大数据、云计算、人工智能、信息安全人才培养丛书
“互联网+”新形态一体化教材

计算机网络安全管理技术

王　亮　袁新颜　廖忠智／主编

中国科学技术出版社
CHINA SCIENCE AND TECHNOLOGY PRESS

大数据、云计算、人工智能、信息安全人才培养丛书
“互联网+”新形态一体化教材

计算机网络安全管理技术

王　亮　袁新颜　廖忠智／主编

中国科学技术出版社
·北　京·

图书在版编目（CIP）数据

计算机网络安全管理技术 / 王亮，袁新颜，廖忠智主编 . -- 北京 : 中国科学技术出版社，2024.3
ISBN 978-7-5236-0594-3

Ⅰ. ①计… Ⅱ. ①王… ②袁… ③廖… Ⅲ. ①计算机网络—网络安全 Ⅳ. ① TP393.08

中国国家版本馆 CIP 数据核字（2024）第 067469 号

策划编辑 王晓义
责任编辑 付晓鑫
装帧设计 唐韵设计
责任校对 张晓莉
责任印制 徐飞

出　　版 中国科学技术出版社
发　　行 中国科学技术出版社有限公司
地　　址 北京市海淀区中关村南大街 16 号
邮　　编 100081
发行电话 010–62173865
传　　真 010–62173081
网　　址 http://www.cspbooks.com.cn

开　　本 889mm × 1194mm　1/16
字　　数 400 千字
印　　张 14.5
版　　次 2024 年 3 月第 1 版
印　　次 2024 年 3 月第 1 次印刷
印　　刷 北京荣玉印刷有限公司
书　　号 ISBN 978–7–5236–0594–3/TP · 480
定　　价 49.80 元

编写委员会

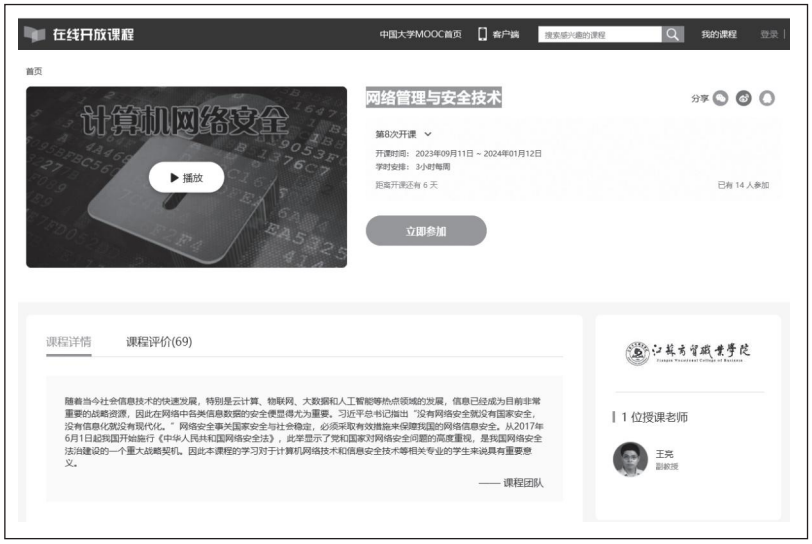
主　编　王　亮　袁新颜　廖忠智

副主编　邵鑫玉　顾玲玲

在线课程说明

本书配套中国大学 MOOC 在线开放课程“网络管理与安全技术”，读者可以通过中国大学 MOOC 在线学习。

进入中国大学 MOOC 在线开放课程官方网站，搜索课程名称“网络管理与安全技术”，选择对应课程，进入课程首页，注册登录后单击“立即参加”按钮即可加入相关课程在线学习。



前言

我国从 2017 年 6 月 1 日起开始施行《中华人民共和国网络安全法》，此举显示了党和国家对网络安全问题的高度重视，是我国网络安全法治建设的一个重大里程碑。习近平总书记指出：“没有网络安全就没有国家安全，没有信息化就没有现代化。”基于以上背景，网络安全管理技术在各行业中越来越受到重视。

本书理论联系实际，在进行充分专业调研的基础上，打破以知识传授为主要特征的传统学科教学模式，转变为以案例、任务和项目形式组织全书内容。本书在编写过程中坚持以能力为本位、以职业实践为主线、以项目为主体的模块化专业教学体系，让学生在学习具体案例、任务和项目的过程中熟悉相关理论知识，掌握计算机网络安全与维护的技能。此外，本书还以当前网络信息安全岗位中涉及的知识结构为依据，以计算机网络安全的典型实际工作项目为载体，将网络安全所需的安全理论知识和技术根据情境需要融入项目中，突出工作任务与知识的联系，让学生在完成工作任务的同时学习并掌握相关理论与操作方面的知识。

本书特色和创新点如下。

（1）贯彻落实党的二十大精神。本书在编写过程中坚持贯彻落实党的二十大精神，在讲解基础知识的同时，将网络强国战略、网络安全融入项目之中。在项目 1 中介绍了网络安全管理相关的法律法规，引导读者树立遵纪守法意识；在项目 2 中介绍了网络安全防护案例，引导读者关注网络安全问题；等等。本书还将 1+X 网络安全运维职业技能等级证书和信息安全等级保护测评知识的相关内容引入，其中包括网络安全基本理论、操作系统的安全配置和网络设备的安全管理等，让读者在网络信息安全行业可以有针对性地开展相关工作。

（2）理论与实际相结合。本书理论联系实际，以典型企业园区网络异地互联的综合项目案例为背景，展开网络安全技术与实施相关知识与技能的讲授。本书结合高职类院校学生的特点，以“项目引领、任务驱动”的模式来培养高素质技术技能型人才。

（3）采用现代化辅助教学。本书的主要任务均利用了仿真技术和虚拟化技术辅助教学，避免由于设备不足而使实训条件受限，读者可以利用单机环境及虚拟仿真软件完成

各个项目任务的学习。

（4）具有丰富的数字化教学资源。本书基于江苏省高校在线开放课程教学资源包，配有多媒体课件、教学视频和试题库等丰富的数字化资源。

本书的编写团队成员都是高职院校一线专业教学人员，他们长期从事信息安全与管理、计算机网络技术及相关专业的教学及科研工作，具有扎实的专业理论知识和实际操作技能、丰富的执教经验、较高的专业服务水平和较强的实践创新能力，团队成员曾多次主持省级相关课题，并参与编写省级重点教材。

由于时间仓促，且编者的水平有限，书中存在的疏漏和不妥之处，恳请各位读者批评、指正。

编　者

2023 年 8 月

目录

项目 4　操作系统的安全管理

项目 5　Web 应用的安全管理

项目 6 信息加密和身份认证技术的应用

项目 7 访问控制列表技术的应用

项目 1 网络安全管理概述

学习目标

知识目标

① 识记：网络安全的主要威胁；国内外网络安全发展现状及发展趋势；网络安全法的相关案例。

② 领会：网络安全的概念；网络安全法的性质、原则和作用。

能力目标

① 会正确安装和配置 VMware Workstation 软件。

② 会正确安装 Packet Tracer 软件并在其环境下搭建网络。

③ 会正确安装和配置 GNS3 软件并在其环境下模拟路由器、交换机和终端设备搭建网络。

素质目标

① 践行社会主义核心价值观，强化安全、文明、科学的上网意识。

② 通过学习网络安全知识，认识到网络安全的重要性，并树立正确的网络安全观。

③ 通过学习网络安全法律法规，做到遵纪守法。

项目引入

现代社会科学技术发展日新月异，信息互联网连接万物，生活中的方方面面都离不开网络。互联网在给人们带来方便快捷的同时，网络安全领域的潜在威胁也在日益增加。

党的十八大以来，我国不断完善网络安全工作顶层设计，有效治理网络空间乱象，推动我国网络安全体系的建立，推动网络强国建设。进入新时代以来，以《中华人民共和国网络安全法》为核心的网络安全法律法规和政策标准体系基本形成，国家网络安全标准体系日益健全。

我国从 2017 年 6 月 1 日起开始施行《中华人民共和国网络安全法》。《中华人民共和国网络安全法》明确了对个人信息的保护、对网络诈骗的打击，以及对破坏我国关键信息基础设施的境外组织和个人加强惩治。此举显示了党和国家对网络安全问题的高度重视，是我国网络安全法治建设的一个重大里程碑。“没有网络安全就没有国家安全，没有信息化就没有现代化”。习近平总书记深刻揭示了国家安全的时代内涵，开启了网络强国建设新征程。

某公司是国内一家从事网络工程建设及网络安全设计、网络安全施工，提供网络安全评估服务的高新技术公司。最近，该公司接到一个国内大型企业的网络信息安全建设项目。为了更好地开展该项目，该公司决定与校企合作单位某职业学院合作共同开展该项目，并委派具体负责项目的张工程师对该公司内部员工进行网络安全知识的培训。张工程师接到该任务后带领学生结合项目需求，制订了如下培训任务：

- 学习网络安全基础知识；
- 了解网络安全相关法律法规；
- 搭建网络安全实训平台。

任务 1.1 网络安全基础知识的认知

任务描述

在信息网络中，涉及个人隐私、企业机密、国家机密等各种敏感信息都有可能被不法分子窃取，网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。在本任务中，为了给公司员工普及网络安全意识，某职业学院学生协助张工程师完成网络安全基础知识的培训。在完成任务的过程中，能够了解网络安全的概念、网络安全的主要威胁种类、网络安全的发展历程及网络安全现状。

任务目标

（1）理解网络安全的定义、目标和特征。

（2）能正确区分网络安全的主要威胁种类。

（3）能描述网络安全的发展历程和现状。

相关知识

网络安全基础知识的认知 -1

网络安全基础知识的认知 -2

1. 网络安全的概念

（1）网络安全的定义。

狭义上，网络安全是指计算机及其网络系统资源和信息资源不受有害因素的威胁和危害。它包括硬件系统的安全、可靠运行、操作系统和应用软件的安全、数据库系统的安全和电磁信息泄露的防护等多个方面。狭义的网络安全侧重于网络传输的安全。

广义上，凡是涉及计算机网络信息安全属性特征的相关技术和理论，都属于网络安全的研究领域。它包括系统连续、可靠、正常地运行，网络服务不中断，系统中的信息不因偶然的或恶意的行为而遭到破坏、更改或泄露等。

网络安全问题包括两方面内容：一是网络的系统安全；二是网络的信息安全。网络安全的最终目标和关键是保护网络的信息安全。

（2）网络安全的目标。

网络安全的目标是在网络的信息传输、存储与处理的整个过程中，提高物理上和逻辑上的防护、监控、反应恢复和对抗的能力。

（3）网络安全的特征。

以下是网络信息安全的五大特征，反映了网络安全的具体目标要求。

①机密性，也称保密性，强调有用信息只被授权对象使用的安全特征。

②完整性，是指信息在传输、交换、存储和处理过程中，保持信息不被破坏或修改、不丢失和信息未经授权不能改变的特性，这也是最基本的安全特征。

③可用性，也称有效性，指信息资源可被授权实体按要求访问、正常使用或在非正常情况下能恢复使用的特性。

④可控性，是指信息系统对信息内容和传输具有控制能力的特性，指网络系统中的信息在一定传输范围和存放空间内的可控程度。

⑤可审查性，又称为拒绝否认性、抗抵赖性或不可否认性，指网络通信双方在信息交互过程中确信参与者本身和所提供的信息的真实同一性。

（4）网络安全的主要内容。

从层次结构上，可将网络安全所涉及的内容概括为以下 5 个方面。

①实体安全也称物理安全，指保护计算机网络设备、设施及其他媒介免遭地震、水灾、火灾、有害气体和其他环境事故破坏的措施及过程。它包括环境安全、设备安全和媒体安全 3 个方面。实体安全是信息系统安全的基础。

②运行安全包括内外网的隔离机制、应急处置机制和配套服务、网络系统安全性监测、网络安全产品运行监测、定期检查和评估、系统升级和补丁处理、跟踪最新安全漏洞、灾难恢复机制与预防、安全审计、系统改造、网络安全咨询等。

③系统安全主要包括操作系统安全、数据库系统安全和网络系统安全。系统安全以网络系统的特点、实际条件和管理要求为依据，通过有针对性地为系统提供安全策略机制、保障措施、应急修复方法、安全建议和安全管理规范等，确保整个网络系统的安全运行。

④应用安全由应用软件开发平台安全和应用系统数据安全两部分组成。应用安全包括应用软件的程序安全性测试分析、业务数据安全检测与审计、数据资源访问控制验证测试、实体的身份鉴别检测、业务现场的备份与恢复机制检查、数据的唯一性测试、数据的一致性测试、数据的防冲突测试、数据保密性测试、系统可靠性测试和系统的可用性测试等。

⑤管理安全主要指对人员及网络系统安全管理的各种法律、法规、政策、策略、规范、标准、技术手段、机制和措施等内容。管理安全具体包括法律法规、政策策略管理、规范标准管理、人员管理、应用系统使用管理、软件管理、设备管理、文档管理、数据管理、操作管理、运营管理、机房管理、安全培训管理等。

2. 网络安全的主要威胁

网络安全的主要威胁表现在主机可能会受到非法入侵者的攻击，网络中的敏感数据有可能泄露或被修改，从内部网向公共网传送的信息可能被他人窃取或篡改等。表 1–1 列出了典型的网络安全威胁种类。

表 1–1　典型的网络安全威胁种类

威胁类型	威胁描述
非授权访问	通过口令、密码和系统漏洞等手段获取系统访问权
窃听	窃听网络传输信息
伪造	将伪造的信息发送给他人
篡改	攻击者对合法用户之间的通信信息篡改后，发送给他人
窃取	盗取系统重要的软件或硬件、信息和资料
截获 / 修改	数据在网络系统传输中被截获、删除、修改、替换或破坏
讹传	攻击者获得某些非正常信息后，发送给他人

续表

威胁类型	威胁描述
行为否认	通信实体否认已经发生的行为
旁路控制	利用系统的缺陷或安全脆弱性的非正常控制
人为疏忽	已授权人为了利益或由于疏忽将信息泄漏给未授权人
信息泄露	信息被泄露或暴露给非授权用户
病毒木马	利用计算机木马病毒及恶意软件进行破坏或恶意控制他人系统
拒绝服务攻击	攻击者以某种方式使系统响应减慢甚至瘫痪，阻止用户获得服务
资源耗尽	故意超负荷使用某一资源，导致其他用户服务中断
信息重发	重发某次截获的备份合法数据，获取信任以实现恶意的目的
信息战	为了国家或集团利益，通过信息战进行网络干扰破坏或恐怖袭击

3. 网络安全的发展历程

（1）通信安全时期。

该时期主要标志是 1949 年香农（C. E. Shannon）发表的《保密系统的通信理论》。这个时期通信技术还不发达，计算机只是零散地位于不同的地点，信息系统的安全仅限于保证电脑的物理安全以及通过密码解决通信安全的保密问题，密码技术获得发展，欧美国家有了信息安全产业的萌芽。

（2）计算机安全时期。

该时期以 1983 年美国国家计算机安全中心（NCSC）公布的可信计算机系统评估准则（trusted computer system evaluation criteria, TCSEC）为标志。半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段。人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标，中国信息安全开始起步，并开始关注物理安全、计算机病毒防护等。

（3）网络安全时期。

该时期是在 20 世纪 90 年代兴起的。由于互联网技术的飞速发展，无论是企业内部信息还是外部信息都得到了极大的开放，而信息安全的焦点已经从传统的保密性、完整性和可用性 3 个原则衍生为诸如可控性、抗抵赖性、真实性等其他的原则和目标。中国安全企业研发的防火墙、入侵检测、安全评估、安全审计、身份认证与管理等产品与服务百花齐放，百家争鸣。

（4）信息安全保障时期。

该时期以 21 世纪的《信息保障技术框架》（IATF）为标志。面向业务的安全防护已经从被动走向主动，安全保障理念从风险承受模式走向安全保障模式。不断出现的安全体系与标准、安全产品与技术带动信息安全行业形成规模，入侵防御、下一代防火墙、APT 攻击检测、MSS/SaaS 服务等新技术、新产品、新模式走上舞台。

4. 国内外网络安全发展现状

（1）国外发展现状。

国外发达国家对网络安全的建设主要体现在以下 8 个方面。

①完善法律法规和制度建设。

②信息安全保障体系。

③网络系统安全测评。

④网络安全防护技术。

⑤故障应急响应处理。

⑥网络系统生存措施。

⑦安全信息关联分析。

⑧密码新技术研究。

（2）国内发展现状。

我国非常重视网络安全建设，虽然起步比较晚，但是发展很快，网络安全建设的发展情况体现在以下 6 个方面。

①加强网络安全管理与保障。

②安全风险评估分析。

③网络安全技术研究。

④网络安全测试与评估。

⑤应急响应与系统恢复。

⑥网络安全检测技术。

任务进阶

学习网络安全的相关案例。

（1）揭露地下黑产，央视曝光网上贩卖个人信息新闻。

2017 年 2 月，央视新闻频道报道了央视记者亲身体验购买个人信息服务，揭秘个人信息泄露黑市状况的新闻。记者暗访得知，在这一地下黑产交易时，只提供一个手机号码，就能买到一个人的身份信息、通话记录、位置信息等多项隐私数据。个人信息的泄露会带来各种隐患，如果不加以整治，势必会影响整个社会治安，威胁到公民的人身安全。

（2）某官方网站再现安全漏洞。

2017 年 4 月，某记者在某官方网站订票时发现，当退出个人账号时，网站页面竟然自动登录他人账号，且与账号相关联的身份证号、联系方式等个人信息均可查看。随后记者在该页面点击常用联系人选项时，页面再次刷新并显示他人账号及账号涵盖的所有信息。记者尝试在网站账户页面的个人信息栏等其他选项进行操作，点击进入后均可得到不同的个人身份信息。

（3）勒索病毒模仿热门手游辅助工具袭击手机。

某款游戏不光吸粉能力超强，吸引病毒的能力也非同一般。2017 年 6 月，某手机卫士发现了一款冒充热门手游辅助工具的手机勒索病毒。该勒索病毒被安装进手机后，会对手机中照片、下载、云盘等目录下的个人文件进行加密，并索要赎金。这种病毒一旦暴发，会威胁几乎所有安卓平台的手机，用户一旦中招，可能丢失所有个人信息。

任务 1.2 网络安全法律法规的认知

任务描述

网络安全法律体系是网络法律体系的重要组成部分。网络安全法律体系是由保障网络安全的法律、行政法规和部门规章等多层次规范相互配合的法律体系。网络安全法律体系重点涵盖网络主权、网络关键基础设施保护、网络运行安全、网络监测预警与应急处置、网络安全审查、网络信息安全以及网络空间各行为主体权益保护等制度。在本任务中，某职业学院学生协助张工程师完成网络安全法律法规相关知识的培训。在完成任务的过程中，学生能够了解网络安全法的性质和特征，熟悉其作用、原则，阅读网络安全相关案例，对网络安全法律法规有一个较为深入的认知。

任务目标

（1）理解网络安全领域相关的法律法规。

（2）了解网络安全法的作用和原则。

网络安全法律法规的认知

相关知识

1. 网络安全法的基本介绍

（1）《中华人民共和国网络安全法》介绍。

为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，国家制定了《中华人民共和国网络安全法》。计算机入侵、制作和传播计算机病毒等威胁信息安全的行为与传统犯罪相比，信息犯罪所涉及的财产数额更大，因而其社会危害性更加明显。一次计算机犯罪往往给社会造成几十万、上百万乃至上亿元的巨额损失，因此网络安全法律法规的制定显得尤为必要。《中华人民共和国网络安全法》发挥了重要的基础性立法作用，为大量的执法活动提供了有力依据，初步实现了维护我国网络安全的既定目标。

（2）保护网络安全的其他法律。

在网络安全管理方面有大量的法律、法规，起着保护网络安全的基础性作用。最为典型的是《中华人民共和国电子签名法》和《中华人民共和国个人信息保护法》。《中华人民共和国电子签名法》由中华人民共和国第十届全国人民代表大会常务委员会第十一次会议于 2004 年 8 月 28 日通过，自 2005 年 4 月 1 日起施行，是一部规范我国电子商务发展的基础性法律。

2. 网络安全法的特征

网络安全立法的目的是维护网络空间的正常秩序，保障信息网络的安全，维护当事人的合法权益。网络安全立法具备以下特征。

（1）技术性。

所谓技术性是指网络安全法是立足信息技术而构建的法律规范。我国在进行网络安全立法时，适应了网络发展的特点，在研究国际立法的基础上，借鉴其先进、科学的法律制度，力求达到与国际标准相统一，避免因法律制度的差异而阻碍网络的应用和发展。

（2）开放性。

所谓开放性是指网络安全法在具体的法律规范的设计上表现出一定的宏观性，这样可以保持网络安全法具有一定的开放性，给今后的发展和适用均预留一定的空间。宏观性和可操作性并不矛盾，对于已经确定的情况，应构建便于操作的具体规范。从维护信息安全的角度出发，保护当事人的正当权益，制定的规范便于当事人的起诉，也便于司法机关办案。

（3）兼容性。

兼容性是针对传统法而言的，是指网络安全法与现有的法律体系相协调一致的特性。计算机网络构筑了一个不同于以往的网络空间，网络空间具有一定的虚拟性。但网络毕竟不是脱离物理空间存在的独立世界，网络只是现实世界的自然延伸和发展。因此网络安全立法不能完全脱离现有法律另起炉灶，而应当针对危害信息安全的新行为做出新的规定，同时又要与现有的法律相协调，尤其是基本的法学理念和法律规范仍应予以继承，从而更好地保护当事人的合法权益。

3. 网络安全法的作用和原则

（1）网络安全法的基本作用。

网络安全法在信息时代起着重要的作用，具体体现在以下几个方面。

①指引作用。法律作为一种行为规范，为人们提供了某种行为模式，指引人们可以实施某种行为，必须实施某种行为或不得实施某种行为。

②评价作用。法律具有判断、衡量他人行为是否合法的评判作用。

③预测作用。当事人可以根据法律规范预先估计他们应该如何实施行为以及实施某种行为时所承担的法律后果。

④教育作用。通过法律的实施对一般人的行为产生影响。

⑤强制作用。法律对违法行为具有制裁、惩罚的作用。

（2）网络安全法的基本原则。

网络安全法的基本原则是贯穿于网络安全立法、执法、司法各个环节，在信息安全法律法规制定过程中必须贯彻和遵循的基本规则，它主要包括以下几条原则。

①预防为主的原则。从手段上讲，积极预防的方式和过程一般会比产生消极后果再补救要简单和轻松许多；另外，从后果上看，各种信息数据一旦被破坏或者泄露，往往会造成难以弥补的损失，因此保障网络信息安全的关键在于预防。

②突出重点的原则。在网络安全法中，凡涉及国家安全和建设的关键领域的信息，或者对经济发展和社会进步有重要影响的信息，都应有明确、具体、有效的法律规范加以保障。在网络安全保密工作中，也应突出重点。如果不区分重点，就会使国家的核心秘密与一般秘密混同，威胁核心秘密的安全。

③主管部门与业务部门相结合的原则。由于涉及领域广泛，网络安全法更显现出其兼容性和综合性。通常，不同领域的管理部门一般负责其相应领域的信息安全管理工作，并对因管理不善造成的后果承担法律责任。网络信息安全法在很多方面体现出主管部门与业务部门相结合的原则。

④依法管理的原则。“三分技术，七分管理”这个在其他领域总结出来的实践经验和原则在信

息安全领域同样适用。对于网络信息安全，不能仅仅强调技术，仅仅依靠网络自身的力量，更应该加强监管、依法管理。

⑤维护国家安全和利益的原则。当前，对重要信息的窃密活动数量日益增加，不仅从原来的政治、军事领域扩大到经济、科技、文化等领域，而且窃密手段越来越多种多样，严重威胁着国家安全和利益。信息安全保密法特别强调维护国家安全和利益的原则。这一原则不仅是保密工作的一项重要的指导思想，而且是信息安全保密法的首要基本原则。

任务进阶

学习网络安全法的相关案例。

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施。这是我国网络领域的基础性法律，明确了对个人信息的保护，对网络诈骗的打击，以及对破坏我国关键信息基础设施的境外组织和个人加强惩治。下面通过几个案例了解一下《中华人民共和国网络安全法》如何为公共信息安全护航，它的实施又将带来哪些影响。

（1）案例一：网站违法收集、留存公民个人信息。

2018 年 4 月，河南某公司存在 Weblogic 反序列漏洞，可致大量公民个人信息泄露，并且该公司未经用户同意违法违规收集、留存大量公民个人信息，未采取技术措施和其他必要措施确保相关公民个人信息安全，未按规定留存相关的网络日志不少于 6 个月。根据《中华人民共和国网络安全法》之规定，依法对该公司罚款 5 万元、对直接责任人董某罚款 1 万元。

（2）案例二：网站因高危漏洞遭入侵被罚。

2017 年 7 月，宜宾市翠屏区“教师发展平台”网站因网络安全防护工作落实不到位，导致网站存在高危漏洞，造成网站被黑客攻击入侵的网络安全事件。宜宾网安部门在对事件进行调查时发现，该网站自上线运行以来，始终未进行网络安全等级保护的定级备案、等级测评等工作，未落实网络安全等级保护制度，未履行网络安全保护义务。根据《中华人民共和国网络安全法》第五十九条第一款之规定，决定给予翠屏区教师培训与教育研究中心和直接负责的主管人员法定代表人唐某某行政处罚，对翠屏区教师培训与教育研究中心处 1 万元罚款，对法人代表唐某某处 5000 元罚款。

（3）案例三：网络公司为留存用户登录日志被查处。

2018 年 2 月，重庆公安局网安总队在日常检查中发现，重庆市某科技发展有限公司自《中华人民共和国网络安全法》正式实施以来，在提供互联网数据中心服务时，存在未依法留存用户登录相关网络日志的违法行为。公安机关根据《中华人民共和国网络安全法》相关规定，决定给予该公司警告处罚，并责令其 15 日内进行整改。

（4）案例四：网站违规发布时政类新闻信息。

2018 年 4 月，“上海爆料城”网站违规发布大量时政类新闻信息，传播虚假不实信息，严重扰乱互联网信息传播秩序，社会影响恶劣。根据《中华人民共和国网络安全法》《互联网信息服务管理办法》等法律法规，上海市网信办会同上海市通信管理局依法注销“上海爆料城”网站备案，停止网站接入并将其域名列入黑名单，停止域名解析。

任务 1.3 网络安全实训平台的搭建

任务描述

在本任务中，某职业学院学生协助张工程师完成网络安全实训平台搭建的培训。本任务包括 VMware Workstation 的安装和使用、Packet Tracer 的安装和使用，以及 GNS3 的安装和使用 3 个子任务。在完成任务的过程中，能够安装和使用 VMware Workstation、Packet Tracer、GNS3 软件，了解它们的作用和特点，并学会正确安装和常规配置。

任务目标

（1）正确安装 VMware Workstation 软件，并掌握使用方法。

（2）正确安装 Packet Tracer 软件，并掌握其环境下搭建网络的方法。

（3）正确安装 GNS3 软件，掌握关联 VMware Workstation 的方法并模拟路由器、交换机、设备终端搭建网络。

子任务 1 VMware Workstation 的安装和使用

任务环境

（1）主流计算机。

（2）VMware Workstation 安装文件。

（3）Windows 操作系统镜像文件。


VMware Workstation 的安装和使用 -1


VMware Workstation 的安装和使用 -2

相关知识

1. VMware Workstation 软件简介

VMware Workstation 是一款功能强大的桌面虚拟计算机软件，提供用户可在单一的桌面上同时运行不同的操作系统和进行开发、测试、部署新的应用程序的最佳解决方案。VMware Workstation 可在一台实体机器上模拟完整的网络环境，以及可便于携带的虚拟机器，其更好的灵活性与先进的技术胜过了市面上其他的虚拟计算机软件。

2. VMware Workstation 软件特点

VMware Workstation 的特点主要包括：计算机虚拟能力、性能与物理机隔离效果非常优秀；功能全面，适合计算机专业人员使用；操作界面简单明了，适用各种计算机领域的用户；但是体积庞大，安装时间耗时较久，使用时占用物理机资源较大。对于企业的 IT 开发人员和系统管理员而言，VMware 在虚拟网络、实时快照、拖曳共享文件夹和支持 PXE 等方面的特点使它成为必不可少的工具。

3. VMware Workstation 软件功能

（1）不需要重新开机就能在同一台电脑上使用多个操作系统。

（2）不需要分区就能在同一台电脑上使用两种以上的操作系统。

（3）完全隔离并且保护不同操作系统的操作环境以及所有安装在操作系统上面的应用软件和资料。

（4）不同的操作系统之间能进行互动操作，包括网络周边文件分享以及复制、粘贴等功能。

（5）有复原（Undo）功能。

（6）能够设定并且随时修改操作系统的操作环境，如内存、磁盘空间和周边设备等。

任务实施

1. VMware Workstation 软件的安装

（1）双击 VMware Workstation 的安装文件，弹出安装界面，在安装界面中单击“下一步”进入许可协议界面。

（2）在最终许可协议界面勾选“我接受许可协议中的条款”进入安装位置设置界面。

（3）在界面中选择安装路径，可以根据情况自行选择，选择好后单击“下一步”按钮出现安装界面，单击“安装”按钮，软件开始安装。

（4）安装完成后，输入许可证密钥，便进入 VMware Workstation 的主界面，如图 1-1 所示。

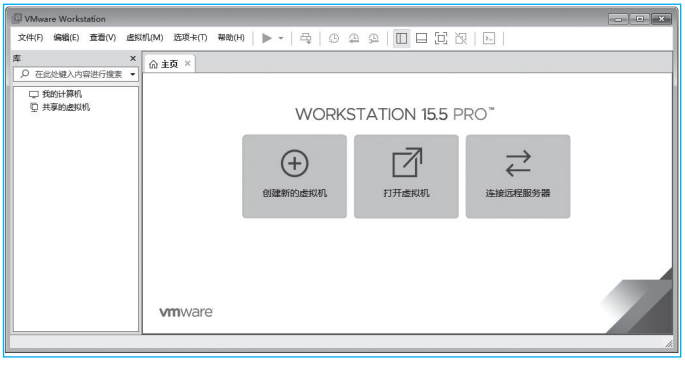


图 1-1　VMware Workstation 主界面

VMware Workstation 的主界面共分为四个部分，上面左侧为菜单栏，右侧为工具栏，左面显示安装的虚拟机信息，右面为工作区。下面来介绍在 VMware Workstation 环境下安装操作系统的过程。

2. 在 VMware Workstation 环境下安装操作系统

（1）选择软件菜单栏中的“文件”→“新建虚拟机”，进入新建虚拟机向导界面。

（2）在新建虚拟机向导中选择安装程序光盘映像文件，输入虚拟机名称和安装路径并设置虚拟机硬件，如图 1–2 所示。

（3）操作完成后单击完成按钮，开始进入安装操作系统的界面，如图 1–3 所示。

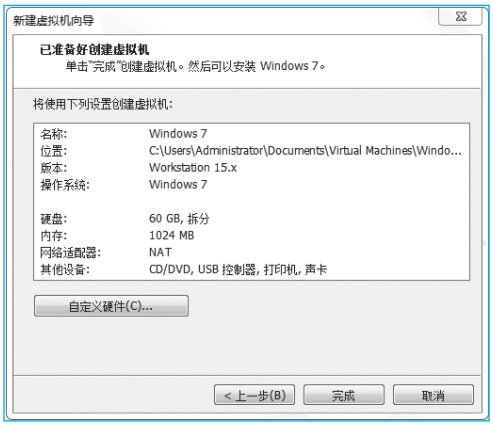


图 1–2　新建虚拟机

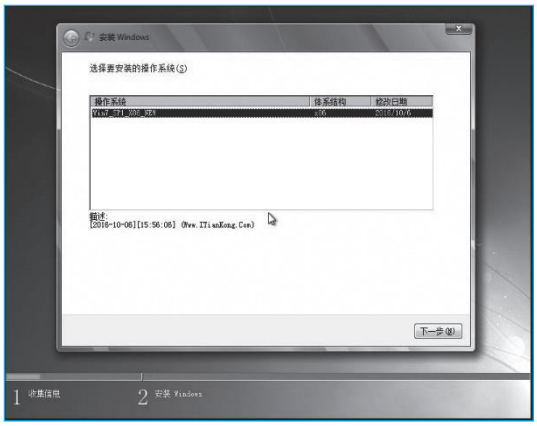


图 1–3　VMware Workstation 安装操作系统

3. VMware Workstation 的基本配置

（1）虚拟机参数的配置。

选择要配置的虚拟机，单击菜单栏中的“虚拟机”→“设置”，软件会出现如图 1–4 所示的界面。在其中可以对该虚拟机的内存、CPU、硬盘和网络等参数进行设置。内存、CPU 和硬盘等参数只需要调整其大小即可，比较简单。而网络参数的设置则相对比较复杂。在 VMware 中给出了桥接模式、NAT 模式、仅主机模式和自定义模式四种模式，一般使用比较多的是桥接模式和主机模式。

在桥接模式下，虚拟机网卡的 IP 地址和真实主机要设在同一 IP 段，这种情况适合局域网，而且在网内没有特别限制的情形下使用，也适合与真实主机或局域网内主机进行网络共享；在主机模式下，虚拟机网卡的 IP 地址和真实主机的 VMnet1 网卡的 IP 地址要设在同一 IP 段，这种情况比较适合于测试和实训。

（2）创建和恢复虚拟机“快照”。

选择要配置的虚拟机，依次单击菜单栏中的“虚拟机”→“快照”→“快照管理器”，软件会出现如图 1–5 的界面。在快照管理器中可以创建、恢复和删除快照。虚拟机“快照”功能相当于系统还原，而且原速度非常快，在测试和实训环境中非常实用。

图 1–4　虚拟机参数配置

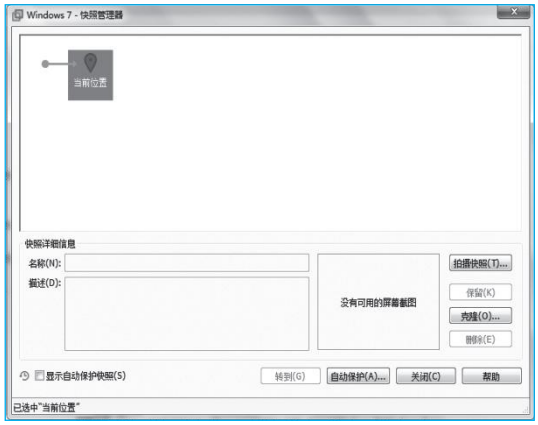


图 1–5　虚拟机快照管理器

（3）虚拟机的文件共享。

①网络共享：无论采用桥接模式还是采用主机模式，只要设置了正确的 IP 参数后，都可以用网络共享的方式对文件进行传输。

②安装 VMware Tools：进入需要安装的虚拟机后，在菜单栏中选择“虚拟机”→“安装 VMware Tools”便可安装 VMware Tools，如图 1–6 所示。安装完成后物理主机内的文件就可以通过拖曳的方法将文件复制到虚拟机中，此方法非常简单方便，也最为常见。

图 1–6　安装 VMware Tools

③使用共享文件夹：选择要配置的虚拟机，单击菜单栏中的“虚拟机”→“设置”后，选择选项栏，在左侧栏中选择共享文件夹选项，此时可以在将物理主机中的文件夹共享至虚拟机中，如图 1–7 所示。

④使用 USB 控制器：如果在虚拟机设置中安装了 USB 控制器，并勾选了“自动连接新的 USB 设备”选项后，如图 1–8 所示，插入 U 盘或 USB 移动硬盘后，虚拟机就可以识别 USB 设备并加载驱动，之后就可以像物理主机那样使用 USB 设备。

图 1–7　配置虚拟机共享文件夹

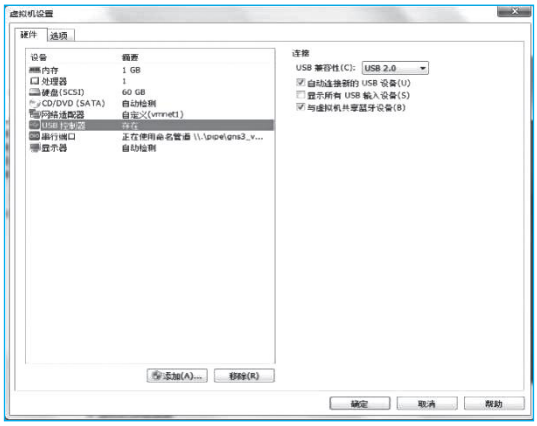


图 1–8　配置虚拟机 USB 控制器

子任务 2　Packet Tracer 的安装和使用

任务环境


Packet Tracer 的安装和使用 -1


Packet Tracer 的安装和使用 -2

（1）主流计算机。

（2）Packet Tracer 安装文件。

相关知识

1. Packet Tracer 软件简介

Packet Tracer 是一款网络学习模拟器，是由思科公司发布的一个辅助学习工具，为学习思科网络课程的初学者去设计、配置、排除网络故障提供了网络模拟环境。用户可以在软件的图形用户界面上直接使用拖曳方法建立网络拓扑，并可提供数据包在网络中行进的详细处理过程，观察网络实时运行情况，可以学习 IOS 的配置、锻炼故障排查能力。

2. Packet Tracer 软件特点

Packet Tracer 是一个功能强大的网络仿真程序，允许学生在其中搭建网络拓扑，并对数据包进行跟踪，提供仿真、可视化、编辑、评估和协作能力，有利于复杂的技术概念的学习。Packet Tracer 中存在几乎无限数量允许学生使用的设备，并鼓励其实践、发现和故障排除。基于仿真的学习环境，可以帮助学生发展创造性和批判性思维，掌握技能并解决问题。Packet Tracer 有利于教师的教学，表现出复杂的技术概念和网络系统的设计。

3. Packet Tracer 软件作用

Packet Tracer 在学习和教育网络技术方面起着至关重要的作用。它通过虚拟仿真实现了真实网络的操作和测试，使得用户能够更深入地了解网络的原理和操作。在各高校和职业培训中，Packet Tracer 被广泛应用于教育和研究。它可以帮助学生和教师更好地理解和实践各种网络技术，提高教学质量和学生的实际操作能力。此外，企业和机构也可以利用 Packet Tracer 进行系统测试和诊断，从而提高网络的可靠性和性能。

任务实施

1. Packet Tracer 软件的安装

（1）双击 Packet Tracer 的安装文件，软件会弹出安装界面，在安装界面中单击“Next”按钮，进入许可协议界面。

（2）勾选接受许可协议后面的单选框，单击“Next”按钮，在出现的界面中选择安装路径，可以根据情况自行选择，选择好后单击“Next”按钮，出现安装界面，单击“Install”按钮，软件开始安装。

（3）安装完成后，便进入 Packet Tracer 的主界面，如图 1–9 所示。

Packet Tracer 的主界面主要分为四个部分：应用程序管理区、工作区、设备选择区和设备操作管理区。

①应用程序管理区：包括标题栏、菜单栏和工具栏，用户可以使用其进行文件的保存、复制、移动等操作。

②工作区：软件的核心区域，在其中显示计算机网络逻辑拓扑结构，用户可以按需设计各种计算机网络拓扑结构，并对每个设备进行功能配置。

③设备选择区：包括各种类型的网络设备，用户可以从其中选择相应的设备，并将其拖至工作区中。

④设备操作管理区：包括选择设备、移动设备、删除设备、查看信息和绘图等功能，方便用户对工作区内的设备进行操作。

图 1–9　Packet Tracer 主界面

2. 在 Packet Tracer 环境下搭建网络

如图 1–10 所示为网络拓扑图，表 1–2 为其 IP 地址分配表。

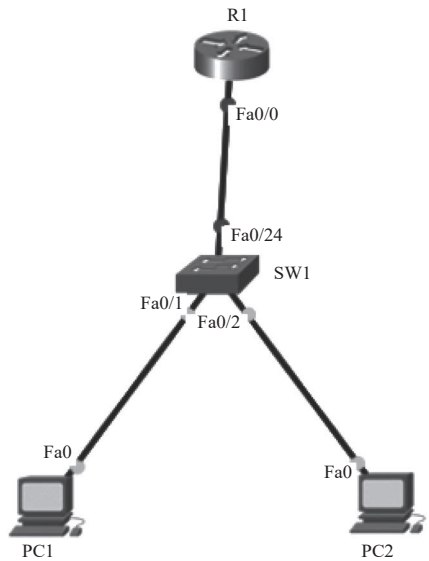


图 1-10　Packet Tracer 环境下搭建的网络拓扑图

表 1–2　Packet Tracer 环境下搭建的网络 IP 地址分配表

设备名	接口	IP 地址 / 子网掩码	默认网关
R1	Fa0/0	192.168.1.254/24	—
PC1	Fa0	192.168.1.1/24	192.168.1.254
PC2	Fa0	192.168.1.2/24	192.168.1.254

（1）绘制网络拓扑图。

首先在设备选择区的网络设备内分别选择路由器 2811 和交换机 2960，将它们添加到工作区，在终端设备内选择个人电脑添加到工作区，在连接线缆中选择合适的线缆将各种设备连接起来。然后，在设备操作管理区内使用工具对工作区内的设备进行标记。最后，选择应用程序管理区的菜单栏中的 Options → Preferences 选项，在其中勾选“Always Show Port Labels in Logical Workspace”选项，同时去掉“Show Device Model Labels”和“Show Device Name Labels”选项，即可绘制出网络拓扑图。

（2）配置网络设备。

单击工作区内的路由器 R1，在弹出的文本框中选择“CLI”选项，在进入的界面中输入“no”，屏幕显示“Router>”，此时便进到了路由器配置界面，如图 1–11 所示。

以下是路由器 R1 的配置命令。

```
Router>en
Router#conf t
Router(config)#host R1
// 配置路由器主机名
R1(config)#int f0/0
R1(config-if)#ip add 192.168.1.254 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
// 配置路由器接口地址
```

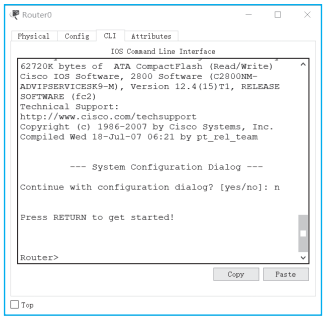


图 1–11　Packet Tracer 环境下网络设备配置界面图

（3）配置终端设备。

单击工作区内的个人电脑 PC1，在弹出的文本框中选择 Desktop 选项，然后再选择 IP Configuration 选项，在其中根据表 1–2 输入 IP 地址、子网掩码和默认网关，如图 1–12 所示。类似的方法配置 PC2。

（4）验证设备间的连通性。

以 PC1 为例，单击工作区内的个人电脑 PC1，在弹出的文本框中选择“Desktop”选项，然后再选择“IP Configuration”选项中的“Command Prompt”选项，在其中使用 ping 命令来验证设备间的连通性。如图 1–13 所示，PC1 和 PC2 之间已经互相连通。

（5）保存文件。

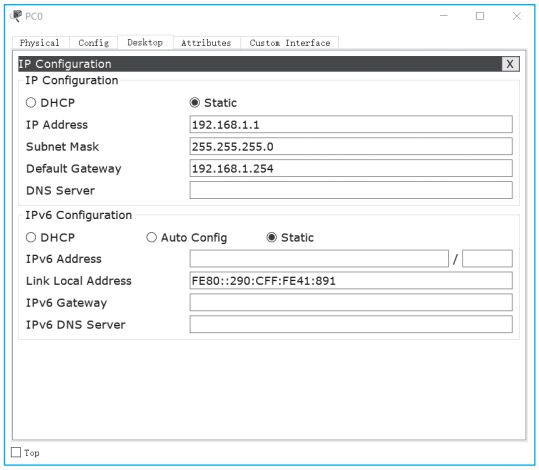


图 1-12　Packet Tracer 环境下终端设备配置界面

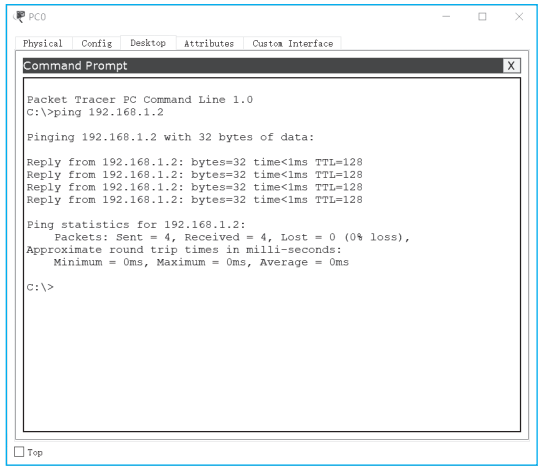


图 1-13　Packet Tracer 环境下验证连通性界面

配置完成后，首先要保存每个网络设备的配置，然后再选择菜单栏或者工具栏中的“保存”选项即可保存文件。

子任务 3　GNS3 的安装和使用

任务环境

（1）主流计算机。
（2）GNS3 安装文件。
（3）VMware Workstation。
（4）GNS3 VM 文件。
（5）IOU 镜像文件和 IOS 镜像文件。

GNS3 的安装和使用 -1　GNS3 的安装和使用 -2　GNS3 的安装和使用 -3

相关知识

1. GNS3 软件简介

GNS3 是一款具有图形化界面、可以运行在多平台（包括 Windows、Linux 和 Mac OS 等）的网络虚拟软件。思科网络设备管理员和想要通过 CCNA、CCNP、CCIE 等思科认证考试的相关人士可以通过它来完成相关的实验模拟操作。同时它也可以用于虚拟体验 IOS 或者是检验将要在真实的路由器上部署实施的相关配置。

2. GNS3 软件特点

GNS3 软件的特点包括如下几个。
（1）设计优秀的网络拓扑结构。

（2）模拟 Cisco 路由设备和 PIX 防火墙。

（3）仿真简单的 Ethernet、ATM 和帧中继交换机。

（4）能够装载和保存为 Dynamips 的配置格式，也就是说对于使用 Dynamips 内核的虚拟软件具有较好的兼容性支持一些文件格式（JPEG，PNG，BMP and XPM）的导出。

3. GNS3 软件功能

GNS3 软件从 1.0 版本后最大的特点是整合了 IOU 和 VMware 的功能。IOU 即 IOS running in Unix，最初是由思科内部人员开发来测试 IOS 的平台，后来流传到互联网经用户改进有了后来的 WEB IOU。GNS3 的 IOU 相比 WEB IOU 在拓扑的构建方面方便灵活了很多。IOU 的后端运行环境是基于 Unix 的操作系统，该系统可以运行在 Oracle VirtualBox 或者 VMware 的虚拟机上。因为是把 IOU 镜像运行在 Unix 系统上，所以对物理机资源的占用需求非常低。

任务实施

1. GNS3 软件的安装

（1）双击 GNS3 的安装文件，弹出安装界面，在安装界面中单击“Next”按钮，进入许可协议界面。

（2）在许可协议界面中单击“I Agree”按钮后，出现安装组件的界面。在此界面中选择需要安装的组件，一般选择默认即可，选择好后单击“Next”按钮，出现选择安装路径界面。

（3）在此界面上选择安装路径，可以根据情况自行选择，选择好后单击“ Install”按钮，软件开始安装。

（4）安装完成后单击 Finish 按钮便进入 GNS3 的主界面，如图 1–14 所示。

GNS3 的主界面默认分为 4 个面板：左侧的面板列出了可用的节点类型，包括各种路由器、交换机和防火墙等图标，当需要搭建拓扑时，便可以从这里拖曳出设备；右侧面板提供拓扑汇总概要信息和服务器汇总概要信息；中间部分包括两个面板，上面的面板是工作区，也是核心部分，用于图形化显示拓扑结构，下面的面板为 console 面板，显示设备工作信息，该面板不常用，可以关闭。

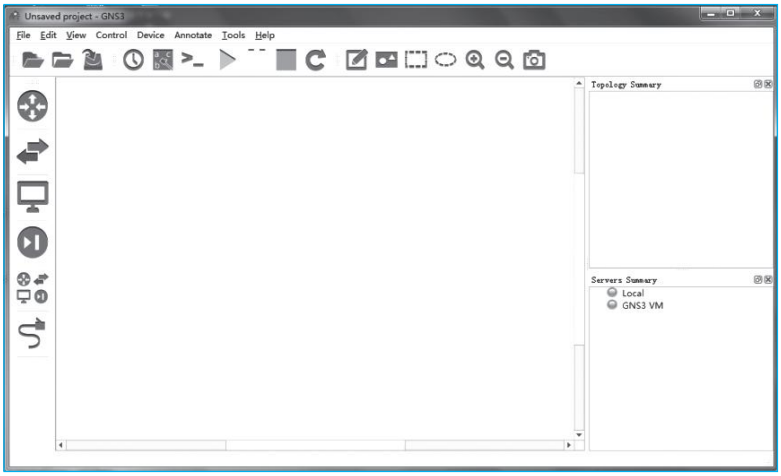


图 1–14　GNS3 主界面

2. GNS3 软件的配置

（1）GNS3 与 VMware Workstation 的关联。

打开 VMware Workstation 软件，依次单击菜单栏的“文件”→“打开”，选择 GNS3 VM 文件，在其中输入虚拟机名称和虚拟机的存储路径后单击“导入”按钮，如图 1–15 所示。

打开 GNS3 软件，在菜单栏中选择“ Help”→“ Setup Wizard”选项，打开 GNS3 配置向导界面，选择 Local GNS3 VM 后单击“ Next”按钮，在出现的界面中设置 GNS3 VM 环境后，单击“ Next”按钮，在 VMware Workstation 环境中就会自动运行 GNS3 VM 虚拟机，运行完成后软件会显示如图 1–16 所示的界面。

图 1–15　导入 GNS3 VM

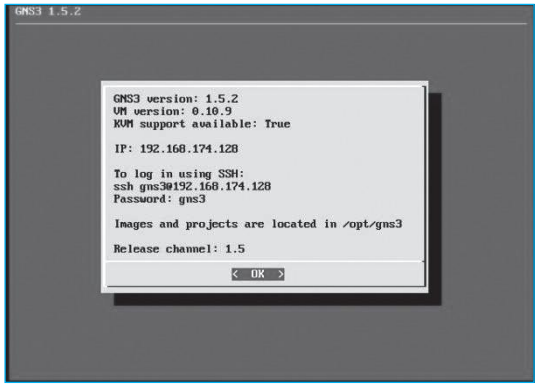


图 1–16　GNS3 VM 运行界面

（2）添加 IOS 设备。

①在如图 1–17 所示的界面上选择 IOS 设备的镜像文件。

②设置 IOS 设备名称、内存大小以及接口模块等。

③在如图 1–18 所示的界面上计算 Idle-PC 值后，IOS 设备即可完成添加。

（3）添加 IOU 设备。

①选择 IOU 设备的镜像文件，如图 1–19 所示为添加二层 IOU 设备，如图 1–20 所示为添加三层 IOU 设备。

②导入 IOU 许可文件，如图 1–21 所示。

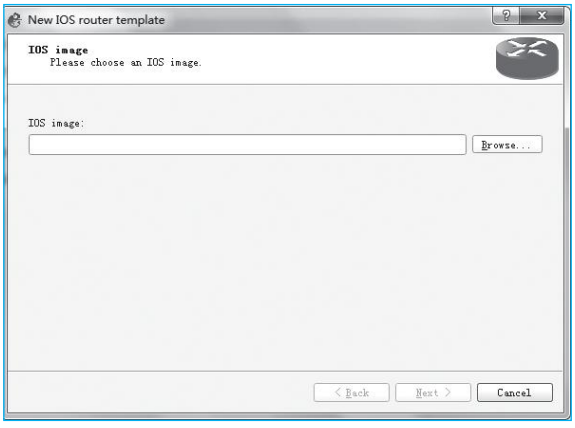


图 1–17　选择 IOS 设备镜像文件

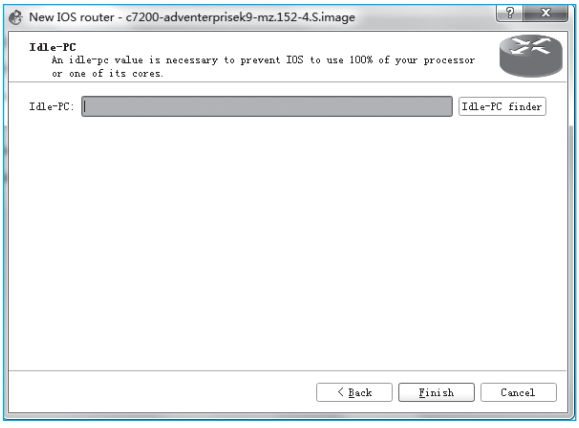


图 1–18　计算 Idle-PC 值

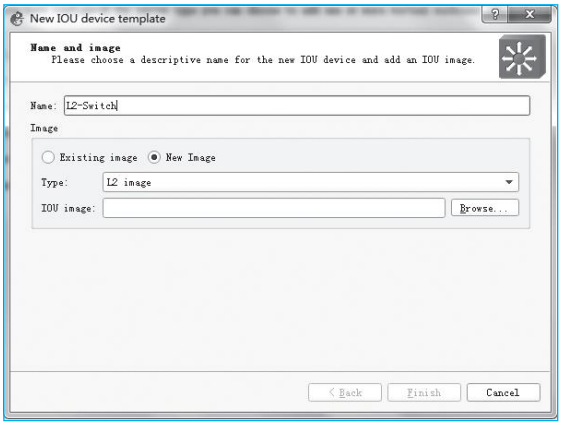


图 1–19　选择二层 IOU 设备镜像文件

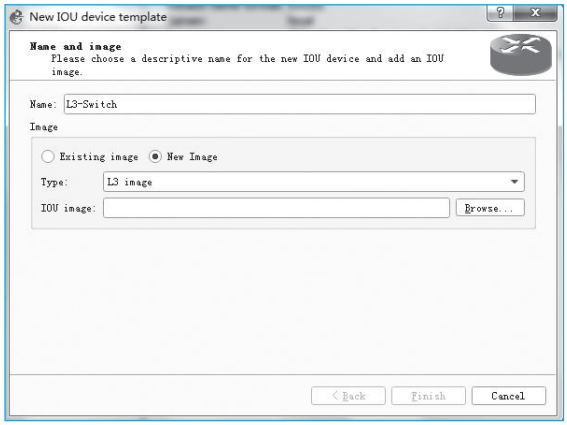


图 1–20　选择三层 IOU 设备镜像文件

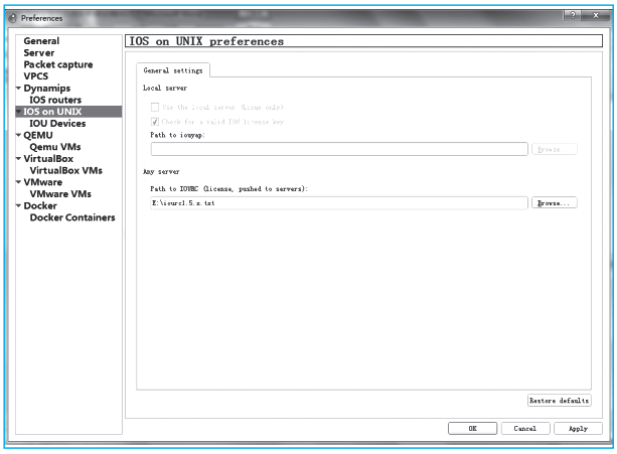


图 1–21　导入 IOU 许可文件

（4）添加终端设备。

在安装 GNS3 软件时可以选择安装 VPCS 设备作为终端设备，但是其功能有限。除此之外，还可以添加 VMware Workstation 中的虚拟机作为终端设备，步骤如下。

①在 VMware Workstation 环境中添加虚拟网络 VMnet2，如图 1–22 所示。

②将需要作为终端设备的虚拟机加入虚拟网络 VMnet2 中，如图 1–23 所示。

③在 GNS3 中将虚拟机添加成终端设备，如图 1–24 和图 1–25 所示。

图 1–22　添加虚拟网络 VMnet2

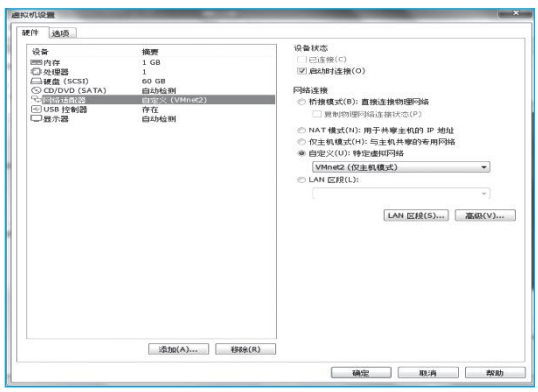


图 1–23　加入虚拟网络 VMnet2

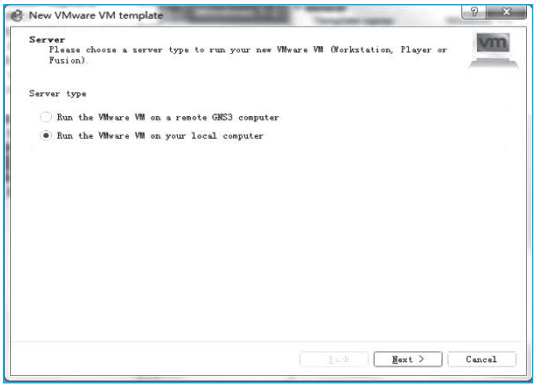


图 1-24　GNS3 中添加虚拟机界面 1

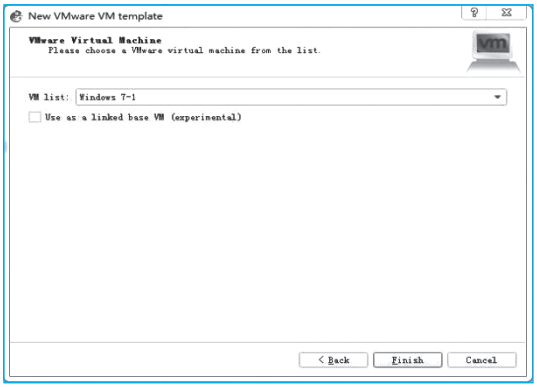


图 1-25　GNS3 中添加虚拟机界面 2

3. 在 GNS3 环境下搭建网络

（1）绘制网络拓扑图。

如图 1–26 所示为网络拓扑图，表 1–3 为其 IP 地址分配表。

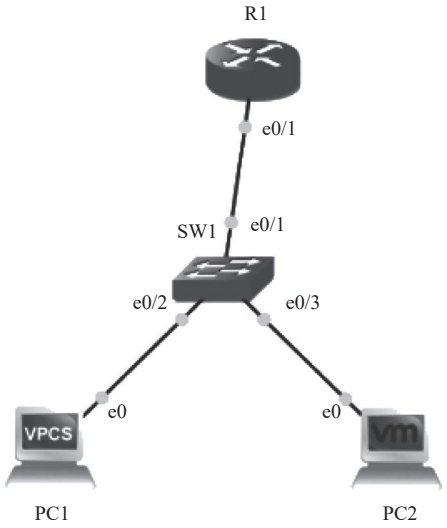


图 1–26　GNS3 环境下搭建的网络拓扑图

表 1–3　GNS3 环境下搭建的网络 IP 地址分配表

设备名	接口	IP 地址 / 子网掩码	默认网关
R1	e0/1	192.168.1.254/24	—
PC1	e0	192.168.1.1/24	192.168.1.254
PC2	e0	192.168.1.2/24	192.168.1.254

首先在左侧面板的路由器和交换机部分分别拖曳两台新添加的 IOU 设备至工作区内，然后在终端设备部分拖曳 VPCS 设备和虚拟机至工作区内，还可以根据情况修改设备的主机名和标识符。右击需要修改的设备，在弹出的菜单中选择“change hostname”和“change symbol”即可进行修改，最后使用连接线缆将各种设备连接起来，单击工具栏中的“ ”图标将接口显示出来，这样网络拓扑图就绘制完成。

（2）开启设备。

与 Packet Tracer 不同，GNS3 中的设备默认是关闭的，可以右击设备，在弹出的菜单中选择

“start”选项便可开启该设备，也可以单击工具栏中的“ ”图标开启所有设备。

（3）配置网络设备。

双击工作区内的路由器 R1 便可对其进行配置，如图 1–27 所示。

路由器的配置命令与在 Packet Tracer 环境下的配置相同，此处不再赘述。

（4）配置终端设备。

①配置 VPCS 设备。双击工作区内的 PC1 便可对其进行配置，如图 1–28 所示。

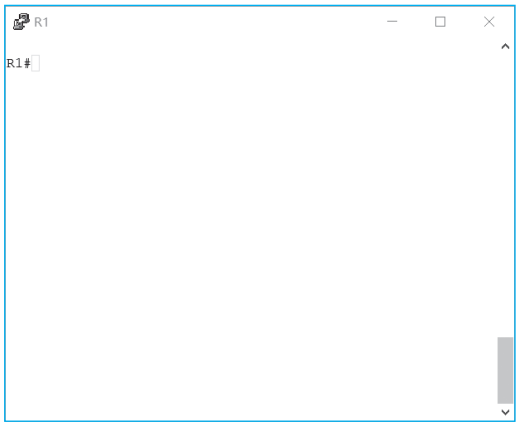


图 1–27　GNS3 环境下网络设备配置界面

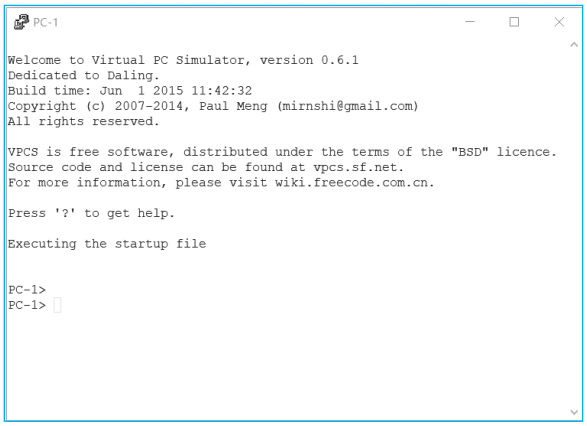


图 1–28　GNS3 环境下终端设备配置界面

配置命令如下：

```
PC1>ip 192.168.1.1/24 192.168.1.254
```

②配置虚拟机。虚拟机中的 IP 地址配置与在 VMware Workstation 环境下相同，此处不再赘述。

（5）验证设备之间的连通性。

以 PC1 为例，双击工作区内的 PC1，在其中使用 ping 命令来验证设备之间的连通性，如图 1–29 所示，PC1 和 PC2 间已经互相连通。

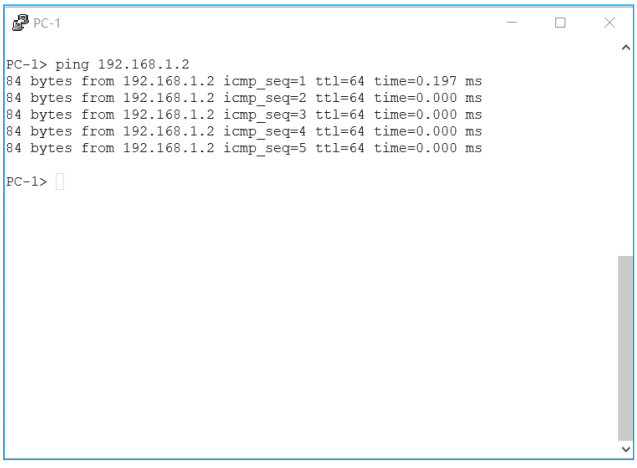


图 1–29　GNS3 环境下验证连通性界面

（6）保存文件。

与 Packet Tracer 类似，在 GNS3 环境下，配置完成后首先要使用 write 命令保存每个网络设备的配置，然后再选择菜单栏中的“保存”选项即可将文件保存起来。

巩固与提高

一、理论知识巩固

1．选择题

（1）实体安全包括哪 3 个方面？（　　）(多选)

A. 环境安全　　B. 设备安全　　C. 媒体安全　　D. 信息安全

（2）强调有用信息只被授权对象使用的安全特征是指网络安全的什么特征？（　　）

A. 完整性　　B. 可用性　　C. 机密性　　D. 可控性

（3）(　　）是指网络通信双方在信息交互过程中，确信参与者本身和所提供的信息真实同一性。

A. 可控性　　B. 可用性　　C. 机密性　　D. 可审查性

（4）（　　）是指信息在传输、交换、存储和处理过程中，保持信息不被破坏或修改、不丢失和信息未经授权不能改变的特性。

A. 完整性　　B. 可用性　　C. 机密性　　D. 可审查性

（5）（　　）是指信息资源可被授权实体按要求访问、正常使用或在非正常情况下能恢复使用的特性。

A. 完整性　　B. 可用性　　C. 机密性　　D. 可控性

（6）（　　）是指信息系统对信息内容和传输具有控制能力的特性，还指网络系统中的信息在一定传输范围和存放空间内可控程度。

A. 可审查性　　B. 可用性　　C. 机密性　　D. 可控性

（7）系统安全主要包括哪 3 个方面的安全？（　　)(多选)

A. 操作系统安全　　B. 设备安全　　C. 网络系统安全　　D. 数据库系统安全

（8）网络安全的主要威胁包括（　　)。(多选)

A. 窃听　　B. 非授权访问　　C. 行为否认　　D. 病毒木马

E. 资源耗尽　　F. 信息战

（9）网络安全法的基本原则包括（　　)。(多选)

A. 预防为主的原则　　B. 突出重点的原则　　C. 主管部门与业务部门相结合的原则

D. 依法管理的原则　　E. 维护国家安全和利益的原则

2．填空题

（1）网络安全问题包括_____和_____两方面内容。

（2）网络安全的目标是在网络的信息传输、存储与处理的整个过程中，提高物理上逻辑上的_____、_____、_____和对抗的能力。

（3）网络安全的发展过程包括_____、_____、_____和_____4 个时期。

（4）网络安全法是_____。

（5）网络安全法的特征包括_____、_____和_____。

（6）网络安全法的基本作用包括_____、_____、_____、_____和_____。

3．简答题

（1）从狭义和广义两个方面简述网络安全的概念。

（2）网络安全所涉及的内容包括哪些部分？

（3）简述国内外网络安全发展现状。

二、实践能力拓展

1．在计算机上安装 VMware Workstation 软件，并在该环境中安装 Windows 10 操作系统，实现以下操作：

（1）修改虚拟机的配置，其中内存大小设置为 2GB，网卡模式设置为主机模式，同时添加一个 20GB 的硬盘。

（2）创建虚拟机快照，并利用此快照克隆一个虚拟机。

（3）使用多种方法实现虚拟机与物理机之间的文件共享。

2．在计算机上安装 Packet Tracer 软件，并在该环境中搭建如图 1–30 所示的网络，其 IP 地址参数详见表 1–4，要求所有的终端设备可以相互访问。

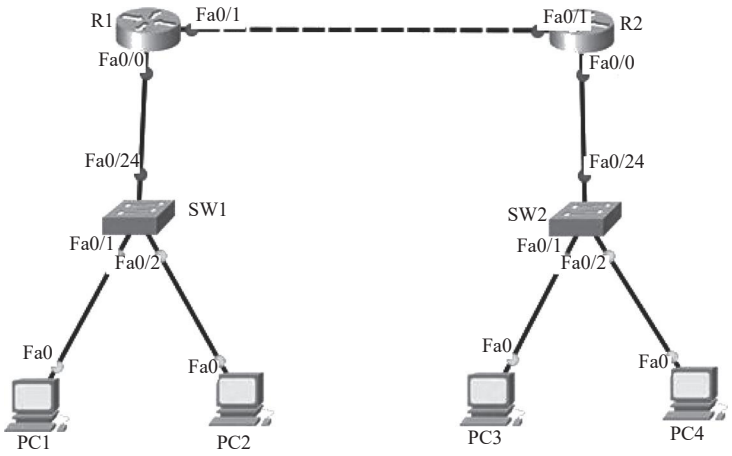


图 1–30　网络拓扑图

表 1–4　网络 IP 地址分配表

设备名	接口	IP 地址 / 子网掩码	默认网关
R1	Fa0/0	192.168.1.254/24	—
	Fa0/1	192.168.0.1/24	—
R2	Fa0/0	192.168.2.254/24	—
	Fa0/1	192.168.0.2/24	—
PC1	Fa0	192.168.1.1/24	192.168.1.254
PC2	Fa0	192.168.1.2/24	192.168.1.254
PC3	Fa0	192.168.2.1/24	192.168.2.254
PC4	Fa0	192.168.2.2/24	192.168.2.254

3．在计算机上安装 GNS3 软件，并在该环境中搭建如图 1–31 所示的网络，其 IP 地址参数详见表 1–5，实现所有的终端设备可以相互访问。

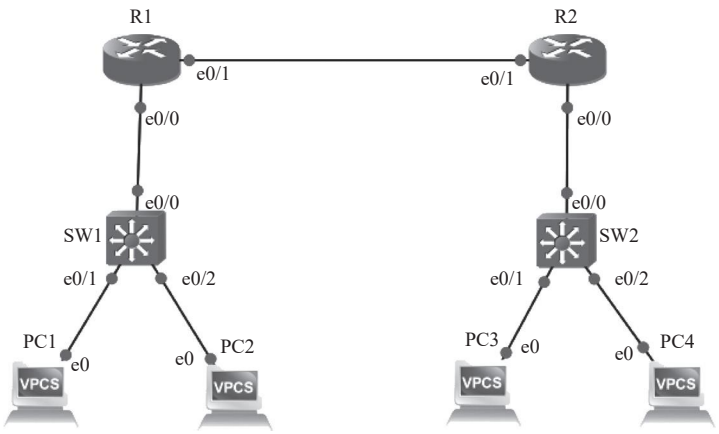


图 1–31　网络拓扑图

表 1–5　网络 IP 地址分配表

设备名	接口	IP 地址 / 子网掩码	默认网关
R1	e0/0	192.168.1.254/24	—
	e0/1	192.168.0.1/24	—
R2	e0/0	192.168.2.254/24	—
	e0/1	192.168.0.2/24	—
PC1	e0	192.168.1.1/24	192.168.1.254
PC2	e0	192.168.1.2/24	192.168.1.254
PC3	e0	192.168.2.1/24	192.168.2.254
PC4	e0	192.168.2.2/24	192.168.2.254

项目 2 网络设备的安全管理

学习目标

知识目标

① 识记：网络设备本地安全的要点；日志服务的特点和工作机制。

②领会：远程访问协议 Telnet 和 SSH 的工作原理；网络时间协议 NTP 的工作原理。

能力目标

① 能实现网络设备本地安全访问。

② 能配置远程访问协议 Telnet 和 SSH 进行远程安全访问。

③ 能配置 NTP 和日志服务。

素养目标

① 树立爱国主义情怀，做到学以致用、报效祖国。

② 通过网络设备安全管理的学习，逐步具备网络安全意识和辨别是非的能力。

项目引入

网络设备是整个网络的核心，可以实现数据在网络中的传输和通信功能。它们确保了数据的快速、稳定和安全的传输，为各种信息和资源的交换提供支持，有利于促进信息化建设和网络强国战略的实施。网络设备的安全问题不仅影响着网络能否正常提供服务，也和信息安全密切相关。2022 年 6 月 22 日，西北工业大学发布公开声明称该校遭受境外网络攻击。调查发现，近年来美国国家安全局对中国国内的网络目标实施了上万次的恶意网络攻击，控制了数以万计的网络设备（网络服务器、上网终端、网络交换机、电话交换机、路由器、防火墙等），窃取了超过 140 GB 的高价值数据。如果网络中的路由器和交换机等设备访问的安全配置薄弱，不法分子就可以非法登录，篡改配置，盗用信息，因此网络设备的安全不容忽视。

为了培养公司员工网络安全意识，提高员工的网络安全防范能力，让公司员工掌握网络设备安全访问的操作技能并学会从网络设备访问控制层面保障网络的安全，项目负责人张工程师制订了如下培训任务：

- 网络设备的本地安全访问配置；
- 网络设备的远程安全访问配置；
- NTP 和日志服务的配置。

任务 2.1 网络设备本地安全访问的配置

任务描述

作为网络管理员必须十分清楚自己所管理的网络设备的安全程度并及时作出调整，确保设备安全，以避免受到攻击而造成不必要的损失。在本任务中，某职业学院学生协助张工程师完成网络设备本地安全访问的配置任务。本任务包括网络设备密码的设置和网络设备其他本地安全配置 2 个子任务。在完成任务的过程中，可以通过设置网络设备各种类型的密码以防范未经授权的人员访问，了解各种密码之间的特点和应用场合，通过加密密码服务、指定密码最小长度、设置 EXE 超时时间和标语信息来确保网络设备本地访问的安全。

任务目标

（1）能正确配置 console 线路下密码认证、用户名密码认证。
（2）能正确配置特权密码。
（3）能合理配置加密密码服务、指定密码最小长度。
（4）能设置 EXEC 超时时间和标语信息。

子任务 1 网络设备密码的设置

任务环境

（1）主流计算机。
（2）Packet Tracer 软件安装包。
（3）网络拓扑图如图 2–1 所示。

网络设备密码的设置

图 2–1　本地安全访问网络拓扑图

相关知识

1. 设置密码的必要性

使用机柜和上锁的机架限制人员实际接触网络设备是不错的做法，但密码仍是防范未经授权的人员访问网络设备的主要手段。每个设备，甚至家用路由器，都应当配置本地密码来限制访问。

2. 设置密码的原则

为了保护网络设备，使用强密码非常重要。以下是需要遵循的标准原则：

（1）使用的密码长度至少为 8 个字符，最好是 10 个或更多字符，密码越长越好。

（2）使用复杂密码。如果条件允许，密码中混合使用大写字母、小写字母、数字和特殊字符等。

（3）密码中避免使用重复的常用字词、字母或数字顺序、用户名、亲属的名字、个人信息（例如出生日期和身份证号码等）或其他易于识别的信息。

（4）故意将密码拼错。

例如，Smith = Smyth = 5mYth 或 Security = 5ecur1ty。

（5）定期更改密码。

（6）请勿将密码写出来并放在显眼位置上，比如桌面上或显示器上。

任务实施

1. 绘制网络拓扑图

首先在设备选择区的网络设备内选择一台路由器 2811 添加到工作区，在终端设备内选择一台个人电脑添加到工作区，在连接线缆内选择 console 线缆将路由器的 console 端口与电脑的 RS232 串口设备连接起来，然后在设备操作管理区内使用工具对工作区内的设备进行标记，完成网络拓扑图绘制。

2. 网络设备的登录

单击工作区内的个人电脑，在弹出的文本框中选择 Desktop 选项，然后再选择 Terminal 选项，单击 ok 按钮便可登录到路由器上。

3. 配置在 console 线路下使用密码访问

配置命令如下所示。

```
Router>en
Router#conf t
Router(config)#line console 0
// 进入 console 线路
Router(config-line)#password P@ssw0rd
```

```
// 定义进入 console 线路下的密码
Router(config-line)#login
// 允许登录
Router(config-line)#end
Router#write
// 保存配置
Router#reload
// 重启路由器
```

路由器重新启动后，可以看到需要输入密码才可以登录，如下所示。

```
User Access Verification
Password：
// 输入时密码隐藏，输入正确后才可以登录
Router>
```

4. 配置 console 线路下使用用户名和密码访问

配置命令如下所示。

```
Router(config)# username user01 password P@ssw0rd
// 设置本地用户名和密码
Router(config)#line console 0
Router(config-line)#login local
// 调用本地用户名和密码登录
Router(config-line)#end
Router#wr
Router#reload
```

路由器重新启动后，可以看到需要输入用户名和密码才可以登录，如下所示。

```
User Access Verification
Username：user01
Password：
// 输入正确的用户名和密码后才可以登录
Router>
```

5. 配置特权密码

（1）password 密码的配置。

```
Router(config)#enable password P@ssw0rd1
```

配置完成后，从用户模式进入特权模式就需要输入密码，如下所示。

```
Router>en
Password：
// 输入特权密码后才可以进入特权模式
```

```
Router#
```

但是该密码为明文存储，通过 show run 命令可以看到，如下所示。

```
Router#show run
…
enable password P@ssw0rd1
…
```

（2）secret 密码的配置。

```
Router(config)#enable secret P@ssw0rd2.
```

配置完成后，此时从用户模式进入特权模式需要输入 secret 密码，password 密码自动失效，因为该密码是加密存储的，优先级高，通过 show run 命令可以看到 secret 密码，如下所示。

```
Router#show run
…
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
…
```


子任务 2　网络设备其他本地安全配置

任务环境

（1）主流计算机。

（2）Packet Tracer 软件。

（3）网络拓扑图同上一个任务。

网络设备其他本地安全配置

相关知识

除了为网络设备设置密码，还需要采取许多其他基本安全措施，其中包括以下几点。

（1）加密密码服务。

使用全局配置命令 service password-encryption 来防止未经授权的个人在配置文件中查看明文形式的密码。该命令会将所有未加密密码进行加密。

（2）指定密码最小长度。

为了确保配置的所有密码至少为指定的最小长度，请在全局配置模式下使用 security passwords min-length 命令。

（3）设置 EXEC 超时时间。

通过设置 EXEC 超时，将告知设备在用户闲置时间达到 EXEC 超时时间值时自动断开线路上

的用户。EXEC 超时可以在控制台、vty 和 aux 端口配置。

（4）设置标语信息。

标语消息类似于一个禁止非法侵入符号。在向法院起诉某人不正当访问系统时，这些标语非常重要。

任务实施

1. 搭建任务环境

绘制网络拓扑图并在终端设备上登录路由器。

2. 配置特权 password 密码

在路由器上配置特权 password 密码并限制在 console 线路下需要使用用户名和密码访问，新建用户 user01，配置命令如下所示。

```
Router(config)#enable password P@ssw0rd1
Router(config)#username user01 password P@ssw0rd2
Router(config)#line console 0
Router(config-line)#login local
```

此时通过 show run 命令可以看到以上两个密码均为明文存储。

3. 配置加密密码服务

```
Router(config)#service password-encryption
```

该命令配置后，所有系统内的 password 密码都被加密，如下所示。

```
Router#show run
Building configuration...
…
enable password 7 08701E1D5D4C53
…
username user01 password 7 0822455D0A16
…
```

4. 设置最短密码长度

```
Router(config)# security passwords min-length 10
// 将密码长度设置为至少 10 位
```

如果此后设置密码时触发规则就会弹出以下信息：

```
Router(config)#enable password P@ssw0rd3
```

```
% Password too short - must be at least 10 characters. Password not configured.
```

5. 设置 EXEC 超时时间

默认情况下，在上一次会话之后的 10 分钟之内，管理接口处于活动状态并呈现为已登录状态，之后接口超时并退出会话。如果在控制台活跃时，管理员离开终端设备，攻击者有长达 10 分钟的时间获取特权级的访问权限。因此强烈建议将时限限制在 2 分钟或 3 分钟之内，如下所示。

```
Router(config)#line con 0
Router(config)# exec-timeout 2
// 将时限限制为 2 分钟
```

6. 配置标语信息

通过配置标语信息向潜在的入侵者显示法律通知：他们在网络上不受欢迎，如下所示。

```
Router(config)# banner login ‘ Warning ’
```

配置完成后，当用户再次登录到设备上时就会出现标语信息。

任务 2.2 网络设备远程安全访问的配置

任务描述

远程终端协议 Telnet 可以实现网络设备的远程访问，防止黑客等非法人员的恶意攻击。安全外壳协议 SSH 是另一种网络设备远程访问协议，在传输过程中能对数据包进行加密，因此逐渐替代 Telnet 协议成为首选的远程访问协议。本任务包括远程终端协议 Telnet 的配置和安全外壳协议 SSH 的配置 2 个子任务。某职业学院学生协助张工程师完成 Telnet 协议、SSH 协议的配置，协助张工程师完成网络设备远程安全访问配置培训，使网络设备在进行远程访问时更加安全，不受到来自外部网络的攻击。

任务目标

（1）能正确配置远程终端协议 Telnet，根据实际网络环境灵活应用。

（2）能配置安全外壳协议 SSH 的服务器端。

（3）学会安全外壳协议 SSH 客户端的操作方法。

子任务 1　远程终端协议 Telnet 的配置

任务环境

（1）主流计算机。

（2）Packet Tracer 软件。

（3）网络拓扑图如图 2–2 所示。

（4）网络 IP 地址分配表如表 2–1 所示。

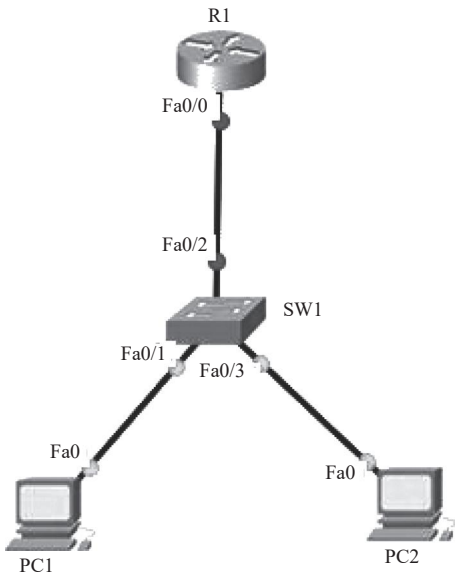


图 2–2　远程安全访问网络拓扑图

表 2–1　网络 IP 地址分配表

设备名	接口	IP 地址 / 子网掩码
R1	Fa0/0	192.168.1.1/24
SW1	Vlan1	192.168.1.2/24
PC1	Fa0	192.168.1.3/24
PC2	Fa0	192.168.1.4/24

相关知识

1. Telnet 协议简介

Telnet 协议是 TCP/IP 协议簇中的一员，是 Internet 远程登录服务的标准协议和主要方式。它为用户提供在本地计算机上完成远程主机工作的能力。在终端使用者的电脑上使用 telnet 程序，用它连接到服务器。终端使用者可以在 telnet 程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样，可以在本地就能控制服务器。

2. Telnet 协议用途

Telnet 是 Internet 远程登录服务的标准协议和主要方式，最初由 ARPANET 开发，现在主要用于 Internet 会话，它的基本功能是允许用户登录进入远程主机系统。

Telnet 可以让我们坐在自己的计算机前通过 Internet 网络登录到另一台远程计算机上，这台计算机可以是在隔壁的房间里，也可以是在地球的另一端。当登录上远程计算机后，本地计算机就等同于远程计算机的一个终端，我们可以用自己的计算机直接操纵远程计算机，享受远程计算机本地终端同样的操作权限。

Telnet 的主要用途就是使用远程计算机上所拥有的本地计算机没有的信息资源，如果远程的主要目的是在本地计算机与远程计算机之间传递文件，那么相比而言使用 FTP 会更加快捷有效。

3. Telnet 协议的安全隐患

虽然 Telnet 较为简单，使用也很方便，但是在格外注重安全的现代网络技术中，Telnet 并不被重用。原因在于 Telnet 是一个明文传送协议，它将用户的所有内容，包括用户名和密码都明文在互联网上传送，具有一定的安全隐患，因此许多服务器都会选择禁用 Telnet 服务。如果用户要使用 Telnet 的远程登录，使用前应在远端服务器上检查并设置允许 Telnet 服务的功能。

任务实施

1. 搭建任务环境

绘制网络拓扑图并根据网络 IP 地址分配表为每个设备接口配置 IP 地址，验证设备之间的连通性。

2. Telnet 协议的配置

（1）配置必须使用密码登录。

将交换机 SW1 配置成 Telnet 服务器端，主要配置命令如下所示。

```
SW1(config)#line vty 0 15
// 进入 vty 线路
SW1(config-line)#password P@ssw0rd1
// 定义进入 vty 线路下的密码
SW1(config-line)#transport input telnet
// 设置 vty 线路上只允许通过 telnet 流量
SW1(config-line)#login
// 允许登录
```

将 PC1 配置成 Telnet 客户端，单击工作区内的个人电脑 PC1，在弹出的文本框中选择 Desktop 选项，然后再选择 Command Prompt 选项，使用 telnet 命令远程登录到 SW1 上，如下所示。

```
Packet Tracer PC Command Line 1.0
C：\>telnet 192.168.1.2
```

```
// 使用 telnet 命令远程登录 SW1
Trying 192.168.1.2 ...Open

User Access Verification

Password：
// 输入正确的密码后便可登录到 SW1 上
SW1> en
% No password set.
// 由于交换机 SW1 上没有设置特权密码，所以无法切换到特权模式，这是远程登录的安全设置
SW1>
```

（2）配置使用用户名和密码登录。

将路由器 R1 配置成 Telnet 服务器端，主要配置命令如下所示。

```
R1(config)#username user01 password P@ssw0rd2
// 创建本地用户 user01 和密码
R1(config)#line vty 0 15
R1(config-line)#transport input telnet
R1(config-line)#login local
// 调用本地用户名登录
```

将 PC2 配置成 Telnet 客户端，使用 telnet 命令远程登录到 R1 上，如下所示。

```
C：\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Username：user01
Password：
// 输入正确的用户名和密码后才可以登录
R1> en
% No password set.
// 同样的原因，由于没有设置特权密码，所以无法切换到特权模式
 R1>
```


子任务 2　安全外壳协议 SSH 的配置

任务环境

（1）主流计算机。

（2）Packet Tracer 软件。

（3）网络拓扑图。同上一个任务。

（4）网络 IP 地址分配表同上一个任务。

相关知识

1. SSH 协议简介

SSH 是 Secure Shell 的缩写，由 IETF 的网络小组所制定。SSH 为建立在应用层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。SSH 客户端适用于多种平台，几乎所有平台都可运行 SSH。

2. SSH 协议组成

SSH 服务由服务端软件 OpenSSH 和连接客户端组成（SSH、SecureCRT、Xshell 等），默认端口是 22。SSH 是一个守护进程，负责实时监听客户端请求，并进行处理。

SSH 协议框架中核心部分的 3 个协议：传输层协议、用户认证协议、连接协议。

（1）传输层协议（The Transport Layer Protocol）：提供服务器认证、数据安全性、信息完整性等功能的支持。

（2）用户认证协议（The User Authentication Protocol）：为服务器提供客户端的身份的识别。

（3）连接协议（The Connection Protocol）：将加密的信息隧道复用成若干个逻辑通道，提供给更高层的应用协议使用，各种高层应用协议可以相对地独立于 SSH 基本体系之外，然后依靠这个基本框架，通过连接协议使用 SSH 的安全机制。

3. SSH 协议功能

传统的网络服务程序，如 FTP、POP 和 Telnet 在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，别有用心的人非常容易就可以截获这些口令和数据。而且这些服务程序的安全验证方式也是有其弱点的，很容易受到“中间人”这种方式的攻击。通过使用 SSH，你可以把所有传输的数据进行加密，这样“中间人”这种攻击方式就不可能实现了，而且也能够防止 DNS 欺骗和 IP 欺骗。使用 SSH 还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，它既可以代替 Telnet，又可以为 FTP、POP，甚至为 PPP 提供一个安全的通道。

任务实施

1. 搭建任务环境

绘制网络拓扑图，根据网络 IP 地址分配表为每个设备接口配置 IP 地址，并验证设备之间的连通性。

2. SSH 协议的配置

（1）SSH 服务器端的配置。

分别将路由器 R1 和 SW1 配置成 SSH 服务器端，生成密钥的主要配置命令如下所示。

```
R1(config)#ip domain-name a.com
// 配置域名
R1(config)#crypto key generate rsa
// 生成密钥
The name for the keys will be：R1.a.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take  a few minutes.
How many bits in the modulus [512]：1024
// 设置密钥的位数，默认 512 位，这里设置为 1024 位
% Generating 1024 bit RSA keys，keys will be non-exportable...[OK]
// 成功生成密钥
```

配置 SSH 服务。

```
R1(config)#username user01 password P@ssw0rd1
R1(config)#line vty 0 15
R1(config-line)#transport input ssh
// 设置 vty 线路上只允许通过 ssh 流量
R1(config-line)#login local
```

按照同样的方法配置 SW1，主要配置命令如下。

```
SW1(config)#ip domain-name b.com
SW1(config)#crypto key generate rsa
…
How many bits in the modulus [512]：1024
% Generating 1024 bit RSA keys，keys will be non-exportable...[OK]
SW1(config)#username user02 password P@ssw0rd2
SW1(config)#line vty 0 15
SW1(config-line)#transport input ssh
SW1(config-line)#login local
```

（2）SSH 客户端的配置。

分别将 PC1 和 PC2 配置成 SSH 客户端，使用 ssh 命令远程登录到 R1 和 SW1 上，如下所示。

```
C：\>ssh -l user01 192.168.1.1
//ssh 命令的用法：ssh -l 用户名 目标 ip 地址
Open
Password：
// 输入正确的密码后便可登录到 R1 上
R1>en
% No password set.
// 由于没有设置特权密码，无法切换到特权模式
R1>

C：\>ssh -l user02 192.168.1.2
//ssh 命令的用法：ssh -l 用户名 目标 ip 地址
Open
Password：
```

```
// 输入正确的密码后便可登录到 SW1 上
SW1>en
% No password set.
// 由于没有设置特权密码，无法切换到特权模式
SW1>
```


任务 2.3 NTP 和日志服务的配置

任务描述

网络时间协议（network time protocol，NTP）可以用来确保网络中所有设备时间的统一，便于管理网络中的设备。在网络中，每台设备都会产生大量的日志信息，如何管理庞大的信息，使其不受非法人员的窥探和篡改是网络管理员非常重要的任务之一。日志服务可以将大量的日志信息存储在服务器中。用户可以根据日志信息对网络状况、网络安全进行监管。本任务包括 NTP 配置和日志服务配置 2 个子任务，某职业学院学生协助张工程师完成 NTP 设置、日志服务的服务器端和客户端的配置培训，从而实现网络中各种设备之间时间的同步和日志信息的安全管理。

任务目标

（1）了解 NTP 和日志服务相关命令的作用和正确使用方法。
（2）能正确配置 NTP 的客户端和服务器时间的同步。
（3）能正确配置日志服务的服务器端和客户端。

子任务 1 NTP 的配置

任务环境

（1）主流计算机。
（2）GNS3 软件。
（3）VMware Workstation 软件。
（4）网络拓扑图如图 2–3 所示。
（5）网络 IP 地址分配表如表 2–2 所示。


NTP 的配置

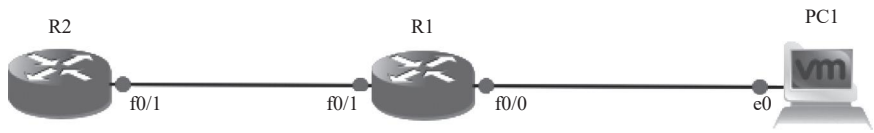


图 2–3　NTP 和日志服务配置网络拓扑图

表 2–2　NTP 配置网络 IP 地址分配表

设备名	接口	IP 地址 / 子网掩码	默认网关
R1	f0/0	192.168.1.1/24	—
	f0/1	192.168.0.1/24	—
R2	f0/1	192.168.0.2/24	—
PC1	e0	192.168.1.2/24	192.168.1.1

相关知识

1. 网络时间协议 NTP 简介

整个网络保持准确的时间是十分重要的，即使是小小的时间误差也会引起大问题。网络时间协议（NTP）适用于运行在计算机上客户端 / 服务器程序和协议，在基本条件下，NTP 客户端发出时间请求，与时间服务器交换时间，这个交换的结果是，客户端能计算出时间的延迟和弥补值，并调整与服务器时间同步。NTP 在设计上是高度容错和可升级的。

2. 网络时间协议 NTP 原理

NTP 提供准确时间，首先要有准确的时间来源，这一时间应该是国际标准时间 UTC。 NTP 获得 UTC 的时间来源可以是原子钟、天文台、卫星，也可以从 Internet 上获取。这样就有了准确而可靠的时间源。时间按 NTP 服务器的等级传播。按照离外部 UTC 源的远近将所有服务器归入不同的 Stratum（层）中。Stratum-1 在顶层，有外部 UTC 接入，而 Stratum-2 则从 Stratum-1 获取时间，Stratum-3 从 Stratum-2 获取时间，以此类推，但 Stratum 层的总数限制在 15 以内。所有这些服务器在逻辑上形成阶梯式的架构相互连接，而 Stratum-1 的时间服务器是整个系统的基础。计算机主机一般同多个时间服务器连接，利用统计学的算法过滤来自不同服务器的时间，以选择最佳的路径和来源来校正主机时间。即使主机在长时间无法与某一时间服务器相联系的情况下，NTP 服务依然可以有效运转。为防止对时间服务器的恶意破坏，NTP 使用了识别（Authentication）机制，来检查对时的信息是否是真正来自所宣称的服务器并检查资料的返回路径，以提供对抗干扰的保护机制。NTP 时间同步报文中包含的时间是格林尼治时间，是从 1900 年开始计算的秒数。

任务实施

1. 搭建任务环境

绘制网络拓扑图，根据网络 IP 地址分配表为每个设备接口配置 IP 地址，并验证设备之间的连通性。

2. 静态路由的配置

在 R2 上配置静态路由，使所有网络可以互通，主要配置命令如下。配置完成后验证 PC1 和 R2 间的连通性。

```
R2(config)# ip route 192.168.1.0 255.255.255.0 192.168.0.1
// 静态路由的配置
```

3. NTP 服务的配置

（1）NTP 服务器端的配置。

将路由器 R2 配置成 NTP 服务器端，主要配置命令如下所示。

```
R2(config)# clock timezone Beijing +8
// 设置时区为 +8，即北京时间
R2(config)#exit
R2#clock set 10：00：00 1 Jan 2020
// 设置时间
R2#conf t
R2(config)#ntp master 5
// 指定为 NTP 服务器，并将层级设置为 5 级
```

查看 NTP 服务器信息。

```
R2#show ntp status
Clock is synchronized，stratum 5，reference is 127.127.1.1
…
reference time is E1B67BC3.6B88C7C1 (10：00：35.420 Beijing Wed Jan 1 2020)
…
// 从以上输出信息中可以看到 NTP 的层级和参考设备的时间
```

（2）NTP 客户端的配置。

将路由器 R1 配置成 NTP 客户端，主要配置命令如下所示。

```
R1(config)# clock timezone Beijing +8
// 设置时区
R1(config)#ntp server 192.168.0.2
// 指定 R2 为其 NTP 服务器
```

（3）查看 R1 的系统时间和 NTP 信息。

```
R1#show clock
10：05：06.739 Beijing Wed Jan 1 2020
// 从以上输出信息中可以看到 R1 的系统时间已经和 R2 同步
R1#show ntp status
Clock is synchronized，stratum 6，reference is 192.168.0.2
…
reference time is E1B67CC0.5B2DF639 (10：04：48.356 Beijing Wed Jan 1 2020)
…
// 从以上输出信息中可以看到 NTP 的层级和参考设备的时间
```

（4）将 PC1 配置成 NTP 客户端。

首先右击任务栏右下角的时钟，在弹出的菜单中选择“调整日期 / 时间”，打开“日期和时间属性”对话框，然后单击“ Internet 时间”选项，选择“与 Internet 时间服务器同步”复选框，并在“服务器”文本框中输入 NTP 服务器的 IP 地址“192.168.0.2”，单击“立即更新”按钮，可以看到其时间已经与 NTP 服务器同步，如图 2–4 所示。

图 2–4　NTP 客户端的配置

子任务 2　日志服务的配置

任务环境

（1）主流计算机。

（2）GNS3 软件。

（3）VMware Workstation 软件。

（4）Kiwi Syslog Server 软件。

（5）网络拓扑图同上一个任务。

（6）网络 IP 地址分配表同上一个任务。

日志服务的配置

相关知识

1. syslog 简介

syslog 常被称为系统日志或系统记录，是一种用来在互联网协议（TCP/IP）的网络中传递记录消息的标准。这个词汇常用来指实际的 syslog 协议，或者那些提交 syslog 消息的应用程序或数据库。

syslog 协议属于一种主从式协议：syslog 发送端发送出一个小的文字消息（小于 1024 位组）到 syslog 接收端。接收端通常名为“ syslogd”“ syslog daemon”或 syslog 服务器。系统日志消息可以被以 UDP 协议或 TCP 协议来发送。这些数据是以明码类型被发送。不过 SSL 加密外套（例如 Stunnel、sslio 或 sslwrap 等）并非 syslog 协议本身的一部分，因此可以被用来透过 SSL/TLS 方式提供一层加密。

syslog 通常被用于信息系统管理及信息安全审核。虽然它有不少缺陷，但仍获得了相当多的设备及各种平台的接收端支持。因此 syslog 能被用来将来自许多不同类型系统的日志记录集成到集中的存储库中。

2. syslog 功能

在 Unix 类操作系统上，syslog 广泛应用于系统日志。syslog 日志消息既可以记录在本地文件中，又可以通过网络发送到接收 syslog 的服务器。接收 syslog 的服务器可以对多个设备的 syslog 消息进行统一的存储，或者解析其中的内容做相应的处理。常见的应用场景是网络管理工具、安全管理系统、日志审计系统。完整的 syslog 日志中包含产生日志的程序模块（Facility）、严重性（Severity 或 Level）、时间、主机名或 IP、进程名、进程 ID 和正文。在 Unix 类操作系统上，能够按 Facility 和 Severity 的组合来决定什么样的日志消息是否需要记录，记录到什么地方，是否需要发送到一个接收 syslog 的服务器等。由于 syslog 简单而灵活的特性，syslog 不再仅限于 Unix 类主机的日志记录，任何需要记录和发送日志的场景，都可能会使用 syslog。

任务实施

1. 搭建任务环境

（1）绘制网络拓扑图，根据网络 IP 地址分配表为每个设备接口配置 IP 地址，并验证设备之间的连通性。

（2）在 R2 上配置静态路由，使所有网络可以互通，配置完成后验证 PC1 和 R2 间的连通性。

2. 日志服务的配置

（1）日志服务器端的配置。

将 PC1 配置成日志服务器端，首先在其中安装 Kiwi Syslog Server 软件，如图 2–5 所示为软件的主界面。

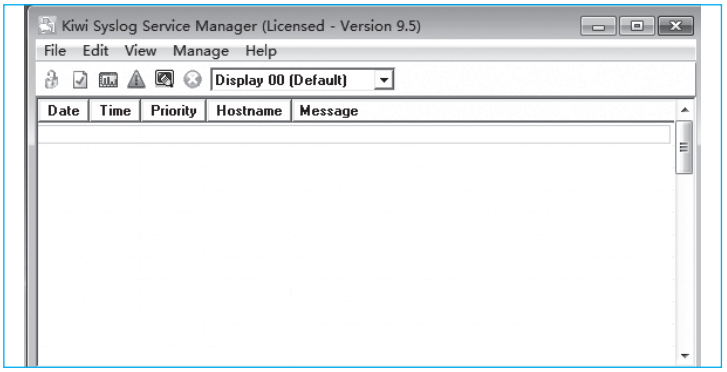


图 2–5　日志服务器软件的主界面

（2）日志客户端的配置。

将路由器 R1 和 R2 配置为日志客户端，主要配置命令如下（以 R1 为例）。

```
R1(config)#logging on
// 开启日志服务
R1(config)#logging host 192.168.1.2
// 指定日志服务器
R1(config)#service timestamps log datetime localtime show-timezone msec
R1(config)#service timestamps debug datetime localtime show-timezone msec
// 日志记录的时间戳设置
R1(config)#logging facility local7
// 定义 facility 级别
R1(config)#logging trap 7
// 定义 severity 级别
```

（3）日志服务器的记录。

配置完成后，日志服务器上会记录下路由器 R1 和 R2 上的所有日志信息，如图 2–6 所示。

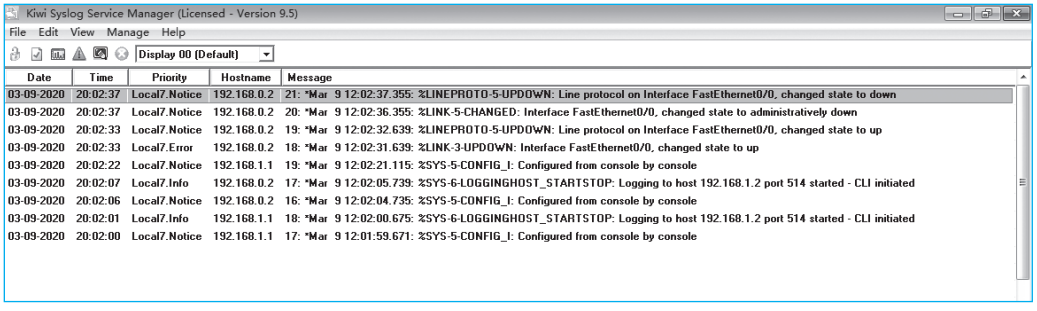


图 2–6　日志服务器的运行界面

巩固与提高

一、理论知识巩固

1．选择题

（1）哪种协议在本质上是安全的？（　　）

A. FTP　　B. POP　　C. Telnet　　D. SSH

（2）为防止对时间服务器的恶意破坏，NTP 使用了（　　）机制，以提供对抗干扰的保护机制。

A. 识别　　B. 认证　　C. 查重　　D. 鉴定

（3）本地安全设置可以采取哪些基本安全措施？（　　）（多选）

A. 加密未加密密码　　B. 指定密码最小长度　　C. 设置标语信息　　D. 设置 EXEC 超时时间

（4）网络设备的远程安全访问协议包括哪些？（　　）（多选）

A. Telnet 协议　　B. FTP 协议　　C. POP 协议　　D. SSH 协议

（5）syslog 服务常见的应用场景包括哪些？（　　）（多选）

A. 网络统计工具　　B. 安全管理系统　　C. 日志审计系统　　D. 网络管理工具

（6）默认情况下，网络设备的 EXEC 超时时间是多少？（　　）

A. 5 分钟　　B. 10 分钟　　C. 15 分钟　　D. 20 分钟

（7）SSH 是建立在（　　）基础上的安全协议。

A. 网络层　　B. 传输层　　C. 物理层　　D. 应用层

（8）在网络时间协议（NTP）中，Stratum 层的总数限制在（　　）以内。

A. 10　　B. 15　　C. 20　　D. 25

（9）完整的 syslog 日志中包含哪些信息？（　　）（多选）

A. 程序模块（Facility）　B. 严重性（Severity）　C. 主机名　　D. 时间

E. 进程名　　F. 正文

2．填空题

（1）在 Unix 类操作系统中，syslog 广泛应用于_____。

（2）使用全局配置命令_____来防止未经授权的个人在配置文件中查看明文形式的密码。

（3）为了确保配置的所有密码至少为指定的最小长度，请在全局配置模式下使用_____。

（4）网络设备的特权模式密码包括_____密码和_____密码两种。

（5）通过配置_____向潜在的入侵者显示法律通知。

（6）NTP 要提供准确时间，首先要有准确的时间来源，这个时间就是_____。

3．简答题

（1）为了保护网络设备，使用强密码非常重要，强密码必须遵循哪些标准原则？

（2）简述 Telnet 协议的主要用途。

（3）与传统的网络服务程序，如 FTP、POP 和 Telnet 等协议相比，SSH 有哪些特点？

二、实践能力拓展

1．某企业是一个跨地区的大型企业，其总部的网络设备需要进行本地安全访问的配置。现要在 Packet Tracer 环境下模拟如图 2–7 所示的网络拓扑图。配置要求如下。

（1）新建路由器本地用户 user，密码为 Se@urity1。

（2）使用本地用户名和密码的登录方式设置 console 线路认证。

（3）设置路由器的特权 secret 密码为 Se@urity2。

（4）开启路由器加密密码服务。

（5）设置路由器最小密码长度为 8 位。

（6）设置路由器 EXEC 超时时间为 3 分钟。

（7）设置路由器登录标语信息为“Legal action will be pursued for any unauthorized use”（未经授

权擅自使用设备将招致诉讼）。

图 2-7　网络拓扑图

2．某企业总部的网络设备已经配置了本地安全访问，其分部的网络设备则需要进行远程安全访问的配置。现要在 Packet Tracer 环境下模拟如图 2-8 所示的网络拓扑图，网络 IP 地址分配表如表 2-3 所示。配置要求如下。

（1）将 R1 配置为 Telnet 服务器，使用密码登录，其中密码为 Se@urity1。

（2）将 SW1 配置为 SSH 服务器，使用用户名和密码登录，其中用户名为 user，密码为 Se@urity2，域名为 network.com，密钥长度为 2048 位。

（3）分别使用 PC1 和 PC2 远程登录到 R1 和 SW1 上进行验证。

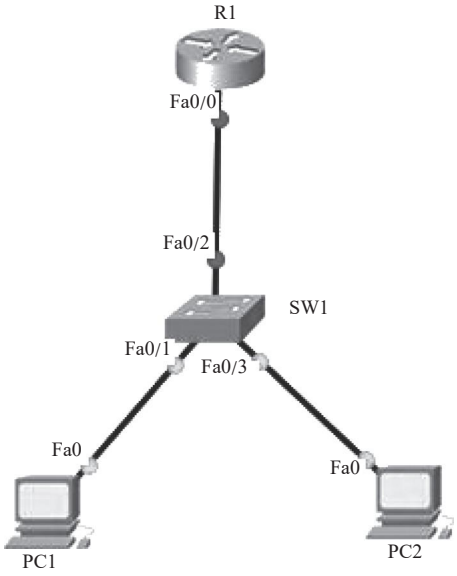


图 2-8　网络拓扑图

表 2-3　网络 IP 地址分配表

设备名	接口	IP 地址 / 子网掩码
R1	Fa0/0	172.16.1.1/24
SW1	Vlan1	172.16.1.2/24
PC1	Fa0	172.16.1.3/24
PC2	Fa0	172.16.1.4/24

3．某企业要求所有的网络设备时间同步，并将其日志信息统一存储在日志服务器中。现要在 GNS3 和 VMware 环境下模拟如图 2-9 所示的网络拓扑图，网络 IP 地址分配表如表 2-4 所示。配置要求如下。

（1）R1 配置成 NTP 服务器端，层级为 3 级，时区为北京，并将时间调节为当前时间；SW1 指定 R1 为 NTP 服务器，时区为北京；PC1 指定 R1 为 NTP 服务器，并观察各设备间的时间是否同步。

（2）PC2 配置成日志服务器端，R1 和 SW1 指定 PC2 为日志服务器，定义 facility 级别为 local7，定义 severity 级别为 7 级，设置相应的日志记录的时间戳，并在日志服务器端查看各设备的

日志信息。

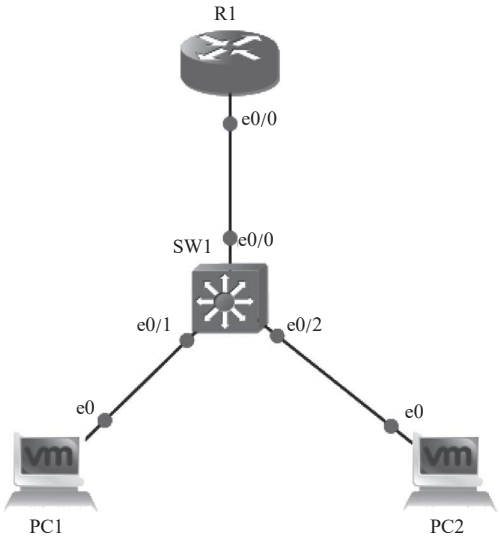


图 2–9　网络拓扑图

表 2–4　网络 IP 地址分配表

设备名	接口	IP 地址 / 子网掩码
R1	e0/0	192.168.1.1/24
SW1	Vlan1	192.168.1.2/24
PC1	e0	192.168.1.3/24
PC2	e0	192.168.1.4/24