



[www.chinatag.com](http://www.chinatag.com)

**CHINATAG**

**70-216SG**

Implementing and Administering a Microsoft  
Windows 2000 Network Infrastructure

**Study Guide**

**DEMO Version**

Copyright (c) 2003 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are not encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

# TABLE OF CONTENTS

## List of Tables

## Introduction

### 1. The Windows 2000 Network

- 1.1 Network Protocols
  - 1.1.1 Transmission Control Protocol/Internet Protocol (TCP/IP)
  - 1.1.2 NetBIOS Enhanced User Interface (NetBEUI)
  - 1.1.3 AppleTalk
  - 1.1.4 NWLink
  - 1.1.5 Data Link Control (DLC)
  - 1.1.6 Remote Connections and Protocols
- 1.2 The TCP/IP Protocol Architecture
  - 1.2.1 The Application Layer
  - 1.2.2 The Transport Layer
    - 1.2.2.1 Transmission Control Protocol (TCP)
    - 1.2.2.2 User Datagram Protocol (UDP)
  - 1.2.3 The Internet Layer
  - 1.2.4 The Network Interface Layer
- 1.3 IP Addressing
  - 1.3.1 IP Address Formats
    - 1.3.1.1 Binary Format
    - 1.3.1.2 Dotted Decimal Format
- 1.4 IP Address Classes
- 1.5 IP Routing
  - 1.5.1 Static IP Routing
  - 1.5.2 Dynamic IP Routing
  - 1.5.3 Routing Protocols
- 1.6. Testing IP Configurations
  - 1.6.1 The IPConfig Utility
  - 1.6.2 The Ping Utility
  - 1.6.3 The Tracert Utility
  - 1.6.4 The Net and Nbtstat Utilities
- 1.7 IP Security (IPSec)
  - 1.7.1 Configuring IPSec

### 2. IP Addressing

- 2.1 Automatic IP Addressing
  - 2.1.1 Dynamic Host Configuration Protocol (DHCP) Addressing
    - 2.1.1.1 The DHCP Lease Process
    - 2.1.1.2 Automatic Lease Renewal
    - 2.1.1.3 Manual Lease Renewal
  - 2.1.2 Automatic Private IP Addressing
- 2.2 Installing and Configuring DHCP
  - 2.2.1 Authorizing DHCP
  - 2.2.2 DHCP Scopes
    - 2.2.2.1 IP Scope Exclusion Range
    - 2.2.2.2 IP Reservations
    - 2.2.2.3 DHCP Scope Configuration Options
  - 2.2.3 Implementing Multiple DHCP Servers
- 2.3 DHCP Relay Agents
- 2.4 Troubleshooting DHCP
  - 2.4.1 Troubleshooting DHCP Clients
  - 2.4.2 Troubleshooting DHCP Servers
- 2.5 Static IP Addressing

### **3. Novell NetWare Interoperability**

- 3.1 NWLink and Windows 2000
- 3.2 NWLink Architecture
  - 3.2.1 IPX
  - 3.2.2 SPX
  - 3.2.3 SPXII
  - 3.2.4 Router Information Protocol (RIP)
  - 3.2.5 Service Advertising Protocol (SAP)
  - 3.2.6 NetBIOS over IPX
  - 3.2.7 Forwarder
- 3.3 Gateway Service for NetWare
- 3.4 Client Services for NetWare
- 3.5 Configuring NWLink
  - 3.5.1 Internal Network Number
  - 3.5.2 Frame Type and External Network Number

### **4. Name Resolution**

- 4.1 Domain Name Services (DNS) Name Resolution
  - 4.1.1 DNS Zones

- 4.1.2 Zone Lookup Types
- 4.1.3 Zone Files
- 4.1.4 Zone Transfers
- 4.1.5 Zone Transfer Security
- 4.1.6 Active Directory Integrated Zones

#### 4.2 Dynamic DNS Updates

- 4.2.1 Secure Dynamic Updates
- 4.2.2 SRV and A Resource Records
- 4.2.3 Creating Resource Records
- 4.2.4 Resolving DNS problems with nslookup
- 4.2.5 DNS Name Server Roles
- 4.2.6 DNS Files
  - 4.2.6.1 Resolver Queries
  - 4.2.6.2 Caching and Time to Live
  - 4.2.6.3 DNS Configuration Files
  - 4.2.6.4 DNS File Types

#### 4.3 NetBIOS Name Resolution

- 4.3.1 The LMHOSTS File
- 4.3.2 WINS
  - 4.3.2.1 WINS Name Registration
  - 4.3.2.2 WINS Name Renewal
  - 4.3.2.3 WINS Name Release
  - 4.3.2.4 WINS Name Query and Name Resolution
- 4.3.3 Installing WINS
- 4.3.4 WINS Replication

#### 4.4 Network Address Translation (NAT)

- 4.4.1 Static and Dynamic Address Mapping
- 4.4.2 Translation of Header Fields
- 4.4.3 NAT Editors
- 4.4.4 NAT and Routing and Remote Access
  - 4.4.4.1 Outbound Internet Traffic
  - 4.4.4.2 Inbound Internet Traffic
  - 4.4.4.3 Additional NAT Routing Protocol Components
- 4.4.5 NAT and Virtual Private Networks

#### 4.5 Internet Connection Sharing

### **5. Routing and Remote Access Service (RRAS)**

#### 5.1 Combining Routing and Remote Access

#### 5.2 Installation and Configuration

- 5.2.1 Allowing Inbound Connections
- 5.2.2 Remote Access Policy (RAP)
- 5.2.3 Remote Access Profiles

5.2.4 Bandwidth Allocation Protocol (BAP)

5.2.5 Remote Access Client

5.2.6 Remote Access Protocols

5.3 Remote Access Security

5.4 Managing Authentication

5.5 Virtual Private Networks (VNP)

5.5.1 VPN Protocols

5.5.2 VNP Tunnelling

5.5.3 Integrating VPN in a Routed Network

5.5.4 Integrating VPN Servers with the Internet

5.6 DHCP and Routing and Remote Access

5.6.1 DHCP Relay Agent

5.7 RRAS Tools

## **6. The Windows 2000 Public Key Infrastructure (PKI)**

6.1 Certificate Services

6.1.1 Types of CAs

6.1.1.1 Enterprise root CA

6.1.1.2 Enterprise Subordinate CA

6.1.1.3 Stand-alone Root CA

6.1.1.4 Stand-alone Subordinate CA

6.1.2 CA Security and Recovery

6.2 Certificate Enrollment

6.3 Certificate Renewal

6.4 Certificate Trust

6.4.1 Trusted CA Roots

6.4.2 Cryptographic Key Storage

6.5 Certificate Management

6.5.1 Certificate Revocation

6.5.2 Issuing Certificates

6.6 Certificate and Key Recovery

6.6.1 Data Recovery Policy

## **7. Monitoring Network Resources**

7.1 Monitoring Access to Shared Folders

7.1.1 Monitoring Shared Folders

- 7.1.2 Modifying Shared Folder Properties
- 7.1.3 Monitoring Open Files
- 7.1.4 Disconnecting Users from Open Files
- 7.1.5 Monitoring Network Users
- 7.1.6 Monitoring User Sessions
- 7.1.7 Disconnecting Users

## 7.2 Auditing

- 7.2.1 Using an Audit Policy
- 7.2.2 Using Event Viewer to View Security Logs
- 7.2.3 Setting Up Auditing
  - 7.2.3.1 Setting an Audit Policy
  - 7.2.3.2 Auditing Access to Files and Folders
  - 7.2.3.3 Auditing Access to Printers

## 7.3 Using Event Viewer

- 7.3.1 Viewing Security Logs
- 7.3.2 Locating Events
- 7.3.3 Managing Audit Logs

## 8. Practice Labs

### 8.1 Installing Active Directory

### 8.2 Installing and Configuring DNS

- 8.2.1 Installing DNS
- 8.2.2 Configuring DNS

### 8.3 Setting up the Internet Connection and Configuring ICS

- 8.3.1 Setting up the Internet Connection
- 8.3.2 Configuring ICS

## LIST OF TABLES

TABLE 1.1: *IP Route commands*

TABLE 1.2: *IPConfig Switches*

TABLE 1.3: *Ping Errors*

TABLE 1.4: *nbstat Commands*

TABLE 2.1: *DHCP Scope Configuration Options*

TABLE 3.1: *The NWLink Protocols*

TABLE 3.2: *NWLink Frame Types*

TABLE 4.1: *DNS Zone Types*

TABLE 4.2: *DNS Resource Record Types*

TABLE 4.3: *DHCP Lease Configuration Options*

TABLE 5.1: *Netsh command-line options*

TABLE 5.2: *Netsh global commands*

TABLE 6.1: *Standard PKI Certificate Stores*

TABLE 7.1: *Options for Filtering and Finding Events*

# Implementing and Administering a Microsoft Windows 2000 Network Infrastructure

**Exam Code: 070-216**

## **Certifications:**

<b>Microsoft Certified (MCP)</b>	
<b>Microsoft Certified Systems Engineer (MCSE)</b>	<b>Core</b>
<b>Microsoft Certified Systems Administrator (MCSA)</b>	<b>Elective</b>
<b>Microsoft Certified Database Administrator (MCDBA)</b>	<b>Elective</b>

## **Prerequisites:**

### **About This Study Guide**

This Study Guide provides all the information required to pass the Microsoft 070-216 exam – Implementing and Administering a Windows 2000 Network Infrastructure. It however, does not represent a complete reference work but is organized around the specific skills that are tested in the exam. Thus, the information contained in this Study Guide is specific to the 070-216 exam and not only to Implementing and Administering a Windows 2000 Network Infrastructure. It includes the information required to answer questions related to Windows 2000, UNIX and Novell Netware clients that may be asked during the exam. Topics covered in this Study Guide includes installing, managing, monitoring, configuring, and troubleshooting DNS, DHCP, Remote Access, Network Protocols, IP Routing, and WINS in a Windows 2000 network infrastructure, as well as managing, monitoring, and troubleshooting Network Address Translation and Certificate Services; IP addressing; and interoperability with Novell Netware and UNIX.

### **Intended Audience**

This Study Guide is targeted specifically at people who wish to take the Microsoft MCSE exam 070-216 – Implementing and Administering a Windows 2000 Network Infrastructure. This information in this Study Guide is specific to the exam. It is not a complete reference work. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt with in this Study Guide are complex and require an understanding of material provided for the MCSA / MCSE exams: 070-210 – Installing, Configuring, and Administering Microsoft Windows 2000 and 070-215 – Installing, Configuring, and Administering Microsoft Windows 2000.

**Note:** There is a fair amount of overlap between 070-216 and 070-215 and 070-218. Don't skim over the information that seems familiar. Read over it again to refresh your memory.

### **How To Use This Study Guide**

To benefit from this Study Guide we recommend that you:

- For best results, use this Study Guide in conjunction with the TestKing Study Guides for exam 070-210 and 070-215. These will provide you with valuable background information.
- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work.
- Perform all labs that are included in this Study Guide to gain practical experience, referring back to the text so that you understand the information better. Remember, it is easier to understand how tasks are performed by practicing those tasks rather than trying to memorize each step.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

**Note:** Remember to pay special attention to these note boxes as they contain important additional information that is specific to the exam.

Good luck!

## 1. The Windows 2000 Network

Windows 2000 supports both Workgroup Networks and Domain-Based Networks. **Workgroup Networks** are also referred to as Peer-to-Peer networks and are the simplest type of network. They are ideal for networks of less than ten computers and supports file and print sharing. **Domain-Based Networks** are common to large companies and benefit from centralized administration. This results in the implementation of stronger security models with users requiring a user account to logon access network resources.

In Windows 2000 you can create number of network connections. These include **Local Area Network (LAN)** connections, remote connections, Virtual Private Network (VPN) connections and direct connections. All these connections are created in the **NETWORK AND DIAL-UP CONNECTIONS** folder. A LAN is also referred to as an intranet and has client support, such as Client for Microsoft Networks and Client Services for NetWare; services, such as Files and Printer Sharing; and uses network protocols.

### 1.1 Network Protocols

A network **protocol** is a set of rules and conventions for computers use to communicate over a network. Although TCP/IP is the core protocol used in Windows 2000 and is the default networking protocol that is installed by default during the installation of Windows 2000, Windows 2000 support many networking protocols. You can optimize network performance on computers that run multiple protocols by specify the **protocol binding** order of the protocols, i.e., by placing the protocol that is used the most at the top of the protocol bindings list. The computer will then attempt to use this protocol first when a user attempts to make a connection to a server.

#### 1.1.1 Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP is the **default** networking protocol used in Windows 2000, and is installed **automatically** during the installation of both Windows 2000 Server and Windows 2000 Professional. It is a **routable** protocol and can be used to communicate with **dissimilar systems**. On TCP/IP networks you can use user friendly names to locate computers and resources. Windows 2000 networks allows for a number of mechanism to facilitate this location of computers and resources by user friendly names instead of IP addresses. These include:

- **Dynamic Host Configuration Protocol (DHCP)** which simplifies the administration and management of IP addresses on a TCP/IP network by **automating address configuration** for network clients.
- **Domain Name System (DNS)** which is a standard **name resolution system** in Windows 2000 and is used to locate IP-based computers by translating user friendly domain names to IP addresses and vice versa.
- **Windows Internet Name Service (WINS)** which is the name resolution system used for **Windows NT 4.0** and earlier operating systems.

#### 1.1.2 NetBIOS Enhanced User Interface (NetBEUI)

**NetBEUI** was developed as a protocol to support small LANs of 20 to 200 computers and is not a routable protocol because it does not have a network layer. NetBEUI is included with Windows 2000 Server and Windows 2000 Professional, primarily as a legacy protocol to support workstations that have not been upgraded to Windows 2000.

### 1.1.3 AppleTalk

AppleTalk is a protocol suite developed by Apple Computer, Inc. for communication between Apple Macintosh computers. Windows 2000 includes support for AppleTalk, which allows Windows 2000 to function as a router for AppleTalk-based Macintosh networks and as a dial-up server for Apple Macintosh clients. Support is provided for file sharing and printer sharing.

**Note:** The AppleTalk protocol requires a Windows 2000 Server that is configured with Windows 2000 Services to function properly.

### 1.1.4 NWLink

NWLink is a Microsoft-compatible IPX/SPX protocol for Windows 2000. It is used to communicate with Novell NetWare client/server computers that use the WinSock or NetBIOS over IPX/SPX protocols. NWLink can be installed on a Windows 2000 Server or Windows 2000 Professional computer that is used to access a Novell NetWare server. However, NWLink alone does not allow a Windows 2000 computer to access files or printers shared on a NetWare server, or to act as a file or print server to a NetWare client. To access files or printers on a NetWare server, Client Service for NetWare on Windows 2000 Professional, or Gateway Service for NetWare on Microsoft Windows 2000 Server must be used. NWLink is included with both Windows 2000 Server and Windows 2000 Professional, and is installed automatically during the installation of Client Service for NetWare or Gateway Service for NetWare. NWLink is also Network Driver Interface Specification (NDIS)-compliant, therefore the Windows 2000 computers can simultaneously run other protocol stacks, such as TCP/IP.

### 1.1.5 Data Link Control (DLC)

Data Link Control (DLC) was developed for IBM mainframe communications. The protocol was not designed to be a primary protocol for network use between personal computers. DLC is also used to print to Hewlett-Packard printers that are directly connected to networks. Network-attached printers use the DLC protocol because the received frames are easy to disassemble and DLC functionality can easily be coded into read-only memory (ROM). Clients that send print jobs to Hewlett-Packard network printers do not need the DLC protocol installed on their computers. Only the print server communicating directly with the printer needs the DLC protocol to be installed on it.

### 1.1.6 Remote Connections and Protocols

In addition Windows 2000 supports a number of protocols designed specifically for remote connections. In Windows 2000 there are two types of remote connections:

- **Routing and Remote Access Services (RRAS)** which allow for mobile users to dial into their corporate LAN; and
- **Virtual Private Networks (VNP)** which use a tunneling protocol to secure a private network that is established across a public network, such as the Internet.

Windows 2000 supports two tunneling protocols that can be used to create a VNP connection. These are:

- **Point-to-Point Tunneling Protocol (PPTP)**, which is a TCP/IP protocol that can encapsulate TCP/IP, IPX/SPX, or NetBEUI protocols. PPTP tunnels must be authenticated by using the same authentication mechanisms as PPP connections; and

- **L2TP**, which is a combination of PPTP and Layer 2 Forwarding. L2TP does not provide data encryption but relies on **Internet Protocol Security (IPSec)**. IPSec is a group of services and protocol that supports the secured transfer of information across a TCP/IP network. It is used to encrypt TCP/IP network traffic and enables secure data transfer between remote clients and private enterprise servers through a VPN connection.

## 1.2 The TCP/IP Protocol Architecture

TCP/IP protocols provide networking support to connect dissimilar hosts and sites, and follow a set of standards for computer communication and network interconnection. TCP/IP protocols follow a four-layer conceptual model known as the Department of Defence (DOD) model. These layers are: Application, Transport, Internet, and Network Interface. This four-layer conceptual model is illustrated in Figure 1.1.

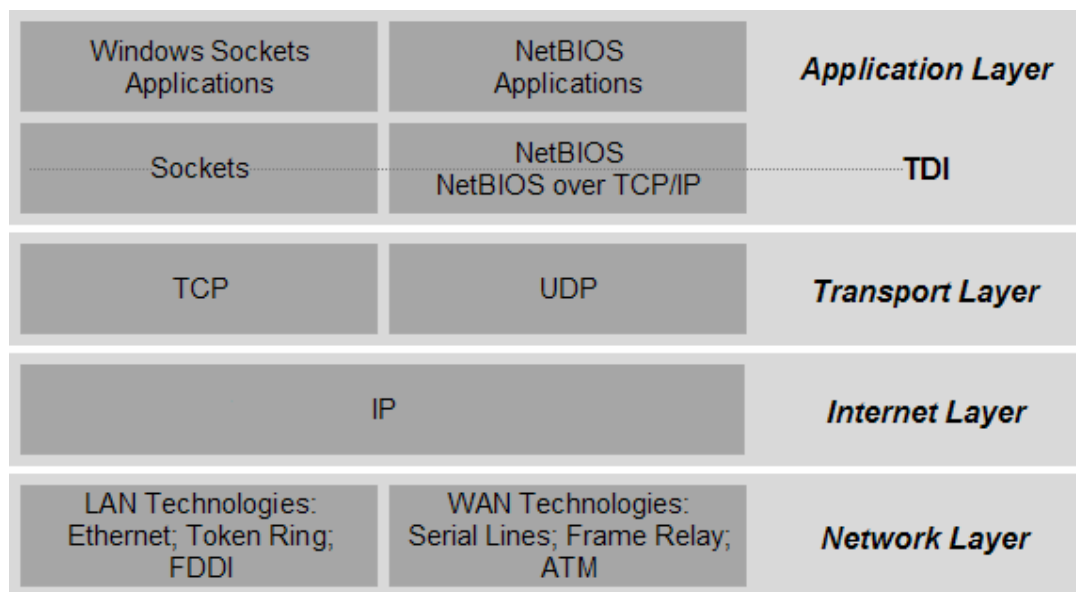


FIGURE 1.1: The TCP/IP Four-Layer Conceptual Model

### 1.2.1 The Application Layer

The Application layer is at the top of the four-layer conceptual TCP/IP model, and is used by software programs to gain access to the network. This layer corresponds roughly to the Session, Presentation, and Application Layers of the OSI model. Some TCP/IP utilities and services run at the Application Layer. These include:

- **HyperText Transfer Protocol (HTTP)** which is the protocol used for Internet communications.
- **File Transfer Protocol (FTP)** which is an Internet service that transfers files from one computer to another.
- **Simple Mail Transfer Protocol (SMTP)** which is a protocol that mail servers use to transfer e-mail.
- **Telnet** which is a terminal emulation protocol that can be used to log on to remote network hosts.
- **Domain Name System (DNS)** which is a set of protocols and services on a TCP/IP network that allows network users to use hierarchical user-friendly names instead of IP addresses when locating hosts.

- **Simple Network Management Protocol (SNMP)** which allows you to manage network nodes such as servers, workstations, routers, bridges, and hubs from a central host. SNMP can also be used to configure remote devices, monitor network performance, detect network faults or inappropriate access, and audit network usage.

Windows 2000 TCP/IP provides two interfaces for network applications to use the services of the TCP/IP protocol stack:

- **WinSock** which is the Windows 2000 implementation of the Sockets application programming interface (API). The Sockets API is the standard mechanism for accessing datagram and session services over TCP/IP.
- **NetBIOS** which is a standard API used as an inter-process communication mechanism in the Windows environment. It is included in Windows 2000 to support legacy applications that require support for the NetBIOS naming and messaging services, such as TCP/IP and NetBEUI.

### 1.2.2 The Transport Layer

The Transport Layer in the DOD model corresponds roughly to the Transport Layer in the OSI model and provides communication sessions between computers and define the type of transport service as either connection-oriented which uses Transmission Control Protocol (TCP) or connectionless datagram-oriented which uses (UDP).

#### 1.2.2.1 Transmission Control Protocol (TCP)

TCP is a reliable, connection-oriented delivery service. It achieves reliability by assigning a sequence number to each segment transmitted indicating to the host how many pieces of data have been transmitted. An acknowledgment verifies that the other host received the data. For each segment sent, the receiving host must return an acknowledgment (ACK) within a specified period. If the sender does not receive an ACK, then the data is retransmitted. If the segment is received damaged, the receiving host discards it. Because in this case an ACK is not sent, the sender retransmits the segment. Therefore TCP provides connection-oriented, reliable communications for applications that typically transfer large amounts of data at one time and for applications that require an acknowledgment for data received. Furthermore, TCP data is transmitted in segments, and a session must be established before hosts can exchange data. TCP uses byte-stream communications, which means that the data is treated as a sequence of bytes.

#### 1.2.2.2 User Datagram Protocol (UDP)

UDP offers a connectionless datagram service that does not guarantee delivery or the correct sequencing of delivered packets. UDP data checksums are optional, providing a way to exchange data over highly reliable networks without unnecessarily consuming network resources or processing time. UDP is used by applications that do not require an acknowledgment of data receipt. These applications typically transmit small amounts of data at one time. These broadcast packets must use UDP. The reliable delivery of data is the responsibility of the application. Applications that use UDP typically transfer small amounts of data at one time. Examples of services and applications that use UDP are DNS, RIP, and SNMP.

### 1.2.3 The Internet Layer

Internet protocols encapsulate packets into Internet datagrams and run all of the necessary routing algorithms. The routing functions that the Internet layer perform is necessary to allow hosts to interoperate with other networks. The Internet Layer corresponds roughly to the Network Layer in the OSI model. Five protocols are implemented at this layer:

- **Address Resolution Protocol (ARP)**, which determines the hardware address of the hosts.
- **Reverse Address Resolution Protocol (RARP)**, which provides reverse address resolution at the receiving host.
- **Internet Control Message Protocol (ICMP)**, which sends error messages to IP when network problems occur.
- **Internet Group Management Protocol (IGMP)**, which informs routers of the availability of members of multicast groups.
- **Internet Protocol (IP)**, which addresses and routes packets.

### 1.2.4 The Network Interface Layer

At the bottom of the model is the Network Interface Layer. This layer is responsible for sending and receiving frames, which are packets of information transmitted on a network as a single unit. The Network Interface Layer puts frames on the network, and pulls frames off the network.

There are two major categories of WAN technologies supported by TCP/IP. These are:

- Serial lines, which include dial-up analog, digital lines, and leased lines; and
- Packet-switched networks, which include X.25, frame relay, and asynchronous transfer mode (ATM).

TCP/IP is transported across a serial line using either the Serial Line Internet Protocol (SLIP) or the Point-to-Point Protocol (PPP). Windows 2000 Server supports both protocols with the Routing and Remote Access Service. However, PPP provides greater security, configuration handling, and error detection than SLIP and is the recommended protocol for serial line communication.

### 1.3 IP Addressing

An IP address is a 32-bit number that identifies a host on a TCP/IP network. A unique IP address is required for each host and network component that communicates on the TCP/IP network. TCP/IP networks are categorized into three main classes that have predefined sizes. Each network can be divided into smaller subnetworks by system administrators by using a subnet mask to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs. Each TCP/IP host is identified by a logical IP address. The IP address is a network layer address.

#### Network Address Translator (NAT)

There are two types of IP addresses: public and private. Public addresses are assigned to you by the Internet service provider (ISP) you use to connect to the Internet. For the hosts within the organization that do not require direct access to the Internet, IP addresses that do not duplicate already assigned public addresses are required. To solve this addressing problem a portion of the IP address space has been reserved as a private address space. An IP address in the private address space is not assigned as a public address. The use of private IP addresses provides protection from network hackers as Internet routers do not have routes to private addresses; private addresses are therefore not directly accessible from the Internet. When using private IP addresses, you need a mechanism to convert the private IP address range on your local network to a public IP address that can be routed. One mechanism is to have private addresses translated into valid public addresses by a network address translator (NAT) before it is sent on the Internet.

For a TCP/IP WAN to work correctly, the routers that pass packets of data between networks do not need to know the exact location of a host for which a packet of information is destined. It only needs to know the network that the destination the host is a member of. The routers then use information stored in their route table to determine how to get the packet to the destination host's network. After the packet is delivered to the destination's network, the packet is delivered to the appropriate host. For this process to work, an IP address has two parts:

- A **Network ID**, which identifies the TCP/IP hosts that are located on the same physical network. All hosts on the same physical network must be assigned the same network ID to communicate with each other. If routers connect your networks, a unique network ID is required for each wide area connection.
- A **Host ID**, which identifies a host within a network. The host ID must be unique to the network designated by the network ID.

### 1.3.1 IP Address Formats

There are two formats for referencing an IP address. These are binary and dotted decimal notation.

#### 1.3.1.1 Binary Format

Binary is a numeral system that uses bits, i.e. 0s and 1s, to denote a value. A 0 denotes that the bit does not carry a value and a 1 denotes that the bit does carry a value. A set of 8 bits form a byte and its value is calculated in multiples of 2 from right to left beginning with 1. Figure 1.2 illustrates a byte with a binary code of 11111111 and the value of each of its eight bits

<b>Binary Code</b>	1	1	1	1	1	1	1	1
<b>Decimal Value</b>	128	64	32	16	8	4	2	1

FIGURE 1.2: Binary Code 11111111

The decimal value of the binary code is the sum of decimal value of each bit. Therefore the decimal value for a binary code of 11111111 is  $1+2+4+8+16+32+64+128=255$

**Note:** The corresponding decimal value of the binary code is calculated from right to left and not left to right

A 0 in the binary code indicates that the corresponding bit has no value. Figure 1.3 illustrates a byte with a binary code of 11101101 and the value of each of its eight bits.

<b>Binary Code</b>	1	1	1	0	1	1	0	1
<b>Decimal Value</b>	128	64	32	0	8	4	0	1

FIGURE 1.3: Binary Code 11101101

The decimal value for this binary code is  $1+0+4+8+0+32+64+128=237$

**Note:** Each bit in the binary code that is marked with a 0 has no value. Therefore the corresponding decimal value of these bits are also 0.

Each IP address is 32 bits long and is composed of four 8-bit sections, which are called octets. These octets are equal to a byte, i.e., 8-bits long. An IP Address expressed as 11000000.10101000.10100110.01111110 in

binary format can be broken into its three octets: 11000000; 10101000; 10100110 and 01111110. These octets are converted to decimal value in Figure 1.4

### 1.3.1.2 Dotted Decimal Format

An IP address is usually expressed in dotted decimal format. This format consists of three decimal numbers that are separated by periods. Each decimal number represents the value of an octet with each octet representing a decimal number ranging from zero to 255.

<b>First Octet</b>	<b>Binary Code</b>	1	1	0	0	0	0	0	0
	<b>Decimal Value</b>	128	64	0	0	0	0	0	0
<b>Second Octet</b>	<b>Binary Code</b>	1	0	1	0	1	0	0	0
	<b>Decimal Value</b>	128	0	32	0	8	0	0	0
<b>Third Octet</b>	<b>Binary Code</b>	1	0	1	0	0	1	1	0
	<b>Decimal Value</b>	128	0	32	0	0	4	2	0
<b>Fourth Octet</b>	<b>Binary Code</b>	0	1	1	1	1	1	1	0
	<b>Decimal Value</b>	0	64	32	16	8	4	2	0

FIGURE 1.4: Binary Code 11000000.10101000.01111011

The decimal value of the first octet is:  $0+0+0+0+0+0+64+128 = 192$

The decimal value of the second octet is:  $0+0+0+8+0+32+0+128 = 168$

The decimal value of the third octet is:  $0+2+4+0+0+32+0+128 = 166$

The decimal value of the fourth octet is:  $0+2+4+8+16+32+64+0 = 126$

In dotted decimal format this IP Address would be expressed as: 192.168.166.126

## 1.4 IP Address Classes

Internet addresses are allocated by an organization that administers the Internet, called the InterNIC. InterNIC has divided the IP Address space into five classes. The most common of these are Classes A, B, and C. Classes D and E are not generally used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet.

- **Class A** addresses are assigned to networks with a very large number of hosts. Class A networks use a default subnet mask of **255.0.0.0** and range from **0.0.0.0 through 126.255.255.255**.
- **Class B** addresses are assigned to medium-sized to large-sized networks. Class B networks use a default subnet mask of **255.255.0.0** and range from **128.0.0.0 through 168.255.255.255** and **170.0.0.0 through 191.255.255.255**.

**Note:** IP addresses with a first octet of 127, i.e. **127.0.0.0 through 127.255.255.255** do not fall in either the Class A address range or the Class B address range. IP addresses that have a first octet of 127 are reserved for diagnostics purposes.

**Note:** In Windows 2000 networks, the IP address range of **169.254.0.1 through 169.254.255.254** and a subnet mask of **255.255.0.0** are reserved for the **Automatic Private IP Addressing (APIPA)** feature of Windows 2000.

- **Class C** addresses are used for small LANs. Class C networks use a default subnet mask of **255.255.255.0** and have a range of **192.0.0.0 through 223.225.225.225**.
- **Class D** addresses are reserved for multicast transmissions. This is commonly used for multimedia presentations across the Internet. **Class D** IP addresses are in the range **224.0.0.0 through 239.255.255.255**.

The IP Address class defines which bits are used for the network ID and which bits are used for the host ID. The IP Address class also defines the number of networks in a domain and the number of hosts per network.

## 1.5 IP Routing

Routing is the process of creating a **path** over which to send network transmissions between different networks and can be used to **link** networks that have different network topologies, such as Ethernet and Token Ring. A router, which is also referred to as a gateway, is a device that forwards the packets from one physical network to another. When a router receives a network packet, the network adapter forwards the datagrams to the **IP Layer**. IP examines the destination address on the datagram and then compares it to an IP routing table. The route to the destination host that requires the **least number of hops**, or that has the **lowest cost** is then determined and the packet is forwarded via this path.

IP Routing can be either static or dynamic.

### 1.5.1 Static IP Routing

Static routing is a function of IP that limits you to fixed routing tables. When using static routers, you must build and update the routing tables **manually**. You can use the **Route command** at a command prompt to add static entries to the routing table. Table 1.1 lists the Route commands

TABLE 1.1: IP Route commands

Route command	Usage
route add [ <i>network</i> ] mask [ <i>netmask</i> ] [ <i>gateway</i> ]	Adds a route
route -p add [ <i>network</i> ] mask [ <i>netmask</i> ] [ <i>gateway</i> ]	Adds a persistent route
route delete [ <i>network</i> ] [ <i>gateway</i> ]	Deletes a route
route change [ <i>network</i> ] [ <i>gateway</i> ]	Modifies a route
route print	Displays the routing table
route -f	Clears all routes

### 1.5.2 Dynamic IP Routing

When a route changes, static routers do not inform each other of the change, nor do static routers exchange routes with dynamic routers. In contrast, dynamic routing automatically updates the routing tables, reducing administrative overhead. However, dynamic routing **increases traffic** in large networks. Dynamic routing is a function of routing protocols, such as the Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). Routing protocols periodically exchange routes to known networks among dynamic routers. If a route changes, other routers are automatically informed of the change. You must have multiple network adapters on a Windows 2000 Server or Windows 2000 Advanced Server. In addition, you must install and

configure Routing and Remote Access because dynamic routing protocols are not installed by default when you install Windows 2000.

### 1.5.3 Routing Protocols

Windows 2000 supports two IP routing protocols that you can choose from, depending on the network size and topology. These routing protocols are:

- **Routing Information Protocol (RIP)**, which is a distance-vector routing protocol provided for backwards-compatibility with existing RIP networks. It allows a router to exchange routing information with other RIP routers. It broadcasts the information to neighboring routers, and sends periodic RIP broadcast packets containing all routing information known to the router. These broadcasts keep all internetwork routers synchronized.
- **Open Shortest Path First (OSPF)**, which is a link-state routing protocol that enables routers to exchange routing information and create a map of the network that calculates the best possible path to each network. When the link state database changes, the routing table is recalculated. However, the memory requirements and route computation times increase as the size of the link state database increases. To address this scaling problem, OSPF divides the internetwork into collections of contiguous networks called areas.

## 1.6. Testing IP Configurations

### 1.6.1 The IPConfig Utility

The IPConfig utility is a command-line utility that can be used to display the **TCP/IP configuration** of your computer. This information can be used to verify that the client computer has received a valid IP configuration from DHCP. It can also display the IP configuration, and parameters for the network connection on your computer. This information can be used to verify that the client computer is configured with the correct WINS and/or DNS server IP addresses.

TABLE 1.2: *IPConfig Switches*

Switch	Function
/all	Displays the configuration all network interfaces.
/release <adapter>	Releases the IP address for a specified network adapter card.
/renew <adapter>	Renew the IP address for the specified network adapter card.
/flushdns	Clears all entries from the DNS Resolver Cache on the local computer.
/registerdns	Renews the local computer's DHCP lease and reregisters DNS names.
/displaydns	Displays the contents of the DNS Resolver Cache on the local computer.
/showclassid <i>adapter</i>	Displays all the DHCP class IDs allowed for the specified network adapter card.
/setclassid <i>adapter</i>	Modifies the DHCP class ID for the specified network adapter card

/? Displays a list of all the IPConfig switches and their functions

**Note:** DNS clients **cache** the name resolution information it receives from DNS responses to its name resolution queries and uses this information to resolve future queries locally. When a query cannot be resolved locally, the client sends the query to the DNS server. However, when a server or remote host renews its IP address lease in DHCP, the local client computer will not hold the correct information in cache and will thus resolving names incorrectly. In this event you can use the **/flushdns** switch of the IPConfig utility to clear the cache on the local client computer.

### 1.6.2 The Ping Utility

The ping utility is another command-line utility that can be used to test low-level communication over IP to another host on the network in the form of an echo request. If the ping utility fails, it returns an error message. You can receive various messages when you use the ping utility:

TABLE 1.3: *Ping Errors*

Error Message	Problem
Destination host unreachable	there is an IP routing problem between your computer and the remote host
Unknown host hostname	none of the client's name resolution mechanisms recognize the name that you typed - check that you typed the host name correctly
Request timed out	the name resolution mechanisms have recognized the name, but the remote host did not receive the request or did not respond to it - check connectivity to the remote host

### 1.6.3 The Tracert Utility

The tracert utility is similar to the **ping** utility, except that it reports back from each router on the path from your client computer to the remote host. If you know the network topology in your organization, you can determine which router is unresponsive or slow.

### 1.6.4 The Net and Nbtstat Utilities

The net command can be used to view the computer's network settings. The **Net config** workstation command is a net command that is used for testing NetBIOS name resolution. The Net config workstation command reports the NetBIOS name and the domain name of the computer while the nbtstat command is used to check the state of current NetBIOS over TCP/IP connections, to **update the Lmhosts cache**, and to determine your registered name. This command can also be used to troubleshoot and preload the NetBIOS name cache.

TABLE 1.4: *nbtstat Commands*

Command	Description
---------	-------------

nbtstat -n	Lists the NetBIOS names registered by the client
nbtstat -c	Displays the NetBIOS name cache
nbtstat -R	Manually reloads the NetBIOS name cache by using entries in the Lmhosts file with a #PRE parameter
nbtstat /?	List all the nbtstat commands

## 1.7 IP Security (IPSec)

Windows 2000 implements IPSec transparently to ensure private, secure communications over IP networks, including the Internet, through the use of cryptographic security services. IPSec is designed to protect IP packets and to provide a defense against network attacks. These goals are met through the use of cryptography-based protection services, security protocols, and dynamic key management. IPSec can also be used to filter data packets on an IP network.

IPSec is based on an end-to-end security model, meaning that both the sending and receiving computers must be configured to use IPSec. Each of these computers is responsible for security at its respective end and assumes that the network over which the communication takes place is not secure. Routers that forward packets between the source and destination are not required to support IPSec. This allows IPSec to be deployed in server/client and peer to peer based LANs; Wide area network (WAN); and Remote dial-up access and Internet access from private networks.

To make use of IPSec protection, users do not have to be in the same domain. They can each be in any trusted domain in the enterprise as IPSec Management allows for the centralized administration of IPSec through the use of security policies, which are created by a domain administrator. These policies are stored in the directory service and assigned to domain policies.

**Note:** It is not possible to use IPSec through NAT or an application proxy as these modify fields in the packet. IPSec does not permit any modification of the packets and will thus drop the packets once it has been modified by NAT or the application proxy. Furthermore, if there is a **firewall** or **filtering router**, IP forwarding must be enabled on the firewall or filtering router on:

- **IP Protocol ID 51.** Both inbound and outbound filters must be configured to pass **AH traffic**.
- **IP Protocol ID 50.** Both inbound and outbound filters must be configured to pass **ESP traffic**.
- **UDP Port 500.** Both inbound and outbound filters must be configured to pass **ISAKMP traffic**.

### 1.7.1 Configuring IPSec

The computers in your network need to have an IPSec security policy defined that is appropriate for your network security. This security policy can be set in the Group Policy snap-in to Microsoft Management Console (MMC) and are listed under IP Security Policies in Active Directory: Group Policy Object.

Windows 2000 has three predefined security policy entries all of which not enabled by default: These security policies are:

- **Client (Respond Only) policy**, which allows clear-text communications but will attempt to negotiate security if a security request is made and uses Kerberos v5 for authentication.
- **Server (Request Security) policy**, which causes the server to attempt to initiate secure communications for every session. However, if a client that is not IPSec-aware initiates a session, that session will be allowed and will not be IPSec protected.
- **Secure Server (Require Security) policy**, which requires Kerberos trust for all IP packets sent from the computer on which it is enabled, with the exception of broadcast, multicast, Resource Reservation Setup Protocol (RSVP), and ISAKMP packets. This policy does not allow unsecured communications with clients. Therefore, any clients who connect to a server with this policy must be IPSec-aware.

## 2. IP Addressing

### 2.1 Automatic IP Addressing

In Windows 2000 client computer can obtain automatically obtain an IP address from a DHCP server or through Automatic Private IP Addressing (APIPA).

#### 2.1.1 Dynamic Host Configuration Protocol (DHCP) Addressing

If the network has a server running the Dynamic Host Configuration Protocol (DHCP Service, it can automatically assign TCP/IP configuration information to the client computers if the client computers are configured as DHCP clients. You can then configure any client running Windows 2000, Windows 95, and Windows 98 to obtain TCP/IP configuration information automatically from the DHCP Service. This can simplify administration and ensure correct configuration information.

##### 2.1.1.1 The DHCP Lease Process

The DHCP client waits one second for an offer. If it does not receive an offer, it rebroadcasts the request four times at 2, 4, 8, and 16 second intervals. If the client does not receive an offer after four requests, it uses an IP address in the reserved range from 169.254.0.1 through 169.254.255.254. This ensures that clients on a subnet without a DHCP server can communicate with each other. The DHCP client continues in an attempt to find a DHCP server every five minutes. When a DHCP server becomes available, clients receive valid IP addresses, allowing them to communicate with hosts both on and off their subnet.

DHCP uses a four-step process to lease IP addressing information to DCHP clients. This process is also referred to as **DORA**: **D**iscovery, **O**ffer, **R**equest, and **A**cknowledgment

- **IP Lease Discovery**

When a client computer either starts or initializes TCP/IP for the first time, it initializes a limited version of TCP/IP and broadcasts a DHCP discovery (**DHCPDISCOVER**) message for IP addressing information. At this stage the client does not have an IP address. It therefore uses **0.0.0.0** as its IP address. The client also does not know the IP address of a DHCP server, and therefore uses **255.255.255.255** as the destination address. The DHCPDISCOVER message is broadcast to the entire subnet and contains the hardware address of the client's network adapter, which is known as the media access control (MAC) address; and the client's computer name so that DHCP servers can determine which client sent the DHCPDISCOVER message.

- **IP Lease Offer**

The second stage in the DHCP lease process is the IP lease offer. All DHCP servers that have an IP address that is valid for the network segment to which the client is connected respond with a DHCP offer (**DHCPOFFER**) message. This message includes:

- The client's hardware address
- An offered IP address
- A subnet mask
- The length of the lease
- The IP address of the offering DHCP server

Each responding DHCP server reserves the offered IP address so that it does not offer it to another DHCP client before the requesting client accepts the address.

- **IP Lease Request**

The third stage is the IP Lease Request. During this stage the DHCP client responds to the first offer that it receives by broadcasting a DHCP request (**DHCPREQUEST**) message to accept the offer. The DHCPREQUEST message includes the server identification of the server whose offer it accepted. All other DHCP servers then retract their offers and retain their IP addresses for other IP lease requests.

- **IP Lease Acknowledgement**

The final stage is IP Lease Acknowledgement during which the DHCP server that issues the accepted offer broadcasts a DHCP acknowledgement (**DHCPACK**) message to acknowledge the successful lease. This message contains a valid lease for the IP address and other configuration information. When the DHCP client receives the acknowledgment, TCP/IP initializes by using the configuration information that the DHCP server provides. The client also binds the TCP/IP protocol to the network services and network adapter, permitting the client to communicate on the network.

### 2.1.1.2 Automatic Lease Renewal

At specific intervals, a DHCP client attempts to renew its lease to ensure that it has up-to-date configuration information. A DHCP client attempts to renew its lease **when 50 percent of the lease duration has expired**. The DHCP client sends a DHCPREQUEST message to the DHCP server from which it obtained the lease. If the DHCP server is available, it renews the lease and sends the client a DHCPACK message with the new lease duration and any updated configuration parameters. The client updates its configuration when it receives the acknowledgment. If the DHCP server is unavailable, the client continues to use its current configuration parameters and a DHCP client cannot renew its lease at the 50 percent interval, the client continues to use its current configuration parameters. It then broadcasts a DHCPDISCOVER message to update its address lease at regular intervals and accepts a lease that is issued by any DHCP server.

#### Client Reservations

You can configure a scope so that the DHCP server always provides the same IP address to a computer that requires a permanent IP address, such as a DNS server. This is called *client reservations*.

### 2.1.1.3 Manual Lease Renewal

You can use the IPConfig command with the /renew switch to manually renew an IP lease if you need to update DHCP configuration information immediately if you want DHCP clients to immediately obtain the address of a newly installed router from a DHCP server, renew the lease from the client to change this configuration. Windows 3.51, Windows NT 4.0, Windows 2000, and Windows XP clients can use the IPConfig command with the /release switch to release a lease while Windows 95 and Windows 98 clients must use the **winipcfg** command. These commands send a DHCPRELEASE message to the DHCP server to release a client lease. After you issue this command, the client can no longer communicate on the network by using TCP/IP.

**Note:** You must **authorize** a DHCP server before the server can issue leases to DHCP clients. This prevents unauthorized DHCP servers from offering incorrect IP configurations to clients. However, only DHCP servers running Windows 2000 Server check for authorization. Other DHCP servers can still operate even though they are not authorized. You must be a member of the Enterprise Administrators group to authorize a DHCP server as you need network-wide administrative privileges to authorize a DHCP server.

### 2.1.2 Automatic Private IP Addressing

Windows 2000 supports a new mechanism for automatic address assignment of IP addresses for simple LAN-based network configurations called **Automatic Private IP Addressing (APIPA)**. This mechanism is an extension of dynamic IP addressing and enables the configuration of IP addresses without using static IP address assignment or installing the DHCP Service.

On a computer running Windows 2000 you must configure a network LAN adapter for TCP/IP and click **Obtain an IP Address Automatically in the Internet Protocol (TCP/IP) Properties** dialog box for the Automatic Private IP Addressing feature to function properly.

APIPA can be used to set up IP configuration to allow network communication on a single subnet and is also used when the client computer cannot contact the DHCP server for IP address configuration. APIPA uses an addressing range from **169.254.0.1 through 169.254.255.254** and a subnet mask of **255.255.0.0**.

When you use DHCP to automatically configure TCP/IP information, the DHCP server supplies the necessary configuration information to the DHCP clients and ensures that the clients use the correct configuration information. Then, DHCP automatically updates client configuration information to reflect changes in network structure and the relocation of users to other physical networks, without manually reconfiguring client IP addresses.

Every time a DHCP client starts, it requests an IP address from a DHCP server. Once the DHCP server receives the request, it selects an IP address from a predefined range of addresses in its database and offers this address to the DHCP client. If the client accepts the offer, the DHCP server leases the IP address to the client for a specified period of time. The default duration of an IP address lease is eight days. The client then uses the IP address to access the network.

The IP addressing information sent by the DHCP server to the DHCP client includes:

- An IP address;
- A subnet mask; and
- Optional values, such as:
  - A default gateway address
  - The IP addresses of Domain Name System (DNS) servers
  - The IP addresses of Windows Internet Name Service (WINS) servers
  - Domain name

## 2.2 Installing and Configuring DHCP

To install a DHCP server:

- Click on the **START** button
- Point to **SETTINGS**
- Clicking **CONTROL PANEL**
- In the **Control Panel**, double-click **ADD/REMOVE PROGRAMS**
- Click **ADD/REMOVE WINDOWS COMPONENTS**
- Under **Components**, scroll to and click **NETWORKING SERVICES**
- Click the **DETAILS** button

- Select **DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)**
- Click **OK**
- Click **NEXT**
- If prompted, type the full path to the Windows 2000 distribution files and click **CONTINUE**. The required files will be copied to your hard disk.
- Click **FINISH** to close the Windows Components Wizard

**Note:** You must configure the DHCP server computer to use a static IP Address. The DHCP server cannot be a DHCP client as the IP configuration information is required during the boot process when the computer, the DHCP server in this case, is switched on. It must therefore have a static IP address, subnet mask, and default gateway address.

### 2.2.1 Authorizing DHCP

When the DHCP server is configured incorrectly or unauthorized and is introduced into the network, it can cause problems by leasing incorrect IP addresses to clients, negatively acknowledging DHCP clients, or attempting to renew current address leases. To avoid these problems you must authorize all DHCP servers before they can service clients.

The authorization process for DHCP server computers in Active Directory depends on the installed role of the server on your network. In Windows 2000 Server there are three roles or server:

- A **Domain Controller**, which keeps and maintains a copy of the Active Directory service database and provides secure account management for domain member users and computers;
- A **Member Server**, which does not operate as a domain controller but has joined a domain in which it has a membership account in the Active Directory service database; and
- A **Stand-Alone Server**, which does not provide secured logon access to shared domain resources.

If you deploy Active Directory, all computers operating as DHCP servers must be either domain controllers or domain member servers before they can be authorized in the directory service and provide DHCP service to clients.

To authorize the DHCP server:

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ADMINISTRATIVE TOOLS**
- Click **DHCP**
- Click on the **ACTION MENU**
- Click **MANAGE AUTHORIZED SERVERS**
- Click **AUTHORIZE**
- Enter the name or IP address of the DHCP server to be authorized
- Click **OK**

**Note:** To authorize a DHCP server, you must be logged on to the network

using an account that has **enterprise administrative privileges** or one that has been **delegated the authority to authorize DHCP** servers for your enterprise.

### 2.2.2 DHCP Scopes

Before a DHCP server can lease an address to DHCP clients, it must have a pool of valid IP addresses available to lease to DHCP clients. This pool of IP addresses is called a scope. At least one must be created for each DHCP server. You can however, create multiple scopes on a DHCP server to centralize administration and to assign IP addresses specific to a subnet and you can assign only one scope to a specific subnet. Because DHCP servers do not share scope information, you must ensure that IP addresses are not duplicated in scopes of multiple DHCP servers. You must also ensure that static IP addresses are not included in any DHCP server's scope

To create a new scope:

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ADMINISTRATIVE TOOLS**
- Click **DHCP**
- Click on the **ACTION MENU**
- Click **NEW SCOPE**
- The **NEW SCOPE WIZARD** appears

#### 2.2.2.1 IP Scope Exclusion Range

After you have defined a scope, you must create an exclusion range for the IP addresses of devices that have been configured with static IP addresses that must not be leased to DHCP clients. This includes the IP addresses that have been assigned to the DHCP servers.

#### 2.2.2.2 IP Reservations

You can also create reservations, i.e. you can reserve some IP addresses for permanent lease assignment to specified computers or devices, such as print servers on the network. You should make reservations only for devices that are DHCP-enabled and that must be reserved for specific purposes on your network. When multiple DHCP servers are deployed, the reservation should be created on all of the DHCP servers that potentially service the reservation client.

**Note:** When reserving an IP address for a new client or an address that is different from its current one, you must verify that the address has not **already been leased** by the DHCP server. If the address is already in use, the client using the address must first release it. To do this, type **ipconfig /release** at the command prompt on the client computer that must release the address. On the new client for which the reservation is made the client must issue a DHCP request message. To do this type **ipconfig /renew** at the command prompt on the new computer.

### 2.2.2.3 DHCP Scope Configuration Options

To provide full configuration for clients, DHCP options need to be configured and enabled for the scope. Table 2.1 describes some of these options supported by Microsoft DHCP clients.

TABLE 2.1: *DHCP Scope Configuration Options*

Option	Description
003 Router	Specifies the IP address of a the <b>gateway address</b> . If the client has a locally defined default gateway, this configuration takes precedence over the DHCP option.
006 DNS Servers	Specifies the IP address of a <b>DNS server</b> .
015 DNS Domain Name	Specifies the DNS domain name for client resolutions.
044 WINS/NBNS servers	Specifies the IP address of the WINS server. If a WINS server address is configured manually on a client, this configuration overrides the values configured for this option.
046 WINS/NBT node type	Specifies the type of NetBIOS over TCP/IP name resolution.
047 NetBIOS Scope ID	Specifies the local NetBIOS scope ID.

### 2.2.3 Implementing Multiple DHCP Servers

Should your internetwork requires multiple DHCP servers, a unique scope must be created for each subnet. To ensure that clients can lease IP addresses in the event of a server failure, it is important to have multiple scopes for each subnet distributed among the DHCP servers in the internetwork. Each DHCP server should have a scope containing approximately 75 percent of the available IP addresses for the local subnet and approximately 25 percent of the available IP addresses for a remote subnet. When a client's DHCP server is unavailable, the client can still receive an address lease from another DHCP server on a different subnet, assuming the router is a DHCP relay agent.

### 2.3 DHCP Relay Agents

The DHCP Relay Agent component provided with the Windows 2000 router is a BOOTP relay agent, which is a small program that relays DHCP/BOOTP messages between clients and servers on different subnets. The DHCP Relay Agent thus relays DHCP messages between DHCP clients and DHCP servers on different IP networks.

**Note:** For each IP network segment, or **subnet**, that contains DHCP clients, either a **DHCP server** or a computer acting as a **DHCP relay agent** is required.

To add the DHCP Relay Agent

- Click on the **START** button
- Point to **PROGRAMS**

- Point to **ADMINISTRATIVE TOOLS**
- Click **ROUTING AND REMOTE ACCESS**
- In the console tree, click **SERVER NAME**
- Click **IP ROUTING**
- Click **GENERAL**
- Right-click **GENERAL**
- Click **NEW ROUTING PROTOCOL**
- In the Select Routing Protocol dialog box, click **DHCP RELAY AGENT**
- Click **OK**

## 2.4 Troubleshooting DHCP

Most DHCP problems are the result of incorrect or missing configuration details. To help prevent the most common types of problems, you should:

- Use the **75/25 rule** for balancing scope distribution of IP addresses when **multiple DHCP servers** are deployed on the internetwork. Furthermore, using more than one DHCP server on the same subnet provides increased fault tolerance for servicing DHCP clients located on that subnet because, when one server is unavailable, the other server can take its place and continue to lease new addresses or renew existing clients.
- Use **superscopes** for multiple DHCP servers on each subnet in a LAN environment. A superscope allows a DHCP server to provide leases from more than one scope to clients on a single physical network
- **Deactivate scopes** only when removing a scope permanently from service.
- **Reservations** should be created on all DHCP servers that can potentially service the reserved client.

### 2.4.1 Troubleshooting DHCP Clients

You can use the Ipconfig TCP/IP utility at the command prompt to get information about the configured TCP/IP parameters on local or remote computers on the network. When a client fails to obtain the correct TCP/IP configuration, you can use this information to quickly identify the source of the problem.

If a DHCP client does not have an IP address configured or has an APIPA address, i.e. an IP address in the range **169.254.0.1 through 169.254.255.254**, it means that the client was not able to contact a DHCP server and obtain an IP address lease. This could be because of a network hardware failure or because the DHCP server is unavailable.

- Verify that the client computer has a functioning network connection, i.e. check that the network adapter is working properly at the client and check the network cable.
- Use the PING command to test connectivity from the client to the server.
- Attempt to renew the client lease, it might be necessary to disable APIPA at the client first.
- Check that the DHCP server is available on the network by pinging it from another computer on the same subnet as the affected DHCP client.

If a DHCP client is missing configuration details, the client might be missing DHCP options in its leased configuration, either because the DHCP server is not configured to distribute them or the client does not support the options distributed by the server.

- On the client, verify that the required options have been configured at either the server, scope, client, or class level of option assignment.
- Check the DHCP option settings.

If the DHCP server is configured with an incorrect DHCP router option.

- Change the IP address list for the router or default gateway option at the applicable DHCP scope and server.
- Set the correct value in the Scope Options tab of the Scope Properties dialog box.

If DHCP clients are unable to get IP addresses from the server:

- The IP address of the DHCP server might have been changed and now DHCP clients cannot get IP addresses. A DHCP server can only service requests for a scope that has a network ID that is the same as the network ID of its IP address, unless superscopes are used. Make sure that the DHCP server IP address falls in the same network range as the scope it is servicing.

If the DHCP clients are located across a router from the subnet where the DHCP server resides, and are unable to receive an address from the server. A DHCP server can provide IP addresses to client computers on remote subnets only if the router that separates them can act as a DHCP relay agent.

- Configure a BOOTP/DHCP relay agent on the client subnet. The relay agent can be located on the router itself or on a Windows 2000 Server computer running the DHCP Relay service component.
- At the DHCP server, configure a scope to match the network address on the other side of the router where the affected clients are located and make sure that the subnet mask is correct for the remote subnet.
- Do not include this scope in superscopes configured for use on the same local subnet or segment where the DHCP server resides.

If multiple DHCP servers exist on the same LAN

- Make sure that multiple DHCP servers do not have overlapping scopes

#### **2.4.2 Troubleshooting DHCP Servers**

When a server fails to provide leases to its clients

- Verify that the DHCP services are running by opening the DHCP service console to view service status, or by opening Services And Applications under Computer Manager.
- If the appropriate service is not started, start the service.
- If the DHCP server is stopped, start Windows 2000 Server, and log on as an administrator. At the command prompt, type `net start dhcpserver`, then press Enter.

If a new scope has been added at the DHCP server for the purpose of renumbering the existing network but the DHCP clients do not obtain leases from the newly defined scope

Only a single DHCP scope can be active on the network at one time. If more than one scope is defined and activated on the DHCP server, only one scope is used to provide leases to clients. The active scope used for distributing leases is determined by whether the scope range of addresses contains the first IP address that is bound and assigned to the DHCP server's network adapter hardware. When additional secondary IP

addresses are configured on a server using the Advanced TCP/IP Properties tab, these addresses have no effect on the DHCP server in determining scope selection or responding to configuration requests from DHCP clients on the network. To solve this problem

- Configure the DHCP server to use a superscope that includes the old scope and the new scope.
- Change the primary IP address (the address assigned in the TCP/IP Properties tab) on the DHCP server's network adapter to an IP address that is part of the same network as the new scope.

## 2.5 Static IP Addressing

Client computers that run Windows 2000, Windows 95, or Windows 98 are configured by default to obtain TCP/IP configuration information automatically from the Dynamic Host Configuration Protocol (DHCP) Service. However, even in a DHCP-enabled environment, you should assign a static IP address to selected network computers, such as the computer running the DHCP Service as it cannot be a DHCP client.

To configure a Windows 2000 computer to use static IP Addressing:

- On the Desktop, right-click **MY NETWORK PLACES**
- Click **PROPERTIES**
- In the **NETWORK AND DIAL-UP CONNECTIONS** window, right-click **LOCAL AREA CONNECTION**
- Click **PROPERTIES**
- In the **LOCAL AREA CONNECTION PROPERTIES** dialog box, click **INTERNET PROTOCOL (TCP/IP)**
- Verify that the **INTERNET PROTOCOL (TCP/IP)** check box is selected
- Click **PROPERTIES**
- In the **INTERNET PROTOCOL (TCP/IP) PROPERTIES** dialog box, click on the **GENERAL** tab
- Click **USE THE FOLLOWING IP ADDRESS**
- Enter the TCP/IP configuration information
- Click **OK**
- Click **OK** again to close the Local Area Connection Properties dialog box
- Close the Network And Dial-Up Connections window