局域网组建、维护与安全监控

实战详解

刘晶　公芳亮　编著

15个网络管理和安全监控案例：

局域网、DHCP服务的搭建，Windows和Linux平台下FTP服务器、Web服务器、数据库的管理与安全防护，局域网数据监控，局域网漏洞扫描，常见网络故障处理，网络设备监控，网络数据捕获与监控，共享服务，木马的检测与防范，单机安全设置，集中式杀毒软件的部署，防火墙解决方案

- 涵盖Windows和Linux两大平台，讲解5大软件Sniffer、MRTG、Cacti、Nagios、PcAnywhere的使用
- 从组建、维护到安全监控，全实例呈现网络管理技术

人民邮电出版社
POSTS & TELECOM PRESS

局域网组建、维护与安全监控

实战详解

刘晶　公芳亮　编著

人民邮电出版社

北京

图书在版编目（CIP）数据

局域网组建、维护与安全监控实战详解 / 刘晶等编著. -- 北京 : 人民邮电出版社, 2010.1
ISBN 978-7-115-21428-7

Ⅰ. ①局… Ⅱ. ①刘… Ⅲ. ①局部网络－基本知识
Ⅳ. ①TP393.1

中国版本图书馆CIP数据核字(2009)第195127号

内 容 提 要

随着局域网应用的普及，局域网维护和安全成为一个热门议题。本书由浅入深，循序渐进地教给读者如何构建、维护局域网以及各类服务器的安全设置。全书内容包括 4 篇，第一篇讲解网络的构成和搭建；第二篇讲解 DHCP、共享服务、FTP、Web 服务、数据库的搭建和安全防护；第三篇讲解网络设备监控、数据捕获、安全检测和网络故障判断与处理；第四篇讲解木马分析、检测和处理，单机安全策略实施，杀毒软件和防火墙应用。

本书适合广大网络维护人员、网站管理人员和大专院校学生阅读。

局域网组建、维护与安全监控实战详解

◆ 编　　著　刘　晶　公芳亮
责任编辑　魏雪萍
执行编辑　张　涛

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：21.75
字数：531 千字　　2010 年 1 月第 1 版
印数：1－3 500 册　　2010 年 1 月河北第 1 次印刷

ISBN 978-7-115-21428-7

定价：39.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

随着网络的发展，网络互连的范围在不断地扩大。局域网的复杂程度也由于网络应用的增加，在快速加大，使每一个网络工程师所要承担的责任和面临的风险也越来越大。如何使用最简单、最快捷的方式管理局域网成为每一个网络工程师必需研究的方向。作者作为大型网络服务器维护人员，长期从事几百台服务器的维护任务，对此深有体会。本书的目的就是为了帮助网络工程师更好地搭建、设置和维护好局域网，提升读者的实战技能。

本书优势

1．内容全面，突出安全

本书完整地讲解局域网管理的各个环节，内容涉及网络构建、服务搭建、网络监控和网络安全实施。内容深入浅出、连贯有序，使读者对整个局域网管理工作有一个整体认识。

2．实例讲解，贴近实战

本书避免同类图书的大篇理论讲解，而是介绍大量的实际应用案例，并结合简单易懂的图例，让读者更容易理解网络的构成和管理。

3．重点突出，监控为主

本书的内容重点是网络监控。在网络管理工作中，大家重视网络搭建，忽视网络监控，从而造成局域网内病毒、木马泛滥。本书着眼实际，详细讲解网络监控。内容涉及 Sniffer、Cacti、Nagios 等专业软件的应用。

本书的组织结构

本书共分为 4 篇。

第一篇为构建篇，包括第 1～3 章。第 1 章帮助读者了解网络的基础，认识 Internet；第 2 章讲解网络的构成；第 3 章讲解局域网的搭建。

第二篇为服务搭建篇，包括第 4～8 章。该篇内容按照标准的安装步骤搭建了 Windows 平台和 Linux 平台下的网络监控环境，并针对其常见的问题给出了解决方案。内容涉及 DHCP、共享、FTP、Web（IIS 和 Apache）、数据库等服务。

第三篇为监控篇，包括第 9～13 章。该篇内容详细地介绍了网络监控的实现。内容包括数据监控、设备监控、安全检测和常见故障排除和处理。本篇涉及了 Pc-Anywhere、Sniffer、SNMP、Mrtg、Cacti、Nagios 等软件应用，并介绍常见协议的监控，以及病毒等安全问题监控。

第四篇为安全实施篇，包括第 14～17 章。该篇内容介绍了网络中各种常见安全问题的

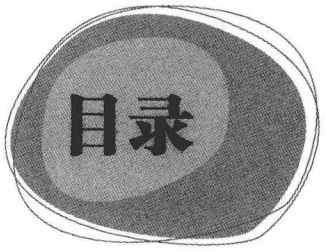
解决方案。内容包括木马问题、单机安全问题、集中式杀毒软件部署和防火墙解决方案。

读者对象

- 计算机网络安全的设计人员。
- 计算机网络安全管理人员。
- 网络爱好者。
- 计算机、信息安全、网络工程、信息工程等相关专业的师生阅读。

在编写本书时，本人精心写作，但由于时间仓促，水平有限，书中难免存有错误或疏漏之处，请读者给予指正，联系邮箱为 zhangtao@ptpress.com.cn。

编者



第一篇 构建篇

第二篇 服务搭建篇

第三篇 监控篇

第四篇 安全实施篇

第一篇

构建篇

第1章 网络概述

随着计算机产业的发展，网络已经越来越多地影响了人们的工作与生活。为了帮助读者理解网络，本章将介绍什么是网络、网络的基本组成、网络的分类以及 Internet。

1.1 计算机网络的定义和功能

计算机网络是现代通信技术与计算机技术相结合的产物。所谓计算机网络，就是把分布在不同地理区域的计算机与专门的外部设备用通信线路互连成一个规模大、功能强的网络系统，从而使众多的计算机可以方便地互相传递信息，共享硬件、软件、数据信息等资源。

1.1.1 计算机网络的定义

多台计算机（两台以上）使用相关的网络协议（如 TCP/IP）由网络设备（如 Hub/交换机/路由器）通过连接设备相连接组成的大型的“计算机集群”系统，称为计算机网络。通常所指的网络是指 Internet 网络以及局域网。图 1-1 所示是一个计算机网络的简要构架。

1.1.2 计算机网络的功能

在目前的主流定义中，网络一般具备如下的功能。

- 数据通信 实现计算机与终端、计算机与计算机间的数据传输，这是计算机网络的基本功能。
- 资源共享 网络上的计算机彼此之间实现资源共享，包括硬件、软件和数据。
- 远程传输 计算机间通过相应的软件以及协议可实现远程传输数据，这样分布在很远地方的用户可以互相传输数据信息，互相交流，协同工作。
- 集中管理 实现数据的集中化，整合化管理，MIS 系统、OA 系统的出现就是集中管理在现代化企业中的最好应用。

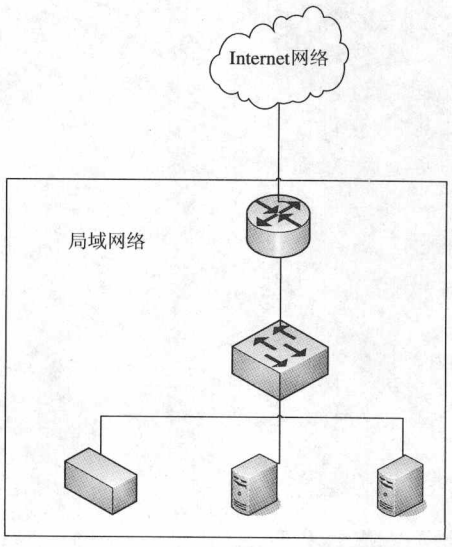


图 1-1 计算机网络的简要构架

● 实现分布式处理 将一个课题分成许多小题目，交给不同的计算机完成，通过网络整合这些数据解决问题，这样能极大地提高工作效率。

● 负荷均衡 负荷均衡是指工作被均匀地分配给网络上的各个节点，当一个节点负荷过重的时候，多余的负荷将通过网络转移到负荷较轻的节点去运行。

1.2 计算机网络的组成

计算机网络通俗地讲就是由多台计算机（或其他网络设备）通过传输介质和软件（或逻辑）连接在一起组成的。本节将对其组成元素进行基本讲解。

1.2.1 硬件设备

硬件设备是网络中必不可缺少的组成元素之一，也是计算机网络最直观的体现之一。组成计算机网络的硬件设备主要包括如下几个部分。

1．服务器

服务器指网络中提供相应的资源和特定服务（如 FTP 服务）的计算机。

2．客户机

客户机是指网络中享受服务的计算机。网络中专用的服务器所提供的服务被客户机所享受，随着计算机的普及以及性能的提高，服务器和客户机的角色可能会相互转变。

3．中继器

在传输介质超过了网段长度后，可用中继器延伸网络的距离。中继器能够对弱信号予以再生放大。根据 IEEE 802 标准规定，最多允许 4 个中继器连接 5 个网段。特殊的中继器包括集线器与交换器（多端口中继器）两种。

● 集线器 是以星型拓扑结构将通信线路集中连接在一起的设备，起到总线的作用。它是局域网中最常用的连接设备。按配置的形式，可分为独立型 Hub、模块化 Hub 和堆叠式 Hub3 种。

● 交换机：把计算机发送的以太网数据包的目的地址以包的形式从发送端口送到目的端口，这样就可以同时传送大量的以太包，从而达到提高网络实际吞吐量的效果。交换机能够同时建立多个相应的传输路径，提高网段上的连接速度。交换机主要用于连接 Hub、服务器和分散式主干网。

4．网桥

网桥也是一种交换设备。网桥可以提供过滤和转发功能，可以连接不同的传输介质，但是没有路径选择能力。

5．调制解调器

调制解调器是指数字设备和模拟电话网之间进行数据转换的设备，可以使用调制解调器来连接电话网，通过信号的转换接入 Internet。

6．网络接口卡

网络接口卡也被称为网卡。它是计算机和网络之间的连接设备，用来接收和发送数据。

网卡可以按照总线、传输速度、接口和需不需网线来分类。

- 按照总线可分为 EISA 接口网卡、ISA 接口网卡、PCI 接口网卡和 USB 接口网卡。其中，PCI 接口网卡是现在最流行的计算机配件。
- 按照传输速度可分为小于 10MB 的网卡、10MB 网卡、10/100MB 自适应网卡、100MB 网卡和 1000MB 网卡。其中，10/100MB 自适应网卡是最常见的网卡。
- 按照接口可分为 RJ-45、AUI、BNC、FDDI。
- 按照是否需要连接网线，又可分为无线网卡和有线网卡两种。

7．网关

网关是用来连接不同网络协议、不同操作系统的网络设备。其主要的功能是将不同的协议、数据格式和速率进行相互的转换，达到它们之间的统一，并提供中转的中间接口。在 Internet 中，网关能够根据用户通信的计算机的 IP 地址，判断是否将用户发出的信息送出本地网络，同时，还判断是否接收外界发送给本地网络计算机的信息。

8．路由器

路由器可以将多个网络或多种介质连接在一起，从而构成一个更大的网络。与网桥相比较，它能够提供更加强大的功能。主要功能包括以下几项。

- 分组转发 为数据包的传输提供最佳路径，将使用不同硬件技术的网络互连，可以对网络进行分组格式和分组长度的相互转换。
- 隔离、划分子网 对子网进行隔离和划分，在路由器的每一端口都可以组成一个单独的子网。
- 提供经济合理的 WAN 接入。
- 提供大规模组网能力 路由器支持备用网络路径、网状网络拓扑、交换机、网桥的无环路拓扑。使用路由器可以将各式各样的通信子网组成一个大范围的网络。

1.2.2 软件组件

组成计算机网络仅仅有硬件是不够的，还需要相应的软件进行支持，这里的软件通常指的是实现网络连接的一些程序，具体可以分为如下几类。

- 网络协议 在网络中实现资源的共享，必须要使用一个相同的语言。交流什么、何时交流、怎样交流，都必须遵从某种互相都能接受的规则，就是称为网络协议（如 TCP/IP）。
- 网络操作系统 是指计算机上所使用的与网络连接的客户端。现在运用最广的是 Windows 系列软件，其余常见的还有 Linux 等。
- 网络应用软件 是指计算机上用户用来使用网络上的相关服务的软件，例如要求浏览网页需要的 IE 浏览器软件。

1.3 计算机网络的分类

计算机网络具有强大的功能，不同类型的网络具有不同功能的应用，本节将具体阐述计算机网络的分类。

1.3.1 按覆盖范围分类

简单的方式是按一个网络覆盖了多少地区来分类，按照这种分类方式计算机网络可以分为如下几类。

- 局域网 它是最小的网络单位，其中包括的计算机数最少为 2 台。局域网是将小区域内的计算机和设备互连在一起的计算机网络。
- 城域网 城市与城市之间的网络连接，一般涉及的计算机数目较多，包括多个局域网。
- 广域网 一般的广域网指的就是全球共享的 Internet 网络。

1.3.2 按数据组织方式分类

由于计算机网络的发展过程经历了很长的时间，期间由于技术的变更、功能的增强等原因，计算机网络的组织方式经历很多次的变革。这也就产生了按照组织方式区分计算机网络的分类方式，具体可以分为如下几类。

- 线路交换网络 早期运用在电话系统中，计算机网络在刚开始发展时也采用相同的方式来传输数据的，特点是数字信号经过变换成为模拟信号后在线路上传输。
- 报文交换网络 一种数字化网络。通信开始时，作为信号源的机器发出一个报文到交换器里并被交换器储存，而交换器根据此计算机发送的报文的目的地址选择路径发送这个报文，这种方式称为存储转发方式。
- 分组交换网络 同样采用报文传输，所不同的是不以不定长的报文作传输的基本单位，而是将一个长的报文划分为定长的报文加以分组，再以分组作为传输的基本单位，从而加速了信息在网络中的传播速度。由于分组交换网络的优越性，因此它已成为计算机网络的主流。

1.4 认识 Internet

Internet 是一组全球信息资源的总汇。有一种粗略的说法，认为 Internet 是由许多小的网络（子网）互连而成的一个逻辑网。每个子网中连接着若干台计算机（主机）。本小节所介绍的是一些关于 Internet 的基础知识，以便帮助读者学习后面的知识。

1.4.1 常用 Internet 的协议简介

目前，Internet 中常用的通信协议主要有 NetBEUI、IPX/SPX 和 TCP/IP 这 3 种。

1．NetBEUI 协议

NetBEUI（NetBIOS Extended User Interface，用户扩展接口）最早出现在 Windows 95/98 和 Windows NT 中，NetBEUI 被作为默认协议安装。NetBEUI 协议是为中小型局域网设计的，用单部命名（Single-Partnames）定义网络节点，它不支持多网段网络，也即通常所说的“不可路由”，这是 NetBEUI 不适合大型网络的一个重要原因。NetBEUI 协议也有它的优点，如安装非常简单、不需要进行配置、在 3 种协议中占用内存最少。

2．IPX/SPX 协议

IPX/SPX（Internetwork Packet eXchange / Sequences Packet eXchange，网际包交换/顺序包交换）是 Novell 公司早期开发的通信协议集。IPX/SPX 协议能够在十分复杂环境下使用。由于在设计之初就考虑了多网段的问题并具有很强的路由功能，所以使得 IPX/SPX 能够适应大型网络的使用。

IPX/SPX 协议是组建 NetWare 网络的最佳协议。但是在非 NetWare 网络环境中，一般不建议使用 IPX/SPX 协议。在 Windows NT 网络和由 Windows 95/98 组成的对等网中，必须使用微软公司提供的 NWLink 通信协议来实现与 NetWare 平台的互连（NWLink 通信协议中包括两个 IPX/SPX 的兼容协议：NWLink SPX/SPX 兼容协议和 NWLink NetBIOS 兼容协议），否则无法直接使用 IPX/SPX 通信协议的。

3．TCP/IP

TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议）是在 Internet 上广泛应用的一种网络通信协议，其优点是能够跨网段、跨系统使用。无论在 UNIX 系统、Windows 平台，还是局域网、广域网、Internet 网络，TCP/IP 都能够提供良好的网络支持，在现在的网络世界中，TCP/IP 作为一种通用的协议被广泛地使用。

同时 TCP/IP 也是一种可路由协议。TCP/IP 使用一种给网络中的每个网络节点配置一个 IP 地址、一个子网掩码、一个网关和一个主机名这种命名方式来管理网络上的计算机，这种方式容易确定网络和子网段之间的关系，从而获得很好的网络适应性、可管理性和较高的网络带宽使用效率。

它和 NetBEUI、IPX/SPX 协议相比较，TCP/IP 的配置和管理更加复杂。NetBEUI 和 IPX/SPX 及其兼容协议不需要进行配置就可以使用，而 TCP/IP 必须设置网络节点的“四要素”（IP 地址、子网掩码、默认网关和主机名）后才能使用，同时这也造成了管理上的不便。下面介绍一下 TCP/IP 的“四要素”。

- IP 地址 标明了计算机在网路上的位置。它分为网络地址和主机地址两部。完整的 IP 地址是一段 32 位（bit）二进制数，每 8 位（1 个字节）为一个段（Segment），分为 4 段，每段之间用“.”号隔开以示区别。但是由于二进制的复杂性，实际的 IP 地址是写为十进制的，如 192.168.0.1 等。
- 子网掩码 被用来界定 IP 地址的网络地址和主机地址的界限，并在多网段环境中扩展 IP 地址中的网络地址部分。
- 网关 连接了两个使用不同协议的网段。它的作用是翻译两个网段中所使用不同传输协议的数据，使这些不同协议的数据能够自由地相互通信，如运行 TCP/IP 的 Windows NT 和运行 IPX/SPX 协议的 NetWare 相互通信的时候，必须由网关设备作为中介，否则是不能完成数据交互的。
- 主机名 标明了网络中主机的身份，但是在实际的应用中，很多的用户发现 IP 地址不容易记忆，这使得对网络的相关操作变得非常不方便。根据这种情况，TCP/IP 采用了给网络中的主机命名的方法来对主机加以区分，体现这种功能的参数就是主机名。在网络中，主机名和相应的 IP 地址是一一对应的。

1.4.2 Internet 物理网的构成

支撑 Internet 的物理网可以分为两类。一类如以太网、FDDI（Fiber Distributed Data Interface）等的局域网，另一类如公共电话网、公共分组交换网、ISDN 等的广域网。对不同的物理网配以相应的网络接口协议，可使上层的网间协议运行在不同的物理网上，如当物理网是以太网时，网络接口协议须使用 IP-E（由 RFC894 规定）；而当物理网是 X·25 分组交换网时，须使用 IP-X·25（由 RFCI356 规定）等。

1.4.3 认识 IP 地址

为了识别接入 Internet 上的计算机主机，必须为这些计算机主机编号，而 IP 地址就是每个连接在 Internet 上的计算机主机编号的 32 位地址。

在 TCP/IP（Transport Control Protocol/Internet Protocol，传输控制协议/网际协议）中规定，IP 地址使用二进制来表示，每个 IP 地址的长度为 32 位，换算成字节，就是 4 个字节。例如一个采用二进制形式的 IP 地址是“00001010000000000000000000000001”。由于使用二进制表示的 IP 地址太过于冗长，所以 IP 地址被转换成十进制的形式表示，中间使用符号“.”分开不同的字节。根据这样的规则，上面的 IP 地址可以表示为“10.0.0.1”，这种表示法叫做“点分十进制表示法”。

在访问 Internet 时，一台计算机只能用一个 IP 地址来标识，但是同一台计算机在 Internet 上可以使用多个 IP 地址。也可以通过特定的技术，使多台服务器共用一个 IP 地址，这些服务器在用户使用的时候可以被看成一台网络主机。

为了更加方便地管理互联网的 IP 地址，国际上建立了一个叫 IANA（Internet Assigned Numbers Authority，互联网网络号分配机构）的组织来统一管理所有的 IP 地址。

由于分配不合理以及 IPv4 协议本身存在的局限，造成了互联网的 IP 地址资源越来越紧张，IANA 将 A、B、C 类 IP 地址的一部分保留下来，作为局域网使用的 IP 地址，保留 IP 地址的范围如下表所示，同时 IANA 还开发新的技术代替 IPv4 协议，如 IPv6。

表 1-1　　局域网使用的 ip 地址范围

网 络 类 别	IP 地址范围	网络容纳主机数
A 类网	10.0.0.0～10.255.255.255.255	1
B 类网	172.16.0.0～182.31.255.255	16
C 类网	192.168.0.0～192.168.255.255	255

所有保留的 IP 地址段不能够在互联网内被使用，在局域网与广域网相连的路由器处理保留的 IP 地址时，是将该数据包丢弃，而不会广播到广域网上去，从而起到了将保留 IP 地址产生的数据隔离在局域网内部的作用。

作为用户可以根据自己的实际情况选择所定义的 IP 地址段，一般来说，在局域网内计算机数量少于 254 台的情况下，可以在 C 类 IP 地址段里选择 IP 地址，如从“192.168.1.1”到“192.168.1.254”。

第2章 网络的构成

了解网络基本概念后，本章将介绍网络的构成。网络主要由软件和硬件两部分构成，软件主要是指 OSI 参考模型以及其中的各类网络协议；硬件主要指各种网络设备，如 Hub、交换机、网卡等。本章将依次详细介绍网络构成的常见部分。

2.1 OSI 参考模型

开放式系统互联模型（OSI）是 1984 年由国际标准化组织（ISO）提出的一个参考模型，作为一个概念性框架，它是不同制造商的设备和应用软件在网络中进行通信的标准。现在，此模型已成为计算机间和网络间进行通信的主要结构模型。目前使用的大多数网络通信协议的结构都是基于 OSI 模型的。

2.1.1 OSI 模型构成

OSI 将通信过程定义为 7 层，即将连网计算机间传输信息的任务划分为 7 个更小、更易于处理的任务组。每一个任务或任务组则被分配到各个 OSI 层，每一层都是独立存在的，因此分配到各层的任务能够独立地执行，这样当变更其中某层提供的方案时不影响其他层。

OSI 7 层模型的每一层都具有清晰的特征。基本上是，第 7 至第 4 层处理数据源和数据目的地之间的端到端通信，第 3 至第 1 层处理网络设备间的通信。另外，OSI 模型的 7 层也可以划分为两层：上层（层 7、层 6 和层 5）和下层（层 4、层 3、层 2 和层 1）。OSI 模型的上层处理应用程序问题，通常只应用在软件上，OSI 模型的下层是处理数据传输的。在网络中，OSI 模型中 7 层含义如表 2-1 所示。

表 2-1　　OSI 七层模型

层　数	含　义
7	应用层
6	表示层
5	会话层
4	传输层
3	网络层
2	数据链路层
1	物理层