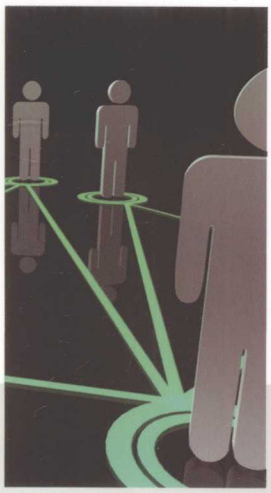
“十二五”职业教育国家规划教材
经全国职业教育教材审定委员会审定

21世纪高等职业教育 计算机系列规划教材

网络安全管控与运维



◆ 武春岭　王　文　主编
◆ 甘　晨　王常亮　何　欢　副主编

NETWORK

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

配备电子课件

“十二五”职业教育国家规划教材
经全国职业教育教材审定委员会审定

21世纪高等职业教育计算机系列规划教材

网络安全管控与运维

武春岭　王　文　主　编
甘　晨　王常亮　何　欢　副主编
北京中数城科技有限公司课程开发支持
杭州思福迪信息技术有限公司产品技术支持

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书针对信息安全行业管控与运维的技术要求和安全服务素质要求，结合高职高专教学特点和多年信息安全技术专业课程教学改革成果，与北京中数城科技有限公司深度合作，以目前企业网络安全管控与运维为技术背景，借鉴国内“注册信息安全专业人员（CISP）”相关安全管理内容，开发出了理实一体化的信息安全管控与运维实用教材。

本书内容有效整合了现代信息安全技术服务企业安全管控与运维技能要求，每章是一个学习项目，开宗明义，从“项目描述”入手，使读者首先清楚本章要完成项目的内容，做到目标明确；然后展开“相关知识”学习，使学习者掌握技能实施必备的理论和技术规范；最后通过“项目实施”细化为若干个实践任务，强化学生技能；体现了“项目牵引、任务驱动”和“教学做”一体化的思想，实用性强、浑然天成。

本书可作为高职院校网络与信息安全技术专业或其他计算机类专业的“信息安全管控与运维”核心课程教材，也适合通信技术专业和其他相关“信息安全管理”领域教学和社会培训使用。

图书在版编目（CIP）数据

网络安全管控与运维 / 武春岭，王文主编. —北京：电子工业出版社，2014.9
“十二五”职业教育国家规划教材

ISBN 978-7-121-24137-6

Ⅰ. ①网… Ⅱ. ①武… ②王… Ⅲ. ①计算机网络—安全技术—高等职业教育—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2014）第 191759 号

策划编辑：徐建军（xujj@phei.com.cn）
责任编辑：郝黎明
印　　刷：北京天宇星印刷厂
装　　订：北京天宇星印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：11.25　字数：288 千字
版　　次：2014 年 9 月第 1 版
印　　次：2014 年 9 月第 1 次印刷
印　　数：3 000 册　　定价：29.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

信息系统运行维护与安全管控是保证信息系统稳定安全运行的重要基础，尤其是在目前大量采用国外设备及技术，以及运行维护工作外包的环境下，通过运行维护的安全管控实现设备的受控使用和维护，对于国家信息安全和行业信息系统稳健运行具有重要意义。

本书以介绍信息系统运行维护与安全管控为重点，通过“项目牵引、任务驱动”的结构方式，让读者置身于实际的工作环境，完成一个个项目任务，从而让读者掌握系统运行维护与安全管控的知识和技能。

“职业导向、突出技能”为本书的设计特色，主要从内容选择、内容组织、内容呈现三个方面具体落实。

1．内容选择：对接职业标准、体现“四新”、融入产业文化。根据学生将来专业学习和职业工作的实际情况，注重新知识、新技能、新产品、新技术等内容的编写。参考、借鉴国外信息安全技术优秀教材的编写经验，做到课程内容的“国际对接”，兼顾专业发展能力，做到职业教育与终身学习对接，充分体现时代特征。顺应新形势需要，注重吸收产业文化和优秀企业文化，将现代产业理念和现代优秀职场文化编入教材。

2．内容组织：以职业工作逻辑为脉络，编制教材大纲，编写开发能力本位教材。并根据实际需要，结合 CISP 所要求的信息安全管理内容，让读者了解系统运行维护与安全管控的相关知识，突出了项目式教材特色。

3．内容呈现：目标先行、动机诱发、科学规范、图文并茂。力求做到学习目标先行、有效激发学习兴趣和动机。根据教育传播规律，采取图文并茂及多样化合理的传播形式，注重提高信息接收效率，提高阅读过程的成就感和愉悦感。

本书主要是介绍系统运行维护与安全管控，与许多介绍系统运行维护的书籍不同，本书偏重于运维的安全管控，实实在在地把运维的安全管控作为重点，而不只是一两章提到运维安全，而实际上一两章是绝对不够介绍运维的安全管控的，只能是蜻蜓点水而已。

这本书以“项目任务型”的叙述方式，让学生通过一个个任务了解运维的安全管控，所包含的 6 个项目涵盖了系统运行维护与安全管控的方方面面，具体内容如下所述。

项目一介绍运行维护的工作内容以及常见的运行维护技术方法。我们从了解常见的运行维护工具开始，逐步了解设备日常巡检的工作内容，了解突发事件应急响应及系统变更的流程。

项目二介绍运行维护设备安全管控。通过完成 4 个任务，读者会对设备的安全管控有新的认识，了解常见的设备分类方法及实现过程，掌握针对设备表单的安全管理措施，掌握常见的新购设备管理过程并生成相关表格，掌握设备分级方法，了解设备的通用安全配置要求，并能对设备进行安全配置。

项目三介绍运行维护人员安全管控。可以让读者了解实施运行维护人员安全管控的意义及基本内容，掌握运行维护人员离职和入职的工作交接程序和具体的安全管控方法，掌握外来运行维护人员的定义及实施安全管控的步骤和方法。

项目四介绍系统运维安全管控平台配置。通过人员管理配置、主机管理配置、权限管理配置及自动改密码配置这 4 个任务了解系统运维安全管控平台的配置方法。

项目五介绍运维操作安全监控，通过综合管控系统实现。通过对 OA 系统设备、业务系统设备及网络支撑设备进行运维操作安全监控，了解运维安全管控平台的审计管理员配置方法，掌握如何通过审计管理员对运维人员的维护过程进行监视，并掌握运维安全管控平台的指令操作授权配置方法。

项目六介绍运维操作数据管理，通过综合审计系统实现。通过本项目可以了解日志的采集技术，了解各个系统日志、网络流量日志采集的技术原理，并了解各种日志的配置过程及日志大小的计算方法，了解如何快速对运维事件进行准确定位，及时发现事件源头，并掌握如何配置统计报告。

本书由重庆电子工程职业学院的武春岭和王文担任主编，何欢老师完成了部分章节的编写工作，北京中数城科技有限公司的甘晨和王常亮给予了大力支持，并亲自参与该书的编写，沈海娟、郑士匠、封建伟、周晓峰和张辉等人也为本书编写做出了重要贡献，在此表示衷心的感谢！本书项目一由王文编写；项目三和项目五由武春岭编写；何欢负责项目二的编写；项目四和项目六主要由企业和兄弟院校朋友编写。

本书所有程序均调试通过，同时为了方便教师教学，本书配有电子教学课件及相关资源，有此需要的读者可登录华信教育资源网（www.hxedu.com.cn）注册后免费进行下载，如有问题可在网站留言板留言或与电子工业出版社联系（E-mail:hxedu@phei.com.cn）。

虽然本书体现了我们近年教学改革积累的经验，但由于开发经验有限，编写时间仓促，书中难免存在疏漏和不足。恳请同行专家和读者给予批评和指正。

编　者

目 录

项目一

了解运行维护

知识目标

- 掌握系统运行维护的基本概念
- 了解系统常见的维护方式
- 了解系统运维的常用工具
- 了解 Windows 系统日常巡检方法
- 了解 Linux 系统日常巡检方法
- 了解网络设备日常巡检方法
- 掌握突发事件应急处理流程
- 掌握应急处理的相关概念
- 了解系统变更的整个工作流程
- 掌握变更管理的基本概念

技能目标

- 掌握 PuTTY 工具的安装、配置和使用
- 掌握 VNC 工具的安装、配置和使用
- 掌握 RDP 协议的配置和使用
- 掌握 Windows 系统日常巡检操作
- 掌握 Linux 系统日常巡检操作
- 掌握网络设备日常巡检操作
- 掌握应急处理的流程与方法
- 掌握应急处理过程中的沟通方法
- 掌握系统变更的实施过程

项目描述

单位新招入 3 名应届毕业生，负责业务服务器、网络设备、办公用个人计算机的运行维护工作。由于应届毕业生初入职场，对日常运行维护过程中涉及的运行维护常用工具的安装、配置、操作等内容都不熟悉，因此单位专门为这 3 名新员工组织了一次运行维护工作入职培训，

主要目的是让他们尽快掌握运行维护工作技能。

技术部经理在 1 天的培训时间内，向他们介绍了日常运行维护过程所涉及的运维工具 putty、VNC（Virtual Network Computing）、RDP（Remote Desktop Protocol）的安装、配置和使用，另外还介绍了运行维护的工作内容以及常见的运行维护技术方法。

单位网络现有 OA 服务器（Windows 操作系统）1 台、业务服务器（Linux 操作系统）1 台、核心交换机（Cisco 设备）1 台、接入交换机（Cisco 设备）1 台、路由器（Cisco 设备）1 台、办公用个人计算机 30 台。这些设备的维护工作都由运维人员完成，他们日常工作中需要了解和掌握的技能包括设备日常检查、应急处理和系统变更。

相关知识

1.1 系统运行维护

1.1.1 系统运行维护的含义

系统运行和维护的主要任务是进行系统的日常运行管理和维护工作，根据要求对系统进行必要的修改，对系统的运行效率、工作质量和经济效益进行评价，对系统运行费用和效果进行监理审计。系统交付使用后，根据用户新增功能的要求和不断适应外部环境变化的要求，进一步对系统做出必要的修改。

系统运行维护是指在信息系统交付使用后，为了改正错误或满足新的需要而修改系统的过程。信息系统是一个复杂的人机系统，系统内外环境，以及各种人为的、机器的因素都不断地在变化着。为了使系统能够适应这种变化，充分发挥软件的作用，产生良好的社会效益和经济效益，就要进行系统维护的工作。

大中型企业软件产品的开发周期一般为 1～3 年，运行周期则可达 5～10 年，在如此长的时间内，除了要改正软件中遗留的错误外，还可能多次更新软件的版本，以适应改善运行环境和加强产品性能等需要，这些活动也属于维护工作的范畴。能不能做好这些工作，将直接影响软件的使用寿命。

系统的维护是系统生存的重要条件。系统维护工作十分重要，统计和估测结果表明，在系统整个生命周期中，信息技术中硬件费用一般占 35%，软件占 65%，而软件后期维护费用有时竟高达软件总费用的 80%，所有前期开发费用仅占 20%。从人力资源的分布看，现在世界上 90%的软件人员在从事系统的维护工作，开发新系统的人员仅占 10%，这些统计数字说明系统维护任务是十分繁重的。重开发、轻维护是造成我国信息系统低水平重复开发的原因之一。

1. 系统运行维护的含义

系统运行维护是指在信息系统交付使用后，为了改正错误或满足新的需要而修改系统的过程。

2. 系统的可维护性

系统的可维护性可通过以下几个方面来衡量。

（1）可理解性

可理解性是指别人能理解系统的结构、界面功能和内部过程的难易程度。模块化、详细设计文档、结构化设计和良好的高级程序设计语言等，都有助于提高系统的可理解性。

（2）可测试性

好的文档资料有利于诊断和测试，诊断和测试的容易程度取决于易理解的程度。同时，程序的结构、高性能的调试工具以及周密计划的测试工序也是至关重要。开发人员在系统设计和编程阶段就应尽力把程序设计成易诊断和测试的。此外，在系统维护时，应该充分利用在系统调试阶段保存下来的调试用例。

（3）可修改性

诊断和测试的容易程度与系统设计所制定的设计原则有直接关系。模块的耦合、内聚、作用范围与控制范围的关系等，都对可修改性有影响。

（4）系统文档

文档是系统可维护性的决定因素。由于长期使用的信息系统在使用过程中必然会经受多次修改，所以文档比程序代码更重要。系统的文档可以分为用户文档和系统文档两类。用户文档主要描述系统功能和使用方法，并不关心这些功能是怎样实现的。系统文档描述系统设计，实现和测试等各方面的内容。

3. 系统运行维护的内容和类型

根据运行维护活动的目的不同，可将系统运行维护分成改正性维护、适应性维护、完善性维护和安全性维护四大类。根据运行维护活动的具体内容不同，可将维护分成程序维护、数据维护、代码维护和设备维护。

（1）根据运行维护活动的目的分类

① 改正性维护。在系统交付使用后，因开发时测试的不彻底、不完全，必然会有部分隐藏的错误遗留到运行阶段。这些隐藏下来的错误在某些特定的使用环境下就会暴露出来。为了识别和纠正软件错误、改正软件性能上的缺陷、排除实施中的误使用，应当进行的诊断和改正错误的过程就称为改正性维护。

② 适应性维护。由于计算机科学技术的迅速发展，新的硬、软件不断推出，使系统的外部环境发生变化。这里的外部环节不仅包括计算机硬、软件的配置，而且包括数据库、数据存储方式在内的“数据环境”。为使系统适应这种变化，而去修改系统的过程就称为适应性维护。

③ 完善性维护。在系统的使用过程中，用户往往会对系统提出新的功能与性能要求。为了满足这些要求，需要修改或再开发软件，以扩充软件功能、增强软件性能、改进加工效率、提高软件的可维护性。这种情况下进行的维护活动称为完善性维护。

④ 安全性维护。信息系统要收集、保存、加工和利用全局的或局部的社会经济信息，涉及企业、地区、部门乃至全国的财政、金融、市场、生产和技术等方面的数据、图表和资料。随着病毒和计算机罪犯的出现，系统对安全性和保密性提出了更为严格和复杂的要求，用户往往会提出增加安全的要求和配套的安全措施，针对安全措施的维护称为安全性维护。

（2）根据运行维护活动的内容分类

① 程序维护。程序维护是指改写一部分或全部程序，程序维护通常都充分利用源程序。修改后的源程序，必须在程序首部的序言性注释语句中进行说明，指出修改的日期、人员。同时，必须填写程序修改登记表，填写内容包括所修改程序的所属子系统名、程序名、修改理由、

修改内容、修改人、批准人和修改日期等。同时，程序维护不一定在发现错误或条件发生改变时才进行，效率不高的程序和规模太大的程序也应不断地设法予以改进。

② 数据维护。数据维护是指不定期地对数据文件或数据库进行修改，这里不包括主文件或主数据库的定期更新。数据维护的内容主要是对文件或数据中的记录进行增加、修改和删除等操作，通常采用专用的程序模块。

③ 代码维护。随着用户环境的变化，原有的代码已经不能继续适应新的要求，这时就必须对代码进行变更。代码的变更（即维护）包括订正、新设计、添加和删除等内容。当有必要变更代码时，应有现场业务经办人和计算机有关人员组成专门的小组进行讨论决定，用书面格式写清并事先组织有关使用者学习，然后输入计算机并开始实施性的代码体系。代码维护过程中的关键是如何使新的代码得到贯彻。

④ 设备维护。系统正常运行的基本条件之一就是保持计算机及外部设备的良好运行状态。因此，要定期地对设备进行检查和保养，应设立专门设备故障登记表和检修登记表，以便设备维护工作的进行。

1.1.2 系统的常见维护方式

1. Windows 系统的常见维护方式

Windows 的维护常见方式为通过 RDP 协议，或者使用特定程序进行维护，专业化的维护程序主要是以 pcAnywhere 为代表的远程控制程序。

使用 RDP 协议的客户可以在远程以图形界面的方式访问服务器，并且可以调用服务器中的应用程序、组件、服务等，和操作本机系统一样。这样的访问方式不仅大大方便了各种各样的用户，而且大大地提高了工作效率，并且能有效地节约企业的成本。

pcAnywhere 是赛门铁克公司的著名产品，该软件适用于所有版本的 Windows 操作系统，支持调制解调器拨号、并口/串口直接连接和 TCP/IP、NetBIOS 网络协议等多种连接方式。该软件的使用与管理方式比较灵活，用户可以按照自己的需要单独安装主控端或被控端的软件，根据需要在被控端上创建各种连接下的远程控制方案，并能根据不同的用户分配不同等级的权限。在安全性能方面，pcAnywhere 提供了多种验证方式和加密方式，用户可以直接使用网络系统上的用户资料库验证远程连接，也可以创建独立的远程控制账户，根据需要选择加密数据的方式，保证在传输的过程中数据不被窃取。

2. UNIX/Linux 系统的常见维护方式

UNIX/Linux 下通常使用 SSH 协议进行远程管理，SSH 协议为字符型界面，因为 SSH 基于成熟的公钥加密体系，所以传输的数据会进行加密，保证数据在传输的时候，不被篡改及泄露，从而提高了系统的安全性。

SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组（Network Working Group）所制定，SSH 为建立在应用层和传输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。SSH 最初是 UNIX 系统上的一个程序，后来又迅速扩展到其他操作平台，几乎所有 UNIX 平台，包括 HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix 都可运行 SSH。

SSH 的基本工作机制是本地的客户端发送一个连接请求到远程的服务端，服务端检查申请

的包和 IP 地址再发送密钥给 SSH 的客户端，本地再将密钥发回给服务端，自此连接建立。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”。

在 Linux 操作系统最流行的图形化操作软件是 VNC，VNC（Virtual Network Computer，虚拟网络计算机）是一套由 AT&T 实验室开发的可操控远程计算机的软件。根据主控端与被控端的不同，VNC 软件可以分为两个部分，分别为 VNC Server 与 VNC Viewer。前者是安装在被控制端上，而后者被安装在主控端上。VNC 软件不仅是开源的，而且是跨平台的。有不少系统管理员喜欢在 Windows 平台上使用这个 VNC 来作为远程管理 Linux 服务器或者客户端的工具。

3. 网络设备的常见维护方式

网络设备可以采用 Telnet 协议和 SSH 协议进行远程管理，在网络设备如交换机的 Telnet 设置前，应当确认已经做好以下准备工作。

（1）在用于管理的计算机中安装有 TCP/IP 协议，并配置好了 IP 地址信息。

（2）在被管理的交换机上已经配置好 IP 地址信息。如果尚未配置 IP 地址信息，则必须通过 Console 端口进行设置。

（3）在被管理的交换机上建立了具有管理权限的用户账户。

在计算机上运行 Telnet 客户端程序（这个程序在 Windows 系统中与 UNIX、Linux 系统中都有，而且用法基本是兼容的，也可以采用专用的工具，如 PuTTY），登录至远程交换机。

4. 数据库的维护方式

对于数据库可以采用命令行进行维护，也可以使用专业客户端。采用命令行方式维护需要对数据库知识非常熟悉，对 SQL 语言也需要全面了解。不仅如此，如果数据库的访问量很大，列表中数据的读取就会相当困难。为了使数据库的维护简单，通常会使用工具。

5. 其他设备或系统的维护方式

其他设备或系统，如安全设备、业务系统等，除了底层维护外，一般的业务维护可使用 https 协议进行远程管理。

https 简单来讲是 http 的安全版，http 是超文本传输协议，信息是明文传输，https 则是具有安全性的 SSL 加密传输协议。http 和 https 使用的是不同的连接方式，用的端口也不一样，前者是 80，后者是 443。http 的连接很简单，是无状态的，https 协议是由 SSL+HTTP 协议构建的可进行加密传输、身份认证的网络协议，比 http 协议安全。

使用 https 的访问方式与人们日常的网络访问无异，即通过 IE 等浏览器进行设备访问。

1.2 设备日常检查

1.2.1 一般巡检

日常巡检是指定期地对系统进行检查，确认系统工作状态，排除可能的系统运行隐患。日常巡检通常会包含一般巡检和高级巡检。

一般巡检的检查周期间隔很短，通常为日检或周检，检查内容较少，能确保系统正常工作即可，管理上也比较简单，维护人员按照检查表依次对系统进行检查，检查结果留存归档即可。一般巡检通常对硬件和软件的基本情况进行检查，包括如下内容。

（1）硬件检查

硬件检查工作主要有防尘、防雷、防静电和检查设备各部件运行情况。

灰尘对于设备的危害是不容忽视的，不但会影响这些设备的正常散热，还很容易导致主板内部的工作电路发生短路现象，严重的能导致设备不断地重新启动，甚至毁坏。

设备很容易在高电压、高电流情况下造成接口电路损坏、保险烧坏、主芯片烧毁等。有时候雷击所造成的感应电压不足以一次击坏设备，但长年累月的过压冲击，很容易引起设备零件加速老化，使设备寿命急剧下降，严重影响网络的稳定性能。因此，日常检查时应检查设备外壳可靠接地，检查连接是否紧固、接触是否良好、接地体附近地面有无异常。

静电也很容易造成设备的硬件损坏。静电能产生极高的电压将晶体管击穿，产生的瞬间电流能将连线熔断。在秋冬季节应保持机房内空气的一定湿度，在对设备进行硬件的日常维护和巡检时，先戴上防静电手环。如果没有条件的话，可以先切断电源，并将手放在墙壁或水管上接触一会儿，放掉自身静电。

设备各部件的运行状态有两种方法可以进行观察，一种是观察设备面板上各指示灯的状态，另一种方法是登录设备的配置界面进行查看。

（2）软件检查

检查设备系统运行状态的工作内容一般包括查看电源工作状态、查看 CPU 使用率、查看内存使用率、查看风扇工作状态、查看接口状态、查看日志信息、查看配置文件。

1.2.2 高级巡检

高级巡检的检查间隔周期较长，通常为季度检查或半年检查，检查内容全面，除了要确保系统正常工作以外，还需要排除可能的隐患。管理上相对复杂，需要对检查表格进行提交和确认，需要制订专门的检查计划，安排专门的时间指定专人实施检查，提交巡检报告，并对检查出来问题进行集中整改。

高级巡检的一个典型的检查表，如表 1-1 所示。该表针对的检查对象为网络设备。

表 1-1 高级巡检检查表

高级巡检检查表		
检查项目	检查子项	结果描述
1. 系统信息	1.1 双主控热备份状态 设备双主控设备的主备板同步状态为实时备份，此时主备板处于同步状态	□完全通过 □部分通过 □未涉及
	1.2 单板状态 设备所有在位单板运行在稳定状态	□完全通过 □部分通过 □未涉及
	1.3 电源状态 电源模块运行在稳定状态	□完全通过 □部分通过 □未涉及
	1.4 风扇状态 设备所有风扇模块运行在正常状态	□完全通过 □部分通过 □未涉及

续表

高级巡检检查表		
检查项目	检查子项	结果描述
1．系统信息	1.5 温度状态 路由器设备单板运行温度保持在温度上下限之间	□完全通过 □部分通过 □未涉及
	1.6 CPU 利用率 路由器设备的 CPU 利用率在 80%以下	□完全通过 □部分通过 □未涉及
	1.7 内存率 路由器设备的内存利用率在 80%以下	□完全通过 □部分通过 □未涉及
	1.8 日志告警信息	□完全通过 □部分通过 □未涉及
	1.9 存储介质空间	□完全通过 □部分通过 □未涉及
2．设备版本与基本配置	2.1 软件版本	□完全通过 □部分通过 □未涉及
	2.2 License 和 PAF 文件	□完全通过 □部分通过 □未涉及
	2.3 单板逻辑	□完全通过 □部分通过 □未涉及
	2.4 启动文件一致性 设备当前运行的软件版本与下一次启动软件版本一致	□完全通过 □部分通过 □未涉及
	2.5 配置文件一致性 要求设备当前运行的配置脚本文件和保存的配置脚本文件的内容完全一致	□完全通过 □部分通过 □未涉及
	2.6 Debug 开关 由于开启的调试信息耗费大量系统资源，要求设备关闭所有 Debug 开关	□完全通过 □部分通过 □未涉及
	2.7 系统名称	□完全通过 □部分通过 □未涉及
	2.8 系统时钟	□完全通过 □部分通过 □未涉及
	2.9 Telnet 登录安全性	□完全通过 □部分通过 □未涉及
	2.10 网络服务	□完全通过 □部分通过 □未涉及
	2.11 设备运行时间	□完全通过 □部分通过 □未涉及
	2.12 系统定义重启时间	□完全通过 □部分通过 □未涉及
3．接口配置	3.1 接口描述	□完全通过 □部分通过 □未涉及
	3.2 接口输入方向流量检查	□完全通过 □部分通过 □未涉及
	3.3 接口输出方向流量检查	□完全通过 □部分通过 □未涉及
	3.4 三层接口状态	□完全通过 □部分通过 □未涉及
	3.5 Loopback 接口地址检查	□完全通过 □部分通过 □未涉及
4. MAC 地址表容量检查	4.1 MAC 地址容量检查	□完全通过 □部分通过 □未涉及
5．ARP 协议	5.1 ARP 协议状态	□完全通过 □部分通过 □未涉及
	5.2 ARP 刷新状态 路由器设备的动态 ARP 表项数量不超过 10.8KB（12KB×90%）个	□完全通过 □部分通过 □未涉及
	5.3 ARP 老化时间 路由器设备的 ARP 老化时间为 20 分钟	□完全通过 □部分通过 □未涉及

续表

高级巡检检查表		
检查项目	检查子项	结果描述
6．STP 协议	6.1 STP 根桥保护	□完全通过 □部分通过 □未涉及
	6.2 STP 的 TC 保护	□完全通过 □部分通过 □未涉及
	6.3 STP 的环路保护	□完全通过 □部分通过 □未涉及
	6.4 STP 的边缘端口设置	□完全通过 □部分通过 □未涉及
7．VRRP 协议	7.1 VRRP 协议状态 VRRP 协议的接口在稳定时组状态为 Master、Slave 或 Backup	□完全通过 □部分通过 □未涉及
	7.2 VRRP 协议时间值	□完全通过 □部分通过 □未涉及
8．OSPF 协议	8.1 OSPF 的 Peer 状态	□完全通过 □部分通过 □未涉及
	8.2 OSPF 的错误统计 设备正常运行时不应该出现 OSPF 协议错误	□完全通过 □部分通过 □未涉及
	8.3 OSPF 虚连接的配置	□完全通过 □部分通过 □未涉及
9．ISIS 协议	9.1 ISIS System Id	□完全通过 □部分通过 □未涉及
	9.2 ISIS 邻居状态	□完全通过 □部分通过 □未涉及
	9.3 ISIS 引入外部路由	□完全通过 □部分通过 □未涉及
	9.4 ISIS Metric 类型	□完全通过 □部分通过 □未涉及
10．BGP 协议	10.1 BGP 邻居状态	□完全通过 □部分通过 □未涉及
	10.2 BGP 发布路由的合理性	□完全通过 □部分通过 □未涉及
	10.3 IBGP 邻居的优化	□完全通过 □部分通过 □未涉及
11．路由汇总信息	11.1 路由汇总信息	□完全通过 □部分通过 □未涉及
12．BGP/MPLS VPN	12.1 MPLS LSR Id	□完全通过 □部分通过 □未涉及
	12.2 LDP 邻居状态	□完全通过 □部分通过 □未涉及
	12.3 BGP VPNv4 邻居状态	□完全通过 □部分通过 □未涉及
	12.4 VPN 实例路由汇总	□完全通过 □部分通过 □未涉及
	12.5 MPLS LSP 数目	□完全通过 □部分通过 □未涉及
13．NTP 协议	13.1 NTP 协议状态 基于服务的可用性，使能 NTP 客户端功能的设备，NTP 协议同步状态应该为 synchronized	□完全通过 □部分通过 □未涉及
14．SNMP 配置	14.1 网管团体名称规范性 建议不使用 public、private 等通用名称	□完全通过 □部分通过 □未涉及
	14.2 SNMP 版本一致性	□完全通过 □部分通过 □未涉及
	14.3 Trap 功能使能 在配置 SNMP 特性时，建议开启 Trap 功能	□完全通过 □部分通过 □未涉及
	14.4 Trap 安全性	□完全通过 □部分通过 □未涉及

当系统内所有设备都检查完毕后，需要提交高级巡检报告，高级巡检报告至少需要描述以下内容。

（1）巡检工作的基本信息，包括检查的时间、检查人员姓名、配合检查相关人员姓名等。

（2）系统基本信息，包括系统名称和系统包含的设备列表。

（3）检查总表，系统所包含设备的所有检查结果汇总。