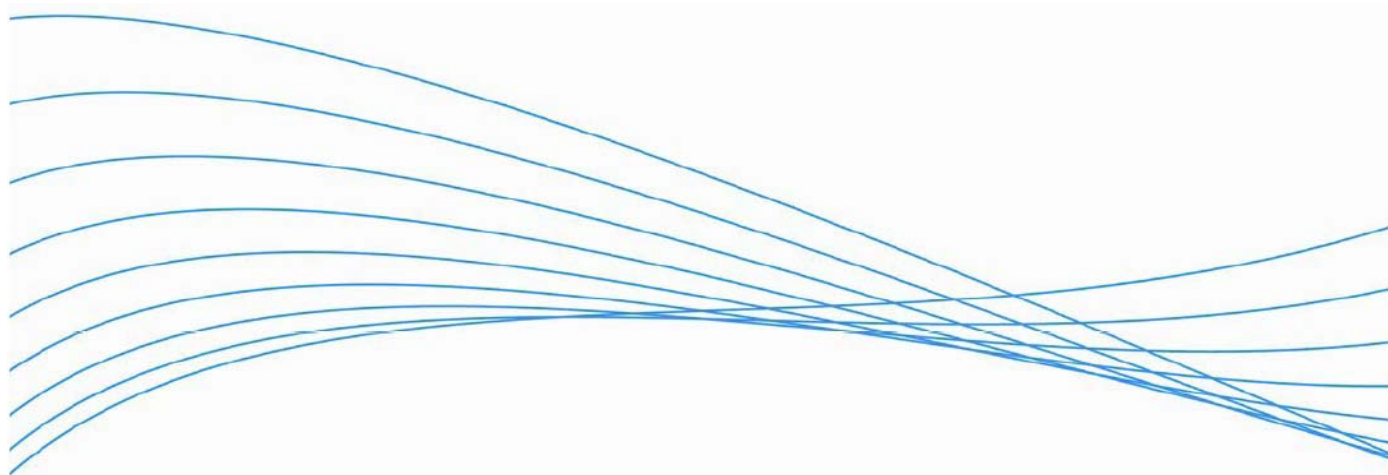


Identity Driven Management (身份驱动管理) 技术概要



简介.....	2
将网络从技术资源转变成业务资源	2
通过身份驱动管理 (IDM) 实现智能化的网络访问.....	3
ProCurve IDM 解决方案.....	3
ProCurve Identity Driven Manager 2.0.....	3
使用 IDM	4
IDM 如何工作.....	4
IDM 架构与实施	5
概要.....	6
更多信息	7

简介

网络基础设施架构正在从纯粹的技术资源发展演变而成为实用的业务资源，而与网络管理和访问控制相关的策略也是如此。

通常，网络管理的主要职责是发现设备，确保其正确配置，以及建立这些设备与网络上的服务之间的连接。因而，在很大程度上忽视了网络用户的独特需要和业务目标。

新的方法可将智能推向基础设施架构的边缘，实施身份驱动管理 (IDM)。ProCurve Networking by HP 领先实现了智能化边缘网络，能够为先进、易管理的动态适应性基础设施架构提供强大的 IDM 功能。

本文将讨论向 IDM 的转变，并重点介绍 ProCurve IDM 解决方案。另外，还描述了该解决方案如何与公司已有的安全和访问框架集成，以提高工作人员的生产率，增强网络安全性、管理和性能，更好地满足整体的业务需要。

将网络从技术资源转变成业务资源

从历史上看，企业网络一直是一项技术工具，而不是业务工具。这是由于长久以来公司将重点都放在用户设备与企业基础设施架构的连接以及防止网络停机上。跨多个域的静态、简单的连接也采用静态、简单的配置，而较为复杂的功能，如流量路由选择、安全性和性能等，则由核心路由交换机来负责。

在这种传统模式下，无论连接网络的用户是来宾还是 CIO，其网络的行为都是一样的。事实上，传统网络始终都无法区分身份不同的用户。

这种有限或毫无任何访问控制的网络管理策略不仅阻碍了工作人员生产率的提高，而且还产生了与网络安全性、管理和性能相关的一些问题。还未对流量进行验证就允许其进入网络，这会产生安全方面的隐患；新的边缘设备、应用和流量类型需要重新配置网络，管理非常烦琐；流量路由选择无效率时，通常会产生不必要的流量，从而影响核心路由器性能。

最重要的是，由于过于强调网络运行的连接和维护，因此在很大程度上忽略了用户在访问、应用、带宽和质量服务 (QoS) 等方面不同的需要。这样便会阻碍工作人员在生产率、信息安全性、网络弹性和总体业务效率方面的不断提高。

幸运的是，网络技术已经成熟，公司认识到了其基础设施架构可以更好地满足组织和用户的需要。这种认识催生了从面向设备和连接的网络向面向用户和业务的网络的转变。

为了实现这种转变，组织将会面临以下几大业务和信息技术 (IT) 挑战。

主要的业务挑战：

- 使得用户访问适当的网络资源，以实现一个业务目标
- 简化企业内部人员的网络权限管理
- 推动网络实时地适应不断变化的业务需要，并部署新型应用

主要的 IT 挑战：

- 使网络行为随用户“适当的”业务需要而改变
- 采用工业标准的方法来控制每一个用户的网络行为
- 建立单一浏览界面来配置和管理网络策略
- 简化和自动完成权限及策略的管理

通过身份驱动管理 (IDM) 实现智能化的网络访问

ProCurve 首创的一种新型网络管理和访问简化模式，是将智能从网络中心推到连接用户和实施策略的网络边缘。利用这一措施，企业可以通过 IDM 实施智能网络访问。

IDM 可通过在集中管理的数据库中定义的安全和管理策略，自动对网络边缘进行配置，帮助公司最充分地利用网络资源，提高生产率。IDM 解决方案使这一切成为可能，网络管理员可以制定网络访问策略，在用户连接网络时动态地应用安全性和性能设置。这些策略根据用户、设备、位置、时间和其它变量而制定，并应用到所有 ProCurve 适应性边缘设备上，包括有线和无线设备。最终结果是实现一个统一的管理基础架构和更加安全、移动的多服务网络。

IDM 是建立智能化网络的基础，该智能化网络能够防止未经授权的使用，在保证重要业务信息安全的同时，可为更富有效率的工作人员提供易适应、便于用户使用的体验。

ProCurve IDM 解决方案

在建立以独特、适当地方式满足每一位用户需要的业务驱动型网络方面，ProCurve 是一个旗舰方案。此类网络的基础是 ProCurve 适应性边缘架构™，它便于实现 ProCurve 中心命令 (ProCurve Manager Plus 和 IDM) 以及边缘控制 (智能化边缘设备和 IDM)。

实现网络边缘智能化后，安全性得到加强、流量优先级得以改善，因此用户就可以随时随地进行连接，畅游网络。借助中心命令功能，公司可以集中控制网络配置，更便于企业实施新的应用和支持新的网络服务。

更重要的是，中心命令、边缘控制使得网络可以动态适应业务和用户需要。

ProCurve Identity Driven Manager 2.0

ProCurve 建立在适应性边缘架构基础之上，现在可通过 ProCurve Identity Driven Manager (IDM) 2.0 提供突破性的 IDM 功能。

IDM 2.0 软件可以动态地管理网络设备来提供适当和优化的网络访问，从而在增强安全性的同时提高生产率和总体效率。可根据用户、设备、设备健康状态、位置和时间等因素自动将安全性、访问和性能等方面的配置应用于网络基础设施架构设备中。IDM 2.0 可与 RADIUS 验证服务器一同管理有线和无线连接，同时实现与现有企业目录中用户和组成员的同步。

IDM 2.0 可通过自动配置智能化的边缘设备实现中心命令，为每个人或组提供独特的服务。它还可通过确保交换机和接入点特性能够在网络周边做出正确的决策和实施策略来提供边缘控制。这使得用户可以轻松管理和促进：

- 访问控制 — 基于用户的业务需要。
- 访问权限 — 不仅基于个人及其组群关系，还要基于其正使用的设备（如，PC、膝上型电脑、PDA 或 VoIP 电话）、日期、时间和位置。
- 策略实施 — 按用户、会话进行实施。IDM 2.0 是 ProCurve Manager Plus 的附加模块，而 ProCurve Manager Plus 是一个完整的并基于 Windows 的网络管理解决方案，适用于使用 ProCurve 产品的公司。ProCurve Manager Plus 允许用户能够发现、配置、监视 ProCurve 设备并进行故障排除，提供配置管理、VLAN 管理、深入的流量监视、组和策略管理、以及自动软件更新等高级特性。

使用 IDM

IDM 2.0 使网络边缘能够适应每一个用户的独特需求。无论用户是来宾、员工还是特殊的高优先级人员，他/她都会得到始终如一却又十分独特的网络体验。无论何时何地访问网络，或者使用何种设备，网络都会根据每一个用户特定的访问权限提供相应的服务。

图 1 显示了典型的 IDM 用户体验。网络管理员建立了适当的用户、组和访问规则之后，网络就能够动态、自动地针对每个用户、每个会话进行配置。

从会议室登陆的“来宾”只能访问互联网，速度限制为 2Mbps。登陆的“员工”在访问互联网的同时，还可以访问企业服务器。另外，如果用户具有较高的优先级，则会用适当的优先位标记他们的流量。

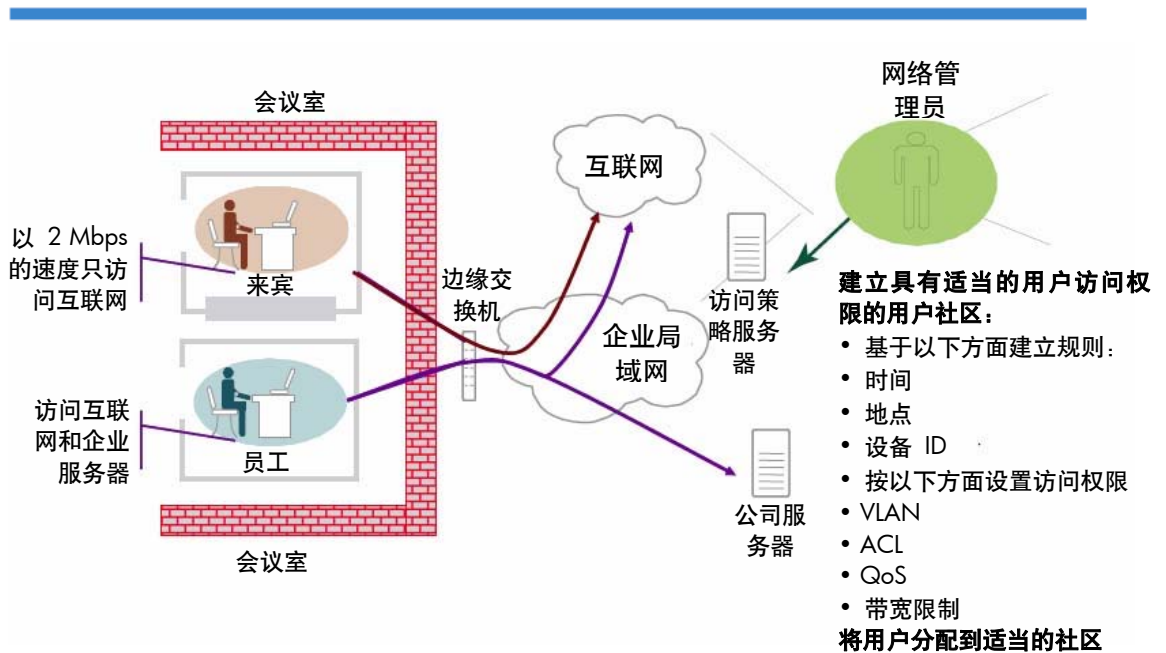


图 1. IDM 用户体验

IDM 如何工作

IDM 2.0 在所谓的“区域”内工作，有时候也称为“域”。域一般是指比较大的组织单位，每一个用户都属于（并且只属于）一个域。而且，很多公司只使用一个域。

ProCurve IDM 解决方案的基本配置模型分为两个步骤以至创建基于用户和组的特征每一个用户都属于一个组（称为访问策略组）。每一个访问策略组都定义一个访问策略，在其用户进入网络时管理应用于该用户的访问权限。

访问策略使用一组访问策略规则定义。这些规则需考虑以下几项输入参数：

- 位置 — 用户从什么地方访问网络？
- 时间 — 用户什么时间访问网络？
- 设备 — 用户使用何种设备访问网络？

IDM 2.0 使用这些输入参数评估每一个规则。如果找到匹配的规则，与该规则相关的访问权限（称为访问档案）就会应用于该用户。访问档案定义了用户访问网络时所属的 VLAN、访问控制列表 (ACLs)、QoS 和带宽速度限制。

IT 人员只需定义访问策略组，并为每个访问档案组建立一个访问档案。这样，便可根据现有公司目录中的信息自动将用户分配到各个组中，或由管理员进行分配。用户被分配给适当的组后，IDM 2.0 将自动处理其余的访问和服务任务。根据访问策略组中定义的规则，用户将获得适当的网络资源访问权限和网络服务。

当新的用户或员工需要访问网络时，IT 人员只需将他们添加到现有的访问策略组中即可。当访问权限需要改变时，人们对特定的访问策略组进行修改，然后该修改将自动传播给组中的每一个用户并且在每个用户的使用中得到实现。

图 2 显示了网络如何自动地为每一个用户进行位置、时间和系统等方面的配置，以实施不同的 VLAN、ACL、QoS 和带宽速度限制策略。

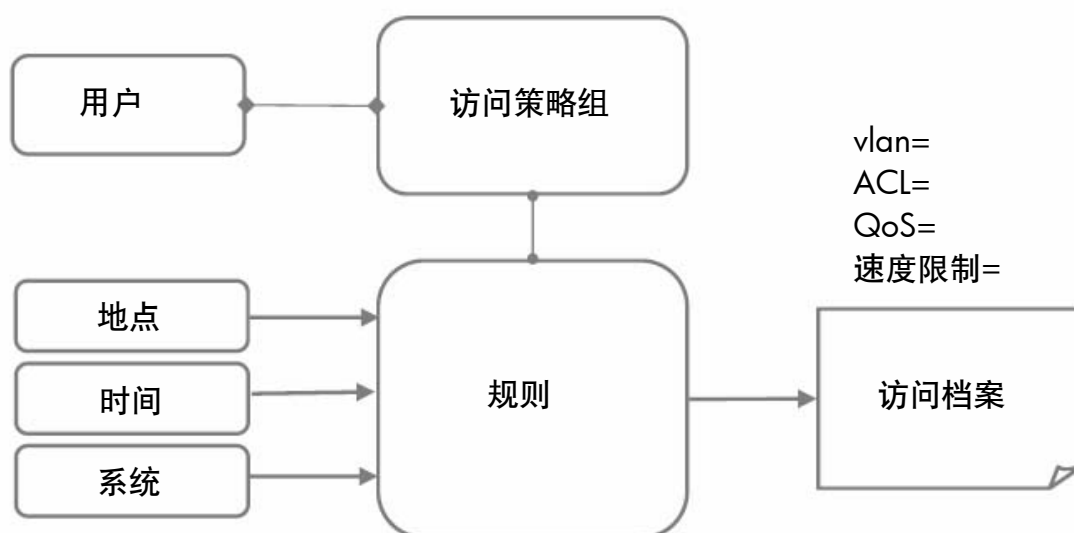


图 2. IDM 配置模型

IDM 架构与实施

实施 IDM 2.0 需要已有的 RADIUS 验证解决方案或 ProCurve 访问控制解决方案。建立此种解决方案有很多选项，但每个选项都包括 3 个主要组件：

- 申请者/客户端（支持 802.1X、Web 验证或 MAC 验证）。
- ProCurve 交换机或无线接入点。
- RADIUS 服务器：Microsoft Internet Authentication Service、Funk Steel-Belted Radius 和 FreeRADIUS。

上述 3 个组件构成了运行 IDM 2.0 的主要框架。

没有 IDM 功能，客户端流量将由边缘交换机或接入点通过标准 RADIUS 协议传送给 RADIUS 服务器。然后 RADIUS 服务器访问用户数据库，以查找有效用户并建立匹配。验证用户之后，RADIUS 服务器将验证信息返回边缘交换机，这样用户就可以在此处连接并访问网络。

在该过程中增加 IDM 功能不会干扰或改变这些流程。IDM 2.0 只是添加到这些流程中。即使使用 IDM 2.0 也不会改变用户验证任务（用户名、密码等）。

IDM 代理与 RADIUS 服务器同时驻留运行，并在用户通过服务器进行网络验证时执行操作。IDM 代理能够限制网络访问和/或在 RADIUS 应答中添加授权参数，然后发送给交换机以指定用户的访问权限。这些参数均以 RADIUS 属性的形式发送，然后交换机在连接期间将它们应用于客户端访问端口。

包含 IDM 2.0 模块的 ProCurve Manager Plus 服务器与安装在 RADIUS 服务器和 ProCurve 边缘设备上的 IDM 代理合作执行下列任务：

- 带 IDM 2.0 的 ProCurve Manager Plus 服务器 — 存储和访问定义的策略
- IDM 2.0 代理 — 实施每一个用户的策略决定
- ProCurve 边缘设备 — 按会话实施策略

IDM 2.0 添加 IT 管理人员定义的高级网络访问权限和参数，只是为了扩充已有的安全系统。

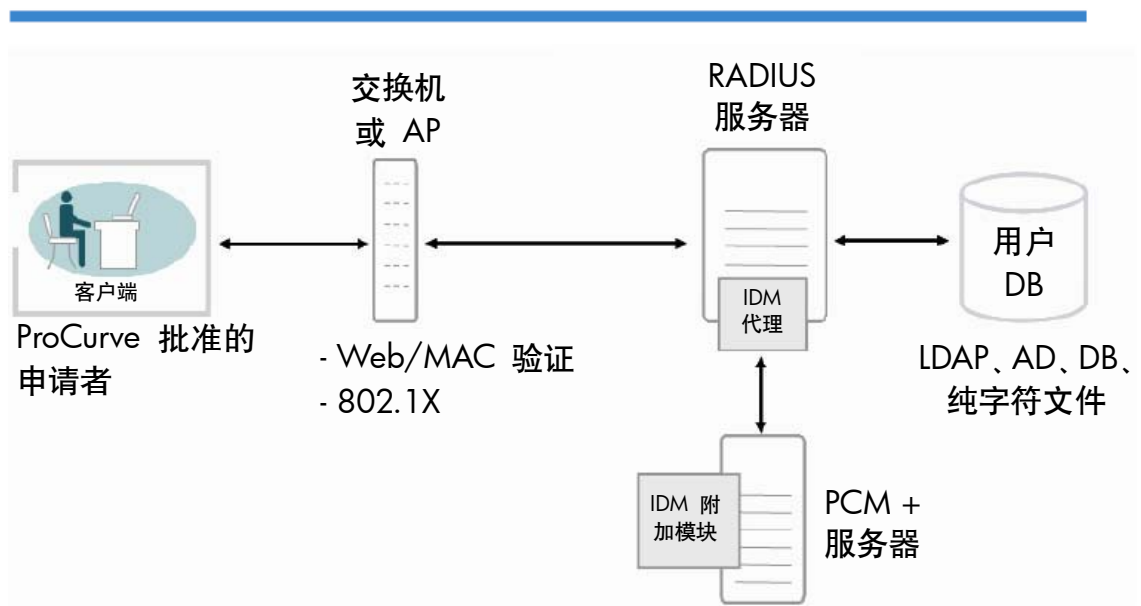


图 3. IDM 架构

概要

公司使用 ProCurve IDM 解决方案后可从动态网络中获益匪浅，并能够为每个用户提供独特而适用的服务。这不仅会提高工作人员的生产率，而且能够改进网络安全性、管理和性能。

最重要的是，由于适应性基础架构根据每个人及其特定访问权限和服务需求自行进行配置，因此，网络不仅仅是简单地实现技术连接，还能够更好地服务于业务和用户目标。

更多信息

欲知有关 ProCurve Networking 的详情，
请访问：www.hp.com.cn/network

欲了解更多信息，请电话垂询当地惠普销售办事处或离您最近的惠普授权经销商。

惠普售前支持热线： 800-820-2255

惠普售后支持热线： 800-810-3888

惠普客户反馈/投诉热线： 800-810-0039

或请访问：www.hp.com.cn
www.hp.com.cn/network

© 2007 Hewlett-Packard Development Company, L.P. 本文所含信息如有更改，恕不另行通知。
惠普产品与服务的全部保修条款在此类产品和服务附带的保修声明中均已列明，本文中的任何信息均不构成额外的保修条款。惠普对于本文中所包含的技术或编辑错误、遗漏概不负责。
所有信息的最终解释权归中国惠普有限公司所有。

P/N: 4AA0-0106CHP Rev. 1, 2007 年 9 月

