 控制开支对于保证盈利能力至关重要。这就是为什么如此多的机构都希望用新的方法将网络与他们的关键业务流程集成到一起的原因。但是，并不是任何网络都可以满足他们的需要。只有那些不光只是传输语音和数据的智能网络才对成功至关重要。一个典型的例子就是思科结构化无线感知网络（SWAN），它可以简化无线LAN（WLAN）的日常运营、确保顺利的WLAN部署，提高安全性，最大限度地提高网络的可用性，同时大幅度地降低部署和运营开支。CiscoWorks无线局域网管理引擎（WLAN）是思科SWAN的核心。CiscoWorks WLSE可以集中地管理位于园区环境和分支机构地点中的成百上千个接入点。 概述 CiscoWorks WLSE是一个集中的系统级解决方案，可以帮助客户管理整个Cisco Aironet WLAN基础设施。先进的无线/射频（RF）和设备管理工具可以消除复杂性，让管理员全面地了解WLAN的运行状况。 CiscoWorks WLSE可以确保在整个网络中统一地应用安全策略，帮助管理员迅速、方便地检测、定位和禁用未经授权的（恶意的）接入点，提高网络的安全性。 CiscoWorks WLSE还可以通过检测和定位RF干扰，以及主动地监控使用情况和故障，优化网络的性能。 图1 CiscoWorks WLSE可以为WLAN提供全面的网络和无线/RF管理 CiscoWorks WLSE可以利用思科SWAN中的Cisco Aironet接入点和日益增长的思科基础设施设备中内置的无线/RF测量功能和多功能特性。这不仅可以降低网络中需要的组件的总数，还可以降低部署所需

要的成本和时间。通过使用辅助性现场调查等工具，能大大降低部署难度。事实上，CiscoWorks WLSE可以自动地执行很多以前非常费时的重复性任务，例如批量固件升级和集中设置接入点、网桥。CiscoWorks WLSE可以通过系统日志消息、简单网络管理协议（SNMP）陷阱和可扩展标记语言，被透明地集成到其他网络管理系统（NMS）、运营支持系统（OSS）和CiscoWorks应用中。这种安全的、基于HTML的用户界面（如图1所示）可以提供随时随地的访问，甚至可以通过防火墙。CiscoWorks WLSE运行在Cisco 1130硬件平台上，该平台的高度为1个机架单元（1RU）。 无线入侵检测CiscoWorks WLSE可以检测、定位和消除由不知情的员工或者恶意的外界入侵者放置的恶意接入点。过去，网络管理人员必须亲自携带手持传感器，在整个建筑物中巡查一遍，才能找到恶意接入点。这种手动、费时、高成本的任务必须定期重复执行，以便及时发现新安装的恶意接入点。CiscoWorks WLSE则可自动完成这项任务。它不仅能通过一个被称为“ 位置管理器 ”（如图2所示）的图形化用户界面显示交换机端口的详细情况，还可以显示它们的物理位置。管理员现在可以迅速地检测、定位和禁用恶意接入点，消除它们所带来的安全威胁。 图2 CiscoWorks WLSE的“ 位置视图 ”可以显示恶意接入点的位置 无线/RF扫描和监控Cisco Aironet接入点提供多种功能，而且内置了RF测量功能。CiscoWorks WLSE可以分析这些RF测量数据。一旦性能降低，CiscoWorks WLSE可以立即发出通知，并显示无线/RF覆盖范围（如图3所示）。任何WiFi客户端设备都可在WLAN中使用。但是，Cisco Aironet WLAN客户端适配器和思科兼容扩展客户端设

备可以提供额外的优势。与Cisco Aironet接入点一样，这些客户端都内置了RF测量功能。事实上，客户端的无线扫描和监控功能所提供的RF测量数据比接入点生成的RF测量数据多出10到20倍。因为WLAN客户端可以在一个建筑物内的所有区域自由移动，所以客户端扫描和监控功能的添加可以将RF监控拓展到最可能包含恶意接入点的区域，同时实现更加准确的恶意接入点检测。 图3 位置管理器显示的无线/RF覆盖范围 干扰检测CiscoWorks WLSE可以对所有受控的接入点的物理位置进行分类，创建一个WLAN安装地图。这使得无线感知网络能检测到对网络性能造成影响的、产生干扰性RF能量的地点。这种未知的RF能量的来源可能是一个恶意接入点或者一个工作在相同频段的设备，例如一部2.4GHz的无绳电话或者存在能量泄露的微波炉。 干扰检测和定位功能对于保持一个可靠的WLAN非常关键。发送到CiscoWorks WLSE的RF测量数据包括IEEE 802.11和非802.11干扰信息。如果干扰幅度超过了某个由管理员定义的阈值，CiscoWorks WLSE就会生成一个错误信息，从而让管理员可以迅速定位和消除干扰源。辅助性现场调查要实现全面、可靠的WLAN覆盖，必须要进行一次详细的现场调查。现场调查是部署期间的一个“ 最佳实践 ”，而且必须定期进行，以适应在网络环境中不断发生的各种变动。过去，现场调查需要专门的知识，而且非常昂贵和费时。大部分机构都聘请外界的顾问来执行这项任务，但是CiscoWorks WLSE现在可以帮助IT管理人员独立自主、经济有效地进行现场调查，而不需要专门聘请精通RF的传播和测量的专家。利用辅助性现场调查工具，CiscoWorks WLSE可以自动地确定最佳频率、发射功率和其他设置，随后由管理

员着手实施（如图4所示）。 图4 辅助性现场调查，“ AP扫描模式 ”设备管理 CiscoWorks WLSE可以自动地执行多种重复性、费时的任务，从而简化Cisco Aironet接入点和网桥的管理。 AutoConfig如果需要，新部署的接入点可以通过一种名为“ AutoConfig ”的功能，利用动态主机配置协议（DHCP），自动地接收由客户定义的缺省配置。这让管理员能在一个迅速扩充的环境中保持控制能力。 批量配置客户可以像配置单个设备一样，配置一个包含数百个设备的群组。配置任务可以定期执行或者在需要的时候执行。 集中固件升级接入点和网桥的硬件可以批量升级。升级可分配到某个特定的设备或者群组。任务可以定期执行或者在需要的时候执行。 动态分组群组让网络变得更加便于理解和管理。设备可以按照管理员所定义的层次化分组进行组织。群组可以跨越多个子网。配置档案配置档案会存储每个设备的最近4个配置版本，从而让管理员可以撤销配置任务。 批量转换到Cisco IOS软件运行VxWorks操作系统的Cisco Aironet 1200和350系列接入点可批量升级到Cisco IOS软件格式。 VLAN配置接入点上的VLAN能进行配置和监控，从而让管理员可以为企业和公开VLAN上的不同用户提供不同的LAN策略和服务，例如安全和服务质量（QoS）。 自动发现CiscoWorks WLSE可以利用思科发现协议，自动发现Cisco Aironet接入点、网桥和连接到接入点的交换机。发现任务可以定期执行或者在需要的时候执行。 集成CiscoWorks WLSE通过系统日志消息、SNMP陷阱和一个XML接口，提供了与第三方NMS的集成。作为CiscoWorks系列网络管理产品的一部分，CiscoWorks WLSE还可以与CiscoWorks LAN管理解决方案（LMS）和其他CiscoWorks

应用集成，从而可以最大限度地提高一个融合式有线或无线网络的管理效率。例如，设备库存信息和信任资格可以在CiscoWorks WLSE和CiscoWorks Resource Manager Essentials（RME）之间导入或导出。后者是一种可以为多种思科设备提供广泛网络管理功能的应用。如果需要，可以关闭CiscoWorks WLSE中的设备发现功能，并使其自动与RME同步库存信息。CiscoWorks WLSE使用的缺省用户角色与RME相同，但是允许定制。CiscoWorks WLSE可以从CiscoWorks 思科管理连接桌面启动，或者通过CiscoWorks园区管理器拓扑图启动。 性能优化和可用性 CiscoWorks WLSE能主动地监控WLAN基础设施的使用情况、故障和性能降低情况。它可以支持以太网和无线通信接口。 干扰检测CiscoWorks WLSE可以不间断地分析由Cisco Aironet系列接入点、Cisco Aironet WLAN客户端适配器和思科兼容扩展客户端设备生成的RF测试数据。在发生干扰时，CiscoWorks WLSE会自动发出通知。 可定制的阈值管理员可以为特定的地点和群组设定不同的故障和性能阈值，以及特定的操作和缺省的优先级。一种包含关于受影响设备和故障的严重性的详细信息的集中故障界面可以帮助管理员迅速地解决问题。故障状态CiscoWorks WLSE可以提供一个所有接入点和用户群组的集中树型视图。彩色代码和群组标志可以显示缺省的状态。故障可以按照优先级过滤和排序，以便于查看和解决故障。 故障通知故障通知和转发可以通过系统日志消息、SNMP陷阱和电子邮件实现。 交换机状态CiscoWorks WLSE会监控与接入点相连的交换机，了解它们的端口、CPU和内存的可用性和使用情况。 增强的安全性 无线入侵检

测CiscoWorks WLSE可以迅速地发现和定位恶意接入点。关于恶意接入点所在的交换机端口的详细信息将让管理员可以禁用恶意接入点。 安全策略监控CiscoWorks WLSE可以监控网络上的所有接入点，以确保安全策略的统一应用。而且CiscoWorks WLSE会对不符合服务集标识符（SSID）、广播、802.1X可扩展身份验证协议（EAP）设置和有线等效加密（WEP）的情况发出警报。警报可以通过电子邮件、系统日志或者SNMP陷阱的形式发出。 IEEE 802.1X服务器可用性的监控CiscoWorks WLSE可以监控IEEE 802.1X EAP服务器包括思科安全接入控制服务器（ACS）的响应时间。支持Cisco EAP（LEAP）、受保护EAP（PEAP）和通用RADIUS身份验证。 安全用户界面CiscoWorks WLSE可以提供一个安全的、基于HTML的用户界面。用户能随时随地访问该界面，甚至通过防火墙。除了基于Web的GUI以外，与Cisco IOS软件类似的命令行界面（CLI）可以提供对于CiscoWorks WLSE的直接控制台、Telnet或者安全壳式协议（SSH）访问，以实现基本的配置和诊断功能。 报告、趋势和规划 CiscoWorks WLSE提供多种预先定义的报告，它们对于诊断和容量规划非常有用。这些报告的内容包括网络使用情况、客户端关联和使用情况、历史和当前客户端使用统计数据，以太网和无线接口状态，以及错误详细信息。CiscoWorks WLSE可以提供群组级和单个设备级的报告。 所有报告都能定期生成，并通过电子邮件发送。报告可输出为CSV、XML和PDF格式。 适用于大型网络的容量 每个CiscoWorks WLSE（产品编号CWWLSE-1130-K9）最多可以管理2500个接入点。 基于角色的访问模式 CiscoWorks WLSE采用了一个灵活的、基于角

色的用户访问模式。例如，帮助台人员的访问角色只能查看报告和故障。WLSE用户可以通过多种通用的身份验证模块（例如TACACS、RADIUS和Microsoft NT域）进行身份验证。 特性和优点 表1总结了CiscoWorks WLSE的特性和优点。 技术规格 表2列出了CiscoWorks WLSE的技术规格。 CiscoWorks WLSE所支持的思科设备 表3列出了CiscoWorks WLSE所支持的接入点和网桥。 注意：对于IEEE 802.11g的支持预计将于2004年度的第二季度推出。 表4列出了CiscoWorks WLSE所支持的交换机。 表5列出了CiscoWorks WLSE所支持的路由器。 表6列出了CiscoWorks WLSE所支持的接入服务器。 CiscoWorks WLSE所支持的Web浏览器 CiscoWorks WLSE可以通过下列Netscape和Internet Explorer浏览器访问。这些浏览器可以运行在一个CPU和内存要求都较低的系统上。 Netscape 4.79 Microsoft Internet Explorer 5.5 （装有Service Pack 2）和Microsoft Internet Explorer 6.0 