

<<自顶向下网络设计>>

图书基本信息

书名：<<自顶向下网络设计>>

13位ISBN编号：9787115265449

10位ISBN编号：7115265445

出版时间：2011-11

出版时间：人民邮电出版社

作者：奥本海默

页数：447

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<自顶向下网络设计>>

内容概要

本书是围绕自顶向下网络设计步骤编写的，提供给网络设计者一种系统的结构化网络设计方法。

本书分为4个部分，即客户需求和目标、逻辑网络设计、物理网络设计，以及网络测试、优化和文档编写。

4个部分分别对应着网络

设计的各个重要阶段，每个阶段都提供给读者详细的设计指导原则，内容涵盖网络设计的方方面面。本书从用户商业和技术目标的分析入手，从而制定出相应的网络流量、负载和qos需求，进而开发网络的逻辑拓扑结构，然后进入地址规划、协议选择、网络安全和网络管理实施策略制定，最后是对网络设备的选型建议以及网络实施、测试和文档编写。

本书每章以复习题和设计环境作为一章的总结和回顾，理论与实践相结合，从而让读者更好地理解 and 掌握自顶向下网络设计的思想。

本书适合cisco代理商、网络运营商、其他网络设备商的网络部署人员、售后技术支持人员阅读；网络维护人员，以及网络技术爱好者也可以从本书中获益。

<<自顶向下网络设计>>

作者简介

作者：(美国)奥本海默(Priscilla Oppenheimer)

<<自顶向下网络设计>>

书籍目录

introduction xxii

part i identifying your customer's needs and goals

chapter analyzing business goals and constraints

using a top-down network design methodology

using a structured network design process

systems development life cycles

plan design implement operate optimize (pdioo) network life cycle

analyzing business goals

working with your client

changes in enterprise networks

networks must make business sense

networks offer a service

the need to support mobile users

the importance of network security and resiliency

typical network design business goals

identifying the scope of a network design project

identifying a customer's network applications

analyzing business constraints

politics and policies

.budgetary and staffing constraints

project scheduling

business goals checklist

summary

review questions

design scenario

chapter analyzing technical goals and tradeoffs

scalability

planning for expansion

expanding access to data

constraints on scalability

availability

disaster recovery

specifying availability requirements

five nines availability

the cost of downtime

mean time between failure and mean time to repair

network performance

network performance definitions

optimum network utilization

throughput

throughput of internetworking devices

application layer throughput

accuracy

efficiency

<<自顶向下网络设计>>

delay and delay variation
causes of delay
delay variation
response time
security
identifying network assets
analyzing security risks
reconnaissance attacks
denial-of-service attacks
developing security requirements
manageability
usability
adaptability
affordability
making network design tradeoffs
technical goals checklist
summary
review questions
design scenario
chapter characterizing the existing internetwork
characterizing the network infrastructure
developing a network map
characterizing large internetworks
characterizing the logical architecture
developing a modular block diagram
characterizing network addressing and naming
characterizing wiring and media
checking architectural and environmental constraints
checking a site for a wireless installation
performing a wireless site survey
checking the health of the existing internetwork
developing a baseline of network performance
analyzing network availability
analyzing network utilization
measuring bandwidth utilization by protocol
analyzing network accuracy
analyzing errors on switched ethernet networks
analyzing network efficiency
analyzing delay and response time
checking the status of major routers, switches, and
firewalls
network health checklist
summary
review questions
hands-on project
design scenario
chapter characterizing network traffic

<<自顶向下网络设计>>

characterizing traffic flow
identifying major traffic sources and stores
documenting traffic flow on the existing network
characterizing types of traffic flow for new network applications
terminal/host traffic flow
client/server traffic flow
peer-to-peer traffic flow
server/server traffic flow
distributed computing traffic flow
traffic flow in voice over ip networks
documenting traffic flow for new and existing network applications
characterizing traffic load
calculating theoretical traffic load
documenting application-usage patterns
refining estimates of traffic load caused by applications
estimating traffic load caused by routing protocols
characterizing traffic behavior
broadcast/multicast behavior
network efficiency
frame size
windowing and flow control
error-recovery mechanisms
characterizing quality of service requirements
atm qos specifications
constant bit rate service category
real-time variable bit rate service category
non-real-time variable bit rate service category
unspecified bit rate service category
available bit rate service category
guaranteed frame rate service category
ietf integrated services working group qos specifications
controlled-load service
guaranteed service
ietf differentiated services working group qos specifications
grade of service requirements for voice applications
documenting qos requirements
network traffic checklist
summary
review questions
design scenario
summary for part i
part ii logical network design
chapter designing a network topology
hierarchical network design

<<自顶向下网络设计>>

why use a hierarchical network design model?

flat versus hierarchical topologies

flat wan topologies

flat lan topologies

mesh versus hierarchical-mesh topologies

classic three-layer hierarchical model

core layer

distribution layer

access layer

guidelines for hierarchical network design

redundant network design topologies

backup paths

load sharing

modular network design

cisco safe security reference architecture

designing a campus network design topology

spanning tree protocol

spanning tree cost values

rapid spanning tree protocol

rstp convergence and reconvergence

selecting the root bridge

scaling the spanning tree protocol

virtual lans

fundamental vlan designs

wireless lans

positioning an access point for maximum coverage

wlans and vlans

redundant wireless access points

redundancy and load sharing in wired lans

server redundancy

workstation-to-router redundancy

hot standby router protocol

gateway load balancing protocol

designing the enterprise edge topology

redundant wan segments

circuit diversity

multihoming the internet connection

virtual private networking

site-to-site vpns

remote-access vpns

service provider edge

secure network design topologies

planning for physical security

meeting security goals with firewall topologies

summary

review questions

design scenario

<<自顶向下网络设计>>

chapter designing models for addressing and numbering
guidelines for assigning network layer addresses
using a structured model for network layer addressing
administering addresses by a central authority
distributing authority for addressing
using dynamic addressing for end systems
ip dynamic addressing
ip version dynamic addressing
zero configuration networking
using private addresses in an ip environment
caveats with private addressing
network address translation
using a hierarchical model for assigning addresses
why use a hierarchical model for addressing and routing?
hierarchical routing
classless interdomain routing
classless routing versus classful routing
route summarization (aggregation)
route summarization example
route summarization tips
discontiguous subnets
mobile hosts
variable-length subnet masking
hierarchy in ip version addresses
link-local addresses
global unicast addresses
ipv addresses with embedded ipv addresses
designing a model for naming
distributing authority for naming
guidelines for assigning names
assigning names in a netbios environment
assigning names in an ip environment
the domain name system
dynamic dns names
ipv name resolution
summary
review questions
design scenario
chapter selecting switching and routing protocols
making decisions as part of the top-down network design
process
selecting switching protocols
switching and the osi layers
transparent bridging
selecting spanning tree protocol enhancements
portfast
uplinkfast and backbonefast

<<自顶向下网络设计>>

unidirectional link detection
loopguard
protocols for transporting vlan information
ieee .q
dynamic trunk protocol
vlan trunking protocol
selecting routing protocols
characterizing routing protocols
distance-vector routing protocols
link-state routing protocols
routing protocol metrics
hierarchical versus nonhierarchical routing protocols
interior versus exterior routing protocols
classful versus classless routing protocols
dynamic versus static and default routing
on-demand routing
scalability constraints for routing protocols
routing protocol convergence
ip routing
routing information protocol
enhanced interior gateway routing protocol
open shortest path first
intermediate system-to-intermediate system
border gateway protocol
using multiple routing protocols in an internetwork
routing protocols and the hierarchical design model
redistribution between routing protocols
integrated routing and bridging
a summary of routing protocols
summary
review questions
design scenario
chapter developing network security strategies
network security design
identifying network assets
analyzing security risks
analyzing security requirements and tradeoffs
developing a security plan
developing a security policy
components of a security policy
developing security procedures
maintaining security
security mechanisms
physical security
authentication
authorization
accounting (auditing)

<<自顶向下网络设计>>

data encryption
public/private key encryption
packet filters
firewalls
intrusion detection and prevention systems
modularizing security design
securing internet connections
securing public servers
securing e-commerce servers
securing remote-access and vpns
securing remote-access technologies
securing vpns
securing network services and network management
securing server farms
securing user services
securing wireless networks
authentication in wireless networks
data privacy in wireless networks
summary
review questions
design scenario
chapter developing network management strategies
network management design
proactive network management
network management processes
fault management
configuration management
accounting management
performance management
security management
network management architectures
in-band versus out-of-band monitoring
centralized versus distributed monitoring
selecting network management tools and protocols
selecting tools for network management
simple network management protocol
management information bases (mib)
remote monitoring (rmon)
cisco discovery protocol
cisco netflow accounting
estimating network traffic caused by network management
summary
review questions
design scenario
summary for part ii
part iii physical network design
chapter selecting technologies and devices for campus

<<自顶向下网络设计>>

networks
lan cabling plant design
cabling topologies
building-cabling topologies
campus-cabling topologies
types of cables
lan technologies
ethernet basics
ethernet and ieee .
ethernet technology choices
half-duplex and full-duplex ethernet
-mbps ethernet
gigabit ethernet
-gbps ethernet
selecting internetworking devices for a campus network design
criteria for selecting campus internetworking devices
optimization features on campus internetworking devices
example of a campus network design
background information for the campus network design project
business goals
technical goals
network applications
user communities
data stores (servers)
current network at wvcc
traffic characteristics of network applications
summary of traffic flows
performance characteristics of the current network
network redesign for wvcc
optimized ip addressing and routing for the campus backbone
wireless network
improved performance and security for the edge of the network
summary
review questions
design scenario
chapter selecting technologies and devices for enterprise networks
remote-access technologies
ppp
multilink ppp and multichassis multilink ppp
password authentication protocol and challenge handshake authentication protocol
cable modem remote access
challenges associated with cable modem systems
digital subscriber line remote access

<<自顶向下网络设计>>

- other dsl implementations
- ppp and adsl
- selecting remote-access devices for an enterprise network design
- selecting devices for remote users
- selecting devices for the central site
- wan technologies
- systems for provisioning wan bandwidth
- leased lines
- synchronous optical network
- frame relay
- frame relay hub-and-spoke topologies and subinterfaces
- frame relay congestion control mechanisms
- frame relay traffic control
- frame relay/atm interworking
- atm
- ethernet over atm
- metro ethernet
- selecting routers for an enterprise wan design
- selecting a wan service provider
- example of a wan design
- background information for the wan design project
- business and technical goals
- network applications
- user communities
- data stores (servers)
- current network
- traffic characteristics of the existing wan
- wan design for klamath paper products
- summary
- review questions
- design scenario
- summary for part iii
- part iv testing, optimizing, and documenting your network design
- chapter testing your network design
- using industry tests
- building and testing a prototype network system
- determining the scope of a prototype system
- testing a prototype on a production network
- writing and implementing a test plan for your network design
- developing test objectives and acceptance criteria
- determining the types of tests to run
- documenting network equipment and other resources
- writing test scripts
- documenting the project timeline
- implementing the test plan

<<自顶向下网络设计>>

tools for testing a network design
types of tools
examples of network testing tools
ciscoworks internetwork performance monitor
wandl network planning and analysis tools
opnet technologies
ixia tools
netiq voice and video management solution
netpredict ' s netpredictor
summary
review questions
design scenario
chapter optimizing your network design
optimizing bandwidth usage with ip multicast technologies
ip multicast addressing
internet group management protocol
multicast routing protocols
distance vector multicast routing protocol
protocol independent multicast
reducing serialization delay
link-layer fragmentation and interleaving
compressed real-time transport protocol
optimizing network performance to meet quality of service requirements
ip precedence and type of service
ip differentiated services field
resource reservation protocol
common open policy service protocol
classifying lan traffic
cisco ios features for optimizing network performance
switching techniques
classic methods for layer packet switching
netflow switching
cisco express forwarding
queuing services
first-in, first-out queuing
priority queuing
custom queuing
weighted fair queuing
class-based weighted fair queuing
low-latency queuing
random early detection
weighted random early detection
traffic shaping
committed access rate
summary
review questions

<<自顶向下网络设计>>

design scenario
chapter documenting your network design
responding to a customer ' s request for proposal
contents of a network design document
executive summary
project goal
project scope
design requirements
business goals
technical goals
user communities and data stores
network applications
current state of the network
logical design
physical design
results of network design testing
implementation plan
project schedule
project budget
return on investment
design document appendix
summary
review questions
design scenario
glossary
index

章节摘录

版权页：插图：One advantage of private network numbers is security. Private network numbers are not advertised to the Internet. Private network numbers must not be advertised to the Internet because they are not globally unique. By not advertising private internal network numbers, a modicum of security is achieved. Additional security, including firewalls and intrusion detection systems, should also be deployed, as discussed in Chapter 5, “Designing a Network Topology,” and Chapter 8. Developing Network Security Strategies. Private addressing also helps meet goals for adaptability and flexibility. Using private addressing makes it easier to change ISPs in the future. If private addressing has been used, when moving to a new ISP, the only address changes required are in the router or firewall providing NAT services and in any public servers. You should recommend private addressing to customers who want the flexibility of easily switching to a different ISP in the future. Another advantage of private network numbers is that an enterprise network can advertise just one network number, or a small block of network numbers, to the Internet. It is good practice to avoid advertising many network numbers to the Internet. One of the goals of modern Internet practices is that Internet routers should not need to manage huge routing tables. As an enterprise network grows, the network manager can assign private addresses to new networks, rather than requesting additional public network numbers from an ISP or RIR. This avoids increasing the size of Internet routing tables. Private network numbers let a network designer reserve scarce Internet addresses for public servers. During the mid-1990s, as the Internet became commercialized and popularized, a scare rippled through the Internet community about the shortage of addresses. Dire predictions were made that no more addresses would be available by the turn of the century. Because of this scare, many companies (and many ISPs) were given a small set of addresses that needed to be carefully managed to avoid depletion. These companies recognize the value of private addresses for internal networks.

<<自顶向下网络设计>>

编辑推荐

《自顶向下网络设计(英文版)(第3版)》：学习网络设计流程。确保网络运作良好而且具有安全性，同时还可以进行扩展.以满足带宽的增长需求：制定网络设计.来为实时应用（比如多媒体、远程教学、视频会议、Teleprescene、虚拟通信和IP电话通讯）提供高带宽和低延迟：掌握用于检查现有网络健康状况的技术.并定制基线来测量新网络设计的性能；制定满足QOS需求的解决方案，其中包括IETF控制的负载和保障服务、IP组播、高级交换、队列和路由算法；识别各种交换和路由协议的优势和劣势。

其中包括RSTP、IEEE 802.1Q、EIGRP、OSPF和BGP4。

《自顶向下网络设计(英文版)(第3版)》是网络技术系列丛书之一。

该系列丛书可以为网络从业人员提供搭建高效网络、学习最新技术、打造辉煌职业生涯所需要的宝贵信息。

《自顶向下网络设计(英文版)(第3版)》新增并扩展了无线网络、VPN、网络安全、网络冗余性、模块化网络设计、IPv4和IPv6的动态寻址、以太网可扩展性选项包括10Gbit/S以太网、城域以太网和长距离以太网），以及承载语音 / 数据流量的网络等相关内容。

除此之外。

读者还将学到如何设计出符合CISCO SAFE安全参考架构的网络，使其能够支持实时视频、协同计算和社交网络工具。

Priscilla Oppenheimer自从1980年在密歇根大学获得信息科学硕士学位后，就投身于数据通信和网络系统的开发。

在以软件开发人员身份工作数年之后，她成为技术指导讲师和培训开发师，并教授过3000余名来自世界500强企业的网络工程师。

她曾先后供职于苹果公司、Network General和思科公司，这些工作经历使她有机会开发一套实用的方法来进行企业网络设计。

Priscilla在世界各地讲授网络设计、配置和排错课程，这使得她可以去实践她在网络咨询业务中的观点。

<<自顶向下网络设计>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>