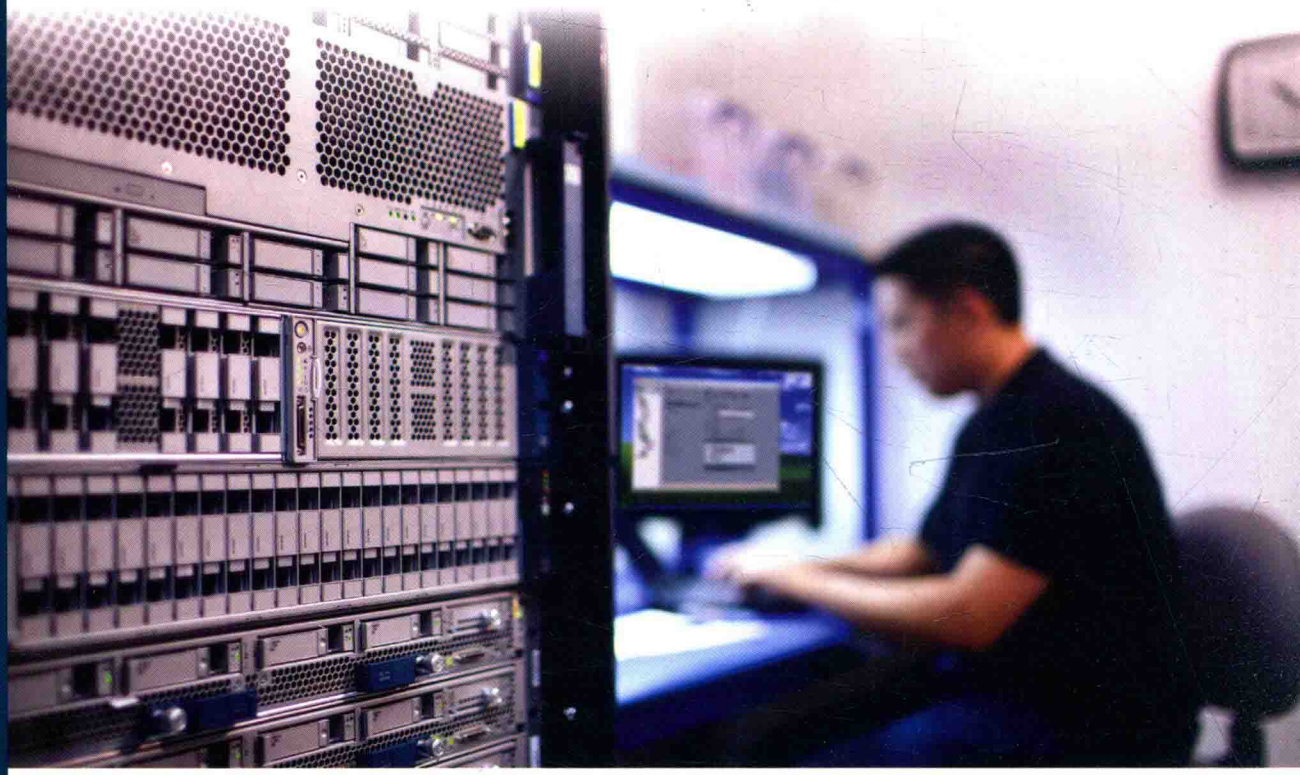
CCNP TSHOOT 300-135 学习指南

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

Foundation Learning Guide

CCNP TSHOOT 300-135



〔加〕 **Amir Ranjbar,** CCIE #8669 著

夏俊杰 译

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

CCNP TSHOOT 300-135 学习指南

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

Foundation Learning Guide

CCNP TSHOOT 300-135

〔加〕**Amir Ranjbar,** CCIE #8669 著

夏俊杰 译

人民邮电出版社

北京

图书在版编目（CIP）数据

CCNP TSHOOT 300-135学习指南 / （加）兰吉巴(Ranjbar,A.）著 ; 夏俊杰译. -- 北京 : 人民邮电出版社, 2015.11
ISBN 978-7-115-40619-4

Ⅰ. ①C… Ⅱ. ①兰… ②夏… Ⅲ. ①计算机网络－工程技术人员－资格考核－自学参考资料 Ⅳ. ①TP393

中国版本图书馆CIP数据核字(2015)第243368号

版 权 声 明

◆ 著 ［加］Amir Ranjbar，CCIE #8669
译 夏俊杰
责任编辑 傅道坤
责任印制 张佳莹 焦志炜

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路 11 号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京天宇星印刷厂印刷

◆ 开本：800×1000 1/16
印张：27.75
字数：652 千字 2015 年 11 月第 1 版
印数：1－3 000 册 2015 年 11 月北京第 1 次印刷
著作权合同登记号 图字：01-2014-7501 号

定价：79.00 元

读者服务热线：(010)81055410 印装质量热线：(010)81055316
反盗版热线：(010)81055315

内容提要

本书是 Cisco CCNP TSHOOT 认证考试的学习指南，涵盖了与 TSHOOT 考试相关的 Cisco Catalyst 交换机和路由器的各种故障检测与排除技术，包括 STP、第一跳冗余性协议、EIGRP、OSPF、BGP、路由重分发、NAT、DHCP、IPv6 以及网络安全等故障检测与排除技术，为广大备考人员提供了丰富的学习资料。为了帮助广大读者更好地掌握各章所学的知识，作者以故障工单的形式提供了大量故障案例，便于读者掌握认证考试中可能遇到的各种复杂场景，并在每章结束时的“本章小结”中总结了本章的关键知识点，方便读者随时参考和复习。此外，每章末尾提供的复习题不仅能够帮助读者评估对各章知识的掌握程度，而且还为广大考生提供了非常好的备考复习提纲。

本书主要面向备考 CCNP TSHOOT 认证考试的考生，但本书相关内容实用性很强，有助于提高大家日常网络维护和排障工作的效率，保证网络的稳定运行，因而也非常适合从事企业网及复杂网络故障检测与排除工作的工程技术人员参考。

译者序

中国互联网产业经过近 20 年的快速发展，已拥有 6.3 亿网民、12 亿手机用户、5 亿微博和微信用户，每天信息发送量超过 200 亿条，全球互联网公司十强中，中国占了 4 家，这些都表明中国的互联网已经进入了一个崭新的发展天地，越来越多的人接触到了互联网，并从互联网世界中获益。特别是中国政府提出“互联网+”战略之后，各行各业都在拥抱互联网，互联网已经从消费型互联网向产业型互联网转移，在社会经济生活中的作用越来越大，人们对互联网的认识也越来越高。在此形势下，电信运营商、ISP 以及企业网的规模不断增大，网络应用的复杂性日新月异，企业对网络的依赖性也日益加大，保障网络的高可用性是所有网络用户共同的呼声，新形势下网络用户对新业务的发展需求推动了各类新业务的广泛部署，使得包括组播、VPN、BGP 等在内的各种复杂技术在企业网中得到大量应用。其次，IPv4 地址空间已经分配完毕，大家不得不正视 IPv4 向 IPv6 过渡的问题，再加上近年来互联网安全事故的增多，使得人们越来越关注互联网以及信息化的安全性。所有的这一切都对互联网从业人员提出了更高、更迫切的要求。全面掌握各类网络故障的检测与排除技术是技术人员保障企业网高效稳定运行、减少因网络宕机而造成损失的重要技能和责任，因而本书对广大 CCNP TSHOOT 考生以及从事企业网设计、优化、排障工作的网络管理员来说，都具有非常重要的参考价值。

本书作者是互联网通信领域的资深专家，对 STP、第一跳冗余性协议、EIGRP、OSPF、BGP、路由重分发、NAT、DHCP 以及 IPv6 和网络安全等各种交换和路由故障检测与排除技术做了深入剖析和延展，本书作为 CCNP TSHOOT 课程的官方学习教材，紧扣 TSHOOT 考试要求，提供了大量故障案例，不但便于读者学习和理解，而且也极具实用参考价值，完全可以应用于复杂企业网的日常维护，译者在翻译过程中更是收获良多，相信本书一定可以成为相关从业人员的案头参考书。

在本书翻译过程中，得到了家人和人民邮电出版社编辑及朋友们的无私支持与帮助，在此一并表示衷心的感谢。

本书内容涉及面广，虽然在翻译过程中为了尽量准确表达作者原意，特别是某些专有名词术语的译法，译者在多年网络通信工程经验的基础上，查阅了大量的相关书籍及标准规范，但由于时间仓促，加之译者水平有限，译文中仍难免有不当之处，敬请广大读者批评指正。

夏俊杰　xiajunjie@msn.com

2015 年 10 月于北京

关于作者

Amir Ranjbar，CCIE #8669，是Cisco认证讲师和高级网络咨询师，创办了AMIRACAN公司，为 Global Knowledge Network 公司提供培训服务，并为各类用户（主要是 Internet 服务提供商）提供咨询服务，同时还为 Cisco Press（Pearson 教育集团）编写技术图书。Amir 出生在伊朗德黑兰，于 1983 年在其 16 岁时移民加拿大，于 1991 年获得知识系统（AI 的一个分支）的硕士学位。日常主要从事培训、咨询及技术写作等工作，可以通过电子邮件 aranjbar@amiracan.com 与 Amir Ranjbar 取得联系。

关于技术审稿人

Ted Kim，CCIE #22769（RS 与 SP 方向），拥有 10 年以上的 IT 从业经验，最近几年重点研究数据中心技术，拥有丰富的大型企业网设计、部署及排障经验。在 Ted 的网络职业生涯中，最初是 Johns Hopkins 的网络工程师，后来于 2013 年加入 Cisco 公司并成为一名网络咨询工程师。

献辞

谨将本书献给我的父亲 Kavos Ranjbar 先生，他于 2013 年 1 月 2 日离开了我们。希望我们能够像父亲那样，永远保持爱心、乐于助人、宽宏大量，而且始终谦逊、热爱和平、温文尔雅。

致谢

本书是大家共同努力的结晶，无论我们是否曾经共同工作过，都希望为所有参与人员奉上最诚挚的谢意。感谢 Mary Beth Ray、Ellie Bru、Tonya Simpson、Keith Cline、Vanessa Evans、Mark Shirar、Trina Wurst 和 Lisa Stumpf 为本书的最终完成付出的大量时间和精力，我渴望再次参加 Person 教育集团的社交聚会并向所有人员当面表达感激之情。感谢 Ted Kim 对本书做出了细致认真的审校工作并提出了大量有益反馈，同样希望有机会能够当面表达我的感激之情。

前言

本书基于 Cisco 公司最新发布的 CCNP 认证考试的 TSHOOT 课程，描述了 Cisco 路由和交换领域的排障及维护知识。本书假定读者已经了解并掌握了 Cisco ROUTE 和 SWITCH 课程所涉及的路由和交换知识。本书为读者提供了足够的 TSHOOT 考试信息。

讲授故障检测与排除技术实非易事，本书向读者展现了很多故障检测与排除方法，并深入分析了这些方法的优缺点。虽然本书扼要回顾了路由与交换的一些基本知识，但重点是讨论各种故障检测与排除命令的使用方法，特别是讲解大量故障检测与排除案例。每章最后的复习题不但能够帮助读者评估对各章知识的掌握程度，而且也可以为备考复习提供非常好的补充材料。

本书阅读对象

本书对任何希望学习现代网络故障检测与排除方法及技术，以及任何希望找到对自己有用的故障检测与排除案例的读者来说都非常有价值，对那些已经拥有一定的路由和交换基础知识，同时又希望进一步学习或增强故障检测与排除技巧的读者来说更为有用。正在备考 Cisco TSHOOT 考试的读者可以从本书找到成功通过认证考试所需的全部内容。Cisco 网络技术学院将本书作为 CCNP TSHOOT 课程的官方教材。

Cisco 认证和考试

Cisco 提供了 4 个级别的路由和交换认证，每个认证级别的专业能力都依次递增，它们分别为入门级、助理级、专业级和专家级。这些认证级别就是常说的 CCENT、CCNA、CCNP 和 CCIE，虽然 Cisco 还提供了其他认证，但本书关注的是与企业网络相关的认证。

对于 CCNP 路由和交换认证来说，必须通过 SWITCH、ROUTE 和 TSHOOT 三门考试。由于 Cisco 通常并不对外公布各种认证考试的合格成绩，因而大家只有在参加完考试之后才能知道是否通过了认证考试。

如果希望了解 CCNP 路由和交换认证的最新需求和最新动态，请访问 Cisco.com 并点击 **Training and Events**，以了解认证考试的细节信息，如考试主题以及注册考试的方式等。

对于备考 TSHOOT 的读者来说，使用本书的策略可能与其他读者有些不同，主要与读者的技巧、知识和经验有关。例如，参加了 TSHOOT 教育课程的读者与通过在职培训学习故障检测与排除技术的读者所采取的策略就有所不同。无论采取哪种策略或者知识背景如何，本书都能指导大家花费最少的时间去通过认证考试。

本书组织方式

虽然可以按部就班地逐页阅读本书，但本书也提供了更为灵活的阅读方式，读者可以根据需要以章节为基础进行跳跃式阅读。虽然某些章节之间具有一定的关联性，但大家完全可以根据自己的情况不按照这些章节顺序阅读本书；如果大家准备通读本书，那么按照本书编排顺序进行阅读应该是最佳方式。

本书每章都覆盖了 CCNP TSHOOT 考试主题的部分内容，以下是本书各章的内容简介。

- 第 1 章介绍了故障检测与排除原理，并讨论了最常见的故障检测与排除方法。
- 第 2 章解释了结构化故障检测与排除方法，并分析了结构化故障检测与排除方法包含的所有子进程。
- 第 3 章介绍了结构化网络维护模型并讨论了网络维护进程和流程，同时讨论了网络维护服务及网络维护工具，探讨了将故障检测与排除操作融入日常网络维护进程的方式与方法。
- 第 4 章回顾了二层交换进程和三层路由进程，并且讨论了利用 IOS **show** 命令、**debug** 命令，以及 ping、Telnet 等工具进行选择性地信息收集工作的方法。
- 第 5 章讨论了故障检测与排除工具，包括流量抓取特性及相关工具、利用 SNMP 收集信息、利用 NetFlow 收集信息以及基于 EEM 的网络事件通告机制。
- 第 6 章到第 10 章都是故障检测与排除案例，每章的示例网络及故障问题均不相同，每个故障都采用现实世界中的故障工单方式，按照结构化故障检测与排除方法，利用相应的排障技术解决故障问题，并且所有故障检测与排除阶段（包括收集信息阶段）都给出了详细的 Cisco IOS 路由器和交换机的输出结果。第 6 章到第 10 章的开头和结尾均提供了网络结构图，为便于参考，读者可以在线下载并打印这些网络结构图的 PDF 文件，也可以在电子设备上查看这些 PDF 文件。访问 ciscopress.com/title/9781587204555 并点击 **Downloads** 即可下载这些 PDF 文件。

此外，本书附录还提供了每章复习题的参考答案。

本书使用的图标

命令语法约定

本书在介绍命令语法时使用与 IOS 命令参考一致的约定，本书涉及的命令参考约定如下：

- 需要逐字输入的命令和关键字用粗体表示，在配置示例和输出结果（而不是命令语法）中，需要用户手工输入的命令用粗体表示（如 **show** 命令）；
- 必须提供实际值的参数用斜体表示；
- 互斥元素用竖线（|）隔开；
- 中括号[ ]表示可选项；
- 大括号表示{ }必选项；
- 中括号内的大括号[{ }]表示可选项中的必选项。

目录

第 1 章

故障检测与排除方法

大多数现代企业都高度依赖网络基础设施的平稳运行。网络宕机时间常常意味着产能、利润和声誉的损失，因而网络故障检测与排除是企业网络支持团队的重要职能。网络支持团队的故障诊断与解决效率越高，企业遭受的损失就越少。对于复杂网络环境来说，故障检测与排除工作是一件令人头痛的事情，要想快速有效地诊断并解决故障，就必须遵循结构化的故障检测与排除方法。结构化的网络故障检测与排除方法需要定义完善的故障检测与排除流程并加以文档化、制度化。

本章将首先介绍故障检测与排除的概念及基本原理，然后讨论 6 种常见的故障检测与排除方法，最后将利用这 6 种故障检测与排除方法来解释相应的故障检测与排除案例。

1.1 故障检测与排除原理

故障检测与排除是一种诊断故障并解决故障（如果可能的话）的过程，故障检测与排除操作通常是由用户报告故障所触发的。对于部署了主动式网络监控工具和技术的现代复杂网络来说，完全可以在用户发现故障或者商业应用受到影响之前就发现故障/问题，甚至修正或解决故障/问题。

某些人直到发现问题并认为是故障且被报告为故障时才知道网络中出现了故障，这就意味着需要找出所报告故障（受限于用户的经验）与实际故障原因之间的差别。报告故障的时间不一定就是产生故障的事件发生时间，报告故障的用户有时会将故障等同于故障现象，而排障人员常常将故障等同于故障根源。例如，某小型企业的 Internet 连接在周六出现了故障，这通常并不是一个故障，但是如果 Internet 连接在周一上午上班时间仍未修复，那么就会演变为故障。虽然故障现象与故障原因之间的差异看起来似乎有些难以理解，但大家必须意识到两者的差异会产生潜在的沟通问题。

通常来说，故障报告会触发故障检测与排除流程。检测与排除故障时，首先要定义故障问题，其次在收集信息、重新定义故障、提出可能的故障原因期间诊断故障，最后就是推断故障的根本性原因。此时就可以提出可能的故障解决方案并加以评估，然后选出最佳解决方案并加以实施。图 1-1 给出了结构化故障检测与排除方法的主要步骤以及这些步骤之间存在的各种转移可能性。

> 注：值得注意的是，有时不一定能够实施网络故障解决方案，此时可能需要搭建一个临时工作环境。解决方案与临时工作环境之间的区别就在于解决方案能够解决故障根源，而临时工作环境只是缓解了故障现象。

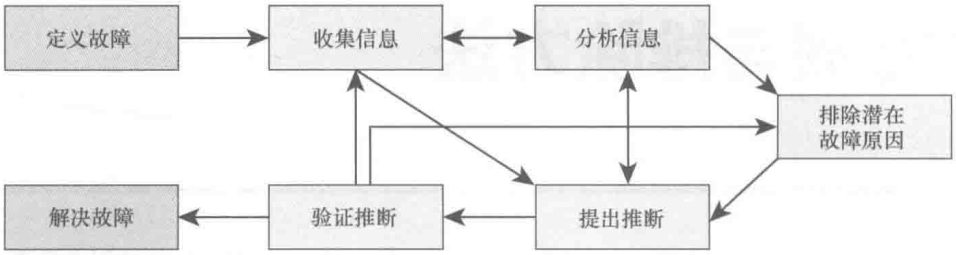


图 1-1 结构化故障检测与排除方法示意图

虽然报告故障和解决故障是故障检测与排除流程中的基本要素，但大部分时间都花在了故障诊断阶段，甚至有些人认为故障检测与排除过程就是故障诊断过程。但无论如何，在网络维护的概念中，报告故障和解决故障确实是故障检测与排除流程中的基本要素，而故障诊断则是发现故障本质以及故障原因的进程，该进程的主要步骤如下。

- **收集信息**：在接到用户（或其他任何人）报告的故障信息之后，就要开始收集信息，包括调研故障所涉及的所有人员（用户）以及采用各种可能的手段收集相关信息。通常来说，故障报告包含的信息都不足以让排障人员做出合理推断，因而所要做的第一件事情就是收集信息。既可以通过观测直接收集信息，也可以通过测试间接收集信息。
- **分析信息**：检查和分析完收集到的信息之后，排障人员就可以将故障现象与自己掌握的系统、进程和基线数据的信息进行分析比对，以便将正常状态从异常状态中分离出来。
- **排除潜在故障原因**：通过将观察到的网络运行状态与期望状态进行对比，就可以排除某些潜在的故障原因。
- **提出推断**：收集和分析信息并排除了潜在故障原因之后，将会剩下一个或若干个潜在故障原因。需要仔细评估每个潜在故障原因的可能性，并推断最可能的故障原因。
- **验证推断**：需要进一步测试推断出的根本性故障原因，以证实或否决该原因是否是故障根源。最简单的方式就是根据故障推断制定解决方案，并验证该解决方案是否有效。如果无效，那么就表明前面的推断有误，就需要进一步收集并分析更多信息。

所有的故障检测与排除方法都包括收集信息、分析信息、排除潜在故障原因、提出推断、验证推断等几个基本步骤，每个步骤都有其用意，需要花费一定的时间和精力，弄清楚如何以及何时从一个步骤过渡到下一个步骤是成功进行故障检测与排除工作的关键。在检测与排除复杂应用场景下的网络故障时，有时可能需要在故障检测与排除的不同阶段之间不断地进行反复操作：收集信息、分析信息、排除潜在故障原因、收集更多信息、再次分析这些信息、提出推断、验证推断、否决推断、排除更多潜在故障原因、收集更多信息，等等。