TABLE OF CONTENTS

Chinatag.com

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

Chinatag.com

Chinatag.com

Chinatag.com

LIST OF TABLES

Chinatag.com

Chinatag.com

Implementing and Administering a Microsoft Windows 2000 Network Infrastructure

Exam Code: 070-216

Certifications:

Microsoft Certified (MCP)	
Microsoft Certified Systems Engineer (MCSE)	**Core**
Microsoft Certified Systems Administrator (MCSA)	**Elective**
Microsoft Certified Database Administrator (MCDBA)	**Elective**

PrereZuisites:

About This Study Guide

This Study Guide provides all the information reZuired 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 reZuired to answer Zuestions 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 reZuire 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.

Chinatag.com

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 reZuire 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!

Chinatag.com

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 reZuiring 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.

Chinatag.com

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 reZuires 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

Chinatag.com

- **L2TP**, which is a combination of PPTP and Layer 2 Forwarding. L2PT 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.

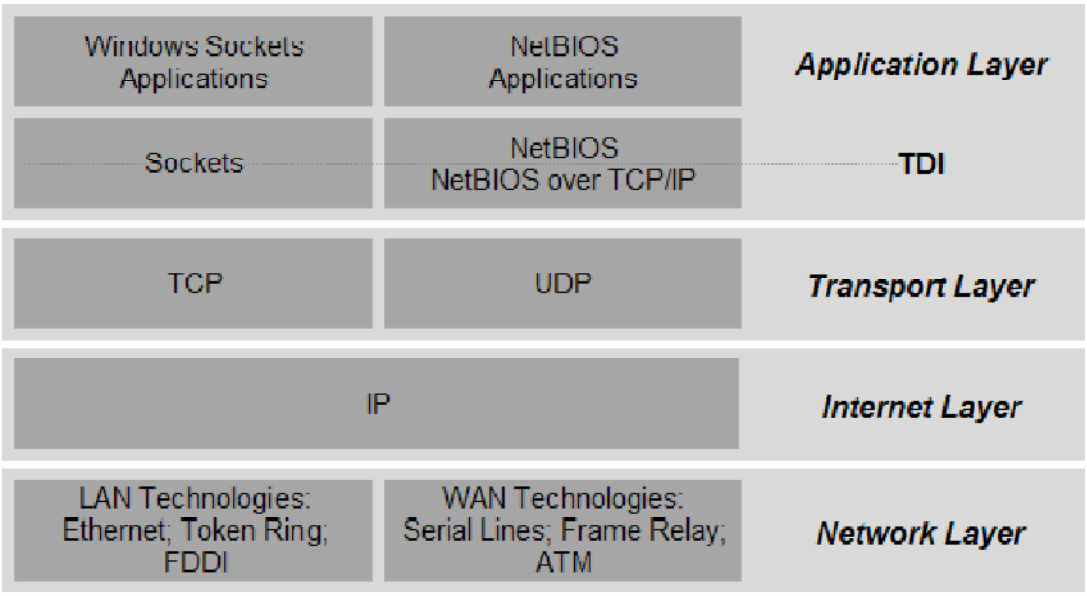

FIGURE 1.1: *The TCP/IP Four-Layer Conceptual Model*

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 UP addresses when locating hosts.

Chinatag.com

- **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 reZuire 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 seZuence 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 reZuire 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 seZuence of bytes.

1.2.2.2 User Datagram Protocol (UDP)

UDP offers a connectionless datagram service that does not guarantee delivery or the correct seZuencing 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 reZuire 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.

Chinatag.com

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.

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 reZuire direct access to the Internet, IP addresses that do not duplicate already assigned public addresses are reZuired. 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.

1.3 IP Addressing

An IP address is a 32-bit number that identifies a host on a TCP/IP network. A uniZue IP address is reZuired 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.

Chinatag.com

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 uniZue network ID is reZuired for each wide area connection.
- **A Host ID**, which identifies a host within a network. The host ID must be uniZue 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

Binary Code	1	1	1	1	1	1	1	1
Decimal Value	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.

Binary Code	1	1	1	0	1	1	0	1
Decimal Value	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 eZual to a byte, i.e., 8-bits long. An IP Address expressed as 11000000.10101000.10100110.01111110 in

Chinatag.com

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.

First Octet	**Binary Code**	1	1	0	0	0	0	0	0
	Decimal Value	128	64	0	0	0	0	0	0
Second Octet	**Binary Code**	1	0	1	0	1	0	0	0
	Decimal Value	128	0	32	0	8	0	0	0
Third Octet	**Binary Code**	1	0	1	0	0	1	1	0
	Decimal Value	128	0	32	0	0	4	2	0
Fourth Octet	**Binary Code**	0	1	1	1	1	1	1	0
	Decimal Value	0	64	32	16	8	4	2	0

FIGURE 1.4: *Binary Code11000000.10101000.01111011*

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.

Chinatag.com

- **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 reZuires 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 of 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 [*network*] mask [*netmask*] [*gateway*]	Adds a route
route -p add [*network*] mask [*netmask*] [*gateway*]	Adds a persistent route
route delete [*network*] [*gateway*]	Deletes a route
route change [*network*] [*gateway*]	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

Chinatag.com

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 reZuirements 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 *adapter*	Displays all the DHCP class IDs allowed for the specified network adapter card.
/setclassid *adapter*	Modifies the DHCP class ID for the specified network adapter card

Chinatag.com

/?	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 Zueries and uses this information to resolve future Zueries locally. When a Zuery cannot be resolved locally, the client sends the Zuery 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 ca be used to test low-level communication over IP to another host on the network in the form of an echo reZuest. 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
ReZuest timed out	the name resolution mechanisms have recognized the name, but the remote host did not receive the reZuest 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: *nbstat Commands*

Command	Description

Chinatag.com

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 nbstat 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 reZuired 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:

Chinatag.com

- **Client (Respond Only) policy**, which allows clear-text communications but will attempt to negotiate security if a security reZuest is made and uses Kerberos v5 for authentication.
- **Server (ReZuest 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 (ReZuire Security) policy**, which reZuires 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.

Chinatag.com