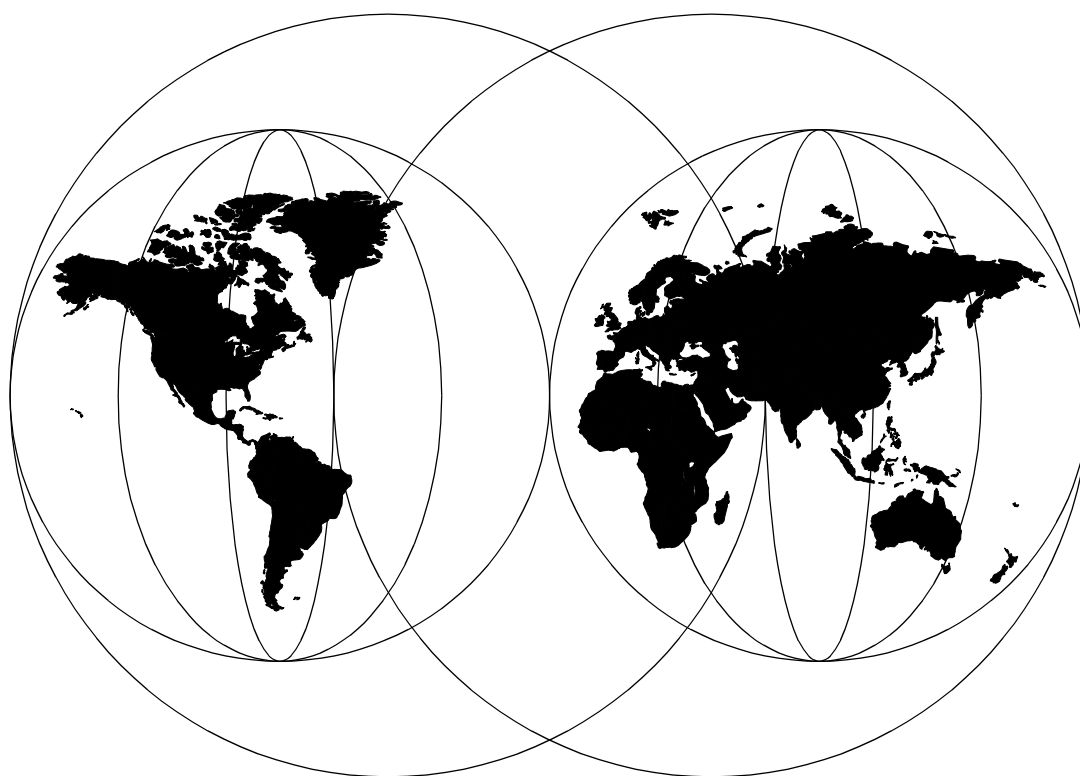


AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support

M. Adan, S. Goodrich, A. Grant, M. Hamada, G. Ilmberger



International Technical Support Organization

<http://www.redbooks.ibm.com>



International Technical Support Organization

SG24-5147-00

**AS/400 TCP/IP Autoconfiguration:
DNS and DHCP Support**

April 1998

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, "Special Notices" on page 441.

First Edition (April 1998)

This edition applies to Version 4 Release 2 of OS/400 (5769-SS1 V4R2), Version 3 Release 1 Modification 3 of Client Access/400 for Windows 95/NT (5763-XD1 V3R1M3), Version 4 Release 1 or Version 4 Release 2 of Firewall for AS/400 (5769-FW1)

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JLU Building 107-2
3605 Highway 52N
Rochester, Minnesota 55901-7829

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Contents	iii
Preface	xi
The Team That Wrote This Redbook	xi
Comments Welcome	xiii
<hr/>	
Part 1. AS/400 DNS Support	1
Chapter 1. Domain Name System Concepts and Overview	3
1.1 Overview	3
1.2 Domain versus Zone of Authority	5
1.3 Name Resolution	7
1.4 Types of Name Servers	9
1.5 Split DNS Concept for Firewalls	11
1.6 Types of Files	12
1.7 Types of Records	14
1.8 Round Robin and Address Sorting	15
1.9 For More Information	15
Chapter 2. AS/400 DNS Server Implementation	17
2.1 DNS Software Prerequisites	17
2.2 DNS Installation	17
2.3 DNS Server Jobs	18
2.4 DNS Configuration Files	18
2.4.1 Logging / Service Files	19
2.5 DNS Server User Interface	22
2.5.1 DNS Server Configuration through Operations Navigator	22
2.5.2 Change DNS Attributes Command (CHGDNSA)	23
2.5.3 Start TCP Server *DHCP	23
2.6 NSLOOKUP	23
2.7 Host Table Migration Program	24
2.8 DNS Server Backup and Recovery Considerations	24
Chapter 3. Implementing Primary and Secondary DNS Servers	25
3.1 Scenario Overview	25
3.1.1 Scenario Objectives	26
3.1.2 Scenario Advantages	26
3.1.3 Scenario Disadvantages	27
3.1.4 Scenario Network Configuration	27
3.2 Task Summary	28
3.2.1 Planning the Primary Domain	29
3.2.2 Creating the Primary Name Server on As1	29
3.2.3 Configuring AS1 as a Mail Server	44
3.2.4 Starting the DNS Server on AS1	52
3.2.5 Verifying That the DNS Server is Operational	53
3.2.6 Creating a Secondary DNS Server	57
3.2.7 Primary Name Server Security Considerations	63
3.2.8 Reconfigure Clients to Use the DNS Server	66
3.3 Summary	68

Chapter 4. Migrating an NT Primary DNS to AS/400 System	71
4.1 Migrating NT DNS Server Primary Domain Files	71
4.1.1 Scenario Objective	72
4.2 Task Summary	72
4.2.1 Reviewing Primary DNS Configuration on the NT Name Server	72
4.2.2 Transferring DNS Files from the NT Server to the AS/400 System IFS	73
4.2.3 Importing the Domain Data	76
4.2.4 Configure Forwarders Manually	78
4.3 Configuring the NT DNS Server as a Secondary DNS Server	79
4.3.1 Deleting the Primary DNS Configuration	80
4.3.2 Configuring the Secondary Name Server	81
4.4 Summary	82
Chapter 5. Growing Your Domain: Creating Subdomains	83
5.1 Scenario Overview	83
5.1.1 Scenario Objectives	87
5.1.2 Scenario Advantages	87
5.1.3 Scenario Disadvantages	88
5.1.4 Scenario Network Configuration	89
5.2 Task Summary	89
5.3 Planning to Subdomain	90
5.3.1 Defining the Zone of Authority	91
5.4 Method 1: Adding a Subdomain and Maintaining Authority	92
5.4.1 Configure AS1 Primary Name Server	93
5.4.2 Configure the Secondary Name Server As5	95
5.5 Method 2: Adding a Subdomain and Delegating Authority	96
5.5.1 Configuring AS1 as Internal Root	96
5.5.2 Removing Subdomain Configuration from the Parent Server AS1	98
5.5.3 Delegating the Subdomain on the Parent Server AS1	99
5.5.4 Delegating the In-Addr.Arpa File on the Parent Server AS1	102
5.5.5 Configuring the Child Server Otherhost	106
5.5.6 Internal Root Server Configuration on the Child Server	109
5.5.7 Reconfigure the Otherdomain Clients	110
5.5.8 Verifying DNS with Name Server Lookup	111
5.5.9 Method 2's Secondary Name Server AS5	115
5.6 Mail Between Otherdomain.mycompany.com and Mycompany.com	116
5.6.1 AS1 as the Only Mail Server in the Network	116
5.6.2 Otherhost as the Mail Server for Otherdomain.mycompany.com	117
5.7 The Child Server Otherhost's IFS Directory Files	120
5.8 Round Robin/Address Sorting	121
5.9 Summary	124
Chapter 6. Split DNS: Hiding Your Internal DNS Behind a Firewall	125
6.1 Scenario 1: Configuring Your DNS to Forward Queries to a Firewall	125
6.1.1 Scenario Objectives	126
6.1.2 Scenario Advantages	127
6.1.3 Scenario Disadvantages	127
6.1.4 Scenario Network Configuration	127
6.2 Task Summary	128
6.2.1 Verify the AS/400 TCP/IP Configuration on AS1	128
6.2.2 Verify the AS/400 Mail Configuration	130
6.2.3 Firewall Installation and Configuration	133

6.2.4	Updating the Firewall Configuration to Use the Internal DNS	138
6.2.5	Configuring Forwarders in the Internal DNS	140
6.2.6	Client Configuration	142
6.3	Sharing a LAN Adapter Between the AS/400 and Integrated PC Server	144
6.3.1	AS/400 System TCP/IP Configuration	145
6.3.2	Firewall Configuration	147
6.3.3	Internal DNS Server Configuration	148
6.4	Scenario 2: Multiple Mail Servers Behind the Firewall	153
6.4.1	Scenario Objectives	153
6.4.2	Scenario Network Configuration	154
6.4.3	Scenario Advantages	154
6.4.4	Scenario Disadvantages	155
6.5	Task Summary	155
6.5.1	Verify the AS/400 TCP/IP Configuration	155
6.5.2	Verify the AS/400 Mail Configuration	156
6.5.3	Verify the Firewall Installation and Configuration	160
6.5.4	Internal DNS Configuration	161
6.5.5	Considerations for Exchanging Mail with Internet Users	167
6.5.6	Solving the CC: Problem	168
Chapter 7. Providing DNS Services on the Internet		173
7.1	Scenario Overview	173
7.1.1	Scenario Objectives	174
7.1.2	Scenario Advantages	174
7.1.3	Scenario Disadvantages	174
7.1.4	Scenario Network Configuration	174
7.2	Task Summary	175
7.2.1	Planning the ASISP Name Server Configuration	176
7.2.2	Create the inc.com Primary Domain Files on ASISP	177
7.2.3	Create the msu.edu Primary Domain Files ASISP	179
7.2.4	Configure the Root Servers on ASISP	179
7.2.5	Create the Secondary Domain Files for mycompany.com on ASISP	181
7.2.6	Create the Secondary Domain Files on ASISP2	183
7.2.7	Configure the Root Servers on ASISP2	184
7.2.8	Configure the Clients	184
Chapter 8. DNS Server Tips, Tools, and Problem Determination		185
8.1	Tips and Tools	185
8.1.1	Tips for Preventing Problems	185
8.1.2	Tips for Performance	186
8.1.3	Tools for Problem Determination	188
8.1.4	AS/400 Job Logs	189
8.1.5	NSLOOKUP	190
8.1.6	Dump Server Statistics	194
8.1.7	Run Debug	197
8.1.8	DNS Server QUERYLOG	199
8.1.9	DNS server Dump Database	201
8.1.10	Tips on Debugging Mail on an AS/400 System	202
8.2	Problem Symptoms and Probable Causes	207
8.3	For Additional Help With Problems	213

Part 2. AS/400 DHCP Server Support	215
Chapter 9. DHCP Concepts and Overview	217
9.1 BOOTP, the Predecessor of DHCP	217
9.2 DHCP Overview	218
9.3 How does DHCP Work?	219
9.3.1 How is Configuration Information Acquired?	220
9.3.2 How are Leases Renewed?	223
9.3.3 What Happens when a Client Moves out of its Subnet?	224
9.3.4 How are Changes Implemented in the Network?	224
9.3.5 What are BOOTP/DHCP Relay Agents?	224
Chapter 10. AS/400 DHCP Server Implementation.	227
10.1 DHCP Software Prerequisites	227
10.2 DHCP Installation	227
10.3 DHCP Server Jobs	228
10.4 DHCP Configuration Files	228
10.4.1 Log Files	229
10.5 DHCP Server User Interface	232
10.5.1 DHCP Server Configuration through Operations Navigator	232
10.5.2 Change DHCP Attributes Command (CHGDHCPA)	233
10.5.3 Start TCP Server *DHCP	233
10.6 BOOTP-to-DHCP Migration Program	234
10.7 DHCP Server Exit Programs	234
10.8 DHCP Server Backup and Recovery Considerations	235
Chapter 11. Start Here: Implementing DHCP in a Simple Network	237
11.1 Scenario Overview	237
11.1.1 Scenario Objectives	237
11.1.2 Scenario Advantages	237
11.1.3 Scenario Disadvantages	238
11.1.4 Scenario Network Configuration	238
11.1.5 Network Addressing Scope Planning	238
11.2 Task Summary	239
11.3 Verify Hardware, Software, and Configuration Prerequisites	239
11.4 Configuration Overview	240
11.4.1 Configure TCP/IP Interface on the AS/400 System	240
11.4.2 Gather Information to Configure the DHCP Server	241
11.4.3 Configure DHCP Server through Operations Navigator	243
11.5 Configuring DHCP Clients	249
11.5.1 Configuring DHCP on Windows 95 Clients	249
11.5.2 Configuring DHCP on the IBM Network Station	251
11.6 Selecting the Bootstrap Host for the IBM Network Station	252
11.7 Summary	259
Chapter 12. Using Multiple DHCP Servers to Minimize Failures.	261
12.1 Scenario Overview	261
12.1.1 Scenario Objectives	262
12.1.2 Scenario Advantages	262
12.1.3 Scenario Disadvantages	262
12.1.4 Scenario Network Configuration	263
12.2 Dividing the Address Pool across Two DHCP Servers	263
12.2.1 Objectives	263

12.2.2 Advantages	264
12.2.3 Disadvantages	264
12.3 Task Summary	264
12.3.1 Verify Hardware, Software, and Configuration Prerequisites	264
12.3.2 Reduce the Primary DHCP Server IP Address Pool	264
12.3.3 Change the Number of Options on the Primary and Backup DHCP Servers	266
12.3.4 Add the Remaining IP Addresses to the Backup Server	266
12.3.5 Change the Lease Time on the Primary and Backup DHCP Servers .	269
12.3.6 Start the Primary and Backup DHCP Servers	270
12.4 Providing Full-DHCP Client Support	271
12.4.1 Objectives	271
12.4.2 Advantages	271
12.4.3 Disadvantages	271
12.4.4 Network Addressing Scope Planning	271
12.4.5 Task Summary	272
12.4.6 Verify Hardware, Software, and Configuration Prerequisites	272
12.4.7 Enlarge the Primary DHCP Server IP Address Pool	272
12.4.8 Add the Remaining IP Addresses to the Backup DHCP Server . .	273
12.4.9 Start the Primary and Backup DHCP Servers	274
12.5 Summary	275
Chapter 13. Multiple Subnets and DHCP Servers	277
13.1 Scenario Overview	277
13.1.1 Scenario Objectives	277
13.1.2 Scenario Advantages	278
13.1.3 Scenario Disadvantages	278
13.1.4 Scenario Network Configuration	278
13.2 Task Summary	279
13.3 Configuration Overview	280
13.3.1 Configuring TCP/IP Interfaces on AS1	280
13.3.2 Gathering Information to Configure DHCP Servers	280
13.3.3 Configuring DHCP Server Support in AS1	285
13.3.4 Configuring TCP/IP Interfaces on AS5	290
13.3.5 Configuring DHCP Server Support on AS5	291
13.3.6 Start the DHCP Server Support on Both Systems	295
13.3.7 Configuring DHCP Clients	296
13.3.8 Analyzing the DHCP Logs	297
13.3.9 Conclusion	302
13.4 Configuring Subnet B on AS1	302
13.5 Summary	312
Chapter 14. Multiple Subnets, DHCP Servers, and Relay Agents	313
14.1 Scenario Overview	313
14.1.1 Scenario Objectives	314
14.1.2 Scenario Advantages	315
14.1.3 Scenario Disadvantages	315
14.1.4 Scenario Network Configuration	316
14.2 Task Summary	317
14.2.1 Planning the TCP/IP Addressing Scheme	317
14.2.2 Gathering Information to Configure DHCP Servers and DHCP Relay Agents	318

14.2.3	Configure the Primary DHCP Server (AS1)	326
14.2.4	Configure the Backup DHCP Server (AS2)	332
14.2.5	Configure Routing Information on Both DHCP Servers	334
14.2.6	Configuring a BOOTP/DHCP Relay Agent	336
14.2.7	Configure the Microsoft NT BOOTP/DHCP Relay Agent	338
14.2.8	Start the DHCP Servers and BOOTP/DHCP Relay Agents	340
14.3	Summary	341
Chapter 15.	Configuring Twinax IBM Network Station with DHCP	343
15.1	Getting Started: Basic IP over Twinax Configuration	343
15.1.1	Scenario Overview	344
15.1.2	Scenario Objectives	344
15.1.3	Scenario Advantages	344
15.1.4	Scenario Disadvantages	345
15.1.5	Scenario Network Configuration	345
15.1.6	Task Summary	345
15.1.7	Define a TCP/IP Address Range	345
15.1.8	Configure and Start the DHCP Server on AS2	346
15.1.9	Start the IBM Network Station	351
15.1.10	Summary	352
15.2	Transparent Subnet Masking	352
15.2.1	ARP and Proxy ARP	353
15.2.2	Twinax Transparent Subnetting	356
15.3	Configuring Twinax IBM Network Station with Local DHCP Server	359
15.3.1	Scenario Objectives	360
15.3.2	Scenario Advantages	360
15.3.3	Scenario Disadvantages	360
15.3.4	Scenario Network Configuration	360
15.4	Task Summary	362
15.4.1	Plan the TCP/IP Addressing Scheme	362
15.4.2	Carve out 64 Addresses from the Administered Address Pool	363
15.4.3	Configure the DHCP Server AS2 for Twinax Support	366
15.4.4	Configure and Start the IBM Network Station	369
15.4.5	Test Connectivity	373
15.4.6	Summary	373
15.5	Configuring Twinax Network Station with a Remote DHCP Server	373
15.5.1	Scenario Overview	374
15.5.2	Scenario Objectives	375
15.5.3	Scenario Advantages	375
15.5.4	Scenario Disadvantages	375
15.5.5	Task Summary	375
15.5.6	Configure the Local DHCP Configuration File on AS2	376
15.5.7	Power on the IBM Network Station	376
15.5.8	Configure and Start BOOTP/DHCP Relay Agent on Local AS/400 System (AS2)	376
15.5.9	Change the DHCP Server Configuration for the Address Pool 10.1.1.x on AS1	378
15.5.10	Configure the Twinax Subnet Address Pool on the Remote DHCP Server	380
15.5.11	Start the IBM Network Station	382
15.5.12	Summary	382
15.6	Configuring Twinax IBM Network Station Using Transparent Subnetting	383
15.6.1	Scenario Overview	383

15.6.2	Scenario Objectives	384
15.6.3	Scenario Advantages	384
15.6.4	Scenario Disadvantages	384
15.6.5	Task Summary	384
15.6.6	Planning the IP Address Scheme	384
15.6.7	Configure As2.mycompany.com	386
15.6.8	Configure As5.mycompany.com	388
15.6.9	Configure the DHCP Server on As1.mycompany.com	392
15.6.10	Summary	398
Chapter 16.	Migrating BOOTP Servers to DHCP	399
16.1	Considerations	399
16.2	Scenario 1: Migrating Existing BOOTP to a New DHCP Configuration	401
16.2.1	Scenario Objectives	401
16.2.2	Existing Environment	401
16.2.3	Migrating BOOTP to a New DHCP Configuration	403
16.2.4	Migrating BOOTP to an Existing DHCP Configuration	405
16.2.5	Summary	406
Chapter 17.	DHCP Problem Determination	407
17.1	Performing Basic Troubleshooting	407
17.1.1	Program Temporary Fixes (PTFs)	407
17.2	Starting and Reading the DHCP Logging Utility	407
17.2.1	Starting the DHCP Logging Utility	407
17.2.2	Reading the DHCP Log	408
17.2.3	Finding the Incoming DHCPDISCOVER Data in the Log	413
17.2.4	Finding and Reading the DHCPOFFER Information in the Log	415
17.2.5	Finding and Reading the DHCPREQUEST and DHCPACK Information	417
17.3	Starting, Formatting, and Decoding an AS/400 Communication Trace	419
17.3.1	Start the AS/400 Communication Trace	419
17.3.2	Stopping the AS/400 Communication Trace	420
17.3.3	Reading and Decoding the AS/400 Communications Trace Data	421
17.4	Symptoms, Problems, and Resolutions	423
17.5	DHCP Server Performance Considerations	428
Appendix A.	Mail Concepts	431
A.1	Basic Mail Configuration	431
A.2	Mail Forwarding	433
A.2.1	Implementing Mail Forwarding	434
A.3	Processing Inbound Mail	437
A.4	Processing Outbound Mail	438
Appendix B.	Special Notices	441
Appendix C.	Related Publications	443
C.1	International Technical Support Organization Publications	443
C.2	Redbooks on CD-ROMs	443
C.3	Other Publications	443
C.4	Web Resources	443
How To Get ITSO Redbooks.	445
How IBM Employees Can Get ITSO Redbooks		445
How Customers Can Get ITSO Redbooks		446

IBM Redbook Order Form	447
Index	449
ITSO Redbook Evaluation	457

Preface

This redbook describes the new Domain Name System (DNS) server and Dynamic Host Configuration Protocol (DHCP) server support that are included in OS/400 V4R2.

The information in this redbook helps you install, tailor, configure, and troubleshoot the new DNS and DHCP support on the AS/400 system through examples that evolve from simple to more complex scenarios. It also contains examples that show the integration of the new DNS server support with mail and Internet firewall implementation on the AS/400 system. Scenarios are included to show the use of DHCP to automate the configuration of clients in a TCP/IP network including LAN and twinax-attached IBM Network Stations.

This book is designed to show the use of the AS/400 system implementation of DNS and DHCP through examples. It also references other publications that contain detailed information on DNS, DHCP, and IP addressing.

The intended audience for this redbook includes the system or network administrator who plans, configures, and maintains TCP/IP AS/400 networks.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Rochester Center.

Marcela Adan is a Senior International Technical Support Representative at the International Technical Support Organization, Rochester Center. She writes extensively and teaches IBM classes worldwide on all areas of AS/400 Internet technologies and system management. She has held several positions as field technical support representative, network administrator, developer, and consultant.

Andrew Grant is a communications specialist working for IBM Managed Operations Group in New Zealand. He has 8 years of experience with IBM mid-range systems, communication, and PC connectivity. His main area of expertise is the design, implementation, and support of large, multi-platform networks including host inter-connectivity and desktop-to-host configuration and trouble shooting over a variety of communication protocols.

Susan M. Goodrich is a Staff Software Analyst with IBM AS/400 Software Service and Support in Rochester, MN. She has 5 years of experience in the area of SNA and TCP/IP communications. Prior to this assignment, she worked as a Staff Systems Engineer in the IBM Marketing organization specializing in S/36, S/38, and AS/400 systems.

Masahiko Hamada is an I/T specialist in IBM Japan. He has 11 years of experience with IBM mid-range systems. His areas of expertise include OO application development, AS/400 connectivity to Microsoft Windows 95/NT, and Client Access/400. He developed ToolBox/400 used in Japanese environments. Currently, his focus is on AS/400 Internet technologies. He has written several technical documents and taught classes in the U.S., Europe, and Japan.

Guenter Ilmberger is an Advisory Technical Support Specialist with IBM Germany. He has 30 years of experience in data processing, including 25 years with IBM. His expertise is in all areas of AS/400 communication and systems management. He frequently conducts presentations at conferences and teaches several workshops on AS/400 communication and systems management topics.

Thanks to the following people for their invaluable contributions to this project:

Suehiro Sakai
Fant Steele
International Technical Support Organization, Rochester Center

Joseph Caldwell
John Corcoran
Gary Diehl
Scott Evans
Frank Gruber
Steve Gruber
Susan Hall
Joseph Miller
Francis Pflug
IBM Endicott Laboratory

Janice Glowacki
Kent Hofer
Mark McKelvey
A.J. Meyers
Marion Pitts
George Romano
Ray Romon
Daryl Spartz
IBM Rochester Laboratory

Peggy Warley
IBM Product Support Services

The editors of this redbook were:
Lois Douglas
Scott Kalar
Jenifer Servais

Comments Welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in “ITSO Redbook Evaluation” on page 457 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

For Internet users <http://www.redbooks.ibm.com>

For IBM Intranet users <http://w3.itso.ibm.com>

- Send us a note at the following address:

redbook@us.ibm.com

Part 1. AS/400 DNS Support

Domain Name System (DNS) handles the mapping of human-friendly names to internet address computers. DNS is also the mechanism used in the Internet to advertise and access a variety of information about hosts. It is used by all internetworking software, including mail, FTP, TELNET, and Internet Firewall.

Part 1 of this book provides an overview of DNS basic concepts and explains the DNS implementation in the AS/400 system through case studies.

Chapter 1. Domain Name System Concepts and Overview

This chapter provides an overview of Domain Name System (DNS) concepts and components. Our intention is to summarize the concepts you need to understand to implement DNS on the AS/400 system. We refer many times throughout this redbook to *DNS and BIND* by Albitz & Liu. This book is a *MUST* for DNS administrators. For more information on the AS/400 implementation of DNS server support, refer to *TCP/IP Configuration and Reference*, SC41-5420-01.

1.1 Overview

The Domain Name System is a distributed database. This allows local control of the segments of the entire database, and data in each segment are also available across the entire network through a client/server scheme.

The structure of the DNS database is similar to the structure of a file system. The whole database or file system is pictured as an inverted tree with the root at the top. Each node in the tree represents a partition of the database. Each domain or directory can be further divided into partitions, called subdomains (such as the file system's subdirectories).

The domain name space is "*tree*" structured. The top-level domains divided the Internet domain name space organizationally. Examples of top-level domains are:

- *com*: Commercial organizations, such as IBM (*ibm.com*), CNN (*cnn.com*), mycompany (*mycompany.com*). *ibm* is a subdomain of the top-level domain *com*.
- *edu*: Educational organizations, such as University of Minnesota (*umn.edu*), New York University (*nyu.edu*).
- *gov*: Government organizations, such as the Federal Bureau of Investigation (*fbi.gov*), and the National Science Foundation (*nsf.gov*).

The tree is limited to 127 levels; this is a limit on subdomains, although there is no limit on the number of branches at each node.

Each node in the tree is labeled with a name (see Figure 1). The root has a null label (" "). The full domain name of any node in the tree is the sequence of names on the path from the node up to the root with a dot between node names. For example, in Figure 1, if you follow the arrows from the bottom label to the top, from the host: *www* to the root label, you can form the full domain name for that host: *www.as400.ibm.com*.

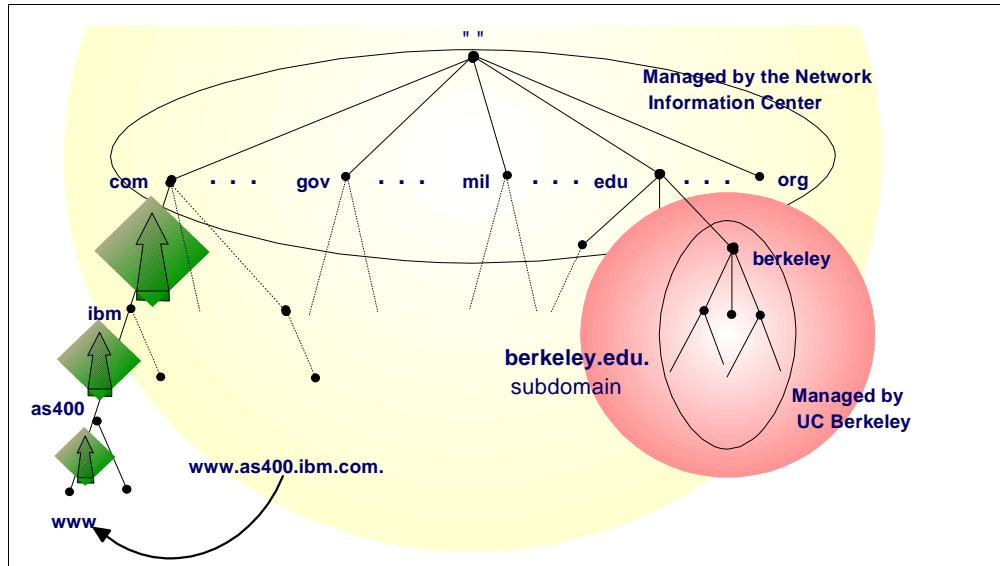


Figure 1. DNS Name Space

In DNS, each domain can be administered by a different organization. Each organization can then break its domains into a number of subdomains and dole out the responsibility for those domains to other organizations. This is because DNS uses a distributed database where you can manage your own domain (*company.com*), or parts of the name space (subdomains) can be delegated to other servers (*department.company.com*). In Chapter 5, “Growing Your Domain: Creating Subdomains” on page 83, we discuss delegating a subdomain to another DNS server.

The DNS servers responsible for the top level Internet domains such as *com* are also called *Internet root servers* that manage information about the top-level domains. For example, the Internet's Network Information Center runs the *edu* domain, but assigns U.C. Berkeley authority over the *berkeley.edu* subdomain.

Domains can contain both hosts and other domains (their subdomains). For example, the *ibm.com* domain contains hosts such as *www.ibm.com*, but it also contains subdomains such as *as400.ibm.com*.

Domain names are used as indexes into the DNS database.

Each host on a network has a domain name with a DNS server that points to information about the host. This information may include an IP address, information about mail routing, and so on.

Why all this complicated structure? It is to solve the problems that a host table has. For example, making names hierarchical eliminates the problem of name collisions. Domains are given unique domain names, so organizations are free to choose names within their domains. Whatever name they choose, it does not conflict with other domain names, since it has its own unique domain name.

For example, we can have several hosts named *www* such as *www.ibm.com* and *www.yahoo.com* because they are in different domains managed by different organizations. See Figure 2.

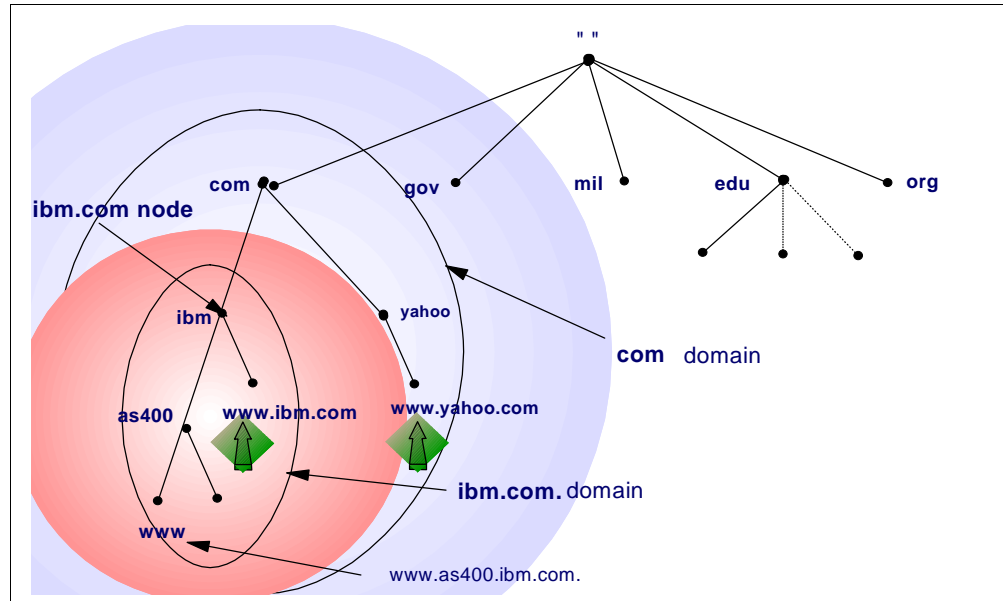


Figure 2. Hosts With Same Names in Different Domains

We can have a host in the same domain that also has the same host name such as *www.ibm.com* and *www.as400.ibm.com* because they belong to different subdomains.

1.2 Domain versus Zone of Authority

The concept of domains versus zones of authority can be a confusing one. We try to explain it in this section.

One of the main goals of the design of the Domain Name System is decentralization. This is achieved through **delegation**. The central DNS administrator in your company administering the company's domain can divide it into subdomains. Each subdomain can be delegated to other administrators. This means that the administrator delegated to becomes responsible for maintaining the subdomain.

A **domain** is a subset or subtree of the name space tree. A **subdomain** is a subset of the domain. Figure 3 on page 7 shows the domain *mycompany.com* as a subset of the *.com* name space. Under *mycompany.com*, there are other subdomains such as *endicott.mycompany.com*, *rochester.mycompany.com*, and *otherdomain.mycompany.com*.

Name Servers are programs running on a system, such as the AS/400 system, with DNS support. In Figure 3 on page 7, *as1.mycompany.com*, *rst.rochester.mycompany.com*, and *otherhost.otherdomain.mycompany.com* are hosts running name server programs; they are called Domain Name System (DNS) servers or simply name servers.

Name servers have information about some part of the domain name space called a **zone** or **zone of authority**. Both domains and zones are subsets of the domain name space. A zone contains host information and data that the domain contains excluding the information that is delegated somewhere else. If a

subdomain of a domain is not delegated, the zone contains host information and data for the subdomain.

Name servers have complete host information and data for a specific zone. Name servers are said to be **authoritative** for the zone for which they have this complete host information and data.

Refer to Figure 3. The *mycompany.com* domain is divided into the subdomains *endicott.mycompany.com*, *rochester.mycompany.com*, and *otherdomain.mycompany.com*. The zone *mycompany.com* contains the hosts: *as1.mycompany.com*, *as2.mycompany.com*, *as5.mycompany.com*, and *NTserver1.mycompany.com*.

It also contains the host information and data in the subdomain *endicott.mycompany.com*: *host1.endicott.mycompany.com* and *host2.endicott.mycompany.com*. The subdomain *endicott.mycompany.com* has not been delegated, and its host information and data remain in the *mycompany.com* zone. The administration of the *endicott.mycompany.com* is the responsibility of the *mycompany.com* administrator. *AS1.mycompany.com* is the name server that has complete host information and data for the *mycompany.com* zone of authority.

The zone *mycompany.com* does *not* contain information in the subdomains that have been delegated.

rochester.mycompany.com is a subdomain of *mycompany.com* and its administration has been delegated. The zone *rochester.mycompany.com* includes host information and data in the subdomain *rochester.mycompany.com*: *rst.rochester.mycompany.com*, *host1.rochester.mycompany.com*, and *host2.rochester.mycompany.com*. *rst.rochester.mycompany.com* is the DNS server that has complete host information and data for the *rochester.mycompany.com* zone.

otherdomain.mycompany.com is a subdomain of *mycompany.com* and its administration has been delegated. The zone *otherdomain.mycompany.com* includes host information and data in the subdomain *otherdomain.mycompany.com*: *otherhost.otherdomain.mycompany.com*, *otherprinter.otherdomain.mycompany.com*, and *otherserver.otherdomain.mycompany.com*. *otherhost.otherdomain.mycompany.com* is the DNS server that has complete host information and data for the *otherdomain.mycompany.com* zone.

Section 5.5, “Method 2: Adding a Subdomain and Delegating Authority” on page 96 discusses a scenario in which a subdomain is delegated to another DNS server.

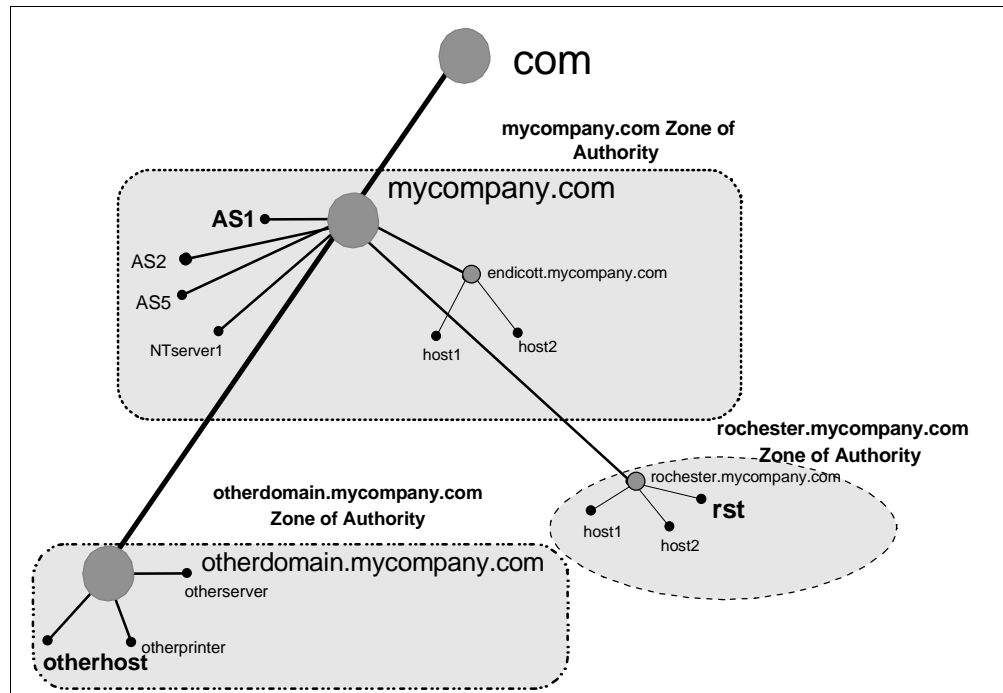


Figure 3. Domain, Subdomain, Delegation, and Zone of Authority

1.3 Name Resolution

Programs called name servers comprise the server half of DNS's client/server mechanism. Name servers contain information about some segment of the database and make it available to clients, called resolvers.

The Domain Name System has two major components:

- **NAME SERVERS** are programs that hold information about the domain name space. A name server may cache information about any part of the domain tree but, in general, a particular name server has complete information about a subset of the domain space and pointers to other name servers that can be used to lead to information from any part of the domain tree. The part of the domain space the name server has complete information for is called a *zone*. It is said that the name server is *authoritative* for that zone. Name servers can be authoritative for multiple zones.
- **RESOLVERS** are programs that extract information from name servers in response to client requests. Resolvers must be able to access at least one name server and use that name server's information to answer a query. A resolver is typically a system routine that is directly accessible to user programs. No protocol is necessary between the resolver and the user program.

Mapping names to addresses, a process called domain name resolution, is provided by independent, cooperating systems called servers. A name server is a server program answering requests from clients called a name resolver.

Each name resolver is configured with a name server to use (and possibly a list of alternatives to contact if the primary is unavailable).

Figure 4 shows schematically how a program uses a name resolver to convert a host name to an IP address on the Internet. A user provides a host name, and the user program uses a library routine, called a resolver, to communicate with a name server that resolves the host name to an IP address and returns it to the resolver, which returns it to the main program. The name server may obtain the answer from its name cache (if it has tried to resolve the name before), its own database, or another name server.

In Figure 4, the resolver sends a query for *www.as400.ibm.com* to its DNS server (in the figure, labeled primary name server). If the query is for information out of the name server's zone of authority (it does not know the answer), the name server sends another query to the Internet root name server, which responds back, "I don't know but query this next DNS server (the *com* DNS server)." And the query is iterated to various DNS servers down the "*com*" branch of the Internet DNS name space until the DNS server is found that is authoritative (is responsible for) the *as400.ibm.com* domain. This last DNS server has the answer and sends the response back to the original DNS server the resolver asked for, which passes the response back to the resolver.

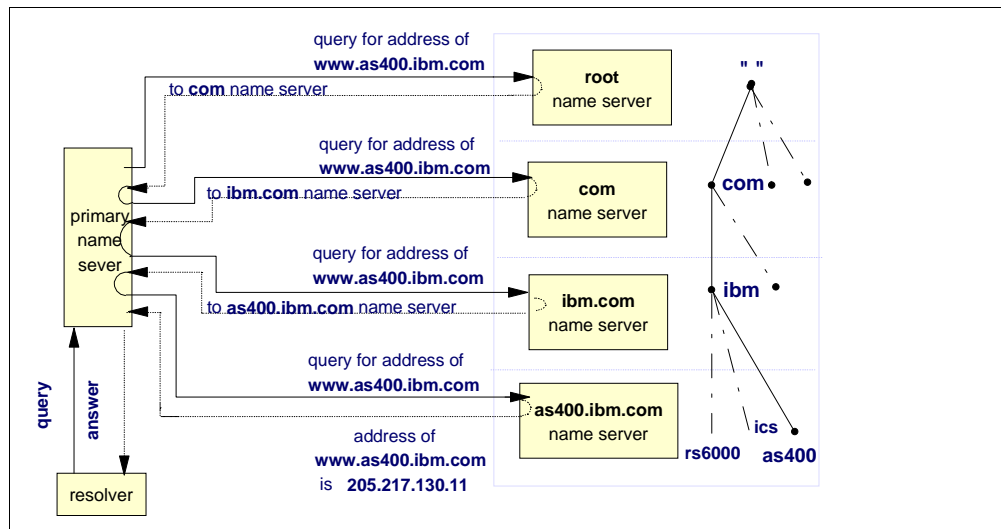


Figure 4. Name Resolution Example

Recursive versus Iterative Queries

There are two types of DNS queries: recursive or iterative.

Figure 4 shows an example of one recursive query and several iterative queries. The first query from the resolver to the primary name server is a recursive query. A recursive query requests that if the name server does not know the answer to the query that it query other name servers until it finds the answer and then sends the answer back to the resolver. Notice in Figure 4, the primary name server did a lot of work: it kept querying other name servers on behalf of the resolver until it could supply the answer. A DNS server is configured to accept recursive queries or only accept iterative queries. The primary name server in Figure 4 was configured to allow recursive queries.

The other name servers queried in Figure 4 (root name server, *com* name server, *ibm.com* name server) were not configured to allow recursive queries. When the primary name server queried the root name server, the query was an iterative

query. This means the root name server responded to the query with the best information it had, which was, "I don't know but check the next DNS server: *com* name server." The recursive query versus iterative query only comes into play when the name server queried does not know the answer to the query. From the example in Figure 4, we cannot tell if the *as400.ibm.com* name server is configured to allow recursive queries because this name server held the answer for the primary name server and responded with the answer.

1.4 Types of Name Servers

Primary name server:

This server is the server that the hosts in the zone of authority are configured on. It is the server that the DNS administrator configures and maintains. When this server gives responses to queries from its primary domain files, the responses are called authoritative. A name server for a primary domain reads the primary domain configuration information directly from files configured by DNS administrator.

Secondary name server:

This server has the same information as the primary name server. However, instead of getting its information directly from the DNS administrator configuring it, it gets its information from another name server through zone transfers over the network. The information that a secondary name server obtains from a zone transfer is read into cache as is data stored from queries.

Note

A DNS server can be a primary name server for one or more domains as well as a secondary name server for one or more domains. It can be a name server for primary and secondary domains.

A **zone transfer** is a TCP/IP transfer of domain files from another DNS server (called a master name server). This is done automatically when the secondary name server starts and also when the secondary name server detects its domain files are downlevel from the master name server's domain files. The zone transfer is initiated from the secondary name server. The zone transfer cannot take place if the master name server is not active.

A secondary name server is used for two reasons: spreading the DNS query workload over more than one server and as a backup in case the primary name server stops responding. When a client is configured with more than one DNS server and the first name server (the primary) does not respond, the client can query the second name server (the secondary). When the secondary name server gives out a response to a query, the response is also called authoritative. In other words, an answer from a secondary name server is considered to be just as "good" as if the answer came from a primary name server.

Master name server:

A master name server is the name server that a secondary name server gets its zone transfer from. A master name server can either be a primary name server or another secondary name server.

Caching-only name server:

A name server that does not have authority over any zone is called a caching-only name server. It gets all of its information by querying. A caching-only name server's responses are always non-authoritative.

Authoritative name server:

A server that is considered to be authoritative for a domain is either the primary server for that domain or a secondary server for that domain. Chapter 3, "Implementing Primary and Secondary DNS Servers" on page 25 shows a scenario that configures a primary and a secondary DNS server. If another name server or a client queries either the primary or the secondary name server for information that they are authoritative for, the response is considered to be authoritative. Can a name server that is not authoritative over a domain give a response to a client about that domain and have that response considered an authoritative response? The answer is yes. If the non-authoritative server does not know the answer and queries an authoritative name server on behalf of the client and then returns the answer to the client, this response is considered to be authoritative. The non-authoritative name server caches this information. If a second client requests this same information from the non-authoritative name server (and this information is still in its cache), the name server gives the response to the client but now this same information is labeled non-authoritative. Why? Because the information in the response this second time came out of the name server's cache. Another way of saying this is: a non-authoritative response at some point came out of a name server's cache.

Parent and child name servers:

The concept of parent and child domains is equivalent to the concept of domain and subdomain: once your domain grows to a certain size, you may need to distribute management by delegating authority of part of your domain to one or multiple subdomains. The upper-level domain is the parent and its subdomains the children.

The name server authoritative for the parent domain is the parent name server and the one authoritative for the subdomain is the child name server. For example, in Figure 3 on page 7, *OTHERDOMAIN* is a subdomain of *mycompany.com*. If a DNS server, AS1, is configured to be responsible for the *mycompany.com* zone of authority and the authority for the zone *OTHERDOMAIN.mycompany.com* is delegated to another DNS server, *OTHERHOST*, then AS1 is considered to be the **parent name server** and *OTHERHOST* is considered to be the **child name server**.

A scenario in which authority is delegated from a parent to a child name server is covered in Section 5.5, "Method 2: Adding a Subdomain and Delegating Authority" on page 96.

Root name servers:

Internet root name servers know where name servers authoritative for the top-level domains are and most of the Internet root name servers are authoritative for the top-level organizational domains (*.com*, *.edu*, *.net*, and so on). The top-level domain servers have information about the second-level domain a given domain is in.

A company can implement internal root name servers. In this case, given a query for a company's subdomain, the internal root name server can provide information for the second-level subdomain the queried subdomain is in.

A root name server is configured in a lower level name server to help it to navigate the name space tree top down when it cannot answer a query with authoritative data or data in its cache.

If we use the example discussed in the previous section, the DNS server *OTHERHOST* is authoritative for the zone *OTHERDOMAIN.mycompany.com* shown in Figure 3 on page 7. AS1 name server is authoritative for the *mycompany.com* zone of authority AND is configured as internal root for the whole company's name space. The internal roots can run on host systems all by themselves or a given host can perform double duty as an internal root and as an authoritative name server for other zones. If *OTHERHOST* cannot answer a query, it asks its root name server, which is AS1, the DNS server at the top of the INTERNAL name space tree. We stress INTERNAL because in this example, these DNS servers are only part of an internal network. We are assuming that the network does not have Internet access; thus, the Internet "com" node is not part of this DNS name space tree. Therefore, the DNS server AS1 in domain *mycompany.com* is at the top of tree. A root name server can be thought of as the name server at the **top** of the DNS name space tree. Just remember that the DNS name space tree may be different, depending on whether the network is an internal network or if the network includes the Internet DNS name space.

An example of using Internet root name servers was covered in Section 1.3, "Name Resolution" on page 7. In this case, the top of the DNS name space tree really was the top of the Internet name space tree and the root name servers used were the Internet root name servers.

Forwarders:

A DNS server can be configured to send the queries it does not know the answer to, to a DNS server called a forwarder name server. Whereas going to a root name server for help in answering a query can be thought of as going to the top of the DNS name space tree, going to a forwarder can be thought of as going side-ways in the DNS name space tree for help. The DNS administrator configures which DNS server is the forwarder. Usually several DNS servers are configured to have the same forwarder. Then the forwarder name server is configured with the root name servers (for example, the Internet root name servers). If the forwarders cannot answer the query, they query the root name servers, get the answer, and cache it. This way, a forwarder name server can build up a large cache of information. As the cache increases, chances are that the forwarder will receive a query in which it has a cached answer for. This, in turn, reduces the number of times a root name server needs to be queried. Using a forwarder name server is an opportunity to build a large cache of information on one (or just a few) name server.

In Chapter 6, "Split DNS: Hiding Your Internal DNS Behind a Firewall" on page 125, we configure an internal DNS server to forward unresolved queries to the company's firewall DNS server.

1.5 Split DNS Concept for Firewalls

When constructing a firewall, we use Domain Names Services in a particular way so that a company's internal users can locate the IP addresses of all systems (internal and public) while users on the Internet can only locate the IP addresses

of the company's public systems. This is part of our effort to hide the company's internal network information from the Internet.

It is not necessary to expose a company's internal network to the Internet. A technique called Split DNS may be used to only expose the company's public machines to the Internet. Split DNS uses two DNS servers, an internal DNS for secure and private names, and a firewall DNS for the company's "public" names.

The internal DNS server manages the company's internal IP data. The firewall DNS is the only company name server containing information visible from the Internet. Only some of the company's hosts need to be known by the Internet: the e-mail relay, the WWW public server, and the firewall name server itself. The Internet Service Provider (ISP) may provide DNS support for the public hosts in addition to or instead of the firewall DNS.

The internal name server forwards queries for information it cannot resolve to the firewall DNS server.

An AS/400 system at release R4V2M0 can now be a company's internal DNS. Once the AS/400 name server is configured, it contains files of all the company's internal hosts. These files map host names to IP addresses (or vice versa). It does this for a particular domain that it is responsible for (called a zone of authority). For example, the IP address of the host with host name *client1.private.mycompany.com* is *192.168.67.3*. The internal name server lets all of the company's internal hosts locate each other by name in the TCP/IP network.

For protection from the Internet, a company also can use a firewall DNS server. The firewall DNS server's zone of authority are the company's hosts that are public. These are the hosts that the company wants to make visible on the Internet. The split DNS concept is used in the configuration scenario discussed in Chapter 6, "Split DNS: Hiding Your Internal DNS Behind a Firewall" on page 125.

1.6 Types of Files

Primary domain files:

These files are the files configured on the primary name server. On the AS/400 system, they are contained in the IFS directory: /QIBM/UserData/OS400/DNS. Primary domain files have a .DB extension.

Secondary domain back up files:

These files contain information that is acquired from zone transfers from the primary name server. They exist on the secondary name server. A secondary name server loads these files and uses them to answer queries provided the zone transfer was successful.

Forward mapping files:

Forward mapping primary domain files reside on the primary name server. They contain all data for mapping host names to IP addresses in a zone. A DNS server is authoritative for a certain part of the DNS name space tree. This part of the tree is called a zone or the DNS server's zone of authority.

TIP

Every forward mapping primary domain file should be configured with the host *localhost* with an IP address of 127.0.0.1.

Reverse mapping files:

The reverse mapping primary domain files reside on the primary DNS server. They contain the information for mapping IP addresses to host names in a zone. They are also called the in-addr.arpa files. An example of a reverse mapping file is the *69.5.10.in-addr.arpa* file. This is the file a DNS server uses if a client resolver queries with an IP address of 10.5.69.222 and asks the DNS server to supply the host name belonging to that IP address. The *69.5.10.in-addr.arpa* file also resides in the AS/400's IFS directory */QIBM/UserData/OS400/DNS* with a file name of *69.5.10.in-addr.arpa.DB*.

Boot file:

The boot file is the file the DNS server first reads when it starts. It contains information such as:

- The type of name server
- The zones that this name server is authoritative for
- Where (file location) the name server should get its information

The boot file is also located in the */QIBM/UserData/OS400/DNS* directory.

NOTE

The presence of the Boot file in the IFS directory */QIBM/UserData/OS400/DNS* determines whether or not the Operations Navigator DNS configuration presents the user with the DNS Wizard windows. If the AS/400 DNS has never been configured, the Boot file does not exist and the first time a user clicks on DNS configuration within Operations Navigator, the Wizard windows are presented. Wizard creates the Boot file.

Cache file:

The cache file contains information about the root name servers. This is where the DNS server should go when it cannot resolve a query itself. This file is located in the */QIBM/UserData/OS400/DNS* directory.

In later chapters, we say that a name server "caches" information it receives from another name server. This is a way a name server "remembers" information so if it receives a query from a client for the same host, it can respond with an answer from its cache and not query the authoritative name server again. It is important to understand that this cached information is **not** contained in the */QIBM/UserData/OS400/DNS/CACHE* file. The *CACHE* file contains information about root servers.

Local file:

The local file contains the PTR record for the local loopback interface. The loopback interface, also known as *localhost*, has the IP address of 127.0.0.1. Hosts use the 127.0.0.1 IP address to direct TCP/IP traffic to themselves.

1.7 Types of Records

The information contained in forward and reverse primary domain files are organized into records called resource records. There are several types of resource records and we try to explain the most common ones in this section. The following list is not a complete list. For more details on resource records, see the second edition of *DNS and BIND* by Albitz & Liu.

- **A record:** An A record is a record that maps a host name to an IP address. There is one A record for every host configured in the DNS server. Consequently, a query that supplies the host name and asks for the IP address is sometimes called an A record query. A records are contained in the forward mapping primary domain file. This type of query is also called a forward mapping query.
- **PTR record:** A PTR record is a record that maps an IP address to a host name. There is usually one PTR record for every host configured in the DNS server. These records are located in the reverse mapping primary domain files, which are also called the in-addr.arpa files. A query supplying the IP address and asking for the host name is sometimes called a reverse mapping query, a reverse lookup, or an in-addr.arpa query.
- **SOA record:** The first record in the forward and reverse mapping primary domain files is the SOA record. The SOA record marks the zone of authority in the domain name space. It contains the domain name, the name of the DNS server that is primary for this zone of authority, and the e-mail address of the zone's technical contact. The SOA record also contains the file's serial number. The serial number can be thought of as the change level of the data in this zone. In other words, if a DNS configuration change is made to this zone, the serial number must be incremented (Operations Navigator does this automatically). Also, the SOA record contains refresh timers, retry rates, and expire timers, all having to do with secondary name servers. These terms are further explained in Section 3.2.6.4, "Controlling Zone Transfer Frequency" on page 60. Lastly, the SOA record contains the default TTL or time to live. This number controls how long another name server can cache the information supplied out of this name server's zone data. There can be a TTL specified on each resource record, which overrides the TTL specified in the SOA record.
- **CNAME record:** The CNAME record defines the canonical name of an alias. It is used to specify an alias name for a host.
- **MX record:** The MX record defines a mail exchanger host for a particular domain. This record is used by SMTP to send mail.
- **NS record:** The NS record defines a name server to this name server, either itself or another name server. The other name server can be a name server authoritative over another domain. Or the other name server can be a secondary name server to this same zone of authority. It is the NS records that allow each name server shown on the right side of Figure 4 on page 8 to tell the primary name server where to query next when it is searching for the answer to the resolver's query. NS records allow a DNS server to find other DNS servers authoritative for other zones.

1.8 Round Robin and Address Sorting

The concept of round robin and address sorting has to do with how a DNS server responds when it receives an A record query for a host that is multi-homed and has two IP addresses. A multi-homed host is attached to at least two networks. The DNS server always includes both IP addresses in its response, but which IP address is given first depends on the location of the client making the query:

1. If the client is physically located in one of the networks that the host it is querying for is located in, the DNS server lists the IP address of that network first in its response. Since clients generally try the IP address that is listed first in the response, this **address sorting** by the DNS server is beneficial because using the host's closer IP address provides better performance.
2. If the client is physically located on a network remote to either network that the host it is querying for is located in, the DNS server alternates which IP address it lists first in the response. The next time the name server is queried for the same host from a client that is remote to the host, the other IP address is listed first in the response. This IP address rotation in the DNS server responses is called **round robin**.

A detailed example of round robin and address sorting is discussed in Section 5.8, "Round Robin/Address Sorting" on page 121.

1.9 For More Information

When a DNS administrator is learning about DNS and how to configure the DNS server on the AS/400 system, we also recommend referring to several other resources on DNS that complement this redbook:

- *TCP/IP Configuration and Reference*, SC41-5420-01
- Operations Navigator online help
- *DNS and BIND* by Albitz & Liu, Second Edition, ISBN 1-56592-236-0
- RFC 1034 (Domain names concepts and facilities), RFC 1035 (Domain names implementations and specifications), and RFC 1912 (Common DNS Operational and Configuration Errors).
- *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162.
- *comp.protocols.dns.bind* newsgroup, which can be located on the Internet by entering the URL www.dns.net/dnsrd and clicking on the Newsgroup link.

Or alternatively, you can locate the same newsgroup by issuing a Find from the URL www.dejanews.com.

Chapter 2. AS/400 DNS Server Implementation

This chapter describes the implementation of the AS/400 DNS server.

2.1 DNS Software Prerequisites

Native DNS support on the AS/400 system in V4R2 requires the following products:

- 5769-SS1 OS/400 V4R2 option 31 - Domain Name System
- 5763-XD1 V3R1M3 - Client Access for Windows 95/NT

The AS/400 DNS implementation is a port of Berkeley Internet Name Domain (BIND) 4.9.3

2.2 DNS Installation

Installing DNS support on your AS/400 V4R2 system involves installing 5769-SS1 OS/400 V4R2 option 31, Domain Name System, and Client Access for Windows 95/NT (5763-XD1 V3R1M3) in your administrator's workstation. Use `GO LICPGM` option 11, *Install licensed programs* to install the DNS OS/400 option.

The installation program performs the following tasks:

- Installs the product library QDNS, which includes the product's objects (programs, message files, job descriptions, and so on).
- Creates two IFS subdirectories: `/QIBM/ProdData/OS400/DNS` and `/QIBM/UserData/OS400/DNS`.
- Creates the files, `TEMPLATE` and `ROOT.FILE`, in the `/QIBM/ProdData/OS400/DNS` subdirectory. `TEMPLATE` is used as a template to create all the DNS configuration files (`BOOT`, `CACHE`, and configuration files). `ROOT.FILE` holds information on root name servers needed to initialize the cache of Internet domain name servers.
- Creates the `ATTRIBUTE` file and `TMP` directory under the `/QIBM/UserData/OS400/DNS` subdirectory.

After the installation, you can proceed with the DNS server configuration using Operations Navigator. Figure 5 provides an overview of the AS/400 DNS server installation and configuration.

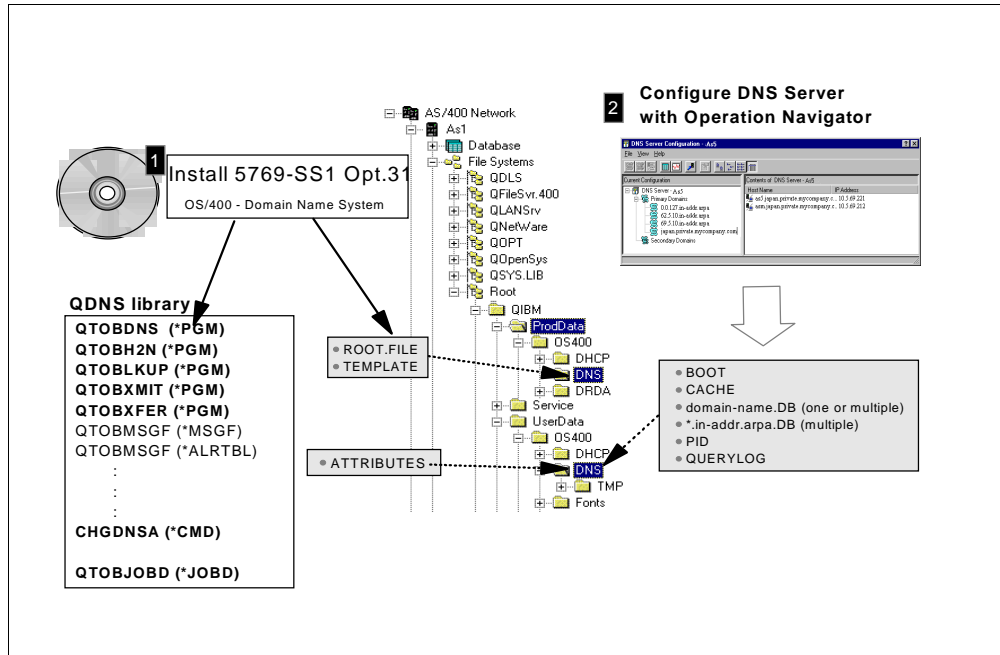


Figure 5. AS/400 DNS Support Installation and Configuration Overview

2.3 DNS Server Jobs

The DNS server jobs run in the QSYSWRK subsystem and they are:

- **QTOBDNS:** This is the DNS server job. It starts with the job description QDNS/QTOBJOBD.
DNS uses well-known port 53. DNS server messages are directed to the QTOBDNS job log. Use the Work with Spooled File (WRKSPLF) command for User QTCP to browse the DNS server job log.
- **QTOBXMIT:** This is the zone transfer job that runs on the AS/400 system acting as the primary master name server for a specific domain.
- **QTOBXFER:** This is the zone transfer job that runs on the AS/400 system acting as the secondary name server for a specific domain.

Note: The BOOT file contains information that determines whether the DNS server should start as a primary or secondary name server for a specific domain. Remember, a single DNS server can be a primary *and* a secondary for one or more primary and secondary domains.

2.4 DNS Configuration Files

All the DNS configuration files reside in the IFS directory `/QIBM/UserData/OS400/DNS` and they are:

- **Domain or forward mapping file (*Domain_Name.DB*):** This file maps host names to IP addresses. The entries in this file are called resource records. This file has the same name as the domain with the `.db` extension.

- Reverse mapping files or (*IP_address.in-addr.arpa.DB*): These files map addresses back to host name. There is one file for each subnet address in the network where the domain's hosts reside.
- Loopback address file (*0.0.127.in-addr.arpa.db*): This covers the loopback network used by the hosts to direct traffic to themselves.
- BOOT file (*BOOT*): This is the DNS server start-up file that ties all the DNS configuration files together.

Figure 6 shows the relationship between the BOOT file and the *.db files.

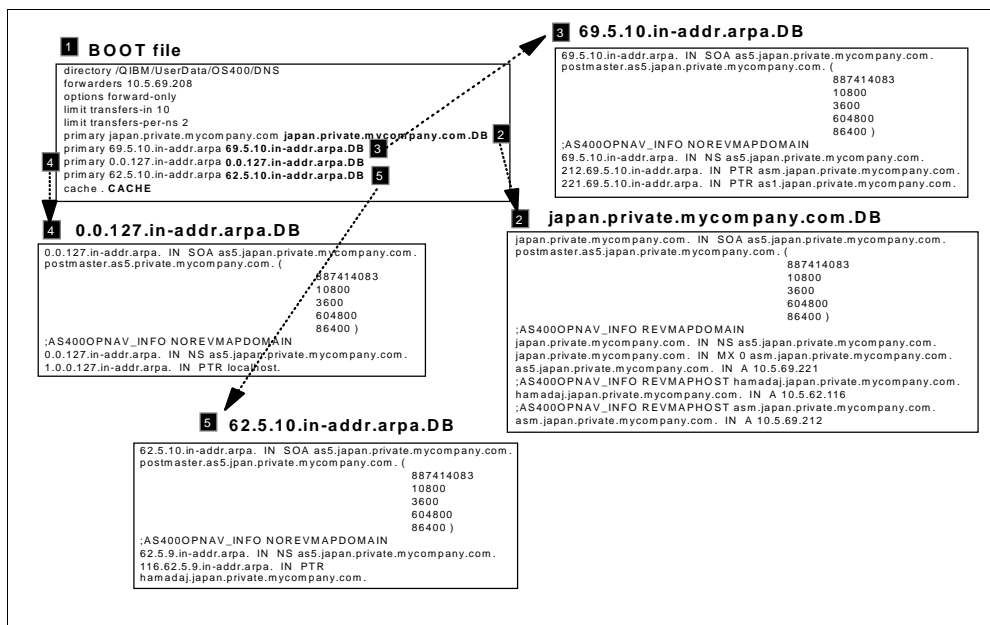


Figure 6. DNS Configuration Files Overview

2.4.1 Logging / Service Files

The following files are used to log DNS server activity and for problem determination:

- **QUERYLOG:** The DNS server logs every query in this file that it receives if it is configured to do so. To view the contents of the log, find it through Operations Navigator. The file name is QUERYLOG in the directory path FileSystems\Root\QIBM\UserData\OS400\DNS for your AS/400 system.

Carefully consider whether you need to log all queries and for how long. There is no limit to the size of the log file. Once you turn it on, it remains on until you disable logging and re-boot the DNS server. Figure 7 shows how to specify that you want the DNS server to log all the queries it receives in the QUERYLOG file.

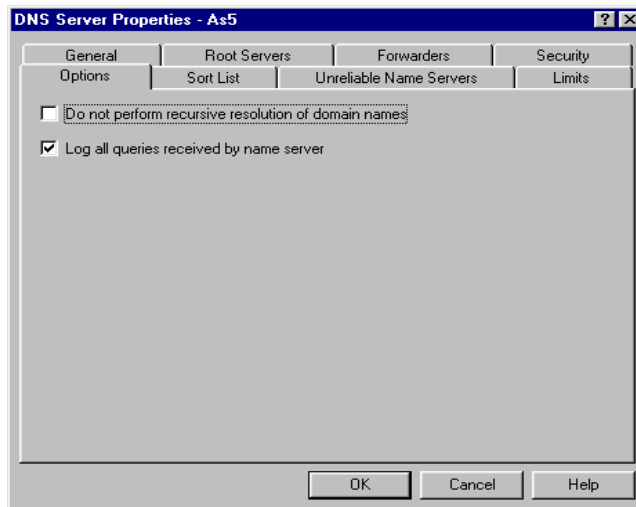


Figure 7. Configuring DNS Server Logging - QUERYLOG

- **STATISTICS:** Logs DNS server statistics. This summarizes the number of query hits the server received and the number of output packets it sent since the last time the server re-booted or reloaded its database. Delete this file when it becomes too large and you need to scroll down several times to find the information you are looking for. If you need to delete the file, you can find it through Operations Navigator. The file name is STATISTICS in the directory path FileSystems\Root\QIBM\UserData\OS400\DNS for your AS/400 system. Figure 8 shows how to display the DNS server statistics.

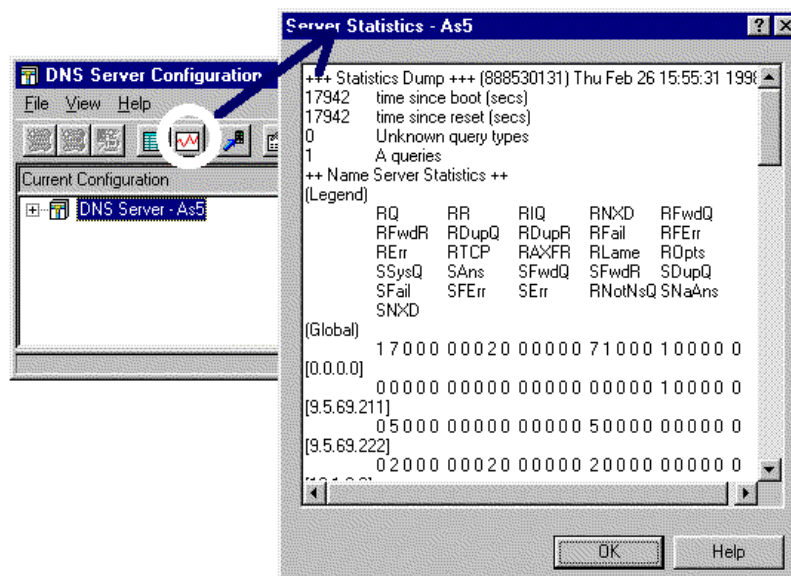


Figure 8. Displaying DNS Server Statistics

- **DUMPDB:** This file contains a dump of the DNS database for this server. You can use this database dump as a debugging tool to determine whether the DNS server is resolving IP addresses to host names correctly. You can match the contents of the database dump to the contents of a particular host's

property pages. The database dump includes the DNS server's authoritative data and cache data as well as information about its root servers. Figure 9 shows how to display the dump of the DNS server database. Monitor the size of this file to prevent it from growing too large.

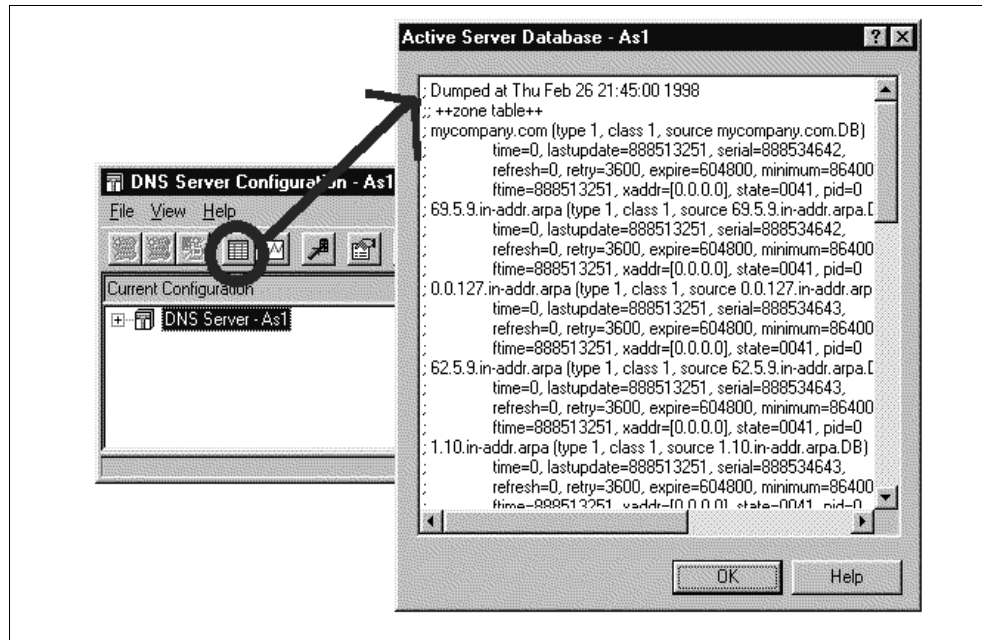


Figure 9. Displaying DNS Server Database

- **RUNDEBUG:** This file logs any debugging information. You can use Operations Navigator to find this file in FileSystems\Root\QIBM\UserData\OS400\DNS for your AS/400 system. You must re-boot the server to have your changes take effect. Figure 10 shows how to specify the debug level.

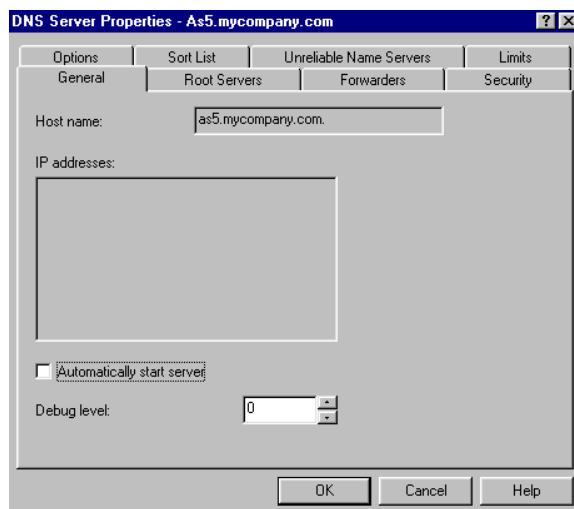


Figure 10. Specifying Debug Level

A Debug level of zero means that no debug information is logged. Debug level 1 through 11 means logging will occur. Level 3 or greater will result in a lot of data.

- **ATTRIBUTES:** This file contains the DNS server version, debug level, and autostart attribute.
- **PID:** This file contains a process ID and it is used for DNS to send signals for Dump Database, Dump Statistics, and Update Server.

The diagram illustrates the steps to set up a DNS server using the QTOB program. It shows the following components and steps:

- Step 1:** A screenshot of the QTOB program's main menu. The 'Start' option is highlighted, and the 'Configuration' option is also visible. Below the menu, the text 'or STRTCPSVR *DNS' is shown.
- Step 2:** An arrow points from the 'Start' option to a box labeled 'BOOT'. Another arrow points from 'BOOT' to a box labeled 'CACHE domain-name.DB (one or multiple) *.in-addr.arpa.DB (multiple)'.
- Step 3:** An arrow points from the 'CACHE' box to a box labeled 'secondarymycompany.com 10.5.69.222 mycompany.com.DB'. Below this, the text 'Zone Transfer JOB' is shown.
- Step 4:** An arrow points from the 'Zone Transfer JOB' box to a box labeled 'Primary DNS server(10.5.69.222)'. Below this, a table is shown with the following data:

Opt	Subsystem/Job	User	Type	CPU %	Function	Status
QSYSWRK	QSYS	SBS	.0			DEQW
QTSMINV	QTCP	BCH	.0		PGM-QVTCSCNC1	DEQW
QTOBNS	QTCP	BCH	.0		PGM-QTOBNS	SELW
QTOBXFER	QTCP	BCH	.5		PGM-QTOBXMIT	RUN
QTODDHCP	QTCP	BCH	.0		PGM-QTODDSVR	SELW
QTPOP00239	QTCP	BCH	.0			DEQW
QTPOP00254	QTCP	BCH	.0			DEQW
- Step 5:** An arrow points from the 'QTOBXFER' row of the table to a box labeled 'QUERYLOG', which is depicted as a notepad.

1. Start the DNS server.
2. The boot file provides start-up information: location of configuration files, server role (primary and/or secondary for specific domains), CACHE file with root name servers data, if acting as a secondary name server, the IP address of the primary master server to transfer zone data from, forwarders information, and so on.
3. The DNS and zone transfer jobs start.
4. The name server is ready to answer queries.
5. DNS queries are logged in the QUERYLOG file if logging is turned on.

The configuration of the AS/400 DNS server is through Operations Navigator. Operations Navigator provides the one and only configuration interface for the

DNS server. The Operations Navigator DNS Configuration Wizard provides a simple process for quickly getting an initial DNS server up and running.

To start the DNS server configuration from Operations Navigator, select your AS400 system name->Network->Server->OS/400; the window in Figure 12 is shown.

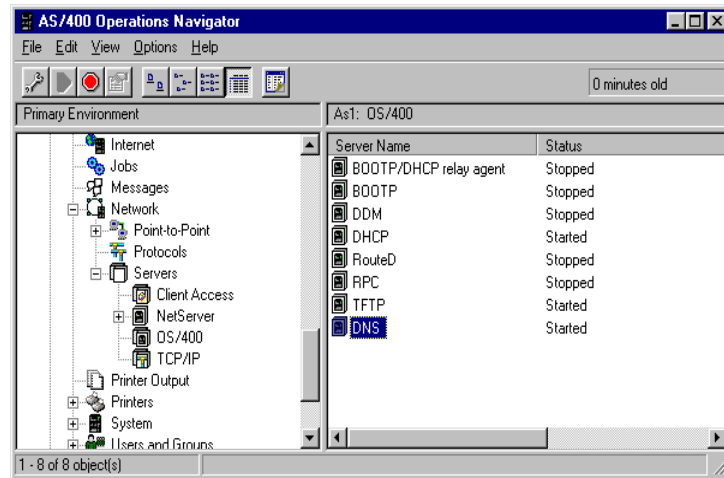


Figure 12. DNS Configuration Using Operations Navigator

To use Operations Navigator, you need to install Client Access/400 for Windows 95/NT V3R1M3 in your administrator's PC. Host servers must be started on your AS/400 system. Use the Start Host Server (STRHOSTSVR) command to start it.

2.5.2 Change DNS Attributes Command (CHGDNSA)

Use the Change DNS Attributes (CHGDNSA) command to set the AUTOSTART attribute, which determines whether or not the DNS server starts automatically when TCP/IP is started using the STRTCP command. This attribute is ignored by the STRTCPSVR command. STRTCPSVR *DNS will start the DNS server regardless of the value of the AUTOSTART attribute. This attribute can be set from the Operations Navigator interface also. The CHGDNSA command allows you to set the debug level that can also be specified through Operations Navigator.

2.5.3 Start TCP Server *DHCP

Use the STRTCPSVR SERVER(*DNS) command to start the DNS server and the ENDTCPSPVR SERVER(*DNS) command to stop it. You can also perform this function through Operations Navigator.

2.6 NSLOOKUP

The AS/400 name server lookup (nslookup) program queries domain name servers in interactive mode. It allows you to query name servers for information about various hosts and domains, or to display a list of hosts in the domain. The syntax of the nslookup program for the AS/400 name server is:

```
call pgm(qdns/qtooblkup)
```

Refer to the TCP/IP Configuration and Reference, SC41-5420-01, for more information on nslookup.

2.7 Host Table Migration Program

You can migrate AS/400 host name table entries to files that the Operations Navigator DNS configuration can maintain. The migration is a two-step process:

- First, the program QDNS/QTOBH2N must convert the AS/400 host table entries you specify to DNS formatted files.
- Second, you must convert each of the DNS formatted files created by the QDNS/QTOBH2N program to a format compatible with the Operations Navigator DNS configuration. The Operations Navigator Import Domain Data function does this conversion.

Refer to *TCP/IP Configuration and Reference*, SC41-5420-01, for more information and usage examples of the host table migration program.

2.8 DNS Server Backup and Recovery Considerations

Plan to back up the DNS server configuration files on a regular basis or every time the DNS administrator updates the DNS server configuration.

- Use the SAV command to back up the DNS configuration files in the /QIBM/UserData/OS400/DNS IFS directory. The files in this directory are customer created DNS configuration files. These files must be backed up frequently as part of your regular backup plan. These files include:
 - BOOT
 - Primary domain files, both forward and reverse mapping. Be sure to include the 0.0.127.in-addr.arpa.DB reverse mapping file created by the Wizard.
 - CACHE (list of root servers)

The files in /QIBM/UserData/OS400/DNS IFS subdirectory that should not be backed up and restored are DUMPDB, STATISTICS, RUNDBG, QUERYLOG, and any files in the TMP subdirectory. These files should be deleted when you no longer want them or they are too large. Backing up and restoring PID is probably of no use either unless the SAME server job is running before and after restore.

When the Operations Navigator DNS server configuration creates a file in the /QIBM/UserData/OS400/DNS directory, the file is created with the Owner value set to the AS/400 user profile that you used to start the Client Access/400 connection. When this user profile is deleted with the parameter *Owned object value* *DLT, objects owned by the user profile are deleted also. In this case, any IFS DNS configuration files owned by this user profile are also deleted.

Tip

To prevent accidentally deleting DNS server files, change the ownership of the files to a system type user profile such as QTCP.

Chapter 3. Implementing Primary and Secondary DNS Servers

This chapter shows you how to get started implementing a DNS server on your AS/400 system. We take you step-by-step from your existing name resolution process based on the AS/400 host table to a full implementation of a primary name server and a secondary DNS server.

Many companies have a simple internal network consisting of one or two subnets and use AS/400 host tables and PC client host tables to resolve TCP/IP host names to IP addresses. The disadvantage of this name resolution method is that every addition of a host may require an update to every client that needs to contact this new host. Configuring one AS/400 system to be a primary DNS server and a second AS/400 system to be a secondary (backup) name server alleviates this problem because adding or deleting a host and its IP address is done only once on the primary name server. The secondary name server automatically transfers the DNS files from the primary DNS server at pre-configured time intervals.

This chapter concentrates on three sections:

- How to configure the first DNS server (called the primary name server) in a small internal network by migrating the AS/400 host table.
- What configuration changes need to be made to allow mail to be delivered to the one AS/400 mail server in the network.
- How to configure a second DNS server (called a secondary name server) to act as a backup to the primary name server. The secondary name server can back up the primary server and balance the query workload.

3.1 Scenario Overview

In this chapter, we use an example network of three subnets connected by routers as shown in Figure 13 on page 26. This network is not connected to the Internet and, consequently, does not have a firewall installed anywhere in the network. The network initially does not include a DNS server and relies on host tables to resolve host names to IP addresses.

In this scenario, we configure a primary DNS server for the domain *mycompany.com*, a secondary DNS server to back up the primary domain server, and we go through the steps to configure the AS/400 mail server so POP3 mail can successfully be delivered to the mail server.

Also in this scenario, we choose not to include the domain *remote.com* in the DNS configuration on AS1. Thus, the DNS on AS1 only includes information about the *mycompany.com* domain shown in Figure 13 on page 26.

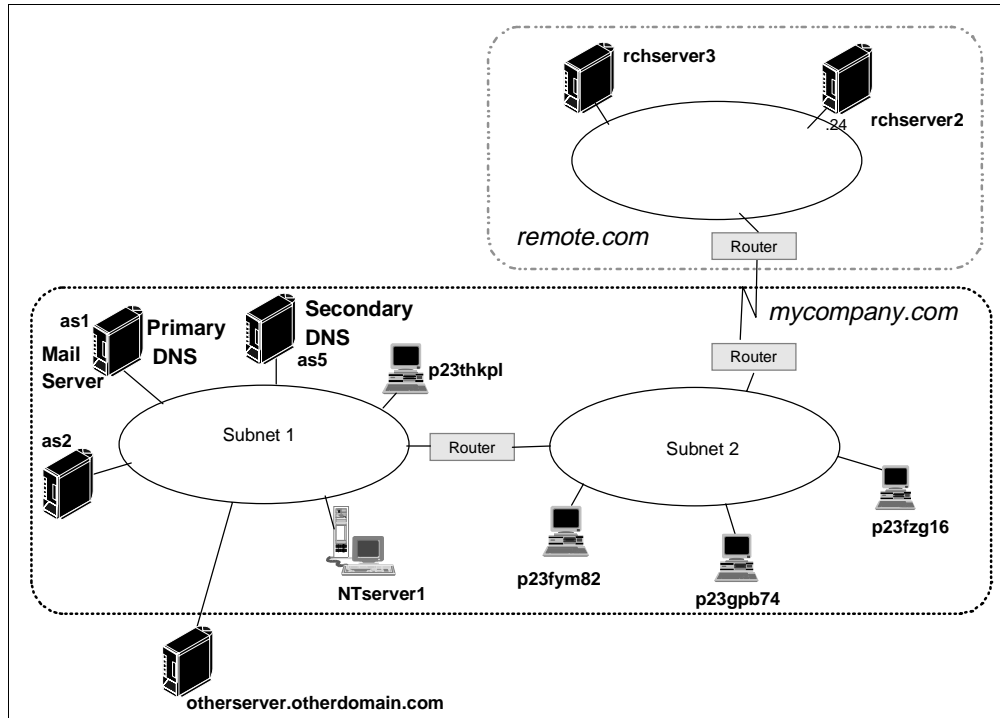


Figure 13. Scenario Network with One Primary Name Server and One Secondary Name Server

3.1.1 Scenario Objectives

In this scenario, we have the following objectives:

1. Plan the primary domain.
2. Configure a primary DNS server on AS1. We migrate the AS1's host table to create the initial DNS configuration on AS1.
3. Configure a mail server on AS1. This mail server serves as both an SMTP outgoing mail server and an incoming POP3 mail server for POP3 clients in the *mycompany.com* domain.
4. Configure a secondary DNS on the AS/400 host table. This name server is used as a backup name server to the AS1 name server and to balance the query workload.
5. Review security options available on the primary name server.
6. Touch briefly on the reconfiguration of clients to use a DNS server instead of their own host table.

3.1.2 Scenario Advantages

The advantages of this scenario are that:

- It assumes the customer is coming from an environment that does not have a name server in the internal network. Thus, this scenario makes a good starting place for customers with little or no experience with name servers.
- It discusses how an AS/400 host table can be migrated into the DNS server configuration, which can make the initial name server configuration go faster and smoother.
- It outlines how to create a secondary name server to back up the primary name server. This prevents the primary name server from becoming a single point of failure in the area of name serving.

- Included in this chapter are steps for configuring the AS/400 system as a POP3 mail server now that a DNS server is in the network.
- It addresses some security issues by explaining how to configure the primary name server to control which secondary name servers can zone transfer from it and which clients (based on IP address or IP network) can be blocked from accessing the data residing on it.

3.1.3 Scenario Disadvantages

- This scenario describes how to configure a primary and secondary name server in a small internal network that does not have access to the Internet and does not have a Firewall installed in the network. This type of network and name server configuration do not meet the needs of network installations that require Internet access and a Firewall.
- This scenario describes how to configure DNS servers for one domain: *mycompany.com*. Thus, all hosts included in this name server configuration must have the domain name of *mycompany.com*.
- This scenario does not describe how to handle subdomains in the *mycompany.com* domain. Subdomains are covered in a subsequent chapter.

3.1.4 Scenario Network Configuration

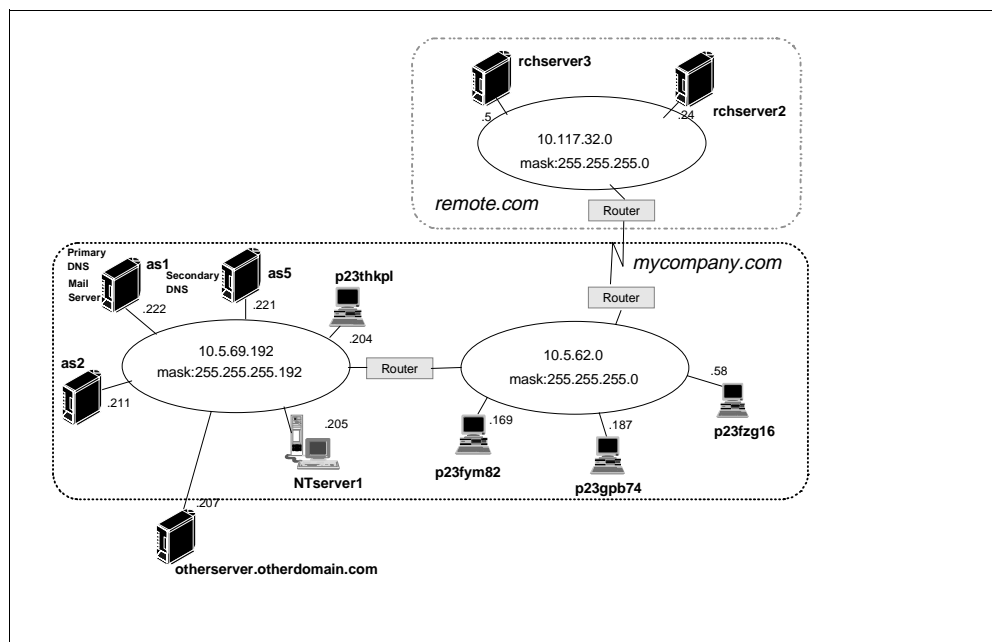


Figure 14. Scenario Network Diagram

The network shown in Figure 14 consists of three subnets connected by routers. The network *mycompany.com* is an internal network and it is not connected to the Internet. The three subnets' network IDs and subnet masks are as follows:

- 10.5.69.192 subnet mask 255.255.255.192
- 10.5.62.0 subnet mask 255.255.255.0
- 10.117.32.0 subnet mask 255.255.255.0

The primary DNS will run on AS1. An AS/400 system's DNS server can be configured for more than one primary domain and more than one secondary

domain; however, in this scenario, the AS1 name server is configured to be primary for the one domain, *mycompany.com*. Because the *mycompany.com* domain includes the subnets 10.5.69.192 and the 10.5.62.0, AS1 is also configured with the primary domain files 69.5.10.in-addr.arpa and 62.5.10.in-addr.arpa. This chapter contains step-by-step instructions for configuring the AS1 primary name server.

One mail server is configured for handling mail in the *mycompany.com* domain. This mail server also resides on AS1. However, it is not a requirement that the mail server be on the same AS/400 system as the DNS server.

Lastly, the AS5 AS/400 system is configured to be a secondary DNS server for the domain *mycompany.com*. This means that the name server on AS5 will act as a backup to the name server on AS1. It contains the same information as the name server on AS1 but the information is in the form of secondary domain files rather than primary domain files. Secondary domain files contain information that was obtained through a zone transfer (an automatic transfer of information using TCP protocol) from the primary name server.

3.2 Task Summary

The tasks required to complete this scenario do not include the initial TCP configuration on the AS/400 system such as creating a line description, creating an IP interface, creating a TCPIP route, starting TCP/IP, and so on. This scenario assumes that the TCP configuration on both AS/400 systems in the network and all other hosts in the network is completed and TCP/IP connectivity has been verified.

The summary of tasks for this scenario are as follows:

1. Plan the primary domain *mycompany.com*.
2. Create the DNS primary name server on As1 using the following substeps:
 - Prepare the local host table for migration on AS1.
 - Migrate the AS1 host table to DNS formatted files. An AS/400 program is used to do this.
 - Use Operations Navigator Import domain data to migrate the DNS formatted files to files that can be maintained by the Operations Navigator DNS configuration.
 - Use Operations Navigator DNS server configuration to make final and ongoing configuration changes, if necessary.
3. Configure AS1 as a mail server. This task is divided into the following substeps:
 - Configure POP3 users.
 - Configure POP3 clients.
 - Configure the domain's mail server in the primary DNS.
 - Verify the TCP/IP and SMTP configurations.
 - Start the mail jobs in the mail server.
4. Start the DNS server on AS1.
5. Verify that the DNS is operational.
6. Create the DNS secondary name server on AS5.
7. Review security options on the primary name server AS1
8. Reconfigure clients to use a DNS server instead of host tables.

3.2.1 Planning the Primary Domain

The first step in moving from host tables to a name server is to determine what domain will become the primary domain. In this scenario, *mycompany.com* is the primary domain on the AS1 name server. Figure 14 on page 27 indicates, by a dotted line box, which hosts are to be included in the domain *mycompany.com*. All the hosts but one on the 10.5.69.192 network are included in this domain. The host *OTHERSERVER*, although it is on the 10.69.192 network, is in the domain *OTHERDOMAIN.com*; thus, it is not part of the *mycompany.com* domain. All the hosts on the 10.5.62.0 network are included in this domain, but no host on the 10.117.32 network is included in the *mycompany.com* domain because the hosts on this network are part of *remote.com* domain. In other words, the hosts located in the *remote.com* domain are excluded in the migration. Consequently, the AS1 name server is unaware of the *remote.com* and its hosts. It is assumed that *remote.com* will continue to use host tables as the method of resolving names to IP addresses.

Thus, in this chapter, the 10.117.32.0 network is not included in the migration but both networks 10.5.59.192 and 10.5.62.0 are included. The specific host *OTHERSERVER* is excluded from the migration because it belongs in another domain of *OTHERDOMAIN.com* even though it is part of the 10.5.69.192 network as indicated in Figure 15 on page 31.

During the planning phase, it is important to verify that the clients that you, as the administrator, have decided belong in *mycompany.com* are configured with a domain name of *mycompany.com*. For example, assume that two NetWare servers are located in the 10.5.62.0 network and are configured with host and domain names of *nw1.payroll* and *nw2.payroll*. You decide to include them in the DNS configuration on AS1 so their domain names must be changed from *payroll* to *mycompany.com*. In other words, in this scenario, every host that is included in AS1's name server configuration must have a domain name of *mycompany.com*.

Chapter 5, "Growing Your Domain: Creating Subdomains" on page 83 discusses the situation where a subdomain is used in a network and needs to be included in the *mycompany.com* domain. However, the scenario in this chapter assumes all hosts included in the AS1 name server have the domain name of *mycompany.com* without any subdomain names used.

3.2.2 Creating the Primary Name Server on As1

We divided the task of creating a primary name server into several subtasks. The following sections discuss each of the steps that we follow to configure AS1 as a primary name server.

3.2.2.1 Preparing the Host Table for Migration

Although this chapter uses a migration of an AS/400 host table as a method to configure the first name server, it is not a requirement that this method be used. It is possible to use Operations Navigator to configure DNS from the beginning. However, since AS1's host table contains the host names and IP addresses of the hosts to be included in the *mycompany.com* domain, the host table migration method saves time, typing, and, consequently, it helps to avoid the possibility of introducing typing errors into the DNS configuration.

Since AS1's host table is used as a starting point for the migration, it is important to "clean up" this host table:

1. Delete any hosts from the table that no longer exist in the network.
2. Make sure all hosts in the *mycompany.com* domain are listed in AS1's Host table.
3. Check for incorrect IP addresses and typing mistakes in the AS1 host table names.
4. Verify that the hosts listed in the client's host tables are included in the AS1's host table.
5. Check for all host names in the host table with domain names other than *mycompany.com*. Do these hosts belong in another domain as listed or should they be included in the *mycompany.com* domain? If they do belong in the *mycompany.com* domain, now is the time to change the domain name on the host itself to *mycompany.com* and update AS1's Host table to reflect the change. However, when changing the domain name of a host, be aware of the impact the change can have on the clients that possibly use this host as a server. If the host you are changing the domain name of is a mail server, the domain name change can have a wide-spread effect.

You must also plan for the hosts that are not included in the migration. Note Figure 14 on page 27 specifies three hosts in the network that are not included in *mycompany.com* domain. The "future" DNS server on AS1 with one primary domain of *mycompany.com* will not resolve queries for host *OTHERSERVER*, nor will it resolve queries for *Rchserver2* and *Rchserver3*. If the AS1 system is the only host that needs to access these systems, leaving their host names/IP addresses in the AS1 host table may be sufficient since an AS/400 system can be configured to check its local host table first, and if the answer is not in the table, then query the DNS server. But if other clients need access to *OTHERSERVER*, *Rchserver2*, or *Rchserver3*, you need to decide how the clients will resolve those hosts names.

For example, consider host *OTHERSERVER* in the domain *OTHERDOMAIN.com*. It is a good idea to review the AS1's host table at this time and determine if this host really needs to belong in a domain of *OTHERDOMAIN.com* or if it can belong in the *mycompany.com* domain. If it can be included in the *mycompany.com* domain, now is a good time to change its domain name and change AS1's host table to also reflect this change so *OTHERSERVER* can be included in the migration. For purposes of illustrating the example of excluding a host from the migration, consider *OTHERSERVER* as part of *OTHERDOMAIN.com* and the migration will exclude this host.

Consider the situation with hosts *Rchserver2* and *Rchserver3*. The AS1 host table shown in Figure 15 on page 31 indicates these two hosts are part of the *remote.com* domain. If the DNS server running on AS1 really needs to resolve DNS queries for these hosts, then a second primary domain of *remote.com* on AS1 DNS server can be created and configured with Operations Navigator. In this case, AS1 has a DNS server running on it and is responsible for two primary domains: *mycompany.com* and *remote.com*. This scenario only concentrates on creating the primary domain of *mycompany.com* on AS1 and the secondary domain on AS5 for the same domain, *mycompany.com*. Thus in this scenario, the *remote.com* domain is excluded. But be aware that it is possible to create additional primary domains and secondary domains if the domain naming scheme and the network require it.

Work with TCP/IP Host Table Entries			System:	AS1
Type options, press Enter.				
1=Add 2=Change 4=Remove 5=Display 7=Rename				
	Internet	Host		
Opt	Address	Name		
	10.5.62.58	p23fzg16		
		p23fzg16.mycompany.com		
	10.5.62.169	p23fym82		
		p23fym82.mycompany.com		
	10.5.62.187	p23gpb74		
		p23gpb74.mycompany.com		
	10.5.69.204	p23thkp1		
		p23thkp1.mycompany.com		
	10.5.69.205	NTserver1		
		NTserver1.mycompany.com		
	10.5.69.207	otherserver		
		otherserver.otherdomain.com		
	10.5.69.211	as2		
		as2.mycompany.com		
	10.5.69.221	as5		
		as5.mycompany.com		
	10.5.69.222	as1		
		as1.mycompany.com		
	10.117.32.5	Rchserver3		
		Rchserver3.Remote.com		
	10.117.33.24	Rchserver2		
		Rchserver2.Remote.com		
	127.0.0.1	LOOPBACK		
		LOCALHOST		

Figure 15. AS1 Host Table

3.2.2.2 Migrating the AS/400 Host Table to DNS Formatted Files

The AS/400 program used to migrate the AS/400 host table to DNS formatted files is called QTOBH2N. There are several options that can be used with this program. A complete list of options is described in the DNS chapter of the TCP/IP Configuration and Reference, SC41-5420-01. In this scenario, we cover only the options used to migrate the AS1 host table in Figure 15.

This migration step is one of the few DNS configuration steps that is executed from an AS/400 "green screen". The following steps migrate the AS1 host table to DNS formatted files:

- Make sure the AS1 host table is cleaned up and accurate.
- Add library QDNS to the user's library list with the AS/400 command
addlibl lib(QDNS).
- Grant the user profile that will run the program QDNS/QTOBH2N *ALLOBJ special authority.
- Change the job Coded Character Set ID (CCSID) for the user job that will run the program QDNS/QTOBH2N to 37. Be sure to record the original job coded character set ID so that you can change it back. Change the CCSID just before you run the program QDNS/QTOBH2N. Change the CCSID back immediately after you run this program.

Note

Note that changing the CCSID back may not be a simple task because of the interaction of DFTCCSID and CCSID when the CCSID is set to 65535. It may be better to run the host table migration program from a batch job. Attempting to change back the CCSID may leave the keyboard in an unusable state in some countries (for example, Japan).

- To change the user job's CCSID:
 1. Enter the AS/400 `CHGJOB` command.
 2. Press **F4** to prompt.
 3. Press **F10** to select additional parameters.
 4. **Page Down** twice to the parameter Coded Character Set ID.
 5. Record the current value for Coded Character Set ID.
 6. Change the coded character set ID to **37**.
 7. Press **Enter**.

The program QTOBH2N will migrate the AS/400 host table to DNS formatted files. On the AS1 AS/400 system, issue the command:

```
call pgm(qdns/qtohb2n) parm( '-d' 'mycompany.com' '-n'
'10.5.62:255.255.255.0' '-n' '10.5.69:255.255.255.0' '-e' 'otherdomain.com'
'-M' )
```

For this chapter's example, the preceding program creates three files: `h2n.mycompany`, `h2n.10.5.62`, and `h2n.10.5.69`.

After the command completes, the job log contains message DNS0417:

```
Process completed successfully, file h2n.mycompany built in directory
```

Although the message does not refer to the `h2n.10.5.62` and the `h2n.10.5.69` files, it implies that these two files were also successfully created.

Tip: At this point, it is important to remember to change the CCSID on the user's job back to what it was before it was changed to 37. Set the DFTCCSID first and then the CCSID. Both should be set to the same value.

The options used to run the QTOBH2N program specified the particulars of how the host table should be migrated. An explanation of the options used is as follows:

1. The `'-d' 'mycompany.com'` option indicates the domain that the name server is primary for is *mycompany.com*.
2. The `'-n' '10.5.62:255.255.255.0'` and `'-n' '10.5.69:255.255.255.0'` indicates that hosts listed in the AS/400 system's host table with IP addresses included in the networks 10.5.62 and the 10.5.69 are included in the migration.
3. Any hosts in the preceding two networks that are in the domain *OTHERDOMAIN.com* are not included in the migration.
4. The migration does not create any MX records because the `-M` option was used. If the `'-M'` option is not used, an MX record is created for EVERY host included in the migration. In this scenario, an MX record for every host is not necessary. There is only one mail server (AS1 host) in this scenario and one domain (*mycompany.com*). We need only one MX record and it is added later using Operations Navigator.

Note 1: The `-e` option needs further explaining. Remember, every host that is included in the migration is included in the *mycompany.com* domain. If the

`OTHERSERVER` host is not excluded with the `-e` option, then `OTHERSERVER` is migrated with a domain of `OTHERDOMAIN.com.mycompany.com`. Even if `OTHERDOMAIN` is a subdomain of `mycompany.com`, the absolute domain name of `OTHERDOMAIN.com.mycompany.com` is not correct. Making `OTHERDOMAIN` a subdomain of `mycompany.com` is discussed in Chapter 5.

Note 2: `Rchserver2` and `Rchserver3` are not included in the migration by default and it is not necessary to eliminate them explicitly with the `'-e'` option. This is because only the hosts residing in the networks specified with the `'-n'` options are included in the migration. Because `Rchserver2` and `Rchserver3` reside on the `10.117.32.0` network, they are not included in the migration.

Note 3: Hosts `AS1`, `NTserver1`, `AS2`, `AS5`, `p23thkp1`, and `OTHERSERVER` have subnet masks of `255.255.255.192`. These hosts are in the `10.5.69.192` network. The migration program does not handle subnetting into the fourth octet. Thus, if `AS1`'s host table did include hosts in the `10.5.69.0` (the `10.5.69.64` or the `10.5.69.128` networks), the migration program includes these hosts whether we want to include them in the migration or not.

In this scenario, the migration program creates three files in the `/QIBM/UserData/OS400/DNS` directory:

```
h2n.mycompany
h2n.10.5.62
h2n.10.5.69
```

At this point, you may want to verify that these files are in the `/QIBM/UserData/OS400/DNS` directory. You may use the `AS/400` command:

```
wrklnk '/QIBM/UserData/OS400/DNS'
```

Then use option 5 to view the next level of the DNS directory:

Work with Object Links

Directory : /QIBM/UserData/OS400/DNS
Type options, press Enter.
3=Copy 4=Remove 5=Next level 7=Rename 8=Display attributes
11=Change current directory ...

Opt	Object link	Type	Attribute	Text
	h2n.mycompany	SIMF		
	h2n.10.5.62	SIMF		
	h2n.10.5.69	SIMF		
	ATTRIBUTES	SIMF		
	TMP	DIR		

The three `h2n` files were created by the `QTOBH2N` program. The `ATTRIBUTES` file and the `TMP` directory existed before the `QTOBH2N` program was run. They were automatically created when you installed the `OS/400` Domain Name System option 31.

To view the contents of `h2n.mycompany`, you can use Operations Navigator:

- Click + next to as1.mycompany.com.
- Click + next to File System.
- Click + next to root.
- Click + next to QIBM.
- Click + next to UserData.
- Click + next to OS400.
- Click + next to DNS.

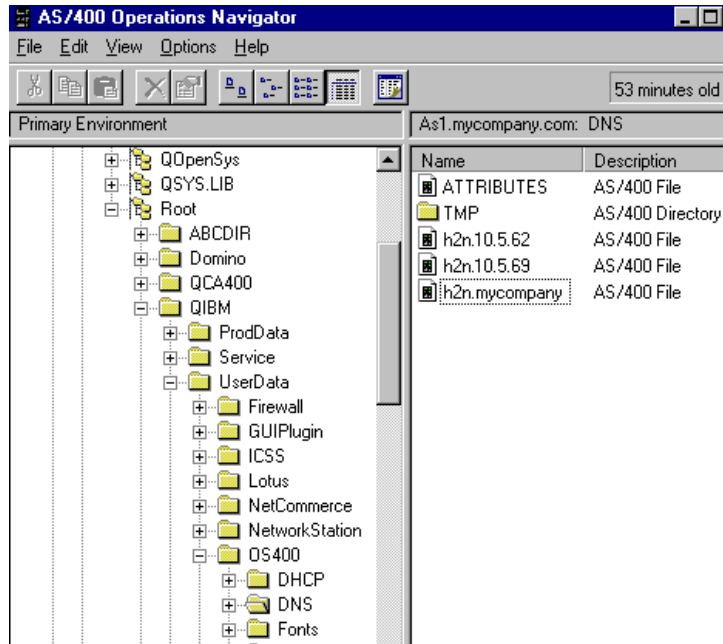


Figure 16. Viewing the Contents of the DNS Directory with Operations Navigator

Note that Figure 16 shows similar information as the WRKLNK command. However, double-clicking on *h2n.mycompany.com* brings up an *Open with* window that allows you to choose your favorite program to view the content of the DNS files. We chose Netscape to browse the *h2n.mycompany* file shown in Figure 17.

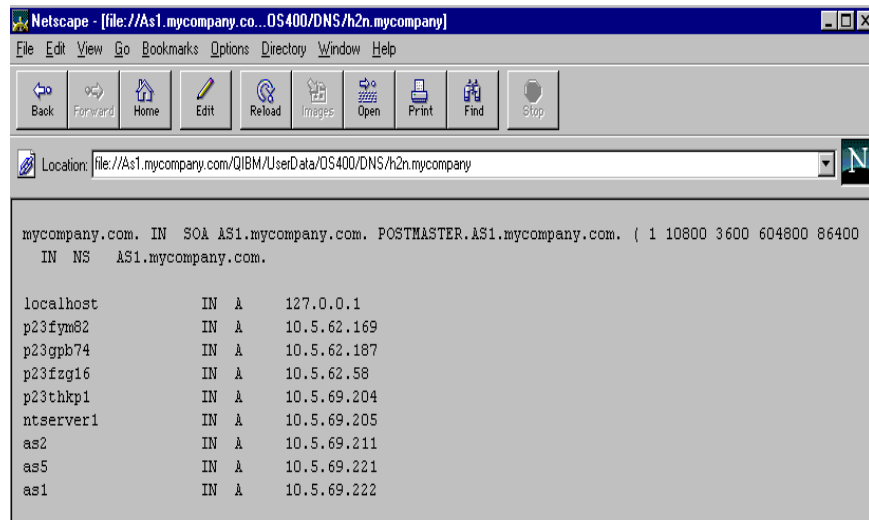


Figure 17. Viewing theContents of h2n.mycompany File with Netscape

Figure 18 and Figure 19 show the contents of h2n.10.5.69 and h2n.10.5.62 browsed with Netscape.

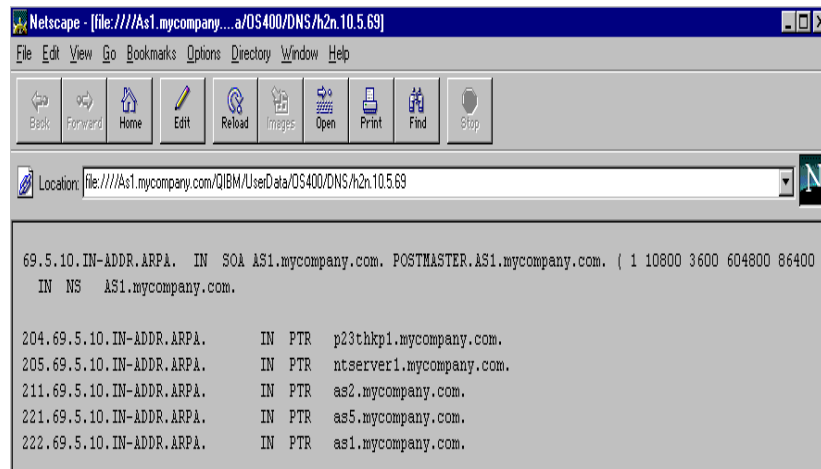


Figure 18. Viewing the h2n.10.5.69 File with Netscape.

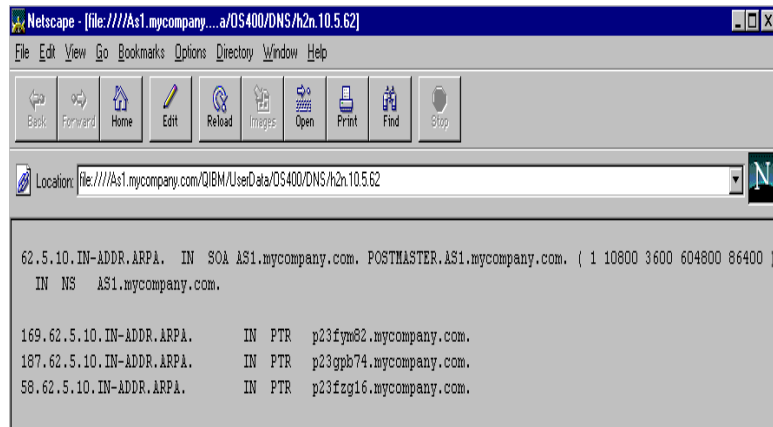


Figure 19. Viewing h2n.10.5.62 with Netscape

3.2.2.3 Importing DNS Formatted Files to Operations Navigator

Once the AS/400 host table has been migrated to DNS formatted files using the QTOBH2N program, it is time to migrate the DNS formatted files to Operations Navigator DNS files. The Operations Navigator DNS Configuration Import Domain Function accomplishes this step.

From a Client Access Windows 95 client, bring up Operations Navigator and follow these instructions:

- Click + next to **As1.mycompany.com**.
- Click + next to **Network**.
- Click + next to **Servers**.
- Click + next to **OS400**.

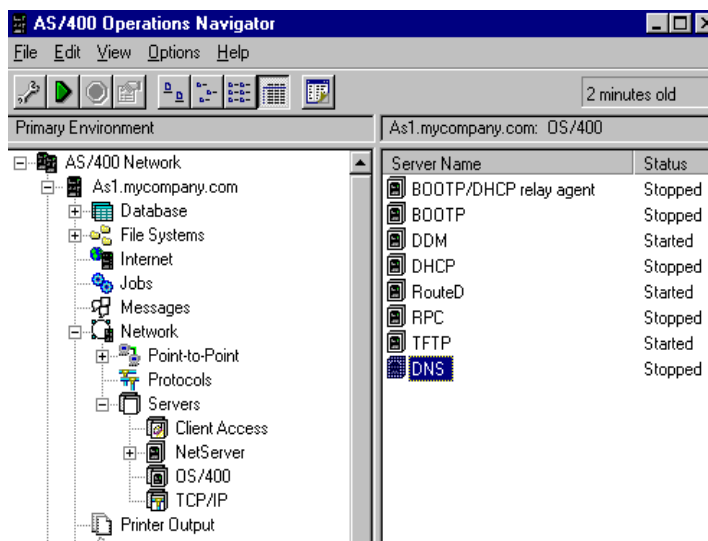


Figure 20. Contents of OS/400 Servers

Double-clicking **DNS** brings up the DNS server configuration wizard. The wizard automatically starts when you enter the DNS configuration for the first time.

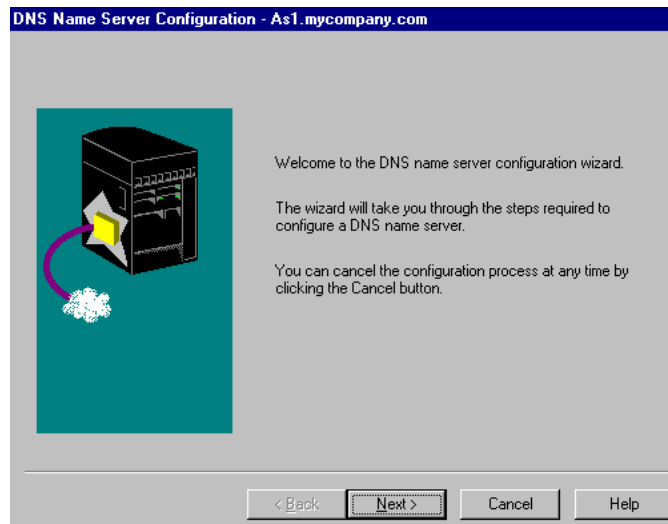


Figure 21. Welcome Window to the DNS Configuration Wizard

Click **Next**.

The next wizard window allows you to Add IP addresses for Root Servers. This chapter's scenario does not make use of Root Servers.

Click **Next** to bypass the Root Server window.

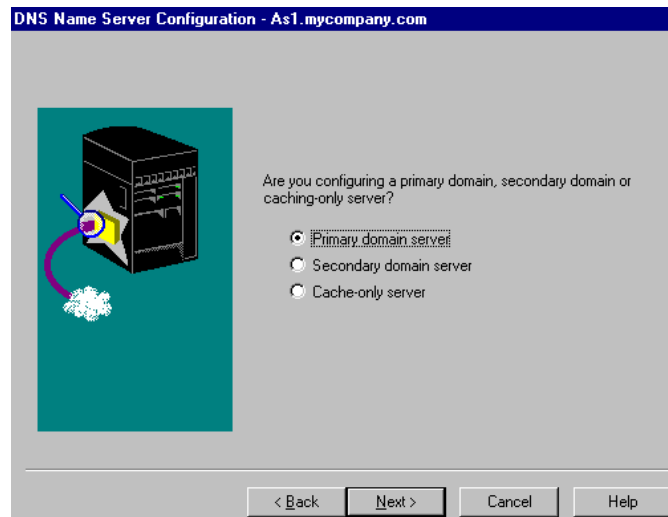


Figure 22. Choosing the Domain Type in the DNS Server Configuration Wizard

AS1 is the primary domain server for the domain *mycompany.com*. Thus, take the default of primary domain server shown in Figure 22 and click **Next**.

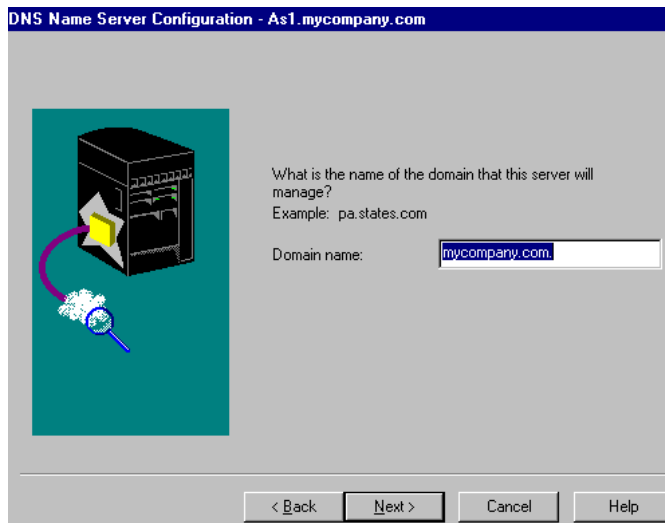


Figure 23. DNS Server Configuration Wizard Default Domain Name

Enter the primary domain name, `mycompany.com` (see Figure 23). Click **Next**.

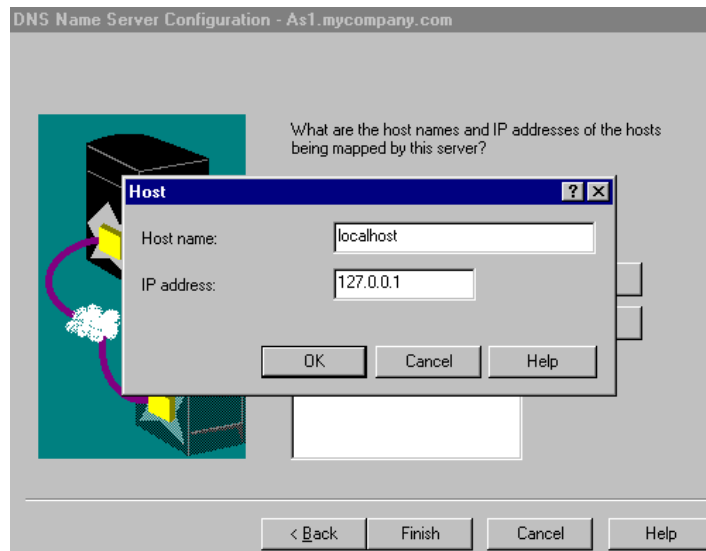


Figure 24. Enter the Host Name and IP Address for Loopback

The next window presented by the wizard allows you to add IP addresses and host names. We need to add only one special host called *localhost*, which exists for the loopback address of 127.0.0.1. See Figure 24.

Click **Add**.

Enter **localhost** for the Host name.

Enter **127.0.0.1** for the IP address.

Click **OK**.

The remaining IP addresses and host names are imported from the h2n files.

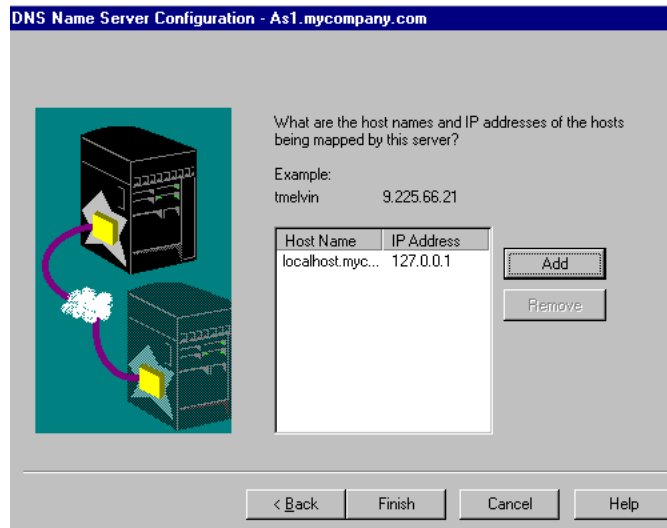


Figure 25. DNS Wizard Host Name/IP Address List

Click **Finish** to exit the wizard. See Figure 25.

At this point, Operations Navigator displays the DNS server *as1.mycompany.com*. Double-click on the **Primary Domain** to view the files that the wizard created. See Figure 26.

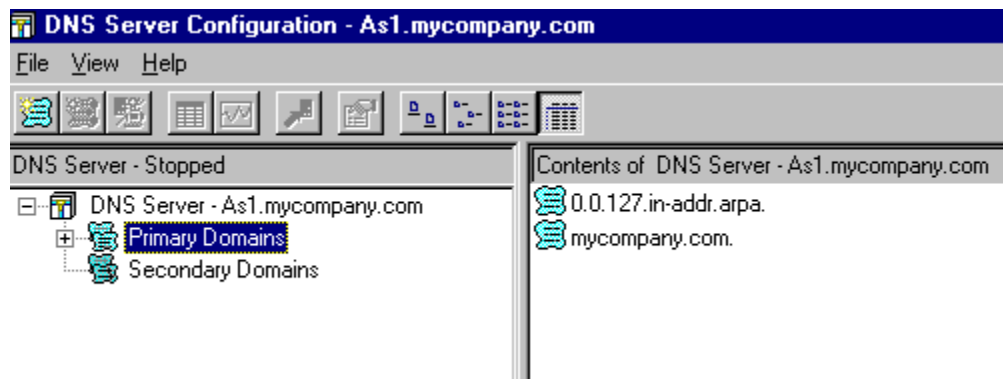


Figure 26. Contents of DNS Server on the As1 System after Wizard Completes

The *Import Domain* function that we are running next attempts to create a *mycompany.com* file. Thus at this point, you need to delete the existing *mycompany.com* file that the wizard automatically created:

1. Right click on *mycompany.com*.
2. Click **Delete**.
3. Click **Yes** to confirm.

Do *not* delete the 0.0.127.in-addr.arpa file.

To save your configuration and write the files to the IFS directory, you need to close the DNS window at this time.

From the list of OS400 servers, double-click **DNS**. This time, you are not taken into the DNS configuration wizard; the DNS configuration graphical interface is displayed.

Right click on the **Primary Domains** to get a pop-up window. See Figure 27.

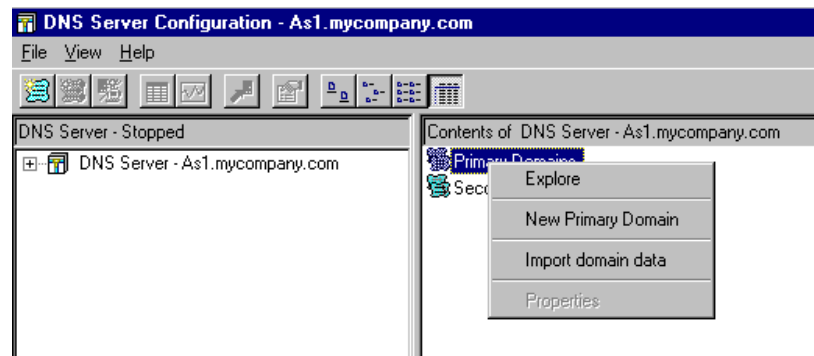


Figure 27. Right click on Primary Domain

Select **Import domain data**.

A window is shown containing a default path of /QIBM/UserData/OS400/DNS. Add the file you want to import to the path. In this case, the first file to be imported is h2n.mycompany. See Figure 28. Click **OK**.

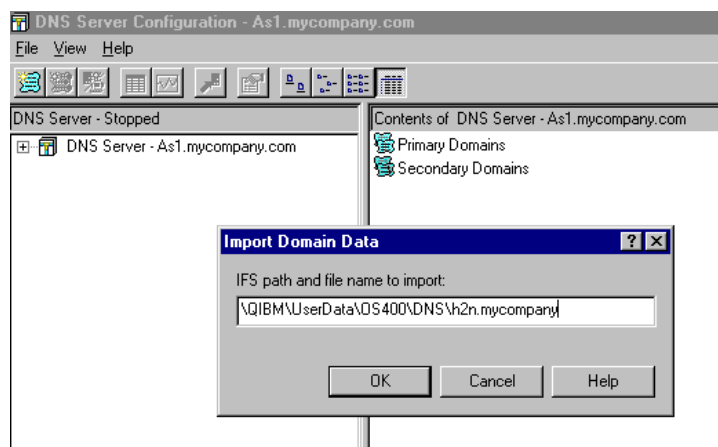


Figure 28. Importing h2n.mycompany.com Using the Import Domain Data Function

A new file, *mycompany.com*, is created under Primary Domains.

Repeat *Import Domain Data* for every h2n file that the QTOBH2N program created. Thus, repeat the Import Domain Data steps two more times for the remaining two h2n migration files: h2n.10.5.62 and h2n.10.5.69.

In summary, for this chapter's scenario, we ran the *Import Domain Data* function three times.

Double-click **Primary Domains** in the Operations Navigator DNS server configuration. At this time, four files are shown in Figure 29.

Note: If the h2n file does not exist but is entered in the Import Domain Data field, no error message is sent to the user.

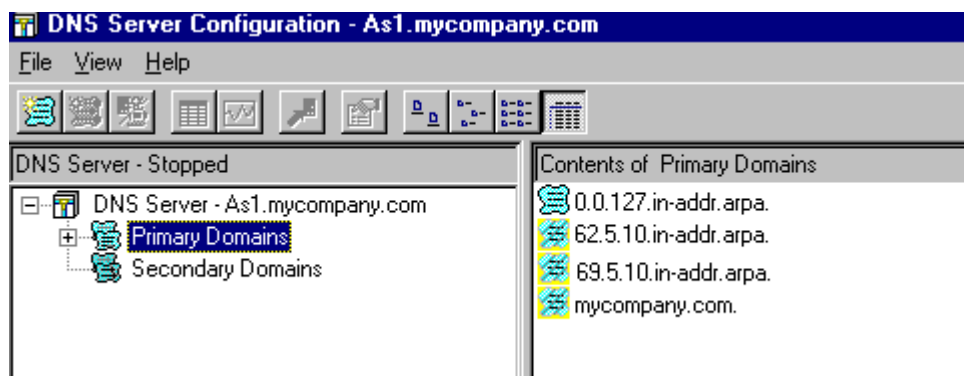


Figure 29. Results of Running Import Domain Function Against All H2n Migration Files

The four files contained in AS1's primary domain are the files the DNS server requires to answer queries for the *mycompany.com* domain with the exception of a query for a mail server. An MX record is added later in this chapter to satisfy that requirement.

Note that the three files, 62.5.10.in-addr.arpa, 69.5.10.in-addr.arpa, and mycompany.com shown in Figure 29, have an icon to the left of the file names that appears to be "hashed". This indicates that the domain is currently Disabled.

The DNS server will *not* load a disabled domain. A disabled domain is like a "sand-box"; a domain can be created without making it live. To enable each domain, right click on each file name and select **Enable**.

Close the Operations Navigator DNS server configuration window to save the DNS configuration.

The migration of the AS/400 host table is completed. However, there are a few more DNS configuration changes that are best accomplished with the Operations Navigator DNS server configuration. We discuss these changes in the next section.

3.2.2.4 Additional DNS Configuration with Operations Navigator

Once the migration of the host table is complete, any additional configuration changes can be made using the Operations Navigator DNS server configuration.

Automatically Create/Delete Reverse Mapping Entries

At this point, change the configuration to automatically create/delete a reverse mapping entry for every forward mapping entry that is added.

Note: A forward mapping entry is also called an A or address record, which is contained in the forward mapping primary domain file. This entry is created by adding a new host to the *mycompany.com* primary domain file. Forward mapping is a host name to IP address mapping.

The reason we make this configuration change can best be explained by an example:

If a new host named *newhost* is added to the 10.5.69.192 network with an IP address of 10.5.69.206, the DNS administrator must add a host to the *mycompany.com* forward mapping primary domain file. This entry allows the DNS server to answer a query for a client who sends the IP address to the DNS server and requests that the DNS server give it the host name for the IP address. If the DNS administrator forgets to add the same new host to the 69.5.10.in-addr.arpa domain, the DNS server cannot answer a query from a client that sends the IP address of 10.5.69.206 and requests its host name. This type of query is sometimes called a "reverse look up". Consequently, another name for the 69.5.10.in-addr.arpa file is reverse mapping file for the 10.5.69 network.

By configuring the DNS server to automatically create and delete the reverse mapping files, a DNS administrator only has to enter the new host into the forward mapping file: *mycompany.com*. The matching entry is automatically added in the appropriate reverse mapping file by Operations Navigator.

There are few situations where a DNS administrator wants a host entered into the forward mapping file but *not* entered into the reverse mapping file. Thus, we recommend this configuration change; it can save time and help prevent mistakes when manually adding new hosts to the primary domain.

To make this configuration change, do the following steps:

1. Right click on the file **mycompany.com**.
2. Select **Properties**.
3. Check *Create and delete reverse mappings by default*. See Figure 30.
4. Click **OK**.
5. Close the Operations Navigator DNS server configuration to save the configuration changes.

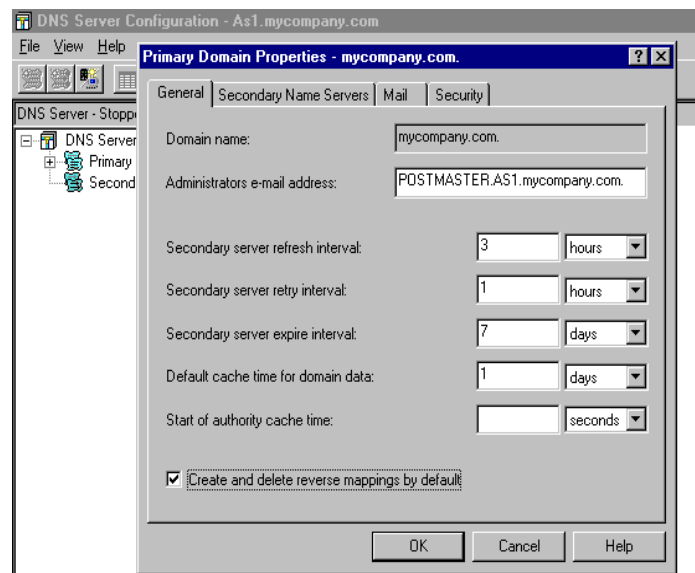


Figure 30. Enable Create and Delete Reverse Mapping by Default for Domain mycompany.com

Reviewing the Primary Domain Files on As1 Name Server

Let's review the contents of each primary domain file on AS1:

1. Double-click **DNS**.
2. Double-click **DNS Server- as1.mycompany.com**.

3. Double-click **Primary Domains**.
4. Double-click the forward mapping file **mycompany.com**.

Figure 31 shows the contents of *mycompany.com* forward mapping primary domain file.

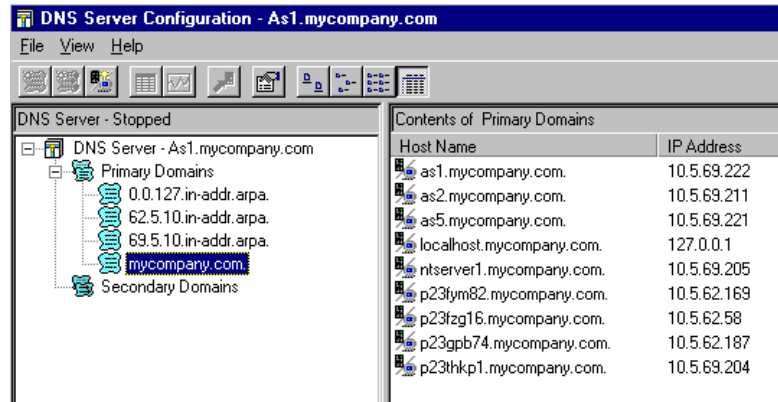


Figure 31. Contents of Mycompany.com Primary Domain File

5. Double-click the **62.5.10.in-addr.arpa** primary domain file to view the contents of the reverse mapping primary domain file for the 10.5.62 network shown in Figure 32.

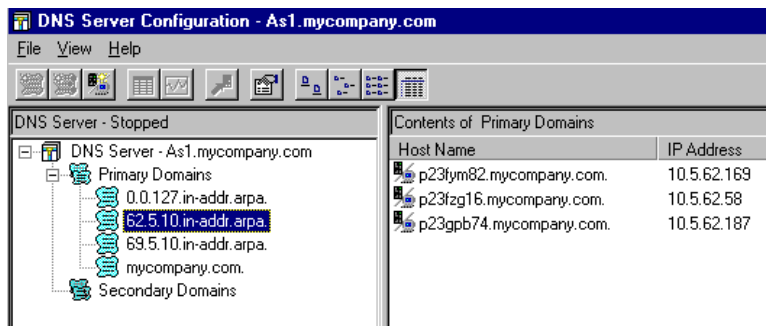


Figure 32. Contents of the 62.5.10.in-addr.arpa Primary Domain

6. Double-click the **69.5.10.in-addr.arpa** primary domain file to view the contents of the reverse mapping primary domain file for the 10.5.69 network shown in Figure 33.

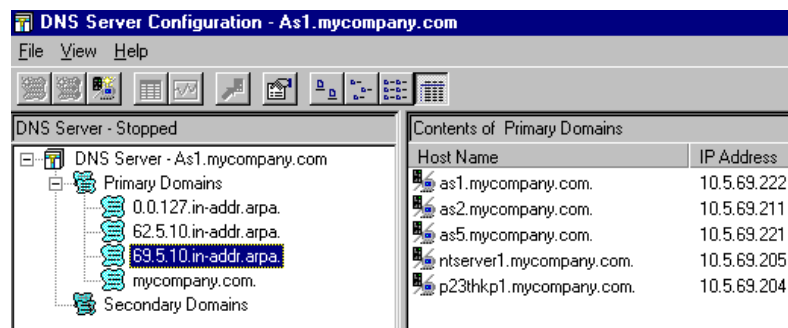


Figure 33. Contents of the 69.5.10.in-addr.arpa Primary Domain

The 0.0.127.in-addr.arpa domain was created by the DNS Configuration Wizard. Figure 34 shows the contents of this primary domain file. Note that the host *localhost* is contained in the *mycompany.com* forward mapping file shown in Figure 31 on page 43. You can think of the host *localhost* as the host that AS1 uses to "talk to itself". This host is a requirement; thus, it is a host that should immediately be added with the Operations Navigator DNS configuration wizard when initially configuring the name server.

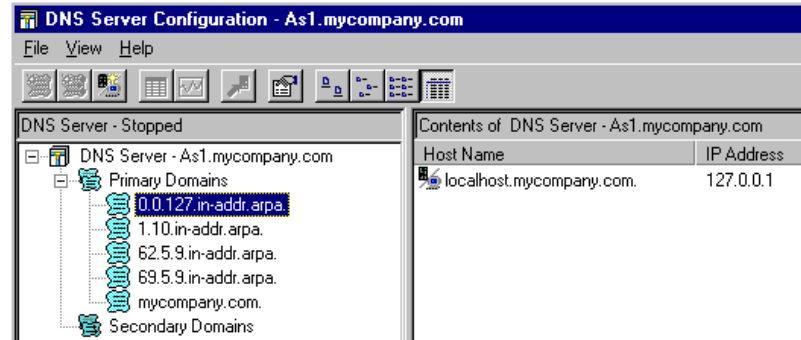


Figure 34. Contents of the Loopback Primary Domain

At this point, we finished the configuration of *mycompany.com* primary DNS server by configuring one forward mapping file (*mycompany.com*) and two reverse mapping files, 62.5.10.in-addr.arpa and 69.5.10.in-addr.arpa. All three files are primary domain files. The wizard created a BOOT file, CACHE file that contains the root name servers, and the 0.0.127.in-addr.arpa reverse mapping file automatically. The directives in the BOOT file are created through Operations Navigator. Note that you cannot view the BOOT and CACHE files from Operations Navigator's DNS configuration windows. However, they are located in the IFS directory: /QIBM/UserData/OS400/DNS and can be viewed with Operations Navigator:

1. Double-click the AS/400 system where the DNS server is running.
2. Click + next to File Systems.
3. Click + next to Root -> QIBM -> UserData -> OS400 ->.
4. Double-click DNS.
5. Double-click BOOT or CACHE file and choose the program you want to use to view the file.

In later chapters, we say that a name server "caches" information it receives from another name server. This is a way a name server "remembers" information so if it receives a query from a client for the same host, it can respond with an answer from its cache and not query the authoritative name server again. It is important to understand that this cached information is *not* contained in the /QIBM/UserData/OS400/DNS/CACHE file. The CACHE file contains information about root servers. This scenario does not require the use of root servers; thus, the CACHE file in this scenario should remain empty.

3.2.3 Configuring AS1 as a Mail Server

In this scenario, the AS1 AS/400 system is the only mail server for the *mycompany.com* domain. The DNS server running on AS1 needs to know this

since it receives queries from clients attempting to learn the IP address for the mail server that accepts mail for users in the domain *mycompany.com*.

Also, in this scenario we made a decision to let users use SMTP domain names of *mycompany.com* as the domain in the mail's destination when addressing their mail. The following example explains this further:

UserA in domain *mycompany.com* wants to send mail to *Tim Jones* who is also a POP3 client in the *mycompany.com* domain. *UserA* sends mail from the POP3 client to the e-mail address of *Tim@mycompany.com*, which should be delivered to *Tim's* POP3 server on AS1. In the following sections, we show how to configure the POP3 directory entry for *Tim* on AS1, how to configure the SMTP server on AS1, and how to configure the DNS server on AS1.

Tip

The easiest way to configure mail in an internal network is to use an SMTP domain name of <host.domain_name>. Mail should be addressed to *user@AS1.mycompany.com*, where AS1 is the host name of the mail server. However, most users do not want to have to remember the host name as part of the SMTP domain name when addressing mail. Thus, in this scenario, we show the configuration to handle both situations: when a user addresses mail to: *user@mycompany.com*, and when the user addresses mail to the same user as *user@AS1.mycompany.com*. In both cases, mail is delivered to the AS1 mail server.

The assumptions for this scenario:

- The outgoing SMTP server for *UserA's* client is AS1.
- The incoming POP3 server for *Tim's* client is AS1.
- *mycompany.com* does not have access to the Internet for the purpose of exchanging mail with Internet users.
- There is no firewall in the *mycompany.com* network.
- AS1 is the only mail server for all *mycompany.com* domain.
- *Tim's* PC where the POP3 client resides is configured to use AS1 as its DNS server.

3.2.3.1 Configuring a POP3 User on AS1

The user *Tim* needs to have a user profile and a POP3 directory entry on AS1.

Tim's user profile is JONEST2. We need to add an entry in the system distribution directory for the POP3 user. Use the Add Directory Entry (ADDDIRE) command shown in Figure 35 and press **Enter**.

```

                                Add Directory Entry (ADDIRE)

Type choices, press Enter.

User identifier:
  User ID . . . . . jonest2           Character value
  Address . . . . . as1             Character value
  User description . . . . . Tim Jones' POP directory entry

User profile . . . . . jonest2       Name, *NONE
System name:
  System name . . . . . *LCL           Character value, *LCL,
  System group . . . . .              Character value
  Network user ID . . . . . *USRID

```

Figure 35. Adding an Entry in the System Distribution Directory for User JONEST2

We now change the newly created directory entry to configure the user as a POP3 user. To change the directory entry, enter the following AS/400 command:

```
WRKDIR
```

Press **F17** to position to the *JONEST2* directory entry. Use option **2** to Change *JONEST2* directory entry.

Once into the Change Directory Entry display, page down four times until you get to the portion of the directory entry that contains the parameters *Mail service level* and *Preferred address*.

A POP3 directory entry *must* have a *mail service level* = **2** (System message store) and a *Preferred address* = **3** (SMTP name). See Figure 36.

```

                                Change Directory Entry

User ID/Address . . . . : JONEST2  AS1

Type changes, press Enter.

Mail service level . .  2                                1=User index
                                                             2=System message store
                                                             4=Lotus Domino
                                                             9=Other mail service

For choice 9=Other mail service:
  Field name . . . . . F4 for list

Preferred address . . .  3                                1=User ID/Address
                                                             2=O/R name
                                                             3=SMTP name
                                                             9=Other preferred address
                                                             F4 for list

Address type . . . . . F4 for list
For choice 9=Other preferred address:
  Field name . . . . . F4 for list

More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F18=Display location details
F19=Change name for SMTP  F20=Specify user-defined fields  F24=More keys

```

Figure 36. Mail Service Level and Preferred Address Values in POP3 Directory Entry

Press **F19** to enter *Tim*'s SMTP user ID and SMTP domain name in the Change Name for SMTP display. Press **Enter** to confirm that you want to add an SMTP userid and SMTP Domain name for this directory entry. Type in:

SMTP user ID = **tim**

SMTP domain = *AS1.mycompany.com*

See Figure 37.

Press **Enter** twice to confirm.

Important

Although users can address mail to *Tim* using the 'Mail To' of: *tim@mycompany.com* (we will show you how to configure it shortly), the SMTP domain name must still be *AS1.mycompany.com*.

Add Name for SMTP

System: AS1

Type choices, press Enter.

User ID : JONEST2

Address : AS1

SMTP user ID **tim**

SMTP domain **as1.mycompany.com**

SMTP route

Figure 37. Adding SMTP UserId and SMTP Domain Name for User JONEST2

3.2.3.2 Configuring POP3 Clients

First, let's summarize: Tim now has a POP3 directory entry on AS1. You can think of this as representing Tim's POP3 mailbox. Mail sent to *Tim@mycompany.com* is delivered to this mailbox until the user Tim takes the option to "Get Mail" from the POP3 client.

Tim's SMTP User ID is **tim** and his SMTP domain name is *AS1.mycompany.com*. Another user in *mycompany.com* can send mail to Tim by addressing mail to *tim@mycompany.com*. Tim must configure his POP3 client (running on his PC, for example, Netscape mail) with a POP3 User Name that matches the POP3 directory entry User profile (JONEST2 in our example). Of course if you want to make your life easier, you can use the same name for User ID and SMTP user ID.

Figure 38 shows the configuration for the POP3 mail client in the Netscape browser. Notice that *AS1.mycompany.com* is both an outgoing mail SMTP server

and an incoming mail POP3 server. The POP3 User Name matches the User profile in the AS/400 system distribution directory entry.

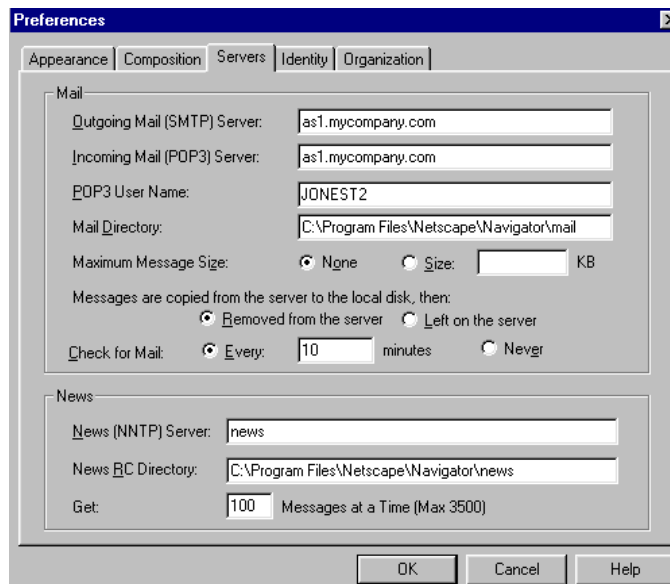


Figure 38. Specifying the Mail Server Option to the Netscape POP3 Mail Client

3.2.3.3 Configuring the Domain's Mail Server in the DNS Server

There must be an A record for the domain's mail server (also called mail exchanger) in the forward mapping primary domain file, *mycompany.com*, in the reverse mapping primary domain file 69.5.10.in-addr.arpa. In our scenario, AS1 already has an A record in both files as shown in Figure 31 on page 43 and Figure 33 on page 43.

To tell the name server that AS1 is the mail server for the domain, we need to add an MX record to the *mycompany.com* primary domain file. We use a wildcard MX record for this. The following steps show how to configure a wildcard MX record:

1. Right click on the *mycompany.com* primary domain.
2. Select **Properties**.
3. Select **Mail Tab**.
4. Click **Add**.
5. Take the default domain (*.*mycompany.com*.) and click **OK**. See Figure 39.

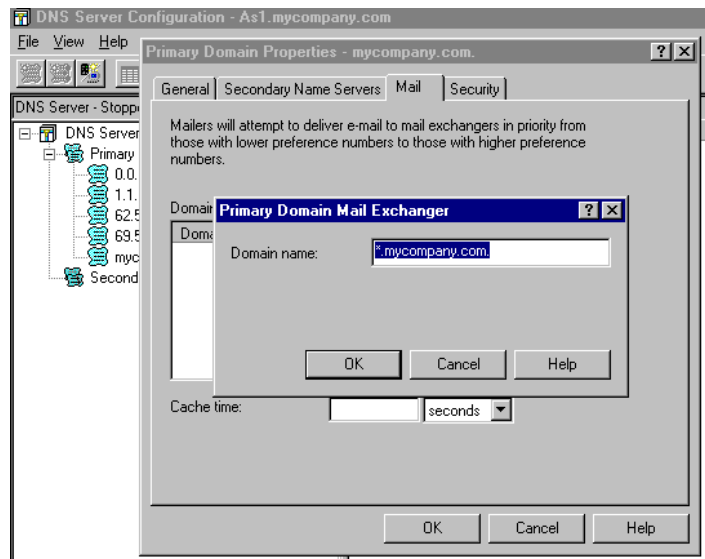


Figure 39. Configuring the DNS Primary Domain Mycompany.com's Mail Server

6. Enter the host name of the mail server (in this case, **as1**, as shown in Figure 40).
7. Click on **OK**. The result is shown in Figure 41.
8. Click on **OK** a second time to exit out of the Properties window.
9. Close the DNS window to Save the DNS Configuration.

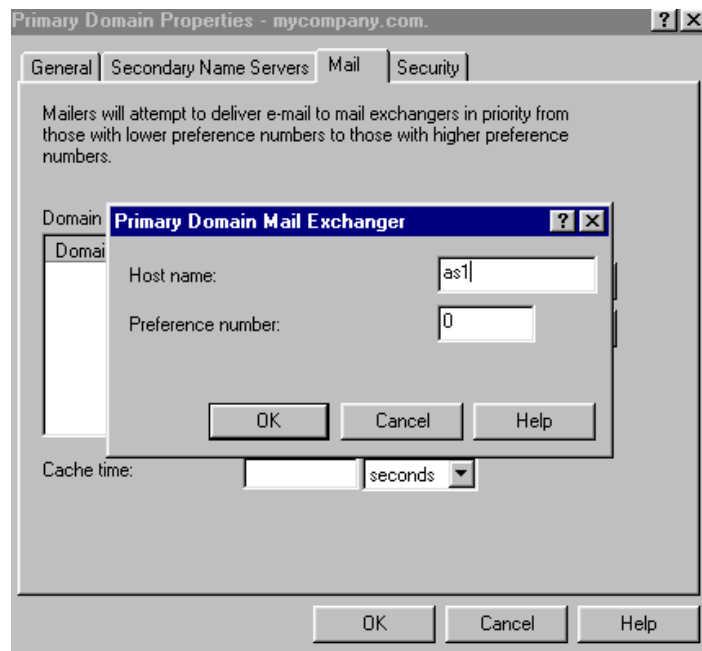


Figure 40. Entering the Mail Server's Host Name

Note: From the Operations Navigator DNS server configuration, the only way to ensure that you entered an MX record is to display the Properties of the

mycompany.com domain and review the contents of the Mail tab. To view the actual MX record, you can use the Operations Navigator File System to display the *mycompany.com.DB* file contained in the */QIBM/UserData/OS400/DNS* path.

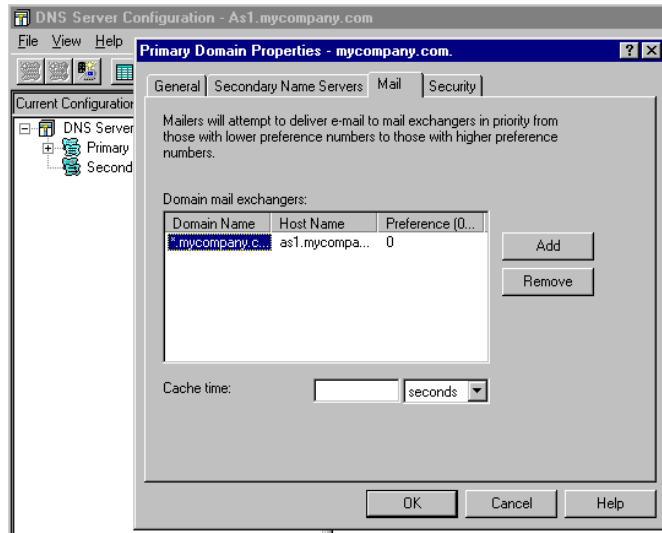


Figure 41. Result of Wildcard MX Record Added to mycompany.com Primary Domain File

Note

The MX record of domain name of **.mycompany.com* is called a wildcard MX record. If a client sends an MX record query to the name server for a host in domain *mycompany.com* and the name server does not have an A record for that host, then the name server sends a response stating that *AS1.mycompany.com* is the mail server for the domain *mycompany.com*.

If an MX query is sent to the name server for a host that **does** have an A record configured on the name server, the wildcard MX record is not used. The name server sends a negative response. However, for SMTP and mail, this is OK because after receiving a negative response for the MX query, the SMTP code sends an A record query for that host to the name server. Since an A record exists for that host, the name server sends a positive response to the A record query and SMTP attempts to send the mail to that host's IP address.

It is not a requirement that the mail server and the DNS server be the same AS/400 system.

3.2.3.4 Verifying the TCP/IP and SMTP Configuration on AS1

We should verify the TCP/IP configuration parameters relevant to mail as well as the SMTP configuration on the mail server (AS1).

Use the Change SMTP Attributes (CHGSMTPA) command to verify the SMTP configuration. Figure 42 shows the SMTP attributes in AS1. Since this network is not connected to the Internet and there is no firewall installed in the network, we want to confirm that the parameter Mail Router = ***NONE** and the parameter Firewall = ***NO**.

```

Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

Mail router . . . . . *NONE

Coded character set identifier      00819      1-65533, *SAME, *DFT
Mapping tables:
  Outgoing EBCDIC/ASCII table .    *CCSID      Name, *SAME, *CCSID, *DFT
    Library . . . . .             Name, *LIBL, *CURLIB

  Incoming ASCII/EBCDIC table .    *CCSID      Name, *SAME, *CCSID, *DFT
    Library . . . . .             Name, *LIBL, *CURLIB
Firewall . . . . . *NO             *YES, *NO, *SAME

```

Figure 42. AS1 SMTP Attributes

Verify the TCP/IP domain configuration. Use the Configure TCP command: CFGTCP option 12.

Verify the host name (AS1) and domain name (*mycompany.com*). Make sure that the *Search First* parameter is ***LOCAL** and the Internet Address is the IP address of AS1's DNS server, which is **10.5.69.222**. This ensures that when the SMTP server on AS1 attempts to deliver mail, it checks the AS/400 host table first and then the DNS server at 10.5.69.222 to resolve host names. We need the local host table searched first because it contains the alias *mycompany.com* for AS1, which the SMTP server needs to find. See Figure 43.

```

Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . 'AS1'

Domain name . . . . . 'mycompany.com'

Host name search priority . . . *LOCAL      *REMOTE, *LOCAL, *SAME

Internet address . . . . . '10.5.69.222'

```

Figure 43. CFGTCP Opt 12 on AS1 System

The last TCP/IP configuration that we need to verify on AS1 is the local host table. Make sure that *mycompany.com* is listed as an alias to AS1 in the host table. Notice in Figure 44 that *mycompany.com* is another host name for the IP interface of 10.5.69.222. This alias listed in the host table combined with the

Search First = *LOCAL (from CFGTCP opt 12) allows mail addressed to *user@mycompany.com* to be delivered to the AS1 mail server. Mail addressed to *user@AS1.mycompany.com* is also delivered to the AS1 with this configuration.

Work with TCP/IP Host Table Entries			System: AS1
Type options, press Enter.			
1=Add 2=Change 4=Remove 5=Display 7=Rename			
Opt	Internet Address	Host Name	
	10.5.62.58	p23fzg16	
		p23fzg16.mycompany.com	
	10.5.62.169	p23fym82	
		p23fym82.mycompany.com	
	10.5.62.187	p23gpb74	
		p23gpb74.mycompany.com	
	10.5.69.204	p23thkp1	
		p23thkp1.mycompany.com	
	10.5.69.205	NTserver1	
		NTserver1.mycompany.com	
	10.5.69.207	otherserver	
		otherserver.otherdomain.com	
	10.5.69.211	as2	
		as2.mycompany.com	
	10.5.69.221	as5	
		as5.mycompany.com	
	10.5.69.222	as1	
		as1.mycompany.com	
		mycompany.com	
	10.117.32.5	Rchserver3	
		Rchserver3.Remote.com	
	10.117.33.24	Rchserver2	
		Rchserver2.Remote.com	
	127.0.0.1	LOOPBACK	
		LOCALHOST	

Figure 44. Configuring mycompany.com as an ALIAS to AS1 and as1mycompany.com

3.2.3.5 Starting Mail Jobs on the Mail Server (AS1)

To start SMTP, POP3, and the mail server framework jobs, issue the following commands:

- strtcpsvr *smtp
- strtcpsvr *pop
- strmsf

If some of these jobs fail and cancel, you need to check the job logs for errors. See Section 8.1.10.4, "SMTP and POP Servers" on page 203.

3.2.4 Starting the DNS Server on AS1

To start the DNS server on AS1:

1. Close the DNS window in Operations Navigator.
2. From the OS400 Server list, right click **DNS**.
3. Click **Start**.

Figure 45 shows the DNS start sequence.

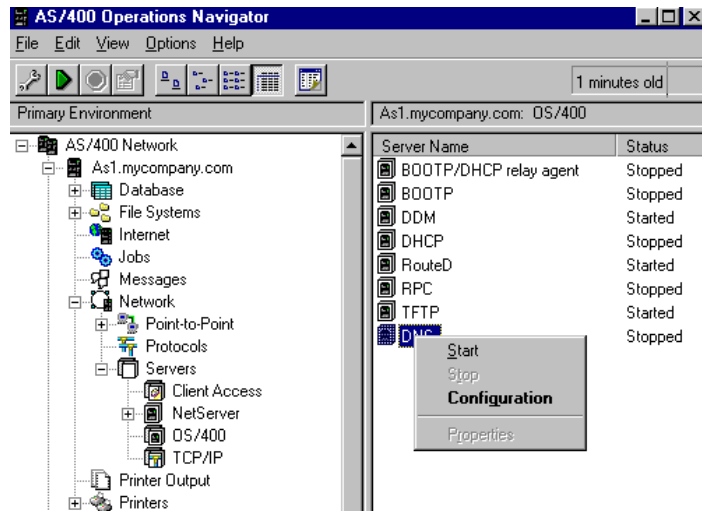


Figure 45. Right Click on DNS to Start the DNS Server

The DNS Server status is now *Started*. This may take a minute. Once the DNS Server is started, there should be one job named QTOBDNS active in the QSYSWRK subsystem on AS1.

3.2.5 Verifying That the DNS Server is Operational

The last step, of course, is to make sure that the name server is working properly. The DNS job logs and NSLOOKUP are the best sources to check for errors and verify that the DNS is operating as expected.

3.2.5.1 Reviewing DNS Job Log QTOBDNS for Errors

It is always a good idea to review the QTOBDNS job log for any errors:

1. From the AS1 command line, enter:

```
wrkactjob sbs(qsyswrk) job(qtobdns)
```

2. Take Option **5** to work with the job.
3. Take Option **10** to display the job log.
4. Press **F10** to display all messages in the job log. You may have to roll up or roll down to view all the messages.
5. Review messages for any errors.

Figure 46 shows the QTOBDNS job log after a successful startup of the DNS server.

```

Job . . : QTOBDNS      User . . : QTCP      Number . . . : 013973

>> CALL PGM(QDNS/QTOBDNS) PARM('-p' '53' '-d' '0' '-b' '/QIBM/UserData/OS400/
DNS/BOOT')
DNS server starting.
Could not assign address to socket.
primary zone mycompany.com (serial number 886456347) loaded successfully.
primary zone 69.5.10.in-addr.arpa (serial number 886456347) loaded
successfully.
primary zone 1.1.10.in-addr.arpa (serial number 886456347) loaded
successfully.
primary zone 62.5.10.in-addr.arpa (serial number 886456347) loaded
successfully.
cache zone . (serial number 0) loaded successfully.
Ready to answer queries

```

Figure 46. QTOBDNS Job Log After a Successful Startup of DNS Server

Note the error message: Could not assign address to socket. Displaying Message Details shows the message ID DNS00E9.

This error message may or may not be a problem. For further details on this error message and what to do if the job log contains it, see , “Problem Symptom 4:” on page 209.

Tip

If an IP interface is started *after* the DNS server starts, the DNS server must be stopped and started again or the Update Server function from Operations Navigator must be run before the name server can accept queries on the newly started IP interface.

3.2.5.2 Using NSLOOKUP to Verify the DNS Configuration for Mail

NSLOOKUP is an interactive tool that can be used on the AS/400 system to simulate a client querying a DNS server.

We used nslookup to verify that the host AS1.mycompany.com, the alias mycompany.com, and the MX record for *.mycompany.com are configured correctly on the AS1 DNS server.

To start an NSLOOKUP session, enter the command:

```
call pgm(qdns/qtoblookup)
```

Address Query Type Using NSLOOKUP

We use query type A (address) to query A (address) records in the name server. The NSLOOKUP default query type is the A (address) record query, thus, from an NSLOOKUP session, enter:

```
as1.mycompany.com.
```

Figure 47 shows the results of this query. To the right of the > symbol, you can see the query that we entered before. The text that follows that line is NSLOOKUP answer. Server and Address refer to the name server NSLOOKUP is querying. The next Name and Address is the DNS server response to the A record

query: the IP address of AS1.*mycompany.com* is 10.5.69.222. We happened to issue an A record query for the same host that runs the DNS server.

```
>
> as1.mycompany.com.
Server:  as1.mycompany.com
Address: 10.5.69.222

Name:    as1.mycompany.com
Address: 10.5.69.222

>

====>

F3=Exit F4=End of File F6=Print F9=Retrieve F17=Top
F18=Bottom F19=Left F20=Right F21=User Window
```

Figure 47. A Record Query for AS1.*mycompany.com* Using NSLOOKUP

MX Record Query Using NSLOOKUP for Unknown Host

To issue an MX record query using nslookup, we first need to change the query type. Enter the NSLOOKUP command:

```
SET TYPE=MX
```

If we issue an MX query for a host that does not have an A record in the DNS configuration, the name server uses the wildcard MX record for *.*mycompany.com*. that we configured in Section 3.2.3.3, “Configuring the Domain’s Mail Server in the DNS Server” on page 48.

The name server answers that AS1.*mycompany.com* is the mail exchanger for the domain *mycompany.com*. For example, Figure 48 shows the result of an MX query for *anyhost.mycompany.com*. The AS1 name server does not have an A record for *anyhost*, which you can verify by referring to Figure 31 on page 43.

```
Default Server:  as1.mycompany.com
Address: 10.5.69.222

>
> set type=mx
>
> anyhost.mycompany.com.
Server:  as1.mycompany.com
Address: 10.5.69.222

anyhost.mycompany.com  preference = 0, mail exchanger = as1.mycompany.com
mycompany.com          nameserver = as1.mycompany.com
as1.mycompany.com      internet address = 10.5.69.222
>
```

Figure 48. Nslookup MX Query for Unknown Host Anyhost

However, if an MX query is issued for a host that has an A record on the name server such as AS2, the name server does not use the wildcard MX record and

simply returns a negative response to the MX query. Figure 49 shows an example of this.

```
>
> set type=mx
>
> as2.mycompany.com.
Server:  as1.mycompany.com
Address: 9.5.69.222

*** No mail exchanger (MX) records available for as2.mycompany.com.
>

===>
```

Figure 49. Nslookup MX Query for Host AS2

If an SMTP client tried to deliver mail to AS2, it first queries for an MX record and receives a negative response. Next, the SMTP client queries for an A record for AS2, receives a positive response, and attempts to establish a connection with the SMTP server running on AS2. In our scenario, however, AS2 is not a mail server; therefore, there is no SMTP server running on AS2 and an SMTP client fails to establish a connection.

MX Query Using NSLOOKUP for Domain Mycompany.com

What does the name server do with an MX query for the domain *mycompany.com*? Will the wildcard MX record **.mycompany.com* be used? The answer is no. See Figure 50.

```
>
> set type=mx
>
> mycompany.com.
Server:  as1.mycompany.com
Address: 9.5.69.222

*** No mail exchanger (MX) records available for mycompany.com.
>

===>
```

Figure 50. Nslookup MX Query for Domain *mycompany.com*.

As we discussed in Section 3.2.3, “Configuring AS1 as a Mail Server” on page 44, if mail is addressed to *user@mycompany.com*, it *will* be delivered. How does it get delivered? The secret to getting mail delivered when it is addressed to the domain only and not <host.domain name> is having the alias of *mycompany.com* listed in the AS/400 local host table and having the *Search First* parameter set to *LOCAL. This was outlined in Section 3.2.3.3, “Configuring the Domain’s Mail Server in the DNS Server” on page 48. This causes the SMTP server on AS1 to search the local host table first, find the alias *mycompany.com* for AS1, determine that the mail is destined for the same AS/400 system that the SMTP is running on, and then attempt to find the POP3 directory entry to deliver the mail. In this case, the DNS server on AS1 is not involved in helping to deliver the mail.

3.2.6 Creating a Secondary DNS Server

We do not recommend that your network relies on only one DNS server for availability reasons. Once the primary name server is operational, we need to create a secondary domain name server that can back up the primary DNS server and also be used to distribute the DNS query workload between two or more servers.

After you configure and start the secondary name server, it attempts to do a zone transfer of the domain files that reside on the primary name server. The server that the secondary name server gets its domain files from is called master server. The master server can be a primary domain name server or another secondary name server. In this scenario, AS5 is the only secondary name server; thus, its master name server must be the primary name server AS1.

Tip

RFCs recommend that a secondary name server does not get zone transfers from another secondary DNS server.

3.2.6.1 Configuring the Secondary Server AS5

Use Operations Navigator DNS server configuration to configure AS5 as a secondary DNS server. Three *secondary* domain files need to be created on AS5 to fully back up AS1:

- *mycompany.com* forward mapping secondary domain file
- 62.5.10.in-addr.arpa reverse mapping secondary domain file
- 69.5.10.in-addr.arpa reverse mapping secondary domain file

To create *mycompany.com* forward mapping secondary domain file:

1. Double-click **as5.mycompany.com**. We are now using Operations Navigator to configure AS5.
2. Double-click **Network**.
3. Double-click **Servers**.
4. Double-click **OS/400**.
5. Double-click **DNS**.
6. Double-click **DNS Server**.
7. The DNS configuration wizard starts if this is the first time you are configuring DNS on AS5.
8. Click **Next**.
9. Click the radio button to the left of **Secondary Server** when the wizard asks which type of server you want to configure.
10. Click **Next**.
11. Enter the domain that this server will be secondary for: *mycompany.com*.
12. Enter the IP address of the primary name server. In this case, it is **10.5.69.222**, which is the IP address of the AS1 AS/400 system.
13. Click on **Finish**.

At this point, the *mycompany.com* domain shows up under Secondary Domain. This is only one of three domain files that you need created to fully back up the AS1 primary domain name server. Let's check to make sure that the wizard enabled *save copies of the master server files*. This guarantees that the secondary domain files are backed up on the secondary server. The secondary server attempts to do a zone transfer every time it starts. If the

primary server is down at that time, the secondary server runs from the backup files. It uses the backup files until the data expires (or a new transfer is successful).

- Double-click **Secondary Domains** in AS5's DNS server configuration. At this point, there should be one secondary domain of *mycompany.com*.
- Double-click the **mycompany.com** secondary domain.
- Ensure that *Save copies of the master server files* is checked off.
- Click **OK**.

Creating 62.5.10.in-addr.arpa Reverse Mapping Secondary Domain File

14. Right click **Secondary Domain**.

15. Select **New Secondary Domain**.

16. Enter the domain: `62.5.10.in-addr.arpa`. Ensure that *Save copies of the master server files* is checked off.

17. Click **Add**.

18. Enter the IP address of the primary name server (AS1): `10.5.69.222`.

19. Click **OK**.

Create 69.5.10.in-addr.arpa Reverse Mapping Secondary Domain File

20. Repeat the previous steps 14 to 19 to create the `69.5.10.in-addr.arpa` secondary domain file. The only difference is step 16; this time the domain is:

`69.5.10.in-addr.arpa`

21. Close the DNS window to save the secondary domain configuration on AS5.

3.2.6.2 Adding NS Record for the Secondary Name Server on AS1

It is good practice, even when not mandatory, to add an NS resource record for the secondary name server in the primary domain files on the primary DNS. When the primary name server responds to queries from clients, the response includes the IP address of the secondary name server if the primary knows about it (NS record for secondary is in primary's configuration). If the client's resolver is smart enough to handle this information, it decides which name server, primary or secondary, is closer based on the IP address. If the secondary DNS server is closer to the client, it sends future queries to it, improving name resolution response time.

To add a resource NS record on AS1's primary domain files, use the following steps:

1. Start the AS1 DNS server configuration in Operations Navigator.
2. Right click on the primary domain file *mycompany.com*.
3. Select **Properties**.
4. Select the **Secondary Name Server** tab.
5. Click **Add**.
6. Verify that the domain name is *mycompany.com*. This is the domain name that the secondary server is located in. Do not forget the trailing period after *com*.
7. Click **OK**.
8. Enter the host name of the secondary name server AS5.
9. Click **OK**. See Figure 51 to review the result.
10. Click **OK**.

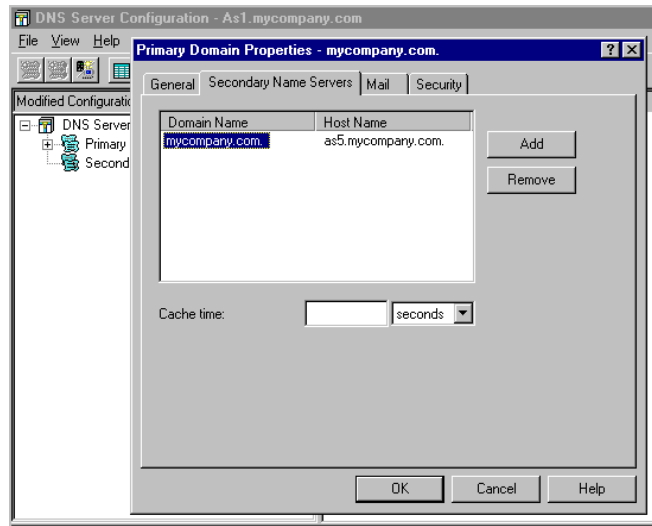


Figure 51. Enrolling the Secondary Server AS5 in the Primary Server's List of Name Servers

11. Repeat steps 2 through 9 for the primary domain file of 69.5.10.in-addr.arpa and again for the primary domain file of 69.5.10.in-addr.arpa. The domain name should be the domain name of the secondary name server, which is *mycompany.com*.
12. If the DNS server is started, click the Update Server smart icon to save the changes to a file and send a signal to the DNS server to reread its configuration files.
13. If the DNS server has been stopped, close the DNS window and start the DNS server. A secondary name server does not successfully initiate a zone transfer if the primary name server is not started.

3.2.6.3 Starting the Secondary Name Server

We are now ready to start the secondary name server on AS5.

Start the AS5 name server with Operations Navigator or with the AS/400 command on AS5:

```
strtcpsvr *dns
```

As the DNS secondary name server starts on AS5, it attempts a zone transfer from AS1 to transfer the three domain files to AS5. The DNS server on AS1 (the primary name server) needs to be active at this time for the zone transfers to be successful.

On AS5, the secondary DNS server job QTOBDNS starts as well as jobs named QTOBXFER. Each QTOBXFER job is responsible for one of the zone transfers on AS5. Each QTOBXFER job ends as soon as the zone transfer finishes. In this scenario, AS5 initiates three zone transfers, one for each domain: *mycompany.com*, *62.5.10.in-addr.arpa*, and *69.5.10.in-addr.arpa*. Figure 52 on page 60 shows the QTOBDNS job log on the secondary DNS server, AS5.

On AS1, the primary name server QTOBDNS job should already be active if the DNS server is started. During the zone transfers, one job named QTOBXMIT starts on the primary name server for every zone transfer that takes place. Each QTOBXMIT ends when the zone transfer it is responsible for finishes.

After the DNS server is started, the QTOBDNS job should remain active in the QSYSWRK subsystem on AS5. Review the QTOBDNS job log on both the primary and secondary name servers for any errors and to verify that the domains transferred successfully. See Figure 52 for an example of a secondary name server's QTOBDNS job log after a successful start.

If there are error messages in the job logs regarding the zone transfer, see 8.2, "Problem Symptoms and Probable Causes" on page 207. There are several *Problem Symptoms* documented in this section dealing with why a zone transfer may fail.

```
Job . . : QTOBDNS      User . . : QTCP      Number . . . : 045012

>> CALL PGM(QDNS/QTOBDNS) PARM('-p' '53' '-d' '0' '-b' '/QIBM/UserData/OS400/
DNS/BOOT')
DNS server starting.
secondary zone mycompany.com (serial number 886456347) loaded
successfully.
secondary zone 62.5.10.in-addr.arpa (serial number 886456347) loaded
successfully.
primary zone 0.0.127.in-addr.arpa (serial number 886464830) loaded
successfully.
secondary zone 62.5.9.in-addr.arpa (serial number 886456347) loaded
successfully.
cache zone . (serial number 0) loaded successfully.
Ready to answer queries.
```

Figure 52. QTOBDNS Job Log on Secondary System After DNS Server Successfully Starts

3.2.6.4 Controlling Zone Transfer Frequency

By now it should be clear that the DNS administrator only updates the DNS files on the primary name server and the secondary name server automatically performs zone transfers of the data from the primary name server (or another secondary name server) to keep its domain data in sync with the domain data on the primary name server. How often should a secondary name server check with the primary name server to make sure its data is in sync with the primary? The answer depends on how often the primary name server is updated with changes; thus, it varies from installation to installation. Therefore, refresh rates and other associated timers can be configured on the primary name server. These configuration rates and times are on the Properties of each primary domain file on the primary name server. Usually the supplied defaults are acceptable for a typical network serviced by a DNS server. Figure 53 shows the defaults for the primary domain *mycompany.com* on AS1. Refer to Section 8.1.2, "Tips for Performance" on page 186 for performance considerations.

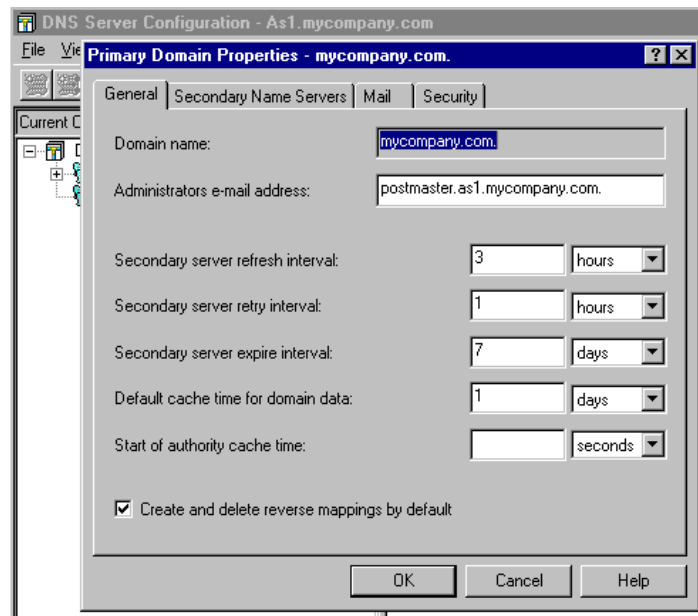


Figure 53. Retry and Refresh Rates for Secondary Name Servers

The information on the Properties page of the primary domain file *mycompany.com* shown in Figure 53 is included in the SOA resource record in the file `/QIBM/UserData/OS400/DNS/mycompany.com.db` file.

Let's define what these numbers mean:

- Secondary server refresh interval:

A secondary server checks to see that it is in sync with the primary by checking the serial number contained in the SOA record. Every time a DNS administrator makes a change to a primary domain file, Operations Navigator automatically increments this serial number. In fact, after starting the primary name server, the QTOBDNS job log contains a message stating the serial number that the primary domain file is running with. See Figure 46 on page 54 for an example of this.

The secondary server refresh interval of three hours means that the secondary server checks the primary name server's serial numbers of the domain files it is configured to back up every three hours. If the serial numbers are different, the secondary name server attempts a zone transfer to refresh its domain files. If the serial numbers are the same, then the zone transfer is not needed and does not take place.

- Secondary server retry interval:

Specifies the time interval that elapses before the secondary domain server can re-attempt to refresh its data from the primary domain server after the previous refresh attempt failed. You can specify the time in seconds, minutes, hours, and days.

- Secondary server expire interval:

If the secondary domain files are configured with *Save copies of master server data* enabled, then a secondary name server saves backup copies of the domain files after successful zone transfers. This allows a secondary name

server to start up from these backup files and then attempt a refresh. If the refresh fails, the secondary name server continues to be active but it serves responses from its backup files that may be down level from the primary domain files on primary name server. The secondary server expire interval of seven days means that the secondary name server can run from its backup files for a limit of seven days. After seven days, the backup files expire and the secondary name server can no longer use them. Remember, if the refresh from the master server fails, the secondary name server re-tries with the frequency specified in the *Secondary server retry interval* field (every hour by default). Thus, for the secondary server's backup files to expire, the master name server must be down for seven days.

- Default cache time for domain data:

This timer affects all the name servers that query this primary name server. When a name server queries AS1 and gets a positive response, it caches the response (saves it) so if another client queries the name server for the same information, the name server can supply the response from its cache and not have to query the AS1 name server again. Default cache time for domain data controls how long name servers can keep AS1's positive responses in their cache. The default setting for this parameter is one day.

Negative responses are cached for a hard-coded value of 10 minutes. This value cannot be configured.

- Start of Authority Cache Time:

By default, the Properties page of each primary domain file leaves this parameter blank. However, this does not mean that the SOA record does not have a cache time setting but rather the SOA cache time defaults to whatever the default cache time for domain data is set to (which is one day, by default).

Let's further explain. The primary domain file contains several types of resource records: one SOA record, at least one NS record, several A records, perhaps CNAME records, and perhaps MX records. Each of these resource records can have a cache timer associated with it, which, for that particular resource record, overrides the default cache time for domain data settings. The Properties page of the *mycompany.com* domain contains the timer for only the SOA resource record.

So where are the timers configured for other resource records? Let's take the A record for example:

- Double-click on the *mycompany.com* primary domain file.
- Right click on any host (for example, *AS2.mycompany.com*).
- Click **Properties** to display the individual host AS2' properties.
- Note that there is a cache time parameter here that defaults to blank. See Figure 54.

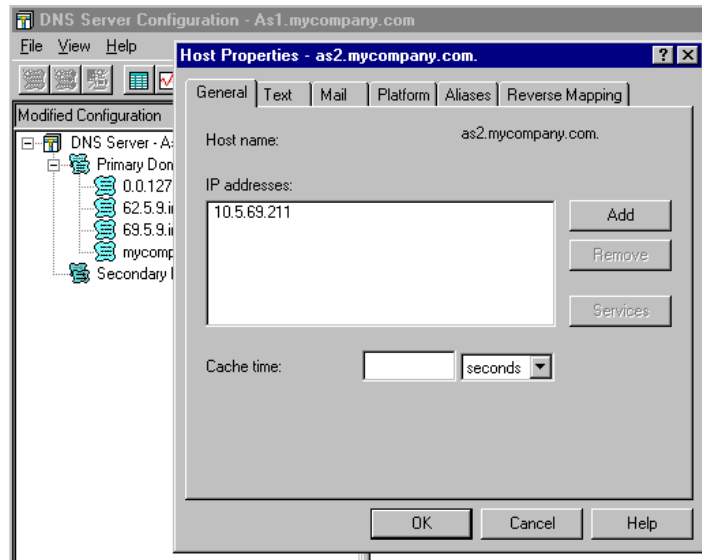


Figure 54. Cache Time for Individual Host AS2

AS2's cache time is blank, which means that the default cache time for domain data of one day is what AS2's cache time defaults to.

Tip

If you determine that you need to override one of the default timers on the *mycompany.com* properties page in Figure 53 on page 61, do not forget to change the same timers on the 62.5.10.in-addr.arpa properties page and the 69.5.10.in-addr.arpa properties page. Remember, the in-addr.arpa files are primary domain files just the same as *mycompany.com*. The changes in any of the tabs in *mycompany.com*'s properties page only affects the primary domain file of *mycompany.com*. You must remember to consider making matching configuration changes to the in-addr.arpa primary domain files if you make configuration changes to the *mycompany.com* primary domain file.

3.2.7 Primary Name Server Security Considerations

The information in the DNS files is security sensitive and you may want to restrict the secondary name servers that are authorized to do zone transfers. Furthermore, you may also want your DNS to answer queries from a pre-determined set of clients. This section discusses some techniques that make your name server more secure.

3.2.7.1 Zone Transfer Security

By default, the primary name server allows any secondary name server to request a zone transfer. If you want to restrict zone transfers to only authorized secondary name servers, you can do so by configuring the *trusted* name servers IP addresses. Use the following steps:

1. Start AS1 DNS server configuration in Operations Navigator.
2. Right click **DNS Server-As1.mycompany.com**.
3. Click **Properties**.
4. Select the **Security** tab.

5. Click **Add**.
6. Enter the IP address of the secondary name server: **10.5.69.221** and the mask of **255.255.255.255**. See Figure 55.

This creates a XFRNETS directive in the BOOT file that takes as its arguments the networks or IP addresses you want to allow to transfer zones from your name server.

Tip

In this example, we are authorizing a specific IP address of a secondary server, AS5. If we want to authorize any secondary server in the network 10.5.69.192, we specify an IP network of 10.5.69.192 with a mask of 255.255.255.192.

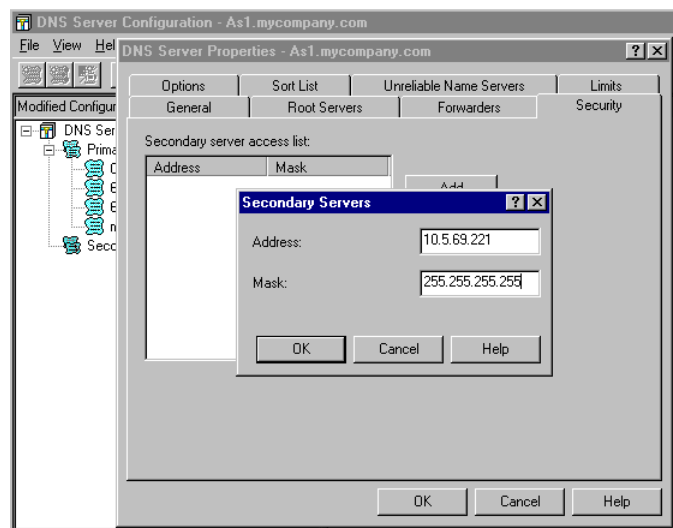


Figure 55. Authorizing Secondary Name Server AS5 to the Primary Name Server AS1

7. Click **OK**.
8. Close the DNS server configuration window.
9. Right click **DNS**.
10. Click **Stop**.
11. Click **Start** to start the DNS server again.

Tips

- When changing the contents of the Security tab on the DNS server, you must run the Update Server function from Operations Navigator for the change to take effect.
- When the Security tab of the DNS server is empty of secondary servers, ANY secondary server is authorized to do a zone transfer from the primary server AS1. As soon as the Security tab is configured with one IP address of a secondary server, then all other secondary servers are denied

3.2.7.2 Restricting Queries by Client's IP Address

It is possible to configure each primary domain file to allow clients with only certain IP addresses to query this primary domain data. From Operations Navigator, go into the primary server AS1's DNS configuration. To authorize only certain clients to query AS1, use the following steps:

1. Start AS1 DNS server configuration in Operations Navigator.
2. Double-click **Primary Domains**.
3. Right click *mycompany.com*.
4. Select **Properties**.
5. Select the **Security tab**.

Note: When we display the Security tab, the *Limit domain data access to subnets* list and the *Limit domain data access to IP address* list are both blank by default. When both of these lists are blank, that means that ANY client that knows the primary name server's IP address and has TCP/IP connectivity to this AS/400 system can successfully query the AS1 name server.

6. Click on **Add** to add the subnet that you want to allow.
7. Enter the subnets of clients that you want to allow to query this name server by entering the subnet's network address: **10.5.69.192** and mask **255.255.255.192**.
8. Click on **OK** (but do not click on the second OK just yet).

Now that we have authorized all clients located in the subnet 10.5.69.192 to query the primary name server AS1, we have *implicitly denied* clients from all other subnets. We have even denied access from *localhost*. For this scenario, we should also give access to clients from the 10.5.62.0 network and give access to the explicit address of 127.0.0.1 for localhost.

9. Repeat steps 6 through 8 for the subnet of 10.5.62.0. The subnet mask for **10.5.62.0** subnet is **255.255.255.0**.
10. Click on the second Add to Limit domain data access to IP addresses.
11. Enter the IP address of localhost **127.0.0.1**. See Figure 56 to view the result.

Note: Once you specify an address or subnet on the primary domain properties' security tab, it is required to specify the 127.0.0.1 IP address in the *Limit domain data access to IP address list*.

12. Click on **OK**.

The previously explained configuration adds *secure-zone* TXT records to the primary domain configuration file. The secure-zone record defines an access list of IP addresses allowed to query your name server for data in a particular zone.

We just authorized all clients from two subnets, 10.5.69.192 and 10.5.62.0, to access the *mycompany.com* primary domain file on the primary name server AS1. However, when a client on one of those networks issues a reverse look up query to the AS1 name server, will it be successful? Yes, because the security tabs on both the 69.5.10.in-addr.arpa and the 62.5.10.in-addr.arpa primary domain files are still blank; by default -- any client has access to these files. Thus, if we need to have the same security on 69.5.10.in-addr.arpa and the 62.5.10.in-addr.arpa primary domain files as we do on *mycompany.com*, we need to repeat steps 3 through 12 for each in-addr.arpa file. And do not forget step 11;

which specifies the *localhost* IP address to be an authorized address on both in-addr.arpa primary domain files' properties security tab also.

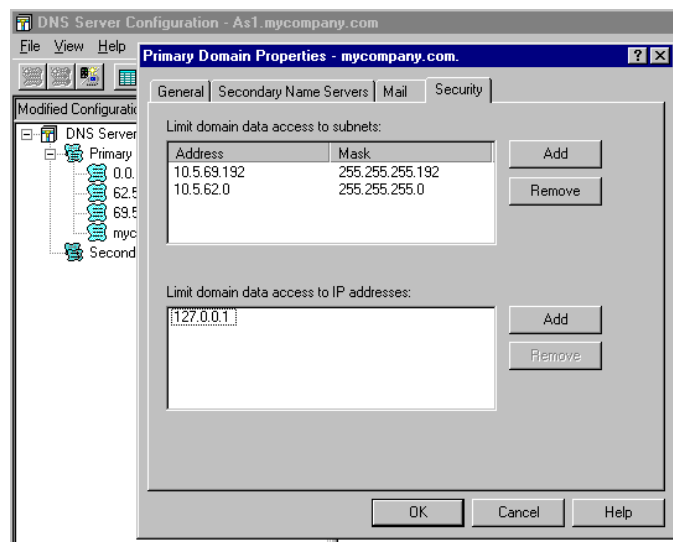


Figure 56. Restricting DNS Queries by Subnet and Client's IP Address

3.2.8 Reconfigure Clients to Use the DNS Server

Now that the primary and secondary DNS servers are active on AS1 and AS5 systems, it is time to reconfigure clients to start using the DNS servers. An AS/400 system can be a client to a name server; thus, the AS/400 systems in the *mycompany.com* domain require a configuration change also.

3.2.8.1 Configuring AS/400 Systems to Query the DNS Server

To reconfigure the AS1 system to query the DNS server, enter the command:

```
CFGTCPIP option 12
```

Figure 57 on page 67 shows the resolver configuration on AS1.

Host name search priority specifies whether to search a remote Domain Name Server (DNS) to resolve a TCP/IP host name, or to search the local TCP/IP host table first.

*LOCAL means that we want this system to first search the TCP/IP host table located on this system to resolve TCP/IP host names.

NOTE: Because AS1 is the mail server, we configured the *Host name search priority* to be *LOCAL. See Section 3.2.3.4, "Verifying the TCP/IP and SMTP Configuration on AS1" on page 50, for details. Figure 57 is taken from AS1; thus, it shows Search First=*LOCAL.

Specify *REMOTE if you want this system to search a remote DNS server to resolve TCP/IP host names before searching the local TCP/IP host table. The remote DNS server to use is specified by the Internet address parameter. For this scenario, all the AS/400 systems in the *mycompany.com* domain except for AS1 specify *REMOTE.

Tip

Often some information in the host table and *LOCAL can keep systems operational to some degree even if the system cannot get to the remote name server. If something happens to the interfaces or the servers, applications can hang, trying to contact the servers and never get to the host table if *REMOTE is selected. For instance, if local host information is in the host table, local mail can still be delivered if *LOCAL is selected.

Internet addresses specifies up to three remote Domain Name Servers (DNS) to be used by this system. In our scenario, the primary name server IP address is **10.5.69.222** and the secondary name server IP address is **10.5.69.221**.

```
Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . 'AS1'

Domain name . . . . . 'mycompany.com'

Host name search priority . . . *LOCAL      *REMOTE, *LOCAL, *SAME

Internet address . . . . . '10.5.69.222'
                          '10.5.69.221'
```

Figure 57. Configuring the AS/400 Resolver

Note

If the DNS server specified first cannot be reached, the AS/400 system queries the next name server in the list.

If the name server configured at the top of the list respond but sends back a negative response (in other words, the first name server does not know the answer), the AS/400 resolver queries the subsequent name servers in the list.

3.2.8.2 Configuring Non-AS/400 Clients to Query the DNS Server

All the clients in your network should have the DNS configuration updated to query the newly implemented primary and secondary DNS servers. How to make this configuration change depends on your clients DNS support; therefore, you do not provide instructions on how to update non-AS/400 client's DNS configuration. Figure 58 shows the DNS configuration for a Windows 95 client.

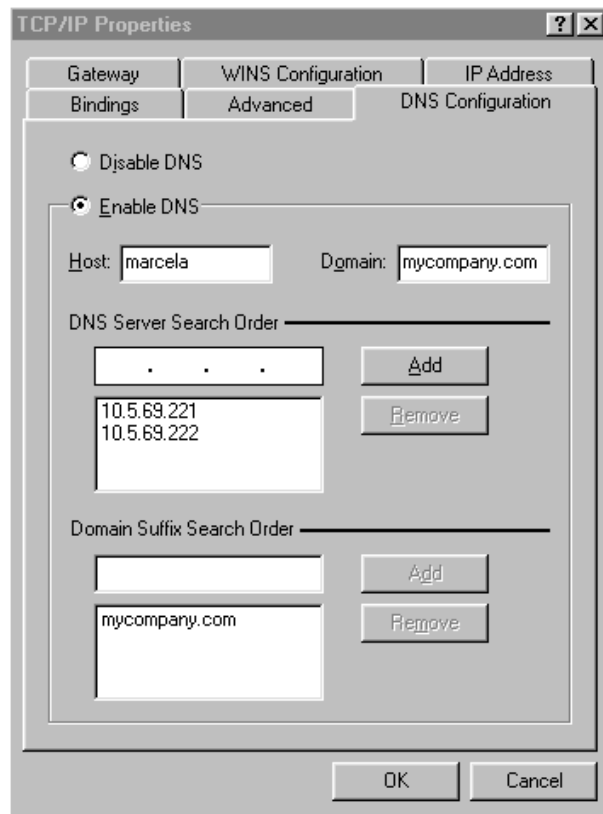


Figure 58. Windows 95 Client DNS Configuration

The DNS administrator should be aware that an answer from a secondary name server is considered "as good" as an answer from a primary name server; they are both called *authoritative* answers. Thus, to balance the name serving workload between AS1 and AS5, the DNS administrator can configure half of the clients in *mycompany.com* to list AS1's IP address first in the client's DNS server configuration and the other half of the clients to query AS5 first by entering AS5's IP address (10.5.69.221) at the top of the list as shown in Figure 58.

3.3 Summary

In this chapter, we took you step-by-step through the implementation of the primary DNS, starting with the migration of the AS/400 host table.

We showed you how to use DNS server configuration through Operations Navigator, discussed the main files in the name server database, and showed you how to configure the AS/400 system as a mail server, including special considerations relative to DNS and mail.

We also explained how to implement a secondary DNS to back up the primary name server. And we showed you how to verify that a name server is operational and functioning as expected.

In addition, we discussed name server security considerations and how to configure the security features in the primary name server to control zone

transfers and access to the DNS based on subnet ID or client IP address. We also covered how to configure clients to query name servers.

Chapter 4. Migrating an NT Primary DNS to AS/400 System

You may have already implemented a name server before the AS/400 system announced DNS server support on V4R2. If you are thinking of making your AS/400 system the primary DNS server, this chapter describes how to migrate an existing primary DNS on a non-AS/400 platform (NT in our scenario) to AS/400 DNS. This chapter also explains how to use the existing NT server as a secondary name server for backup and workload balancing purposes.

4.1 Migrating NT DNS Server Primary Domain Files

The migration from a DNS server on a non-AS/400 platform (NT in our scenario) to the AS/400 DNS server is fairly simple provided the non-AS/400 platform DNS server supports DNS files in the format described by RFC 1035. This is the case for the NT 4.0 DNS server. Figure 59 shows an overview of how to migrate NT DNS files to the AS/400 DNS server.

Tip

Migration should be between servers at the same level of BIND. The AS/400 system DNS support is BIND 4.9.3. Versions of BIND beyond 4.9.3 may have records not recognized by the AS/400 system BIND 4.9.3 server.

The first step is to bring the files from the NT server to the AS/400 IFS directory `\QIBM\UserData\DNS`. The second step is to run *Import Domain Data*. Finally, you may need to make some manual adjustments to the DNS server configuration on the AS/400 system.

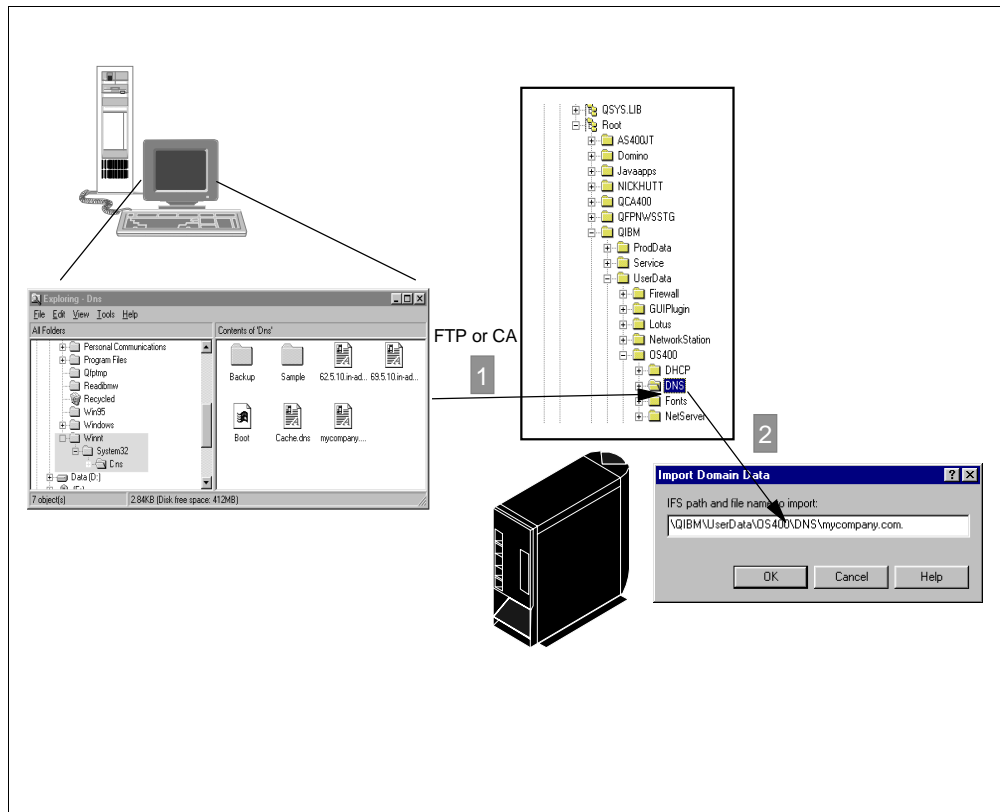


Figure 59. Migrating NT DNS Server to AS/400 DNS Server Overview

4.1.1 Scenario Objective

The objectives of this scenario are to:

1. Show how to migrate an existing primary DNS on a non-AS/400 platform to an AS/400 DNS server.
2. Show how to configure the existing primary DNS as a secondary DNS to back up the new primary name server running on the AS/400 system.

4.2 Task Summary

1. Review the current DNS server configuration on the NT server.
2. Transfer the DNS db files from the NT server to the IFS on the AS/400 system.
3. Import the domain data.
4. Perform final configuration adjustments if necessary.

4.2.1 Reviewing Primary DNS Configuration on the NT Name Server

To review the current DNS configuration on the NT server, use the following steps:

1. Select **Administrative Tools (Common)** from the *Start* pop-up menu.
2. Select **DNS Manager**.
3. Click + next to **NTSERVER1** (NT server name).

- Double-click *mycompany.com*. The primary domain forward mapping file is displayed on the right panel (Figure 60). You can display the content of the reverse mapping files *.in-addr.arpa as well.

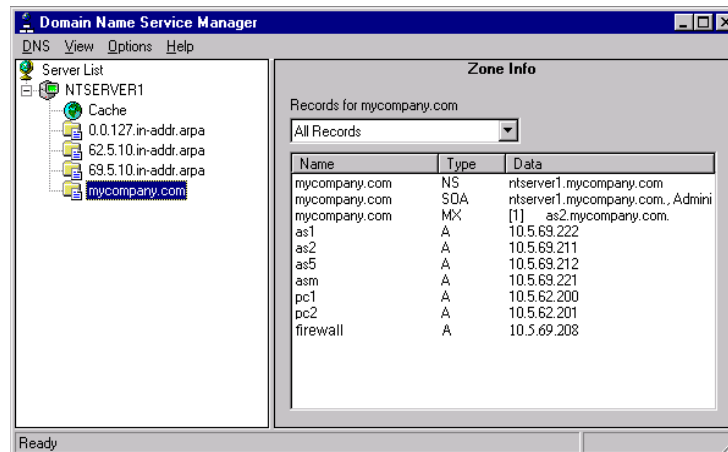


Figure 60. NT DNS Server db Files

- Right-click **NTSERVER1** and select **Properties**.
- Click **Forwarders**. Take note of the forwarders configuration (Figure 61).

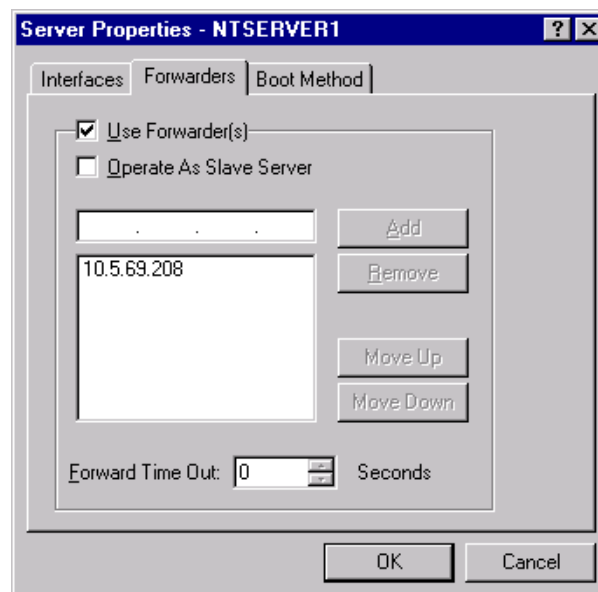


Figure 61. NT DNS Forwarders Configuration

- Select the **Boot Method** tab. Usually, the NT DNS server is configured to boot from the data contained in the registry, which means that the BOOT file cannot be migrated and you need to manually make adjustments to the AS/400 DNS server configuration.

4.2.2 Transferring DNS Files from the NT Server to the AS/400 System IFS

The NT server DNS configuration files reside on the path `\winnt\system32\Dns.`

Note: Winnt is the directory where Windows NT is installed.

In this scenario, the following DNS configuration files are in the NT server DNS directory:

- mycompany.com.dns (primary domain forward mapping file)
- 0.0.127.in-addr.arpa.dns (reverse mapping file for localhost)
- 69.5.10.in-addr.arpa.dns (primary domain reverse mapping file)
- 62.5.10.in-addr.arpa.dns (primary domain reverse mapping file)
- BOOT (boot file)
- Cache.dns (cache file)

We need to copy the primary domain files to the IFS directory

QIBM\UserData\OS400\DNS on the AS/400 system. We do not need to migrate the BOOT files since the BOOT data is in the Registry; therefore, we need to manually add the forwarders configuration after the DNS server migration.

Figure 62, Figure 63, and Figure 64 show the content of the primary domain files on the NT DNS server in our scenario.

```
;
; Database file mycompany.com.dns for mycompany.com zone.
;   Zone version:  31
;
@
IN      SOA      ntserver1.mycompany.com.      Administrator.mycompany.com. (
                                3                ; serial number
                                3600             ; refresh
                                600              ; retry
                                86400            ; expire
                                3600             ) ; minimum TTL
;
; Zone NS records
;
@
IN      NS      ntserver1.mycompany.com.
;
; Zone records
;
@
firewall      IN      MX      1      as2
firewall      IN      A       10.5.69.208
as1           IN      A       10.5.69.222
as2           IN      A       10.5.69.211
asm          IN      A       10.5.69.212
as5           IN      A       10.5.69.221
pc1           IN      A       10.5.62.200
pc2           IN      A       10.5.62.201
```

Figure 62. Contents of mycompany.com.dns File on NT Server

```

;
; Database file 69.5.10.in-addr.arpa.dns for 69.5.10.in-addr.arpa zone.
;   Zone version: 31
;
;
@           IN      SOA   ntserver1.ycompany.com. Administrator.mycompany.com. (
                        3      ; serial number
                        3600   ; refresh
                        600    ; retry
                        86400  ; expire
                        3600   ) ; minimum TTL
;
; Zone NS records
;
@           IN      NS    ntserver1.ms.com.
;
; Zone records
;
208         IN      PTR   firewall.mycompany.com.
222         IN      PTR   as1.mycompany.com.
211         IN      PTR   as2.mycompany.com.
212         IN      PTR   asm.mycompany.com.
221         IN      PTR   as5.mycompany.com.

```

Figure 63. Contents of 69.5.10.in-addr.arpa File on NT Server

```

;
; Database file 62.5.10.in-addr.arpa.dns for 62.5.10.in-addr.arpa zone.
;   Zone version: 31
;
;
@           IN      SOA   ntserver1.ycompany.com. Administrator.mycompany.com. (
                        3      ; serial number
                        3600   ; refresh
                        600    ; retry
                        86400  ; expire
                        3600   ) ; minimum TTL
;
; Zone NS records
;
@           IN      NS    ntserver1.ms.com.
;
; Zone records
;
200         IN      PTR   pc1.mycompany.com.
201         IN      PTR   pc1.mycompany.com.

```

Figure 64. Contents of 62.5.10.in-addr.arpa File on NT Server

Perform the following steps:

1. Copy the three primary domain files to the IFS directory
\QIBM\UserData\OS400\DNS on the AS/400 server.
mycompany.com.dns
69.5.10.in-addr.arpa.dns
62.5.10.in-addr.arpa.dns
2. Insert two or more spaces between Administrator.*mycompany.com*. and the parenthesis (in the SOA record in all the files you are migrating).

3. Replace the *at* (@) sign in the files by the domain name (*mycompany.com.*). Do not forget the trailing dot.

Figure 65 shows the primary domain file from the NT DNS server prepared for the *Import domain data* function. Notice that the @ sign in the original file (see Figure 62 on page 74) is replaced by *mycompany.com.* and there are extra spaces between *Administrator.mycompany.com.* and (in the SOA record).

```
;
; Database file mycompany.com.dns for mycompany.com zone.
; Zone version: 31
;
mycompany.com.      IN      SOA      ntserver1.mycompany.com. Administrator.mycompany.com. (
                    3        ; serial number
                    3600     ; refresh
                    600      ; retry
                    86400    ; expire
                    3600     ) ; minimum TTL
;
; Zone NS records
;
mycompany.com.      IN      NS       ntserver1.mycompany.com.
;
; Zone records
;
mycompany.com.      IN      MX       1      as2
firewall            IN      A        9.5.69.208
as1                 IN      A        9.5.69.222
as2                 IN      A        9.5.69.211
asm                 IN      A        9.5.69.212
as5                 IN      A        9.5.69.221
pc1                 IN      A        10.5.62.200
pc2                 IN      A        10.5.62.201
```

Figure 65. *mycompany.com.dns* File from NT Server Prepared for "Import Domain Data" Function

4.2.3 Importing the Domain Data

1. Start Operations Navigator
2. Click + next to **As1.mycompany.com.**
3. Click + next to **Network.**
4. Click + next to **Servers.**
5. Click + next to **OS/400.**
6. Double-click **DNS** to start the DNS server configuration.

The DNS server configuration wizard starts, assuming this is the first time you configure DNS server on this AS/400 system.

7. Click **Next.**
8. Click **Next** to bypass the Root servers window (there are no root servers in this scenario).
9. Select **Primary domain server.** Click **Next.**
10. Enter the primary domain name or accept the default if it is correct (Figure 66). Click **Next.**

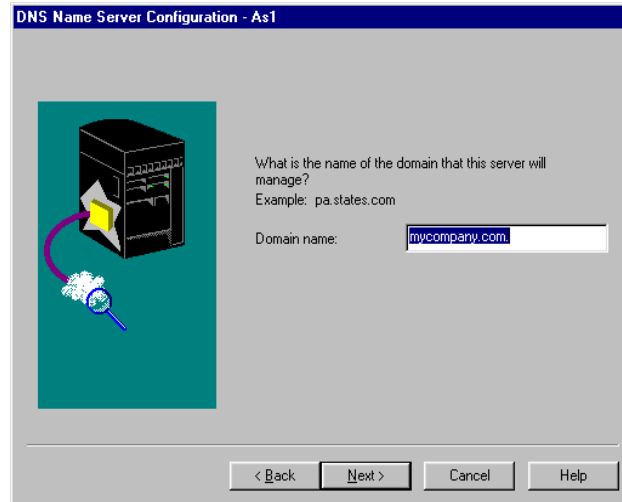


Figure 66. Primary Domain Name

11. Click **Add** to add the local host name and IP address:

Host name: localhost

IP address: 127.0.0.1

Click **OK**.

12. Click **Finish** to exit the wizard.

13. The DNS server configuration created by the wizard is displayed at this point. Double-click **Primary Domains** to view the files that the wizard created (Figure 67).

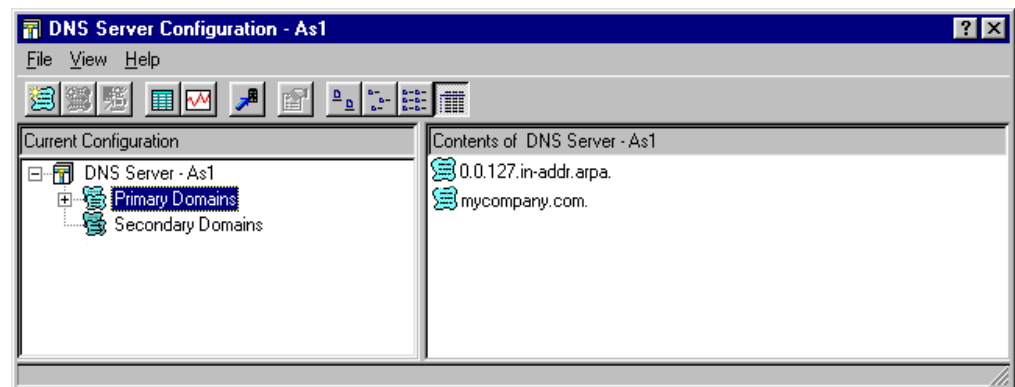


Figure 67. DNS Server Configuration Created by the DNS Configuration Wizard

14. The Import domain data function that we are running next tries to create a mycompany.com.db file. We, therefore, need to delete the mycompany.com.db file created by the wizard:

1. Right-click on **mycompany.com**.
2. Click **Delete**.
3. Click **Yes** to confirm the Delete.

Do not delete the 0.0.127.in-addr.arpa file.

15. To import the NT server DNS configuration files, right-click **Primary Domains** and select **Import domain data**.

Note: Import Domain Data flags in error "orphan" records (records not associated with a specific host name). CNAME resource records not associated with a host (with no corresponding A resource record) fall into this category.

16. Enter the name and path (or accept the default path) of the forward mapping primary domain file (Figure 68). Click **OK**.

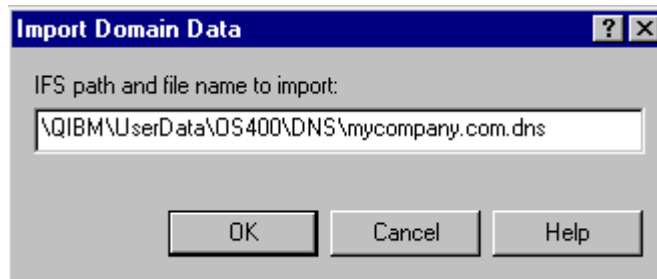


Figure 68. Importing Primary Domain Data

17. Repeat the previous step for all the primary domain files that you transferred from the NT server (**69.5.10.in-addr.arpa.** and **62.5.10.in-addr.arpa.**).

4.2.4 Configure Forwarders Manually

Since we are not migrating the BOOT file from the NT server, we need to manually add the forwarders configuration. Use the following steps:

1. From Operations Navigator DNS server configuration, right-click **As1.mycompany.com** and select **Properties**.
2. Click **Forwarders** tab.
3. Enter the IP address of the DNS server that acts as a forwarder. Verify that the box **Contact only forwarders for off-site queries** is checked (Figure 69).

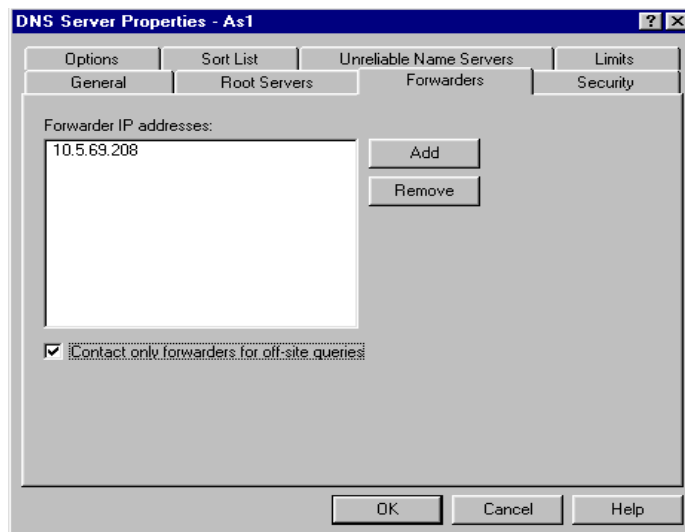


Figure 69. Adding the Firewall Secure Port IP Address to the Forwarders List

Note: Figure 69 shows the "slave" option enabled. The NT boot file does not have this box checked. The options *forward-only* directive is listed in the BOOT file since we enabled the check box *Contact only forwarders for off-site queries*.

4. Enable the domain files and start the DNS server.

Figure 70 shows the BOOT file created in the AS/400 DNS server after the migration.

```
directory /QIBM/UserData/OS400/DNS
forwarders 10.5.69.208
options forward-only
limit transfers-in 10
limit transfers-per-ns 2
primary mycompany.com mycompany.com.DB
primary 0.0.127.in-addr.arpa 0.0.127.in-addr.arpa.DB
primary 69.5.10.in-addr.arpa 69.5.10.in-addr.arpa.DB
primary 62.5.10.in-addr.arpa 62.5.10.in-addr.arpa.DB
cache . CACHE
```

Figure 70. Boot File

Figure 71 shows the *mycompany.com.db* forward mapping file after the migration. Delete the NS record with the name of the old DNS server (ntserver1 in our scenario).

```
mycompany.com. IN SOA as1.mycompany.com. Administrator.mycompany.com. (
    888347389
    3600
    600
    86400
    3600 )
;AS400OPNAV_INFO NOREVMAPDOMAIN
mycompany.com. IN NS as1.mycompany.com.
mycompany.com. IN NS ntserver1.mycompany.com.
mycompany.com. IN MX 1 as2.mycompany.com.
as1.mycompany.com. IN A 10.5.69.222
as2.mycompany.com. IN A 10.5.69.211
asm.mycompany.com. IN A 10.5.69.212
as5.mycompany.com. IN A 10.5.69.221
pc1.mycompany.com. IN A 10.5.62.200
pc2.mycompany.com. IN A 10.5.62.201
```

Figure 71. *mycompany.com.DB* File After Migration

4.3 Configuring the NT DNS Server as a Secondary DNS Server

After migrating the primary name server to the AS/400 system, it is a good idea to configure the NT server as a secondary server for backup purposes and workload balancing. In this section, we describe how to configure the NT server as a secondary DNS server for *mycompany.com* domain.

4.3.1 Deleting the Primary DNS Configuration

Before configuring the NT server as a secondary server, you must delete the primary name server configuration. Use the following steps:

1. Stop the DNS server:

Open the **Control Panel**, open **Services**, and select **Microsoft DNS Server** (Figure 72). Click **Stop** to stop the DNS server.

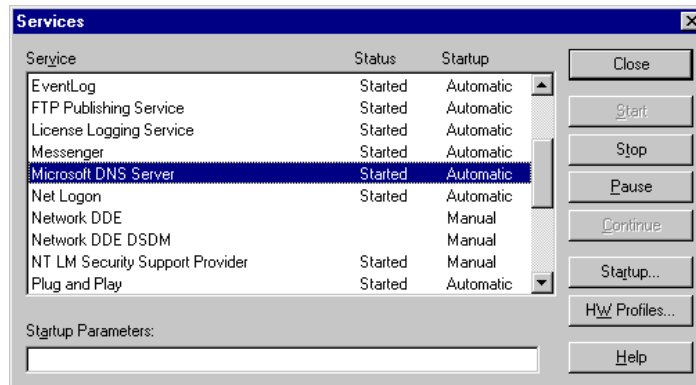


Figure 72. Stop the NT DNS Using Service Window

The Status should change to *stopped*.

2. Delete the DNS server configuration:

1. Select the Administrative Tools.
2. Select **DNS manager**.
3. Select *mycompany.com* in the *Domain Name Service Manager* window and right-click on it.
4. Select **Delete Zone** (Figure 73).
5. Click **OK** to confirm delete.

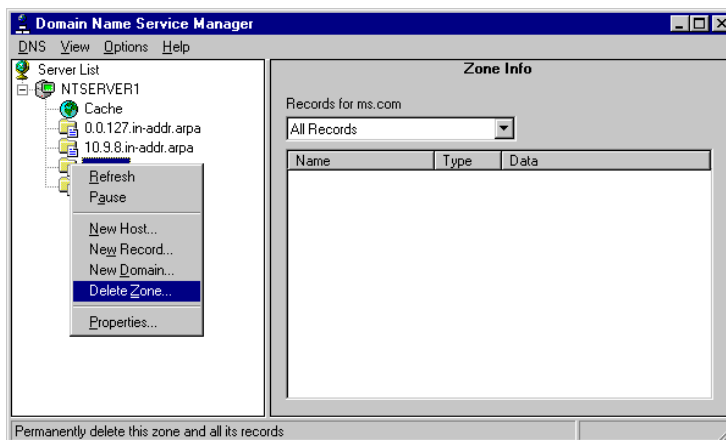


Figure 73. Delete Primary Domain Configuration Files

Repeat the previous steps to delete the other primary domain configuration files.

4.3.2 Configuring the Secondary Name Server

To configure the NT server as a secondary name server for *mycompany.com*, use the following steps:

1. Select Administrative Tools.
2. Select Domain Name Services Manager.
3. Select NTSERVER1 and right-click on it.
4. Select New Zone...(Figure 74).

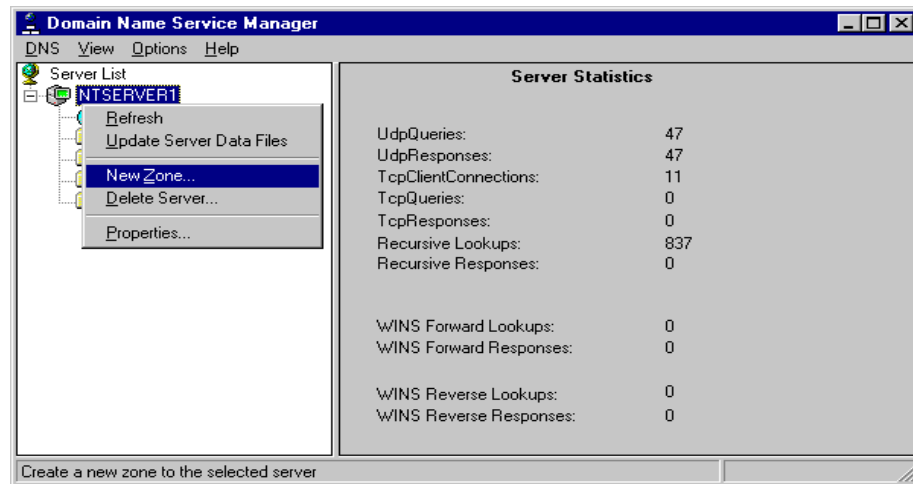


Figure 74. Create the New Zone on the NT Server

5. Select Secondary in the Creating new zone for NTSERVER1 window (Figure 75). Click **Next**.

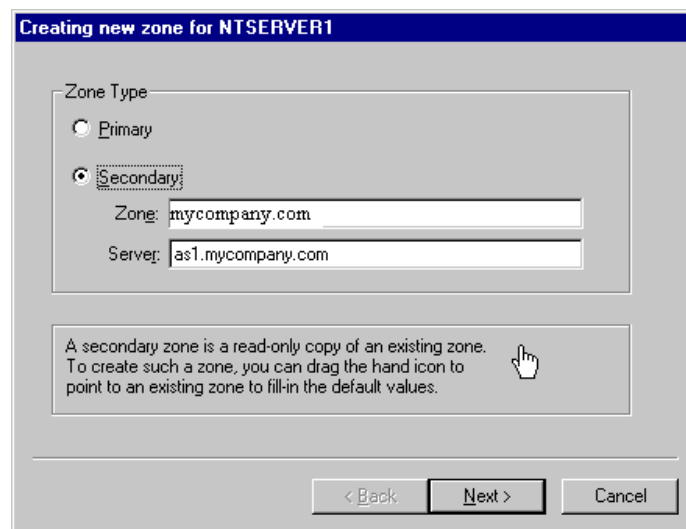


Figure 75. Creating a Secondary Domain on the NT Server

6. Enter the domain name and the name of the file the secondary server must retrieve during a zone transfer (Figure 76).

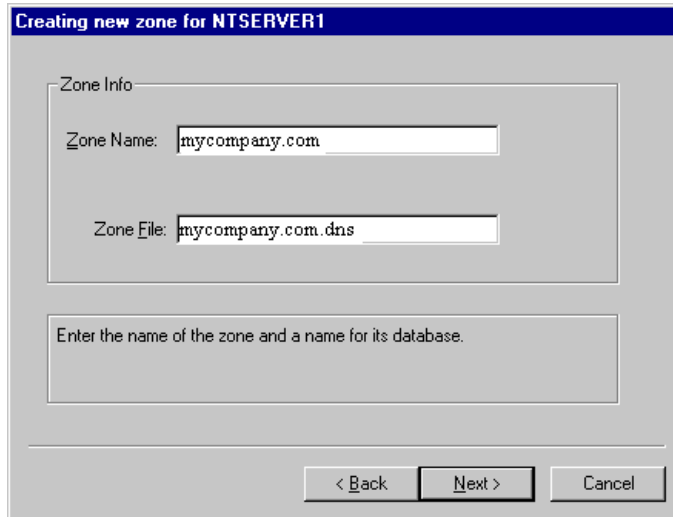


Figure 76. Specify Zone Name and Zone File

7. Specify the IP address of the primary name server, the AS/400 system AS1 in our scenario (Figure 77). Click **Next**.

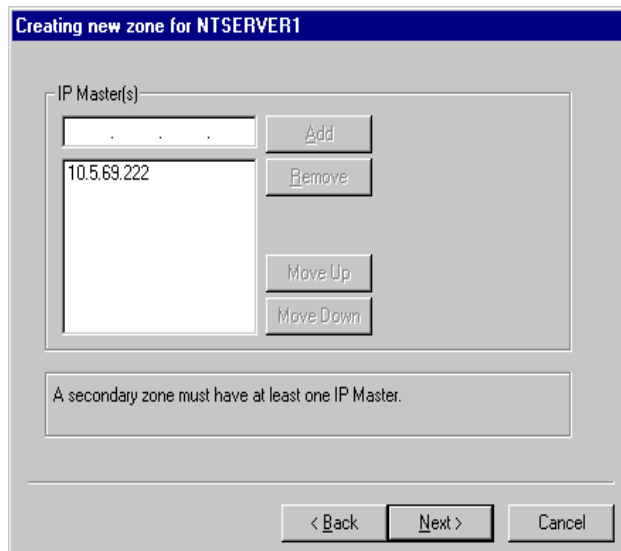


Figure 77. Specify Master Server's IP Address

8. At the final confirmation dialog box, click Finish and start the secondary DNS server.

4.4 Summary

In this chapter, we showed you how to migrate an existing primary DNS server running on an NT server to an AS/400 name server by migrating the DNS configuration files. We also explained how to configure the NT server as a secondary server.

Chapter 5. Growing Your Domain: Creating Subdomains

As your company grows or acquires new divisions, the need for grouping hosts by geographies or business units will arise. It also becomes very complex to administer the entire name space from a single point. This chapter explains how to create subdomains and, eventually, delegate administration from parents to children.

5.1 Scenario Overview

The scenario used in this chapter builds upon the scenario used in Chapter 3, “Implementing Primary and Secondary DNS Servers” on page 25. If you remember from that chapter, a primary domain server was configured on AS1 and a secondary domain server was configured on AS5. The primary domain was defined as *mycompany.com*. In this chapter, we grow the network by adding an additional subnet of 10.1.1.0. The hosts on this subnet have a domain name of *OTHERDOMAIN.mycompany.com*. See Figure 78.

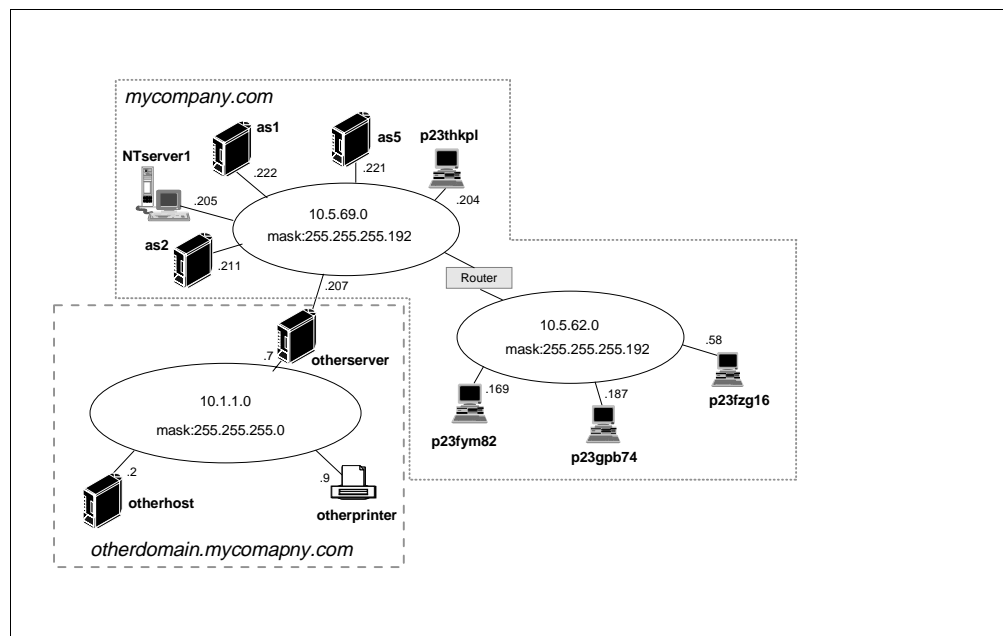


Figure 78. Network of *mycompany.com* Domain and *OTHERDOMAIN* Subdomain

In Chapter 3, we decided not to include the *OTHERSERVER* host in the *mycompany.com* domain when planning the host table migration. By excluding *OTHERSERVER*, we implied that this host belonged in a domain separate from the *mycompany.com* domain. For example, its domain is *OTHERDOMAIN.com*. The domain name space inverted tree for the scenario in Chapter 3 might look similar to the tree shown in Figure 79.

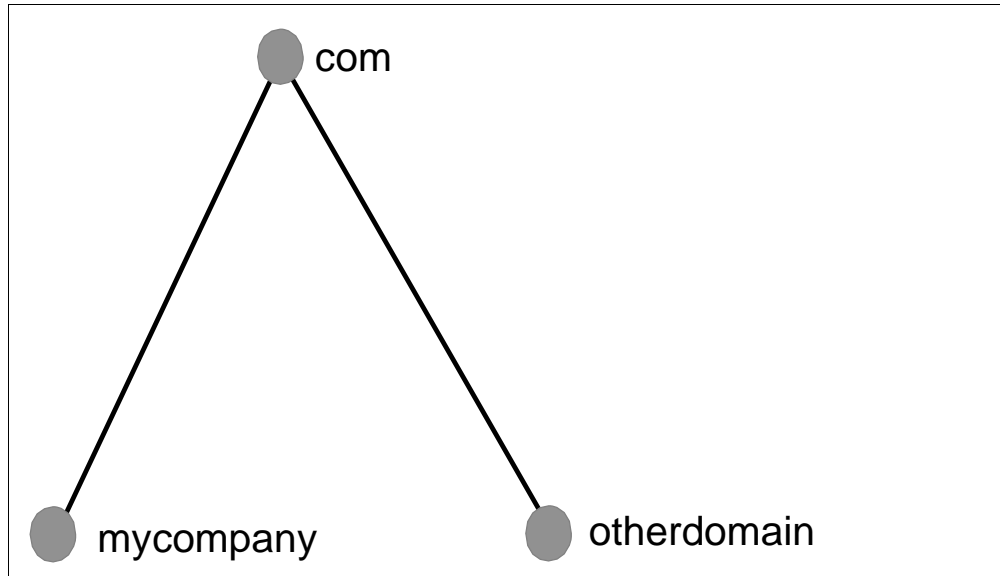


Figure 79. The Structure of Chapter 3's Scenario's Name Space

We want to introduce the subject of subdomains in this chapter. We assume that *OTHERDOMAIN.com* was purchased by *mycompany.com* and now we want it to be a subdomain of the *mycompany.com* domain. The structure of this chapter's name space looks different from Figure 79. See Figure 80 for the new structure of the name space that we use in this chapter.

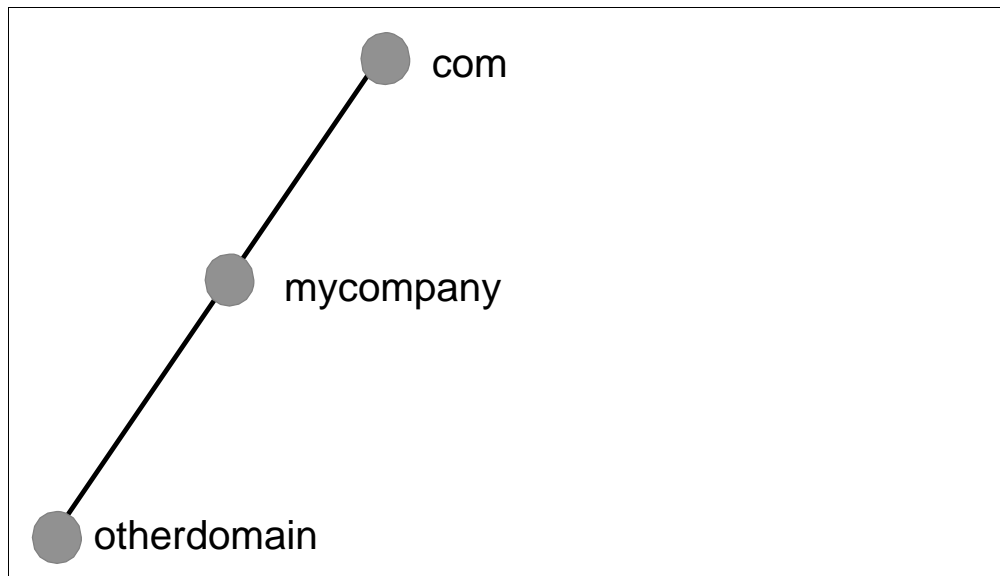


Figure 80. The Structure of This Chapter's Scenario's Name Space

Figure 80 shows that the *OTHERDOMAIN* domain is a subdomain of *mycompany.com*. The absolute domain name of *OTHERDOMAIN* is *OTHERDOMAIN.mycompany.com*. (the trailing period indicates the absolute domain, not the end of the sentence). Another way of saying this is that *OTHERDOMAIN* is now part of *mycompany.com*. Therefore, the question comes up that if this new subdomain is part of *mycompany.com*, how is the DNS server

on AS1 configured to answer queries about the new hosts in *OTHERDOMAIN.mycompany.com*? There is more than one answer to this question. This chapter outlines two methods of including the hosts in *OTHERDOMAIN.com* under *OTHERDOMAIN.mycompany.com*. for the purposes of DNS.

To understand the difference between the two methods of including *OTHERDOMAIN.com* in *mycompany.com*, you need to understand the concept of a zone of authority and the difference between a domain and a zone as described in Chapter 1, “Domain Name System Concepts and Overview” on page 3.

In Method 1, we propose to maintain one zone of authority over all of *mycompany.com* including *OTHERDOMAIN.mycompany.com*. This means that the AS1 name server is authoritative over all of *mycompany.com*. The grayed rectangle in Figure 81 represents the *mycompany.com* zone of authority. This zone of authority does include the *OTHERDOMAIN.mycompany.com* subdomain. Remember the *OTHERDOMAIN.mycompany.com* subdomain is part of *mycompany.com* domain.

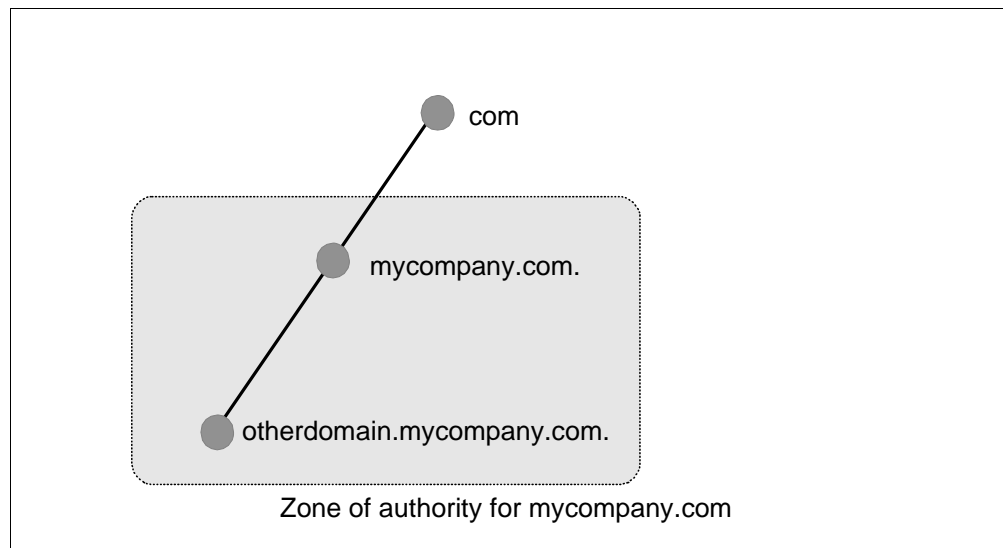


Figure 81. Method 1: One Zone of Authority for *mycompany.com*.

Another way of saying this is that the AS1 name server is responsible for answering queries for every host within the grayed rectangle in Figure 81. Consequently, the DNS administrator for AS1 is responsible for maintaining the DNS configuration for any changes in the network that are included within the grayed rectangle in Figure 81.

But let's consider the situation in which the *OTHERDOMAIN.mycompany.com* subdomain starts growing and many hosts are added to the *OTHERDOMAIN.mycompany.com* subdomain. What if the AS1's DNS administrator does not have time to configure new *OTHERDOMAIN.mycompany.com* hosts in the DNS configuration on AS1 and wants to have the *OTHERDOMAIN.mycompany.com* subdomain hosts maintained on another DNS server and have another DNS administrator maintain the growing *OTHERDOMAIN.mycompany.com* subdomain? This is called delegating authority, which is described by Method 2.

In Method 2, we propose to delegate the authority of the *OTHERDOMAIN.mycompany.com* subdomain out of *mycompany.com*'s zone of authority to create two zones of authority. These two zones are represented by two separate grayed rectangles in Figure 82. The AS1 DNS server is authoritative over the *mycompany.com* zone and a new DNS server is authoritative over the *OTHERDOMAIN* zone as shown in Figure 82.

Remember that the *OTHERDOMAIN.mycompany.com* subdomain is still part of the *mycompany.com* domain, even with a Method 2 configuration.

So far in Chapter 3, "Implementing Primary and Secondary DNS Servers" on page 25 and this chapter, we have used the terms of primary domain, secondary domain, primary name server, secondary name server, and authoritative. Let's review the definitions of these terms:

- Primary name server - This server is the server that the hosts in the zone of authority are configured on. It is the server that the DNS administrator configures and maintains. When this server gives responses to queries from its primary domain files, the responses are called authoritative.
- Secondary name server - This server has the same information on it as the primary name server. However, instead of getting its information directly from the DNS administrator configuring it, it gets its information from the primary server through zone transfers over the network. A secondary name server is used for two reasons: spreading the DNS query workload over more than one server and as a backup. When the secondary name server gives out a response to a query, the response is also called authoritative. In other words, an answer from a secondary name server is considered to be just as "good" as if the answer came from a primary name server.
- Primary domain files - These files are the files configured on the primary name server.
- Secondary domain backup files - These files contain information that was acquired from zone transfers from the primary name server. They exist on the secondary name server. These files only exist if you checked the box *Save copies of master server data* when configuring the secondary domain. This checkbox specifies whether you want to backup the domain data that this secondary server receives from the primary domain server. The advantage of backing up the domain data is that the secondary server can function even if the primary server is down. If you do not check this box, the zone transfer information only exists in cache. When the secondary server boots, it checks first to see if a backup exists. If it does, it automatically loads the backup file. It then contacts the primary server to see if the primary server has more recent data. If the data is more recent, then the secondary server loads that data from the primary server through a zone transfer.
- Authoritative - A server that is considered to be authoritative for a domain is either the primary server for that domain or a secondary server for that domain. In Chapter 3, "Implementing Primary and Secondary DNS Servers" on page 25, both AS1 and AS5 name servers are authoritative for the *mycompany.com* domain. If another name server or a client queries either AS1 or AS5 for information in the *mycompany.com* domain, the response is considered to be authoritative. Can a name server that is not authoritative over a domain give a response to a client about that domain and have that response considered an authoritative response? The answer is yes. If the non-authoritative server does not know the answer and queries an authoritative name server on behalf of the client and then returns the answer

to the client, this response is considered to be authoritative. The non-authoritative name server will cache this information. If a second client requests this same information from the non-authoritative name server (and this information is still in its cache), the name server gives the response to the client but now this same information is labeled non-authoritative. Why? Because the information in the response this second time came out of the name server's cache. Another way of saying this is that a non-authoritative response at some point came out of a name server's cache.

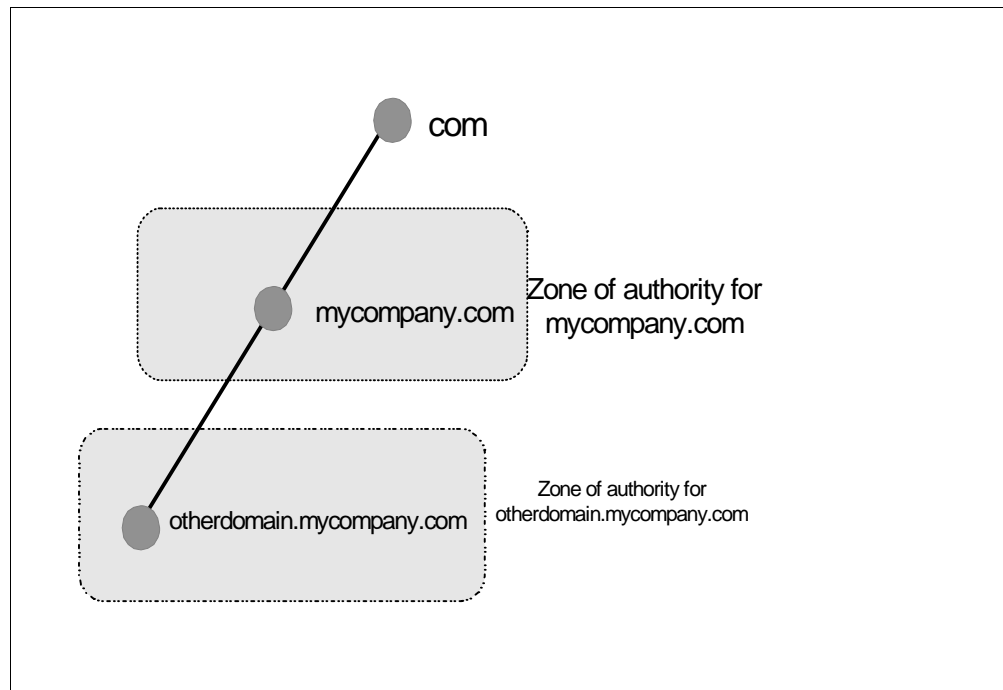


Figure 82. Method 2: Two Zones of Authority: *mycompany.com* Zone and *OTHERDOMAIN* Zone

5.1.1 Scenario Objectives

In this scenario, we have the following objectives:

1. **Method 1:** Create a subdomain *OTHERDOMAIN.mycompany.com* within the domain of *mycompany.com*, keeping authority within *mycompany.com*. Either the primary DNS on AS1 or the secondary DNS on AS5 responds to DNS queries.
2. **Method 2:** Delegate authority of the subdomain *OTHERDOMAIN.mycompany.com* to a child DNS server, which, in this scenario, is *OTHERHOST*.
3. Test Method 2 configuration with *nslookup*.
4. Explain how the network's mail configuration may change with Method 2.
5. Explain how a DNS server will answer a forward mapping query for a multi-homed host (for example, *OTHERSERVER*).

5.1.2 Scenario Advantages

In this scenario, we must consider the advantages of keeping centralized control (Method 1) and the advantages of delegating authority (Method 2).

Advantages of Keeping Authority Over Subdomain Otherdomain

When a network is not too large, the simplest way to add a subdomain is to include it in the primary domain's zone. This means that the primary domain's administrator (*mycompany.com*'s DNS server administrator on AS1) is responsible for the DNS configuration of hosts in *OTHERDOMAIN.mycompany.com*. The same name server (AS1) answers DNS queries for hosts in both *mycompany.com* and its subdomain, *OTHERDOMAIN.mycompany.com*. Control over the DNS configuration of *OTHERDOMAIN.mycompany.com* remains in the hands of the same DNS administrator and the *OTHERDOMAIN.mycompany.com* DNS configuration remains on the same name server, AS1.

Advantages of Delegating Authority of Otherdomain

When a network becomes large and administering the DNS configuration of the zone becomes too much workload for one person, then delegating authority is the recommended technique to spread the administrative workload across more than one person and name server.

5.1.3 Scenario Disadvantages

In this scenario, we must consider the disadvantages of keeping centralized control (method 1) and the disadvantages of delegating authority (method 2).

Disadvantages of Keeping Authority Over Subdomain Otherdomain

If the subdomain *OTHERDOMAIN.mycompany.com* becomes very large, it may not be practical to have one DNS administrator maintain the *mycompany.com*'s zone of authority, which, in this case, includes the subdomain of *OTHERDOMAIN.mycompany.com*.

It is tempting to add a subdomain to the original primary domain and keep authority with the thought that if the administration gets to be too much workload for one person, then we delegate authority later. Although this is possible, keep in mind that the administration work of adding *OTHERDOMAIN* hosts to the primary DNS domain files must be repeated on another server at a future delegation time. In other words, there is no automated way to "port" *OTHERDOMAIN.mycompany.com*'s hosts from the parent DNS server to the child DNS server.

Disadvantages of Delegating Authority of Otherdomain

Delegating part of the zone of authority away means that another name server is required to become the primary DNS server for the *OTHERDOMAIN.mycompany.com*. In our scenario, an AS/400 system on the 10.1.1.0 network becomes the primary DNS server for *OTHERDOMAIN.mycompany.com* while AS1 continues to be the primary server for the remaining zone of authority of *mycompany.com*. If an additional host with DNS capability does not exist in the network, delegation of part of the *mycompany.com*'s zone of authority is not possible.

Delegation also implies that there is another DNS administrator with the necessary skill to maintain the new zone of authority. A person with these skills must be available to take over the workload of administering the new zone of authority or a new person must be trained to perform this task. If the *OTHERDOMAIN.mycompany.com* subdomain is delegated and the primary domain files for *OTHERDOMAIN.mycompany.com* are located on another server

(the child server) but maintained by the same DNS administrator, you have defeated the purpose of delegation. Delegating implies delegating the workload of administration. If the only purpose of adding a new server is to handle some of the DNS workload and to back up the primary, a secondary server should be used; this was explained in Chapter 3.2.6, “Creating a Secondary DNS Server” on page 57.

Delegating authority requires you to maintain a system of internal roots and to understand a more complicated setup.

5.1.4 Scenario Network Configuration

As you can see in Figure 83, the network is similar to the network in Chapter 3, “Implementing Primary and Secondary DNS Servers” on page 25 (see Figure 14 on page 27) with the exception that we added the subnet 10.1.1.0 with a subnet mask of 255.255.255.0. Hosts in this subnet belong to the domain *OTHERDOMAIN*, which is a subdomain of *mycompany.com*. Hosts in the 10.1.1.0 network have an absolute domain name of *OTHERDOMAIN.mycompany.com*.

With Method 1 described in Section 5.1 on page 83, all hosts pictured in Figure 83 are configured in the AS1 primary name server. AS5 remains the secondary name server to AS1.

With Method 2 described in Section 5.1 on page 83, the hosts located in the domain *OTHERDOMAIN.mycompany.com* are configured in a child DNS server called *OTHERHOST* (IP address 10.1.1.2). The majority of this chapter is devoted to the configuration steps necessary to implement Method 2.

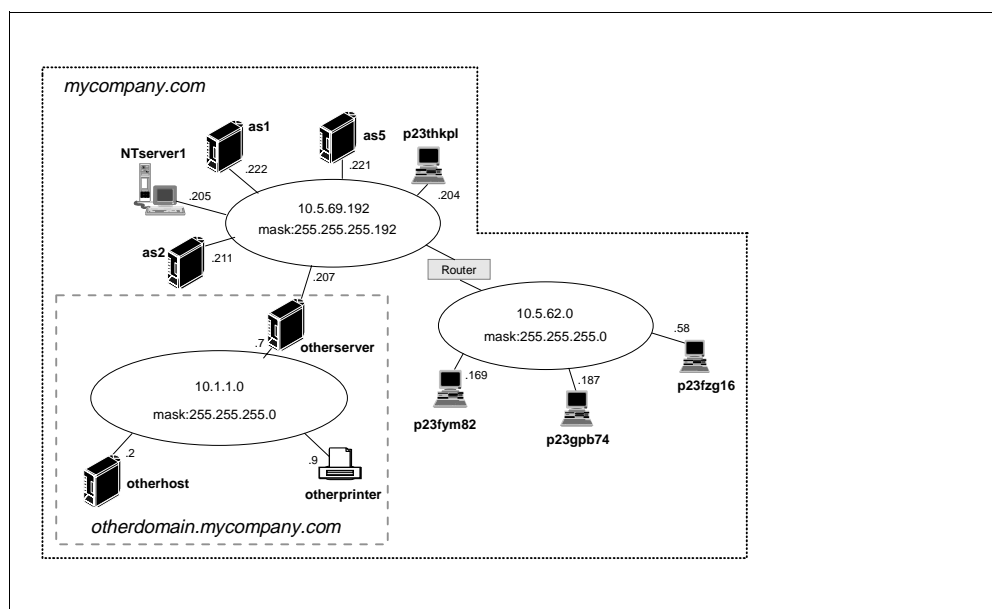


Figure 83. Detailed Network Diagram of mycompany.com domain

5.2 Task Summary

The tasks required to complete this scenario do not include the TCP/IP configuration on the AS/400 system, nor does it include configuring the first DNS

server in the network. This scenario builds on what was already configured in Chapter 3.

This chapter is divided into two major sections: Method 1 and Method 2. As we see in the planning section, Method 1 versus Method 2 is really an either/or situation. A DNS administrator must choose which one of the two methods to use. For clarity, we divide the task summary into two main sections: one for Method 1 and one for Method 2. Most of this chapter is devoted to the configuration for Method 2 because it is more complicated.

Overall Task Summary

- Planning to subdomain:

This section describes the subdomain two methods as they pertain to DNS configuration. This section also covers the consequences of choosing Method 1 and later changing to Method 2.

- Method 1:
 1. Configure the AS1 primary name server.
 2. Configure the AS5 secondary name server.
- Method 2:
 1. Configure AS1 as internal root server.
 2. Remove the configuration for Method 1 from the AS1 primary name server.
 3. Configure AS1 to delegate the *OTHERDOMAIN.mycompany.com* subdomain.
 4. Configure AS1 to delegate the 1.1.10.in-addr.arpa subdomain.
 5. Configure *OTHERHOST* to be authoritative for the primary domains *OTHERDOMAIN.mycompany.com* and 1.1.10.in-addr.arpa.
 6. Configure the internal root server for *OTHERHOST* to be AS1.
 7. Reconfigure hosts located in the *OTHERDOMAIN.mycompany.com* subdomain.
 8. Verify the configuration for Method 2 with nslookup.
 9. Configure changes to the AS5 secondary name server.
 10. Configure *OTHERHOST* to be the *OTHERDOMAIN.mycompany.com*'s mail server.
 11. Configure changes to *OTHERHOST* DNS server.
 12. Configure changes to *OTHERHOST* TCP/IP and SMTP configuration.
 13. Configure changes to AS1 (*mycompany.com*'s mail server) TCP/IP configuration.
 14. Explain Round Robin/Address Sorting.

5.3 Planning to Subdomain

When adding a subdomain within a domain, you need to decide as early as possible whether the subdomain will be maintained in the zone of authority of the primary domain or if the authority of this subdomain should be delegated and an additional zone of authority created.

5.3.1 Defining the Zone of Authority

The importance of planning when getting ready to subdomain is best explained by an example. Let's imagine that the *OTHERDOMAIN* subdomain has just been added to the domain of *mycompany.com*. And for the sake of this example, let's imagine that the *OTHERDOMAIN.mycompany.com* subdomain contains 100 hosts.

With Method 1 where the subdomain *OTHERDOMAIN.mycompany.com* is included in the *mycompany.com*'s zone of authority, the DNS administrator needs to add an A record for each of the 100 hosts. This is added into the forward mapping file of *mycompany.com* on the primary server AS1. See Figure 84.

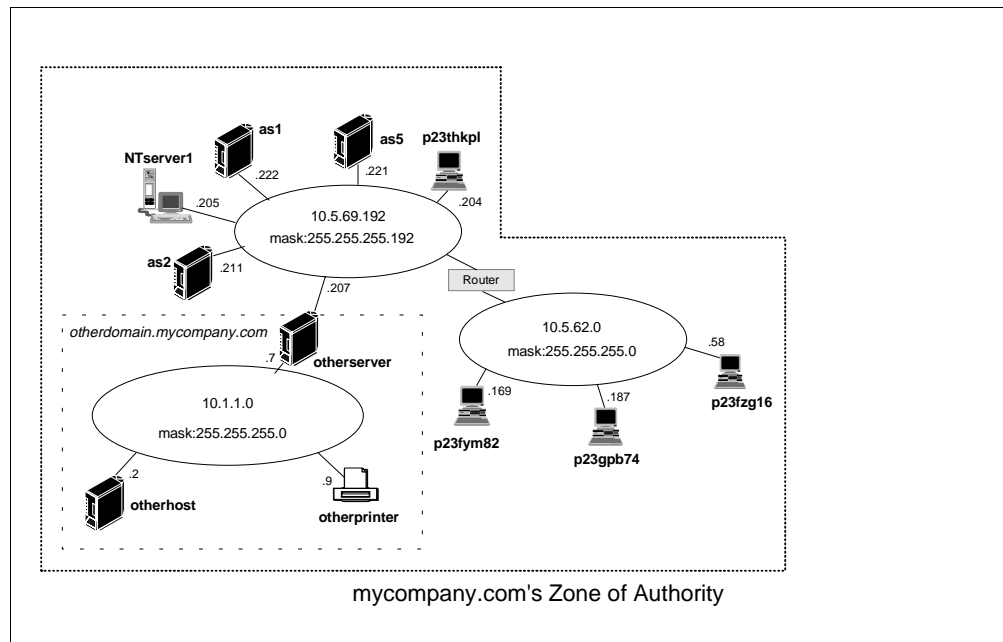


Figure 84. Method 1's Network Diagram Showing *mycompany.com*'s Zone of Authority

Later in time, the DNS administrator decides to delegate the authority of the *OTHERDOMAIN.mycompany.com* subdomain to another server for a second DNS administrator to maintain (earlier in the chapter, we described this as Method 2).

This requires two zones of authority. The first zone of authority is *mycompany.com* and does not include any hosts belonging in the *OTHERDOMAIN.mycompany.com* subdomain. The second zone of authority is the *OTHERDOMAIN.mycompany.com*'s zone of authority. This zone contains all the hosts in the *OTHERDOMAIN.mycompany.com*'s subdomain. See Figure 85.

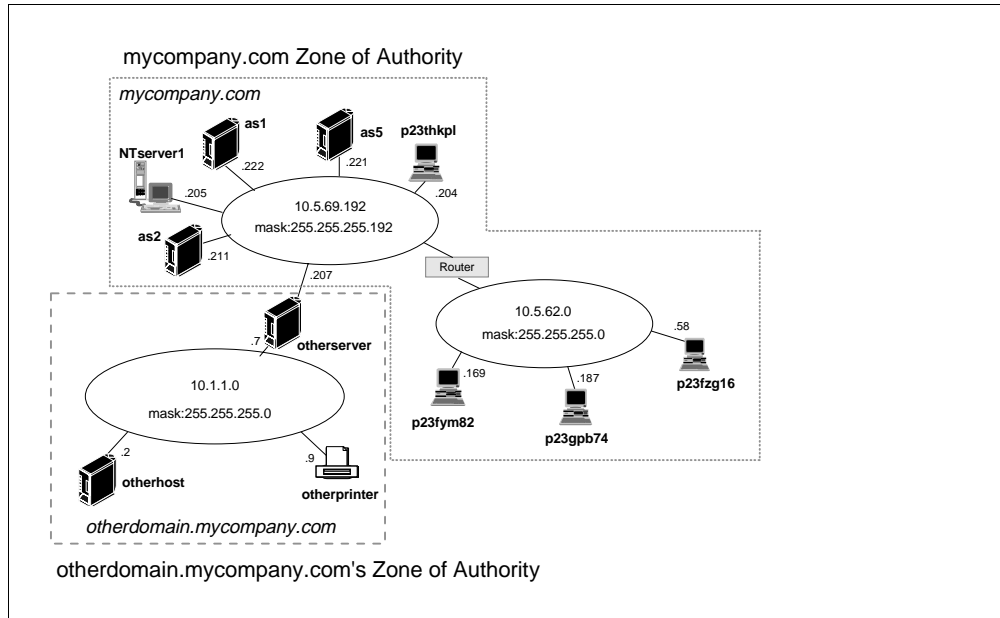


Figure 85. *OTHERDOMAIN* Subdomain as a Second Zone of Authority

To go from Method 1 to Method 2, you need to follow these steps:

1. The parent DNS server (AS1) must be configured to be aware of the child DNS server. We describe how to do this later in the chapter.
2. The new child server that now contains the primary domain file for the *OTHERDOMAIN.mycompany.com* subdomain needs to have all 100 A records added for the 100 hosts within *OTHERDOMAIN.mycompany.com* subdomain. Also, if *OTHERDOMAIN.mycompany.com* has a separate mail server other than the mail server in *mycompany.com*, an MX record must be added.
3. The parent server needs to have those 100 A records for hosts belonging to the *OTHERDOMAIN.mycompany.com* subdomain deleted.

The work involved in step 3 can be avoided by deciding to use Method 2 from the beginning. Method 2 requires an additional server and an additional DNS administrator. If these requirements are satisfied, consider configuring for Method 2 while you are adding subdomains. It is less work to go directly to Method 2 when adding a subdomain than it is to configure Method 1 and later reconfigure for Method 2.

5.4 Method 1: Adding a Subdomain and Maintaining Authority

In this section, we discuss how to add hosts in *OTHERDOMAIN.mycompany.com* to the *mycompany.com* primary DNS file on the primary DNS system AS1. The absolute domain name of these hosts is *OTHERDOMAIN.mycompany.com*. The configuration steps for Method 1 consist of simply adding new hosts to the primary DNS configuration except that when we specify the domain name of the host, it is *OTHERDOMAIN.mycompany.com*.

As you can see in Figure 83 on page 89, the *OTHERDOMAIN.mycompany.com* subdomain consists of three hosts: *OTHERSERVER*, *OTHERPRINTER*, and *OTHERHOST*. We must add these three hosts to the primary domain of *mycompany.com*, and to the

appropriate in-addr.arpa primary domain on the primary name server, AS1. In this scenario, these three hosts reside on a new network of 10.1.1.0 (subnet mask of 255.255.255.0) so we must also add a new primary domain of 1.1.10.in-addr.arpa on AS1.

In Method 1, we perform most configuration steps on the primary name server AS1. As in Chapter 3, “Implementing Primary and Secondary DNS Servers” on page 25, the secondary name server is AS5. The AS5 secondary server requires some configuration change that we cover in Section 5.4.2 on page 95.

5.4.1 Configure AS1 Primary Name Server

The configuration steps to add the new subdomain hosts to the primary server AS1 are as follows:

1. Start Operations Navigator AS1's DNS server configuration.
2. On the **General** tab of *mycompany.com*'s **Properties** page, make sure the *Create and delete reverse mappings by default* field is checked. This causes the 1.1.10.in-addr.arpa primary domain file to be automatically created and the PTR record to be automatically added in the 1.1.10.in-addr.arpa primary domain file when we manually add new hosts in the *mycompany.com* primary domain file.
3. Click **OK**.
4. Right click *mycompany.com* primary domain file.
5. Click **New Host**.
6. Click **Add**.
7. Enter a host name of *OTHERSERVER.OTHERDOMAIN.mycompany.com* (remember to include the trailing dot after *com*).
8. Enter *OTHERSERVER*'s first IP address of 10.1.1.7
9. Click **OK**.
10. Highlight the host *otherserver.otherdomain.mycompany.com* (right panel under Contents of DNS server - AS1.*mycompany.com*), right click on it, and select **Properties**. The **General** tab is displayed. We need to perform steps 9 through 13 for the host *OTHERSERVER* because it has two IP addresses, one in the 10.5.69.192 network and one in the 10.1.1.0 network. See Figure 83 on page 89. We want the AS1 name server to be aware of both *OTHERSERVER*'s IP addresses.
11. Click **Add**.
12. Enter the host *OTHERSERVER*'s second IP address: **10.5.69.207**.
13. Click **OK**. Steps 9 through 13 are not necessary for the two remaining hosts in the *OTHERDOMAIN.com*. subdomain because each of those hosts only has one IP address.
14. Click **OK** to finish adding the new host. Note that the reverse mapping file of 1.1.10.in-addr.arpa has been automatically created.
15. Repeat steps 4 through 8 to add hosts *OTHERHOST* and *OTHERPRINTER*. Do not perform steps 9 through 13; click **OK** a second time to finish adding each new host.
16. Right click the 1.1.10.in-addr.arpa file.
17. Click **Enable**.
18. If the AS1 name server is already started, then click on the **Update Server** smart icon to restart the name server to pick up the changes.

Or, if the name server is stopped, close the DNS configuration window to save the configuration. Right click **DNS** and click **Start** to start the DNS server if it is not already started.

Figure 86, Figure 87, and Figure 88 show the contents of *mycompany.com* primary domain file, the 1.1.10.in-addr.arpa primary domain file, and the 69.5.10.in-addr.arpa primary domain file. Steps 1 through 18 changed the contents of these three files from what they were after doing the configuration steps in Chapter 3, “Implementing Primary and Secondary DNS Servers” on page 25.

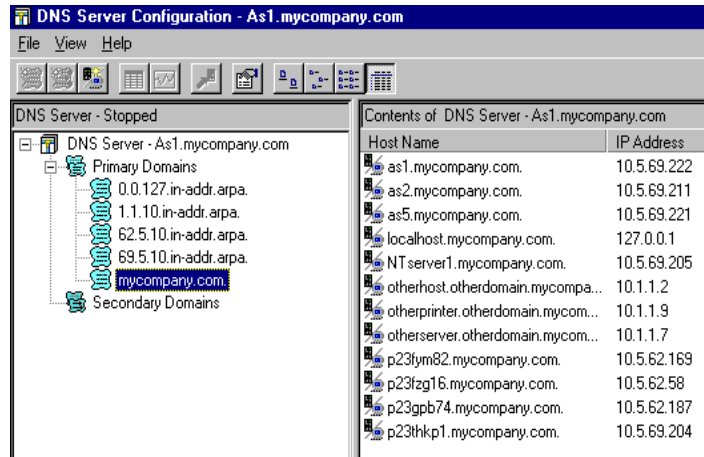


Figure 86. *mycompany.com* Domain File After Adding OTHERDOMAIN.mycompany.com Hosts

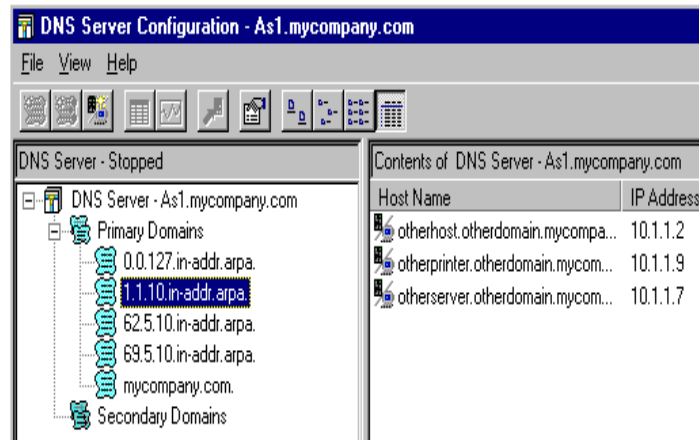


Figure 87. 1.1.10.in-addr.arpa Domain File After Adding OTHERDOMAIN.mycompany.com Hosts

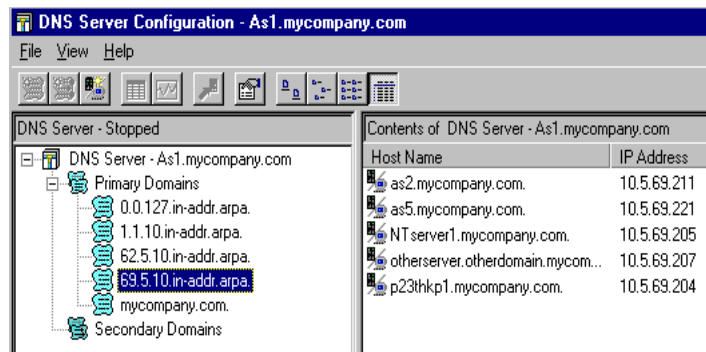


Figure 88. 69.5.10.in-addr.arpa Domain File After Adding OTHERDOMAIN.mycompany.com Hosts

5.4.2 Configure the Secondary Name Server As5

The secondary name server must reflect the changes made to the primary domain files on the primary name server AS1.

mycompany.com Domain File

In Section 5.4.1, “Configure AS1 Primary Name Server” on page 93, we added hosts to the primary forward mapping domain file *mycompany.com*. In Section 3.2.6, “Creating a Secondary DNS Server” on page 57, we configured the secondary forward mapping domain file *mycompany.com* on the secondary name server AS5. Since *mycompany.com* is already configured on the secondary name server the changes we made to *mycompany.com* on AS1 are picked up by AS5 in the next zone transfer.

New 1.1.10.in-addr.arpa File

In Section 5.4.1, “Configure AS1 Primary Name Server” on page 93, a new reverse mapping primary domain file is automatically created for us on AS1: the 1.1.10.in-addr.arpa file. This is because the new hosts we added to *mycompany.com* are located on a network that is new to the AS1 DNS server. Since this is a new primary domain file, we need to configure this domain file as a secondary domain file on the secondary name server AS5 so this new primary domain can be zone transferred. The steps on how to add a new secondary domain are covered in Section 3.2.6.1, “Configuring the Secondary Server AS5” on page 57. Now we must configure a new secondary domain on AS5, 1.1.10.in-addr.arpa, and the IP address of the master name server remains the IP address of AS1, 10.5.69.222.

Refreshing the Secondary Name Server As5

With the default secondary server refresh interval of three hours (see Section 3.2.6.4, “Controlling Zone Transfer Frequency” on page 60 for an explanation of this timer), the AS5 secondary name server picks up the changes to AS1 within three hours, assuming that the primary name server AS1 is started.

Tip

If the DNS administrator determines that three hours is too long to wait for the refresh of the secondary name server files, a zone transfer can be forced by running the Update Server function or stopping and starting the AS5 secondary name server.

5.5 Method 2: Adding a Subdomain and Delegating Authority

This section discusses how to group hosts in *OTHERDOMAIN.mycompany.com* into a separate primary domain file and how to administer the subdomain on a different DNS server called a child server. By doing this, you are creating a second zone of authority that includes *OTHERDOMAIN.mycompany.com*. The original zone of authority is *mycompany.com*, but, unlike Method 1, in this section, the *mycompany.com*'s zone of authority does not include the *OTHERDOMAIN.mycompany.com* subdomain. However, keep in mind that *OTHERDOMAIN.mycompany.com* is still a subdomain of *mycompany.com* regardless of what method you use.

5.5.1 Configuring AS1 as Internal Root

In this method, you are creating an independent name space that contains information about your company. The assumption is that the *mycompany.com* domain is growing into multiple subdomain and zones with multiple name servers authoritative for each zone.

Tip

You can use internal root name servers if you don't need to make the Internet name space available to your users. Internal root name servers allow name servers all over your company to locate and query each other. However, creating internal roots creates an independent name space for your company and are recommended for large networks, with **no** Internet connectivity.

The first step is to establish an *internal root name server* or *internal root*. The internal roots contain delegation to your main forward mapping domains and *in-addr.arpa* domains. Internal roots allow your internal name servers to find each other.

An internal root delegates to any internal domain. In method 2, the parent name server (AS1), delegates *OTHERDOMAIN.mycompany.com* to the child name server, *otherhost.OTHERDOMAIN.mycompany.com*. Therefore, the internal root only needs to delegate to the parent server.

If you have multiple subdomains and multiple zones administered by multiple name servers that are not in a parent/child relationship, the internal root delegates directly to any domain that you administer. See Chapter 15 in *DNS and BIND* by Albitz & Liu for more information.

Any internal name server can run an internal root and be an authoritative name server for other zones. In this scenario, AS1 runs the internal root and, at the same time, is the primary DNS server for *mycompany.com*.

Perform the following steps on AS1 to configure the internal root name server:

1. From Operations Navigator *DNS Server Configuration* right click **Primary Domains**.
2. Select **New Primary Domains**.
3. Select **General** tab.
4. In the *Domain name field* enter a dot (.).

5. Leave the box *Create and delete reverse mappings by default* unchecked.
6. Select the **Secondary Name Servers** tab.

Tip

Remember, here you are *not* configuring secondary DNS servers; you are actually delegating internal subdomains to internal name servers. The *Secondary Name Servers* tab is the Operations Navigator interface to add NS records to the DNS configuration file.

7. Add the internal domain names and corresponding host name of the name server authoritative for each internal domain. In this scenario, you only need to add the parent domains.

The internal root must delegate also the *in-addr.arpa* domains.

Add the internal domains under AS1 zone of authority as shown in Figure 89. Click **OK**.

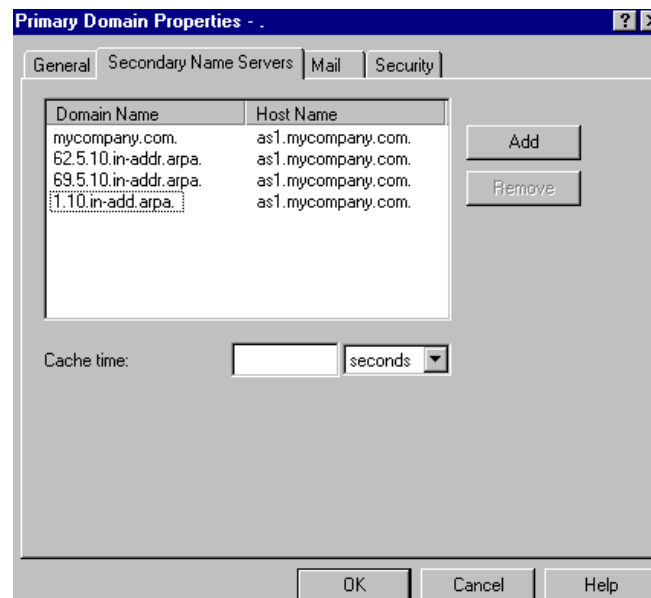


Figure 89. Internal Root Delegating Internal Domains

8. Right click on the internal root primary domain represented by a dot (".").
9. Select **New Host**.
10. Enter the host name and IP address of the parent name server:

as1.mycompany.com 10.5.69.222

Click **OK**.

Figure 90 shows the parent name server configuration in the internal root.

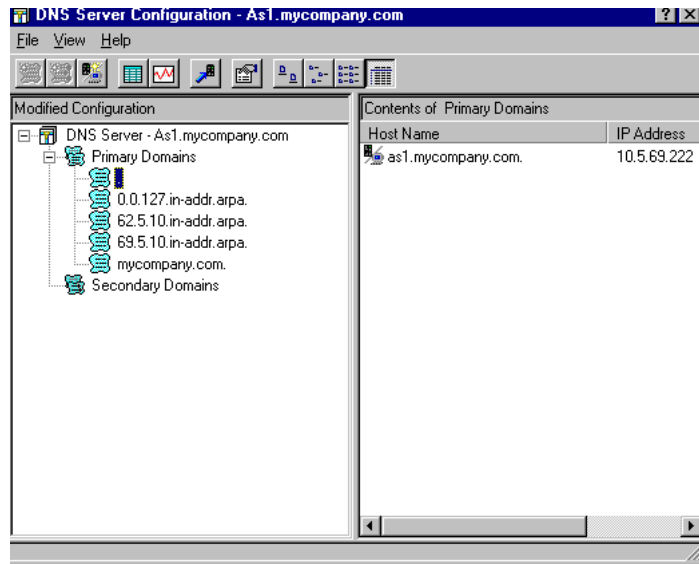


Figure 90. Internal Name Server in Internal Root

5.5.2 Removing Subdomain Configuration from the Parent Server AS1

If you initially used Method 1 to create subdomain *OTHERDOMAIN.mycompany.com* and maintain authority on AS1's DNS server, you need to reverse the configuration steps outlined in Method 1 from AS1's DNS primary domain files: *mycompany.com*, *1.1.10.in-addr.arpa* and *69.5.10.in-addr.arpa* files. Because we delegate authority of the *OTHERDOMAIN.mycompany.com*'s subdomain to the child server *OTHERHOST*, the host records for hosts in the *OTHERDOMAIN.mycompany.com* subdomain no longer belong on AS1's DNS server (the parent) but belong on *OTHERHOST*'s DNS server (the child).

Perform the following steps on AS1, the parent server:

1. Start AS1's DNS server configuration in Operations Navigator.
2. Double-click **Primary Domains**.
3. Click **on** *mycompany.com* primary domain file to highlight it. The list of hosts configured within this file appear in the right window.
4. Right click ***mycompany.com***.
5. Click **Properties**.
6. Confirm that *Create and delete reverse mapping by default* is enabled; check it.
7. Click **OK**.
8. Double-click on the ***mycompany.com*** primary domain file.
9. Right click *OTHERHOST.OTHERDOMAIN.mycompany.com*.
10. Click **Delete** to remove this host from the *mycompany.com* primary domain file. See Figure 91.

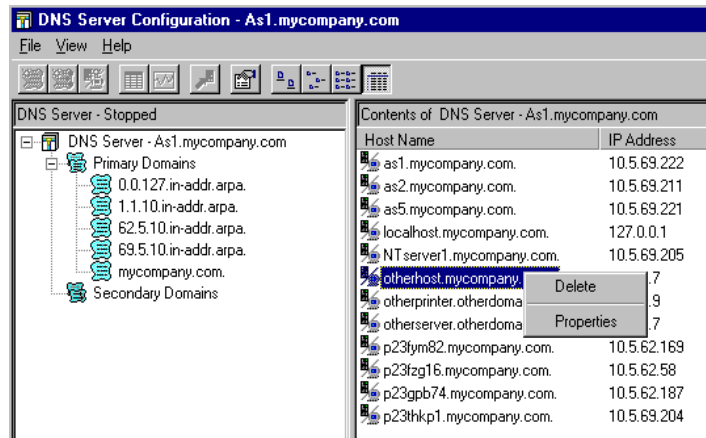


Figure 91. Deleting OTHERHOST host From mycompany.com Primary Domain File

11. Click on **Yes** to confirm the delete operation. The host `OTHERHOST` is removed from the `mycompany.com` file and the PTR record in the `1.1.10.in-addr.arpa` file for `OTHERHOST` host is automatically deleted.
12. Repeat steps 9 through 11 to delete the remaining `OTHERDOMAIN` hosts contained in the `mycompany.com` primary domain file: `OTHERSERVER` and `OTHERPRINTER`.
13. Notice that the `1.1.10.in-addr.arpa` is empty but the file still exists. If you click on this primary domain file to display its contents, you find that it now contains no records. However, since all the hosts residing on the `10.1.1.0` network are part of the `OTHERDOMAIN.mycompany.com` subdomain, we do not want this primary domain file on the parent server, AS1. Right click on **1.1.10.in-addr.arpa** and click on **Delete** followed by **Yes** to confirm the delete. We are not finished with the AS1 configuration for Method 2 so do not close the DNS window just yet. Continue on to the next section.

5.5.3 Delegating the Subdomain on the Parent Server AS1

Perform the following steps on AS1 also, which is the primary DNS server for `mycompany.com` domain. We also refer to this name server as the parent server.

14. Right click the `mycompany.com` file and select **Properties**. On the **General** tab, disable the *Create and delete reverse mappings by default*. You do this by making sure the X is not in the check box. Do not click OK just yet.
Note: The previous step is important. We are creating an A record for the child server in the subsequent steps and we do not want the corresponding `in-addr.arpa` file to be created on the parent server AS1.
15. Click the **Secondary Name Servers** tab (you still should be in `mycompany.com`'s Properties page).
16. Click **Add**.
17. Enter the domain of the child server: **`otherdomain.mycompany.com.`** (remember to include the trailing period after `com`). Do not use the default that is displayed in the window, which is `mycompany.com`. See Figure 92.

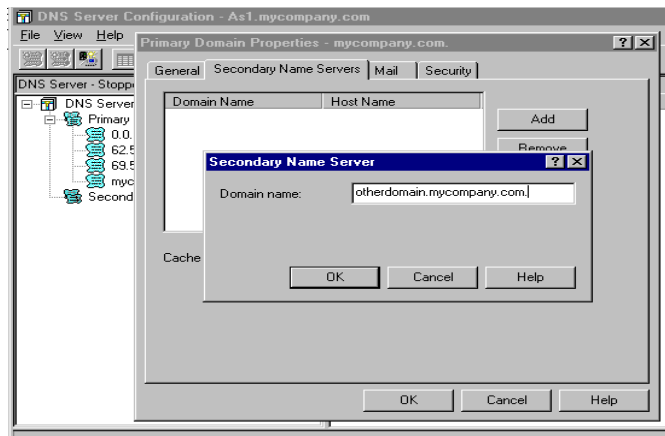


Figure 92. Entering the Domain Name of the Child Server OTHERHOST

18. Click **OK**.

19. Enter the host name of the child server: **OTHERHOST**. See Figure 93.

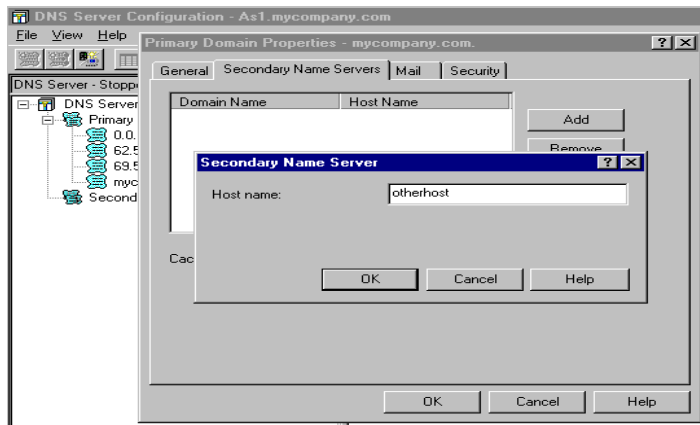


Figure 93. Entering Host Name OTHERHOST for mycompany.com's NS Record

20. Click **OK**.

21. Click **OK**.

You have just created an NS record for
OTHERHOST. *OTHERDOMAIN.mycompany.com* on the parent server AS1.

Tip

The label on the Secondary Name Servers tab under *mycompany.com*'s properties can be a bit misleading. Entering domain and host names under this tab creates an NS record in the QIBM/UserData/OS400/DNS/mycompany.com.DB file. NS records are necessary for identifying other name servers. It is better if this tab is just labeled "Name Servers". In this step, we create an NS record for the purpose of delegating authority to a child DNS server, which is unrelated to the concept of a secondary name server.

22. Right click the *mycompany.com* primary domain file again.

23. Click **New Host**.

24. Click **Add**.
25. Enter the Host Name of: `OTHERHOST.OTHERDOMAIN.mycompany.com`. (do not forget the trailing dot after `com`).
26. Enter the IP address of `OTHERHOST`: **10.1.1.2**.
27. Click **OK**.
28. Click **OK**.

You have just created an A record in AS1's `mycompany.com` primary domain file for the host `OTHERHOST.OTHERDOMAIN.mycompany.com`.

29. Right click `mycompany.com` primary domain and select **Properties**. On the General tab, enable the *Create and delete reverse mappings by default*. Do this step only if you finished delegating subdomains. In this scenario, the `OTHERDOMAIN.mycompany.com` subdomain is the only subdomain we are delegating. If there are other subdomains to delegate, the previous steps must be repeated for the additional subdomains. Since we finished delegating our one subdomain `OTHERDOMAIN.mycompany.com`, we complete this step by ensuring that the check box *Create and delete reverse mappings by default* is enabled.
30. The DNS configuration on AS1 is not finished yet. Do not close the DNS server configuration window yet. Continue with the next section.

The NS and A record that we have just created together allow the parent server, in this case AS1, to query `OTHERHOST` child server on behalf of a client that needs to resolve a host name for a host contained in the `OTHERDOMAIN.mycompany.com` subdomain. Another way of saying this is that the NS and A record allow the DNS server on AS1 to "look down" the DNS name space tree to find the server (`OTHERHOST` in our case) that has authority for the subdomain `OTHERDOMAIN.mycompany.com`.

Figure 94 shows the contents of the forward mapping primary domain file `mycompany.com.DB` located in the `/QIBM/UserData/OS400/DNS` directory on AS1, the parent server. The MX record was created in Section 3.2.3.3 on page 48. What is of interest in Figure 94 is the NS record for `OTHERHOST.OTHERDOMAIN.mycompany.com` and the A record for `OTHERHOST`.

```

mycompany.com. IN SOA as1.mycompany.com. postmaster.as1.mycompany.com. (
                                889119579
                                10800
                                3600
                                604800
                                86400 )

;AS400OPNAV_INFO REVMAPDOMAIN
mycompany.com. IN NS as1.mycompany.com.
otherdomain.mycompany.com. IN NS otherhost.otherdomain.mycompany.com.
*.mycompany.com. IN MX 0 as1.mycompany.com.
;AS400OPNAV_INFO REVMAPHOST NTserver1.mycompany.com.
NTserver1.mycompany.com. IN A 10.5.69.205
;AS400OPNAV_INFO REVMAPHOST as5.mycompany.com.
as5.mycompany.com. IN A 10.5.69.221
;AS400OPNAV_INFO REVMAPHOST as1.mycompany.com.
as1.mycompany.com. IN A 10.5.69.222
;AS400OPNAV_INFO REVMAPHOST p23fym82.mycompany.com.
p23fym82.mycompany.com. IN A 10.5.62.169
;AS400OPNAV_INFO REVMAPHOST p23thkpl.mycompany.com.
p23thkpl.mycompany.com. IN A 10.5.69.204
;AS400OPNAV_INFO REVMAPHOST as2.mycompany.com.
as2.mycompany.com. IN A 10.5.69.211
;AS400OPNAV_INFO REVMAPHOST p23fzg16.mycompany.com.
p23fzg16.mycompany.com. IN A 10.5.62.58
;AS400OPNAV_INFO REVMAPHOST localhost.mycompany.com.
localhost.mycompany.com. IN A 127.0.0.1
;AS400OPNAV_INFO REVMAPHOST otherhost.otherdomain.mycompany.com.
otherhost.otherdomain.mycompany.com. IN A 10.1.1.2
p23qpb74.mycompany.com. IN A 10.5.62.187

```

Figure 94. Contents of /QIBM/UserData/OS400/DNS/MYCOMPANY.COM.DB File on AS1

Figure 95 shows the boot file in the parent name server AS1. Notice that this server runs also the internal root name server (.).

```

directory /QIBM/UserData/OS400/DNS
limit transfers-in 10
limit transfers-per-ns 2
primary mycompany.com mycompany.com.DB
primary . .DB
primary 62.5.10.in-addr.arpa 62.5.10.in-addr.arpa.DB
primary 0.0.127.in-addr.arpa 0.0.127.in-addr.arpa.DB
primary 69.5.10.in-addr.arpa 69.5.10.in-addr.arpa.DB
cache . CACHE

```

Figure 95. BOOT file /QIBM/UserData/OS400/DNS/BOOT File on AS1

5.5.4 Delegating the In-Addr.Arpa File on the Parent Server AS1

In this scenario, we decided that the 1.1.10.in-addr.arpa primary domain file will be maintained on child server *OTHERHOST*. To do this, we need to delegate the reverse mapping file to the child server also. The way to do this is to subnet the 1.1.10.in-addr.arpa file. First we explain the steps to do this on the parent server and give a further explanation about why we have to do this.

Note

It is important to notice that in this section, we configure a **2-byte** in-addr arpa file, 1.10.in-addr.arpa on AS1. This is a different primary domain file than the **3-byte** in-addr.arpa file, 1.1.10.in-addr.arpa file that is created on the child server *OTHERHOST*. Right now, this may be a little confusing so just be aware that 1.10.in-addr.arpa is a different primary domain from the 1.1.10.in-addr.arpa primary domain. This is similar in concept to saying that the *mycompany.com* primary domain is a different primary domain from the *OTHERDOMAIN.mycompany.com* that we configure later on in the child server *OTHERHOST*.

Complete the following steps on the parent server AS1:

1. Right click on the label **Primary Domains** under the title of DNS *Server-as1.mycompany.com*.
2. Click on **New Primary Domain**. See Figure 96.

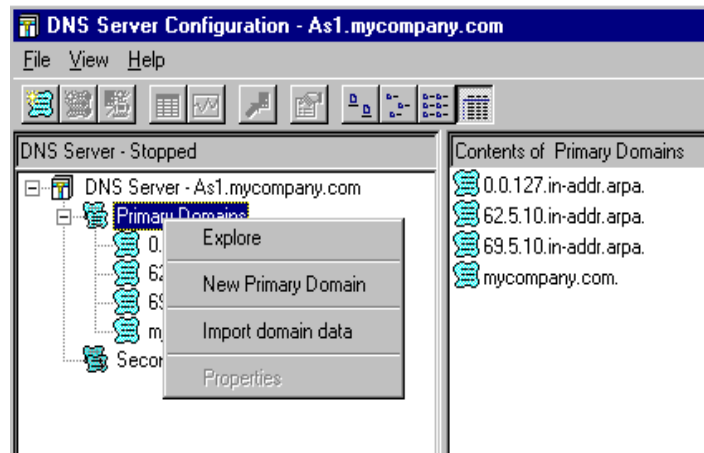


Figure 96. Creating the Two-Byte Primary Domain File 1.10.in-addr.arpa on AS1

Under the General Tab's Domain Name field, type in **1.10.in-addr.arpa**. and leave the *Create and delete reverse mappings by default* check box unchecked. See Figure 97.

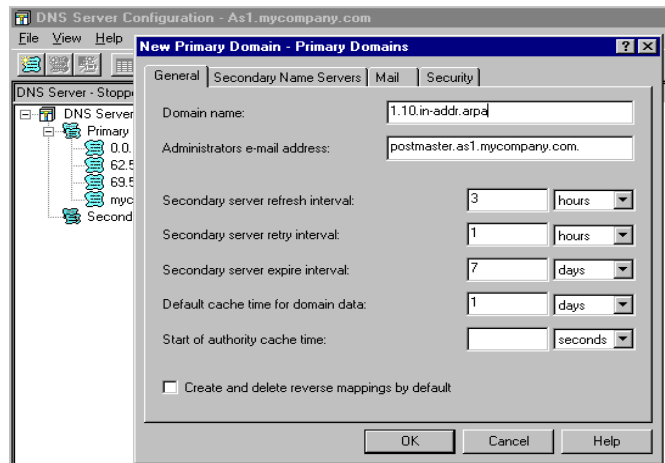


Figure 97. Entering the Domain Name when Creating the 1.10.in-addr.arpa Primary Domain File

3. Click **OK**. The new primary domain file of 1.10.in-addr.arpa should be displayed in the list of primary domain files.
4. Right click the **1.10.in-addr.arpa** primary domain file.
5. Click **Properties**.
6. Click the **Secondary Name Server** Tab.
7. Click **Add**.
8. In the domain name field, enter the domain name of the three byte in-addr.arpa domain: **1.1.10.in-addr.arpa**. (do not forget the trailing period after *com*). See Figure 98.

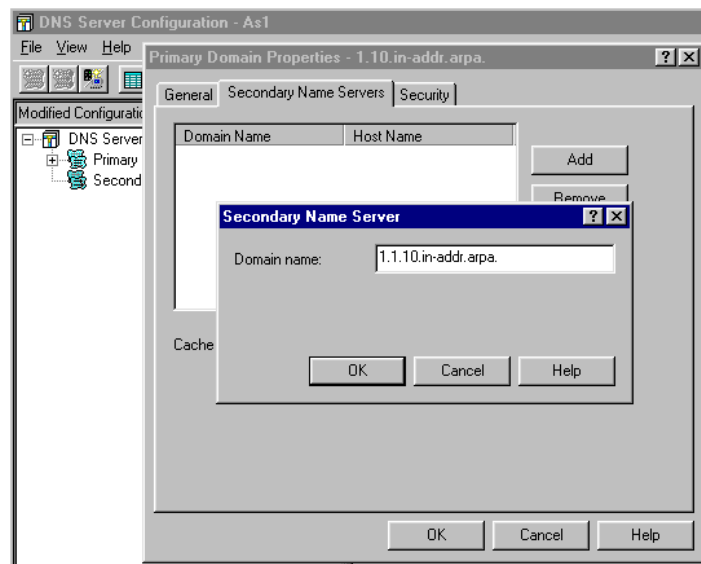


Figure 98. Entering 1.1.10.in-addr.arpa's Domain Name for Secondary Name Server in 1.10.in-addr.arpa File

9. Click **OK**.
10. In the host field, enter **OTHERHOST.OTHERDOMAIN.mycompany.com**. (Do not forget the trailing dot after *com*.)
11. Click **OK**.
12. Click **OK**.
13. Right click the **1.10.in-addr.arpa** file.

14. Click **Enable** to enable this primary domain.

Tip

At this point, you may be wondering "what did we just do?" We created a new primary domain file but we did not add any hosts to it. If we click on the 1.10.in-addr.arpa file, we see that it is empty of any records. In steps 5 through 12, we created an NS record specifying the child server *OTHERHOST* for the 1.1.10.in-addr.arpa primary domain file. Essentially this is telling the parent server AS1 that the primary reverse mapping file of 1.1.10.in-addr.arpa exists on the child server *OTHERHOST*. You can think of the NS record in this case as a pointer to help the parent server, AS1, find its way down the DNS name space tree to the server that is authoritative for the 1.1.10.in-addr.arpa domain, which is the child server *OTHERHOST*. In conclusion, we just delegated the 1.1.10.in-addr.arpa domain to the child name server *OTHERHOST*.

If a client sends a reverse lookup query to the parent server AS1 (for example, the client knows the IP address 10.1.1.9 and is querying AS1 for corresponding host name), the name server on AS1 uses the NS record we just created within 1.10.in-addr.arpa to find out that the authority for the 1.1.10.in-addr.arpa resides on the child server *OTHERHOST*. AS1 either tells the client to go query the *OTHERHOST* name server for the answer or AS1 will query the *OTHERHOST* DNS server on the client's behalf.

Continuing on.....:

We now need to add the *OTHERSERVER* host to the 69.5.10.in-addr.arpa primary domain file on the parent server AS1. Although the *OTHERSERVER* host is in the *OTHERDOMAIN* subdomain that the child server *OTHERHOST* is authoritative for, the parent server AS1 is authoritative for the entire 69.5.10.in-addr.arpa primary domain file. Because *OTHERSERVER* has an IP address in the 10.5.69.192 network, this host must be added into the 69.5.10.in-addr.arpa file on the parent server AS1. See Figure 83 on page 89 to review the network diagram and IP addresses.

15. Right click the **69.5.10.in-addr.arpa** primary domain file.

16. Select **New Host**.

17. Click **Add**.

18. Enter host name: *OTHERSERVER.OTHERDOMAIN.mycompany.com*. (do not forget the trailing period after *com*).

19. In the same window, enter the IP address of **10.5.69.207**.

20. Click **OK**.

21. Click **OK**.

22. Close the DNS server configuration window to save the configuration on the parent server, AS1.

Figure 99 shows the contents of the 2-byte 1.10.in-addr.arpa primary domain file on AS1. This file is in the IFS directory /QIBM/UserData/OS400/DNS. Unlike the 3-byte in-addr.arpa files, this file does not contain any PTR records. The purpose of this file is to contain an NS record that points to the child name server *OTHERHOST*. The child name server *OTHERHOST* contains the 3-byte 1.1.10.in-addr.arpa primary domain file for the network 10.1.1.0 and that is the in-addr.arpa file that contains the PTR records for the hosts in this network. AS1's 1.10.in-addr.arpa file is what the AS1 name server uses to "find" the name server (*OTHERHOST*) authoritative for the 1.1.10.in-addr.arpa domain.

```

1.10.in-addr.arpa. IN SOA as1.mycompany.com. postmaster.as1.mycompany.com. (
                                                889639021
                                                10800
                                                3600
                                                604800
                                                86400 )
;AS400OPNAV_INFO NOREVMAPDOMAIN
1.10.in-addr.arpa. IN NS as1.mycompany.com.
1.1.10.in-addr.arpa. IN NS otherhost.otherdomain.mycompany.com.

```

Figure 99. Contents of 1.10.in-addr.arpa Domain File on AS1

Summary of Method 2 Configuration

The configuration of the delegation of domain *OTHERDOMAIN* and the 1.1.10.in-addr.arpa domain on the parent server AS1 is complete. We still need to perform additional configuration changes on the child server, *OTHERHOST*, which we cover in the next section. Figure 100 shows the list of primary domain files (in the left column of the Operations Navigator display) residing on AS1 parent server. Notice the 1.10.in-addr.arpa primary domain. Figure 100 also shows the contents of the *mycompany.com* primary domain file (in the right column of the Operations Navigator display).

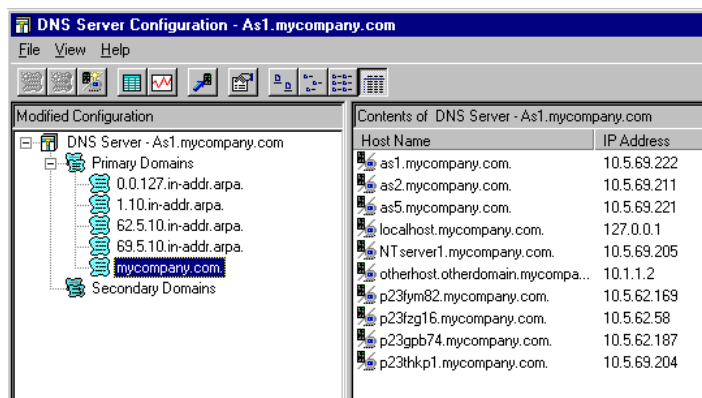


Figure 100. Contents of AS1's mycompany.com Primary Domain File

5.5.5 Configuring the Child Server Otherhost

We are still configuring our name servers for Method 2. In the last few sections, all the configuration took place on the parent server AS1. We are finished configuring Method 2 on AS1 but we still need to configure the child server, *OTHERHOST*, to be authoritative for the *OTHERDOMAIN.mycompany.com* domain. The steps to do this are similar to the configuration steps completed in Method 1 of this chapter except that these steps are performed on the child server *OTHERHOST* instead of the AS1's name server as we did in Method 1.

If DNS has never been configured on *OTHERHOST*, the DNS configuration wizard starts.

Perform the following steps on *OTHERHOST*, the child name server. We are assuming a DNS configuration does not exist on this AS/400 system yet.

1. Open Operations Navigator and double-click on *OTHERHOST.OTHERDOMAIN.mycompany.com*.
2. Click + next to **Network**.

3. Click **+** next to **Servers**.
4. Click **+** next to **OS400**.
5. Double-click **DNS** under the Server Name column.
6. The DNS server configuration wizard starts the first time you enter DNS server configuration. Click **Next**.
7. Click **Next** to bypass the Root Server window. We are configuring a root server on this child name server but we do this later in this chapter. For now, bypass the root server window.
8. Enter the name of the primary domain we are configuring:
OTHERDOMAIN.mycompany.com.
9. Click **Next**.
10. The next window gives you an opportunity to add IP address and host names. We need to configure only the local host for the loopback address of 127.0.0.1 with the wizard. Click **Add**.
11. Enter **localhost** as the host name. (We really want you to type the word **localhost** here; do not type the TCP/IP host name of the AS/400 system you are configuring on.)
12. Enter **127.0.0.1** as the IP address.
13. Click **OK**.
14. Click **Finish**.

Add the remaining IP addresses and host names outside of the Wizard DNS server configuration.

15. The DNS server configuration with wizard is complete. Continue with Step 16.

Note: If this is not the first time you are configuring DNS with Operations Navigator, the DNS server configuration wizard is not shown. In this case, use the following unnumbered steps and then proceed with Step 16. Use Operations Navigator to go into the *OTHERHOST*'s DNS server configuration.

- Right click on the **Primary Domain** under DNS
server-*OTHERHOST.mycompany.com*.
 - Click **New Primary Domain**.
 - In the window that follows, ensure that the Domain field is: *OTHERDOMAIN.mycompany.com*. Assuming that this AS/400 system is configured with that domain name (you can check with the AS/400 CFGTCP command, press Enter, take Option 12, and check the Domain name listed). This should be the default domain in this window. If it is not, type in *OTHERDOMAIN.mycompany.com* for the Domain Name.
 - In the same window, check the box *Create and delete reverse mappings by default* to enable this option.
 - Click **OK**.
 - Right click *OTHERDOMAIN.mycompany.com*.
 - Click **New Host**.
 - Click **Add**.
 - Enter the host name **localhost**. (We really want you to type in the word **localhost** here.)
 - Enter the IP address **127.0.0.1**.
 - Click on **OK**.
16. Up to this point, we created (either by using the DNS server configuration wizard or the preceding unnumbered steps) the primary domain forward mapping file of *OTHERDOMAIN.mycompany.com* on *OTHERHOST*'s name server. Right click on *OTHERDOMAIN.mycompany.com*.
 17. Select **Properties**.

18. Ensure that *Create and Delete reverse mappings by default* is enabled.
19. Click **OK**.
20. Right click the *OTHERDOMAIN.mycompany.com* primary domain file.
21. Click **Enable**.

The following steps add the new hosts (A records) to the *OTHERDOMAIN.mycompany.com* primary domain file:

22. Right click on the *OTHERDOMAIN.mycompany.com* primary domain file.
23. Click **New Host**.
24. Click **Add**.
25. Enter the host name **otherhost.otherdomain.mycompany.com**. (do not forget the trailing period after *com*).
26. On the same window, enter the IP address: **10.1.1.2**. See Figure 101.

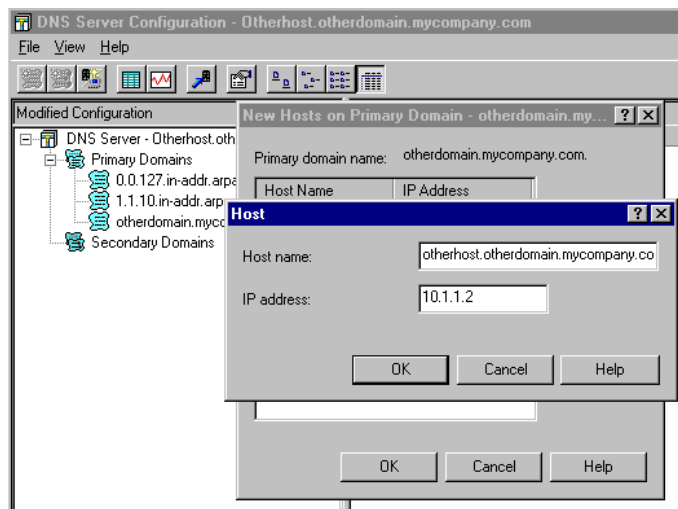


Figure 101. Adding OTHERHOST Host to the OTHERDOMAIN Primary Domain File on Child Server

27. Click **OK**.
28. Click **OK**.

Notice that the *1.1.10.in-addr.arpa* primary domain file is automatically created. At this point, it contains one PTR record for the *OTHERHOST* host. By the time we finish with these steps, this file will also contain the PTR records for *OTHERSERVER* host and *OTHERPRINTER* host.

29. Repeat steps 22 through 28 to add New Host *OTHERPRINTER* with an IP address of 10.1.1.9.
30. Repeat steps 22 through 28 again to add New Host *OTHERSERVER* with an IP address of 10.1.1.7.
31. Right click on the **1.1.10.in-addr.arpa** primary domain file.
32. Select **Enable** to enable the *1.1.10.in-addr.arpa* file.
33. Double-click *OTHERHOST.OTHERDOMAIN.mycompany.com* file. The contents of this file is displayed in the right window.
34. Right click host *OTHERSERVER*.
35. Select **Properties**.
36. Click **Add**.
37. Enter *OTHERSERVER*'s second IP address: **10.5.69.207**. See Figure 83 on page 89 if you need to refresh your memory on the network diagram and the IP addressing used.

Note

Because we added a second IP address to *OTHERSERVER* and because *Create and delete reverse mappings by default* was enabled, a new primary domain file was created: *69.5.10.in-addr.arpa*. It contains one PTR record for *OTHERSERVER*. If you remember the DNS configuration on the parent server *AS1*, you remember that a *69.5.10.in-addr.arpa* primary domain file exists on that server already. The same PRIMARY domain file cannot exist on two different servers. If the same file exists on another server, it must exist under a secondary domain configuration (and the *69.5.10.in-addr.arpa* backup file does exist on the secondary name server *AS5* as configured in Chapter 3). The primary domain file of *69.5.10.in-addr.arpa* on the child server *OTHERHOST* must be deleted on the child server *OTHERHOST*.

38. Right click **69.5.10.in-addr.arpa** file on the child server *OTHERHOST*.

39. Click **Delete**.

40. Click **Yes** to confirm the Delete.

The *OTHERDOMAIN.mycompany.com* primary domain should look similar to Figure 102.

41. We need to perform one more configuration step on the child server, *OTHERHOST*, in the next section so do not close the DNS window to save the configuration just yet.

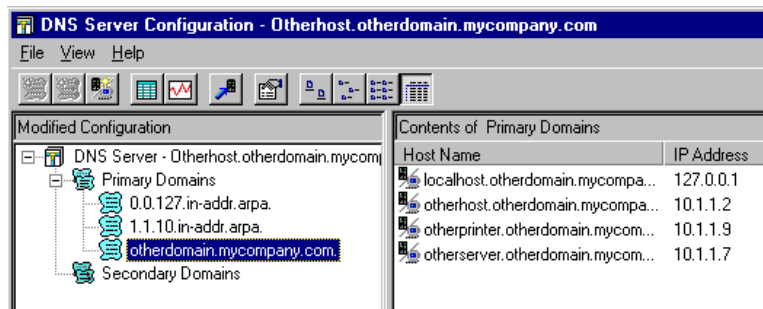


Figure 102. *OTHERDOMAIN.mycompany.com* Primary Domain on the Child Server *OTHERHOST*

We almost finished the child server configuration. The next section explains how to configure the child server to resolve queries for domains above itself in the DNS name space tree: the root server configuration.

5.5.6 Internal Root Server Configuration on the Child Server

In Section 5.5.3, “Delegating the Subdomain on the Parent Server *AS1*” on page 99, we configured an A record and an NS record for the child server on the parent server. This was so that if the parent server receives a query for information that the child server is authoritative for, the parent server knows how to “look down” the DNS name space tree to find the server authoritative for the primary domain the query was for.

The root server configuration on the child server allows the child server to look to the top of the name space tree when it receives a query for information in the *mycompany.com* zone of authority that is above it in the tree structure. Section

5.5.1, “Configuring AS1 as Internal Root” on page 96, shows how to configure the internal root name server for the internal name space.

Perform the following steps on the child server *OTHERHOST*:

1. Start the DNS server configuration in Operations Navigator and right click on **DNS Server-OTHERHOST.OTHERDOMAIN.mycompany.com**.
2. Click **Properties**.
3. Select the **Root Servers** tab.
4. Click **Add**.
5. Enter the host name of the parent server: *AS1.mycompany.com*. (do not forget the trailing period after the *com*).
6. On the same window, enter the IP address: 10.5.69.222. See Figure 103.

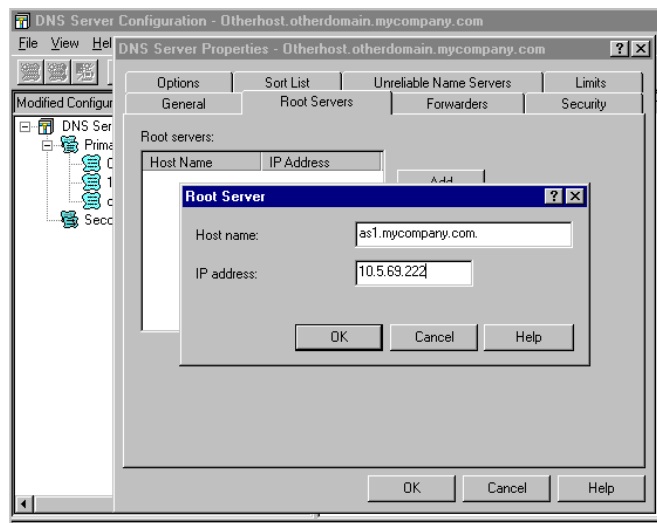


Figure 103. Adding a Root Name Server to the Child Server *OTHERHOST*

7. Click **OK**.
8. Click **OK**.
9. Close the DNS window to save the configuration.

5.5.7 Reconfigure the Otherdomain Clients

If the hosts in *OTHERDOMAIN.mycompany.com* are configured with a domain name of *OTHERDOMAIN.com* prior to changing *OTHERDOMAIN* to be a subdomain of *mycompany.com*, you must change the hosts' domain names. Hosts located within *OTHERDOMAIN.mycompany.com* no longer should have a domain name of *OTHERDOMAIN.com* but should now have a domain name of *OTHERDOMAIN.mycompany.com*. Updating the hosts' domain names to be *OTHERDOMAIN.mycompany.com* is necessary for both Method 1 and Method 2 because in both methods, *OTHERDOMAIN* became a subdomain of *mycompany.com*. The difference between Method 1 and Method 2 involved the zone of authorities.

For example, in our scenario *OTHERHOST* is an AS/400 system. To change its domain name use the AS/400 command:

```
CFGTCIP
```

Then use Option 12. Retype the domain name:
OTHERDOMAIN.mycompany.com.

Several AS/400 TCP/IP applications (SMTP included) require the local AS/400 system to be listed in the TCP/IP host table with both the short name (that is, *OTHERHOST*) and the long name (*OTHERHOST.OTHERDOMAIN.mycompany.com*). Do not forget to use the AS/400 command:

```
CFGTCIP
```

Then use Option 10 to update the long name of *OTHERHOST.OTHERDOMAIN.com* to *OTHERHOST.OTHERDOMAIN.mycompany.com*.

5.5.8 Verifying DNS with Name Server Lookup

The AS/400 Name Server Lookup (nslookup) queries a name server through a "green screen" interactive mode. In this section, we use nslookup to query the parent server AS1 and the child server *OTHERHOST* to verify these name servers are answering the queries and giving the responses we expect.

To enter the nslookup interactive mode, enter the following command on the AS1 command line:

```
call pgm(qdns/qtoblkup)
```

The result of this command is shown in Figure 104:

```
Press ENTER to end terminal session.
Default Server:  as1.mycompany.com
Address: 10.5.69.222

>

====>

F3=Exit F4=End of File F6=Print F9=Retrieve F17=Top
F18=Bottom F19=Left F20=Right F21=User Window
```

Figure 104. Entering Nslookup Interactive Mode

Figure 104 shows nslookup displaying the default server of AS1, which indicates that the server that nslookup queries by default is the AS1 name server.

The default type of query that nslookup uses is an A record query (that is, have the host name need an IP address). We can query for the IP address of the host NTserver1. By entering **NTserver1** on the command line, we are querying AS1 name server's A record for NTserver1. Nslookup also adds a default domain name to the NTserver1 host name that we entered. The default domain name is *mycompany.com*, which is correct for the host NTserver1. The result is shown in Figure 105. You can see that name server AS1 supplied nslookup with NTserver1's IP address of 10.5.69.205.

```

>
  Press ENTER to end terminal session.
  Default Server:  as1.mycompany.com
  Address:  10.5.69.222

>
> ntserver1
  Server:  as1.mycompany.com
  Address:  10.5.69.222

  Name:    ntserver1.mycompany.com
  Address:  10.5.69.205

>

===>

```

Figure 105. Result of Nslookup Query for ntserver1

Next let's query AS1 for an A record that the child server `OTHERHOST` is authoritative for, `OTHERPRINTER`. To do this, we enter `OTHERPRINTER` on the command line. Whoops.... nslookup caught us using the incorrect domain name for `OTHERPRINTER`. The result we get is "No A records found". This is because the query was made for `OTHERPRINTER.mycompany.com`, which is not correct. Next we enter the correct query: `otherprinter.OTHERDOMAIN.mycompany.com` and get the answer we expected: 10.1.1.9. Both queries and their results are shown in Figure 106. The AS1 name server responds with `OTHERPRINTER`'s IP address of 10.1.1.9. But AS1 is not authoritative for `OTHERPRINTER`'s domain. How did AS1 know the answer? AS1 queried the child server `OTHERHOST` for `OTHERPRINTER`'s IP address to respond to nslookup's query. AS1 cached the answer. The next time AS1 is queried for the IP address of `OTHERPRINTER`, it will get the answer from its cache (assuming the cache has not timed out or the name server has not been stopped and started on AS1) and does not bother `OTHERHOST`.

```

>
> otherprinter
  Server:  as1.mycompany.com
  Address:  10.5.69.222

  *** No address (A) records available for otherprinter
>
> otherprinter.otherdomain.mycompany.com
  Server:  as1.mycompany.com
  Address:  10.5.69.222

  Name:    otherprinter.otherdomain.mycompany.com
  Address:  10.1.1.9

>

===>

F3=Exit F4=End of File F6=Print F9=Retrieve F17=Top
F18=Bottom F19=Left F20=Right F21=User Window

```

Figure 106. Querying for `OTHERPRINTER` and `OTHERPRINTER.OTHERDOMAIN.mycompany.com`

To submit a reverse mapping query, which is to supply the IP address and ask the name server to respond with the host name, we need to change to a query type of PTR within nslookup. First, we issue the nslookup command:

```
set type=ptr
```

Second, we issue the command `10.5.69.221` to query the AS1 name server for 10.5.69.221's host name. The result is shown in Figure 107.

Let's explain, line-by-line, what nslookup is displaying on the window:

- `> 10.5.69.221` - This is our query. What is to the right of the `>` symbol is what the user typed.
- `Server: as1.mycompany.com` - This is the name server that nslookup queried.
- `Address: 10.5.69.222` - This is the IP address of the name server.
- `221.69.5.10.in-addr.arpa name = as5.mycompany.com` - This is the answer to our query answer. nslookup lists the absolute in-addr.arpa domain name of AS5, along with the fully qualified host name of `AS5.mycompany.com`.
- `69.5.10.in-addr.arpa nameserver=as1.mycompany.com` - This is the name of the primary domain file that the answer was located in. This line also contains the name of the name server authoritative for the primary domain file.
- `as1.mycompany.com internet address=10.5.69.222.` - This is the fully-qualified name and IP address of the name server authoritative for the domain file the answer was located in.

```
>
> set type=ptr
>
> 10.5.69.221
Server:  as1.mycompany.com
Address: 10.5.69.222

221.69.5.10.in-addr.arpa      name = as5.mycompany.com
69.5.10.in-addr.arpa         nameserver = as1.mycompany.com
as1.mycompany.com            internet address = 10.5.69.222
>

===>

F3=Exit F4=End of File F6=Print F9=Retrieve F17=Top
F18=Bottom F19=Left  F20=Right F21=User Window
```

Figure 107. Nslookup Reverse Lookup Query for 10.5.59.221

Let's now use nslookup to query the AS1 name server for a reverse lookup for an IP address that the child name server `OTHERHOST` is authoritative for. Remember the primary domain file of `1.1.10.in-addr.arpa` resides on the child server `OTHERHOST`. This time, AS1 gives a non-authoritative answer along with where you can find the authoritative answer. See Figure 108.

```

>
> 10.1.1.7
Server:  as1.mycompany.com
Address: 10.5.69.222

Non-authoritative answer:
7.1.1.10.in-addr.arpa      name = otherserver.otherdomain.mycompany.com

Authoritative answers can be found from:
1.1.10.in-addr.arpa      nameserver = otherhost.otherdomain.mycompany.com
otherhost.otherdomain.mycompany.com      internet address = 10.1.1.2
>

====>

F3=Exit F4=End of File F6=Print F9=Retrieve F17=Top
F18=Bottom F19=Left F20=Right F21=User Window

```

Figure 108. Using Nslookup to Query AS1 for 10.1.1.7 Host Name

What does it mean to get a *non-authoritative* answer? It means that at some time earlier, the AS1 name server got the reverse mapping information for 10.1.1.7 from the child server `OTHERHOST` and cached it. When we just now used nslookup to query for 10.1.1.7, the AS1 name server supplied us with the answer from its cache. Note that AS1 tells us where to find the authoritative answer, which is the child server, `OTHERHOST`.

So let's query the child server `OTHERHOST` for an authoritative answer for the reverse lookup of 10.1.1.7. We can do this right from the AS1's session, but we need to tell Nslookup that we want to switch name servers. We switch to querying `OTHERHOST` by issuing the command:

```
server otherhost.otherdomain.mycompany.com.
```

Set the query type to PTR by entering the command:

```
set type=ptr
```

Then, enter the command: 10.1.1.7

The results of all three commands are shown in Figure 109.

```

>
> server otherhost.otherdomain.mycompany.com
Default Server: otherhost.otherdomain.mycompany.com
Address: 10.1.1.2

>
> set type=ptr
>
> 10.1.1.7
Server: otherhost.otherdomain.mycompany.com
Address: 10.1.1.2

7.1.1.10.in-addr.arpa      name = otherserver.otherdomain.mycompany.com
1.1.10.in-addr.arpa       nameserver = otherhost.otherdomain.mycompany.com
>

===>

F3=Exit F4=End of File F6=Print F9=Retrieve F17=Top
F18=Bottom F19=Left F20=Right F21=User Window

```

Figure 109. Querying OTHERHOST Using Nslookup on AS1

This time nslookup has an authoritative answer:

```
name = otherserver.otherdomain.mycompany.com.
```

This is the answer we are looking for. The 10.1.1.7 IP address belongs to OTHERSERVER. The answer came from the primary domain file of 1.1.10.in-addr.arpa that resides on the child server OTHERHOST.OTHERDOMAIN.mycompany.com. This is the name server that nslookup was using; therefore, the answer had to be authoritative.

5.5.9 Method 2's Secondary Name Server AS5

In the past few sections, we made some major configuration changes from the name server configuration in Chapter 3's scenario. Thus, we should be asking ourselves: what about a backup? We now have two name servers (the parent and the child) that contain primary domain files. How should we back them up?

Backing Up the Parent Server AS1

In this scenario, using Method 2 to delegate the zone of authority to the child name server OTHERHOST, we made some changes to the parent name server's primary domain files that already existed from Chapter 3's scenario. We also created one new primary domain file on AS1: 1.10.in-addr.arpa. Except for the new primary domain file of 1.10.in-addr.arpa, the primary domain files on AS1 are already backed up on AS5, which is the secondary name server for AS1. AS5 was configured as a secondary name server in Section 3.2.6 on page 57.

So the question comes up: do we need to create a new secondary domain file on the secondary name server AS5 for 1.10.in-addr.arpa? This domain file only contains an SOA record and one NS record. See Figure 99 on page 106 to review the contents of the 1.10.in-addr.arpa file.

The answer to the question depends on how the child name server OTHERHOST is backed up. If the secondary name server to OTHERHOST is a different name server

than AS5, the 1.10.in-addr.arpa domain file must add a secondary domain file on AS5, which is AS1's secondary name server.

If the secondary name server to the primary name server *OTHERHOST* is also AS5, then the secondary domain file of 1.1.10.in-addr.arpa exists on AS5 and there is no need for a secondary domain file 1.10.in-addr.arpa on AS5.

Backing Up the Child Name Server Otherhost

We configured two primary domain files on the child name server *OTHERHOST*: 1.1.10.in-addr.arpa and *OTHERDOMAIN.mycompany.com*. These primary domain files should be backed up on a secondary name server.

We can use the name server on AS5 as the secondary name server to the child name server *OTHERHOST* as well as the parent name server AS1. Whether the secondary name server is AS5 or it is a different AS/400 name server, the steps are the same:

1. On the secondary name server, create two new secondary domains:
OTHERDOMAIN.mycompany.com and 1.1.10.inaddr.arpa are the names of the domains.

The IP address of the master server is the IP address of the child name server 10.1.1.2.
2. On the child name server *OTHERHOST*, use the Properties' Secondary Name Server tab on each of the two primary domains to specify the domain name of the domain to be backed up and the fully-qualified host name of the secondary name server. This step was explained in detail in Section 3.2.6.2 on page 58.

When reviewing the *OTHERDOMAIN.mycompany.com.DB* file in Figure 113 on page 121, an NS record exists for AS5. This indicates we did make a decision to back up the child name server *OTHERHOST* with the secondary name server AS5.

5.6 Mail Between Otherdomain.mycompany.com and Mycompany.com

Now that we separated the domain *OTHERDOMAIN.mycompany.com* into a second zone of authority from the *mycompany.com* domain, the question is what configuration changes we need to make, if any, for the purposes of delivering mail. The answer to that question depends on whether AS1 remains the only mail server in the network or if a second mail server will handle the mail for users in the *OTHERDOMAIN.mycompany.com* domain.

5.6.1 AS1 as the Only Mail Server in the Network

The two zones of authority: *mycompany.com* and *OTHERDOMAIN.mycompany.com* are separated for the purposes of DNS only. The DNS server on AS1 is authoritative over the *mycompany.com* domain and the DNS server on *OTHERHOST* is authoritative over the *OTHERDOMAIN.mycompany.com* domain. All hosts on the three networks, 10.5.69.192, 10.5.62.0, and 10.1.1.0, have TCP/IP connectivity to each other and the mail administrator certainly may choose to have the AS1 mail server as the only mail server in the network. In other words, users in the *OTHERDOMAIN.mycompany.com* can have their POP3 client configured to have both their SMTP outgoing mail server and POP incoming mail server AS1.*mycompany.com*. Mail to this user is addressed to *User@mycompany.com*

and it arrives on the user's POP3 mailbox on AS1 as we explained in Chapter 3.2.3, "Configuring AS1 as a Mail Server" on page 44.

For the preceding example where AS1 remains the only mail server in the network, there is no need for any further DNS server configuration changes on the parent name server AS1 nor on the child name server *OTHERHOST* beyond what was already configured for Chapter 3.2.3, "Configuring AS1 as a Mail Server" on page 44. The users in the *OTHERDOMAIN.mycompany.com* can have their PC configured to use *OTHERHOST*'s IP address as its DNS server. The name server on *OTHERHOST* resolves the mail server's IP address, which is AS1's IP address.

In conclusion, even with the *OTHERDOMAIN* domain's zone of authority delegated to the child server *OTHERHOST*, the mail configuration outlined in Chapter 3.2.3, "Configuring AS1 as a Mail Server" on page 44 is the only mail configuration necessary if AS1 remains the only mail server for the network. All POP3 users need a POP3 directory entry on AS1 with their SMTP domain name equal to *AS1.mycompany.com*. Mail can be addressed to the user using either:

SMTP_UserId@mycompany.com
or
SMTP_UserId@AS1.mycompany.com

Both of the previous "mail to:" addresses allow mail to be delivered to the AS1 mail server.

5.6.2 Otherhost as the Mail Server for Otherdomain.mycompany.com

If *OTHERDOMAIN.mycompany.com* has its own mail server, and assuming that, for example, *OTHERHOST* is that mail server, we need to make configuration changes to *OTHERHOST* and also to the mail server AS1.

5.6.2.1 Mail Configuration on Otherhost Mail Server

The mail configuration required on *OTHERHOST* is similar to the mail configuration outlined in Chapter 3.2.3, "Configuring AS1 as a Mail Server" on page 44.

1. The POP3 user needs a user profile and POP3 directory entry on the *OTHERHOST* AS/400 system. It is important when configuring the SMTP domain name for each user to make it equal to *OTHERHOST.OTHERDOMAIN.mycompany.com*. See Chapter 3.2.3.1, "Configuring a POP3 User on AS1" on page 45 for details.
2. We need to update the DNS configuration on the *OTHERHOST* child name server. The following steps are similar to what was outlined in Chapter 3.2.3.3, "Configuring the Domain's Mail Server in the DNS Server" on page 48. However, this time, we perform the following DNS configuration steps outlined on the child server *OTHERHOST*.
 - Configure a wildcard MX entry. Start *OTHERHOST*'s DNS server configuration in Operations Navigator.
 1. Double-click **Primary Domains**.
 2. Right click on *OTHERDOMAIN.mycompany.com*.
 3. Right click on **Properties**.
 4. Click on **Mail** tab.
 5. Click **Add**.
 6. Take the default domain presented in the window:
*.OTHERDOMAIN.mycompany.com.

7. Click **OK**.
8. Enter the host name of the mail server:
`OTHERHOST.OTHERDOMAIN.mycompany.com`. (Use the fully-qualified host and domain name. Also, do not forget the trailing dot after *com*.)
9. Click **OK**.
10. Click **OK**.
- Verify that the mail server is listed as a host in the primary domain file of `OTHERDOMAIN.mycompany.com`. It is, in this case. We added `OTHERHOST` as a new host in `OTHERDOMAIN.mycompany.com` earlier in this chapter.
- Verify that the mail server is listed as a host in the `1.1.10.in-addr.arpa` primary domain file. It is; it was automatically added when we added `OTHERHOST` as a new host earlier in this chapter.
- Close the DNS window to save the configuration. Or, if the DNS server is already active, click on the Update Server smart icon to reload the DNS configuration changes while the DNS server continues to be active.
3. Check the TCP/IP and SMTP Configuration on `OTHERHOST`.

We need to verify the TCP/IP domain information and SMTP attributes. These steps are similar to the steps outlined in Chapter 3.2.3.4, “Verifying the TCP/IP and SMTP Configuration on AS1” on page 50 except that this time, the steps are performed on `OTHERHOST`.

- Use the `CFGTCP` command, option 12 to verify that the Search First is ***LOCAL**.
- On the same display, verify that the Internet address is `10.1.1.2`, which is the IP address of the local AS/400 `OTHERHOST` itself. The SMTP server running on `OTHERHOST` first searches the local host table to determine where to deliver the mail and if it does not find what it needs in the local host table on the AS/400 system, it queries the DNS at IP address `10.1.1.2` (`OTHERHOST`).
- Use the `CFGTCP` command, option 10 (on `OTHERHOST` system) to make sure that the host `OTHERHOST` is listed, has an Internet address of `10.1.1.2`, and has an entry with a host name of `OTHERDOMAIN.mycompany.com` (do not put a period at the end of *com* when using `CFGTCP` option 10).
- Use `CFGTCP` option 10 (on `OTHERHOST` system) to make sure that the host AS1 is listed with an IP address of `10.5.69.222` and has an entry with a host name of `mycompany.com`.
- Use the `CHGSMTPA` command followed by F4 (to prompt) and page down once to check on the Mail Router and Firewall parameters. Mail Router should be equal to ***NONE**. The Firewall parameter should be set to ***NO**.
- 4. Add host name to the AS1 system’s local host table.
 - On the AS1 system, issue `CFGTCP` option 10. Make sure the host `OTHERHOST` is listed with an Internet address of **10.1.1.2** and has an entry with a host name of `OTHERDOMAIN.mycompany.com`.
- 5. Make sure that SMTP, POP, and QMSF jobs are active on both mail servers `OTHERHOST` and AS1.
 - Check the status of the SMTP server jobs, the POP server jobs, and the QMSF job or jobs. All jobs should be running under the `QSYSWRK` subsystem. Then use the `WRKACTJOB SBS(QSYSWRK)` command to view all active jobs in the `QSYSWRK` subsystem. You may have to page down several times to find the jobs we are looking for.
 - The SMTP server is active if the following four jobs are active:
`QTSMTBPRCL`
`QTSMTBPRSR`

QTSMTPLNT

QTSMTPSVR

If these jobs are not active, you can start the SMTP server with the command:

```
STRTCPSVR *SMTP.
```

If the previous jobs are active and you made changes to CFGTCP option 10, option 12, or with the CHGSMTPA command, you must end and start the SMTP applications for the changes to take effect.

- The POP server is active if at least one job is active with the name QTPOPxxxxx, where xxxxx is any number. For example:

QTPop00595

QTPop00597

QTPop00637

QTPop00653

If at least one QTPOPxxxxx is not active, then start the POP server with the command:

```
STRTCPSVR *POP.
```

- Make sure at least one QMSF job is active under the QSYSWRK subsystem. The job name is QMSF. If a QMSF job is not active, then start one with the command:

```
STRMSF.
```

Starting the DNS server on OTHERHOST:

- If the DNS server is not started on OTHERHOST, the following AS/400 command will start it:

```
STRTCPSVR *DNS
```

- Once the DNS server is active, a job named QTOBDNS starts in the QSYSWRK subsystem. Its job log should be the first place the DNS administrator looks if there is a problem. The job runs under the user profile QTCP. If the QTOBDNS job has ended, use the WRKSPLF QTCP command and then F18 to go to the bottom of the list of job logs. This should help you locate the QTOBDNS spooled job log.

TIP

As a child name server queries a parent name server (or vice versa) to get responses for queries that it is not authorized for, it caches the response. Thus, if the child name server is queried for the same information again, the name server will give the answer out of its cache instead of querying the parent server again. However, if the child server is stopped and started, it clears its cache. Therefore, it is beneficial to try to minimize the number of times the name server is stopped and started once it is in production. If configuration changes need to be made to the name server while it is active, the recommended method is to use Operations Navigator and the Update Server smart icon to load the configuration changes while the name server is still active. This allows the name server to keep its cache rich with information.

5.7 The Child Server Otherhost's IFS Directory Files

Let's display the contents of the files within the child server `OTHERHOST`'s IFS directory that were created or altered by Method 2's configuration.

First, let's list the files in `/QIBM/UserData/OS400/DNS` that we do not display in this section.

- The `0.0.127.in-addr.arpa` file only contains the *localhost* host PTR record.
- The `ATTRIBUTES` file is automatically created when the DNS OS/400 option is installed on `OTHERHOST`. Use the `AS/400 CHGDNSA` command to change the contents of this file or use Operations Navigator DNS server configuration -> DNS server Properties -> General tab -> *Automatically start server* check box and *Debug level*.
- The `/TMP` directory in the DNS directory is also automatically created when the DNS OS/400 option is installed. Do not delete this directory. It is used when a secondary name file attempts a zone transfer to this name server.

The `OTHERHOST`'s `/QIBM/UserData/OS400/DNS/BOOT` file is displayed in Figure 110.

```
directory /QIBM/UserData/OS400/DNS
limit transfers-in 10
limit transfers-per-ns 2
primary otherdomain.mycompany.com otherdomain.mycompany.com.DB
primary 0.0.127.in-addr.arpa 0.0.127.in-addr.arpa.DB
primary 1.1.10.in-addr.arpa 1.1.10.in-addr.arpa.DB
cache . CACHE
```

Figure 110. Otherhost's BOOT File

The `OTHERHOST`'s `/QIBM/UserData/OS400/DNS/CACHE` file is displayed in Figure 111.

```
. 3600000 IN NS asl.mycompany.com.
asl.mycompany.com. 3600000 IN A 10.5.69.222
```

Figure 111. Otherhost's CACHE File

The `OTHERHOST`'s `/QIBM/UserData/OS400/DNS/1.1.10.in-addr.arpa.DB` file is displayed in Figure 112.


```

1.1.10.in-addr.arpa. IN SOA otherhost.otherdomain.mycompany.com.
                        postmaster.otherdomain.mycompany.com. (
                        889638632
                        10800
                        3600
                        604800
                        86400 )

;AS400OPNAV_INFO NOREVMAPDOMAIN
1.1.10.in-addr.arpa. IN NS otherhost.otherdomain.mycompany.com
2.1.1.10.in-addr.arpa. IN PTR otherhost.otherdomain.mycompany.com.
9.1.1.10.in-addr.arpa. IN PTR otherprinter.otherdomain.mycompany.com.
7.1.1.10.in-addr.arpa. IN PTR otherserver.otherdomain.mycompany.com.

```

Figure 112. Otherhost's 1.1.10.in-addr.arpa.DB File

The OTHERHOST's /QIBM/UserData/OS400/DNS/otherdomain.mycompany.com.DB file is displayed in Figure 113.

```

otherdomain.mycompany.com. IN SOA otherhost.otherdomain.mycompany.com.
                        postmaster.otherdomain.mycompany.com. (
                        889638631
                        10800
                        3600
                        604800
                        86400 )

;AS400OPNAV_INFO REVMAPDOMAIN
otherdomain.mycompany.com. IN NS otherhost.otherdomain.mycompany.com.
;AS400OPNAV_INFO REVMAPHOST localhost.otherdomain.mycompany.com.
localhost.otherdomain.mycompany.com. IN A 127.0.0.1
;AS400OPNAV_INFO REVMAPHOST otherhost.otherdomain.mycompany.com.
otherhost.otherdomain.mycompany.com. IN A 10.1.1.2
;AS400OPNAV_INFO REVMAPHOST otherprinter.otherdomain.mycompany.com.
otherprinter.otherdomain.mycompany.com. IN A 10.1.1.9
;AS400OPNAV_INFO REVMAPHOST otherserver.otherdomain.mycompany.com.
otherserver.otherdomain.mycompany.com. IN A 10.1.1.7
;AS400OPNAV_INFO REVMAPHOST otherserver.otherdomain.mycompany.com.
otherserver.otherdomain.mycompany.com. IN A 10.5.69.207

```

Figure 113. Otherhost's Otherdomain.mycompany.com.DB File

TIP

Notice that in Figure 112 and Figure 113, the SOA record in both the *1.1.10.in-addr.arpa* and *otherdomain.mycompany.com.* includes the e-mail address of the DNS administrator responsible for these primary domain files:

postmaster.otherhost.otherdomain.mycompany.com.

This is the default. If this default is used, then the AS/400 *otherhost* should have a user profile and a POP3 directory entry of *postmaster* configured.

5.8 Round Robin/Address Sorting

So far, this chapter addressed DNS server configuration issues dealing with adding a subdomain and delegating authority to a child server. A customer's network can grow in another direction also: adding IP addresses to existing hosts or adding an entire additional IP network.

Let us look at an example of adding a second LAN adapter to host AS2, which is in the domain *mycompany.com*. This second LAN adapter is located on the 10.5.62.0 network. AS2 has a second IP address of 10.5.62.217. Figure 114 shows the network diagram including AS2 with two IP addresses.

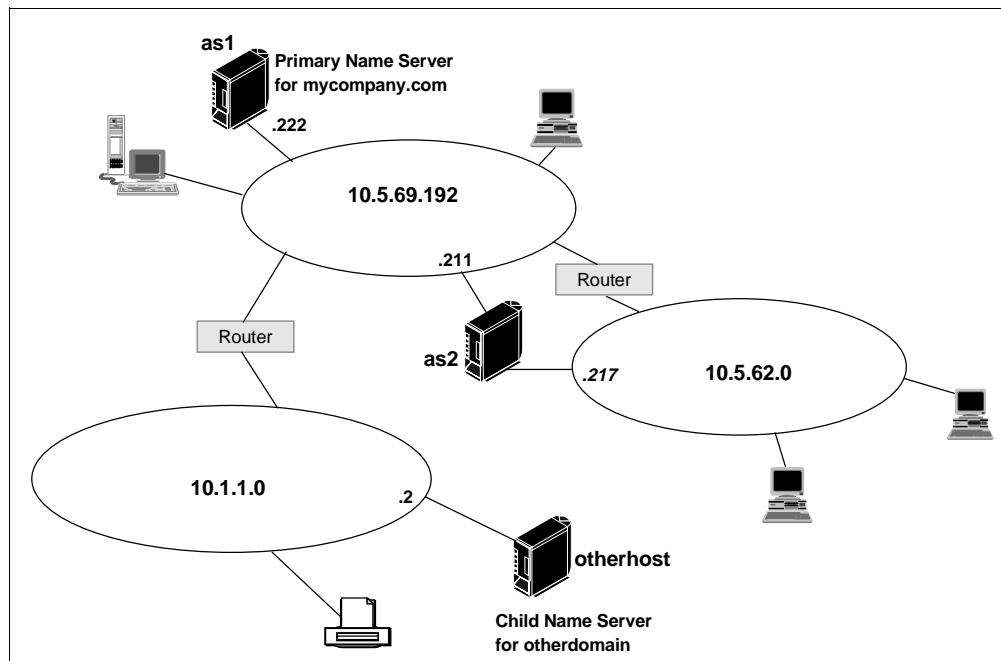


Figure 114. Host AS2 with Two IP Addresses

AS2 needs to have its TCP/IP configuration updated and a line description created for this new LAN adapter. See the TCP/IP Configuration and Reference, SC41-5420-01, for details concerning this configuration.

The name server that is authoritative for the domain *mycompany.com*, AS1, must be updated with the new *second* IP address for AS2. The steps to do this have already been covered in Chapter 5.5.5, “Configuring the Child Server Otherhost” on page 106.

The two-IP-address-for-one-host configuration brings up a common question: If a host has two IP addresses, which one will the DNS server respond with when a client issues an A record query for this host? The answer is that the DNS server gives out both IP addresses in the A record query response. However, which IP address is listed first depends on a few things that we attempt to outline here.

If a client is sending an A record query for AS2 to the AS1 name server, the response the client gets from AS1 depends on the client’s location in the network. The DNS server attempts to order AS2’s IP addresses with the first IP address closest to the client. This concept is called address sorting.

For example, assume that a client located in the network 10.5.62.0 queries the AS1 name server for the IP addresses of AS2. The name server responds with both of AS2’s IP addresses but the 10.5.62.217 is listed first. Since clients

typically attempt to use the IP address listed first in a DNS A record response, listing this address first is most efficient for the client.

If another client sends the same query to the AS1 name server but the client resides in the 10.5.69.192 network, the name server sends the query response to the client with the 10.5.69.221 address listed first.

But what if the client is not in one of these two networks? What if the client is located on the 10.1.1.0 network, which is remote to AS2? Again, the name server responds to a query listing both IP addresses but it alternates which IP address is listed first. Alternating IP addresses in response to A type queries is called round robin.

We can use nslookup on the child server `OTHERHOST` to show how round robin works. Let's query for the IP addresses of AS2. The reason we are using nslookup on `OTHERHOST` is because `OTHERHOST` is located in the 10.1.1.0 network, which is the one network AS2 is not connected to. Running nslookup on `OTHERHOST` allows us to use `OTHERHOST` as a client querying the AS1 name server (in other words, we are not using `OTHERHOST`'s name serving capabilities here, we are just using nslookup on `OTHERHOST`). When AS1 name server is queried, the name server sees the client making the query as having the IP address of 10.1.1.2. If we send multiple A record queries for host AS2, we should see an example of round robin.

From the `OTHERHOST` AS400 command line, enter nslookup interactive mode by issuing the following command:

```
call pgm(qdns/qtoblkup)
```

Since we entered nslookup on the `OTHERHOST` AS/400 system, the preceding command defaults to the `OTHERHOST` DNS server as the server we are querying. We want to query the DNS server on AS1 so we change nslookup to use the DNS server AS1 by issuing the nslookup command:

```
server 10.5.69.222    (10.5.69.222 is the IP address of AS1).
```

The `as2.mycompany.com` command yields an answer with two IP addresses; 10.5.69.211 is given first, and 10.5.62.217 is given second. Issuing the command a second time produces an answer with the order of the two IP addresses reversed. Figure 115 on page 124 shows both queries and both responses.

The DNS server AS1 alternates the order that the two IP addresses are given in the query response. This is because the query is coming from a source that is not located on the 10.5.69.192 network nor on the 10.5.62.0. The source, in this case, is the AS/400 `OTHERHOST`, which is located on the 10.1.1.0 network.

```

>
> as2.mycompany.com.
Server: [10.5.69.222]
Address: 10.5.69.222

Name: as2.mycompany.com
Addresses: 10.5.69.211, 10.5.62.217

>
> as2.mycompany.com.
Server: [10.5.69.222]
Address: 10.5.69.222

Name: as2.mycompany.com
Addresses: 10.5.62.217, 10.5.69.211

>

```

Figure 115. =Nslookup Receiving Round Robined IP Addresses for As2

5.9 Summary

In this chapter, we discussed adding a subdomain *OTHERDOMAIN* to the domain of *mycompany.com*. We discussed two methods of handling *OTHERDOMAIN* with respect to the DNS server configuration:

Method 1 demonstrated keeping *OTHERDOMAIN* subdomain within *mycompany.com*'s zone of authority. This means that the DNS server primary for *mycompany.com* (AS1) is configured with the additional *OTHERDOMAIN* hosts. Therefore, Method 1 really is a continuation of the configuration methods discussed in Chapter 3, "Implementing Primary and Secondary DNS Servers" on page 25 except that the new hosts (from the *OTHERDOMAIN* subdomain) have longer domain names.

Method 2 presented delegating the *OTHERDOMAIN* subdomain to a child DNS server. The parent DNS server AS1 is then configured with the hosts residing in *mycompany.com* but without the hosts residing in *OTHERDOMAIN*. The child DNS server *OTHERHOST* is then configured with hosts located in the *OTHERDOMAIN* subdomain.

This chapter also explained verifying the DNS configuration with nslookup, how the mail configuration may change with Method 2, and the concept of round robin/address sorting.

Chapter 6. Split DNS: Hiding Your Internal DNS Behind a Firewall

Now that you have finished the job of implementing DNS, you want to connect the network to the Internet! Your DNS databases contain information too valuable to be exposed to millions of potential hackers. This chapter explains how to configure your DNS to forward requests to the firewall name server when it cannot resolve names outside your company's domain. We also explore mail exchange between your company's internal mail servers and Internet mail servers.

6.1 Scenario 1: Configuring Your DNS to Forward Queries to a Firewall

When connecting your internal network to the Internet, there are many resources that you should protect; your internal domain name server is one of them. Your DNS contains valuable company information that you do not want to expose to hackers.

In the first scenario of this chapter, we discuss how to configure an internal DNS to forward queries to a firewall DNS to resolve external names. The internal name server and internal (secure) mail server run on the same AS/400 system where the Integrated PC Server running the IBM for AS/400 Firewall product is installed.

The firewall DNS server has authority for the public server in the company's public domain (*mycompany.com*) and receives all external access requests for the public server for host name resolution. The firewall DNS is also responsible for resolving Internet host names in response to queries from the internal DNS. When internal users want to browse an Internet Web site specifying its name in the URL, the internal client queries the internal DNS, and it, in turn, forwards the query to the firewall DNS.

Note: The above statement is true for browser clients accessing the firewall through SOCKS and also for stand-alone client applications. For client browsers accessing the firewall through PROXY, the PROXY server in the firewall performs the name resolution, not the client.

This way, you make your corporate domain name space invisible to the outside world. Figure 116 provides an overview of how name resolution queries flow in this environment.

1. The resolver in the PC1 workstation sends a query to the name server configured in its TCP/IP configuration (AS1 in Figure 116).
2. If AS1 DNS finds the host name locally, it sends back the response. If the query is for an external host, the forwarders directive in the AS1 name server tells it to forward the query to the firewall DNS.
3. If the query is for a host that is in the firewall DNS database (primary or cache), the firewall responds immediately. If not, it forwards the query to the ISP DNS.
4. The ISP DNS obtains the answer (or negative response, if the host is not found) and returns it to the firewall DNS.
5. The firewall DNS returns the answer to the internal DNS server in AS1.
6. The internal DNS server sends the answer back to the PC client.

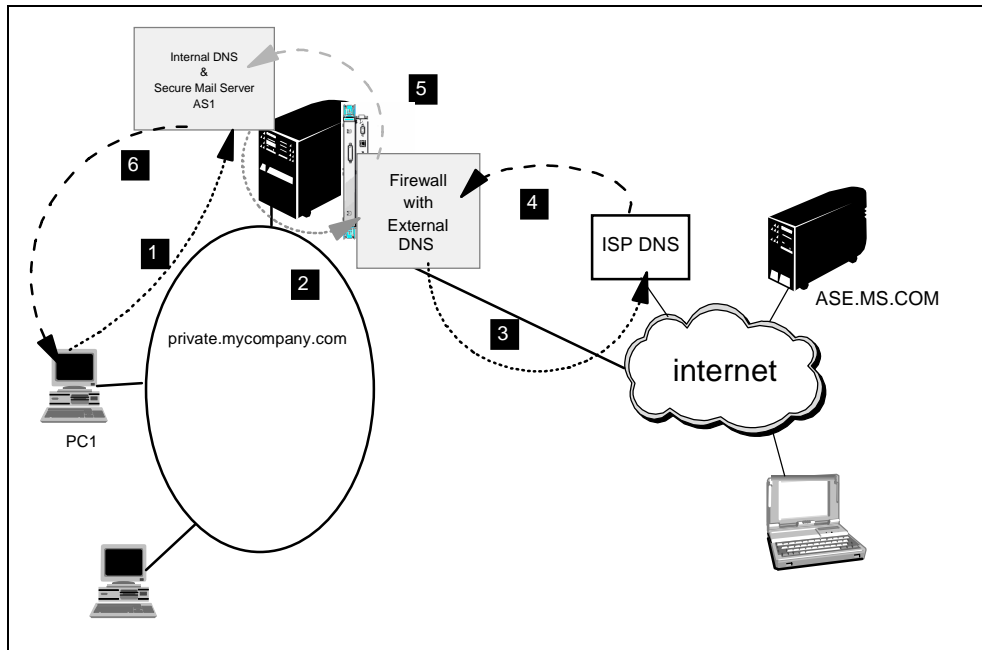


Figure 116. AS/400 as Internal Name Server and Secure Mail Server Behind and Internet Firewall

Tip

The flow diagram in Figure 116 is also valid for internal users querying the company's public servers in front of the firewall. This is true as long as the company's public domain name (*mycompany.com* in our scenario) and the company's internal domain name (*private.mycompany.com* in our scenario) are *not* the same, as is the case in scenario 1.

If the company's internal and public domain names are the same (for example, *mycompany.com* for both internal and public), you must configure address records for the public hosts in front of the firewall in the internal DNS server for the internal name server to resolve the public hosts names. If you do not add A records for the public hosts in the internal DNS server configuration when an internal client queries, for example, *WWW.mycompany.com*, the query receives a negative response. The internal DNS server looks at its own data since it is authoritative for *mycompany.com*. If it does not find the WWW host in its own database, it does not forward the query to the firewall, but returns a negative response instead.

6.1.1 Scenario Objectives

In this scenario, our objectives are to:

1. Show how to configure the internal DNS to forward queries for external hosts to the firewall name server.
2. Show the relationship between the Firewall for AS/400 configuration and the TCP/IP and DNS configurations on the AS/400 system.

3. Show how to change your current firewall configuration to take advantage of the internal DNS implementation of OS/400 V4R2 if your firewall is currently running without internal DNS.
4. Provide an overview of the AS/400 TCP/IP configuration, Firewall for AS/400 configuration, AS/400 DNS server configuration, AS/400 SMTP, and POP server configuration to help you get started in a similar environment.

6.1.2 Scenario Advantages

The main advantages of this scenario are that:

- It shows how easy it is to *safely* make the Internet name space available to your existing network by configuring your internal DNS to forward off-site queries to the DNS running in the firewall.
- It shows how a single AS/400 system can provide DNS services to the secure network, house the Integrated PC Server where the firewall runs, be the secure mail server, and at the same time, be a reliable application server.

6.1.3 Scenario Disadvantages

This scenario is simple and applies mainly to small networks. We discuss more complex environments in later scenarios.

6.1.4 Scenario Network Configuration

Figure 117 shows the testing environment that we used for this scenario.

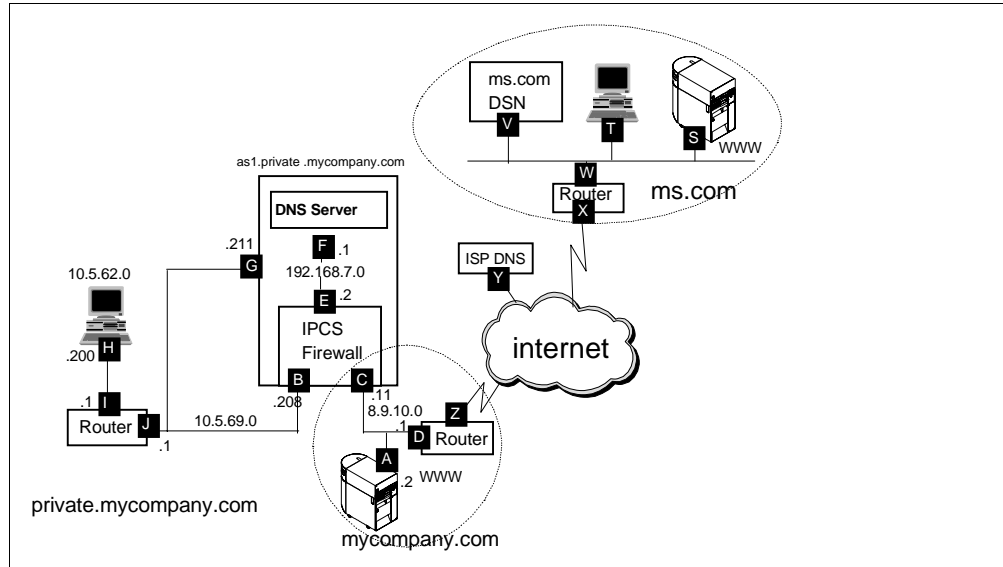


Figure 117. Scenario 1 - Network Topology

Terminology

There are three separate name servers in this scenario:

- Internal name server: DNS server responsible for the company's private name space. It provides name services to hosts in the secure network. In this scenario, this DNS server is authoritative for *private.mycompany.com* and runs on *as1.private.mycompany.com*.
- Firewall name server: DNS server responsible for the company's public name space. It is authoritative for *mycompany.com*, and runs on the firewall.
- External name server: we also call this name server the Sips DNS server. It is the first name server in the Internet the firewall DNS server queries for names outside the company's domain.

The main characteristics of these scenarios are:

- The name server running on the AS/400 system (*as1.private.mycompany.com*) provides name resolution services for hosts that are in the internal (secure) domain (*private.mycompany.com*). It provides authoritative name resolution for names in the internal domain, including the host name of the firewall on the secure interface. The forwarders list is used for name resolution for information *not* in the authoritative data or cache.
- The firewall name server is responsible for resolving external (Internet) host names in response to requests from the internal name server.
- The internal name server must be configured to forward queries to the firewall DNS.
- The firewall name server contains only names that are visible from the Internet such as the public Web server, *WWW.mycompany.com*. The firewall DNS has authority for the public domain *mycompany.com*.
- All inbound mail sent from the Internet to users in *mycompany.com* is forwarded by the firewall mail relay function to the secure mail server specified during the firewall configuration. In this scenario, the secure mail server runs on the AS/400 system where the firewall is installed (*as1.mycompany.com*).

6.2 Task Summary

To implement this scenario, you need to perform the following tasks:

1. Verify the AS/400 TCP/IP configuration.
2. Verify the AS/400 mail configuration.
3. Verify the firewall configuration.
4. Change the internal DNS configuration to forward queries for external hosts to the firewall DNS.
5. Verify the clients configuration.

6.2.1 Verify the AS/400 TCP/IP Configuration on AS1

The following checklist shows the TCP/IP configuration options you need to verify. We assume that they are already configured in your environment.

6.2.1.1 Verify the TCP/IP Interface Configuration

To check the configuration of the TCP/IP interface, do the following steps:

- 1. On an AS/400 command line, type:

CFGTCP

Press **ENTER** to display the Configure TCP (CFGTCP) menu.

- 2. Select option **1** (Work with TCP/IP interfaces) to see the Work with TCP/IP Interfaces display (Figure 118).
- 3. Locate your AS/400 LAN adapter (labeled **G** in Figure 117 on page 127). The LAN adapter is listed under the **Line Description** column.

Work with TCP/IP Interfaces					System:AS1
Type options, press Enter.					
1=Add 2=Change 4=Remove 5=Display 9=Start 10=End					
Opt	Internet Address	Subnet Mask	Line Description	Line Type	
	10.5.69.211	255.255.255.192	AS1LAN	*TRLAN	

Figure 118. Work with TCP/IP Interfaces Display

- 4. Press **F11** to view the status for the LAN adapter and verify that the status is active.

Note

If the TCP/IP interface for the LAN adapter is inactive, you must start the interface by using option **9** on the Work with TCP/IP Interfaces display (Figure 118 on page 129). Then, press **F5** to refresh the display and verify that the interface has started.

After you verify that the LAN adapter is active, you must verify that the AS/400 system host and secure domain names are configured.

6.2.1.2 Verifying the AS/400 System Host and Secure Domain Names

Before you install the firewall, ensure that you have configured a host and secure domain name for the home AS/400 system.

To verify that the AS/400 system has a host and secure domain name, do the following steps:

- 1. On an AS/400 command line, type:

CFGTCP

Press **ENTER** to display the Configure TCP menu.

- 2. Select option **12** (Change TCP/IP domain) to see the Change TCP/IP Domain display (Figure 119).
- 3. Verify that the **Local domain name**, **Local host name**, and name server Internet address fields have the correct values for the secure network.

```

Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . as1

Domain name . . . . . private.mycompany.com


Host name search priority . . . *REMOTE      *REMOTE, *LOCAL, *SAME

Internet address . . . . . 10.5.69.211

```

Figure 119. Change Local Domain and Host Names and Name Server IP Address Display

Note: If you are using the host table in the AS/400 system to resolve any host name to complement the internal DNS, the *Host name search priority* must be *LOCAL. Specifying *LOCAL in this parameter causes the host table to be searched first, and then the internal DNS server is queried.

Note

In this scenario, we assume that the secure network's DNS server runs on the same AS/400 system where the firewall Integrated PC Server is installed. We call this name server the internal name server or internal DNS.

6.2.2 Verify the AS/400 Mail Configuration

The following checklist shows mail-related configuration options you need to verify. We assume they are already configured in your environment.

To route mail for Internet users to the firewall, you must configure the SMTP attributes in the AS/400 system to point to the firewall as the mail router. Enter the name of the firewall in the Mail router field. This tells the STMP server where to forward mail that it cannot deliver itself.

You must enter ***YES** in the Firewall field. This tells the STMP server that it is located behind a firewall.

On an AS/400 command line, type:

```
CHGSMTPA
```

Press **F4**.

Enter the correct values as shown in Figure 120 and press **Enter**.

```

Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

Mail router . . . . . 'firewall.private.company.com'

Coded character set identifier      00819      1-65533, *SAME, *DFT
Mapping tables:
  Outgoing EBCDIC/ASCII table .    *CCSID      Name, *SAME, *CCSID, *DFT
    Library . . . . .              Name, *LIBL, *CURLIB

  Incoming ASCII/EBCDIC table .    *CCSID      Name, *SAME, *CCSID, *DFT
    Library . . . . .              Name, *LIBL, *CURLIB
  Firewall . . . . .              *YES        *YES, *NO, *SAME

```

Figure 120. Simple Mail Transfer Protocol Attributes

Start the SMTP server:

```
STRTCPSVR SERVER(*SMTP)
```

6.2.2.1 Add Mail Users to the System Distribution Directory

Add an entry in the system distribution directory for each mail user. Use the Work with Directory Entry (WRKDIRE) command and option 1, *Add*. Alternatively, you can use the Add Directory Entry (ADDIRE) command. The following displays show **only** the relevant parameters (use option 2, *Change* of WRKDIRE, only to display the parameters you want to see).

```

Change Directory Entry

User ID/Address . . . . : USER1      AS1

Type changes, press Enter.

Description . . . . . Pop user
System name/Group . . . AS1          F4 for list
User profile . . . . . USER1        F4 for list
Network user ID . . . . USER1      AS1

More...

```

Figure 121. Directory Entry for Pop User - General Information

To get to the next display, page down four times.

```

Change Directory Entry

User ID/Address . . . . . :  USER1      AS1

Type changes, press Enter.

Mail service level . . . 2
                                1=User index
                                2=System message store
                                4=Lotus Domino
                                9=Other mail service

For choice 9=Other mail service:
Field name . . . . .      F4 for list

Preferred address . . . . 3
                                1=User ID/Address
                                2=O/R name
                                3=SMTP name
                                9=Other preferred address
                                F4 for list

Address type . . . . .
For choice 9=Other preferred address:
Field name . . . . .      F4 for list
More...

```

Figure 122. Mail Service Level = System Message Storage - Preferred Address = SMTP Name

Press **F19** to configure the SMTP name for the user.

```

Change Name for SMTP
System:  AS1

User ID/Address . . . . . :  USER1      AS1

Type choices, press Enter.

SMTP user ID . . . . .    user1
SMTP domain . . . . .    as1.private.mycompany.com

SMTP route . . . . .

```

Figure 123. User's SMTP Name

4. Start the POP3 Server and Mail Server Framework:

```

STRTCPSVR SERVER(*POP)
STRMSF

```

6.2.3 Firewall Installation and Configuration

Table 1 on page 133 provides a summary of the values used during the firewall installation in our test environment.

Table 1. Firewall Installation Wordiest

Installation		
Integrated PC Server - if you have more than one Integrated PC Server, you need to know which one is the one where you want to install the firewall (for example, CC01). You can use the WRKHDWRSC command to find this information.	CC07	
Firewall Name - create a new unique name for your firewall. This name is also used to create a network server description object (for example, FRW01).	firewall	
	Port 1	Port 2
Type of LAN - Ethernet, 4 Mbps token-ring, or 16 Mbps token-ring.	16M, TRN	16M, TRN
Adapter Address - create a new unique address for each port. This address must not already be used on your LAN (for example, 400000000000 or 020000000000).	400000000001	400000000002
Port IP address * (for example, 10.1.2.3)	10.5.69.208	8.9.10.11
Port Subnet Mask * (for example, 255.255.255.0)	255.255.255.192	255.255.255.0
IP address of your router * (for example, 10.2.3.1)	8.9.10.1	
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.		

At the end of the installation, a summary of the information that you provided is shown in the Complete the Firewall Installation page (Figure 124). Review the information; then click the **Install** button to finish.



Complete the Firewall Installation

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, click the **Install** button to complete the firewall installation. This step takes several minutes to run. Please be patient.

Firewall Name	FIREWALL	
Firewall Language	2924	
Firewall Resource Name	CC07	
Router IP Address	8 . 9 . 10 . 1	

	Port 1	Port 2
LAN Type	Token Ring (16Mb)	Token Ring (16Mb)
Adapter Address	400000000001	400000000002
IP Address	10 . 5 . 69 . 208	8 . 9 . 10 . 11
Subnet Mask	255 . 255 . 255 . 192	255 . 255 . 255 . 0

Figure 124. Firewall Installation Summary Page

Table 2 provides a summary of the values used during the firewall configuration in our test environment.


Table 2. Configuration Worksheet

Configuration	
Secure Mail Server Name - if you have a secure mail server, enter the name here. For example, if the mail server's host name is mailsvr and it is part of the domain mynetwork.mycompany.com, then enter: mailsvr.mynetwork.mycompany.com	asl.private.mycompany.com
Secure Port - if your Integrated PC Server has two ports, you need to know which one is attached to your secure port.	port 1
Non-Secure Domain Name * - this is the domain that is outside of the firewall and accessible by outsiders. If your secure domain name is mynetwork.mycompany.com, you probably should name your non-secure domain mycompany.com.	mycompany.com
Non-Secure Domain Name Server IP Addresses * (for example, 208.222.150.7)	7.10.10.240
Non-Secure Hosts * - list the names and IP addresses of up to four non-secure hosts. These are systems that are placed outside of the firewall. For example, you may want to place a WWW server machine outside of the firewall.	WWW - 8.9.10.2
Proxy Server - decide which services you want to configure.	HTTP,HTTPS

Table 2. Configuration Worksheet

Configuration	
SOCKS Server - decide which services you want to configure.	HTTP, HTTPS
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.	

At the end of the configuration, a summary of the information that you provided is shown in the Review Configuration page (Figure 125, Figure 126, and Figure 127 on page 136). Review the information; then click on **OK** to finish.



Review Configuration

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, print the page for future reference. This creates all the firewall configuration settings including those for IP packet filtering, domain name serving (DNS), proxy serving, and sockets serving (SOCKS). This may take a few minutes to run, so please be patient.

Secure Port IP Address:

☒ Port 1 IP Address: 10.5.69.208

☐ Port 2 IP Address: 8.9.10.11

Secure Domain Name: private.mycompany.com

Secure Domain Name Servers:

10.5.69.211

Secure Mail Server: .private.mycompany.com

Figure 125. Firewall Review Configuration (1 of 3)

Non-Secure Domain Name:

mycompany.com

Non-Secure Domain Name Servers:	7	.	10	.	10	.	240
		.		.		.	
		.		.		.	
		.		.		.	

Non-Secure Hosts: A non-secure host is a system placed outside of the Firewall. The non-secure domain name is automatically appended to the non-secure hostname. Therefore, if you have any non-secure hosts, you should only input the host names here.

Non-Secure Hosts	Non-Secure Host IP Addresses
www	8 . 9 . 10 . 2

Figure 126. Firewall Review Configuration (2 of 3)

Outbound enabled services:

	Proxy Server	Sockets Server (SOCKS)
Web Server (HTTP)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Secure Web Server (HTTPS)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Transfer Protocol (FTP)	<input type="checkbox"/>	<input type="checkbox"/>
Telnet	<input type="checkbox"/>	<input type="checkbox"/>
Gopher	<input type="checkbox"/>	<input type="checkbox"/>
Wide Area Information Servers (WAIS)	<input type="checkbox"/>	
Internet Relay Chat (IRC)		<input type="checkbox"/>

RealAudio Yes ☐ No ☒

OK Cancel

Figure 127. Firewall Review Configuration (3 of 3)

After you install and configure the firewall, the network server description that contains the firewall configuration points to the name server configured in the AS/400 (using the CHGTCPDMN command). This is the internal DNS server. The firewall as a TCP/IP host belongs to your internal network (domain *private.mycompany.com*).

Figure 128 shows the internal and external name servers configured in the firewall. The internal DNS server IP address matches the name server Internet address in the AS/400 system where the firewall is installed. The external DNS server is usually the ISP DNS server IP address specified during the firewall configuration.

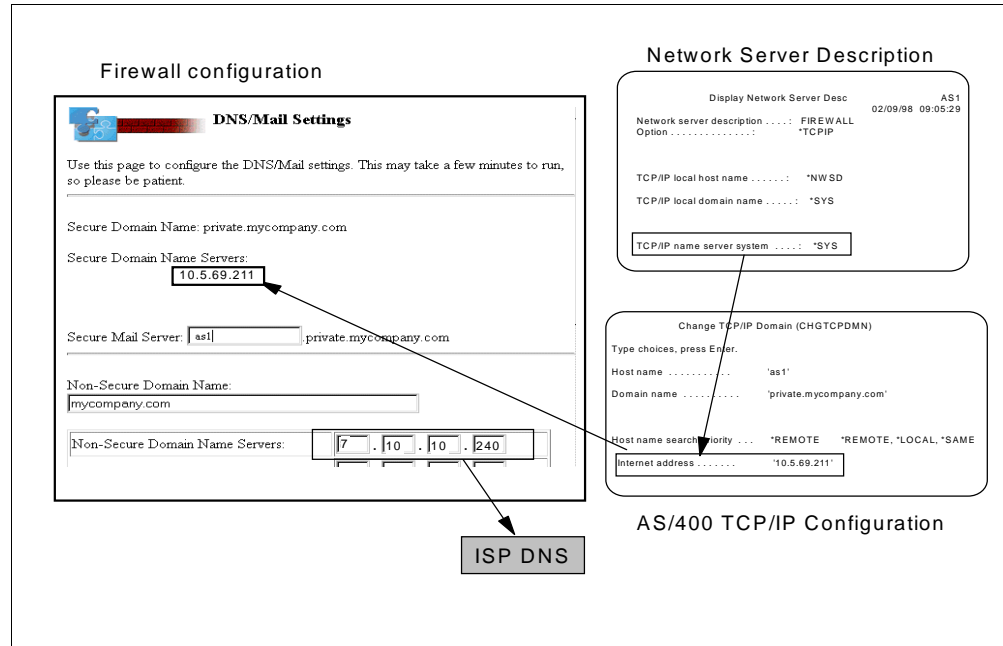


Figure 128. Firewall DNS Server Configuration

When the proxy server in the firewall receives a URL from a browser, it queries the internal DNS server to resolve the name. Usually, it is an Internet host not known by the internal name server. The internal DNS server is configured to forward queries to the firewall DNS server that it cannot resolve. At that point, the firewall DNS queries the ISP DNS.

When inbound mail for users in the *mycompany.com* domain reaches the firewall mail relay, the resolver queries the internal DNS server, on behalf of SENDMAIL (the mail relay program in the firewall) to resolve the IP address for the secure mail server specified in the firewall configuration.

6.2.3.1 Firewall DNS Filters

The firewall basic configuration adds filters to prevent direct queries and responses to and from the internal DNS and the Internet DNS. All queries and responses must go through the DNS in the firewall (*routing is local*). Figure 129 shows the DNS filters created by basic configuration in the firewall.

```
#####
### Both-side settings
#####

permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 udp eq 53 eq 53 both local both
  f=y l=n t=0 # Permit servers to query & reply to each other.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 udp eq 53 ge 1024 both local both
  f=y l=n t=0 # Permit nameserver to reply to clients.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 udp ge 1024 eq 53 both local both
  f=y l=n t=0 # Permit clients to query nameserver.

#####
### Non-Secure side settings
#####

permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp eq 53 eq 53 non-secure local
  both f=y l=n t=0 # Permit external & firewall dns to query & reply to
  each other.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 53 eq 53 non-secure
  local both f=y l=n t=0 # Permit reply.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp ge 1024 eq 53 non-secure local
  inbound f=y l=n t=0 # Permit external client queries to firewall dns.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 53 ge 1024 non-secure
  local outbound f=y l=n t=0 # Permit reply.
#####
### Secure side settings
#####

permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp eq 53 eq 53 secure local
  inbound f=y l=n t=0 # Permit internal dns to query firewall dns.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 53 eq 53 secure local
  outbound f=y l=n t=0 # Permit reply.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp ge 1024 eq 53 secure local
  both f=y l=n t=0 # Permit internal client queries to firewall dns.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 53 ge 1024 secure local
  both f=y l=n t=0 # Permit reply.
```

Figure 129. Firewall DNS Filters

DNS queries and responses are most often contained within UDP packets. Zone transfers are over TCP. Notice that the filters allowed both protocols.

6.2.4 Updating the Firewall Configuration to Use the Internal DNS

If you already have IBM Firewall for AS/400 configured to work with no internal DNS, you can now change the configuration to take advantage of the V4R2 DNS support. If this is the case, you probably have configured the firewall as explained in Chapter 4 of the ITSO redbook, *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162. You need to change:

- The *TCP/IP name server* parameter in the firewall network server description to point to the internal DNS. Use the following steps:
 1. Verify the domain name server Internet address configured in the AS/400 system where the firewall Integrated PC Server is installed. See Figure 119 on page 130.
 2. End the firewall application:

```
ENDNWSAPP NWSAPP(*FIREWALL) NWS(FIREWALL)
```

3. Vary off the firewall network server description:

```
VRYCFG CFGOBJ(FIREWALL) CFGTYPE(*NWS) STATUS(*OFF)
```

4. Change the firewall network server description to reset the *TCP/IP name server system* parameter to ***SYS**:

```
CHGNWSD NWSD(FIREWALL) TCPNAMSVR(*SYS)
```

5. Vary on the firewall network server description:

```
VRYCFG CFGOBJ(FIREWALL) CFGTYPE(*NWS) STATUS(*ON)
```

This updates the firewall configuration to take the new value for the name server.

6. Start the firewall application:

```
STRNWSAPP NWSAPP(*FIREWALL) NWS(FIREWALL)
```

- The firewall DNS configuration. Before V4R2, you did not have a DNS server in the secure network that the mail relay function in the firewall could query to find the secure mail server to deliver inbound mail. Therefore, you had to configure the secure mail server in the firewall DNS so that it could resolve the IP address of the secure mail server. To do that, you configured the firewall DNS using the Advanced Domain Name Server settings. Now (V4R2) that you have an internal DNS server, you can delete those changes to use the internal DNS server to locate the secure mail server. Complete the following steps:

1. Go to firewall **Configuration**.
2. Click on **DNS/Mail**.
3. Verify the values for the Secure Domain Name Server and Secure Mail Server. Click on **OK** and click on **Done** to quit.
This removes the changes that you made using the Advanced Domain Name Server configuration option of the firewall.
4. Go to firewall **Administration**.
5. At the Administration menu, click on **Status**.
6. Restart the DNS and Mail firewall functions shown in Figure 130 and click on **OK**.

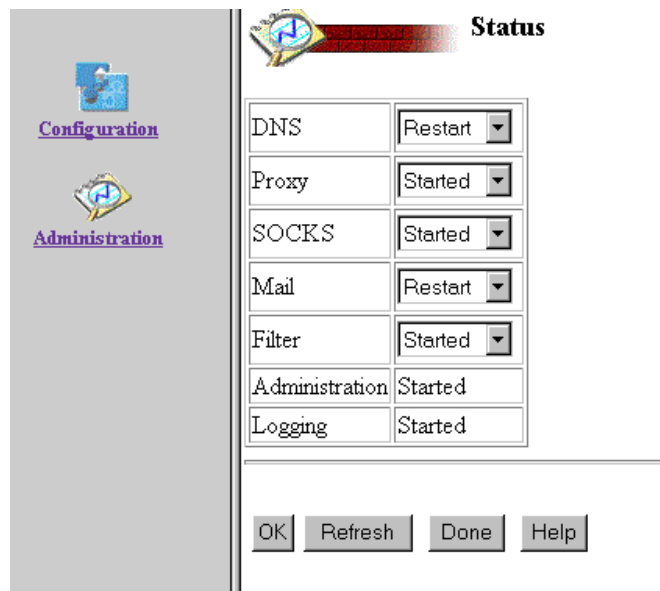


Figure 130. Restarting DNS and Mail Functions in the Firewall

6.2.5 Configuring Forwarders in the Internal DNS

If you designate the firewall name server in your internal DNS as *forwarders*, all off-site queries are sent to the forwarders. The DNS in the firewall builds a rich cache of information. For a given query in a remote domain, there is a probability that the firewall DNS can answer the query from its cache.

One advantage of using only forwarders for off-site queries is having the large cache of the forwarder server available to all the systems using it.

To configure the forwarders directive to send unresolved queries to the firewall DNS, use the following steps:

1. Go to the DNS configuration for *as1.private.mycompany.com* through Operations Navigator.
2. Right-click on DNS Server - *as1.private.mycompany.com* and select **Properties**.
3. Click on the **Forwarders** tab.
4. Click on **Add** to add the IP address of the firewall secure port shown in Figure 131.

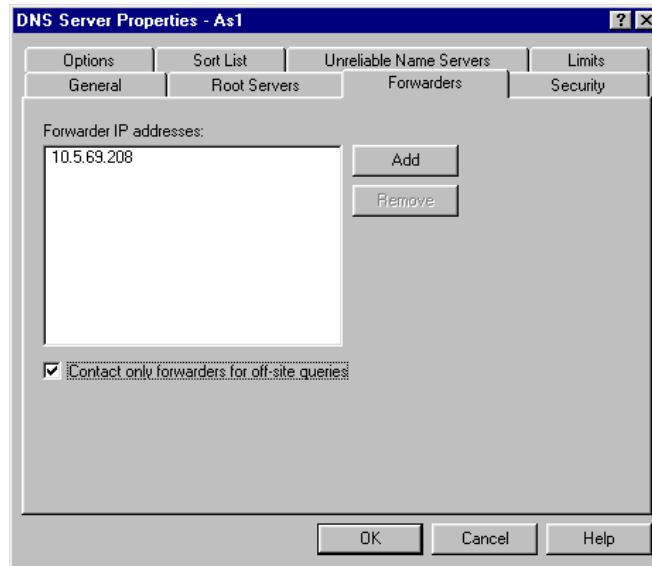


Figure 131. Adding the Firewall Secure Port IP Address to the Forwarders List

5. Click on **Contact only forwarders for off-site queries**. This field specifies whether you want to use the DNS server as a slave server to the forwarder servers. This means that, if the DNS server cannot respond to a query for an address based on its authoritative data or its cache, you want the DNS server to forward queries based only on your list of forwarder servers. The DNS server does not forward queries to other domain servers or root servers. The DNS server forwards queries to only those in the Forwarder IP address list shown in Figure 131.
6. Click on **OK** and close the DNS server configuration.

For completeness, we include the configuration of the DNS server running in AS1 during our tests.

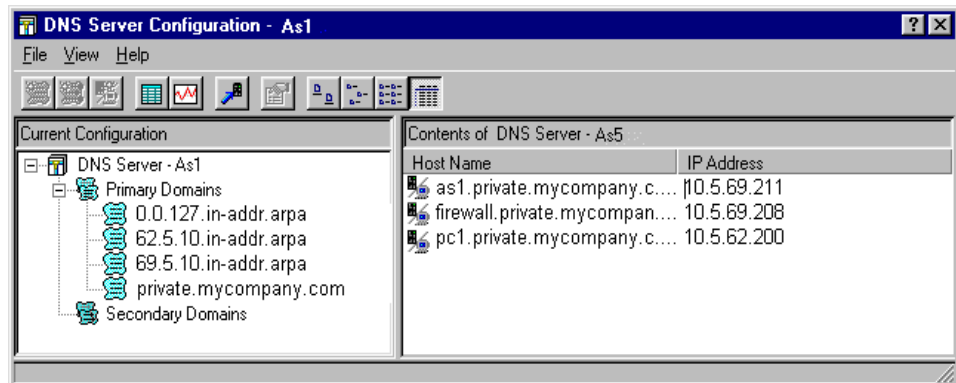


Figure 132. DNS Server Configuration - as1.private.mycompany.com

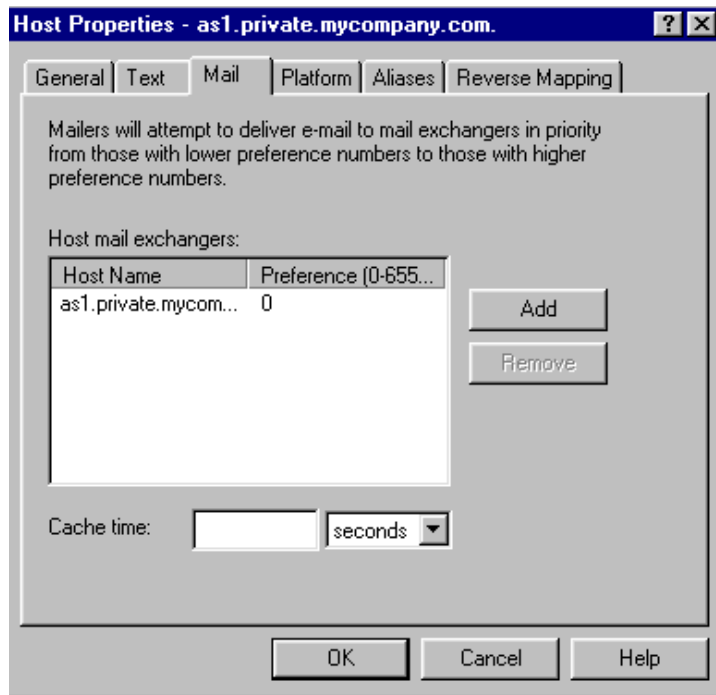


Figure 133. Mail Exchanger Configuration

6.2.6 Client Configuration

The clients used in this scenario must have the internal DNS server specified in their DNS server configuration for name resolution. Figure 134 shows the DNS configuration for a Windows 95 client (PC1 in our scenario).

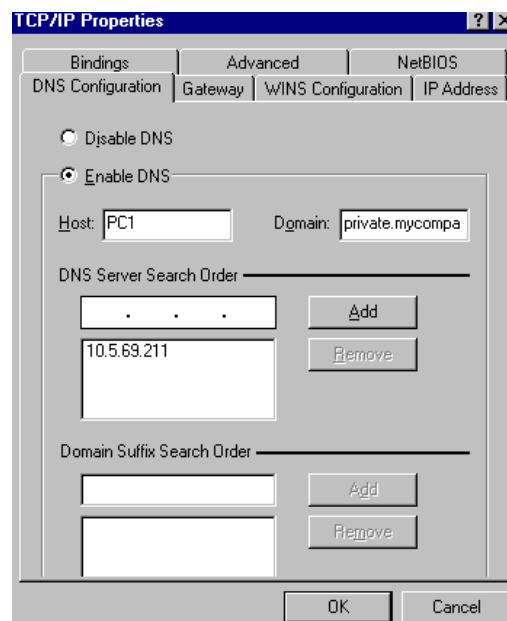


Figure 134. DNS Server Configuration in Windows 95

The browser proxy and SOCKS configuration must point to the firewall secure port as shown in Figure 135.

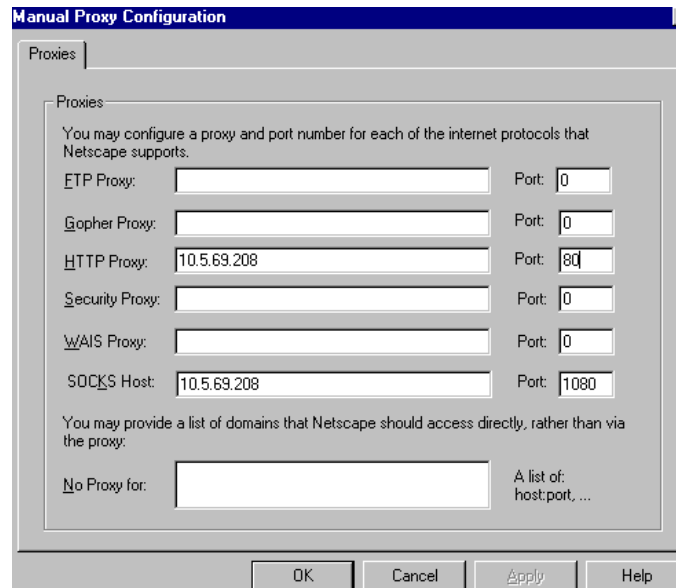


Figure 135. Netscape Browser Proxy and SOCKS Configuration

The POP client must point to the secure SMTP mail server for outgoing mail and POP3 server for incoming mail. Figure 136 and Figure 137 show the Netscape browser mail preferences used in our scenario.

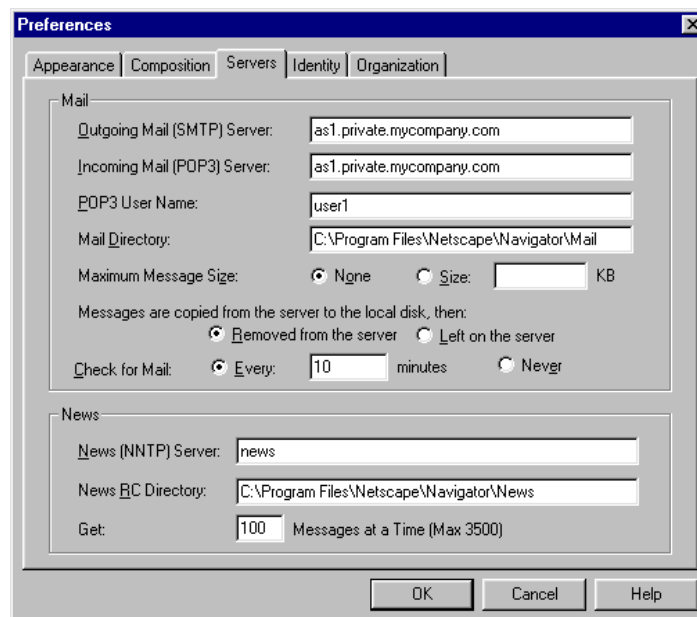


Figure 136. POP3 Client Mail Servers Configuration

Note: The POP3 User Name must match the user ID specified in Figure 121 on page 131.

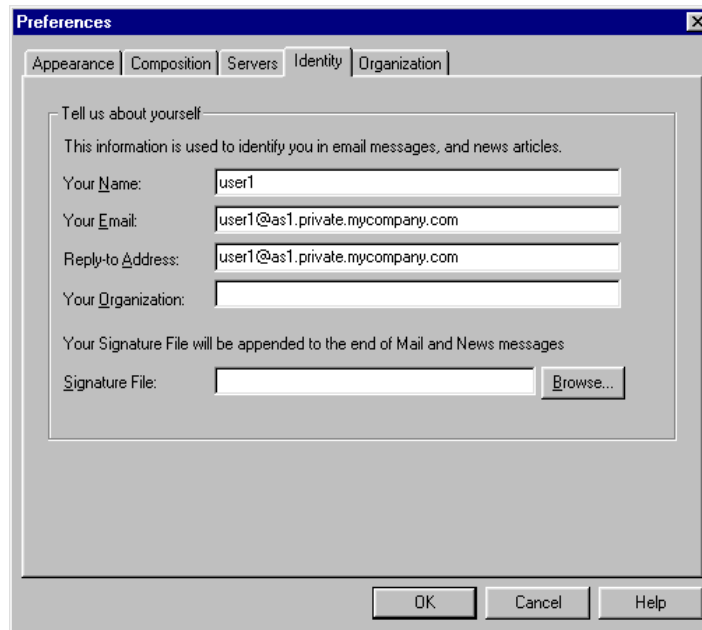


Figure 137. POP3 Client Identity Configuration

6.3 Sharing a LAN Adapter Between the AS/400 and Integrated PC Server

The Integrated PC Server (IPCS) requires two LAN connections for firewall functions. One LAN adapter is connected to the internal secure network and the other to the unsecure network (for example, the Internet). Although we recommend that the AS/400 system on which the firewall is installed have a LAN adapter of its own for connection to the internal secure network, this is not possible on all AS/400 models. Fortunately, the Integrated PC Server (IPCS) provides the ability to share its LAN adapters with the AS/400 system on which it is installed. Only the LAN adapter connected to the internal (secure) network should be shared. The LAN adapter connected to the unsecure network should not be shared because it can bypass firewall functions.

Note

Communication between the firewall application running on the Integrated PC Server and applications running on the AS/400 system that houses the Integrated PC Server, can only flow between the *INTERNAL ports. In other words, both hosts (the AS/400 and the Integrated PC Server) **cannot** talk to each other through the IP interfaces configured over the shared LAN adapter.

In this section, we explain how to implement Scenario 1 in this chapter when the AS/400 system and the Integrated PC Server must share the same LAN adapter. For complete configuration information of the AS/400 system and firewall in this situation, refer to the AS/400 firewall home page (<http://www.as400.ibm.com/tstudio/firewall/fwindex.htm> —>Resources —>Tech Tips) or the redbook *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162.

When configuring the AS/400 system and the firewall in this situation, you must keep in mind that all communication between both hosts must flow through the *INTERNAL ports.

Figure 138 shows that the AS/400 system, which houses the Integrated PC Server where the firewall is installed, and the Integrated PC Server share the same LAN adapter. The AS/400 interface 10.5.69.211 (labeled **G** in Figure 138) and the Integrated PC Server secure port IP interface 10.5.69.208 (labeled **B** in Figure 138) are configured over the same LAN adapter, which is the secure port of the firewall.

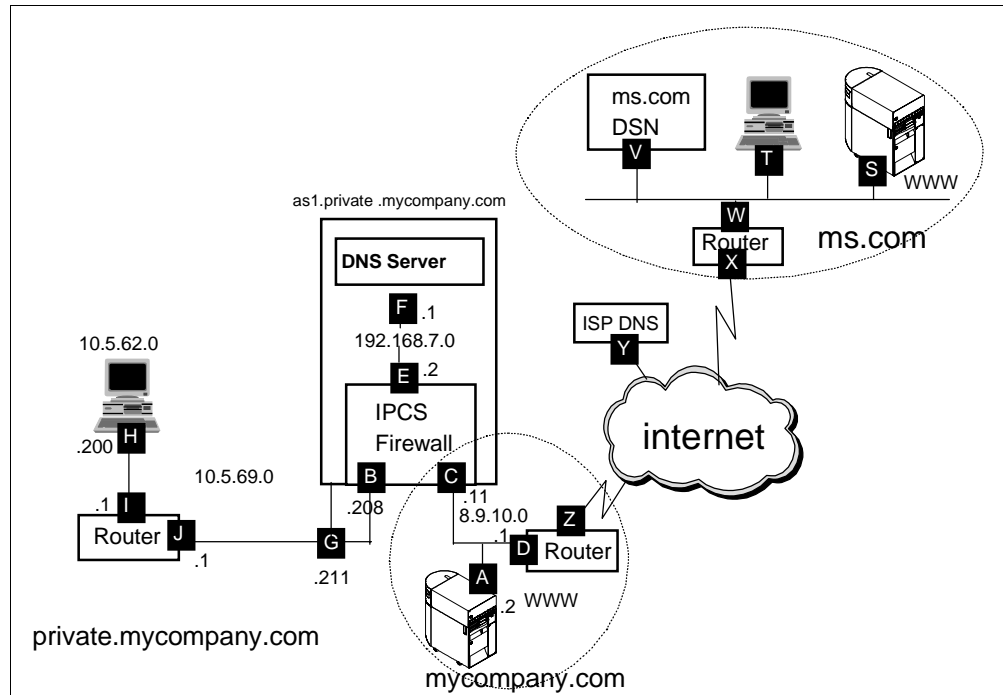


Figure 138. AS1 and Firewall Sharing LAN Adapter

6.3.1 AS/400 System TCP/IP Configuration

The following sections summarize the TCP/IP configuration in the AS/400 system that houses the firewall Integrated PC Server.

6.3.1.1 TCP/IP Interface Configuration

Configure the AS/400 system IP interface for communication with the internal or secure network on the same line description as the one used by the firewall secure port. This configuration shows how both hosts share the same LAN adapter.

Figure 139 shows the results of CFGTCP option 1, *Work with TCP/IP interfaces*.

```

Work with TCP/IP Interfaces
System: AS1

Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display 9=Start 10=End

Internet Subnet Line Line
Opt Address Mask Description Type

10.5.69.211 255.255.255.0 FIREWALL01 *TRIAN
192.168.7.1 255.255.255.0 FIREWALL00 *TRIAN

```

Figure 139. AS/400 External IP Interface Configured Over FIREWALL01 Line Description

6.3.1.2 AS/400 System Host and Secure Domain Names

The internal DNS server runs on the AS/400 system in this scenario. When the firewall resolver queries the internal DNS (for example, to locate the MX record for the secure mail server), it should use the AS/400 system *INTERNAL port IP address, 192.168.7.1 in this scenario. The AS/400 resolver can also use the *INTERNAL port IP address to query the internal DNS server. Configure the AS/400 system *INTERNAL port IP address in the *Internet address* field of the Change TCP/IP Domain (CHGTCPDMN) command. The firewall installation program uses this value by default as the internal DNS server IP address when it creates the firewall network server description (NWSD).

Configure the *Host name search priority* field in the CHGTCPDMN command as *LOCAL. Later, you will configure a TCP/IP host table entry on the AS/400 system with the firewall name and *INTERNAL port IP address. Search priority *LOCAL causes SMTP to find this host table entry.

Figure 140 shows the configuration values in the CHGTCPDMN command (or CFGTCP option 12).

```

Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . as1

Domain name . . . . . private.mycompany.com

Host name search priority . . . *LOCAL *REMOTE, *LOCAL, *SAME

Internet address . . . . . 192.168.7.1

```

Figure 140. Internal DNS IP address is AS/400 System's *INTERNAL Port - Search Priority *LOCAL

6.3.1.3 AS/400 System TCP/IP Host Table Entries

For the AS/400 system to resolve the mail router name (*firewall.private.mycompany.com*) to the firewall *INTERNAL port IP address, you must configure an entry for the firewall on the AS/400 TCP/IP host table. Figure 141 shows the TCP/IP host table configuration (CFGTCP option 10).

Work with TCP/IP Host Table Entries

System: AS1

Type options, press Enter.

1=Add
2=Change
4=Remove
5=Display
7=Rename

Internet Opt	Address	Host Name
	192.168.7.2	FIREWALL
		FIREWALL.PRIVATE.MYCOMPANY.COM

Figure 141. Firewall Configuration on AS/400 TCP/IP Host Table

6.3.1.4 AS/400 System SMTP Attributes Configuration

The SMTP attributes configuration is the same as in the situation where the LAN adapter is not shared by the AS/400 system and the firewall Integrated PC Server. Figure 120 on page 131 shows the SMTP attributes configuration on the AS/400 system.

6.3.2 Firewall Configuration

The procedure to install and configure the firewall is the same as the one described in Section 6.2.3, “Firewall Installation and Configuration” on page 133. The only difference is that, when the firewall and the AS/400 system share the secure port’s LAN adapter, the Secure Domain Name Server in the firewall configuration must be the AS/400 *INTERNAL port IP address. The installation program uses the value specified in the domain name server configuration of the AS/400 system, as we explained in Section 6.3.1.2, “AS/400 System Host and Secure Domain Names” on page 146.

Figure 142 shows the firewall DNS/Mail settings in this environment.

DNS/Mail Settings

Use this page to configure the DNS/Mail settings. This may take a few minutes to run, so please be patient.

Secure Domain Name: PRIVATE.MYCOMPANY.COM

Secure Domain Name Servers: 192.168.7.1

Secure Mail Server: as1.PRIVATE.MYCOMPANY.COM

Non-Secure Domain Name: mycompany.com

Non-Secure Domain Name Servers: 7, 10, 10, 240

Non-Secure Hosts: www, 8, 9, 10, 2

Non-Secure Hosts: A non-secure host is a system placed outside of the Firewall. The non-secure domain name is automatically appended to the non-secure hostname. Therefore, if you have any non-secure hosts, you should only input the host names here.

Figure 142. Firewall DNS/Mail Settings - Secure DNS Server is AS/400 *INTERNAL Port IP Address

6.3.3 Internal DNS Server Configuration

The DNS server configuration in this environment must include:

- A forwarder directive pointing to the firewall *INTERNAL port IP address (E in Figure 138 on page 145). Remember that the DNS server application running on the same AS/400 system where the firewall is installed and the firewall Integrated PC Server can only communicate through the *INTERNAL ports. See Figure 143.

DNS Server Properties - As1.private.mycompany.com

Options | Sort List | Unreliable Name Servers | Limits

General | Root Servers | Forwarders | Security

Forwarder IP addresses:

192.168.7.2

Add

Remove

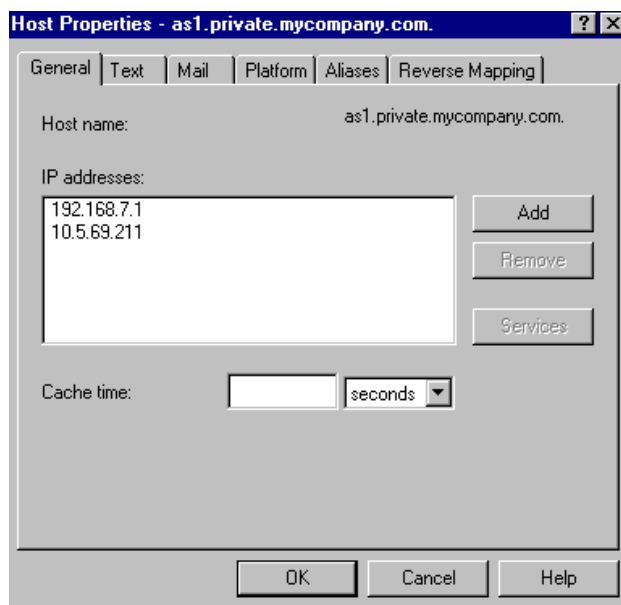
☒ Contact only forwarders for off-site queries

OK Cancel Help

Figure 143. Adding the Firewall *INTERNAL Port IP Address to the Forwarders List

- Two A (address) records for the AS/400 system. One A record has the IP address of the AS/400 system external interface configured over the shared

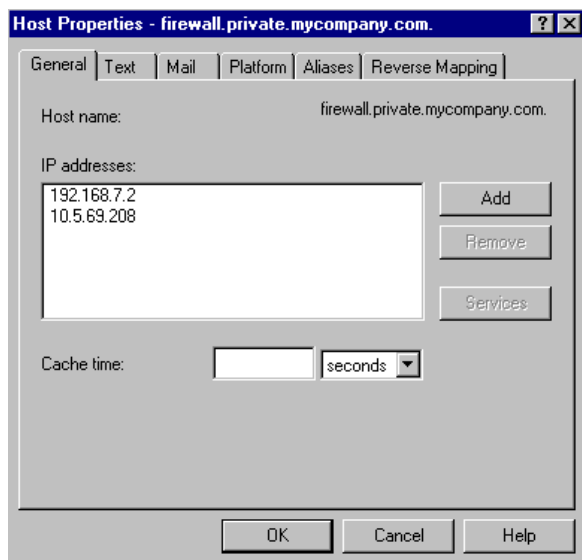
LAN (**G** in Figure 138 on page 145), for communication with hosts in the secure network. The other A record has the IP address of the AS/400 system *INTERNAL port (**F** in Figure 138 on page 145) for communication with the firewall. See Figure 144.



The screenshot shows the 'Host Properties' dialog box for the host 'as1.private.mycompany.com'. The 'General' tab is selected. The 'Host name' field contains 'as1.private.mycompany.com.'. The 'IP addresses' list contains two entries: '192.168.7.1' and '10.5.69.211'. To the right of the list are buttons for 'Add', 'Remove', and 'Services'. Below the list is a 'Cache time' field with a dropdown menu set to 'seconds'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Figure 144. Configuring AS1 External and *INTERNAL Ports IP Addresses

- Two A (address) records for the firewall. One A record has the IP address of the firewall secure port (**B** in Figure 138 on page 145) for communication with hosts in the secure network. The other A record has the IP address of the firewall *INTERNAL port (**E** in Figure 138 on page 145) for communication with the AS/400 system. See Figure 145.



The screenshot shows the 'Host Properties' dialog box for the host 'firewall.private.mycompany.com.'. The 'General' tab is selected. The 'Host name' field contains 'firewall.private.mycompany.com.'. The 'IP addresses' list contains two entries: '192.168.7.2' and '10.5.69.208'. To the right of the list are buttons for 'Add', 'Remove', and 'Services'. Below the list is a 'Cache time' field with a dropdown menu set to 'seconds'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Figure 145. Configuring Firewall External and *INTERNAL Ports IP Addresses

Tip

When a host in the secure network (IP address 10.5.0.0) queries the internal DNS server for the firewall's IP address, the query comes over the external IP interface, and the DNS server returns the closer IP address to that host, 10.5.69.208. When the firewall queries the internal DNS server for AS1's IP address, the query comes through the *INTERNAL port and the DNS returns the IP address of the AS/400 *INTERNAL port.

In this environment, the DNS server running on *as1.private.mycompany.com* is also primary for the reverse mapping 7.168.192.in-addr.arpa. domain.

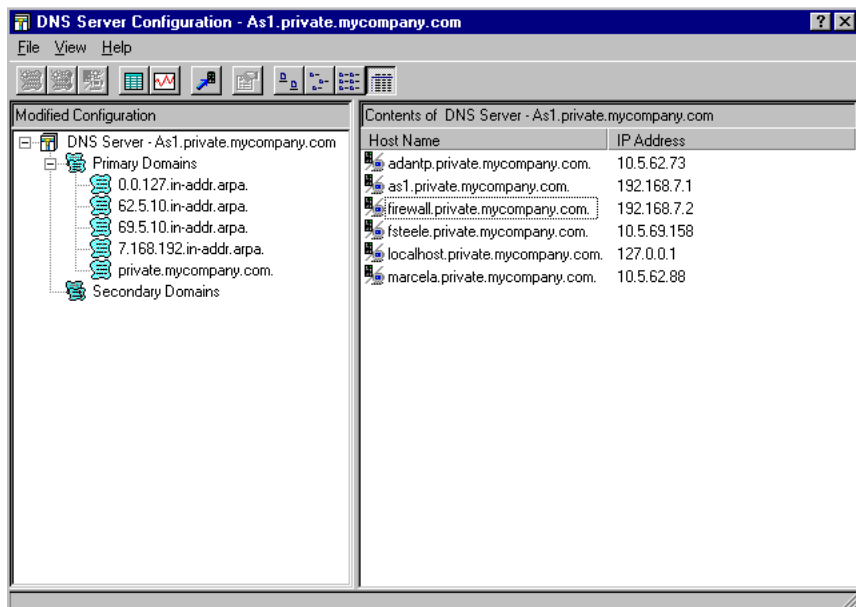


Figure 146. Internal DNS Server Configuration in AS1

There must be an MX record for the secure mail server configured in the firewall.

Figure 147 shows the mail exchanger configuration.

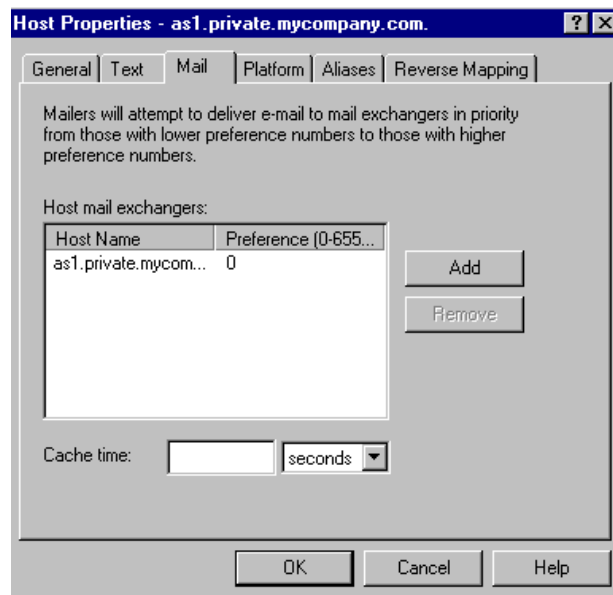


Figure 147. Mail Exchanger Configuration - Secure Mail Server

Figure 148 shows the content of the forward mapping file for the *private.mycompany.com* domain.

```
private.mycompany.com. IN SOA as1.private.mycompany.com. postmaster.as1.private.mycompany.com. (
    893098040
    10800
    3600
    604800
    86400 )
private.mycompany.com. IN NS as1.private.mycompany.com.
as1.private.mycompany.com. IN A 192.168.7.1
as1.private.mycompany.com. IN A 10.5.69.211
as1.private.mycompany.com. IN MX 0 as1.private.mycompany.com.
fsteele.private.mycompany.com. IN A 10.5.69.158
adantp.private.mycompany.com. IN A 10.5.62.73
marcela.private.mycompany.com. IN A 10.5.62.88
localhost.private.mycompany.com. IN A 127.0.0.1
firewall.private.mycompany.com. IN A 192.168.7.2
firewall.private.mycompany.com. IN A 10.5.69.208
```

Figure 148. Content of *private.mycompany.com.DB* file

Figure 148 shows the content of the boot file for the AS1 DNS server.

```
directory /QIBM/UserData/OS400/DNS
forwarders 192.168.7.2
options forward-only
limit transfers-in 10
limit transfers-per-ns 2
options query-log
primary private.mycompany.com private.mycompany.com.DB
primary 62.5.10.in-addr.arpa 62.5.10.in-addr.arpa.DB
primary 7.168.192.in-addr.arpa 7.168.192.in-addr.arpa.DB
primary 0.0.127.in-addr.arpa 0.0.127.in-addr.arpa.DB
primary 69.5.10.in-addr.arpa 69.5.10.in-addr.arpa.DB
cache . CACHE
```

Figure 149. Boot File in AS1 DNS Server

6.4 Scenario 2: Multiple Mail Servers Behind the Firewall

In this scenario, we are building on what we discussed in “Scenario 1: Configuring Your DNS to Forward Queries to a Firewall” on page 125. The private network now has three mail servers: ASM, AS1, and AS2, which is also the secure mail server. All inbound mail from the Internet is relayed by the firewall to the secure mail server (AS2). The *forwarding* function in AS2 forwards the mail for the users to the corresponding internal mail server (AS1, ASM, or delivers it locally for AS2 users). For an overview of the mail concepts that you need as background to this scenario, refer to Appendix A.1, “Basic Mail Configuration” on page 431). Internal mail for internal users is delivered to the corresponding internal mail server. Outbound mail sent from the internal users to Internet users is relayed by the firewall to the corresponding Internet mail server. Figure 150 provides an overview of how outbound mail is forwarded from the internal mail servers to the firewall configured as mail router in each system in the secure network. The figure shows how inbound mail received by the firewall mail relay function is passed to the secure mail server (AS2) and forwarded to the internal mail servers based on the mail recipient.

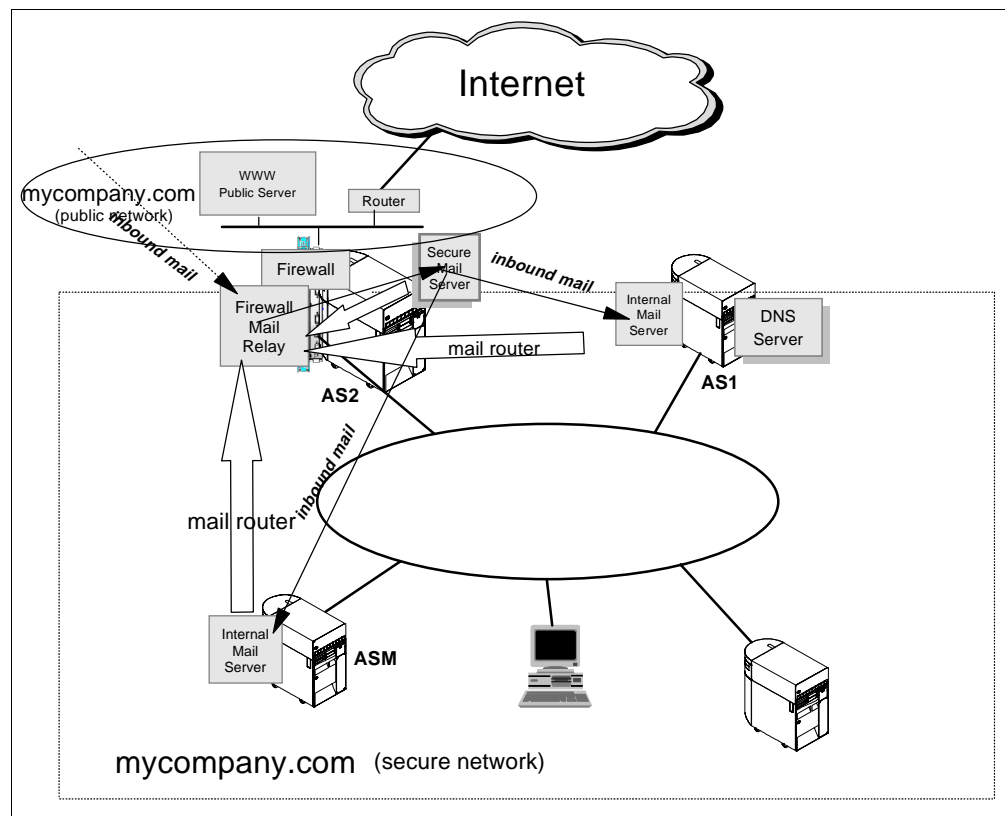


Figure 150. Multiple Internal Mail Servers Behind the Internet Firewall

6.4.1 Scenario Objectives

In this scenario, our objectives are to:

1. Show how to configure the internal DNS to route internal mail to the appropriate mail exchanger in the secure network (AS1, AS2, or ASM).

2. Show how to implement the forwarding function in the secure mail server (AS2) so that inbound mail from the Internet is delivered to the appropriate internal mail server based on the recipient's user ID.

6.4.2 Scenario Network Configuration

Figure 151 shows the testing environment that we used for this scenario.

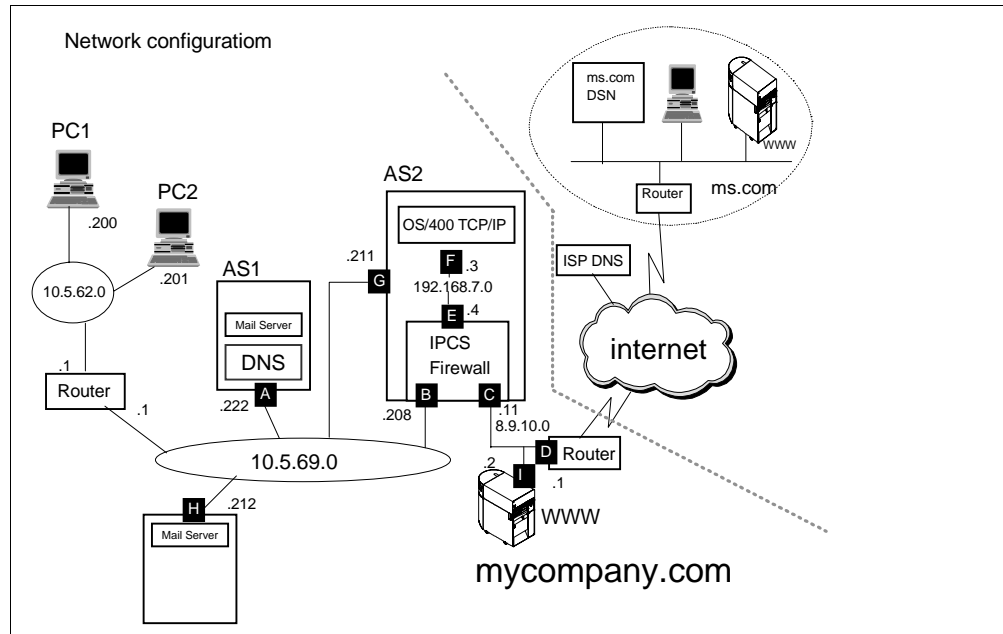


Figure 151. Scenario 2 - Network Topology

The main characteristics of this scenario are:

1. The firewall relays all inbound mail from the Internet destined to *mycompany.com* users to the secure mail server *as2.mycompany.com*.
2. For inbound mail, the firewall changes the recipient's domain *user@mycompany.com* to *user@as2.mycompany.com*. For outbound mail, the firewall changes the originator's name from *user@asx.mycompany.com* to *user@mycompany.com*.

Note: ASx represents the originator's mail server's system name.

3. The secure domain name is the same as the public domain name (*mycompany.com*).
4. All internal mail servers route mail for Internet domains to the firewall.

6.4.3 Scenario Advantages

The advantages of this scenario are that:

- All mail servers in the internal network are protected by a single firewall.
- Internet inbound mail for all internal users (regardless of the internal mail server they are on) is addressed to the *user@public_domain*; the firewall forwards all inbound mail to the secure mail server.

- Using the mail forwarding function in the secure mail server, we forward the mail to the user at the appropriate internal mail server.

6.4.4 Scenario Disadvantages

The main disadvantages of this scenario are:

- To forward mail to users at internal mail servers using the mail forwarding function, you must configure a system distribution directory entry for every user in the secure mail server.
- The firewall does not hide all of the internal network information (mail server host name and domain name) for users in the CC: list. This causes problems if the recipient of the mail in the Internet uses the Reply All function to respond. We show a circumvention to this problem in Section 6.5.5, “Considerations for Exchanging Mail with Internet Users” on page 167.

6.5 Task Summary

To implement this scenario, you need to perform the following tasks:

1. Verify the AS/400 TCP/IP configuration.
2. Verify the AS/400 mail configuration. Mail for domains other than *mycompany.com* must be routed to the firewall mail relay.
3. Verify the firewall configuration.
4. Configure the internal DNS server to forward mail to the appropriate internal mail server based on the recipient’s domain.
5. Configure the internal DNS to forward name resolution for hosts outside *mycompany.com* to the firewall DNS.

6.5.1 Verify the AS/400 TCP/IP Configuration

In this section, we merely summarize the TCP/IP configuration used in our test environment. Table 3 summarizes the TCP/IP configuration values used in our test network.

Table 3. Scenario 2 - TCP/IP Configuration Summary

TCP/IP Configuration	AS1	AS2	ASM
IP address (CFGTCP op. 1)	10.5.69.222 (A)	10.5.69.211 (G)	10.5.69.212 (H)
Host Name (CFGTCP op. 12)	AS1	AS2	ASM
Domain Name (CFGTCP op. 12)	<i>mycompany.com</i>	<i>mycompany.com</i>	<i>mycompany.com</i>
Host name search priority (CFGTCP op. 12)	*REMOTE	*REMOTE	*REMOTE
DNS Internet address (CFGTCP op. 12)	10.5.69.222 (A)	10.5.69.222 (A)	10.5.69.222 (A)

Note: The letters in bold between brackets refer to the ports shown in Figure 151 on page 154.

6.5.2 Verify the AS/400 Mail Configuration

This section provides a summary of the mail configuration required in each internal mail server. Refer to Appendix A.1, “Basic Mail Configuration” on page 431 for background information.

Table 4 shows a summary of the mail configuration used in our test network.

Table 4. Scenario 2 - Mail Configuration Summary

Mail Configuration	AS1	AS2	ASM
Mail router (CHGSMTPA)	firewall.mycompany.com	firewall.mycompany.com	firewall.mycompany.com
Firewall (CHGSMTPA)	*YES	*YES	*YES
UserID/Address (ADDIRE)	AS1USR/AS1	AS2USR/AS2	ASMUSR/ASM
System name / Group (ADDIRE)	AS1	AS2	ASM
User profile (ADDIRE)	AS1USR	AS2USR	ASMUSR
Mail service level (WRKDIRE)	2 - System message store	2 - System message store	2 - System message store
Preferred address (WRKDIRE)	3 - SMTP name	3 - SMTP name	3 - SMTP name
SMTPAUSRID (WRKDIRE + F19)	as1usr	as2usr	asmusr
SMTPDMN (WRKDIRE + F19)	as1.mycompany.com	as2.mycompany.com	asm.mycompany.com

6.5.2.1 Implementing Mail Forwarding in the Secure Mail Server

As explained in Section 6.3.2, “Scenario Network Configuration” on page 154, the firewall relays all inbound mail from the Internet destined to *mycompany.com*’s users to the secure mail server *as2.mycompany.com*.

For inbound mail, the firewall changes the recipient’s domain *user@mycompany.com* to *user@as2.mycompany.com*. For outbound mail, the firewall changes the originator’s name from *user@asx.mycompany.com* to *user@mycompany.com*, where *asx* is the internal mail server for the user.

The secure mail server (AS2 in our scenario) acts as a mail hub receiving all inbound mail from the firewall. We need to implement a mail forwarding function on AS2 to forward mail to the corresponding internal mail server based on the recipient’s User ID. Refer to Appendix A.2, “Mail Forwarding” on page 433 for a general description of the mail forwarding function.

Figure 152 shows the system distribution directory entries on each mail server. There must be a system distribution directory entry for every user in the secure mail server (AS2). The entries for non-local users (users on ASM and AS1) must include the user-defined field *forwarding* pointing to the corresponding local user and internal mail server.

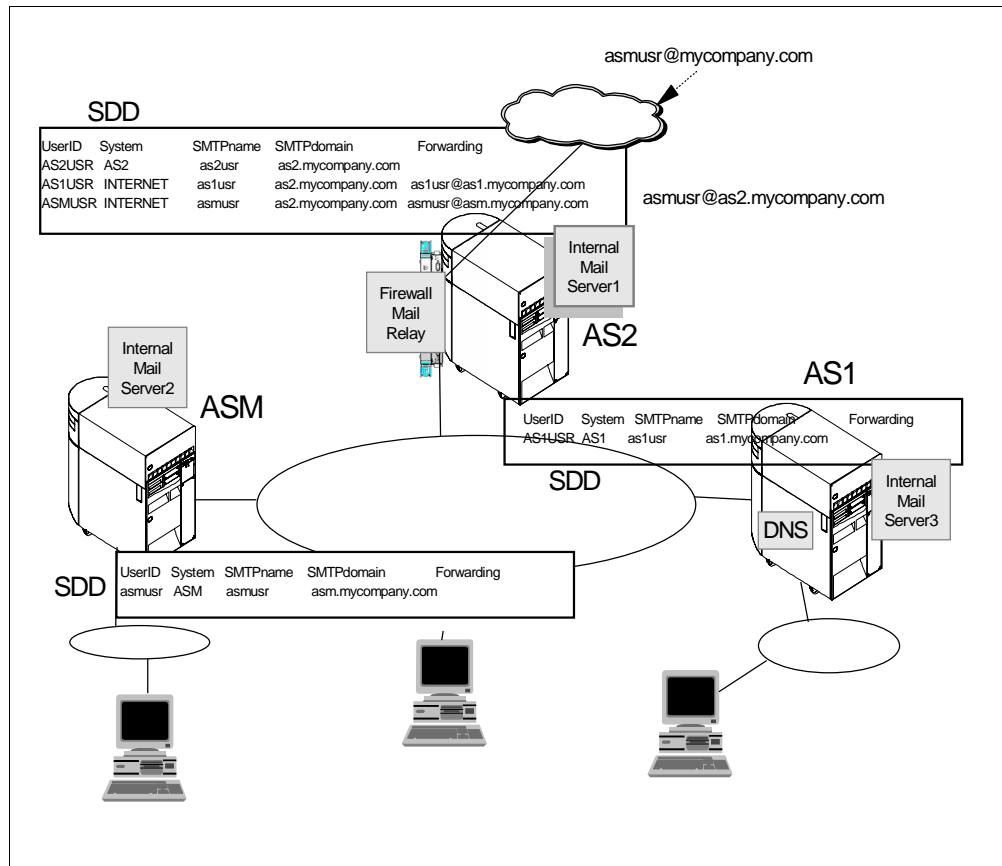


Figure 152. Mail Forwarding Using User-Defined Fields in the System Distribution Directory

To summarize, to implement the mail forwarding function in the mail hub (secure mail server in our scenario), you must:

1. Add two user-defined fields to the system distribution directory on AS2:
 1. Create two user-defined fields in the system distribution directory using the Change System Directory Attributes (CHGSYSDIRA) command.
 2. Enter the CHGSYSDIRA command and press **F4**.
 3. Page down until the user-defined field parameters are displayed.
 4. Fill in the information as shown in Figure 153.

Change System Dir Attributes (CHGSYSDIRA)

Type choices, press Enter.

User-defined fields:

Field name	FORWARDING	Character value, *SAME
Product ID	*NONE	Character value, *NONE
Function	> *ADD	*ADD, *RMV, *CHG, *KEEP
Field type	*ADDRESS	*DATA, *MSFSRVLVL, *ADDRESS
Maximum field length	256	1-512
Field name	FWDSRVLVL	Character value
Product ID	*NONE	Character value, *NONE
Function	> *ADD	*ADD, *RMV, *CHG, *KEEP
Field type	*MSFSRVLVL	*DATA, *MSFSRVLVL, *ADDRESS
Maximum field length	001	1-512

More..

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display

Figure 153. Adding User-Defined Fields to the System Distribution Directory

2. Add a directory entry for each user in the network on AS2 to forward mail to the user's mail server:
 1. From an AS/400 command entry display, enter the command:
WRKDIRE
Press **Enter**.
 2. Select option **1**, Add.
 3. Enter the following information. Notice that ASMUSR and INTERNET are values that we chose arbitrarily; they do not have to match any other configuration value.

Add Directory Entry

Type choices, press Enter.

User ID/Address	ASMUSR	AS2
Description	Forward Mail to asmusr@asm.mycompany.com	
System name/Group . . .	INTERNET	F4 for list
User profile		F4 for list
Network user ID		

4. Page down until the display in Figure 154 is shown. Fill in the information as indicated in Figure 154.

Add Directory Entry

Type choices, press Enter.

Mail service level . . . 9	1=User index 2=System message store 4=Lotus Domino 9=Other mail service
For choice 9=Other mail service:	
Field name FWDSRVLV	F4 for list
Preferred address . . . 9	1=User ID/Address 2=O/R name 3=SMTP name 9=Other preferred address
Address type ATMIME	F4 for list
For choice 9=Other preferred address:	
Field name FORWARDING	F4 for list

Figure 154. Adding Directory Entry to Forward SMTP/MIME Mail

Note: Address type MIME is equivalent to ATMIME. If the ATMIME option does not show on your system, select MIME.

5. Press **F19** to enter the SMTP user ID and SMTP domain in the incoming mail to the mail hub. This must match the user ID and domain in the piece of mail relayed by the firewall to the secure mail server.

Specify User-Defined Fields

Type choices, press Enter.

SMTPAUSRID	SMTP	asmusr
SMTPDMN	SMTP	as2.mycompany.com

Figure 155. Specify SMTP User ID and SMTP Domain as Received by the Secure Mail Server

Press **Enter**.

6. Press **F20** to specify the forwarding information shown in Figure 156.

Specify User-Defined Fields

Type choices, press Enter.

FORWARDING	asmusr@asm.mycompany.com
FWDSRVLVL	

Figure 156. Specifying Mail Forwarding Information

Press **Enter** to add the directory entry to the system distribution directory.

6.5.3 Verify the Firewall Installation and Configuration

For information about Firewall installation and configuration, refer to Section 6.2.3, "Firewall Installation and Configuration" on page 133.

After you install and configure the firewall, the network server description that contains the firewall configuration will point to the internal DNS. The firewall as a TCP/IP host belongs to your internal network (domain *mycompany.com*).

Figure 157 shows the internal and external name servers configured in the firewall. The internal DNS IP address matches the name server Internet address configured in the AS/400 system where the firewall is installed. Notice that in this scenario, the internal name server is running on AS1 and the secure mail server is on the AS/400 system where the firewall is installed (AS2). The external DNS is usually the ISP DNS IP address specified during the firewall configuration.

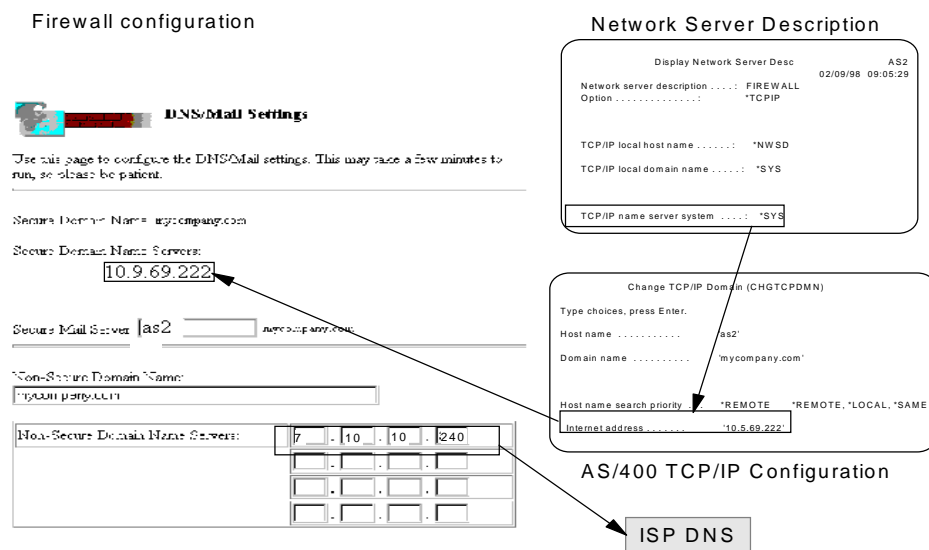


Figure 157. Firewall DNS and Secure Mail Server Configuration

6.5.4 Internal DNS Configuration

In our scenario, the primary server for *mycompany.com* in the secure network runs on AS1.

The main aspects of the primary DNS configuration are:

1. Configuring all hosts in *mycompany.com* for name to address resolution.
2. Configuring the forwarders directive to forward name to address resolutions for hosts outside the *mycompany.com* domain to the firewall DNS.
3. Configuring the mail exchangers for the internal network.
4. Configuring Hosts in the *mycompany.com* **Domain**

To verify the DNS configuration in our test environment:

1. Use Operations Navigator to get to the DNS Configuration for *DNS Server - As1.mycompany.com*.
2. Double-click on **Primary Domains**.
3. Right-click *mycompany.com*; the configured hosts names and IP addresses in the forward resolution file are shown in Figure 158.

Tip

If the company's internal and public domain names are the same (as in this scenario, the domain name is *mycompany.com* both internal and public), you must configure address records for the public hosts in front of the firewall in the internal DNS server for the internal name server to resolve the public hosts names. If you do not add A records for the public hosts in the internal DNS server configuration when an internal client queries, for example, *WWW.mycompany.com*, the query receives a negative response. The internal DNS server looks at its own data since it is authoritative for *mycompany.com* and, if it does not find the WWW host in its own database, it does not forward the query to the firewall but returns a negative response instead.

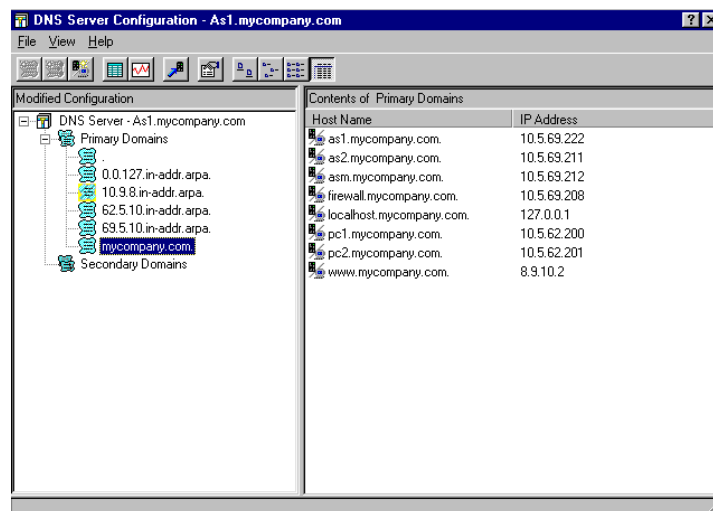


Figure 158. Content of Primary DNS for *mycompany.com* in AS1

In a similar fashion, you can display the content of the reverse mapping files **62.5.10.in-addr.arpa.** and **69.5.10.in-addr.arpa.**

6.5.4.1 Configuring Forwarders Pointing to the Firewall

As explained in Section 6.2.5, “Configuring Forwarders in the Internal DNS” on page 140, the forwarders directive directs off-site queries to the IP address specified. In our scenario, we want to forward queries for hosts outside the *mycompany.com* domain to the firewall. To add or verify your forwarders configuration, use the following steps:

1. Use Operations Navigator to get to the DNS Configuration for *DNS Server - As1.mycompany.com*.
2. Right-click on **DNS Server-As1.mycompany.com** and select **Properties**.
3. Click on the **Forwarders** tab. Enter the firewall’s secure port IP address and verify that the box **Contact only forwarders for off-site queries** is checked as shown in Figure 159.

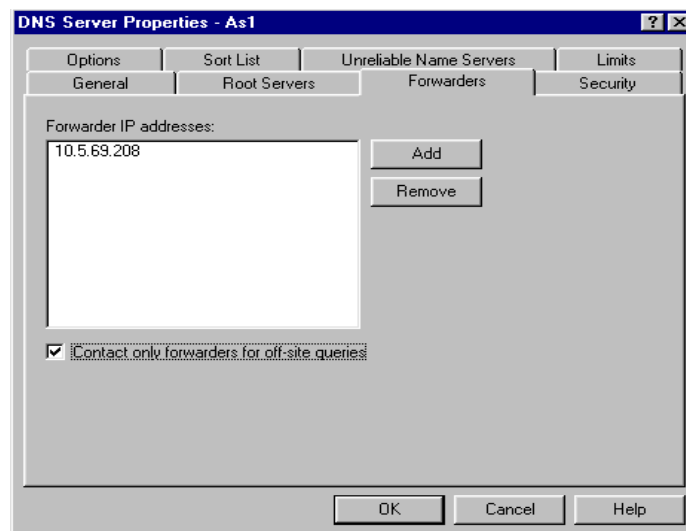


Figure 159. Adding the Firewall Secure Port IP Address to the Forwarders List

6.5.4.2 Configuring the Secondary DNS Server

For backup and workload balancing purposes, we now configure AS2 as a secondary DNS for the *mycompany.com* domain.

To configure AS2 as the secondary DNS on AS2, access the DNS configuration through Operations Navigator and use the following steps:

1. In the DNS server Configuration window, right-click on **Secondary Domains** (Figure 160).

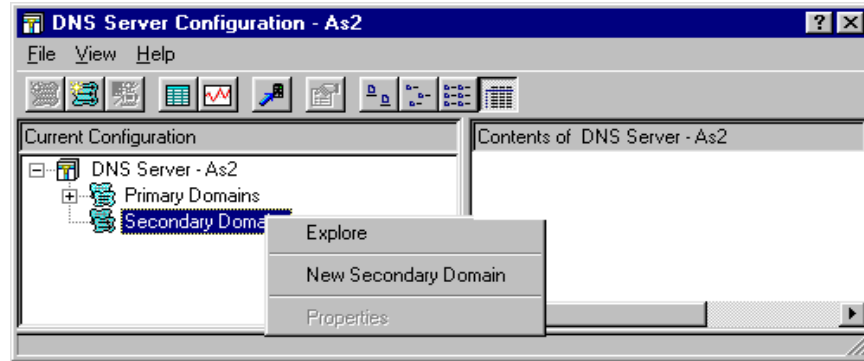


Figure 160. Configuring AS2 as Secondary DNS for mycompany.com

2. Select **New Secondary Domain**.
3. Specify the domain name and IP address of the primary name server (Figure 161).

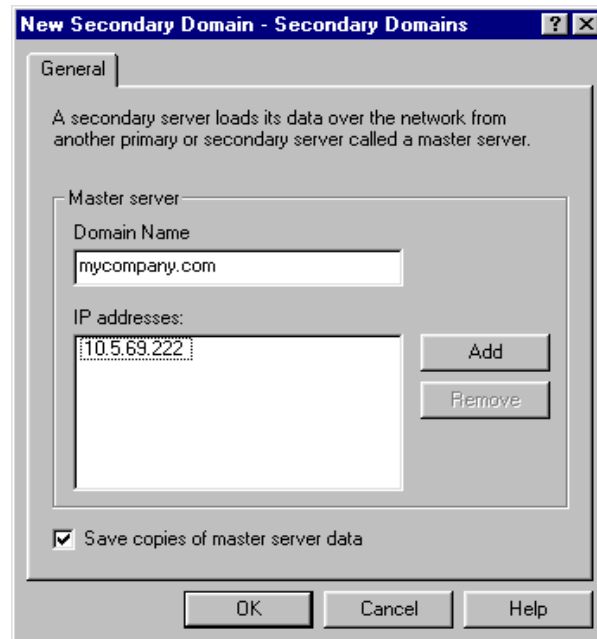


Figure 161. Primary Domain Name and Name Server IP Address

Repeat steps 1 through 3 to configure AS2 as secondary server for the 69.5.10.in-addr.arpa and 62.5.10.in-addr.arpa domains.

4. Right-click on **DNS server-As2.mycompany.com** and select **Properties**.
5. Click on the **Forwarders** tab. Enter the IP address of the firewall secure port: 10.5.69.208 and verify that the box **Contact only forwarders for off-site queries** is checked.

Figure 162 shows the AS2 DNS server boot file for this scenario.

```
directory /QIBM/UserData/OS400/DNS
forwarders 10.5.69.208
options forward-only
limit transfers-in 10
limit transfers-per-ns 2
secondary mycompany.com 10.5.69.222 mycompany.com.DB
secondary 62.5.10.in-addr.arpa 10.5.69.222 62.5.10.in-addr.arpa.DB
secondary 69.5.10.in-addr.arpa 10.5.69.222 69.5.10.in-addr.arpa.DB
```

Figure 162. AS2 Mycompany.com DNS Boot File /QIBM/UserData/OS400/DNS/BOOT

6.5.4.3 Configuring the Mail Exchangers in the Internal Network

Mail sent by users in the secure network to other users in the secure network is routed to the appropriate mail server by the internal DNS server. See Appendix A.3, "Processing Inbound Mail" on page 437 and Appendix A.4, "Processing Outbound Mail" on page 438 for background information on this topic.

In this scenario, we have three mail servers in the secure network: *as1.mycompany.com*, *as2.mycompany.com*, and *asm.mycompany.com*. The internal DNS server must route mail destined, for example, for *asmusr@asm.mycompany.com* to the ASM mail server. To configure the mail exchangers in the *As1.mycompany.com* DNS server, use the following steps:

1. Use Operations Navigator to get to the DNS Configuration for *DNS Server - As1.mycompany.com*.
2. Click + next to Primary Domains.
3. Double-click *mycompany.com*.
4. Select the host **as1.mycompany.com** on the right window and right click on it.
5. Select **Properties**.
6. Select the **Mail** tab.
7. Click on **Add**.
8. Enter **AS1** in the *Host name* field. Click **OK**. See Figure 163 on page 165.

This adds an MX record for *AS1.mycompany.com*.

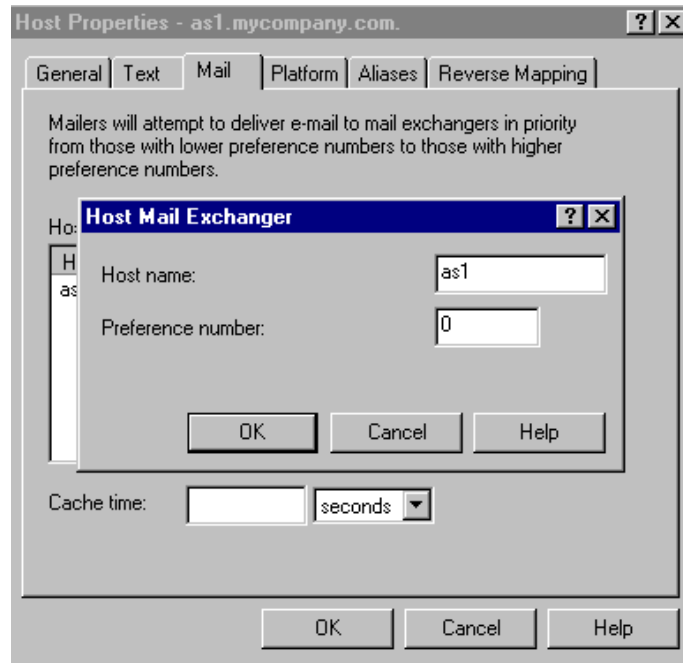


Figure 163. Adding an MX Record for *as1.mycompany.com*

Repeat steps 4 through 8 to add MX records for *asm.mycompany.com* and *as2.mycompany.com*.

Figure 164 shows the DNS boot file for this scenario. Notice the forwarders directive and the forward-only option.

```

directory /QIBM/UserData/OS400/DNS
forwarders 10.5.69.208
options forward-only
limit transfers-in 10
limit transfers-per-ns 2
options query-log
primary mycompany.com mycompany.com.DB
primary 69.5.10.in-addr.arpa 69.5.10.in-addr.arpa.DB
primary 0.0.127.in-addr.arpa 0.0.127.in-addr.arpa.DB
primary 62.5.10.in-addr.arpa 62.5.10.in-addr.arpa.DB
cache . CACHE

```

Figure 164. *Mycompany.com* DNS Boot File /QIBM/UserData/OS400/DNS/BOOT on AS1

Figure 165 shows the *mycompany.com.db* file for this scenario.

```

mycompany.com. IN SOA as1.mycompany.com.
postmaster.as1.mycompany.com. (
                                887921919
                                10800
                                3600
                                604800
                                86400)
;AS400OPNAV_INFO REVMAPDOMAIN
mycompany.com. IN NS as1.mycompany.com.
as1.mycompany.com. IN MX 0 as1.mycompany.com.
as2.mycompany.com. IN MX 0 as2.mycompany.com.
asm.mycompany.com. IN MX 0 asm.mycompany.com.
;AS400OPNAV_INFO REVMAPHOST as1.mycompany.com.
as1.mycompany.com. IN A 10.5.69.222
as2.mycompany.com. IN A 10.5.69.211
asm.mycompany.com. IN A 10.5.69.212
firewall.mycompany.com IN A 10.5.69.208
pc1.mycompany.com. IN A 10.5.62.200
pc2.mycompany.com. IN A 10.5.62.201
localhost.mycompany.com. IN A 127.0.0.1

```

Figure 165. mycompany.com.DB in /QIBM/UserData/OS400/DNS on AS1

Figure 166 shows the partial content of the QUERYLOG file. Notice the **MX** queries followed by **A** queries.

```

XX /10.5.69.216 /ASM.MYCOMPANY.COM.mycompany.com/A : Thu Feb 19 20:16:12
1998
XX /10.5.69.216 /FIREWALL.MYCOMPANY.COM.mycompany.com/A : Thu Feb 19 20:16:13
1998
XX /10.5.69.216 /FIREWALL.MYCOMPANY.COM/A : Thu Feb 19 20:16:13 1998
XX /10.5.69.216 /222.695.10 .IN-ADDR.ARPA PTR : Thu Feb 19 20:16:13 1998
XX /10.5.69.216 'ASM.MYCOMPANY.COM.mycompany.com/A : Thu Feb 19 20:16:44 1998
XX /10.5.69.216 ;/ASM.MYCOMPANY.COM.mycompany.com/A : Thu Feb 19 20:16:45 1998
XX /10.5.69.216 /ASM.MYCOMPANY.COM.any.com/A : Thu Feb 19 20:16:45 1998
XX /10.5.69.216 /AS1.MYCOMPANY.COM.mycompany.com/A : Thu Feb 19 20:18:35 1998
XX /10.5.69.216 /AS1.MYCOMPANY.COM/A : Thu Feb 19 20:18:35 1998
XX /10.5.69.216 /as1.mycompany.com/MX : Thu Feb 19 20:18:36 1998
XX /10.5.69.216 /as1.mycompany.com/A : Thu Feb 19 20:18:36 1998
XX /10.5.69.216 /AS1.MYCOMPANY.COM.mycompany.com/A : Thu Feb 19 20:18:36 1998
XX /10.5.69.216 /AS2.MYCOMPANY.COM.mycompany.com/A : Thu Feb 19 20:19:59 1998
XX /10.5.69.216 /AS2.MYCOMPANY.COM/A : Thu Feb 19 20:19:59 1998
XX /10.5.69.216 /as2.mycompany.com/MX : Thu Feb 19 20:20:00 1998
XX /10.5.69.216 ;/as2.mycompany.com/A : Thu Feb 19 20:20:00 1998
XX /10.5.69.217 /AS2.MYCOMPANY.COM.MYCOMPANY.COM/A : Thu Feb 19 20:20:01 1998
XX /10.5.69.217 /AS2.MYCOMPANY.COM.Y.COM/A : Thu Feb 19 20:20:01 1998
XX /10.5.69.217 '/AS2.MYCOMPANY.COM/A : Thu Feb 19 20:20:01 1998

```

Figure 166. QIBM/UserData/OS400/DNS/QUERYLOG

6.5.5 Considerations for Exchanging Mail with Internet Users

As explained in Section 6.4.2, “Scenario Network Configuration” on page 154, for outbound mail, the firewall replaces the sender’s internal domain in the *From:* field by the public domain. For example, if user *as1usr@as1.mycompany.com* sends mail to an Internet user, the domain in the *From:* field is changed by the firewall to *as1usr@mycompany.com*. However, the firewall does not change the domain for users in the *CC:* list. If *as1usr* copies *as2usr@as2.mycompany.com*, the user in the Internet receives *as2usr*’s address unchanged. The Internet users cannot use the *Reply all* function to respond because the domain *as2.mycompany.com* is a domain *not* known in the Internet. Figure 167 illustrates this problem.

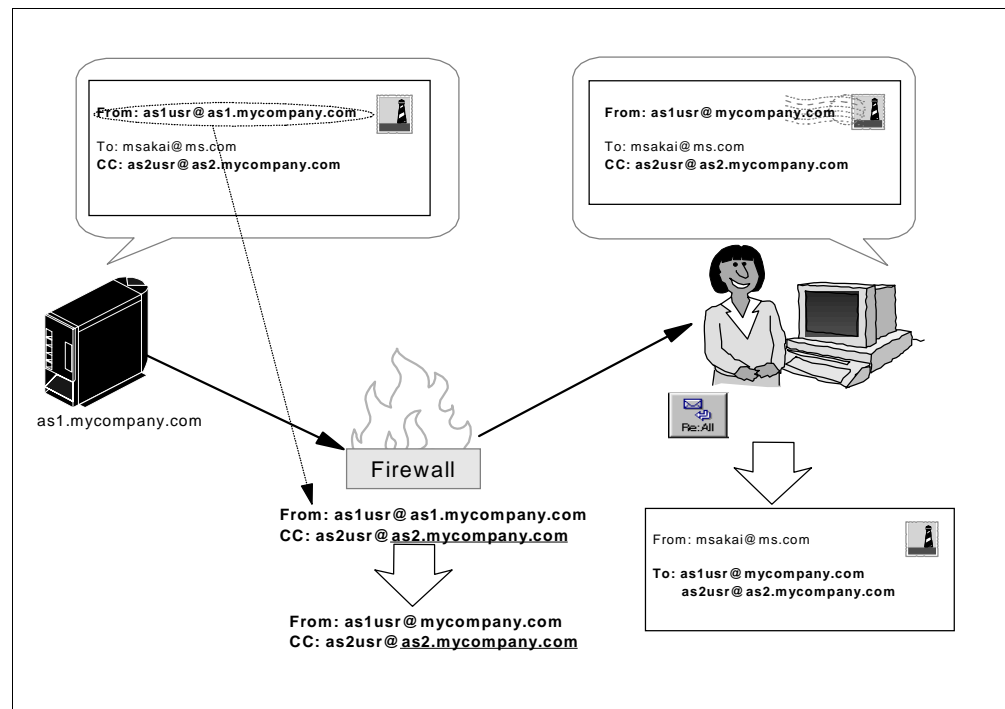


Figure 167. Sending Mail to External Users and CC: Internet Users

Figure 168 shows a piece of mail as it is received by the Internet user (*msakai@ms.com*). Notice the address in the *CC:* field (*as2usr@as2.mycompany.com*).

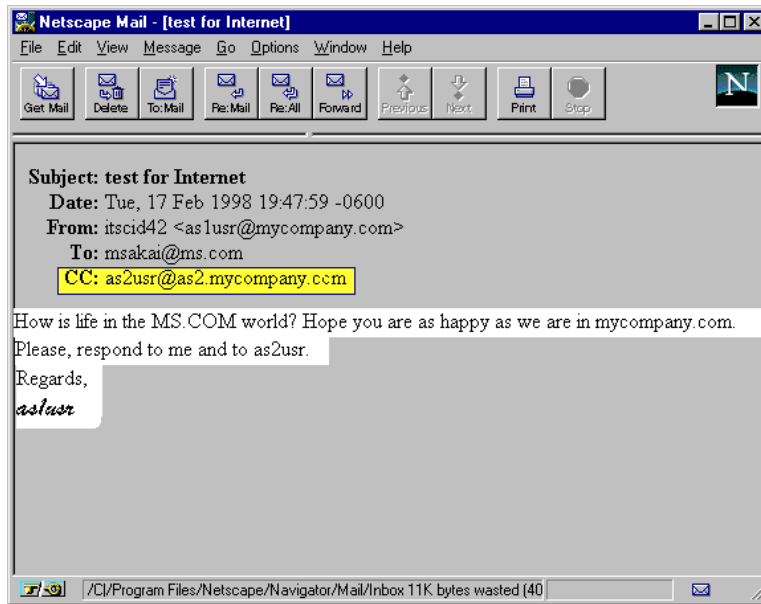


Figure 168. Mail Received by the Internet User

Figure 169 shows the mail generated by the *Reply All* function. Notice the *as2usr* address.

```
Date: Tue, 17 Feb 1998 20:07:37 -0600
From: msakai <msakai@ase2.ms.com>
Reply-To: msakai@ase2.ms.com
X-Mailer: Mozilla 3.0Gold (Win95; I)
MIME-Version: 1.0
To: as1usr@mycompany.com, msakai@ms.com, as2usr@as2.mycompany.com
Subject: Re: test for Internet
References: <34EA3DCF.4157@as1.mycompany.com> <34EA4178.448@ase2.ms.com>
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Hello as1usr and as2usr,
I'm just fine.
Hope you both get my reply,
Regards,
msakai
```

Figure 169. Reply All Function Using Internal Mail Address

6.5.6 Solving the CC: Problem

One possible work around for the problem explained in Section 6.5.5, “Considerations for Exchanging Mail with Internet Users” on page 167 is to send mail internally to *user@public_domain*. If the user in the CC: list is *as2usr@mycompany.com*, there is no need to alter the domain, and the *Reply All* function from the Internet back to the original network works with no problems.

To implement this solution, use the following steps:

1. Add *mycompany.com* as a local host alias in each internal mail server's host table (Figure 170).

```
Add TCP/IP Host Table Entry (ADDTCPHTE)

Type choices, press Enter.

Internet address . . . . . > '10.5.69.222'
Host names:
  Name . . . . . mycompany.com

+ for more values
Text 'description' . . . . . Alias for local host
```

Figure 170. Configuring *mycompany.com* Local Host Alias

2. Change the host name search priority to **LOCAL* (Figure 171).

```
Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . 'AS1'
Domain name . . . . . 'mycompany.com'

Host name search priority . . . *LOCAL *REMOTE, *LOCAL, *SAME

Internet address . . . . . '10.5.69.222'
```

Figure 171. Changing the Host Name Search Priority to **LOCAL*

3. On each internal mail server, each local user must have two system distribution directory entries with the following fields (Table 5):

Table 5. System Distribution Directory Entries for Local Users in AS1

UserID/System	SMTP Name	SMTP Domain	Forwarding
AS1USR/AS1	as1usr	as1.mycompany.com	
AS1USR/INTERNAL	as1usr	mycompany.com	as1usr@as1.mycompany.com

4. On each internal mail server, each internal remote user must have a system distribution directory entry with the following fields (Table 6):

Table 6. System Distribution Directory Entry for Remote Internal Users in AS1

UserID/System	SMTP Name	SMTP Domain	Forwarding
AS2USR/INTERNAL	as2usr	mycompany.com	as2usr@as2.mycompany.com

5. At the mail hub (secure mail server), each user in the secure domain must have a system distribution directory entry with the following fields (Table 7):

Table 7. System Distribution Directory Entry for All mycompany.com Users in AS2 (Secure Mail)

UserID/System	SMTP Name	SMTP Domain	Forwarding
AS1USR/AS1	as1usr	as2.mycompany.com	as1usr@as1.mycompany.com

Table 8 summarizes the TCP/IP configuration for the internal mail servers in this scenario.

Table 8. Solving the CC: Problem - TCP/IP Configuration Summary

TCP/IP Configuration	AS1	AS2	ASM
IP address (CFGTCP op. 1)	10.5.69.222	10.5.69.211	10.5.69.212
Host Name (CFGTCP op. 12)	AS1	AS2	ASM
Domain Name (CFGTCP op. 12)	mycompany.com	mycompany.com	mycompany.com
Host name search priority (CFGTCP op. 12)	*LOCAL	*LOCAL	*LOCAL
DNS Internet address (CFGTCP op. 12)	10.5.69.222	10.5.69.222	10.5.69.222

Table 9 shows *mycompany.com* as an alias for the local host in the internal mail servers.

Table 9. mycompany.com Local Host Alias

TCP/IP Configuration	AS1	AS2	ASM
IP interface address (ADDTCPHTE)	10.5.69.222	10.5.69.211	10.5.69.212
Host Name (ADDTCPHTE)	mycompany.com	mycompany.com	mycompany.com

Figure 172 summarizes the system distribution directory configuration in each internal mail server.

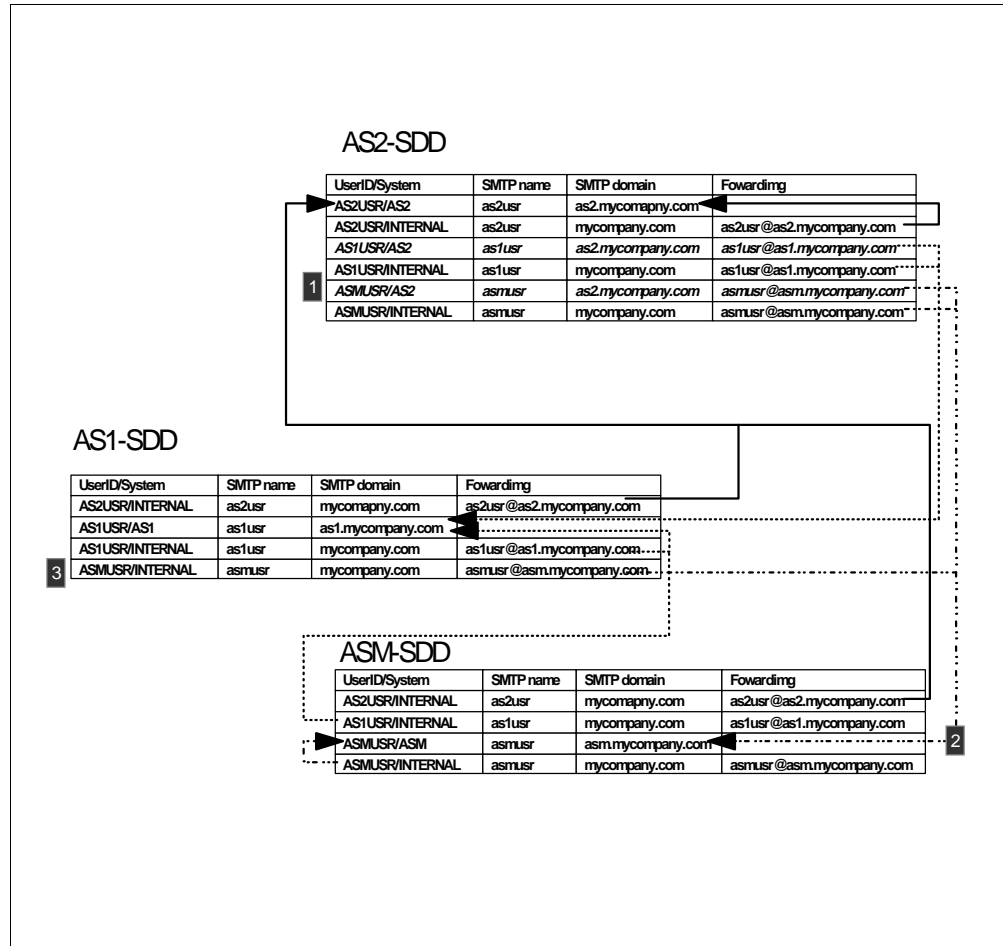


Figure 172. Solving the CC: Problem - System Distribution Directory Configuration

1. The firewall changes inbound mail from the Internet to *asmusr@mycompany.com* to *asmusr@as2.mycompany.com*. The SMTP server in AS2 decides that *as2.mycompany.com* is the local system and searches the local distribution directory for a user with the same SMTP name and SMTP domain name. The ASMUSR/AS2 directory entry is a match and the mail is forwarded to the user in the forwarding field (*asmusr@asm.mycompany.com*).
2. At *asm.mycompany.com*, there is a directory entry for a local user (ASMUSR/ASM) that matches the incoming SMTP name and SMTP domain with the forwarding field blank. The mail is delivered to that user in ASM.
3. When internal mail is sent from AS1 to *asmusr@mycompany.com*, the SMTP server in AS1 decides that *mycompany.com* is the local system per alias configuration. It searches the local system distribution directory for an SMTP name and SMTP domain match and it finds the ASMUSR/INTERNAL with the forwarding field to forward mail to *asmusr@asm.mycompany.com*.

Chapter 7. Providing DNS Services on the Internet

This chapter describes how you can configure a DNS server authoritative for multiple primary/secondary zones. We also explain how to configure the DNS server so it can forward queries directly to the Internet root name servers.

7.1 Scenario Overview

In this scenario, we are configuring a DNS server that is authoritative for two unrelated domains and secondary to the firewall DNS that was configured in Section 6.2.3, “Firewall Installation and Configuration” on page 133. In this scenario, the AS/400 system we are configuring is an Internet service provider (ISP) DNS server. It provides DNS server services for a fee to its customers. In this scenario, we assume the domain names and IP addresses are registered with the InterNIC.

Figure 173 outlines four domains: *isp.net*, *inc.com*, *msu.edu*, and *mycompany.com*. The ISP DNS server ASISP, which is located in the domain *isp.net*, is configured to be authoritative for *inc.com* and *msu.edu*. The firewall DNS within *mycompany.com* is authoritative for the public domain *mycompany.com* discussed in Chapter 6, “Split DNS: Hiding Your Internal DNS Behind a Firewall” on page 125. ASISP is configured to be secondary (that is, backup) to the Firewall DNS running on the Integrated PC Server installed on AS1.

The DNS server running on ASISP2 is configured as the secondary DNS server to the primary name server ASIPS to back up the primary domains *inc.com*, *msu.edu*, and their respective in-addr.arpa domains.

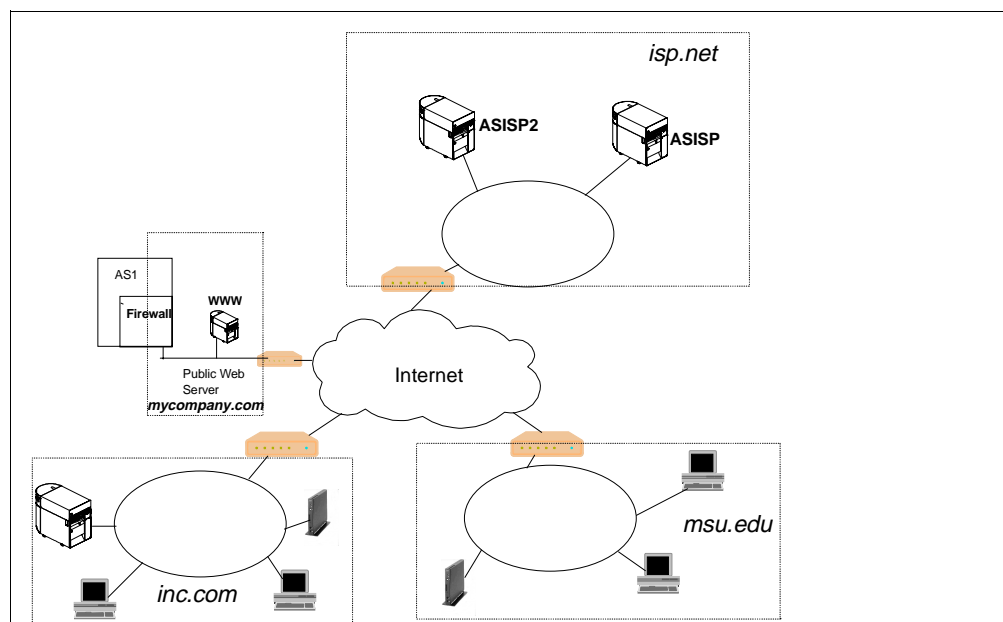


Figure 173. Scenario Network Diagram

7.1.1 Scenario Objectives

In this scenario, our objectives are to:

1. Configure a primary DNS server to be authoritative over two customers' domain name spaces that are unrelated to one another. This includes configuring the forward mapping file and reverse (in-addr.arpa) mapping file for each customer.
2. Configure the same DNS server to be secondary to the *mycompany.com*'s firewall DNS server that was configured in Chapter 6, "Split DNS: Hiding Your Internal DNS Behind a Firewall" on page 125.
3. Configure the DNS server's root servers to be the Internet root name servers.
4. Discuss configuring the ISP's secondary DNS server to back up the primary domain files residing on the primary DNS server.
5. Briefly discuss the client configuration.

7.1.2 Scenario Advantages

Many companies are starting to provide Web sites to advertise or sell goods or services. If the Web site allows Internet access, its domain name and Internet address must be contained in a primary domain that some DNS server is authoritative for. Some companies prefer to hire an Internet Service Provider (ISP) to provide the DNS name services they need rather than provide required systems and skills in-house. This scenario is an example of how an ISP can configure an AS/400 system to provide Internet DNS services to the ISP's customers.

This scenario discusses how to configure the root servers to be the name servers authoritative for the top-level domains. These Internet root name servers are crucial to name and address resolution on the Internet.

7.1.3 Scenario Disadvantages

This scenario configuration of Internet root name servers is not necessary when a DNS server is authoritative for domains that are internal (that is, the domain is private). Earlier chapters discuss DNS server configuration scenarios for internal networks.

7.1.4 Scenario Network Configuration

This chapter's scenario focuses on domains with registered InterNIC names and IP addresses. The hosts that are configured in the DNS server are all on the Internet including the DNS server.

The network in Figure 174 shows the ISP DNS servers ASISP and ASISP2 connected to the 7.10.10.0 network with a subnet mask of 255.255.255.0. ASISP is the primary DNS server in this scenario. Figure 151 on page 154 shows this ISP DNS server with an IP address of "Y", which is 7.10.10.240.

ASISP2 is configured to be a secondary name server to back up the primary domain files residing on ASISP.

The domain *inc.com* is contained on the network 11.5.6.0 with a subnet mask of 255.255.255.0. The domain *msu.edu* is located on network 12.5.6.0 with a subnet mask of 255.255.255.0. ASISP is configured to be primary for both of these domains.

In Section 6.2.3, “Firewall Installation and Configuration” on page 133, the firewall configuration lists the non-secure domain name as *mycompany.com*. This is the public domain name for the hosts residing on the 8.9.10.0 network. See Figure 117 on page 127. The DNS running on *firewall.mycompany.com* at IP address of 8.9.10.11 is authoritative for this public domain of *mycompany.com*. This chapter’s scenario shows how to configure the ASISP name server to be secondary to the firewall DNS.

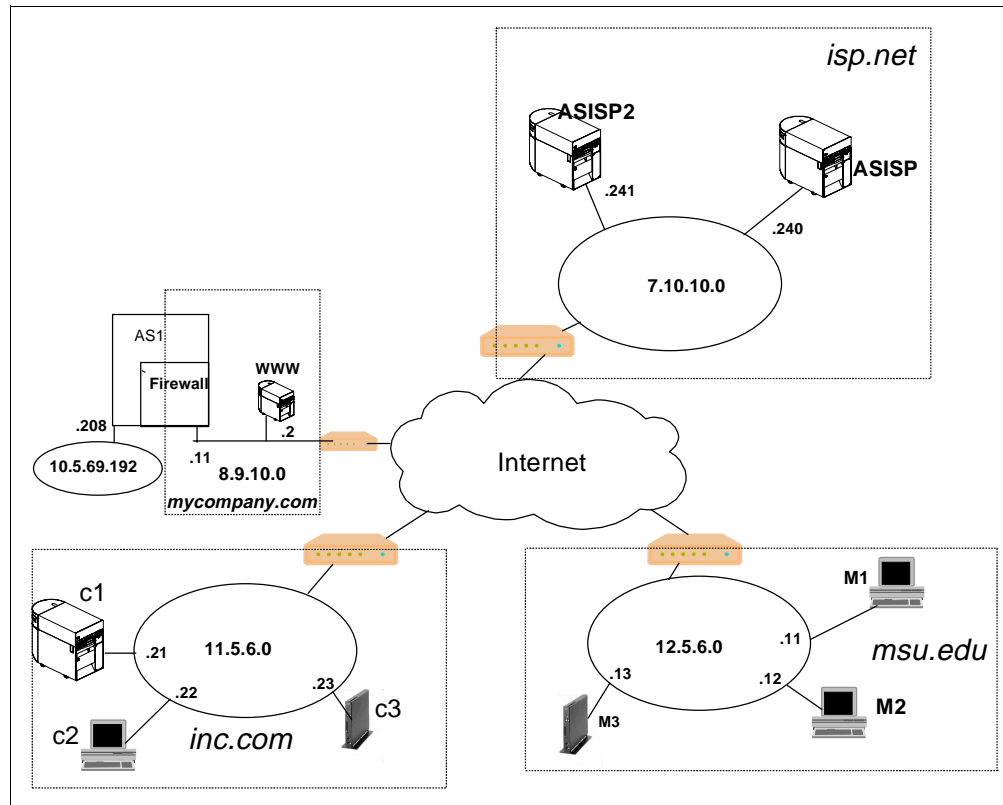


Figure 174. Detailed Network Diagram

7.2 Task Summary

The tasks required to complete this scenario do not include the initial TCP configuration on the AS/400 ASISP or ASISP2. This scenario assumes that the TCP configuration on both AS/400 systems in the network is complete and TCP connectivity has been verified.

The summary of tasks for this scenario are as follows:

1. Create the primary domain files for *inc.com* on the ASISP name server.
2. Create the primary domain files for *msu.edu* on the ASISP name server.
3. Configure the root servers to be the Internet root servers on the ASISP name server.
4. Configure the secondary domain files for *mycompany.com* on ASISP to back up the DNS server running on *firewall.mycompany.com*.

5. Configure the secondary domain files on the secondary name server ASISP2 to back up the *inc.com* primary domain files on ASISP and the *msu.edu* primary domain files on ASISP.
6. Configure the root servers to be the Internet root servers on the secondary name server ASISP2.
7. Configure the clients in *msu.edu* and *inc.com* to use ASISP or ASISP2 as their DNS server.

7.2.1 Planning the ASISP Name Server Configuration

Before configuring ASISP DNS server, you must decide its zone of authority, secondary DNS server, and register domains with the InterNIC.

Zone of Authority and DNS Configuration Planning

The process of setting up a DNS server should start with the careful planning of the zones of authority that the name server is configured for.

The DNS servers ASISP and ASISP2 are located in the domain *isp.net*. We made a decision in the planning phase that the name servers ASISP and ASISP2 are not authoritative for the domain that they are located in. These two DNS servers are only authoritative for customer's domains. Another DNS server in the *isp.net* is configured to be authoritative for the ISP's own domain space *isp.net*.

Figure 175 shows part of the Internet DNS name space tree. The DNS servers ASISP and ASISP2 are physically located in the *isp.net* domain. The zones they are authoritative for are also shown in the figure: *mycompany.com*, *msu.edu* and *inc.com*.

The root name servers that ASISP and ASISP2 are configured with are the Internet root name servers, which can be thought of as being located at the top level Internet domain name space. These Internet name servers know where to go to resolve queries near the top of the tree such as the *com* node, the *edu* node, and so on, and how to work down the respective nodes by knowing who their child name servers are.

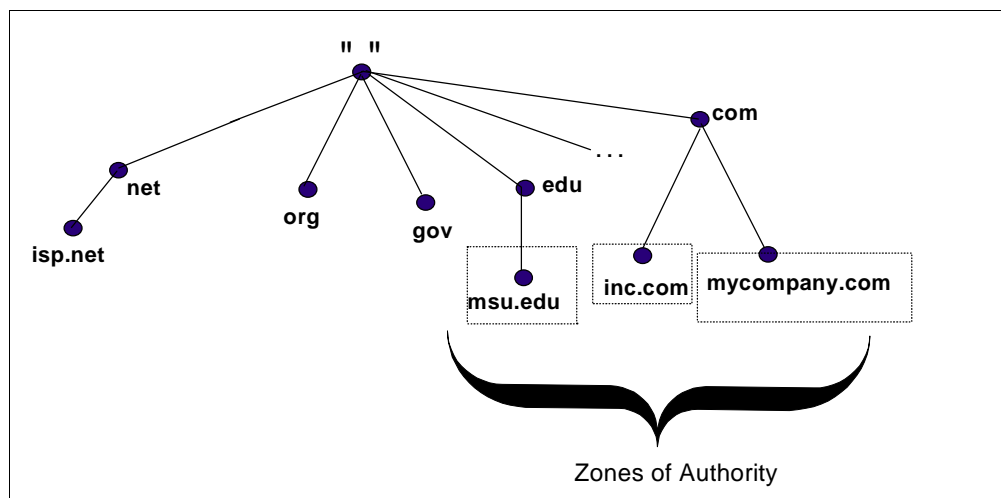


Figure 175. Part of the DNS Name Space Tree

Planning for the Secondary Name Server

The primary domain files for *inc.com* and *msu.edu* are located on ASISP. The planning phase also includes deciding how these files should be backed up. We have decided that ASISP2 AS/400 is a secondary DNS server to the ASISP primary domain name server. For the sake of simplicity in describing the scenario, we have placed both ASISP and ASISP2 on the same physical network. However, in real life, we recommend that a secondary name server should be placed in a physically separate location from the primary name server and on a different network if at all possible. The reason for this is to eliminate as many single points of failure as possible.

InterNIC Registration

The domains and IP addresses we are using in this scenario should be registered with the InterNIC. The current form used to register the name of the domains such as *isp.net*, *inc.com*, *msu.edu*, and *mycompany.com* can be located at:

<http://rs.internic.net/rs-internic.html>

The ASISP DNS server is primary for the in-addr.arpa domains of 11.5.6.in-addr.arpa and 12.5.6.in-addr.arpa. These reverse domains also need to be registered with the InterNIC. The URL previously listed is also the location to get the current form used to register the in-addr.arpa domains.

Part of the InterNIC registration includes listing the fully-qualified domain names and IP addresses of the primary and secondary DNS servers. Also, the DNS servers should be up and running and answering queries at the time the registration forms are submitted.

The primary name server for the 10.9.8.in-addr.arpa file that is associated with *mycompany.com* is *firewall.mycompany.com*. We assume that the DNS administrator for *mycompany.com* has registered the 10.9.8.in-addr.arpa file with the InterNIC as well as the domain name *mycompany.com*.

7.2.2 Create the inc.com Primary Domain Files on ASISP

If this is the first time the Operations Navigator DNS configuration is used on ASISP, the DNS configuration takes the user into the DNS configuration Wizard. For this scenario, the only thing the Wizard should be used for is to configure the *localhost* host with the IP address of 127.0.0.1. See Section 3.2.2, “Creating the Primary Name Server on As1” on page 29 for details on the Wizard windows.

There are two primary domains that need to be created on ASISP for *inc.com*:

inc.com. and 6.5.11.in-addr.arpa.

To create *inc.com*, go into Operations Navigator DNS configuration on ASISP and right-click on **Primary Domains**. Click on **New Primary Domain**. In the next window that Operations Navigator presents, we must override the default domain name. Type in **inc.com**. (do not forget the trailing period after *com*). Although we are configuring the *inc.com* domain, the administrator for this domain is probably located in the domain that the AS/400 ASISP is located in, *isp.net*. Therefore, the default for Administrator's e-mail may be correct:

postmaster.ASISP.isp.net.

Also, **enable** the *Create and delete reverse mappings* by default check box, which is located on the same window as the domain name. This causes the 6.5.11.in-addr.arpa primary domain file to be created automatically when the first new host is added to the *inc.com* primary domain. Click on **OK**.

Tip

The default e-mail address of the DNS administrator is the address of:

postmaster.ASISP.isp.net.

If we use this address, the AS/400 ASISP needs to have a user profile and a POP3 user for *postmaster*.

The *inc.com* primary domain file has been created but it contains no hosts.

1. Right-click on *inc.com* and select **New Host**.
2. Click on **Add** and type in the first host name: **c1** and its IP address: **11.5.6.21**.
3. Click **OK** twice.

Notice that the reverse mapping domain of 6.5.11.in-addr.arpa has been automatically created. It also contains the *c1* host.

Repeat the procedure to add *c2* and *c3* to the *inc.com* domain the same way *c1* was added.

Every forward mapping primary domain file should include the host name of *localhost* with the IP address of 127.0.0.1. If the *localhost* host was not added with the Wizard, we need to add one last new host of **localhost** with IP address of **127.0.0.1** to the *inc.com* domain.

Figure 176 shows the contents of *inc.com* primary domain file. Notice that the reverse mapping files of 0.0.127.in-addr.arpa and 6.5.11.in-addr.arpa are also listed as primary domains.

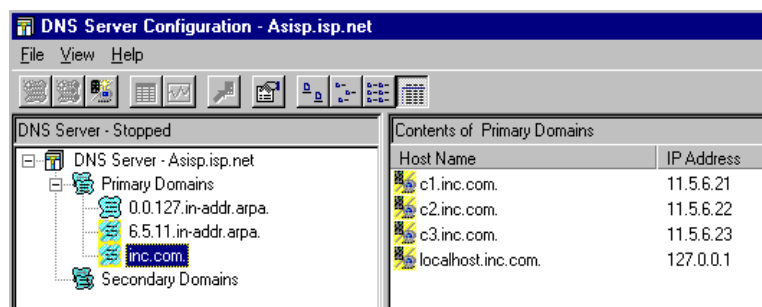


Figure 176. Contents of *inc.com* Primary Domain File on ASISP

Figure 176 also shows that the two primary domains *inc.com* and 6.5.11.in-addr.arpa are disabled by the hashing behind the icons to the left of

each domain file. Even if the name server is updated or restarted, the DNS server cannot use these files until they are enabled.

To enable *inc.com* and 6.5.11.in-addr.arpa, right-click on each primary domain file and click on **enable**.

Use the **update server** smart icon to refresh the DNS configuration with the new primary domain files.

7.2.3 Create the msu.edu Primary Domain Files ASISP

For ASISP DNS server to support name and address resolution for the customer with the domain *msu.edu*, we need to create two new primary domains:

msu.edu and 6.5.12.in-addr.arpa.

The preceding two primary domain files should be created in the same way explained for the two primary domain files for *inc.com* in Section 7.2.2, "Create the inc.com Primary Domain Files on ASISP" on page 177.

We then need to add new hosts to the *msu.edu* primary domain file:

m1, *m2*, *m3*, and *localhost*

The preceding hosts are added automatically in the 6.5.12.in-addr.arpa file if we enable the *Create and delete reverse mappings by default* option when we create the primary domain *msu.edu*.

Figure 177 shows the contents of the *msu.edu* primary domain file. The figure shows both *msu.edu* and 6.5.12.in-addr.arpa domains disabled.

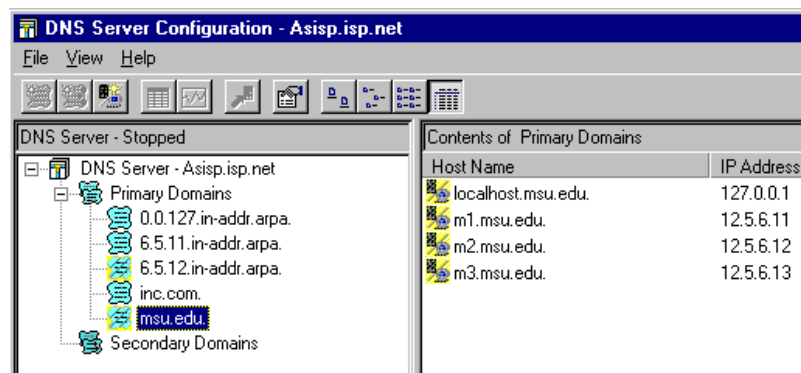


Figure 177. Contents of msu.edu Primary Domain File on ASISP

We now need to enable *msu.edu* and 6.5.12.in-addr.arpa primary domain files and click on the **update server** smart icon when we are ready to "go live" with the new DNS configuration.

7.2.4 Configure the Root Servers on ASISP

The root name server is a configuration parameter that affects the entire DNS server configuration. This configuration is contained in the Properties of the name server itself.

1. Right-click on the **DNS server-Asisp.isp.net** and click on **Properties**.
2. Click on the **Root Servers** tab and click **Load Defaults**.

The result is shown in Figure 178. The AS/400 DNS server support is shipped with an IFS file containing the Internet root name server list for the DNS administrator's convenience. By clicking on the Load Defaults box, these Internet root name servers are placed in the /QIBM/UserData/OS400/DNS/CACHE file once the DNS configuration is saved or the server is updated.

Note

The /QIBM/UserData/OS400/CACHE file does not contain the query responses that the DNS server has cached but contains the information about the root name servers. Do not let the name of this file mislead you.

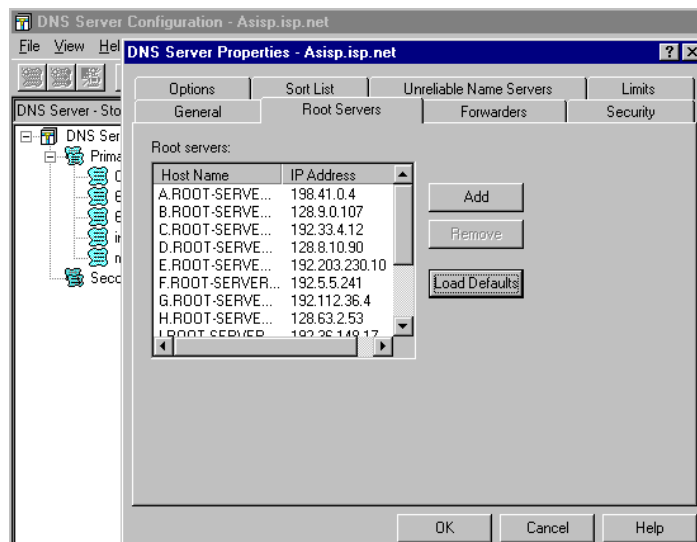


Figure 178. Load Default Root Servers on ASISP

At this point click, on **OK**. If the name server is already started, click on the update server smart icon to refresh the configuration. If the name server is stopped, close the DNS window to save the configuration.

The contents of /QIBM/UserData/OS400/DNS/CACHE is displayed in Figure 179. This figure displays the default Internet root name server list that was current at the time this redbook was written. This list is shipped in a file named ROOT.FILE located in the IFS directory: /QIBM/ProdData/OS400/DNS. The ROOT.FILE list is refreshed (if necessary) at every OS/400 release. Therefore, between releases, it is important for the DNS administrator to ensure that this list remains current. See the tip at the end of this section for more details.

```

. 3600000 IN NS M.ROOT-SERVERS.NET.
. 3600000 IN NS L.ROOT-SERVERS.NET.
. 3600000 IN NS K.ROOT-SERVERS.NET.
. 3600000 IN NS J.ROOT-SERVERS.NET.
. 3600000 IN NS I.ROOT-SERVERS.NET.
. 3600000 IN NS H.ROOT-SERVERS.NET.
. 3600000 IN NS G.ROOT-SERVERS.NET.
. 3600000 IN NS F.ROOT-SERVERS.NET.
. 3600000 IN NS E.ROOT-SERVERS.NET.
. 3600000 IN NS D.ROOT-SERVERS.NET.
. 3600000 IN NS C.ROOT-SERVERS.NET.
. 3600000 IN NS B.ROOT-SERVERS.NET.
. 3600000 IN NS A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000 IN A 198.41.0.4
B.ROOT-SERVERS.NET. 3600000 IN A 128.9.0.107
C.ROOT-SERVERS.NET. 3600000 IN A 192.33.4.12
D.ROOT-SERVERS.NET. 3600000 IN A 128.8.10.90
E.ROOT-SERVERS.NET. 3600000 IN A 192.203.230.10
F.ROOT-SERVERS.NET. 3600000 IN A 192.5.5.241
G.ROOT-SERVERS.NET. 3600000 IN A 192.112.36.4
H.ROOT-SERVERS.NET. 3600000 IN A 128.63.2.53
I.ROOT-SERVERS.NET. 3600000 IN A 192.36.148.17
J.ROOT-SERVERS.NET. 3600000 IN A 198.41.0.10
K.ROOT-SERVERS.NET. 3600000 IN A 198.41.0.11
L.ROOT-SERVERS.NET. 3600000 IN A 198.32.64.12

```

Figure 179. Contents of CACHE File when Load Defaults Option is Taken

Tip

By using the default Internet root name server list provided with the OS/400 V4R2M0 DNS option, you assume the default list is current. You can verify the list is current by downloading a new list from the Internet.

To do this use, anonymous *ftp* to get the file *named.root* from the subdirectory of *domain*. This file is located on host *ftp.rs.internic.net* at IP address of 198.41.0.5.

The AS/400 system shipped default Internet root name server list is stored in /QIBM/ProdData/OS400/DNS/ROOT.FILE.

7.2.5 Create the Secondary Domain Files for mycompany.com on ASISP

One of the objectives for the DNS configuration on ASISP is to be a backup to the firewall DNS server running on AS/400 AS1. The Firewall DNS is authoritative (that is, primary) for the public *mycompany.com* domain located in the 8.9.10.0 network. This is the public or non-secure side of the firewall. This configuration is described in Section 6.2.3, "Firewall Installation and Configuration" on page 133.

To back up the firewall's DNS server, we need to configure ASISP to be a secondary name server to the primary name server firewall at 8.9.10.11. To do this, follow these steps:

On ASISP's Operations Navigator DNS configuration:

1. Right-click on **Secondary Domains**.
2. Click on **New Secondary Domain**.
3. On the next window override the default domain by typing:
mycompany.com. (Do not forget the trailing period after *com*.)
4. Click on **Add**. Type in the IP address of the master name server, which, in this case, is the non-secure port of the firewall: **8.9.10.11**.

Make sure the save copies of the master server data are enabled (there should be a check in the small box). Figure 180 shows how the DNS configuration of the secondary domain file of *mycompany.com* should look before clicking on OK.

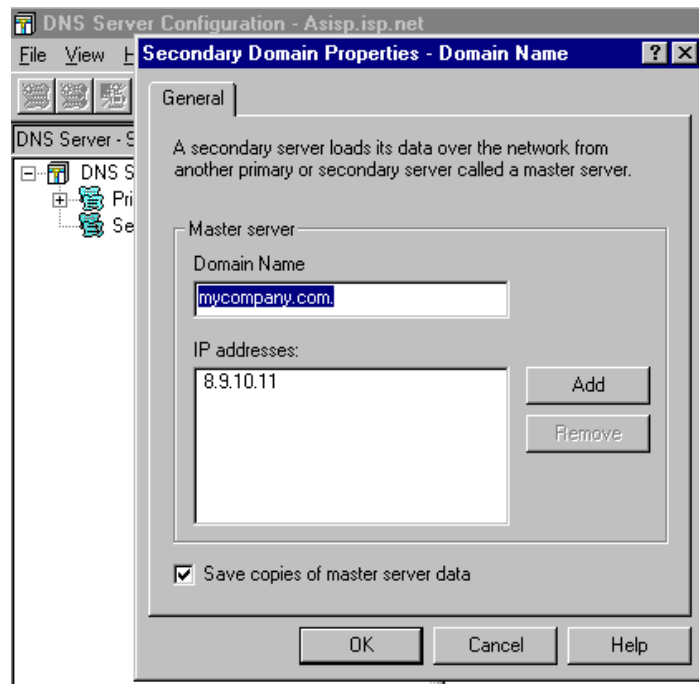


Figure 180. Creating a Secondary Domain File for *mycompany.com*. on ASISP

5. Click on **OK**.

We are only half finished with providing a backup for the firewall DNS server. We still need to create a secondary domain file on ASISP for the 10.9.8.in-addr.arpa domain.

6. Right-click again on **Secondary Domains**.
7. Click on **New Secondary Domain** and override the default domain by typing: **10.9.8.in-addr.arpa**.
8. Click on **Add**. Type in the IP address of the master name server firewall: **8.9.10.11**.
9. Click on **OK**.

10. Click on **update server** smart icon to refresh the DNS configuration (or if the DNS server is stopped, close the DNS configuration window to save the configuration).

Figure 181 shows the two secondary domains we have just created: 10.9.8.in-addr.arpa and *mycompany.com*.

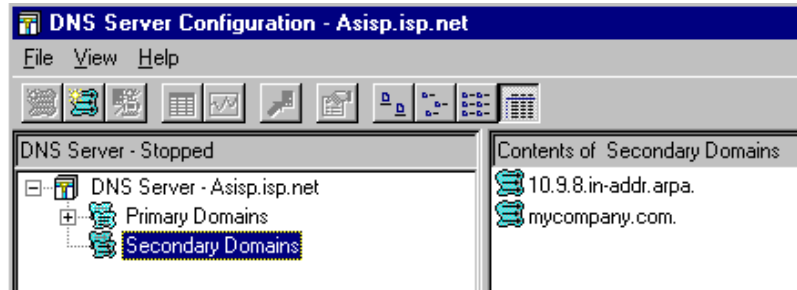


Figure 181. The Secondary Domains on ASISP to Backup Firewall.mycompany.com

7.2.6 Create the Secondary Domain Files on ASISP2

The ASISP2 DNS server is the secondary name server to the ASISP primary name server. Thus, we need to create four new secondary domains on ASISP2, which are:

- *inc.com*.
- 6.5.11.in-addr.arpa.
- *msu.edu*.
- 6.5.12.in-addr.arpa.

In each case, the master server IP address needs to be the IP address of the primary name server ASISP, which is 7.10.10.240.

Figure 182 shows the four secondary domains residing on the secondary name server ASISP2.

NOTE

For a thorough example of configuring a secondary domain server, please see Section 3.2.6 on page 57.

We are almost finished configuring the secondary name server ASISP2. The last step is outlined in the next section.

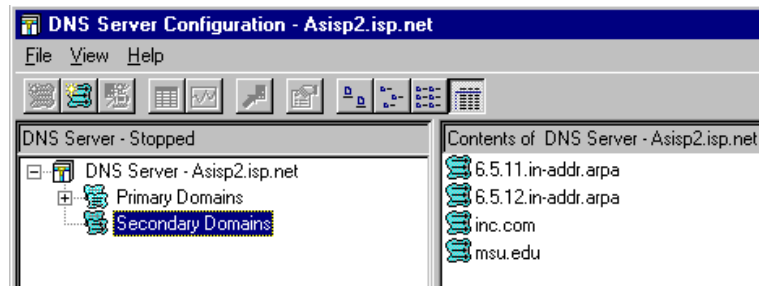


Figure 182. Secondary Domains on Secondary Name Server ASISP2

7.2.7 Configure the Root Servers on ASISP2

The ASISP2 DNS server does more than back up the primary domain files that reside on ASISP. If the ASISP DNS server does not respond, the secondary name server ASISP2 needs to handle all of the queries that ASISP normally handles. That includes more than just the queries for information that the name server is authoritative for. ASISP2 also needs to know where to go when it does not have the answer to a query. ASISP2 needs to be configured to go to the same place that ASISP goes when it cannot answer a query: the Internet root name servers.

Thus, the configuration steps outlined in Section 7.2.4 on page 179 also need to be repeated on ASISP2 to load the default Internet root server list.

Lastly, when finished, the update server smart icon needs to be clicked to refresh the DNS configuration on ASISP2. Or if the DNS server is currently stopped, the DNS configuration window needs to be closed to save the new configuration.

Tip

At this point, the primary name server ASISP should have its configuration updated to include an NS record stating that ASISP2 is secondary to the primary domain files. This should be done on ASISP with the Secondary Name Server tab of the Properties for each primary domain file. Details about this configuration step and why we recommend it is in Section 3.2.6.2 on page 58.

7.2.8 Configure the Clients

Once the DNS servers ASISP and ASISP2 are configured and started, and the domain names, in-addr.arpa files, and IP addresses are registered with InterNIC, the clients located in *msu.edu* and *inc.com* should be configured to use either ASISP or ASISP2 DNS servers.

Both name servers are considered to be authoritative for *msu.edu* and *inc.com*. Half of the clients can be configured with ASISP's IP address for its DNS server and the other half of the clients can be configured with ASISP2's IP address for its DNS server. This balances the workload between the two name servers.

Many clients can be configured with more than one IP address for its DNS server. If this is the case, both IP addresses should be listed, half the clients with ASISP's IP address listed first and the other half with ASISP2's IP address listed first. This also balances the workload between the two name servers.

Chapter 8. DNS Server Tips, Tools, and Problem Determination

This chapter describes tips to prevent DNS server problems, performance considerations, and how to identify problem symptoms, and use the appropriate diagnostic tools, logs, or traces to debug problems.

8.1 Tips and Tools

This section contains some tips to prevent problems and tips for performance. It also describes the various tools available to a DNS administrator to troubleshoot DNS problems and how to use those tools.

8.1.1 Tips for Preventing Problems

IFS File Ownership

When the Operations Navigator GUI creates DNS files in the IFS directory /QIBM/UserData/OS400/DNS, the file is created with the owner value set to the AS/400 user profile that the user used to connect. If this user profile is deleted, all objects owned by this user profile are also deleted.

Tip

To prevent accidentally deleting the DNS files (if the user's user profile is deleted), change the ownership of the files to a system-supplied user profile such as QTCP.

Restarting the DNS Server

As a DNS server queries other name servers for information it is not authoritative for, it stores the answers in its cache. That way if another client asks for the same query, the name server can supply the response from its cache instead of querying the authoritative name server again.

Completely stopping and starting the DNS server clears the cache. Therefore, to keep a DNS server's cache rich with information, avoid stopping and starting the name server needlessly. If a configuration change is made, the smart icon "update server" should be used to update the configuration without stopping and starting the name server. The "update server" smart icon does not clear the name server's cache.

The Postmaster Electronic Mail Address

As we create a new primary domain, the Operations Navigator DNS configuration displays a default administrator's e-mail address of:

postmaster.<hostname>.<domain name>.

The preceding e-mail address is the address of the person responsible for the data in this zone. If we keep the default, the preceding e-mail address is inserted in the SOA record of the primary domain file. The AS/400 system does not automatically create a user profile or a POP3 system directory entry of *postmaster*. Thus, the DNS administrator needs to remember to manually create a POP3 directory entry of postmaster and add an associated SMTP system alias table entry of:

SMTP UserId = **postmaster**

SMTP Domain Name = <hostname>.<domain name>.

Manually editing the DB files in DNS IFS directory:

Every primary domain file configured with Operations Navigator's DNS configuration results in the creation of a file with a .DB extension in the IFS directory /QIBM/UserData/OS400/DNS. We recommend that you do *not* manually edit these files. If changes need to be made, use the Operations Navigator DNS configuration displays. The reasons for this recommendation are as follows:

- Every DB file contains an SOA record. This record contains the serial number that secondary name servers check to make sure their secondary domain files are at the same level as the primary domain files. Therefore, when changes are made to the primary domain files, the Operations Navigator DNS configuration automatically increments this serial number. If the DB files are edited manually, it is up to the DNS administrator to remember to manually increment the serial number in the SOA record.
- When the Operations Navigator DNS configuration is used to add (or delete) hosts to the forward mapping primary domain files, Operations Navigator automatically adds (or deletes) the host to the corresponding reverse mapping (in-addr.arpa) file if the enable Create and delete reverse mappings by default is checked. This saves the DNS administrator configuration time and prevents inadvertently omitting the hosts in the in-addr.arpa file. This convenience is lost when primary domain files are manually edited. A DNS administrator must remember to add or delete a host from the in-addr.arpa file as well as the forward mapping file.
- When a change is made in the DB files, the DNS server needs to be stopped and started or restarted to pick up the change. The AS/400 STRTCPSVR SERVER(*DNS) RESTART(*DNS) command stops and starts the DNS server, which causes the cache to be cleared - we do not recommend doing this. The recommended method to pick up configuration changes is to use the Operations Navigator DNS configuration "update server" smart icon. The configuration is then refreshed without clearing the cache. Since Operations Navigator should be used to pick up the configuration changes, the DNS administrator should make the changes with this GUI in the first place.

The LOCALHOST Host

Every primary forward mapping domain file created for a DNS server should include the host *localhost* with an IP address of 127.0.0.1. Consequently, every DNS server should have a reverse mapping domain 0.0.127.in-addr.arpa created also.

8.1.2 Tips for Performance

Use this list of tips if you are concerned about performance:

1. SOA record on a primary domain identifies the frequency of zone transfers. See page 79 in the second edition of *DNS and BIND* by Albitz & Liu, or RFC 1537 and RFC 1912 for more information.
2. The default **TTL** (time to live) value in the SOA record for a primary domain identifies how long a RR record will stay in the cache of another server. A longer value can will create less network traffic.

Operations Navigator GUI Default = 1 day

RFC 1537 recommends 4 days

RFC 1912 considers 1 to 5 days typical and recommends 3 days and considers this timer value the most important.

DNS and BIND by Albitz & Liu, second edition considers 3 hours aggressive, 1/2 day reasonable, 8-24 hours possible. Temporary changes to this time can be made when major updates are planned.

The TTL value on individual resource records that are referred to, but do not change often, can be configured for a longer time. The individual TTL value on a resource record overrides the TTL value in the SOA record. In this case, long times (1 to 2 weeks) are reasonable for an MX, an A, and a PTR record for mail hosts, a NS record of a zone, and an A record of name server.

3. The **refresh** timer in the SOA record is the time a secondary waits to check if an update is needed:

Operations Navigator GUI default = 3 hours

RFC 1537 recommends 24 hours.

RFC 1912 considers 20 min to 2 hours short and 2 to 12 hours long.

4. The **retry** timer on the SOA record is the time a secondary waits before re-attempting a refresh if the refresh query fails.

Operations Navigator GUI default = 1 hour

RFC 1537 recommends 2 hours.

RFC 1912 just says to use a fraction of the refresh timer.

5. The **expire** timer is the time a secondary stops using its data to answer queries and must complete a zone transfer to continue to answer queries.

Operations Navigator GUI default = 7 days

RFC 1537 RECOMMENDS 30 days.

RFC 1912 suggests 2-4 weeks, longer than a major outage.

6. The **round robin** function of the DNS server will perform a simple form of load sharing, however, this is not load balancing. For details, see pages 211 and 212 in the second edition of *DNS and BIND* by Albitz & Liu.

The round robin function is reasonable for terminal servers, FTP servers, or Web servers. The recommendation is to reduce the TTL for these hosts' resource records so they do not stay in cache.

7. Running with a debug level of greater than 3 significantly increases the startup time of your DNS server.
8. We recommend you locate your name server on a network with the most traffic.
 - Create additional name servers to increase performance. The creation of additional secondary or cache-only servers can reduce the load on the primary and first secondary name servers.
 - RFC 1912 recommends *not* configuring secondaries to get their zone transfer from another secondary.
9. The DNS Server Statistics information can be used to calculate information to determine how your DNS server is performing.

- The Stats information can also be used to determine exactly where all queries received are coming from. The statistics are reported as totals (the global numbers) and by requesting address.
 - You can make a calculation using some of the data in the Statistics dump to determine how busy the name server is. An example of this calculation is in a Tip at the end of Section 8.1.6, “Dump Server Statistics” on page 194.
10. Page 272 in the second edition of the *DNS and BIND* by Albitz & Liu warns that a bad connection or a network outage may be masqueraded as poor DNS server performance. Use the debug tool, and *ping* to check if there are addresses that are never responding.
11. AS/400 considerations:
- Some DNS reference materials refer to STATS information that is logged every hour automatically and placed in a job log or the name server’s equivalent to an AS/400 job log. This is not the case with the AS/400 system’s DNS server. To view STATS information, you must use the Operations Navigator GUI to manually dump the STATS information. For more information and a sample STATS output, see Section 8.1.6, “Dump Server Statistics” on page 194 .
 - The run priority for the DNS QTOBDNS job in V4R2 defaults to 50.

8.1.3 Tools for Problem Determination

In this section, several tools are documented for troubleshooting DNS problems. However, some of these tools should only be used on rare occasions and some only if instructed to do so by AS/400 Software and Service Support. The most important debug methods **in order of usefulness** is as follows:

1. Operations Navigator DNS Configuration displays:

The Operations Navigator DNS Configuration displays should be used to check for completeness, for mis-typed domain names, mis-typed host names, and mis-typed IP addresses. From Operations Navigator, the DNS administrator can make sure the server has been updated after a DNS configuration change has been made, ensure newly created domains are enabled, and verify the server is started.

2. The AS/400 job logs:

After configuring a name server for the first time or after any major configuration changes, always review the QTOBDNS job log for errors after the name server has been started. Many DNS configuration errors cause errors to be posted in this job log. Thus, this job log is a critical tool when debugging a DNS problem.

3. Nslookup interactive tool:

Nslookup is a way to pose queries to the name server and view its responses interactively. This tool can be useful if you suspect a query is not being resolved the way you think it should be. It is also useful as an informal testing mechanism after a name server is first configured.

4. Querylog file in AS/400 IFS:

This is a log of the queries the name server has received. It can be useful to verify that the query from a client actually made it to the name server (that is,

the TCP connectivity exists and the client is indeed sending the query as you expect). Querylog is sometimes useful when debugging mail delivery problems.

With the exception of Operations Navigator DNS configuration, the preceding tools are discussed in more detail in the following sub-sections as well as some additional tools that have less importance when troubleshooting a DNS problem.

8.1.4 AS/400 Job Logs

8.1.4.1 The Active QTOBDNS Job Log

With so much time spent on Operations Navigator to configure the AS/400 DNS server, it is easy to overlook one of the most informative logs for DNS problem determination: the AS/400 job log of the DNS job: QTOBDNS.

If the DNS server is started, the QTOBDNS job is active and running under the QSYSWRK subsystem. You can locate it with the following AS/400 command:

```
WRKACTJOB SBS(QSYSWRK)
```

Once QSYSWRK's active jobs are displayed, page down until you find the job named QTOBDNS. Choose option 5 in front of this job to work with the job and on the next display, choose option 10 to display the job log. When the job log is shown, press F10 to display the detailed messages. The bottom of the job log is displayed. You may need to page up to find error messages logged at the time you had a problem. If you find an error message in the job log that needs investigating, you can see more details by placing the cursor on the message itself and pressing F1 for help.

Tip

When you finish configuring the AS/400 DNS server and start the DNS server for the first time, we highly recommend that you review the QTOBDNS job log for errors that are logged when the DNS server starts. For example, spelling errors in the names of primary domain files and spelling errors in the domain names of hosts cause error messages to be posted to the QTOBDNS job log.

Tip

When you finish configuring a secondary name server and start it for the first time, we highly recommend that you review **both** QTOBDNS job logs: the QTOBDNS job log on the secondary name server and the QTOBDNS job log on the primary name server. Remember that if a secondary name server's configuration has the *Backup Primary Domain Files* checked off, the secondary name server is booted using the backup files and then attempts to do the zone transfer from the primary name server. In this case, the zone transfer can fail but the secondary name server is started. This is actually good from the standpoint of availability, but the point is that the DNS administrator never knows the zone transfer failed without reviewing the QTOBDNS job log on the secondary name server.

8.1.4.2 The Inactive QTOBDNS Job Log

Sometimes it is necessary to review the job log of QTOBDNS after the DNS has been stopped and the job QTOBDNS has ended. Or, even more importantly, the DNS server is having such a severe problem that the QTOBDNS job starts and ends before you have a chance to review the active QTOBDNS job log.

To find the job log of a job that is no longer active, you need to find the job's spooled output. It helps to know the user that job runs under. The DNS jobs run using the QTCP user profile. Therefore, use the following command:

```
WRKSPLF QTCP
```

If the job has recently ended, the job's spooled file may be near the bottom of the resulting list. Use F18 to go to the bottom of the Work With Spooled Files List. The name of the job is listed under the User Data column.

8.1.4.3 The QTOBXFER Job

The QTOBXFER job is a job that starts and is active on the secondary name server for the duration of a zone transfer. This job typically starts and ends quickly and to review its job log, you need to review the job's spooled files because the job has usually ended. The job runs using QTCP user profile; therefore, use the `WRKSPLF QTCP` command and F18 to go to the bottom of the list to locate the spooled file containing the ended job's job log.

If the secondary name server is configured to have three secondary domains as it was in Chapter 3.2.6, "Creating a Secondary DNS Server" on page 57, three QTOBXFER jobs will start. There is always one QTOBXFER job for each domain file that is being zone transferred.

Tip

If a zone transfer fails, look in the QTOBXFER job log. Also, *always* review the QTOBDNS job logs on both the secondary and the primary name servers when troubleshooting.

8.1.4.4 The QTOBXMIT Job

The QTOBXMIT job is a job that starts and is active on the primary name server for the duration of a zone transfer. This job typically starts and ends quickly and to review its job log, you need to review the job's spooled files. See previous sections for how to display a job's spooled files and locate a job log of an ended job.

Tip

If a zone transfer fails, look in the QTOBXMIT job log. Also, always review the two QTOBDNS job logs, one on the secondary name server and one on the primary name server.

8.1.5 NSLOOKUP

The AS/400 Name Server Lookup program (nslookup) is a program that allows you to interactively simulate a client to query the DNS server and view the

responses. You can use the nslookup program interactively by entering the following AS/400 command:

```
CALL PGM(QDNS/QTOBLKUP)
```

After entering the command, the AS/400 display should look similar to Figure 183.

```
Default Server:  as1.mycompany.com
Address:  10.5.69.222

>

====>

F3=Exit F4=End of File F6=Print F9=Retrieve F17=Top
F18=Bottom F19=Left F20=Right F21=User Window
```

Figure 183. Initial NSLOOKUP Display

If you get an error message initially instead of the Default Server and Address as in Figure 183, then check “Problem Symptom 2:” on page 208.

With nslookup, you can query your DNS server and make sure it is giving out the responses you expect it to. When you enter nslookup, the type of query that nslookup defaults to is the A record query, which is: type in a host name and the server will respond by giving the IP address of that host.

Several examples of nslookup queries are listed in Chapter 5.5.8, “Verifying DNS with Name Server Lookup” on page 111.

Some of the other types of queries that nslookup accepts are:

```
SET TYPE=MX
```

After the set type=mx command is entered, any text entered subsequently causes the name server to be queried for MX records for the host or the domain you typed in. For example, if a wildcard MX record of:

```
*.mycompany.com IN MX AS1.mycompany.com.
```

was entered in the primary domain file of *mycompany.com*. (see Chapter 3.2.3, “Configuring AS1 as a Mail Server” on page 44 for an example on how to do this). This allows a query of <any host>.mycompany.com. to be responded to with the information that AS1.mycompany.com. is the mail

server as long as <any host> does not have an A record configured for itself. Figure 184 shows an MX query for host *asx* and the name server's response. The type had already been set to MX before the query was entered.

```
>
> asx.mycompany.com.
Server:  as1.mycompany.com
Address: 10.5.69.222

asx.mycompany.com      preference = 0, mail exchanger = as1.mycompany.com
mycompany.com          nameserver = as1.mycompany.com

as1.mycompany.com      internet address = 10.5.69.222

>

===>

F3=Exit F4=End of File F6=Print F9=Retrieve F17=Top
F18=Bottom F19=Left F20=Right F21=User Window
```

Figure 184. Mx Query Using Nslookup

Note: When viewing the results of nslookup, be aware that the text to the right of a > is what the user typed in. The text that does not have a > to the left of it is text that nslookup displayed. After a query is typed by the user, nslookup always first lists the name server and the name server IP address that is giving the response; then nslookup lists the name server's response below.

SET TYPE=PTR

The preceding command allows subsequent commands to query PTR records. In other words, enter an IP address and get a response supplying the host name.

LS -D <domain name> (for example, ls -d mycompany.com)

The preceding command is querying the name server for all the information it knows about the domain file listed. In the example command, this domain is *mycompany.com*. Figure 185 on page 193 shows the nslookup query and the name server's response.


```

>
> ls -d mycompany.com.
[as1.mycompany.com]
mycompany.com.      SOA  as1.mycompany.com postmaster.as1.mycomp
any.com. (888531153 10800 3600 604800 86400)
mycompany.com.      NS   as1.mycompany.com
mycompany.com.      NS   as5.mycompany.com
as5                  A    10.5.69.221
otherdomain          NS   otherhost.otherdomain.mycompany.com
otherhost.otherdomain A    10.1.1.2
p23gb74              A    10.5.62.187
* MX      0      as1.mycompany.com
as1                  A    10.5.69.222
p23thkp1             A    10.5.69.204
as2                  A    10.5.69.211
mycompany.com.      SOA  as1.mycompany.com postmaster.as1.mycomp
any.com. (888531153 10800 3600 604800 86400)
>

```

Figure 185. Nslookup Result of `ls -d mycompany.com` Command

```

>
> otherserver.otherdomain.mycompany.com.
Server:  as1.mycompany.com
Address: 10.5.69.222

Name:    otherserver.otherdomain.mycompany.com
Addresses: 10.5.69.207, 10.1.1.7

>
> otherserver.otherdomain.mycompany.com.
Server:  as1.mycompany.com
Address: 10.5.69.222

Non-authoritative answer:
Name:    otherserver.otherdomain.mycompany.com
Addresses: 10.5.69.207, 10.1.1.7

>

===>

F3=Exit F4=End of File F6=Print F9=Retrieve F17=Top
F18=Bottom F19=Left F20=Right F21=User Window

```

Figure 186. Two Queries for Otherserver

Figure 186 shows the nslookup results of two queries for `OTHERSERVER.OTHERDOMAIN.mycompany.com`. If you remember the details from Chapter 5.5 on page 96, the child name server `OTHERHOST` is authoritative for the hosts located in `OTHERDOMAIN`. The name server in AS1 is authoritative for `mycompany.com`. Thus, the first time nslookup queries the name server AS1 for `OTHERSERVER`, the name server AS1 must query the child server `OTHERHOST` on behalf of nslookup and then return `OTHERHOST`'s response to nslookup. Because the answer was really from the `OTHERHOST` name server, the response back to nslookup is considered an "authoritative" response. The AS1 name server then caches this answer so the second time we use nslookup to submit the same

query to the AS1 name server, it returns the response directly from its cache. Thus, the second response listed in Figure 186 is considered non-authoritative. Any time a response is labeled non-authoritative, it is a response that came out of a name server's cache.

For more information on how to use nslookup, see the DNS chapter in the *TCP/IP Configuration and Reference*, SC41-5420-01.

8.1.6 Dump Server Statistics

Dumping the name server statistics can tell you how busy your name server is and can help a DNS administrator balance the workload between primary and secondary name servers. The first time the name server statistics is dumped, a file named STATISTICS is created in the /QIBM/UserData/Os400/DNS directory. Subsequent requests to dump the server statistics causes additional information to be added to the same file. When the server statistics is dumped, a pop-up window displays the server statistics in the Operations Navigator DNS configuration window. However, the dump file is easier to view when you use Operations Navigator File Systems to view the /QIBM/UserData/OS400/DNS/STATISTICS file using a program such as Netscape.

To dump the name server statistics, follow these steps:

1. Use Operations Navigator to go into the DNS configuration.
2. Click on **View**.
3. Click on **Server Statistics** (see Figure 189 on page 201; the same pull-down menu contains the option to dump the active server database).
4. After a short wait, a pop-up window is shown containing the server statistics.
5. If you have a program on your client such as Netscape, you can use Operations Navigator File Systems to open the STATISTICS file with Netscape and view it with a much larger window. Again, the STATISTICS file is located in the /QIBM/UserData/OS400/DNS directory.

The following example shows a Statistics dump taken from a STATISTICS file. Please note that the name server the dump was taken from was a test name server and, therefore, not very busy.

```
+++ Statistics Dump +++ (888832902) Mon Mar 2 10:01:42 1998
```

```
241630 time since boot (secs)
```

```
241630 time since reset (secs)
```

```
6    Unknown query types
```

```
387  A queries
```

```
3    NS queries
```

```
1    CNAME queries
```

```
59   SOA queries
```

```
301  PTR queries
```

```
49   MX queries
```

2 AXFR queries

41 ANY queries

++ Name Server Statistics ++

(Legend)

RQ RR RIQ RNXD RFwdQ
RFwdR RDupQ RDupR RFail RFErr
RErr RTCP RAXFR RLame ROpts
SSysQ SAns SFwdQ SFwdR SDupQ
SFail SFErr SErr RNotNsQ SNaAns
SNXD

(Global)

849 2 0 2 2 2 0 0 0 0 0 4 2 0 0 0 843 2 2 0 0 0 0 463 550 27

[10.5.62.187]

8 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 8 0 0 0 0 0 0 8 6 0

[10.5.69.208]

432 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 432 0 0 0 0 0 0 432 257 0

[10.5.69.217]

61 0 0 0 0 0 0 0 0 0 0 4 2 0 0 0 57 0 0 0 0 0 0 4 0 0

[10.5.69.221]

331 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 331 0 0 0 0 0 0 2 282 26

[10.5.69.222]

17 0 0 0 2 0 0 0 0 0 0 0 0 0 0 0 15 0 2 0 0 0 0 17 5 1

[10.1.1.2]

0 2 0 2 0 2 0 0 0 0 0 0 0 0 0 0 0 2 0 0 0 0 0 0 0 0

-- Name Server Statistics --

--- Statistics Dump --- (888832902) Mon Mar 2 10:01:42 1998

We have defined some of the more useful statistics in the previous dump:

- 241630 seconds have elapsed since the name server was started.
- 241630 seconds have elapsed since the name server was last updated.
- The name server received six queries of which it did not recognize the type.

- The name server has received 387 A record queries since the name server started. This is usually the most common type of query: an address lookup based on a host name.
- The name server has received three NS queries. A name server can do an NS query when it is trying to look up a name server for a root domain, or an application such as NSLOOKUP can do a NS query.
- The name server has received one CNAME query. A CNAME query is a query that is trying to find out about aliases for a host.
- The server has received 59 SOA record queries. A secondary name server queries the SOA record of the primary name server to verify its domain files are at the latest level.
- The name server has received 301 PTR queries. These are reverse look up queries; the client has the IP address and is querying for the host name.
- The name server has received 49 MX record queries. This query type is used for mail.
- The name server received two AXFR queries. A secondary name server sends a AXFR query to initiate a zone transfer.
- The name server received four ANY queries. This type of query is used to gather any type of information the name server has for a particular host name. This includes A records, CNAME records, and MX records. *Sendmail* uses this type of query. The IBM Firewall for AS/400 uses *sendmail*.

The next section of the dump is the legend, which is the key that needs to be used to identify the string of numbers listed below the legend. For example, the first number under the *global* heading is 849, which according to the first term in the legend, is RQ. The second number under *global* is 0, which is RR, the second term in the legend, and so on.

This particular statistics dump was taken on AS1 with a configuration similar to the one described in Chapter 5.5. Thus, AS1 is a parent server, primary for *mycompany.com*.

Here we identify the non-zero *global* numbers:

- 849 - RQ: The name server has received 849 queries total since it was started.
- Two - RR: This is the number of responses the name server has received. These are responses for queries this name server has sent.
- Two - RNXD: This number is how many "no such domain" answers this name server received.
- Two - RFwdQ: The number of queries this name server received that needed additional processing before they could be answered.
- Two - RFwdR: The number of responses this name server received that answered the original query and were passed back to the application that made the query.
- Four - RTCP: The name server has received four queries over TCP/IP protocol instead of UDP.
- Two - RAXFR: There were two zone transfers initiated by another secondary name server to this name server.
- 843 -SAns: The count of responses sent by this server.
- Two - SFwdQ: The number of queries that were sent by this name server to another name server when this name server did not have the answer in its domain data or its cache.

- Two - SFwdR: The number of responses from another name server that were forwarded to some other name server or client.
- 463 - RNotNsQ: The count of queries that were not from other name servers.
- 550 - SNaAns: The number of non-authoritative responses (that is, from a name server's cache) sent by this name server.
- 27 - SNXD: The number of "no such domain" responses sent by this name server.

There are similar strings of numbers below the Global numbers that are a break out of the same statistics for individual clients identified by IP address.

For more information on the Statistics dump and a complete definition of the legend, see pages 140-149 in the second edition of *DNS and BIND* by Albitz & Liu.

Tip

To determine how busy your server is, a helpful calculation is taking the Global RQ (the number of queries the server has received) and divide it by the number of seconds the server has been active. This gives an average queries per second. In the previous sample statistics dump, the calculation is:

840/241630 queries/second, which is 0.208 queries per minute or 12.5 queries per hour (not a very busy name server).

We recommend that you make the preceding calculation for your name server and review the AS/400 free disk space before changing the name server's debug level or enabling logging on your name server. Those two name server tools are explained in the next sections.

8.1.7 Run Debug

For troubleshooting purposes, you may be instructed by AS/400 Software Service and Support to run your name server in debug mode. We recommend that you run with the debug level of zero unless instructed to run with a higher level by AS/400 Software Service and Support. The default level for debug is zero, which saves no debug information. To increase the level to debug, use the following steps:

- Use Operations Navigator to go into the DNS configuration.
- Right-click on the **DNS server - <server name >**.
- Click on **Properties**.
- Use the Up arrow to increase the Debug level to a value from 1 to 11. A debug level of 3 is a good starting place for troubleshooting. The higher the debug level is, more information is recorded. See Figure 187.
- Stop and start the name server to pick up the debug level change.
- Create the failure or DNS problem you are attempting to troubleshoot.
- A debug level greater than 0 creates a file named RUNDEBUG in the /QIBM/UserData/OS400/DNS directory.
- Review this file for help in troubleshooting or deliver the file to AS/400 Software Support per their instructions.
- After capturing the problem with the appropriate debug level, go back into the DNS configuration, turn debug level back down to 0, and stop and start the DNS server to pick up the configuration change.

- Once the problem has been debugged and the RUNDEBUB file is no longer needed, delete it to free up the AS/400 disk space.

Be Careful: A busy name server with debug level set to a level higher than 0 can cause the RUNDEBUB file to become large quickly. Before using a debug level of greater than 0, check the status of AS/400 disk space to make sure the system has space for a large file and check the activity of the name server with a Statistics dump.

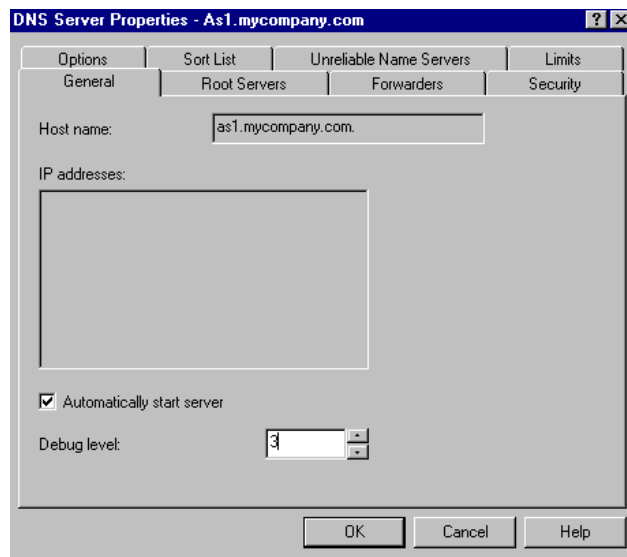


Figure 187. Debug Level Setting Change

The following excerpt is from the RUNDEBUB on AS1 name server. An A record query was sent to AS1 from a client with IP address 10.1.1.2. The query was for: AS2.mycompany.com.

As you can see, **one** A record query caused **16** lines to be logged in the RUNDEBUB file. This is with only a debug level of 3. The response to the A record query was IP address 10.5.69.211. Notice that a level of 3 did not cause the IP address in the response to be logged in the RUNDEBUB file. If the response the name server gives needs to be reviewed, you can use the nslookup interactive tool (the recommended method) or a higher level of RUNDEBUB can be used.

Excerpt from RUNDEBUB as a Result of One A Record Query

```
datagram from [10.1.1.2].53, fd 7, len 35; now Fri Feb 27 11:08:56 1998
req: nlookup(as2.mycompany.com) id 50914 type=1 class=1
req: found 'as2.mycompany.com' as 'as2.mycompany.com' (cname=0)
wanted(SPP:0000 :1aefQTOBDNS QTCP 023250 :39040:33:22, 1, 1) [IN A]
finddata: added 1 class 1 type 1 RRs
req: foundname=1, count=1, founddata=1, cname=0
```

```

sort_response(1)

findns: SOA found

req: leaving (as2.mycompany.com, rcode 0)

free_nsp: as1.mycompany.com rcnt 1

findns: 1 NS's added for 'mycompany'

free_nsp: as1.mycompany.com rcnt 1

doaddinfo() addcount = 1

do additional "as1.mycompany.com" (from "mycompany.com")

found it

ns_req: answer -> [10.1.1.2].53 fd=7 id=50914 size=145 Local

```

For more information on reading the RUNDEBBUG file, see Pages 237-256 in the second edition of *DNS and BIND* by Albitz & Liu.

Important: We recommend that you do not run your DNS server with a debug level greater than zero unless instructed to do so by AS/400 Software Service and Support. Depending on how busy your name server is, any debug level greater than zero can cause the RUNDEBBUG file to become large. Also, after the file has been used to troubleshoot the problem, we recommend deleting the file to free up the AS/400 disk space.

8.1.8 DNS Server QUERYLOG

It is possible to log all queries to the DNS server in a file named QUERYLOG, which is located in the /QIBM/UserData/OS400/DNS directory.

If a DNS server is busy, the QUERYLOG can become quite large very fast; therefore, we recommend that you only turn the logging on after you have monitored and reviewed the summary DNS server statistics and determined that your AS/400 system has enough file space if the QUERYLOG should become large.

To turn on logging, use the following steps:

1. Right-click on **DNS Server-<server name>**.
2. Click on **Properties**.
3. Click on the **Options** tab.
4. Place a check in the small box labeled: **log all queries received by name server**. See Figure 188.
5. Stop and start the name server for the change to take effect.
6. After you finish troubleshooting your problem, go back into DNS server properties, disable logging, stop and start your DNS server to pick up the configuration change, and delete the QUERYLOG file after it is no longer needed to free up disk space.

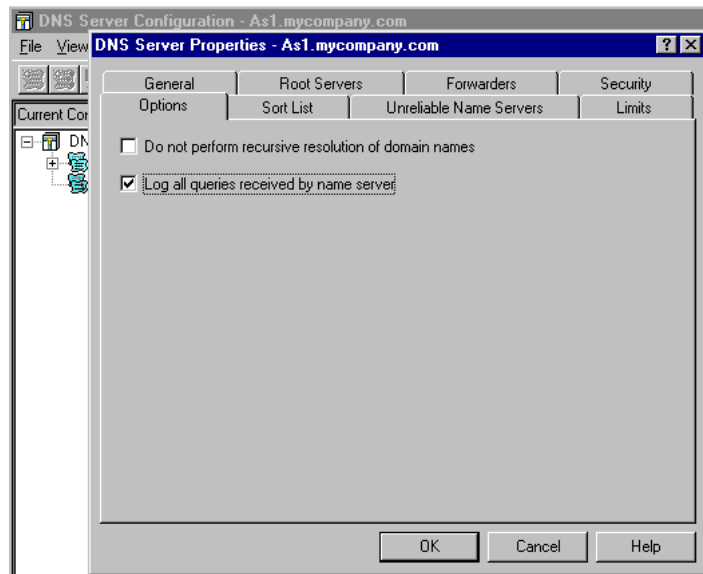


Figure 188. Enable Query Logging

The file QUERYLOG can be reviewed using Operations Navigator file systems and a program such as Netscape. The following example shows a portion of a QUERYLOG file:

Excerpt from QUERYLOG

XX /10.5.69.222/OTHERDOMAIN.MYCOMPANY.COM.mycompany.com/A: Tue Feb 24 15:49:16 1998

XX /10.5.69.222/OTHERDOMAIN.MYCOMPANY.COM/A: Tue Feb 24 15:49:16 1998

XX /10.5.69.222/otherdomain.mycompany.com/MX: Tue Feb 24 15:49:18 1998

XX /10.5.69.222/otherhost.otherdomain.mycompany.com/MX: Tue Feb 24 15:49:19 1998

XX /10.5.69.222/otherhost.otherdomain.mycompany.com/A: Tue Feb 24 15:49:19 1998

The preceding query log was from the AS1 parent name server running on an IP address of 10.5.69.222. The configuration was that of 5.6, "Mail Between Otherdomain.mycompany.com and Mycompany.com" on page 116. Notice that the queries were coming from 10.5.69.222 (the IP address listed to the left in each line of QUERYLOG is the source of the query), which is the AS/400 system the name server running on. This means an application on the AS/400 system is querying the name server. In this case, the application was SMTP and Mail Framework. Mail was arriving on AS1 (as a PC client's SMTP outgoing mail server) but the mail was destined for a POP mailbox on the OTHERHOST AS/400 system. Thus, the SMTP and Mail Framework applications on AS1 were querying the name server in an attempt to determine where to send the mail.

By understanding the configuration steps in 5.6, "Mail Between Otherdomain.mycompany.com and Mycompany.com" on page 116, you can

guess that of the five queries previously listed, only the last one received a positive response from the AS1 name server.

The tool QUERYLOG is of minor importance except in one area since the log does not contain the responses that the name server is giving out, only the queries the name server is receiving. The one area in which QUERYLOG has greater importance in troubleshooting is in mail problem determination. When SMTP and Mail Framework applications are attempting to deliver mail, they also make queries to the name server. QUERYLOG can be used to identify which queries SMTP and Mail Framework are sending to the name server. The IP address of the client sending the query is the IP address of the AS/400 system itself when SMTP and Mail Framework are the applications doing the querying. The queries listed in QUERYLOG can then be jotted down and nslookup can then be used with those same queries to determine what name server responses the SMTP and Mail Framework applications are receiving.

Additional information on debugging mail is contained in Section 8.1.10, "Tips on Debugging Mail on an AS/400 System" on page 202.

8.1.9 DNS server Dump Database

It is possible to dump the DNS server database for troubleshooting purposes if AS/400 Software Support instructs you to do so. The resulting file contains the complete configuration of the DNS server as well as the contents of the name server's cache. Usually, the contents of the name server's cache is not the cause of a problem and the configuration itself can be easily reviewed using Operations Navigator; thus, the Dump Database is a troubleshooting tool of relatively minor importance.

Within Operations Navigator DNS configuration, there is a smart icon labeled Database. Clicking on this icon causes the name server database to be dumped. An alternative method to dump the database is to:

- From Operations Navigator DNS Configuration, click on **View**.
- Click on **Active Server Database**. See Figure 189. It takes a few seconds to finish dumping the database.

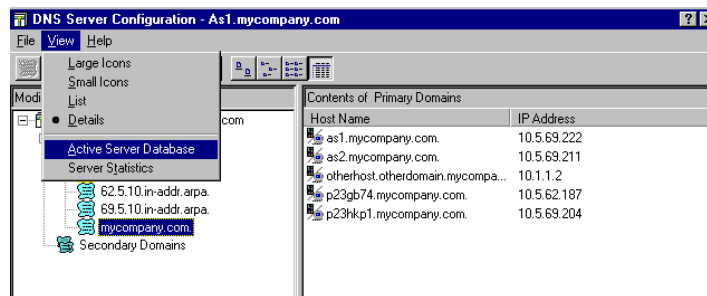


Figure 189. Dumping the Active Server Database

When the active name server database is dumped, a file named DUMPDB is created in the /QIBM/UserData/OS400/DNS directory. The following few lines are an excerpt from the DUMPDB file on

OTHERHOST. OTHERDOMAIN.mycompany.com. A few queries were posed to OTHERHOST, which caused it to query the parent server AS1 at IP address of 10.5.69.222. OTHERHOST cached the responses from AS1. The following portion of

DUMPDB is the contents of `OTHERHOST`'s cache. Cached information can be identified by the credibility tag:

Cr=

Thus Cr=auth [10.5.69.222] on the right-hand side of the line indicates that the information is a cached authoritative response from an IP address of 10.5.69.222.

any 86357 IN MX 0 as1.mycompany.com. ;Cr=auth [10.5.69.222]

p23thkp1 86332 IN A 10.5.69.204 ;Cr=auth [10.5.69.222]

as1 86320 IN A 10.5.69.222 ;NT=42 Cr=auth [10.5.69.222]

For more information on reading the Database Dump, please see Pages 260-263 in the second edition of *DNS and BIND* by Albitz & Liu.

8.1.10 Tips on Debugging Mail on an AS/400 System

When mail is not being delivered as expected, a DNS/Mail administrator is faced with one of the most challenging troubleshooting areas in TCP/IP.

8.1.10.1 The Starting and Ending Place

The first step in debugging mail is always knowing exactly what the users are using to address the mail to. If possible, visit the users at the client location and watch them type in the "Mail To" value: <user Id@smtp domain name>. Watch for mis-typing. Make sure the user is using the @ symbol and not using the word *at*.

The second step is to find the SMTP User ID and the SMTP Domain name in the AS/400 system alias table on the AS/400 system for the POP client the mail should be delivered to.

These two pieces of information are the starting and ending place for mail. Mail delivery starts by using the "Mail To:" information and ends by delivering the mail to the POP mailbox on the AS/400 system associated with the SMTP User ID and the SMTP Domain name.

What the user types to the right of the @ sign in the "Mail To" should match the SMTP Domain name in the AS/400 SMTP system alias table for the POP3 user who should be receiving the mail with *one exception*: when aliases are used.

For example, in Chapter 3.2.3, "Configuring AS1 as a Mail Server" on page 44, the scenario mail was addressed to:

user@mycompany.com

However, the AS/400 SMTP system alias table listed this user's SMTP Domain name as *AS1.mycompany.com*. This discrepancy is OK and mail is successfully delivered because AS1's local host table listed *mycompany.com* as an alias to *AS1.mycompany.com* and the Search First parameter in `CFGTCP` opt 12 is set to `*LOCAL`.

8.1.10.2 The POP3 Directory Entry

The POP3 directory entry can be a source of confusion for an AS/400 administrator configuring POP3 for the first time. What makes a directory entry a **POP3** directory entry?

The answer is: two parameters in the directory entry determine if the entry is a POP3 directory entry. They are:

- Mail Service Level = 2 (System message store)
- Preferred address = 3 (SMTP name)

For an complete example of configuring a POP3 directory entry, see Chapter 3.2.3.1, "Configuring a POP3 User on AS1" on page 45.

TIP: The POP directory entry needs to be configured on the AS/400 system that is the final resting place for the mail (until the user "Get's the Mail"). This is the AS/400 system that the POP3 client has its Incoming POP Server configured as. It is the AS/400 system where the POP3 client "GETS" mail. There is another kind of directory entry that can be used to forward mail. It is a different type of directory entry than the POP directory entry. It is explained in Appendix A.2, "Mail Forwarding" on page 433.

TCP/IP Configuration

Verify the SMTP client sending the mail and the POP client receiving the mail have TCP/IP connectivity to their respective servers. Also verify that each client can successfully ping their server by IP address. If the PING is not successful, you need to debug a TCP/IP connectivity problem before proceeding to debugging a mail problem:

- Make sure the appropriate AS/400 line descriptions are active.
- Verify the associated IP interface has been started on the AS/400 system.
- Verify the TCP/IP route exists if the client is on another subnet from the SMTP, POP, or DNS server.

If the mail client is configured to have the SMTP Outgoing Mail Server or Incoming Mail Server to be a host.domain name rather than an IP address, then verify that PING to the host name is successful. If PING by IP address works but PING by host name fails, you need to debug a DNS problem before proceeding to debugging a mail problem.

8.1.10.3 DNS Server

Verify the DNS server is started and an active QTOBDNS job exists in QSYSWRK subsystem. Check its job log for errors. Verify the IP interfaces that the DNS server should be bound to are started including the Internet address listed on the same AS/400 system's CFGTCP opt 12.

If changes or corrections have been made to the DNS server, make sure the DNS server has been updated to pick up those changes.

Use nslookup to verify the DNS server is responding with the answers you expect. For example, is the DNS server resolving the SMTP domain name used to the right of the @ symbol in the "Mail To" address? If not, this can be a problem unless an alias is used in the AS/400 local host table and Searched First =*LOCAL is used (this alias technique was explained in Chapter 3.2.3.4, "Verifying the TCP/IP and SMTP Configuration on AS1" on page 50).

8.1.10.4 SMTP and POP Servers

Verify that the SMTP and POP servers are active. If active, their corresponding jobs are listed as active jobs in the QSYSWRK subsystem. Use the following command:

```
WRKACTJOB SBS(QSYSWRK)
```

Page down.

If the SMTP server is active, you should find four SMTP jobs named:

```
QTSMTPBRCL
```

```
QTSMTPBRSR
```

```
QTSMTPCLNT
```

```
QTSMTPSRVR
```

If the POP server is active, locate one or more jobs with the names:

```
QTPOP00622
```

```
QTPOP00635
```

```
QTPOP00681
```

Where the last five numbers in the POP job name can be any number. Also, even one QTPOPxxxxx job active indicates the POP server is active.

If the preceding jobs do not exist under QSYSWRK subsystem, then start these servers with the following commands:

```
STRTCPSVR SERVER(*SMTP)
```

```
STRTCPSVR SERVER(*POP).
```

If you issue the previous commands and still cannot find the associated active jobs in the QYSWRK subsystem, it is possible that these jobs are starting but ending before you can locate them. First, check for any errors in the user job log that issued the STRTCPSVR commands. If your own interactive job was used to issue the commands, review your own job log with the following command:

```
DSPJOBLOG
```

Press Enter followed by F10, and then page up to look for error messages.

Also, if the SMTP or POP jobs are ending with an error, review their spooled job logs for error messages. These jobs run using the QTCP user profile; thus, to find the spooled job logs of the inactive jobs, use the following command:

```
WRKSPLF QTCP
```

Press Enter followed by F18 to go to the bottom of the list. The job name is usually displayed in the User Data field in the Work With Spooled files display.

If the SMTP and POP jobs are active and mail is still not being delivered, always check the STMP and POP active job's job logs for any error messages. Any error messages in these job logs can give you clues as to what is going wrong.

TIP: If changes to the AS/400 TCP/IP domain or host table have been made with the CFGTCP command, opt 12 or opt 10, the SMTP server needs to be ended and started again to pick up the changes.

8.1.10.5 QMSF Job

For mail to be successfully delivered on an AS/400 system, at least one QMSF job needs to be active under the QSYSWRK subsystem. This job should autostart when the QSYSWRK subsystem goes active. However, certain errors can cause the QMSF job to end; thus, if mail is not being delivered, one of the first things to check is to verify that QMSF is active. To do so, issue the following command:

```
WRKACTJOB SBS(QSYSWRK)
```

QMSF should be listed as an active job. If it is not listed, you can start the QMSF job by issuing the following command:

```
STRMSF
```

If you issue the `STRMSF` command and still cannot find QMSF as an active job under QSYSWRK, the job may be starting but ending right away with an error. If this is the case, the ended job's job log should be reviewed for error messages. The QMSF job runs using the QMSF user profile; thus, to find the spooled file for the QMSF job log, issue the following command:

```
WRKSPLF QMSF
```

Use F18 to go to the bottom of the list. Many of these QMSF job log spooled files may be listed. Use the F11 key to display the date and time stamps of these jobs to help locate the one you are looking for.

If the QMSF job is active and mail is still not being delivered, check the active QMSF job log for errors.

8.1.10.6 The IBM Firewall for the AS/400

If the IBM Firewall is involved in the network configuration and the mail should be flowing across the firewall, verify that the firewall is active with the following command:

```
WRKCFGSTS *NWS <firewall name>
```

If it is not active, you may vary it on with option 1 from the `WRKCFGSTS` display.

Verify that the secure mail server is configured correctly on the firewall. If you have made changes to the AS/400 TCP/IP domain information using CFGTCP opt 12 and the Firewall's network server description is configured to use this information, you must vary off and vary back on the firewall network server description to pick up the changes.

To review how an IBM Firewall for AS/400 should be configured when an internal DNS server exists in the secure network, please refer to 6, "Split DNS: Hiding Your Internal DNS Behind a Firewall" on page 125.

If mail inbound from the Internet is not making it to the secure mail server, you can check the mail queue on the firewall. If the mail makes it to the firewall but the firewall cannot relay it, the mail is left on the firewall in the mail queue.

To check the mail queue, check:

```
K:\firewall\mqueue\
```

If the mail is still on the firewall's mail queue, its control file may contain useful information. The control file is the file that begins with a q (for example, qfRAA002.11). The associated data file begins with a d such as dfRAA002.11.

You may also want to check the mail log located in:

E:\mptn\etc\mail.log

And you also may want to check the error file, which is a file that only exists if there is a mail problem. The error file is located in:

E:\mptn\etc\sendmail.err

For additional firewall problem determination including mail, please see the redbook AS/400 Internet Security: IBM Firewall for AS/400, SG24-2162-00.

8.1.10.7 The POP Mailbox on the AS/400 System

When POP3 mail is successfully delivered on the AS/400 system, it is located in a "POP mailbox" on the AS/400 system until the POP3 user issues the "GET MAIL" command from the POP3 client. It is possible to review the contents of an AS/400 IFS directory to determine if a POP3 user has any mail distributions in the POP3 mailbox. This is useful when debugging a mail problem because an administrator does not have to continue to use the POP3 client and issue "GET MAIL" to see if mail is finally working but rather can check for mail with one "green screen" command, which is:

```
WRKLNK ' /QTCPTMM/MAIL/JONEST2 '
```

where JONEST2 in the command is the system directory User ID of the POP3 client; this may be different from their SMTP User Id. The *JONEST2* User ID was used in an example in Figure 36 on page 46. The SMTP user ID used in the same example was *tim* as shown in Figure 37 on page 47.

If the POP3 mailbox exists, the previous command shows the following display:

```
Work with Object Links

Directory . . . . : /QTCPTMM/MAIL

Type options, press Enter.
 3=Copy  4=Remove 5=Next level  7=Rename  8=Display attributes
11=Change current directory ...

Opt  Object link      Type  Attribute  Text
    JONEST2          DIR

Parameters or command
```

Bottom

Figure 190. Locating a POP3 Mailbox on the AS/400 System

NOTE: If the previous command is issued and the error message "object not found" is issued to the user's job log, the POP3 mailbox does not exist. It is important to realize that the POP3 mailbox does not exist until the first distribution of mail is delivered to it. If the POP3 mailbox (in the form of the directory listed in Figure 190) is missing, it does not necessarily mean that the POP3 directory entry was misconfigured. It may just mean that mail has never been delivered to this mailbox yet.

From the display in Figure 190, take option 5 to view the next level. The next level shows any mail distributions that exist in the POP3 mailbox. Figure 191 shows that the two mail distributions are located in JONEST2 POP3 mailbox. These distributions disappear after the POP3 user issues a "GET MAIL" from the POP3 client. You cannot read the contents of these mail distributions from an AS/400 "green screen".

```
Work with Object Links

Directory . . . . : /QTCPTMM/MAIL/JONEST2

Type options, press Enter.
  3=Copy  4=Remove  5=Next level  7=Rename  8=Display attributes
  11=Change current directory ...

Opt  Object link      Type  Attribute  Text
     JW122040.NOT     SIMF
     JW122735.NOT     SIMF
```

Bottom

Figure 191. Mail Distributions Located in JONEST2 POP3 Mailbox on the AS/400 System

8.2 Problem Symptoms and Probable Causes

As the authors of this redbook prepared their DNS configurations to match the scenarios explained in this book, they, of course, made common mistakes and the same as any other DNS administrators, had to troubleshoot their problems. These problem symptoms are documented in this section to give a headstart to other DNS administrators who may run into the same problems or mistakes when configuring their name servers. It is by all means not a complete list of all problems that can occur when configuring name servers.

Problem symptom 1:

Secondary server fails to load data for zone. You receive a message in the secondary server's DNS job log (QTOBDNS in subsystem QSYSRWK), indicating that the server could not load data for zone. Example:

```
Could not retrieve serial number for zone 62.5.10.in_addr.arpa
Secondary DNS server could not load data for zone 62.5.10.in_addr.arpa
Could not retrieve serial number for zone 62.5.10.in_addr.arpa
```

Probable cause 1:

You have made a typing mistake in the domain name. In our example, the domain name for the reverse mapping files includes an underscore character _ instead of a dash -. The correct name is 62.5.10.in-addr.arpa

Probable cause 2:

The primary server is not active. A zone transfer cannot take place on a secondary name server if the primary server it is trying to load from is inactive.

Probable cause 3:

The primary server is active but a security configuration on the primary server is preventing the zone transfer. Check the Properties' security tab on the primary server's DNS server and review the Secondary Server Access List. By explicitly listing one secondary server, you implicitly prevent any other secondary server from completing a zone transfer.

Also check the Properties Security tab of the primary domain file that you are trying to zone transfer. Review the Domain data access for both subnets and IP addresses. By listing a subnet or an IP address here, you implicitly deny access to all other subnets and IP addresses.

Problem Symptom 2:

NSLOOKUP fails with error message:

```
*** Can't find server name for address 10.5.69.222: Non-existent host/domain
*** Default servers are not available
```

Probable cause 2:

There is no PTR record in the reverse lookup file for the DNS server. From the previous error message, the 69.5.10.in-addr.arpa primary domain needs to be checked to ensure that the host (in this case, AS1) the DNS server is running on is listed in this file. If it is not listed, add the host to the 69.5.10.in-addr.arpa file and then click on Update Server smart icon to refresh the name server with the configuration change. Retry the NSLOOKUP.

Problem Symptom 3:

NSLOOKUP fails to give a response to the query but displays the following text:

```
> otherserver.otherdomain.mycompany.com.
```

```
Server: as1.mycompany.com
```

```
Address: 10.5.69.222
```

```
*** as1.mycompany.com can't find otherserver.otherdomain.mycompany.com.:
No response from server
```

Probable Cause 1:

The query for OTHERSERVER posed to the DNS server AS1 is for information that AS1 is not authoritative for; thus, the AS1 name server must query the child server OTHERHOST, which should respond back to the parent server AS1, which should respond back to nslookup. In this case, the child DNS server OTHERHOST was not started. Thus, the AS1 could not get the answer to the query.

Recovery: Start the child DNS server, OTHERHOST.

Probable Cause 2:

Once the child DNS server `OTHERHOST` was started, the same `nslookup` query posed to AS1 resulted in the same error message. The QTOBDNS job log was reviewed on the `OTHERHOST` and it concluded that `OTHERHOST` was active and ready for queries. However, `OTHERHOST`, in this case, had more than one LAN adapter; thus, it had more than one IP address that the DNS server was listening on. AS1's DNS server configuration indicated that `OTHERHOST`'s IP address was 10.1.1.2. When CFGTCP, option 1 was issued on `OTHERHOST` (check the TCP/IP interfaces), it discovered that the 10.1.1.2 IP interface was Inactive.

A closer scrutiny of `OTHERHOST`'s QTOBDNS job log resulted in the discovery of error message: DNS00E9, Could not assign address to socket. Placing the cursor on this error message and pressing F1 for help shows the message detail, which specifies the address that is inactive: 10.1.1.2.

Recovery: Start the 10.1.1.2 IP interface on `OTHERHOST` child name server. Then stop and start the DNS server.

Problem Symptom 4:

The DNS server starts but the QTOBDNS job log contains the error message DNS00E9. See Figure 192.

```
>> CALL PGM(QDNS/QTOBDNS) PARM('-p' '53' '-d' '0' '-b' '/QIBM/UserData/OS400/
DNS/BOOT')
DNS server starting.
Could not assign address to socket.
```

Figure 192. QTOBDNS Job Log: Could Not Assign Address to Socket Error

Probable Cause 1:

The following error message appears:

```
Could not assign address to socket
```

This indicates that upon startup of the DNS server, the server discovered an IP interface that was inactive. This may or may not be a problem. Sometimes IP interfaces are configured and left inactive deliberately and, in that case, the error message could be normal.

Recovery: Place the cursor on the error message and press **F1** for Help. This shows the message details that indicate which IP interface was inactive. If you need the DNS server to respond to queries on this IP interface, the interface needs to be started with the following command:

```
CFGTCP
```

Use option 1, position the cursor on the Inactive interface, and use option 9 to start the interface. Use the F5 key to refresh the display and, if necessary, F11 to display the status of the interface. If the interface continues to be inactive, check the status of the line with the following command:

```
WRKCFGSTS *LIN <line description name>
```

If the status of the line is FAILED, Varied Off, RCYPND, or RCYCNL, attempt to vary off the line and vary it back on. Once the line goes active (or vary on pending), go back to CFGTCP, option 1, and attempt to start the interface associated with that line description again.

If you cannot get the line description to go to ACTIVE or VARY ON PND, you may have a hardware problem. Check for associated error messages in the AS/400 history log with the following command:

DSPLOG

Press F4 to prompt and enter the time range that you attempted to vary on the line.

Tip

If you start an interface *after* the DNS server is started, it will take some time before the DNS server answers queries on the newly started interface. If you want the name server to answer queries on this interface immediately, run the Update Server function.

Problem Symptom 5:

The DNS server starts but the QTOBDNS job log contains the error message:

DNS000F: Host mycompany.com can only have CNAME data.

Also, a secondary name server fails to zone transfer the primary domain file *mycompany.com*. The QTOBXFER job log on the secondary name server contains error message:

DNS006B SOA zone information type, class, or time to live value not valid.

The QTOBDNS job log on secondary name server contains error message:

DNS00C6 Secondary DNS server could not load data for zone mycompany.com.

Probable Cause 1:

The key to this problem is the error message in the QTOBDNS job log on the primary name server. An alias of name of *mycompany.com* is being used somewhere in the *mycompany.com*.DB file on the left hand side of a resource record, which is not a CNAME resource record. The *mycompany.com*.DB file is located in the /QIBM/UserData/OS400/DNS directory. A review of the *mycompany.com*.DB file confirms this: *mycompany.com* is used on the left hand side of the NS record. Of course it is because *mycompany.com* is the name of the domain itself -- the NS record must be listed with *mycompany.com* to the left. The problem is not with the NS record. The problem is with the CNAME record. A domain name cannot be an alias name for a host. This CNAME record must be deleted and the server needs to be then updated (that is, configuration refreshed).

Problem Symptom 6:

The secondary name server's QTOBDNS job log contains some messages that are confusing:

secondary zone mycompany.com (serial number 887939256) loaded successfully.

But then a few messages later in the same job log, the following messages are logged:

Ready to answer queries.

Secondary DNS server could not load data for zone mycompany.com.

Also, the primary server QTOBDNS job log contains the message:

primary zone mycompany.com (serial number 888511902) loaded successfully.

The preceding messages seem to indicate a secondary name server starting successfully from its backup files and failing when it tries to contact the primary master file to check serial numbers.

Note that the two serial numbers of the two messages are not the same. The secondary name server's job was to stay in synch with the primary name server and it does that by checking the serial number of the domain. Thus, why is the secondary name server running with a serial number for *mycompany.com* of 887939256, yet the primary name server is running with a serial number of 888511902?

Probable Cause 1:

The messages in the secondary name server indicate that there was a problem. The secondary name server could not complete a zone transfer from the primary name server. The cause was the problem explained in the probable cause to problem symptom 5. However, let's discuss the messages further. When the secondary domain of *mycompany.com* was configured on the secondary name server, the box labeled *Save Copies of Master Server Data* was checked. This means that when the secondary name server completes its first zone transfer of the domain file of *mycompany.com*, it backs up this file on the AS/400 system that it is running on. The next time the secondary name server is started, it is booted with the backup copy of *mycompany.com* (in this case, serial number 887939256). Then the secondary name server checks the serial number of the primary domain file on the primary name server. If the two serial numbers are different (as in this case), the secondary name server attempts a zone transfer. In this case, the zone transfer failed; thus, the secondary name server is up and running and is capable of answering queries for domain *mycompany.com* but it is running on a downlevel version of the domain file of *mycompany.com*.

Probable Cause 2:

The zone transfer failed because the primary name server is not started.

Probable Cause 3:

The zone transfer failed because the primary name server is started but the IP interface on the primary name server is inactive.

Recovery: check the configuration on the secondary name server to determine which primary name server IP address it is attempting to zone transfer from. On the primary name server, verify that this IP interface is active with the `CFGTCP` command followed by option 1.

Probable Cause 4:

The zone transfer failed because a security configuration on the primary name server is preventing the zone transfer from this particular secondary name server. See Chapter 3.2.7, "Primary Name Server Security Considerations" on page 63, for more information on how security is configured on the primary name server.

Probable Cause 5:

There is a typing mistake in the name of the secondary name server's domain name that the zone transfer is trying to take place against. See Problem Symptom 1.

Problem Symptom 7:

When reviewing the *mycompany.com*. database primary forward mapping file using Operations Navigator File Systems and Netscape, one of the resource records (for example, A record) has a host name listed of:

host1.mycompany.com.mycompany.com.

The *mycompany.com* domain listed twice is incorrect.

And when using Operations Navigator's DNS configuration to display the *mycompany.com* primary domain file, the same problem is shown again. The host *host1* is listed as:

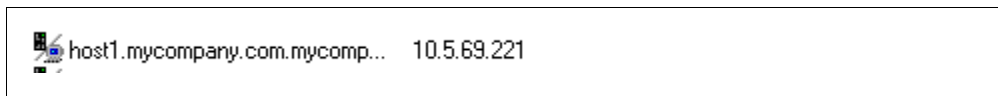


Figure 193. Misconfigured Host in *mycompany.com* Primary Domain File

The *mycompany.com* domain is listed twice, which is incorrect. Where did the second *mycompany.com* come from?

Probable Cause 1:

When using Operations Navigator DNS configuration to add a new host to the primary forward mapping file, the domain name was typed in and the trailing period after the *com* was inadvertently left off. When the DNS configuration sees a domain without a period at the end, it "tries to help" by adding the domain to end of what was typed.

Recovery: Use the Operations Navigator DNS configuration to delete the host *host1* and then add a new host:

host1.mycompany.com.

This time, make sure the trailing period is typed in after *com*.

Problem Symptom 8:

The Operations Navigator DNS configuration displays were used to create new primary domains and the GUI displays them correctly. However, after starting the DNS server, the QTOBDNS job log does not contain any messages that confirm that these primary domain files were successfully loaded. But the job log does not contain any error messages related to loading these files either.

Probable Cause 1:

If primary domain files are not being loaded by the DNS server, there is either a problem with them that should cause an error message to be posted in the QTOBDNS job log or these primary domain files are disabled. When creating primary domains with Operations Navigator DNS configuration, they are initially disabled by default. The DNS administrator must enable each primary domain when the configuration is finished. To enable a primary domain, right-click on the primary domain and click on enable. Then click on the smart icon "update server" to refresh the DNS server's configuration.

8.3 For Additional Help With Problems

AS/400 Specific DNS Problems or Questions

AS/400 Software Service and Support in your respective country can help you with questions or problems with the AS/400 DNS server provided you have a Support Line contract and your question is not one of a consulting nature.

DNS Questions Not Specific to the AS/400 Implementation

There is a DNS news group which is accessible over the Internet that can provide answers to DNS questions not specific to the AS/400's implementation of the DNS server. The newsgroup is:

comp.protocols.dns.bind

It can be located from the URL www.dns.net/dnsrd. (from here, click on *newsgroups*). Or from the URL www.dejanews.com, use the *Find* option to find *comp.protocols.dns.bind*.

Part 2. AS/400 DHCP Server Support

The Dynamic Host Configuration Protocol (DHCP) provides configuration parameters to TCP/IP hosts. It is a client/server protocol that centrally controls and delivers configuration parameters to dynamically configured clients.

Part 2 of this book provides an overview of DHCP concepts and describes how DHCP is implemented in the AS/400 system through case studies.

Chapter 9. DHCP Concepts and Overview

Dynamic Host Configuration Protocol, or DHCP, is a client/server protocol that enables you to centrally locate and dynamically distribute configuration information, including IP addresses.

This chapter provides an overview of DHCP concepts and components. The intention is to summarize concepts that you need to implement DHCP on the AS/400 system. For more information on this subject, refer to *TCP/IP Configuration and Reference*, SC41-5420-01.

9.1 BOOTP, the Predecessor of DHCP

DHCP and its predecessor, Bootstrap Protocol (BOOTP), came about to fulfill the need of diskless workstations to acquire IP addresses and bootstrap information from a server in the network.

BOOTP is an example of how you use the client/server paradigm to bootstrap a diskless workstation and to provide it with IP address configuration. The BOOTP server listens on well-known port 67, and diskless computers usually contain a start-up program in non-volatile storage, or ROM. Because all the workstations start from the same program, it is impossible to store IP addresses in that code. A diskless machine needs to know its IP address to participate in a TCP/IP network. It also needs to know the address of the file server machine where the bootstrap image is stored.

The BOOTP client uses the special broadcast IP address of all ones (255.255.255.255) to obtain its IP address. It is responsible for retransmitting requests if the server does not respond.

The mapping between the client hardware address and the IP address is kept in the BOOTP table, which is manually maintained by the administrator.

BOOTP is the first step of a two-step bootstrap procedure. It does *not* provide the clients with a memory image. Instead, it provides the client only with the information that it needs to obtain an image. The client obtains this memory image after initiating a Trivial FTP (TFTP) request to the server, whose IP address it received from the BOOTP server. Up to V4R1, BOOTP and TFTP were the two protocols that supported the IBM Network Station on the AS/400 system.

Figure 194 on page 218 shows the BOOTP flow between a client and a server. When the server receives a BOOTP request from a client, the server looks up the defined IP address based upon the client's MAC address. It then replies with the client IP address and the name of the load file. The client initiates a TFTP request to the server for the load file.

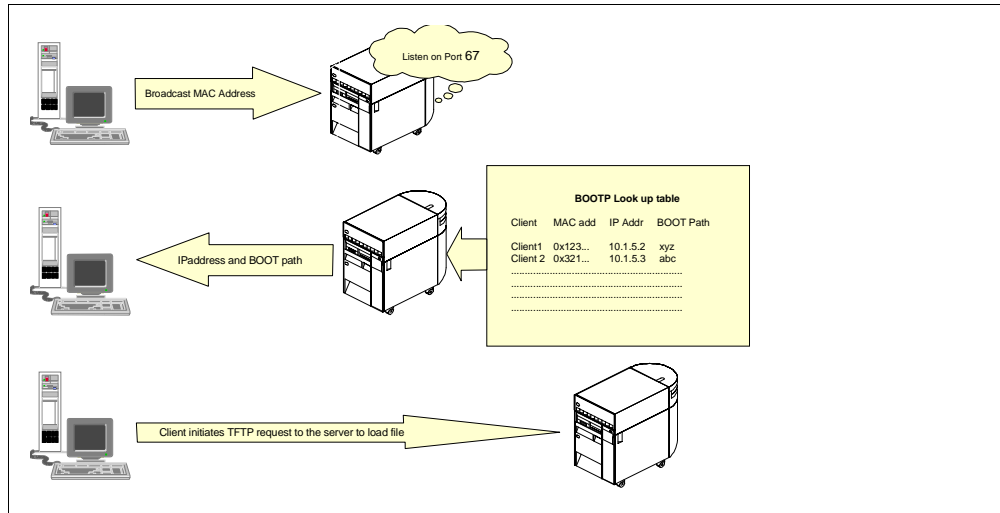


Figure 194. BOOTP Flow between Client and Server

BOOTP uses a limited broadcast address for the BOOTP request. It requires the server in the same subnet as the client that requests configuration information. BOOTP forwarding is a mechanism for routers to forward a BOOTP request between subnets. The agents that forward the BOOTP packets between clients and servers on different subnets are called Relay Agents.

DHCP adds the capability of automatically allocating reusable network addresses and distributing additional host configuration options. DHCP clients and servers use existing BOOTP Relay Agents.

BOOTP clients can interact with DHCP servers and DHCP servers and BOOTP servers can coexist if configured properly. DHCP clients cannot interoperate with BOOTP servers.

The AS/400 DHCP server support in V4R2 accommodates the already existing BOOTP server that was available in earlier releases of OS/400. This AS/400 DHCP server support also accommodates BOOTP clients. Additionally, it performs all of the functions specific to BOOTP as well as all of the added functionality that a DHCP server is assumed to carry. BOOTP and DHCP servers cannot run at the same time on the same system because both use the well-known ports 67 and 68.

IETF RFCs 2131 and 2132 describe DHCP protocols.

9.2 DHCP Overview

DHCP provides a framework for passing configuration parameters to hosts on a TCP/IP network.

The following three types of network components make up a DHCP network.

- **DHCP host clients.** These hosts run the DHCP client programs. The DHCP clients work together with their server counterparts to obtain and implement configuration information to automatically access IP networks. Examples of DHCP clients are the IBM Network Station and the DHCP client support that is

included in TCP/IP for Windows 95. The AS/400 system cannot be a DHCP client.

- **DHCP Servers.** DHCP servers provide the addresses and configuration information to DHCP and BOOTP clients on the network. DHCP servers contain information about the network configuration and host operational parameters, as specified by the network administrator. The AS/400 system in V4R2 can be a DHCP server.
- **BOOTP/DHCP Relay Agent.** Relay Agents (also called BOOTP helpers) are used in IP router products to forward information between DHCP clients and servers on different subnets. BOOTP/DHCP Relay Agents eliminate the need for a DHCP server on each subnet to service the broadcast requests from DHCP clients. The AS/400 system can be a BOOTP/DHCP Relay Agent.

Figure 195 shows the different components in a DHCP network.

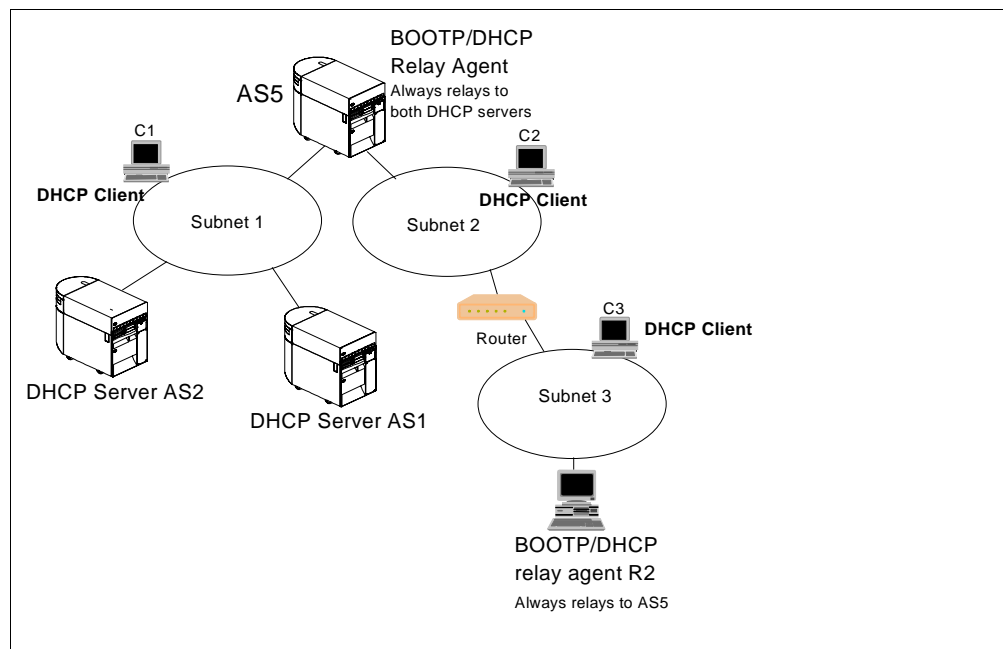


Figure 195. Components in a DHCP Network

9.3 How does DHCP Work?

DHCP allows clients to obtain IP network configuration, including an IP address, from a central DHCP server. DHCP servers control whether the addresses they provide to clients are allocated permanently or leased for a specific period of time. When the server allocates a leased address, the client must periodically check with the server to re-validate the address and renew the lease.

The DHCP client and server programs handle address allocation, leasing, and lease renewal. All of these processes are transparent to end users.

To further explain how DHCP works, this section answers the following questions:

- How is configuration information acquired?

- How are leases renewed?
- What happens when a client moves out of the network?
- How are changes implemented in the network?
- What are BOOTP/DHCP Relay Agents?

9.3.1 How is Configuration Information Acquired?

DHCP allows DHCP clients to obtain an IP address and other configuration information through a request process to a DHCP server. DHCP clients use RFC-architected messages to accept and use the options served them by the DHCP server.

Figure 196 shows a high-level overview of the DHCP protocol cycle.

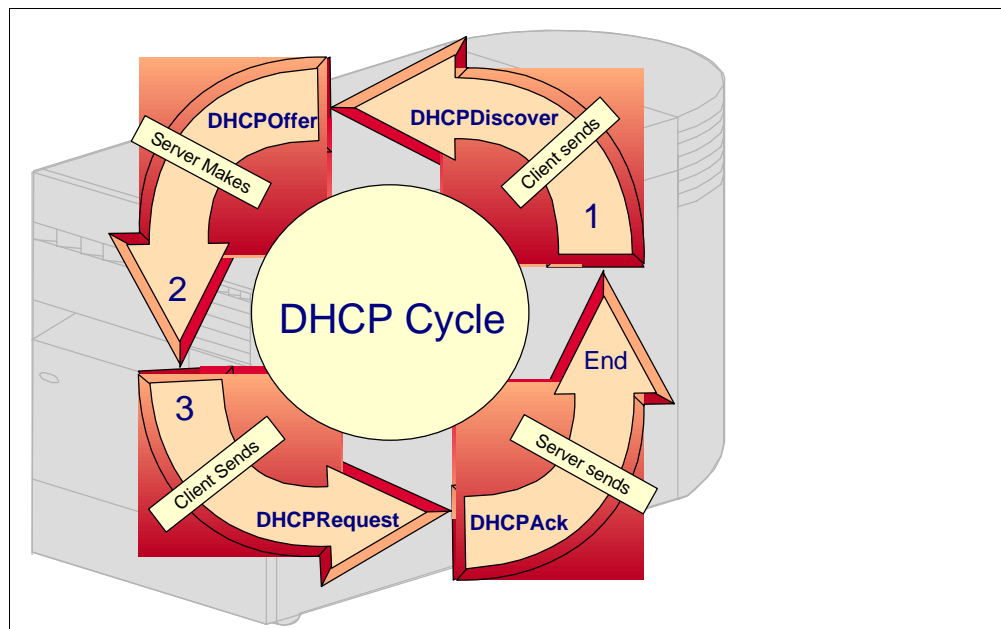


Figure 196. DHCP Cycle Overview

For example:

1. The client broadcasts a message that contains its client ID and announces its presence. The message also requests an IP address (DHCPDISCOVER message) and desired options, such as subnet mask, domain name server, domain name, and static route. See Figure 197.

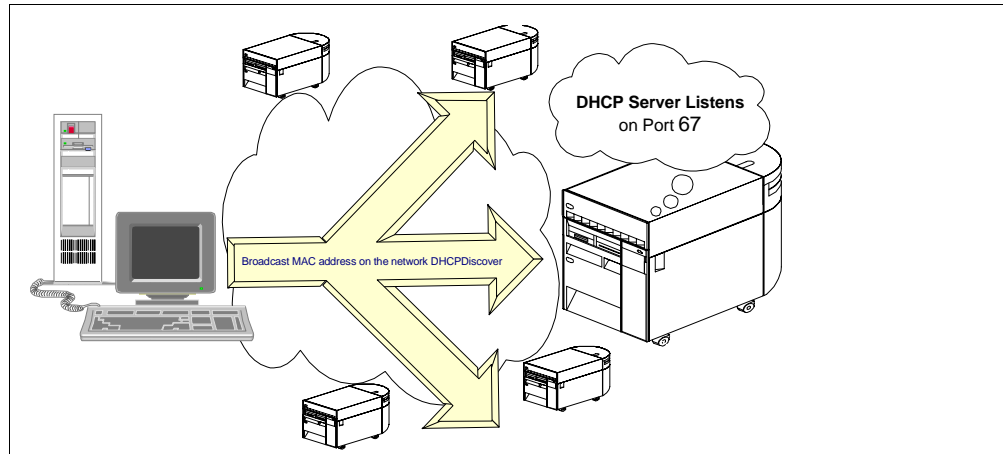


Figure 197. 1- DHCP Client Broadcasts DHCPDISCOVER on its Subnet

Note: If you configure routers on the network to forward DHCP and BOOTP messages (using BOOTP/DHCP Relay Agent capabilities), the broadcast message is forwarded to DHCP servers on the attached networks.

- Each DHCP server that receives the client's DHCPDISCOVER message can send a DHCPOFFER message to the client offering an IP address. If the address has not been previously assigned, the DHCP server checks that the address is not already in use on the network before issuing an offer.

The server checks the configuration file to see if it needs to assign a static or dynamic address to this client.

In the case of a dynamic address, the server selects an address from the **address pool**, choosing the least recently used address. An address pool is a range of IP addresses that are leased to clients. In the case of a static address, the server uses a client statement from the DHCP server configuration file to assign an static address to the client. Upon making the offer, the AS/400 DHCP server reserves the offered address. See Figure 198.

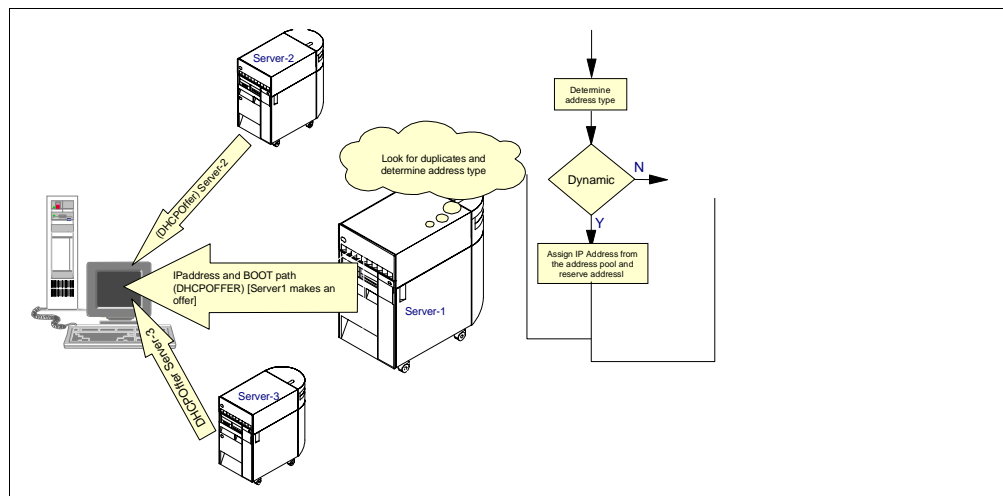


Figure 198. All DHCP in the Subnet Send DHCPOFFER

3. The client receives the offer messages and selects the server it wants to use. Upon receiving an offer, some DHCP clients have the capability to make note of how many requested options are included in the offer. The DHCP client continues to receive offers from DHCP servers for a period of time after the first offer is received. The client takes note of how many requested options are included in each offer. At the end of that time, the DHCP client compares all offers and selects the one that meets its criteria.

Note: Not all DHCP clients have the capability to wait and evaluate the offers that they receive. Many DHCP clients on the market today accept the first offer that arrives.

4. The client broadcasts a message indicating which server it selected and requesting the use of the IP address that server offers (DHCPREQUEST message). See Figure 199.

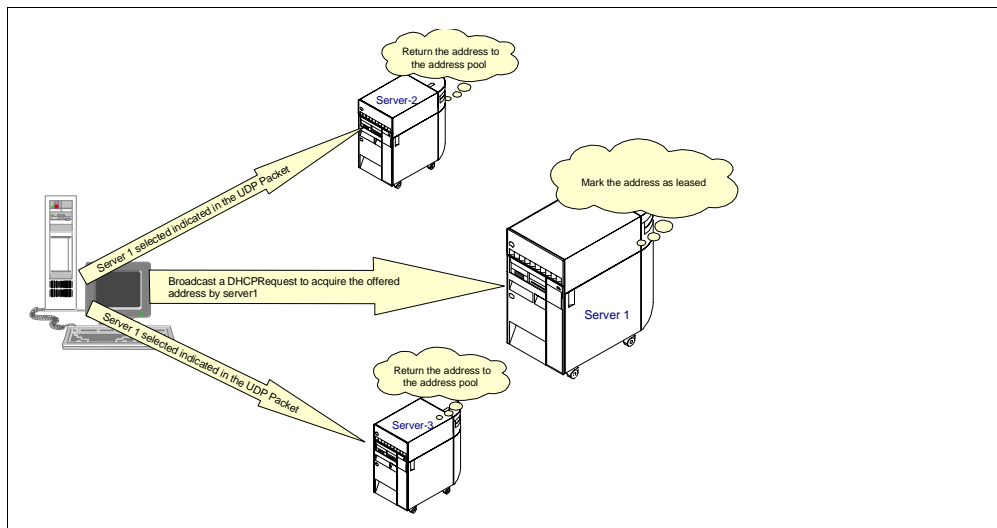


Figure 199. DHCP Client Accepts DHCP OFFER from Server 1

5. If a server receives a DHCPREQUEST message indicating that the client has accepted the server's offer, the server marks the address as leased. If the server receives a DHCPREQUEST message indicating that the client has accepted an offer from a different server, the server returns the address to the available pool. If no message is received within a specified time, the server returns the address to the available pool. The selected server sends an acknowledgment that contains additional configuration information to the client (DHCPACK message). See Figure 200.

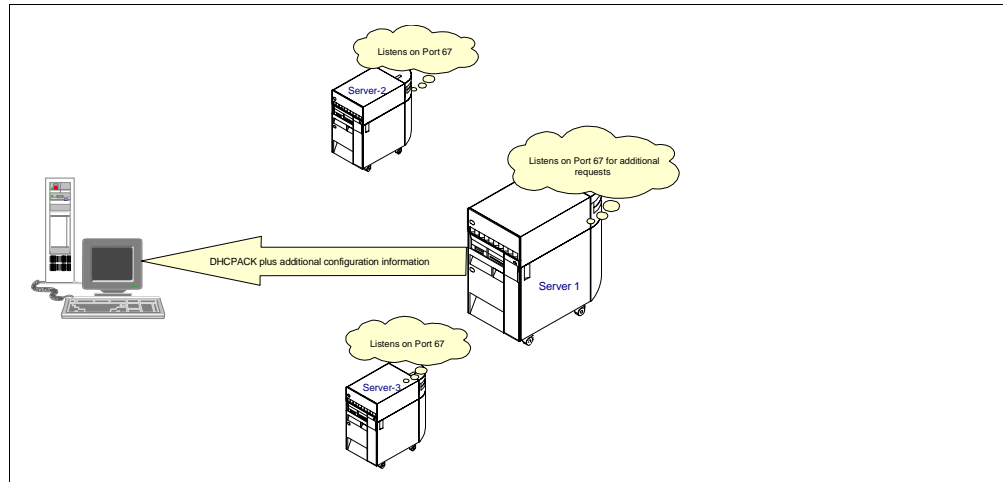


Figure 200. Selected Server Sends Acknowledgment with Additional Configuration to Client

6. The client determines whether the configuration information is valid. Accepting a valid lease, the client specifies a BINDING state with the DHCP server and proceeds to use the IP address and options.

To DHCP clients that request options, the DHCP server typically provides options that include subnet mask, domain name server, domain name, static route, class-identifier (which indicates a particular vendor), and user class.

A DHCP client can request its own, unique set of options. For example, Windows NT 3.5.1 DHCP clients are required to request options. The default set of client-requested DHCP options that IBM provides includes subnet mask, domain name server, domain name, and static route.

9.3.2 How are Leases Renewed?

The DHCP client keeps track of how much time is remaining on the lease. At a specified time prior to the expiration of the lease (usually when half of the lease time has passed), the client sends a renewal request to the leasing server. This request contains its current address and configuration information. If the server responds with a DHCPACK, the DHCP client's lease is renewed.

If the DHCP server explicitly refuses the request, the DHCP client continues to use the IP address until the lease time expires. At this time, the client initiates the address request process, including broadcasting the address request. If the server is unreachable, the client continues to use the assigned address until the lease expires (see Figure 201).

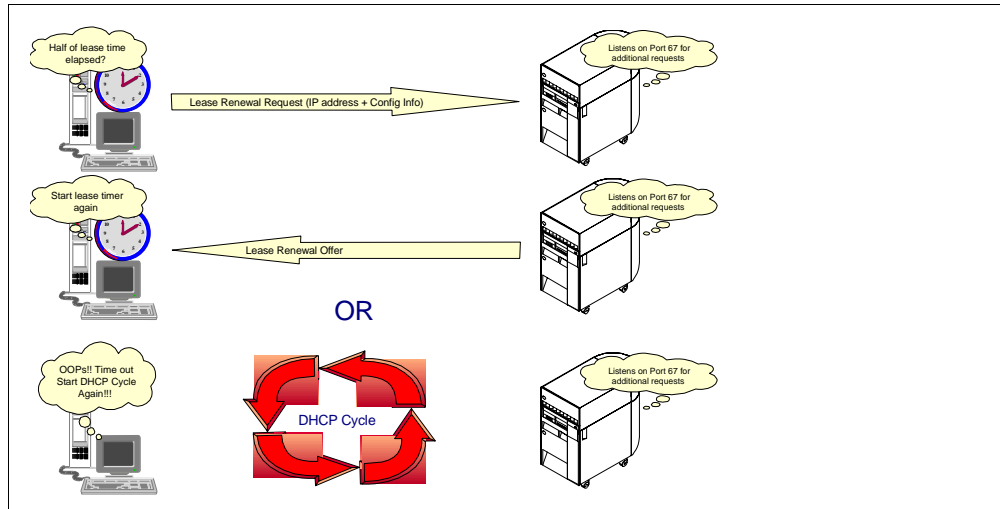


Figure 201. How are Leases Renewed?

9.3.3 What Happens when a Client Moves out of its Subnet?

DHCP provides a client host with the freedom to move from one subnet to another without having to know what IP configuration information it needs on the new subnet. As long as the subnets to which a host relocates have access to a DHCP server, a DHCP client automatically configures itself to access those subnets correctly.

For DHCP clients to reconfigure and access a new subnet, the client host must be re-booted. When a host restarts on a new subnet, the DHCP client tries to renew its old lease with the DHCP server that originally allocated the address. The server refuses to renew the request because the address is not valid on the new subnet. The client then initiates the IP address request process to obtain a new IP address and access the network.

9.3.4 How are Changes Implemented in the Network?

With DHCP, you make changes at the server, re-initialize the server, and distribute the changes to all the appropriate clients. A DHCP client retains DHCP option values that are assigned by the DHCP server for the duration of the lease. If you implement configuration changes at the server while a client is already up and running, the DHCP client does not process those changes until it either attempts to renew its lease or is restarted.

9.3.5 What are BOOTP/DHCP Relay Agents?

The function of a Relay Agent is to forward any BOOTP/DHCP requests that it receives on its subnet or from other subnets in the direction of the DHCP server. The mechanism of operation of a Relay Agent is as follows:

1. The Relay Agent knows the address of the DHCP server beforehand, and it knows where to forward the requests for that server. The Relay Agent can, therefore, be a router that receives and forwards requests.
2. The DHCP client creates a packet with a special field called RELAY AGENT. Initially, the client places all zeros in it. The Relay Agent recognizes that the

RELAY AGENT field is all zeros and puts its own IP address in this field. It then pushes the packet into the next subnet and increments the hop count.

3. The next Relay Agent, if any, sees that the RELAY AGENT field in the packet is not all zeros, forwards the packet to the next server, and increments the hop count by one. This process is repeated until the packet reaches the DHCP server.
4. The DHCP server sends the DHCPOFFER back to the first Relay Agent and the Relay Agent forwards it to the originator client that broadcasted the DHCPDISCOVER. Once the client receives an IP address, the communication is direct between server and client.

The AS/400 system on V4R2 can function as either a DHCP server or [as](#) a BOOTP/DHCP Relay Agent.

Chapter 10. AS/400 DHCP Server Implementation

This chapter describes the implementation of the AS/400 DHCP sever.

10.1 DHCP Software Prerequisites

Native DHCP support on AS/400 in V4R2 requires the following products:

- 5769-SS1 OS/400 V4R2 option 3
- 5763-XD1 V3R1M3 -- Client Access for Windows 95/NT

10.2 DHCP Installation

Installing DHCP support on your AS/400 V4R2 system involves installing 5769-SS1 OS/400 V4R2 option 3 and Client Access for Windows 95/NT (5763-XD1 V3R1M3) in your administrator's workstation. The installation program performs the following tasks:

- Creates an IFS subdirectories: /QIBM/UserData/OS400/DHCP.
- Sets up the IFS files required for DHCP in the preceding directory. If any file already exists, it remains "as is".

Tip

To reset an existing configuration and start over, perform the following steps:

1. Delete the IFS file `dhcpcsd.cfg` file in /QIBM/UserData/OS400/DHCP.
2. `CALL QSYSDIR/QTODDINS` from an AS/400 command entry display. This program creates a blank configuration file that the Operations Navigator's GUI can edit.

You can also perform these steps if you suspect some DHCP files are corrupted. Reinstalling 5769-SS1 option 3 does not replace existing files.

After the installation, proceed with the DHCP server configuration using Operations Navigator. Figure 202 provides an overview of AS/400 DHCP server installation and configuration.

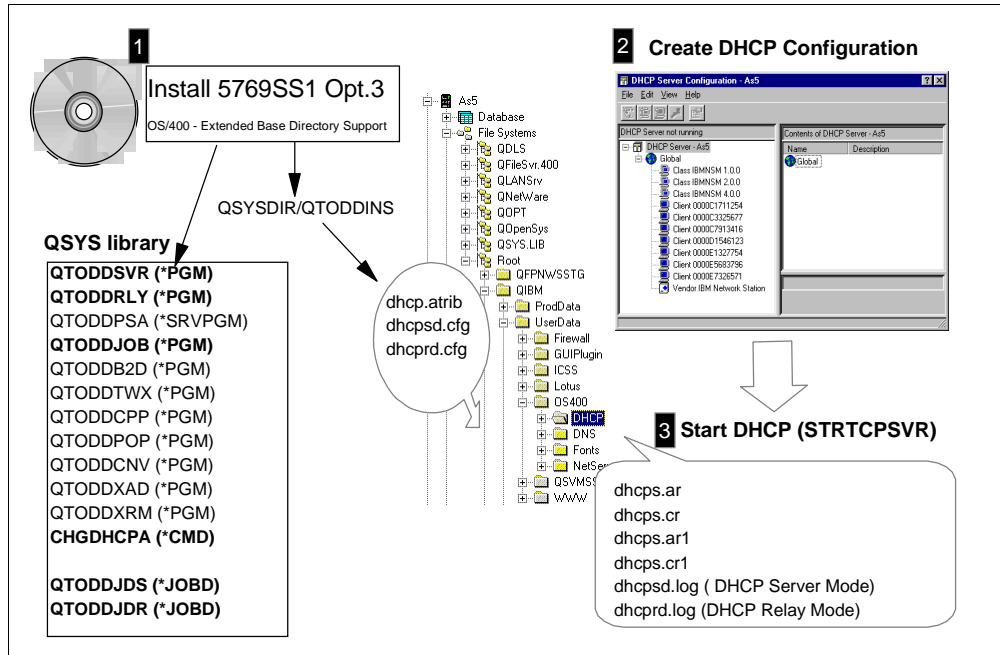


Figure 202. AS/400 DHCP Server Support Installation and Configuration Overview

10.3 DHCP Server Jobs

The DHCP server jobs run in the QSYSWRK subsystem. They are as follows:

- **QTODDHCPs**. This is the DHCP server program that runs when the DHCP Mode attribute is *SERVER. The AS/400 system that runs this program functions as a regular, DHCP transaction-processing server. The DHCP server uses well-known ports 67 and 68. DHCP server messages are directed to the job log. Use the *Work with Spooled File* (WRKSPLF) command for *User* QTCP to browse the DHCP server job log. This job starts with job description QTODDJDS.
- **QTODDHCPR**. This is the DHCP server job that runs when the DHCP Mode attribute is *RELAY. The AS/400 system running this job runs as a BOOTP/DHCP Relay Agent. The BOOTP/DHCP Relay Agent runs on well-know port 67. This job starts with the job description QTODDJDR.

10.4 DHCP Configuration Files

The files that DHCP requires are in the IFS directory /QIBM/UserData/OS400/DHCP. These files are as follows:

- **dhcpsd.cfg**. This is the configuration file that DHCP reads when it runs as a regular DHCP server (transaction processing server).
- **dhcprd.cfg**. This is the configuration file that DHCP reads when it runs as a BOOTP/DHCP Relay Agent server.
- **dhcps.ar**. DHCP server non-volatile address records.

This file contains up-to-the minute, actual address allocation from the address pools that the DHCP server administers when running in regular DHCP server mode.

- **dhcps.cr.** DHCP server non-volatile client records:

This file contains up-to-the minute data on the actual clients that this DHCP server is servicing when running in regular DHCP server mode.

- **dhcps.ar1.** DHCP server backup of non-volatile address records:

The DHCP server takes an hourly backup of **dhcps.ar**, the non-volatile address record file.

- **dhcps.cr1.** DHCP backup of server non-volatile client records:

The DHCP server takes an hourly backup of **dhcps.cr**, the non-volatile client records file.

- **dhcp.attrib.** DHCP attributes file:

Stores the current value of the CHGDHCPA command parameters, with the exception of the AUTOSTART parameter.

10.4.1 Log Files

The following files in the IFS directory `/QIBM/UserData/OS400/DHCP` are used to log DHCP server activity. They are also used for problem determination:

- **dhcpsd.log.** DHCP uses this file as the default logging/tracing file it runs as a regular DHCP server. You can enable logging through a configuration option in Operations Navigator, and you can configure this file to roll into multiple files based on the maximum size. To enable DHCP logging, select the **Logging** tab in the DHCP Server Properties. Specify the type of logging that you want to perform, depending on the types of things that you want to log. Typically, you perform either minimal logging or no logging at all. Figure 203 shows how to enable logging on the AS/400 DHCP server.

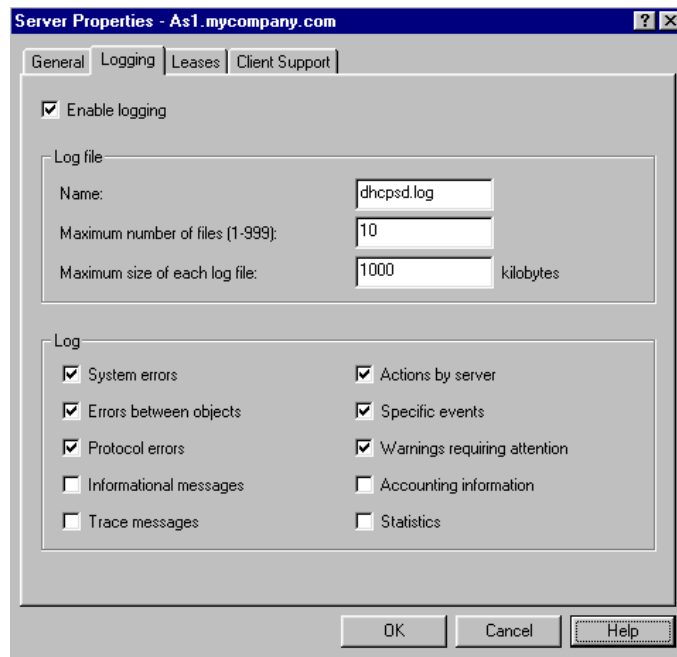


Figure 203. Configuring DHCP Server Logging -- DHCP.DLOG

- **dhcprd.log.** DHCP uses this file as the default logging/tracing file when it runs as a BOOTP/DHCP Relay Agent. You can enable logging through a configuration option in Operations Navigator, and you can configure this file to roll into multiple files based on the maximum size.

Figure 204 provides an overview of the DHCP server jobs, files, and logs.

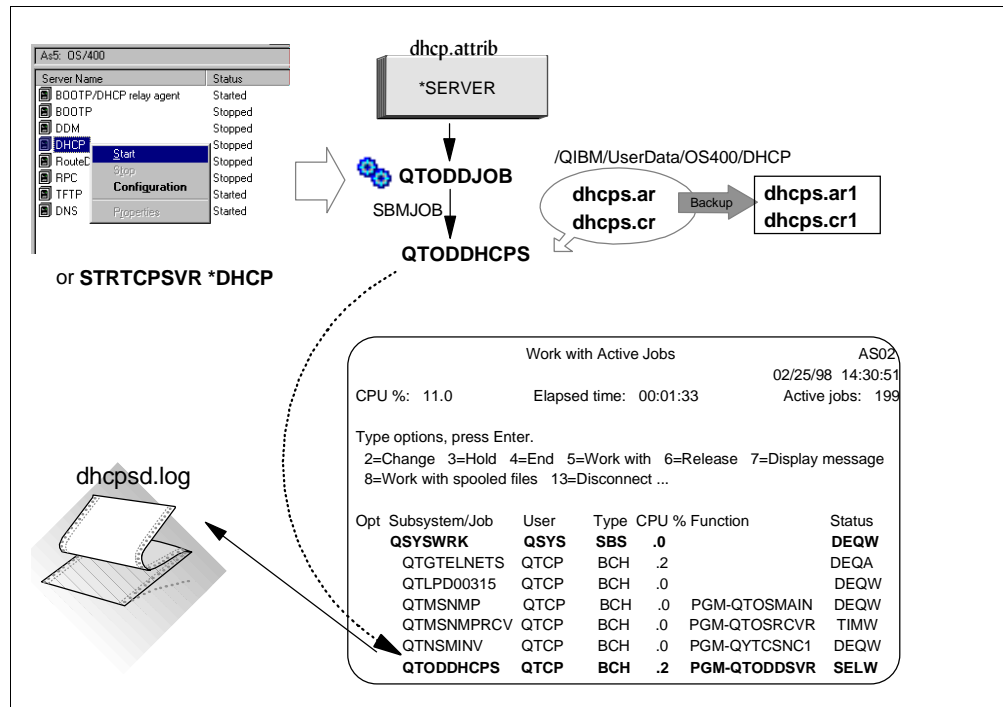


Figure 204. DHCP Server Jobs, Files, and Logs

Figure 205 provides an overview of the BOOTP/DHCP Relay Agent jobs, files, and logs.

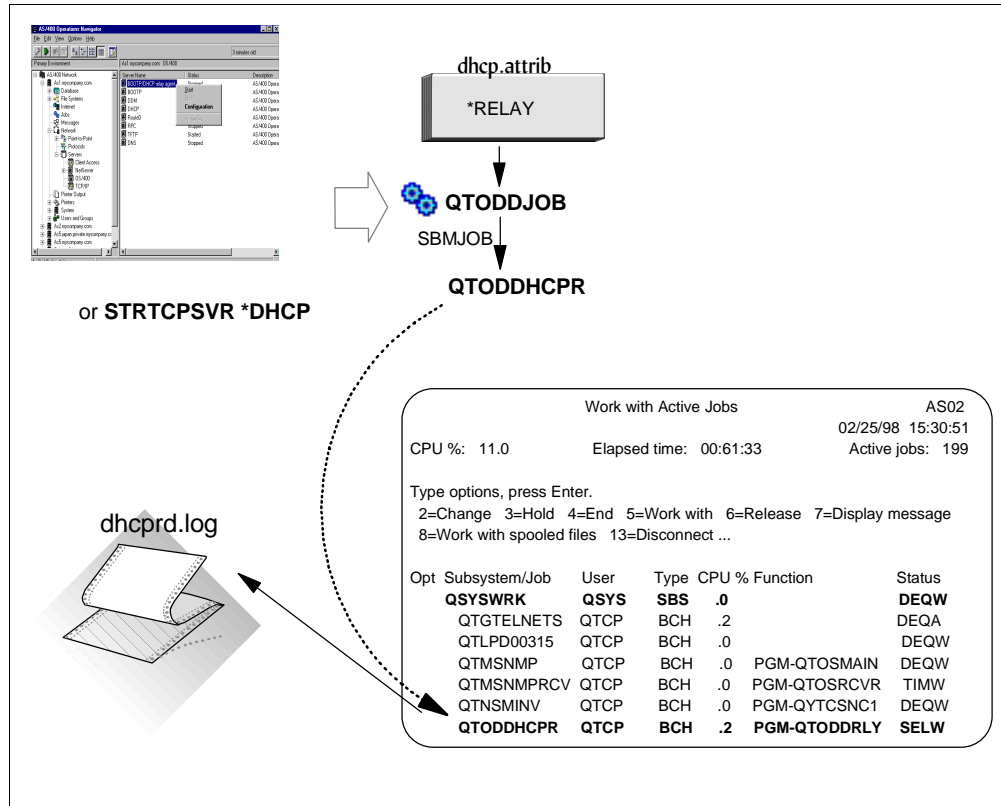


Figure 205. BOOTP/DHCP Relay Agent Jobs, Files, and Logs

10.5 DHCP Server User Interface

This section describes the user interface that is available in the AS/400 DHCP server.

10.5.1 DHCP Server Configuration through Operations Navigator

Install and configure the AS/400 DHCP server is through Operations Navigator. Operations Navigator provides the one and only configuration interface for the DHCP server. The Operations Navigator DHCP Configuration Wizard provides a simple process for quickly configuring and starting initial DHCP server.

To start the DHCP server configuration from Operations Navigator, select **AS400system name->Network->Server->OS400**. The window shown in Figure 206 is displayed.

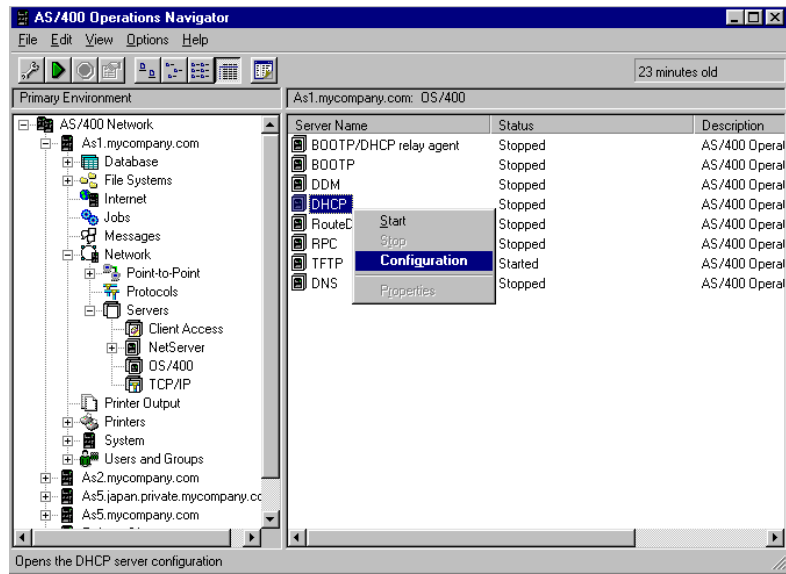


Figure 206. DHCP Configuration Using Operations Navigator

To use Operations Navigator, you need to install Client Access/400 for Windows 95/NT V3R1M3 in your administrator's PC. Host servers must be started on your AS/400 system. Use the *Start Host Server* (STRHOSTSVR) command to start it.

10.5.2 Change DHCP Attributes Command (CHGDHCPA)

Use the *Change DHCP Attributes* (CHGDHCPA) command to set the AUTOSTART attribute, which determines whether or not the DHCP server starts automatically when TCP/IP is started using the STRTCP command. This attribute is ignored by the STRTCPSVR command. STRTCPSVR *DHCP starts the DHCP server regardless of the value of the AUTOSTART attribute. You set this attribute from the Operations Navigator interface as well.

Use the CHGDHCPA command to set the MODE attribute that determines the DHCP server behavior.

Set the MODE attribute to *SERVER if you want the DHCP server to automatically assign reusable IP addresses to DHCP clients in response to DHCP requests. Set the MODE attribute to *RELAY if you want the DHCP server to function only as a BOOTP/DHCP Relay Agent. A BOOTP/DHCP Relay Agent forwards BOOTP or DHCP packets from hosts to active BOOTP or DHCP servers and from the servers back to the hosts. It performs no BOOTP or DHCP server functions.

The attributes file `/QIBM/UserData/OS400/DHCP/dhcp.attrib` is updated with the values that you specify in the CHGDHCPA command.

10.5.3 Start TCP Server *DHCP

Use the STRTCPSVR SERVER(*DHCP) command to boot the DHCP server and the ENDTCPSPVR SERVER(*DHCP) command to stop it. You can perform this function through Operations Navigator as well.

10.6 BOOTP-to-DHCP Migration Program

This migration program, QSYS/QTODDB2D, is called by Operations Navigator. If the program detects that there is a BOOTP table in the system, it gives you options through the Operations Navigator to migrate the BOOTP table to a DHCP server configuration. Figure 207 shows the BOOTP migration window that the DHCP configuration wizard presents.

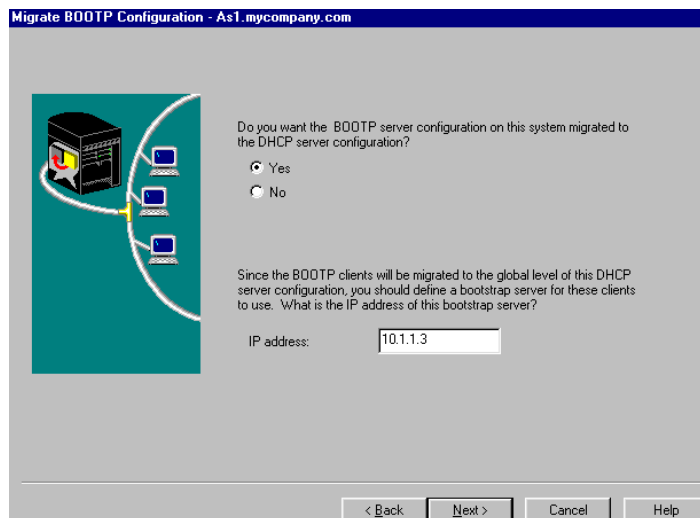


Figure 207. Migrate BOOTP

10.7 DHCP Server Exit Programs

The AS/400 DHCP server assigns and releases TCP/IP addresses from client hosts in a network. Exit points have been provided so that user-written programs are called from the running DHCP server. They allow for customer-supplied security validation of incoming client requests as well as for notification when an IP address is assigned or release.

The exit programs and their functions are as follows:

- **DHCP address Binding Notification** exit program. This program allows for notification each time the DHCP server assigns an IP address to a specific host.
- **DHCP Address Release Notification** exit program. This program allows for notification each time the DHCP server releases an IP address from its specific client host assignment binding.
- **DHCP Request Packet Validation** exit program. This program provides additional control for restricting which incoming DHCP and BOOTP message request packets from client hosts are processed and which are rejected by their DHCP server.

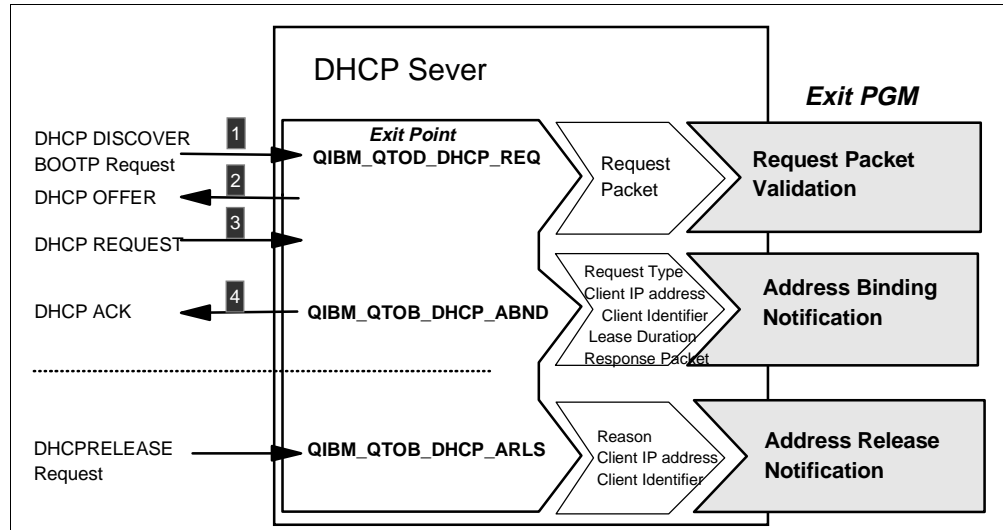


Figure 208. DHCP Server Exit Programs

Refer to *System API Programming*, SC41-5800 for information on how to use the DHCP exit programs.

10.8 DHCP Server Backup and Recovery Considerations

You need to back up the following files on a regular basis and as part of your normal backup procedures:

- Back up the following files if you are running a DHCP Server:
 - /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
 - /QIBM/UserData/OS400/DHCP/dhcps.ar
 - /QIBM/UserData/OS400/DHCP/dhcps.cr
 - /QIBM/UserData/OS400/DHCP/dhcps.ar1
 - /QIBM/UserData/OS400/DHCP/dhcps.cr1
- Back up the following files if you are running a BOOTP/DHCP Relay Agent:
 - /QIBM/UserData/OS400/DHCP/dhcprd.cfg
- Back up /QIBM/UserData/OS400/DHCP/dhcp.attrib to back up the general DHCP attributes.

Note: Shut down the servers before you take these backups. This avoids taking the backup while one or more files are in the middle of an update.

Optionally, you can save everything in the IFS directory /QIBM/UserData/OS400/DHCP/*.*. In this case, your backup includes other files that exist in this directory, such as log files. The other files are not required for recovery, but this might be an easier approach to avoid remembering to back up individual files.

Perform the previous backups using the `SAV` command. When the files are restored, they automatically retain their ownership, CCSID, and authorizations that are required. If you use the `CPY` command, the resulting copies might end up with ownership and authorizations based upon the User IDs that issue the copy command, as opposed to the original ones.

To recover DHCP files saved using the **SAV** command, use following guidelines:

- Use the `RST` command to restore.
- If you restore **all** of the previous files in the three categories (server, relay, and attributes) and the problem requiring the restore did not actually affect all three, you can wipe out changes made to others since the backup was taken. Carefully consider what it is that you truly need to restore.
- If you want to restore only the DHCP server, we recommend that you restore all of the files that are listed in that group.

There might be instances where you want to restore only the DHCP server configuration file but not the non-volatile state files, or vice versa. If you are restoring the non-volatile state files, you must restore them in a synchronous group, such as (/QIBM/UserData/OS400/DHCP/dhcps.ar and /QIBM/UserData/OS400/DHCP/dhcps.cr)

- or -

(/QIBM/UserData/OS400/DHCP/dhcps.ar1 and /QIBM/UserData/OS400/DHCP/dhcps.cr1).

Note: You must shut down the servers prior to restoring any file.

The following backups take place automatically during the normal operation of the DIP server:

- After every transaction processed, the server stores its current state in the following non-volatile files:
/QIBM/UserData/OS400/DHCP/dhcps.ar and
/QIBM/UserData/OS400/DHCP/dhcps.cr

Hourly backups of the previous, non-volatile state files are taken in:
/QIBM/UserData/OS400/DHCP/dhcps.ar1 and
/QIBM/UserData/OS400/DHCP/dhcps.cr1.

The following run-time recoveries take place automatically:

- If the DHCP server is shut down intentionally or terminates abnormally, you need to start the server again. You must also have it re-initialize itself to the state it was in just after it processed its last successful transaction. It does this by reading the /QIBM/UserData/OS400/DHCP/dhcps.ar and the /QIBM/UserData/OS400/DHCP/dhcps.cr files.
- If the previous re-initialization fails due to the corruption of one or both of the primary non-volatile files, the DHCP server automatically deletes them. It then renames the hourly backup versions to the primary version file names and tries again. It sends messages to the log to signal this event.
- If both of your re-initialization attempts fail, you need to recover using your own backups.

Chapter 11. Start Here: Implementing DHCP in a Simple Network

This chapter shows how to implement a DHCP server on your AS/400 system. It takes you through the detailed steps of setting up your AS/400 system so you can connect to your LAN and configure a DHCP server. It also describes how to configure both a Windows 95 client and the IBM Network Station as DHCP clients.

11.1 Scenario Overview

This scenario sets up the AS/400 system to act as a DHCP server in a simple TCP/IP network. It also installs two different DHCP clients that request TCP/IP addresses from the AS/400 DHCP server. Further, it demonstrates the DHCP protocol flow between the server and the client.

This scenario assumes that there is no existing logical network. Therefore, it uses a simple TCP/IP addressing scheme. It also assumes that the local area network is physically complete (all systems and clients are cabled to the network and can attach).

11.1.1 Scenario Objectives

This scenario has the following three objectives:

1. To demonstrate the ease with which you can configure a simple TCP/IP network for DHCP using OS/400 support.
2. To demonstrate how to set up a Windows 95 client and an IBM Network Station to act as a DHCP client and have their TCP/IP addresses served to them from the AS/400 DHCP server.
3. To show the protocol flow between the server and the client. This flow is helpful to understanding how DHCP works and can be useful in problem determination.

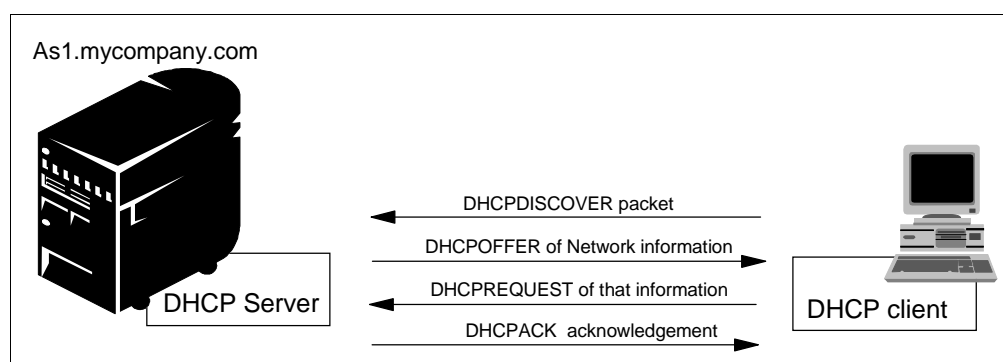


Figure 209. DHCP Client and DHCP Server Protocol Flow

11.1.2 Scenario Advantages

This scenario has the advantage of being simple and showing the ease with which you can set up your AS/400 system to act as a DHCP server. The same simplicity also applies to the client setup.

11.1.3 Scenario Disadvantages

It is assumed in this scenario that this is a new network. Therefore, you are free to choose any possible TCP/IP addressing scheme. This scenario does not show the complexities that arise with an existing network and hardcoded TCP/IP addresses. It also does not discuss the possible migration from BOOTP or deal with complex subnetting issues.

You can consider the DHCP server in this example a single point of failure because it has no backup. Clients that have already queried the DHCP server for a network address remain connected if the DHCP server fails. New clients attempting to connect are unable to gain a TCP/IP address.

11.1.4 Scenario Network Configuration

The following figure depicts the logical topology for this scenario:

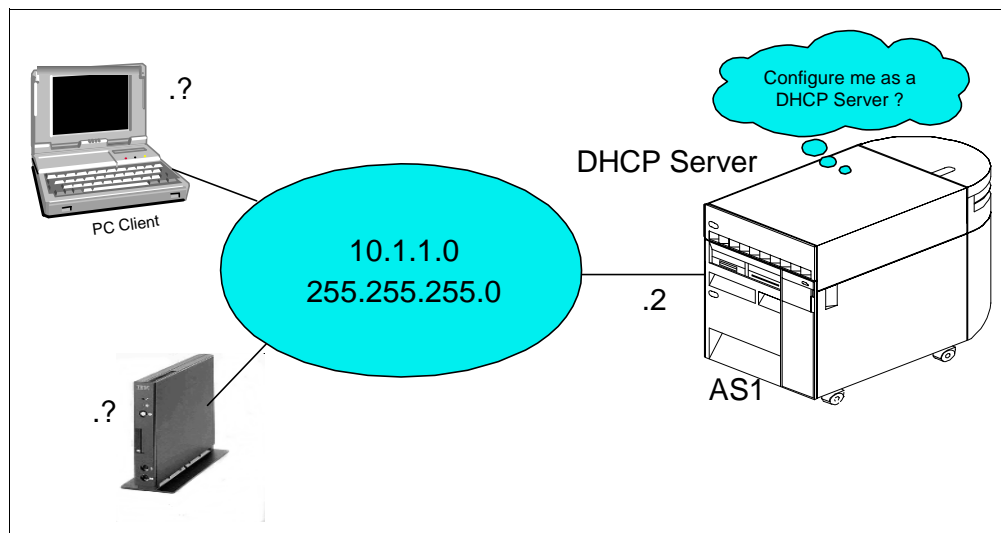


Figure 210. Simple Example Network

The following scenario characteristics influence the DHCP configuration:

- There is a single AS/400 DHCP server with a class A addressing scheme with a single subnet.
- A subnet mask allows the AS/400 DHCP server to service 253 clients. The AS/400 host address remains constant and is removed from the addressing pool.
- Routers and bridges do not exist within this network.

11.1.5 Network Addressing Scope Planning

The network 10.1.1.0 is used in this example. It is highly recommended to do a hierarchical partitioning of a network to ease administration. You can accomplish this as follows:

10.x.y.z where x = site or region, y = department, z = hosts, x + y = subnet.

The small example network (10.1.1.0 and a mask of **255.255.255.0**) allows up to 254 hosts. If you need to expand the network to connect with more hosts, change

the mask to **255.255.254.0**. This reduces the subnet addressing scope (x + y) by one bit, but it generates one bit more for the host addressing scope (z). This means the creation of up to 510 hosts. This technique shows an easy way to increase the number of host addresses that are available to either the subnet or the network. It also lets the network grow without major changes.

11.2 Task Summary

To configure the DHCP server and clients in this scenario, perform the following steps:

1. Verify hardware, software, and configuration prerequisites.
2. Configure the AS/400 network interface.
3. Configure and start a TCP/IP interface.
4. Gather information to configure the DHCP server.
5. Configure the DHCP server.
6. Start the DHCP server.
7. Configure the Windows 95 DHCP client.
8. Configure the IBM Network Station client.

11.3 Verify Hardware, Software, and Configuration Prerequisites

Before you configure your AS/400 system to act as a DHCP server, you must ensure the following:

1. Hardware prerequisites:
 1. Ensure your AS/400 system has a LAN adapter installed and cabled to the network.
 2. Ensure that all the clients in your network have the correct network interface card. Make certain that you have installed all the drivers you need.
2. Software prerequisites:
 1. The DHCP support is part of 5769-SS1, base option 3, *OS/400 -- Extended Base Directory Support*.
 2. Ensure licensed program product 5769-SS1, option 12 (*OS/400 -- Host Servers*), is installed.
 3. For the administrator to configure DHCP on the AS/400 system, you need to ensure that the AS/400 Operations Navigator is installed and configured on the administrator's PC.

Note

With V4R2, the Client Access code for the client requires no license. Effectively, the base Client Access code is free.

4. For PC clients that connect to the network, DHCP support is included in Windows 95.
5. To use and connect an IBM Network Station, you need to ensure that IBM Network Station Manager for AS/400 code is installed. The license

program number is 5648-B07. However, all references to this product on the AS/400 system and online information (including the product installation command) refer to the product as 5733-A07.

3. Configuration prerequisites:

You must add a line description for your AS/400 LAN interface. Usually, a line description already exists. If so, you can skip this step.

11.4 Configuration Overview

1. Configure TCP/IP and add at least one IP Interface.
2. Configure the DHCP server support through Operations Navigator.
3. Change some DHCP attributes.
4. Configure the clients to use DHCP.

11.4.1 Configure TCP/IP Interface on the AS/400 System

To configure the TCP/IP interface, perform the following steps:

1. On an AS/400 command line, type the command:

```
GO CFGTCP
```

Press Enter to display the Configure TCP (CFGTCP) menu.

2. Select option 1 (Work with TCP/IP interfaces) to display the Work with TCP/IP Interfaces display (see Figure 211).

Work with TCP/IP Interfaces

System: AS1

Type options, press Enter.

1=Add 2=Change 4=Remove 5=Display 9=Start 10=End

	Internet	Subnet	Line	Line
Opt	Address	Mask	Description	Type
—	_____			

Figure 211. Work with TCP/IP Interfaces Display

3. Select option 1 to add a TCP/IP interface and specify the TCP/IP address of the host. Press Enter to continue.
4. Add the line description name and the subnet mask for the interface.

Add TCP/IP Interface (ADDTCPIFC)

Type choices, press Enter.

Internet address	> '10.1.1.2'	
Line description	TRNLINE1	Name, *LOOPBACK
Subnet mask	255.255.255.0	
Associated local interface . . .	*NONE	
Type of service	*NORMAL	*MINDELAY, *MAXTHRPUT...
Maximum transmission unit . . .	*LIND	576-16388, *LIND
Autostart	*YES	*YES, *NO
PVC logical channel identifier	_____	001-FFF
+ for more values		
X.25 idle circuit timeout . . .	60	1-600
X.25 maximum virtual circuits .	64	0-64
X.25 DDN interface	*NO	*YES, *NO
TRLAN bit sequencing	*MSB	*MSB, *LSB

Bottom

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
 F24=More keys

5. Press Enter to create the TCP/IP interface.
6. Press **F11** to view the status of the interface and verify that the status is active.

Note

If the TCP/IP interface is inactive, you must start the interface by using option **9** on the Work with TCP/IP Interfaces display (see Figure 211 on page 240). You must then press **F5** to refresh the display and verify that the interface has started.

11.4.2 Gather Information to Configure the DHCP Server

To use the Operations Navigator DHCP configuration effectively, you need to know how you want to set up and manage your networks and subnets with DHCP. You also need to know what address range or ranges you want to use for leasing. Further, you must decide which system is the DHCP server, which ones are the BOOTP/DHCP Relay Agents, and which one performs DHCP backup functions. You must also know the IP addresses that must be reserved for special hosts such as routers, DNS servers, and firewalls. It is useful to refer to a network diagram that shows the subnet masks and IP addresses for your networks, routers, and clients while you are configuring DHCP.

The starting point of this scenario is the network diagram shown in Figure 210 on page 238. The information shown in the following tables is based on the network picture and other network data.

Table 10 shows general information about AS1 as a TCP/IP host. Table 11 provides more specific information about AS1 as a DHCP server.

Table 10. Planning the DHCP Server -- AS1 TCP/IP Information

Host Name	As1
Description	DHCP server
Domain Name	mycompany.com
IP Address	10 . 1 . 1 . 2
Mask	255.255.254.0
Line Description	TRNLINE1

Note: The *Configuration Reference* column in the following tables points to the place in Operations Navigator DHCP server configuration where you can configure the particular parameter. You can specify many of these configuration options through the DHCP configuration wizard the first time you configure DHCP.

Table 11. Planning the DHCP Server AS1 -- DHCP Server Overview

#	Question	Answer	Configuration Reference
1	Is the BOOTP Server already configured on your system?	No	DHCP configuration wizard
2	Do you want to migrate the BOOTP configuration to DHCP?	N/A	File -->Migrate BOOTP
3	What is the default lease time for this server?	24 hours	Global-->Properties-->Leases
4	Start the DHCP server when TCP/IP starts?	Yes	Server Properties --> General
5	List the DHCP server IP interfaces that will be serving DHCP clients.	10.1.1.2	See network diagram.
6	List the subnets that will be administered by this DHCP server.	10.1.1.0	See subnet planning table
7	Do you want to add a new subnet to be administered by this server?	Yes	Global --> New Subnet - Basic Global-->New Subnet - Advanced See subnet planning table
8	Do you want to log DHCP server activity?	Yes	Server Properties --> Logging
9	Do you want the DHCP server to support any client from any subnet?	Yes	Server Properties --> Client Support
10	Do you want the DHCP server to support BOOTP clients?	No	Server Properties --> Client Support
11	Do you want the DHCP server to reject requests from specific clients (for example, for security reasons)?	No	Global->Properties-> Exclude Client
11	Can your DHCP clients (other than IBM Network Stations) identify the class they belong to?	No	

#	Question	Answer	Configuration Reference
12	If answer to 11 is Yes, do you want to add a new class to serve the DHCP clients that belong to that class?	N/A	Global --> New Class

Table 12 provides information about subnet 10.1.0.0 being administered by the DHCP server AS1. Notice that AS1 administers 50% of the IP addresses available while the rest is assigned to AS2, the backup DHCP server.

Table 12. Planning the Subnet 10.1.1.0 Administered by AS1

#	Question	Answer	Configuration Reference
1	Subnet name	10.1.1.0	Subnet Properties --> General
2	Subnet description	Our_Company	Subnet Properties --> General
3	Subnet address	10.1.1.0	Subnet Properties --> Address Pool
4	Subnet mask	255.255.255.0	Subnet Properties --> Address Pool
5	Address range	10.1.1.1 10.1.1.254	Subnet Properties --> Address Pool
6	Lease time	Inherit from server (12 hours)	Subnet Properties --> Leases
7	Exclusions (exclude hosts that required a particular IP address and are manually configured).		Subnet Properties --> Address Pool
	Name: Router x Description: Reserved for future router IP address: 10.1.1.1	AS1 DNS/DHCP server 10.1.1.2	
8	Domain Name Server IP address to deliver to clients in this subnet.	10.1.1.2	Subnet Properties --> Options--> Option 6 (Domain name server)
9	Gateway IP address to deliver to clients in this subnet.	N/A	Subnet Properties --> Options--> Option 3 (Router)
10	Offer options to client in this subnet 01 - Subnet mask 06 - Domain name server	255.255.254.0 10.1.1.2	Subnet Properties --> Options-->

11.4.3 Configure DHCP Server through Operations Navigator

If you are configuring DHCP on a system that does not have an existing configuration, Operations Navigator automatically starts the DHCP configuration wizard. This wizard helps you create a basic DHCP server configuration.

Tip

To reset an existing configuration and start over, perform the following steps:

1. Delete the IFS file `dhcpcsd.cfg` file in `/QIBM/UserData/OS400/DHCP`.
2. CALL `QSYSDIR/QTODDINS` from an AS/400 command entry display. This program creates a blank configuration file that the Operations Navigator's GUI can edit.

To start the DHCP configuration wizard, perform the following steps:

1. Start Operations Navigator.
2. Click *as1.mycompany.com* to select the system name.

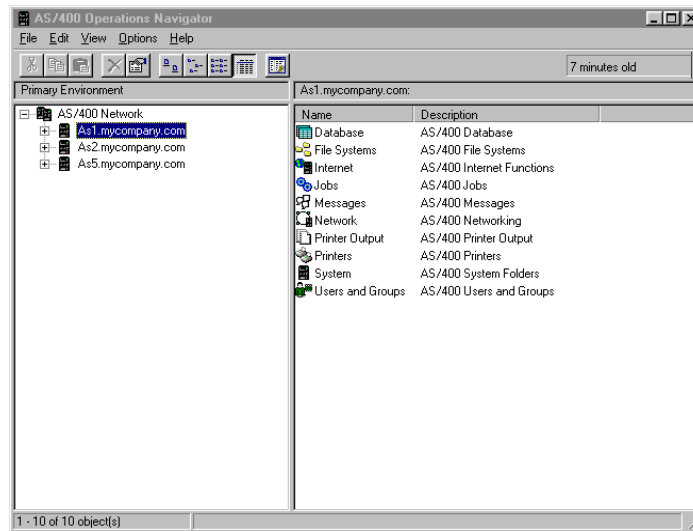


Figure 212. AS/400 Operations Navigator -- Selecting the System to Configure the DHCP Server

3. Double-click **Network**.
4. Double-click **Server**.
5. Double-click **OS/400**.
6. Double-click **DHCP**. This starts the DHCP configuration wizard.

Note

If you are not presented with the DHCP configuration wizard, it is likely that a DHCP configuration already exists. To start the wizard and replace the existing configuration, select **File > New Configuration**.

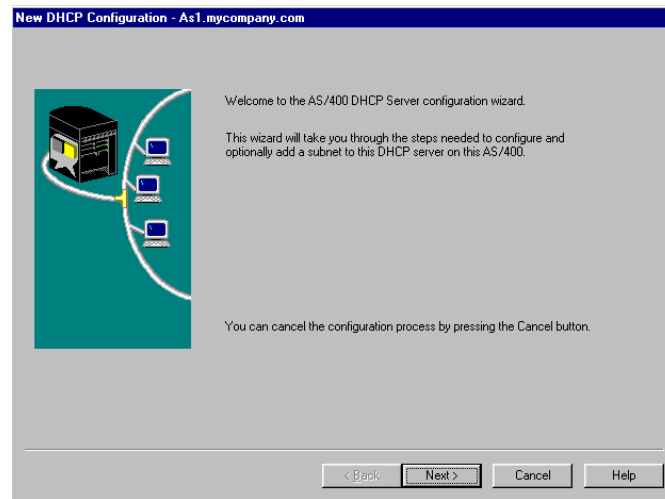


Figure 213. The DHCP Configuration Wizard

7. Click **Next**.
8. Select **Yes** to add a new subnet to the DHCP server.
9. Leave the *Twinax IP workstation controller address* box blank and click **Next**.
10. Define the range of addresses to use within the subnet.

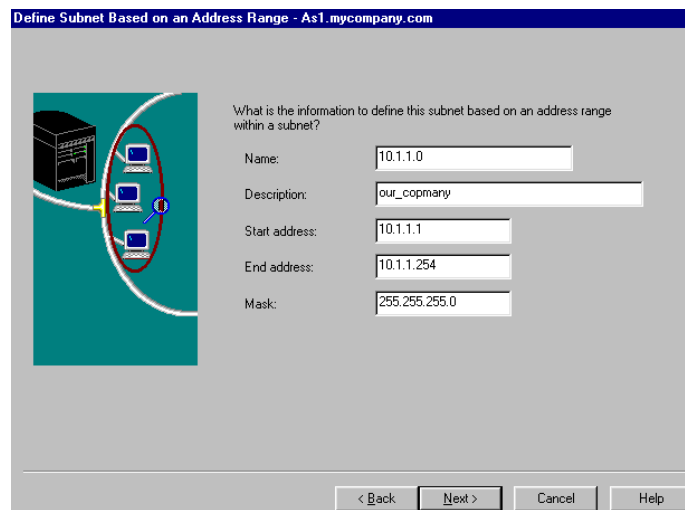


Figure 214. Subnet Configuration

11. Define a lease time for the client to keep the address served. Click **Next** to use the default lease time of one day.
12. Specify the IP addresses of the hosts to be excluded. The DHCP server does not deliver these addresses to clients (see Figure 215).

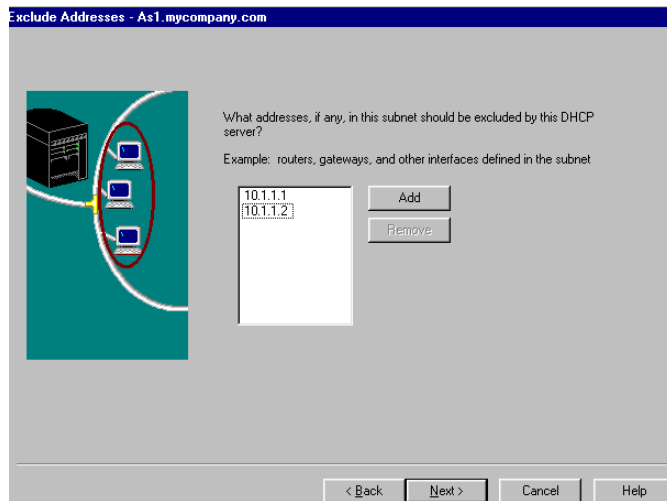


Figure 215. Excluded IP Addresses in the Subnet

13. Click **Next** to *not* deliver the IP address of a gateway to clients. There is only one subnet in this scenario.
14. Answer **Yes** to the question "Would you like the DHCP server to deliver domain name server address to clients in this subnet?" Specify the DNS IP address (see Figure 216). Click **Next**.

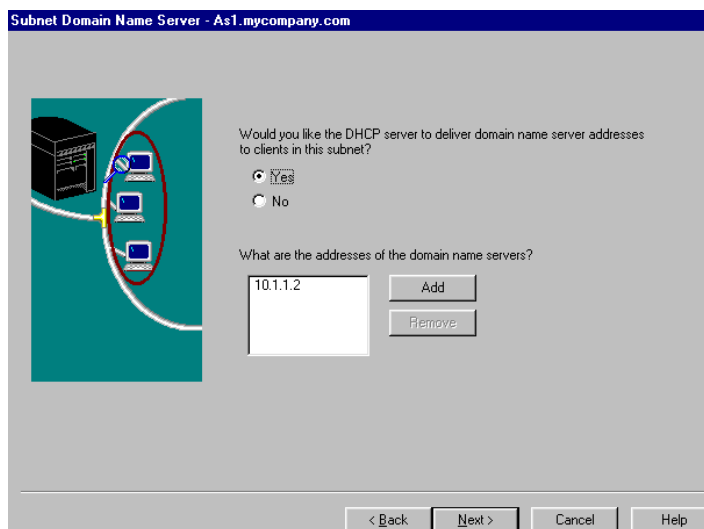


Figure 216. Configuring the DNS IP Address to Deliver to Clients in this Subnet

15. Answer **No** to the question "Would you like the DHCP server to deliver domain names to clients in this subnet?" Click **Next**.
16. Select *Support any clients on this subnet*. Click **Next**.
17. Select **Yes** to start the DHCP server when TCP/IP starts and Select **No** to start the DHCP server now. Click **Next**.
18. The DHCP configuration summary window shows all the options that you have selected to this point. Click **Finish**.

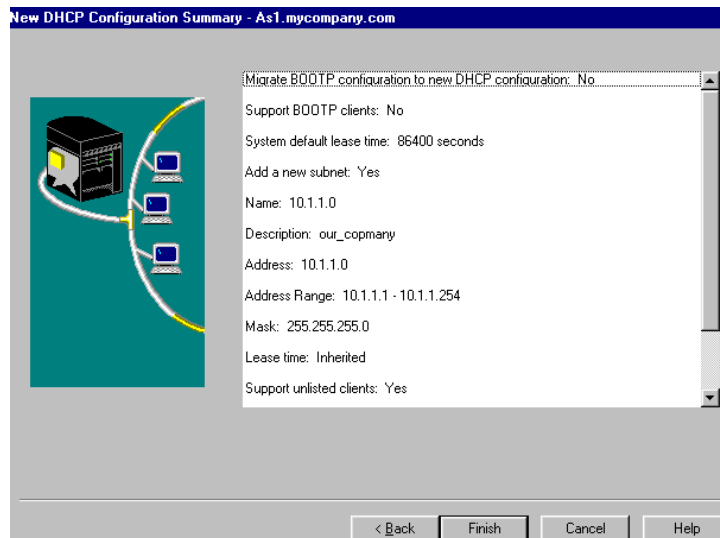


Figure 217. The DHCP Configuration Summary

19. Now the DHCP server configuration is displayed.

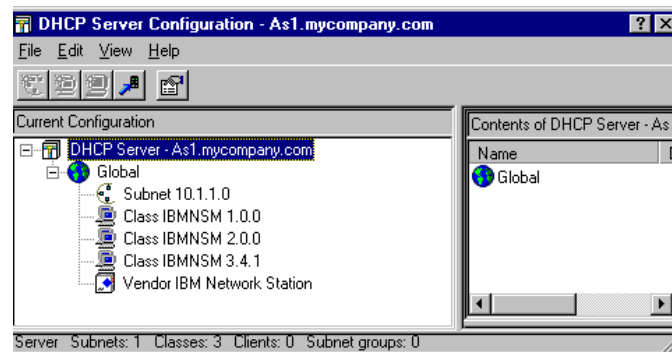


Figure 218. DHCP Server Configuration

The configuration of a simple network to use DHCP is complete. You have created one subnet from a class A IP address using the mask 255.255.255.0. This allows up to 254 IP addresses within the subnet pool to be served to clients.

1. From the DHCP Server configuration display shown in Figure 218 on page 247, click **Subnet 10.1.1.0** to open a context menu and select **Properties**.
2. Click the **Options** tab to add a subnet mask that is served to the clients.
3. Highlight option **1, subnet mask**, from the **Available options** window and then click **Add**.
4. At the bottom of the display, specify the appropriate subnet mask for the clients to use in the Subnet mask window.

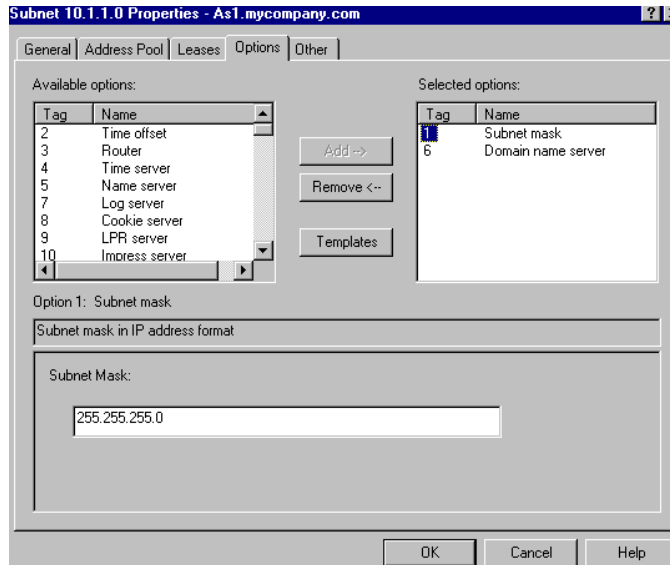


Figure 219. DHCP Server Options

Notice in Figure 219 that the domain name server option **3** is already configured. Specify the IP address of the domain name server when prompted by the configuration wizard.

5. Click **OK**.

Now we are going to assign a longer lease time for any token-ring attached IBM Network Station. A longer lease time can be useful for clients that are not mobile. A longer lease reduces the number of lease renewals the client must request, which in turn reduces some of the network traffic. One way to specify a longer lease time for the token-ring IBM Network Station is to specify a lease time for the class they request.

1. From the DHCP Server configuration display shown in Figure 218 on page 247, right-click **Class IBMNSM 1.0.0**. to open a context menu. This class is for token-ring-attached IBM Network Stations. The two other available classes are Class **IBMNSM 2.0.0** for Ethernet-attached IBM Network Stations and **IBMNSM 3.4.1** for Twinax-attached IBM Network Stations.
2. Select **Properties**.
3. Click the **Leases** tab.
4. Click **Duration**. From the pull-down menu, choose *weeks* and specify **1** to set the lease duration to one week.
5. Click **OK**.

The DHCP server services requests from BOOTP clients. However, this is not the default and must be enabled.

To enable the DHCP server to service BOOTP requests, perform these steps:

1. On the DHCP Server configuration display shown in Figure 218 on page 247, right-click **DHCP Server -- As1.mycompany.com** to open a context menu and select **Properties**.

2. Click the **Client support** tab and click both *BOOTP clients* and *Unlisted clients*.
3. Click **OK**.

11.5 Configuring DHCP Clients

To use the DHCP server, clients must support DHCP and be appropriately configured. There are many DHCP clients available on the market, but the tests performed for this book used only IBM Network Station and Windows 95. This section describes how to set up the IBM Network Station and the Windows 95 DHCP clients. Refer to your DHCP client documentation for information about your client's DHCP support.

11.5.1 Configuring DHCP on Windows 95 Clients

To enable DHCP on your Windows 95 workstation, perform the following steps:

1. Double-click **My Computer** on your desktop.
2. Double-click **Control Panel**.
3. Double-click **Network**.
4. Right-click **TCP/IP** to open a context menu and select **Properties**.
5. Click *Obtain an IP address automatically*.

Note

If a TCP/IP address already exists in the TCP/IP properties window, it is removed once you click **OK**. It can be advantageous to record the existing TCP/IP address and subnet mask before you change the setting.

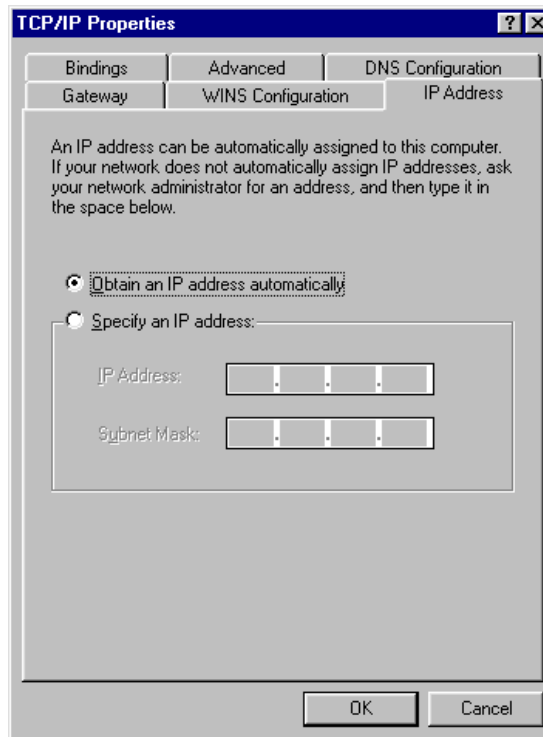


Figure 220. Enabling DHCP on a Windows 95 Client

6. Click **OK**.
7. Click **OK** again and follow the Windows prompts to restart your computer.

At this point, your Windows 95 client broadcasts a DHCPDISCOVER message. To verify the current Windows 95 IP configuration, use the Windows program

WINIPCFG.EXE. It displays a dialog similar to the one shown in Figure 221.

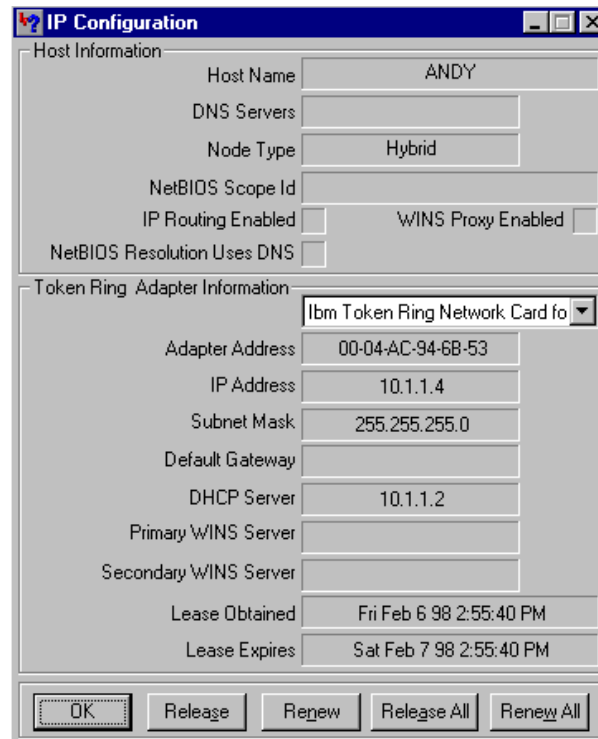


Figure 221. Windows 95 IP Configuration Information -- WINIPCFG

11.5.2 Configuring DHCP on the IBM Network Station

If the IBM Network Station is new and just out of the box, the default settings within the non-volatile RAM (NVRAM) are set to use DHCP. Once you have completed the previous steps and configured the DHCP server so that it is running on the local subnet, plug the IBM Network Station into your network (attaching a display, keyboard, and mouse) and turn it on. The IBM Network Station attempts to locate a DHCP server first. If a DHCP does not respond, it attempts to find a BOOTP server.

Tip

Default settings for the IBM Network Station are to boot DHCP first and BOOTP second (factory settings are DHCP '1', BOOTP '2'). We recommend that the BOOTP boot be disabled (set to 'D'). In a DHCP environment, there is no good reason to boot using BOOTP if the client supports DHCP. If the IBM Network Station times out before the DHCP server can respond, then the IBM Network Station switches to BOOTP mode. This is undesirable because BOOTP leases are permanent.

If the IBM Network Station has been used previously and you are unsure what has been entered into the NVRAM, perform the following steps to reset the NVRAM to the factory defaults:

1. Power on the IBM Network Station. The IBM logo is followed by a memory and keyboard check.

2. After seeing the message `NS0500 Search for Host System`, press the **ESC** key to stop the startup sequence.

If prompted for an administrator password, enter it now. This is the password an administrator sets using the IBM Network Station Manager program.

3. Invoke the IBM Network Station Boot Monitor program by pressing the following key sequence:

- For 101/102 keyboards:

Press and hold **Left Shift + Left Alt + Left Ctrl**. Press **F1**.

- For 5250/3270 keyboards:

Press and hold **Left Shift + Left Alt**. Press **F1**.

4. Enter **NV** at the Boot Monitor prompt (**>**) to access the NVRAM utility.
5. Enter **L** to reset the NVRAM.
6. Enter **S** to save the defaults into NVRAM.
7. Specify **Y** to the question *Are you sure?* and press Enter.
8. Power the IBM Network Station off and then on again. It starts with the factory settings previously described.

To verify the IP configuration of the IBM Network Station, let it boot at least once so that the configuration values are stored in NVRAM. After one successful boot, you can verify the configuration values by performing the following steps:

1. Stop the boot process at the message `NS00500 Search for Host System` by pressing the **ESC** key. You now see the *Set up Utility* display.
2. Press **F5**, *Set the Network Parameters*. You now see the *IBM Network Station, Set Network Parameters* display.
3. In the *IP Addressed from* field, use the right-arrow-key to move the cursor and highlight **NVRAM**. You must display the configuration values that are stored in the NVRAM from the last boot. This displays the current configuration values.
4. Press **F12** to cancel.

11.6 Selecting the Bootstrap Host for the IBM Network Station

It is possible to have the IBM Network Station send a request to a DHCP server for network information and have that information returned. The returned information contains the name or IP address of a different host that is the server from which the IBM Network Station downloads its kernel and user configuration data (see Figure 222).

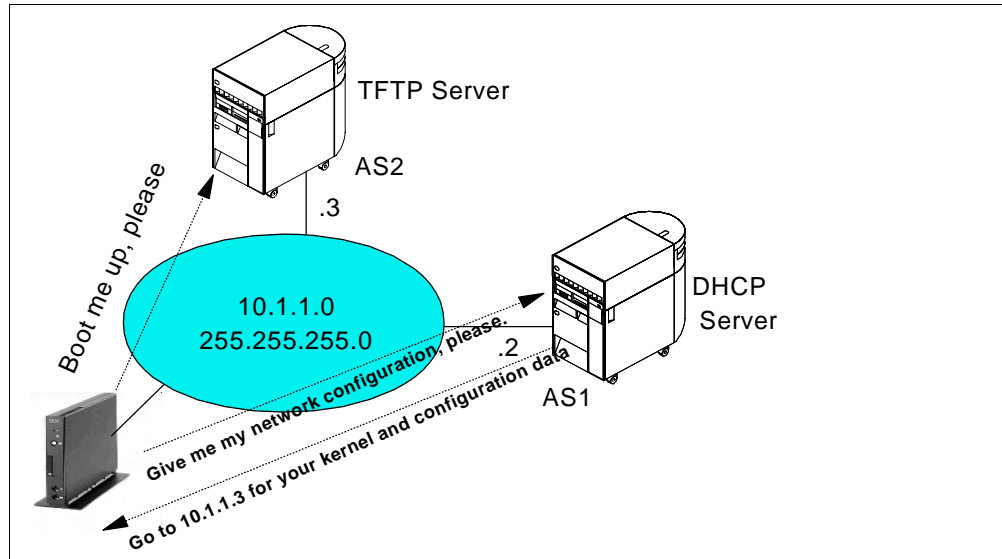


Figure 222. Obtaining Network Configuration from AS1 and Kernel from AS2

You can also configure the AS/400 DHCP server to provide the options that are necessary to instruct the IBM Network Station to load its kernel from a server other than the DHCP host. You can specify up to two systems from which to load the user configuration data.

When you have configured the AS/400 DHCP server, the three following IBM Network Station default classes are built for you in Operations Navigator DHCP configuration:

IBMNSM 1.0.0	This class is for token-ring attached IBM Network Stations.
IBMNSM 2.0.0	This class is for Ethernet attached IBM Network Stations.
IBMNSM 3.4.1	This class is for Twinax-attached IBM Network Station.

Important

The previous list is *not* a comprehensive list of the IBM Network Station classes. At the time of writing, Operations Navigator DHCP configuration included the classes previously described as examples. You must check the IBM Network Station documentation to verify the class name for the model of IBM Network Station you are installing. You must also create the corresponding class. Refer to *IBM Network Station Manager Installation and Use*, SC41-0664-01 or later, for information on IBM Network Station class names and configuration.

Note

Verify that you have the most current service pack available for 5763-XD1 V3R1M3, *after* service pack SF46891, before you configure the IBM Network Station using the default classes in Operations Navigator DHCP configuration.

You can change these classes to serve the IBM Network Station under them.

In this example, the DHCP server provides the network information to the IBM Network Station, which loads its kernel and configuration data from another AS/400 system.

The assumption is made that the DHCP server already functions correctly. It is also assumed that the default classes exist and that the user has not deleted them.

To configure a bootstrap server for the IBM Network Station other than the DHCP server, perform the following steps:

1. Use the AS/400 Operations Navigator to open the DHCP server configuration window.
2. Right-click the class you want to change (such as **IBMNSM 1.0.0** for token-ring attached IBM Network Stations). This opens a context menu.
3. Select **Properties**.
4. Click the **Options** tab.
5. Select the **1** tag at the *Available options* window and click **Add** to specify the class subnet mask (255.255.255.0 in the example).

Important

Defining a subnet mask at the class level is global: all IBM Network Stations, regardless of the subnet location, will get this subnet mask. We are assuming here that there is only one subnet in the network. In general, we recommend defining the subnet mask option at the subnet level.

6. Select the **66** tag at the *Available options* window and click **Add** to specify a trivial FTP (TFTP) server name or IP address. You must specify the IP address of the TFTP server, 10.1.1.3.
7. Option 67 is preconfigured with the boot file path:
`/QIBM/ProdData/NetworkStation/kernel`
You do not need to specify this information. It is already configured for you.

For this configuration to work, you must add user defined options to the DHCP server settings. To do that, use templates by performing the following steps:

8. Click **Templates**.
9. Click **New**. To add user option **211**, *protocol to use for loading the user configuration data*, specify the following data:

New Option Template - As1.mycompany.com

Tag : 211

Name: Config. Protocol

Value label: rfs/400

Description : Protocol to use for the loading of user configuration data. Values are rfs or rfs/400

OK Cancel Help

Figure 223. Option 211 (Configuration Protocol) Template

10. Click **OK**.

11. Repeat the steps for the user options **212**, **213**, and **214** as shown in the following figures:

New Option Template - As1.mycompany.com

Tag : 212

Name: Terminal server

Value label: Enter IP address : 10.1.1.2

Description : Terminal configuration server IP address. Up to 2 terminal configuration servers can be entered and must be separated by a blank.

OK Cancel Help

Figure 224. Option 212 (Terminal Configuration Server) Template

New Option Template - As1.mycompany.com

Tag : 213

Name: Config file path

Value label: /QIBM/ProdData/NetworkStation/configs/

Description : The path name of the configuration data. Up to 2 path names can be entered separated by a blank.

OK Cancel Help

Figure 225. Option 213 (Configuration File Path Name) Template

New Option Template - As1.mycompany.com

Tag : 214

Name: Option 212 protocol

Value label: rfs/400

Description : Protocol to use for option 212. Possible values are tftp, nfs or rfs/400.

OK Cancel Help

Figure 226. Option 214 (Protocol to Use to Load the Terminal Configuration Data) Template

The new tags defined by the templates appear in the *Available options* window.

Now that you have the user-defined tags, you must add the corresponding values. For each of the defined tags, first click the tag number and then click **Add** to add the value. Refer to Figure 227 on page 256 through Figure 230 on page 258 to add values to the user-defined tags.

Class IBMNSM 1.0.0 Properties - As1.mycompany.com

General Address Pool Leases Options Other

Available options:

Tag	Name
76	STDA server
78	Directory agent
79	Service scope
80	Naming authority
212	Terminal server
213	Config File Path
214	Terminal Server Protocol

Selected options:

Tag	Name
1	Subnet mask
66	Server name
67	Boot file name
211	Config Protocol

Option 211: Config Protocol

rfs/400:

Enter ASCII string or hexadecimal data:

ASCII text: rfs/400

Hexadecimal:

OK Cancel Help

Figure 227. User-Defined Option 211 -- Protocol to Download Configuration Data

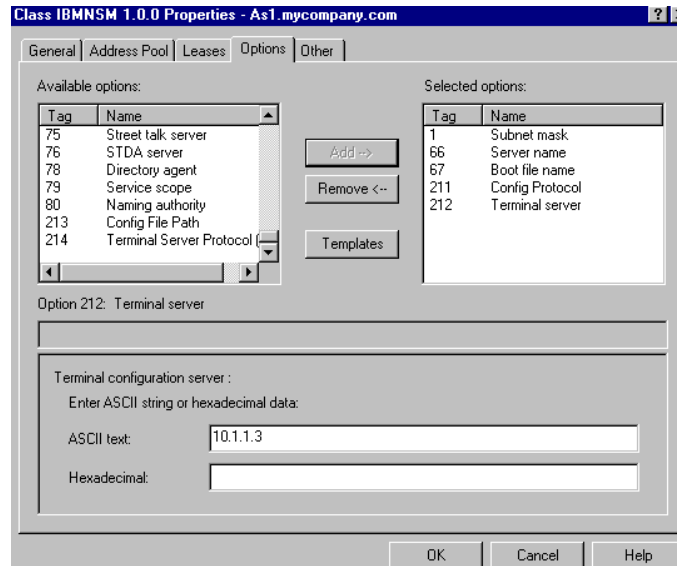


Figure 228. User-Defined Option 212 -- Terminal Configuration Server Name or IP Address

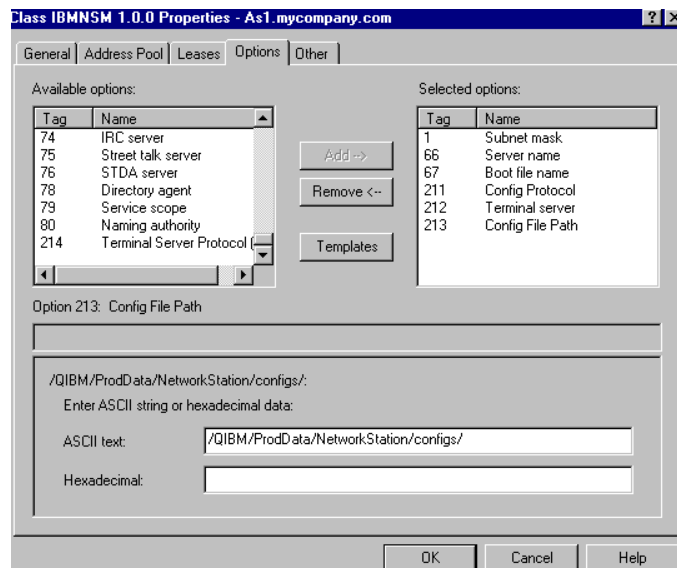


Figure 229. User-Defined Option 213 -- Configuration File Path

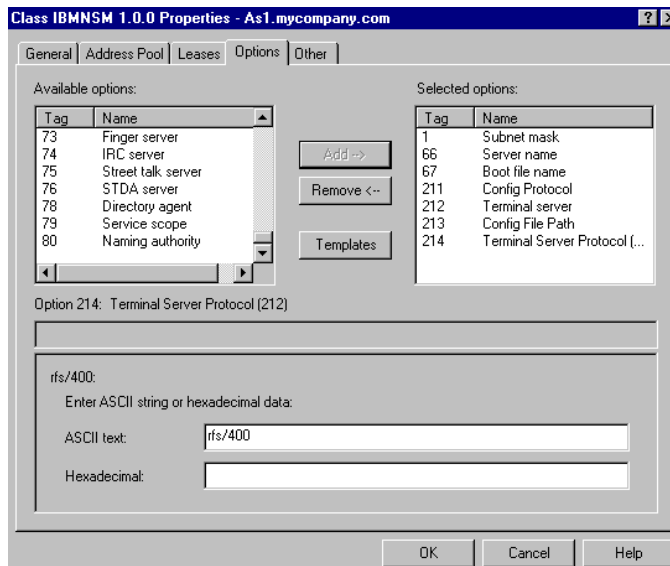


Figure 230. User-Defined Option 214 -- Protocol to Download Terminal Config (Option 212)

For information on installing and configuring the IBM Network Station, refer to *IBM Network Station Manager Installation and Use*, SC41-0664.

Figure 231 shows the options that you selected for the IBM Network Station configuration. Figure 232 on page 259 shows the options values.

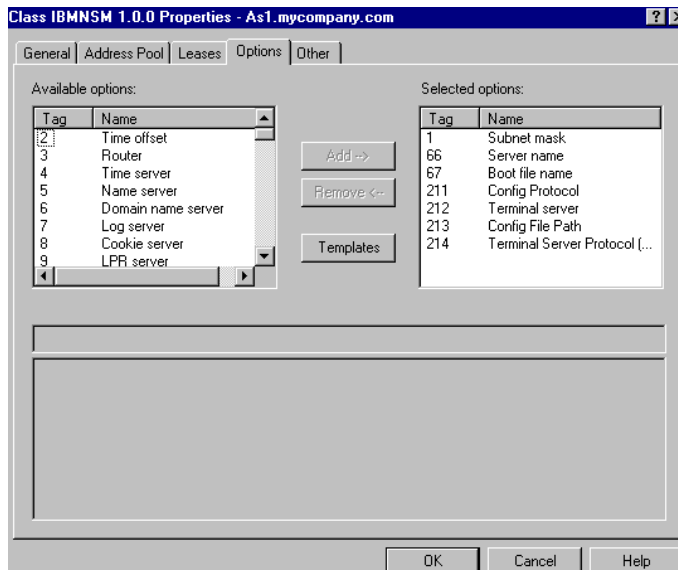


Figure 231. IBM Network Station Options Summary -- Tags

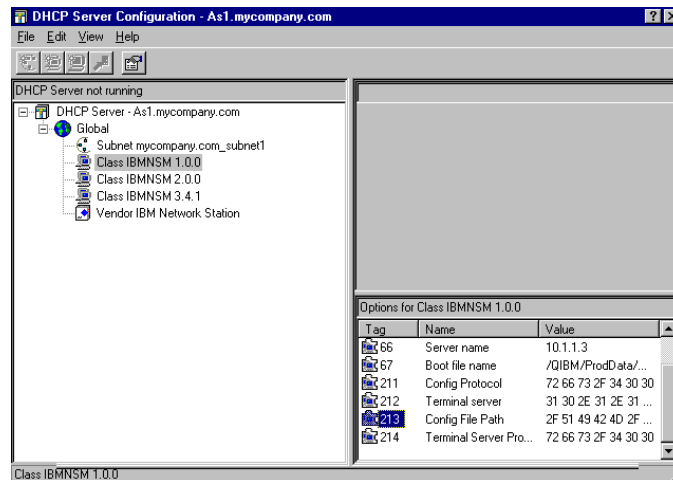


Figure 232. IBM Network Station Options Summary -- Values

11.7 Summary

This chapter demonstrated how to get started with DHCP in a simple network.

First, we helped you to understand your network addressing scheme and collect information about servers, routers, and lease times. Table 11 on page 242 and Table 12 on page 243 helped you gather the information.

Next, you learned how to run the Operations Navigator DHCP configuration wizard, which took you through a series of steps to configure the DHCP server. This chapter also explained how to configure two popular DHCP clients: Windows 95 and IBM Network Station.

Finally, we described how to make the IBM Network Station boot from a TFTP server that is different from the DHCP server. We also explained how to add options to classes and how to create user-defined options.

Chapter 12. Using Multiple DHCP Servers to Minimize Failures

Using multiple DHCP servers decreases the probability of having a DHCP-related network access failure, but it does not guarantee against it. The DHCP protocol does not implement a full backup mechanism such as the one available in DNS through the primary and secondary DNS zone transfer concept.

To avoid a single point of failure, configure two or more DHCP servers to serve the same subnet. If one server fails, the other can continue to serve the subnet. Each of the DHCP servers must be accessible either by direct attachment to the subnet or by using a BOOTP/DHCP Relay agent. As you read the rest of this section to determine whether you want to run multiple DHCP servers, keep in mind that you cannot run more than one DHCP server on any individual system.

Multiple DHCP servers require multiple systems. Because two DHCP servers cannot serve the same addresses, address pools that you have defined for a subnet must be unique across DHCP servers. Therefore, when you are using two or more DHCP servers to serve a particular subnet, you must divide the complete list of addresses for that subnet among the servers.

If a DHCP server for a particular subnet fails, the other DHCP server might be unable to service all of the requests from new clients. This exhausts the server's limited pool of available addresses.

You can bias which DHCP server exhausts its pool of addresses first. Some DHCP clients tend to select the DHCP server that offers more options. To bias service toward the DHCP server with 70% of the available addresses, offer fewer DHCP options from the server that holds 30% of the available addresses for the subnet.

Note: To bias the service, the client must wait to receive offers from more than one server. In our tests, the Windows 95 DHCP client always accepted the offer from the first server that responded regardless of the number of options offered by the DHCP servers.

This chapter describes how to implement DHCP backup techniques under the following conditions:

- There is a constraint on the number of IP addresses available, which you must split across different DHCP servers. This is sometimes referred to as the *70/30 split technique*.
- There is no constraint on the number of available IP addresses. Each server manages a large enough pool of addresses to satisfy DHCP requests from all of the DHCP clients in the network.

12.1 Scenario Overview

This scenario is based upon scenario number one (see Chapter 11, "Start Here: Implementing DHCP in a Simple Network" on page 237), in which an AS/400 system acts as a DHCP server in a simple, flat TCP/IP network. However, this scenario introduces a second DHCP server in an attempt to eliminate the single point of failure. This section does not discuss DHCP client configuration. Instead,

it concentrates on providing techniques to eliminate possible DHCP server outages.

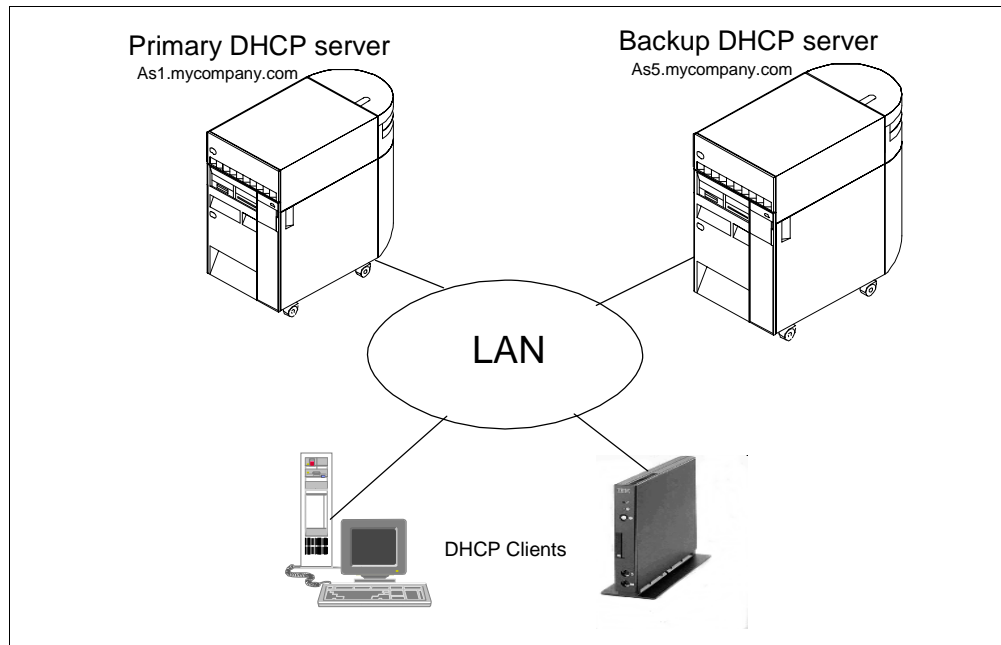


Figure 233. Network Overview Diagram

12.1.1 Scenario Objectives

This scenario has the following two objectives:

1. To provide partial DHCP support for clients connecting to the network in the event a DHCP server fails.
2. To show techniques on how to provide full-DHCP client support when there is no TCP/IP addressing constraint.

12.1.2 Scenario Advantages

This scenario shows how to provide support for DHCP clients that connect to your network if one of the DHCP servers is offline. It discusses several techniques and shows you how to implement them.

12.1.3 Scenario Disadvantages

Some of the techniques discussed in this chapter depend on TCP/IP addressing, which is the limitation that all network administrators and designers face. If you are free to use any type of IP addressing scheme, then implementing a backup DHCP server to support every client in your network is quite achievable.

Unfortunately, you might be unable to use the IP addressing scheme of your choice. There is a chance that you already have a functioning TCP/IP network as well. In these instances, you have to make some sacrifices and decide on which method provides you and your network with the best fall-back DHCP support.

12.1.4 Scenario Network Configuration

The following figure depicts the logical network topology for this scenario:

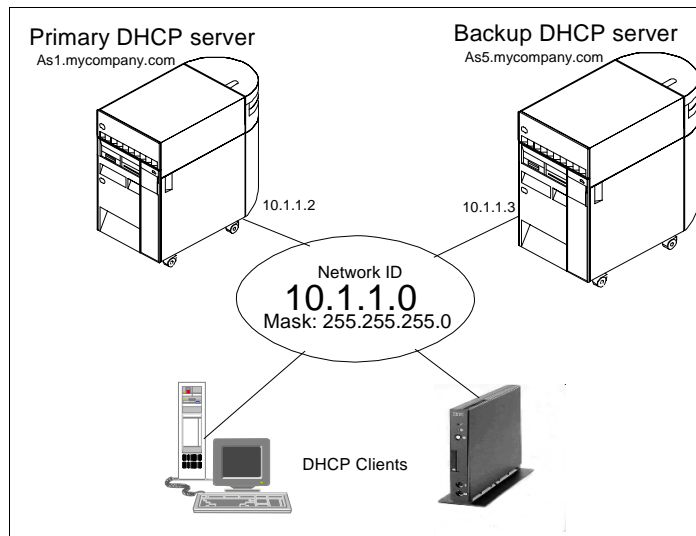


Figure 234. Scenario Network Diagram Showing Primary and Backup DHCP Servers

The following scenario characteristics influence the DHCP configuration:

- There are two AS/400 systems acting as DHCP servers, where one is the primary server and the other is the backup server.
- There is only a single subnet with a mask that allows up to 254 addresses and a client base of 250.
- There are no relay agents, routers, or bridges in the example.

12.2 Dividing the Address Pool across Two DHCP Servers

This method allows you take your existing TCP/IP address pool on the primary server and allot a percentage of the address pool to the backup DHCP server.

This method allows only partial support of the DHCP clients during a failure. This is due to a limited or constrained IP address range.

You can divide up your address pool however you want to suit your purpose, but remember that each address pool must be unique.

You can try to bias the client toward the primary DHCP server but this may not be possible if the client always accepts the offer from the first DHCP server that responds. If the primary server fails, then the backup still has an unused pool of IP addresses that has not been exhausted.

12.2.1 Objectives

There are four objectives:

- Divide the current IP address pool between two DHCP servers.
- Bias one server, if possible, to look more favorable to the DHCP client by serving or providing more options to the client.

- Use a small lease time to return IP addresses to the DHCP pool more quickly.
- Use the existing DHCP server as the primary server and the new DHCP server as the backup.

12.2.2 Advantages

Using this method to provide a DHCP server backup is straightforward. You do not need to change your TCP/IP addressing structure on the network.

Existing clients that have been served network information can remain connected even though the DHCP server is offline, depending on the lease time given and the client implementation of the DHCP code.

12.2.3 Disadvantages

If you decide to split the address pool in a percentage manner, you may encounter the following limitations:

- If the primary DHCP server that contains 70% of the address pool fails before it exhausts its address pool (or even uses a high percentage of it), then the backup DHCP server does not contain enough addresses to service the remaining clients.
- Decreasing the lease time is an attempt to reduce the length of time that the client stays on the network. Think of this as a *time share*, although it is dependent on the client implementation of DHCP. As such, the client may or may not relinquish the address.

12.3 Task Summary

To configure a second DHCP server as a backup and to divide the address pool in this scenario, perform the following steps:

1. Verify hardware, software, and configuration prerequisites.
2. Reduce the primary DHCP server IP address pool and exclude the backup DHCP server from the IP address range.
3. Add the remaining IP addresses to the backup server.
4. Start the primary and backup DHCP servers.

12.3.1 Verify Hardware, Software, and Configuration Prerequisites

To verify the prerequisites for the backup DHCP server, see Chapter 11.3, “Verify Hardware, Software, and Configuration Prerequisites” on page 239.

12.3.2 Reduce the Primary DHCP Server IP Address Pool

You must decide how you to divide the IP address pool on your existing DHCP server. In this example, there is only one IP address range and no complex subnetting issues. You are dividing the address pool in a 70/30% manner between the primary and backup DHCP servers.

You must also exclude the IP address of the backup DHCP server. To divide the existing IP address pool on the primary DHCP server, perform the following steps:

1. Start the AS/400 Operations Navigator.
2. Click *As1.mycompany.com* to select the system name.

This is your existing DHCP server that becomes the primary DHCP server.

3. Double-click **Network**.
4. Double-click **Server**.
5. Double-click **OS/400**.
6. Double-click **DHCP**. This starts the DHCP server configuration.
7. Right-click the subnet you want to divide. This opens a context menu.
8. Select **Properties**
9. Click the **Address Pool** tab.
10. Exclude the backup DHCP servers' IP address from this subnet. Click **Add** and specify the IP address of the backup DHCP server.
11. Reduce the IP address pool range to 70% of its maximum by specifying a new *End address* as shown in Figure 235 on page 265.

Note

The first three IP addresses (10.1.1.1, 10.1.1.2, and 10.1.1.3) are reserved for a future router, the primary DHCP server, and the backup DHCP server. This leaves a possible 251 IP addresses from 10.1.1.4 through 10.1.1.254. Specify the upper limit of the range as 10.1.1.175 on the primary DHCP server.

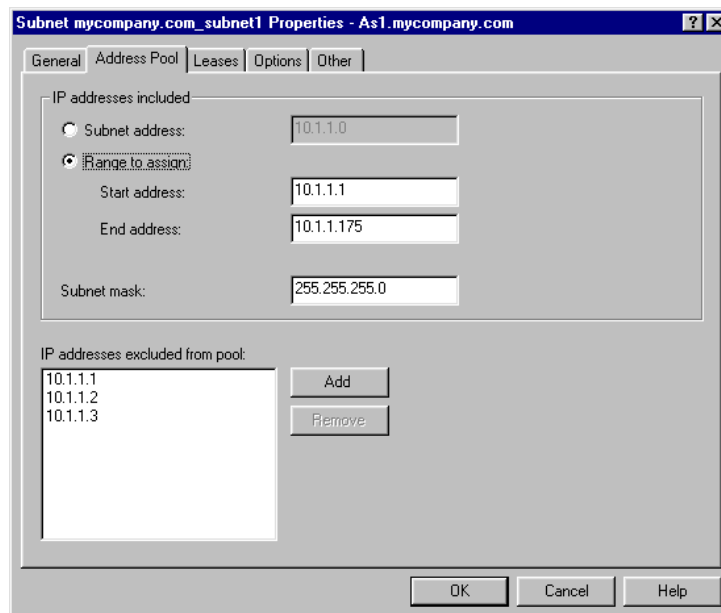


Figure 235. Reducing the IP Addressing Range

12. Click **OK**.

12.3.3 Change the Number of Options on the Primary and Backup DHCP Servers

The DHCP clients favor a DHCPOFFER packet that contains more DHCP options than one from another DHCP server. To allow the primary DHCP server to exhaust its IP address range, it is necessary to configure the primary with more options than the backup DHCP server.

Note

In the testing environment, an attempt was made to get both a Windows 95 client and the IBM Network Station to favor a certain DHCP server. The attempt to accomplish this by sending more options and setting a longer lease time did not work. A Windows'95 client and the IBM Network Station did not appear to wait long for all incoming DHCPOFFERS to arrive. Both appeared to take the first offer that was sent to them.

In the latest level of code being developed for the next release of the IBM Network Station (April/May 98), the boot monitor has been enhanced to look for multiple DHCPOFFERS arriving.

12.3.4 Add the Remaining IP Addresses to the Backup Server

You must now add an IP address range on the backup host to use during fall back. This address range is the second half of the pool that you split into two on the primary DHCP server.

To add an address pool that serves as the backup DHCP server, perform the following steps:

Note: Configure the DHCP server by using the AS/400 Operations Navigator GUI. Operations Navigator automatically starts the DHCP configuration wizard, which helps you to create a basic DHCP server configuration. The wizard starts only the first time you configure DHCP on the AS/400 system. These steps are explained in more detail in "Configure DHCP Server through Operations Navigator" on page 243.

To start the DHCP configuration wizard, perform the following steps:

1. Start the AS/400 Operations Navigator.
2. Click *As5.mycompany.com* to select the system name of your backup DHCP server.

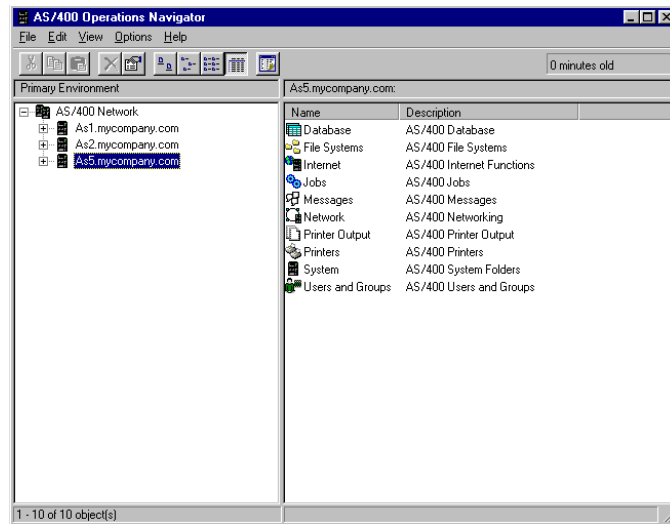


Figure 236. Selecting As5.mycompany.com Using the AS/400 Operations Navigator

3. Double-click **Network**.
4. Double-click **Server**.
5. Double-click **OS/400**.
6. Double-click **DHCP**. This starts the DHCP configuration wizard.

Note

If the DHCP configuration wizard is not shown, it is likely that a DHCP configuration already exists. To start the wizard and replace the existing configuration, select **File > New Configuration**, or just add the new subnet to the existing configuration.

7. Click **Next**.
8. Select **Yes** to add a new subnet to the DHCP server.
9. Leave the *Twinax IP workstation controller address* box blank and click **Next**.
10. Define the range of addresses to use within the subnet. Specify a range that includes the remaining 126 IP addresses.

Define Subnet Based on an Address Range - As5.mycompany.com

What is the information to define this subnet based on an address range within a subnet?

Name:

Description:

Start address:

End address:

Mask:

< Back Next > Cancel Help

Figure 237. Backup DHCP Server Subnet Range

11. Define a lease time for the client to keep the address served. Click **Next** to use the default lease time of one day.

Note

The lease duration is an important consideration that is discussed in more detail in Chapter 12.3.5, "Change the Lease Time on the Primary and Backup DHCP Servers" on page 269.

12. Click **Next** to *not* deliver the IP address of the domain name server. There is no DNS server in this scenario.

13. Select **No** to the question for setting other options and click **Next**.

14. Select **Yes** to *Start the DHCP server when TCP/IP starts?* and select **No** to *start the DHCP server now?* Click **Next**.

15. The DHCP configuration summary window shows all of the options that you have selected so far. Click **Finish**.

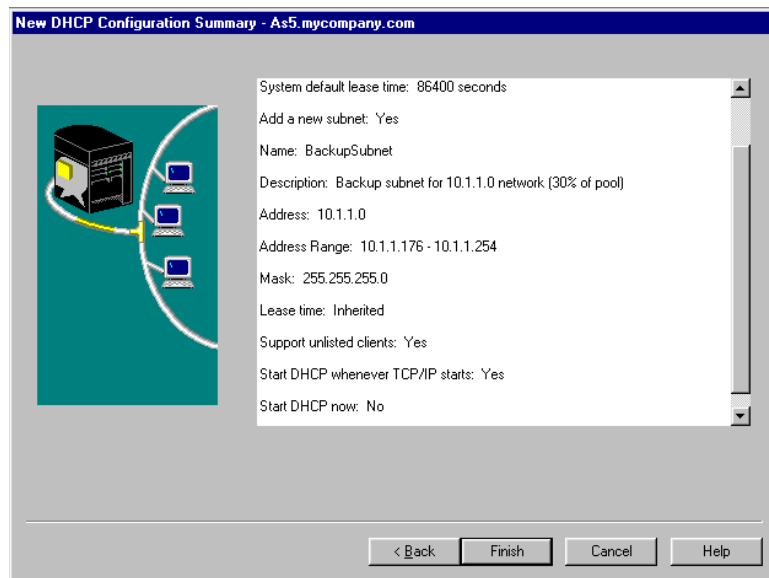


Figure 238. DHCP Configuration Summary - AS5.mycompany.com

16. Now that the DHCP server configuration is displayed, add a subnet mask for the clients by right-clicking the new subnet, *BackupSubnet*, and opening a context menu.
17. Select **Properties**.
18. Click the **Options** tab to add a subnet mask that is served to the clients.
19. Highlight option **1**, the subnet mask from the Available options window, and then click **Add**.
20. At the bottom of the display, specify 255.255.255.0 for the subnet mask that the clients use.
21. Click **OK**.

12.3.5 Change the Lease Time on the Primary and Backup DHCP Servers

The lease time is the amount of time that the client is allowed to keep the IP address served using DHCP. The default lease time is one day, or 86400 seconds.

Depending on the number of available IP addresses in your address pool, how many of those addresses are typically in use by DHCP clients, and how often the DHCP clients restart or change subnets, you might need to change the duration of the lease.

If you have a large number of IP addresses available in the address pool and relatively few DHCP clients, you can increase the length of the lease duration. Increasing the length reduces the number of lease renewals across your network and slightly reduces the load on your DHCP server.

If you have a constraint with the number of available IP addresses in your DHCP address pool and if most of those addresses are in use at any given time, it is desirable to reduce the lease duration. Additionally, it is also beneficial to reduce the lease time if your DHCP clients are mobile, changing from one subnet to

another, and requiring a new IP address. A reduction in the lease time returns the IP address to the pool more quickly. This allows it to be available for another client. The trade-off here is that there is an increased amount of network traffic that requests lease renewals, and the DHCP server needs to service the renewal requests. This trade-off is considered minor because it is usually more important to have the clients connect to the network.

If the primary DHCP server fails in fail-back scenarios, you need to set the lease time to a smaller value. The clients attempt to renew their leases on the IP address when half of the lease time has expired. They again make the attempt when approximately 85% of the time has expired (provided the DHCP server has not extended the lease by then).

12.3.6 Start the Primary and Backup DHCP Servers

It is suggested that if you use the method previously described, then you need to start the primary DHCP server first and leave it running until it has exhausted nearly all of its IP range. Indeed, it is conceivable to leave the backup server offline until the primary server fails. This is due to the fact that each DHCP client implementation appears slightly different. During the testing for this book, the primary DHCP client was not favored over the backup even when more options were provided to the client. To ensure that each client is always served an address from the primary server from initialization, start the primary server first. Once the client has contacted the DHCP server, it always attempts to return and request a lease renewal from the primary.

To start the DHCP servers, perform the following steps:

1. From the AS/400 Operations Navigator, right-click **DHCP** to open a context menu (see Figure 239 on page 270).
2. Select **Start**.
3. Repeat the process for the backup server.

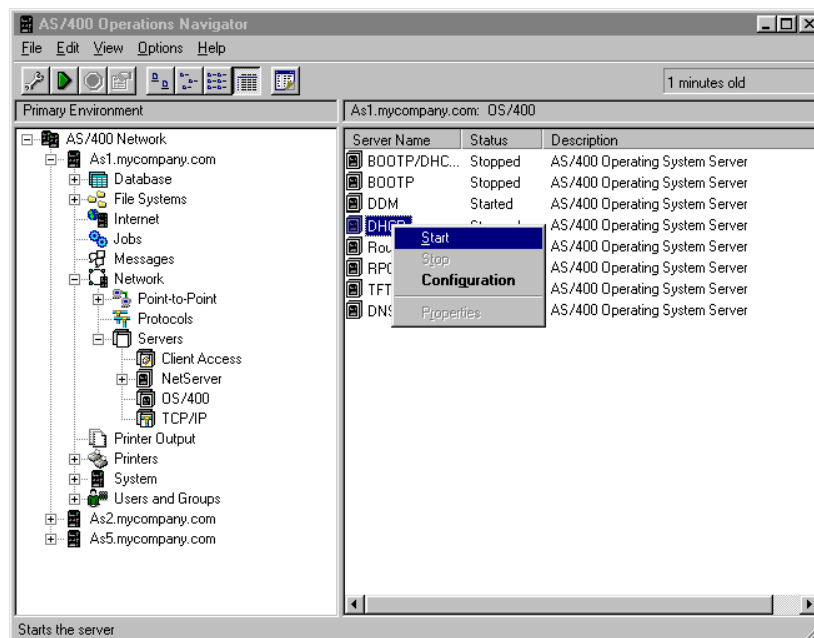


Figure 239. Starting the DHCP Server

12.4 Providing Full-DHCP Client Support

This section describes how to provide full DHCP client support from two DHCP servers in a simple TCP/IP network that has no constraints with IP addresses.

The configuration on each DHCP server has a large enough IP address range or pool to service 100% of the clients in the network.

In this example, the network has 250 clients. Use a subnet mask over a class A private network to provide up to 510 IP addresses in the pool.

12.4.1 Objectives

Using two DHCP servers, this scenario demonstrates a method that allows each server to service 100% of the client base, even if one of the DHCP servers is offline for any reason.

12.4.2 Advantages

This method has the major advantage of allowing all of the clients to connect to the network during a DHCP failure.

12.4.3 Disadvantages

This scenario assumes that you have an unlimited range of TCP/IP addresses. As such, many IP addresses are not in use at any given time. You can consider these IP addresses wasted.

12.4.4 Network Addressing Scope Planning

This example uses the network 10.1.1.0. We recommend that you perform a hierarchical partitioning of a network to ease administration. To accomplish this, enter:

10.x.y.z where x = site or region, y = department, z = hosts, x + y = subnet.

The small, example network (10.1.1.0 and a mask of **255.255.255.0**) allows up to 254 hosts. If you need to expand your network to connect to more hosts, change the mask to **255.255.254.0**. This reduces the subnet addressing scope (x + y) by one bit, but it creates one extra bit for the host-addressing scope (z). That generates up to 510 hosts. This means that the network address changes to 10.1.0.0, and the host address range is from 0.0.0.1 through 0.0.1.254. This technique shows an easy way to increase the number of host addresses that are available to the subnet or the network. It also lets the network grow without too much change.

You can use this technique to increase the number of supported clients by using the appropriate subnet mask. For example, a subnet mask of 255.255.252.0 gives you 1022 addresses with which you can support up to 511 clients on each DHCP server.

If you use this method to allow support for up to 250 hosts on each DHCP server, they have a combined TCP/IP address range for 510 clients.

12.4.5 Task Summary

The steps required to configure this scenario are as follows:

1. Verify hardware, software, and configuration prerequisites.
2. Enlarge the primary DHCP server IP address pool.
3. Add the remaining IP addresses to the backup server.
4. Start the primary and backup DHCP servers.

12.4.6 Verify Hardware, Software, and Configuration Prerequisites

To verify the prerequisites for the backup DHCP server, see Chapter 11.3, “Verify Hardware, Software, and Configuration Prerequisites” on page 239.

Note

Because you are changing the subnet range by altering the mask, you must also ensure that the TCP/IP interface for each physical connection to the same network also has had the mask changed to 255.255.254.0.

12.4.7 Enlarge the Primary DHCP Server IP Address Pool

In this example, use the IP address range from 10.1.0.1 through 10.1.1.254 with a mask of 255.255.254.0. This provides up to 510 host addresses on network 10.1.0.0. Refer to Chapter 12.4.4, “Network Addressing Scope Planning” on page 271.

The host portion of the network address is divided in half, allowing the primary DHCP server to have 255 addresses and the backup server to have 255 addresses.

In this example, you cannot exclude the IP address of the primary server, backup server, or router because they exist in the address range that you configure on the backup DHCP server.

To create the new addressing pool on the primary DHCP server, perform the following steps:

1. Start the AS/400 Operations Navigator.
2. Click *As1.mycompany.com* to select the system name.

This is the existing DHCP server that becomes the primary DHCP server.

3. Double-click on **Network**.
4. Double-click on **Server**.
5. Double-click on **OS/400**.
6. Double-click on **DHCP**. This starts the DHCP server configuration.
7. Right-click the subnet that you want to divide. This opens a context menu. Select **Properties**.
8. Click the **Address Pool** tab.

9. Add the new TCP/IP address range. In this case, use the range from 10.1.0.1 through 10.1.0.254 with a mask of 255.255.254.0, shown in Figure 240 on page 273.

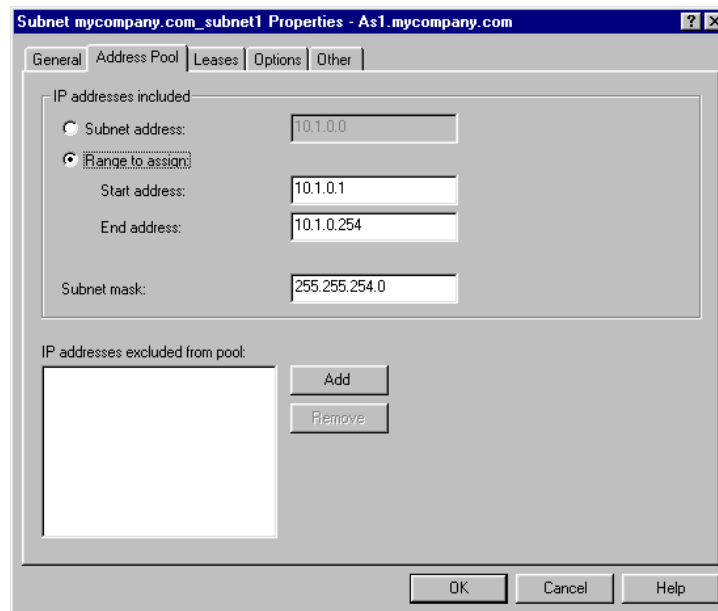


Figure 240. As1.mycompany.com Subnet Configuration

10. Click **OK**.

12.4.8 Add the Remaining IP Addresses to the Backup DHCP Server

You need to configure the remaining 50% of the IP address pool on the backup DHCP server. In this example, add the range from 10.1.1.0 through 10.1.1.254 with a subnet mask of 255.255.254.0.

This provides the other 255 host addresses on network 10.1.0.0. Please refer to Chapter 12.4.4, "Network Addressing Scope Planning" on page 271.

You must also exclude the IP address of the primary server, backup server, and future router because their addresses exist in this range. The steps to do this are contained here.

To create the new addressing pool on the backup DHCP server, perform the following steps:

1. Start the AS/400 Operations Navigator.
2. Click *As5.mycompany.com* to select the system name.

This is your existing backup DHCP server.

3. Double-click **Network**.
4. Double-click **Server**.
5. Double-click **OS/400**.
6. Double-click **DHCP**. This starts the DHCP server configuration.

7. Right-click on the subnet that you want to divide. This opens a context menu. Select **Properties**.
8. Click the **Address Pool** tab.
9. Add the new TCP/IP address range. In this case, use the range from 10.1.1.0 through 10.1.1.254 with a mask of 255.255.254.0, shown in Figure 241 on page 274.

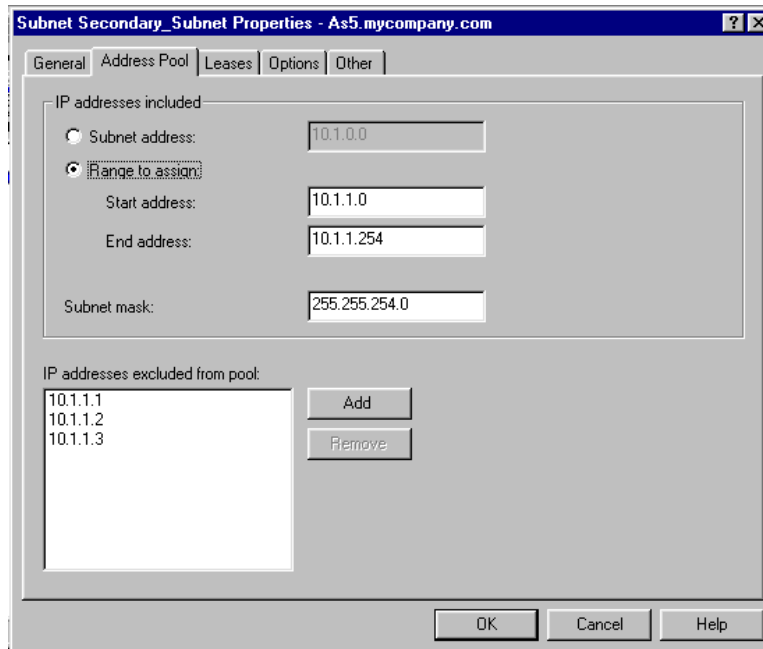


Figure 241. As5.mycompany.com Subnet Configuration

10. Click **Add** to exclude the IP addresses of the primary server, backup server, and future router.
11. Click **OK**.

12.4.9 Start the Primary and Backup DHCP Servers

You can now start the primary and backup DHCP servers as follows:

1. From the Operations Navigator, right-click **DHCP** to open a context menu (see Figure 242 on page 275).
2. Select **Start**.
3. Repeat the process for the backup server.

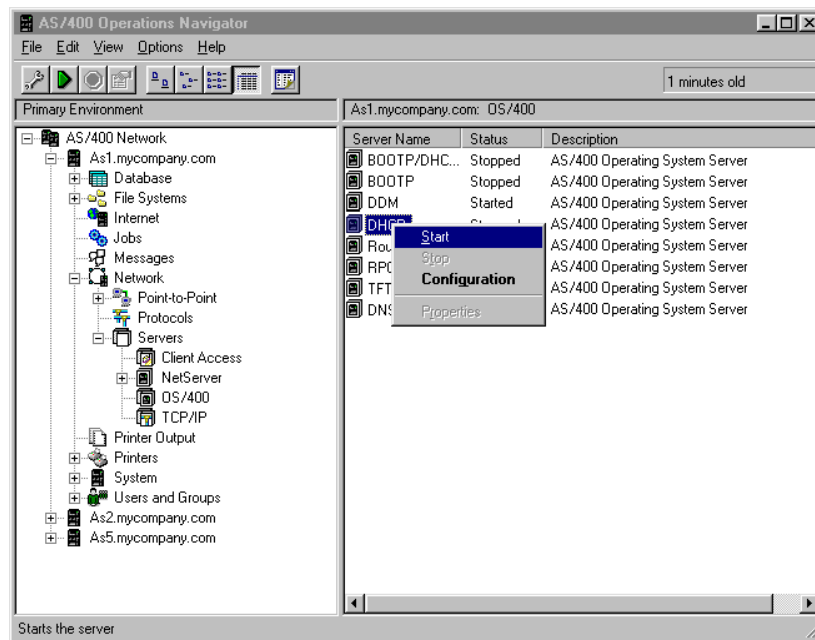


Figure 242. Starting the DHCP Server

12.5 Summary

It is important to remember that installing a backup DHCP server on your network does not guarantee that addresses are available for all clients during an unplanned primary DHCP server outage.

If you have a constrained IP addressing scheme, then you can only provide a partial fall-back support. This is sometimes referred to as the 70/30 split technique.

You can favor which server the DHCP client chooses by providing more options to the client. In the test environment, however, the first DHCP server that responded was selected, regardless of the options offered.

If you do not have any constraints on your IP addressing scheme, it is possible to serve every client from any server. Using this method results in most of the IP addresses not being used unless one of the DHCP servers fails. The IP addresses in the pool are effectively unusable by any other non-DHCP client. This is considered wasteful but you might be able to afford it if you are using a class A 10.x.x.x network. There is another alternative with a primary DHCP server and a backup DHCP server using a BOOTP/DHCP Relay Agent to forward packets to both servers but that introduces a delay when forwarding to the backup DHCP server. This option is discussed in Chapter 14, “Multiple Subnets, DHCP Servers, and Relay Agents” on page 313.

Multiple DHCP servers require multiple systems.

The DHCP servers must be accessible either by direct attachment to the subnet or by using a BOOTP/DHCP Relay Agent.

Chapter 13. Multiple Subnets and DHCP Servers

If your network is larger than the one shown in 11, “Start Here: Implementing DHCP in a Simple Network” on page 237, you may have to work with multiple LANs and subnets. This chapter covers the considerations you need to take into account when providing DHCP services to a simple, multi-LAN and multi-subnet network.

13.1 Scenario Overview

This scenario provides DHCP services to clients that are connected to multiple LANs. The network is still fairly simple. It has no routers and only two AS/400 systems that you can use as DHCP servers. Further, it is assumed that there are no more than 254 clients in subnet A and no more than 510 clients in subnet B.

The DHCP server AS1 is configured to serve addresses to the terminals that request an address in subnet A. The DHCP server AS5 is configured to serve addresses to the terminals that request an address in subnet B. However, there is also a need for communication between the two subnets by way of IP datagram forwarding. Therefore, a second TCP/IP interface is configured on the AS1 AS/400 system. Figure 243 shows the sample network.

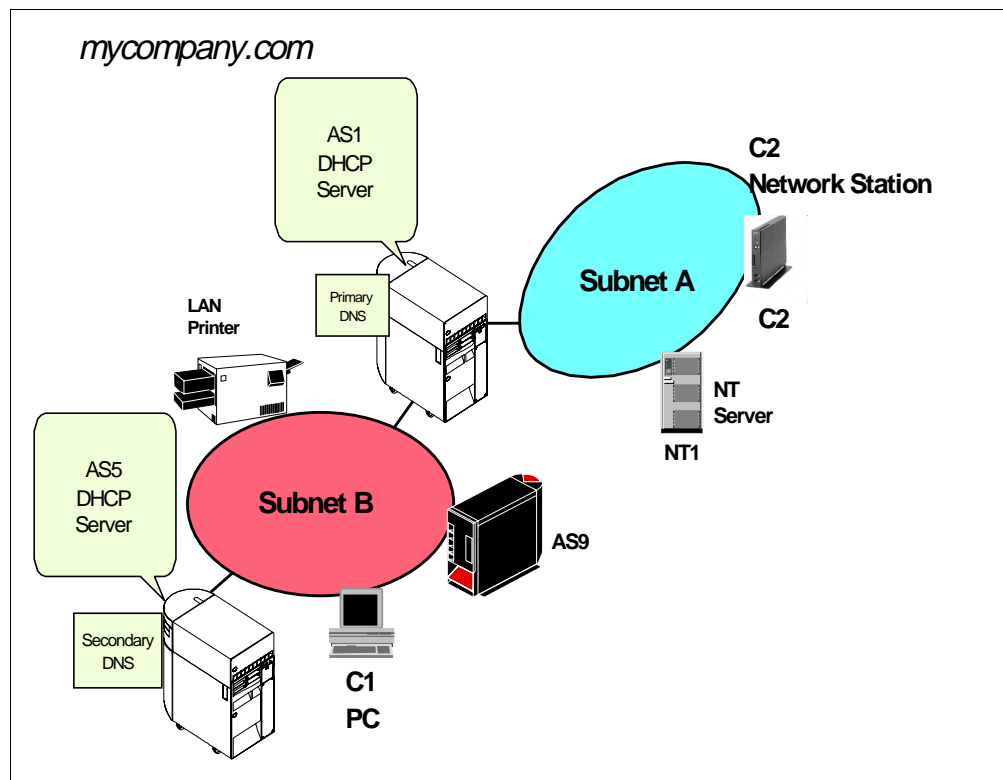


Figure 243. Scenario Network Diagram

13.1.1 Scenario Objectives

The objectives of this scenario are to:

1. Show that if you configure AS1 as a DHCP server for subnet A and AS5 as a DHCP server for subnet B, AS1 still receives DHCPDISCOVER packets from subnet B through the second IP interface (10.1.0.3 in the sample network).
2. Show how to configure AS1 as a DHCP server for both subnet A and subnet B and how to use AS5 as a backup for subnet B only. This scenario assumes that subnet B is more critical to the business.

13.1.2 Scenario Advantages

This scenario shows how you can implement a simple, multi-subnet network using a single AS/400 system as a gateway, a DHCP server, and a DNS server. The proposed solution implements a DHCP server on AS1, which is configured as a **multi-homed** host. A multi-homed host is a host with two or more physical interfaces to multiple subnets.

Even though it is not shown in this scenario, you can configure AS5 as a backup DHCP server for network B.

13.1.3 Scenario Disadvantages

1. The DHCP protocol flow can be confusing. When C2 broadcasts a DHCPDISCOVER packet, only the DHCP server AS1 sees it. When C1 broadcasts a DHCPDISCOVER packet, both AS1 and AS5 see it because AS1 is multi-homed. If you have not configured the AS1 interface on subnet B for DHCP serving, it logs the DHCP packets that it is not servicing (those that are intended for AS5).
2. There is no full DHCP server backup. If AS1 fails, subnet A cannot have access to a DHCP server. AS5 performs DHCP server backup functions for subnet B. To provide full DHCP server backup, you need to introduce a relay agent to back up AS1. Refer to Chapter 14, "Multiple Subnets, DHCP Servers, and Relay Agents" on page 313, for more information on relay agents.

13.1.4 Scenario Network Configuration

Figure 244 on page 279 shows the network detail for this scenario. Note that subnet B has a network ID of 10.1.0.0 and a mask of 23 contiguous bits, allowing a range of 510 TCP/IP addresses.

The main characteristics of this scenario's network are as follows:

- There are two physical network segments.
- There are two subnets, one for each physical segment.
- There is one multi-homed host, AS1. It has one physical interface on subnet A and another one on subnet B.
- AS1 is the gateway between both subnets with one physical interface on each one and IP forwarding turned on.
- There are two DHCP servers, AS1 and AS5, in the first part of this scenario. AS1 serves subnet A and AS5 serves subnet B.
- There is only one DHCP server, AS1, serving both networks in the second part of this scenario.
- There is a primary DNS server, AS1, and a secondary DNS server, AS5.
- The network implements a class A TCP/IP addressing scheme, and subnet B uses a complex mask, 255.255.254.0.

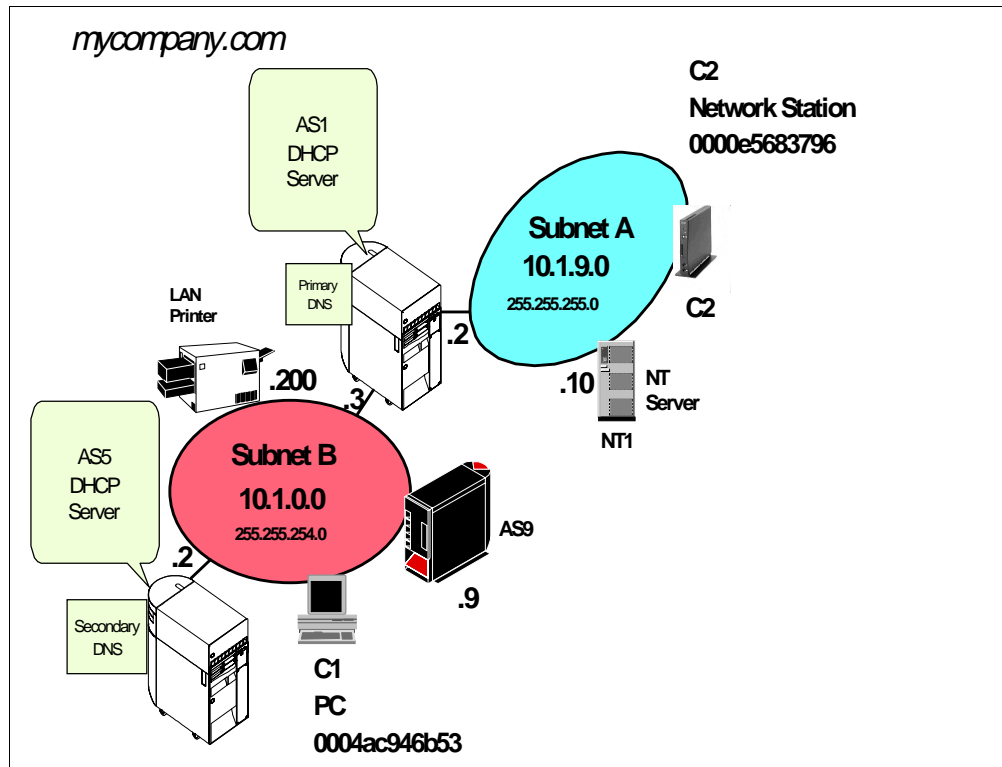


Figure 244. Scenario Network Topology

13.2 Task Summary

To configure the DHCP server and clients in this scenario, perform the following steps:

1. Configure and start a TCP/IP interface on both DHCP servers.
2. Plan the DHCP server configuration and gather information to configure the DHCP servers.
3. Configure the DHCP support on AS1 for Subnet A and on AS5 for Subnet B.
4. Start the DHCP server support on DHCP AS1 and AS5.
5. Configure the Windows 95 client for DHCP support.
6. Configure the IBM Network Station client for DHCP support.

13.3 Configuration Overview

1. Configure TCP/IP and add an IP interface on AS5 and two IP interfaces on AS1.
2. Configure the DHCP server support through Operations Navigator on both AS/400 systems.
3. Configure the clients to use DHCP.

13.3.1 Configuring TCP/IP Interfaces on AS1

To configure the TCP/IP interface, perform the following steps:

1. On an AS/400 command entry display, type the command:

```
GO CFGTCP
```

Press Enter to display the Configure TCP (CFGTCP) menu.

2. Select option **1** (Work with TCP/IP interfaces) to display the Work with TCP/IP Interfaces display (see Figure 245).
3. Select option **1** to add a TCP/IP interface and specify the TCP/IP address of the host. Press Enter to continue.
4. Add the line description name and the subnet mask for the interface.
5. Press Enter to create the TCP/IP interface.
6. After you have done this for the interface addresses 10.1.0.3 and 10.1.9.2, you see a display similar to the one in Figure 245.

System: As1

Work with TCP/IP Interfaces

Type options, press Enter.

1=Add 2=Change 4=Remove 5=Display 9=Start 10=End

Opt	Internet Address	Subnet Mask	Line Description	Line Type
	10.1.0.3	255.255.254.0	TRNLINE1	*TRLAN
	10.1.9.2	255.255.255.0	TRNLINE2	*TRLAN
	127.0.0.1	255.0.0.0	*LOOPBACK	*NONE

Bottom

F3=Exit F5=Refresh F6=Print list F11=Display interface status

F12=Cancel F17=Top F18=Bottom

Figure 245. Work with TCP/IP Interfaces -- AS1

7. Press **F11** to view the status of the interface and verify that the status is active. If it is not, start the interface with option **9**.

13.3.2 Gathering Information to Configure DHCP Servers

To use Operations Navigator DHCP configuration effectively, you need to know how you want to set up and manage your networks and subnets with DHCP. You also need to know what address range or ranges you want to use for leasing. You must decide which system is the DHCP primary server and which one performs

DHCP backup functions. Further, you need to know which IP addresses to reserve for special hosts such as routers, DNS servers, and firewalls. It is useful to refer to a network diagram that shows the subnet masks and IP addresses for your networks, routers, and clients while you are configuring DHCP.

The starting point in this scenario is the network diagram that is shown in Figure 244 on page 279. The information shown in the following tables is based upon the network picture and other network data.

13.3.2.1 AS1 DHCP Server and Administered Subnets Information

Table 13 shows general information about AS1 as a TCP/IP host, and Table 14 provides more specific information about AS1 as a DHCP server.

Table 13. Planning the DHCP Server - AS1 TCP/IP Information

Host Name	AS1
Description	Subnet A DHCP server
Domain Name	mycompany.com
IP Address	10 . 1 . 0. 3
Mask	255.255.254.0
Line Description	TRNLINE1
IP Address	10 . 1 . 9 . 2
Mask	255.255.255.0
Line Description	TRNLINE2

Note: The *Configuration Reference* column in the following tables points to the place in Operations Navigator DHCP server configuration where you can configure the particular parameter. You can enter many of these configuration options through the DHCP configuration wizard the first time you configure DHCP.

Table 14. Planning the DHCP Server AS1 -- DHCP Server Overview

#	Question	Answer	Configuration Reference
1	Is the BOOTP Server already configured on your system?	No	DHCP configuration wizard
2	Do you want to migrate the BOOTP configuration to DHCP?	N/A	File -->Migrate BOOTP
3	What is the default lease time for this server?	12 hours	Global-->Properties-->Leases
4	Start the DHCP server when TCP/IP starts?	Yes	Server Properties --> General
5	List the DHCP server IP interfaces that will be serving DHCP clients.	10.1.9.2	See network diagram.
6	List the subnets that will be administered by this DHCP server.	10.1.9.0	See subnet planning table
7	Do you want to add a new subnet to be administered by this server?	Yes	Global --> New Subnet - Basic Global-->New Subnet - Advanced See subnet planning table

#	Question	Answer	Configuration Reference
8	Do you want to log DHCP server activity?	Yes	Server Properties --> Logging
9	Do you want the DHCP server to support any client from any subnet?	Yes	Server Properties --> Client Support
10	Do you want the DHCP server to support BOOTP clients?	No	Server Properties --> Client Support
11	Do you want the DHCP server to reject requests from specific clients (for example, for security reasons)?	No	Global->Properties-> Exclude Client
11	Can your DHCP clients (other than IBM Network Stations) identify the class they belong to?	No	
12	If answer to 11 is Yes, do you want to add a new class to serve the DHCP clients that belong to that class?	N/A	Global --> New Class

Table 15 provides information about subnet 10.1.9.0 being administered by AS1 DHCP server. Notice that AS1 administers 100% of the IP addresses available in this subnet.

Table 15. Planning the Subnet 10.1.9.0 Administered by AS1 from IP Interface 10.1.9.2

#	Question	Answer	Configuration Reference
1	Subnet name	Subnet_A_10.1.9.0	Subnet Properties --> General
2	Subnet description	Services	Subnet Properties --> General
3	Subnet address	10.1.9.0	Subnet Properties --> Address Pool
4	Subnet mask	255.255.255.0	Subnet Properties --> Address Pool
5	Address range	10.1.9.1 10.1.9.254	Subnet Properties --> Address Pool
6	Lease time	Inherit from server (12 hours)	Subnet Properties --> Leases
7	Exclusions (exclude hosts that required a particular IP address and are manually configured).		Subnet Properties --> Address Pool
	Name: Router x Description: Reserved for future router IP address: 10.1.9.1	AS1 DNS/DHCP server 10.1.9.2	NT1 NT file server 10.1.9.10
8	Domain Name Server IP address to deliver to clients in this subnet.	10.1.9.2 10.1.0.2	Subnet Properties --> Options--> Option 6 (Domain name server)
9	Gateway IP address to deliver to clients in this subnet.	10.1.9.2	Subnet Properties --> Options--> Option 3 (Router)
10	Offer options to client in this subnet 01 - Subnet mask 03 - Router 06 - Domain name server	255.255.254.0 10.1.9.2 10.1.9.2 10.1.0.2	Subnet Properties --> Options-->

Note

Option 67 (boot file name) and option 51 (IP address lease time) for IBM Network Station clients on this subnet are those shipped by default in Class **IBMNSM 1.0.0**. This class is for token-ring attached IBM Network Stations and the default values are as follows:

Option 67: /QIBM/ProdData/NetworkStation/kernel

Option 51: 1 day

13.3.2.2 AS5 DHCP Server and Administered Subnets Information

Table 16 shows general information about AS5 as a TCP/IP host and Table 17 provides more specific information about AS5 as a DHCP server.

Table 16. Planning the DHCP Server -- AS5 TCP/IP Information

Host Name	As5
Description	Subnet B DHCP server
Domain Name	mycompany.com
IP Address	10 . 1 . 0. 2
Mask	255.255.254.0
Line Description	TRNLINE1

Note: The *Configuration Reference* column in the following tables points to the place in Operations Navigator DHCP server configuration where you can configure the particular parameter. You can enter many of these configuration options through the DHCP configuration wizard the first time you configure DHCP.

Table 17. Planning the DHCP Server AS5 -- DHCP Server Overview

#	Question	Answer	Configuration Reference
1	Is the BOOTP Server already configured on your system?	No	DHCP configuration wizard
2	Do you want to migrate the BOOTP configuration to DHCP?	N/A	File -->Migrate BOOTP
3	What is the default lease time for this server?	12 hours	Global-->Properties-->Leases
4	Start the DHCP server when TCP/IP starts	Yes	Server Properties --> General
5	List the DHCP server IP interfaces that will be serving DHCP clients.	10.1.0.2	See network diagram.
6	List the subnets that will be administered by this DHCP server.	10.1.0.0	See subnet planning table
7	Do you want to add a new subnet to be administered by this server?	Yes	Global --> New Subnet - Basic Global-->New Subnet - Advanced See subnet planning table
8	Do you want to log DHCP server activity?	Yes	Server Properties --> Logging

#	Question	Answer	Configuration Reference
9	Do you want the DHCP server to support any client from any subnet?	Yes	Server Properties --> Client Support
10	Do you want the DHCP server to support BOOTP clients?	No	Server Properties --> Client Support
11	Do you want the DHCP server to reject requests from specific clients (for example, for security reasons)?	No	Global->Properties-> Exclude Client
11	Can your DHCP clients (other than IBM Network Stations) identify the class they belong to?	No	
12	If answer to 11 is Yes, do you want to add a new class to serve the DHCP clients that belong to that class?	N/A	Global --> New Class

Table 18 provides information about subnet 10.1.0.0 administered by AS5 DHCP server. Notice that AS5 administers 100% of the IP addresses available in this subnet.

Table 18. Planning the Subnet 10.1.0.0 Administered by AS5 from IP Interface 10.1.0.2

#	Question	Answer	Configuration Reference
1	Subnet name	Subnet_B_10.1.0.0	Subnet Properties --> General
2	Subnet description	Marketing and Manufacturing	Subnet Properties --> General
3	Subnet address	10.1.0.0	Subnet Properties --> Address Pool
4	Subnet mask	255.255.254.0	Subnet Properties --> Address Pool
5	Address range	10.1.0.0 10.1.1.254	Subnet Properties --> Address Pool
6	Lease time	Inherit from server (12 hours)	Subnet Properties --> Leases
7	Exclusions (exclude hosts that required a particular IP address and are manually configured).		Subnet Properties --> Address Pool
	Name: Router x Description: Reserved for future router IP address: 10.1.0.1	AS5 DNS/DHCP server 10.1.0.2	AS1 DNS/Gateway 10.1.0.3
8	Domain Name Server IP address to deliver to clients in this subnet.	10.1.0.3 10.1.0.2	Subnet Properties --> Options--> Option 6 (Domain name server)
9	Gateway IP address to deliver to clients in this subnet.	10.1.0.3	Subnet Properties --> Options--> Option 3 (Router)
10	Offer options to client in this subnet 01 - Subnet mask 03 - Router 06 - Domain name server	255.255.254.0 10.1.9.2 10.1.9.2 10.1.0.2	Subnet Properties --> Options-->

13.3.3 Configuring DHCP Server Support in AS1

You must configure the DHCP server using the AS/400 Operations Navigator GUI for servicing the DHCP clients on subnet A.

You are configuring DHCP on a system without an existing configuration. Refer to Chapter 11.4.3, “Configure DHCP Server through Operations Navigator” on page 243, for information on how to reset the existing DHCP configurations and start over. Operations Navigator automatically starts the DHCP Configuration Wizard. This wizard helps you create a basic DHCP server configuration.

To start the DHCP configuration wizard, perform the following steps:

1. Start the AS/400 Operations Navigator.
2. Click the system *As1.mycompany.com* to select it.
3. Double-click **Network**.
4. Double-click **Server**.
5. Double-click **OS/400**.
6. Double-click **DHCP**. This starts the DHCP configuration wizard.
7. Click **Next**.

Note

The sequence of the following steps might be different in your situation, depending on such factors as whether you already have a BootP table on your system and the navigation path you have chosen. Consider this as just an example. The important point is that you understand how to implement the planned configuration.

8. Select the default lease time for the whole network (all subnets administered by this server):
12 hours
Click **Next**.
9. Select **Yes** to add a new subnet to the DHCP server. Start configuring *Subnet A -- 10.1.9.0*.
10. Answer **No** to the question “*Will this subnet manage twinax devices?*”
Click **Next**.
11. Select **Define subnet based on entire subnet**. You are configuring the whole subnet range.
12. Specify the information as shown in Figure 246. Click **Next**.

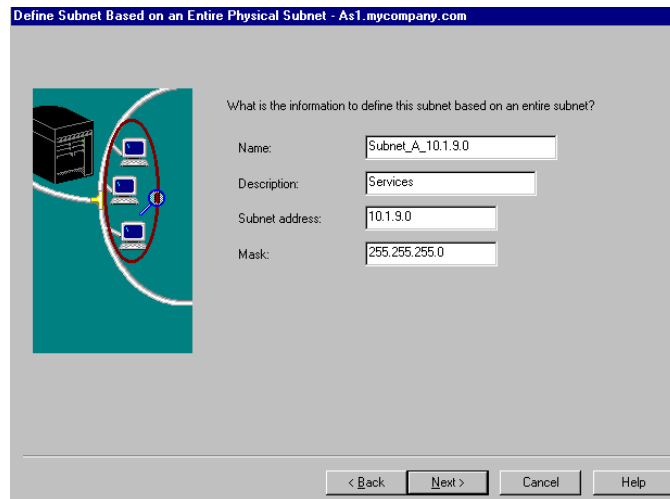


Figure 246. Defining Subnet A -- 10.1.9.0 Based on Entire Subnet

13. Exclude the IP addresses of the hosts in this subnet that you have already configured with permanent IP addresses. In this scenario, those hosts are reserved for a router in the event that one is needed in the future for AS1 and NT1.

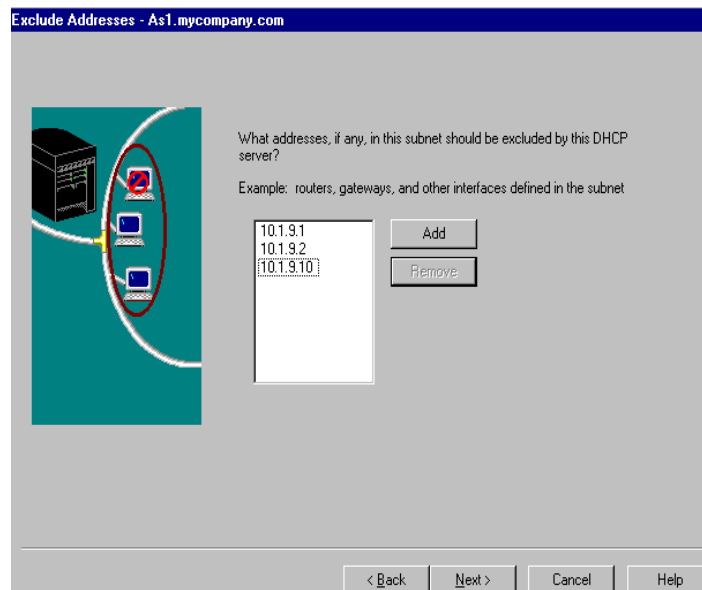


Figure 247. Exclude IP Addresses Already Assigned to Hosts in Subnet A -- 10.1.9.0

Click **Next**.

14. Accept *Inherit the server's default lease time (12 hours)*.
15. Answer **Yes** to the question "Would you like the DHCP Server to deliver gateway addresses to clients in this subnet?"

16. Add the gateway IP address that is the AS1 interface on this subnet. In this simple network, the AS/400 system AS1 acts as a gateway between the two subnets.

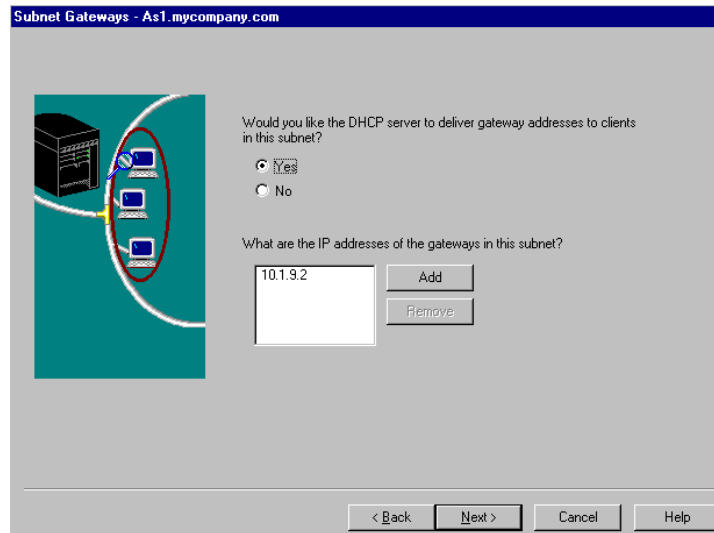


Figure 248. Configuring Subnet A's Gateway Information

Click **Next**.

17. Answer Yes to the question “Would you like DHCP to deliver domain name server addresses to clients in this subnet?” In this simple network, the same AS/400 system (AS1) provides DNS services for the whole network.
18. Add the DNS IP address. Notice that the DNS server for *mycompany.com* runs on the same AS/400 system, AS1 (see Figure 244 on page 279).

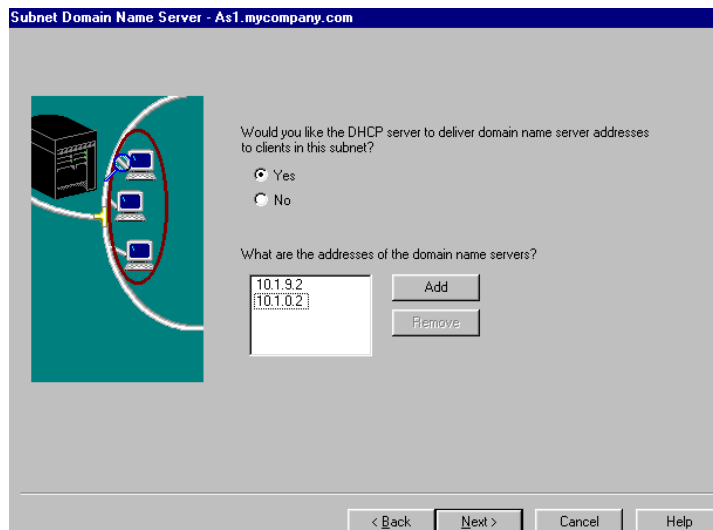


Figure 249. Configuring DNS Information for Clients in Subnet A -- AS1 DHCP Server

Click **Next**.

19. Answer **No** to the question “Would you like the DHCP server to deliver the domain name to the clients in this subnet?”
20. Answer **No** to the question “Would you like to set other options for this subnet?”
Click **Next**.
21. Select *Support any client for this subnet* and click **Next**.
22. Answer **Yes** to the question “Do you want the DHCP server to start when TCP/IP starts?”
23. Answer **No** to the question “Do you want the DHCP server to start now?”
24. At the *New DHCP Configuration Summary* window, click **Finish**.

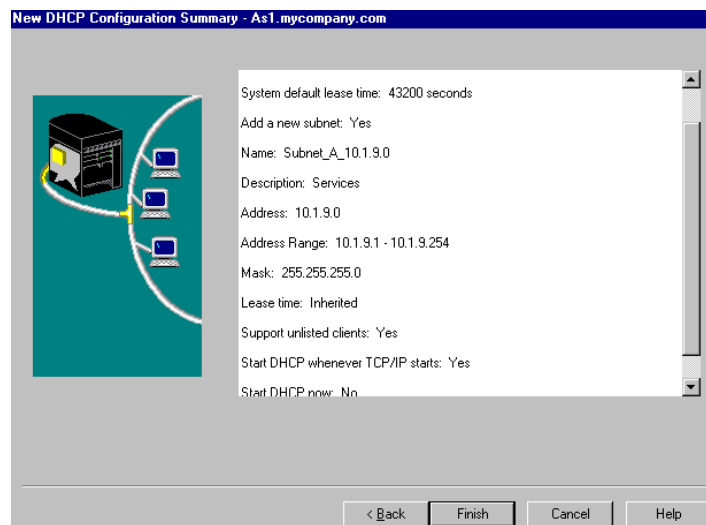


Figure 250. New DHCP Configuration Summary -- Subnet_A_10.1.9.0

25. The DHCP Server Configuration for *As1.mycompany.com* window now looks similar to the one shown in Figure 251.

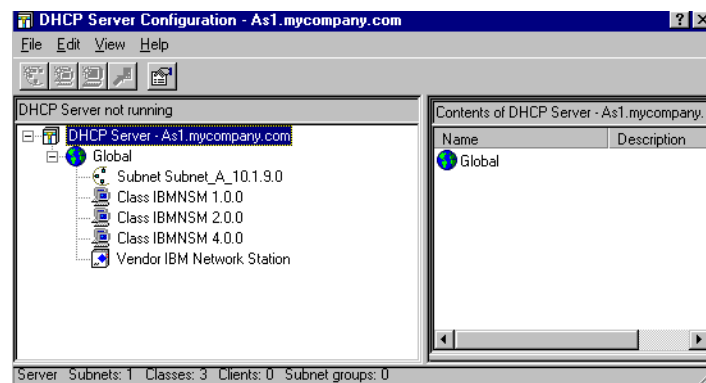


Figure 251. DHCP Server Configuration -- As1.mycompany.com

26. To add the subnet mask option for the subnet, perform the following steps:

1. Right-click **Subnet Subnet_A_10.1.9.0** to open a context menu. Select **Properties**.
2. Click **Options**.
3. Select tag **1**, Subnet mask, and click **Add**.
4. In the Subnet Mask field, specify the following mask for all clients in subnet A:
255.255.255.0
See the example in Figure 252.

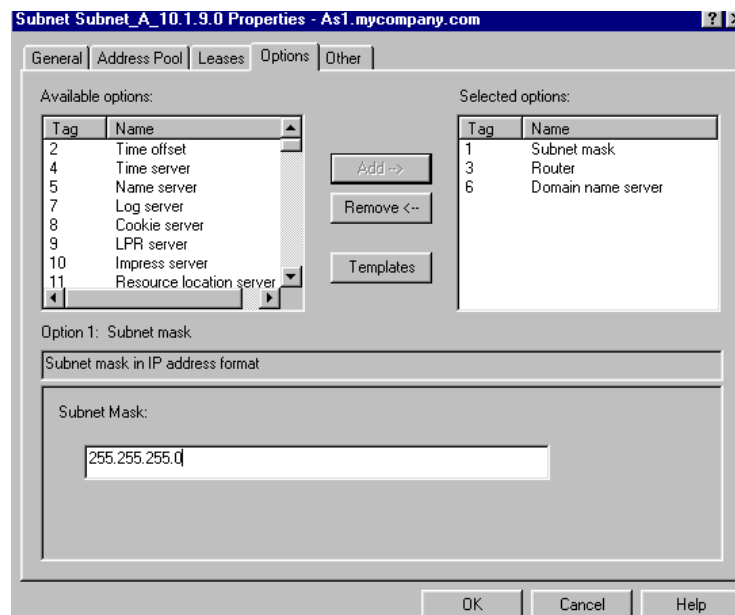


Figure 252. Adding the Subnet Mask Option for Subnet A

You have completed the configuration of Subnet A in DHCP server AS1. Figure 253 on page 290 shows the options configured for Subnet_A_10.1.1.0 on DHCP Server AS1.

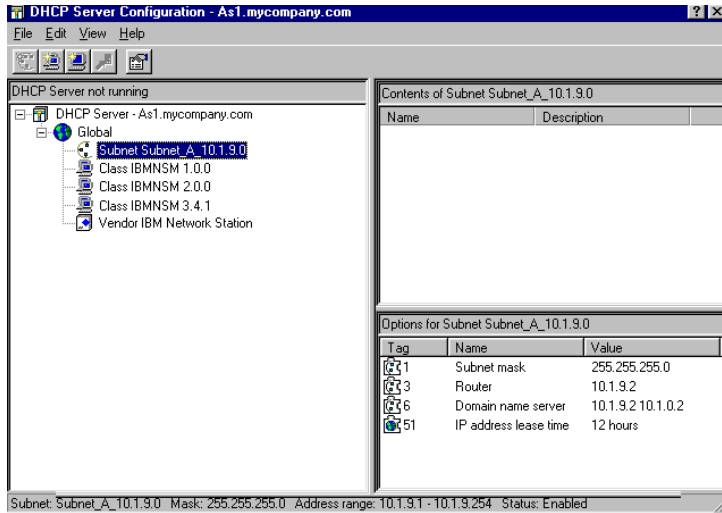


Figure 253. Configured Options for Subnet A -- AS1 DHCP Server

13.3.4 Configuring TCP/IP Interfaces on AS5

To configure the TCP/IP interface, perform the following steps:

1. On an AS/400 command line, type the command:

```
GO CFGTCP
```

Press **ENTER** to display the Configure TCP (CFGTCP) menu.

2. Select option **1** (Work with TCP/IP interfaces) to display the Work with TCP/IP Interfaces display (see Figure 245).
3. Select option **1** to add a TCP/IP interface and specify the TCP/IP address of the host. Press Enter to continue.
4. Add the line description name and the subnet mask for the interface.
5. Press Enter to create the TCP/IP interface. You now see a display similar to the one shown in Figure 254.

Work with TCP/IP Interfaces System: As5

Type options, press Enter.

1=Add 2=Change 4=Remove 5=Display 9=Start 10=End

Opt	Internet Address	Subnet Mask	Line Description	Line Type
	10.1.0.2	255.255.254.0	TRNLINE	*IRLAN
	127.0.0.1	255.0.0.0	*LOOPBACK	*NONE

Bottom

F3=Exit F5=Refresh F6=Print list F11=Display interface status
F12=Cancel F17=Top F18=Bottom

Figure 254. Work with TCP/IP Interfaces -- AS5

6. Press **F11** to view the status of the interface and verify that the status is active.

13.3.5 Configuring DHCP Server Support on AS5

To start the DHCP configuration wizard, perform the following steps:

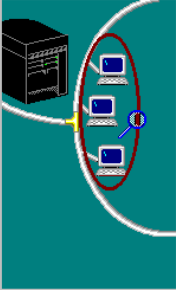
1. Start the AS/400 Operations Navigator.
2. Click the system *As5.mycompany.com* to select it.
3. Double-click **Network**.
4. Double-click **Server**.
5. Double-click **OS/400**.
6. Double-click **DHCP**. This starts the DHCP configuration wizard.
7. Click **Next**.

Note

The sequence of the following steps might be different in your situation, depending on such factors as whether you already have a BootP table on your system and the navigation path you have chosen. Consider this as just an example. The important point is that you understand how to implement the planned configuration.

8. Select the following default lease time for the network that you want this DHCP server (*As5.mycompany.com*) to configure:
12 hours
Click **Next**.
9. Select **Yes** to add a new subnet to the DHCP server. Start configuring *Subnet B -- 10.1.0.0*.
Click **Next**.
10. Answer **No** to the question “*Will this subnet manage twinax devices?*”
Click **Next**.
11. Select **Define subnet based on entire subnet**. Configure the entire subnet range.
12. Specify the information shown in Figure 255. Click **Next**.

Define Subnet Based on an Entire Physical Subnet - As5.mycompany.com



What is the information to define this subnet based on an entire subnet?

Name: Subnet_B_10.1.0.0

Description: Marketing and Manufacturing

Subnet address: 10.1.0.0

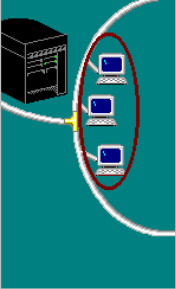
Mask: 255.255.254.0

< Back Next > Cancel Help

Figure 255. Defining Subnet B -- 10.1.0.0 Based on Entire Subnet

13. Exclude the IP addresses of the hosts that you have already configured with permanent IP addresses in this subnet. In this scenario, those hosts are 10.1.0.1 and are reserved for routers if needed in the future -- AS1 (10.1.0.3), AS5 (10.1.0.2), AS9 (10.1.0.9), and LAN Printer (10.1.0.200).

Exclude Addresses - As5.mycompany.com



What addresses, if any, in this subnet should be excluded by this DHCP server?

Example: routers, gateways, and other interfaces defined in the subnet

10.1.0.1
10.1.0.2
10.1.0.3
10.1.0.9
10.1.0.200

Add Remove

< Back Next > Cancel Help

Figure 256. Exclude IP Addresses Already Assigned to Hosts in Subnet B -- 10.1.0.0

Click **Next**.

14. Accept *Inherit the server's default lease time (12 hours)*.
15. Answer **Yes** to the question "*Would you like the DHCP Server to deliver gateway addresses to clients in this subnet?*"
16. Add the gateway IP address that is the AS1 interface on this subnet. In this simple network, the AS/400 system AS1 acts as a gateway between the two

subnets. See Figure 257 on page 293.

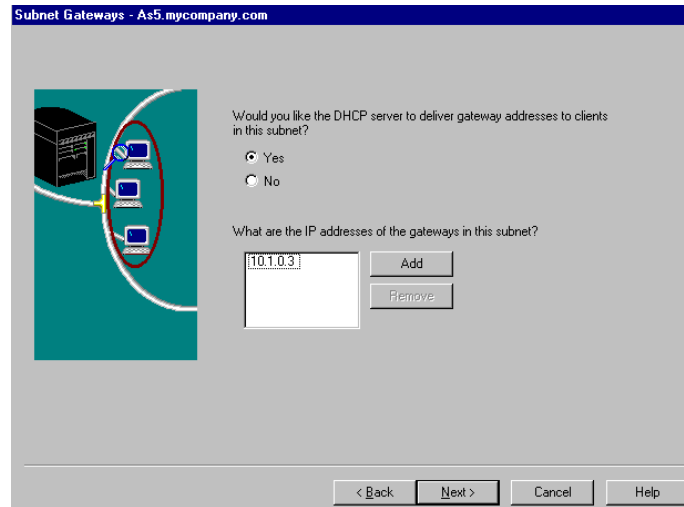


Figure 257. Configuring Subnet B's Gateway Information

Click **Next**.

17. Answer **Yes** to the question "Would you like DHCP to deliver domain name server addresses to clients in this subnet?" In this simple network, the same AS/400 system (AS1) provides DNS services for the whole network. AS5 is the secondary DNS.

18. Add the DNS IP address that is the DNS server on AS1. See Figure 258.

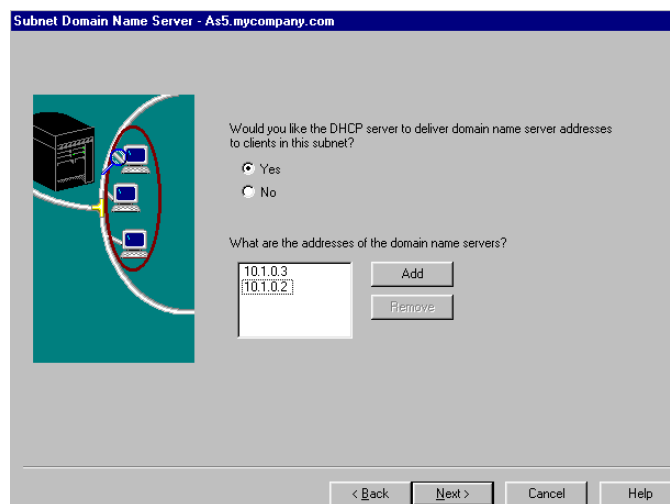


Figure 258. Configuring DNS Information for Clients in Subnet B -- AS5 DHCP Server

Click **Next**.

19. Answer **No** to the question "Would you like the DHCP server to deliver the domain name to the clients in this subnet?"

20. Answer **No** to the question “Would you like to set other options for this subnet?” Click **Next**.
21. Select *Support any client for this subnet* and click **Next**.
22. Answer **Yes** to the question “Do you want the DHCP server to start when TCP/IP starts?”
23. Answer **No** to the question “Do you want the DHCP server to start now?”
24. At the *New DHCP Configuration Summary* window, click **Finish**.

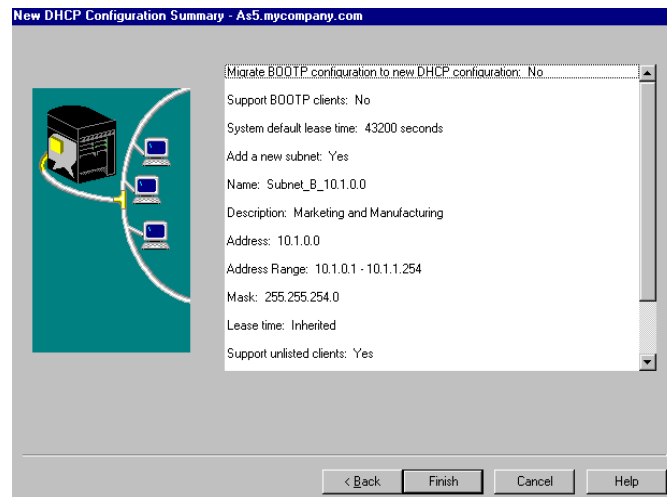


Figure 259. New DHCP Configuration Summary -- Subnet_B_10.1.0.0

25. The DHCP Server Configuration for *As5.mycompany.com* is displayed in a window similar to the one in Figure 260.

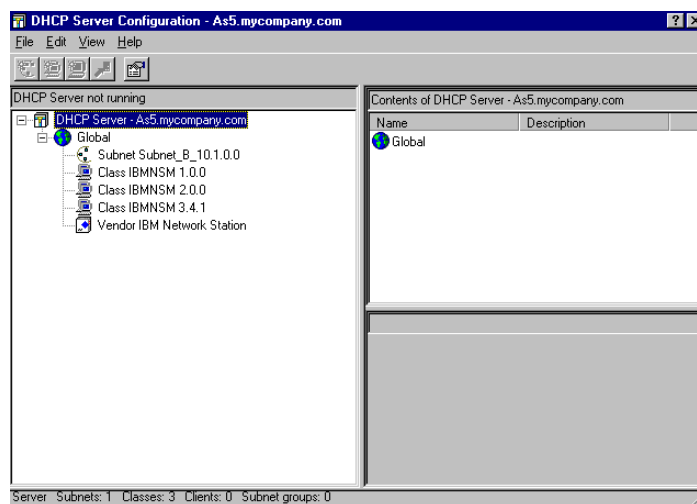


Figure 260. DHCP Server Configuration -- As5.mycompany.com

26. To add the subnet mask option for the subnet, perform the following steps:
 1. Right-click **Subnet Subnet_B_10.1.0.0** to open a context menu. Select **Properties**.
 2. Click **Options**.

3. Select tag 1, Subnet mask, and click **Add**.
4. In the Subnet Mask field, specify the following mask for all clients in subnet B:
255.255.254.0
See Figure 261.

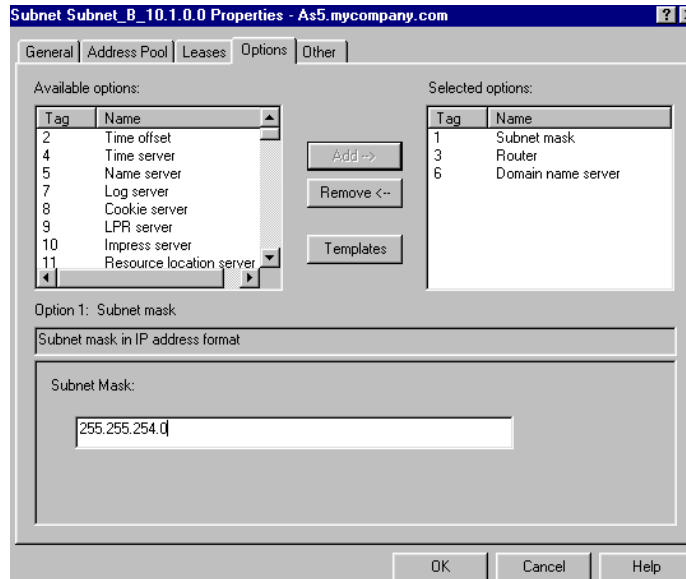


Figure 261. Adding the Subnet Mask Option for Subnet B

You have completed the configuration of Subnet B in DHCP server AS5. Figure 262 shows the options configured for Subnet_B_10.1.0.0 on DHCP server AS5.

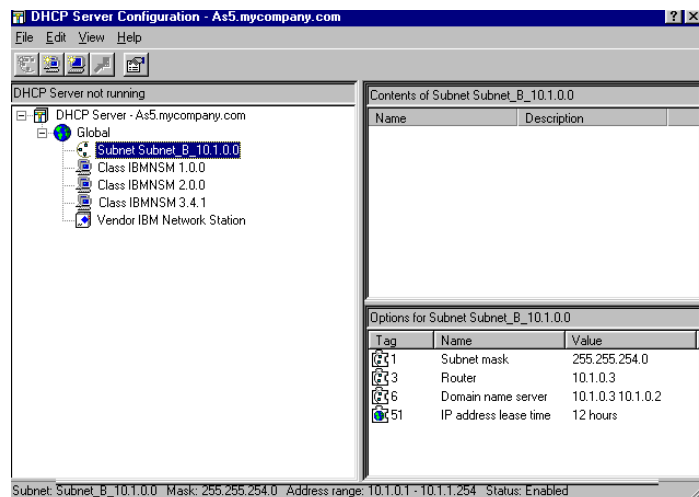


Figure 262. Configured Options for Subnet B -- AS5 DHCP Server

13.3.6 Start the DHCP Server Support on Both Systems

You can start the DHCP server support on the AS/400 system from either the command line interface or the AS/400 Operations Navigator interface.

To start the DHCP server support from the AS/400 command line interface, type `STARTCPSVR *DHCP`. To start the DHCP server support from the AS/400 Operations Navigator interface, perform the following steps:

1. Click the system *As1.mycompany.com* to select it.
2. Double-click **Network**.
3. Double-click **Server**.
4. Double-click **OS/400**.
5. Right-click **DHCP**.
6. Select **Start**.

13.3.7 Configuring DHCP Clients

For DHCP client configuration, refer to Chapter 11.5, “Configuring DHCP Clients” on page 249.

Figure 263 shows the configuration on the C1 client from WINIPCFG.EXE.

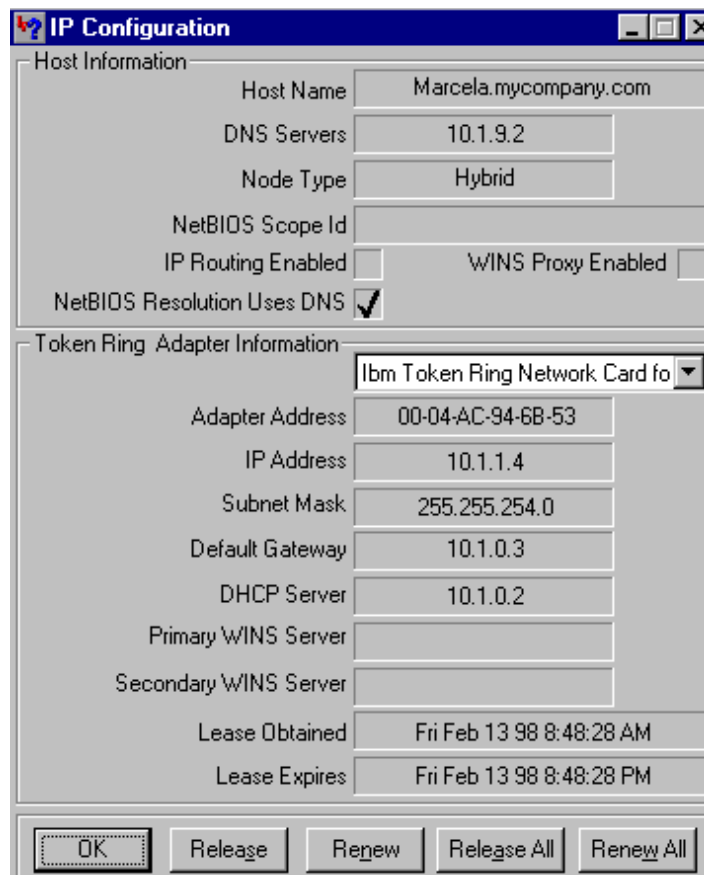


Figure 263. PC Client C1 on Subnet B after Receiving TCP/IP Configuration from DHCP Server AS5

13.3.8 Analyzing the DHCP Logs

After implementing both DHCP servers as described in the previous sections, take a close look at the DHCP logs (*dhcpd.log* file) on both servers. For information on how to create and use the DHCP log, refer to Chapter 17.2, “Starting and Reading the DHCP Logging Utility” on page 407.

By analyzing the DHCP log on AS1, you notice that this server was receiving DHCPDISCOVER packets from clients in subnet B. Even when you do not configure a subnet B range of IP addresses to service from the AS1 DHCP server, AS1’s interface on subnet B (10.1.0.3) received the requests. As expected, the clients on subnet B received no response from AS1. From the AS1 DHCP log, you see the flow generated by the PC client C1 on network B (MAC address 0004ac946b53). Refer to Section 13.3.8.1, “DHCP Log on AS1” on page 297 for an example of such a log.

On the other hand, you see the flow on the AS1 DHCP log that is generated by the Network Station DHCP client on subnet A (MAC address 000e5683796) starting with a DHCPDISCOVER served by AS1. See Section 13.3.8.1, “DHCP Log on AS1” on page 297.

The AS5 DHCP log shows only DHCP packets from subnet B. In the log, include the flow generated by the PC client C1. Refer to Section 13.3.8.2, “DHCP Logs on AS5” on page 300.

13.3.8.1 DHCP Log on AS1

Client PC x’0004ac946b53’ From Interface 10.1.0.3

=====> DHCPDISCOVER with no reply generated <=====

```
02/12 19:51:37 : TRACE: .... legibleRequest:  DHCP msg type DHCPDISCOVER
02/12 19:51:37 : TRACE: .. process_bootrequest: Request is self-consistent
02/12 19:51:37 : TRACE:  Packet from client 6-0x0004ac946b53 was accepted
by user exit verification processing.
```

..... log truncated

```
02/12 19:51:37 : TRACE: ..... locateConfiguredClient: no ipaddress supplied,
returning
```

```
02/12 19:51:37 : INFO: ..... pr_queryAddr:  10.1.0.3 has no
profile in this server
```

..... log truncated

```
02/12 19:51:39 : INFO: ..... pr_queryAddr:  10.1.0.3 has no
profile in this server
```

```
02/12 19:51:39 : OBJERR: ..... am_addressClient:  Failed to query
address portfolio for 10.1.0.3
```

```
02/12 19:51:39 : WARNING:..... am_addressClient:  Request might have
come from a (sub)net for which
```

```
02/12 19:51:39 : WARNING:..... am_addressClient:  this server is not
configured to manage
```

```
02/12 19:51:39 : TRACE: ..... nonvolatilizeAR: function Entered
```

```
02/12 19:51:39 : TRACE: ..... nonvolatilizeCR: function Entered
```

```

02/12 19:51:39 : OBJERR: ..... am_reserve: Failed to address client
6-0x0004ac946b53
02/12 19:51:39 : OBJERR: .... processDISCOVER: Failed to have an address
reserved for 6-0x0004ac946b53
02/12 19:51:39 : ACTION: .. reply_generator: No reply is generated
02/12 19:51:39 : TRACE: .. No reply is to be generated.

```

IBM Network Station x'0000e56h3796' on Interface 10.1.9.2

=====> DHCPDISCOVER from IBM Network Station <=====

```

02/12 19:53:38 : TRACE: .. receiveMailbox: DHCP comm descriptor selected
02/12 19:53:38 : TRACE: .. receiveMailbox: recvfrom got 548 bytes.
02/12 19:53:38 : TRACE: .. receiveMailbox: SELECT_SEMAPHORE
02/12 19:53:38 : TRACE: Size of incoming packet is: 548
02/12 19:53:38 : TRACE: .. process_bootrequest: function entered
02/12 19:53:38 : TRACE: .. process_bootrequest: received packet xid = b03
02/12 19:53:38 : INFO: .... primeOptions: Option: 53, length:1
02/12 19:53:38 : INFO: .... primeOptions: Option: 57, length:2
02/12 19:53:38 : INFO: .... primeOptions: Option: 77, length:12
02/12 19:53:38 : INFO: .... primeOptions: Option: 60, length:19
02/12 19:53:38 : TRACE: .... identifiableClient: function entered
02/12 19:53:38 : TRACE: .... identifiableClient: Using htype, hlen and chaddr
to id client
02/12 19:53:38 : TRACE: .... legibleRequest: function entered
02/12 19:53:38 : TRACE: .... legibleRequest: DHCP msg type DHCPDISCOVER
02/12 19:53:38 : TRACE: Packet from client 6-0x0000e5683796 was accepted
by user exit verification processing.

```

..... log truncated

```

02/12 19:53:39 : TRACE: ..... pr_check_subnet_movement: clue =
10.1.9.2
02/12 19:53:39 : TRACE: ..... pr_check_subnet_movement: Comparing
requested ip 10.1.9.3 & subnetmask 255.255.255.0 against subnet
10.1.9.0

```

..... log truncated

```

02/12 19:53:40 : INFO: ..... am_addressClient: Client
6-0x0000e5683796 had 10.1.9.3 mapped previously

```

..... log truncated

=====> DHCP OFFER to IBM Network Station <=====

```

02/12 19:53:40 : INFO: .. generate_bootreply: Generating a DHCP OFFER
reply

```

..... log truncated

```

02/12 19:53:40 : TRACE: .... setSendWithoutARP: Entering setSendWithoutARP,
value 1.
02/12 19:53:40 : TRACE: .. transmitMailbox: transmitting to (10.1.9.3
#68)

```

02/12 19:53:40 : TRACE: setSendWithoutARP: Entering setSendWithoutARP,
value 0.

=====> DHCPREQUEST from IBM Network Station <=====

02/12 19:53:46 : TRACE: .. receiveMailbox: DHCP comm descriptor selected
02/12 19:53:46 : TRACE: .. receiveMailbox: **recvfrom got 548 bytes.**
02/12 19:53:46 : TRACE: .. receiveMailbox: SELECT_SEMAPHORE
02/12 19:53:46 : TRACE: Size of incoming packet is: 548
02/12 19:53:46 : TRACE: .. process_bootrequest: function entered
02/12 19:53:46 : TRACE: .. process_bootrequest: received packet xid = b03
02/12 19:53:46 : INFO: primeOptions: Option: 53, length:1
02/12 19:53:46 : INFO: primeOptions: Option: 50, length:4 value:
167840003 (0x0a010903)
02/12 19:53:46 : INFO: primeOptions: Option: 54, length:4 value:
167840002 (0x0a010902)
02/12 19:53:46 : INFO: primeOptions: Option: 57, length:2
02/12 19:53:46 : INFO: primeOptions: Option: Parameter Request List,
length:12
02/12 19:53:46 : INFO: primeOptions: Option 66 requested
02/12 19:53:46 : INFO: primeOptions: Option 67 requested
02/12 19:53:46 : INFO: primeOptions: Option 3 requested
02/12 19:53:46 : INFO: primeOptions: Option 6 requested
02/12 19:53:46 : INFO: primeOptions: Option 2 requested
02/12 19:53:46 : INFO: primeOptions: Option 4 requested
02/12 19:53:46 : INFO: primeOptions: Option 12 requested
02/12 19:53:46 : INFO: primeOptions: Option 28 requested
02/12 19:53:46 : INFO: primeOptions: Option 31 requested
02/12 19:53:46 : INFO: primeOptions: Option 49 requested
02/12 19:53:46 : INFO: primeOptions: Option 48 requested
02/12 19:53:46 : INFO: primeOptions: Option 15 requested
02/12 19:53:46 : INFO: primeOptions: Option: 77, length:12
02/12 19:53:46 : INFO: primeOptions: Option: 60, length:19
02/12 19:53:46 : TRACE: identifiableClient: function entered
02/12 19:53:46 : TRACE: identifiableClient: Using htype, hlen and chaddr
to id client
02/12 19:53:46 : TRACE: legibleRequest: function entered
02/12 19:53:46 : TRACE: legibleRequest: **DHCP msg type DHCPREQUEST**
02/12 19:53:46 : TRACE: .. process_bootrequest: Request is self-consistent
02/12 19:53:46 : TRACE: **Packet from client 6-0x0000e5683796 was**
accepted by user exit verification processing.

..... log truncated

=====> DHCPACK to IBM Network Station <=====

02/12 19:53:46 : TRACE: processREQUEST: **Offer was selected by**
client 6-0x0000e5683796
02/12 19:53:46 : TRACE: addressManager: Function entered

..... log truncated

02/12 19:53:46 : TRACE: processREQUEST: **Address 10.1.9.3 has been**
bound to 6-0x0000e5683796
02/12 19:53:46 : INFO: .. generate_bootreply: **Generating a DHCPACK reply**

```

.....log truncated.....
02/12 19:53:46 : TRACE: .... setSendWithoutARP: Entering setSendWithoutARP,
value 1.
02/12 19:53:46 : TRACE: .. transmitMailbox: transmitting to (10.1.9.3
#68)
02/12 19:53:46 : TRACE: .... setSendWithoutARP: Entering setSendWithoutARP,
value 0.
..... log truncated.....

```

13.3.8.2 DHCP Logs on AS5

Client PC x'0004ac946b53' From Interface 10.1.0.2

=====> DHCPDISCOVER from PC <=====

```

02/12 19:54:02 : TRACE: .. receiveMailbox: DHCP comm descriptor selected
02/12 19:54:02 : TRACE: .. receiveMailbox: recvfrom got 300 bytes.
02/12 19:54:02 : TRACE: .. receiveMailbox: SELECT_SEMAPHORE
02/12 19:54:02 : TRACE: Size of incoming packet is: 300
02/12 19:54:02 : TRACE: .. process_bootrequest: function entered
02/12 19:54:02 : TRACE: .. process_bootrequest: received packet xid = 789f789f
02/12 19:54:02 : INFO: .... primeOptions: Option: 53, length:1
02/12 19:54:02 : INFO: .... primeOptions: Option: 61, length:7
02/12 19:54:02 : INFO: .... primeOptions: Option: 50, length:4 value:
167837956 (0x0a010104)
02/12 19:54:02 : INFO: .... primeOptions: Option: 12, length:5
02/12 19:54:02 : TRACE: .... identifiableClient: function entered
02/12 19:54:02 : TRACE: .... identifiableClient: DHCP option
Client-identifier specified
02/12 19:54:02 : TRACE: .... legibleRequest: function entered
02/12 19:54:02 : TRACE: .... legibleRequest: DHCP msg type DHCPDISCOVER
02/12 19:54:02 : TRACE: .. process_bootrequest: Request is self-consistent
02/12 19:54:02 : TRACE: Packet from client 6-0x0004ac946b53 was
accepted by user exit verification processing.

```

```

..... log truncated .....

02/12 19:54:02 : TRACE: ..... pr_queryAddr: clue = [0x0a010104], 167837956
02/12 19:54:02 : TRACE: ..... pr_queryAddr: netaddr = 10.0.0.0
02/12 19:54:02 : TRACE: ..... pr_queryAddr: hostaddr = 0.1.1.4
02/12 19:54:02 : TRACE: ..... locateConfiguredClient: look for client match
in this subnet

```

```

..... log truncated .....

```

=====> DHCP OFFER to PC <=====

```

02/12 19:54:02 : INFO: generate_bootreply: Generating a DHCP OFFER reply

..... log truncated .....

02/12 19:54:02 : TRACE: .... setSendWithoutARP: Entering setSendWithoutARP,
value 1.
02/12 19:54:02 : TRACE: .. transmitMailbox: transmitting to (10.1.1.4
#68)

```

02/12 19:54:02 : TRACE: setSendWithoutARP: Entering setSendWithoutARP,
value 0.

=====> DHCPREQUEST from PC <=====

02/12 19:54:02 : TRACE: .. receiveMailbox: DHCP comm descriptor selected
02/12 19:54:02 : TRACE: .. receiveMailbox: **recvfrom got 300 bytes.**
02/12 19:54:02 : TRACE: .. receiveMailbox: SELECT_SEMAPHORE
02/12 19:54:02 : TRACE: Size of incoming packet is: 300
02/12 19:54:02 : TRACE: .. process_bootrequest: function entered
02/12 19:54:02 : TRACE: .. process_bootrequest: received packet xid = b7a0b7a0
02/12 19:54:02 : INFO: primeOptions: Option: 53, length:1
02/12 19:54:02 : INFO: primeOptions: Option: 61, length:7
02/12 19:54:02 : INFO: primeOptions: Option: 50, length:4 value:
167837956 (0x0a010104)
02/12 19:54:02 : INFO: primeOptions: Option: 54, length:4 value:
167837698 (0x0a010002)
02/12 19:54:02 : INFO: primeOptions: Option: 12, length:5
02/12 19:54:02 : INFO: primeOptions: Option: Parameter Request List,
length:7
02/12 19:54:02 : INFO: primeOptions: Option 1 requested
02/12 19:54:02 : INFO: primeOptions: Option 3 requested
02/12 19:54:02 : INFO: primeOptions: Option 15 requested
02/12 19:54:02 : INFO: primeOptions: Option 6 requested
02/12 19:54:02 : INFO: primeOptions: Option 44 requested
02/12 19:54:02 : INFO: primeOptions: Option 46 requested
02/12 19:54:02 : INFO: primeOptions: Option 47 requested
02/12 19:54:02 : INFO: primeOptions: Option: 43, length:4
02/12 19:54:02 : TRACE: identifiableClient: function entered
02/12 19:54:02 : TRACE: identifiableClient: DHCP option
Client-identifier specified
02/12 19:54:02 : TRACE: legibleRequest: function entered
02/12 19:54:02 : TRACE: legibleRequest: **DHCP msg type DHCPREQUEST**
02/12 19:54:02 : TRACE: .. process_bootrequest: Request is self-consistent
02/12 19:54:03 : TRACE: **Packet from client 6-0x0004ac946b53 was**
accepted by user exit verification processing.

..... log truncated

02/12 19:54:03 : TRACE: ..02/12 19:54:03 : TRACE: pr_queryAddr: clue
= [0x0a010002], 167837698
02/12 19:54:03 : TRACE: pr_queryAddr: netaddr = 10.0.0.0
02/12 19:54:03 : TRACE: pr_queryAddr: hostaddr = 0.1.0.2
02/12 19:54:03 : TRACE: pr_check_subnet_movement: Comparing requested
ip 10.1.1.4 & subnetmask 255.255.254.0 against subnet 10.1.0.0

..... log truncated

02/12 19:54:03 : TRACE: locateConfiguredClient: look for client match
in this subnet
02/12 19:54:03 : TRACE: locateConfiguredClient: look for client match
in global clients
02/12 19:54:03 : TRACE: processREQUEST: **Offer was selected by**
client 6-0x0004ac946b53

..... log truncated

```
02/12 19:54:03 : TRACE: .... processREQUEST: Address 10.1.1.4 has been
bound to 6-0x0004ac946b53
```

```
..... log truncated .....
```

```
=====> DHCPACK to a PC <=====
```

```
02/12 19:54:03 : INFO: .. generate_bootreply: Generating a DHCPACK reply
```

```
..... log truncated .....
```

```
02/12 19:54:03 : TRACE: .... setSendWithoutARP: Entering setSendWithoutARP,
value 1.
```

```
02/12 19:54:03 : TRACE: .. transmitMailbox: transmitting to (10.1.1.4
#68)
```

```
02/12 19:54:03 : TRACE: .... setSendWithoutARP: Entering setSendWithoutARP,
value 0.
```

```
02/12 19:54:03 : TRACE: .. processNotifyBindUsrExits: function entered
```

```
02/12 19:54:03 : TRACE: .. processNotifyBindUsrExits: Initiating user exit
program ADDRESS-BIND notification processing.
```

13.3.9 Conclusion

After analyzing the logs, you can determine that a better approach is having the AS1 function as the DHCP server for the whole network, servicing both subnets. Since AS1 is connected to both the networks and there is no way to shut down AS1's interface on subnet B from listening to DHCP requests, it is more productive to have AS1 servicing the whole network.

Subnet B was configured on the AS1 DHCP server as described in Section 13.3.5, "Configuring DHCP Server Support on AS5" on page 291.

This scenario did not implement a DHCP backup server. One (provided you have enough IP addresses available) option is to configure a range of IP addresses on AS1 to service the clients on subnet B as a primary DHCP server. You can configure another range of subnet IP addresses on AS5 to use it as a backup DHCP server only for subnet B in the event that AS1 becomes unavailable.

Note

You cannot configure the same range of IP addresses for the same subnet in the primary and back-up DHCP servers. Even if you start DHCP services on the back-up AS/400 system only if the primary server is unavailable, there is no control over what IP addresses from the range are already in use. The only way to guarantee that the back-up DHCP server does not give away already leased IP addresses is to configure totally different IP address ranges in both DHCP servers.

13.4 Configuring Subnet B on AS1

To add subnet B to the DHCP server configuration on AS1, perform the following steps:

1. Use Operations Navigator to get to the DHCP configuration on AS1.
2. Right-click **Global** to open a context menu.
3. Select **Add new subnet** (see Figure 264).

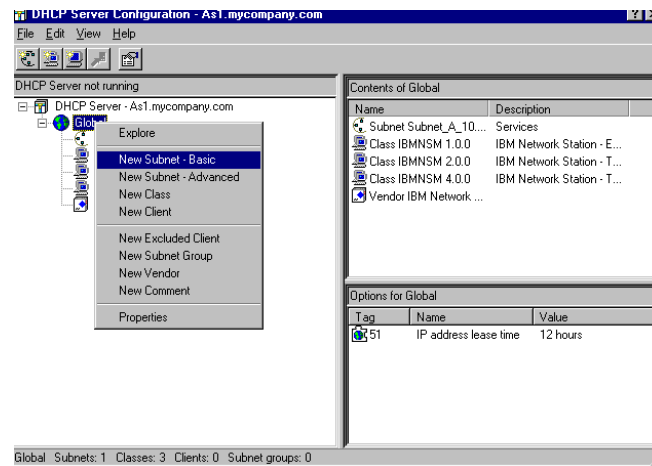


Figure 264. Adding Subnet B to AS1

4. The *New DHCP subnet wizards* window displays. Click **Next**.
5. Answer **No** to the question “*Will this subnet manage twinax devices?*” Click **Next**.
6. Select **Define subnet based on entire subnet**. Click **Next**.
7. Specify your subnet information as shown in Figure 265. Click **Next**.

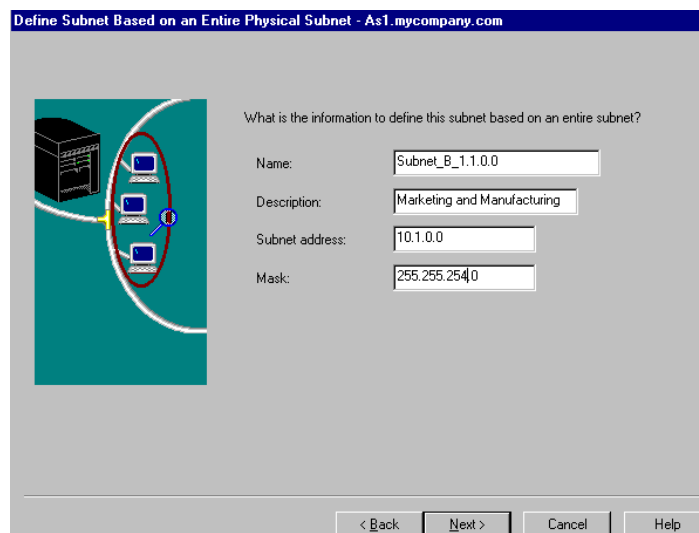


Figure 265. Define Subnet B -- 10.1.0.0 Based on Entire Subnet

8. Exclude the IP addresses of the hosts in this subnet that you have already configured, as shown in Figure 244 on page 279. Specify the values shown in Figure 266.

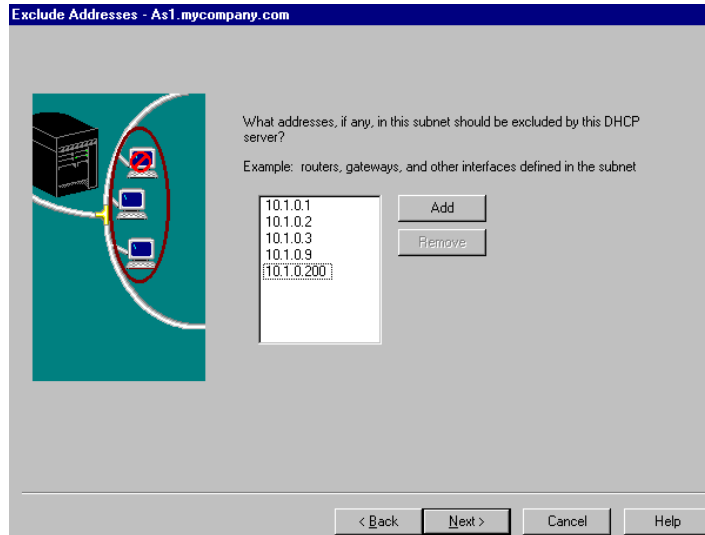


Figure 266. Exclude IP Addresses Already Assigned to Hosts on Subnet B

9. Accept *Inherit the server's default lease time (12 hours)*.
10. Answer **Yes** to the question "Would you like the DHCP server to deliver gateway addresses to clients in this subnet?"
11. Specify the gateway IP address, which is the AS1 interface on this subnet (see Figure 267).

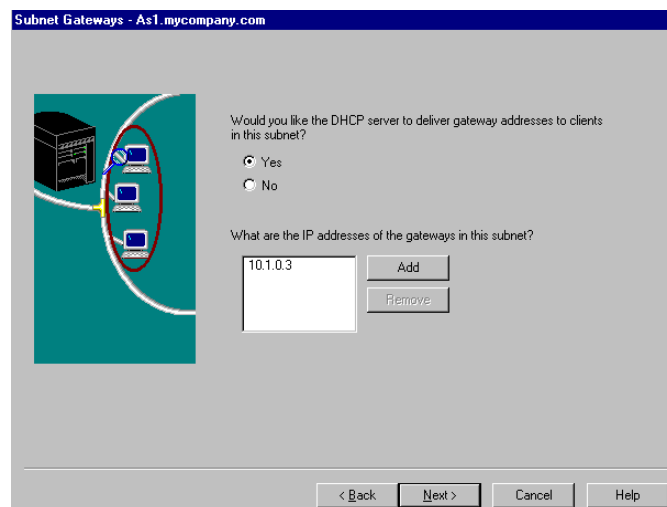


Figure 267. Configuring Subnet B Gateway Information

Click **Next**.

12. Answer **Yes** to the question “*Would you like the DHCP server to deliver domain name server addresses to the clients in this subnet?*” AS1 is the DNS server in the sample network.
13. Add the DNS IP address, which is the DNS server running on AS1 and AS5 as a secondary DNS (see Figure 268).

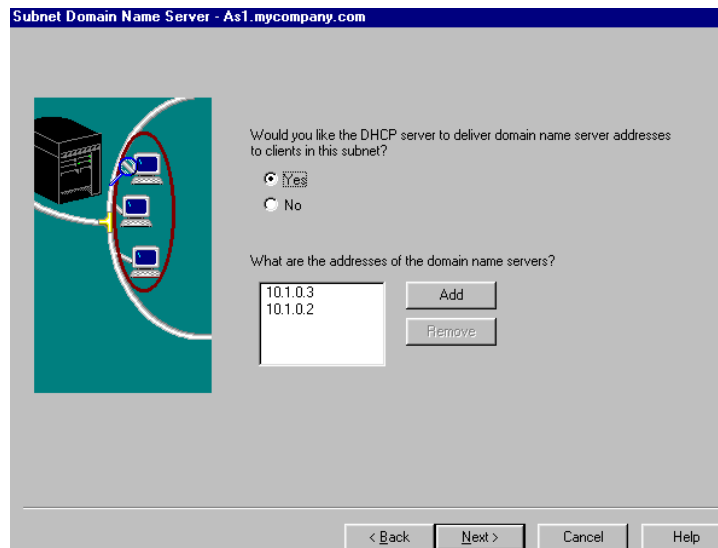


Figure 268. Configuring DNS Information for Clients in Subnet B

Click **Next**.

14. Answer **No** to the question “*Would you like the DHCP server to deliver domain name server addresses to the clients in this subnet?*”

Click **Next**.

15. Answer **No** to the question “*Would you like to set other options for this subnet?*”

16. Answer **Yes** to the question “*Do you want the DHCP server to start when TCP/IP starts?*”

17. Answer **No** to the question “*Do you want the DHCP server to start now?*”

18. At the *New DHCP Subnet Summary* window, click **Finish**.

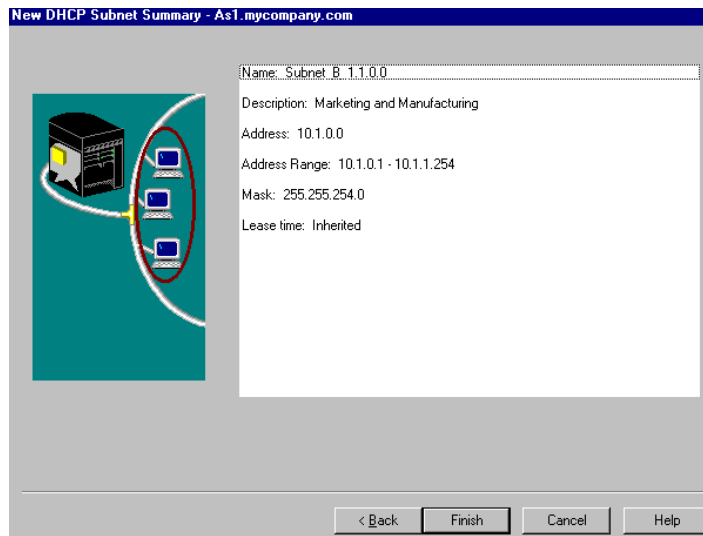


Figure 269. *New DHCP Subnet Summary -- Subnet B on AS1*

19. To add the subnet mask option for the subnet, perform the following steps:

1. Right-click Subnet Subnet_B_10.1.0.0 to open the context menu. Select **Properties**.
2. Click **Options**.
3. Select tag **1**, Subnet mask, and click **Add**.
4. In the Subnet Mask field, specify the following mask for all clients in subnet B:
255.255.254.0

See Figure 270.

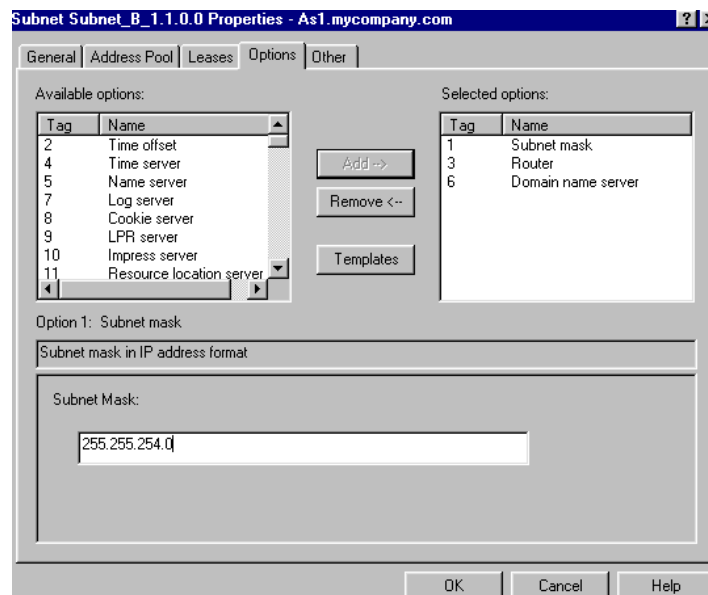


Figure 270. *Adding the Subnet Mask Option for Subnet B*

20. The DHCP server configuration window for *As1.mycompany.com* is displayed. Figure 271 shows subnet B options on the AS1 DHCP server.

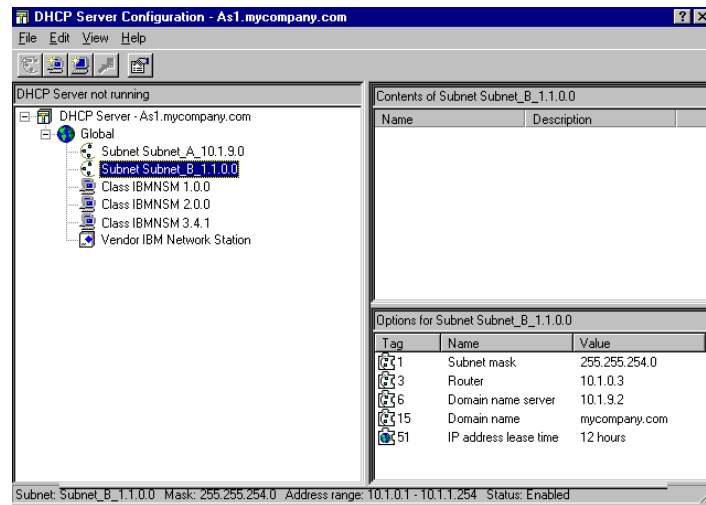


Figure 271. DHCP Server -- As1.mycompany.com -- Subnet B Options

Figure 272 shows the configuration of the PC client C1 on subnet B after receiving the configuration options from AS1.

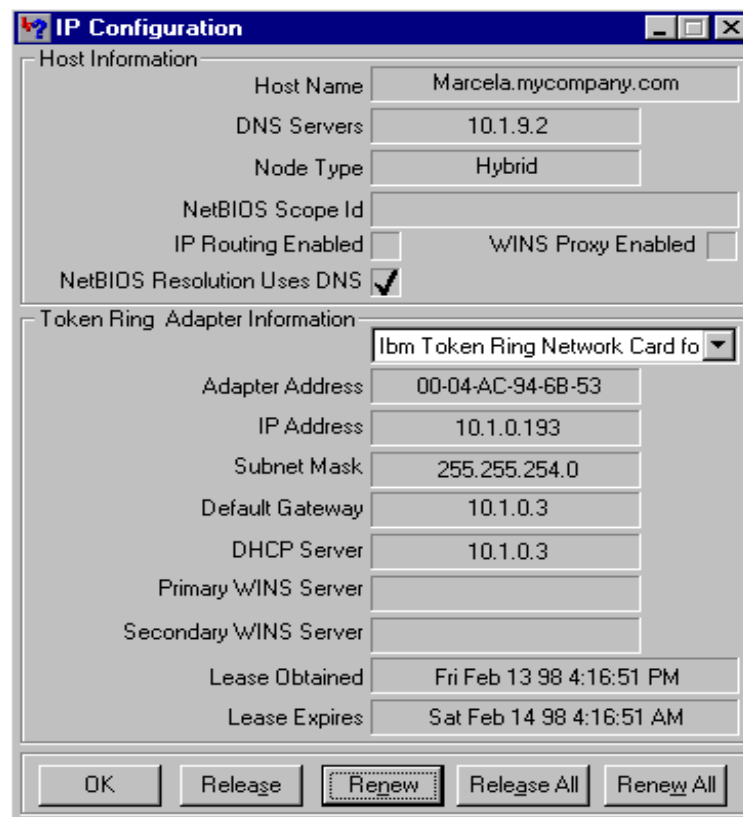


Figure 272. Client C1 on Subnet B after Receiving TCP/IP Configuration from DHCP Server AS1

Section 13.4.0.1, "DHCP Log on AS1" on page 308, shows the DHCP Log in AS1 after configuring subnet B. This time, AS1 serves C1 through the 10.1.0.3 interface.

13.4.0.1 DHCP Log on AS1

Client PC x'0004ac946b53' From Interface 10.1.0.3

=====> DHCP Server Startup <=====

..... log truncated

: INFO: **DHCP Server Initialized** at Fri Feb 13 16:05:47 1998Ö

==> DHCPDISCOVER from the PC client x'0004ac946b53' <=====

```
02/13 16:10:08 : TRACE: .. receiveMailbox: DHCP comm descriptor selected
02/13 16:10:08 : TRACE: .. receiveMailbox: recvfrom got 300 bytes.
02/13 16:10:08 : TRACE: .. receiveMailbox: SELECT_SEMAPHORE
02/13 16:10:08 : TRACE: Size of incoming packet is: 300
02/13 16:10:08 : TRACE: .. process_bootrequest: function entered
02/13 16:10:08 : TRACE: .. process_bootrequest: received packet xid = 85a085a
02/13 16:10:08 : INFO: .... primeOptions: Option: 53, length:1
02/13 16:10:08 : INFO: .... primeOptions: Option: 61, length:7
02/13 16:10:08 : INFO: .... primeOptions: Option: 50, length:4 value:
167837889 (0x0a0100c1)
02/13 16:10:08 : INFO: .... primeOptions: Option: 12, length:5
02/13 16:10:08 : TRACE: .... identifiableClient: function entered
02/13 16:10:08 : TRACE: .... identifiableClient: DHCP option
Client-identifier specified
02/13 16:10:08 : TRACE: .... legibleRequest: function entered
02/13 16:10:08 : TRACE: .... legibleRequest: DHCP msg type DHCPDISCOVER
02/13 16:10:08 : TRACE: .. process_bootrequest: Request is self-consistent
02/13 16:10:08 : TRACE: Packet from client 6-0x0004ac946b53 was
accepted by user exit verification processing.
02/13 16:10:08 : TRACE: .. reply_generator: function entered
02/13 16:10:08 : TRACE: .... processDISCOVER: function entered
02/13 16:10:08 : TRACE: ..... locateExchange: function entered
02/13 16:10:08 : TRACE: ..... newExchangeBlock: function entered
02/13 16:10:08 : TRACE: ..... locateConfiguredClient: function entered
02/13 16:10:08 : TRACE: ..... locateConfiguredClient: no ipaddress supplied,
returning
02/13 16:10:08 : TRACE: ..... addressManager: Function entered
02/13 16:10:08 : TRACE: ..... am_queryClient: Function entered
02/13 16:10:08 : TRACE: ..... am_queryMapper: function Entered
02/13 16:10:08 : TRACE: ..... locateClientRecord: function Entered
02/13 16:10:08 : TRACE: ..... locateClientRecord: Located client
6-0x0004ac946b53 in client records
```

```

02/13 16:10:08 : WARNING:..... am_queryMapper: Client 6-0x0004ac946b53
has no address mapped to it, status=2
02/13 16:10:08 : TRACE: ..... locateConfiguredClient: function entered
02/13 16:10:08 : TRACE: ..... pr_queryAddr: function entered
02/13 16:10:08 : TRACE: ..... pr_queryAddr: clue = [0x0a010003],
167837699
02/13 16:10:08 : TRACE: ..... pr_queryAddr: netaddr = 10.0.0.0
02/13 16:10:08 : TRACE: ..... pr_queryAddr: hostaddr = 0.1.0.3
02/13 16:10:08 : TRACE: ..... locateConfiguredClient: look for client
match in this subnet
02/13 16:10:08 : TRACE: ..... locateConfiguredClient: look for client
match in global clients
02/13 16:10:08 : TRACE: ..... am_queryClient: Client 6-0x0004ac946b53 is
known to address mapper, status=2
02/13 16:10:08 : TRACE: .... processDISCOVER: binder.subnet [0x00000000]
02/13 16:10:08 : TRACE: .... processDISCOVER: AM_STATUS_AUTHENTIC
02/13 16:10:08 : TRACE: ..... isAddressInUse: Function Entered
02/13 16:10:10 : TRACE: ..... isAddressInUse: IP address 10.1.0.193, not
in use. rc=-26758468
02/13 16:10:10 : TRACE: ..... pr_check_subnet_movement: function entered
02/13 16:10:10 : TRACE: ..... pr_check_subnet_movement: clue = 10.1.0.3
02/13 16:10:10 : TRACE: ..... pr_queryAddr: function entered
02/13 16:10:10 : TRACE: ..... pr_queryAddr: clue = [0x0a010003], 167837699
02/13 16:10:10 : TRACE: ..... pr_queryAddr: netaddr = 10.0.0.0
02/13 16:10:10 : TRACE: ..... pr_queryAddr: hostaddr = 0.1.0.3
02/13 16:10:10 : TRACE: ..... pr_check_subnet_movement: Comparing
requested ip 10.1.0.193 & subnetmask 255.255.254.0 against subnet
10.1.0.0
02/13 16:10:10 : TRACE: ..... addressManager: Function entered

..... log truncated
.....

02/13 16:10:10 : TRACE: ..... locateAddressRecord: function Entered
02/13 16:10:10 : INFO: ..... am_addressClient: Client
6-0x0004ac946b53 suggested 10.1.0.193 is in range
02/13 16:10:10 : INFO: ..... am_addressClient: Client
6-0x0004ac946b53 had no previous mapping, getting one
02/13 16:10:10 : TRACE: ..... indexAddressRecord: function Entered
02/13 16:10:10 : TRACE: ..... nonvolatilizeAR: function Entered
02/13 16:10:10 : TRACE: ..... nonvolatilizeCR: function Entered
02/13 16:10:10 : ACTION: .... processDISCOVER: Address 10.1.0.193 has
been reserved
02/13 16:10:10 : TRACE: ..... pr_new_menu : Function entered
02/13 16:10:10 : TRACE: ..... pr_fill_menu_net: function entered
02/13 16:10:10 : TRACE: ..... pr_queryAddr: function entered
02/13 16:10:10 : TRACE: ..... pr_queryAddr: clue = [0x0a0100c1], 167837889
02/13 16:10:10 : TRACE: ..... pr_queryAddr: netaddr = 10.0.0.0
02/13 16:10:10 : TRACE: ..... pr_queryAddr: hostaddr = 0.1.0.193
02/13 16:10:10 : TRACE: ..... locateAddressRecord: function Entered

..... log truncated
.....

02/13 16:10:10 : TRACE: ..... newReplyPacket: function entered
02/13 16:10:10 : TRACE: ..... enqueueExchange: function entered
02/13 16:10:10 : TRACE: .. generate_bootreply: function entered

```

====> Generating a DHCP OFFER to the client x'0004ac946b53' <====

```
02/13 16:10:10 : INFO:   generate_bootreply: Generating a DHCP OFFER reply
02/13 16:10:10 : TRACE:   .... locateConfiguredClient: function entered
02/13 16:10:10 : TRACE:   ..... pr_queryAddr: function entered
02/13 16:10:10 : TRACE:   ..... pr_queryAddr: clue = [0x0a0100c1], 167837889
02/13 16:10:10 : TRACE:   ..... pr_queryAddr: netaddr = 10.0.0.0
02/13 16:10:10 : TRACE:   ..... pr_queryAddr: hostaddr = 0.1.0.193
02/13 16:10:10 : TRACE:   .... locateConfiguredClient: look for client match in
this subnet
02/13 16:10:10 : TRACE:   .... locateConfiguredClient: look for client match in
global clients
```

```
..... log truncated
.....
```

```
02/13 16:10:10 : TRACE:   .... pr_queryAddr: function entered
02/13 16:10:10 : TRACE:   .... pr_queryAddr: clue = [0x0a0100c1], 167837889
02/13 16:10:10 : TRACE:   .... pr_queryAddr: netaddr = 10.0.0.0
02/13 16:10:10 : TRACE:   .... pr_queryAddr: hostaddr = 0.1.0.193
02/13 16:10:10 : TRACE:   .... locateAddressRecord: function Entered
02/13 16:10:10 : TRACE:   .... setSendWithoutARP: Entering setSendWithoutARP,
value 1.
02/13 16:10:10 : TRACE: transmitMailbox: transmitting to (10.1.0.193 #68)
02/13 16:10:10 : TRACE:   .... setSendWithoutARP: Entering setSendWithoutARP,
value 0.
```

=====> DHCP REQUEST from the client x'0004ac946b53' <=====

```
02/13 16:10:11 : TRACE:   .. receiveMailbox: DHCP comm descriptor selected
02/13 16:10:11 : TRACE:   .. receiveMailbox: recvfrom got 300 bytes.
02/13 16:10:11 : TRACE:   .. receiveMailbox: SELECT_SEMAPHORE
02/13 16:10:11 : TRACE:   Size of incoming packet is: 300
02/13 16:10:11 : TRACE:   .. process_bootrequest: function entered
02/13 16:10:11 : TRACE:   .. process_bootrequest: received packet xid = b5b0b5b
02/13 16:10:11 : INFO:   .... primeOptions: Option: 53, length:1
02/13 16:10:11 : INFO:   .... primeOptions: Option: 61, length:7
02/13 16:10:11 : INFO:   .... primeOptions: Option: 50, length:4 value:
167837889 (0x0a0100c1)
02/13 16:10:11 : INFO:   .... primeOptions: Option: 54, length:4 value:
167837699 (0x0a010003)
02/13 16:10:11 : INFO:   .... primeOptions: Option: 12, length:5
02/13 16:10:11 : INFO:   .... primeOptions: Option: Parameter Request List,
length:7
02/13 16:10:11 : INFO:   .... primeOptions: Option 1 requested
02/13 16:10:11 : INFO:   .... primeOptions: Option 3 requested
02/13 16:10:11 : INFO:   .... primeOptions: Option 15 requested
02/13 16:10:11 : INFO:   .... primeOptions: Option 6 requested
02/13 16:10:11 : INFO:   .... primeOptions: Option 44 requested
02/13 16:10:11 : INFO:   .... primeOptions: Option 46 requested
02/13 16:10:11 : INFO:   .... primeOptions: Option 47 requested
02/13 16:10:11 : INFO:   .... primeOptions: Option: 43, length:4
02/13 16:10:11 : TRACE:   .... identifiableClient: function entered
02/13 16:10:11 : TRACE:   .... identifiableClient: DHCP option
Client-identifier specified
02/13 16:10:11 : TRACE:   .... legibleRequest: function entered
02/13 16:10:11 : TRACE:   .... legibleRequest: DHCP msg type DHCPREQUEST
```

```

02/13 16:10:11 : TRACE: .. process_bootrequest: Request is self-consistent
02/13 16:10:11 : TRACE: Packet from client 6-0x0004ac946b53 was
accepted by user exit verification processing.
02/13 16:10:11 : TRACE: .. reply_generator: function entered
02/13 16:10:11 : TRACE: .... processREQUEST: function entered

```

```

..... log truncated
.....

```

```

02/13 16:10:11 : TRACE: ..... pr_queryAddr: clue = [0x0a010003], 167837699
02/13 16:10:11 : TRACE: ..... pr_queryAddr: netaddr = 10.0.0.0
02/13 16:10:11 : TRACE: ..... pr_queryAddr: hostaddr = 0.1.0.3
02/13 16:10:11 : TRACE: ..... pr_check_subnet_movement: Comparing
requested ip 10.1.0.193 & subnetmask 255.255.254.0 against subnet
10.1.0.0
02/13 16:10:11 : TRACE: ..... locateConfiguredClient: function entered

```

```

..... log truncated
.....

```

=====> Offer was selected by the Client x'0004ac946b53' <=====

```

02/13 16:10:11 : TRACE: .... processREQUEST: Offer was selected by
client 6-0x0004ac946b53
02/13 16:10:11 : TRACE: ..... addressManager: Function entered
02/13 16:10:11 : TRACE: ..... am_commit: Function entered
02/13 16:10:11 : TRACE: ..... locateClientRecord: function Entered
02/13 16:10:11 : TRACE: ..... locateClientRecord: Located client
6-0x0004ac946b53 in client records
02/13 16:10:11 : TRACE: ..... indexAddressRecord: function Entered
02/13 16:10:11 : TRACE: ..... nonvolatilizeAR: function Entered
02/13 16:10:11 : TRACE: ..... nonvolatilizeCR: function Entered
02/13 16:10:11 : TRACE: .... processREQUEST: Address 10.1.0.193 has been
bound to 6-0x0004ac946b53
02/13 16:10:11 : TRACE: ..... pr_new_menu : Function entered
02/13 16:10:11 : TRACE: ..... pr_fill_menu_net: function entered
02/13 16:10:12 : TRACE: ..... pr_queryAddr: function entered
02/13 16:10:12 : TRACE: ..... pr_queryAddr: clue = [0x0a0100c1], 167837889
02/13 16:10:12 : TRACE: ..... pr_queryAddr: netaddr = 10.0.0.0
02/13 16:10:12 : TRACE: ..... pr_queryAddr: hostaddr = 0.1.0.193
02/13 16:10:12 : TRACE: ..... locateAddressRecord: function Entered

```

```

..... log truncated
.....

```

```

02/13 16:10:12 : TRACE: ..... pr_queryAddr: clue = [0x0a0100c1],
167837889
02/13 16:10:12 : TRACE: ..... pr_queryAddr: netaddr = 10.0.0.0
02/13 16:10:12 : TRACE: ..... pr_queryAddr: hostaddr = 0.1.0.193
02/13 16:10:12 : TRACE: ..... locateConfiguredClient: look for client
match in this subnet
02/13 16:10:12 : TRACE: ..... locateConfiguredClient: look for client
match in global clients
02/13 16:10:12 : TRACE: ..... pr_queryAddr: function entered
02/13 16:10:12 : TRACE: ..... pr_queryAddr: clue = [0x0a0100c1], 167837889

```

```

..... log truncated
.....

02/13 16:10:12 : TRACE: ..... newReplyPacket: function entered

=====> DHCPACK to the client x'0004ac946b53' <=====

02/13 16:10:12 : TRACE: .. generate_bootreply: function entered
02/13 16:10:12 : INFO: .. generate_bootreply: Generating a DHCPACK reply
02/13 16:10:12 : TRACE: .... locateConfiguredClient: function entered

..... log truncated
.....

002/13 16:10:12 : TRACE: .... setSendWithoutARP: Entering setSendWithoutARP,
value 1.
02/13 16:10:12 : TRACE: .. transmitMailbox: transmitting to (10.1.0.193
#68)
02/13 16:10:12 : TRACE: .... setSendWithoutARP: Entering setSendWithoutARP,
value 0.
02/13 16:10:12 : TRACE: .. processNotifyBindUsrExits: function entered
02/13 16:10:12 : TRACE: .. processNotifyBindUsrExits: Initiating user exit
program ADDRESS-BIND notification processing.
02/13 16:10:45 : TRACE: .. event_timeout: function entered
02/13 16:10:45 : TRACE: .. event_timeout: Garbage collection (every 60
seconds).
02/13 16:10:45 : TRACE: .... am_removeExpiredLeases: function Entered
02/13 16:10:45 : TRACE: .... update_statistic_list: function Entered

```

13.5 Summary

This scenario showed through the DHCP logs that a DHCP server listens for DHCP packets on all its interfaces. This is true even if it is not configured to serve that range of IP addresses from which the DHCP packets are coming.

You configured two DHCP servers, one per subnet in our network. You then changed to a single DHCP server that was connected to both subnets. This server serviced the whole network by configuring a range of IP addresses on each subnet.

Although you did not implement DHCP server backup in this scenario, it discussed how to use AS5 to back up subnet B.

Chapter 14. Multiple Subnets, DHCP Servers, and Relay Agents

As your network grows, the number of subnets grows with it. You can still keep centralized configuration administration by using BOOTP/DHCP Relay Agent support in routers or AS/400 systems. This chapter shows you how to configure the AS/400 BOOTP/DHCP Relay Agent and how it works together with the AS/400 DHCP server. This chapter also introduces a Microsoft NT BOOTP/DHCP Relay Agent and briefly outlines how to configure the NT system.

Inherently with TCP/IP networks, broadcast messages are not allowed to leave their own subnet or LAN. This is part of the TCP/IP architecture, and it ensures that the network does not become flooded with broadcast messages. A router or gateway that recognizes a broadcast message usually examines the packet to see if it is relevant. If it is not, it is discarded.

The BOOTP/DHCP Relay Agent overcomes this problem by intercepting the broadcast message and forwarding the packet directly to a preconfigured destination address. Most routers today have BOOTP/DHCP Relay Agent support, and so does the AS/400 system in V4R2.

The BOOTP/DHCP Relay Agent intercepts broadcast messages that arrive on port 67. It then places its own IP address in the DHCPDISCOVER packet and forwards it directly (unicast) to the DHCP server. The DHCP server forwards the DHCPOFFER directly back to the relay agent, and the relay agent broadcasts the offer back onto the network, where the client picks it up.

You can define multiple DHCP servers to which the BOOTP/DHCP Relay Agent sends DHCP requests. The BOOTP/DHCP Relay Agent sends the same packet to each of the DHCP servers that you configure (multicast).

You can configure the BOOTP/DHCP Relay Agent to send the DHCP message to another BOOTP/DHCP Relay Agent, which in turn forwards it to another BOOTP/DHCP Relay Agent, and so on. You can limit the number of hops that the DHCP message makes because routers do not increase the hop count. Only BOOTP/DHCP Relay Agents increase the hop count. The relay agent stops forwarding the message once it has reached the hop count.

There is also a feature that allows you to delay the forwarding of a DHCP message by way of a BOOTP/DHCP Relay Agent. Consequently, you might bias a DHCP server by allowing it to respond without delay. This increases the length of time that it takes for the message to reach the backup DHCP server.

14.1 Scenario Overview

This scenario provides DHCP services to clients that are connected to multiple LANs. The network is now more complex than the one discussed in Chapter 13, "Multiple Subnets and DHCP Servers" on page 277. Figure 273 on page 314 shows a high-level view of the network used in this scenario.

Configure two BOOTP/DHCP Relay Agents. One is an AS/400 relay agent, and one is an NT relay agent. These relay agents intercept BOOTP and DHCP broadcasts and forward them to the DHCP server. You are not using BOOTP clients, but because both BOOTP and DHCP use the same port for incoming and

outgoing transmissions, the relay agents perform the same task for both protocols without intervention.

The AS/400 system AS1 is a primary DHCP server for all three subnets, and the DHCP server running on AS2 is a backup DHCP server for the same three subnets. Configure BOOTP/DHCP Relay Agent AS5 as a BOOTP/DHCP Relay Agent that always forwards to both DHCP servers, and place a delay on forwarding to the backup DHCP server. The NT server (BOOTP/DHCP Relay Agent R2) is also a BOOTP/DHCP Relay Agent on a different subnet that always forwards to the BOOTP/DHCP Relay Agent AS5.

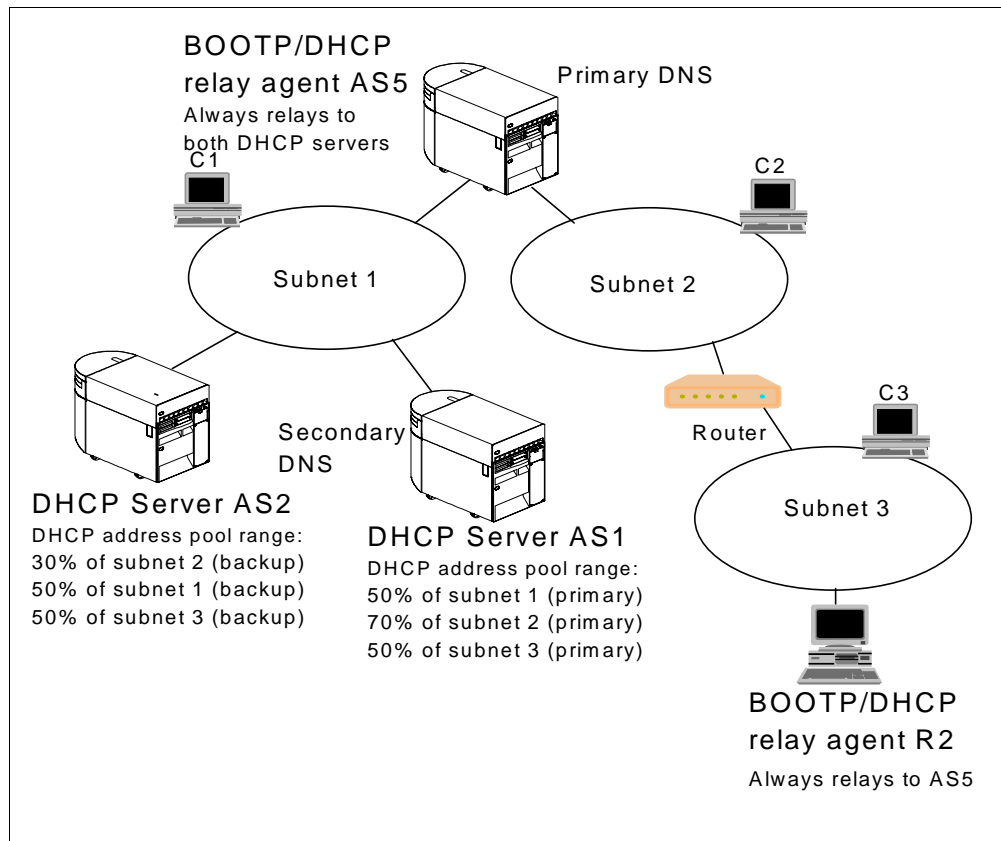


Figure 273. Multi-LAN and Multi-Subnet Network with DHCP Server, DHCP Relay Agents, and Routers

Use an addressing scheme that allows all clients to attach even if one of the DHCP servers failed. The exception to this is subnet 2, which is split in a 70/30 manner.

14.1.1 Scenario Objectives

This scenario has the following objectives:

1. Define and configure multiple DHCP servers.
2. Define and configure multiple BOOTP/DHCP Relay Agents.
3. Introduce a technique to delay DHCP messages reaching the backup DHCP server.
4. Provide both full and partial DHCP backups in the event of failure.

5. Show how the relay agent works with the DHCP server.
6. Use a multiple subnet network.

14.1.2 Scenario Advantages

The advantages of this scenario include:

- Full and partial DHCP backup support:

This scenario shows a method that you can use for DHCP backup support by using the BOOTP/DHCP Relay Agent. The TCP/IP addressing schemes are a concern because they limit complete, full-DHCP backup support. A limited range was chosen to represent a realistic situation.

- The ability to keep the network administration centralized:

A backup DHCP server means that the DHCP configuration is split between two systems. If no DHCP backup is used, however, the BOOTP/DHCP Relay Agent forwards all messages to the single DHCP server, keeping the administration centralized.

- The ease with which you can configure the AS/400 system as a BOOTP/DHCP Relay Agent:

This is a simple task if you understand your network topology.

- The flexibility of using a BOOTP/DHCP Relay Agent:

The BOOTP/DHCP Relay Agent allows you to delay the arrival of DHCP messages to the backup DHCP server. This allows the primary DHCP server to respond first.

- No need to change your router configuration to support DHCP or BOOTP in your network:

Router configuration can be complex, and sometimes it requires a network outage. You can start, stop, and change the AS/400 relay agent without interrupting system availability.

- Subnet growth within your network:

As your company grows and you attach new networks to your AS/400 system, you do not need to purchase expensive network equipment.

Note: While the AS/400 system in V4R2 performs many of the same tasks that dedicated, intelligent network nodes can perform, it is still a multi-user application system. As such, it requires system maintenance such as backups, storage reclamation, and periodic IPLs. Generally, routers require only a backup of the initial configuration. They then perform only the task for which they have been optimized.

14.1.3 Scenario Disadvantages

The disadvantages of this scenario are that:

- The NT BOOTP/DHCP Relay Agent (R2) is a single point of failure for subnet 3.
- Unavailability of the AS/400 AS5 BOOTP/DHCP Relay Agent (R1) causes an outage for clients on subnet 2 and 3 trying to access the DHCP server AS1.
- The network has many single point of failures, and there are no backups for routers between subnets.

- You cannot run both the DHCP server and the BOOTP/DHCP Relay Agent on the same system simultaneously.

14.1.4 Scenario Network Configuration

Figure 274 shows the network detail for this scenario. Note that the network 10.1.0.0 has a mask of 23 contiguous bits, allowing a range of 510 TCP/IP addresses.

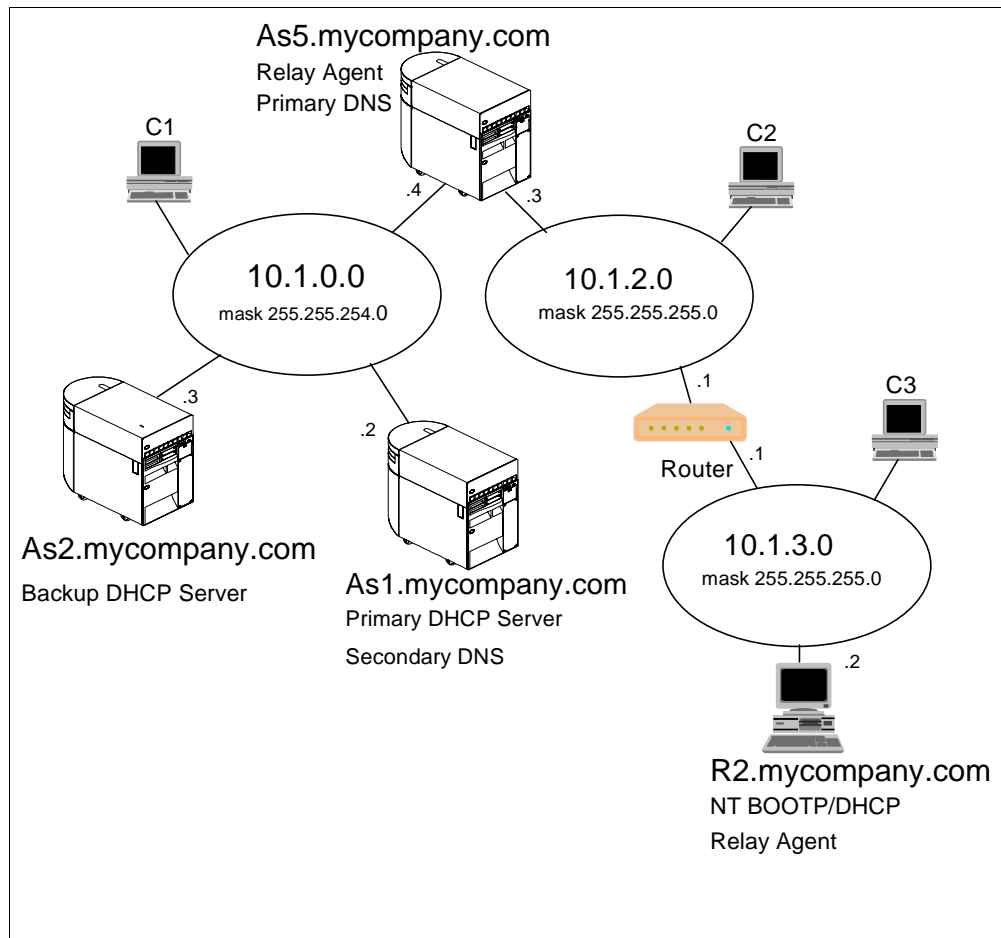


Figure 274. Scenario Network Topology

The following scenario characteristics influence both the DHCP server and the BOOTP/DHCP Relay Agent configuration:

- There are three physical network segments.
- There are three subnets, one for each physical segment.
- There is one multi-homed host (AS5).
- There is a router in the network.
- There are two DHCP servers (AS1 and AS2).
- There is a primary DNS server (AS5) and a secondary DNS server (AS2).
- There are two BOOTP/DHCP Relay Agents (AS5 and R2).
- The network implements a class A TCP/IP addressing scheme, and one subnet is using a complex mask (255.255.254.0).
- There is a primary DHCP server (AS1) and a backup DHCP server.

- There are no diskless workstations in the network (for example, IBM Network Stations).
- The router is not configured to act as a BOOTP/DHCP Relay Agent.
- AS5 performs gateway functions between subnet 1 and subnet 2. IP forwarding is enabled on AS5.

14.2 Task Summary

The tasks required to complete this scenario do not include the building of line descriptions and TCP/IP interfaces on the AS/400 system. It is assumed that the TCP/IP configuration on the AS/400 system is up and running.

The summary of tasks for this scenario is as follows:

1. Plan the TCP/IP addressing scheme.
2. Gather information to configure DHCP servers and BOOTP/DHCP Relay Agents.
3. Configure the primary DHCP server.
4. Configure the backup DHCP server.
5. Add routing information to both of the DHCP servers.
6. Configure the AS/400 BOOTP/DHCP Relay Agent.
7. Configure the Microsoft NT BOOTP/DHCP Relay Agent.

14.2.1 Planning the TCP/IP Addressing Scheme

In a TCP/IP network with multiple subnets and TCP/IP address ranges, it is imperative to pay careful attention to the addressing scheme. This topic shows you the addressing scheme in detail.

Use class A IP addresses from the Internet Assigned Numbers Authority (IANA) in your internal network. They cannot be routed through the Internet, but Class A provides you with good growth potential for the future.

There are 250 clients on subnet 10.1.0.0 (subnet mask 255.255.254.0) with a total of 510 TCP/IP addresses in the range. You must split this range evenly between both DHCP servers to allow full fall-back support if one server fails.

On subnet 10.1.2.0, there are 170 DHCP clients. This subnet supports up to 175 clients when the primary DHCP server is active. However, during fallback when the primary fails, the backup DHCP server only supports up to 76 DHCP clients.

On the remote subnet (10.1.3.0), there are only 110 DHCP clients. You can provide full support during failure of one of the DHCP servers.

Figure 19 details the IP addresses for each subnet and in which DHCP server pool they reside.

The Net ID column is the network portion of the TCP/IP address for the subnet.

The Subnet Mask column has the mask that you must apply to the subnet.

The Host Range column is the TCP/IP address range to be used once the mask has been applied.

The DHCP Server ID column lists the DHCP server that administers the IP address pool.

The last column, labeled %, shows the percentage of the total host range assigned to the DHCP server.

Table 19. TCP/IP Addressing and Allocation of IP Address Range by DHCP Server

Net ID	Subnet Mask	Host Range	DHCP Server ID	%
10.1.0.0	255.255.254.0	0.0.0.1~0.0.0.254	As1.mycompany.com	50
10.1.2.0	255.255.255.0	0.0.0.1~0.0.0.178	As1.mycompany.com	70
10.1.3.0	255.255.255.0	0.0.0.1~0.0.0.127	As1.mycompany.com	50
10.1.0.0	255.255.254.0	0.0.1.1~0.0.1.254	As2.mycompany.com	50
10.1.2.0	255.255.255.0	0.0.0.179~0.0.0.254	As2.mycompany.com	30
10.1.3.0	255.255.255.0	0.0.0.128~0.0.0.254	As2.mycompany.com	50

You need to exclude the IP addresses of the DHCP servers, BOOTP/DHCP Relay Agents, and the router from each relevant subnet range as in the following example:

In the subnet pool 10.1.0.0 Exclude 10.1.0.1, 10.1.0.2, 10.1.0.3 and 10.1.0.4

Note:Exclude 10.1.0.1 for future use by router on this subnet.

In the subnet pool 10.1.2.0 Exclude 10.1.2.1 and 10.1.2.3

In the subnet pool 10.1.3.0 Exclude 10.1.3.1 and 10.1.3.2

14.2.2 Gathering Information to Configure DHCP Servers and DHCP Relay Agents

To use Operations Navigator DHCP configuration effectively, you need to know how you want to set up and manage your networks and subnets with DHCP. You also need to know what address range or ranges you want to use for leasing. You must decide which system is the DHCP server, which one is the BOOTP/DHCP Relay Agent, and which one performs DHCP backup functions. Further, you need to know which IP addresses to reserve for special hosts such as routers, DNS servers, and firewalls. It is useful to refer to a network diagram that shows the subnet masks and IP addresses for your networks, routers, and clients while you are configuring DHCP.

The starting point in this scenario is the network diagram shown in Figure 274 on page 316. The information shown in the following tables is based on the network picture and other network data.

14.2.2.1 AS1 DHCP Server and Administered Subnets Information

Table 20 shows some general information about AS1 as a TCP/IP host, while Table 21 provides more specific information about AS1 as a DHCP server.

Table 20. Planning the Primary DHCP Server -- AS1 TCP/IP Information

Host Name	As1
Description	Primary DHCP server
Domain Name	mycompany.com
IP Address	10 . 1 . 0 . 2

Mask	255.255.254.0
Line Description	TRNLINE1

Note: The Configuration Reference column in the following tables points to the place in the Operations Navigator DHCP server configuration where you can configure the particular parameter. You can specify many of these configuration options through the DHCP configuration wizard the first time you configure DHCP.

Table 21. Planning the Primary DHCP Server AS1 -- DHCP Server Overview

#	Question	Answer	Configuration Reference
1	Is the BOOTP server already configured on your system?	No	DHCP configuration wizard
2	Do you want to migrate the BOOTP configuration to DHCP?	N/A	File -->Migrate BOOTP
3	What is the default lease time for this server?	24 hours	Global-->Properties-->Leases
4	Start the DHCP server when TCP/IP starts?	Yes	Server Properties --> General
5	List the DHCP server IP interfaces that will be serving DHCP clients.	10.1.0.2	See network diagram.
6	List the subnets that will be administered by this DHCP server.	10.1.0.0 10.1.2.0 10.1.3.0	See subnet planning table
7	Do you want to add a new subnet to be administered by this server?	Yes	Global --> New Subnet - Basic Global-->New Subnet - Advanced See subnet planning table
8	Do you want to log DHCP server activity?	Yes	Server Properties --> Logging
9	Do you want the DHCP server to support any client from any subnet?	Yes	Server Properties --> Client Support
10	Do you want the DHCP server to support BOOTP clients?	No	Server Properties --> Client Support
11	Do you want the DHCP server to reject requests from specific clients (for example, for security reasons)?	No	Global->Properties-> Exclude Client
11	Can your DHCP clients (other than IBM Network Stations) identify the class they belong to?	No	
12	If answer to 11 is Yes, do you want to add a new class to serve the DHCP clients that belong to that class?	N/A	Global --> New Class

Table 22 provides information about subnet 10.1.0.0 being administered by DHCP server AS1. Notice that AS1 administers 50% of the IP addresses available and that the rest is assigned to AS2, the backup DHCP server.

Table 22. Planning the Subnet 10.1.0.0 Administered by AS1 from IP Interface 10.1.0.2

#	Question	Answer	Configuration Reference
1	Subnet name	10.1.0.0	Subnet Properties --> General
2	Subnet description	Marketing	Subnet Properties --> General
3	Subnet address	10.1.0.0	Subnet Properties --> Address Pool
4	Subnet mask	255.255.254.0	Subnet Properties --> Address Pool
5	Address range	10.1.0.1 10.1.0.254	Subnet Properties --> Address Pool
6	Lease time	Inherit from server (24 hours)	Subnet Properties --> Leases
7	Exclusions (exclude hosts that required a particular IP address and are manually configured).		Subnet Properties --> Address Pool
	Name: Router x AS1 AS2 Description: Reserved for future router DNS/DHCP server backup DHCP server IP address: 10.1.0.1 10.1.0.2 10.1.0.3 Name: AS5 Description: DNS/DHCP Relay IP Address: 10.1.0.4		
8	Domain Name server IP address to deliver to clients in this subnet.	10.1.0.4 10.1.0.2	Subnet Properties --> Options--> Option 6 (Domain name server)
9	Gateway IP address to deliver to clients in this subnet.	10.1.0.4	Subnet Properties --> Options--> Option 3 (Router)
10	Offer options to client in this subnet 01 - Subnet mask 03 - Router 06 - Domain name server	255.255.254.0 10.1.0.4 10.1.0.4 10.1.0.2	Subnet Properties --> Options-->

Table 23 provides information about subnet 10.1.2.0 being administered by DHCP server AS1. Notice that AS1 administers 70% of the IP addresses available and that the rest is assigned to AS2, the backup DHCP server.

Table 23. Planning the Subnet 10.1.2.0 Administered by AS1 from IP Interface 10.1.0.2

#	Question	Answer	Configuration Reference
1	Subnet name	10.1.2.0	Subnet Properties --> General
2	Subnet description	Manufacturing	Subnet Properties --> General
3	Subnet address	10.1.2.0	Subnet Properties --> Address Pool
4	Subnet mask	255.255.255.0	Subnet Properties --> Address Pool
5	Address range	10.1.2.1 10.1.2.178	Subnet Properties --> Address Pool

#	Question	Answer	Configuration Reference
6	Lease time	Inherit from server (24 hours)	Subnet Properties --> Leases
7	Exclusions (exclude hosts that required a particular IP address and are manually configured).		Subnet Properties --> Address Pool
	Name: Router Description: Router to next subnet IP address: 10.1.2.1	AS5 DNS/DHCP relay 10.1.2.3	
8	Domain Name server IP address to deliver to clients in this subnet.	10.1.2.3 10.1.0.2	Subnet Properties --> Options--> Option 6 (Domain name server)
9	Gateway IP address to deliver to clients in this subnet.	10.1.2.1	Subnet Properties --> Options--> Option 3 (Router)
10	Offer options to client in this subnet 01 - Subnet mask 03 - Router 06 - Domain name server	255.255.255.0 10.1.2.1 10.1.2.3 10.1.0.2	Subnet Properties --> Options-->

Table 24 provides information about subnet 10.1.3.0 being administered by DHCP server AS1. Notice that AS1 administers 50% of the IP addresses available and that the rest is assigned to AS2, the backup DHCP server.

Table 24. Planning the Subnet 10.1.3.0 Administered by AS1 from IP Interface 10.1.0.2

#	Question	Answer	Configuration Reference
1	Subnet name	10.1.3.0	Subnet Properties --> General
2	Subnet description	Research	Subnet Properties --> General
3	Subnet address	10.1.3.0	Subnet Properties --> Address Pool
4	Subnet mask	255.255.255.0	Subnet Properties --> Address Pool
5	Address range	10.1.3.1 10.1.3.127	Subnet Properties --> Address Pool
6	Lease time	Inherit from server (24 hours)	Subnet Properties --> Leases
7	Exclusions (exclude hosts that required a particular IP address and are manually configured).		Subnet Properties --> Address Pool
	Name: Router Description: Router to next subnet IP address: 10.1.3.1	R2 NT DHCP relay 10.1.3.2	
8	Domain Name server IP address to deliver to clients in this subnet.	10.1.2.3 10.1.0.2	Subnet Properties --> Options--> Option 6 (Domain name server)
9	Gateway IP address to deliver to clients in this subnet.	10.1.3.1	Subnet Properties --> Options--> Option 3 (Router)

#	Question	Answer	Configuration Reference
10	Offer options to client in this subnet 01 - Subnet mask 03 - Router 06 - Domain name server	255.255.255.0 10.1.3.1 10.1.2.3 10.1.0.2	Subnet Properties --> Options-->

14.2.2.2 AS2 DHCP Server and Administered Subnets Information

Table 25 shows some general information about AS2 as a TCP/IP host, while Table 26 provides more specific information about AS2 as a DHCP server.

Table 25. Planning the Primary DHCP Server -- AS2 TCP/IP Information

Host Name	AS2
Description	Backup server
Domain Name	mycompany.com
IP Address (Interface)	10 . 1 . 0 . 3
Mask	255.255.254.0
Line Description	TRNLINE1

Note: The Configuration Reference column in the following tables points to the place in the Operations Navigator DHCP server configuration where you can configure the particular parameter. You can specify many of these configuration options through the DHCP configuration wizard the first time you configure DHCP.

Table 26. Planning the Primary DHCP Server AS2 -- DHCP Server Overview

#	Question	Answer	Configuration Reference
1	Is the BOOTP server already configured on your system?	No	DHCP configuration wizard
2	Do you want to migrate the BOOTP configuration to DHCP?	N/A	File -->Migrate BOOTP
3	What is the default lease time for this server?	24 hours	Global-->Properties-->Leases
4	Start the DHCP server when TCP/IP starts?	Yes	Server Properties --> General
5	List the DHCP server IP interfaces that will be serving DHCP clients.	10.1.0.3	See network diagram.
6	List the subnets that will be administered by this DHCP server.	10.1.0.0 10.1.2.0 10.1.3.0	See subnet planning table
7	Do you want to add a new subnet to be administered by this server?	Yes	Global --> New Subnet - Basic Global-->New Subnet - Advanced See subnet planning table
8	Do you want to log DHCP server activity?	Yes	Server Properties --> Logging
9	Do you want the DHCP server to support any client from any subnet?	Yes	Server Properties --> Client Support

#	Question	Answer	Configuration Reference
10	Do you want the DHCP server to support BOOTP clients?	No	Server Properties --> Client Support
11	Do you want the DHCP server to reject requests from specific clients (for example, for security reasons)?	No	Global->Properties-> Exclude Client
11	Can your DHCP clients (other than IBM Network Stations) identify the class they belong to?	No	
12	If answer to 11 is Yes, do you want to add a new class to serve the DHCP clients that belong to that class?	N/A	Global --> New Class
12	Clients with static addr./ spec. options?	Yes/No	Server->Popup->NewClient

Table 27 provides information about subnet 10.1.0.0 being administered by DHCP server AS2. Notice that AS2 administers 50% of the IP addresses available and that the rest is assigned to AS1, the primary DHCP server.

Table 27. Planning the Subnet 10.1.0.0 Administered by As2 from IP Interface 10.1.0.3

#	Question	Answer	Configuration Reference
1	Subnet name	10.1.0.0	Subnet Properties --> General
2	Subnet description	Marketing	Subnet Properties --> General
3	Subnet address	10.1.0.0	Subnet Properties --> Address Pool
4	Subnet mask	255.255.254.0	Subnet Properties --> Address Pool
5	Address range	10.1.1.1 10.1.1.254	Subnet Properties --> Address Pool
6	Lease time	Inherit from server (24 hours)	Subnet Properties --> Leases
7	Exclusions (exclude hosts that required a particular IP address and are manually configured).		Subnet Properties --> Address Pool
	NONE. All the excluded hosts in this subnet fall outside the range of addresses administered by this server.		
8	Domain Name server IP address to deliver to clients in this subnet.	10.1.0.4 10.1.0.2	Subnet Properties --> Options--> Option 6 (Domain name server)
9	Gateway IP address to deliver to clients in this subnet.	10.1.0.4	Subnet Properties --> Options--> Option 3 (Router)
10	Offer options to client in this subnet 01 - Subnet mask 03 - Router 06 - Domain name server	255.255.254.0 10.1.0.4 10.1.0.4 10.1.0.2	Subnet Properties --> Options-->

Table 28 provides information about subnet 10.1.2.0 being administered by the DHCP server AS2. Notice that AS2 administers 30% of the IP addresses available and that the rest is assigned to AS1, the primary DHCP server.

Table 28. Planning the Subnet 10.1.2.0 Administered by AS2 from IP Interface 10.1.0.3

#	Question	Answer	Configuration Reference
1	Subnet name	10.1.2.0	Subnet Properties --> General
2	Subnet description	Manufacturing	Subnet Properties --> General
3	Subnet address	10.1.2.0	Subnet Properties --> Address Pool
4	Subnet mask	255.255.255.0	Subnet Properties --> Address Pool
5	Address range	10.1.2.179 10.1.2.254	Subnet Properties --> Address Pool
6	Lease time	Inherit from server (24 hours)	Subnet Properties --> Leases
7	Exclusions (exclude hosts that required a particular IP address and are manually configured).		Subnet Properties --> Address Pool
	NONE. All the excluded hosts in this subnet fall outside the range of addresses administered by this server.		
8	Domain Name server IP address to deliver to clients in this subnet.	10.1.2.3 10.1.0.2	Subnet Properties --> Options--> Option 6 (Domain name server)
9	Gateway IP address to deliver to clients in this subnet.	10.1.2.1	Subnet Properties --> Options--> Option 3 (Router)
10	Offer options to client in this subnet 01 - Subnet mask 03 - Router 06 - Domain name server	255.255.255.0 10.1.2.1 10.1.2.3 10.1.0.2	Subnet Properties --> Options-->

Table 29 provides information about subnet 10.1.3.0 being administered by DHCP server AS1. Notice that AS2 administers 50% of the IP addresses available and that the rest is assigned to AS1, the primary DHCP server.

Table 29. Planning the Subnet 10.1.3.0 Administered by AS2 from IP Interface 10.1.0.3

#	Question	Answer	Configuration Reference
1	Subnet name	10.1.3.0	Subnet Properties --> General
2	Subnet description	Research	Subnet Properties --> General
3	Subnet address	10.1.3.0	Subnet Properties --> Address Pool
4	Subnet mask	255.255.255.0	Subnet Properties --> Address Pool
5	Address range	10.1.3.128 10.1.3.254	Subnet Properties --> Address Pool
6	Lease time	Inherit from server (24 hours)	Subnet Properties --> Leases
7	Exclusions (exclude hosts that required a particular IP address and are manually configured).		Subnet Properties --> Address Pool
	NONE. All the excluded hosts in this subnet fall outside the range of addresses administered by this server.		

#	Question	Answer	Configuration Reference
8	Domain Name server IP address to deliver to clients in this subnet.	10.1.2.3 10.1.0.2	Subnet Properties --> Options--> Option 6 (Domain name server)
9	Gateway IP address to deliver to clients in this subnet.	10.1.3.1	Subnet Properties --> Options--> Option 3 (Router)
10	Offer options to client in this subnet 01 - Subnet mask 03 - Router 06 - Domain name server	255.255.255.0 10.1.3.1 10.1.2.3 10.1.0.2	Subnet Properties --> Options-->

Table 30 shows the information that is necessary to configure BOOTP/DHCP Relay Agent AS5.

Table 30. Planning the BOOTP/DHCP Relay Agent -- AS5

Host Name	AS5
Description	BOOTP/DHCP Relay Agent
Domain Name	mycompany.com
Interface to accept DHCP packets	10 . 1 . 2 . 3
Destination server / relay agent	10 . 1 . 0 . 2 - AS2
Maximum number hops to DHCP server	4
Packet transm. delay (ms)	0
Interface to accept DHCP packets	10 . 1 . 2 . 3
Destination server / relay agent	10 . 1 . 0 . 3
Maximum hops	4
Packet transm. delay (ms)	5000

Table 31 shows the information that is necessary to configure BOOTP/DHCP Relay Agent R2, which runs on an NT server.

Table 31. Planning DHCP Relay Agent R2

Host Name	R2
Description	NT BOOTP/DHCP Relay Agent
Domain Name	mycompany.com
Interface to accept DHCP packets	10 . 1 . 3 . 2
Destination server / relay agent	10 . 1 . 2 . 3
Maximum hops	4
Seconds threshold	0

14.2.3 Configure the Primary DHCP Server (AS1)

It is assumed that this is the first time you are configuring the DHCP server. Therefore, the Operations Navigator DHCP server configuration wizard starts.

1. Start Operations Navigator in your workstation.
2. Click *As1.mycompany.com* to select the system.

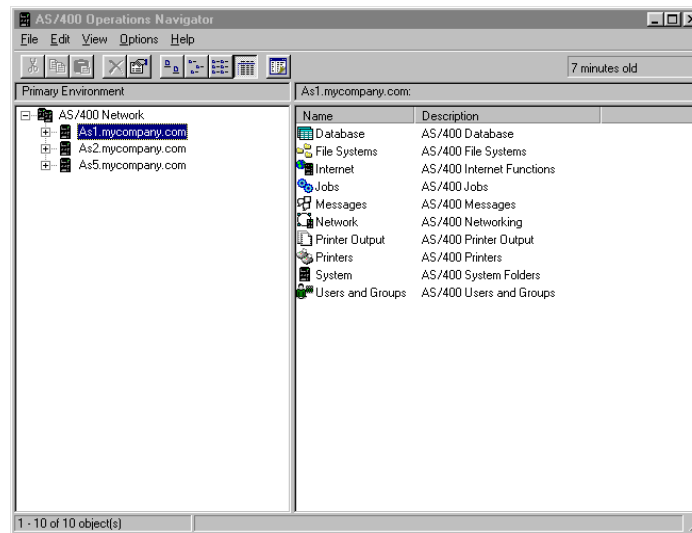


Figure 275. AS/400 Operations Navigator -- Selecting the System to Configure DHCP Server

3. Double-click **Network**.
4. Double-click **Server**.
5. Double-click **OS/400**.
6. Double-click **DHCP**. This starts the DHCP configuration wizard.

Note

If the DHCP configuration wizard is not shown, it is likely that a DHCP configuration already exists. To start the wizard and replace the existing configuration, select **File > New Configuration**.

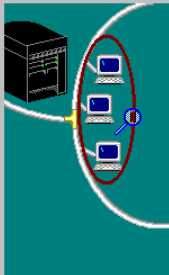
7. Click **Next**.

Note

The following steps do not reflect the exact sequence of prompts that you see during the DHCP configuration. Only those configuration parameters that are the most relevant to this scenario are included.

8. Select **Yes** to add a new subnet to the DHCP server.
9. Leave the Twinax IP workstation controller address box blank and click **Next**.
10. Define the range of addresses to use within the subnet.

Define Subnet Based on an Address Range - As1.mycompany.com



What is the information to define this subnet based on an address range within a subnet?

Name:

Description:

Start address:

End address:

Mask:

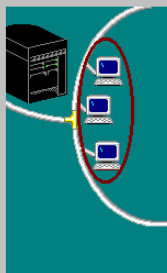
< Back Next > Cancel Help

Figure 276. IP Address Range for Subnet 1 (10.1.0.0) on AS1

Define a lease time for the client to keep the address served. Click **Next** to use the default lease time of one day.

11. Exclude the IP address permanently assigned to servers and routers (see Figure 277).

Exclude Addresses - As1.mycompany.com



What addresses, if any, in this subnet should be excluded by this DHCP server?

Example: routers, gateways, and other interfaces defined in the subnet

10.1.0.1
10.1.0.2
10.1.0.3
10.1.0.4

Add Remove

< Back Next > Cancel Help

Figure 277. Exclude IP Address in 10.1.0.0 Subnet -- AS1 DHCP Server

12. Specify the Gateway information for this subnet (see Figure 278).

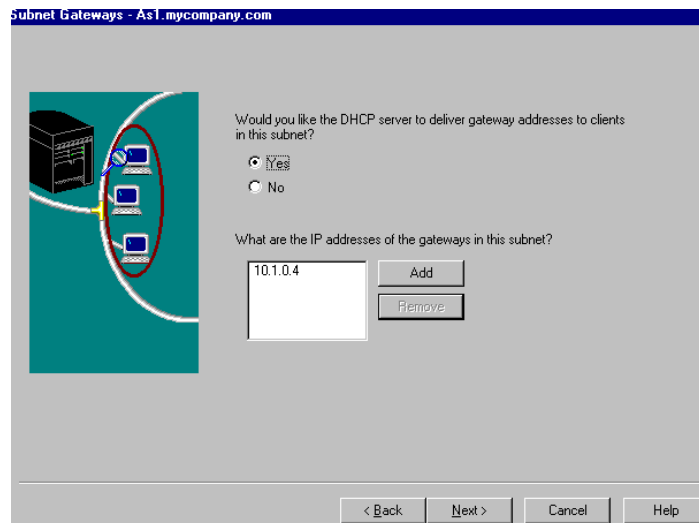


Figure 278. Subnet 10.1.0.0 Gateway Configuration

13. Specify the DNS IP address (see Figure 279) and click **Next**.

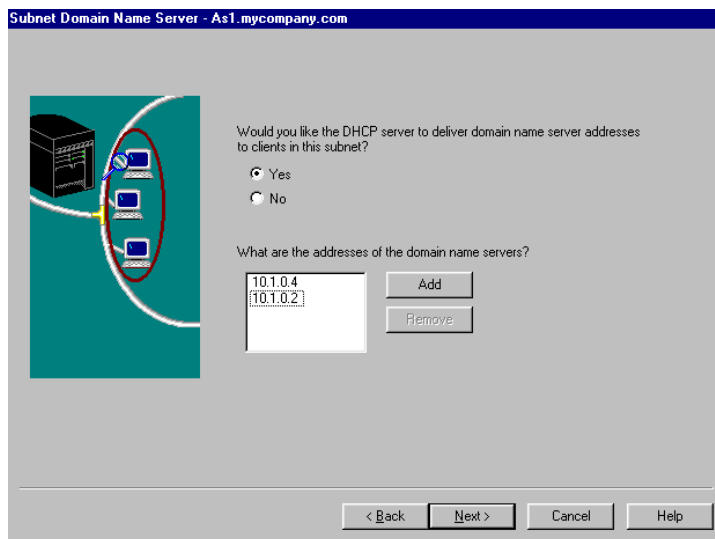


Figure 279. DNS Configuration for Clients in 10.1.0.0 Subnet -- AS1 DHCP Server

14. Answer **No** to the question "Would you like the DHCP server to deliver domain name to clients in this subnet?" Click **Next**.

15. Check *Support any clients form this subnet*.

16. Answer **No** to the question "Would you like to set other options for this subnet?" Click **Next**.

17. Select **Yes** to start the DHCP server when TCP/IP starts, and select **No** to start the DHCP server now. Click **Next**.

18. The DHCP configuration summary window shows all the options that you have selected so far. Click **Finish**. Now the DHCP server configuration is displayed.

19. Add the subnet mask. To use this subnet, right-click subnet 10.1.0.0 to open a context menu and select **Properties**.
20. Click the **Options** tab at the top of the dialog.
21. Highlight option number **1**, *Subnet mask*, and click **Add**.
22. Specify the mask value to use for this subnet in the field at the bottom of the dialog. The mask to specify is **255.255.254.0**.
23. Click **OK**.

The next step is to add the other two subnets to the primary DHCP server, *As1.mycompany.com*.

24. From the DHCP Server Configuration window, right-click **Global** to open a context menu and **New>Subnet-Advanced** (see Figure 280).

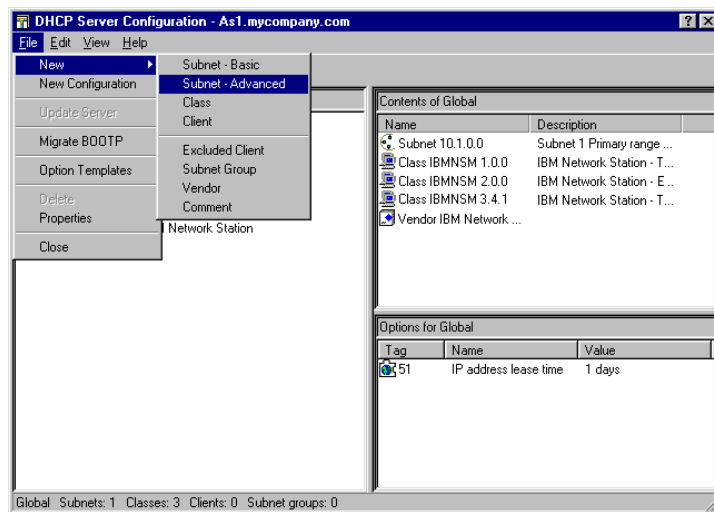


Figure 280. AS1 DHCP Server Configuration -- Adding Subnet 10.1.2.0

25. Ensure the **General** tab is selected and specify the network ID (for documentation purposes only) in the field labeled *Name* (see Figure 281).
26. Place a description of the subnet in the *Description* field (see Figure 281).

New Subnet Properties - As1.mycompany.com

General | Address Pool | Leases | Options | Other

Name: 10.1.2.0

☐ Twinax subnet

Controller's IP address:

State

☒ Enabled

☐ Disabled

Description:

Manufacturing - Subnet 2 primary range (705)

OK Cancel Help

Figure 281. Subnet Properties -- Adding the Name and Description for Subnet #2 (10.1.2.0)

27. Click the **Address pool** tab.

28. Click *Range to assign* and specify the second IP address range, *As1.mycompany.com* from Table 19 on page 318.

29. Click **Add** and exclude the IP addresses of the routers *As1.mycompany.com* and *As5.mycompany.com* shown in Figure 282.

New Subnet Properties - As1.mycompany.com

General | Address Pool | Leases | Options | Other

IP addresses included

☐ Subnet address:

☒ Range to assign:

Start address: 10.1.2.1

End address: 10.1.2.178

Subnet mask: 255.255.255.0

IP addresses excluded from pool:

10.1.2.1

10.1.2.3

Add

Remove

OK Cancel Help

Figure 282. 10.1.2.0 Subnet Address Range and Exclusions

30. Click the **Options** tab to add a subnet mask to serve to the clients.

31. Highlight option 1, *subnet mask*, from the **Available options** window and click **Add**.

32. Specify the appropriate subnet mask for the clients to use in the Subnet mask window at the bottom of the display. In this example, specify 255.255.255.0.
33. Highlight option **3**, *router*, from the *Available options* panel and then click **Add**.
34. Specify the appropriate router information for the subnet's clients. In this example, specify 10.1.2.1.
35. Highlight option **6**, *Domain name server*, from the **Available options** dialog and then click **Add**.
36. Specify the appropriate DNS information for the subnet's clients. In this example, specify 10.1.2.3 and 10.1.0.2.
37. Click **OK**.

Figure 283 shows the options configured for subnet 10.1.2.0 on DHCP server AS1.

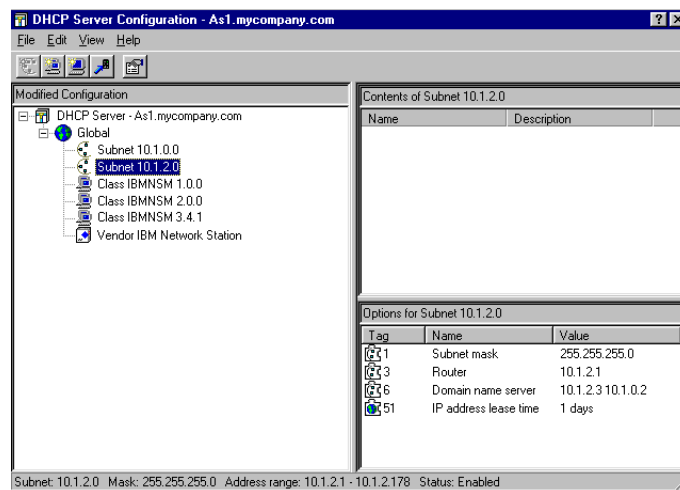


Figure 283. Subnet 10.1.2.0 Options on AS1 DHCP Server

Repeat steps 25 through 37 to add the third subnet pool range to *As1.mycompany.com*. Figure 284 on page 332 shows an example of the pool range for subnet 3 (10.1.3.1) on *As1.mycompany.com*.

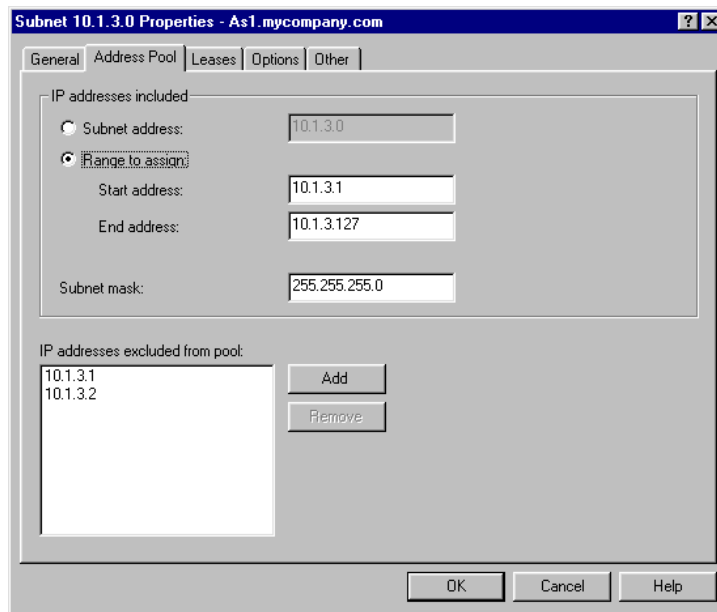


Figure 284. Subnet 10.1.3.0 IP Address Range and Exclusions

Figure 285 shows the configuration options for clients on subnet 10.1.3.0.

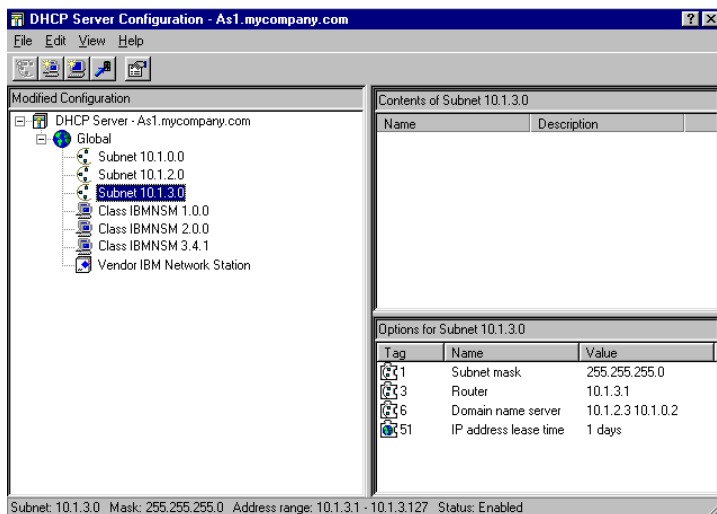


Figure 285. Subnet 10.1.3.0 Configuration Options -- AS1 DHCP Server

14.2.4 Configure the Backup DHCP Server (AS2)

The backup DHCP server is *As2.mycompany.com*. The steps to configure the backup DHCP server are the same as those that you used to configure the primary DHCP server in “Configure the Primary DHCP Server (AS1)” on page 326.

The only difference between the two sets of steps is the TCP/IP address range that you use on the backup DHCP server. This address range for the backup DHCP server must be different from the primary DHCP servers range.

Use Table 19 on page 318 to decide the range of IP addresses to use in each subnet for the backup DHCP server.

Samples of the subnet properties windows are provided for each of the subnets on the backup DHCP server.

Figure 286 on page 333 shows the range of IP addresses for the network 10.1.0.0 with a mask of 255.255.254.0 that you can use on the backup DHCP server.

Figure 287 on page 334 shows the range of addresses for the network 10.1.2.0 that you can use on the backup DHCP server.

Figure 288 on page 334 shows the range of addresses for the network 10.1.3.0 that you can use on the backup DHCP server.

Note

No addresses are excluded in the examples for the backup DHCP server. This is because the upper range of the TCP/IP addresses is used for the subnets on the DHCP backup server. The IP addresses that need to be excluded do not fall into the ranges defined on the backup DHCP server. They cannot be excluded.

The mask, router, and DNS information to be delivered to clients on the three subnets is the same as those in the primary DHCP server, AS1.

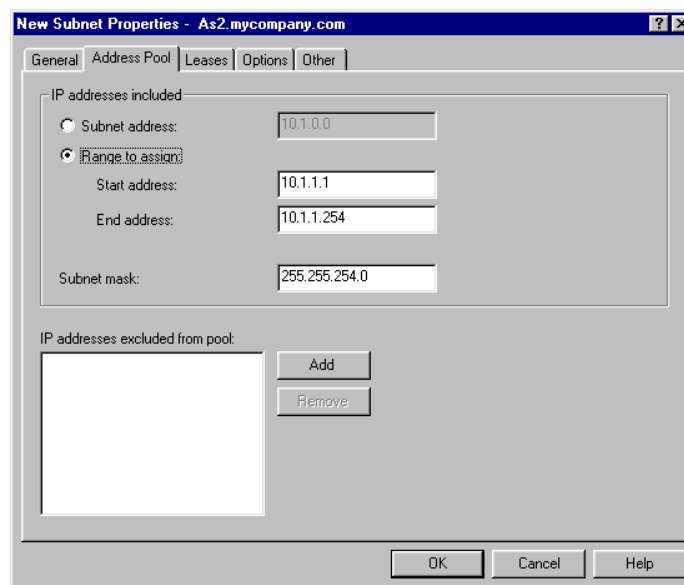


Figure 286. Backup Subnet #1 (10.1.0.0) IP Address Range Properties

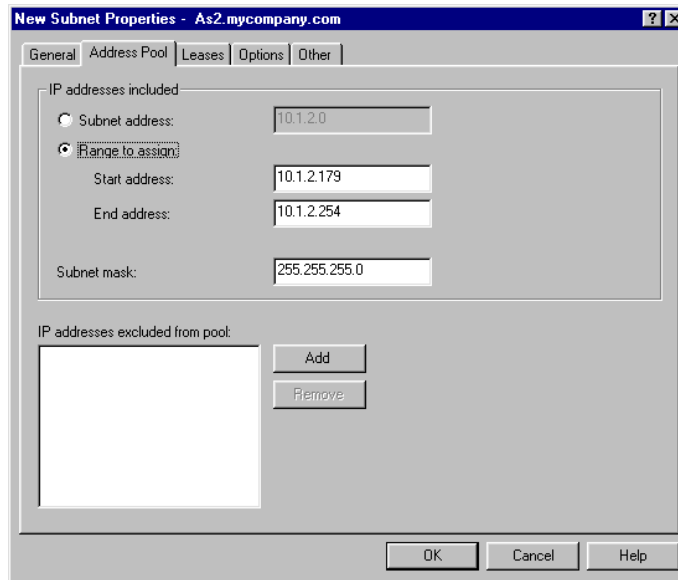


Figure 287. Backup Subnet #2 (10.1.2.0) IP Address Range Properties

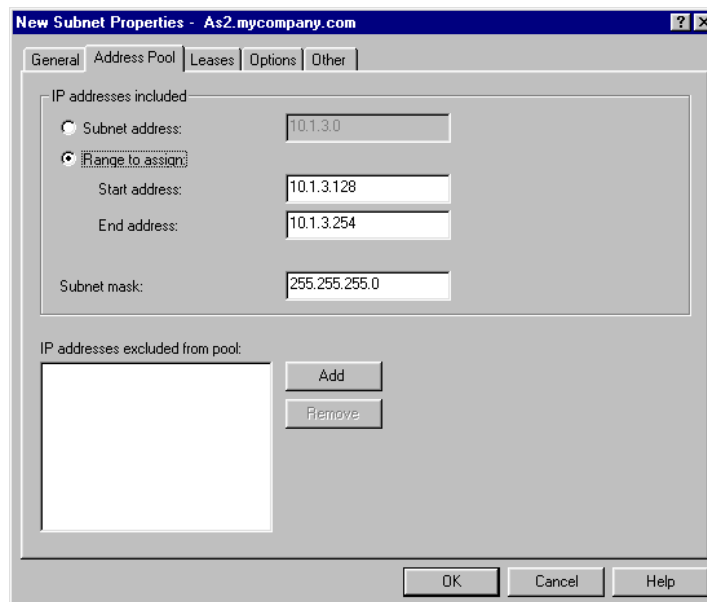


Figure 288. Backup Subnet #3 (10.1.3.0) IP Address Range Properties

14.2.5 Configure Routing Information on Both DHCP Servers

The BOOTP/DHCP Relay Agent configures the IP address on the interface that is listening for broadcast DHCP messages. The BOOTP/DHCP Relay Agent then places this address into the packet that it forwards to the DHCP server. The DHCP server uses this address as a clue to select the correct address pool from which to offer an IP address to the client. The DHCP server sends all DHCP replies *directly* to this address. Once the client receives the DHCPOFFER, all communication after that is directly between the client and the DHCP server. The DHCP client sends the DHCPREQUEST directly to the DHCP server. The DHCP server then responds directly to the client with the DHCPACK.

Because the client IP address is not on the same subnet to which the DHCP server is connected, either the DHCP server must have a route configured with next hop information or a routing protocol such as RIP must be running within the network. Alternatively, if you have active routers in your network, you must configure them to provide a route to the remote subnet where the clients generating the DHCP broadcasts reside.

In this scenario, RIP is not running on the AS/400 hosts, and subnets 10.1.0.0 and 10.1.2.0 are not joined by a router.

You must configure a static route within TCP/IP to ensure the DHCP servers know where to send the DHCP replies.

To configure routing information, perform the following steps:

- 1. From the AS/400 command line, specify `CFGTCPIP` and press Enter.
- 2. Select option **2**, Work with TCP/IP routes, and press Enter.
- 3. Specify a **1** to add routing information (see Figure 289).

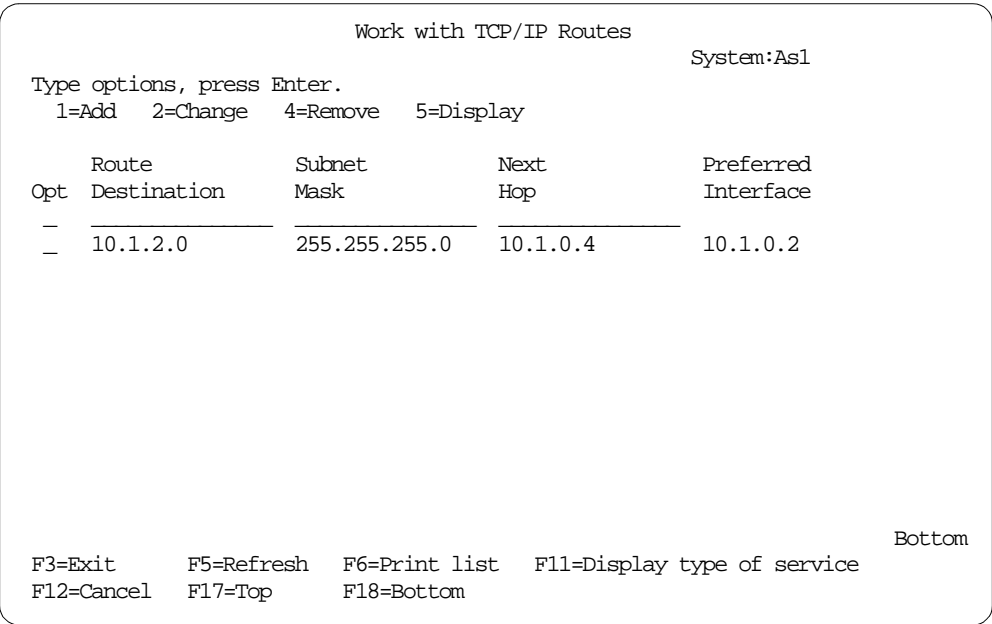


Figure 289. Routing Information on AS1 DHCP Server Required to Send Replies Directly to Clients

- 4. Repeat these steps for both DHCP servers. Ensure that you have set the Preferred Interface parameter correctly to 10.1.0.3 on *As2.mycompany.com*.
- 5. Test connectivity by pinging the remote subnet interface on the BOOTP/DHCP Relay Agent.

On *As1.mycompany.com* and *As2.mycompany.com*, specify the following command:

PING ('10.1.2.3')

You should receive a reply back.

14.2.6 Configuring a BOOTP/DHCP Relay Agent

It is simple to configure the AS/400 system to act as a BOOTP/DHCP Relay Agent. Remember that you cannot run the BOOTP/DHCP Relay Agent and the DHCP server on the same system simultaneously.

In this scenario, you are configuring AS/400 system AS5 as a BOOTP/DHCP Relay Agent to forward DHCP messages directly and without delay to the primary DHCP server, AS1. You are also configuring the AS/400 system to send the same DHCP messages to the backup DHCP server but also to delay the arrival of the message. This is done to ensure that the primary DHCP server replies first.

To configure the AS/400 BOOTP/DHCP Relay Agent, perform these steps:

1. Sign on to an AS/400 command entry session and specify the following command:
`CHGDHCPA MODE(*RELAY)`
Press Enter. This changes the mode of the DHCP server so that it can function as a BOOTP/DHCP Relay Agent.
2. From Operations Navigator, select
As5.mycompany.com>Network>Servers>OS400, and double-click **BOOTP/DHCP Relay Agent** (see Figure 290).

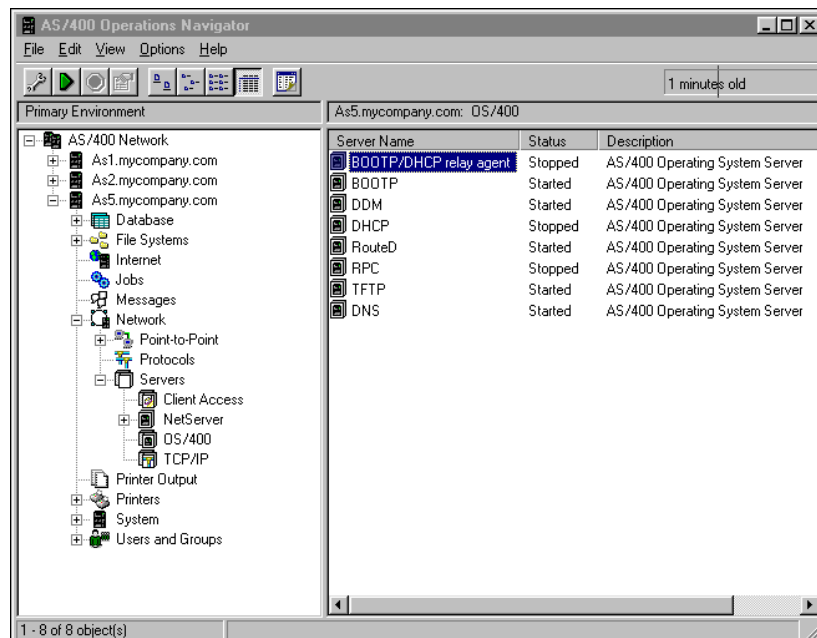


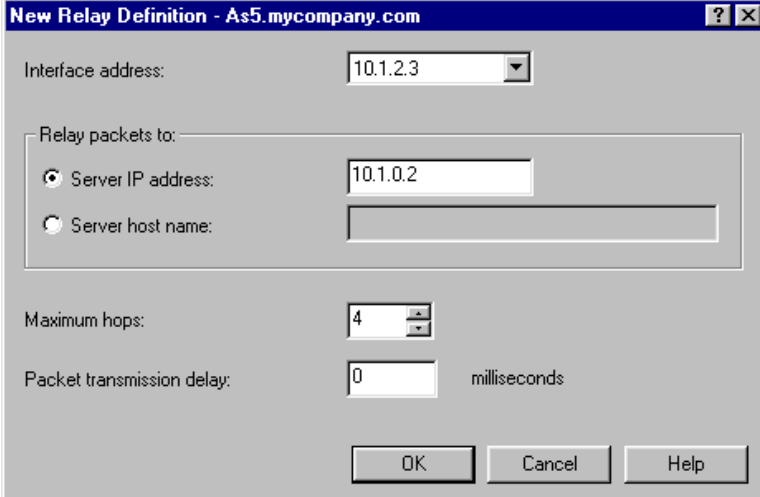
Figure 290. AS/400 Operations Navigator -- Starting BOOTP/DHCP Relay Agent

3. The BOOTP/DHCP Relay Agent properties window appears. Click *Start when TCP/IP is started* to ensure that it is checked.
4. Click **Add**.
5. Using the pull-down option on the *Interface address* field at the top of the window, select the TCP/IP interface on which the DHCP broadcast message arrives. This scenario uses 10.1.2.3.

6. Specify the IP address of the primary DHCP server to which the DHCP messages are sent. This scenario uses 10.1.0.2, the address on the primary DHCP server. Refer to Figure 291 on page 337.

Note: You can specify the system name if your DNS server can resolve the IP address or if you have correctly configured your host table.

7. Leave the *Packet transmission delay* value at zero.
8. Leave the *Maximum hops* value set to the default of 4.

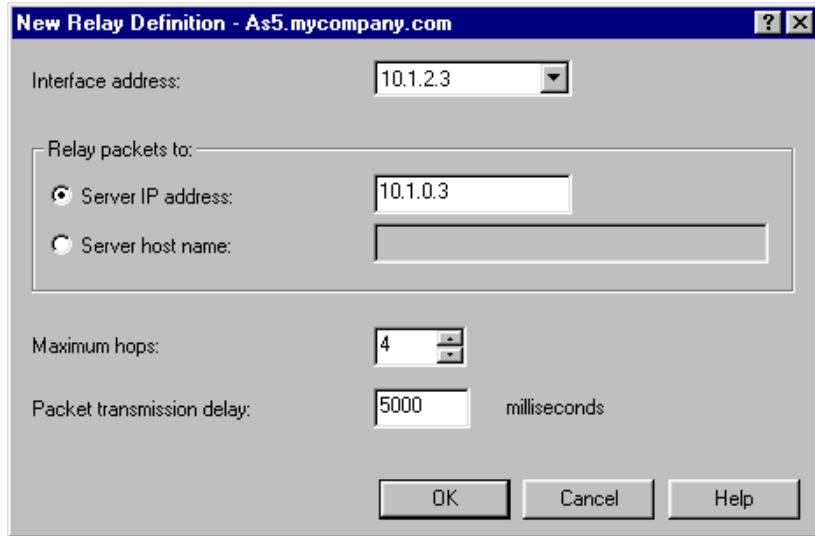


The screenshot shows a Windows-style dialog box titled "New Relay Definition - As5.mycompany.com". It contains the following fields and controls:

- Interface address:** A pull-down menu showing "10.1.2.3".
- Relay packets to:** A group box containing two radio buttons:
 - Server IP address:** Selected, with a text field containing "10.1.0.2".
 - Server host name:** Unselected, with an empty text field.
- Maximum hops:** A spin box set to "4".
- Packet transmission delay:** A text field set to "0" followed by the label "milliseconds".
- Buttons:** "OK", "Cancel", and "Help" at the bottom right.

Figure 291. BOOTP/DHCP Relay Agent Definitions

9. Click **OK**.
10. You are returned to the BOOTP/DHCP Relay Agent Properties dialog. Click **Add** to add the backup DHCP server information to the relay configuration.
11. Leave the *Interface address* pull-down menu on 10.1.2.3. If it is not already at this value, select this interface again.
12. In the *Server IP address* field, specify 10.1.0.3 as the IP address of the backup DHCP server (see Figure 292 on page 338).
13. Change the *Packet transmission delay* value to 5000 milliseconds. This delays the forwarding of the DHCP messages to the backup DHCP server by 5 seconds.
14. Leave the *Maximum hops* value set to the default of 4.



The dialog box 'New Relay Definition - As5.mycompany.com' contains the following fields and controls:

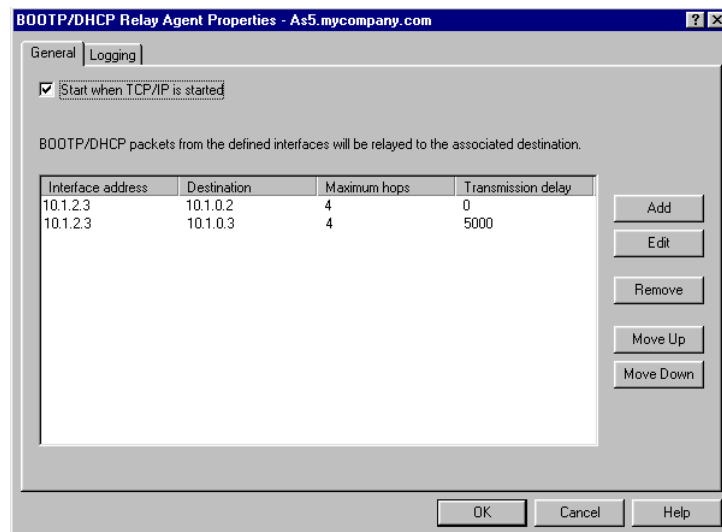
- Interface address:** A dropdown menu showing '10.1.2.3'.
- Relay packets to:** A group box containing:
 - Server IP address:** A radio button (selected) and a text box containing '10.1.0.3'.
 - Server host name:** A radio button (unselected) and an empty text box.
- Maximum hops:** A spin box set to '4'.
- Packet transmission delay:** A text box containing '5000' followed by the label 'milliseconds'.
- Buttons:** 'OK', 'Cancel', and 'Help' at the bottom right.

Figure 292. Relay Forwarding Configuration to the Backup DHCP Server

15. Click **OK**.

16. Click **OK**.

Figure 293 shows that any DHCP messages arriving on the 10.1.2.3 interface are forwarded to 10.1.0.2, the primary DHCP server. The BOOTP/DHCP Relay Agent forwards the packets to the backup DHCP server (interface 10.1.0.3) with a 5-second delay.



The dialog box 'BOOTP/DHCP Relay Agent Properties - As5.mycompany.com' has two tabs: 'General' (selected) and 'Logging'.

- General Tab:**
 - Start when TCP/IP is started:** A checked checkbox.
 - Description:** 'BOOTP/DHCP packets from the defined interfaces will be relayed to the associated destination.'
 - Table:**

Interface address	Destination	Maximum hops	Transmission delay
10.1.2.3	10.1.0.2	4	0
10.1.2.3	10.1.0.3	4	5000
 - Buttons:** 'Add', 'Edit', 'Remove', 'Move Up', and 'Move Down' are located to the right of the table.
- Bottom Buttons:** 'OK', 'Cancel', and 'Help'.

Figure 293. BOOTP/DHCP Relay Agent Configuration

14.2.7 Configure the Microsoft NT BOOTP/DHCP Relay Agent

In this scenario, the Windows NT BOOTP/DHCP Relay Agent is located on the far side of a routed network. You must configure the NT BOOTP/DHCP Relay Agent to always forward each DHCP message to the AS/400 BOOTP/DHCP Relay Agent, *As5.mycompany.com*.

To configure the NT server to act as a BOOTP/DHCP Relay Agent, perform the following steps:

1. Double-click **My Computer** on the desk top.
2. Double-click **Control Panel**.
3. Double-click **Networks**.
4. Click the **Services** tab.
5. Click **Add**.
6. Select BOOTP/DHCP Relay Agent from the list and click **OK**.

Insert the appropriate Windows NT installation CDROM.

7. Click **OK**.
8. Click the **Protocols** tab.
9. Right-click **TCP/IP** to open a context menu and select **Properties**.
10. Click the **DHCP Relay** tab.
11. Change the *Seconds threshold* value to zero seconds.
12. Leave the *Maximum hops* value field at 4.

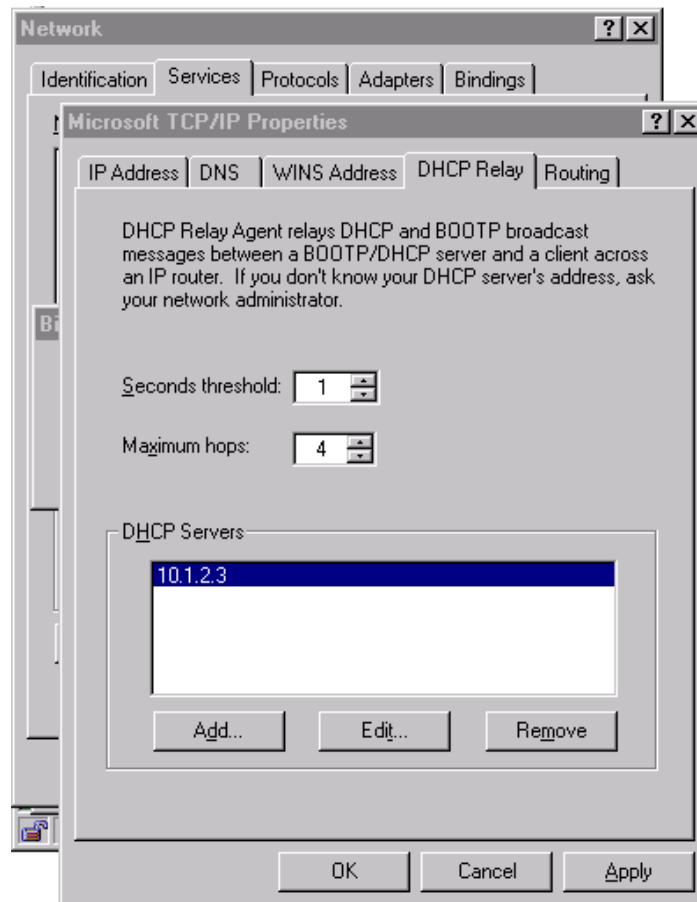


Figure 294. Windows NT BOOTP/DHCP Relay Agent Configuration

13. Click **Add**.

14. Specify 10.1.2.3 as the IP address of the AS/400 BOOTP/DHCP Relay Agent.
15. Click **Add**.
16. Click **OK**.
17. Select **Yes** to shut down the NT server.

The NT BOOTP/DHCP Relay Agent is now configured to send DHCP messages from subnet 10.1.3.0 to the AS/400 BOOTP/DHCP Relay Agent *As5.mycompany.com*. It is also configured for forwarding to both DHCP servers.

14.2.8 Start the DHCP Servers and BOOTP/DHCP Relay Agents

The first time you start the DHCP servers and BOOTP/DHCP Relay Agents, you must perform the start-up procedure in an ordered manner. Because DHCP clients remember and attempt to gain the same IP address they last used, you must start the primary DHCP server first. Follow this by starting the primary AS/400 BOOTP/DHCP Relay Agent and then the NT BOOTP/DHCP Relay Agent. Start the backup DHCP server last.

Note: If you receive an error message when attempting to start either the DHCP server or the BOOTP/DHCP Relay Agent, ensure that neither the BOOTP server nor the DHCP server is running while you start the relay agent.

The order to start the systems in listed format is as follows:

1. Start the Primary DHCP server, *As1.mycompany.com*.

From Operations Navigator, right-click **DHCP** to open a context menu and select **Start** (see Figure 295 on page 341). Alternatively, on an AS/400 command entry display, you can enter the following command:

```
STRTCPSVR SERVER(*DHCP)
```

2. Start the AS/400 BOOTP/DHCP Relay Agent, *As5.mycompany.com*.

From Operations Navigator, right-click on **BOOTP/DHCP relay agent** to open a context menu and select **Start**, (see Figure 296). Alternatively, on an AS/400 command entry display, you can enter the command:

```
STRTCPSVR SERVER(*DHCP)
```

3. Start the Windows NT BOOTP/DHCP Relay Agent, *R2.mycompany.com*.

Click **OK**.

4. Start the backup DHCP server, *As2.mycompany.com*.

From Operations Navigator, right-click **DHCP** to open a context menu and select **Start** (see Figure 296 on page 341). Alternatively, on an AS/400 command entry display, you can enter the command:

```
STRTCPSVR SERVER(*DHCP)
```

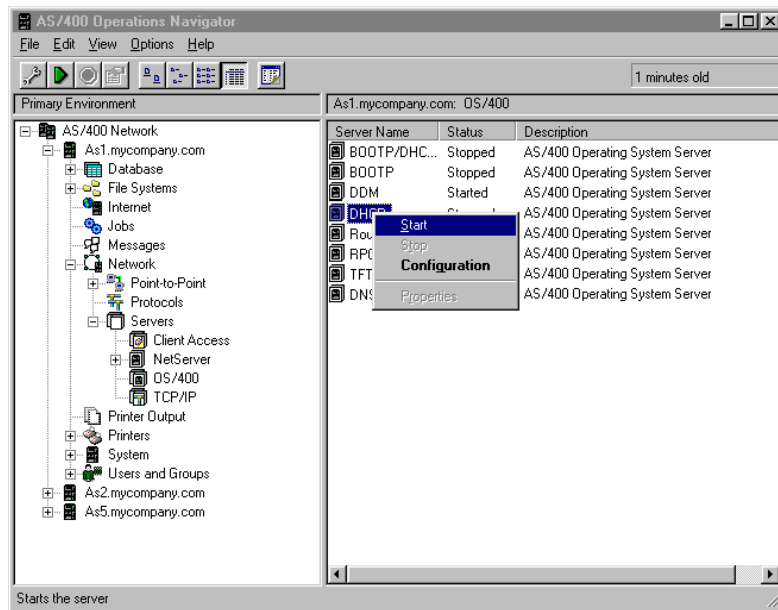


Figure 295. Starting the Primary DHCP Server

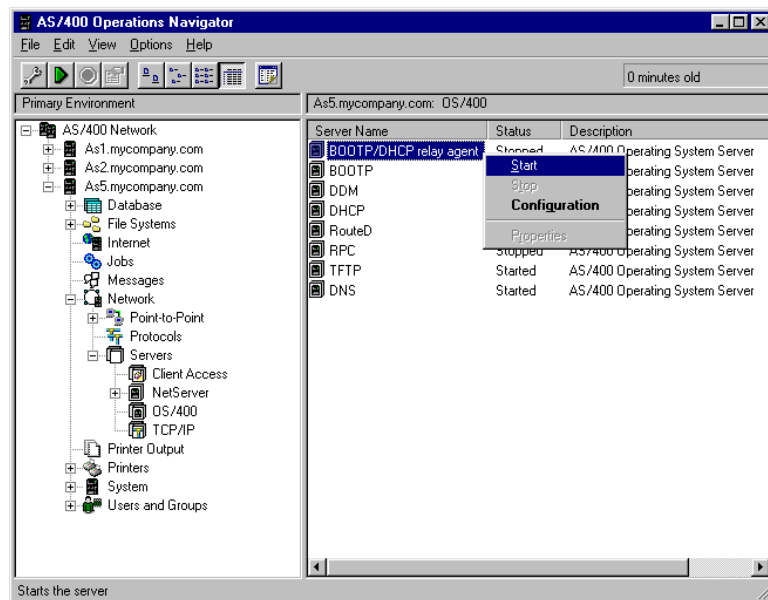


Figure 296. Starting the BOOTP/DHCP Relay Agent on As5.mycompany.com

14.3 Summary

This scenario configured a multi-subnetted network. It provided complete fall-back support in the event that the primary DHCP server fails for subnets 10.1.0.0 and 10.1.3.0. Partial support of approximately 30% for the subnet 10.1.2.0 was provided. This was due mainly to the addressing scheme and the use of the 70/30 split technique.

On DHCP servers AS1 and AS2, you configured a TCP/IP route to reach the remote subnets through AS5.

You configured an AS/400 BOOTP/DHCP Relay Agent to forward DHCP messages to both the primary and backup DHCP servers. You also biased the primary by making a delay when sending messages to the back-up DHCP server. Using this method allowed the primary DHCP server to respond first to the client.

You also configured an NT BOOTP/DHCP Relay Agent on a remote subnet joined by a router or gateway that forwards DHCP messages from subnet 10.1.3.0 to the AS/400 BOOTP/DHCP Relay Agent.

In the event that the primary DHCP server fails, no change is required in the configuration of the DHCP servers and DHCP relay agents. If the NT BOOTP/DHCP Relay Agent fails, the clients on the subnet 10.1.3.0 are unable to connect.

Chapter 15. Configuring Twinax IBM Network Station with DHCP

The BOOTP protocol was developed for bootstrapping, and it is the predecessor of DHCP. Previous chapters showed how to provide initial configuration to LAN-attached IBM Network Stations using the DHCP server. This chapter describes how to use DHCP to configure twinax-attached IBM Network Stations. It also introduces the concepts of *transparent subnetting* and *Proxy ARP*. This concept is necessary to understand routing concepts for DHCP clients that are attached to twinax workstation controllers on an AS/400 system.

With V4R2 comes the ability to run the TCP/IP protocol encapsulated within Twinaxial Data Link Control (TDLC) frames. This gives you the ability to replace 5250 type devices, which are attached through the local workstation controller with IBM Network Stations without having to change your investment in cabling. The IBM Network Station gives users the ability to access your intranet or the Internet while still keeping the same 5250 emulation displays to which they are accustomed. The twinax-attached IBM Network Stations coexist with other non-TCP/IP 5250 devices on the same controller.

TCP/IP over twinax is introduced in V4R2 to support twinax-attached IBM Network Stations 8361 Model 341. IBM Network Station Manager release 3.0 (5648-C05) is required.

There are a number of distance limitations on any twinax workstation controller when used in express mode. Refer to the following URLs for further information: www.networking.ibm.com/525xpres/525xwire.html or www.networking.ibm.com/525xpres/525xpress.html for Express support.

No previous releases of OS/400 or Network Station Manager support the IBM Network Station model 341.

To accommodate the TCP/IP twinax subnet into your addressing scheme and to allow the twinax subnet access to the LAN and beyond, the AS/400 system utilizes a concept called *transparent subnet masking*. The implementation is based on RFC 1027, "Using ARP to Implement Transparent Subnet Gateways." All hosts that implement transparent subnetting use a variable length mask to identify the different subnets.

The DHCP configuration in Operations Navigator is *twinax aware*. From a DHCP administrator's point of view, it is easy to configure the twinax-attached IBM Network Stations if you understand the addressing structure of the network.

15.1 Getting Started: Basic IP over Twinax Configuration

This scenario shows how to get started with IP over twinax. It demonstrates how to configure a simple environment where one AS/400 system has IBM Network Stations attached by way of twinax. The network in this scenario is mainly SNA, and the only TCP/IP connection besides the twinax-attached IBM Network Stations is a connection to the Internet by way of a firewall. The IBM Network Stations on the twinax network are used for 5250 emulation to the attached host and for Web browsing through the firewall.

15.1.1 Scenario Overview

This scenario has one AS/400 system with one TCP/IP connection to a firewall. All other network connectivity to the host is through SNA. This scenario greatly simplifies the TCP/IP addressing considerations that you encounter in a TCP/IP-based network.

The IBM Network Stations are used to run 5250 emulation to the attached host and for Internet access, such as Web browsing.

This scenario does not discuss the firewall configuration.

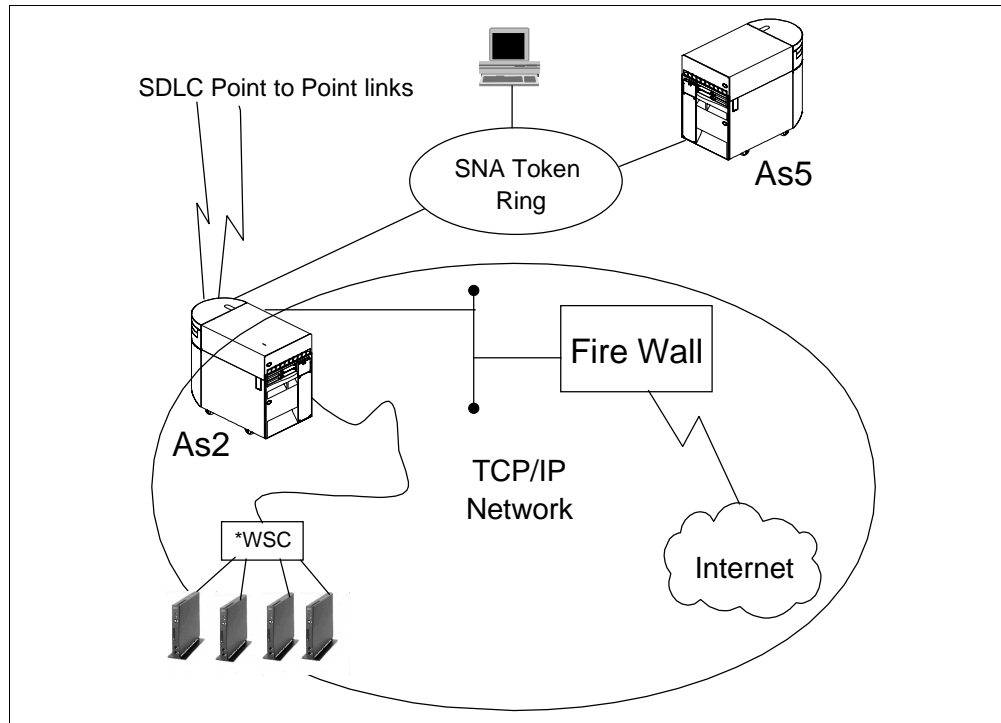


Figure 297. Basic IP over Twinax Configuration -- Scenario Overview

15.1.2 Scenario Objectives

The objectives of this scenario are as follows:

- Configure twinax-attached IBM Network Stations.
- Configure DHCP server to support the twinax subnet.
- Allow the twinax-attached IBM Network Stations connectivity to the Internet.

15.1.3 Scenario Advantages

The advantages of this scenario are that it:

- Is simple to implement.
- Allows Internet access for the twinax-attached devices with minor configuration changes.
- Requires few TCP/IP address considerations and planning steps.

15.1.4 Scenario Disadvantages

The disadvantages of this scenario are that:

- No consideration has been given to the future growth of the TCP/IP network.
- The IBM Network Stations are unable to directly access the host, AS5.
They are required to connect to AS2 and then pass through (STRPASTHR) to the host, AS5.
- Only TCP/IP-attached devices gain Internet Web access.

15.1.5 Scenario Network Configuration

Figure 298 shows the logical network topology of the simple TCP/IP network. None of the SNA network nodes or control points are shown.

Configure the twinax subnet to use a small portion of the 10.1.1.0 address space.

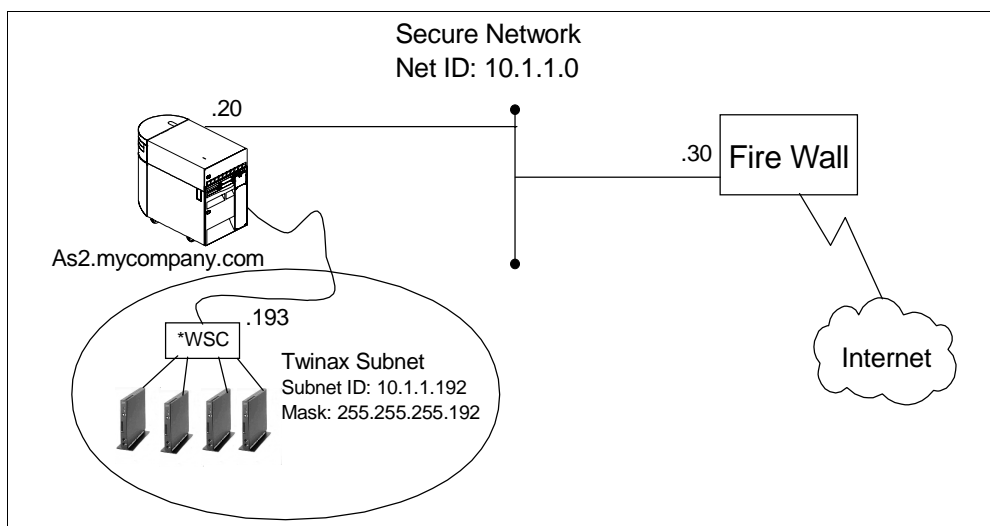


Figure 298. Logical Network Topology of the TCP/IP Network Only

15.1.6 Task Summary

The following list is a high-level view of the tasks required to implement this scenario:

1. Define a TCP/IP address range to use on the twinax subnet.
2. Configure and start the DHCP server on AS2 to support the twinax subnet.
3. Start the IBM Network Station.

15.1.7 Define a TCP/IP Address Range

Use an IP address range on your twinax subnet that is a subset of the overall network address 10.1.1.0. This automatically gives the twinax-attached IBM Network Stations connectivity to the firewall for incoming and outgoing network traffic. This method of using a chunk of address space from the LAN utilizes Proxy ARP and is called *transparent subnet masking*. For more information on transparent subnetting and Proxy ARP, refer to Section 15.2, "Transparent Subnet Masking" on page 352.

The addresses used on the twinax subnet must be contiguous. You can assign a maximum of 64 contiguous addresses.

Use the IP address range of 10.1.1.192 through 10.1.1.254 on the twinax subnet.

You must ensure that the addresses contained in this range are not used anywhere else within the network.

15.1.8 Configure and Start the DHCP Server on AS2

You are configuring DHCP on a system without an existing configuration. Operations Navigator automatically starts the DHCP Configuration Wizard, which helps create a basic, twinax DHCP server configuration.

Tip

If you want to reset an existing configuration and start over, select File -> New Configuration from Operations Navigator.

To start the DHCP configuration wizard, perform the following steps:

1. Start Operations Navigator.
2. Click *As2.mycompany.com* to select the system.

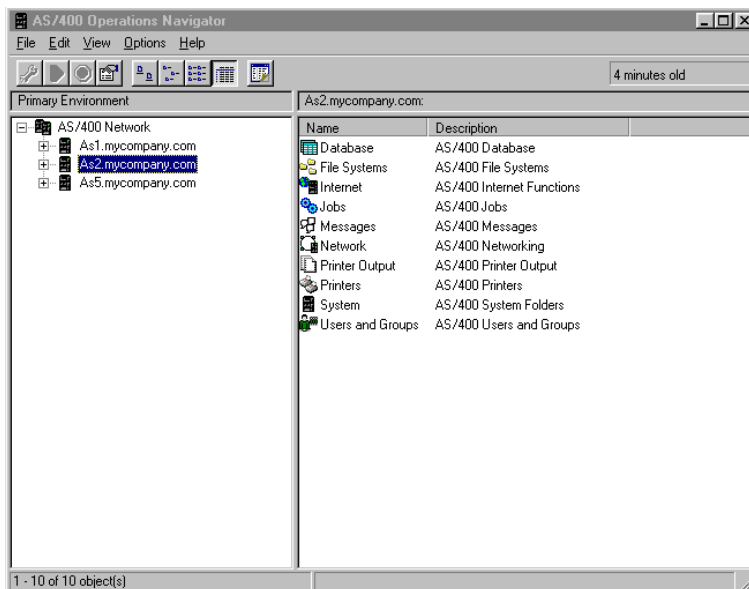


Figure 299. Operations Navigator -- Selecting the System to Configure DHCP Server

3. Double-click **Network**.
4. Double-click **Server**.
5. Double-click **OS/400**.
6. Double-click **DHCP** to start the DHCP configuration wizard.

Note

If the DHCP configuration wizard does not appear, it is likely that a DHCP configuration already exists. To start the wizard and replace the existing configuration, select **New Configuration** from the **File** menu.

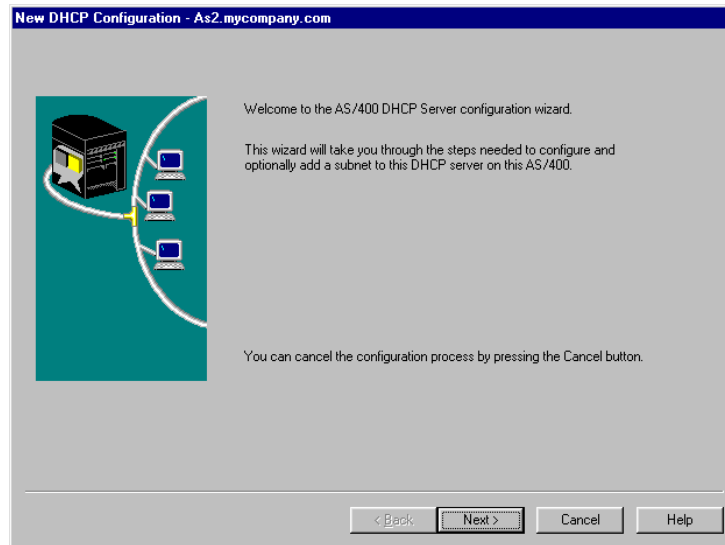


Figure 300. The DHCP Configuration Wizard

7. Click **Next**.
8. Select **Yes** to add a new subnet to the DHCP server.
9. Answer **Yes** to the question "Will this subnet manage twinax devices?"
10. Specify 10.1.1.193 as the IP address to use for the twinax controller (see Figure 301). Click **Next**.

The first usable address in the subnet defined for the twinax network should be used for the workstation controller. 10.1.1.192 is a subnet boundary and cannot be used to address a device.

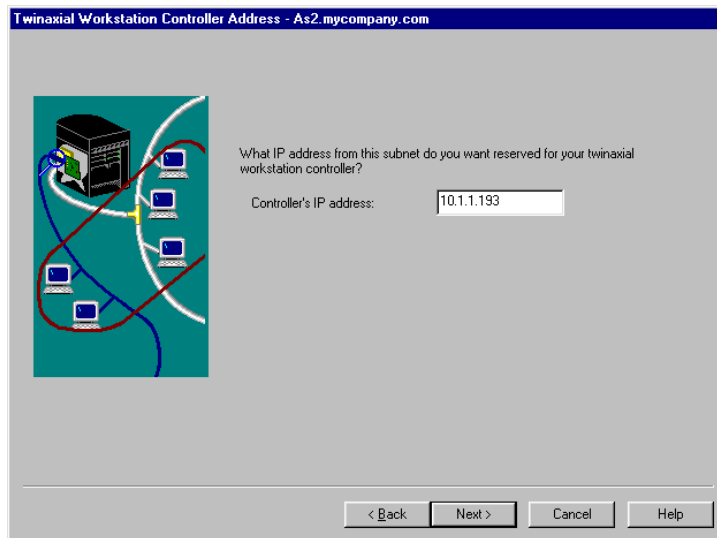


Figure 301. Specify the IP Address to be Used by the Workstation Controller

11. Specify the subnet name, description, and the range of addresses to use within the subnet (in this case, specify all 64). Supply a subnet mask (see Figure 304).

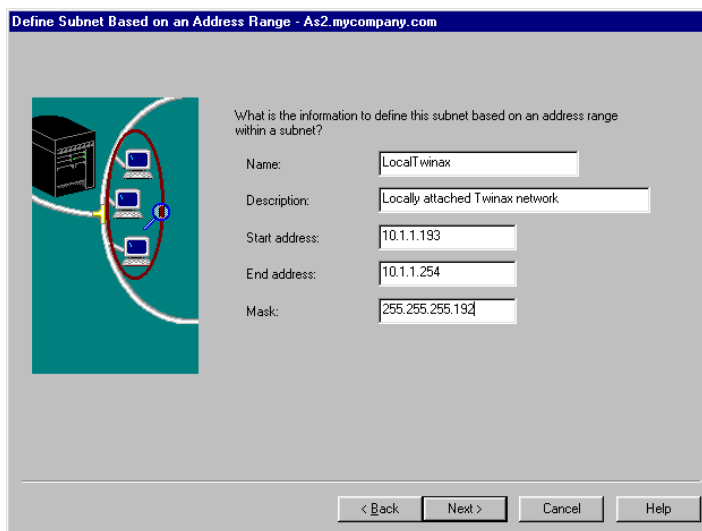


Figure 302. Twinax Subnet Configuration

12. Specify a lease time for the client to keep the address served. Specify the lease time as *never expire*. Selecting a large lease renewal value reduces the lease renewal request traffic on your twinax network.
13. Click **Yes** to have the DHCP server deliver the IP address of the firewall Domain Name Server to the twinax-attached IBM Network Stations.
14. Click **Add** and specify the address 10.1.1.30, which is the firewall's secure port IP address.

Note: To resolve host names in the Internet name space, the IBM Network Station client must use the firewall DNS. No internal DNS is available in the secure network for this scenario.

15. Click **Next**.

16. Answer **No** to the question "Would you like to set other options for this subnet?" These are added later. Click **Next**.

17. Select **Yes** to start the DHCP server when TCP/IP starts, and Select **No** to start the DHCP server now. Click **Next**.

18. The DHCP configuration summary window shows all the options that you have selected so far. Click **Finish**.

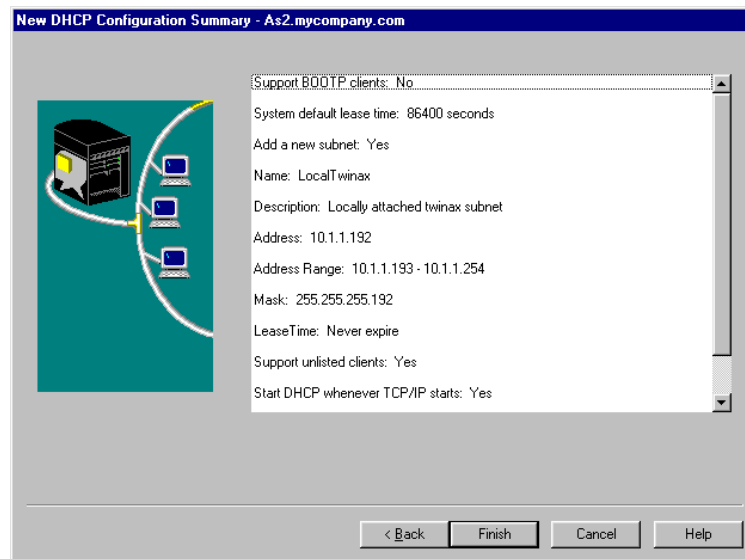


Figure 303. DHCP Configuration Summary

19. Now the DHCP server configuration is displayed. Right-click the subnet called *LocalTwinax* to open a context menu and select **Properties** (see Figure 304).

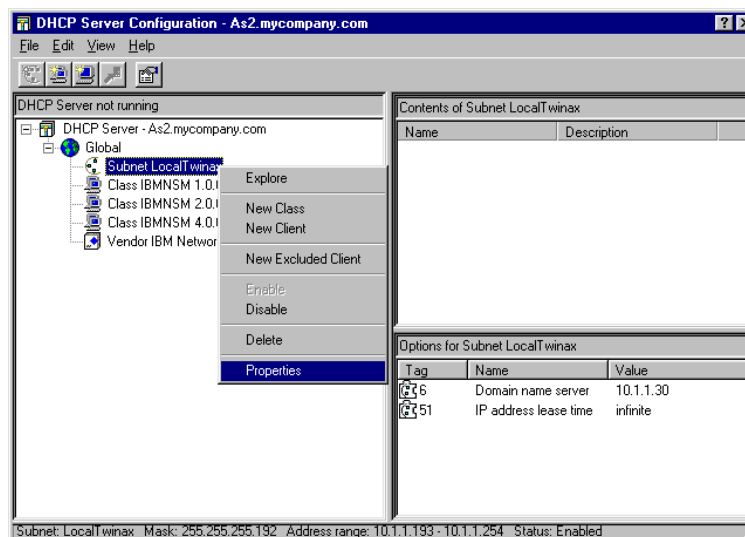


Figure 304. DHCP Server Configuration

20. Ensure that the **General** tab is selected. Click the check box labeled *Twinax subnet*.

21. Specify 10.1.1.193 as the IP address of the workstation controller (see Figure 305).

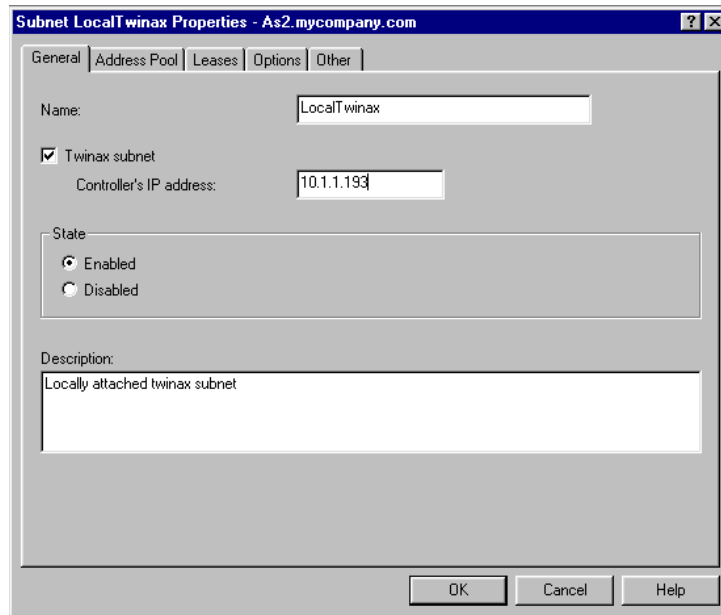


Figure 305. Adding a Twinax Subnet in the DHCP Configuration

You must also serve the subnet mask and other options to the clients.

22. Click the **Options** tab to add a subnet mask that is served to the clients.
23. Highlight option **1, subnet mask**, from the *Available options* window and click **Add**.
24. Specify the mask 255.255.255.192 for the clients to use in the Subnet mask window at the bottom of the display (see Figure 306).
25. Highlight option **3, Router**, from the *Available options* window and click **Add** (see Figure 306).
26. Specify the router or gateways IP address. The gateway for the twinax subnet is the workstation controller at IP address **10.1.1.193** (see Figure 306).
27. Highlight option **66, Server name**, from the *Available options* window and use the workstations controllers address of **10.1.1.193** (see Figure 306).
28. Verify option **67, Boot file name**, from the *Available options* window for the IBM Network Station class. It should be **/QIBM/ProdData/NetworkStation/kernel** (see Figure 306).

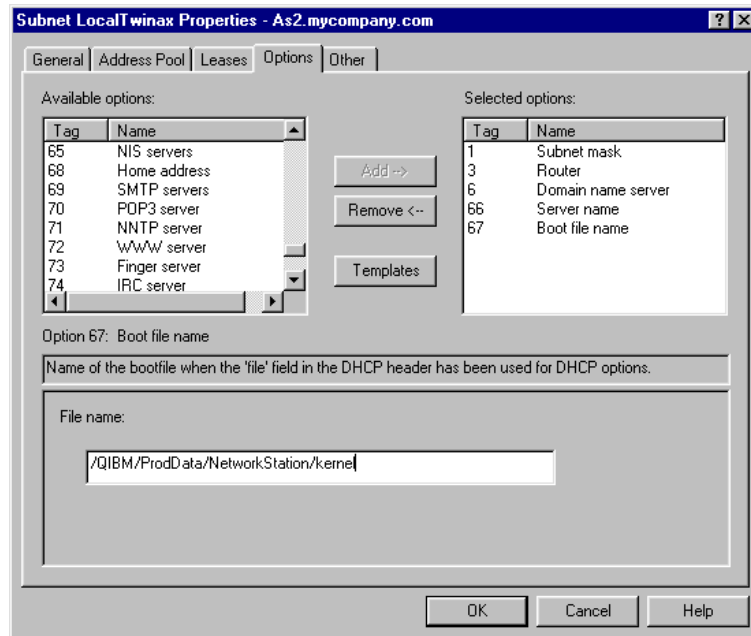


Figure 306. DHCP Server Options

29. Click **OK**.

30. Close the DHCP configuration display.

31. Right-click **DHCP** from Operations Navigator to open a context menu. Select **Start**.

The DHCP server is now running and configured only to serve the local twinax subnet.

15.1.9 Start the IBM Network Station

The twinaxial-attached network stations are different from the normal token-ring or Ethernet stations. The NVRAM options are presented differently, although functionally they remain the same. Details about the differences and new features of the IBM Network Station are outside the scope of this book.

It is also assumed that you have cabled the twinax IBM Network Station correctly.

Note

The twinax IBM Network Station requires that you specify the address to use on the port to which it is connected. Therefore, if you are replacing non-programmable terminals with the IBM Network Station, make a note of the address the old device was using, such as port 02 and address 05. Otherwise, you must ensure that no other device is configured to use the same address on the same port.

When the twinax IBM Network Station is first powered on, it prompts you to specify the address to use for the port to which it is connected. This is not the TCP/IP address. It is an address from 0 to 6 to use on the workstation controller port to which the IBM Network Station is connected.

To configure the IBM Network Station for use over twinax, perform the following steps:

1. Power on the IBM Network Station.
2. Specify the local controller address to use when prompted to do so. Press Enter.

The IBM Network Station checks to see if anyone else is using that address. If not, it uses DHCP to default to startup and continues to boot until completion, provided the DHCP server is started.

Detailed instructions on how to reset the IBM Network Station to factory defaults is described in Section 15.4.4.1, "Resetting NVRAM" on page 370.

For a detailed reference of the startup tasks that occur when the first twinax attached IBM Network Station is powered on, refer to Section 15.4.4.2, "The Startup Sequence" on page 371.

15.1.10 Summary

This scenario attached IP over twinax devices to a local workstation controller on *As2.mycompany.com*.

It also used a contiguous chunk of IP addresses from the network 10.1.1.0 for the twinax subnet.

You configured and started the DHCP server on *As2.mycompany.com* to service the twinax subnet.

The IBM Network Station was powered on and the necessary line, controller, device, and TCP/IP interface for the workstation controller was built automatically.

15.2 Transparent Subnet Masking

Transparent subnet masking is new to the AS/400 system in V4R2. It uses variable length masks to identify the different subnets and, in terms of connectivity, allows IP over twinax devices to appear as though they were on the local network. The AS/400 system implementation is based on RFC1027, "Using ARP to Implement Transparent Subnet Gateways."

The term *transparent subnet masking* is slightly misleading. Another way to describe it is with the term *IP address grouping*. Using different masks over the same network ID, you can segment or group contiguous ranges of IP addresses together to use either for twinax subnets or for remote LANs attached to the AS/400 host. The transparency part comes into play when Proxy ARP is enabled, which happens automatically when the hosts on the network share the same network ID. In effect, the subnetting within your network is transparent because a router or gateway is not required to join the subnets.

Note

The twinax subnet requires a contiguous range of TCP/IP addresses to be assigned to it. You cannot use any address at random from the pool and dynamically allocate an address to a device on the twinax subnet. We recommend, therefore, that you assign the maximum amount of TCP/IP addresses, which is 64, to the twinax subnet if you can. If you assign up to 64 addresses to the twinax subnet, you can easily add additional IP over twinax devices without having to change or shuffle any IP addressing schemes within your network. The limit of 64 devices is imposed by the workstation controller.

Figure 307 shows an example of a network that is using transparent subnet masking and Proxy ARP.

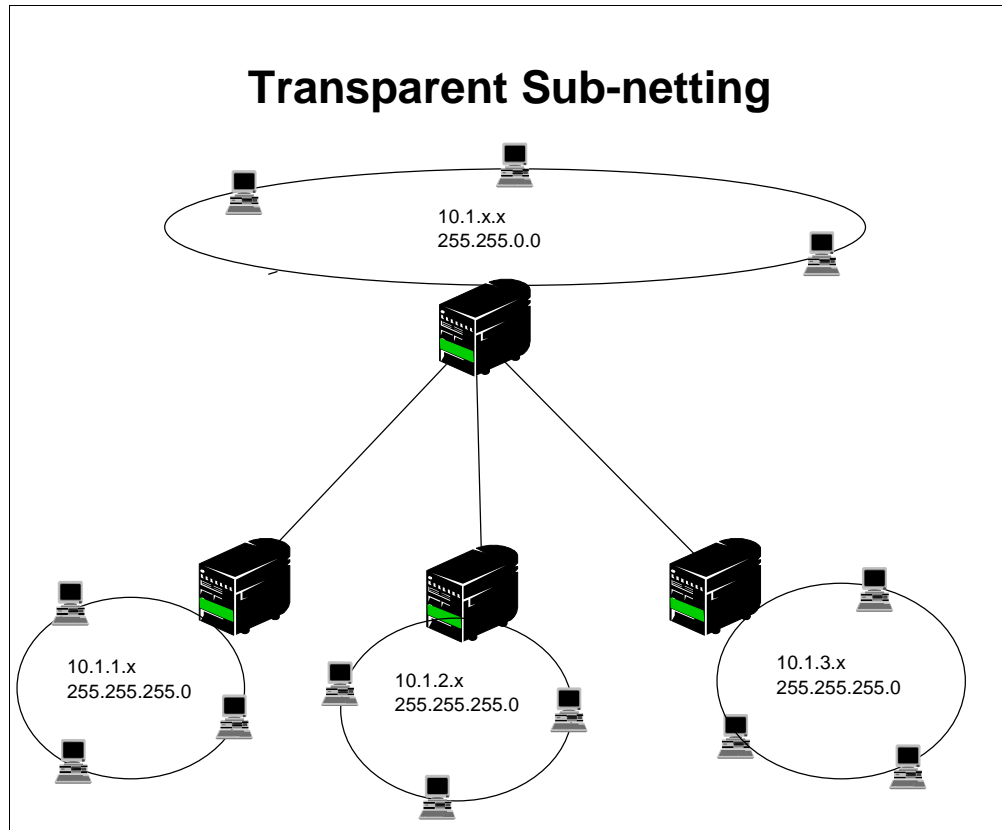


Figure 307. Transparent Subnetting Example

Figure 307 shows that all the networks and hosts are on the same TCP/IP network ID, 10.1.x.x. The figure is somewhat simplistic, but it shows the concept that, even though the three remote networks are on subnets different from the main ring, each host is the Proxy ARP agent for the subnet beneath it.

15.2.1 ARP and Proxy ARP

IP addresses only make sense to the TCP/IP protocol suite. LAN addresses (for example, Ethernet or token ring) are used when an Ethernet frame is sent from one host in the LAN to another. RFC 826 deals with Address Resolution Protocol.

Its purpose is to present a method for converting protocol addresses (IP Addresses) to LAN addresses (for example, Ethernet or Token Ring). Figure 308 shows ARP (address resolution protocol) and RARP (reverse address resolution protocol).

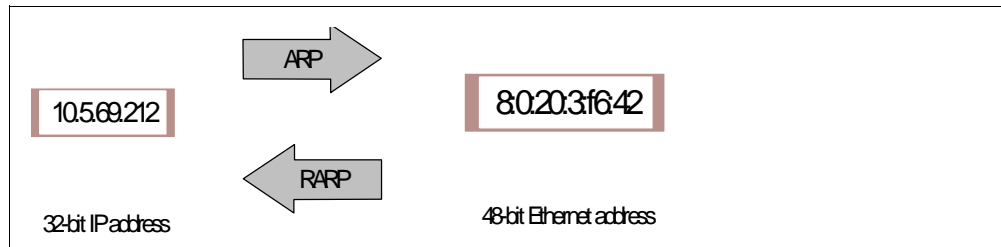


Figure 308. Mapping between 32-Bit IP Address and 48-Bit Ethernet Address

Figure 309 shows how the ARP cache is built in each host.

1. The TCP/IP protocol on HOST A decides that it wants to transmit to target HOST B at IP address IP(B).
2. The sending host, HOST A, must convert the 32-bit IP address into the 48-bit Ethernet address (assuming Ethernet LAN). This is the function of ARP.
3. ARP broadcasts an *ARP request* to all the hosts in the network containing HOST B IP address, IP(B), and asking whomever is HOST B to respond with the hardware address MAC(B).
4. The HOST B recognizes that IP(B) is a local interface and sends back its hardware address (Ethernet, for example), MAC(B), to HOST A in an *ARP reply*.
5. Now HOST A knows HOST B's hardware address and sends the IP datagram to it.

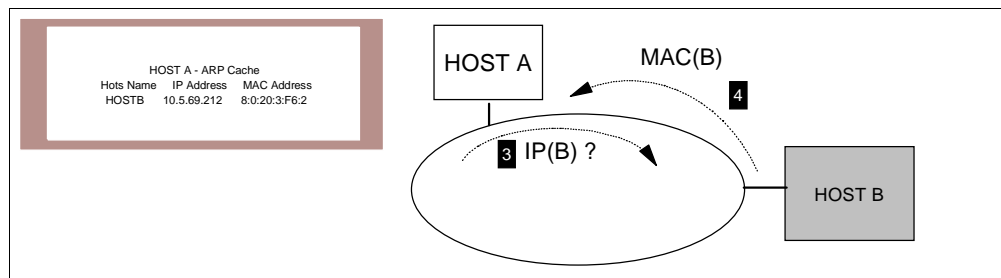


Figure 309. Building the ARP Cache

To make the operation of ARP more efficient, each hosts maintains an ARP cache with the most recent mappings from IP addresses to hardware addresses.

If hosts A and B are on different networks, HOST B does not receive the ARP broadcast request from HOST A and cannot respond to it. However, if both physical networks are connected by a gateway, the gateway sees the ARP request from HOST A. The gateway also knows, based on subnet number, that the request is for a host on a different physical network (assuming that subnet numbers are made to correspond to physical networks). The gateway then acts as an agent for HOST B, responding to the ARP request from HOST A on behalf of HOST B with the gateway's hardware address. HOST A sees the reply, caches

it, and sends future IP packets for HOST B to the gateway. The gateway is acting as an agent for HOST B. This technique is called *Proxy ARP*. Proxy ARP is discussed on RFC 1027. Figure 310 illustrates this concepts.

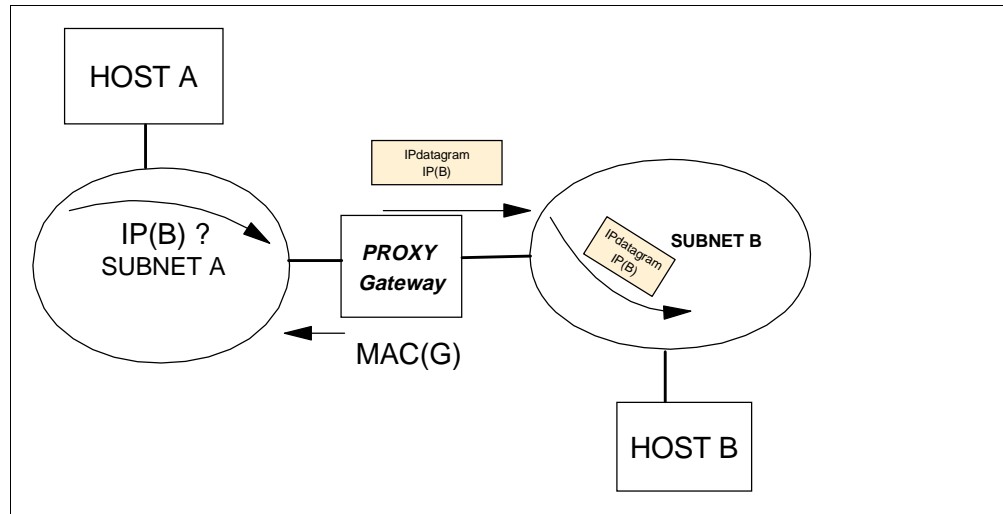


Figure 310. Proxy ARP

Provided that all hosts and devices are on the same network ID, Proxy ARP permits the AS/400 system to join subnets in a fashion similar to the way a router forwards packets from one subnet to another. This scenario implements the class A network ID of 10.0.0.0. While some hosts are on different subnets of the network ID, they are all part of the network 10.0.0.0. Proxy ARP is enabled automatically on the AS/400 system when hosts share a common network ID.

Proxy ARP is useful with twinax-attached devices running TCP/IP because it allows the twinax device to appear as part of the local network.

Figure 311 on page 356 shows a scenario where the twinax devices are on subnet 10.1.1.192 with the mask of 255.255.255.192. The first hop or gateway off their subnet is the workstation controller 10.1.1.193, which has the same mask. The AS/400 host (AS2) is attached to the LAN 10.1.1.0 with a different mask of 255.255.255.0 through a token-ring interface. The AS/400 system is aware of two local networks, the twinax subnet and the IP LAN.

It is the mask setting on the twinax interface that determines the block of addresses for which the IP LAN interface on the AS/400 system needs to Proxy ARP. In this example, the IP LAN interface on the AS/400 system proxies for addresses 10.1.1.192 through 10.1.1.255. The *associated local interface* specified on the twinax TCP/IP interface tells the TCP/IP stack which LAN IP interface is doing the proxying for the twinax subnet. Figure 311 provides an overview of the AS/400 system implementation of Proxy ARP to support twinax-attached IBM Network Stations.

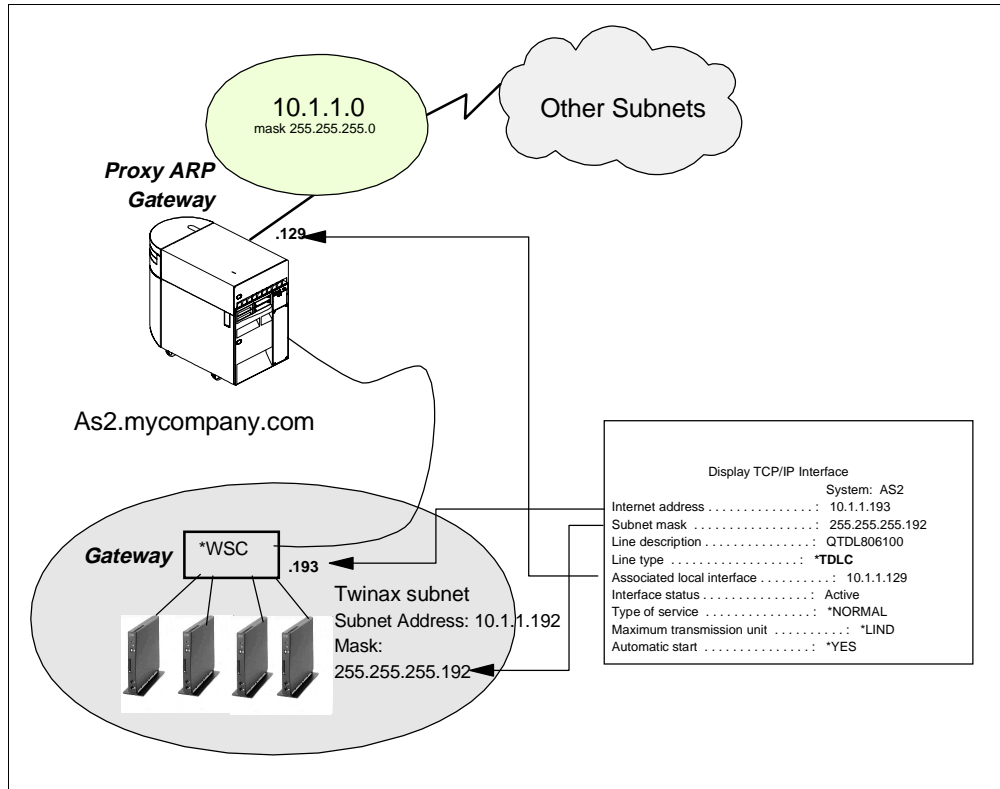


Figure 311. Using Proxy ARP to Support Twinax IBM Network Station -- AS/400 System Implementation

A remote, LAN-attached host with a packet to send to one of the twinax-attached devices knows the twinax device IP address, but the IP stack on the host does not know the MAC address of the twinax device. This is essential to completing the datagram and placing it on the network. The source system sends out a broadcast ARP request containing the IP address of the target but not the MAC address. The target AS/400 system (that is, the AS/400 system with the attached twinax devices, AS2) intercepts the ARP broadcast because it knows that the IP address in the ARP packet falls within the range of addresses of the twinax subnet. The AS/400 associated local interface places *its own* MAC address into the ARP reply. From this point on (or until the ARP cache expires on the remote host), all traffic to the devices on the twinax subnet is sent to the MAC address of the AS/400 associated local interface. The AS/400 system forwards the packet to the twinax device.

For outbound traffic from the twinax subnet to a remote host, the twinax workstations forward datagrams to their gateway (the workstation controller), and the gateway passes them on to the AS/400 system. The AS/400 system uses simple IP routing to determine on which interface the datagram belongs.

15.2.2 Twinax Transparent Subnetting

The twinax subnet requires a contiguous range of TCP/IP address to be defined and allocated to it. Figure 312 is useful in determining which mask to apply and what range or contiguous groups of addresses you can use.

Look at Figure 312 for an example. If you use a mask of 128 in the last octet, you effectively have two address ranges, .1 to .126 and .129 to .254. The subnet boundary addresses .127 and .128 cannot be used.

The same applies for a mask of .240. This mask gives you 16 groups of 16 (-2) contiguous addresses. Refer to Figure 312 again. The boundary addresses cannot be used.

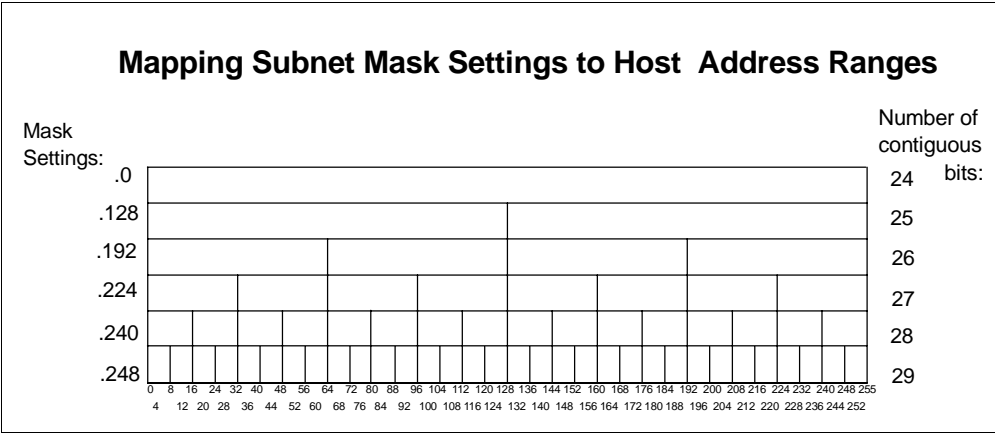


Figure 312. Subnet Mask Boundaries and Address Ranges

Note:

- A Host ID of all 0s is a special case and cannot be assigned.
- A Host ID of all 1s is a special case (broadcast) and cannot be assigned.
- Subnets with mask 252 are used primarily as point-to-point networks (there are only two usable host IDs).
- A mask of 254 is not valid and is unacceptable.
- You can use subnets with a mask of 255 to map a single IP address to an unnumbered point-to-point network.

The next example uses a class C TCP/IP address that has been divided into four different groups or address ranges. Assign three subnet groups for three different TCP/IP over twinax networks and leave a large range of addresses available for the rest of the network.

Note

This example does not follow the recommendation of allowing a maximum contiguous range of 64 TCP/IP addresses allocated to the twinax subnet. It is intended to provide an example of transparent subnetting. Unless you are forced by your IP addressing scheme to use an example such as this, allocate the maximum number of IP addresses to the twinax subnet. This recommendation is made for future proofing rather than functionality.

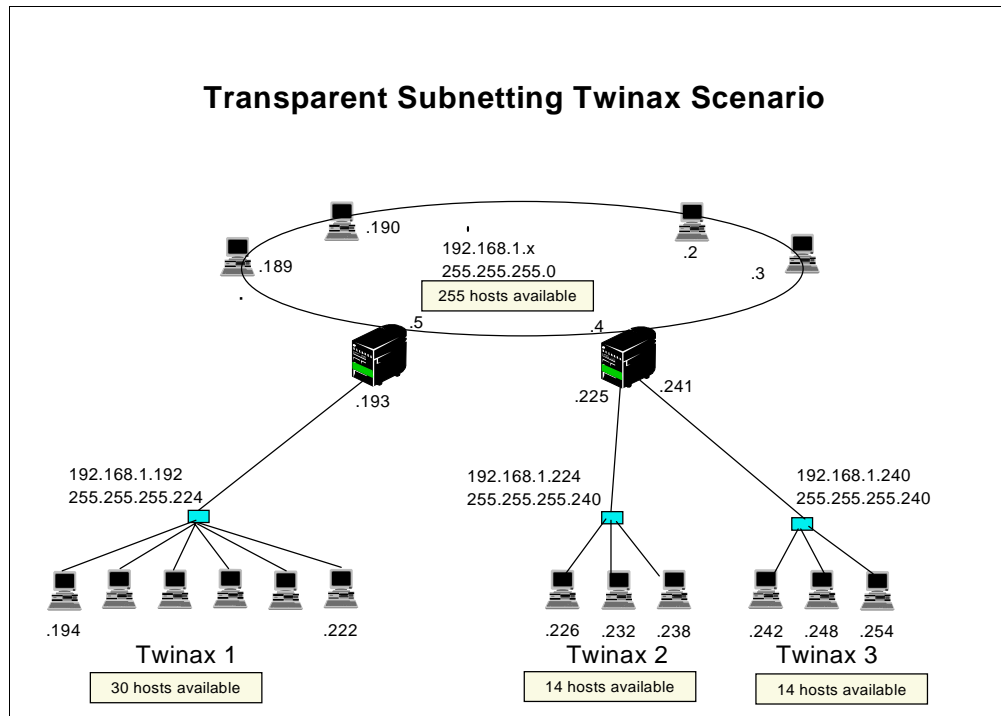


Figure 313. Transparent Subnetting Twinax Scenario with Class C TCP/IP Address

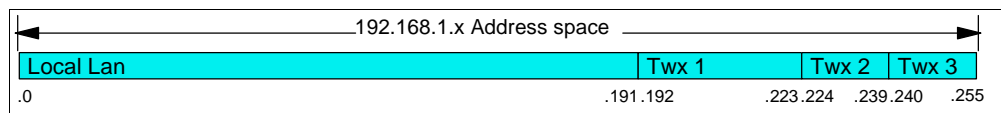


Figure 314. Transparent Subnetting Class C Address Example

The *Local LAN* has a network address of 192.168.1.0 and a mask of 255.255.255.0. This mask gives you the entire range of addresses to use in the last byte or octet of the address. However, within the DHCP configuration, you are required to break up the range using masks. You are also required to build a subnet group that ends the range of usable IP addresses at 190. The range of 193 to 254 is reserved for different subnets.

The next group of addresses, *Twx1*, has a subnet address of 192.168.1.192 and a mask of 255.255.255.224. The mask gives you eight blocks of 32 contiguous addresses, of which you use only the block containing the range of addresses from 193 through 222. It is the subnet address 192.169.1.192 that tells you to start at the subnet boundary of 192. Only the range of addresses from 192.168.1.193 to 192.168.1.222 is specified in the DHCP address pool.

The third group, *Twx2*, has a subnet address of 192.168.1.224 and a mask of 255.255.255.240. This mask gives you 16 blocks of 16 contiguous IP addresses, of which you use only the block containing the range of addresses from 225 through 238. It is this range that is specified in the DHCP address pool. The subnet address of 192.168.1.224 tells you that the first address is 192.168.1.225.

The last group, *Twx3*, has a subnet address of 192.168.1.240 and a mask of 255.255.255.240. This mask gives you 16 blocks of 16 contiguous IP addresses,

of which you only use the block containing the range of addresses from 241 through 254 is used. It is the network address of 192.168.1.240 that tells you to start at address 241. The valid range of addresses is from 241 through 254. Use all of this range in the DHCP address pool.

15.3 Configuring Twinax IBM Network Station with Local DHCP Server

This scenario attaches the IBM Network Station to a local workstation controller on the AS/400 system. The local workstation controller is CTL01 (or QCTL), the same controller that supports the system console. Use DHCP to configure the workstation controller with an IP address and to serve the IBM Network Stations with network start-up information.

You are using a network addressing scheme that enables Proxy ARP automatically. It also allows the IBM Network Station to see and be seen across the network.

Figure 315 on page 359 shows a high-level view of the topology used in this scenario.

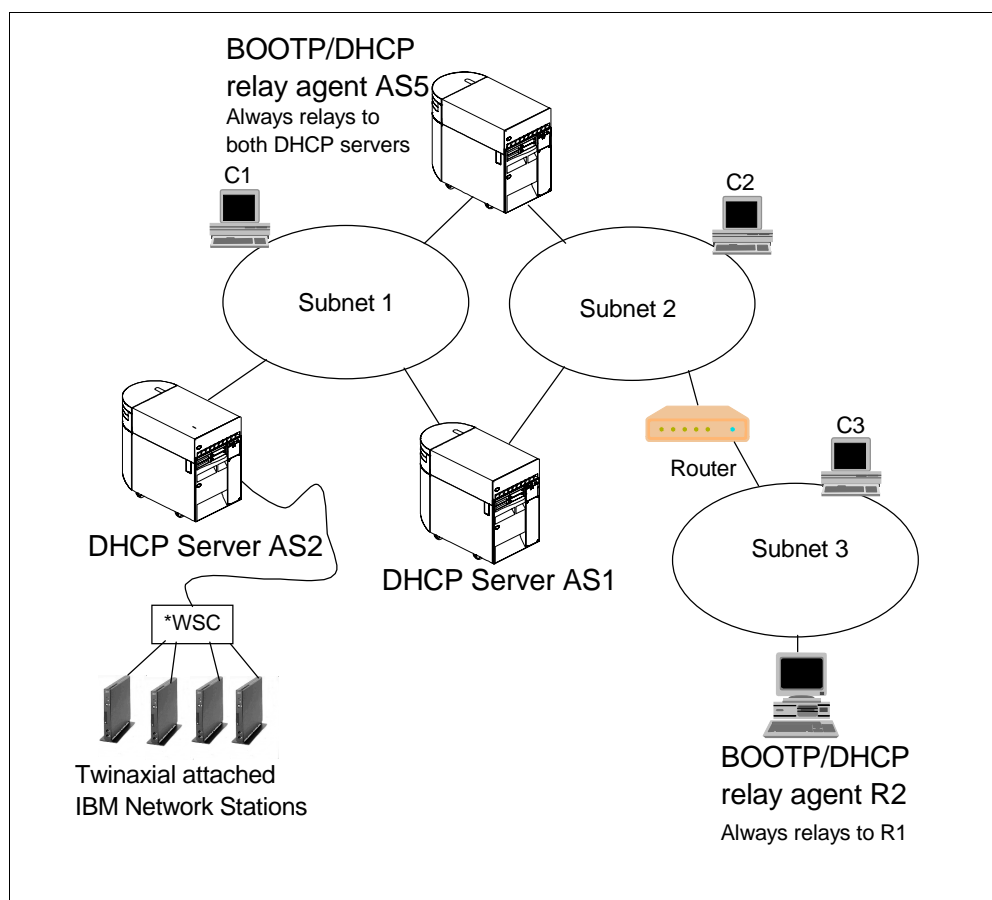


Figure 315. Twinaxial-Attached IBM Network Stations Running TCP/IP over Twinax

The twinax-attached IBM Network Stations are connected to the backup DHCP server, AS2. This system is the backup DHCP server in this scenario. The IBM Network Stations receive start-up information from the AS2 system. The IBM

Network Stations are on their own subnet, which has the same TCP/IP *network* address as subnet 1.

Once the IBM Network Stations have been started, demonstrate that Proxy ARP is working by pinging the IBM Network Stations from a remote host on the same network.

15.3.1 Scenario Objectives

This scenario has the following objectives:

1. Configure the DHCP server AS2 to support the locally attached twinax IBM Network Stations.
2. Set up and start the twinax-attached IBM Network Stations.
3. Ensure LAN connectivity across the network.

This scenario also explains how Proxy ARP works to make the IBM Network Stations visible on a subnet to which they are not directly attached.

15.3.2 Scenario Advantages

The advantages of this scenario are as follows:

- The ease with which you connect twinax-attached IBM Network Stations to an existing network.
- The simplicity of configuring DHCP to support the twinax-attached IBM Network Stations.
- The automatic routing of datagrams from the twinax subnet to the attached LAN and vice versa when using Proxy ARP.

15.3.3 Scenario Disadvantages

The following disadvantages apply to this scenario:

- You might need to understand underlying concepts such as subnetting and Proxy ARP if your network has a somewhat restricted addressing scheme.

15.3.4 Scenario Network Configuration

Figure 316 shows the network configuration for this scenario.

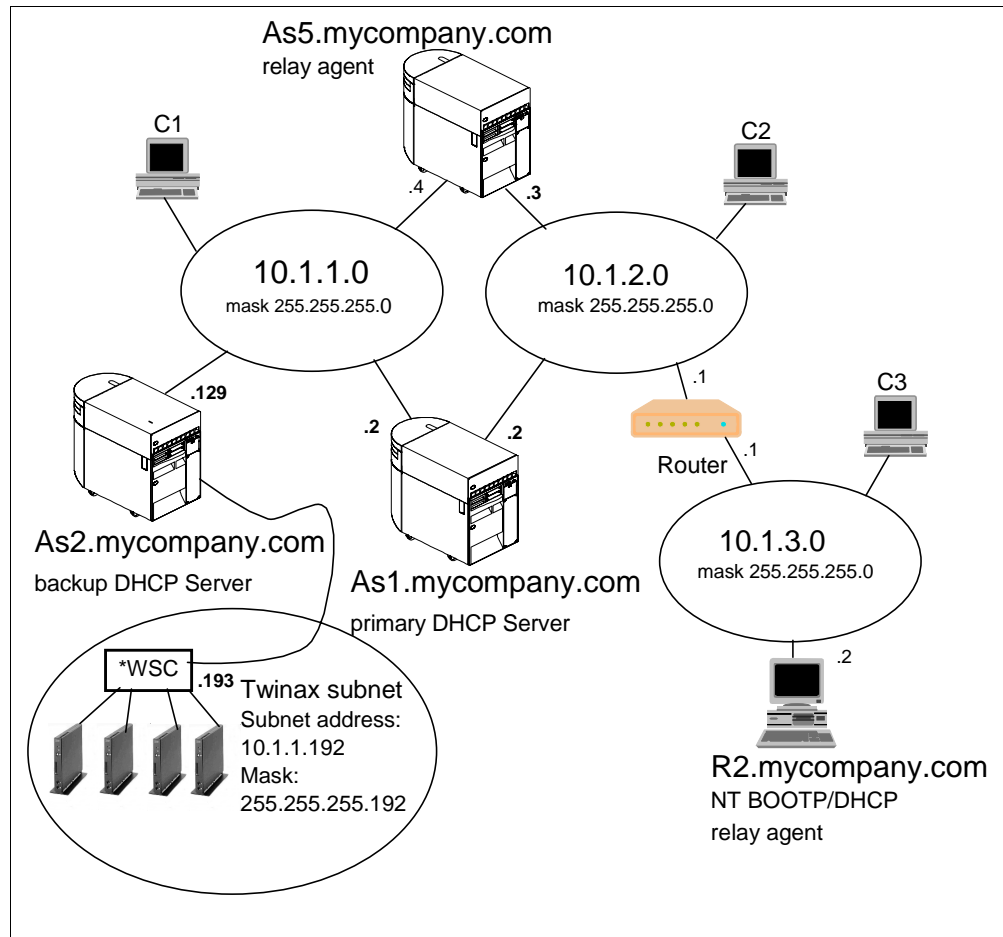


Figure 316. Scenario Network Topology with an IP over Twinax Subnet

The twinax subnet address 10.1.1.192 with the mask of 255.255.255.192 is a subset of the network 10.1.1.x. It lets you use 64 TCP/IP addresses on the twinax subnet. This is also the maximum number of IP addresses that you can allocate to the twinax subnet because it is the maximum number of devices that the workstation controllers supports.

The following characteristics influence this scenario:

- A subnet was carved out of the address space 10.1.1.0, and a mask was applied to reduce the number of valid TCP/IP addresses to 64.
- The DHCP server, AS2, is required to service the twinax subnet.
- AS2, the backup DHCP server for the network, is the primary DHCP server for the twinax subnet.
- AS2 is the only DHCP server for the twinax subnet. If AS2 fails, then the twinax subnet loses connectivity to the host. This is because the host, AS2, powers the twinax network.
- The IP address range of 10.1.1.1 through 10.1.1.254 is divided in half between AS1, the primary DHCP server, and AS2, the backup DHCP server.
- AS2, the backup DHCP server, administers IP addresses in the range from 10.1.1.128 through 10.1.1.254.
- The twinax subnet is serviced from the range of addresses from 10.1.1.192 through 10.1.1.254.

- The twinax network must be able to see out onto the LAN.
- The LAN-attached devices and hosts must be able to communicate with the twinax subnet.

15.4 Task Summary

These setup tasks assume that you are installing twinax-attached IBM Network Stations in an existing network similar to the example in Figure 316 on page 361. This scenario uses the backup DHCP server on the network as the primary DHCP server for the twinax-attached IBM Network Stations. This is essentially any DHCP server that has locally attached twinax IBM Network Stations. The point to remember is that, depending on the TCP/IP addressing scheme, you must ensure that the address pool for the twinax subnet is not duplicated in another pool on another DHCP server within the network. Operations Navigator DHCP server configuration does not allow you to create duplicate IP addresses in two subnets of the *same* DHCP server.

From the range of addresses from 10.1.1.128 through 10.1.1.254 (the address range administered by AS2), you must carve another subnet for the twinax devices that starts at 10.1.1.191 and ends at 10.1.1.254.

The tasks required to complete this scenario are as follows:

1. Plan the TCP/IP addressing scheme.
2. Carve out 64 IP addresses from the address pool of 10.1.1.128 through 10.1.1.254 to use for the twinax subnet on AS2.
3. Configure the DHCP server for twinax support.
4. Configure and start the IBM Network Station.
5. Test connectivity.

15.4.1 Plan the TCP/IP Addressing Scheme

In a TCP/IP network with multiple subnets and TCP/IP address ranges, it is imperative to pay careful attention to the addressing scheme. This topic shows you in detail the addressing scheme to use for the twinax subnet in this scenario.

Use a Class A type of IP address from the Internet Assigned Numbers Authority (IANA) on your internal network. This type cannot be routed through the Internet, yet still provides you with good growth potential for the future.

From the existing LAN IP address space, carve a contiguous range of 64 IP addresses. These are for the IBM Network Stations to use on the twinax subnet. Use the last 64 addresses of the range from 10.1.1.128 through 10.1.1.254. Use 10.1.1.192 as the network address for the twinax subnet. Apply a mask of 255.255.255.192, which gives you the maximum allowed TCP/IP address range (64) that you can use on a twinax subnet. The usable host IP address range is from 0.0.0.1 through 0.0.0.63. Write the full TCP/IP address range as 10.1.1.193 through 10.1.1.254.

Note

The range of addresses that you choose for the twinax subnet is extremely important. If you have the ability in your network to allocate 64 IP addresses to the twinax subnet, you must do so and forget about the IP addresses that are not used. It becomes extremely difficult in networks other than class A to reallocate and shift addressing schemes around simply to gain another IP address to install another IP over twinax device.

Since this address range is a subset of the main network (10.1.1.x), Proxy ARP is enabled automatically.

15.4.2 Carve out 64 Addresses from the Administered Address Pool

The back-up DHCP server, AS2, services the twinax-attached IBM Network Stations with IP addresses in the address that this server administers (10.1.1.128 through 10.1.1.254).

Note

You must define a subnet within the server configuration where, when the mask is applied to the subnet address, the server's LAN interface falls into the valid range of the subnet. In other words, there must be a subnet in the configuration file where, if the entire range is used, the server interface is in that range. The server does not need to administer the entire range. You must exclude the server's IP address from the *administered* range to prevent the server from giving away its own address.

For example, Subnet 10.1.1.128 with the mask 255.255.255.128 has a valid range of addresses from 10.1.1.128 through 10.1.1.254. Assume that the administered range of this subnet is from 10.1.1.128 through 10.1.1.200. For the server to hand out addresses to locally attached clients, the server's LAN IP address must fall within the valid range of the subnet (that is, from 10.1.1.128 through 10.1.1.254). This means that a server with an IP address of 10.1.1.205 works, but a server IP address of 10.1.1.3 does not because it is not in the subnet range from 10.1.1.128 through 10.1.1.254. If the server's IP address is 10.1.1.3 and a DHCP discovery arrives on that interface, the DHCP server states that there are no addresses available for that subnet.

There is a method to group the valid subnet addresses to administer together with a subnet that encompasses the server's IP address. Defining a subnet group allows the server to pull addresses out of the other subnet that has the real range.

For example, Subnet 10.1.1.128 with a mask of 255.255.255.128 has an administered range from 10.1.1.128 through 10.1.1.200. The server's IP address is 10.1.1.3, which is outside the entire subnet range. Define a second subnet in the server that encompasses the server's IP address, such as 10.1.1.0 with the mask 255.255.255.248. This creates the entire valid range from 10.1.1.1 through 10.1.1.6, but you must change the administered range to 10.1.1.3 through 10.1.1.3 and then exclude 10.1.1.3 from the pool. Group both the 10.1.1.128 subnet and the 10.1.1.0 subnet together to form one subnet group.

This allows you to administer the addresses from 10.1.1.128 through 10.1.1.200 and to keep your server's address at 10.1.1.3. Do not administer any subnet addresses in the range from 10.1.1.1 through 10.1.1.7.

The twinax subnet addresses that you use must be and are a subset of the address space 10.1.1.0. This means that you must divide the backup address pool (the range of addresses from 10.1.1.128 through 10.1.1.254 that exists on the backup DHCP server, AS2) into two ranges. One range is for the twinax subnet. Use the remaining addresses to service the main LAN.

Split the address space from 10.1.1.128 through 10.1.1.254 in half to give two ranges of 64 addresses each. Accomplish this by applying a mask of 255.255.255.192 to the subnet ID 10.1.1.128 in the DHCP configuration. This creates the range of addresses from 10.1.1.128 through 10.1.1.191 as the first half of the pool.

The second half of the address space now starts at 10.1.1.192. Applying the mask 255.255.255.192 in the DHCP configuration tells the server to use the next 64 addresses. This means that the range is now from 10.1.1.192 through 10.1.1.254. This is the twinax subnet.

Once you have divided the address space from 10.1.1.128 through 10.1.1.254 into two ranges, refer to Figure 317 on page 365 for a visual representation.

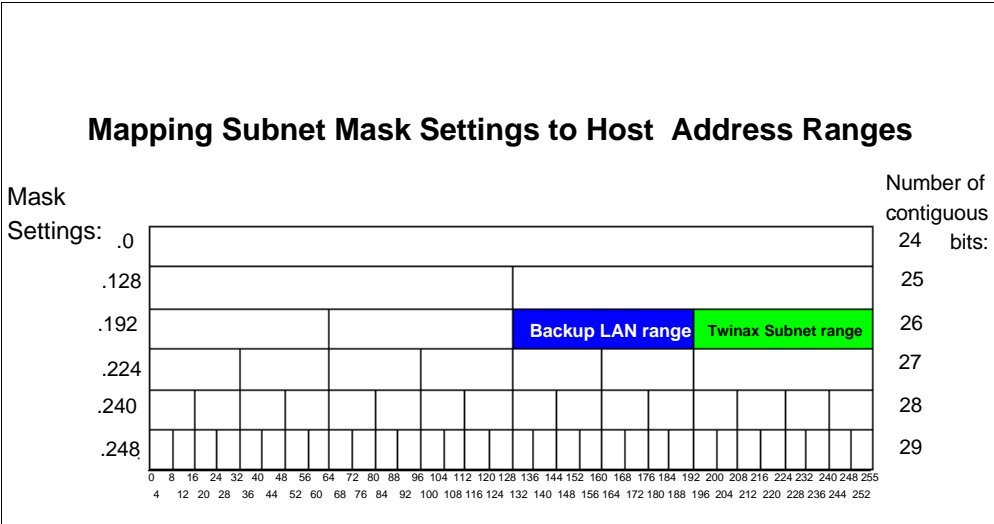


Figure 317. Applying Subnet Masks to Split Address Range 10.1.1.128 through 10.1.1.191

Define the first pool in the DHCP server configuration. Refer to Figure 318 for an example of the DHCP configuration of the backup LAN range of addresses from 10.1.1.128 through 10.1.1.190.

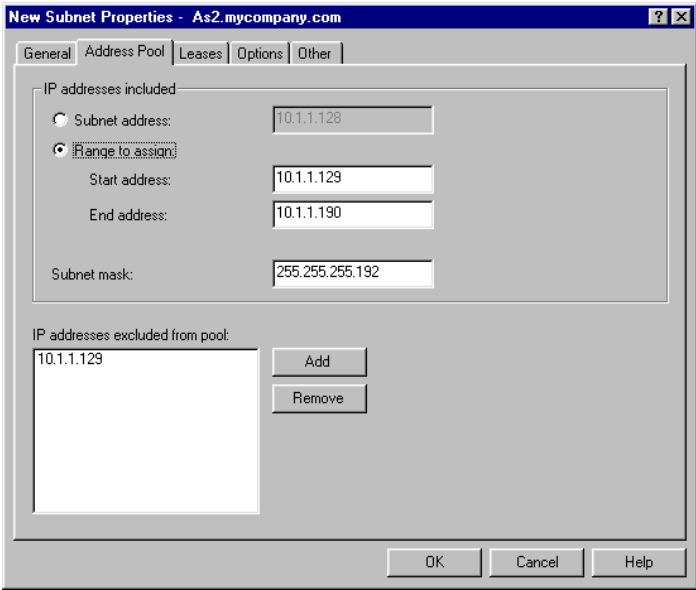


Figure 318. DHCP Configuration -- Dividing the 10.1.1.128 Address Pool with a Mask

For this group, select the **Options** tab and configure DHCP option 1 to pass along the real mask to use on this network, which is 255.255.255.0. Configure any other additional options that clients on the main network require.

15.4.3 Configure the DHCP Server AS2 for Twinax Support

Operations Navigator DHCP configuration is twinax-aware. Provided you have planned which IP addresses to use on the twinax subnet, the configuration is extremely straightforward.

On the backup DHCP server (AS2), which has the IBM Network Stations attached by way of twinax, follow these steps to configure DHCP support for TCP/IP over twinax:

1. Start the AS/400 Operations Navigator.
2. Click *As2.mycompany.com* to select the system.

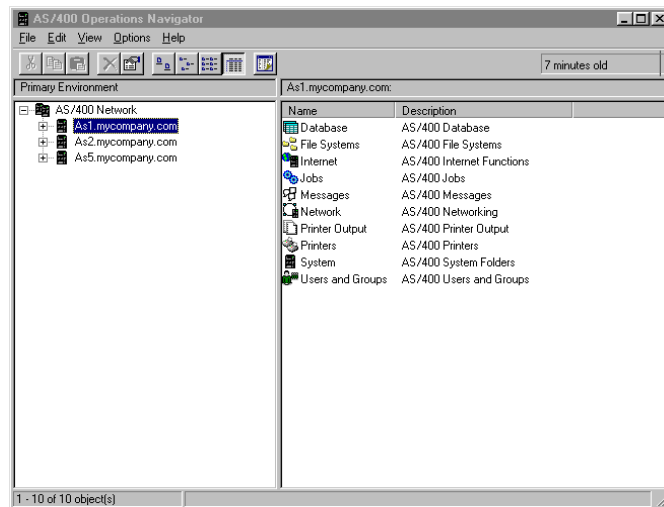


Figure 319. AS/400 Operations Navigator -- Selecting the System to Configure DHCP Server

3. Double-click **Network**.
4. Double-click **Server**.
5. Double-click **OS/400**.
6. Double-click **DHCP**. This displays the DHCP server configuration window, as shown in Figure 320.

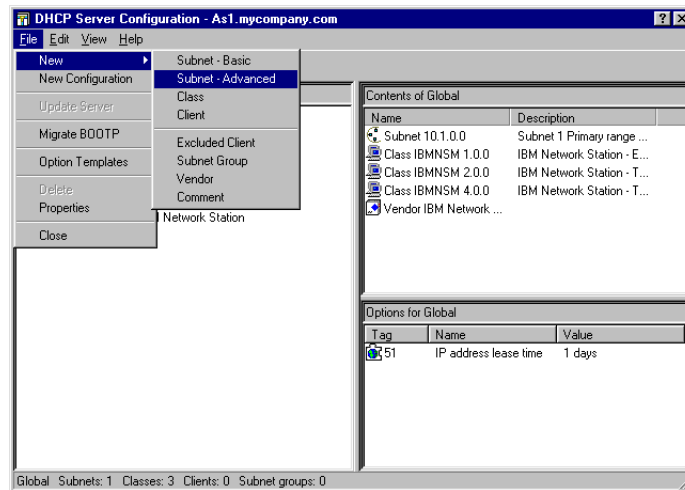


Figure 320. DHCP Server Configuration

7. From the DHCP Server Configuration window, ensure *Global* is highlighted. Select **File>New>Subnet-Advanced**, as shown in Figure 320.
8. Ensure the **General** tab is selected. Specify *TwinaxSubnet10.1.1.192* in the field labeled *Name*. Specify a network ID to make it easier to distinguish the twinax subnet from the other subnets.
9. Check *Twinax subnet* to enable it.
10. Specify the IP address of the workstation controller in the field *Controller's IP address*. Use the first usable address of **10.1.1.193**.
11. Specify a short description in the field labeled *Description*, as shown in Figure 321.

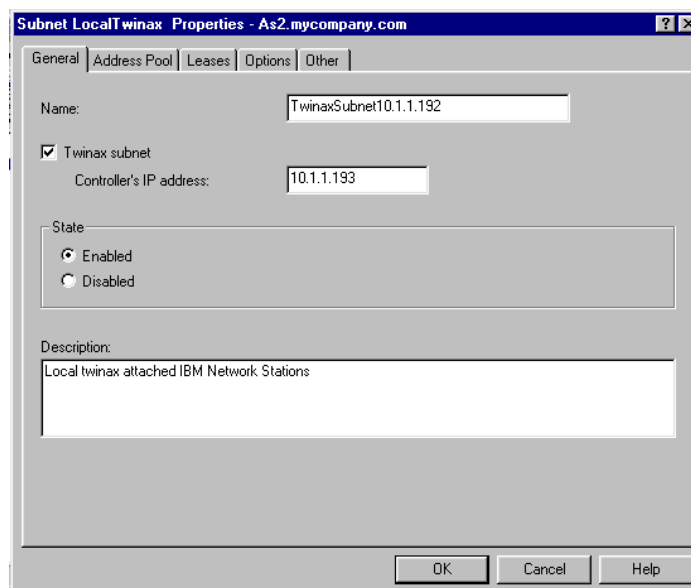


Figure 321. DHCP Server Configuration Twinax Subnet

12. Click the **Address Pool** tab.

You see in Figure 322 on page 368 that the DHCP configuration dialog has already calculated the correct IP address range. The dialog calculated this range based upon the network ID and the IP address that you have used for the twinax workstation controller. You can change the subnet mask on this dialog and have the DHCP configuration GUI calculate the values for you. Remember, though, that the maximum number of address that can be allocated to the twinax subnet is 64.

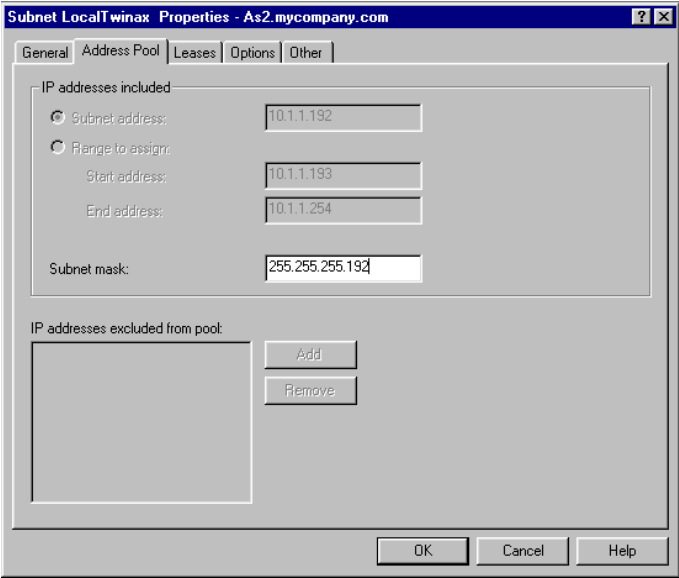


Figure 322. DHCP Twinax Address Pool Range

Tip

You do not need to exclude the workstation controller IP address from the range. It is excluded automatically.

- 13.Click the **Leases** tab.
- 14.Set the lease time to **Never expire** for the twinax subnet.
- 15.Click the **Options** tab.

You need to add the following options for the DHCP server to serve to the twinax-attached network stations:

Option	Value
1 Subnet Mask	255.255.255.192
3 Router	10.1.1.193 (the WSC is the first hop-attached device)
66 Server name	10.1.1.193
67 Boot file name	/QIBM/ProdData/NetworkStation/kernel

Note: You should not need to add option 67; it is included in the twinax IBM Network Station class, IBMNS 3.4.1.

- 1. To add the options, highlight the option number from the window on the left labeled *Available options*.

2. Click **Add**.
3. Fill in the value for each option in the window at the bottom of the display (see Figure 323 on page 369).

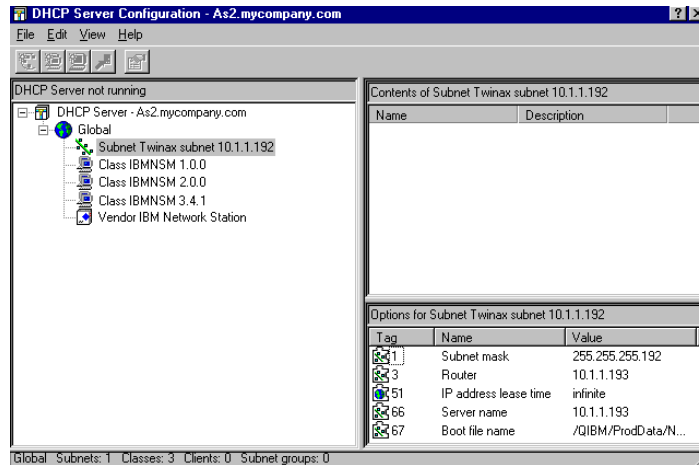


Figure 323. Twinx-Attached DHCP Options Configuration

16. Click **OK**.
17. Close the DHCP configuration window. If the DHCP server is running, you are asked to save the changes you made. Click **Yes**. If the DHCP server is not running, the configuration GUI closes.
18. Start the DHCP server.

15.4.4 Configure and Start the IBM Network Station

The twinaxial-attached network stations are different from the normal token ring or Ethernet stations. The NVRAM options are presented differently, although functionality remains the same. This section does not go into details about these differences. Any new features of the IBM Network Station fall outside the scope of this book.

It is assumed that you have cabled the twinax IBM Network Station correctly.

Note

The twinax IBM Network Station requires you to specify an address to use on the port to which it is connected. Therefore, if you are replacing non-programmable terminals with the IBM Network Station, you must make a note of the address that the old device was using, such as port 02 and address 05. Otherwise, you must ensure that no other device is configured to use the same address on the same port.

When the twinax IBM Network Station is first powered on, it prompts you to specify the address to use for the port to which it is connected. This is not the TCP/IP address. Rather, it is an address from 0 through 6 to use on the workstation controller port to which the IBM Network Station is connected.

Follow these steps to configure the IBM Network Station for use over twinax.

1. Power on the IBM Network Station.

2. When prompted to do so, specify the local controller address to use. Press Enter.

The IBM Network Station checks to see if anyone else is using that address. If no one else is using that address, the IBM Network Station defaults to startup using DHCP. It continues booting until completion, provided the DHCP server is started.

15.4.4.1 Resetting NVRAM

If the IBM Network Station has been used previously and you are not sure what has been entered into the NVRAM, follow these steps to reset the NVRAM to the factory defaults:

1. Power on the IBM Network Station. You see the IBM logo followed by a memory and keyboard check.
2. After seeing the message `NS0500 Search for Host System`, press the **ESC** key to stop the startup sequence.

If prompted for an administrator password, enter it now. (This is the password an administrator sets using the IBM Network Station Manager program.)

3. Invoke the IBM Network Station Boot Monitor program by pressing the following key sequence:
 - For 101/102 keyboards:
Press and hold **Left Shift + Left Alt + Left Ctrl**. Press **F1**.
 - For 5250/3270 keyboards:
Press and hold **Left Shift + Left Alt**. Press **F1**.
4. Enter **NV** at the Boot Monitor prompt (**>**) to access the NVRAM utility.
5. Enter **L** to reset the NVRAM.
6. Enter **S** to save the defaults into NVRAM.
7. Enter **Y** to the question "Are you sure?"
8. Enter **Q** to quit.
9. Power the IBM Network Station off and then on again. It starts with the factory settings.

Alternatively, you can specify the twinax address to use by pressing the **ESC** key when the message `NS0500 Search for Host System` appears and selecting option 8, Set Twinax Station Address.

Once you have set the IBM Network Station to factory defaults and specified the correct twinax address, the IBM Network Station attempts to start using DHCP first. The IBM Network Station starts without further intervention.

Tip

Any time you configure or reset the IBM Network Station we *strongly* recommend that you disable the BOOTP protocol on the IBM Network Station. The IBM Network Station defaults to a priority scheme where it sends a DHCPDISCOVER first and, if it does not receive a response, it switches to BOOTP. Sometimes the IBM Network Station times out while the DHCP server is processing its DHCPDISCOVER and the IBM Network Station switches to BOOTP without waiting for the DHCPOFFER from the DHCP server. If this happens, the server assigns a permanent address to it.

To disable the BOOTP protocol in the IBM Network Station, from the *Set up Utility* display, press **F5**, *Set the Network Parameters*, select **1** for DHCP and **D** for BOOTP.

15.4.4.2 The Startup Sequence

When the first IP over twinax IBM Network Station starts, OS/400 checks to see if a TCP/IP interface of type *TDL exists. If not, the workstation controller calls the program QSYS/QTODDTWX to query the DHCP server configuration file (*dhcpsd.cfg*) for a TCP/IP address and mask to use.

The system automatically builds a QTDLxxxxxx line, controller, and device for TCP/IP to associate with and run over. A device type of 5150 is created underneath the workstation controller description. Figure 324 shows the QTDLxxxxxx objects that autoconfiguration creates.

Work with Configuration Status			
			System: AS2
Position to		Starting characters	
Opt	Description	Status	-----Job-----
	QTDL806100	ACTIVE	
	QTDL8NET	ACTIVE	
	QTDL8TCP	ACTIVE	QTCPPIP QTCP 022134

Figure 324. QTDLxxxxxx Line, Controller, and Device Descriptions

Figure 325 shows the twinaxial data link control line description.

Display Line Description		AS2
		03/02/98 17:55:20
Line description	: QTDL806100	
Option	: *BASIC	
Category of line	: *TDL	
Attached work station ctl		CTL01
Network controller		QTDL8NET
Online at IPL		*NO
Text		CREATED BY AUTO-CONFIGURATION

Figure 325. QTDLxxxxxx Line Description

The local workstation controller description shown in Figure 326 contains the name of the QTDLxxxxxx line that auto-configuration built.

```

                                Display Controller Description
                                AS2
                                03/04/98 08:02:39

Controller description . . . . . : CTL01
Option . . . . . : *BASIC
Category of controller . . . . . : *LWS

Controller type . . . . . : 6050
Controller model . . . . . : 1
Resource name . . . . . : CTL01
TDLC line . . . . . : QTDL806200
Online at IPL . . . . . : *YES
Auto-configuration controller . . : *YES
Text . . . . . : CREATED BY AUTO-CONFIGURATION

```

Figure 326. Workstation Controller Description -- CTL01

The device created underneath the workstation controller CTL01 is shown in Figure 327.

```

                                Display Device Description
                                AS2
                                03/02/98 18:02:45

Device description . . . . . : DSP04
Option . . . . . : *BASIC
Category of device . . . . . : *DSP

Device class . . . . . : *LCL
Device type . . . . . : 5150
Device model . . . . . : 3
Port number . . . . . : 2
Switch setting . . . . . : 2
Internet address . . . . . : 10.1.1.194
Online at IPL . . . . . : *YES
Attached controller . . . . . : CTL01
Keyboard language type . . . . . : USB
Print device . . . . . : *SYSVAL
Output queue . . . . . : *DEV

```

Figure 327. Device Type 5150 Under CTL01

The system automatically creates a TCP/IP interface for the workstation controller as well. With one exception, this is similar to any other TCP/IP interface that you have configured. The TCP/IP interface for the workstation controller contains a parameter that allows you to utilize Proxy ARP. This parameter is called the *Associated Local Interface* (*LCLIFC), and its value must be the LAN interface of the AS/400 system where the twinax workstation controller resides. In this case, the value for the associated local interface is 10.1.1.129.

To view the associated local interface parameter, perform the following steps:

1. On the AS/400 system's command line, enter **CFGTCP**.
2. Select option **1**, *Work with TCP/IP interfaces*.

3. Select option **5**, *Display*, beside the interface that has a line type of ***TDLC**. Press Enter (see Figure 328).

```
Display TCP/IP Interface                                     System:  AS2
Internet address . . . . . : 10.1.1.193
Subnet mask . . . . . : 255.255.255.192
Line description . . . . . : QIDL806100
Line type . . . . . : *TDLC
Associated local interface . . . . : 10.1.1.129
Interface status . . . . . : Active
Type of service . . . . . : *NORMAL
Maximum transmission unit . . . . : *LIND
Automatic start . . . . . : *YES
```

Figure 328. TCP/IP Interface for the Local Workstation Controller

15.4.5 Test Connectivity

Now that you have configured the DHCP server for the twinax environment, started a twinax-attached IBM Network Station, and ensured that the associated interface parameter is correct in the TCP/IP interface of type ***TDLC**, you can test for connectivity across your network.

To prove that the IBM Network Station sees out past the local workstation controller, start a 5250 TELNET session to host *As5.mycompany.com*, which has the TCP/IP address of 10.1.1.4.

The real test of Proxy ARP is to ping the twinax-attached IBM Network Station from a remote host. From *As5.mycompany.com*, send an ICMP echo, or ping, to the address 10.1.1.194 and wait for a reply.

15.4.6 Summary

This scenario installed a twinax subnet on the backup DHCP server. The twinax address range that you used is a subset of the address space 10.1.1.x. The backup DHCP server already had a range defined within DHCP that included the address you needed to use for the twinax subnet. This range was broken down into two groups, and a restrictive mask was placed over the range during the DHCP configuration. This allowed you to stop the range at 10.1.1.191.

You built a DHCP server configuration for the twinax subnet and powered on the twinax-attached IBM Network Station, which automatically built a TCP/IP interface for the workstation controller and a TDLC line description.

Once you started the IBM Network Station, you tested connectivity to the rest of the network by starting a TELNET session to a remote host and sending an ICMP echo (ping) to the network station from a remote host.

15.5 Configuring Twinax Network Station with a Remote DHCP Server

This topic demonstrates how to configure and use a remote DHCP server to supply network information to twinax-connected IBM Network Stations.

It is not necessary to use the same system as your DHCP server to which the twinax-attached IBM Network Stations are connected. You can utilize another DHCP server in your network.

This section does not discuss how to have the locally attached IBM Network Stations load their kernel and terminal configuration settings from a different host. This has already been discussed in Chapter 11.6, "Selecting the Bootstrap Host for the IBM Network Station" on page 252. Refer to this chapter for more information.

Load the kernel and terminal configuration settings from the local system.

15.5.1 Scenario Overview

In this scenario, there are twinax-attached IBM Network Stations connected to a local system that is not running the DHCP server. The local system is and must be running the BOOTP/DHCP Relay Agent.

Locally attached IP over twinax devices have their DHCP DISCOVER messages forwarded to a DHCP server that is running on a different system. This is done to obtain a network address and the startup information that is required to boot up.

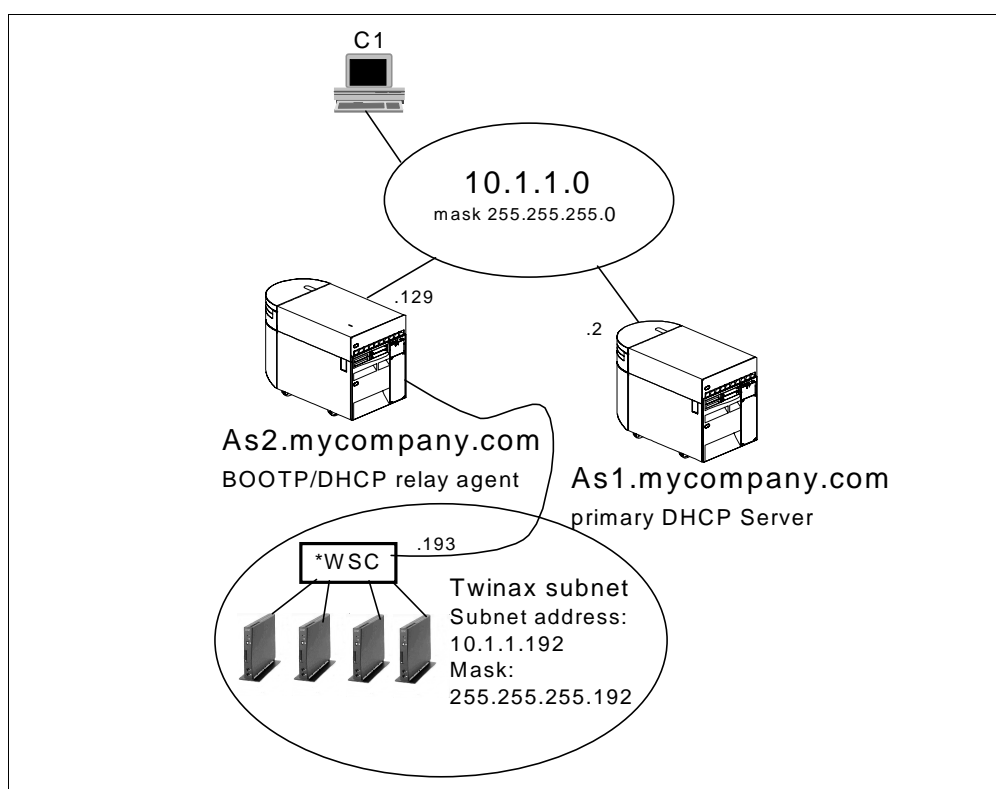


Figure 329. Using Remote DHCP Server to Configure Twinax IBM Network Stations

Figure 329 shows the logical network topology that is used in this scenario. The network has been simplified from the previous scenario so the only subnet for which the DHCP server is configured is the subnet 10.1.1.x. There is no backup DHCP server on the network. The twinax IBM Network Stations are attached to

the BOOTP/DHCP Relay Agent, which forwards all DHCP broadcasts originating from the twinax subnet to the primary DHCP server.

15.5.2 Scenario Objectives

This scenario's objective is:

To use one primary DHCP server to supply network information to remote twinax attached devices.

This objective also means that you do not have to run a DHCP server agent on every AS/400 system with twinax-attached IBM Network Stations. You can set up a backup DHCP server and have the local BOOTP/DHCP Relay Agent send the DHCP discovers to both DHCP servers. See 14, "Multiple Subnets, DHCP Servers, and Relay Agents" on page 313 for more information on providing a backup DHCP server.

15.5.3 Scenario Advantages

The advantage that this scenario provides is that:

You need only one DHCP server in your network to support twinax-attached IBM Network Stations.

It is not necessary to run a DHCP server on every AS/400 system that has twinax-attached IBM Network Stations.

15.5.4 Scenario Disadvantages

A disadvantage of this scenario is that you need to understand underlying concepts such as subnetting and Proxy ARP if your network has a somewhat restricted addressing scheme.

15.5.5 Task Summary

In these setup steps, the assumption is made that you have cabled the IBM Network Station correctly and that you have defined a local twinax address. The assumption is also made that the IBM Network Station starts as a DHCP client. The following tasks start from the point when the first IBM Network Station is ready to be powered on:

1. Configure the local AS/400 DHCP configuration file on *As2.mycompany.com*.
2. Power on and off the IBM Network Station.
This builds the TCP/IP interface on the AS/400 system for the workstation controller automatically.
3. Configure and start the BOOTP/DHCP Relay Agent on *As2.mycompany.com*.
4. Change the DHCP configuration for the pool of addresses from 10.1.1.1 through 10.1.1.254 on *As1.mycompany.com*.
5. Configure an address pool for the twinax subnet on the remote DHCP server (*As1.mycompany.com*).
6. Start the IBM Network Station.

15.5.6 Configure the Local DHCP Configuration File on AS2

You must build a DHCP server configuration file (*dhcpsd.cfg*) on the system to which the twinax subnet is directly attached. You do not start the DHCP server on this system, but the configuration file must exist. When you power on the first IBM Network Station, the workstation controller calls the program QSYS/QTODDTWX. This program queries the DHCP configuration file for its IP address and mask.

Use Operations Navigator to create this file.

Please refer to Section 15.4.3, “Configure the DHCP Server AS2 for Twinax Support” on page 366 and follow steps 1 through 12. This scenario uses the same IP addressing scheme that is defined in that section. It is unnecessary to configure the DHCP server on AS2 to provide options for the twinax-attached devices because this DHCP server is not used.

Note: Ensure that the DHCP server is in a *stopped* state once you have completed the configuration. Do *not* start the DHCP server. To be safe, disable the subnet on this system by right-clicking on the subnet and clicking on **Disable**.

15.5.7 Power on the IBM Network Station

The network station must be started for the AS/400 system to build the TCP/IP interface and line description for the workstation controller.

Power on the twinax-attached IBM Network Station.

The message `NS0510 System 10.1.1.193 contacted` is an indication that the system has completed building the TCP/IP interface for the workstation controller.

The IBM Network Station sits on this message because a DHCP server cannot respond to this request and should be powered off again at this stage.

Tip

If you are curious and want to see what the automatic configuration did, use the AS/400 `CFGTCIP` command and specify option 1, *Work with TCP/IP interfaces*. There should now be an interface with the type of *TDLC. This is the TCP/IP interface of the workstation controller.

Use the AS/400 `CFGTCIP` command and specify option 1, *Work with TCP/IP interfaces*.

There is now be an interface with the type of *TDLC. This is the TCP/IP interface of the workstation controller.

Once this interface exists, move on to the next step.

15.5.8 Configure and Start BOOTP/DHCP Relay Agent on Local AS/400 System (AS2)

After building the DHCP configuration file for the twinax subnet, it is time to turn *As2.mycompany.com* into a BOOTP/DHCP Relay Agent.

In this scenario, you are configuring the AS/400 BOOTP/DHCP Relay Agent to forward DHCP messages directly and without delay from the twinax subnet to the primary DHCP server.

If another DHCP server exists in your network, you can forward DHCP messages from the twinax subnet to that DHCP server as well. Refer to 14, “Multiple Subnets, DHCP Servers, and Relay Agents” on page 313 for more information.

To configure the AS/400 BOOTP/DHCP Relay Agent, perform the following steps:

1. Sign on to the AS/400 system. From a command line, enter the `CHGDHCPA MODE(*RELAY)` command, and press Enter. This changes the mode of the DHCP server to be a BOOTP/DHCP Relay Agent.
2. From Operations Navigator select **As2.mycompany.com>Network>Servers>OS400**, and right-click **BOOTP/DHCP Relay Agent**, as shown in Figure 330.
3. Click **Configuration** to select it.

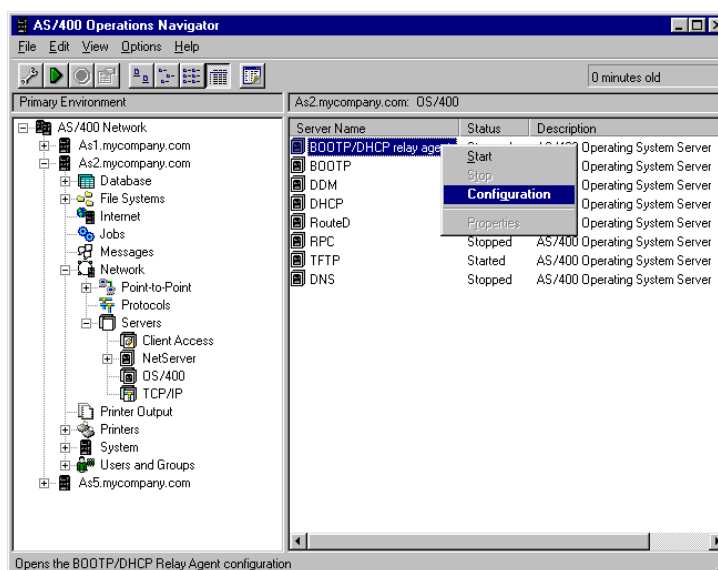


Figure 330. AS/400 Operations Navigator -- Configuring BOOTP/DHCP Relay Agent

4. The BOOTP/DHCP Relay Agent properties window appears. Click the *Start when TCP/IP is started* check box to ensure that it is checked.
5. Click **Add**.
6. Use the pull-down option on the Interface address field at the top of the dialog to select the TCP/IP interface from which the BOOTP/DHCP Relay Agent accepts DHCP packets. This is the workstation controller interface that has just been built 10.1.1.193.
7. Specify the IP address of the primary DHCP server to which the DHCP messages from the clients are sent. Use the address on the primary DHCP server 10.1.1.2. Refer to Figure 316 on page 361.
Note: Specify the system name if your DNS server resolves IP addresses or if you have configured your host table correctly.
8. Leave the *Maximum hops* set to the default of 4.
9. Leave the *Packet transmission delay* at zero.

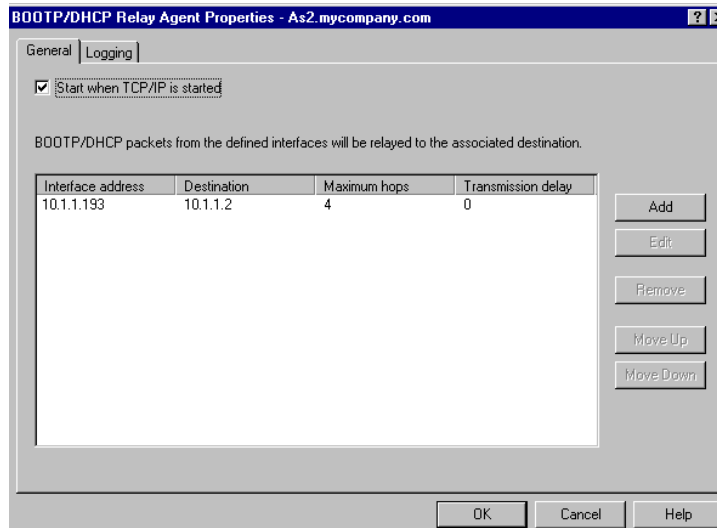


Figure 331. BOOTP/DHCP Relay Agent Configuration

10. Click **OK**.

11. From Operations Navigator, right-click BOOTP/DHCP Relay Agent to open a context menu. Select **Start** to start the server.

The BOOTP/DHCP Relay Agent now forwards DHCP messages from the workstation controller interface to the primary DHCP server.

15.5.9 Change the DHCP Server Configuration for the Address Pool 10.1.1.x on AS1

The twinax subnet addresses that you use must be and are a subset of the address space 10.1.1.x. Because of this, you must break the pool of addresses from 10.1.1.1 through 10.1.1.254 into two ranges. You must also reduce the pool so that it does not include the addresses from 10.1.1.192 through 10.1.1.254. These addresses are used for the twinax subnet.

In this case, you must break up the address range from 10.1.1.1 through 10.1.1.254 into two groups by applying masks to the range within the DHCP configuration. You must then group the two groups back together within the DHCP configuration to form one pool. You also need to use DHCP option 1 to specify and to pass back to the client the correct mask to use on this subnet.

The masks that are needed to split the range also reduce the pool so it does not include the twinax subnet addresses.

To split the group into two pools and allow the address range to end at 10.1.1.191, apply the mask 255.255.255.128 in the DHCP configuration. This allows two groups of 128 addresses. This is the first group, which starts at 10.1.1.1 and ends at 10.1.1.127. The second group has the mask 255.255.255.192 applied to it, which creates the range of addresses from 10.1.1.128 through 10.1.1.191.

Note: You cannot use the subnet boundary addresses. Therefore, you lose three IP addresses from this range.

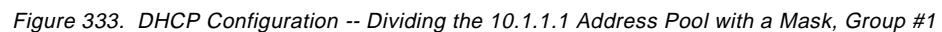
Mapping Subnet Mask Settings to Host Address Ranges

Mask Settings:

Number of contiguous bits:

Mask Settings	Number of contiguous bits
.0	24
.128	25
.192	26
.224	27
.240	28
.248	29

You must define the two pools in the DHCP configuration. Refer to Figure 333 for an example of the DHCP configuration of the first group and to Figure 334 on page 380 for an example of the DHCP configuration of the second group.



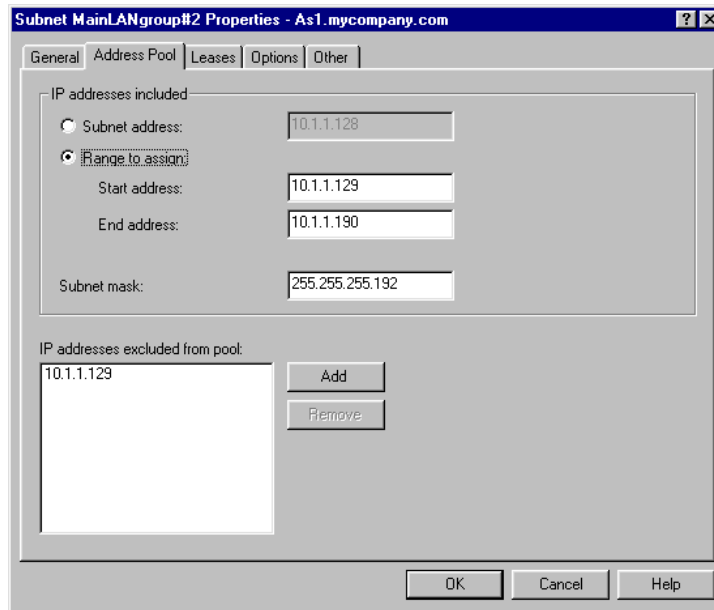


Figure 334. DHCP Configuration -- Dividing the 10.1.1.1 Address Pool with a Mask, Group #2

For both of these groups, select the *Options* tab and configure DHCP option **1** to pass the real mask to use on this network, which is 255.255.255.0. You also must configure any other relevant options that clients on the main network require.

The next step is to group the two address ranges together again to form one pool in the DHCP server configuration.

To form a subnet group within the DHCP configuration, perform the following steps:

1. From the Operations Navigator DHCP window, right-click **Global**.
2. Click **New Subnet Group** to select it.
3. Specify a valid description in the *Name* field. Blanks are not valid.
4. Highlight the first address group and click **Add**. Repeat this step for the second group.

Note: Step 5 is optional.

5. Click the *Address Order* tab. Click either **In order** or **Balanced** to select the appropriate option. In order is the default.

15.5.10 Configure the Twinax Subnet Address Pool on the Remote DHCP Server

You now have to add a TCP/IP address pool on the primary DHCP server to provide network start-up information to the remote twinax clients.

To accomplish this, you *do not* build a special twinax subnet pool (as discussed in Section 15.4.3, “Configure the DHCP Server AS2 for Twinax Support” on page 366). Instead, build a normal IP address pool, as the twinax-attached stations are not attached locally.

1. Open the DHCP configuration window from Operations Navigator.
2. Right-click **Global** to open a context menu. Select **New Subnet -- Advanced**.

- Click the **General** tab and name the subnet AS.2RemoteTwinax. In the *Description* field, specify Remote twinax subnet on As2.mycompany.com.

Note: Do not click *Twinax Subnet*. Leave this box unchecked. Refer to Figure 335.

Subnet RemoteTwinax Properties - As1.mycompany.com

General Address Pool Leases Options Other

Name: As2.RemoteTwinax

☐ Twinax subnet
Controller's IP address:

State
☒ Enabled
☐ Disabled

Description:
Remote twinax subnet on As2.mycompany.com

OK Cancel Help

Figure 335. Remote Twinax DHCP Configuration Example

- Click the **Address Pool** tab.
- Click *Subnet Address* and specify the twinax subnet address as 10.1.1.192.
- In the *Subnet mask* field, specify the mask 255.255.255.192. Refer to Figure 336.

Subnet RemoteTwinax Properties - As1.mycompany.com

General Address Pool Leases Options Other

IP addresses included

☐ Subnet address: 10.1.1.192

☒ Range to assign
Start address: 10.1.1.193
End address: 10.1.1.254
Subnet mask: 255.255.255.192

IP addresses excluded from pool

Add
Remove

OK Cancel Help

Figure 336. Remote Twinax IP Address Pool Example

7. Click the **Options** tab and add the following options to send to the remote twinax-attached client:

Option	Value
1 Subnet Mask	255.255.255.192
3 Router	10.1.1.193 (the WSC is the first hop for attached devices.)
66 Server name	10.1.1.193
67 Boot file name	/QIBM/ProdData/NetworkStation/kernel

8. Click **OK**.
9. Update or start the DHCP server on *As1.mycompany.com*.

15.5.11 Start the IBM Network Station

Start the IBM Network Station again. It now boots to completion.

15.5.12 Summary

This scenario built a DHCP configuration file on the local AS/400 system, AS2, from which the workstation controller obtains the network information.

The first IBM Network Station that powers on causes the workstation controller to query the DHCP configuration file. The workstation controller gains network information, and the TCP/IP interface is built automatically.

You configured the AS/400 system to which the twinax IBM Network Stations are attached locally as a BOOTP/DHCP Relay Agent.

You split the address pool 10.1.1.x on the DHCP server into two parts with restrictive masks and then re-grouped them to form a single pool.

You added an IP address pool for the twinax subnet to an existing DHCP server. You also had the BOOTP/DHCP Relay Agent forward DHCP messages from the locally attached twinax subnet to the remote DHCP server.

Once all of the configuration was complete, you started the IBM Network Station again. This time, the DHCP messages were forwarded by the local BOOTP/DHCP Relay Agent to the remote DHCP server, and the IBM Network Station gained the network start-up information that it needed to boot.

15.6 Configuring Twinax IBM Network Station Using Transparent Subnetting

This scenario demonstrates the concepts of transparent subnetting that are described in Section 15.2.2, “Twinax Transparent Subnetting” on page 356.

15.6.1 Scenario Overview

This scenario uses three IP-over-twinax subnets. Two of these subnets are attached to one AS/400 system and the other subnet is attached to a different AS/400 system.

Use a remote DHCP server on another system to store and serve the necessary network start-up information for all three twinax subnets.

Use a class C IP addressing scheme of 192.168.1.0 and split or group that address space into four contiguous address ranges.

The logical network topology is shown in Figure 337 on page 383.

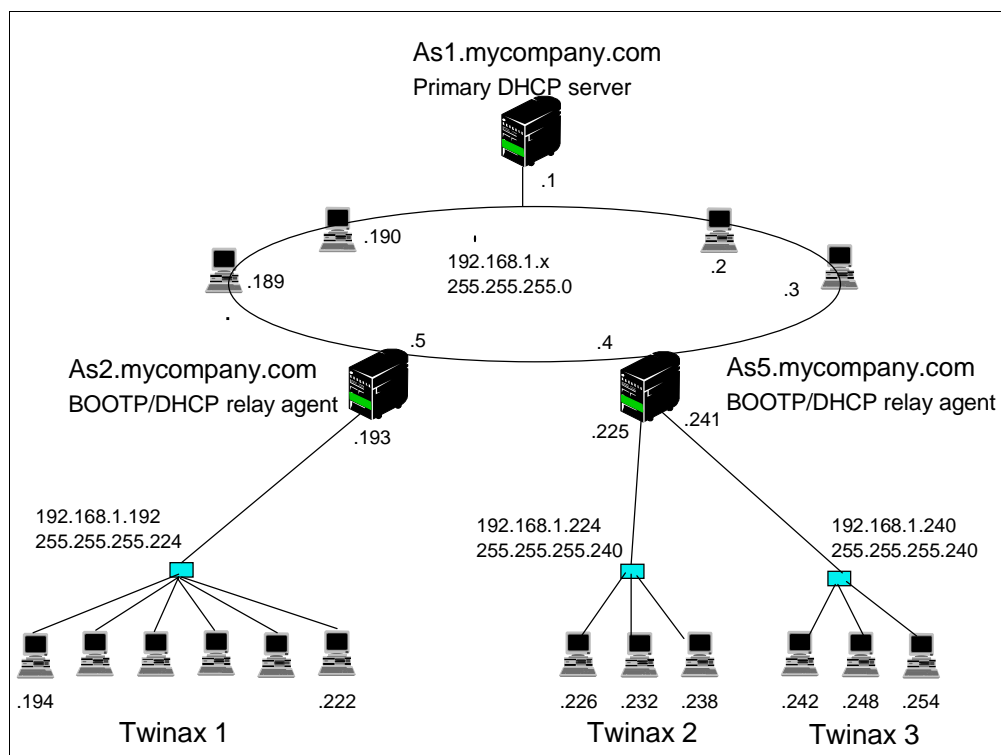


Figure 337. Transparent Subnetting and Twinax IBM Network Station Configuration

The systems **As2.mycompany.com** and **As5.mycompany.com** are both BOOTP/DHCP Relay Agents. They both forward DHCP messages from the attached twinax subnets to **As1.mycompany.com**, the primary DHCP server.

As1.mycompany.com contains the complete TCP/IP address configuration for this network. There is no backup DHCP server in this scenario.

Note

This scenario does not allocate the maximum TCP/IP address range of 64 contiguous addresses to each subnet. Therefore, future device and TCP/IP address additions to the twinax subnets are difficult. Allocate the maximum range of 64 IP addresses to each twinax subnet wherever possible.

15.6.2 Scenario Objectives

The objective of this scenario is to demonstrate how to configure the DHCP server and to use transparent subnetting when a contiguous block of 64 IP addresses is unavailable.

15.6.3 Scenario Advantages

This scenario shows how to use transparent subnetting to solve the problem that results when all of the contiguous IP addresses that you need to configure the twinax IBM Network Stations are unavailable.

15.6.4 Scenario Disadvantages

This example has the disadvantages associated with using a class C addressing scheme. You can only configure up to 254 hosts on your network. Do not allocate the recommended number of IP addresses to the twinax subnets of 64 contiguous addresses.

15.6.5 Task Summary

The following list is a high-level view of the tasks required to implement this scenario:

1. Plan the IP address scheme.
2. Configure *As2.mycompany.com*.
 1. Build a DHCP configuration file.
 2. Start and stop the IBM Network Station to complete the automatic setup of the workstation controller.
 3. Configure the BOOTP/DHCP Relay Agent.
3. Configure *As5.mycompany.com*.
 1. Build a DHCP configuration file.
 2. Start and stop the IBM Network Station to complete the automatic setup of the workstation controller.
 3. Configure the BOOTP/DHCP Relay Agent.
4. Configure the DHCP server on *As1.mycompany.com*.

15.6.6 Planning the IP Address Scheme

The IP address scheme used in this scenario is the same one discussed in Section 15.2, "Transparent Subnet Masking" on page 352.

Use the class C network 192.2.168.1.0 and split the address range of 254 host addresses into four contiguous segments.

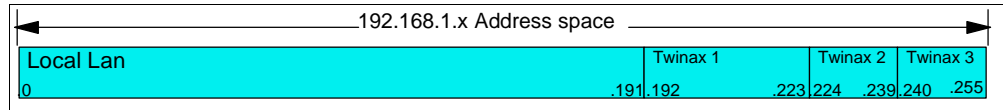


Figure 338. Transparent Subnetting Class C Address Example

The *Local LAN* has a network ID of 192.168.1.x and a mask of 255.255.255.0. This mask gives you the entire range of addresses to use in the last byte or octet of the address. However, within the DHCP configuration you are required to break up the range by using masks and to build a subnet group that ends the range of usable IP addresses at 190.

The next group of addresses, *Twinax 1*, has a network ID of 192.168.1.192 and a mask of 255.255.255.224. The mask provides eight blocks of 32 contiguous addresses, of which only the block containing the range from 193 through 222 is used. It is the network ID of 192.168.1.192 that indicates to start at the subnet boundary of 192. Only the range of addresses from 192.168.1.193 through 192.168.1.222 is specified in the DHCP address pool.

The third group, *Twinax 2*, has a network ID of 192.168.1.224 and a mask of 255.255.255.240. This mask provides 16 blocks of 16 contiguous IP addresses, of which only the block containing the range from 225 through 238 is used. It is this range that is specified in the DHCP address pool. The network address of 192.168.1.224 indicates that the first address is 192.168.1.225.

The last group, *Twinax 3*, has the network ID of 192.168.1.240 and a mask of 255.255.255.240. This mask provides 16 blocks of 16 contiguous IP addresses, of which only the block containing the range from 241 through 254 is used. It is the network address of 192.168.1.240 that indicates to start at address 241. The valid range of addresses is from 241 through 254. Use all of this range in the DHCP address pool.

The chart in Figure 339 is useful because it shows at a glance where each IP range begins and ends. It also shows which subnet mask is required to isolate a certain contiguous range of addresses.

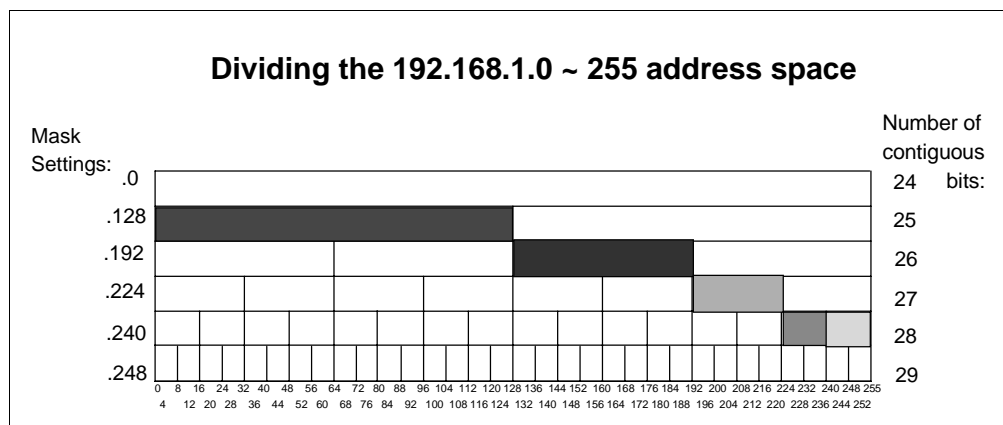


Figure 339. Address Ranges for the 192.168.1.0 Network

15.6.7 Configure As2.mycompany.com

There are different tasks required to complete the configuration of *As2.mycompany.com*.

15.6.7.1 Build a DHCP Configuration File

As2.mycompany.com is running the BOOTP/DHCP Relay Agent, but first you need to build a DHCP server configuration file. This must be done to complete the automatic setup of the workstation controller TCP/IP interface on the system. You do not need to start the DHCP server, but the DHCP configuration file must exist.

Refer to Section 15.4.3, “Configure the DHCP Server AS2 for Twinax Support” on page 366 for detailed instructions.

The first configuration dialog is shown in Figure 340 on page 386.

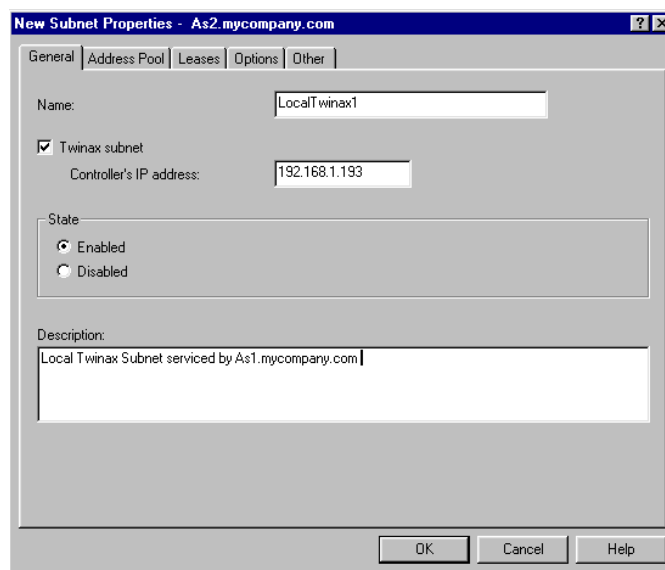


Figure 340. Twinax 1 Subnet (192.168.1.192) on AS2 Configuration Display

Click the **Address Pool** tab. Reduce the address range down to 32 contiguous IP addresses by specifying a subnet mask of 255.255.255.224. Refer to Figure 341.

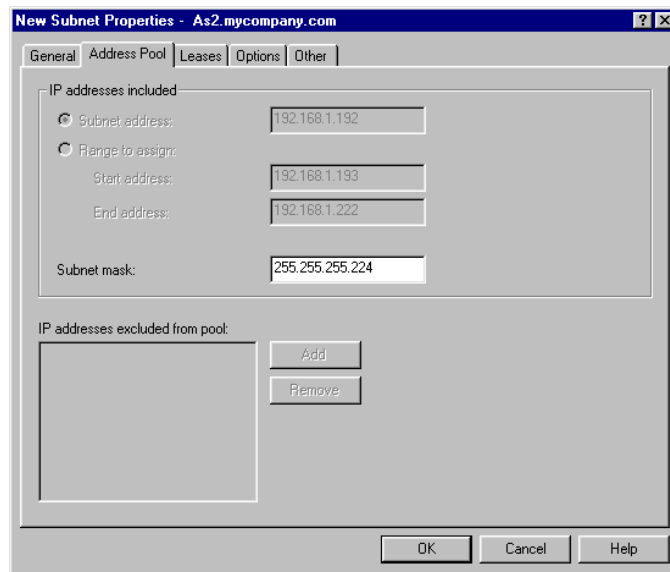


Figure 341. DHCP Server Configuration -- Subnet Mask Setting for the Twinax 1 Address Range

Click **OK**.

Note: The mask setting on the twinax interface determines the block of addresses for which the AS/400 system needs to Proxy ARP. In this example, the AS/400 system proxies for addresses 192.168.1.193 through 192.168.1.222. The associated local interface that is specified on the twinax interface (workstation controller TCP/IP interface) tells the IP stack which interface is proxying for the twinax subnet.

There is no need to configure any options or lease times on *As2.mycompany.com* because you do not start the DHCP server.

Note: Ensure that the DHCP server is in a *stopped* state once you have completed the configuration. Do *not* start the DHCP server. To be safe, disable the subnet on this system by right-clicking on the subnet and clicking on **Disable**.

If you experience a failure on the primary DHCP server, however, the BOOTP/DHCP Relay Agent on AS2 can end, and the DHCP server can start to service the local subnet. If you are planning to end the BOOTP/DHCP Relay Agent and start the DHCP server in an emergency, we recommend that you complete the entire configuration for the twinax subnet specifying options, lease times, DNS servers, and kernel load source information.

15.6.7.2 Start and Stop the IBM Network Station

Once you have built the DHCP configuration file, start the IBM Network Station. The AS/400 system builds the TCP/IP interface and line description for the workstation controller.

- Power on the twinax-attached IBM Network Station.

The message `NS0510 System 192.168.1.193 contacted` on the IBM Network Station is a good indication that the system has completed building the TCP/IP interface for the workstation controller.

The IBM Network Station sits on this message, so you can power it off at this time. It does not have enough information to complete the boot process at this stage.

Tip

If you are curious and want to see what the automatic configuration did, use the AS/400 `CFGTCP` command and specify option 1, *Work with TCP/IP interfaces*. There should now be an interface with the type of *TDLC. This is the TCP/IP interface of the workstation controller.

Once the workstation controller interface is auto-configured, move on to the next step.

15.6.7.3 Configure the BOOTP/DHCP Relay Agent

Once the system has automatically built the workstation controller TCP/IP interface, configure the BOOTP/DHCP Relay Agent. The relay agent forwards DHCP messages from the local workstation controller interface to the primary DHCP server on the main network.

For detailed instructions on configuring and starting a BOOTP/DHCP Relay Agent, refer to Section 15.1.8, “Configure and Start the DHCP Server on AS2” on page 346.

Refer to Figure 342 for a configuration example.

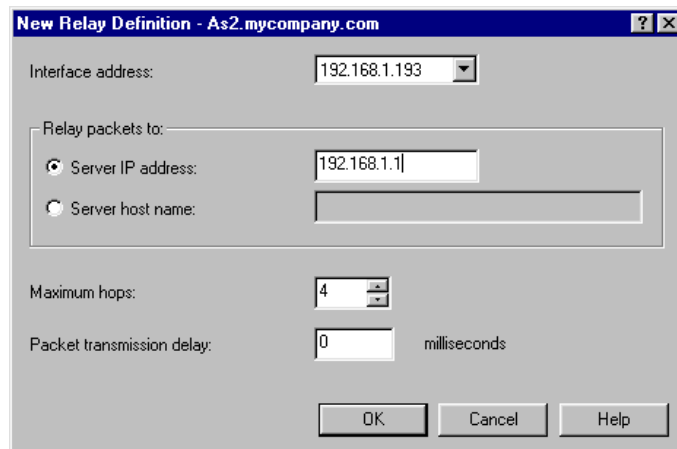


Figure 342. As2.mycompany.com Relay Configuration

Once you have saved the BOOTP/DHCP Relay Agent configuration, ensure that the server is started.

15.6.8 Configure As5.mycompany.com.

There are different tasks required to complete the configuration of *As5.mycompany.com*.

15.6.8.1 Build a DHCP Configuration File

As5.mycompany.com is running the BOOTP/DHCP Relay Agent, but first you must build a DHCP server configuration file to complete the automatic setup of

the workstation controller TCP/IP interface on the system. You do not need to start the DHCP server, but the DHCP configuration file must exist.

Refer to Section 15.4.3, “Configure the DHCP Server AS2 for Twinax Support” on page 366 for detailed instructions.

The first configuration dialog is shown in Figure 343 on page 389.

The dialog box is titled "New Subnet Properties - As5.mycompany.com". It has five tabs: General, Address Pool, Leases, Options, and Other. The General tab is active. It contains the following fields and controls:

- Name: LocalTwinax2
- ☒ Twinax subnet
- Controller's IP address: 192.168.1.225
- State:
☒ Enabled
☐ Disabled
- Description: Local Twinax Subnet serviced by AS1.mycompany.com
- Buttons: OK, Cancel, Help

Figure 343. Twinax 2 Subnet (192.168.1.224) on AS5 Configuration

Click the **Address Pool** tab. Reduce the address range down to 16 contiguous IP addresses by specifying the subnet mask of 255.255.255.240 (see Figure 344).

The dialog box is titled "New Subnet Properties - As5.mycompany.com". It has five tabs: General, Address Pool, Leases, Options, and Other. The Address Pool tab is active. It contains the following fields and controls:

- IP addresses included:
☒ Subnet address: 192.168.1.224
☐ Range to assign:
Start address: 192.168.1.225
End address: 192.168.1.238
Subnet mask: 255.255.255.240
- IP addresses excluded from pool:
Add
Remove
- Buttons: OK, Cancel, Help

Figure 344. AS5 DHCP Server Configuration -- Subnet Mask Settings for the Twinax 2 Address Range

Click **OK**.

Repeat the same steps for the second twinax subnet on this server (Twinax 3), 192.168.1.240. See Figure 345 and Figure 346 for configuration examples.

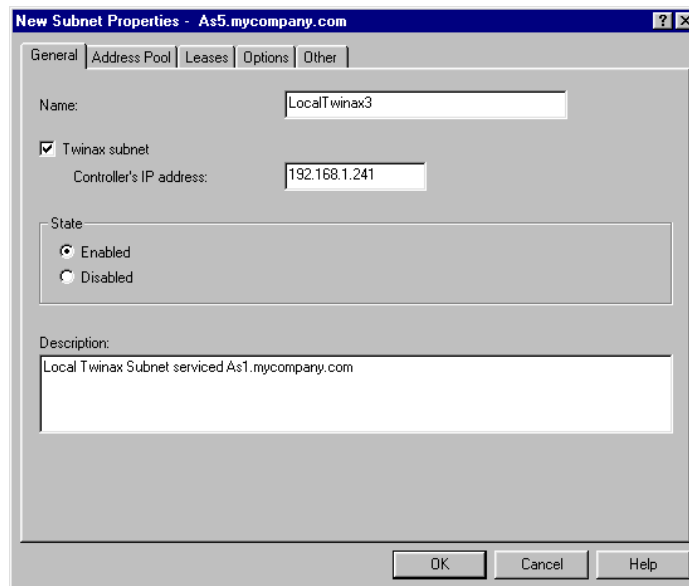


Figure 345. Twinax 3 Subnet (192.168.1.240) on AS5 Configuration

Click the **Address Pool** tab. Reduce the address range down to 16 contiguous IP addresses by specifying the subnet mask of 255.255.255.240. Refer to Figure 346.

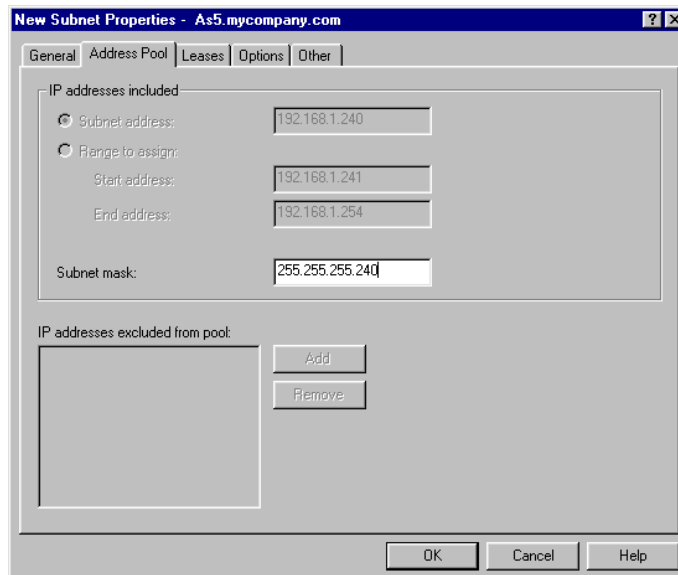


Figure 346. DHCP Server Configuration -- Subnet Mask Setting for the Twinax 3 Address Range

Click **OK**.

Because the DHCP server is not started, there is no need to configure any options or lease times on *As5.mycompany.com* for the twinax subnets.

Note: Ensure that the DHCP server is in a *stopped* state once you have completed the configuration. Do *not* start the DHCP server. To be safe, disable the subnet on this system by right-clicking on the subnet and clicking on **Disable**.

In the event of a failure on the primary DHCP server, however, you can end the BOOTP/DHCP Relay Agent on AS5 and start the DHCP server to service the local subnet. If you ever want to end the BOOTP/DHCP Relay Agent and start the DHCP server in an emergency, complete the entire configuration for the twinax subnet by specifying options, lease times, DNS servers, and kernel load source information.

Note: The mask setting on the twinax interface determines the block of addresses for which the AS/400 system needs to Proxy ARP. In these two examples, the AS/400 system proxies for addresses 192.168.1.225 through 192.168.1.254. The associated local interface that is specified on the twinax interface (workstation controller TCP/IP interface) tells the IP stack which interface is proxying for the twinax subnet.

15.6.8.2 Start and Stop the IBM Network Station

Once you have built the DHCP configuration file, start the IBM Network Station. The AS/400 system builds the TCP/IP interface and line description for the workstation controller.

Power on the IBM Network Station that is located on the Twinax 2 subnet (192.168.1.224).

The message `NS0510 System 192.168.1.225 contacted` on the IBM Network Station indicates that the system has completed building the TCP/IP interface for the workstation controller.

The IBM Network Station sits on this message, so you can power it off again at this time. It does not have enough information to complete the boot process at this stage.

Power on the IBM Network Station that is located on the Twinax 3 subnet (192.168.1.240).

Once the workstation controller interface is auto-configured, move on to the next step.

15.6.8.3 Configure the BOOTP/DHCP Relay Agent

Once the system automatically builds the workstation controller TCP/IP interface, configure the BOOTP/DHCP Relay Agent. The relay agent forwards DHCP messages from the local workstation controller interface to the primary DHCP server on the main network.

For detailed instructions on configuring and starting a BOOTP/DHCP Relay Agent, refer to Section 15.5.8, “Configure and Start BOOTP/DHCP Relay Agent on Local AS/400 System (AS2)” on page 376.

Figure 347 shows a BOOTP/DHCP Relay Agent configuration example for the twinax subnet 2 (192.168.1.224).

New Relay Definition - As5.mycompany.com

Interface address: 192.168.1.225

Relay packets to:

☒ Server IP address: 192.168.1.1

☐ Server host name:

Maximum hops: 4

Packet transmission delay: 0 milliseconds

OK Cancel Help

Figure 347. As5.mycompany.com Relay Definition for Twinax 2 (192.168.1.224)

Figure 348 shows a BOOTP/DHCP Relay Agent configuration example for the Twinax subnet 3 (192.168.1.240).

New Relay Definition - As5.mycompany.com

Interface address: 192.168.1.241

Relay packets to:

☒ Server IP address: 192.168.1.1

☐ Server host name:

Maximum hops: 4

Packet transmission delay: 0 milliseconds

OK Cancel Help

Figure 348. As5.mycompany.com Relay Configuration for Twinax 3 (192.168.1.240)

Once you have saved the BOOTP/DHCP Relay Agent configuration, ensure that the server is started.

15.6.9 Configure the DHCP Server on As1.mycompany.com

When you configure the DHCP server *As1.mycompany.com* to service the entire network (including the three twinax subnets), you need to break up the main address range, 192.168.1.x, into separate pools.

Define the address pool or range from which the DHCP clients in the main LAN are serviced. This is the pool that services clients or hosts that are directly connected to the token-ring LAN (excluding the twinax subnets).

The best way to demonstrate this is to show you what *not* to do. Figure 349 on page 393 is an example of what one might expect the configuration to be. Specify a subnet of 192.168.1.0 and a mask of 255.255.255.0, then change the address range to start at 192.168.1.1 and finish at 192.168.1.190. This appears to leave the range from 192.168.1.192 through 192.168.1.254 out of the main pool to be

used for the twinax subnets, but this appearance is *incorrect*. This is because the twinax subnet address range falls within this address space. For example, although twinax subnet 1 (192.168.1.192) is outside of the specified range, it *is* part of the address space 192.168.1.0 with a mask of 255.255.255.0, as shown in Figure 349 on page 393. The server, which always tries its best to serve an address to the client, gives an IP address from this pool to the client. This occurs even though you have defined the address pools for the twinax subnets.

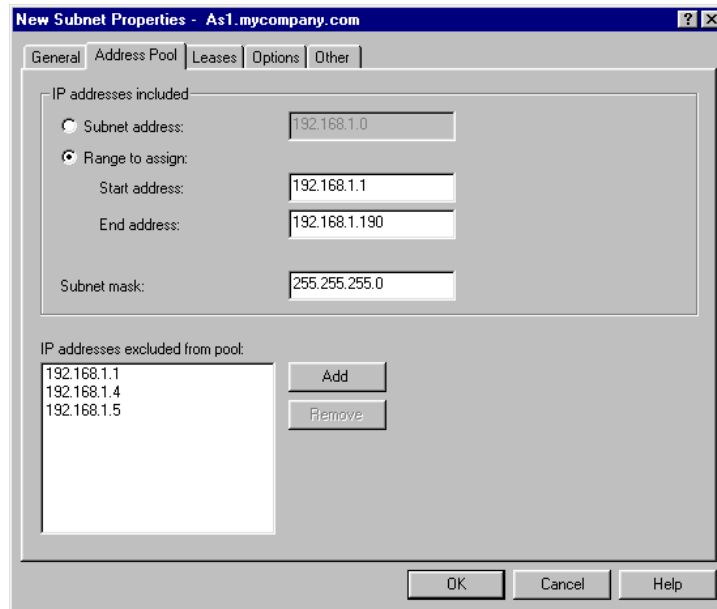


Figure 349. An Example of What **Not** to Do in this Scenario

The correct way to configure the main address pool (192.168.1.1 through 192.168.1.190) is to *lie* to the DHCP server by breaking down the address range into subnet groups and using more restrictive masks.

You must break up the address range from 192.168.1.1 through 192.168.1.254 into two groups (in this case) by applying masks to the range within the DHCP configuration. You then need to group the two groups back together within the DHCP configuration to form one pool. You also need to use DHCP option **1** to specify and pass back to the client the correct mask to use on this subnet.

To split the group into two pools, first apply the mask 255.255.255.128. This provides a range of 192.168.1.1 through 192.168.1.126. Next, apply the mask 255.255.255.192 to get the second group range of 192.168.1.129 through 192.168.1.190. Refer to Figure 350 on page 394 for a visual representation of the masking and grouping.

Note: You cannot use the subnet boundary addresses. Therefore, you lose three IP addresses from this range.

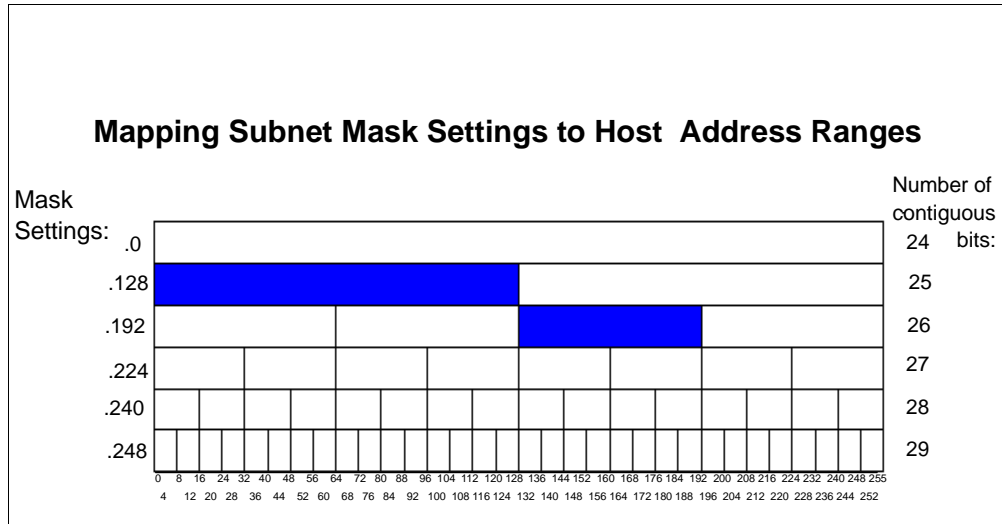


Figure 350. Applying Subnet Masks to Split Address Range 192.168.1.1 through 192.168.1.190

You must define the two pools in the DHCP configuration. Refer to Figure 351 for an example of the DHCP configuration of the first group. Refer to Figure 352 on page 395 for an example of the DHCP configuration of the second group.

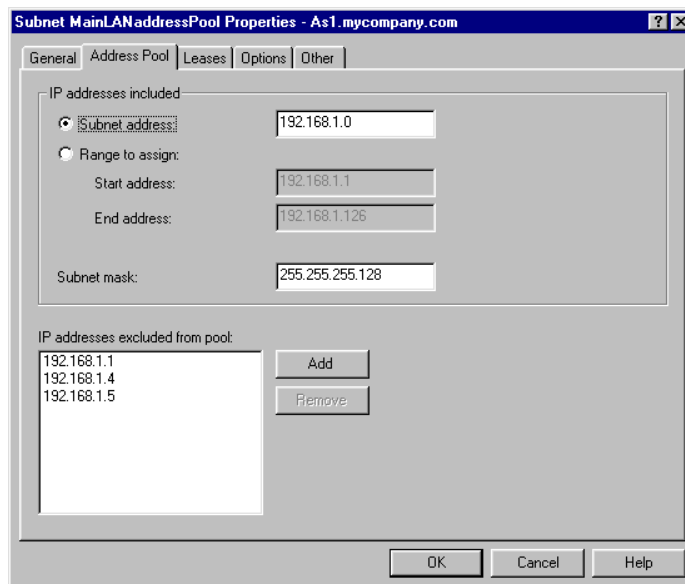


Figure 351. DHCP Configuration -- Dividing the Main LAN Address Pool with a Mask, Group #1

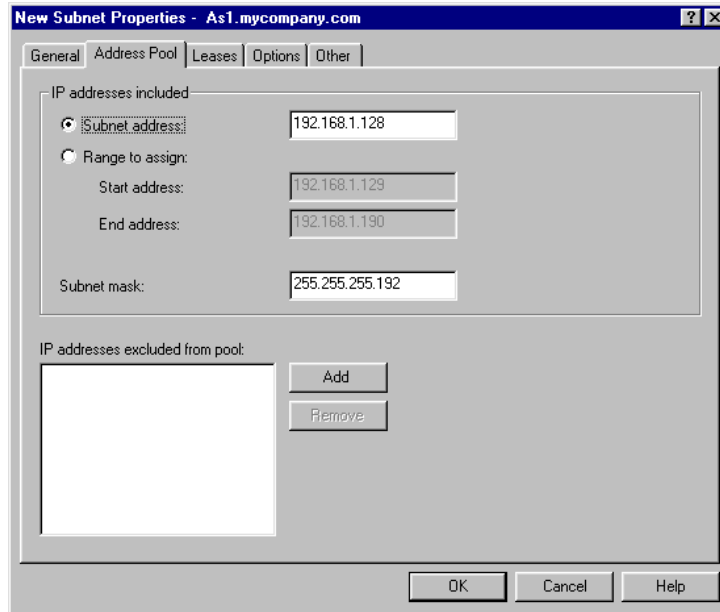


Figure 352. DHCP Configuration -- Dividing the Main LAN Address Pool with a Mask, Group #2

For both of these groups, you need to select the *Options* tab and configure DHCP option **1** to pass the real mask to use on this network, which is 255.255.255.0. You also need to configure any other relevant options that clients on the main network require.

The next step is to group the two address ranges together again to form one pool in the DHCP server configuration.

To form a subnet group within the DHCP configuration, perform the following steps:

1. From the Operations Navigator DHCP configuration, right-click **Global** to open a context menu.
2. Select **New Subnet Group**.
3. Specify a valid description in the *Name* field. Blanks are not valid.
4. Highlight the first address group and click **Add**. Repeat this step for the second group.

Note: Step 5 is optional.

5. Click the **Address Order** tab and click either **In order** or **Balanced**. In order is the default.

Figure 353 on page 396 shows the subnet group in the DHCP server configuration.

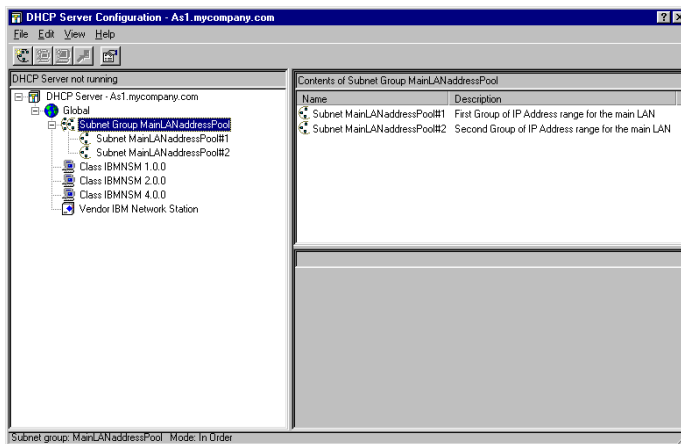


Figure 353. DHCP Server Configuration -- Subnet Group

You now need to configure the Twinax subnets on the DHCP server. Because these subnets are not directly attached, you do not build a twinax subnet configuration. Instead, build a normal subnet pool.

Figure 354 on page 397 shows the subnet ID and mask configuration that is used for the twinax subnet on *As2.mycompany.com*.

Figure 355 on page 397 shows the subnet ID and mask configuration that is used for the twinax subnet on *As5.mycompany.com*.

Figure 356 on page 398 shows the subnet ID and mask configuration that is used for the twinax subnet on *As5.mycompany.com*.

Note: It is necessary to exclude the IP address of the workstation controller from the twinax subnet pool and to provide the following options:

Option	Value
1 Subnet Mask	Twinax #1 255.255.255.224
	Twinax #2 255.255.255.240
	Twinax #3 255.255.255.240
3 Router	This value is the IP address of the workstation controller
	Twinax #1 192.168.1.193
	Twinax #2 192.168.1.225
66 Server Name	Twinax #3 192.168.1.241
	Twinax #1 192.168.1.193
	Twinax #2 192.168.1.225
	Twinax #3 192.168.1.241

Note

Configuring option 66 in this manner requires running TFTP on all three of the AS400 systems. Therefore, the kernel file must be maintained on all three systems as well. This is better for performance reasons but you can use a single TFTP server for all three twinax subnets as well. Any TFTP server (ANY valid IP address) can be used.

67 Boot File name /QIBM/ProdData/NetworkStation/kernel

It is also possible to load the terminal configurations setting for the IBM Network Stations from a central source, such as the DHCP server. Refer to 11.6, “Selecting the Bootstrap Host for the IBM Network Station” on page 252 for more information.

The screenshot shows a Windows-style dialog box titled "Subnet RemoteTwinax#1 Properties - As1.mycompany.com". It has five tabs: "General", "Address Pool", "Leases", "Options", and "Other", with "General" selected. The "IP addresses included" section has two radio buttons: "Subnet address" (selected) and "Range to assign". The "Subnet address" field contains "192.168.1.192". The "Range to assign" section has "Start address" (192.168.1.193) and "End address" (192.168.1.222) fields. The "Subnet mask" field contains "255.255.255.224". Below this, the "IP addresses excluded from pool" section has a list box containing "192.168.1.193" and "Add" and "Remove" buttons. At the bottom are "OK", "Cancel", and "Help" buttons.

Figure 354. DHCP Server Configuration Example for Twinax Subnet #1 on AS2

The screenshot shows a Windows-style dialog box titled "Subnet RemoteTwinax#2 Properties - As1.mycompany.com". It has five tabs: "General", "Address Pool", "Leases", "Options", and "Other", with "General" selected. The "IP addresses included" section has two radio buttons: "Subnet address" (selected) and "Range to assign". The "Subnet address" field contains "192.168.1.224". The "Range to assign" section has "Start address" (192.168.1.225) and "End address" (192.168.1.238) fields. The "Subnet mask" field contains "255.255.255.240". Below this, the "IP addresses excluded from pool" section has a list box containing "192.168.1.225" and "Add" and "Remove" buttons. At the bottom are "OK", "Cancel", and "Help" buttons.

Figure 355. DHCP Server Configuration Example for Twinax Subnet #2 on AS5

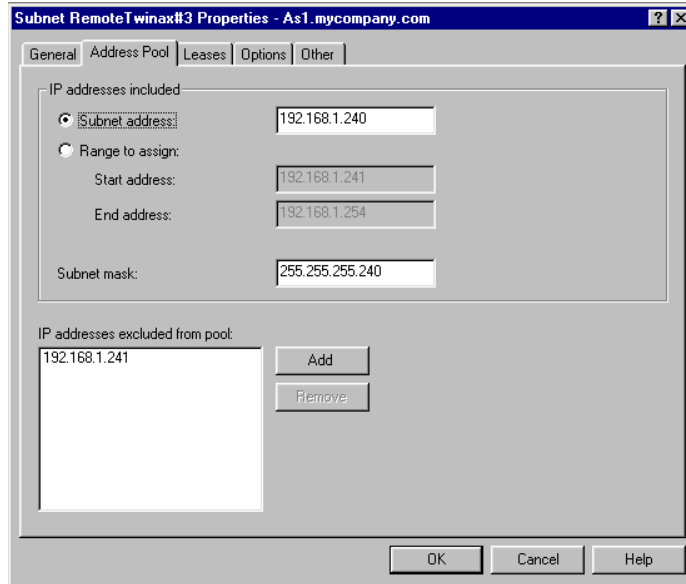


Figure 356. DHCP Server Configuration Example for Twinax Subnet #3 on AS5

15.6.10 Summary

This scenario showed the techniques required to divide your address space into contiguous portions of IP addresses for twinax subnets.

It described transparent subnet masking in detail. It also discussed how to split and to group IP address ranges in DHCP to support transparent subnetting and Proxy ARP, which allows connectivity for the twinax devices across your network.

Chapter 16. Migrating BOOTP Servers to DHCP

Bootstrap Protocol (BOOTP) provides a method for associating workstations with servers. It also provides a method for assigning workstation IP addresses and initial program load (IPL) sources. BOOTP is a TCP/IP protocol that allows a media-less workstation client (for example, an IBM Network Station) to request an IP address and the location of the initial code from a server on the network. PC-based clients, UNIX platforms, and others use the BOOTP protocol to gain an IP address and subnet mask to participate in the network.

The BOOTP server listens on the well-known BOOTP server port 67. When a client sends a BOOTP request, it places its MAC address into the packet. The BOOTP server compares this MAC address against a preconfigured BOOTP table that has IP addresses and MAC address mapped together. If the server finds the MAC address of the client in the table, it replies to the client with the IP address and mask to use.

To use the BOOTP boot method, you must record the MAC address of all the IBM Network Stations, PCs, and hosts that are using BOOTP. You must then assign each of them an IP address and specify those assignments in a BOOTP table. When you need to change the IP addresses, you can make the changes centrally on the table in the boot server. You do not need to make them individually on each client or host.

Refer to *IBM Network Station Manager Installation and Use*, SC41-0664, for information on installing and configuring the IBM Network Station.

Note

You must have *IOSYSCFG special authority to make changes to the BOOTP server.

16.1 Considerations

Prior to planning your migration from BOOTP to DHCP, consider if you truly need BOOTP support in your network at all. It makes sense to change the BOOT clients in your network to DHCP, discard the BOOTP table, and use a new DHCP configuration that suits your network.

BOOTP clients do not lease IP addresses the same as DHCP clients do. Instead, the DHCP server assigns an infinite lease time to the IP address for the client. With DHCP, the client gives up the IP address when the lease time expires, and the server returns it to the pool for the next DHCP client that requests an IP address. This effectively lets the DHCP server support more physical devices than you have IP addresses for, although not all at the same time.

It is possible that you have configured BOOTP to serve IBM Network Stations with information regarding the source from which to load its kernel and from which server it downloads the terminal configuration data. You must identify and reconfigure these options on the DHCP server to continue to support those devices with special needs. In the DHCP configuration, you can add options at a

global, subnet, class, or client level. This allows you to pass an option to every IBM Network Station that is part of the class, such as IBMNSM2.0.0. This is simpler than the BOOTP configuration that requires you to add a single entry in the BOOTP table for every IBM Network Station.

Operations Navigator detects the presence of a BOOTP table in your system when you start the DHCP server configuration. If the BOOTP table is found, the user is presented with a window to migrate the table to a DHCP server configuration.

If you choose to migrate the BOOTP table, a migration program reads each record in the file, bypassing comment records (which start with a # character) and empty or blank records.

Actual entry records are parsed apart through their BOOTP tags, and converted to valid DHCP configuration file **client** and **option** keyword values. Table 32 shows the mapping of BOOTP tags to DHCP configuration file keywords/options.

Table 32. BOOTP Tags to DHCP Configuration Keywords/Options

BOOTP tag and Description	DHCP Configuration Keyword or Option
ht= Hardware Type	1st parm of client keyword
ha= Hardware Address	2nd parm of client keyword
ip= IP Address	3rd parm of client keyword
sa= Boot Server	bootStrapServer
% hd= Home Directory	option 67
% bf= BOOTFILE	option 67
Note: If both hd and bf exist, only one option 67 is created, and its value is the hd value with the bf value appended to it (if the hd value did NOT end with /, a / is appended to it prior to appending the bf value).	
sm= subnet mask	option 1
to= time offset	option 2
gw= Gateway or Router	option 3
ts= Time Server	option 4
ns= Name Server	option 5
ds= Domain Server	option 6
lg= Log Server	option 7
cs= Cookie Server	option 8
lp= LPR Server	option 9
rl= Resource Locator Server	option 11
bs= Boot File Size	option 13
bt= BOOT_TYPE	nothing comparable - ignored
<anything_else_encountered>	ignored

16.2 Scenario 1: Migrating Existing BOOTP to a New DHCP Configuration

The following two methods are available to gain network startup information with OS/400 V4R2:

- BOOTP
- DHCP

You can use the DHCP server even if you currently use the BOOTP server on your AS/400 system. However, the BOOTP server and the DHCP Server cannot be active at the same time. The DHCP server recognizes BOOTP requests and services BOOTP clients if the server is configured to support BOOTP clients.

Note

To check or change the parameter to support BOOTP clients from the DHCP server configuration display, right-click *DHCP Server -- As1.mycompany.com* to open a context menu and select **Properties**.

Click the *Client Support* tab and ensure that **BOOTP clients** is checked.

You have the option to migrate from BOOTP to DHCP. This lets you take advantage of the more advanced and dynamic features of DHCP.

This section describes how to migrate from the AS/400 BOOTP server to the DHCP server.

16.2.1 Scenario Objectives

The objectives of this scenario are to:

1. Show how to migrate BOOTP client data to a new DHCP configuration.
2. Show how to migrate BOOTP client data to an existing DHCP configuration.

16.2.2 Existing Environment

An example of an existing environment with IBM Network Stations attached to the BOOTP server is shown in Figure 357 on page 402.

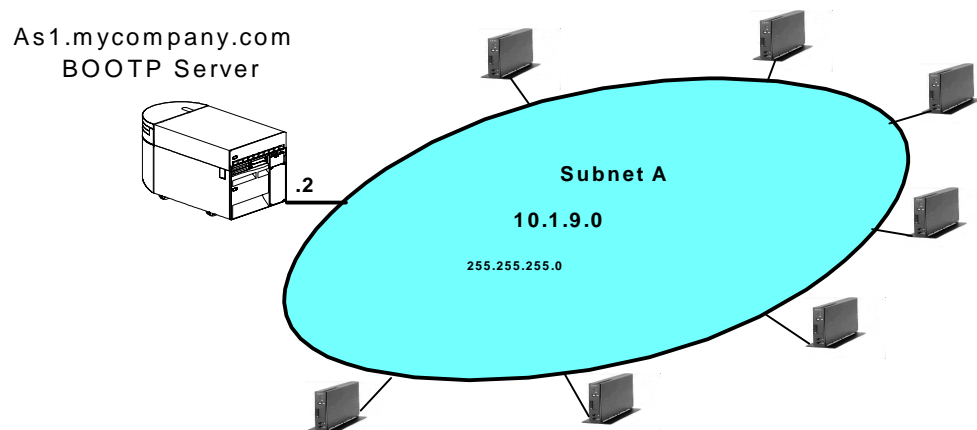


Figure 357. Example of an Existing Network with IBM Network Stations Attached

Use the Work with BOOTP Table (WRKBPTBL) command to display the existing BOOTP table entries (see Figure 358).

```

Work with BOOTP Table
System: AS1

Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display

Client
Host      MAC      IP
Opt  Name      Address  Address

ns04.mycompany.com  00.00.A3.78.56.41  10.1.9.14
ns05.mycompany.com  00.00.A5.88.45.23  10.1.9.15
ns06.mycompany.com  00.00.A7.33.23.12  10.1.9.16
ns07.mycompany.com  00.00.C1.42.51.17  10.1.9.17
5  NS01.mycompany.com  00.00.E5.68.37.96  10.1.9.11
   NS02.mycompany.com  00.00.E7.95.35.11  10.1.9.12
   NS03.mycompany.com  00.00.E9.73.10.90  10.1.9.13

F3=Exit  F6=Print list  F11=Set BOOTP Table Defaults  F12=Cancel  F17=Top
F18=Bottom
Bottom

```

Figure 358. BOOTP Table Entries of an Existing Network

Enter **5**, *Display* (see Figure 358), to display the details for the selected BOOTP table entry.

Display BOOTP Table Entry

System: AS1

Network device:
Client host name . . : NS01.mycompany.com

MAC address : 00.00.E5.68.37.96
IP address : 10.1.9.11
Hardware type : 6

Network routing:
Gateway IP address . :
Subnet mask :

Boot:
Type : ibmnsn
File name : kernel

File path : /QIBM/ProdData/NetworkStation

Press Enter to continue.

F3=Exit F12=Cancel

Figure 359. Display BOOTP Table Entry Details

The migration of the client configuration data depends on whether you are migrating BOOTP support to a new DHCP configuration or to an existing DHCP server.

16.2.3 Migrating BOOTP to a New DHCP Configuration

When you configure DHCP on a system without an existing configuration, Operations Navigator automatically starts the DHCP Configuration Wizard. Operations Navigator also supports the migration of the BOOTP configuration data into the new DHCP configuration.

To start the DHCP configuration wizard, perform the following steps:

1. Start Operations Navigator.
2. Click *As1.mycompany.com* to select the system.
3. Double-click **Network**.
4. Double-click **Server**.
5. Double-click **OS/400**.
6. Double-click **DHCP**. This starts the DHCP configuration wizard.
7. The DHCP configuration wizard is displayed. If not, it is likely that a DHCP configuration already exists. To start the wizard and replace the existing configuration, see Chapter 11.4.3, “Configure DHCP Server through Operations Navigator” on page 243.
8. Click **Next**.
9. Select **Yes** on the question “Do you want to disable the BOOTP server now?”

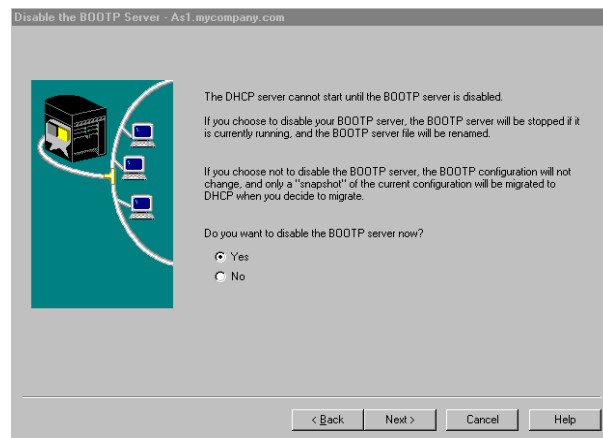


Figure 360. Disabling the BOOTP Server

10. Answer **No** to the question “Do you want to add a new subnet to the DHCP server?”

11. Click **Next**. The DHCP Configuration Summary is displayed.

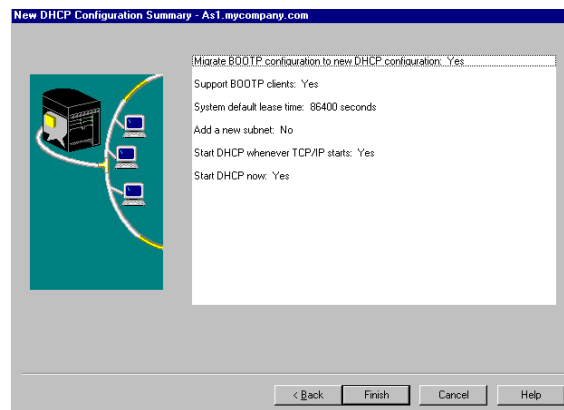


Figure 361. New DHCP Configuration Summary

12. Click **Finish** to display the results of the migration (see Figure 362 on page 405).

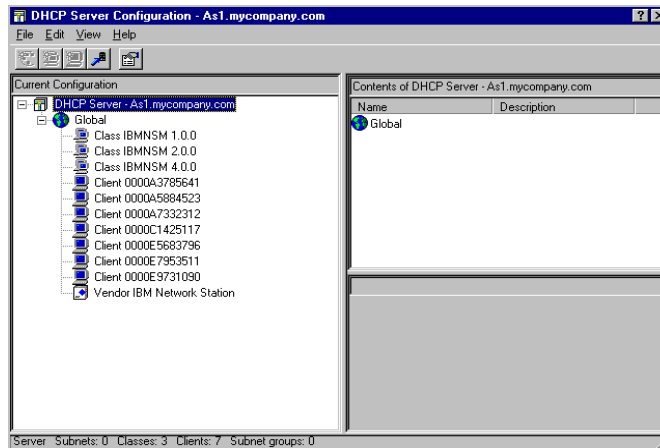


Figure 362. New DHCP Server Configuration after BOOTP Migration

16.2.4 Migrating BOOTP to an Existing DHCP Configuration

You can migrate BOOTP configuration data to an AS/400 system that you have already configured to act as a DHCP server but that you have not yet started. The BOOTP server and the DHCP server cannot be active at the same time on the same system. You can disable the BOOTP server at any time after you have done the migration. The DHCP server can serve all the clients that the BOOTP server previously served. The DHCP server provides some additional functions as well.

Note

It is possible that you have configured subnets within the DHCP server in which the address range you have specified includes currently active BOOTP clients. If so, the addresses used by the BOOTP clients have the lease time set to *infinite* or *never expire* when you migrate from BOOTP to DHCP. This means that the DHCP server does not hand out IP addresses that are in use by BOOTP clients after the migration from BOOTP to DHCP is complete.

Through Operations Navigator, perform the following the steps:

1. Click *As1.mycompany.com* to select the system.
2. Double-click **Network**.
3. Double-click **Server**.
4. Double-click **OS/400**.
5. Double- click **DHCP**. This shows the existing DHCP configuration.
6. Select **File**.
7. Select **Migrate BOOTP**.
8. If your system has a BOOTP configuration file, the Migrate BOOTP Configuration Dialog display in Figure 363 on page 406 appears.

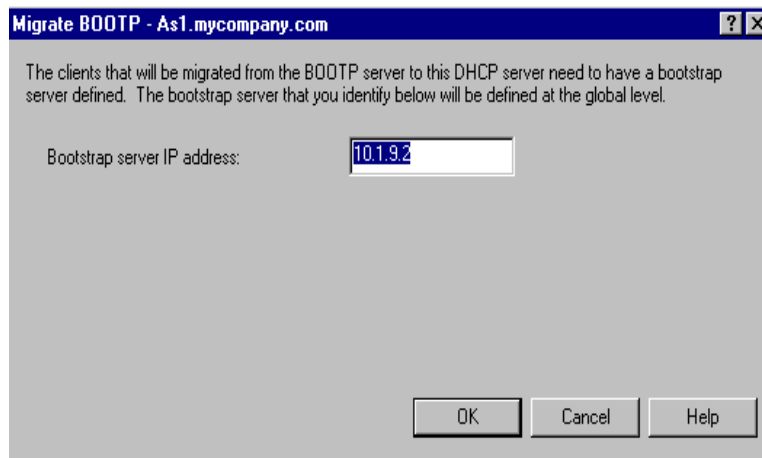


Figure 363. Migrate BOOTP Configuration Dialog

9. Specify the Bootstrap server IP address for the migrated clients to use.
10. Click **OK**. You see the DHCP Server configuration dialog with the client statements and an infinite lease time added for each client migrated, as shown here:

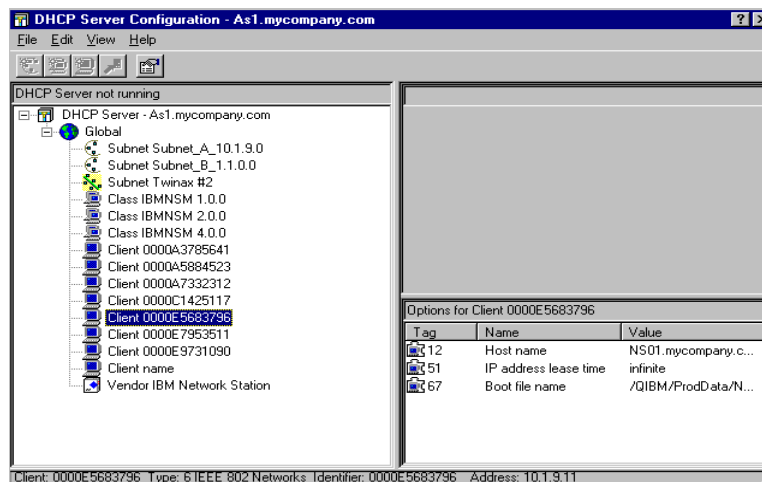


Figure 364. DHCP Server Configuration with Client Statements Added

16.2.5 Summary

This scenario demonstrated how to migrate an existing BOOTP table into a new DHCP server configuration.

It demonstrated how to migrate a BOOTP configuration into an existing DHCP server. You cannot run both the DHCP server and BOOTP server at the same time. The DHCP configuration was built prior to the migration, but the DHCP server was never activated until the migration was complete.

Chapter 17. DHCP Problem Determination

This chapter provides as much information as possible about the various types of problems you might have with the IBM AS/400 DHCP support. It also provides some guidelines and suggestions for solving these problems.

The problems and suggested solutions are divided into the following categories:

- Performing basic troubleshooting
- Starting and reading the DHCP logging utility
- Starting and decoding the AS/400 communication trace
- Resolving DHCP setup and installation problems
- Resolving error messages
- Resolving DHCP configuration problems
- Resolving DHCP client problems

17.1 Performing Basic Troubleshooting

Whenever you have a problem with your AS/400 DHCP server, perform the basic troubleshooting solutions that this section provides before you attempt more sophisticated solutions. Doing so can prevent you from creating larger problems with your AS/400 DHCP server.

17.1.1 Program Temporary Fixes (PTFs)

Always make sure that you have the latest PTFs installed. Because a code defect can cause the problem you are having with your AS/400 DHCP server, you can save yourself time and aggravation by ensuring you have installed the latest PTFs.

17.2 Starting and Reading the DHCP Logging Utility

The DHCP server has a logging feature that is helpful for problem determination. This section describes how to start, stop, and read the DHCP log.

17.2.1 Starting the DHCP Logging Utility

To start the DHCP server logging facility, perform the following steps:

1. Start the DHCP Configuration utility window through AS/400 Operations Navigator by double-clicking the **DHCP** server.
2. From the pull-down menu, select **File>Properties**.
3. Click the **Logging** tab.

To stop DHCP logging, uncheck the relevant check boxes.

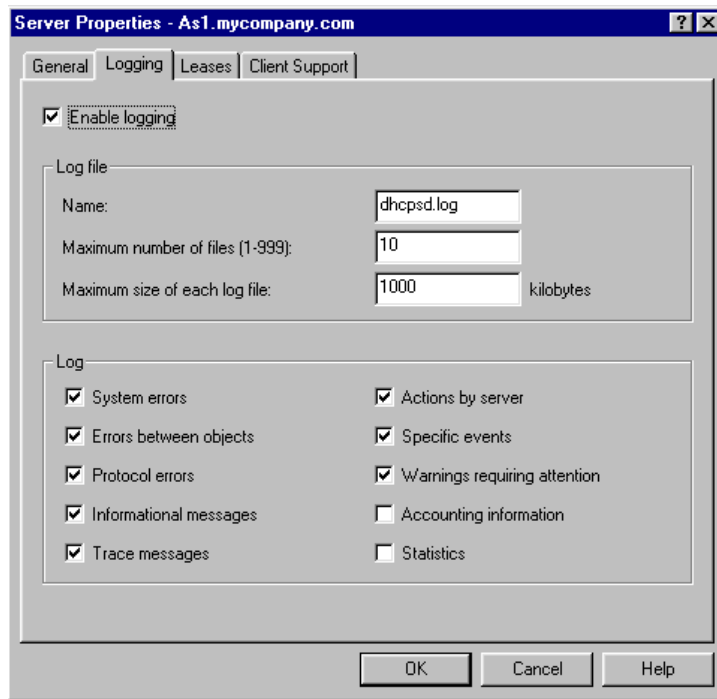


Figure 365. The Server Properties -- DHCP Server Logging Configuration in Operations Navigator

4. Ensure that the logging dialog looks the same as Figure 365. Check the *Enable logging* check box at the top of the dialog. At this stage, do not worry about the *Accounting information* and the *Statistics* check boxes.
5. Click **OK** to return to the DHCP Server Configuration window.

17.2.2 Reading the DHCP Log

This section explains how to access the DHCP log. It also shows you the cycle and steps of the DHCP protocol as it serves network information to the DHCP clients.

To locate the DHCP log, perform the following steps:

1. From the AS/400 Operations Navigator, select **File Systems>Root>QIBM>UserData>OS400>DHCP**.
2. The log file is called `dhcpd.log`. There can be several DHCP logs, depending on the options you set (see Figure 365). The DHCP server automatically closes the log when it is full, appends a sequenced number to it, and opens a fresh log file. You can open the file by using a simple editor, such as Notepad.

There are four basic steps that the client and server go through to request and bind a TCP/IP address. These steps are shown in Figure 366 on page 409.

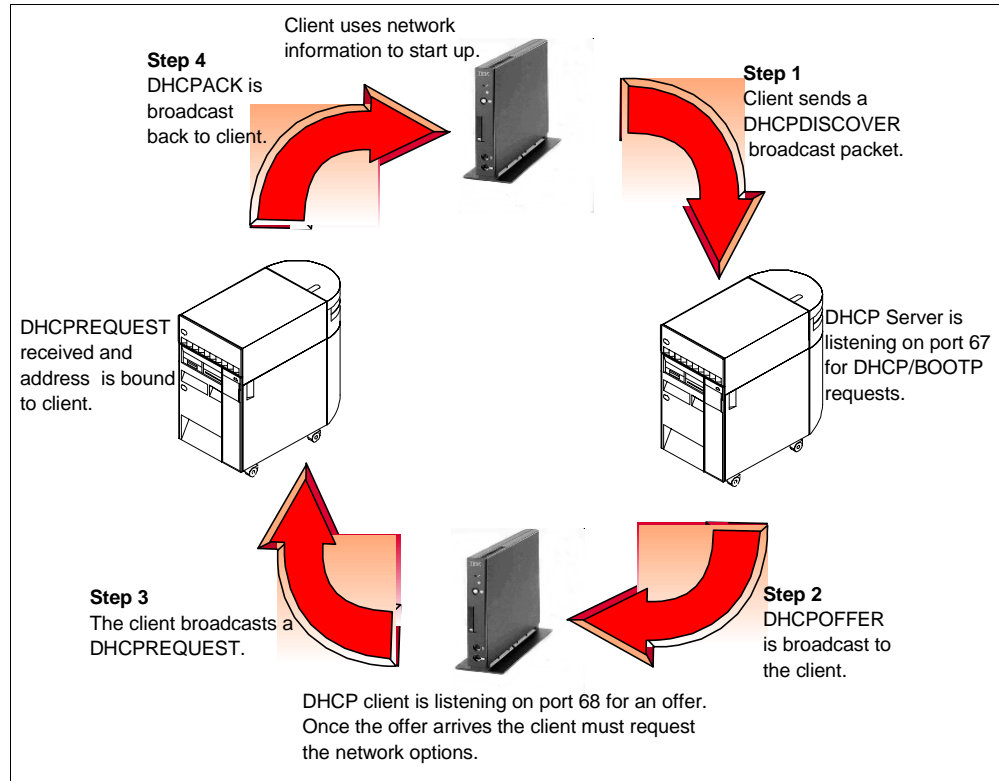


Figure 366. The Four Steps of the DHCP Client/Server Protocol

Table 33. Hexadecimal Value, DHCP Option Conversion Table

Hex Value	DHCP Option Number	DHCP Option Description
'01'	1	Subnet Mask.
'02'	2	Time off set of the clients subnet in seconds from Coordinated Universal time.
'03'	3	Router or gateway IP address listed in order of preference.
'04'	4	IP addresses (in order of preference) of the time servers available to the client.
'05'	5	IP addresses (in order of preference) of the IEN 116 name servers available to the client.
'06'	6	IP addresses (in order of preference) of the Domain Name System servers available to the client.
'07'	7	IP addresses (in order of preference) of the MIT-LCS UDP Log servers available to the client.
'08'	8	IP addresses (in order of preference) of the Cookie, or quote-of-the-day servers available to the client.
'09'	9	IP addresses in order of preference of line printer servers.
'0A'	10	IP addresses (in order of preference) of the Imagen Impress servers available to the client.

Table 34. Hexadecimal Value, DHCP Option Conversion Table, Continued

Hex Value	DHCP Option Number	DHCP option description
'0B'	11	IP addresses (in order of preference) of the Resource Location (RLP) servers available to the client.
'0C'	12	Host name of the client (which may include the local domain name).
'0D'	13	The length (in 512-octet blocks) of the default boot configuration file for the client.
'0E'	14	The path name of the merit dump file in which the client's core image is stored if the client crashes.
'0F'	15	Domain name that the client uses when resolving host names using the Domain Name System.
'10'	16	IP address of the client's swap server.
'11'	17	Path that contains the client's root disk.
'12'	18	The extensions path option allows you to specify a string that can be used to identify a file that is retrievable using Trivial File Transfer Protocol (TFTP).
'13'	19	Enable or disable forwarding by the client of its IP layer packets.
'14'	20	Enable or disable forwarding by the client of its IP layer datagrams with non-local source routes.
'15'	21	IP address-net mask pair used to filter datagrams with non-local source routes.
'16'	22	Maximum size datagram the client will reassemble. The minimum value is 576.
'17'	23	Default time-to-live (TTL) the client uses on outgoing datagrams.
'18'	24	Timeout used to age Path Maximum Transmission Unit (MTU) values discovered by the mechanism described in RFC 1191.
'19'	25	Table of MTU sizes to use in Path MTU discover as defined in RFC 1191. The minimum MTU value is 68.
'1A'	26	Maximum Transmission Unit (MTU) to use on this interface. The minimum MTU value is 68.
'1B'	27	Client assumes all subnets use the same Maximum Transmission Unit (MTU). A value of disabled means the client assumes some subnets have smaller MTUs.
'1C'	28	Broadcast address used on the client's subnet.
'1D'	29	Client performs subnet mask discovery using Internet Control Message Protocol (ICMP).
'1E'	30	Client responds to subnet mask requests using Internet Control Message Protocol (ICMP).

Table 35. Hexadecimal Value, DHCP Option Conversion Table, Continued

Hex Value	DHCP option number	DHCP option description
'1F'	31	Client solicits routers using router discovery as defined in RFC 1256.
'20'	32	Address to which a client transmits router solicitation requests.
'21'	33	Destination address-router pairs (in order of preference) the client installs in its routing cache. The first address is the destination address; the second address is the router for the destination.
'22'	34	Client negotiates the use of trailers when using Address Resolution Protocol (ARP). For more information, see RFC 893.
'23'	35	Timeout for Address Resolution Protocol (ARP) cache entries.
'24'	36	For an Ethernet interface, client uses IEEE 802.3 Ethernet encapsulation described in RFC 1042 or Ethernet V2 encapsulation described in RFC 894.
'25'	37	Default time-to-live (TTL) the client uses for sending TCP segments.
'26'	38	Interval the client waits before sending a keep-alive message on a TCP connection. 0 indicates the client does not send messages unless requested by the application.
'27'	39	Client sends TCP keep-alive messages that contain an octet of garbage for compatibility with previous implementations.
'28'	40	The client's Network Information Service (NIS) domain.
'29'	41	IP addresses (in order of preference) of Network Information Service (NIS) servers available to the client.
'2A'	42	IP addresses (in order of preference) of Network Time Protocol (NTP) servers available to the client.
'2B'	43	Vendor specific information. See RFC2132 for more information.
'2C'	44	IP addresses (in order of preference) of NetBIOS name servers (NBNS) available to the client.
'2D'	45	IP addresses (in order of preference) of NetBIOS datagram distribution (NBDD) name servers available to the client.
'2E'	46	Node type used for NetBIOS over TCP/IP configurable clients as described in RFC 1001 and RFC 1002.
'2F'	47	NetBIOS over TCP/IP scope parameter for the client, as specified in RFC 1001/1002.
'30'	48	IP addresses (in order of preference) of X Window System font servers available to the client.
'31'	49	IP addresses (in order of preference) of systems running X Window System Display Manager available to the client.
'32'	50	Used in a DHCPDISCOVER to allow the client to request an IP address.
'33'	51	IP address lease time used in the DHCPDISCOVER and DHCPREQUEST packets.

Table 36. Hexadecimal Value, DHCP Option Conversion Table, Continued

Hex value	DHCP option number	DHCP option description
'34'	52	Option overload used to indicate that the DHCP 'sname' or 'file' fields are being used to carry DHCP options.
'35'	53	DHCP message type (1=Discover,2=Offer, 3=Request, 4=Decline, 5=Ack, 6=Nak, 7=Release and 8=Inform).
'36'	54	Server Identifier used by the DHCP client to distinguish between lease offers.
'37'	55	Used by the DHCP client to request values for specified configuration parameters.
'38'	56	Used to convey an error message to the DHCP client in a DHCPNAK packet.
'39'	57	Maximum DHCP message size the client will accept.
'3A'	58	Interval between the time the server assigns an address and the time the client transitions to the renewing state.
'3B'	59	Interval between the time the server assigns an address and the time the client enters the rebinding state.
'3C'	60	Vendor class identifier.
'3D'	61	Client identifier.
'3E'	62	Netware/IP Domain Name.
'3F'	63	A general purpose option code used to convey all the NetWare/IP related information except for the NetWare/IP domain name.
'40'	64	Network Information Service (NIS)+ V3 client domain name.
'41'	65	IP addresses (in order of preference) of Network Information Service (NIS)+ V3 servers available to the client.
'42'	66	Trivial File Transfer Protocol (TFTP) server name used when the 'sname' field in the DHCP header has been used for DHCP options.
'43'	67	Name of the bootfile when the 'file' field in the DHCP header has been used for DHCP options.
'44'	68	IP addresses (in order of preference) of the mobile IP home agents available to the client.
'45'	69	IP addresses (in order of preference) of the Simple Mail Transfer Protocol (SMTP) servers available to the client.

Note: RFC 2132 contains details for these options, which you can find on the Internet at <http://ds.internic.net/rfc/rfc2132.txt>.

Table 37. Hexadecimal Value, DHCP Option Conversion Table, Continued

Hex value	DHCP option number	DHCP option description
'46'	70	IP addresses (in order of preference) of the Post Office Protocol (POP) servers available to the client.
'47'	71	IP addresses (in order of preference) of the Network News Transfer Protocol (NNTP) servers available to the client.
'48'	72	IP addresses (in order of preference) of the World Wide Web (WWW) servers available to the client.
'49'	73	IP addresses (in order of preference) of the Finger servers available to the client.
'4A'	74	IP addresses (in order of preference) of the Internet Relay Chat (IRC) servers available to the client.
'4B'	75	IP addresses (in order of preference) of the StreetTalk servers available to the client.
'4C'	76	IP addresses (in order of preference) of the StreetTalk Directory Assistance servers available to the client.
'4D'	77	Specified by the client to indicate to the server what class the client is from.
'4E'	78	A framework for passing configuration information to hosts using the Service Location Protocol.
'4F'	79	A scope used by a service agent responding to Service Request messages specified by the Service Location Protocol.
'50'	80	A naming authority specifying the syntax for schemes used in URLs used by entities with the Service Location Protocol.
'51'	81	A non-dynamic IP client allows the DHCP server to update the client's 'A' (1=true, 0=false). In either case, the client also sends its fully qualified domain name in the DHCPREQUEST.

17.2.3 Finding the Incoming DHCPDISCOVER Data in the Log

If you look in the log file of the DHCP server, you see the following information for step 1 in Figure 366 on page 409, the incoming DHCPDISCOVER packet.

Use the Notepad *find* option and search on DHCPDISCOVER.

The following steps walk you through the log data:

```

#1 16:21:35 : TRACE: .. receiveMailbox: DHCP comm descriptor selected
#2 16:21:35 : TRACE: .. receiveMailbox: recvfrom got 548 bytes.
#3 16:21:35 : TRACE: .. receiveMailbox: SELECT_SEMAPHORE
#4 16:21:35 : TRACE: Size of incoming packet is: 548
#5 16:21:35 : TRACE: .. process_bootrequest: function entered
#6 16:21:35 : TRACE: .. process_bootrequest: received packet xid = 627
#7 16:21:35 : INFO: .... primeOptions: Option: 53, length:1
#8 16:21:35 : INFO: .... primeOptions: Option: 57, length:2
#9 16:21:35 : INFO: .... primeOptions: Option: 77, length:12
#10 16:21:35 : INFO: .... primeOptions: Option: 60, length:19
#11 16:21:35 : TRACE: .... identifiableClient: function entered
#12 16:21:35 : TRACE: .... identifiableClient: Using htype, hlen and
chaddr to id client
#13 16:21:35 : TRACE: .... legibleRequest: function entered
#14 16:21:35 : TRACE: .... legibleRequest: DHCP msg type DHCPDISCOVER
#15 16:21:35 : TRACE: .. process_bootrequest: Request is self-consistent
#16 16:21:35 : TRACE: Packet from client 6-0x0000e5683796 was
accepted by user exit verification processing.
#17 16:21:35 : TRACE: .. reply_generator: function entered
#18 16:21:35 : TRACE: .... processDISCOVER: function entered

```

Figure 367. DHCP Log Data with a DHCPDISCOVER Request

1. On line #4, you see the size in bytes on the incoming DHCPDISCOVER packet.
 - The IBM Network Station and OS/2 clients typically send through a packet of 548 bytes.
 - Windows 95 typically sends through a packet size of around 300 bytes.
2. Line 7, 8, 9, and 10 are the `primeOptions` that the client needs to know to join the network and boot up. The options in this case are as follows:
 - Option 53** The DHCP message type in this case is a DHCPDISCOVER.
 - Option 57** The maximum DHCP message size that the client is willing to accept.
 - Option 77** The user class (IBMNSM 1.0.0.0 in this case).
 - Option 60** The vendor class identifier.

Note: To view the values of the options, you must run and decode an AS/400 communication trace. Refer to Section 17.3, “Starting, Formatting, and Decoding an AS/400 Communication Trace” on page 419, for more information.
3. Line #14 shows the message type, a **DHCPDISCOVER**.
4. Line #16 gives you the MAC address of the client. The number preceding the MAC address is the physical network layer code, as shown in the following examples:
 - Type 1** Ethernet
 - Type 6** Token ring
 - Type 26** TwinAxial

Note: PCs with a twinax card report hardware type 1.

5. Line #18 shows that the DHCPDISCOVER function has been entered.

17.2.4 Finding and Reading the DHCPOFFER Information in the Log

The DHCPOFFER packet is sent by the DHCP server in response to a DHCPDISCOVER packet that arrives on port 67. If the DHCP server has a valid subnet range of IP addresses defined for the network from which the DHCPDISCOVER packet originated, the DHCPOFFER is sent out.

Figure 368 on page 416 details the DHCPOFFER being generated in the DHCP log.

```

#1 16:23:56 : TRACE: ..... locateClientRecord: Located client
6-0x0000e5683796 in client records
#2 16:21:35 : TRACE: ..... locateConfiguredClient: function
entered
#3 16:21:35 : TRACE: ..... pr_queryAddr: netaddr = 10.0.0.0
#4 16:21:35 : TRACE: ..... pr_queryAddr: hostaddr = 0.1.1.3
#5 16:21:35 : TRACE: ..... locateConfiguredClient: look for client
match in this subnet
#6 16:21:35 : TRACE: ..... locateConfiguredClient: look for
client match in global clients
#7 16:21:35 : TRACE: ..... am_queryClient: Client
6-0x0000e5683796 is known to address mapper, status=4
#8 16:21:35 : TRACE: .... processDISCOVER: AM_STATUS_BOUND
#9 16:21:35 : WARNING:.... processDISCOVER: DISCOVER from client
6-0x0000e5683796 already bound with 10.1.1.3
#10 16:21:35 : TRACE: ..... pr_check_subnet_movement: Comparing
requested ip 10.1.1.3 & subnetmask 255.255.255.0 against subnet
10.1.1.0
#11 16:21:35 : TRACE: ..... isAddressInUse: Function Entered
#12 16:21:37 : TRACE: ..... isAddressInUse: IP address
10.1.1.3, not in use. rc=-26758468
#13 16:21:37 : TRACE: ..... locateAddressRecord: function Entered
#14 16:21:37 : INFO: ..... am_addressClient: Client
6-0x0000e5683796 suggested 10.1.1.3 is in range
#15 16:21:37 : INFO: ..... am_addressClient: Client
6-0x0000e5683796 had 10.1.1.3 mapped previously
#16 16:21:37 : TRACE: ..... indexAddressRecord: function Entered
#17 16:21:37 : ACTION: .... processDISCOVER: Address 10.1.1.3 has
been reserved
#18 16:21:37 : TRACE: ..... pr_queryAddr: netaddr = 10.0.0.0
#19 16:21:37 : TRACE: ..... pr_queryAddr: hostaddr = 0.1.1.3
#20 16:21:37 : TRACE: ..... locateConfiguredClient: look for client
match in this subnet
#21 16:21:37 : TRACE: ..... locateConfiguredClient: look for client
match in global clients
#22 16:21:37 : TRACE: ..... pr_queryAddr: function entered
#23 16:21:37 : TRACE: ..... pr_queryAddr: clue = [0x0a010103],
167837955
#24 16:21:37 : TRACE: ..... pr_queryAddr: netaddr = 10.0.0.0
#25 16:21:37 : TRACE: ..... pr_queryAddr: hostaddr = 0.1.1.3
#26 16:21:37 : TRACE: ..... locateAddressRecord: function Entered
#27 16:21:37 : TRACE: .. generate_bootreply: function entered
#28 16:21:37 : INFO: .. generate_bootreply: Generating a
DHCP OFFER reply
#29 16:21:37 : TRACE: .... locateConfiguredClient: function entered
#30 16:21:37 : TRACE: .... setSendWithoutARP: Entering setSendWithoutARP,
value 1.
#31 16:21:37 : TRACE: .. transmitMailbox: transmitting to
(10.1.1.3 #68)

```

Figure 368. DHCP Log Data Showing the DHCP OFFER being Generated

- Line #1 in the log, `locateClientRecord`, is an internal function of the DHCP server. The server compares the MAC address of the client to see if it already knows about the client.
- Line #7, `am_queryClient`, *has* found the address in the mapper records. This client has queried this DHCP server before.
- Line #9 tells you that the client has requested the same address it used last time.
- Line #10 is the comparison of the requested IP address from the client against the configured subnet pool on the DHCP server.
- Line #12, `isAddressInUse`, checks if the requested address has already been leased to another client.
- Lines #14 and #15 tell you that everything is currently satisfactory, that the address is in the subnet pool range, and that the internal address mapper remembers the client had this address last time.
- Line #17, `processDISCOVER`, reserves the address so it can offer it to the client.
- Line #28, `generate_bootreply`, is the generation of the offer.
- Line #31, `transmitMailbox`, sends the offer to the client or relay agent. The IP address and port ID are listed here.

17.2.5 Finding and Reading the DHCPREQUEST and DHCPACK Information

The client sends the DHCPREQUEST after it receives a DHCP OFFER, and the client requests the information that the DHCP server supplied. The client can also query the DHCP server for additional options.

Once the DHCP server receives the DHCPREQUEST, it issues a DHCPACK to tell the client to use the supplied IP address and network options.

If there are multiple DHCP servers, it is this request broadcasted back to the selected server that tells the other DHCP servers to release the address they had offered and reserved for the client because they have not been selected.

Figure 369 on page 418 shows the log data for the incoming DHCPREQUEST. The DHCPACK is then generated. Once again, the log has been cut to improve clarity.

Use the Notepad *find* option and search on DHCPREQUEST.

The following steps walk you through the sequence in the log file:

```

#1 16:23:56 : TRACE: .. receiveMailbox: DHCP comm descriptor selected
#2 16:23:56 : TRACE: .. receiveMailbox: recvfrom got 548 bytes.
#3 16:23:56 : TRACE: .. receiveMailbox: SELECT_SEMAPHORE
#4 16:23:56 : TRACE: Size of incoming packet is: 548
#5 16:23:56 : TRACE: .. process_bootrequest: function entered
#6 16:23:56 : TRACE: .. process_bootrequest: received packet xid = 627
#7 16:23:56 : INFO: .... primeOptions: Option: 53, length:1
#8 16:23:56 : INFO: .... primeOptions: Option: 50, length:4 value:
167837955 (0x0a010103)
#9 16:23:56 : INFO: .... primeOptions: Option: 54, length:4 value:
167837953 (0x0a010101)
#10 16:23:56 : INFO: .... primeOptions: Option: 57, length:2
#11 16:23:56 : INFO: .... primeOptions: Option: Parameter Request List,
length:12
#12 16:23:56 : INFO: .... primeOptions: Option 66 requested
#13 16:23:56 : INFO: .... primeOptions: Option 67 requested
#14 16:23:56 : INFO: .... primeOptions: Option 3 requested
#15 16:23:56 : INFO: .... primeOptions: Option 6 requested
#16 16:23:56 : INFO: .... primeOptions: Option 2 requested
#17 16:23:56 : INFO: .... primeOptions: Option 4 requested
#18 16:23:56 : INFO: .... primeOptions: Option 12 requested
#19 16:23:56 : INFO: .... primeOptions: Option 28 requested
#20 16:23:56 : INFO: .... primeOptions: Option 31 requested
#21 16:23:56 : INFO: .... primeOptions: Option 49 requested
#22 16:23:56 : INFO: .... primeOptions: Option 48 requested
#23 16:23:56 : INFO: .... primeOptions: Option 15 requested
#24 16:23:56 : INFO: .... primeOptions: Option: 77, length:12
#25 16:23:56 : INFO: .... primeOptions: Option: 60, length:19
#26 16:23:56 : TRACE: .... identifiableClient: function entered
#27 16:23:56 : TRACE: .... identifiableClient: Using htype, hlen and
chaddr to id client
#28 16:23:56 : TRACE: .... legibleRequest: function entered
#29 16:23:56 : TRACE: .... legibleRequest: DHCP msg type DHCPREQUEST
#30 16:23:56 : TRACE: .. process_bootrequest: Request is self-consistent
#31 16:23:56 : TRACE: Packet from client 6-0x0000e5683796 was accepted by
user exit verification processing.
#32 16:23:56 : TRACE: ..... locateExchange: function entered
#33 16:23:56 : TRACE: ..... locateExchange: Client id matches an
active exchange
#34 16:23:56 : TRACE: ..... pr_check_subnet_movement: Comparing requested
ip 10.1.1.3 & subnetmask 255.255.255.0 against subnet 10.1.1.0
#35 16:23:56 : TRACE: ..... locateConfiguredClient: function entered
#36 16:23:56 : TRACE: ..... locateConfiguredClient: look for client match
in this subnet
#37 16:23:56 : TRACE: ..... locateConfiguredClient: look for client
match in global clients
#38 16:23:56 : TRACE: .... processREQUEST: Offer was selected by client
6-0x0000e5683796
#39 16:23:56 : TRACE: ..... addressManager: Function entered
#40 16:23:56 : TRACE: .... processREQUEST: Address 10.1.1.3 has
been bound to 6-0x0000e5683796
#41 16:23:57 : TRACE: .. generate_bootreply: function entered
#42 16:23:57 : INFO: .. generate_bootreply: Generating a DHCPACK
reply

```

Figure 369. DHCP LOG Data with the Incoming DHCPREQUEST and a DHCPACK being Generated

1. Line #4 shows the incoming packet and size.
2. Line #6 shows the transaction ID.
3. Lines #7 to #25 are the incoming options that the client wants to resolve. The first four options, #53, #50, #54, and #57 must be completed. The client wants the rest of the options but can attach to the network without them.
4. Line #33, `locateExchange`, compares the transaction ID and verifies that there is an active exchange between this server and the client.
5. Line #40, `processREQUEST`, binds the IP address to the client's MAC address and sets the address to `In-use`.
6. The last line, `generate_bootreply`, generates the DHCPACK packet and sends it to the client or relay agent.

Note

Unfortunately, the DHCP log does not show which options the DHCP server supplied to the client. You must interrogate the AS/400 communications trace to find that information. See Section 17.3.3, "Reading and Decoding the AS/400 Communications Trace Data" on page 421 for more information. You can also use the `QIBM_QTOB_DHCP_ABND` user exit program to retrieve the options.

17.3 Starting, Formatting, and Decoding an AS/400 Communication Trace

This section contains instruction on how to start, stop, and format trace data that is collected by the AS/400 communication trace facility. This section also shows the method to decode the data within the trace if you want to see what options are being passed to and from the DHCP clients and servers.

17.3.1 Start the AS/400 Communication Trace

To start the AS/400 communications trace, perform the following steps:

1. From the AS/400 command line, enter the `STRSST` command. This starts the System Service Tools.
2. Enter option **1** to start a service tool.
3. Enter option **3** to work with a communications trace.
4. Press **F6** to start a communication trace.

5. Fill in the name of your line, the buffer size, and a description. Leave the rest of the options as defaults.

```

                                Start Trace

Type choices, press Enter.

Configuration object . . . . . TRNLINE1

Type . . . . . 1          1=Line, 2=Network interface
                           3=Network server

Trace description . . . . . Tracing DHCP

Buffer size . . . . . 4      1=128K, 2=256K, 3=2M, 4=4M
                           5=6M, 6=8M, 7=16M, 8=32M
                           9=64M

Stop on buffer full . . . . . N      Y=Yes, N=No

Data direction . . . . . 3      1=Sent, 2=Received, 3=Both

Number of bytes to trace:
  Beginning bytes . . . . . *CALC  Value, *CALC
  Ending bytes . . . . . *CALC  Value, *CALC

F3=Exit  F5=Refresh  F12=Cancel

```

6. Press **Enter**.
7. On the **Trace Options** display, select option **1** to gather all the data without filtering.
8. Press **Enter**. The trace is now active.

17.3.2 Stopping the AS/400 Communication Trace

Once the problem has been recreated, stop the AS/400 communications trace as soon as possible.

To end the communications trace, perform the following steps:

1. From the AS/400 command line, enter the command `STRSST`. This starts the System Service tools.
2. Enter option **1** to start a service tool.
3. Enter option **3** to work with a communications trace.
4. Enter a **2** to stop the trace.
5. Enter **6** to format and print the trace.
6. You are now prompted for the format information. Change the data format to ASCII and format the broadcast data and TCP/IP data only, as shown in the following display:

```

                                Format Trace Data

Configuration object . . . . : TRNLINE1
Type . . . . . : LINE

Type choices, press Enter.

Controller . . . . . *ALL      *ALL, name

Data representation . . . . 1      1=ASCII, 2=EBCDIC, 3=*CALC

Format RR, RNR commands . . . N      Y=Yes, N=No
Format Broadcast data . . . Y      Y=Yes, N=No
Format MAC or SMT data only . N      Y=Yes, N=No
Format UI data only . . . . N      Y=Yes, N=No
Format SNA data only . . . . N      Y=Yes, N=No
Format TCP/IP data only . . . Y      Y=Yes, N=No
Format IPX data only . . . . N      Y=Yes, N=No

F3=Exit      F5=Refresh      F12=Cancel

```

7. Press **Enter**.
8. You are now asked if you want to filter out TCP/IP addresses. This is unnecessary in this example because you have a controlled environment. If you have a busy network and you know the clients IP address, then specify it here.
9. Press **Enter**. The trace is being formatted. This can take some time, depending on how large the sample is.
10. Once the trace is formatted, you are returned to the *Work with Communications trace* display, and the line trace is in a stopped state. It is okay to leave the trace stopped as long as it is not running then. You can always return to this display and format the trace again if you desire to do so. However, if you delete it, you must start over to gather the data.
11. Exit *System Service Tools* by following the prompts.
12. To find the formatted trace data, enter the `WRKSPLF` command.

17.3.3 Reading and Decoding the AS/400 Communications Trace Data

This section discusses the AS/400 communications trace data that you captured and formatted in the previous steps.

This section concentrates only on reading the first discovery packet that the client sent. The method used to decode the data and find the options being sent or received is the same.

To locate and decode the DHCP line trace data, follow these steps:

1. Locate the spooled file and view the data online. Online viewing allows you to search for keywords more quickly.
2. Perform a *find* on `BOOTPS`, and press **F16** (Shift + PF4) to search. Figure 370 on page 422 shows the result.

Note: It is common for the DHCP client to send out multiple DHCPDISCOVER packets before it receives a DHCPOFFER.

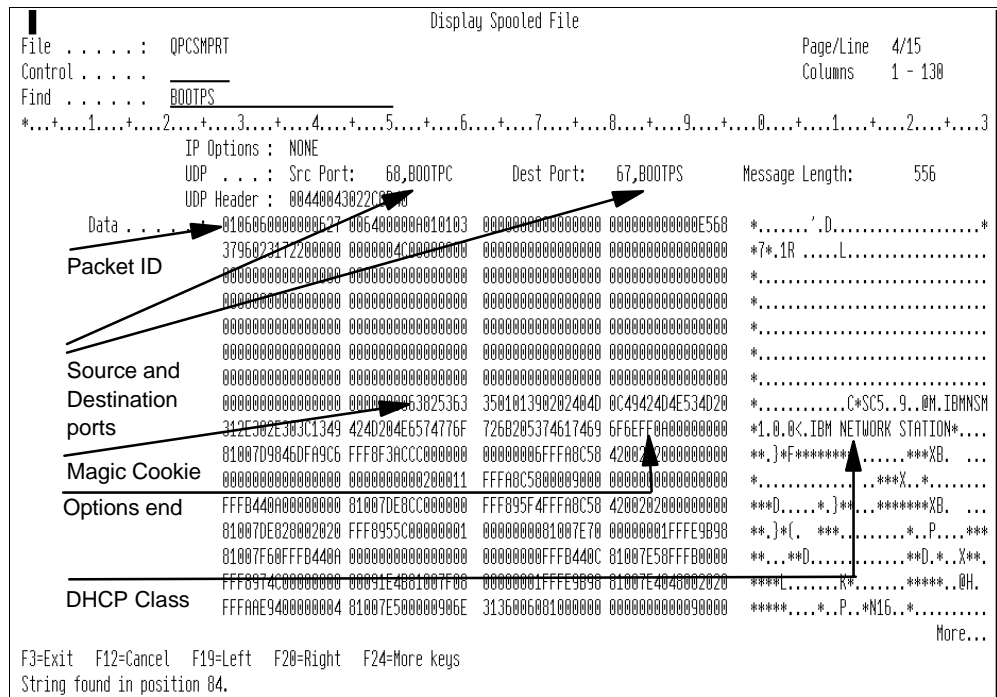


Figure 370. DHCP Boot Request in the Communication Trace

3. The information required for problem determination in the DHCP boot request is described in detail, as follows:

- The first byte in the data, '01', states that this is a request. 02 is a reply.
- The source and destination ports are shown. This packet is from the DHCP client. The server always listens on port 67, and the client always listens on port 68.
- The magic cookie in hex '63 82 53 63' signifies the start of the DHCP options. This is defined in RFC 2132.
- The byte 'FF' in hex signals the end of the DHCP options.

All options that are defined in RFC 2132 start with the options code in hex. The next byte states the length of the data.

4. The first three bytes after the magic cookie are as follows: hex '35 01 01', which is converted to decimal; hex '35', which is option number 53 (refer to Table 33 on page 409); and '01', which is the length of the following data that contains the value '01'. The following list shows that '01' is a DHCPDISCOVER. RFC2132 states that this option must have a length of one byte and that the type is also one byte.

The value of the type byte for option 35 is as follows:

- | | |
|-----------|--------------|
| 01 | DHCPDISCOVER |
| 02 | DHCPOFFER |
| 03 | DHCPREQUEST |
| 04 | DHCPDECLINE |
| 05 | DHCPACK |

06	DHCPNAK
07	DHCPRELEASE
08	DHCPINFORM

5. The next four bytes in hex are '39 02 02 40'. Hex '39' in decimal is 57. The RFC states that option 57 is the maximum DHCP message size that the client accepts. The second byte (hex '02') is the length of the option, and the last two bytes are expressed as an unassigned, 16-bit integer. Converting hex '02 40' to decimal produces 576 bytes, which is the maximum length that the client accepts. The RFC also states that this is the minimum length as well.
6. The next group of bytes are hex '4D 0C 49 42 4D 4E 53 4D 20 31 2E 30 2E 30'. The second byte always states the length, so you must get the next 12 bytes. The first byte hex '4D' is 77 in decimal, Option **77** is the user class that clients use to indicate to DHCP servers the class of which they are a member.
 - The remaining 12 bytes converted to decimal are as follows:
73 66 77 78 83 77 32 49 46 48 46 48
 - Convert them to ASCII, and you get the following values:
I B M N S M 1 . 0 . 0

The trace data on the right has been converted to ASCII. This is also one of the user classes, which is defined automatically when you build the DHCP configuration.
7. The next group of bytes in hex are '3C 13 49 42 4D 20 4E 65 74 77 6F 72 6B 20 53 74 61 74 69 6F 6E'. Hex '3C' converted to decimal is option **60**, the vendor class identifier. When the next byte (hex '13') is converted to decimal, it states that the length is 19 bytes. Once the rest of the string has been converted to decimal and applied to the ASCII code table, you can see that the vendor information being passed has the value of *IBM Network Station*. This is also shown on the right in ASCII in the trace data.
8. The next byte in hex is 'FF'. This indicates the end of the user options.

17.4 Symptoms, Problems, and Resolutions

17.4.0.1 Symptom: DHCP Client cannot ping hosts on the network.

A Windows 95 DHCP client has loaded its IP stack without error but cannot ping other hosts on the network. A ping to the loop back address works, confirming that the IP stack is functioning.

Possible cause: No subnet mask was supplied to the client, or an unacceptable TCP/IP address was given.

Verify: On the Windows 95 client, run the executable WINIPCFG.EXE. This displays the IP address and the subnet mask that the client is using.

Solution: If the address or the mask is not valid, use Operations Navigator to check the DHCP server configuration.

To further resolve the problem, view the DHCP logging information as described in Section 17.2, "Starting and Reading the DHCP Logging Utility" on page 407. It might then be necessary to view the options that are being passed to the DHCP client by using the AS/400 communication tracing facility. This is described in

Section 17.3, “Starting, Formatting, and Decoding an AS/400 Communication Trace” on page 419.

17.4.0.2 Symptom: DHCP client cannot ping hosts on different subnet

The DHCP client can ping clients in the local subnet but fails to ping clients on remote subnet.

Possible cause: No router information was supplied or the wrong router IP address was configured.

Solution: Verify and option 3 (router) and configure it properly.

17.4.0.3 Symptom: DHCP Server not forwarding to DHCP relay.

The DHCP relay appears to be forwarding DHCP messages to the DHCP server. Further, the DHCP server generates replies and sends them back to the BOOTP/DHCP Relay Agent. However, the BOOTP/DHCP Relay Agent never gets the message or sends it to the client.

Diagnostics: Check the BOOTP/DHCP Relay Agent log file first to determine if the relay agent is performing the forwarding *to* and *from* the server correctly.

The log can be found in the directory

/As5.mycompany.com/QIBM/UserData/OS400/DHCP/dhcprd.log

Figure 371 is an example from the BOOTP/DHCP Relay Agent log. It shows broadcasted DHCP messages from subnet 10.1.2.0 being sent to the DHCP server at address 10.1.0.2 on port 67.

```
02/12 10:42:49 : TRACE:   Size of incoming packet is: 548
02/12 10:42:49 : TRACE: .. process_incoming_msg: function entered
02/12 10:42:49 : TRACE: .... relay_to_server: function entered
02/12 10:42:49 : INFO: .... relay_to_server: assign giaddr as 167838211
02/12 10:42:49 : ACTION: .... relay_to_server: Relay packet from
interface 10.1.2.3 to server to at 10.1.0.2
02/12 10:42:49 : TRACE: ..... transmitMailbox: transmitting to
(10.1.0.2 #67)
02/12 10:42:49 : TRACE: ..... setSendWithoutARP: Entering
setSendWithoutARP, value 0.
```

Figure 371. BOOTP/DHCP Relay Agent Forwarding to DHCP Server Log File Extract

Figure 372 is a working example of the BOOTP/DHCP Relay Agent log showing the returned DHCP message from the DHCP server being forwarded to the client.


```

02/12 10:42:54 : TRACE:   Size of incoming packet is: 548
02/12 10:42:54 : TRACE: .. process_incoming_msg: function entered
02/12 10:42:54 : TRACE: .... relay_to_client: function entered
02/12 10:42:54 : TRACE: ..... setSendWithoutARP: Entering
setSendWithoutARP, value 1.
02/12 10:42:54 : ACTION: .... relay_to_client: unicast reply to
client
02/12 10:42:54 : TRACE: ..... transmitMailbox: transmitting to
(10.1.2.4 #68)
02/12 10:42:54 : TRACE: ..... setSendWithoutARP: Entering
setSendWithoutARP, value 0.

```

Figure 372. BOOTP/DHCP Relay Agent Forwarding to DHCP Client Log File Extract

If the line with the statement `relay_to_client` does not appear in the log file, this indicates that the BOOTP/DHCP Relay Agent is not receiving a reply from the DHCP server.

Verify that the DHCP server log is receiving messages from the BOOTP/DHCP Relay Agent. Also verify that the DHCP server is transmitting the DHCP messages back to the BOOTP/DHCP Relay Agent.

Figure 373 is an extract from the DHCP server log. It shows the incoming DHCPDISCOVER message from the BOOTP/DHCP Relay Agent.

```

02/25 09:26:35 : TRACE: .. receiveMailbox: DHCP comm descriptor selected
02/25 09:26:35 : TRACE: .. receiveMailbox: rcvfrom got 548 bytes.
02/25 09:26:35 : TRACE: .. receiveMailbox: SELECT_SEMAPHORE
02/25 09:26:35 : TRACE:   Size of incoming packet is: 548
02/25 09:26:35 : TRACE: .. process_bootrequest: function entered
02/25 09:26:35 : TRACE: .. process_bootrequest: received packet xid = b03
02/25 09:26:35 : INFO: .... primeOptions: Option: 53, length:1
02/25 09:26:35 : INFO: .... primeOptions: Option: 57, length:2
02/25 09:26:35 : INFO: .... primeOptions: Option: 77, length:12
02/25 09:26:35 : INFO: .... primeOptions: Option: 60, length:19
02/25 09:26:35 : TRACE: .... identifiableClient: function entered
02/25 09:26:35 : TRACE: .... identifiableClient: Using htype, hlen and
chaddr to id client
02/25 09:26:35 : TRACE: .... legibleRequest: function entered
02/25 09:26:35 : INFO: .... legibleRequest: Relay agent on 10.1.2.3
is 1 from the client
02/25 09:26:35 : TRACE: .... legibleRequest: DHCP msg type
DHCPDISCOVER

```

Figure 373. DHCP Server Log Extract with Incoming Transmission from the BOOTP/DHCP Relay Agent

The line that reads `Relay agent on 10.1.2.3 is 1 from the client` tells you that the client's DHCP message has travelled through one hop, or one BOOTP/DHCP Relay Agent.

Figure 374 is another extract from the DHCP server log that shows the response being transmitted to the BOOTP/DHCP Relay Agent.

```

02/25 09:26:35 : INFO:  .. generate_bootreply: Generating a DHCP OFFER reply
02/25 09:26:35 : TRACE:  .. transmitMailbox: transmitting to (10.1.2.3 #67)
02/25 09:26:35 : TRACE:  .... setSendWithoutARP: Entering setSendWithoutARP, value 0.

```

Figure 374. DHCP Server Log Extract with Outgoing Transmission to the BOOTP/DHCP Relay Agent

Possible Cause: No route is configured on the DHCP server to return the DHCP messages to the relay agent. The DHCP server sends the DHCP messages back to the interface on which the DHCP relay is listening for DHCP broadcasts. The DHCP server log informs you that the message has been sent, but the BOOTP/DHCP Relay Agent does not have a log entry, as shown in Figure 372.

Refer to Figure 375 on page 426, which shows the message flow. The BOOTP/DHCP Relay Agent intercepts the broadcasted DHCP messages and forwards them directly to the DHCP server through interface 10.1.0.4. The replies from the DHCP server are sent to interface 10.1.2.3 on the BOOTP/DHCP Relay Agent. This is because the BOOTP/DHCP Relay Agent places its IP address from the interface on the subnet that received the DHCP broadcast. It does this so that the DHCP server can tell which subnet the client is on and serve the correct IP address.

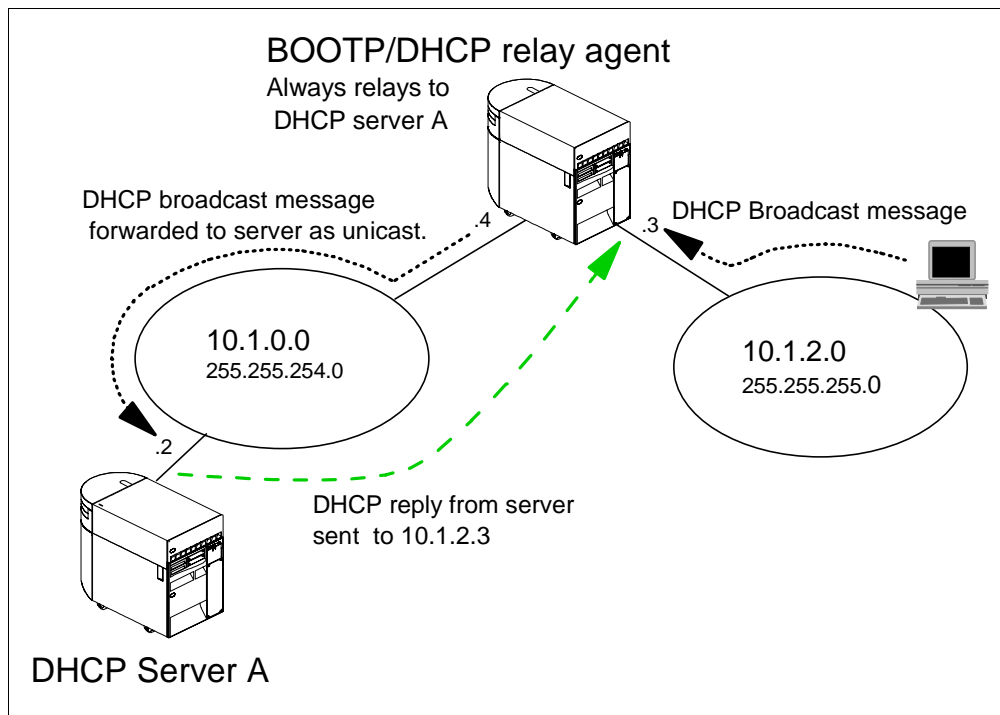


Figure 375. BOOTP/DHCP Relay Agent Message Flow.

Note

Once the DHCP client has accepted an offer from the DHCP server, lease renewals for the client's IP address are sent directly to the DHCP server's IP address. Lease renewals are not broadcast and, therefore, not forwarded by a BOOTP/DHCP Relay Agent. Valid routing information must exist within a subnetted network.

Verify: To verify that there is no route to subnet 10.1.2.0, attempt to ping interface 10.1.2.3 from the DHCP server. A negative response indicates that the DHCP server does not have visibility to the subnet.

Solution: If the ping failed, you need to add routing information on the DHCP server so that it can access subnet 10.1.2.0. Alternatively, you can enable RIP on the AS/400 systems to advertise the route to the subnet.

To configure a TCP/IP route, perform the following steps:

1. From the AS/400 command line, specify `CFGTCPIP` and press **Enter**.
2. Select option **2**, Work with TCP/IP routes, and press **Enter**.
3. Enter a **1** to add routing information. See the following display for details:

```
Work with TCP/IP Routes                                     System:Asl.mycompany.com
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display

Route      Subnet      Next      Preferred
Opt  Destination  Mask      Hop      Interface
--  -
_   10.1.2.0      255.255.255.0  10.1.0.4  10.1.0.2

F3=Exit    F5=Refresh  F6=Print list  F11=Display type of service
F12=Cancel F17=Top     F18=Bottom

Bottom
```

17.4.0.4 Symptom: IBM Network Stations not starting through DHCP.

The twinax-attached IBM Network Stations do not load the kernel and complete a boot up.

Possible cause: There are many factors that can hinder the startup of a twinax-attached IBM Network Station. The DHCP server can be configured incorrectly, or it might not be started. The options passed to the client might be

incorrect, or if a BOOTP/DHCP Relay Agent is involved, this might also be configured incorrectly or be in need of starting.

Verify: Check the DHCP server log (as described in Section 17.2.2, “Reading the DHCP Log” on page 408) and verify that the DHCP discover message is being heard. Also verify that an offer is being sent to the IBM Network Station. Check the IP address to which the offer is being sent. The offer should be sent to the IP address of the client. If the offer being made has the IP address of the workstation controller and if it looks as though the offer is, in fact, being sent to the workstation controller’s address, this is incorrect.

Solution: Somehow the lease data in the DHCP server might have become corrupted. The DHCP server must never give out the workstation controller’s IP address to a client.

In this situation, clearing out the existing twinax leases solves the problem. You can accomplish this easily through Operations Navigator.

To reset the lease information for any subnet that is configured in the DHCP server, perform the following steps:

1. In the DHCP configuration window from the left-most window, right-click the twinax subnet to open a context menu and select **Disable**.
2. Click **OK** on the informational pop-up window that reads *The Subnet will not be disabled until the DHCP server is updated*.
3. On the tool bar, click the following **Update server** icon:



4. Right-click the twinax subnet again to open another context menu and select **Enable**.
5. Click **OK** on the informational pop-up window that reads *The Subnet will not be disabled until the DHCP server is updated*.
6. On the tool bar, click the **Update server** icon previously shown.

The whole range of addresses in the twinax subnet is now free.

17.5 DHCP Server Performance Considerations

The following factors negatively affect DHCP processing server run-time performance:

- User exit programs. The magnitude of degradation increases for each exit program registered.
- **pingTime** configuration parameter. The higher the value is, the worse the overall response time per request.
- **leaseExpireInterval**. This configuration parameter can negatively impact performance if set extremely low (one minute or lower).

- Logging. The number of **logItem** value enabled and type. **TRACE** is the most verbose.
- Startup or restart time is proportional to the number of items configured to be managed, the size of the items stored in the non-volatile storage, and how drastic the changes in the configuration are from what was stored in non-volatile storage.

The following factors negatively affect BOOTP/DHCP Relay Agent run-time performance:

- Transmission delay configuration parameter.
- Logging. The number of **logItem** value enabled and type. **TRACE** is the most verbose.

Appendix A. Mail Concepts

This appendix intends to summarize some concepts and functions of the AS/400 mail implementation that you need to understand to follow the examples in Chapter 6, “Split DNS: Hiding Your Internal DNS Behind a Firewall” on page 125. If you are already familiar with the mail implementation on the AS/400 system, please skip this appendix.

A.1 Basic Mail Configuration

The basic configuration that you need to perform to deliver mail from / to POP3 clients follows:

1. Configure the AS/400 SMTP server. To do that, use the following the steps:
 - Configure the host name and domain name using the Change TCP Domain (CHGTCPDMN) command or CFGTCP option 12:

Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name 'as1'

Domain name 'mycompany.COM'

Host name search priority . . . *REMOTE *REMOTE, *LOCAL, *SAME

Internet address '10.5.69.222'

Figure 376. Configuring Host and Domain Names

- Verify that there is an IP address associated with the host name for the system either in the DNS server configuration or local host table.

Add an A record in the DNS server configuration for the SMTP mail server host:

DNS

as1.mycompany.com IN A 10.5.69.222

If you are not using a DNS server, use the Add TCP Host Table Entry (ADDTCPHTE) command or CFGTCP option 10 to add the host's IP address to the host table. The host table entry should look similar to this:

Internet	Host
Address	Name
10.5.69.222	AS1.MYCOMPANY.COM

2. Add an entry in the system distribution directory for the user. The following displays show **only** the relevant parameters.

```

Change Directory Entry

User ID/Address . . . . : USER1      AS1

Type changes, press Enter.

Description . . . . . Pop user
System name/Group . . . AS1          F4 for list
User profile . . . . . USER1        F4 for list
Network user ID . . . . USER1      AS1
                                         More...

```

Figure 377. Directory Entry for Pop User - General Information

To get to the next display, page down four times.

```

Change Directory Entry

User ID/Address . . . . : USER1      AS1

Type changes, press Enter.

Mail service level . .  2              1=User index
                                         2=System message store
                                         4=Lotus Domino
                                         9=Other mail service

For choice 9=Other mail service:
Field name . . . . . F4 for list

Preferred address . . .  3              1=User ID/Address
                                         2=O/R name
                                         3=SMTP name
                                         9=Other preferred address
                                         F4 for list

Address type . . . . .
For choice 9=Other preferred address:
Field name . . . . . F4 for list
                                         More...

```

Figure 378. Mail Service Level = System Message Storage - Preferred Address = SMTP Name

Press **F19** to configure the SMTP name for the user.

Change Name for SMTP

System: AS1

User ID/Address : USER1 AS1

Type choices, press Enter.

SMTP user ID user1

SMTP domain as1.mycompany.com

SMTP route

Figure 379. User's SMTP Name

3. Start the mail servers:

1. Start the SMTP server

```
STRTCPSVR SERVER(*SMTP)
```

2. Start the POP3 server:

```
STRTCPSVR SERVER(*POP)
```

3. Start the Mail Server Framework:

```
STRMSF
```

A.2 Mail Forwarding

Assume *user1@as1.mycompany.com* moves to *user1@research.mycompany.com*. We want to have all the SMTP/MIME mail sent to user1 at the old address automatically forwarded to the new address.

Likewise, if your company's internal network is connected to the Internet through a firewall, all the incoming mail is passed by the firewall to the system configured as the secure mail server. If there is more than one mail server in your internal network, you need a *forwarding* function in the secure mail server that forwards the piece of mail to the mail server where the *To:* user resides.

Figure 380 on page 434 illustrates this concept.

1. Mail from the Internet is sent to *user@mycompany.com*. In our example, two pieces of mail arrive at *mycompany.com*'s firewall's mail relay: one destined to *userx@mycompany.com*; the other one to *user5@mycompany.com*.

Note: In this scenario, the internal and external domain names are the same: *mycompany.com*.

2. The firewall changes the domain name in the piece of mail to *user@"secure_mail_server.private_domain_name"*. In our example, this is *user5@as1.mycompany.com* and *userX@as1.mycompany.com*. The mail relay in the firewall forwards all the inbound mail to the configured secure mail server (AS1 in our example).

3. The forwarding function in AS1 (the mail hub) decides that *user5* resides in internal mail server AS3 and that *userX* resides in internal mail server AS2 and forwards the mail to the corresponding mail server.

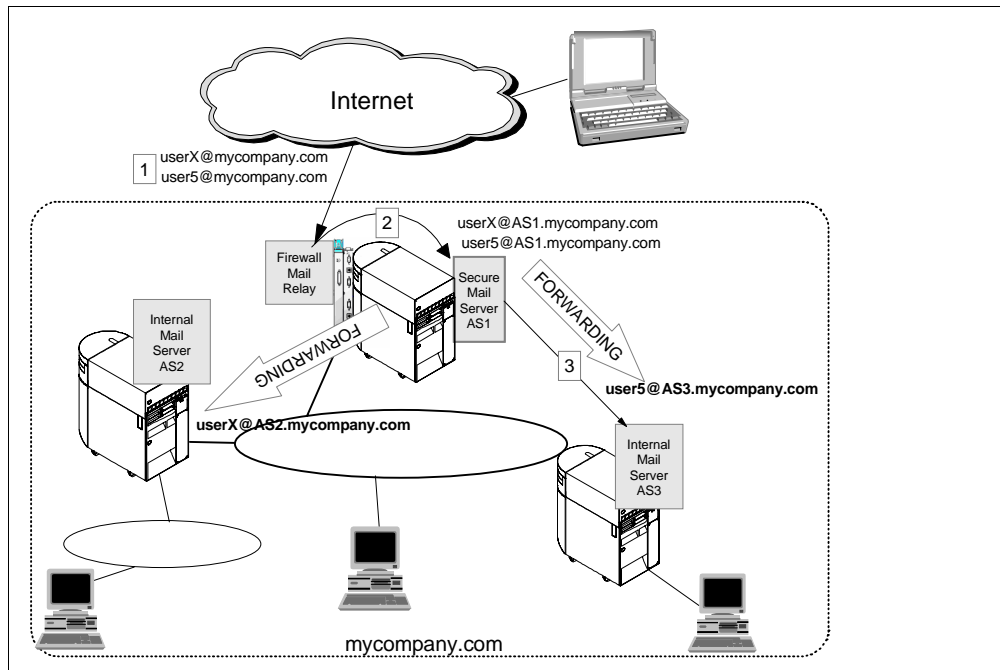


Figure 380. Forwarding Mail From the Secure Mail Server to the Destination Internal Mail Server

A.2.1 Implementing Mail Forwarding

To implement the mail forwarding function, you need to perform two main configuration tasks at the mail hub (the system that receives the piece of mail and decides if it is for *this* mail server or must be forwarded):

1. Add two “user-defined” fields to the system distribution directory.
2. Add an entry in the system distribution directory for *every single user* in the entire network protected by the firewall. This is how the AS/400 mail hub (secure mail server) knows what real SMTP address to use to forward the mail for the user.

Note

To perform the mail forwarding function through user-defined fields, the following fixes are required:

V3R2: 5763-SS1 PTF SF43715 and 5763-TC1 PTF SF43699

V3R7: 5716-SS1 PTF SF43803 and 5716-TC1 PTF SF43799

A.2.1.1 Adding User-Defined Fields to System Distribution Directory

Create two user-defined fields in the system distribution directory using the Change System Directory Attributes (CHGSYSDIRA) command.

1. Enter the CHGSYSDIRA command and press **F4**.

2. Page down until the User-defined field parameters are displayed.
3. Fill in the information as shown in Figure 381.

Change System Dir Attributes (CHGSYSDIRA)

Type choices, press Enter.

User-defined fields:

Field name	FORWARDING	Character value, *SAME
Product ID	*NONE	Character value, *NONE
Function	> *ADD	*ADD, *RMV, *CHG, *KEEP
Field type	*ADDRESS	*DATA, *MSFSRVLVL, *ADDRESS
Maximum field length	256	1-512
Field name	FWDSRVLVL	Character value
Product ID	*NONE	Character value, *NONE
Function	> *ADD	*ADD, *RMV, *CHG, *KEEP
Field type	*MSFSRVLVL	*DATA, *MSFSRVLVL, *ADDRESS
Maximum field length	001	1-512

More..

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display

Figure 381. Adding User-Defined Fields to the System Distribution Directory

A.2.1.2 Adding Directory Entries to Perform the Forwarding Function

For each user in your internal network, you must add an entry in the system distribution directory at the mail hub (secure mail server or *old* mail server if you are implementing the function to redirect mail).

1. From an AS/400 command entry display, enter the command:
WRKDIR
Press **Enter**.
2. Select option **1**, Add.
3. Enter the following information. Notice that IUSER5 and INTERNET are values that we chose arbitrarily; they do not match any other configuration value.

Add Directory Entry

Type choices, press Enter.

User ID/Address	IUSER5	AS1
Description	Forward Mail to user5@as3.mycompany.com	
System name/Group	INTERNET	F4 for list
User profile		F4 for list
Network user ID		

4. Page down until the display in Figure 382 is shown. Fill in the information as indicated in Figure 382.

Add Directory Entry

Type choices, press Enter.

Mail service level . . . 9	1=User index 2=System message store 4=Lotus Domino 9=Other mail service
For choice 9=Other mail service:	
Field name FWDSRVLV	F4 for list
Preferred address . . . 9	1=User ID/Address 2=O/R name 3=SMTP name 9=Other preferred address
Address type ATMIME	F4 for list
For choice 9=Other preferred address:	
Field name FORWARDING	F4 for list

Figure 382. Adding Directory Entry to Forward SMTP/MIME Mail

Note: Address type MIME is equivalent to ATMIME. If the ATMIME option does not show in the F4 list on your system, select MIME.

5. Press **F19** to enter the SMTP user ID and SMTP domain in the incoming mail to the mail hub. This must match the user ID and domain in the piece of mail relayed by the firewall to the secure mail server (step 2 in Figure 380 on page 434.)

Specify User-Defined Fields

Type choices, press Enter.

SMTPAUSRID	SMTP	user5
SMTPDMN	SMTP	as1.mycompany.com

Figure 383. Specify SMTP User ID and SMTP Domain as Received by the Mail Hub

Press **Enter**.

6. Press **F20** to specify the forwarding information as shown in Figure 384.

Specify User-Defined Fields

Type choices, press Enter.

FORWARDING **user5@as3.mycompany.com**

FWDSRVLVL

Figure 384. Specifying Mail Forwarding Information

Press **Enter** to add the directory entry to the system distribution directory.

Figure 385 shows the relationship between parameters in the directory entry at the mail hub (AS1) and the directory entry for the user at the real mail server (AS3).

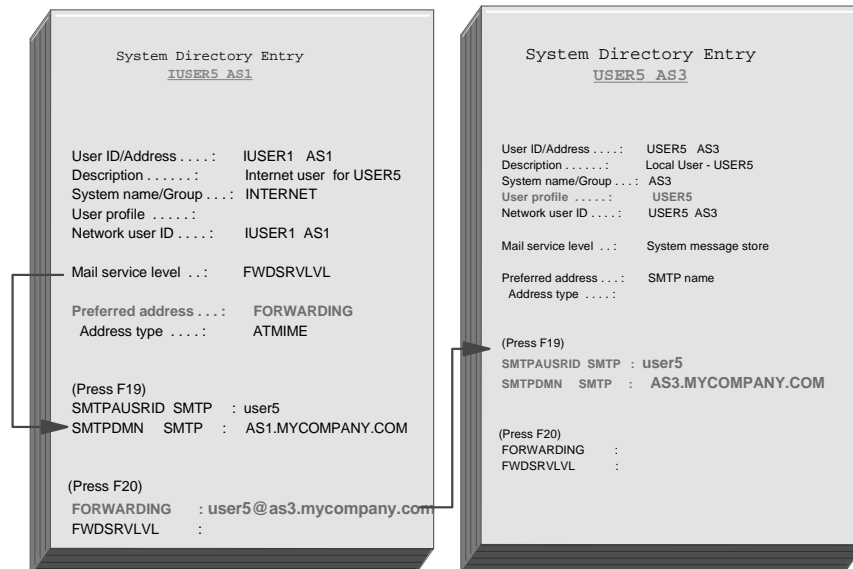


Figure 385. Relationship Between Directory Entries in Mail Hub and User's Mail Server

A.3 Processing Inbound Mail

Now that we have discussed the configuration needed to process inbound mail on an AS/400 SMTP server, let's put everything together. Figure 386 shows a high level overview of how the AS/400 SMTP server processes inbound SMTP/MIME mail. Notice that in all our examples, we are always assuming that the recipient is a POP user.

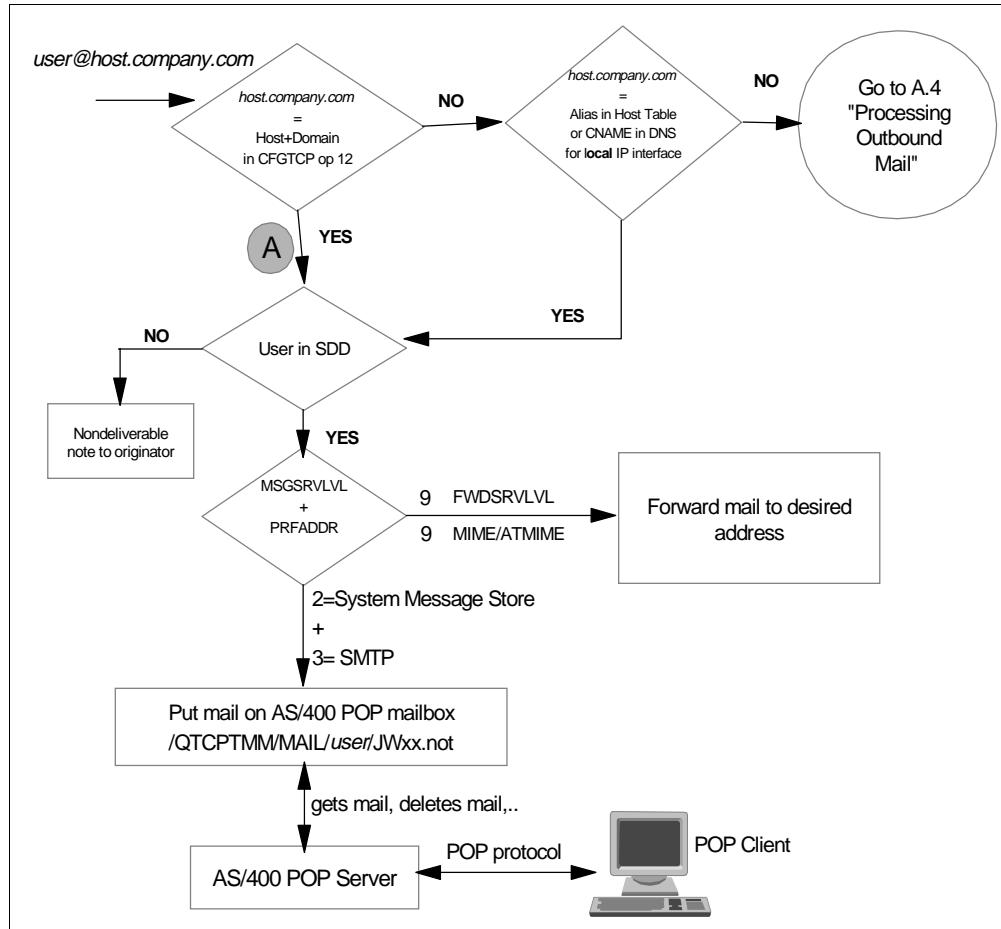


Figure 386. Processing Inbound Mail in an AS/400 SMTP Server

A.4 Processing Outbound Mail

The way an AS/400 SMTP server processes outbound mail varies slightly depending on the firewall configuration in the SMTP attributes.

Figure 387 shows the high level overview of how outbound mail is processed by an AS/400 SMTP server when no firewall is installed on the system.

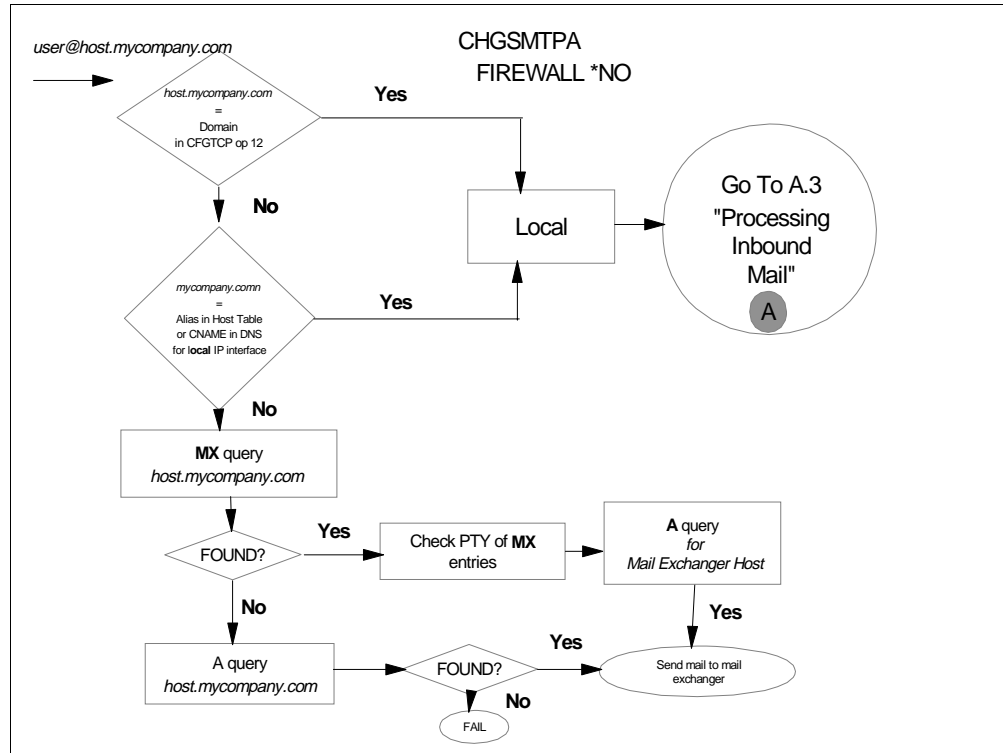


Figure 387. Processing Outbound Mail in an AS/400 SMTP Server - CHGSMTPA Firewall(*NO)

If you have a firewall installed in your AS/400 system, you must specify Firewall(*YES) in the Change SMTP Attributes (CHGSMTPA) command.

```
CHGSMTPA MAILROUTER(FIREWALL.MYCOMPANY.COM) FIREWALL(*YES)
```

Outbound mail is processed as shown in Figure 388.

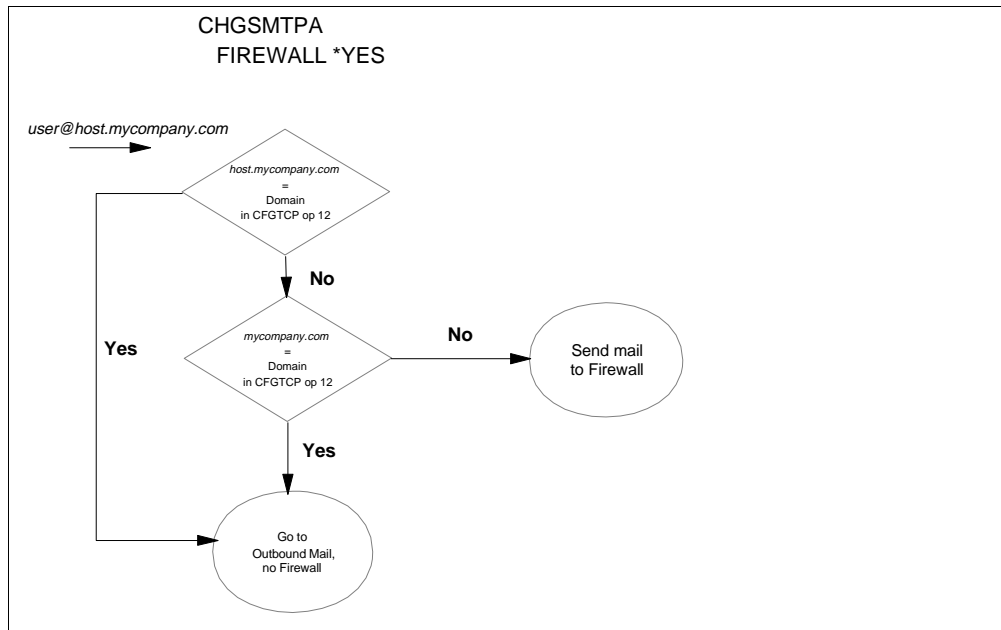


Figure 388. Processing Outbound Mail in an AS/400 SMTP Server - CHGSMTPA Firewall(*YES)

Appendix B. Special Notices

This publication is intended to help AS/400 system and network administrators to install, configure, tailor, and troubleshoot the DNS and DHCP support available in OS/400 V4R2. The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM Operating System/400. See the PUBLICATIONS section of the IBM Programming Announcement for OS/400 V4R2 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these

names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

IBM ®	AS/400
OS/400	Client Access
Client Access/400	IBM Firewall for AS/400
400	OS/2

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Appendix C. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

C.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How To Get ITSO Redbooks" on page 445.

- *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162 (available at a later date)
- *TCP/IP Tutorial and Technical Overview*, GG24-3376-04
- *The Basics of IP Network Design*, SG24-2580

C.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
Application Development Redbooks Collection	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection	SBOF-7250	SK2T-8042

C.3 Other Publications

These publications are also relevant as further information sources:

- *DNS and BIND* by Albitz & Liu
- *Internetworking with TCP/IP* by Douglas Comer
- *TCP/IP Addressing* by Buck Graham
- *TCP/IP Configuration and Reference*, SC41-5420-01
- *IBM Network Station Manager Installation and Use*, SC41-0664 (available at a later date)
- *System API Programming*, SC41-5800
- *IBM Firewall for AS/400*, SC41-5424-00

C.4 Web Resources

These Web sites are also relevant as further information sources:

- www.redbooks.ibm.com and select *Additional Redbook Materials*

- www.as400.ibm.com/firewall.
- Use a search engine to find the following RFCs:

Table 38. DNS RFC Information

RFC number	RFC Title
RFC920	Domain Requirements
RFC974	Mail Routing and Domain System
RFC1032	Domain Administrator's Guide
RFC1033	Domain Administrator's Operations Guide
RFC1034	Domain Names: Concepts and Facilities
RFC1035	Domain Names: Implementation and Specification
RFC1101	DNS Encoding of Network Names and Other Types
RFC1183	New DNS RR Definitions
RFC1535	Security Problems in DNS Software
RFC1537	Common DNS Data File Configuration File Errors
RFC1713	Tools for DNS Debugging
RFC1912	Common DNS Operational and Configuration Errors
RFC1982	Serial Number Arithmetic

Table 39. DHCP RFC Information

RFC number	RFC Title
RFC2131	Dynamic Host Configuration Protocol
RFC2132	DHCP Options and BOOTP Vendor Extensions
RFC951	Bootstrap Protocol
RFC1542	Clarifications and Extensions to the Bootstrap Protocol
RFC1027	Using ARP to Implement Transparent Subnet Gateways
RFC826	An Ethernet Address Resolution Protocol

How To Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at <http://www.redbooks.ibm.com>.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** – to order hardcopies in United States
- **GOPHER link to the Internet** – type `GOPHER WTSCPOK.ITSO.IBM.COM`
- **Tools disks**

To get LIST3820s of redbooks, type one of the following commands:

```
TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
```

To get lists of redbooks:

```
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
```

To register for information on workshops, residencies, and redbooks:

```
TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
```

For a list of product area specialists in the ITSO:

```
TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
```

- **Redbooks Web Site on the World Wide Web**

<http://w3.itso.ibm.com/redbooks>

- **IBM Direct Publications Catalog on the World Wide Web**

<http://www.elink.ibm.link.ibm.com/pbl/pbl>

IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** – send orders to: `USIB6FPL` at `IBMMAIL` or `DKIBMBSH` at `IBMMAIL`
- **Internet Listserver**

With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibm.link.ibm.com with the keyword `subscribe` in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (<http://www.redbooks.ibm.com/redpieces.html>). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** (Do not send credit card information over the Internet) – send orders to:

	IBMMAIL	Internet
In United States	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** – send orders to:

	IBM Publications	IBM Direct Services
IBM Publications	IBM Publications	Sortemosevej 21
Publications Customer Support	144-4th Avenue, S.W.	DK-3450 Allerød
P.O. Box 29570	Calgary, Alberta T2P 3N5	Denmark
Raleigh, NC 27626-0570	Canada	
USA		

- **Fax** – send orders to:

United States (toll free)	1-800-445-9269
Canada	1-800-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States) or (+1) 408 256 5422 (Outside USA)** – ask for:

Index # 4421 Abstracts of new redbooks
Index # 4422 IBM redbooks
Index # 4420 Redbooks for last six months

- **Direct Services** – send note to softwareshop@vnet.ibm.com

- **On the World Wide Web**

Redbooks Web Site	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibm.link.ibm.com/pbl/pbl

- **Internet Listserver**

With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibm.link.ibm.com with the keyword `subscribe` in the body of the note (leave the subject line blank).

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (<http://www.redbooks.ibm.com/redpieces.html>). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity
-------	--------------	----------

First name	Last name
------------	-----------

Company

Address

City	Postal code	Country
------	-------------	---------

Telephone number	Telefax number	VAT number
------------------	----------------	------------

☐ Invoice to customer number

☐ Credit card number

Credit card expiration date	Card issued to	Signature
-----------------------------	----------------	-----------

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

Symbols

"green screen" 31
*ALLOBJ special authority 31
.DB extension file 186
.db file 19

Numerics

0.0.127.in-addr.arpa reverse mapping file 44
69.5.10.in-addr.arpa secondary domain file 58

A

A record 41
absolute domain name 84
Add Directory Entry (ADDDIRE) command 45, 131
ADDDIRE command 45
adding
 additional subnet of 10.1.1.0 83
 new host 92
 subdomain 90
address file
 loopback 19
address pool 221
 changing the DHCP server configuration 378
 dividing across DHCP servers 263
 enlarging 272
 reducing 264
address record 41
Address Resolution Protocol (ARP) 353
address sorting 15
addressing scheme 317, 362
advantage of keeping centralized control 87
alias
 using 202
AS/400 communication trace
 reading and decoding 421
 starting 419
 stopping 420
AS/400 job log 188
ATTRIBUTES file 22, 33
authoritative 6
authoritative answer 114
authoritative name server 10, 11, 86, 184
authoritative server 109
authority
 maintaining 92
autostart 205
AUTOSTART attribute 23

B

backing up
 firewall DNS server 182
 parent server 115
 primary domain file 184
basic IP over twinax 343
bibliography 443

BOOT file 18, 19, 44, 79
Boot file 13
BOOTP
 migrating to a new DHCP configuration 401, 403
 migrating to an existing DHCP configuration 405
 overview 217
BOOTP/DHCP Relay Agent 219, 224, 313
 configuring 318, 336, 376, 388, 391
 configuring for Win NT 338
 starting 340, 376
browser proxy 143

C

cache file 13, 44, 87
cached authoritative response 202
caching-only name server 10
CC
 field 167
 list 167
 Problem 168
CCSID (coded character set ID) 31
CFGTCP command 51
Change DNS Attributes (CHGDNSA) command 23
Change SMTP Attributes (CHGSMTPA) command 50
Change System Directory Attributes (CHGSYSDIRA) command 157, 434
Change TCP Domain (CHGTCPDMN) command 431
changing
 domain name 30
checking
 mail queue 205
CHGDNSA command 23
CHGSMTPA command 50, 118
child DNS name server 89
child server 99
 configuring 106
CNAME record 14
coded character set ID (CCSID) 31
command
 Add Directory Entry (ADDDIRE) 131
 ADDDIRE 45
 CFGTCP 51
 Change System Directory Attributes (CHGSYSDIRA) 157, 434
 Change TCP Domain (CHGTCPDMN) 431
 CHGDNSA 23
 CHGSMTPA 50, 118
 Configure TCP/IP (CFGTCP) 110, 129, 204
 ENDTCPSVR SERVER(*DNS) 23
 SAVLICPGM 24
 Start Host Server (STRHOSTSVR) 23
 STRTCP 23
 STRTCPSVR 23
 STRTCPSVR SERVER(*DNS) 23
 Work with Directory Entry (WRKDIRE) 131
 Work with Spooled File (WRKSPLF) 18
 WRKLNK 34

- common mistake 207
- communication trace
 - reading and decoding 421
 - starting 419
 - stopping 420
- Complete the Firewall Installation page 133
- concept
 - zone of authority 85
- configuration wizard 36, 76
- Configure TCP/IP (CFGTCP) command 51, 110, 129, 204
- configuring
 - adding a subnet to a DHCP server configuration 302
 - backup DHCP server 332
 - BOOTP/DHCP Relay Agent 336, 388, 391
 - BOOTP/DHCP Relay Agent for Win NT 338
 - child server 106
 - DHCP clients 296
 - DHCP on IBM Network Station 251
 - DHCP on Win 95 clients 249
 - DHCP server 243, 326
 - DHCP server support 291
 - domain mail server 48
 - firewall 134
 - forwarder 140
 - forwarders 78
 - IBM Network Stations with DHCP 343, 359, 366, 369, 373
 - local BOOTP/DHCP Relay Agent 376
 - local DHCP configuration file 376
 - mail exchanger 164
 - mail server 44
 - POP3 client 28, 47
 - POP3 user 28, 45
 - primary name server 93
 - root name server 179
 - root server 107, 174
 - routes on DHCP servers 334
 - secondary DNS server 79
 - secondary name server 81, 95
 - TCP/IP interface 240, 280, 290
 - transparent subnetting 383
 - twinax 343, 359, 366, 373
 - twinax subnet address pool 380
- creating
 - A record 99
 - DNS primary name server 28
 - primary domain 179
 - primary name server 29
 - reverse mapping entry 41
 - secondary domain 183
 - secondary domain server 57
 - user-defined field 434
- Creating new zone 81

D

- data
 - DHCPACK 417
 - DHCPDISCOVER 413
 - DHCPOFFER 415

- DHCPREQUEST 417
- debug level 21, 23
- debug method 188
- debug problem 185
- debugging
 - mail 202
 - mail delivery problems 189
- default administrator's e-mail address 185
- default cache time 62
- default domain name 177
- default Internet root name server list 180
- default secondary server refresh interval 95
- default TTL (time to live) value 186
- defining
 - zone of authority 91
- delegate reverse mapping file 102
- delegating
 - authority 85, 88
 - subdomain 101
 - the workload 89
- delegation 5
- deleting
 - reverse mapping entry 41
- deleting primary name server configuration 80
- deliver mail 116, 431
- DHCP
 - acquiring configuration information 220
 - BOOTP/DHCP Relay Agent 219, 224, 313
 - clients connected to multiple LANs 277, 313, 316
 - concepts 217
 - configuring a BOOTP/DHCP Relay Agent 336
 - configuring a BOOTP/DHCP Relay Agent for Win NT 338
 - configuring clients 296
 - configuring IBM Network Stations 343, 359, 366, 373
 - configuring local configuration file 376
 - configuring on IBM Network Station 251
 - configuring on Win 95 clients 249
 - configuring the BOOTP Relay Agent 376, 388, 391
 - configuring twinax subnet address pool 380
 - full client support 271
 - host clients 218
 - implementing changes 224
 - log 297, 413, 415, 417
 - logging utility 407, 408
 - migrating BOOTP to a new DHCP configuration 401, 403
 - migrating BOOTP to an existing DHCP configuration 405
 - multiple servers 261
 - network components 218
 - overview 217, 218
 - problem determination 407
 - Program Temporary Fixes (PTFs) 407
 - renewing leases 223
 - server 219
 - simple network scenario 237
 - starting a BOOTP/DHCP Relay Agent 340
 - starting server support 295
 - starting servers 270, 274

- symptoms, problems, and resolutions 423
- two-server scenario 261
- DHCP server 313
 - adding a subnet to an existing configuration 302
 - adding IP addresses to backup 266, 273
 - changing configuration of an address pool 378
 - changing the lease time 269
 - changing the number of options 266
 - configuring 318, 326
 - configuring a backup server 332
 - configuring information 241
 - configuring routing information 334
 - configuring support 291
 - configuring through Operations Navigator 243
 - dividing an address pool 263
 - enlarging the address pool 272
 - minimizing failures 261
 - multiple servers 261
 - multiple subnets 277
 - reducing the primary address pool 264
 - remote 373
 - starting 270, 274, 340
 - starting support 295
- DHCPACK data 417
- DHCPDISCOVER data 413
- DHCPOFFER data 415
- DHCPREQUEST data 417
- diagnostic tools 185
- disadvantage of keeping centralized control 88
- distributed database 3
- DNS administrator 177
- DNS configuration 90, 117
 - file 18
 - graphical interface 40
 - verifying 161
 - Windows 95 client 142
- DNS Configuration Wizard 23
- DNS configuration wizard 44, 106, 177
- DNS directory 33
- DNS filter 137
- DNS job log 53
- DNS name space 4
- DNS server
 - backup 24
 - cache 185
 - configuration 22
 - configuration wizard 36
 - firewall 181
 - implementing primary 25
 - implementing secondary 25
 - job 18
 - recovery 24
 - starting 52
 - statistics information 187
 - user interface 22
- DNS support
 - installing 17
- DNS0417 message 32
- domain 5
- domain file

- primary 12
- secondary 12
- domain mapping file 18
- domain name system 3, 5
 - concepts 3
- dump file 194
- DUMPDB file 20, 201
- dumping
 - server statistics 194

E

- e option 32
- ENDTCPSVR SERVER(*DNS) command 23
- error message DNS00E9 209
- example
 - statistics dump 194
- expire interval 61
- expire timer 187
- external name server 128

F

- file
 - cache 13
 - local 13
- firewall 11
 - configuration 134
 - DNS 125, 173
 - DNS server 181
 - installation 133
 - mail relay 137
 - name server 125, 128
 - network server description 138, 205
 - parameter 50, 118
 - problem determination 206
- forward mapping 41
- forward mapping file 12, 18
- forward mapping secondary domain file 57
- forward resolution file 161
- forwarder 11
 - configuring 140
- forwarders configuration 73
 - verifying 162
- forwarding function 153, 433
- full domain name 3
- full-DHCP client support 271

G

- grow the network 83

H

- hardware problem 210
- hierarchical partitioning 238, 271
- history log 210
- host client
 - multihomed 278
- host clients
 - DHCP 218
- host domain name

- updating 110
- host name 29
- host name search priority 66

I

- IBM Network Station
 - configuring 369
 - configuring DHCP 251
 - configuring with DHCP 343, 359, 366, 373, 376
 - powering on 376
 - starting 351, 369, 387, 391
 - startup sequence 371
 - stopping 387, 391
 - testing connectivity 373
 - using transparent subnetting 383
- IBM Network Stations
 - NVRAM 370
- IFS directory 180
- IFS directory file 120
- implementing
 - DNS server 25
 - mail forwarding 156
 - mail forwarding function 434
- Import Domain Data 40, 71
- importing domain data 76
- inbound SMTP/MIME mail
 - processing 437
- Incoming Mail Server 203
- increase debug level 197
- individual resource record 187
- installing
 - DNS support 17
 - firewall 133
- Integrated PC Server 144
 - LAN connections 144
- interface
 - configuring 240, 280, 290
- internal DNS 125
 - server configuration 148
- internal domain name server 125
- Internal name server
- name server
 - internal 128
- internal root 11, 96
- Internet
 - domain name space 176
 - root name server 176
 - root server 4
 - service provider (ISP) DNS server 173
- InterNIC registration 177
- IP address 4, 29, 184
 - adding to backup DHCP server 273
 - adding to backup DHCP servers 266
- IP interface
 - verifying 203
- ISP DNS IP address 136
- ISP DNS server 128
- iterative query 8

K

- keeping centralized control
 - advantage 87
 - disadvantage 88

L

- LAN adapter 129
- lease
 - changing lease time on DHCP servers 269
 - renewing 223
- Load Defaults box 180
- local file 13
- local host
 - alias 169
 - table 51
- localhost 38
- localhost host 178, 186
- log
 - DHCP 297, 407, 408
 - DHCPACK data 417
 - DHCPDISCOVER data 413
 - DHCPOFFER data 415
 - DHCPREQUEST data 417
- Loopback address file 19

M

- MAC address 217, 399
- mail 117
 - configuration 117
 - debugging 202
 - delivery 431
 - hub 435
 - implementation 431
 - router parameter 50
 - routing 4
 - server framework job 52
 - service level 46
- mail exchanger
 - configuring 164
- mail forwarding
 - implementing 156
- mail forwarding function 156
 - implementing 434
- mail queue
 - checking 205
- mail relay
 - firewall 137
- mail server 117
- Mail Service Level parameter 203
- maintaining
 - authority 92
- manually configure forwarders 78
- mapping file
 - domain 18
 - forward 12, 18
 - reverse 13, 19
- master name server 9
- master server 86
- message DNS0417 32

- migrate host name table entry 24
- migrating
 - AS1 host table 28
 - DNS formatted file 28
- migrating BOOTP to DHCP 399
 - to a new DHCP configuration 401, 403
 - to an existing DHCP configuration 405
- migrating from DNS server 71
- multihomed host 278
- MX query 50, 55, 166
- MX record 14, 32, 49
- MX record query 55
- mycompany.com.db forward mapping file 79

N

- name resolution 7
- name server 5, 7
 - authoritative 10
 - caching-only 10
 - external 128
 - firewall 128
 - forwarder 11
 - lookup (nslookup) program 23
 - master 9
 - parent and child 10
 - primary 9
 - root 10
 - secondary 9
 - statistics 194
- Netscape browser mail preference 143
- network addressing 238, 271
- network configuration 27
- network server description
 - firewall 138
- new host
 - adding 92
- non-authoritative answer 114
- non-zero global number 196
- NS record 14, 100, 115
- NS resource record 58
- NSLOOKUP 53
- nslookup 111, 203
 - interactive tool 188
 - program 23, 190
 - query 192
- NVRAM 370

O

- Operations Navigator
 - configuring DHCP server 243
 - DNS configuration 28, 177, 186
 - DNS configuration import domain function 36
- options
 - changing on DHCP servers 266
- outbound mail
 - processing 438

P

- parameter
 - firewall 50
 - mail router 50
 - Mail Service Level 203
 - Preferred address 203
 - search first 202
- parent and child name server 10
- parent server 96
- partitioning 238, 271
- PID file 22
- ping 188, 203
- planning
 - secondary name server 177
 - zone of authority 176
- planning phase 29
- POP mailbox 206
- POP3 directory entry 45, 117, 202
 - postmaster 185
- POP3 server 143
- POP3 system directory entry 185
- POP3 user
 - configuring 45
- postmaster
 - POP3 directory entry 185
- preferred address 46
- Preferred address parameter 203
- preventing problems 185
- primary DNS server 71
- primary domain
 - creating 179
- primary domain file 12, 86
- primary name server 8, 9, 86
 - configuring 93
- primary name server configuration
 - deleting 80
- probable error causes 207
- problem determination
 - communication trace 419
 - DHCP 407
 - DHCP symptoms, problems, and resolutions 423
 - Program Temporary Fixes (PTFs) for DHCP 407
- problem symptom 207
- processing
 - inbound SMTP/MIME mail 437
 - outbound mail 438
- Program Temporary Fixes (PTFs) 407
- Proxy ARP 343, 345, 353, 355
- proxy server 137
- PTR record 14

Q

- QMSF job 205
- QSYSWRK subsystem 18, 118, 189, 204
- QTCP user profile 190
- QTOBDNS job 189, 203
- QTOBDNS job log 53, 60, 61, 188, 190, 210
- QTOBDNS server job 18
- QTOBH2N migration program 31

- QTOBH2N program 32, 36
- QTOBXFER job 59, 190
- QTOBXFER job log 210
- QTOBXFER secondary server zone transfer job 18
- QTOBXMI transfer job 18
- QTOBXMIT job 190
- query
 - DNS server 66
 - iterative 8
 - recursive 8
 - reverse look up 42
 - type 114
- QUERYLOG file 19, 166, 188, 199
- QUERYLOG file example 200

R

- reconfigure client 66
- record
 - CNAME 14
 - file 14
 - MX 14
 - NS 14
 - SOA 14
- recursive query 8
- refresh timer 187
- regular backup plan 24
- Relay Agent 219, 224, 313
 - configuring 318, 336, 376, 388, 391
 - configuring for Win NT 338
 - starting 340, 376
- remote DHCP server 373
 - twinax subnet address pool 380
- remote.com domain 30
- resolver 7
- retry interval 61
- retry timer 187
- reverse look up query 42
- reverse mapping
 - file 13, 19
 - primary domain file 95
- reverse mapping entry
 - creating 41
 - deleting 41
- Review Configuration page 135
- RFC 1537 186
- RFC 1912 186
- root name server 10
 - configuring 179
- root server 37
 - configuring 107, 174
 - internal 96
- ROOT.FILE list 180
- round robin 15
- round robin function 187
- route
 - configuring on a DHCP server 334
- RUNDBG file 21
- RUNDEBUG file 22, 198

S

- SAVLICPGM command 24
- scenarios
 - DHCP clients connected to multiple LANs 277, 313, 316
 - network with two DHCP servers 261
 - simple DHCP network 237
- scope planning 238, 271
- search first parameter 202
- secondary DNS server 162
 - configuring 79
- secondary domain 58
 - back-up file 12
 - creating 183
 - file 86
- secondary domain server
 - creating 57
- secondary name server 9, 86
 - configuring 81, 95
 - planning 177
- secondary server
 - expire interval 61
 - retry interval 61
- secure mail server 156, 433
- secure zone record 65
- security
 - consideration 63
 - zone transfer 63
- server
 - configuration 17, 71
 - DHCP 219
 - firewall DNS 125
 - implementation 17
- server statistics 20
 - dumping 194
- service file 19
- SET TYPE=MX command 191
- SET TYPE=PTR command 192
- SMTP domain name 45, 117, 171
- SMTP mail server 143
- SMTP Outgoing Mail Server 203
- SMTP server 119, 171
- SMTP system alias table 202
- SMTP system alias table entry 185
- SOA cache time 62
- SOA record 14, 61, 115, 185, 186, 187
- SOA resource record 61
- SOCKS configuration 143
- software prerequisite 17
- split DNS 12
- Start Host Server (STRHOSTSVR) command 23
- starting
 - DNS Server 52
 - secondary name server 59
 - the IBM Network Station 351
- statistics dump example 194
- STATISTICS log file 20
- STATS information 188
- STRHOSTSVR command 23
- STRMSF command 205

- STRTCP command 23
- STRTCPSPVR command 23
- STRTCPSPVR SERVER(*DNS) command 23
- STRTCPSPVR SERVER(*DNS) RESTART(*DNS) command 186
- subdomain 3, 5
 - adding 90
 - delegating 101
- subnet
 - adding a subnet to a DHCP server configuration 302
 - multiple subnets 313
 - multiple subnets and DHCP servers 277
- subnetting
 - transparent 383
- system concepts
 - domain name 3
- system distribution directory entry 156, 169

T

- TCP/IP configuration 128, 145, 170
 - host table entries 146
 - interface 145
- TCP/IP configuration value 155
- terminology 128
- TMP directory 33
- traces 185
- transparent subnetting 343, 345, 352, 383
 - twinax 356
- troubleshooting DNS problems 185, 188
- twinax configuration 343, 359, 366, 373
 - basic IP 343
 - local DHCP configuration file 376
 - remote DHCP server 380
 - transparent subnetting 356, 383

U

- UDP packet 138
- unique domain name 4
- unrelated domain 173
- update server smart icon 185
- updating
 - host domain name 110
- user@public_domain 168
- user-defined field
 - creating 434
- using
 - alias 202

V

- verify TCP/IP domain information 118
- verifying
 - DNS configuration 161
 - forwarders configuration 162
 - IP interface 203
 - mail-related configuration option 130
 - SMTP configuration 50
 - TCP/IP configuration 50
 - TCP/IP interface 129

W

- wildcard MX entry 117
- wildcard MX record 48, 55
- Windows 95 clients
 - configuring DHCP 249
- Windows NT
 - configuring a BOOTP/DHCP Relay Agent 338
- wizard
 - configuration 36
 - window 37
- Work with Directory Entry (WRKDIRE) command 131
- Work with Spooled File (WRKSPLF) command 18
- WRKACTJOB SBS(QSYSWRK) command 205
- WRKCFGSTS *NWS command 205
- WRKLNK command 34
- WRKSPLF command 18
- WRKSPLF QMSF command 205

X

- XFRNETS directive 64

Z

- zone of authority 5, 96, 116
 - concept 85
 - defining 91
 - planning 176
- zone transfer 9, 59, 81, 86
 - frequency 60
 - security 63

ITSO Redbook Evaluation

AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support
SG24-5147-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at <http://www.redbooks.com>
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@vnet.ibm.com

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

What other redbooks would you like to see published?

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)



Printed in U.S.A.