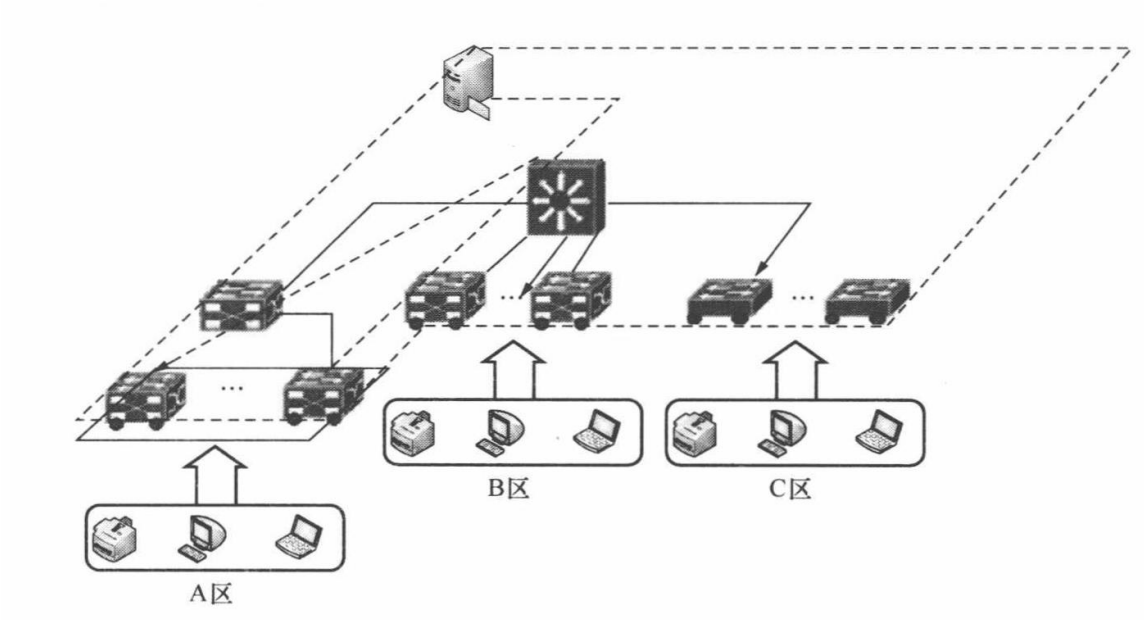


图 7-3　某医院网络拓扑结构图

2. U 盘管理

针对信息办公点的移动介质，该医院需要一套移动介质管理系统来解决 U 盘乱插，移动介质泄密等问题。

3. 补丁分发

该医院需要一套完整的强制补丁分发系统，分发时需要终端用户更新补丁后才能入网，做到能够及时的高强度的分发补丁和堵住计算机漏洞，防止终端电脑被黑客利用漏洞而入侵，导致内网被攻击的现象。

4. 终端安全性统一管理

该医院需要一套终端安全性统一分析和管理的系统，以便于帮助其维护、解决终端常见故障分析，帮助该医院的网管人员减少维护量，加快维护速度。

7.2.4　解决方案

最终的方案采用某公司的纯硬件独立准入控制管理平台，在该医院行政管理大楼机房的核心交换机上部署硬件准入控制设备，整个方案基于策略路由准入控制技术，如图 7-4 所示。

通过一系列高级路由协议来控制入网终端，将终端流量进行旁路引流的方式来进行准入。

入网设备设备经过身份认证和安全检查后方可入网进行正常访问，如果是安全检查不合格的设备，需要安全修复才能入网。如果是来宾入网，则需要正式员工入网后为其申请一个来宾码的方式才能入网。所有设备由准入设备统一安全规划。整个网络边界明确，入网流程清晰，终端使用规范安全。

图 7-4 基于策略路由准入控制解决方案部署示意图

7.3 财政行业网络准入控制案例

7.3.1 基本情况

某省财政厅下属该省地市市的财政分局和预算单位财政部门，是全省的财政枢纽。该厅的“金财专网”全省各地市网络经过多年的发展，已经建立了相对完善的内部局域网系统。包含业务应用系统、信息网络系统和安全保障体系 3 个方面，即以应用为中心，以网络为支撑，以安全为保障。

由于目前所辖终端众多，其他政府预算单位也需要向财政局进行资金申请，导致网络接入数庞大，接入方式复杂多样，且遍布范围十分广泛，给信息安全工作带来了不小的难度。在这种情况下，如何对网内分散各地的众多接入计算机进行统一管理，如何确保整个金财专网业务系统的安全性，如何进一步提升全网信息安全水平并符合国家等级保护等相关法律法规的要求，降低管理成本，提高管理效率，就成为当下较为紧迫的问题。

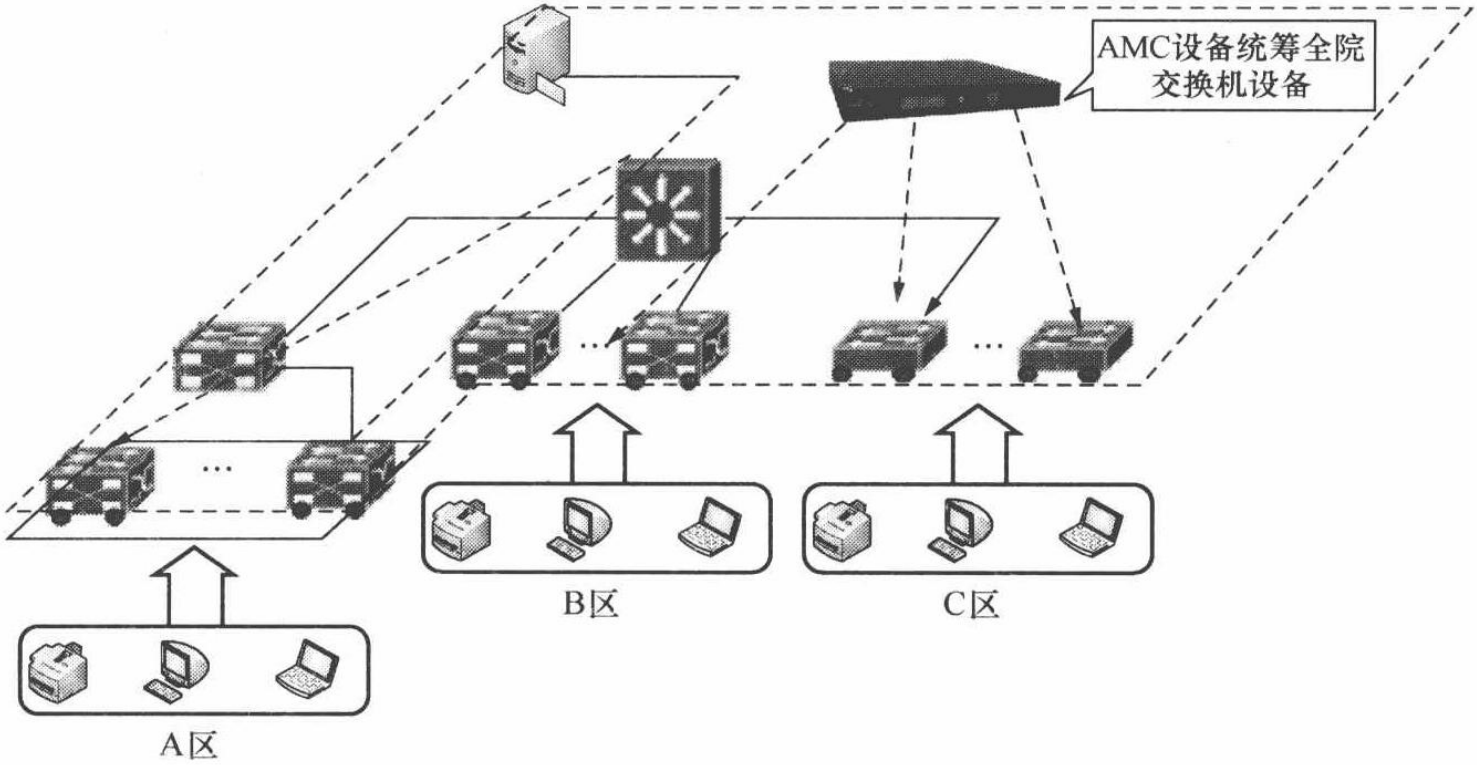
7.3.2 需求分析

应用规模：厅本部 21 个内设机构、省级预算单位终端设备，包括各台式机、笔记本、移动设备、打印机，其中还包括一定数量的特殊系统工作站，建设规模近 14 000 点。

该财政厅内网安全建设的基本需求包括以下几个方面。

1. 智能化接入管理

智能化的有效管理，做到管理制度和技术手段相结合，即能够实现对内网终端的合法入网，也能够避免外来设备随意接入，真正做到终端入网安全管理的及


AMC设备统筹全院
交换机设备
A区
B区
C区

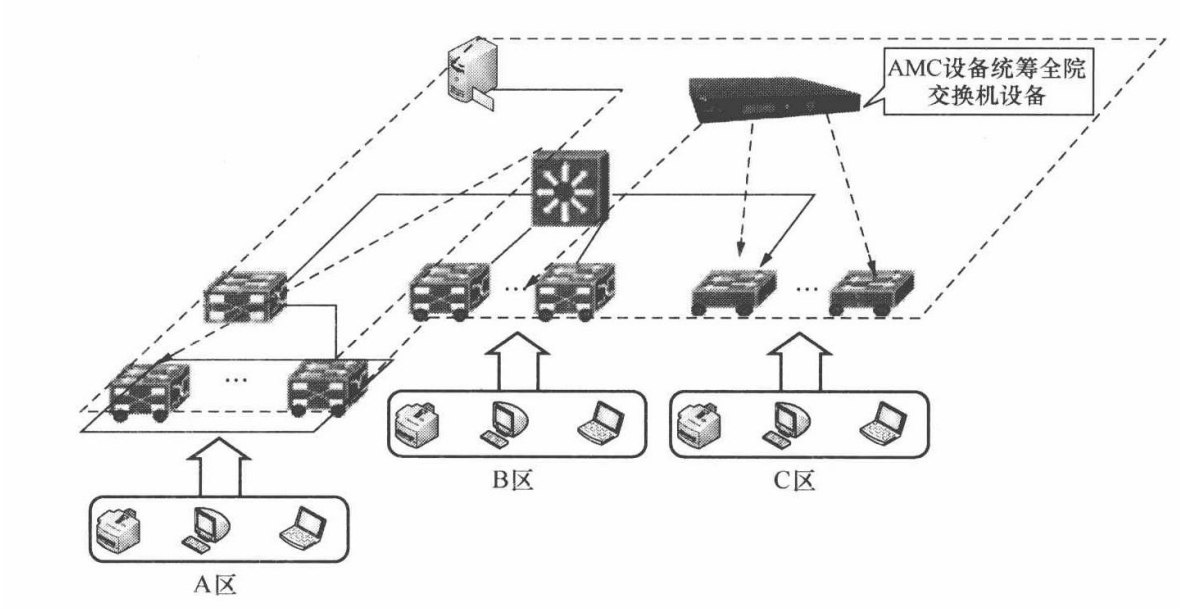


图 7-4 基于策略路由准入控制解决方案部署示意图

7.3 财政行业网络准入控制案例

7.3.1 基本情况

某省财政厅下属该省地市市的财政分局和预算单位财政部门，是全省的财政枢纽。该厅的“金财专网”全省各地市网络经过多年的发展，已经建立了相对完善的内部局域网系统。包含业务应用系统、信息网络系统和安全保障体系 3 个方面，即以应用为中心，以网络为支撑，以安全为保障。

由于目前所辖终端众多，其他政府预算单位也需要向财政局进行资金申请，导致网络接入数庞大，接入方式复杂多样，且遍布范围十分广泛，给信息安全工作带来了不小的难度。在这种情况下，如何对网内分散各地的众多接入计算机进行统一管理，如何确保整个金财专网业务系统的安全性，如何进一步提升全网信息安全水平并符合国家等级保护等相关法律法规的要求，降低管理成本，提高管理效率，就成为当下较为紧迫的问题。

7.3.2 需求分析

应用规模：厅本部 21 个内设机构、省级预算单位终端设备，包括各台式机、笔记本、移动设备、打印机，其中还包括一定数量的特殊系统工作站，建设规模近 14 000 点。

该财政厅内网安全建设的基本需求包括以下几个方面。

1. 智能化接入管理

智能化的有效管理，做到管理制度和技术手段相结合，即能够实现对内网终端的合法入网，也能够避免外来设备随意接入，真正做到终端入网安全管理的及

时有效性。

2. 入网设备安全规范化

对入网 PC 的规范性（杀毒软件安装、补丁更新、弱口令、屏保等）进行扫描并提供及时修复的技术手段，特别是桌面管理客户端代理的 100%存活率保障。

3. 软件推送

财政系统的金财专网是一套 B/S（Browser/Server）和 C/S（Client/Server）结合的办公系统，因此需要一套系统对内部网络进行终端软件推送，确保应用系统的客户端安装到用户桌面，方便各单位办公和进行业务交流。

4. 多级管理

能够进行分区域和多级管理，能够使现有的管理结构更加明晰、合理、细化。并可以对管理员进行细粒度的权限分配，以确保用户根据管理范围的不同具有相应的管理权限。

5. 认证管理

统一身份认证加强，突破空间和时间的限制，结合现有的 CA 认证体系，确保合法用户使用合法的资源，避免出现越权访问的现象。

7.3.3　网络拓扑

某财政厅网络拓扑结构如图 7-5 所示。该单位网络采用分级结构，从县级单位级联至市级单位再级联至省中心，各级采用华为路由器进行级联，最后访问省财政信息中心的应用服务器，极为适合策略路由部署模式。

7.3.4　解决方案

图 7-6 所示为基于策略路由准入解决方案部署示意图。

通过一系列方案的商讨和调研，最终确定采用某公司的独立硬件准入系统，通过策略路由的部署模式，对内网的终端进行精确到 IP 的流量准入控制，如图 7-6所示。最终部署后，实现了以下功能。

① 接入终端安全性扫描，包括杀毒软件和补丁推送。

② 桌面管理客户端存活率保障。

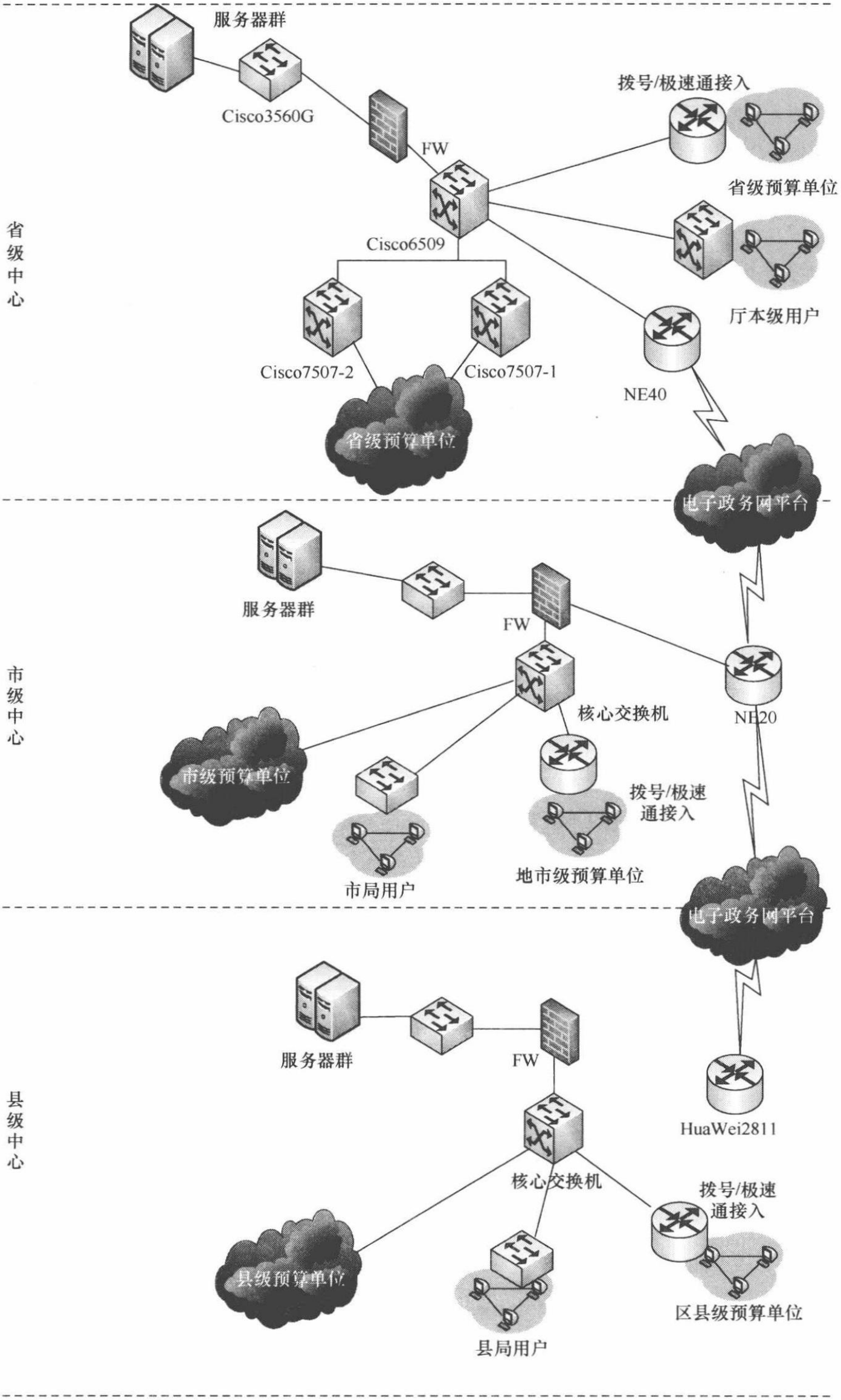
③ CA 认证系统联动认证。

④ 相关程序安装推送等。

⑤ IP/MAC 地址绑定。

⑥ 和地市、区县构建省市县三级“集中管理、分布部署”的管理模式。

图 7-5　某财政厅网络拓扑结构图


省级中心
服务器群
Cisco3560G
FW
拨号/极速通接入
省级预算单位
Cisco6509
厅本级用户
Cisco7507-2
Cisco7507-1
NE40
省级预算单位
电子政务网平台
市级中心
服务器群
FW
核心交换机
NE20
市级预算单位
拨号/极速
通接入
市局用户
地市级预算单位
电子政务网平台
县级中心
服务器群
FW
HuaWei2811
核心交换机
拨号/极速
通接入
县级预算单位
区县级预算单位
县局用户

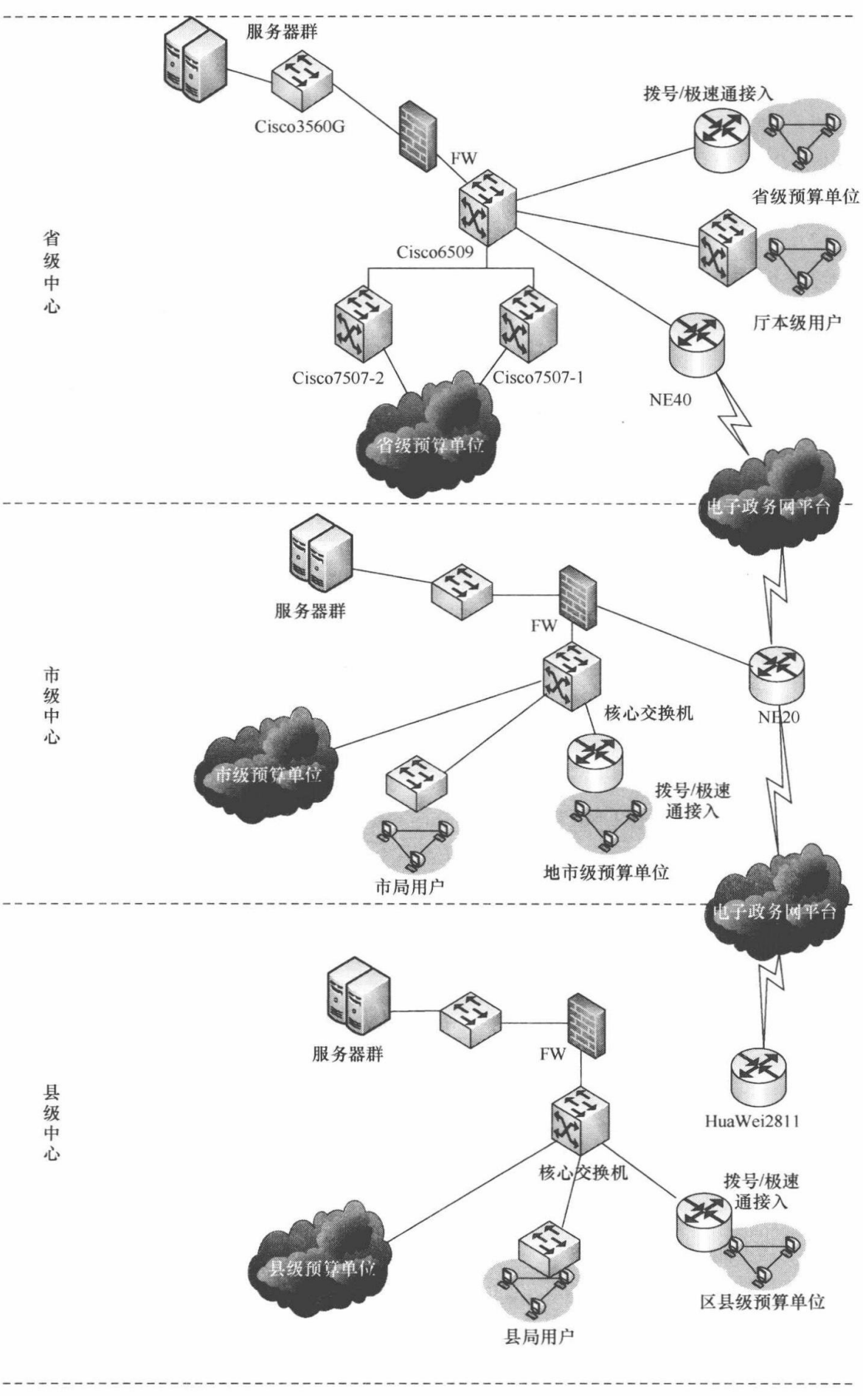
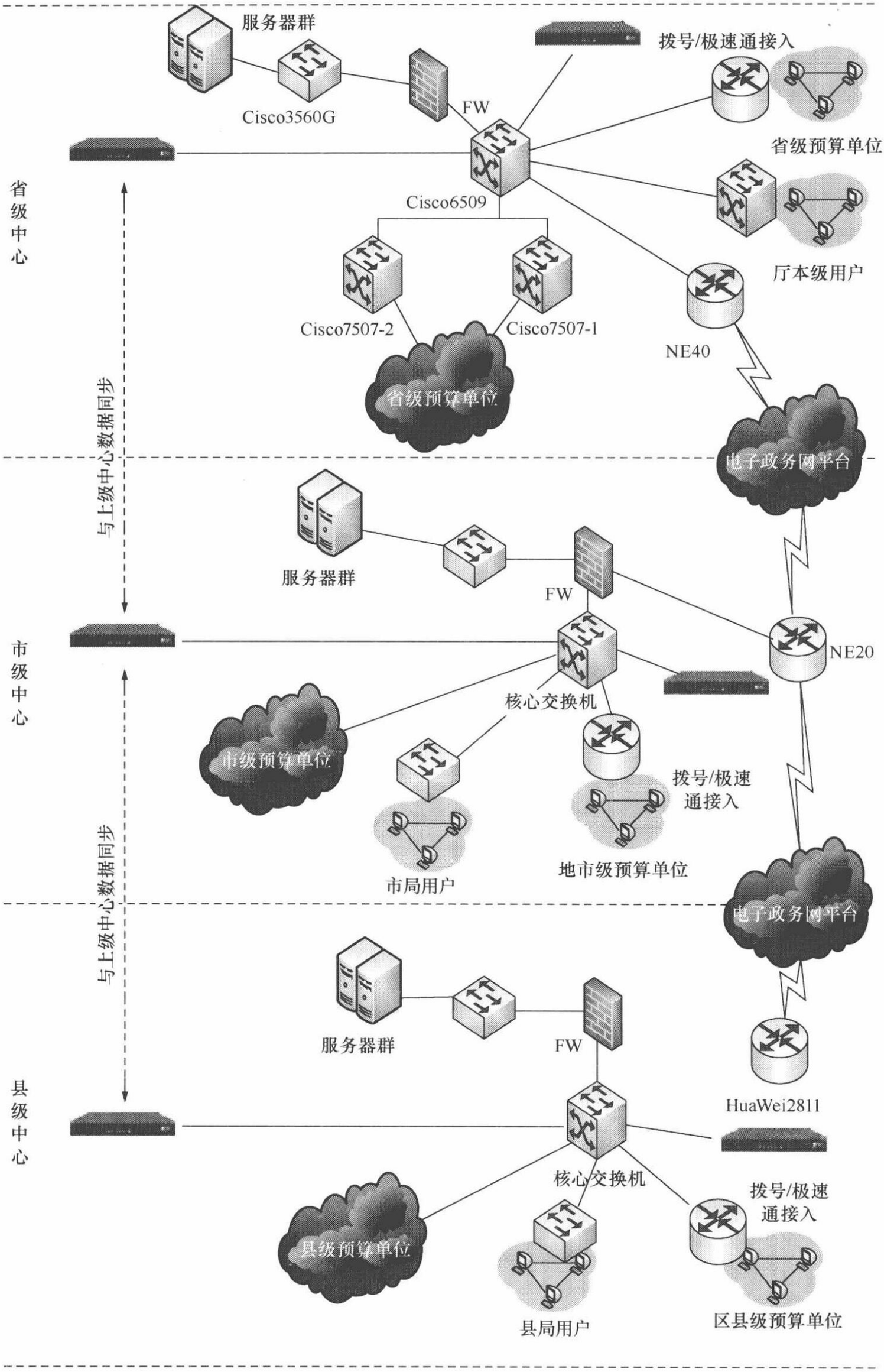


图 7-5 某财政厅网络拓扑结构图

图 7-6　基于策略路由准入解决方案部署示意图


服务器群
Cisco3560G
FW
拨号/极速通接入
省级预算单位
省级中心
Cisco6509
厅本级用户
Cisco7507-2
Cisco7507-1
NE40
省级预算单位
电子政务网平台
与上级中心数据同步
服务器群
FW
市级中心
NE20
核心交换机
市级预算单位
拨号/极速
通接入
市局用户
地市级预算单位
电子政务网平台
与上级中心数据同步
服务器群
FW
HuaWei2811
县级中心
核心交换机
拨号/极速
通接入
县级预算单位
县局用户
区县级预算单位

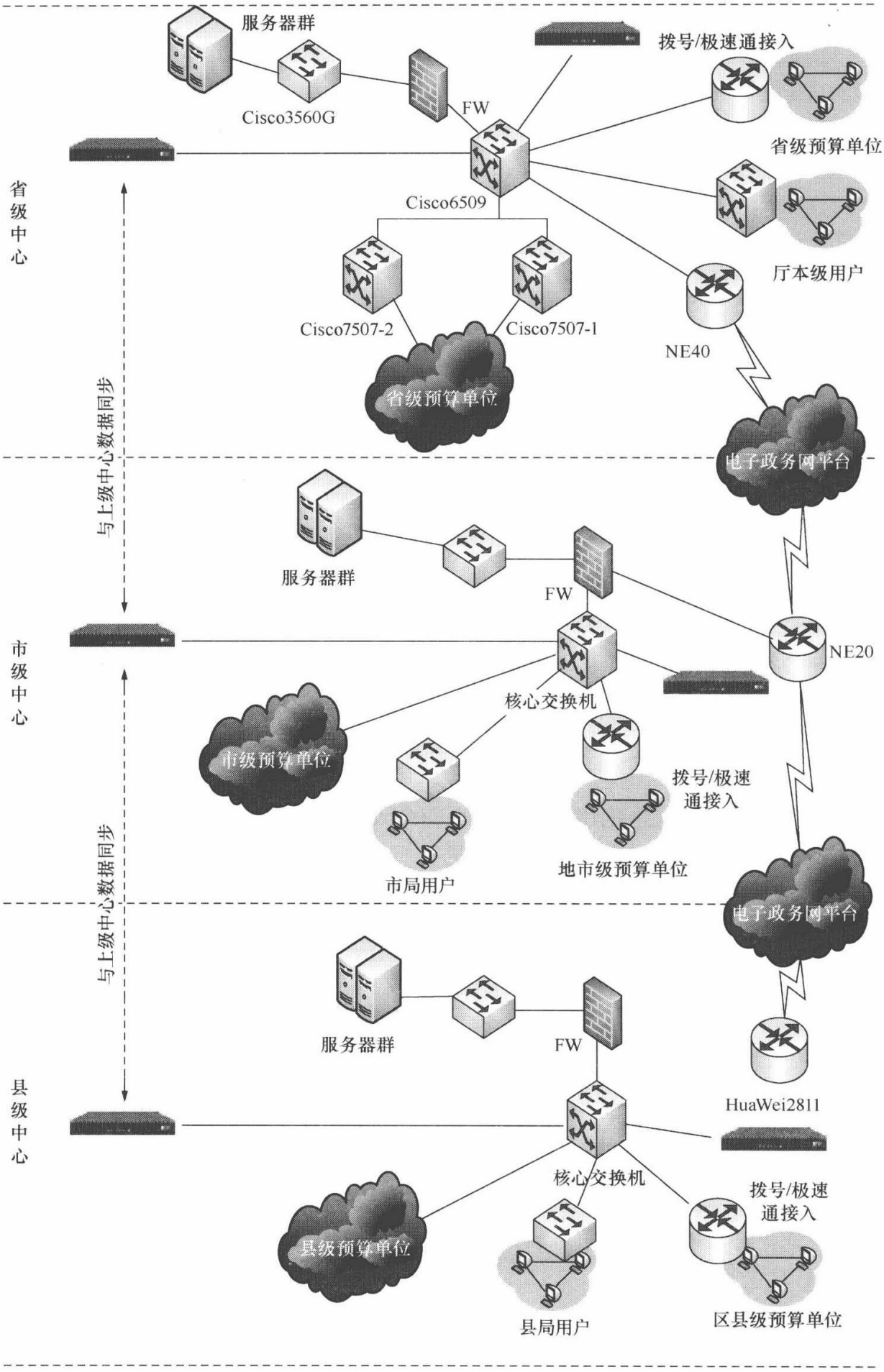


图 7-6　基于策略路由准入解决方案部署示意图

通过此次 NAC 项目实施，该财政厅获得了不小的收益。

① 通过技术手段确保了应用系统客户端、桌面管理代理客户端程序的有效执行，真正做到了存活率达到 100%；

② 及时下发杀毒软件，更新病毒库及系统补丁，加固了终端计算机的安全；

③ 实现省、市、区/县多层次的分级分权限有序管理；

④ 入网身份注册，将信息资产列表和责任人有机地结合起来，让信息中心对于内网整体的安全情况有明确的认知。

通过本次项目实施，对整个网络重新进行了安全规划和加固：一是优化了原有网络接入方式，保证了网络的安全性和可靠性；二是对省本级和升级预算单位等 4000 多个信息点的接入做了控制，必须达到安全规范才能接入业务网，确保每个接入网络的终端都安装了最新的防病毒软件，重要补丁都得到安装等；从网络与终端等方面立体化地加固了网络的安全性。

7.4 某部队网络准入控制案例

7.4.1 基本情况

某部队单位有 36 个部门，80 多个处室，3 个直属分队，近 5000 台终端计算机，包括各品牌台式机、移动设备、笔记本电脑、打印机，其中还包括一定数量的特殊系统工作站。

7.4.2 安全现状

在国家对军队信息化建设日益重视的今天，该部队已经建立起了完善的内网信息系统，各部门基于内网信息系统进行日常工作和管理，效率高、使用便捷。由于目前所辖部门众多，导致网络接入用户总数众多，且遍布该部队单位各个角落。在多年的网络使用过程中，发现始终存在以下难以解决的问题。

① 入网不能有效进行统计，无法清楚了解每日有多少台设备进入了单位网络。

② 来宾入网不能有效控制，无法统计入网的人员数量和每日来访的宾客数量。

③ 管理规范不能有效落实到位，缺乏有效手段对用户的操作行为（如随意安装娱乐程序、私自更改 IP 地址、不登录到域等）进行控制。

④ 安全策略不能统一，人员计算机水平参差不齐，导致入网电脑的安全性难以保证，许多电脑不装杀毒软件或不打补丁就直接入网，内网经常有病毒感染或 ARP 攻击事件发生。

7.4.3 网络拓扑

图 7-7 所示为某部队网络拓扑结构图。该单位网络采用全智能交换机双机热

备的方式进行接入，因此在部署 MVG 准入技术上有一定的天然条件。

图 7-7　某部队网络拓扑结构图

7.4.4　解决方案

在经过众多的方案筛选和调研后，决定采用独立厂商的 NAC 系统。在其信息中心的机房部署一台硬件设备，使用 MVG 方式进行准入控制，通过完全旁路的方式来管理网络，如图 7-8 所示。

该单位在部署完准入控制系统后解决了以下几个问题。

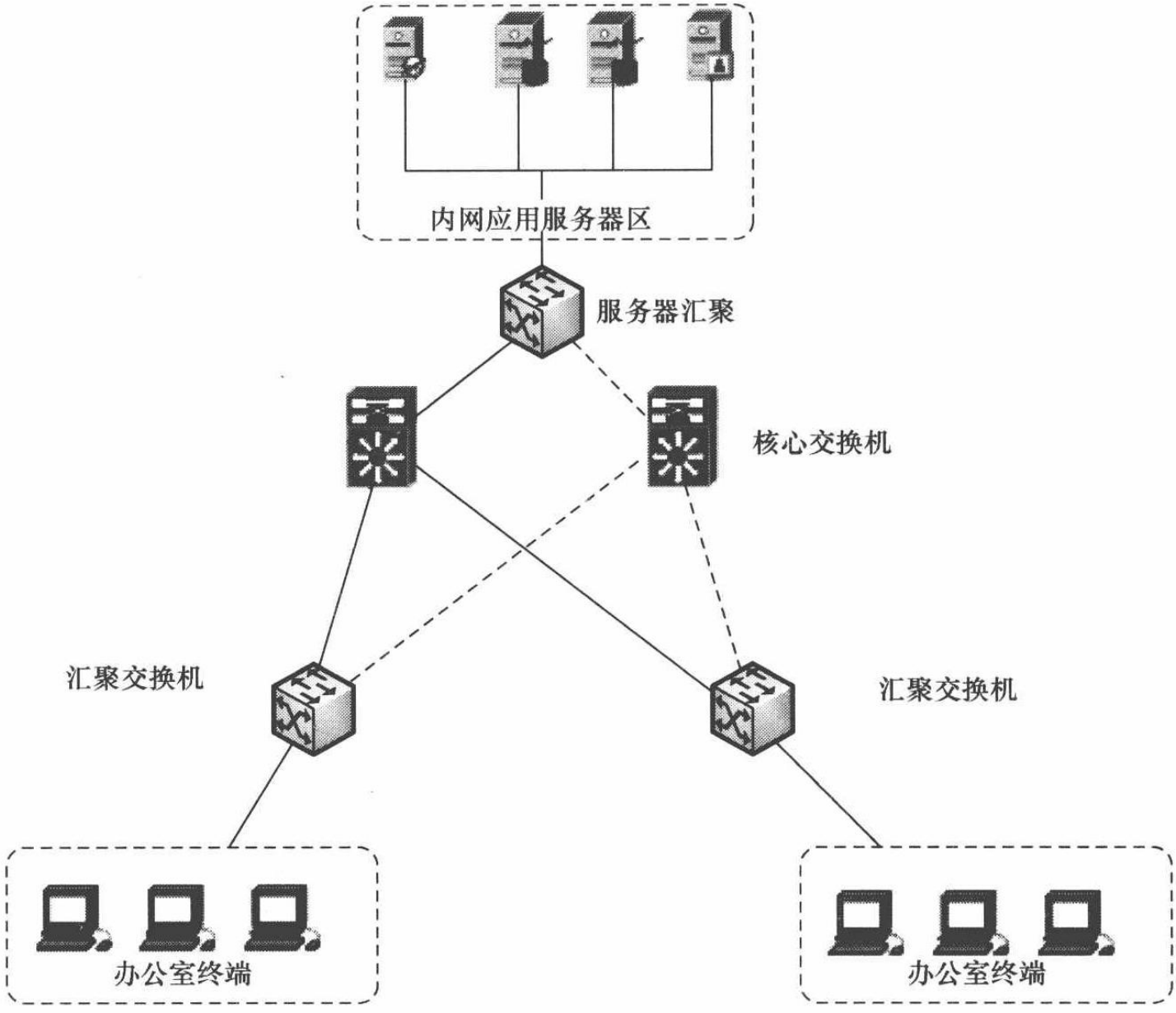
① 通过技术手段统计了入网的设备、人员、时间等信息。

② 有效地控制和管理了来宾入网的权限和记录。

③ 实现终端用户对于计算机管理，如：IP 管理，软件管理等的有序管理。

④ 确保终端用户安装并且更新了杀毒软件的病毒库，大大加强了内部网络的安全性。

通过本次项目实施，对整个网络重新进行了安全规划和加固：一是优化了原有网络接入方式，保证了网络的安全性和可靠性；二是对全网 5000 多个信息点的接入做了控制，必须达到安全规范才能接入业务网，确保每个接入网络的终端都安装了最新的防病毒软件，重要补丁都得到安装等；三是对每个终端的软件资产作了采样，统计终端的软件违规排行，并且对异常行为的终端采取措施。从网络与终端等方面立体化地加固了网络的安全性。


内网应用服务器区
服务器汇聚
核心交换机
汇聚交换机
汇聚交换机
办公室终端
办公室终端

备的方式进行接入，因此在部署 MVG 准入技术上有一定的天然条件。

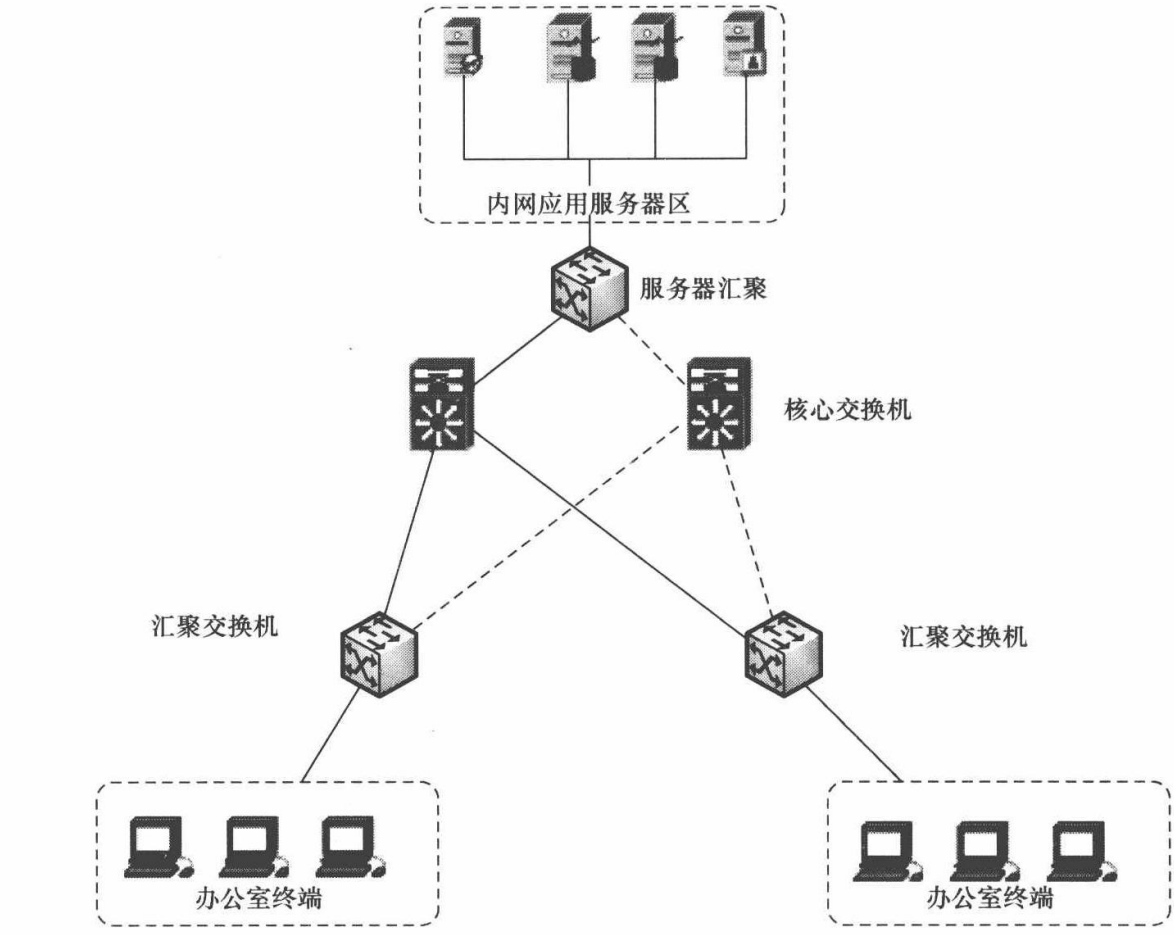


图 7-7　某部队网络拓扑结构图

7.4.4　解决方案

在经过众多的方案筛选和调研后，决定采用独立厂商的 NAC 系统。在其信息中心的机房部署一台硬件设备，使用 MVG 方式进行准入控制，通过完全旁路的方式来管理网络，如图 7-8 所示。

该单位在部署完准入控制系统后解决了以下几个问题。

① 通过技术手段统计了入网的设备、人员、时间等信息。

② 有效地控制和管理了来宾入网的权限和记录。

③ 实现终端用户对于计算机管理，如：IP 管理，软件管理等的有序管理。

④ 确保终端用户安装并且更新了杀毒软件的病毒库，大大加强了内部网络的安全性。

通过本次项目实施，对整个网络重新进行了安全规划和加固：一是优化了原有网络接入方式，保证了网络的安全性和可靠性；二是对全网 5000 多个信息点的接入做了控制，必须达到安全规范才能接入业务网，确保每个接入网络的终端都安装了最新的防病毒软件，重要补丁都得到安装等；三是对每个终端的软件资产作了采样，统计终端的软件违规排行，并且对异常行为的终端采取措施。从网络与终端等方面立体化地加固了网络的安全性。

图 7-8 MVG 准入控制方式部署示意图

7.5 某运营商网络准入控制案例

7.5.1 基本情况

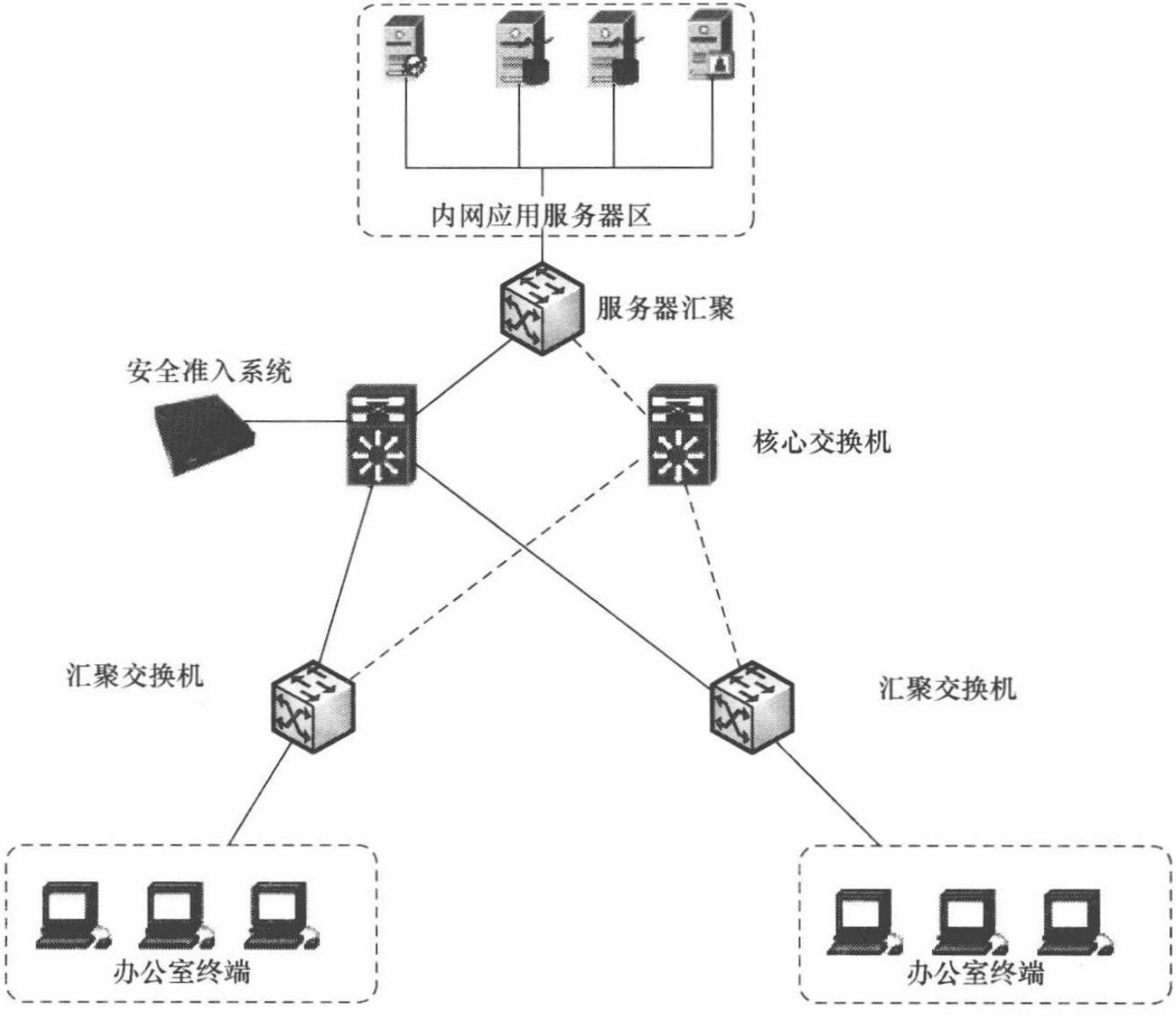
中国电信某省分公司是该省最大的基础网络运营商和综合信息服务提供商，是省内唯一拥有完整的固定网、移动网、基础网、数字网和数据网的通信运营企业，可以向客户提供丰富多彩、优质高效的信息通信服务，能够满足客户的各种通信及信息服务需求。目前，省公司下属两个一级部门共约 2500 台终端，主要涉及办公台式机、笔记本电脑及外来集成公司人员终端。

7.5.2 安全现状

该省电信网络连接了众多部门的 PC 终端，地域分布较广，由于没有一套切实有效的入网安全管理规范，在日常运行过程中暴露出以下安全性隐患问题。

1. 外来机器可以随意接入

电信公司有大量的合作伙伴，经常需要接入到单位网络，如果非授权人员随


内网应用服务器区
服务器汇聚
安全准入系统
核心交换机
汇聚交换机
汇聚交换机
办公室终端
办公室终端

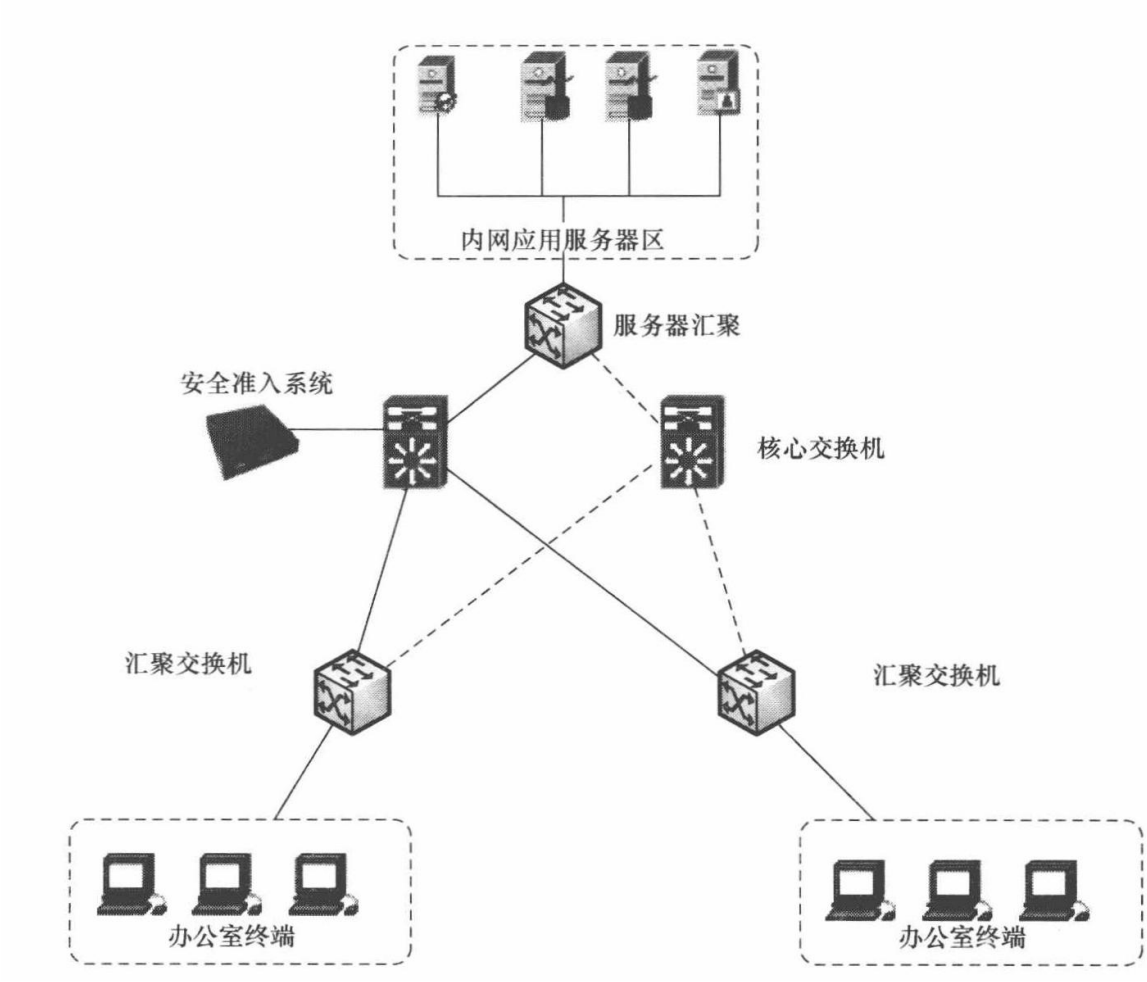


图 7-8 MVG 准入控制方式部署示意图

7.5 某运营商网络准入控制案例

7.5.1 基本情况

中国电信某省分公司是该省最大的基础网络运营商和综合信息服务提供商，是省内唯一拥有完整的固定网、移动网、基础网、数字网和数据网的通信运营企业，可以向客户提供丰富多彩、优质高效的信息通信服务，能够满足客户的各种通信及信息服务需求。目前，省公司下属两个一级部门共约 2500 台终端，主要涉及办公台式机、笔记本电脑及外来集成公司人员终端。

7.5.2 安全现状

该省电信网络连接了众多部门的 PC 终端，地域分布较广，由于没有一套切实有效的入网安全管理规范，在日常运行过程中暴露出以下安全性隐患问题。

1. 外来机器可以随意接入

电信公司有大量的合作伙伴，经常需要接入到单位网络，如果非授权人员随

意将外来笔记本电脑接入内网的某个网络端口，容易产生占用网络带宽，并带来有意无意的攻击等，影响单位内部网络的正常运行。

2. 无法明确内部机器的安全性

省电信内部所属的近 3000 台接入终端在网络中的安全性始终没有可靠的统计数据，这就无法形成全网的整体安全视图，从而对管理员的有效控制带来了盲点。

3. 内网机器违规出网

经常有工作人员把电脑带回家或者出差连接了互联网，一旦进行了违规的外联操作，那么在再次接回到电信单位内网的时候就很容易带入木马病毒或其他病毒，这些机器均可能是网络内部破坏攻击的风险源头。

4. 无法有效地对内网机器进行安全修复

信息部人员在管理过程中，对诸如如何保证内部 PC 机的操作系统没有漏洞，补丁得到有效更新；如何保证所有机器的杀毒软件版本统一及病毒库都符合要求；如何保证终端操作系统必须具有一定强度的账号密码等问题缺乏，有效的解决手段，对于存在各种安全隐患的终端，无法提供相应的机制或者平台来对其进行快速、有效、智能的安全修复。

7.5.3　网络拓扑和需求

图 7-9 所示为某省电信分公司网络拓扑结构图。该省电信网络在接入层交换机（楼层交换机）这一平台上普遍采用了 Cisco 3560 这一系列，因此构成了一个典型的 EOU 准入环境。

该单位建设需求是：利用建设中的准入平台，能够通过技术手段对内部的计算机接入网络进行安全管理，并进行安全评估、桌面管理、内网终端相应的资产管理及快速补丁分发和安装，从而保障单位内部的信息安全，保护该省电信所属的计算机不受病毒侵袭，防止重要商业信息以及国家敏感信息的泄漏。

7.5.4　解决方案

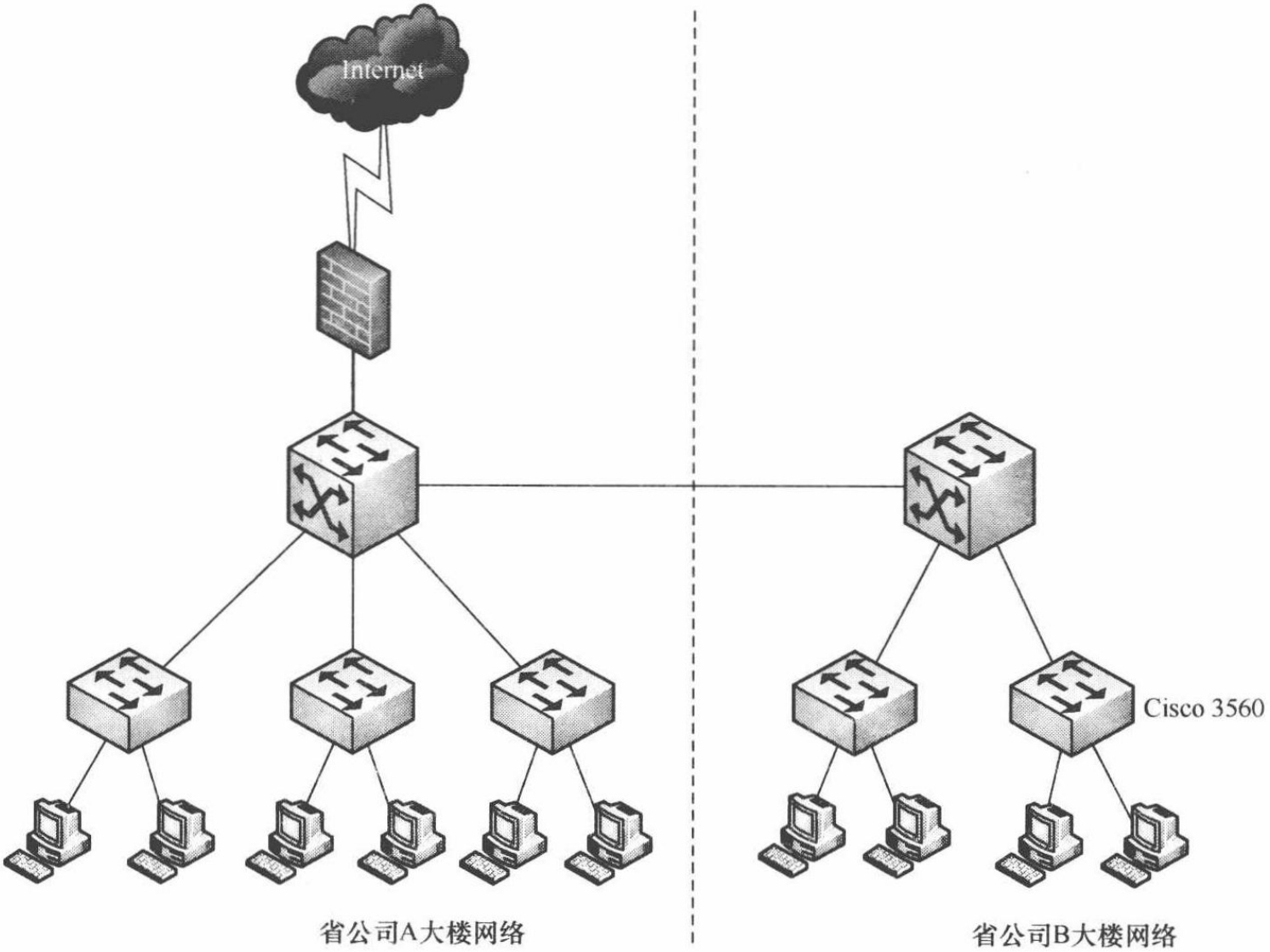
最终的方案采用某公司的一体化准入管理平台，在省公司所属两幢办公大楼机房分别部署准入控制设备，整个方案基于 Cisco EOU 准入强制技术，如图 7-10所示。

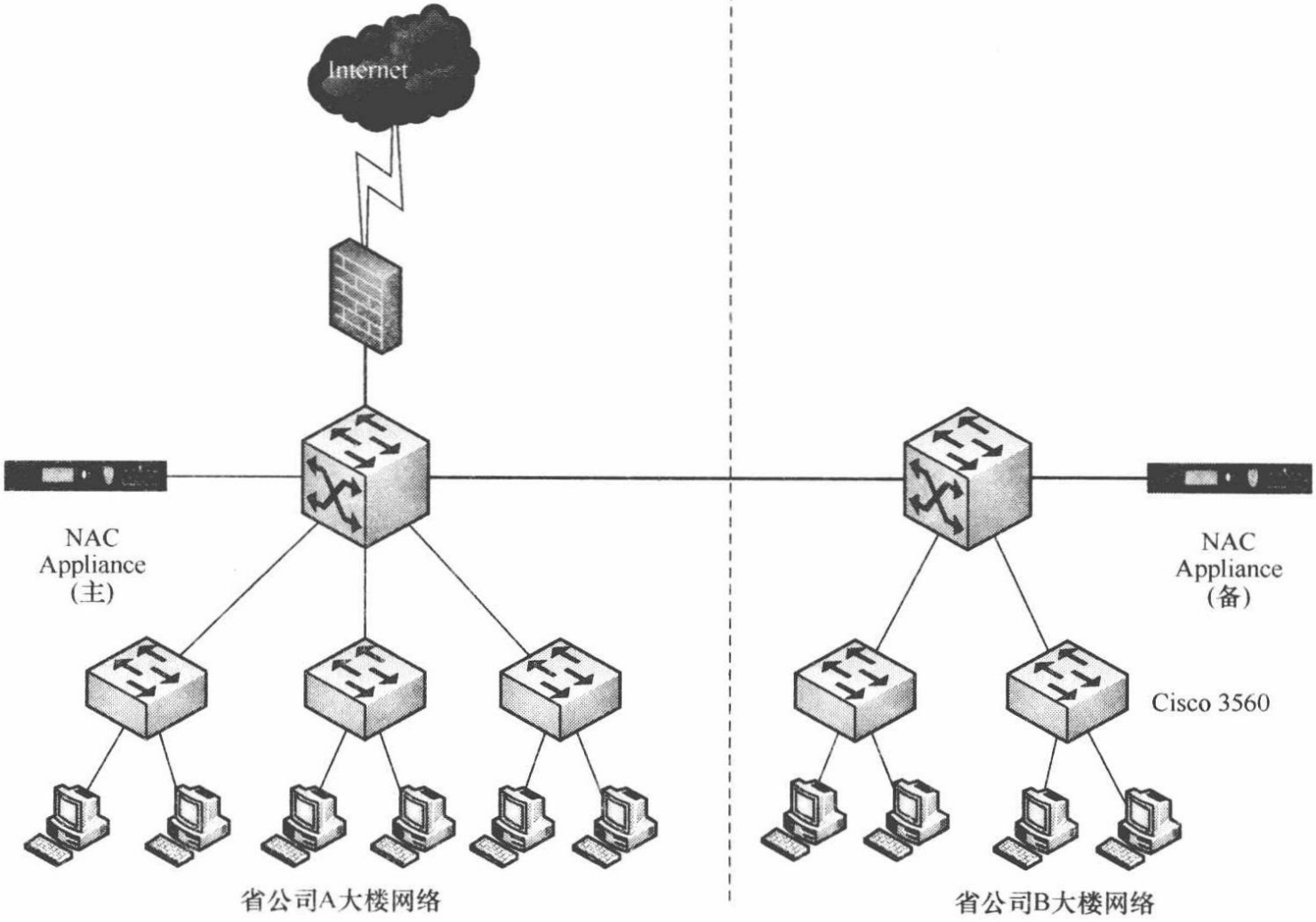
如图 7-10 所示，合法设备经过安全检查合格或修复完成后方可入网进行正常访问，外来设备只有经过管理员审核批准后才能够接入网络。整个网络边界明确，入网流程清晰，终端使用规范安全。

具体实现的功能包括以下几个方面。

图 7-9 某省电信分公司网络拓扑结构图

图 7-10 基于 Cisco EOU 准入技术部署示意图


Internet
Cisco 3560
省公司A大楼网络
省公司B大楼网络


Internet
NAC
Appliance
(主)
NAC
Appliance
(备)
Cisco 3560
省公司A大楼网络
省公司B大楼网络

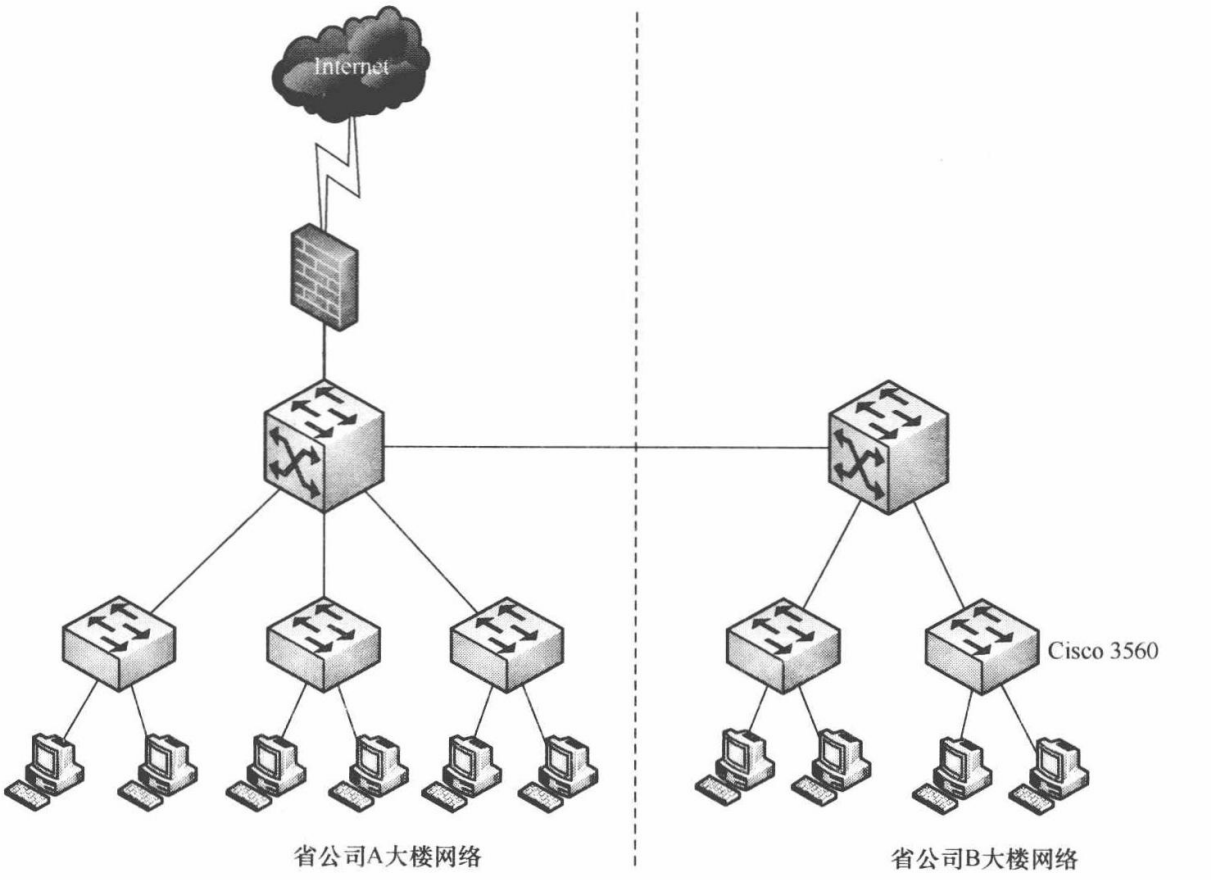


图 7-9 某省电信分公司网络拓扑结构图

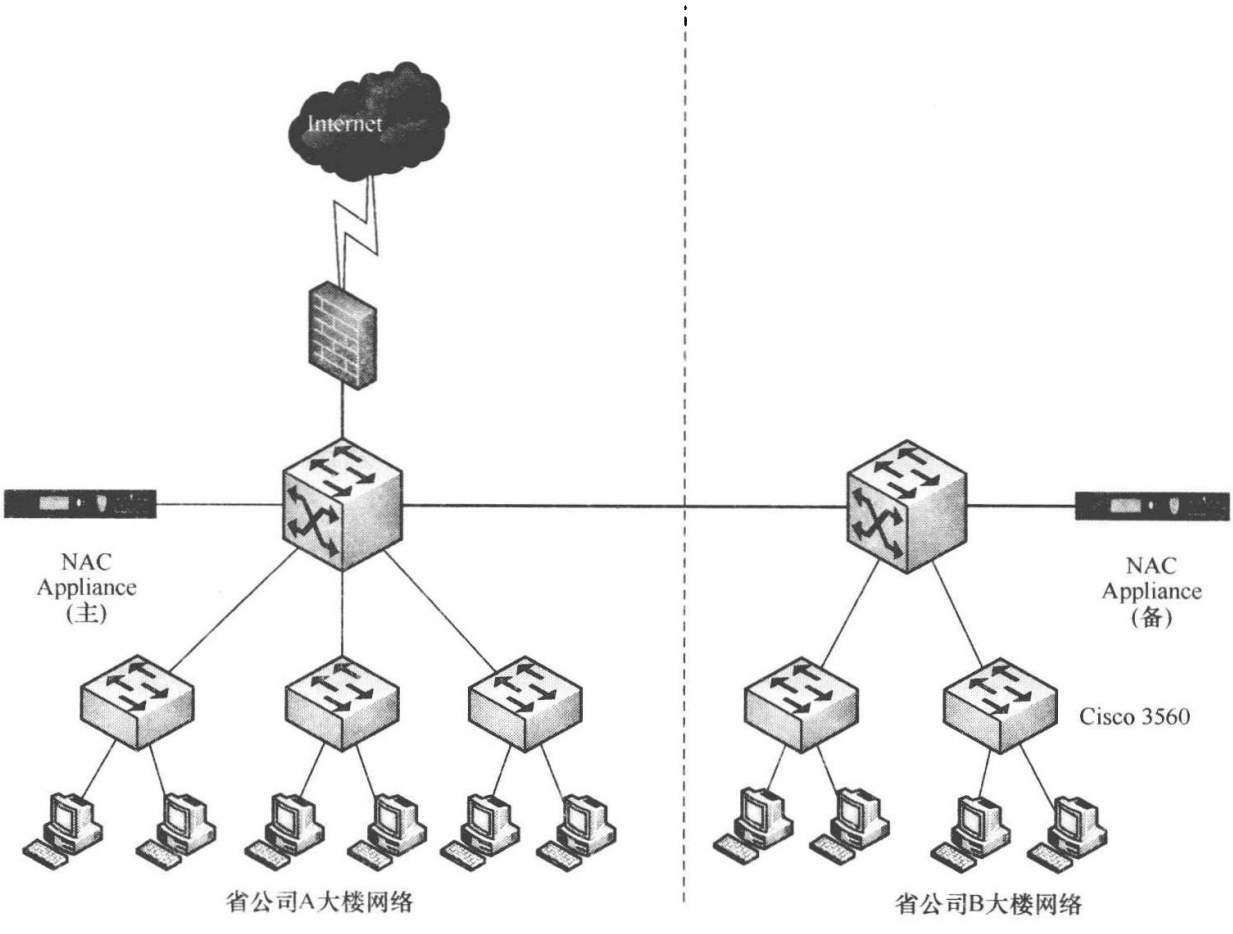


图 7-10 基于 Cisco EOU 准入技术部署示意图

1. 解决终端非法接入问题

终端入网必须遵循一整套规范的安全流程，没有得到管理员许可，任何非法终端将无法接入网络。

2. 对内网终端进行安全性检查与过滤

通过各项安全策略，对入网终端自身安全性（健康性）进行检查，如果发现存在安全问题，管理平台将自动阻断终端对网络的访问，终端必须完成了相应的加固修复后，方可依据策略访问相应授权区域。

3. 对访问网络进行合理切换

对于业务上有访问外网需要的设备，通过策略限制确保了终端在一个时间点只能访问一个网络，比如只能访问互联网，或者只能访问内网，从而避免了终端同时访问两个网络时形成两个网络之间隐蔽通道的问题。

7.6　某大型企业网络准入控制案例

7.6.1　基本情况

某机械国际重工股份有限公司是一家以工程机械、农业装备、车辆为主体业务的大型产业装备制造企业，位列中国 100 最具价值品牌排行榜前列。整个网络规模中，本部涵盖 4 个事业部，各事业部下属约 50 多个车间，另外在全国各地部署了 8 个分公司，网络内共 5000 多个接入终端。

7.6.2　安全现状

该企业长期以来对内网信息化建设十分重视，全网采用 Cisco、Juniper、Bluecoat 等国外设备，已逐渐达到了国际化水平。但企业内网仍然存在以下难以解决的问题。

① 外来终端轻松接入内网，轻松访问内网资源，极易导致机密资料外泄。

② 内网边界到底在哪里，私接交换机、Hub 如何处理。

③ 已有桌面管理和加密系统，安装客户端部署麻烦，有抵触，担心实施及维护工作量大怎么办。

④ 网络设备资产统计不全，全网交换机数量不明，且无法定位到交换机端口下的个人。

⑤ 无法识别接入网络的用户名及设备身份，无法定位到设备使用人到底是谁。

7.6.3　网络拓扑和需求

该企业全网采用 Cisco 设备，拓扑示意如图 7-11 所示。

图 7-11 某企业网络拓扑结构示意图

针对准入控制技术选型来说，在诸多准入厂商与设备中，如何选择适合自身网络环境的准入技术成为了一大难题，需要解决的问题包括以下几个方面。

① 如何做到全网无盲点的准入控制，如网络打印机。

② 既要做到接入层的控制又不想改变交换机，怎么办。

③ 既要让接入终端所受影响小，又要让接入终端严格遵守各种规范，怎么办。

④ 如何智能管理全网交换机、IP-mac 设备、快速定位到设备所在交换机端口。

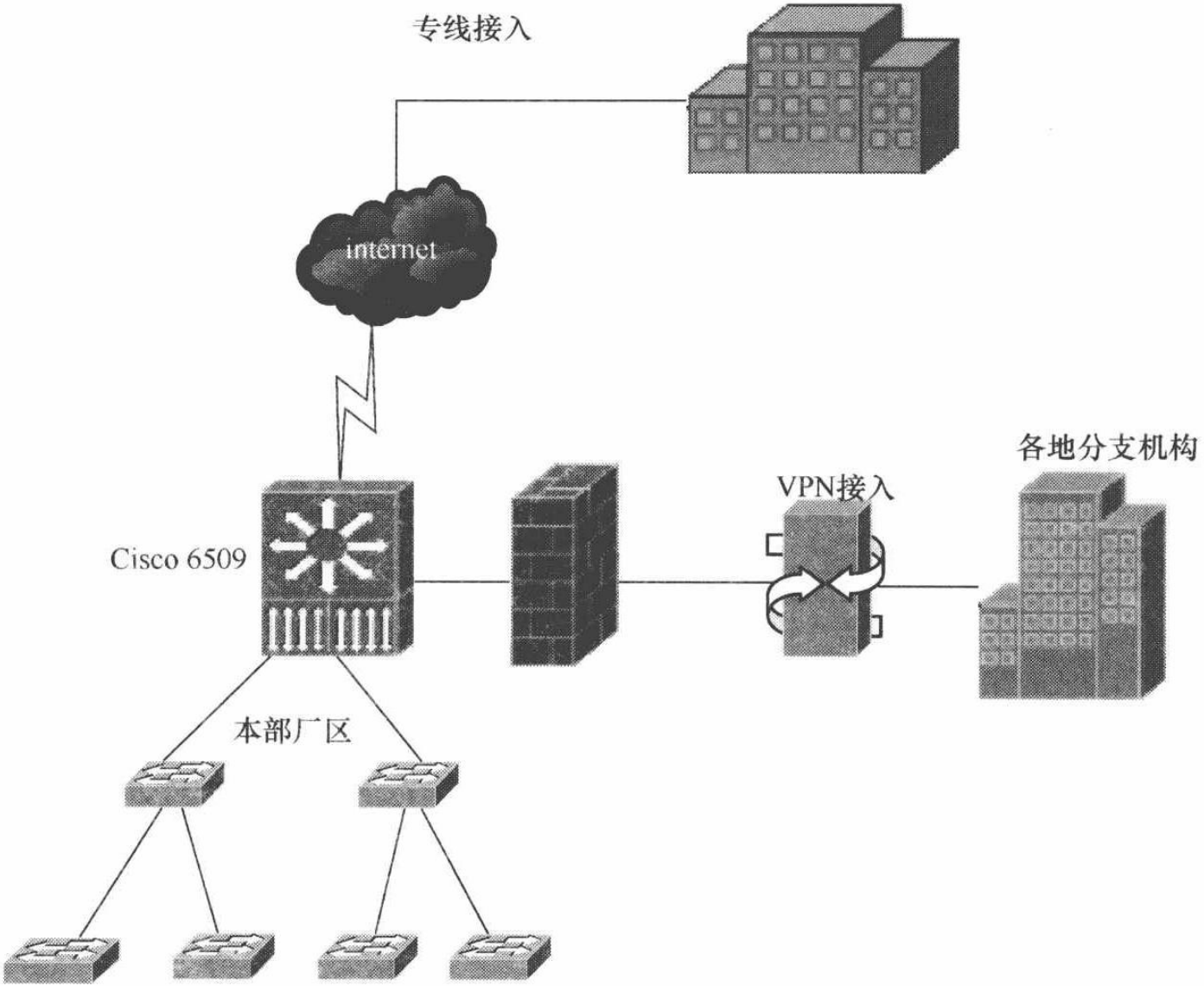
7.6.4 解决方案

经过前期的严格测试和选型，该企业最终选择了某国内公司的准入方案，全网采用 MVG 准入控制设备接入在核心交换，管理全网接入层交换机，如图 7-12 所示。

部署效果如下：

① 对全网交换机、打印机、终端进行统一管理。并以图形化交换机面板显示端口使用情况，根据交换机端口状态、部门、主机 IP、MAC 定位到交换机端口下的终端所属部门、使用人等信息。

② Hub 管理细分化，针对 Hub 下终端，认证通过后正常入网。认证不通过设备自动进入隔离修复区。


专线接入
internet
Cisco 6509
VPN接入
各地分支机构
本部厂区

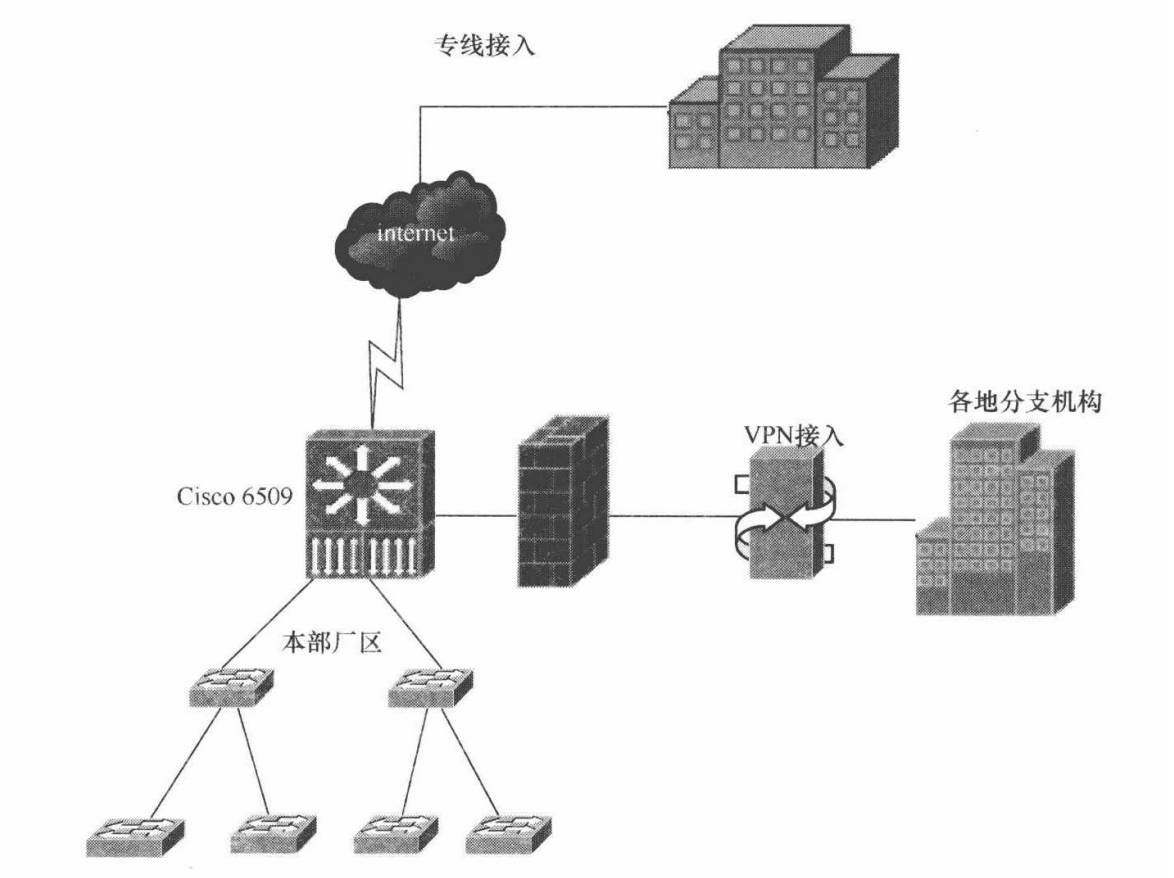


图 7-11 某企业网络拓扑结构示意图

针对准入控制技术选型来说，在诸多准入厂商与设备中，如何选择适合自身网络环境的准入技术成为了一大难题，需要解决的问题包括以下几个方面。

① 如何做到全网无盲点的准入控制，如网络打印机。

② 既要做到接入层的控制又不想改变交换机，怎么办。

③ 既要让接入终端所受影响小，又要让接入终端严格遵守各种规范，怎么办。

④ 如何智能管理全网交换机、IP-mac 设备、快速定位到设备所在交换机端口。

7.6.4 解决方案

经过前期的严格测试和选型，该企业最终选择了某国内公司的准入方案，全网采用 MVG 准入控制设备接入在核心交换，管理全网接入层交换机，如图 7-12 所示。

部署效果如下：

① 对全网交换机、打印机、终端进行统一管理。并以图形化交换机面板显示端口使用情况，根据交换机端口状态、部门、主机 IP、MAC 定位到交换机端口下的终端所属部门、使用人等信息。

② Hub 管理细分化，针对 Hub 下终端，认证通过后正常入网。认证不通过设备自动进入隔离修复区。

图 7-12　MVG 技术解决方案部署示意图

③ 采用 Agentless 无客户端模式，友好 Web 引导界面。实施部署快速、无抵触情绪。

④ 平台推送桌面管理、加密系统客户端。后台一键式修复。最大限度减少了实施成本。

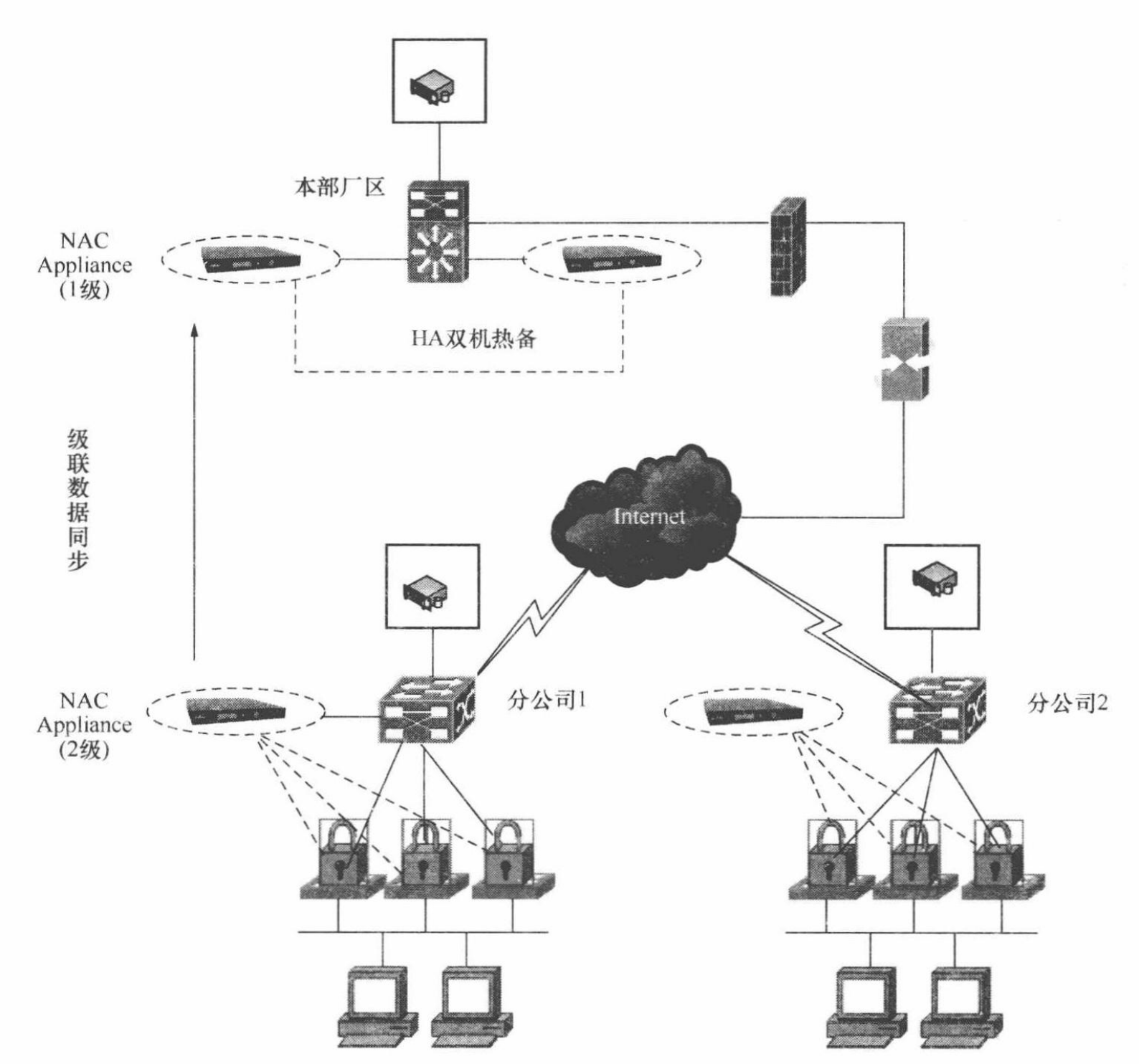
⑤ 与第三方 OA 业务系统联动进行双实名认证。保障接入终端身份的合法性。

⑥ 所有外来终端接入必须经管理员审批才能入网，有效地保护了内网资源。

7.7　某省工商行政管理局准入控制案例

7.7.1　基本情况

××省工商行政管理局是主管××省市场监督管理和行政执法工作的省级政府直属机构，包括省局、9 个地市市局和 50 多个县局，各级通过实行垂直管理，


本部厂区
NAC
Appliance
(1级)
HA双机热备
级联数据同步
Internet
NAC
Appliance
(2级)
分公司1
分公司2

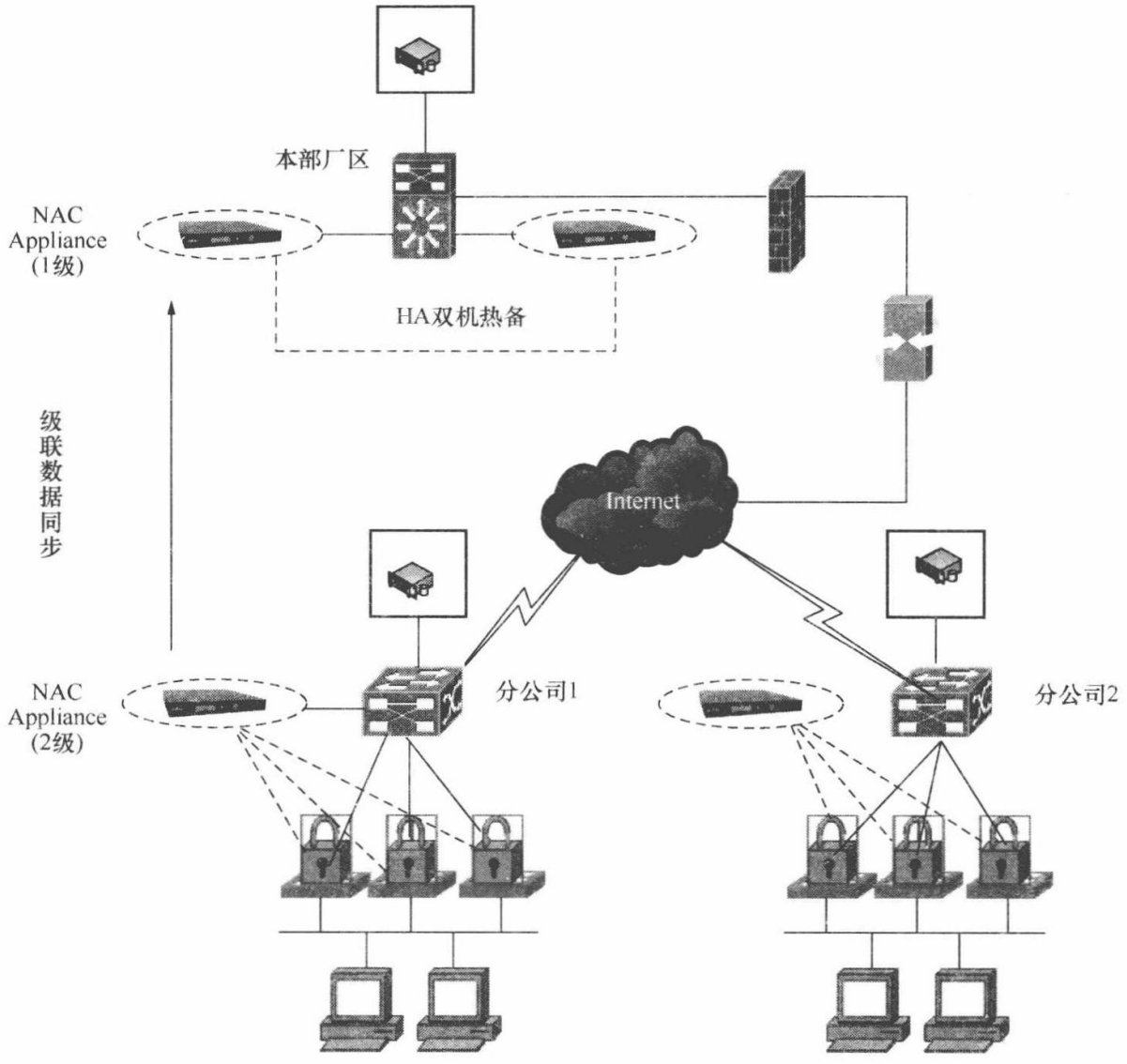


图 7-12　MVG 技术解决方案部署示意图

③ 采用 Agentless 无客户端模式，友好 Web 引导界面。实施部署快速、无抵触情绪。

④ 平台推送桌面管理、加密系统客户端。后台一键式修复。最大限度减少了实施成本。

⑤ 与第三方 OA 业务系统联动进行双实名认证。保障接入终端身份的合法性。

⑥ 所有外来终端接入必须经管理员审批才能入网，有效地保护了内网资源。

7.7　某省工商行政管理局准入控制案例

7.7.1　基本情况

××省工商行政管理局是主管××省市场监督管理和行政执法工作的省级政府直属机构，包括省局、9 个地市市局和 50 多个县局，各级通过实行垂直管理，

形成覆盖全省的工商管理系统。主要职能是：主管全省工商企业登记注册工作，依法确认各类经营者的主体资格，监督管理或参与监督管理各类市场，依法规范市场交易行为，保护公平竞争，查处经济违法行为，取缔非法经营，保护正常的市场经济秩序。该单位终端用户达到 12 000 多点，运用规模庞大，包括全省范围省市县三级各工商局的内部办公网中的台式机、移动接入设备和打印机；涉及的运用包括办公网络、OA 系统和各工商业务系统。

7.7.2 安全现状

近年来，随着××省工商局信息化建设的不断发展，门户信息网等业务系统逐渐上线运行，工商局内各部门的日常办公也越来越离不开网络。与此同时，用户非受控接入带来的安全隐患也随之产生，给内部网络办公管理带来了不小的麻烦。为了更好地开展电子政务和网上交易的监督管理机制，保证工商局内部网络的安全、高效运作，××省工商网络部门决定采用终端用户准入控制的方案，针对接入内网的终端进行安全认证。其内网主要安全风险有如下几个方面。

1. 外来终端随意接入

由于工作需要，外来的人员携带的笔记本电脑经常需要接入网络中，若接入的设备对内网进行嗅探、抓包等攻击可以很容易的获取网络中明文传输的信息，加上外来设备如果携带病毒，很可能通过内网传染给其他终端，造成网络大面积感染，后果不堪设想。

2. 补丁问题安全隐患

大部分员工对打补丁以提高安全防护的认识不足。据现场调研，终端补丁未打或未打全现象在局内员工电脑中十分普遍，加上终端处于内部网络环境之中，无法通过 WSUS 等服务器在网上打补丁，使补丁安全规范一直无法落到实处。这样不仅容易给不法分子留下后门，一旦遭遇病毒或木马攻击，终端设备将成为威胁来源和风险的跳板，对内部网络形成巨大的安全隐患。

3. 移动介质滥用

内部网络虽然从物理上隔绝与 Internet 的联系，防止遭到外部网络上病毒和黑客的攻击。但是还是能够从一些移动介质（如 U 盘、移动硬盘等）中感染病毒。特别是一些别有用心的人，将很轻易地把重要文件、机密数据等通过移动介质拷到网络外部造成泄密，从而给企业和政府部门造成重大损失。

4. 终端行为无法审计、告警

终端的一些行为常常会无意识的对网络安全造成影响。而管理员往往缺乏及时有效的手段，准确快捷的掌握每个终端的运行状况，如终端对一些文档的读

写、U 盘对文件的复制、修改，邮件的发送和接受等均缺乏一个方便直观的审计平台。除此之外一些威胁行为也无法得到快速的定位。

7.7.3　网络拓扑和需求

某局的网络环境如图 7-13 所示。

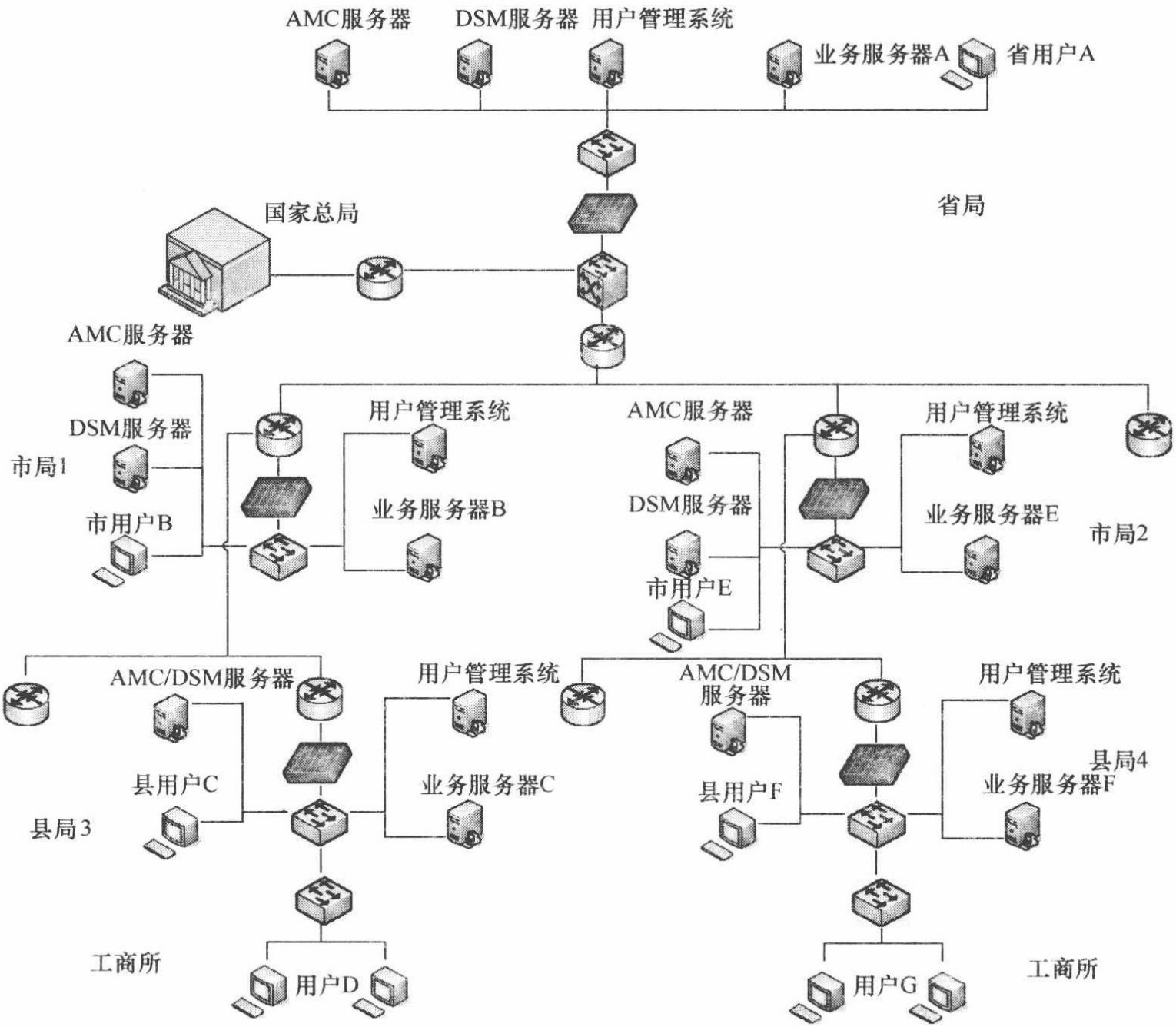
图 7-13　某局网络拓扑结构图

从实际情况看，此单位网络中的交换机品牌众多，包括 H3C、锐捷等，型号也不尽相同。此外接入层中还有 D-Link 等非网管的傻瓜交换机，需要根据不同环境和设备做一定的配置调整和升级，这给全网的规范化管理带来了不小的困难。

总体来看，该单位的内网安全建设有如下需求点。

1. 准入控制

用户接入时自动启动登录界面对入网设备和人员进行认证，只有通过了账号密码认证并且安装了多维终端安全管理平台客户端的设备才允许接入网络；准入


AMC服务器
DSM服务器
用户管理系统
业务服务器A
省用户A
国家总局
省局
AMC服务器
DSM服务器
市局1
市用户B
用户管理系统
业务服务器B
AMC服务器
DSM服务器
市用户E
用户管理系统
业务服务器E
市局2
AMC/DSM服务器
县用户C
县局3
用户管理系统
业务服务器C
工商所
用户D
AMC/DSM
服务器
县用户F
用户管理系统
县局4
业务服务器F
工商所
用户G

写、U 盘对文件的复制、修改，邮件的发送和接受等均缺乏一个方便直观的审计平台。除此之外一些威胁行为也无法得到快速的定位。

7.7.3　网络拓扑和需求

某局的网络环境如图 7-13 所示。

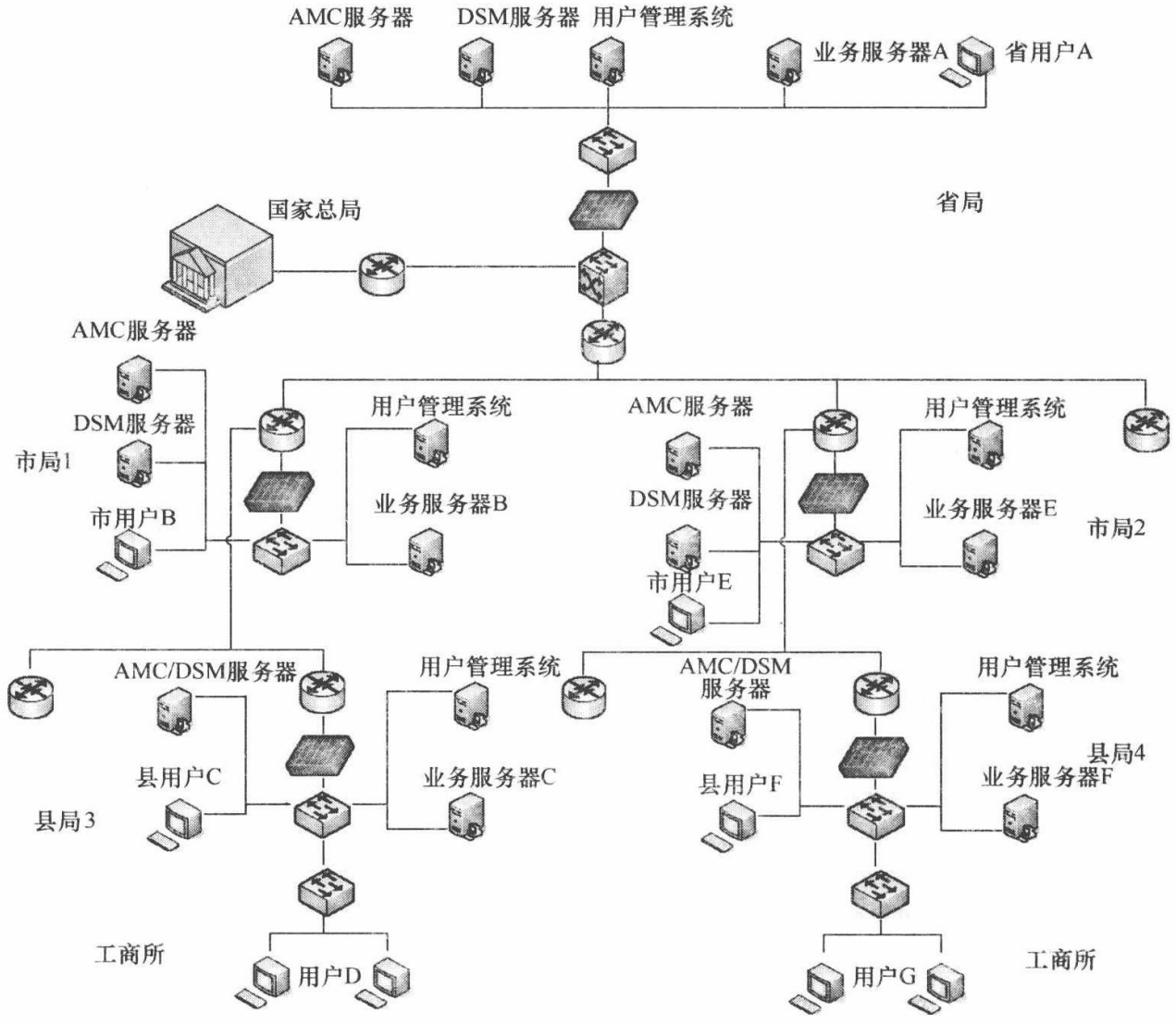


图 7-13　某局网络拓扑结构图

从实际情况看，此单位网络中的交换机品牌众多，包括 H3C、锐捷等，型号也不尽相同。此外接入层中还有 D-Link 等非网管的傻瓜交换机，需要根据不同环境和设备做一定的配置调整和升级，这给全网的规范化管理带来了不小的困难。

总体来看，该单位的内网安全建设有如下需求点。

1. 准入控制

用户接入时自动启动登录界面对入网设备和人员进行认证，只有通过了账号密码认证并且安装了多维终端安全管理平台客户端的设备才允许接入网络；准入

控制技术采用 802.1x，平台必须具备逃生功能，在宕机后可以紧急放开。

2. 桌面管理

对网络中的 IP 进行统一管理，包括使用者、所属部门、地址绑定、是否通过验证以及添加可信等；软硬件资产管理，保障资产的安全；软件分发，对工商业务系统的软件进行统一升级；移动介质 U 盘管理，所有内网中使用的 U 盘必须经过注册才能使用，且带出内网后无法使用；黑白程序策略，对特定的软件如暴风影音和其他游戏软件等在上班时间予以禁止使用。

7.7.4 解决方案

为保证最高安全性和对网络环境的兼容性，该企业最终选择了某国内公司的准入方案，该公司为此项目提供的方案中采用了 AMC 作为 Radius 服务器，在接入层配置 802.1x 的部署方案，与 H3C S5120、RG S2126 等系列交换机配合，提供准入控制，有效防病毒，补丁自动升级等，保证高安全，并且能够兼容网内极其复杂的交换机环境。同时，部署一套 DSM 桌面管理平台，与 AMC 进行联动，对入网设备的行为进行统一管理，对非法用户的上网行为进行审计，对异常流量进行实时的流量分析。

认证流程图如图 7-14 所示。

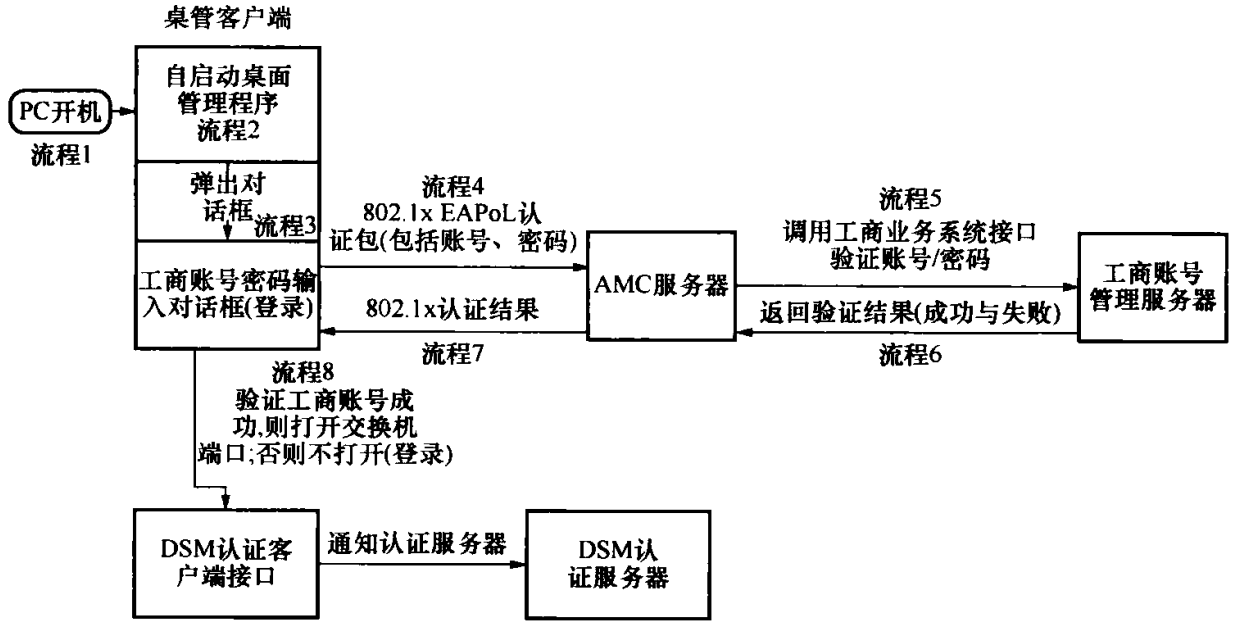


图 7-14 准入控制认证流程

具体来看，该解决方案有如下特点。

1. 严格的身份认证

除可采用用户名和密码的身份认证外，安全准入还支持 U-key 认证。每个允许接入的员工发给一个经过认证的外接 U-key 设备，登录网络前必须将 U-key

插入电脑，经过认证后才能入网，而且入网后若拔出 U-key 将出现断网。

2. 完备的安全状态评估

根据管理员配置的安全策略，安全准入客户端能够对终端进行包括病毒库版本、补丁、安装的应用软件、代理、拨号配置等安全认证检查；同时，此终端准入系统还支持和微软 WSUS 系统的配合使用，支持和瑞星、江民、金山、Symantec、McAfee、MSE、360、卡巴斯基等国内外主流防病毒厂商联动。

3. 基于角色的网络授权

安全准入可基于终端用户的角色，向安全联动设备下发事先配置的接入控制策略，按照用户角色权限规范用户的网络使用行为。

4. 准入与桌面管理融合

终端准入方案将用户管理和网络管理进行了智能融合，通过网络准入不仅能够了解到网络设备信息和状态，通过桌面管理还可以实现对接入用户的直观管理，实现查看用户信息、强制用户卸载、执行安全检查等操作。

5. 桌面资产管理

通过终端准入客户端提供了对网络终端资产全方位的监控和管理的功能，可以对网络终端软硬件使用情况、变更情况进行监控，同时还支持网络终端资产的配置管理和软件的统一分发，实现对资产的有效管理。

7.8　某电力行业网络准入控制案例

7.8.1　基本情况

国电某集团公司是中国国电集团新能源产业中一家专门从事风电设备制造的高新技术企业，也是国内风机产业链分布最广、发展最快的大型国有控股风电设备制造企业。公司以北京总部为中心，下设四大总装和两大主要部件生产基地，分布于河北、内蒙古、江苏和西北地区。该企业共 6 个办公区域，下设保定、连云港、赤峰等地 4 个分公司，涵盖局域网接入及 VPN 接入的多种网络环境。

7.8.2　安全现状

在多年的网络使用过程中，信息部门发现始终存在以下难以解决的问题。

① 无法清楚了解每日有多少台设备进入了公司的网络。

② 外来用户通过一根网线、一个内网 IP 就可以随意访问内网资源。

③ 内网用户私自更改 IP 地址，常常造成内网 IP 冲突，IP 资源管理困难。

④ 全网终端众多，对 IT 资产无法进行统计和有效管理，维护工作量日益加重。

⑤ 缺乏有效手段对用户的操作行为（如随意安装娱乐程序、私自更改 IP 地址）等进行规范管理。

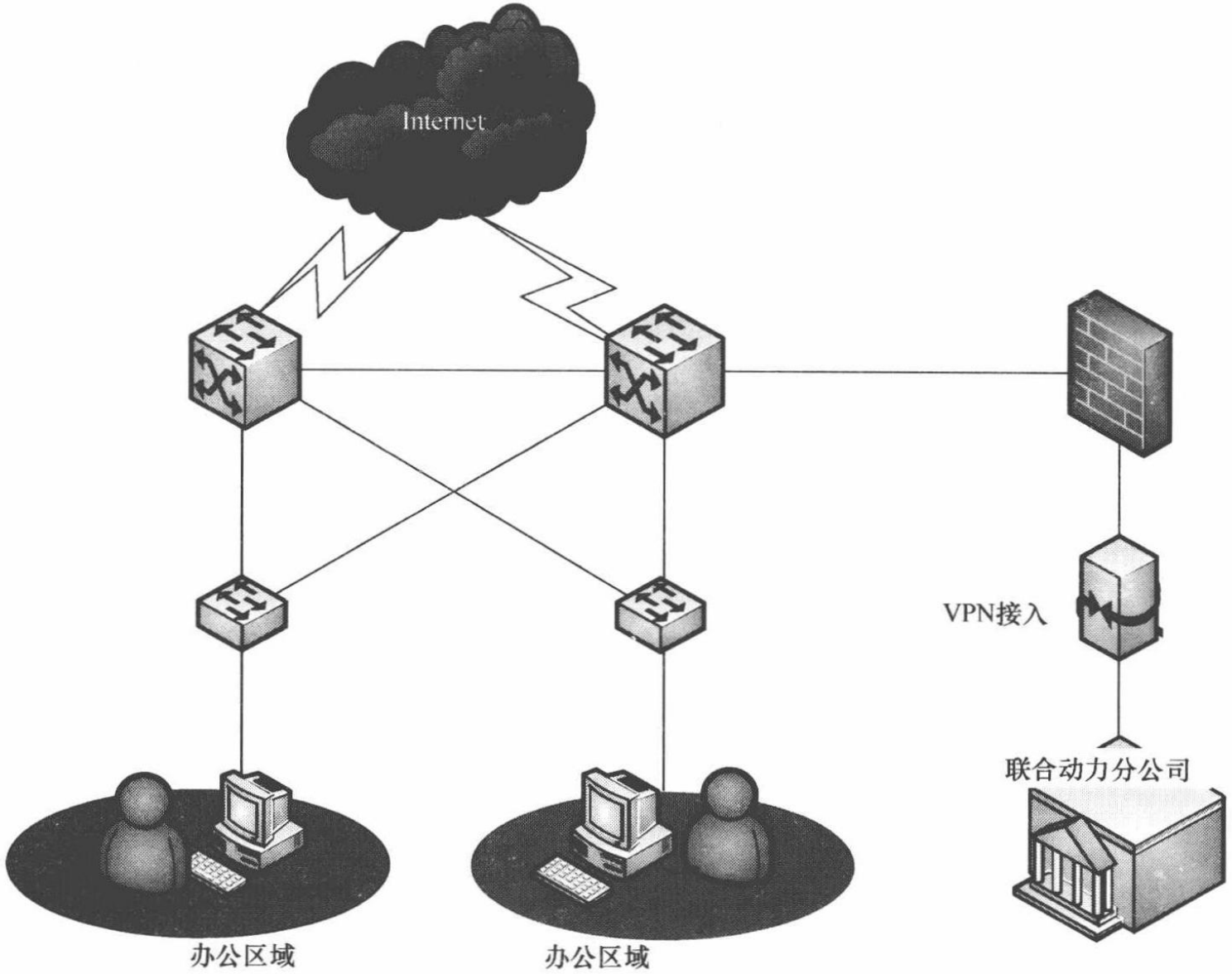
为了解决长期困扰网络信息部门的上述问题，本着遵循《信息安全等级保护管理办法》中内网安全控制条款和满足上市公司内部信息安全控制和安全体系建设要求，在公司领导的重视下提出建设内网安全准入控制系统。该项目主要的安全目标在于控制来宾对于内网重要资源的访问，控制内网设备的安全性，规范用户的入网行为，并且对安全系数低的设备进行跟踪和修复。

7.8.3 网络拓扑和需求

作为一家国内、国外技术领先的电力能源企业，该公司长期以来一直十分重视信息化建设，内部网络主体架构采用 Cisco 设备。拓扑示意如图 7-15 所示。

图 7-15 某公司网络拓扑结构图

该公司对网络准入控制的主要需求为：对内网的设备接入网络进行控制和管理，解决公司员工在工作时段对设备和网络的各类非法使用问题，进行内网的整体安全管理。实现功能主要包括：MVG、透明网桥准入认证、设备安全性扫描及修复、IP-Mac 地址绑定、IT 资产统计、远程维护等。


Internet
VPN接入
联合动力分公司
办公区域
办公区域

④ 全网终端众多，对 IT 资产无法进行统计和有效管理，维护工作量日益加重。

⑤ 缺乏有效手段对用户的操作行为（如随意安装娱乐程序、私自更改 IP 地址）等进行规范管理。

为了解决长期困扰网络信息部门的上述问题，本着遵循《信息安全等级保护管理办法》中内网安全控制条款和满足上市公司内部信息安全控制和安全体系建设要求，在公司领导的重视下提出建设内网安全准入控制系统。该项目主要的安全目标在于控制来宾对于内网重要资源的访问，控制内网设备的安全性，规范用户的入网行为，并且对安全系数低的设备进行跟踪和修复。

7.8.3 网络拓扑和需求

作为一家国内、国外技术领先的电力能源企业，该公司长期以来一直十分重视信息化建设，内部网络主体架构采用 Cisco 设备。拓扑示意如图 7-15 所示。

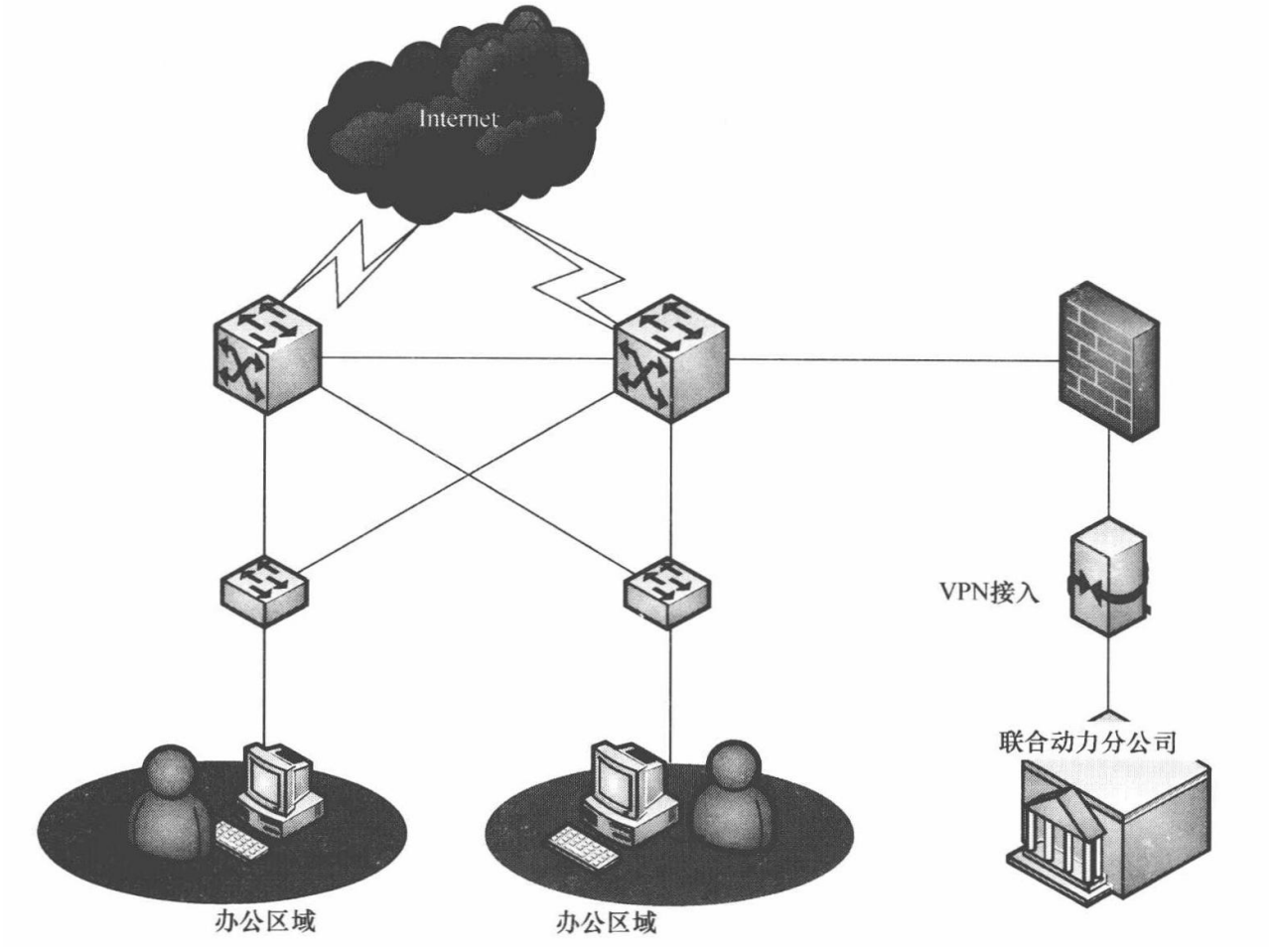


图 7-15 某公司网络拓扑结构图

该公司对网络准入控制的主要需求为：对内网的设备接入网络进行控制和管理，解决公司员工在工作时段对设备和网络的各类非法使用问题，进行内网的整体安全管理。实现功能主要包括：MVG、透明网桥准入认证、设备安全性扫描及修复、IP-Mac 地址绑定、IT 资产统计、远程维护等。

7.8.4　解决方案

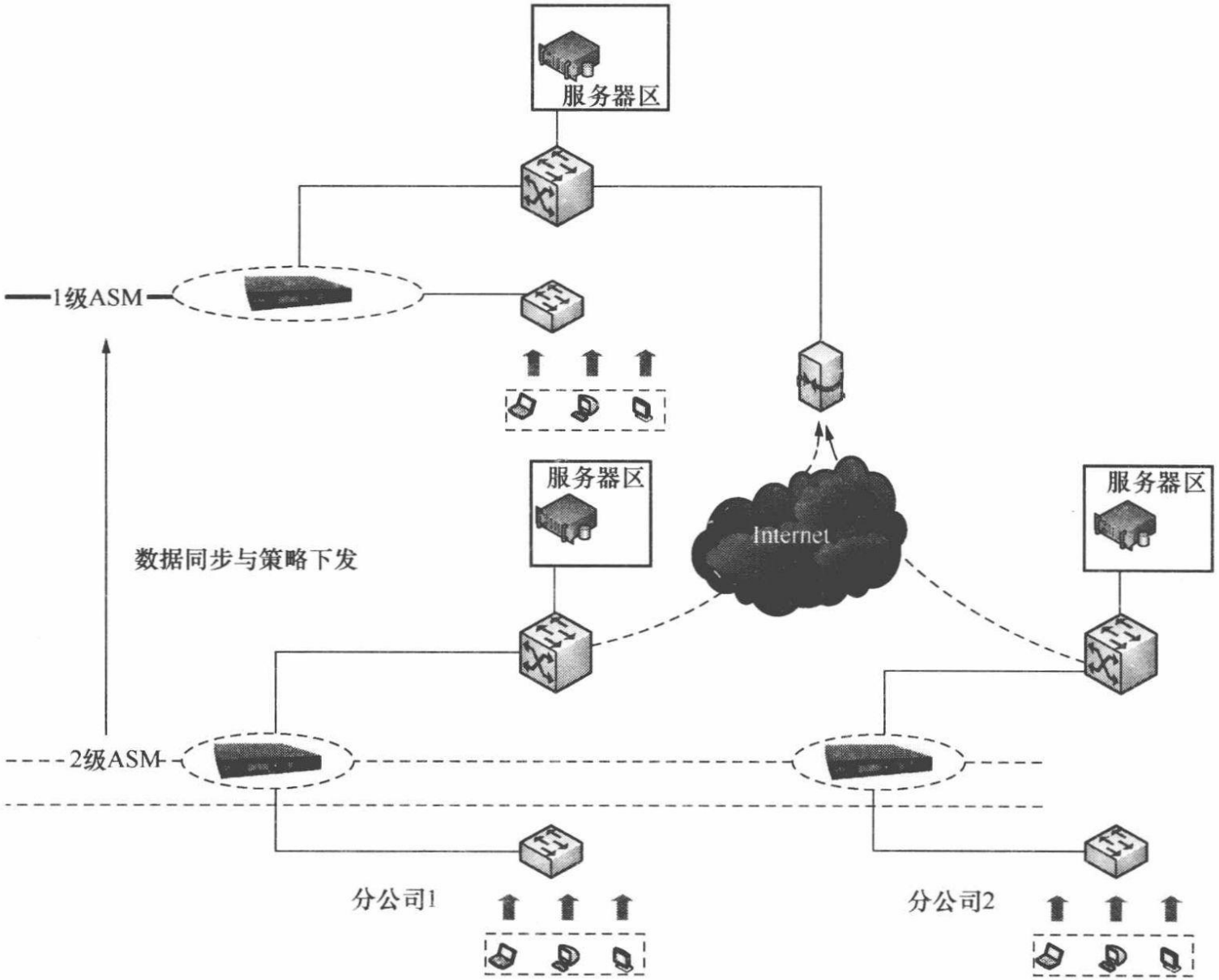
经过前期的严格测试和选型，最终选择了同行业中技术领先、性能稳定的某公司的入网规范管理系统作为整个项目的准入控制平台，采用透明网桥的方式连接核心与汇聚层交换机，以近似网络安全网关的方式实现内网准入安全。在国电总部和 2 个分公司分别部署 1 台准入控制设备，利用级联方式实现上下级之间的管理和数据同步，如图 7-16 所示。

图 7-16　基于透明网桥的准入技术解决方案部署示意图

部署准入控制系统后，在该公司内网安全体系中实现了如图 7-17 所示的准入控制效果。

1. 入网身份验证

所有接入内网的设备均需要验证其身份，未通过身份验证的设备拒绝其入网。外来设备选择“来宾模式”后能够访问互联网和收发邮件，但不能进入内网。


服务器区
1级ASM
数据同步与策略下发
服务器区
Internet
服务器区
2级ASM
分公司1
分公司2

7.8.4　解决方案

经过前期的严格测试和选型，最终选择了同行业中技术领先、性能稳定的某公司的入网规范管理系统作为整个项目的准入控制平台，采用透明网桥的方式连接核心与汇聚层交换机，以近似网络安全网关的方式实现内网准入安全。在国电总部和 2 个分公司分别部署 1 台准入控制设备，利用级联方式实现上下级之间的管理和数据同步，如图 7-16 所示。

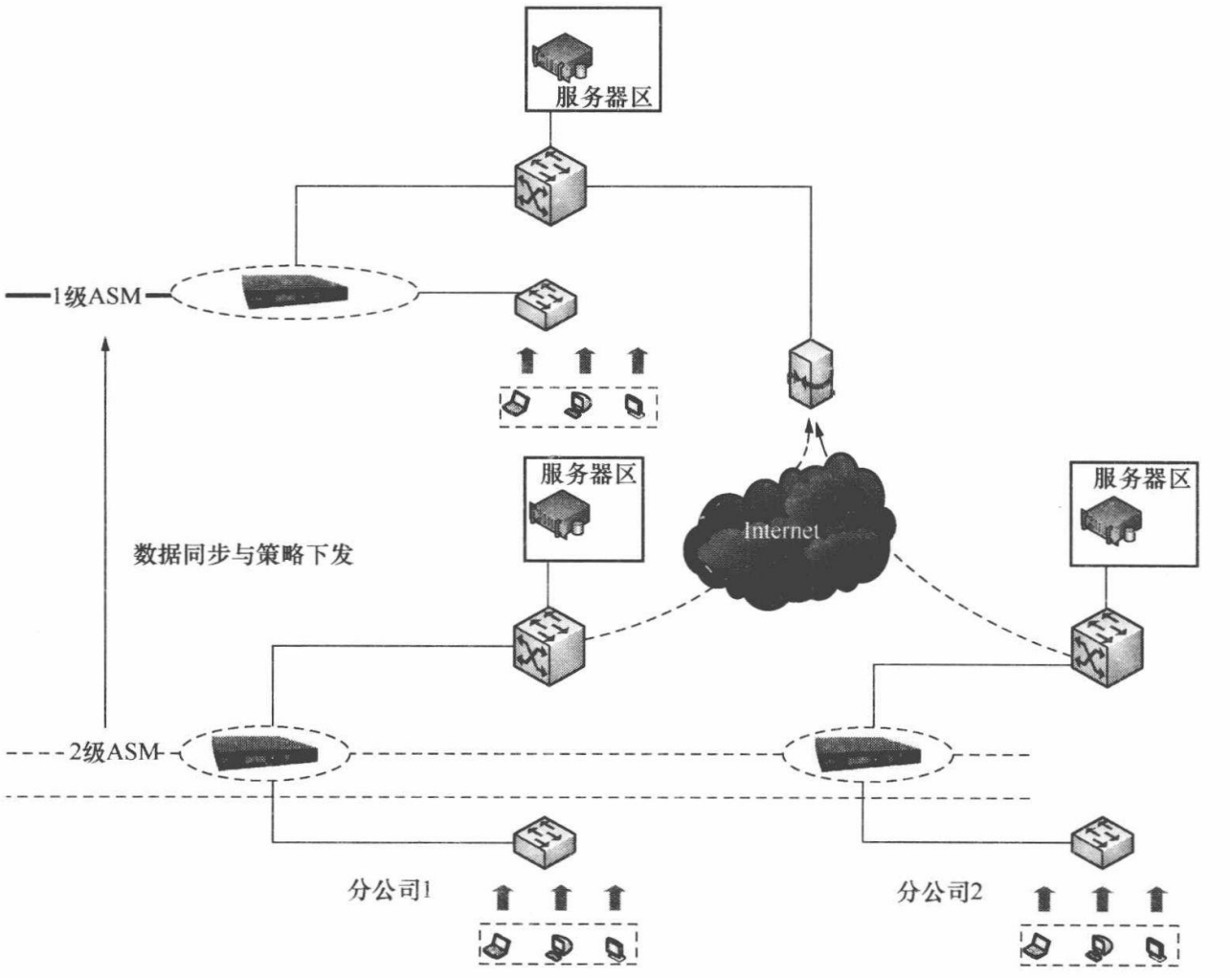


图 7-16　基于透明网桥的准入技术解决方案部署示意图

部署准入控制系统后，在该公司内网安全体系中实现了如图 7-17 所示的准入控制效果。

1. 入网身份验证

所有接入内网的设备均需要验证其身份，未通过身份验证的设备拒绝其入网。外来设备选择“来宾模式”后能够访问互联网和收发邮件，但不能进入内网。

图 7-17 准入控制部署实施效果图

2. 入网设备安全规范检查

对于公司内部所有设备进行安全规范的检查，主要包括杀毒软件检查、补丁检查、弱口令检查等。对于不符合安全要求的设备进行自动修复（如自动打补丁），“一键式”修复合格后，设备能够正常入网，安全性不合格设备则被强制隔离出网。

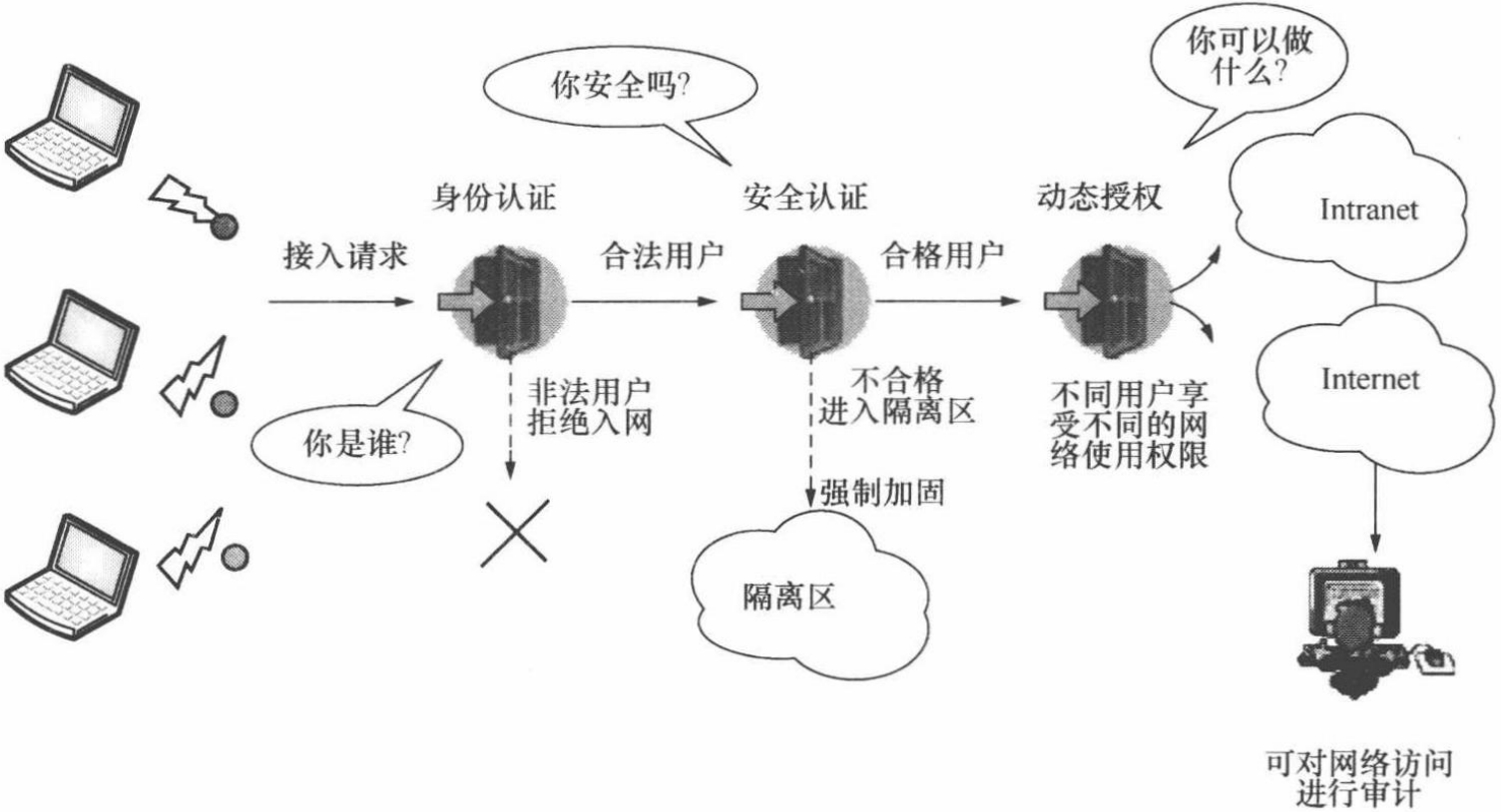
3. 入网设备行为管理

对于一个健康运行的网络来说，IP 资源、网络带宽资源都是需要严格管理的，这也符合上市公司对于本单位内部资源配置的控制要求，对于内网某些用户私改 IP 行为利用本次准入平台将能够进行人性化的自动还原。

4. IT 资产管理

实现资产管理过程中资产领用、资产维修、资产变更、资产报废等各阶段的无缝衔接，有效地提高了资产维护、报表结算及时性和准确率，保证网络建设和网络维护中资产的高效运行。

总体来说，部署网络准入控制系统后，实现了有效的设备入网控制，使管理员能够及时了解新设备的入网情况，并依据身份认证和安全性进行相应的权限审核，有效地搭建了内网的整体安全防御平台，极大地提高了信息部门的人员工作效率，真正地保障了内部网络的接入安全，对企业的网络正常运行提供了有效的安全支撑。


你安全吗?
你可以做什么?
身份认证
安全认证
动态授权
接入请求
合法用户
合格用户
Intranet
Internet
你是谁?
非法用户
拒绝入网
不合格
进入隔离区
强制加固
不同用户享受不同的网络使用权限
隔离区
可对网络访问进行审计

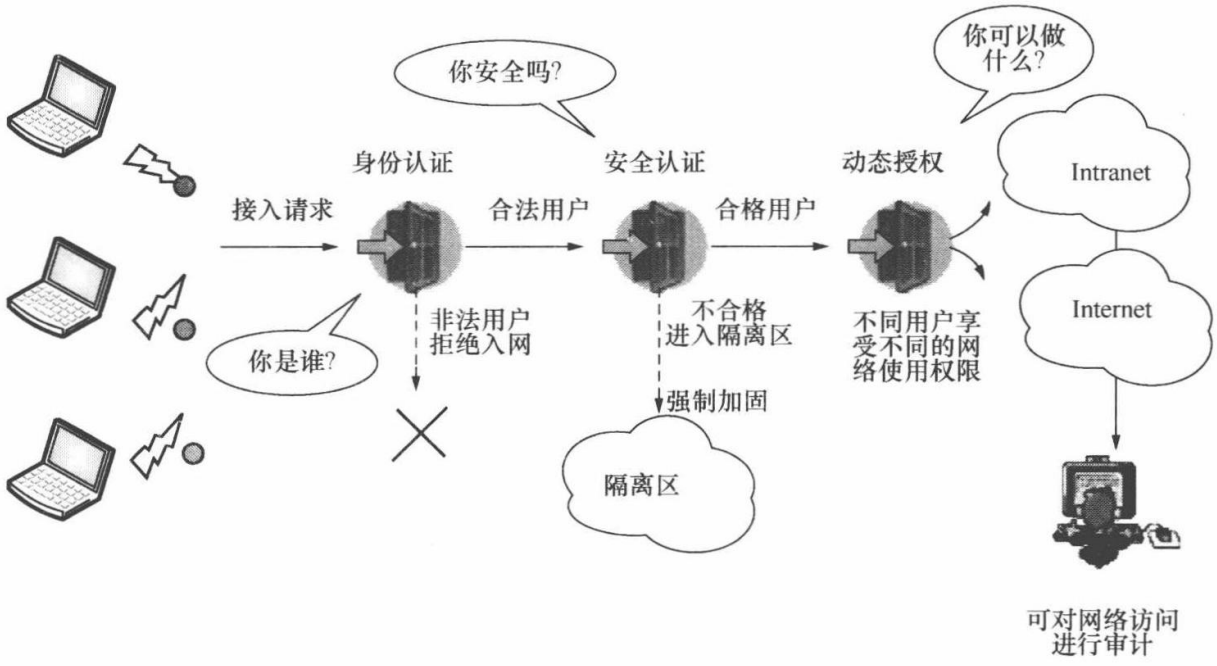


图 7-17 准入控制部署实施效果图

2. 入网设备安全规范检查

对于公司内部所有设备进行安全规范的检查，主要包括杀毒软件检查、补丁检查、弱口令检查等。对于不符合安全要求的设备进行自动修复（如自动打补丁），“一键式”修复合格后，设备能够正常入网，安全性不合格设备则被强制隔离出网。

3. 入网设备行为管理

对于一个健康运行的网络来说，IP 资源、网络带宽资源都是需要严格管理的，这也符合上市公司对于本单位内部资源配置的控制要求，对于内网某些用户私改 IP 行为利用本次准入平台将能够进行人性化的自动还原。

4. IT 资产管理

实现资产管理过程中资产领用、资产维修、资产变更、资产报废等各阶段的无缝衔接，有效地提高了资产维护、报表结算及时性和准确率，保证网络建设和网络维护中资产的高效运行。

总体来说，部署网络准入控制系统后，实现了有效的设备入网控制，使管理员能够及时了解新设备的入网情况，并依据身份认证和安全性进行相应的权限审核，有效地搭建了内网的整体安全防御平台，极大地提高了信息部门的人员工作效率，真正地保障了内部网络的接入安全，对企业的网络正常运行提供了有效的安全支撑。

附录 A　网络准入控制法令法规简析

信息安全技术经过这些年的不断发展，国际上出现了很多行业性的标准，我国现在对信息安全、网络安全也是越来越重视，不仅重点扶持国内安全厂商，有相应的采购规定优先考虑国内安全厂商，而且国家安全相关部门相继推出了关于信息安全的法令法规。早在 2010 年就已经由公安部联合国内外 5 家知名安全厂商制定了准入控制国标，其技术实现细则的初稿也早已提交，但由于国内准入技术发展的日新月异，加上无客户端化浪潮的不断演进，原有技术细则中过多偏向于 802.1x 技术实现的弊病也显露无疑。标准颁布后无法匹配现实甚至大大滞后于现实，这是标准制定方乃至厂商都不愿看到的结局，在这个背景下，标准的实际颁布日期确是扑朔迷离。下面重点分析现有的法令法规以及行业标准。

1.《信息安全等级保护管理办法》（公通字［2007］43 号）等法令

《信息安全等级保护管理办法》明确规定，从技术和管理两个方面入手共同完成信息系统的安全保护。与内网安全相关主要涵盖了终端接入控制、边界完整性检查、主机身份鉴别、内网访问控制、安全审计、资产管理、介质管理、监控管理、恶意代码防范和系统安全管理等方面。

网络准入控制系统解决入网身份认证、安全检测、安全修复、访问控制及行为审计等信息系统等级保护相关具体要求，满足等级保护要求精髓之一：接入可控。

2.《ISO27001 信息安全管理体系》

《ISO27001 信息安全管理体系》指出，信息安全是通过实现组合控制获得的，以防止信息受到的各种威胁，确保业务连续性，使业务受到损害的风险减至最小，使投资回报和业务机会最大。

安全控制可以是策略、惯例、规程、组织结构和软件功能。《ISO27001 信息安全管理体系》中明确指出接入网络的管理规范和设备要求规范。

3.《萨班斯 SOX 法案》IT 内控体系

萨班斯法案对公司治理、内部控制及外部审计同时做出了严格的要求。萨班斯法案覆盖了非常全面的管理层面，其中 404 条款（内部控制的管理评估）明确要求对企业内部的控制规范要求。

按萨班斯法案信息安全提出了 IT 内控要求涉及到四个方面：一是针对网络准入控制；二是针对补丁管理；三是针对配置管理；四是终端所遵从的一些检查。

A.1 国家等级保护方法中对 NAC 的要求

A.1.1 第一级的安全准入要求

1. 技术要求

1）网络安全

访问控制（G1）包括：

① 应在网络边界部署访问控制设备，启用访问控制功能。

注释：必须部署安全准入系统进行入网访问控制。

② 应根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包出入。

注释：需要对来源设备或访问设备的数据进行控制，在符合安全控制要求的情况下允许通过，否则拒绝入网。

③ 应通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度至少为用户组。

注释：至少对用户组实现对网络的访问控制力度。

2）主机安全

（1）访问控制（S1），包括：应及时删除多余的、过期的账户，避免共享账户的存在。

注释：能够及时发现系统中的 guest 账户并采取处理措施。

（2）入侵防范（G1），包括：操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并保持系统补丁及时得到更新。

注释：必须对入网终端的操作系统补丁进行及时有效的更新。

（3）恶意代码防范（G1），包括：应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

注释 1：主机应安装杀毒软件，对恶意代码进行有效的防范处理。

注释 2：杀毒软件必须保证版本的及时更新和病毒库的有效性。

2. 管理要求

1）安全管理制度

安全制度制定和发布（G1），包括：应指定或授权专门的人员负责安全管理制度的制定。

注释：必须保证安全管理制度的制定和有效落实。

2）安全管理机构

授权和审批（G1），包括：应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行

审批。

注释：在网络系统接入及对重要资源进行访问时必须进行相应的审核。

3）人员安全管理

人员离岗（G1），包括：应立即终止由于各种原因离岗员工的所有访问权限。

注释：员工的访问必须进行有效的时间控制，离岗员工必须在访问权限上进行时间终止。

4）系统运维管理

（1）系统安全管理（G1），包括：

① 应根据业务需求和系统安全分析确定系统的访问控制策略。

注释：根据自身需要进行安全规范的可配置化管理。

② 应定期进行漏洞扫描，对发现的系统安全漏洞进行及时的修补。

注释：周期性地进行漏洞扫描或对漏洞风险持续跟踪，对必要漏洞开展修补工作。

③ 应安装系统的最新补丁程序，并在安装系统补丁前对现有的重要文件进行备份。

注释：确保系统补丁更新及时。

（2）恶意代码防范管理（G1），包括：应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。

注释 1：主机应安装杀毒软件，从而对恶意代码进行有效的防范处理。

注释 2：杀毒软件必须保证版本的及时更新和病毒库的有效性。

（3）安全事件处置（G1），包括：应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点。

注释：形成网络安全评估的有效报告，从而及时发现网络中的安全弱点、隐患和安全趋势。

A.1.2　第二级的安全准入要求

1. 技术要求

1）网络安全

（1）访问控制（G2），包括：

① 应在网络边界部署访问控制设备，启用访问控制功能。

注释：必须部署安全准入系统进行入网访问控制。

② 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为网段级。

注释：网络边界访问控制设备应设定访问规则集，其中应涵盖对出入边界的数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝。

③ 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

注释：每个网络接入用户都有对应的访问安全域。

④ 应限制具有拨号访问权限的用户数量。

注释：对拨号接入互联网后进入内网访问的用户进行严格的数量控制和访问控制。

（2）边界完整性检查（S2），包括：应能够对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。

注释：严格控制内网外联行为，包括使用电话拨号、ADSL 拨号、无线上网卡、代理等外部网络连接方式。

2）主机安全

（1）身份鉴别（S2），包括：操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

注释：必须对入网设备的操作系统用户的口令复杂度进行统一设定，并规定密码更换时间。

（2）访问控制（S2），包括：应及时删除多余的、过期的账户，避免共享账户的存在。

注释：能够及时发现系统中的 guest 账户并采取处理措施。

（3）入侵防范（G2），包括：操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

注释：必须确保网络中有补丁升级服务器，并对入网终端的操作系统补丁进行及时有效的更新。

（4）恶意代码防范（G2），包括：

① 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

注释 1：主机应安装杀毒软件，对恶意代码进行有效的防范处理。

注释 2：杀毒软件必须保证版本的及时更新和病毒库的有效性。

② 应支持防恶意代码软件的统一管理。

注释：统一检测系统的杀毒软件安装和运行情况，并及时提供有效的修复措施。

2. 管理要求

1）安全管理制度

（1）管理制度（G2），包括：

① 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体

目标、范围、原则和安全框架等。

注释：必须制定与信息安全相关的网络管理规范制度。

② 应对安全管理活动中重要的管理内容建立安全管理制度。

注释：网络管理规范制度的制定必须结合等级保护评级的相关重要内容。

（2）评审和修订（G2），包括：应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。

注释：及时根据网络的安全评估结果对网络管理规范制度进行修订和配置。

2）安全管理机构

（1）授权和审批（G2），包括：应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批。

注释：在网络接入及对重要资源进行访问时必须进行相应的审核。

（2）审核和检查（G2），包括：安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

注释：明确系统的安全检查周期，定期对全网进行安全性评估。

3）人员安全管理

（1）人员离岗（G2），包括：应规范人员离岗过程，及时终止离岗员工的所有访问权限。

注释：员工的访问必须进行有效的时间控制，离岗员工必须在访问权限上进行时间终止。

（2）外部人员访问管理（G2），包括：应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。

注释：外来人员的访问可控，必须经过审核和适当的权限分配。

4）系统运维管理

（1）系统安全管理（G2），包括：

① 应根据业务需求和系统安全分析确定系统的访问控制策略。

注释：根据自身需要进行安全规范的可配置化管理。

② 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。

注释：周期性地进行漏洞扫描或对漏洞风险持续跟踪，对必要漏洞开展修补工作。

③ 应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。

注释：确保系统更新的补丁安全、有效，经过严格测试环境的测试，并进行了分级归类处理。

（2）恶意代码防范管理（G2），包括：

① 应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计

算机或存储设备接入网络系统之前也应进行病毒检查。

注释 1：主机应安装杀毒软件，从而对恶意代码进行有效的防范处理。

注释 2：杀毒软件必须保证版本的及时更新和病毒库的有效性，对杀毒软件的升级进行及时的检测和告知，并提供有效的修复方式。

② 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。

注释：周期性进行杀毒软件的使用情况检查审计记录，并形成报表和总结汇报。

（3）安全事件处置（G2），包括：应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点。

注释：形成网络安全评估的有效报告，从而及时发现网络中的安全弱点、隐患和安全趋势。

A.1.3 第三级的安全准入要求

1. 技术要求

1）网络安全

（1）访问控制（G3），包括：

① 应在网络边界部署访问控制设备，启用访问控制功能。

注释：必须部署安全准入系统进行入网访问控制。

② 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力。

注释：网络边界访问控制设备应设定访问规则集，其中应涵盖对出入边界的数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝。

③ 重要网段应采取技术手段防止地址欺骗。

注释 1：禁用重要网段内终端设备的闲置端口。

注释 2：重要网段必须采用 IP-Mac 地址绑定等方式防止地址欺骗。

④ 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

注释：每个网络接入用户都有对应的访问安全域。

⑤ 应限制具有拨号访问权限的用户数量。

注释：对拨号接入互联网后进入内网访问的用户，进行严格的数量控制和访问控制。

（2）边界完整性检查（S3），包括：

① 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

注释 1：必须对非授权设备的私自接入进行检测。

注释 2：能够自动定位入网设备并进行有效的阻断。

注释 3：监控非授权连接，一旦发现，产生报警记录。

② 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

注释 1：严格控制内网外联行为，包括使用电话拨号、ADSL 拨号、无线上网卡、代理等外部网络连接方式。

注释 2：能够对非法外联行为进行定位和上报，同时进行有效地阻断。

(3) 恶意代码防范 (G3)，包括：

① 应在网络边界处对恶意代码进行检测和清除。

注释：确保网络边界的清晰，并在接入终端处就有效实施防病毒系统。

② 应维护恶意代码库的升级和检测系统的更新。

注释：及时有效维护防病毒系统的版本升级和病毒库更新。

2) 主机安全

(1) 身份鉴别 (S3)，包括：操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度，要求并定期更换。

注释：必须对入网设备的操作系统用户的口令复杂度进行统一设定，并规定密码更换时间。

(2) 访问控制 (S3)，包括：应及时删除多余的、过期的账户，避免共享账户的存在。

注释：能够及时发现系统中的 guest 账户并采取处理措施。

(3) 入侵防范 (G3)，包括：操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

注释：必须确保网络中有补丁升级服务器，并对入网终端的操作系统补丁进行及时、有效的更新。

(4) 恶意代码防范 (G3)，包括：

① 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

注释 1：主机应安装杀毒软件，对恶意代码进行有效的防范处理。

注释 2：杀毒软件必须保证版本的及时更新和病毒库的有效性。

② 应支持防恶意代码的统一管理。

注释：统一检测系统的杀毒软件安装和运行情况，并及时提供有效的修复措施。

2. 管理要求

1) 安全管理制度

管理制度 (G3)，包括：

① 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。

注释：必须制定与信息安全相关的网络管理规范制度。

② 应对安全管理活动中的各类管理内容建立安全管理制度。

注释： 网络管理规范制度的制定必须结合等级保护评级的相关重要内容。

③ 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

注释： 网络管理规范制度必须涵盖有效的技术实现（安全策略）、规范文档（管理制度）和审计汇报（操作规程）。

2）安全管理机构

（1）授权和审批（G3），包括：应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。

注释： 在物理访问、网络接入及对重要资源进行访问时必须进行相应的审核。

（2）审核和检查（G3），包括：

① 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

注释： 必须定期进行系统的安全性检查。

② 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

注释： 安全检查结果必须形成报表和汇总文档，上报为安全检查报告。

3）人员安全管理

（1）人员离岗（G3），包括：应严格规范人员离岗过程，及时终止离岗员工的所有访问权限。

注释： 员工的访问必须进行有效的时间控制，离岗员工必须在访问权限上进行时间终止。

（2）外部人员访问管理（G3），包括：

① 应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案。

注释： 外来人员的访问可控，必须经过申请、审核和适当的权限分配，并与内部人员进行关联方便监督。

② 对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。

注释： 外来人员的访问必须定义相应的访问安全域和安全控制策略。

4）系统建设管理

系统定级（G3），包括：应明确信息系统的边界和安全保护等级。

注释： 对信息系统进行明晰的边界控制。

5）系统运维管理

（1）监控管理和安全管理中心（G3），包括：

① 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

注释：利用安全检测和报警记录的数据进行及时的安全趋势分析和评审。

② 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

注释：配备专用的安全管理中心或平台，综合管理和审计设备安全状态、防病毒软件情况、补丁情况和各类安全审计事件，形成相应的安全报告。

（2）网络安全管理（G3），包括：

① 应保证所有与外部系统的连接均得到授权和批准。

注释：必须严格控制外联行为。

② 应禁止便携式和移动式设备接入网络。

注释：对网络中的认证用户和固定设备进行一对一绑定，外来移动设备拒绝认证入网。

③ 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

注释：严格控制内网外联行为，包括使用电话拨号、ADSL 拨号、无线上网卡、代理等外部网络连接方式。

（3）系统安全管理（G3），包括：

① 应根据业务需求和系统安全分析确定系统的访问控制策略。

注释：根据自身需要进行安全规范的可配置化管理。

② 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。

注释：周期性地进行漏洞扫描或对漏洞风险持续跟踪，对必要漏洞开展修补工作。

（4）恶意代码防范管理（G3），包括：

① 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。

注释 1：主机应安装杀毒软件，从而对恶意代码进行有效的防范处理。

注释 2：杀毒软件必须保证版本的及时更新和病毒库的有效性，对杀毒软件的升级进行及时的检测和告知，并提供有效的修复方式。

② 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。

注释：周期性进行杀毒软件的使用情况检查审计记录，并形成报表和总结汇报。

A.1.4 第四级的安全准入要求

1. 技术要求

1）网络安全

（1）访问控制（G4），包括：

① 应在网络边界部署访问控制设备，启用访问控制功能。

注释：必须部署安全准入系统进行入网访问控制。

② 应不开放远程拨号访问功能。

注释：对远程拨号的接入进行禁止和阻断。

（2）边界完整性检查（S4），包括：

① 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

注释 1：必须对非授权设备的私自接入进行检测。

注释 2：能够自动定位入网设备并进行有效的阻断。

注释 3：监控非授权连接，一旦发现，产生报警记录。

② 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

注释：包括使用电话拨号、ADSL 拨号、手机、无线上网卡等无线拨号方式及其他外部网络连接方式。

（3）恶意代码防范（G4），包括：

① 应在网络边界处对恶意代码进行检测和清除。

注释：确保网络边界的清晰，并在接入终端处有效实施防病毒系统。

② 应维护恶意代码库的升级和检测系统的更新。

注释：及时有效维护防病毒系统的版本升级和病毒库更新。

2）主机安全

（1）身份鉴别（S4），包括：操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

注释：必须对入网设备的操作系统用户的口令复杂度进行统一设定，并规定密码更换时间。

（2）访问控制（S4），包括：应及时删除多余的、过期的账户，避免共享账户的存在。

注释：能够及时发现系统中的 guest 账户并采取处理措施。

（3）入侵防范（G4），包括：操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

注释：必须确保网络中有补丁升级服务器，并对入网终端的操作系统补丁进行及时有效的更新。

（4）恶意代码防范（G4），包括：

① 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

注释 1：主机应安装杀毒软件，对恶意代码进行有效的防范处理。

注释 2：杀毒软件必须保证版本及时更新和病毒库的有效性。

② 应支持防恶意代码的统一管理。

注释：统一检测系统的杀毒软件安装和运行情况，并及时提供有效的修复措施。

2. 管理要求

1）安全管理制度

管理制度（G4），包括：

① 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。

注释：必须制定与信息安全相关的网络管理规范制度。

② 应对安全管理活动中的各类管理内容建立安全管理制度。

注释：网络管理规范制度的制定必须结合等级保护评级的相关重要内容。

③ 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

注释：网络管理规范制度必须涵盖有效的技术实现（安全策略）、规范文档（管理制度）和审计汇报（操作规程）。

2）安全管理机构

（1）授权和审批（G4），包括：应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。

注释：在物理访问、网络接入及对重要资源进行访问时必须进行相应的审核。

（2）审核和检查（G4），包括：

① 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

注释：必须定期进行系统的安全性检查。

② 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

注释：安全检查结果必须形成报表和汇总文档，上报为安全检查报告。

3）人员安全管理

（1）人员离岗（G4），包括：应制定有关管理规范，严格规范人员离岗过程，及时终止离岗员工的所有访问权限。

注释：员工的访问必须进行有效的时间控制，离岗员工必须在访问权限上进行时间终止。

（2）外部人员访问管理（G4），包括：

① 应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案。

注释：外来人员的访问可控，必须经过申请、审核和适当的权限分配，并与内部人员进行关联方便监督。

② 对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。

注释：外来人员的访问必须定义相应的访问安全域和安全控制策略。

③ 对关键区域不允许外部人员访问。

注释：外来人员的访问相关安全域不得包括系统的关键区域。

4）系统建设管理

系统定级（G4），包括：应明确信息系统的边界和安全保护等级。

注释：对信息系统进行明晰的边界控制。

5）系统运维管理

（1）监控管理和安全管理中心（G4），包括：

① 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

注释：利用安全检测和报警记录的数据进行及时的安全趋势分析和评审。

② 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

注释：配备专用的安全管理中心或平台，综合管理和审计设备安全状态、防病毒软件情况、补丁情况和各类安全审计事件，形成相应的安全报告。

（2）网络安全管理（G4），包括：

① 应保证所有与外部系统的连接均得到授权和批准。

注释：必须严格控制外联行为。

② 应禁止便携式和移动式设备接入网络。

注释：对网络中的认证用户和固定设备进行一对一绑定，外来移动设备拒绝认证入网。

③ 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

注释：严格控制内网外联行为，包括使用电话拨号、ADSL 拨号、无线上网卡、代理等外部网络连接方式。

（3）系统安全管理（G4），包括：

① 应根据业务需求和系统安全分析确定系统的访问控制策略。

注释：根据自身需要进行安全规范的可配置化管理。

② 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。

注释：周期性地进行漏洞扫描或对漏洞风险持续跟踪，对必要漏洞开展修补工作。

（4）恶意代码防范管理（G4），包括：

① 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。

注释 1：主机应安装杀毒软件，从而对恶意代码进行有效的防范处理。

注释 2：杀毒软件必须保证版本的及时更新和病毒库的有效性，对杀毒软件的升级进行及时的检测和告知，并提供有效的修复方式。

② 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。

注释：周期性进行杀毒软件的使用情况检查审计记录，并形成报表和总结汇报。

A.2　《ISO27001 信息安全管理体系》对 NAC 的要求

《ISO27001 信息安全管理体系》（以下简我 IS027001）指出，信息安全是通过实现组合控制获得的，以防止信息受到的各种威胁，确保业务连续性，使业务受到损害的风险减至最小，使投资回报和业务机会最大。

安全控制可以是策略、惯例、规程、组织结构和软件功能。ISO27001 中明确指出接入网络的管理规范和设备要求规范。

经过数月的讨论，ISO 组织正式批准了 ISE/IEC 27035：2011 标准，公众通过此条标准将能够获知对安全事件进行有效通告的信息安全最佳实践流程。

ISO27000 体系是众所周知的信息安全国际标准，用户可以依据 ISO27000 体系中的各项条款组织建设自身的信息安全管理体系（ISMS，Information Security Management System），ISO27000 体系中的 ISO27001 作为该体系的第一款标准发布于 2005 年，故全称为 ISO27001：2005，其最初制定的目的是为了给网络的信息安全体系设立建设规范。如今整个的 ISO27000 体系已经发展到了第 7 个年头，而其家族也发展到了第 35 位成员。

与 ISO27000 体系前从宏观角度给出整体化安全体系建设规范不同的是，ISE/IEC27035 标准更侧重于对安全事件的处理和响应办法，依据商业标准组织的建议，各种机构如果能够采纳 ISE/IEC27035：2011 中对于安全事件进行管理的方法和规范，那么它将帮助用户减少 IT 类安全威胁所带来的各种影响。ISO 声称，安全漏洞会使得企业的运营体系受损，会中断机构的业务运行，另外，ISO 还强调，在采用适时的、有效的方式进行准备和响应的情况下，一次灾难性的事故也能够被转换成一个较小的事件，从而减少损失。

这些正是信息安全事件管理系统所涵盖的内容，其使得各机构能够适时地对事件进行控制和流程化的处理，从而对广泛的各种安全事件和漏洞进行有效管理。ISO/IEC 27035：2011 沿袭了之前的条款，给出了指导管理者对信息安全事

件及漏洞进行检测、上报和评估的各种方法。

ISO 注意到，这个标准将帮助企业迅速对信息安全事件进行响应，如对入侵事件立即进行适当的控制，并减少损失及迅速进行系统恢复，通过这些处理流程，管理者能够熟悉并增强他们的总体安全方案。

Edward Humphreys 带领的团队负责了 ISO/IEC TR 18044：2004 标准的原始版本制定，他也表示，对重大安全事件是否能进行有效和迅速的处理将导致两种截然不同的结局，要么成功地从灾难中恢复，要么陷入系统瘫痪的泥沼。

“新的 ISO/IEC 27035 标准提供了经过实践与测试验证的有关流程与方法的建议，管理者可以部署到自身网络中以确保对信息安全事件进行有效的管理”，Edward Humphreys 解释说。“小事件一般只影响单个的业务系统，与此不同的是，重大事件往往会导致全部业务瘫痪”，“部分安全事件会导致机构及业务资源的使用中断 24～72 小时，甚至更长时间；部分安全事件会造成数据泄露或损坏，还有一部分甚至会使机构面临牢狱之灾。ISO/IEC 27035：2011 为这些都提供了全面的解决方案。” Edward Humphreys 最后说道。

我们注意到，在替换了老的 ISO/IEC TR 18044：2004 技术报告标准后，新颁布的 ISO/IEC 27035：2011 标准支持在 ISO/IEC 27001：2005 中所规定的常规概念，保持了继承性。新标准适用于任何机构，任何规模的用户。它覆盖了一系列的信息安全事件，适用于蓄意、偶然、技术性、物理上的各种攻击。

新颁布的 ISO27035：2011 标准在国内得到广泛应用还需要一定的时间，但依据标准所透露出来的基本处理方式对广大的管理者是一个很好的借鉴。其首要的思想就是对信息安全事件进行分层次处理，因为所有的入侵、攻击、泄露事故均发起于某一点，而最终影响到整个网络层面，或造成整体管理制度上的极坏影响。

对于信息安全的管理者而言，在没有形成应对安全事件的标准规范之前，学会如何将风险控制在源头是十分重要的一环，而网络风险的基本源头就在接入的边界。传统意义的边界指的是外网，也就是防火墙通常放置的位置之外，而如今网络边界的定义则得到了极大的拓展，因为内网的边界往往比外网边界更为宽泛，各类设备，包括 PCs（Windows、Linux、solaris，Etc）、laptops、PDA、smartphone（iPhone/iPad，Blackberry，Android，Windows Mobile and Nokia Symbian）、IP-enabled facilities（such as vending machines，laundry machines，IP surveillance cameras，and others）都会通过各种方式从内网边界进入管理者的辖区。因此，控制好纷繁的内网接入源将是形成规范化管理的第一步，也是最重要的一步。在这一方面，NAC（网络准入控制）为我们做出了很好的榜样，坐落在天堂杭州的准入控制行业领导者盈高科技在 2011 年底提出了基于其准入产品 ASM 的一体化安全事件防范体系，这也将对接入边界的控制提高到了整体网络解决方案的高度。

A.3　《萨班斯 SOX 法案》IT 内控体系摘要

SOX 法案背景

针对安然、世通等财务欺诈事件，美国国会出台了《2002 年公众公司会计改革和投资者保护法案》（Sarbanes-Oxley Act）。该法案由美国众议院金融服务委员会主席奥克斯利和参议院银行委员会主席萨班斯联合提出，有被称作《2002 年萨班斯——奥克斯利法案》（简称萨班斯或 SOX 法案）。该法案的法律效力适用于在美国证券交易委员会注册的公司，在美国上市的中国公司也受它约束。SOX 法案对上市公司管理层提出了非常苛刻的要求，直接相关的条款包括：302 条款（公司对财务报告的责任）、404 条款（管理层对内部控制的评价）、906 条款（强化白领刑事责任）。

IT 在 SOX 遵从的角色

SOX 法案强调了要设计和执行有效公司内部控制来保证财务报告职能的行之有效，随着越来越多公司对于信息技术依赖性的提高，IT 控制在公司内部控制体系中的重要性也日益增加，主要体现如下方面：a. 公司业务流程的部分甚至全部由 IT 系统驱动和承载；b. 公司内部控制目标的实现通常取决于以 IT 为基础的控制；c. 许多控制需要依赖 IT 系统生成的数据。

IT 通过应用控制和一般控制来帮助控制财务报告的相关风险，以达到控制目标。其中：IT 应用控制（IT Application Control）嵌在各个应用系统中，控制业务流程和交易处理，直接对财务报告产生影响；IT 一般控制（IT General Control，也译作通用计算机控制）是分布在 IT 流程中的控制活动，用来保障 IT 整体运维环境的可靠，并支持应用控制的有效运作。

美国公众公司会计监管委员会（PCAOB）特别举例强调，IT 控制对于公司总体控制目标的实现具有广泛和深远的影响。所以，建立维护合理的 IT 控制体系、并保证其有效执行是 SOX 法案遵从的重要组成部分。

IT 遵从的常用框架和方法

如何建立和维护一套有效的 IT 内控体系，并能得到外部审计师的认同，较为有效的方法是采用业界通行的框架。COSO 是目前唯一被 PCAOB 明文确认可接受的内控框架，该框架确定了 3 项内部控制目标，将分布于公司各个层面的内控分解为控制环境、风险评估、控制活动、信息和沟通、监督 5 个组成要素。

熟悉 COSO 的人士都知道，COSO 框架并没有具体描述 IT 风险与控制目标，相对来说 Cobitreg；（Control Objectives for Information and related Technology）更有针对性。Cobit 框架由 IT Governance Institute 发布，2007 年新版本是 Cobit4.1，它定义了 IT 控制的 7 项信息标准（有效性、经济性、机密性、完整性、可用性、合规性、可靠性）、4 大领域（计划组织、开发获取、交付支持、监控评价）和 34 过程。

比较可贵的是，ITGI 在 2004 年及时研究发布了《SOX 法案遵从 IT 控制目标》（英文全称为 IT Control Objcctives for Sarbanes-Oxley：The Role of IT in the Design and Implementation os Internal Control OVER Financial Reporting），其为 SOX 遵从的风险识别与控制过程指明了方向。2006 年 9 月 ITGI 发布了该项目工作的第二版，更加收到了业界欢迎。

IT 控制目标明确后，需求具体落实在 IT 组织、人员、技术和流程中。这个落实过程可以参考 IT 服务管理标准（新的 ITSM 国际标准为 ISO20000），建议重点借鉴 IT 基础设施库（ITIL）的变更管理、问题管理、事件管理、配置管理等服务支持流程。在信息安全管理方面，ISO17799 是一个可参照的国际标准。

从上面的几点分析，萨班斯法案对公司治理、内部控制及外部审计同时做出了严格的要求。萨班斯法案覆盖了非常全面的管理层面，其中 404 条款（内部控制的管理评估）明确要求对企业内部的控制规范要求。

按萨班斯法案信息安全提出了 IT 内控要求涉及到下面四个方面：一是针对网络准入控制；二是针对补丁管理；三是针对配置管理；四是终端所遵从的一些检查。

附录 B　PDCA 安全模型

PDCA 安全模型是指基于策略（policy）、保护（protection）、检测（detection）和响应（response）的 P2DR 安全模型，在 P2DR 安全模型的基础上，提出了针对各种系统普适的信息安全建设的原则；在对系统进行威胁分析和网络分区防护的基础上，对信息安全体系建设提出了详细的建设方案，其中，颇多内容值得在网络准入控制系统建设中借鉴。

B.1　P2DR 模型简介

P2DR 模型是美国国际互联网安全系统公司（ISS）提出的动态网络安全体系的代表模型，也是动态安全模型的雏形。美国 ISS 公司认为没有一种技术可完全消除网络中的安全漏洞。系统的安全实际上是理想中的安全策略和实际的执行之间的一个平衡，提出了一个可适应网络安全模型 ANSM（Adaptive Network Security Model）P2DR 安全模型，如图 B-1 所示。

该模型是在整体安全策略的控制和指导下，在综合运用防护工具的同时，利用检测工具了解和评估系统的安全状态，通过适当的反应将系统调整到相对最安全和风险最低的状态。P2DR 强调在监控、检测、响应、防护等环节的循环过程，通过这种循环达到保持安全水平的目的。P2DR 安全模型是整体的动态的安全模型，所以称为可适应安全模型。

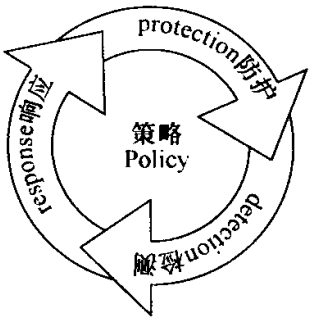


图 B-1　P2DR 安全模型

模型的基本描述为：

安全＝风险分析＋执行策略＋系统实施＋漏洞监测＋实时响应

B.2　P2DR 模型主要组成

P2DR 模型包括 4 个主要部分：策略、防护、检测和响应。下面分别介绍。

1. 策略

策略是模型的核心，所有的防护、检测和响应都是依据安全策略实施的。网络安全策略一般包括总体安全策略和具体安全策略两个部分组成。安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制订、评估、执行等。制订可行的安全策略取决于对网络信息系统的了解程度。

2. 防护

防护是根据系统可能出现的安全问题而采取的预防措施，这些措施通过传统的静态安全技术实现。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网（VPN）技术、防火墙、安全扫描和数据备份等。

所谓防护就是采用一切手段保护信息系统的保密性、完整性、可用性、可控性和不可否认性。应该依据不同等级的系统安全要求来完善系统的安全功能、安全机制，通常采用传统的静态安全技术及方法来实现，主要有防火墙、加密、认证等方法。保护主要在边界提高抵御能力。界定网络信息系统的边界通常是困难的，一方面，系统是随着业务的发展不断扩张或变化的；另一方面，要保护无处不在的网络基础设施成本很高。边界防卫通常将安全边界设在需要保护的信息周边，例如存储和处理信息的计算机系统的外围，重点阻止诸如冒名顶替、线路窃听等试图“越界”的行为，相关的技术包括数据加密、数据完整性、数字签名、主体认证、访问控制和公证仲裁等，这些技术都与密码技术密切相关。

边界保护技术可分为物理实体的保护技术和信息保护（防泄露、防破坏）技术。

（1）物理实体的保护技术。这类技术主要是对有形的信息载体实施保护，使之不被窃取、复制或丢失，如磁盘信息消除技术，室内防盗报警技术，密码锁、指纹锁、眼底锁等。信息载体的传输、使用、保管、销毁等各个环节都可应用这类技术。

（2）信息保护技术。这类技术主要是对信息的处理过程和传输过程实施保护，使之不被非法入侵、外传、窃听、干扰、破坏、拷贝。对信息处理的保护主要有两种技术：一种是计算机软、硬件的加密和保护技术，如计算机口令字验证、数据库存取控制技术、审计跟踪技术、密码技术、防病毒技术等；另一种是计算机网络保密技术，主要指用于防止内部网秘密信息非法外传的保密网关、安全路由器、防火墙等。对信息传输的保护也有两种技术：一种是对信息传输信道采取措施，如专网通信技术、跳频通信技术（扩展频谱通信技术）、光纤通信技术、辐射屏蔽和干扰技术等，以增加窃听的难度；另一种是对传递的信息使用密码技术进行加密，使窃听者即使截获信息也无法知悉其真实内容。常用的加密设备有电话保密机、传真保密机、IP 密码机、线路密码机、电子邮件密码系统等。

3. 检测

检测是动态响应和加强防护的依据，是强制落实安全策略的工具，当攻击者穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。通过不断地检测和监控网络及系统来发现新的威胁和弱点，通过循环反馈来及时作出有效的响应。网络的安全风险是实时存在的，检测的对象主要针对系统自身的脆弱性及外部威胁，利用检测工具了解和评估系统的安全状态。

检测包括：检查系统存在的脆弱性；在计算机系统运行过程中检查和测试信息是否发生泄漏、系统是否遭到入侵，并找出泄漏的原因和攻击的来源。如计算机网络入侵检测、信息传输检查、电子邮件监视、电磁泄漏辐射检测、屏蔽效果测试、磁介质消磁效果验证等。

入侵检测是发现渗透企图和入侵行为。在近年发生的网络攻击事件中，突破边界防卫系统的案例并不多见，攻击者的攻击行动主要是利用各种漏洞，人们可通过入侵检测尽早发现入侵行为，并予以防范。入侵检测基于入侵者的攻击行为与合法用户的正常行为有着明显的不同，实现对入侵行为的检测和告警，以及对入侵者的跟踪定位和行为取证。

4. 响应

响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。系统一旦检测到入侵，响应系统就开始工作，进行事件处理。在检测到安全漏洞之后必须及时做出正确的响应，从而把系统调整到安全状态，对于危及安全的事件、行为、过程，及时做出处理，杜绝危害进一步扩大，使系统力求提供正常的服务，例如关闭受到攻击的服务器。

B.3　P2DR 模型基本原理

P2DR 模型是在整体的安全策略的控制和指导下，在综合运用防护工具（如防火墙、操作系统身份认证、加密等）的同时，利用检测工具（如漏洞评估、入侵检测等）了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。

该理论的最基本原理就是认为，信息安全相关的所有活动，不管是攻击行为、防护行为、检测行为和响应行为等都要消耗时间。因此可以用时间来衡量一个体系的安全性和安全能力。

作为一个防护体系，当入侵者要发起攻击时，每一步都需要花费时间。当然攻击成功花费的时间就是安全体系提供的防护时间 Pt；在入侵发生的同时，检测系统也在发挥作用，检测到入侵行为也要花费时间—检测时间 Dt；在检测到入侵后，系统会做出应有的响应动作，这也要花费时间—响应时间 Rt。

P2DR 模型就可以用一些典型的数学公式来表达安全的要求。

公式 1

$$Pt > Dt + Rt$$

其中，Pt 代表系统为了保护安全目标设置各种保护后的防护时间；或者理解为在这样的保护方式下，黑客（入侵者）攻击安全目标所花费的时间。Dt 代表从入侵者开始发动入侵开始，系统能够检测到入侵行为所花费的时间。Rt 代

表从发现入侵行为开始，系统能够做出足够的响应，将系统调整到正常状态的时间。那么，针对于需要保护的安全目标，如果上述数学公式满足防护时间大于检测时间加上响应时间，也就是在入侵者危害安全目标之前就能被检测到并及时处理。

公式 2

$$Et = Dt + Rt \qquad (Pt = 0)$$

此公式的前提是假设防护时间为 0。Dt 代表从入侵者破坏了安全目标系统开始，系统能够检测到破坏行为所花费的时间。Rt 代表从发现遭到破坏开始，系统能够做出足够的响应，将系统调整到正常状态的时间。比如，对 Web Server 被破坏的页面进行恢复。那么，Dt 与 Rt 的和就是该安全目标系统的暴露时间 Et。针对于需要保护的安全目标，如果 Et 越小系统就越安全。

通过上面两个公式的描述，实际上给出了安全一个全新的定义："及时的检测和响应就是安全"，"及时的检测和恢复就是安全"。

而且，这样的定义为安全问题的解决给出了明确的方向：提高系统的防护时间 Pt，降低检测时间 Dt 和响应时间 Rt。

P2DR 模型也存在一个明显的弱点，就是忽略了内在的变化因素，如人员的流动、人员的素质和策略贯彻的不稳定性。实际上，安全问题牵涉面广，除了涉及到防护、检测和响应，系统本身安全的"免疫力"的增强、系统和整个网络的优化，以及人员这个在系统中最重要角色的素质的提升，都是此安全系统没有考虑到的问题。

B.4 安全规划原则

现有网络大多是以连通性作为中心进行设计的，而很少考虑安全性。例如最典型的网络三层架构模型（核心层、汇聚层、接入层架构）中，网络是向核心层集中的而并没有考虑同一层不同节点之间的安全隔离问题。因此，网络系统整网安全建设中，首先需要改变的就是将以连通性为中心的设计思路转变为以安全为中心的设计思路，并按照该设计思路的要求对网络进行重新设计。

所谓以安全为核心的设计思路就是要求在进行网络设计时，首先根据网络系统现有以及未来的网络应用和业务模式，将网络分为不同的安全区域，在不同的安全区域之间进行某种形式的安全隔离。

1. 防火墙隔离各安全区域

防火墙作为不同网络或网络安全域之间信息的出入口，能根据安全策略控制出入网络系统的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。在逻辑上，防火墙是一个分离器、限制器和分析器，可以有效地监控网络系统不同安全域之间的任何活动。防火墙在网络

间实现访问控制，网络系统可以称之为“被信任应受保护的网络”，其他非安全网络称为“某个不被信任并且不需要保护的网络”，比如 Internet 出口。防火墙就位于网络系统和一个不受信任的网络之间，通过一系列的安全手段来保护受网络系统信任的信息。

2. 对关键路径进行深入检测防护

虽然网络系统目前一切运行完好，但是，如果出现有害代码伪装成客户正常业务进行传播时，网络的带宽利用率就会居高不下，应用系统的响应速度会越来越慢，最后导致整个网络瘫痪。产生这个问题的原因并不是当初网络设计不周，而是入侵技术日益演变到应用层面（L7）的结果。一般防火墙等安全产品的软硬件设计当初仅按照其工作在 L2—L4 时的情况考虑，不具有对数据流进行综合、深度监测的能力，自然就无法有效识别伪装成正常业务的非法流量，结果蠕虫、攻击、间谍软件、点到点应用等非法流量可轻而易举地通过防火墙开放的端口进出网络。

因此，在网络系统的关键路径上部署独立的具有深度检测防御的 IPS 系统非常重要。深度检测防御是为了检测网络系统中违反安全策略的行为。一般认为违反安全策略的行为有以下两种。

① 入侵：非法用户的违规行为。

② 滥用：用户的违规行为。

深度检测防御识别出网络系统中任何不希望有的活动，从而限制这些活动，以保护网络系统的安全。深度检测防御的应用目的是在入侵攻击对网络系统发生危害前，检测到入侵攻击，并利用报警与防护系统驱逐入侵攻击。在入侵攻击过程中，能减少入侵攻击对网络系统所造成的损失。

3. 对终端进行安全访问控制

目前，网络系统还没有针对病毒、蠕虫的防御体系，当发现新的病毒或新的网络攻击时，一般是由网络管理员发布病毒告警或补丁升级公告，要求网络中的所有主机安装相关防御软件。从网络病毒泛滥、损失严重的结果来看，网络系统当前的防御方式并不能有效应对病毒和蠕虫的威胁，主要表现在以下 3 个方面。

① 被动防御：缺乏主动抵抗能力。

② 单点防御：对病毒的重复、交叉感染缺乏控制。

③ 分散管理：安全策略不统一，缺乏全局防御能力。

只有从网络系统内部用户的接入终端进行安全控制，才能够从源头上防御威胁，但是，分散管理的终端难以保证分散的主机安全状态符合网络系统的安全统一策略，无法有效地从网络接入点进行安全防范。在网络系统当前分散管理的安全体系中，新的补丁发布了却无人理会、新的病毒出现了却不及时升级病毒库的现象普遍存在，无法彻底解决病毒和操作系统漏洞带来的网络安全威胁，只有集

中管理、强制终端用户执行，才能够起到统一策略、全局防范的效果。

4. 全网部署防病毒系统

在所有计算机安全威胁中，计算机病毒是最为严重的，它往往发生的频率高、损失大、潜伏性强、覆盖面广。

由于 Internet 技术及信息技术的普及和发展，病毒的传播速度越来越快。Internet 的发展使得病毒没有国界，如 5 分钟以前在美国发现的病毒，有可能在 5 分钟之后就到了我国。依赖于 Internet，病毒可以通过邮件、HTTP、网络共享、系统漏洞等实时的方式感染到网络系统内部。另外，在网络系统内部的群件系统和办公自动化、工作流系统的使用（如 Notes、Exchange），使得病毒在网络系统内部的传播速度加快，各个员工在共享信息的同时，有可能共享病毒，同时，在群件环境中，部分机器的防病毒能力弱，会导致整个系统的防病毒能力弱，因此，全网部署防病毒系统就显得非常重要。部署一套具有方便、易用的防病毒系统，使计算机环境免受病毒和其他恶意代码的攻击。对系统进行主动保护，以免遭受可能来自 U 盘、网络下载、电子邮件附件、网络共享文件、CD-ROM、在线服务和其他更多途径的感染。同时提供免遭受移动代码，如恶意的 ActiveX 和 Java 小程序的攻击的保护，并对通用的压缩文件类型进行扫描，以便在病毒发作之前即可自动阻止其发作。通过寻找新病毒发作的典型活动来查询新的攻击。

5. 充分利用网络以及资源管理系统

在网络系统中，首先要确保网络设备的安全，保证非授权用户不能访问任意一台服务器、路由器、交换机或防火墙等网络设备，采用网络管理系统是一种有效的解决方法。通过网络管理系统提供的配置管理、性能管理、失效管理和安全管理功能，可以实现网络设备安全有效的配置，为整个网络系统提供安全运行的基石。

6. 根据实际需要部署其他安全系统

以上的安全系统部署基本可以涵盖网络系统的安全需求，但是很多特殊的应用也需要特别的应用保护系统。此外，管理员也需要一些其他的安全工具对网络安全运行进行审计、评估等操作。

参 考 文 献

陈劲. 2005. 访问控制技术的研究. 福建电脑，(3)：12-13.

陈利，周永彬，马建国，方三辉. 2009. 基于端口的网络访问控制应用模式. 计算机工程，35 (16)：90-92.

方三辉，陈利. 2010. 网络准入技术的发展与展望. 微计算机信息，26 (3)：80-82.

郭幽燕，杜晔，王杨，韩向非，孙毅，陈洁，蒋琳. 2010. 基于 ARP 协议的内网访问控制系统. 计算机工程与科学，32 (1)：21-24.

金亮. 2012. 构建世博园区可信网络的基石-准入控制. http://www.doc88.com/p-959596196350.html [2012-1-31].

鞠洪尧. 2009. 基于复合网关的网络互联策略实现. 宁波大学学报 (理工版)，22 (2)：212-216.

李俊杰，冯南梓. 2008. DHCP_接入控制技术分析及安全防范探讨. 广东通信技术，(2)：7-11.

李昕，左明. 2003. Web 认证及 802.1x 认证的比较. 现代计算机，(11)：52-54.

毛拥华. 2004. 802.1x 认证技术分析及其应用建议. 通信世界，(31)：41-42.

孙力芾，李生红. 2005. DHCP 及 Option82 安全机制的原理与实现. 信息技术，(8)：29-32.

唐晓雷，余镇危，刘知一，李罡. 2005. 准入控制研究综述. 计算机工程与应用，(5)：129-131.

王国芬，李建华. 2005. 用户接入控制在网络安全体系中的应用. 网络安全技术与应用，(3)：53-55.

王辉，赵志军. 2003. 基于 TCP/IP 网络探针实现技术. 计算机与现代化，(12)：30-31.

王莉莉，孟晓景. 2009. 基于网络访问控制的校园网安全管理. 计算机与信息技术，(11)：57-59.

杨铭，周矛欣，许秀文. 2010. 浅谈网络探针接入控制技术. 中国管理信息化，13 (15)：82-83.

叶忠文. 2004. 基于 802.1x 认证的校园网的优化. 广东技术师范学院学报，(6)：34-36.

于微伟，卢泽新，康东明，吴建国. 2011. 关于网络准入控制系统的分析与优化. 计算机工程与科学，33 (8)：39-44.

曾新潮. 2011. 网络安全准入控制技术的应用. 信息技术与标准化，(8)：50-54.

张德安. 2011. 浅谈 802.1x 协议的网络准入控制技术. 广东科技，(6)：43-45.

张莉，齐锦，吕鲁宁，柏新才. 2009. 网络准入控制技术与设计. 信息安全与通信保密，(9)：60-62.

赵卫栋. 2011. 云计算数据中心虚拟化综合安全网关. 计算机安全，(10)：88-89.

周超，周城，丁晨路. 2011. 计算机网络终端准入控制技术. 计算机系统应用，20 (1)：89-94.

周祥峰. 2010. 基于 802.1x 协议的网络准入控制技术在电力企业的推广应用. 现代计算机 (专业版)，(8)：101-105.

```
{
  "before_pdg2pic_conversion": {
    "filename": "MTMyMjU5NTIuemlw",
    "filename_decoded": "13225952.zip",
    "filesize": 16991658,
    "md5": "f4e1d146f79ce780f7714d94147476fa",
    "header_md5": "6a64cee9904802d3330c66ff121a2a81",
    "sha1": "83cc1e833ae5959b867829476aec99d6319885e6",
    "sha256": "207f0b6fe912bfb4491d3adeef7c2df6de52237c6936864a0b21566364674b41",
    "crc32": 3450450809,
    "zip_password": "",
    "uncompressed_size": 17731943,
    "pdg_dir_name":
"\u2550\u00b0\u252c\u03c4\u256b\u255d\u255a\u03b4\u2510\u256a\u2553\u255e\u2555\u253c\u252c\u2588_13225952",
    "pdg_main_pages_found": 225,
    "pdg_main_pages_max": 225,
    "total_pages": 232,
    "total_pixels": 10655744
  },
  "after_pdg2pic_conversion": {
    "filename": "MTMyMjU5NTIuemlw",
    "filename_decoded": "13225952.zip",
    "filesize": 59214816,
    "md5": "f6b411f54a3451bc42d948a953d450ac",
    "header_md5": "79baa443e3cd3cf963a47311a7c07350",
    "sha1": "f697e36f47fac5368a3ab984c8ce23f03d1da71c",
    "sha256": "732e5868ece7939a233972f4fa9c1e7a1445fe20a91de7a1913ac1bdcd120f01",
    "crc32": 1818149964,
    "zip_password": "",
    "uncompressed_size": 62323443,
    "pdg_dir_name": "",
    "pdg_main_pages_found": 225,
    "pdg_main_pages_max": 225,
    "total_pages": 232,
    "total_pixels": 1236985472
  },
  "pdf_generation_missing_pages": false
}
```