

等级考试三级网络技术复习笔记第六章 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/137/2021_2022__E7_AD_89_E7_BA_A7_E8_80_83_E8_c98_137376.htm

第六章 网络安全技术 网络管理包括五个功能：配置管理，故障管理，性能管理，计费管理和安全管理。代理位于被管理的设备内部，它把来自管理者的命令或信息请求转换为本设备特有的指令，完成管理者的指示，或返回它所在设备的信息。管理者和代理之间的信息交换可以分为两种：从管理者到代理的管理操作；从代理到管理者的事件通知。配置管理的目标是掌握和控制网络和系统的配置信息以及网络各设备的状态和连接管理。现代网络设备由硬件和设备驱动组成。配置管理最主要的作用是可以增强网络管理者对网络配置的控制，它是通过对设备的配置数据提供快速的访问来实现的。故障就是出现大量或严重错误需要修复的异常情况。故障管理是对计算机网络中的问题或故障进行定位的过程。故障管理最主要的作用是通过提供网络管理者快速的检查问题并启动恢复过程的工具，使网络的可靠性得到增强。故障标签就是一个监视网络问题的前端进程。性能管理的目标是衡量和呈现网络特性的各个方面，使网络的性能维持在一个可以接受的水平上。性能管理包括监视和调整两大功能。计费管理的目标是跟踪个人和团体用户对网络资源的使用情况，对其收取合理的费用。计费管理的主要作用是网络管理者能测量和报告基于个人或团体用户的计费信息，分配资源并计算用户通过网络传输数据的费用，然后给用户开出帐单。安全管理的目标是按照一定的方法控制对网络的访问，以保证网络不被侵害，并保

证重要的信息不被未授权用户访问。安全管理是对网络资源以及重要信息访问进行约束和控制。在网络管理模型中，网络管理者和代理之间需要交换大量的管理信息，这一过程必须遵循统一的通信规范，我们把这个通信规范称为网络管理协议。网络管理协议是高层网络应用协议，它建立在具体物理网络及其基础通信协议基础上，为网络管理平台服务。目前使用的标准网络管理协议包括：简单网络管理协议SNMP，公共管理信息服务/协议CMIS/CMIP，和局域网个人管理协议LMMP等。SNMP采用轮循监控方式。代理/管理站模式。管理节点一般是面向工程应用的工作站级计算机，拥有很强的处理能力。代理节点可以是网络上任何类型的节点。

。SNMP是一个应用层协议，在TCP/IP网络中，它应用传输层和网络层的服务向其对等层传输信息。CMIP的优点是安全性高，功能强大，不仅可用于传输管理数据，还可以执行一定的任务。信息安全包括5个基本要素：机密性，完整性，可用性，可控性与可审查性。

1 D1级。D1级计算机系统标准规定对用户没有验证。例如DOS，WINDOS3.X及WINDOW 95（不在工作组方式中）。Apple的System7。X。

2 C1级提供自主式安全保护，它通过将用户和数据分离，满足自主需求。C1级又称为选择安全保护系统，它描述了一种典型的用在Unix系统上的安全级别。C1级要求硬件有一定的安全级别，用户在使用前必须登陆到系统。C1级的防护的不足之处在与用户直接访问操作系统的根。

3 C2级提供比C1级系统更细微的自主式访问控制。为处理敏感信息所需要的最底安全级别。C2级别还包含有受控访问环境，该环境具有进一步限制用户执行一些命令或访问某些文件的权限，而且

还加入了身份验证级别。例如UNIX系统。XENIX。Novell 3.0或更高版本。WINDOWS NT。4 B1级称为标记安全防护，B1级支持多级安全。标记是指网上的一个对象在安全保护计划中是可识别且受保护的。B1级是第一种需要大量访问控制支持的级别。安全级别存在保密，绝密级别。5 B2又称为结构化保护，他要求计算机系统中的所有对象都要加上标签，而且给设备分配安全级别。B2级系统的关键安全硬件/软件部件必须建立在一个形式的安全方法模式上。6 B3级又叫安全域，要求用户工作站或终端通过可信任途径连接到网络系统。而且这一级采用硬件来保护安全系统的存储区。B3级系统的关键安全部件必须理解所有客体到主体的访问，必须是防窜扰的，而且必须足够小以便分析与测试。7 A1 最高安全级别，表明系统提供了最全面的安全，又叫做验证设计。所有来自构成系统的部件来源必须有安全保证，以此保证系统的完善和安全，安全措施还必须担保在销售过程中，系统部件不受伤害。网络安全从本质上讲就是网络上的信息安全。凡是涉及到网络信息的保密性，完整性，可用性，真实性和可控性的相关技术和理论都是网络安全的研究领域。安全策略是在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。安全策略模型包括了建立安全环境的三个重要组成部分：威严的法律，先进的技术和严格的管理。网络安全是网络系统的硬件，软件以及系统中的数据受到保护，不会由于偶然或恶意的原因而遭到破坏，更改，泄露，系统能连续，可靠和正常的运行，网络服务不中断。保证安全性的所有机制包括以下两部分：1 对被传送的信息进行与安全相关的转换。2 两个主体共享不希望对手得知的保密信

息。安全威胁是某个人，物，事或概念对某个资源的机密性，完整性，可用性或合法性所造成的危害。某种攻击就是某种威胁的具体实现。安全威胁分为故意的和偶然的两类。故意威胁又可以分为被动和主动两类。中断是系统资源遭到破坏或变的不能使用。这是对可用性的攻击。截取是未授权的实体得到了资源的访问权。这是对保密性的攻击。修改是未授权的实体不仅得到了访问权，而且还篡改了资源。这是对完整性的攻击。捏造是未授权的实体向系统中插入伪造的对象。这是对真实性的攻击。被动攻击的特点是偷听或监视传送。其目的是获得正在传送的信息。被动攻击有：泄露信息内容和通信量分析等。主动攻击涉及修改数据流或创建错误的流，它包括假冒，重放，修改信息和拒绝服务等。

100Test 下载频道开通，各类考试题目直接下载。详细请访问
www.100test.com