# 项目7　网络安全管理

**授课教师： 职称： 授课年级： 专业：**

一、**组织教学**

课前3分钟，教师开启电脑、投影仪等所需设备，检查设备情况，并将所需课件拷贝到电脑上；检查黑板是否擦干净。

上课铃响，教师宣布上课，师生问好。

教师检查人数，查找缺席学生及原因。

教师将学生以4~5人一组，分成若干小组。

（本课程中涉及到小组讨论环节时，按照此次组员编排进行）

**二、引入新课**

本项目主要介绍网络管理的概念、目的、范围和功能，网络管理的协议，网络管理系统的组成和功能，网络管理软件的基本分类，典型的网络管理系统，网络安全的概念，网络安全技术，计算机病毒及其防治等。

## 7.1　网络管理概述

### 7.1.1　网络管理的概念

随着计算机技术和Internet的发展，企业和政府部门开始大规模地建立网络来推动电子商务和政务的发展。伴随着网络的业务和应用的丰富，对计算机网络的管理与维护也就变得至关重要。网络管理（包括网络管理系统即“网管系统”)就是为了加强和完善网络的性能。人们普遍认为，网络管理是计算机网络的关键技术之一，尤其在大型计算机网络中更是如此。

### 7.1.2　网络管理的目的

国际标准化组织（ISO)在ISO/IEC7498-4中定义并描述了开放系统互连（OSI)管理的术语和概念，提出了一个OSI管理的结构并描述了OSI管理应有的行为。它认为：开放系统互连管理是指这样一些功能，它们控制、协调、监视OSI环境下的一些资源，这些资源保证OSI环境下的通信。

### 7.1.3　网络管理的范围

网络管理的范围涉及两方面，即网络管理的对象范围和内容范围。网络管理的对象范围经历了由窄到宽的发展。以前网络管理主要是对少数常用的网络节点设备进行维护，现在则主要是管理所有支持代理进程（委托代理）处理能力的网络设备，包括从个人数字助理到大型计算机的全部计算机设备。网络管理可以运行在当代各种联网协议上。

### 7.1.4　网络管理的功能

根据国际标准化组织的定义，网络管理有五大功能：故障管理、配置管理、计费管理、性能管理、安全管理。这五大功能保证一个网络系统正常的运行,在网管设计和实施中通常都需要考虑实现。与这五大功能相对应的五种管理形式常用首字母缩写词FCAPS表示。

F：Fault Management(故障管理）。

C：Configuration Management(配置管理）。

A：Accounting Management(计费管理）。

P：Performance Management(性能管理）。

S：Security Management(安全管理）。

## 7.2　简单网络管理协议

### 7.2.1　什么是SNMP

SNMP是简单网络管理协议Simple Network Management Protocol的英文缩写，它是由Internet工程任务组织（Internet Engineering Task Force)的研究小组为了解决Internet上的路由器管理问题而提出的。SNMP不但提供了一种从网络上的设备中收集网络管理信息的方法，也为设备向网络管理中心报告问题和错误提供了一种方法。

SNMP为网络管理系统提供了底层网络管理的框架。SNMP的应用范围非常广泛，诸多种类的网络设备、软件和系统中都有所采用。

### 7.2.2　SNMP的发展

最初的SNMP协议版本是SNMP v1，它简单地定义了一个基本的用于实现设备的基础管理，涵盖了系统/网络/应用/服务等方面的内容，但几乎没有任何有效的验证方式。

后来又发展出了SNMP v2,最常见到的是SNMP v2c、SNMP v2c与SNMP v1向后兼容,并且改善了安全模型和访问控制。

最新的SNMP版本是SNMP v3,它不但采用了新的SNMP消息格式，在安全方面也有很大加强。最大的变化就是采用了一种基于视图的安全模型，使管理者可以基于组和用户来详细定义每个对象的访问权限。

### 7.2.3　SNMP的内容

SNMP是一系列协议组和规范，它们提供了一种从网络上的设备中收集网络管理信息的方法。SNMP定义了数据包的格式和网络管理员与管理代理之间的信息交换的方式，它还控制着管理代理的MIB数据对象，因此，可用于处理管理代理定义的各种任务。SNMP之所以易于使用,是因为它对外提供了三种用于控制MIB对象的基本操作命令。它们是Set、Get和Trap。

Set:它是一个特权命令，通过它可以改动设备的配置或控制设备的运转状态。

Get：它是SNMP协议中使用率最高的一个命令，因为该命令是从网络设备中获得管理信息的基本方式的。

Trap：它的功能就是在网络管理系统没有明确要求的前提下，由管理代理通知网络管理系统有一些特别的情况或问题发生了。

## 7.3　网络管理系统

### 7.3.1　网络管理系统的组成和功能

一个典型的网络管理系统包括四个要素：管理员、管理代理、管理信息数据库、代理服务设备。一般来说，前三个要素是必需的,第四个是可选项。

### 7.3.2　网络管理软件的分类

根据网管软件的发展历史,可以将网管软件划分为三代。

第一代网管软件就是最常用的命令型方式，结合一些简单的网络监测工具。它不仅要求使用者精通网络的原理及概念，还要求使用者了解不同厂商的不同网络设备的配置方法。

第二代网管软件有着良好的图形化界面。用户无须过多地了解设备的配置方法，就能图形化地对多台设备同时进行配置和监控。这就大大提高了工作效率，但仍然存在着由于人为因素造成的设备功能使用不全面或不正确的问题。

第三代网管软件相对来说比较智能，它是真正将网络和管理进行有机结合的软件系统，具有“自动配置”和“自动调整”功能。对网管人员来说，只要把用户情况、设备情况以及用户与网络资源之间的分配关系输入网管系统，系统就能自动地建立图形化的人员与网络的配置关系，并自动鉴别用户身份，分配用户所需的资源(如电子邮件、Web文档服务等）。

### 7.3.3　典型网络管理系统介绍

根据网络管理软件产品功能的不同，网络管理系统又可细分为5类，即网络故障管理软件、网络配置管理软件、网络性能管理软件、网络服务/安全管理软件、网络计费管理软件。一个完整的网管系统往往同时具备这五种功能，不过功能侧重点有所不同。当然，市面上现在也有许多小的工具软件，能辅助网络管理员实现网络管理的部分功能，它们也可以为网络管理系统。

就国外网管厂商而言，主要有三大家：CA Unicenter、HP OpenView NNM和IBM Tivoli NetView。这些系统的特点是功能强大，覆盖网络管理的计费、认证、配置、性能和故障的各个方面。缺点是需要专业化的技术团队进行管理，投入大、实施周期长、运营和维护非常麻烦。

## 7.4　网络安全概述

### 7.4.1　网络安全的概念

国际标准化组织(ISO)将计算机安全定义为“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露”，我国提出的定义是计算机系统的硬件、软件、数据受到保护，不因偶然的或恶意的原因而遭到破坏、更改、显露，系统能连续正常运行”。因此，所谓网络安全就是指基于网络的互连互通和运作而涉及的物理线路和连接的安全、网络系统的安全、操作系统的安全、应用服务的安全和人员管理的安全等几个方面。但总的说来，计算机网络的安全性是由数据的安全性、通信的安全性和管理人员的安全意识三部分组成的。

### 7.4.2　网络安全问题的主要原因

产生网络安全问题的原因有很多，从不同的角度思考会得出不同的结论，但在技术层面上来说，网络安全问题主要是由于网络技术本身设计上的缺陷和现实利益的驱动相结合产生的。众所周知，计算机网络的最大特点就是开放和共享，而对于安全来说，这又是它致命的弱点。计算机网络发展的初期，为了让各种不同的计算机能够互连，网络通信协议的推广采用了开放式的策略，任何人都能很容易地获得通信协议等详细的技术细节，从而对协议存在的缺陷了如指掌，为通过网络进行攻击提供了可能性。

### 7.4.3　我国面临的网络安全问题

目前,我国网络安全问题日益突出的主要标志为如下几种。

1.系统遭受病毒感染和破坏的情况相当严重

2.电脑黑客活动已形成重大威胁

3.信息基础设施面临网络安全的挑战

4.网络政治颠覆活动频繁

## 7.5　网络安全技术

网络系统的安全涉及平台的各个方面。按照网络OSI的7层模型，网络安全贯穿于网络的各个层次，在不同的网络层次可以采用不同的技术手段来实现和防范某些网络威胁。在OSI七个层次的基础上，将安全体系划分为四个级别：网络级安全、系统级安全、应用级安全及企业级的安全管理，而安全服务渗透到每一个层次，从尽量多的方面考虑问题，有利于减少安全漏洞和缺陷。

## 7.6　计算机病毒及其防治

### 7.6.1　计算机病毒起源

总的来说，计算机病毒的发展历史可以划分为如下四个阶段。

第一代病毒(1986—1989年）：这一期间出现的病毒可以称之为传统的病毒，是计算机病毒的萌芽和滋生时期。

第二代病毒(1989—1991年）：第二代病毒又称为混合型病毒，这一阶段是计算机病毒由简单发展到复杂，由单纯走向成熟的阶段。

第三代病毒（1992—1995年）：第三代病毒称为“多态性”病毒或“自我变形”病毒。这个时期是病毒的成熟发展阶段。

第四代病毒（1996年至今）：第四代病毒是20世纪90年代中后期产生的病毒。随着互联网的盛行,病毒流行面更加广泛，病毒的流行迅速突破了地域限制。

### 7.6.2　计算机病毒的特征及分类

计算机病毒本质上也是一段程序代码/在区分正常程序与病毒的时候，一般按照以下特征判断。

(1)非授权可执行性用户调用执行一个程序时,把系统控制交给这个程序，并分配给它相应系统资源(如内存），从而使之能够运行,并完成用户的需求。

(2)隐蔽性。

(3)传染性。

(4)潜伏性。

(5)表现性，或破坏性。

(6)可触发性。

计算机病毒若按破坏性划分可分为良性病毒与恶性病毒,若按传染方式划分可分为以下几种类型。

(1)引导型病毒。

(2)文件型病毒。

(3)网络型病毒。

(4)新型病毒。

### 7.6.3　计算机病毒的防治

一个企业网的防病毒体系是建立在每个局域网的防病毒系统上的，应该根据每个局域网的防病毒要求，建立局域网防病毒控制系统，分别设置有针对性的防病毒策略。

1.增加安全意识

2.小心邮件

3.挑选合适的防病毒软件

## 实践操作任务11防火墙软件的安装与配置