

Contents

Preface	xxv
Chapter 1: TCP/IP Overview	1
Introduction	2
TCP/IP's "Net" Worth	2
More Power, More Flexibility—and More Potential for Problems	4
What's Ahead in This Chapter	4
TCP/IP: Where It Came From, and Where It's Going	5
History of the TCP/IP Protocols	5
The Role of the U.S. Department of Defense	6
From ARPANet to the Internet	7
Another Contender for the Title: The OSI Protocol Suite	8
The Future of TCP/IP	10
Looking Ahead to IPv6	10
Networking Models	14
The Purpose of the Models	15
Why Use Layered Models?	15
The ISO OSI Model	16
Seven Layers of the Networking World	16
Layer 7: The Application Layer	18
Layer 6: The Presentation Layer	19
Layer 5: The Session Layer	20
Layer 4: The Transport Layer	21
Layer 3: The Network Layer	24
Layer 2: The Data Link Layer	25
Layer 1: The Physical Layer	29
The DoD Model	33
The Application/Process Layer	34
The Host-to-Host (Transport) Layer	34
The Internetworking Layer	34
The Network Interface Layer	34
The Microsoft Windows 2000 Networking Model	34
The Application and User Mode Services Component	35
The API Boundary Layer	36
The File System Drivers	37
The TDI Boundary Layer	37
The Network Transport Protocol Component	38
The NDIS Boundary Layer	38
The NDIS Wrapper	38
A Family of Protocols: The TCP/IP Suite	38
Application Layer Protocols	38
FTP	39
SNMP	39

Telnet	40
SMTP	40
HTTP	41
NNTP	41
Transport Layer Protocols	42
TCP	42
UDP	42
Network Layer Protocols	42
IP	42
ARP and RARP	42
ICMP	43
IGMP	43
TCP/IP Utilities	43
Basic Network Design	44
Planning as Preventative Medicine	44
Testing and Implementation	44
Prototyping	44
Pilot Programs	45
Rollout	46
Summary	47
FAQs	48

Chapter 2: Setting Up a Windows 2000 TCP/IP Network

51

Introduction	52
Designing a New Windows 2000 TCP/IP Network	52
The Planning Team	53
Planning the Hardware Configurations	53
Planning the Physical Layout	54
Diagramming the Network Layout	55
Planning for Sites	56
What Is an Active Directory Site?	56
Planning the Namespace	59
Planning the Addressing Scheme	60
Installing and Configuring Windows 2000 TCP/IP	61
Installing TCP/IP on a Windows 2000 Computer	62
The Protocol Installation Process	63
Configuring TCP/IP	66
Upgrading to Windows 2000 from Windows NT 4.0	68
The Windows NT Domain Models	68
Single Domain	69
Single Master Domain	69
Multiple Master Domains	71
Complete Trust	72

Which Model Is Easiest to Upgrade?	73
Other Pre-Upgrade Issues	75
Windows 32-Bit Applications	75
DOS Applications	75
Windows 16-Bit Applications	76
OS/2 and POSIX Application Support in Windows 2000	76
Application Support Summary	77
Common Upgrade Problems	78
Migrating to Windows 2000 from Novell NetWare	78
Understanding the NetWare Implementation of TCP/IP	79
Premigration Issues	80
Using the Directory Services Migration Tool	80
Common Migration Problems	82
Migrating to Windows 2000 from UNIX	82
Understanding the UNIX Implementation of TCP/IP	83
Summoning the Daemons	83
UNIX TCP/IP Utilities	83
Peaceful Coexistence: The Hybrid Network Environment	84
NetWare Interoperability	84
Client Services for NetWare (CSNW)	85
Gateway Services for NetWare (GSNW)	85
NetWare Protocol Support	85
File and Print Services for NetWare	85
Troubleshooter	86
UNIX Interoperability	86
Interoperability with IBM Mainframe Networks	86
Summary	87
FAQs	88
Chapter 3: General Windows 2000 TCP/IP	
Troubleshooting Guidelines	91
Introduction	92
The Ten Commandments of Troubleshooting	92
1: Know Thy Network	92
2: Use the Tools of the Trade	93
3: Take It One Change at a Time	93
4: Isolate the Problem	94
5: Recreate the Problem	95
6: Don't Overlook the Obvious	95
7: Try the Easy Way First	96
8: Document What You Do	96
9: Practice the Art of Patience	97
10: Seek Help from Others	98
Windows 2000 Troubleshooting Resources	99
Microsoft Documentation	99

Help Files	100
Resource Kits	101
White Papers	102
TechNet	103
Newsgroups	104
Third-Party Documentation	105
Internet Mailing Lists	105
Usenet Newsgroups	106
Web Resources	106
General Troubleshooting Models	107
Differential Diagnosis Model	108
Examination	108
Diagnosis	109
Treatment	109
Follow-Up	109
SARA Model	110
Scanning	110
Analysis	111
Response	111
Assessment	112
Putting the Models to Work for You	112
The Information-Gathering Phase	112
Questions to Ask	112
Question Format	113
Log Files	117
Application Log	117
System Log	117
Security Log	120
Tools of the Trade	122
The Problem Isolation Phase	122
Organizing and Analyzing the Information	123
Setting Priorities	125
Prioritizing the Problems	126
Prioritizing the Solutions	126
Taking Corrective Measures	127
One Change at a Time	127
Order of Implementation	127
Monitoring Results	127
Using Forms and Check lists	128
Summary	131
FAQs	133
Chapter 4: Windows 2000 TCP/IP Internals	135
Introduction	136
RFC Compliance	136
Enhancements to the TCP/IP Stack in Windows 2000	138
RFC 1323: TCP Extensions for High Performance	140

Scalable TCP Window Size	140
TCP Timestamps	150
RFC 2018: SACK (Selective Acknowledgment)	152
RFC 1577: IP over ATM	153
RFC 2001: TCP Fast Retransmit	155
RFCs 2211 and 2212: Quality of Service	156
RFC 2205: Resource Reservation Protocol	157
IPSec	158
Purpose and Uses of IPSec	158
IP Security Options	159
IPSec Configuration	160
IPSec Troubleshooting	161
NDIS 5.0	164
Inside the Windows 2000 Internet Protocol (IP)	165
Classless Inter-Domain Routing	166
Multihoming	167
Problems Related to Multihoming	168
IP Multicasting	169
Multicast Address Range	170
Troubleshooting IP Multicasting	171
Duplicate IP Address Detection	171
Inside the Windows 2000 Transport Protocols (TCP and UDP)	172
Transmission Control Protocol	172
Dead Gateway Detection	173
Delayed Acknowledgments	173
TCP Keep-Alives	174
Avoiding the Silly Window Syndrome	174
User Datagram Protocol	175
Understanding TCP/IP Registry Settings	175
Using the Registry Editing Tools	176
Configuring TCP/IP Behavior through the Registry	178
Creating a New Value	179
Editing Common TCP/IP Registry Values	180
Registry Settings that Should Not Be Edited	181
Summary	182
FAQs	185
Chapter 5: Using Network Monitoring and Troubleshooting Tools in Windows 2000	187
Introduction	188
Windows 2000 Monitoring Tools	188
Basic Monitoring Guidelines	188
Baselining	188
Documentation	189
Backing Up	189
Analysis	189

Performance Logs and Alerts	190
Counters	192
Log File Format	196
Alerts	196
Network Monitor	198
Filtering	199
Security Issues	199
Installation	199
Using the Program	199
Capture Window Panes	200
Extra Tools	200
Buffers	202
Collecting Data	204
Filtered Captures	207
Event Viewer	216
Using TCP/IP Utilities	219
PING	219
-t Switch	220
-n Switch	220
-r Switch	220
-i Switch	221
-w Switch	221
Using PING	221
nslookup	223
PATHPING	223
tracert	225
ARP	227
Using ARP	227
Static ARP Cache Entries	227
ipconfig	228
netstat and nbtstat	233
netdiag	238
Using netdiag	239
SNMP	242
What SNMP Does	242
Installing the Agent	244
Using IPsec Encryption	250
Network Management Programs	250
Microsoft Systems Management Server	250
NTManage	251
Summary	251
FAQs	252
Chapter 6: Troubleshooting Windows 2000	
NetBIOS Name Resolution Problems	257
Introduction to Name Resolution Services	258
NetBIOS Name Resolution	258

Windows 2000 Methods of NetBIOS Name Resolution	261
NetBIOS Name Cache	261
NetBIOS Name Server	262
Broadcast	263
LMHOSTS	263
HOSTS	265
DNS Server	266
The Order of NetBIOS Resolution	266
B-Node	266
P-Node	267
M-Node	267
H-Node	268
The Windows 2000 Windows Internet Name Service (WINS)	271
NetBIOS Name Registration	271
NetBIOS Name Query Request	273
NetBIOS Name Release	274
Multihomed Computers and WINS	274
WINS Proxy Agents	275
WINS Configuration Issues	276
Static Mappings	276
WINS Replication	277
Partnership Agreements	278
WINS Partner Autodiscovery	281
WINS Network Topologies	282
Spoke and Hub topology	283
Push and Pull Partnerships	283
Backing Up the WINS Database	288
Scavenging the Database	290
Interactions with DNS Servers	290
Pointing WINS Servers to Themselves	296
The Browser Service, WINS and Multihomed Masters	299
Windows 2000 WINS Enhancements	302
Persistent Connections	302
Manual Tombstoning	302
Is WINS Ever Going to Go Away?	305
Troubleshooting Common NetBIOS Communication Problems	306
Summary	309
Don't Multihome Your WINS Server	309
Use a WINS Proxy Agent on Segments with non-WINS Clients	310
Avoid Static Records in the WINS Database	310
Define Replication Partners Based on Link Factors	310
Avoid Split Registration	311
Use the Hub and Spoke Model in Multisite Environments	311
Configure DNS Servers to Resolve NetBIOS Names	311
Don't Multihome Master Browsers	311
Use Manual Tombstoning Instead of Deleting Records	312
Consider the Ramifications before Disabling NetBT	312
FAQs	313

Chapter 7: Troubleshooting Windows 2000 DNS Problems	317
Introduction	318
The Difference between NetBIOS Names and Host Names	319
Flat versus Hierarchical Namespace	319
NetBIOS on a TCP/IP Network	320
Characteristics of Host Names	321
The Need for a Name Resolution Service	321
Domains: The “Family Name”	321
The Domain Name System	322
A Hierarchical Naming System	322
Domain Levels	323
Fully Qualified Domain Names	324
Host Name Resolution	329
Name Resolution Sequence	329
The Caching Resolver	329
Using the HOSTS File for Name Resolution	331
Sending the DNS Query to a DNS Server	332
The Recursion Process	333
UNC Paths and DNS Queries	335
Connecting over the Internet via UNC	335
Qualified versus Unqualified Names	336
Appending DNS Suffixes	338
Host Name Resolution via WINS Lookups	338
Multiple DNS Zones and WINS	338
Naming Conventions and Issues	339
Windows 2000 Support for RFC 2181	339
The Controversial Underscore Character	340
Integrity Check	340
Extended Character Set and Zone Transfers	342
Lowercase Only	342
Domain Naming Schemes and Implementation Problems	342
Same Intranet and Internet Domain Name	343
Solution: Separate DNS Zone Databases	343
Different Intranet and Internet Domain Names	345
Advantages of Using Different Internal and External Domain Names	345
Proxy Configuration	345
Corporate Mergers and Domain Management	345
The Problem: Corporate Merger	346
Proposed Solution	347
Testing the Solution	348
DNS Zone Design and Troubleshooting	350
Standard Zones	352
Zone Transfer	358
Refresh Interval	360

DNS Notify	361
Request for Information Query	362
Fast Transfer	362
Reverse Lookup Zones	363
The in-addr.arpa Domain	364
Pointer Records	364
Active Directory Integrated Zones	366
Common Problems with Integrated DNS Zones	366
Advantages of Active Directory Integration	367
Zone Delegations	369
Troubleshooting Delegation Problems	370
Special Troubleshooting Issues with Windows 2000 DDNS Servers	371
DNS Security and Internet Intruders	371
Tracking Down the Problem	372
The Solution: Forwarders and Slaves	372
Solving WINS Client Ambiguity with WINS Lookup Zones	373
Setting Up a Dedicated Zone for WINS Referrals	374
Interoperability Problems	376
WINS and WINS-R Incompatibility with BIND Servers	377
DHCP and Resource Record Updates	379
Troubleshooting Tools for Windows 2000 DDNS Servers	380
nslookup	380
ipconfig	382
Event Viewer	382
Network Monitor	383
DNS Trace Logs	386
Performance	387
Summary	390
FAQs	394

Chapter 8: Troubleshooting Windows 2000

IP Addressing Problems 397

Introduction	398
How IP Addressing Works	399
Logical IP Addresses versus Physical MAC Addresses	399
What an IP Address Represents	400
Subnet Masking	403
Determining Address Class	405
How Network IDs Are Assigned	408
How Host IDs Are Assigned within the Network	408
Private versus Public Addresses	413
How IP Addresses Are Used in Network Communications	414
A Map for the Mail Carrier	415
Getting from the Logical to the Physical	415
Putting It All Together	417
IP Communications on a Nonrouted Network (within the Subnet)	417
IP Communications on a Routed Network (to a Remote Subnet)	418

Overview: IP Addressing Configuration Errors	420
Duplicate IP Addresses	420
Locating the Other Computer that Is Using the Address	421
Address Conflicts with Computers Using DHCP	422
Invalid IP Addresses	422
DHCP Configuration Problems	423
How DHCP Works: Condensed Version	423
Common DHCP Problems	425
Server Configuration Problems	426
Client Configuration Problems	443
Other Common DHCP Problems	444
Automatic Addressing (APIPA)	446
How to Disable APIPA	447
Hardware Address Problems	448
Duplicate MAC Addresses	448
Troubleshooting Subnetting Problems	448
Why Divide the Network?	449
Subnetting Scenario 1	450
Subnetting Scenario 2	450
Subnets	450
Subnet Masks	451
ANDing	451
Tricking IP	452
Making the Mask	452
Subnet Masking for a Class A Network	452
Subnet Masking for a Class B Network	455
Subnet Masking for a Class C Network	457
Errors in Subnet Masking	459
Summary	460
FAQs	463

Chapter 9: Troubleshooting Remote

Access in a Windows 2000 TCP/IP Network 465

Introduction	466
Overview of Windows 2000 Remote Access Services	467
Types of Remote Access	467
Distinguishing between Remote Access and Remote Control	468
Establishing a Remote Access Connection	470
Software Needed for a Remote Access Connection	470
The WAN Link	471
The Remote Access Protocols	482
Serial Line Internet Protocol	484
The Point-to-Point Protocol	484
Preventing Problems Related to the WAN Protocol	486
Understanding Encapsulation	486
Tools for Troubleshooting PPP Connections	487
Using Network Monitor for PPP Analysis	487

Enabling PPP Event Logging	487
Enabling PPP Tracing	487
Troubleshooting Remote Access Configuration Problems	489
Remote Access Server Problems	489
Inability to Establish a Remote Access Connection with the Server	489
Inability to Aggregate the Bandwidth of Multiple Telephone Lines	492
Inability to Access the Entire Network	494
Client Configuration Problems	494
Inability to Establish a Remote Connection	494
Troubleshooting Remote Access Policy Problems	496
Determining Which Multiple Policy Is Causing the Problem	497
Troubleshooting NAT and ICS Configuration Problems	498
The Difference between ICS and NAT	498
Common NAT Configuration Problems	498
Incorrect Public Address Range	500
Incompatible Application Programs	500
Other NAT Problems	501
Troubleshooting VPN Connectivity Problems	502
The Tunneling Protocols	502
PPTP: Point-to-Point Tunneling Protocol	502
L2TP: Layer 2 Tunneling Protocol	502
Troubleshooting VPN Connections	502
Inability to Connect to the Remote Access Server	503
Summary	503
FAQs	505

Chapter 10: Troubleshooting Windows 2000 Connectivity Problems at the Network Interface Level	509
Introduction	510
Problems with Network Interface Card Configuration	510
The Role of the NIC	511
Types of NICs	511
Driver Issues	512
Updating Drivers	512
Problems with Cable and Other Network Media	514
Network Cable Specifications	514
Cable Length Issues	515
The Role of Network Connectivity Devices	516
Understanding Layer 1 and 2 Connectivity Devices	517
How and Why Repeaters and Hubs Are Used	517
How and Why Switches Are Used	521
How and Why Bridges Are Used	523
Understanding Upper-Layer Connectivity Devices	526

How Routers Work	526
How and Why Routers Are Used	528
How and Why Brouters Are Used	529
How and Why Layer 3 Switches Are Used	530
How and Why Gateways Are Used	530
Troubleshooting Layer 1 and 2 Connectivity Devices	531
Problems with Repeaters and Hubs	531
The 5-4-3 Rule	531
Passive, Active, and Intelligent Hubs	532
Problems with Passive Hubs	532
Problems with Active Hubs	532
Problems with “Intelligent” Hubs	532
Problems with Bridges	532
Performance Problems	533
Bridge Latency	533
Bridge Looping	533
Network Monitoring Problems	536
Selecting a Connectivity Device	537
Summary	538
FAQs	539

Chapter 11: Troubleshooting Windows 2000 Connectivity Problems at the Internetwork Level 541

Introduction	542
A Routing Example	543
IP Routing Overview	544
Routing Fundamentals	545
Direct Routing	545
Indirect Routing	546
The Default Gateway	547
Routing Interfaces	549
Routing Tables	550
Viewing the Routing Table	550
Understanding the Routing Table	552
Simple Routing Scenario	553
The Windows 2000 Router	553
Routing Protocols	555
How Static Routing Works	555
Characteristics of Static Routing	557
The Dynamic Routing Protocols	558
RIP for IP	558
OSPF	563
Windows 2000 as an IP Router	570
Installing Routing Protocols	571
Windows 2000 Router Management Tools	572
Remote Router Administration	572
Using ICMP Router Discovery	574

Using the Netshell Utility (NETSH)	574
Router Configuration	576
Preconfiguration Check List	576
Configuring Windows 2000 Static IP Routing	577
Troubleshooting Static Routing Configuration	578
Configuring RIP for IP	578
Troubleshooting RIP Configuration	580
Configuring OSPF	581
OSPF Password Protection	583
Windows 2000 Router Logging	583
Using Event Logging	583
Using the Tracing Function	584
Troubleshooting Common Windows 2000 Routing Problems	586
Troubleshooting Static Routing	586
Using PING and TRACERT	586
Using the ROUTE Command	586
Static Routing and Routing Loops	586
Troubleshooting RIP for IP	588
Viewing RIP Neighbors	588
Viewing the Routing Table	589
Summary: Common RIP Problems	589
Troubleshooting OSPF	590
Resetting the Windows 2000 Router	591
Summary	591
FAQs	595

Chapter 12: Troubleshooting Selected Services on a Windows 2000 TCP/IP Network

599

Introduction	600
Troubleshooting IIS Problems	600
Log Files	602
Enabling Site Logging	602
Log File Formats	604
Logging Problems	608
Troubleshooting Web Server Problems	609
Performance Problems	609
Problems with Site Name Resolution	611
Inaccessible Virtual Directories	612
Problems with Hosting Multiple Sites on a Windows 2000 Server	613
Some Clients Unable to Access Site	614
Changing IIS Properties	616
Troubleshooting FTP Server Problems	617
End-User Problems	617
New Connections Not Being Accepted	617
Users Prompted for Username and Password	619
Connection Limit Exceeded	620
Troubleshooting NNTP Server Problems	621

Using Event Viewer for NNTP Troubleshooting	621
Common NNTP Problems	622
Summary	626
FAQs	628
Chapter 13: Windows 2000 TCP/IP Fast Track	631
Introduction	632
TCP/IP: What It Is (and Isn't)	632
TCP/IP History and Future in a Nutshell	632
Where TCP/IP Fits into the Networking Models	633
The Members of the Suite	634
Network Design and Planning Issues	635
Design and Setup of a Windows 2000 Network	635
Special Considerations for Windows 2000 Networks	636
Active Directory Sites	636
Active Directory Namespace	636
IP Addressing Scheme	636
Network Design Check List	637
Installing and Configuring the TCP/IP Protocol	637
Special Considerations when Upgrading from NT 4.0	637
Upgrading the Single Domain Model	637
Upgrading the Single Master Domain Model	637
Upgrading the Multiple Master Domain Model	638
Upgrading the Complete Trust Model	638
Upgrade Tools	638
Special Considerations when Migrating from NetWare	639
Migration Problems	639
Special Considerations when Migrating from UNIX	639
Hybrid Networks	639
General Troubleshooting Guidelines	640
Troubleshooting Resources	640
Troubleshooting Models	641
Differential Diagnosis Model	641
SARA Model	641
Information-Gathering Tips	641
Questions to Ask	641
Log Files	642
Organizing Information	642
Forms and Check Lists	642
Inside TCP/IP	643
Windows 2000 Enhancements	643
Inside IP	643
CIDR Support	643
Multihoming	643
IP Multicasting	644
Duplicate Address Detection	644
Inside TCP and UDP	644

TCP	644
UDP	644
TCP/IP Registry Settings	645
Network Monitoring Tools	645
Monitoring Guidelines	645
Baselining	645
Documentation	645
Performance Logs and Alerts	645
Network Monitor	646
Capture Filters	646
Display Filters	646
Event Viewer	647
TCP/IP Utilities	647
Name Resolution Problems	647
WINS and NetBIOS Name Resolution	648
DNS and Host Name Resolution	649
Resolving Host Names to IP Addresses	649
Planning the DNS Namespace	649
Zones	650
Tools	650
IP Addressing Issues	650
The IP Address	650
How IP Addresses Are Assigned	651
ARP	651
Common IP Addressing Errors	652
DHCP	652
Subnetting Problems	653
Remote Access Connectivity	653
Remote Access versus Remote Control	653
Remote Access Links	654
Remote Access Protocols	654
RRAS Configuration Problems	654
Server Configuration	654
Client Configuration	655
Multilink	655
Network Access	655
Remote Access Policy	655
NAT and ICS	655
NAT Configuration	656
Virtual Private Networking (VPN)	656
The Network Interface Level	657
Connectivity Devices	657
Repeaters	657
Hubs	657
Switches	657
Bridges	657
The 5-4-3 Rule	658
The 80/20 Rule	658

Looping	658
The Internetwork Level	658
Routing Tables	659
Features of the Windows 2000 Router	659
Routing Protocols	659
RIP Features	660
OSPF Features	660
Windows 2000 Router Logging	661
Selected Services	661
Site Logging	662
Web Server	662
FTP Server	662
NNTP Server	663
Summary	663
Appendix A: TCP/IP Troubleshooting Secrets	665
Lesser-Known Shortcuts	666
Finding the Consoles	666
Control the Index Server	666
Windows 2000 Telnet Client and Server	667
Telnet Server	668
Under-Documented Features and Functions	670
The FTP Command Set	670
The nslookup Utility	671
Using ipconfig Switches	672
For Experts Only	674
The Future of IP Communications	674
IP Telephony	674
TAPI 3.0 and H.323	675
Telephony and Active Directory	675
Planning the Transition to IPv6	676
How Is IPv6 Different?	676
The Scary Part	676
How to Prepare for the Transition	677
Securing IP: IPSec	677
End-to-End Security	677
IPSec Functions	678
Security Troubleshooting	678
Tunnel Mode	678
IPSec and NAT	679
Index	681