

System Administration Guide: IP Services



Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819-3000-04
March 2009

Copyright 2009 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Sun Quad FastEthernet, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2009 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux Etats-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certains composants de ce produit peuvent être dérivées du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, le logo Solaris, le logo Java Coffee Cup, docs.sun.com, Sun Quad FastEthernet, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc., ou ses filiales, aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Contents

Preface 23

Part I TCP/IP Administration 29

1 Solaris TCP/IP Protocol Suite (Overview) 31

 What's New in This Release 31

 Introducing the TCP/IP Protocol Suite 31

 Protocol Layers and the Open Systems Interconnection Model 32

 TCP/IP Protocol Architecture Model 33

 How the TCP/IP Protocols Handle Data Communications 38

 Data Encapsulation and the TCP/IP Protocol Stack 39

 TCP/IP Internal Trace Support 42

 Finding Out More About TCP/IP and the Internet 42

 Computer Books About TCP/IP 42

 TCP/IP and Networking Related Web Sites 42

 Requests for Comments and Internet Drafts 43

2 Planning an IPv4 Addressing Scheme (Tasks) 45

 Network Planning (Task Map) 46

 Determining the Network Hardware 47

 Deciding on an IP Addressing Format for Your Network 47

 IPv4 Addresses 48

 IPv4 Addresses in CIDR Format 48

 DHCP Addresses 48

 IPv6 Addresses 49

 Private Addresses and Documentation Prefixes 49

 Obtaining Your Network's IP Number 49

- Designing an IPv4 Addressing Scheme 50
 - Designing Your IPv4 Addressing Scheme 51
 - IPv4 Subnet Number 52
 - Designing Your CIDR IPv4 Addressing Scheme 53
 - Using Private IPv4 Addresses 54
 - How IP Addresses Apply to Network Interfaces 54
- Naming Entities on Your Network 55
 - Administering Host Names 55
 - Selecting a Name Service and Directory Service 55
- Planning for Routers on Your Network 57
 - Network Topology Overview 58
 - How Routers Transfer Packets 59
- 3 Planning an IPv6 Addressing Scheme (Overview) 61**
 - Major Features of IPv6 61
 - Expanded Addressing 62
 - Address Autoconfiguration and Neighbor Discovery 62
 - Header Format Simplification 62
 - Improved Support for IP Header Options 62
 - Application Support for IPv6 Addressing 62
 - Additional IPv6 Resources 63
 - IPv6 Network Overview 64
 - IPv6 Addressing Overview 66
 - Parts of the IPv6 Address 67
 - Abbreviating IPv6 Addresses 68
 - Prefixes in IPv6 68
 - Unicast Addresses 69
 - Multicast Addresses 71
 - Anycast Addresses and Groups 72
 - IPv6 Neighbor Discovery Protocol Overview 72
 - IPv6 Address Autoconfiguration 73
 - Stateless Autoconfiguration Overview 73
 - Overview of IPv6 Tunnels 74

4 Planning an IPv6 Network (Tasks)	75
IPv6 Planning (Task Maps)	75
IPv6 Network Topology Scenario	76
Preparing the Existing Network to Support IPv6	78
Preparing the Network Topology for IPv6 Support	78
Preparing Network Services for IPv6 Support	79
Preparing Servers for IPv6 Support	79
▼ How to Prepare Network Services for IPv6 Support	80
▼ How to Prepare DNS for IPv6 Support	80
Planning for Tunnels in the Network Topology	81
Security Considerations for the IPv6 Implementation	82
Preparing an IPv6 Addressing Plan	82
Obtaining a Site Prefix	82
Creating the IPv6 Numbering Scheme	83
 5 Configuring TCP/IP Network Services and IPv4 Addressing (Tasks)	 85
What's New in This Chapter	85
Before You Configure an IPv4 Network (Task Map)	86
Determining Host Configuration Modes	87
Systems That Should Run in Local Files Mode	87
Systems That Are Network Clients	88
Mixed Configurations	88
IPv4 Network Topology Scenario	89
Adding a Subnet to a Network (Task Map)	90
Network Configuration Task Map	90
Configuring Systems on the Local Network	91
▼ How to Configure a Host for Local Files Mode	92
▼ How to Set Up a Network Configuration Server	94
Configuring Network Clients	95
▼ How to Configure Hosts for Network Client Mode	95
▼ How to Change the IPv4 Address and Other Network Configuration Parameters	96
Packet Forwarding and Routing on IPv4 Networks	101
Routing Protocols Supported by the Solaris OS	102
IPv4 Autonomous System Topology	105
Configuring an IPv4 Router	107

- Routing Tables and Routing Types 113
- Configuring Multihomed Hosts 116
- Configuring Routing for Single-Interface Systems 119
- Monitoring and Modifying Transport Layer Services 124
 - ▼ How to Log the IP Addresses of All Incoming TCP Connections 124
 - ▼ How to Add Services That Use the SCTP Protocol 124
 - ▼ How to Use TCP Wrappers to Control Access to TCP Services 128
- 6 Enabling IPv6 on a Network (Tasks) 129**
 - Configuring an IPv6 Interface 129
 - Enabling IPv6 on an Interface (Task Map) 130
 - ▼ How to Enable an IPv6 Interface for the Current Session 130
 - ▼ How to Enable Persistent IPv6 Interfaces 132
 - ▼ How to Turn Off IPv6 Address Autoconfiguration 134
 - Configuring an IPv6 Router 134
 - IPv6 Router Configuration (Task Map) 134
 - ▼ How to Configure an IPv6-Enabled Router 135
 - Modifying an IPv6 Interface Configuration for Hosts and Servers 139
 - Modifying an IPv6 Interface Configuration (Task Map) 139
 - Using Temporary Addresses for an Interface 139
 - Configuring an IPv6 Token 142
 - Administering IPv6-Enabled Interfaces on Servers 145
 - Tasks for Configuring Tunnels for IPv6 Support (Task Map) 146
 - Configuring Tunnels for IPv6 Support 147
 - ▼ How to Manually Configure IPv6 Over IPv4 Tunnels 147
 - ▼ How to Manually Configure IPv6 Over IPv6 Tunnels 148
 - ▼ How to Configure IPv4 Over IPv6 Tunnels 149
 - ▼ How to Configure a 6to4 Tunnel 149
 - ▼ How to Configure a 6to4 Tunnel to a 6to4 Relay Router 153
 - Configuring Name Service Support for IPv6 155
 - ▼ How to Add IPv6 Addresses to DNS 155
 - ▼ How to Display IPv6 Name Service Information 156
 - ▼ How to Verify That DNS IPv6 PTR Records Are Updated Correctly 157
 - ▼ How to Display IPv6 Information Through NIS 157

7 Administering a TCP/IP Network (Tasks)	159
Major TCP/IP Administrative Tasks (Task Map)	159
Monitoring the Interface Configuration With the <code>ifconfig</code> Command	160
▼ How to Get Information About a Specific Interface	161
▼ How to Display Interface Address Assignments	162
Monitoring Network Status With the <code>netstat</code> Command	164
▼ How to Display Statistics by Protocol	165
▼ How to Display the Status of Transport Protocols	166
▼ How to Display Network Interface Status	168
▼ How to Display the Status of Sockets	168
▼ How to Display the Status of Transmissions for Packets of a Specific Address Type	170
▼ How to Display the Status of Known Routes	171
Probing Remote Hosts With the <code>ping</code> Command	172
▼ How to Determine if a Remote Host Is Running	172
▼ How to Determine if a Host Is Dropping Packets	172
Administering and Logging Network Status Displays	173
▼ How to Control the Display Output of IP-Related Commands	173
▼ How to Log Actions of the IPv4 Routing Daemon	175
▼ How to Trace the Activities of the IPv6 Neighbor Discovery Daemon	175
Displaying Routing Information With the <code>traceroute</code> Command	176
▼ How to Find Out the Route to a Remote Host	177
▼ How to Trace All Routes	177
Monitoring Packet Transfers With the <code>snoop</code> Command	178
▼ How to Check Packets From All Interfaces	178
▼ How to Capture snoop Output Into a File	179
▼ How to Check Packets Between an IPv4 Server and a Client	180
▼ How to Monitor IPv6 Network Traffic	181
Monitoring Packets by Using IP Layer Devices	181
Administering Default Address Selection	186
▼ How to Administer the IPv6 Address Selection Policy Table	186
▼ How to Modify the IPv6 Address Selection Table for the Current Session Only	188
8 Troubleshooting Network Problems (Tasks)	189
General Network Troubleshooting Tips	189
Running Basic Diagnostic Checks	189

- ▼ How to Perform Basic Network Software Checking 190
- Common Problems When Deploying IPv6 190
 - IPv4 Router Cannot Be Upgraded to IPv6 191
 - Problems After Upgrading Services to IPv6 191
 - Current ISP Does Not Support IPv6 191
 - Security Issues When Tunneling to a 6to4 Relay Router 191
 - Known Issues With a 6to4 Router 192

- 9 TCP/IP and IPv4 in Depth (Reference) 195**
 - TCP/IP Configuration Files 195
 - /etc/hostname.*interface* File 196
 - /etc/nodename File 196
 - /etc/defaultdomain File 196
 - /etc/defaultrouter File 197
 - hosts Database 197
 - netmasks Database 200
 - inetd Internet Services Daemon 203
 - Network Databases and the nsswitch.conf File 204
 - How Name Services Affect Network Databases 204
 - nsswitch.conf File 206
 - bootparams Database 208
 - ethers Database 209
 - Other Network Databases 210
 - protocols Database 211
 - services Database 212
 - Routing Protocols in the Solaris OS 212
 - Routing Information Protocol (RIP) 213
 - ICMP Router Discovery (RDISC) Protocol 213
 - Network Classes 213
 - Class A Network Numbers 213
 - Class B Network Numbers 214
 - Class C Network Numbers 215

- 10 IPv6 in Depth (Reference) 217**
 - IPv6 Addressing Formats Beyond the Basics 217

6to4-Derived Addresses	218
IPv6 Multicast Addresses in Depth	220
IPv6 Packet Header Format	221
IPv6 Extension Headers	222
Dual-Stack Protocols	222
Solaris 10 IPv6 Implementation	223
IPv6 Configuration Files	223
IPv6-Related Commands	228
IPv6-Related Daemons	234
IPv6 Neighbor Discovery Protocol	238
ICMP Messages From Neighbor Discovery	238
Autoconfiguration Process	238
Neighbor Solicitation and Unreachability	240
Duplicate Address Detection Algorithm	241
Proxy Advertisements	241
Inbound Load Balancing	241
Link-Local Address Change	242
Comparison of Neighbor Discovery to ARP and Related IPv4 Protocols	242
IPv6 Routing	244
Router Advertisement	244
IPv6 Tunnels	245
Configured Tunnels	247
6to4 Automatic Tunnels	249
IPv6 Extensions to Solaris Name Services	253
DNS Extensions for IPv6	253
Changes to the <code>nsswitch.conf</code> File	253
Changes to Name Service Commands	254
NFS and RPC IPv6 Support	254
IPv6 Over ATM Support	255
Part II DHCP	257
11 About Solaris DHCP (Overview)	259
About the DHCP Protocol	259
Advantages of Using Solaris DHCP	260

How DHCP Works	261
Solaris DHCP Server	264
DHCP Server Management	265
DHCP Data Store	265
DHCP Manager	266
DHCP Command-Line Utilities	267
Role-Based Access Control for DHCP Commands	268
DHCP Server Configuration	268
IP Address Allocation	269
Network Configuration Information	270
About DHCP Options	270
About DHCP Macros	271
Solaris DHCP Client	272
12 Planning for DHCP Service (Tasks)	275
Preparing Your Network for the DHCP Service (Task Map)	275
Mapping Your Network Topology	276
Determining the Number of DHCP Servers	277
Updating System Files and Netmask Tables	278
Making Decisions for Your DHCP Server Configuration (Task Map)	279
Selecting a Host to Run the DHCP Service	280
Choosing the DHCP Data Store	280
Setting a Lease Policy	281
Determining Routers for DHCP Clients	282
Making Decisions for IP Address Management (Task Map)	282
Number and Ranges of IP Addresses	283
Client Host Name Generation	283
Default Client Configuration Macros	284
Dynamic and Permanent Lease Types	285
Reserved IP Addresses and Lease Type	285
Planning for Multiple DHCP Servers	286
Planning DHCP Configuration of Your Remote Networks	286
Selecting the Tool for Configuring DHCP	287
DHCP Manager Features	287
dhcpconfig Features	287

Comparison of DHCP Manager and dhcpconfig	288
13 Configuring the DHCP Service (Tasks)	289
Configuring and Unconfiguring a DHCP Server Using DHCP Manager	289
Configuring DHCP Servers	290
▼ How to Configure a DHCP Server (DHCP Manager)	292
Configuring BOOTP Relay Agents	293
▼ How to Configure a BOOTP Relay Agent (DHCP Manager)	294
Unconfiguring DHCP Servers and BOOTP Relay Agents	295
DHCP Data on an Unconfigured Server	295
▼ How to Unconfigure a DHCP Server or a BOOTP Relay Agent (DHCP Manager)	296
Configuring and Unconfiguring a DHCP Server Using dhcpconfig Commands	297
▼ How to Configure a DHCP Server (dhcpconfig -D)	297
▼ How to Configure a BOOTP Relay Agent (dhcpconfig -R)	298
▼ How to Unconfigure a DHCP Server or a BOOTP Relay Agent (dhcpconfig -U)	298
14 Administering DHCP (Tasks)	301
About DHCP Manager	302
DHCP Manager Window	302
DHCP Manager Menus	303
Starting and Stopping DHCP Manager	304
▼ How to Start and Stop DHCP Manager	304
Setting Up User Access to DHCP Commands	305
▼ How to Grant Users Access to DHCP Commands	305
Starting and Stopping the DHCP Service	305
▼ How to Start and Stop the DHCP Service (DHCP Manager)	306
▼ How to Enable and Disable the DHCP Service (DHCP Manager)	307
▼ How to Enable and Disable the DHCP Service (dhcpconfig -S)	307
DHCP Service and the Service Management Facility	308
Modifying DHCP Service Options (Task Map)	308
Changing DHCP Logging Options	310
▼ How to Generate Verbose DHCP Log Messages (DHCP Manager)	311
▼ How to Generate Verbose DHCP Log Messages (Command Line)	312
▼ How to Enable and Disable DHCP Transaction Logging (DHCP Manager)	312
▼ How to Enable and Disable DHCP Transaction Logging (Command Line)	313

- ▼ How to Log DHCP Transactions to a Separate sys log File 314
 - Enabling Dynamic DNS Updates by a DHCP Server 314
- ▼ How to Enable Dynamic DNS Updating for DHCP Clients 315
 - Client Host Name Registration 317
 - Customizing Performance Options for the DHCP Server 318
- ▼ How to Customize DHCP Performance Options (DHCP Manager) 318
- ▼ How to Customize DHCP Performance Options (Command Line) 319
- Adding, Modifying, and Removing DHCP Networks (Task Map) 320
 - Specifying Network Interfaces for DHCP Monitoring 320
- ▼ How to Specify Network Interfaces for DHCP Monitoring (DHCP Manager) 321
- ▼ How to Specify Network Interfaces for DHCP Monitoring (dhcpconfig) 322
 - Adding DHCP Networks 322
- ▼ How to Add a DHCP Network (DHCP Manager) 323
- ▼ How to Add a DHCP Network (dhcpconfig) 324
 - Modifying DHCP Network Configurations 325
- ▼ How to Modify the Configuration of a DHCP Network (DHCP Manager) 326
- ▼ How to Modify the Configuration of a DHCP Network (dhtadm) 327
 - Removing DHCP Networks 328
- ▼ How to Remove a DHCP Network (DHCP Manager) 328
- ▼ How to Remove a DHCP Network (pntadm) 329
- Supporting BOOTP Clients With the DHCP Service (Task Map) 330
 - ▼ How to Set Up Support of Any BOOTP Client (DHCP Manager) 331
 - ▼ How to Set Up Support of Registered BOOTP Clients (DHCP Manager) 332
- Working With IP Addresses in the DHCP Service (Task Map) 333
 - Adding IP Addresses to the DHCP Service 336
 - ▼ How to Add a Single IP Address (DHCP Manager) 338
 - ▼ How to Duplicate an Existing IP Address (DHCP Manager) 339
 - ▼ How to Add Multiple IP Addresses (DHCP Manager) 339
 - ▼ How to Add IP Addresses (pntadm) 340
 - Modifying IP Addresses in the DHCP Service 340
 - ▼ How to Modify IP Address Properties (DHCP Manager) 342
 - ▼ How to Modify IP Address Properties (pntadm) 342
 - Removing IP Addresses From the DHCP Service 343
 - Marking IP Addresses as Unusable by the DHCP Service 343
 - ▼ How to Mark IP Addresses as Unusable (DHCP Manager) 343
 - ▼ How to Mark IP Addresses as Unusable (pntadm) 344

Deleting IP Addresses From the DHCP Service	344
▼ How to Delete IP Addresses From DHCP Service (DHCP Manager)	345
▼ How to Delete IP Addresses From the DHCP Service (pntadm)	346
Assigning a Reserved IP Address to a DHCP Client	346
▼ How to Assign a Consistent IP Address to a DHCP Client (DHCP Manager)	347
▼ How to Assign a Consistent IP Address to a DHCP Client (pntadm)	348
Working With DHCP Macros (Task Map)	348
▼ How to View Macros Defined on a DHCP Server (DHCP Manager)	350
▼ How to View Macros Defined on a DHCP Server (dhtadm)	351
Modifying DHCP Macros	351
▼ How to Change Values for Options in a DHCP Macro (DHCP Manager)	352
▼ How to Change Values for Options in a DHCP Macro (dhtadm)	353
▼ How to Add Options to a DHCP Macro (DHCP Manager)	353
▼ How to Add Options to a DHCP Macro (dhtadm)	354
▼ How to Delete Options From a DHCP Macro (DHCP Manager)	354
▼ How to Delete Options From a DHCP Macro (dhtadm)	355
Creating DHCP Macros	355
▼ How to Create a DHCP Macro (DHCP Manager)	356
▼ How to Create a DHCP Macro (dhtadm)	357
Deleting DHCP Macros	358
▼ How to Delete a DHCP Macro (DHCP Manager)	358
▼ How to Delete a DHCP Macro (dhtadm)	358
Working With DHCP Options (Task Map)	359
Creating DHCP Options	362
▼ How to Create DHCP Options (DHCP Manager)	363
▼ How to Create DHCP Options (dhtadm)	364
Modifying DHCP Options	365
▼ How to Modify DHCP Option Properties (DHCP Manager)	365
▼ How to Modify DHCP Option Properties (dhtadm)	366
Deleting DHCP Options	367
▼ How to Delete DHCP Options (DHCP Manager)	367
▼ How to Delete DHCP Options (dhtadm)	367
Modifying the Solaris DHCP Client's Option Information	368
Supporting Solaris Network Installation With the DHCP Service	368
Supporting Remote Boot and Diskless Boot Clients (Task Map)	369
Setting Up DHCP Clients to Receive Information Only (Task Map)	370

- Converting to a New DHCP Data Store 371
 - ▼ How to Convert the DHCP Data Store (DHCP Manager) 372
 - ▼ How to Convert the DHCP Data Store (dhcpconfig -C) 373
- Moving Configuration Data Between DHCP Servers (Task Map) 373
 - ▼ How to Export Data From a DHCP Server (DHCP Manager) 375
 - ▼ How to Export Data From a DHCP Server (dhcpconfig -X) 376
 - ▼ How to Import Data on a DHCP Server (DHCP Manager) 377
 - ▼ How to Import Data on a DHCP Server (dhcpconfig -I) 377
 - ▼ How to Modify Imported DHCP Data (DHCP Manager) 378
 - ▼ How to Modify Imported DHCP Data (pntadm, dhtadm) 379
- 15 Configuring and Administering the DHCP Client 381**
 - About the Solaris DHCP Client 381
 - DHCPv6 Server 382
 - Differences Between DHCPv4 and DHCPv6 382
 - The Administrative Model 382
 - Protocol Details 383
 - Logical Interfaces 384
 - Option Negotiation 384
 - Configuration Syntax 385
 - DHCP Client Startup 385
 - DHCPv6 Communication 386
 - How DHCP Client Protocols Manage Network Configuration Information 387
 - DHCP Client Shutdown 388
 - Enabling and Disabling a Solaris DHCP Client 389
 - ▼ How to Enable the Solaris DHCP Client 389
 - ▼ How to Disable a Solaris DHCP Client 389
 - DHCP Client Administration 390
 - ifconfig Command Options Used With the DHCP Client 390
 - Setting DHCP Client Configuration Parameters 392
 - DHCP Client Systems With Multiple Network Interfaces 393
 - DHCPv4 Client Host Names 394
 - ▼ How to Enable a Solaris DHCPv4 Client to Request a Specific Host Name 394
 - DHCP Client Systems and Name Services 395
 - Setting Up DHCP Clients as NIS+ Clients 397

DHCP Client Event Scripts	400
16 Troubleshooting DHCP (Reference)	405
Troubleshooting DHCP Server Problems	405
NIS+ Problems and the DHCP Data Store	405
IP Address Allocation Errors in DHCP	408
Troubleshooting DHCP Client Configuration Problems	411
Problems Communicating With the DHCP Server	411
Problems With Inaccurate DHCP Configuration Information	420
Problems With the DHCP Client-Supplied Host Name	421
17 DHCP Commands and Files (Reference)	425
DHCP Commands	425
Running DHCP Commands in Scripts	426
Files Used by the DHCP Service	433
DHCP Option Information	435
Determining if Your Site Is Affected	435
Differences Between dhcptags and inittab Files	436
Converting dhcptags Entries to inittab Entries	437
Part III IP Security	439
18 IP Security Architecture (Overview)	441
What's New in IPsec?	441
Introduction to IPsec	443
IPsec RFCs	444
IPsec Terminology	444
IPsec Packet Flow	445
IPsec Security Associations	448
Key Management in IPsec	448
IPsec Protection Mechanisms	449
Authentication Header	449
Encapsulating Security Payload	449
Authentication and Encryption Algorithms in IPsec	451

IPsec Protection Policies	452
Transport and Tunnel Modes in IPsec	453
Virtual Private Networks and IPsec	455
IPsec and NAT Traversal	456
IPsec and SCTP	457
IPsec and Solaris Zones	457
IPsec Utilities and Files	457
Changes to IPsec for the Solaris 10 Release	459
19 Configuring IPsec (Tasks)	461
Protecting Traffic With IPsec (Task Map)	461
Protecting Traffic With IPsec	462
▼ How to Secure Traffic Between Two Systems With IPsec	463
▼ How to Use IPsec to Protect a Web Server From Nonweb Traffic	466
▼ How to Display IPsec Policies	467
▼ How to Generate Random Numbers on a Solaris System	468
▼ How to Manually Create IPsec Security Associations	469
▼ How to Verify That Packets Are Protected With IPsec	472
▼ How to Configure a Role for Network Security	474
▼ How to Manage IKE and IPsec Services	475
Protecting a VPN With IPsec	477
Examples of Protecting a VPN With IPsec by Using Tunnels in Tunnel Mode	477
Protecting a VPN With IPsec (Task Map)	479
Description of the Network Topology for the IPsec Tasks to Protect a VPN	480
▼ How to Protect a VPN With an IPsec Tunnel in Tunnel Mode Over IPv4	482
▼ How to Protect a VPN With an IPsec Tunnel in Tunnel Mode Over IPv6	489
▼ How to Protect a VPN With an IPsec Tunnel in Transport Mode Over IPv4	492
▼ How to Protect a VPN With an IPsec Tunnel in Transport Mode Over IPv6	496
▼ How to Prevent IP Spoofing	499
20 IP Security Architecture (Reference)	503
IPsec Service Management Facility	503
ipseccomp Command	504
ipsecinit.conf File	505
Sample ipsecinit.conf File	505

Security Considerations for <code>ipsecinit.conf</code> and <code>ipsecconf</code>	506
<code>ipsecalgs</code> Command	506
Security Associations Database for IPsec	507
Utilities for Key Generation in IPsec	507
Security Considerations for <code>ipseckey</code>	508
<code>snoop</code> Command and IPsec	509
21 Internet Key Exchange (Overview)	511
What's New in IKE?	511
Key Management With IKE	512
IKE Key Negotiation	512
IKE Key Terminology	512
IKE Phase 1 Exchange	513
IKE Phase 2 Exchange	514
IKE Configuration Choices	514
IKE With Preshared Keys	514
IKE With Public Key Certificates	514
IKE and Hardware Acceleration	515
IKE and Hardware Storage	515
IKE Utilities and Files	516
Changes to IKE for the Solaris 10 Release	517
22 Configuring IKE (Tasks)	519
Configuring IKE (Task Map)	519
Configuring IKE With Preshared Keys (Task Map)	520
Configuring IKE With Preshared Keys	520
▼ How to Configure IKE With Preshared Keys	521
▼ How to Refresh IKE Preshared Keys	524
▼ How to View IKE Preshared Keys	525
▼ How to Add an IKE Preshared Key for a New Policy Entry in <code>ipsecinit.conf</code>	526
▼ How to Verify That IKE Preshared Keys Are Identical	529
Configuring IKE With Public Key Certificates (Task Map)	530
Configuring IKE With Public Key Certificates	531
▼ How to Configure IKE With Self-Signed Public Key Certificates	531
▼ How to Configure IKE With Certificates Signed by a CA	537

- ▼ How to Generate and Store Public Key Certificates on Hardware 543
- ▼ How to Handle a Certificate Revocation List 547
- Configuring IKE for Mobile Systems (Task Map) 549
- Configuring IKE for Mobile Systems 549
 - ▼ How to Configure IKE for Off-Site Systems 550
- Configuring IKE to Find Attached Hardware (Task Map) 557
- Configuring IKE to Find Attached Hardware 558
 - ▼ How to Configure IKE to Find the Sun Crypto Accelerator 1000 Board 558
 - ▼ How to Configure IKE to Find the Sun Crypto Accelerator 4000 Board 559
- Changing IKE Transmission Parameters (Task Map) 560
- Changing IKE Transmission Parameters 560
 - ▼ How to Change the Duration of Phase 1 IKE Key Negotiation 561

- 23 Internet Key Exchange (Reference) 563**
 - IKE Service Management Facility 563
 - IKE Daemon 564
 - IKE Policy File 564
 - IKE Administration Command 565
 - IKE Preshared Keys Files 566
 - IKE Public Key Databases and Commands 566
 - ikecert tokens Command 567
 - ikecert certlocal Command 567
 - ikecert certdb Command 568
 - ikecert certrlb Command 568
 - /etc/inet/ike/publickeys Directory 568
 - /etc/inet/secret/ike.privatekeys Directory 569
 - /etc/inet/ike/crls Directory 569

- 24 Solaris IP Filter (Overview) 571**
 - What's New in Solaris IP Filter 571
 - Packet Filter Hooks 571
 - IPv6 Packet Filtering for Solaris IP Filter 572
 - Introduction to Solaris IP Filter 572
 - Information Sources for Open Source IP Filter 572
 - Solaris IP Filter Packet Processing 573

Guidelines for Using Solaris IP Filter	576
Using Solaris IP Filter Configuration Files	576
Working With Solaris IP Filter Rule Sets	576
Using Solaris IP Filter's Packet Filtering Feature	577
Using Solaris IP Filter's NAT Feature	580
Using Solaris IP Filter's Address Pools Feature	581
Packet Filter Hooks	582
IPv6 for Solaris IP Filter	583
Solaris IP Filter Man Pages	584
 25 Solaris IP Filter (Tasks)	585
Configuring Solaris IP Filter	585
▼ How to Enable Solaris IP Filter	586
▼ How to Re-Enable Solaris IP Filter	587
▼ How to Enable Loopback Filtering	588
Deactivating and Disabling Solaris IP Filter	589
▼ How to Deactivate Packet Filtering	589
▼ How to Deactivate NAT	590
▼ How to Disable Packet Filtering	591
Working With Solaris IP Filter Rule Sets	591
Managing Packet Filtering Rule Sets for Solaris IP Filter	592
Managing NAT Rules for Solaris IP Filter	599
Managing Address Pools for Solaris IP Filter	601
Displaying Statistics and Information for Solaris IP Filter	603
▼ How to View State Tables for Solaris IP Filter	603
▼ How to View State Statistics for Solaris IP Filter	604
▼ How to View NAT Statistics for Solaris IP Filter	605
▼ How to View Address Pool Statistics for Solaris IP Filter	606
Working With Log Files for Solaris IP Filter	606
▼ How to Set Up a Log File for Solaris IP Filter	606
▼ How to View Solaris IP Filter Log Files	607
▼ How to Flush the Packet Log File	609
▼ How to Save Logged Packets to a File	609
Creating and Editing Solaris IP Filter Configuration Files	610
▼ How to Create a Configuration File for Solaris IP Filter	610

	Solaris IP Filter Configuration File Examples	612
Part IV	IP Quality of Service (IPQoS)	617
26	Introducing IPQoS (Overview)	619
	IPQoS Basics	619
	What Are Differentiated Services?	619
	IPQoS Features	620
	Where to Get More Information About Quality-of-Service Theory and Practice	620
	Providing Quality of Service With IPQoS	622
	Implementing Service-Level Agreements	622
	Assuring Quality of Service for an Individual Organization	622
	Introducing the Quality-of-Service Policy	622
	Improving Network Efficiency With IPQoS	623
	How Bandwidth Affects Network Traffic	623
	Using Classes of Service to Prioritize Traffic	624
	Differentiated Services Model	624
	Classifier (ipgpc) Overview	625
	Meter (tokenmt and tswtclmt) Overview	626
	Marker (dscpmk and dlcosmk) Overview	626
	Flow Accounting (flowacct) Overview	627
	How Traffic Flows Through the IPQoS Modules	627
	Traffic Forwarding on an IPQoS-Enabled Network	629
	DS Codepoint	629
	Per-Hop Behaviors	629
27	Planning for an IPQoS-Enabled Network (Tasks)	633
	General IPQoS Configuration Planning (Task Map)	633
	Planning the Diffserv Network Topology	634
	Hardware Strategies for the Diffserv Network	634
	IPQoS Network Topologies	634
	Planning the Quality-of-Service Policy	637
	QoS Policy Planning Aids	637
	QoS Policy Planning (Task Map)	638

▼ How to Prepare a Network for IPQoS	639
▼ How to Define the Classes for Your QoS Policy	640
Defining Filters	642
▼ How to Define Filters in the QoS Policy	643
▼ How to Plan Flow Control	644
▼ How to Plan Forwarding Behavior	646
▼ How to Plan for Flow Accounting	649
Introducing the IPQoS Configuration Example	649
IPQoS Topology	650
28 Creating the IPQoS Configuration File (Tasks)	653
Defining a QoS Policy in the IPQoS Configuration File (Task Map)	653
Tools for Creating a QoS Policy	654
Basic IPQoS Configuration File	655
Creating IPQoS Configuration Files for Web Servers	655
▼ How to Create the IPQoS Configuration File and Define Traffic Classes	658
▼ How to Define Filters in the IPQoS Configuration File	660
▼ How to Define Traffic Forwarding in the IPQoS Configuration File	661
▼ How to Enable Accounting for a Class in the IPQoS Configuration File	664
▼ How to Create an IPQoS Configuration File for a Best-Effort Web Server	666
Creating an IPQoS Configuration File for an Application Server	668
▼ How to Configure the IPQoS Configuration File for an Application Server	671
▼ How to Configure Forwarding for Application Traffic in the IPQoS Configuration File	673
▼ How to Configure Flow Control in the IPQoS Configuration File	675
Providing Differentiated Services on a Router	678
▼ How to Configure a Router on an IPQoS-Enabled Network	679
29 Starting and Maintaining IPQoS (Tasks)	681
Administering IPQoS (Task Map)	681
Applying an IPQoS Configuration	682
▼ How to Apply a New Configuration to the IPQoS Kernel Modules	682
▼ How to Ensure That the IPQoS Configuration Is Applied After Each Reboot	683
Enabling syslog Logging for IPQoS Messages	683
▼ How to Enable Logging of IPQoS Messages During Booting	683
Troubleshooting with IPQoS Error Messages	684

- 30 Using Flow Accounting and Statistics Gathering (Tasks) 689**
 - Setting Up Flow Accounting (Task Map) 689
 - Recording Information About Traffic Flows 689
 - ▼ How to Create a File for Flow-Accounting Data 690
 - Gathering Statistical Information 692

- 31 IPQoS in Detail (Reference) 695**
 - IPQoS Architecture and the Diffserv Model 695
 - Classifier Module 695
 - Meter Module 698
 - Marker Module 700
 - flowacct Module 705
 - IPQoS Configuration File 707
 - action Statement 709
 - Module Definitions 709
 - class Clause 710
 - filter Clause 710
 - params Clause 711
 - ipqosconf Configuration Utility 711

- Glossary 713**

- Index 723**

Preface

Welcome to System Administration Guide: IP Services for the Solaris Express, Developer Edition 1/08. This book is part of a nine-volume set that covers a significant part of the Solaris™ system administration information. This book assumes that you have already installed the Solaris operating system (Solaris OS). You should be ready to configure your network or ready to configure any networking software that is required on your network. The Solaris OS is part of the Solaris product family, which also includes the Solaris Common Desktop Environment (CDE). The Solaris OS is compliant with AT&T's System V, Release 4 operating system.

Note – This Solaris release supports systems that use the SPARC® and x86 families of processor architectures: UltraSPARC®, SPARC64, AMD64, Pentium, and Xeon EM64T. The supported systems appear in the *Solaris 10 Hardware Compatibility List* at <http://www.sun.com/bigadmin/hcl>. This document cites any implementation differences between the platform types.

In this document these x86 related terms mean the following:

- “x86” refers to the larger family of 64-bit and 32-bit x86 compatible products.
- “x64” points out specific 64-bit information about AMD64 or EM64T systems.
- “32-bit x86” points out specific 32-bit information about x86 based systems.

For supported systems, see the *Solaris 10 Hardware Compatibility List*.

How the System Administration Guides Are Organized

Here is a list of the topics that are covered by the System Administration Guides.

Book Title	Topics
<i>System Administration Guide: Basic Administration</i>	User accounts and groups, server and client support, shutting down and booting a system, managing services, and managing software (packages and patches)

Book Title	Topics
<i>System Administration Guide: Advanced Administration</i>	Terminals and modems, system resources (disk quotas, accounting, and crontabs), system processes, and troubleshooting Solaris software problems
<i>System Administration Guide: Devices and File Systems</i>	Removable media, disks and devices, file systems, and backing up and restoring data
<i>System Administration Guide: IP Services</i>	TCP/IP network administration, IPv4 and IPv6 address administration, DHCP, IPsec, IKE, Solaris IP filter, Mobile IP, and IPQoS
<i>System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)</i>	DNS, NIS, and LDAP naming and directory services, including transitioning from NIS to LDAP and transitioning from NIS+ to LDAP
<i>System Administration Guide: Naming and Directory Services (NIS+)</i>	NIS+ naming and directory services
<i>System Administration Guide: Network Interfaces and Network Virtualization</i>	Networking stack, NIC driver property configuration, network interface configuration, administration of VLANs and link aggregations, IP networking multipathing (IPMP), WiFi wireless networking configuration, and virtual NICs (VNICs).
<i>System Administration Guide: Network Services</i>	Web cache servers, time-related services, network file systems (NFS and Autofs), mail, SLP, and PPP
<i>System Administration Guide: Security Services</i>	Auditing, device management, file security, BART, Kerberos services, PAM, Solaris Cryptographic Framework, privileges, RBAC, SASL, and Solaris Secure Shell
<i>System Administration Guide: Virtualization Using the Solaris Operating System</i>	Resource management features, which enable you to control how applications use available system resources; zones software partitioning technology, which virtualizes operating system services to create an isolated environment for running applications; and virtualization using Sun™ xVM hypervisor technology, which supports multiple operating system instances simultaneously
<i>Solaris CIFS Administration Guide</i>	Solaris CIFS service, which enables you to configure a Solaris system to make CIFS shares available to CIFS clients; and native identity mapping services, which enables you to map user and group identities between Solaris systems and Windows systems
<i>Solaris ZFS Administration Guide</i>	ZFS storage pool and file system creation and management, snapshots, clones, backups, using access control lists (ACLs) to protect ZFS files, using ZFS on a Solaris system with zones installed, emulated volumes, and troubleshooting and data recovery
<i>Solaris Trusted Extensions Administrator's Procedures</i>	System installation, configuration, and administration that is specific to Solaris Trusted Extensions

Book Title	Topics
<i>System Administration Guide: Solaris Printing</i>	Solaris printing topics and tasks, using services, tools, protocols, and technologies to set up and administer printing services and printers

Related Books

The following trade books are referred to in this book:

- Ferguson, Paul and Geoff Huston. *Quality of Service*. John Wiley & Sons, Inc., 1998.
- Hunt Craig. *TCP/IP Network Administration, 3rd Edition*. O'Reilly, 2002.
- Kilkki, Kalevi. *Differentiated Services for the Internet*. Macmillan Technical Publishing, 1999.
- Stevens, W. Richard. *TCP/IP Illustrated, Volume 1, The Protocols*. Addison Wesley, 1994.

Related Third-Party Web Site References

Third party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Solaris IP Filter is derived from open source IP Filter software. To view license terms, attribution, and copyright statements for IP Filter, the default path is `/usr/lib/ipf/IPFILTER.LICENCE`. If Solaris OS has been installed anywhere other than the default, modify the given path to access the file at the installed location.

Acknowledgment

Glenn Herteg contributed to the preparation and review of the information about Solaris IP Filter.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (<http://www.sun.com/documentation/>)
- Support (<http://www.sun.com/support/>)
- Training (<http://www.sun.com/training/>)

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P-1 Typographic Conventions

Typeface	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your .login file. Use ls -a to list all files. machine_name% you have mail.
AaBbCc123	What you type, contrasted with onscreen computer output	machine_name% su Password:
<i>aabbcc123</i>	Placeholder: replace with a real name or value	The command to remove a file is rm <i>filename</i> .
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . A <i>cache</i> is a copy that is stored locally. Do <i>not</i> save the file. Note: Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX® system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P-2 Shell Prompts

Shell	Prompt
C shell	machine_name%
C shell for superuser	machine_name#
Bourne shell and Korn shell	\$
Bourne shell and Korn shell for superuser	#



PART I

TCP/IP Administration

This part contains tasks and conceptual information for configuring, administering, and troubleshooting TCP/IP networks.

Solaris TCP/IP Protocol Suite (Overview)

This chapter introduces the Solaris implementation of the TCP/IP network protocol suite. The information is intended for system and network administrators who are unfamiliar with basic TCP/IP concepts. The remaining parts of this book assume that you are familiar with these concepts.

This chapter contains the following information:

- “Introducing the TCP/IP Protocol Suite” on page 31
- “How the TCP/IP Protocols Handle Data Communications” on page 38
- “Finding Out More About TCP/IP and the Internet” on page 42

What's New in This Release

Starting with Solaris Express Developer Edition 9/07, the Mobile IP feature is no longer available in the Solaris Express Developer's releases. See the Solaris Express Developer Edition 9/07 Release Notes for more information.

Introducing the TCP/IP Protocol Suite

This section presents an in-depth introduction to the protocols that are included in TCP/IP. Although the information is conceptual, you should learn the names of the protocols. You should also learn what each protocol does.

“TCP/IP” is the acronym that is commonly used for the set of network protocols that compose the *Internet Protocol suite*. Many texts use the term “Internet” to describe both the protocol suite and the global wide area network. In this book, “TCP/IP” refers specifically to the Internet protocol suite. “Internet” refers to the wide area network and the bodies that govern the Internet.

To interconnect your TCP/IP network with other networks, you must obtain a unique IP address for your network. At the time of this writing, you obtain this address from an Internet service provider (ISP).

If hosts on your network are to participate in the Internet Domain Name System (DNS), you must obtain and register a unique domain name. The InterNIC coordinates the registration of domain names through a group of worldwide registries. For more information on DNS, refer to [System Administration Guide: Naming and Directory Services \(DNS, NIS, and LDAP\)](#).

Protocol Layers and the Open Systems Interconnection Model

Most network protocol suites are structured as a series of layers, sometimes collectively referred to as a *protocol stack*. Each layer is designed for a specific purpose. Each layer exists on both the sending and receiving systems. A specific layer on one system sends or receives exactly the same object that another system's *peer process* sends or receives. These activities occur independently from activities in layers above or below the layer under consideration. In essence, each layer on a system acts independently of other layers on the same system. Each layer acts in parallel with the same layer on other systems.

OSI Reference Model

Most network protocol suites are structured in layers. The International Organization for Standardization (ISO) designed the Open Systems Interconnection (OSI) Reference Model that uses structured layers. The OSI model describes a structure with seven layers for network activities. One or more protocols is associated with each layer. The layers represent data transfer operations that are common to all types of data transfers among cooperating networks.

The OSI model lists the protocol layers from the top (layer 7) to the bottom (layer 1). The following table shows the model.

TABLE 1-1 Open Systems Interconnection Reference Model

Layer No.	Layer Name	Description
7	Application	Consists of standard communication services and applications that everyone can use.
6	Presentation	Ensures that information is delivered to the receiving system in a form that the system can understand.
5	Session	Manages the connections and terminations between cooperating systems.

TABLE 1-1 Open Systems Interconnection Reference Model (Continued)

Layer No.	Layer Name	Description
4	Transport	Manages the transfer of data. Also assures that the received data are identical to the transmitted data.
3	Network	Manages data addressing and delivery between networks.
2	Data link	Handles the transfer of data across the network media.
1	Physical	Defines the characteristics of the network hardware.

The OSI model defines conceptual operations that are not unique to any particular network protocol suite. For example, the OSI network protocol suite implements all seven layers of the OSI model. TCP/IP uses some of OSI model layers. TCP/IP also combines other layers. Other network protocols, such as SNA, add an eighth layer.

TCP/IP Protocol Architecture Model

The OSI model describes idealized network communications with a family of protocols. TCP/IP does not directly correspond to this model. TCP/IP either combines several OSI layers into a single layer, or does not use certain layers at all. The following table shows the layers of the Solaris implementation of TCP/IP. The table lists the layers from the topmost layer (application) to the bottommost layer (physical network).

TABLE 1-2 TCP/IP Protocol Stack

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
5,6,7	Application, session, presentation	Application	NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP, SCTP
3	Network	Internet	IPv4, IPv6, ARP, ICMP
2	Data link	Data link	PPP, IEEE 802.2
1	Physical	Physical network	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI, and others

The table shows the TCP/IP protocol layers and the OSI model equivalents. Also shown are examples of the protocols that are available at each level of the TCP/IP protocol stack. Each system that is involved in a communication transaction runs a unique implementation of the protocol stack.

Physical Network Layer

The *physical network layer* specifies the characteristics of the hardware to be used for the network. For example, physical network layer specifies the physical characteristics of the communications media. The physical layer of TCP/IP describes hardware standards such as IEEE 802.3, the specification for Ethernet network media, and RS-232, the specification for standard pin connectors.

Data-Link Layer

The *data-link layer* identifies the network protocol type of the packet, in this instance TCP/IP. The data-link layer also provides error control and “framing.” Examples of data-link layer protocols are Ethernet IEEE 802.2 framing and Point-to-Point Protocol (PPP) framing.

Internet Layer

The Internet layer, also known as the *network layer* or *IP layer*, accepts and delivers packets for the network. This layer includes the powerful Internet Protocol (IP), the Address Resolution Protocol (ARP), and the Internet Control Message Protocol (ICMP).

IP Protocol

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the following:

- **IP addressing** – The IP addressing conventions are part of the IP protocol. [“Designing an IPv4 Addressing Scheme” on page 50](#) introduces IPv4 addressing and [“IPv6 Addressing Overview” on page 66](#) introduces IPv6 addressing.
- **Host-to-host communications** – IP determines the path a packet must take, based on the receiving system's IP address.
- **Packet formatting** – IP assembles packets into units that are known as *datagrams*. Datagrams are fully described in [“Internet Layer: Where Packets Are Prepared for Delivery” on page 41](#).
- **Fragmentation** – If a packet is too large for transmission over the network media, IP on the sending system breaks the packet into smaller fragments. IP on the receiving system then reconstructs the fragments into the original packet.

The Solaris OS supports both IPv4 and IPv6 addressing formats, which are described in this book. To avoid confusion when addressing the Internet Protocol, one of the following conventions is used:

- When the term “IP” is used in a description, the description applies to both IPv4 and IPv6.
- When the term “IPv4” is used in a description, the description applies only to IPv4.
- When the term “IPv6” is used in a description, the description applies only to IPv6.

ARP Protocol

The Address Resolution Protocol (ARP) conceptually exists between the data-link and Internet layers. ARP assists IP in directing datagrams to the appropriate receiving system by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

ICMP Protocol

The Internet Control Message Protocol (ICMP) detects and reports network error conditions. ICMP reports on the following:

- **Dropped packets** – Packets that arrive too fast to be processed
- **Connectivity failure** – A destination system cannot be reached
- **Redirection** – Redirecting a sending system to use another router

[Chapter 7, “Administering a TCP/IP Network \(Tasks\),”](#) contains more information on the Solaris OS commands that use ICMP for error detection.

Transport Layer

The TCP/IP *transport layer* ensures that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets. This type of communication is known as *end-to-end*. Transport layer protocols at this level are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). TCP and SCTP provide reliable, end-to-end service. UDP provides unreliable datagram service.

TCP Protocol

TCP enables applications to communicate with each other as though they were connected by a physical circuit. TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discrete packets. This transmission consists of the following:

- Starting point, which opens the connection
- Entire transmission in byte order
- Ending point, which closes the connection.

TCP attaches a header onto the transmitted data. This header contains many parameters that help processes on the sending system connect to peer processes on the receiving system.

TCP confirms that a packet has reached its destination by establishing an end-to-end connection between sending and receiving hosts. TCP is therefore considered a “reliable, connection-oriented” protocol.

SCTP Protocol

SCTP is a reliable, connection-oriented transport layer protocol that provides the same services to applications that are available from TCP. Moreover, SCTP can support connections between systems that have more than one address, or *multihomed*. The SCTP connection between sending and receiving system is called an *association*. Data in the association is organized in chunks. Because SCTP supports multihoming, certain applications, particularly applications used by the telecommunications industry, need to run over SCTP, rather than TCP.

UDP Protocol

UDP provides datagram delivery service. UDP does not verify connections between receiving and sending hosts. Because UDP eliminates the processes of establishing and verifying connections, applications that send small amounts of data use UDP.

Application Layer

The *application layer* defines standard Internet services and network applications that anyone can use. These services work with the transport layer to send and receive data. Many application layer protocols exist. The following list shows examples of application layer protocols:

- Standard TCP/IP services such as the `ftp`, `tftp`, and `telnet` commands
- UNIX “r” commands, such as `rlogin` and `rsh`
- Name services, such as NIS and the domain name system (DNS)
- Directory services (LDAP)
- File services, such as the NFS service
- Simple Network Management Protocol (SNMP), which enables network management
- Router Discovery Server protocol (RDISC) and Routing Information Protocol (RIP) routing protocols

Standard TCP/IP Services

- **FTP and Anonymous FTP** – The File Transfer Protocol (FTP) transfers files to and from a remote network. The protocol includes the `ftp` command and the `in.ftpd` daemon. FTP enables a user to specify the name of the remote host and file transfer command options on the local host's command line. The `in.ftpd` daemon on the remote host then handles the requests from the local host. Unlike `rcp`, `ftp` works even when the remote computer does not run a UNIX based operating system. A user must log in to the remote system to make an `ftp` connection, unless the remote system has been configured to allow anonymous FTP.

You can obtain an enormous amount of material from *anonymous FTP servers* that are connected to the Internet. Universities and other institutions set up these servers to offer software, research papers, and other information to the public domain. When you log in to this type of server, you use the login name `anonymous`, hence the term “anonymous FTP server.”

Using anonymous FTP and setting up anonymous FTP servers is outside the scope of this manual. However, many books, such as *The Whole Internet User's Guide & Catalog*, discuss anonymous FTP in detail. Instructions for using FTP are in [System Administration Guide: Network Services](#). The `ftp(1)` man page describes all `ftp` command options that are invoked through the command interpreter. The `ftpd(1M)` man page describes the services that are provided by the `in.ftpd` daemon.

- **Telnet** – The Telnet protocol enables terminals and terminal-oriented processes to communicate on a network that runs TCP/IP. This protocol is implemented as the `telnet` program on local systems and the `in.telnetd` daemon on remote machines. Telnet provides a user interface through which two hosts can communicate on a character-by-character or line-by-line basis. Telnet includes a set of commands that are fully documented in the `telnet(1)` man page.
- **TFTP** – The Trivial File Transfer Protocol (`tftp`) provides functions that are similar to `ftp`, but the protocol does not establish `ftp`'s interactive connection. As a result, users cannot list the contents of a directory or change directories. A user must know the full name of the file to be copied. The `tftp(1)` man page describes the `tftp` command set.

UNIX “r” Commands

The UNIX “r” commands enable users to issue commands on their local machines that run on the remote host. These commands include the following:

- `rcp`
- `rlogin`
- `rsh`

Instructions for using these commands are in the `rcp(1)`, `rlogin(1)`, and `rsh(1)` man pages.

Name Services

The Solaris OS provides the following name services:

- **DNS** – The domain name system (DNS) is the name service provided by the Internet for TCP/IP networks. DNS provides host names to the IP address service. DNS also serves as a database for mail administration. For a complete description of this service, see [System Administration Guide: Naming and Directory Services \(DNS, NIS, and LDAP\)](#). See also the `resolver(3RESOLV)` man page.
- **/etc files** – The original host-based UNIX name system was developed for standalone UNIX machines and then adapted for network use. Many old UNIX operating systems and computers still use this system, but it is not well suited for large complex networks.
- **NIS** – Network Information Service (NIS) was developed independently of DNS and has a slightly different focus. Whereas DNS focuses on making communication simpler by using machine names instead of numerical IP addresses, NIS focuses on making network administration more manageable by providing centralized control over a variety of network

information. NIS stores information about machine names and addresses, users, the network itself, and network services. NIS name space information is stored in NIS maps. For more information on NIS Architecture and NIS Administration, see [System Administration Guide: Naming and Directory Services \(DNS, NIS, and LDAP\)](#).

Directory Service

The Solaris OS supports LDAP (Lightweight Directory Access Protocol) in conjunction with the Sun Open Net Environment (Sun ONE) Directory Server, as well as other LDAP directory servers. The distinction between a name service and a directory service is in the differing extent of functionality. A directory service provides the same functionality of a naming service, but provides additional functionalities as well. See [System Administration Guide: Naming and Directory Services \(DNS, NIS, and LDAP\)](#).

File Services

The NFS application layer protocol provides file services for the Solaris OS. You can find complete information about the NFS service in [System Administration Guide: Network Services](#).

Network Administration

The Simple Network Management Protocol (SNMP) enables you to view the layout of your network and the status of key machines. SNMP also enables you to obtain complex network statistics from software that is based on a graphical user interface (GUI). Many companies offer network management packages that implement SNMP.

Routing Protocols

The Routing Information Protocol (RIP) and the Router Discovery Server Protocol (RDISC) are two available routing protocols for TCP/IP networks. For complete lists of available routing protocols for the Solaris 10 OS, refer to [Table 5–1](#) and [Table 5–2](#).

How the TCP/IP Protocols Handle Data Communications

When a user issues a command that uses a TCP/IP application layer protocol, a series of events is initiated. The user's command or message passes through the TCP/IP protocol stack on the local system. Then, the command or message passes across the network media to the protocols on the remote system. The protocols at each layer on the sending host add information to the original data.

Protocols on each layer of the sending host also interact with their peers on the receiving host. [Figure 1–1](#) shows this interaction.

Data Encapsulation and the TCP/IP Protocol Stack

The packet is the basic unit of information that is transferred across a network. The basic packet consists of a header with the sending and receiving systems' addresses, and a body, or *payload*, with the data to be transferred. As the packet travels through the TCP/IP protocol stack, the protocols at each layer either add or remove fields from the basic header. When a protocol on the sending system adds data to the packet header, the process is called *data encapsulation*. Moreover, each layer has a different term for the altered packet, as shown in the following figure.

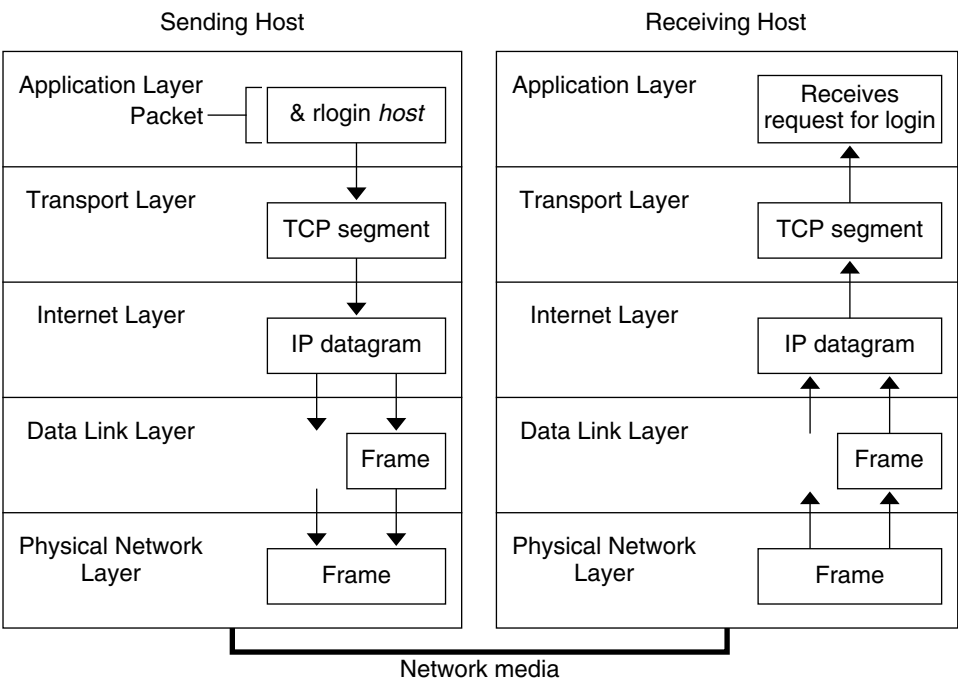


FIGURE 1-1 How a Packet Travels Through the TCP/IP Stack

This section summarizes the life cycle of a packet. The life cycle starts when you issue a command or send a message. The life cycle finishes when the appropriate application on the receiving system receives the packet.

Application Layer: Where a Communication Originates

The packet's history begins when a user on one system sends a message or issues a command that must access a remote system. The application protocol formats the packet so that the appropriate transport layer protocol, TCP or UDP, can handle the packet.

Suppose the user issues an `rlogin` command to log in to the remote system, as shown in [Figure 1-1](#). The `rlogin` command uses the TCP transport layer protocol. TCP expects to receive data in the form of a stream of bytes that contain the information in the command. Therefore, `rlogin` sends this data as a TCP stream.

Transport Layer: Where Data Encapsulation Begins

When the data arrives at the transport layer, the protocols at the layer start the process of data encapsulation. The transport layer encapsulates the application data into transport protocol data units.

The transport layer protocol creates a virtual flow of data between the sending and receiving application, differentiated by the transport port number. The port number identifies a *port*, a dedicated location in memory for receiving or sending data. In addition, the transport protocol layer might provide other services, such as reliable, in order data delivery. The end result depends on whether TCP, SCTP, or UDP handles the information.

TCP Segmentation

TCP is often called a “connection-oriented” protocol because TCP ensures the successful delivery of data to the receiving host. [Figure 1-1](#) shows how the TCP protocol receives the stream from the `rlogin` command. TCP then divides the data that is received from the application layer into segments and attaches a header to each segment.

Segment headers contain sending and receiving ports, segment ordering information, and a data field that is known as a *checksum*. The TCP protocols on both hosts use the checksum data to determine if the data transfers without error.

Establishing a TCP Connection

TCP uses segments to determine whether the receiving system is ready to receive the data. When the sending TCP wants to establish connections, TCP sends a segment that is called a *SYN* to the TCP protocol on the receiving host. The receiving TCP returns a segment that is called an *ACK* to acknowledge the successful receipt of the segment. The sending TCP sends another *ACK* segment, then proceeds to send the data. This exchange of control information is referred to as a *three-way handshake*.

UDP Packets

UDP is a “connectionless” protocol. Unlike TCP, UDP does not check that data arrived at the receiving host. Instead, UDP formats the message that is received from the application layer into *UDP packets*. UDP attaches a header to each packet. The header contains the sending and receiving ports, a field with the length of the packet, and a checksum.

The sending UDP process attempts to send the packet to its peer UDP process on the receiving host. The application layer determines whether the receiving UDP process acknowledges the reception of the packet. UDP requires no notification of receipt. UDP does not use the three-way handshake.

Internet Layer: Where Packets Are Prepared for Delivery

The transport protocols TCP, UDP, and SCTP pass their segments and packets down to the Internet layer, where the IP protocol handles the segments and packets. IP prepares them for delivery by formatting them into units called *IP datagrams*. IP then determines the IP addresses for the datagrams, so that they can be delivered effectively to the receiving host.

IP Datagrams

IP attaches an *IP header* to the segment or packet's header, in addition to the information that is added by TCP or UDP. Information in the IP header includes the IP addresses of the sending and receiving hosts, the datagram length, and the datagram sequence order. This information is provided if the datagram exceeds the allowable byte size for network packets and must be fragmented.

Data-Link Layer: Where Framing Takes Place

Data-link layer protocols, such as PPP, format the IP datagram into a *frame*. These protocols attach a third header and a footer to “frame” the datagram. The frame header includes a *cyclic redundancy check* (CRC) field that checks for errors as the frame travels over the network media. Then, the data-link layer passes the frame to the physical layer.

Physical Network Layer: Where Frames Are Sent and Received

The physical network layer on the sending host receives the frames and converts the IP addresses into the hardware addresses appropriate to the network media. The physical network layer then sends the frame out over the network media.

How the Receiving Host Handles the Packet

When the packet arrives on the receiving host, the packet travels through the TCP/IP protocol stack in the reverse order from which it was sent. [Figure 1–1](#) illustrates this path. Moreover, each protocol on the receiving host strips off header information that is attached to the packet by its peer on the sending host. The following process occurs:

1. The physical network layer receives the packet in its frame form. The physical network layer computes the CRC of the packet, then sends the frame to the data link layer.
2. The data-link layer verifies that the CRC for the frame is correct and strips off the frame header and the CRC. Finally, the data-link protocol sends the frame to the Internet layer.

3. The Internet layer reads information in the header to identify the transmission. Then, the Internet layer determines if the packet is a fragment. If the transmission is fragmented, IP reassembles the fragments into the original datagram. IP then strips off the IP header and passes the datagram on to transport layer protocols.
4. The transport layer (TCP, SCTP, and UDP) reads the header to determine which application layer protocol must receive the data. Then, TCP, SCTP, or UDP strips off its related header. TCP, SCTP, or UDP sends the message or stream to the receiving application.
5. The application layer receives the message. The application layer then performs the operation that the sending host requested.

TCP/IP Internal Trace Support

TCP/IP provides internal trace support by logging TCP communication when an RST packet terminates a connection. When an RST packet is transmitted or received, information on as many as 10 packets, which were just transmitted, is logged with the connection information.

Finding Out More About TCP/IP and the Internet

Information about TCP/IP and the Internet is widely available. If you require specific information that is not covered in this text, you can probably find what you need in the sources cited next.

Computer Books About TCP/IP

Many trade books about TCP/IP and the Internet are available from your local library or computer bookstore. The following two books are considered the classic texts on TCP/IP:

- Craig Hunt. *TCP/IP Network Administration* – This book contains some theory and much practical information for managing a heterogeneous TCP/IP network.
- W. Richard Stevens. *TCP/IP Illustrated, Volume I* – This book is an in-depth explanation of the TCP/IP protocols. This book is ideal for network administrators who require a technical background in TCP/IP and for network programmers.

TCP/IP and Networking Related Web Sites

The Internet has a wealth of web sites and user groups that are devoted to TCP/IP protocols and their administration. Many manufacturers, including Sun Microsystems, offer web-based resources for general TCP/IP information. The following are helpful web resources for TCP/IP information and general system administration information.

Web Site	Description
The Internet Engineering Task Force (IETF) web site (http://www.ietf.org/home.html)	The IETF is the body responsible for the architecture and governance of the Internet. The IETF web site contains information about the various activities of this organization. The site also includes links to the major publications of the IETF.
Sun Microsystem's BigAdmin Portal (http://www.sun.com/bigadmin)	BigAdmin provides information for administering Sun computers. The site offers FAQs, resources, discussions, links to documentation, and other materials that pertain to Solaris OS administration, including networking.

Requests for Comments and Internet Drafts

The Internet Engineering Task Force (IETF) working groups publish standards documents that are known as *Requests for Comments* (RFCs). Standards that are under development are published in *Internet Drafts*. The Internet Architecture Board (IAB) must approve all RFCs before they are placed in the public domain. Typically RFCs and Internet drafts are directed to developers and other highly technical readers. However, a number of RFCs that deal with TCP/IP topics contain valuable information for system administrators. These RFCs are cited in various places throughout this book.

Generally, For Your Information (FYI) documents appear as a subset of the RFCs. FYIs contain information that does not deal with Internet standards. FYIs contain Internet information of a more general nature. For example, FYI documents include a bibliography that list introductory TCP/IP books and papers. FYI documents provide an exhaustive compendium of Internet-related software tools. Finally, FYI documents include a glossary of Internet and general networking terms.

You will find references to relevant RFCs throughout this guide and other books in the Solaris System Administrator Collection.