

- 服务等级协议的监测。服务等级协议 (Service Level Agreement, SLA) 是契约, 定义了特定的性能测度和网络提供商提供的相对于这些性能测度的可接受性能等级 [Huston 1999a]。Verizon 和 Sprint 是两个网络提供商, 它们与其他 ISP 一样向其用户提供确保的 SLA [AT&T SLA 2012; Verizon 2012]。这些 SLA 包括服务可用性 (断线率)、时延、吞吐量和断线通知要求。很显然, 如果性能标准是网络提供商和其用户间服务协议的一部分的话, 那么测量和管理性能对于网络管理员是十分重要的。
- 入侵检测。当网络流量来自一个可疑源或预定要流向一个可疑源 (例如, 主机或端口号) 时, 网络管理员可能希望得到提示。类似地, 网络管理员可能希望检测 (并在许多情况下过滤) 某类流量的存在 (例如, 源路由选择分组或指向给定主机的大量 SYN 分组), 这被认为具有安全性攻击类型的特征, 我们已在第 8 章中讨论过了。

国际标准化组织 (ISO) 已经建立了一个网络管理模型, 该模型对于将上述各种各样的情况放置于更为结构化的框架中是有用的。该模型定义了网络管理的 5 个领域:

- 性能管理 (performance management)。性能管理的目标是量化、测量、报告、分析和控制不同网络部件的性能 (如利用率和吞吐量)。这些部件包括各个设备 (如链路、路由器和主机) 以及如通过某网络的路径那样的端到端抽象。我们很快将会看到, 如简单网络管理协议 (Simple Network Management Protocol, SNMP) [RFC 3410] 这样的协议标准在因特网性能管理中起着最重要的作用。
- 故障管理 (fault management)。故障管理的目标是记录、检测和响应网络中的故障情况。故障管理和性能管理之间的区别是相当模糊的。我们能够认为故障管理是对暂时性网络故障 (例如, 链路、主机及路由器硬件或软件的停转) 的及时处理, 而性能管理采取更为长期的观点, 面对变化的流量要求和偶尔的网络设备故障, 提供可接受的性能等级。与性能管理一样, SNMP 协议在故障管理中起着最重要的作用。
- 配置管理 (configuration management)。配置管理允许网络管理员跟踪被管理网络中的那些设备, 跟踪这些设备的硬件和软件配置。有关基于 IP 网络的配置管理和要求的概述可参见 [RFC 3139]。
- 账户管理 (accounting management)。账户管理允许网络管理员定义、记录、控制用户和设备访问网络资源。限额使用、基于使用的收费和分配资源访问权限都属于账户管理的范围。
- 安全管理 (security management)。安全管理的目标是根据某些定义明确的策略控制对网络资源的访问。我们在 8.3 节中讨论的密钥分发中心是安全管理的一部分。使用防火墙监视和控制网络的外部接入点既是我们在 8.9 节中讨论的一个主题, 也是本章的一个重要部分。

在本章中, 我们仅将涉及网络管理的入门知识。我们有意识地关注有限的范围, 讨论网络管理的基础设施, 即总体体系结构、网络管理协议和信息库, 网络管理员将通过该信息库保持网络正常运行。我们将不涉及网络管理员的决策过程, 其中网络管理员必须对传送到 NOC 的网络信息进行规划、分析和做出响应。在这个领域中, 诸如故障标识和管理 [Katzela 1995; Medhi 1997; Labovitz 1997; Steinder 2002; Feamster 2005; Wu 2005; Teix-