Before Installing TCP/IP

You need to know the following information before you install Microsoft TCP/IP on a Windows NT computer:

- Whether you can use Dynamic Host Configuration Protocol (DHCP) configuration. You can choose this option if a DHCP server is installed on your internetwork; you cannot choose this option if this computer will be a DHCP server.
- Whether this computer will be a DHCP server, a Windows Internet Name Service (WINS) server, or a Domain Name System (DNS) server. These options are available only for Windows NT Server computers.

If you cannot use DHCP to configure TCP/IP automatically, obtain the following values from your network administrator so you can configure TCP/IP manually:

- The IP address and subnet mask for each network adapter card installed on the computer.
- The IP address for the default local gateway (IP router).
- If your computer will be using DNS, the name of your DNS domain and the IP addresses of the DNS servers on the internetwork.
- If WINS servers are available on your network, the IP addresses for WINS server addresses.

{button ,AL("A_InstallTCPIPTopics")} Related Topics

To Install TCP/IP

1 Click here ↖ to display **Network** properties.

2 Click **Add**.

3 In the **Network Protocol** list, click **TCP/IP Protocol**, and then click **OK**.

4 Click **Yes** to use DHCP to configure TCP/IP automatically.

Or, click **No** to configure TCP/IP manually.

5 Type the full path to the Windows NT distribution files and click **Continue**.

All necessary files are copied to your hard disk.

Note

- The settings take effect after you restart the computer.

{button ,AL("BeforeInstallingTCPIP;TCPIPInstallationOptions;A_ConfigTCPIPTopics")} Related Topics

TCP/IP Installation Options

TCP/IP Internetworking Protocol

Connectivity Utilities

SNMP Service

TCP/IP Network Printing Support

Simple TCP/IP Services

DHCP Server Service

WINS Server Service

Domain Name System (DNS) Service

Enable Automatic DHCP Configuration

Sample Files

Diagnostic Utilities

{button ,AL("A_InstallTCPIPTopics")} Related Topics

TCP/IP Internetworking Protocol

Installs TCP/IP protocols, NetBIOS over TCP/IP, the Windows Sockets interface, and the TCP/IP diagnostics utilities automatically.

Connectivity Utilities

Installs the TCP/IP connectivity utilities.

SNMP Service

Installs the Simple Network Management Protocol (SNMP) service, which allows you to administer this computer remotely (using remote management tools such as Sun Net Manager or HP Open View) and to monitor statistics for TCP/IP services (using Performance Monitor).

TCP/IP Network Printing Support

Allows this computer to print to UNIX print queues or TCP/IP printers that are connected directly to the network. You must also install this option to use the Lpdsvr service, which enables UNIX computers to print to Windows NT printers.

Simple TCP/IP Services

Installs the server software that allows this computer to respond to requests from other computers that support the TCP/IP services Echo, Daytime, Chargen, and Discard.

DHCP Server Service

Installs the DHCP server software to support automatic configuration and addressing for computers using TCP/IP on your internetwork.

If you select this option, you must manually configure the IP address, subnet mask, and default gateway for this computer. You must also provide configuration information for the computers that use this service to automatically configure TCP/IP.

WINS Server Service

Installs the server software to support WINS, a dynamic name resolution service for computers on a Windows internetwork.

Select this option if this computer is to be installed as a primary or secondary WINS server. Do not select this option if this computer will be a WINS proxy agent.

Domain Name System (DNS) Service

Installs the server software to support DNS, a distributed name resolution service for computers on TCP/IP internetworks. DNS is the name resolution service used by the Internet.

Select this option if this computer is to be installed as a primary or secondary DNS server.

Enable Automatic DHCP Configuration

Turns on automatic configuration of TCP/IP parameters for this computer. Select this option if there is a DHCP server on your internetwork that supports dynamic host configuration. This is the preferred method for configuring TCP/IP on most Windows NT computers.

This option is not available if the **DHCP Server Service** option is selected.

Sample Files

After TCP/IP is installed, the %SystemRoot%\System32\Drivers\Etc folder contains several files, including sample HOSTS, LMHOSTS, NETWORKS, PROTOCOLS, QUOTES, and SERVICES files.

Diagnostic Utilities

Isolates network hardware problems and incompatible configurations. You can use the diagnostic utilities (such as **ping**) if you are having trouble installing TCP/IP on your computer.

TCP/IP Configuration Options

For TCP/IP to work on your computer, it must be configured with IP addresses, subnet masks, and default gateway for each network adapter on the computer. TCP/IP can be configured in one of two ways:

- Automatically, if there is a Dynamic Host Configuration Protocol (DHCP) server on your internetwork.
- Manually, if there is no DHCP server, or if you are configuring a Windows NT Server computer to be a DHCP server.

{button ,AL("A_ConfigTCPIPTopics")} Related Topics

Preliminary Notes

The best method for ensuring easy and accurate installation of TCP/IP is to use Dynamic Host Configuration Protocol (DHCP), which automatically configures your local computer with the correct IP address, subnet mask, and default gateway.

You can take advantage of this method for configuring TCP/IP if there is a DHCP server installed on your network. Contact your network administrator to find out if this option is available.

Note

- You cannot use DHCP configuration for a server that you are installing as a DHCP server or a WINS server. You must manually configure TCP/IP settings for DHCP servers.

To Configure TCP/IP Automatically with DHCP

Preliminary Notes

1 If you are installing TCP/IP, in the **Network** dialog box, click **Close**.

Or, if you are reconfiguring TCP/IP, click here ↖ to display **Network** properties.

2 In the **Network Protocol** list, click **TCP/IP Protocol**, and then click **OK**.

3 Click **Obtain an IP address from a DHCP server** and then click **OK**.

Note

- To initiate automatic configuration by the DHCP server, restart your computer.

Other Considerations

{button ,AL("A_ConfigTCPIPTopics;ToInstallaDHCPServer")} Related Topics

Other Considerations

If you subsequently attempt to reconfigure TCP/IP, any settings you enter manually will override the automatic settings provided by DHCP. As a general rule, you should not change the automatic settings.

Preliminary Notes

If you are installing TCP/IP on a DHCP server or a WINS server, or if you cannot use automatic DHCP configuration, you must manually enter valid addressing information after the TCP/IP protocol software is installed on your computer.

For a WINS server computer that has more than one network adapter card, WINS always binds to the first adapter in the list of adapters bound by TCP/IP. Make sure that this adapter address is not set to zero (0), and that the binding order of IP addresses is not changed.

Notes

- To configure TCP/IP, you must be logged on as a member of the Administrator group for the local computer.
- To avoid duplicate addresses, be sure to use the values for IP addresses and subnet masks that are supplied by your network administrator. Duplicate addresses can cause some computers on the network to function unpredictably.

To Configure TCP/IP Manually

Preliminary Notes

1 If you are installing TCP/IP, in the **Network** dialog box, click **Close**.

Or, if you are reconfiguring TCP/IP, click here ↰to display **Network** properties.

2 In the **Network Protocol** list, click **TCP/IP Protocol**, and then click **Properties**.

3 In the **Adapter** list, click the network adapter for which you want to set IP addresses.

4 For each bound network adapter, type values in the **IP Address** and **Subnet Mask** boxes.

5 For each network adapter, type the correct IP address value in the **Default Gateway** box.

Note

- The settings take effect after you restart the computer.

Other Considerations

{button ,AL("A_ConfigTCPIPmanually")} Related Topics

Other Considerations

If you click **Obtain an IP address from a DHCP server**, any values you enter in this dialog box will override the automatic values set by DHCP.

After TCP/IP is installed, the %SystemRoot%\System32\Drivers\Etc folder will contain several files, including default HOSTS and sample LMHOSTS files.

Preliminary Notes

If your computer has multiple network adapters connected to different networks using TCP/IP, you would typically select this option.

To Configure Advanced TCP/IP Options

Preliminary Notes

1 Click here to display **Network** properties.

2 In the **Network Protocol** list, click **TCP/IP Protocol**, and then click **Properties**.

3 On the **IP Address** tab, click **Advanced**.

4 In the **Adapter** box, click the network adapter for which you want to specify advanced configuration values.

The IP address, default gateway, and Point-to-Point Tunneling Protocol (PPTP) filtering settings in this dialog box are defined for the selected network adapter only.

5 Under **IP Addresses**, click **Add**. In the **IP Address** and **Subnet Mask** boxes, type an additional IP address and subnet mask for the selected adapter, and then click **Add** to move them to the **IP Addresses** list.

If your network card uses multiple IP addresses, repeat this process for each additional IP address. This list specifies up to five additional IP addresses and subnet masks for identifying the selected network adapter. This can be useful for a computer connected to one physical network that contains multiple logical IP networks.

6 Under **Gateways**, click **Add**. In the **Gateway Address** box, type the IP address for an additional gateway that the selected adapter can use, and then click **Add** to move the IP address to the **Gateways** list.

Repeat this process for each additional gateway. This list specifies up to five additional default gateways for the selected network adapter.

7 If you want to enable PPTP filtering, click **Enable PPTP Filtering**.

PPTP is a networking technology that supports multiprotocol virtual private networks (VPNs), enabling remote users to access corporate networks securely across the Internet.

8 If you want to enable TCP/IP security, click **Enable Security**, and then click **Configure**.

9. Continue with To Configure Advanced TCP/IP Security.

Notes

- The settings take effect after you restart the computer.
- To change the priority order for the gateways, click an address to move, and then click **Up** or **Down**. To remove a gateway, click it, and then click **Remove**.

Important

- If you select PPTP filtering, you effectively disable the selected network adapter for all other protocols. Only PPTP packets will be allowed. Typically, you would use this is with a multihomed computer with one network adapter (with PPTP filtering enabled) connected to the Internet and another network adapter connected to the internal corporate network. Clients outside the corporate network can use PPTP to connect to this machine from across the Internet and thus gain secure access to the corporate network.

For more information on PPTP filtering, see the *Windows NT Server Networking Supplement*..

{button ,AL("A_ConfigAdvancedTCPIP;ToConfigureTCPIPManually")} Related Topics

Preliminary Notes

TCP/IP Security allows you to control the type of TCP/IP network traffic that reaches your Windows NT Server. This is one of the security mechanisms typically used on Internet servers.

You can also use TCP/IP Security to control the protocols and well-known services that clients are allowed to connect with on your server. For example, you could allow only TCP (Protocol 6) connections and block all other IP protocols, or you could allow clients to connect to FTP (TCP Port 21) but disallow connections to all other well-known services, such as finger (TCP Port 79).

Important

■ This is an advanced feature. Setting these parameters incorrectly could limit your server's ability to function on the internetwork.

To Configure Advanced TCP/IP Security

Preliminary Notes

1 Click here to display **Network** properties.

2 In the **Network Protocol** list, click **TCP/IP Protocol**, and then click **Properties**.

3 On the **IP Address** tab, click **Advanced**.

4 Click **Enable Security**, and then click **Configure**.

5 In the **Adapter** list, select the network adapter for which you want to set TCP/IP security.

6 You can set filtering by **TCP Ports**, **UDP Ports**, and **IP Protocols**. For each of the three filters, click either **Permit All** (the default setting) or **Permit Only**, as follows:

- To allow all connections of that type to pass through, click **Permit All**.
- To block all connections of that type, click **Permit Only,** click **Add,** and then type the port or protocol numbers that you want to re-enable. If you leave the list blank, all connections of that type are disabled.

Note

- To delete a port or protocol from a list, click it, and then click **Remove**.

{button ,AL("A_ConfigAdvancedTCPIP")} Related Topics

Preliminary Notes

Although TCP/IP uses IP addresses to identify and reach computers, most users prefer to use names. Domain Name System (DNS) is a naming service that maps computer names to IP addresses. Windows Sockets applications and TCP/IP utilities (such as FTP and Telnet) typically use DNS (or the HOSTS files).

To find out whether you should configure your computer to use DNS, contact your network administrator. Typically, you use DNS if you are using TCP/IP to communicate over the Internet, or if your private internetwork uses DNS for name resolution.

If you choose to use DNS, you must install TCP/IP and then configure your computer to use DNS and the HOSTS file. DNS configuration is global for all network adapters installed on a computer.

Note

- A DNS domain is not the same as a Windows NT or a Microsoft LAN Manager domain.

To Configure TCP/IP to Use DNS

Preliminary Notes

1 Click here ■ to display **Network** properties.

2 In the **Network Protocol** list, click **TCP/IP Protocol**, and then click **Properties**.

3 Click the **DNS** tab.

4 Optionally, type a name in the **Host Name** box.

5 Optionally, type a name in the **Domain Name** box.

6 Under **DNS Server Search Order**, click **Add**.

If you are using DHCP, it may already be set up to automatically configure the **DNS Server Search Order**. Contact your network administrator to find out if this is the case.

If you are not using DHCP, or DHCP is not set up to provide this information, type the IP address of the DNS server that will provide name resolution, and then click **Add** to move the address to the **DNS Server Search Order** box.

7 Under **Domain Suffix Search Order**, click **Add**, type the DNS domain suffix to append to host names during name resolution, and then click **Add** to move the suffix to the **Domain Suffix Search Order** box.

Notes

- The settings take effect after you restart the computer.
- You can add up to three IP addresses for DNS servers. The servers running DNS will be queried in the order listed. To change the order in which they appear, click an address to move, and then click **Up** or **Down**. To remove an IP address, click it, and then click **Remove**.
- You can add up to six DNS domain suffixes. The suffixes will be appended in the order listed. To change the order in which they appear, select a suffix to move, and then click **Up** or **Down**. To remove a domain suffix, click it, and then click **Remove**.

{button ,AL("ToConfigureTCPIPManually;ToInstallaDNSServer")} Related Topics

Preliminary Notes

Although TCP/IP uses IP addresses to identify and reach computers, most users prefer to use names. Windows Internet Name Service (WINS) is a dynamic naming service that resolves NetBIOS computer names to IP addresses.

Typically, DHCP automatically configures your computer for WINS. To find out whether you should manually configure your computer to use WINS, contact your network administrator.

To Configure TCP/IP to Use WINS (and Broadcast Name Resolution)

Preliminary Notes

1. Click here ■ to display **Network** properties.
2. In the **Network Protocol** list, click **TCP/IP Protocol**, and then click **Properties**.
3. Click the **WINS Address** tab.
4. In the **Adapter** list, select the network adapter for which you want to set WINS addresses.
5. In the **Primary WINS Server** box, and, optionally, the **Secondary WINS Server** box, type IP addresses.

   Repeat this process to specify primary and secondary WINS servers for each network adapter. If addresses are not provided for WINS servers, Windows NT uses name query broadcasts plus the local LMHOSTS file to resolve computer names to IP addresses. Broadcast resolution is limited to the local network.
6. If you want to use DNS for name resolution on Windows networks and you want to have DNS Support in UNC Names., select the **Enable DNS for Windows Name Resolution** check box.

   If this check box is selected, Windows NT finds the DNS server by using the IP address specified in the **DNS** dialog box, as described in To Configure TCP/IP to Use DNS.
7. If you want to use the LMHOSTS file for NetBIOS name resolution on Windows networks, select the **Enable LMHOSTS Lookup** check box, and then click **Import LMHOSTS** and specify the folder for the LMHOSTS file you want to use.

   By default, Windows NT uses the LMHOSTS file found in the %SystemRoot%\System32\Drivers\Etc folder.
8. If your internetwork uses NetBIOS over TCP/IP and has its own scope identifier, type the scope identifier in the **Scope ID** box.

   To communicate with each other, all computers on a TCP/IP internetwork must have the same scope ID. Usually this value is left blank. A scope ID may be assigned to a group of computers that will only communicate with each other. Such computers can find each other if their scope IDs are identical. Scope IDs are used only for communication based on NetBIOS over TCP/IP.

Note

- The settings take effect after you restart the computer.

{button ,AL("ToConfigureTCPIPManually;ToInstallaWINSServer")} Related Topics

To Install the DHCP Relay Agent Service

1 Click here ■ to display **Network** properties

2 Click **Add**.

3 In the **Network Service** list, click **DCHP Relay Agent**, and then click **OK**.

4 Type the full path to the Windows NT distribution files and click **Continue**.

All necessary files are copied to your hard disk.

5 Continue with To Configure a DHCP Relay Agent.

Notes

- The settings take effect after you restart the computer.
- The DHCP Relay Agent service is only available on Windows NT Server.

Preliminary Notes

If you have routers separating your DHCP clients from your DHCP servers, and it is neither practical nor possible to configure your routers for DHCP/BOOTP relay, you can configure a Windows NT Server computer on the DHCP clients' network to be a DHCP relay agent.

A DHCP relay agent intercepts DHCP (and BOOTP) broadcast messages and sends the packets directly to the DHCP server. These directed messages can cross IP routers. In this way, a DHCP relay agent acts as a local proxy for the remote DHCP servers.

DHCP/BOOTP relay agents are defined in Request for Comment (RFC) 1542.

To Configure a DHCP Relay Agent

Preliminary Notes

1 Click here ■ to display **Network** properties.

2 In the **Network Protocol** list, click **TCP/IP Protocol**, and then click **Properties**.

3 Click the **DHCP Relay** tab.

4 To change the value in the **Seconds threshold** box, click it and type in a new value or click the arrows to select a new value.

The default value is four.

5 To change the value in the **Maximum Hops** box, click it and type in a new value or click the arrows to select a new value.

The default value is four.

6 Under **DHCP Servers**, click **Add**.

7. In the **Domain Server** box, type the IP address of a server to which you want to relay DHCP messages, and then click **Add** to move the address to the DHCP Servers list.

Repeat this process for any additional server addresses.

8 When you are done setting DHCP relay options, click **OK**.

If you have not already installed the DHCP Relay Agent service, you will be prompted to do so now.

9 Continue with To Install the DHCP Relay Agent Service.

Notes

- If you are installing and configuring a DHCP relay agent, the settings take effect after you restart the computer.
- If you are just reconfiguring a DHCP relay agent, the changes take effect immediately without restarting the computer.
- To make changes to an entry in the DHCP Servers list, click it, and then click **Edit**.
- To delete an entry in the DHCP Servers list, click it, and then click **Remove**.

Preliminary Notes

IP forwarding (routing) allows a multihomed computer running Windows NT to participate with other static routers on a network. You should select this option if you have two or more network cards and your network uses static routing, which also requires the addition of static routing tables. For information about creating static routing tables, see the Route command.

This option is not available if your computer has only one network adapter and one IP address. Also, this option does not support routers running the Routing Information Protocol (RIP).

To Configure a Multihomed Computer for IP Routing

Preliminary Notes

1. Click here ■ to display **Network** properties.
2. Click **TCP/IP Protocol**, click **Properties**, and then click the **Routing** tab.
3. To turn on static routing, click **Enable IP Forwarding**.

Note

- The settings take effect after you restart the computer.

To Install and Configure the FTP Server Service

The FTP Server Service is now part of the Internet Information Server (IIS).

For information about installing and configuring an FTP Server, see the *Microsoft Internet Information Server Installation and Planning Guide*. If you do not have a printed copy of this guide, you can find it on the World Wide Web at:

http://www.microsoft.com/infoserv/docs/iisdocs.htm

TCP/IP Reference

For detailed technical information, refer to the following texts and articles:

Allard, J. "DHCP--TCP/IP Network Configuration Made Easy," *ConneXions*, Volume 7, No. 8, August 1993.

Allard, J., K. Moore, and D. Treadwell. "Plug into Serious Network Programming with the Windows Sockets API," *Microsoft Systems Journal,* July: 35 - 40, 1993.

Comer, D. *Internetworking with TCP/IP Volume 1: Principles, Protocols, and Architecture*. Third edition. Englewood Cliffs, NJ: Prentice Hall, 1995.

Comer, D. and D. Stevens. *Internetworking with TCP/IP Volume II: Design, Implementation, and Internals*. Englewood Cliffs, NJ: Prentice Hall, 1991.

Comer, D. and D. Stevens. *Internetworking with TCP/IP Volume III: Client-Server Programming and Applications*. Englewood Cliffs, NJ: Prentice Hall, 1991.

Genty, M. "Microsoft Windows NT from a Unix Point of View," *A White Paper from the Business Systems Technology Series,* September 1995.

Hall, M., et al. *Windows Sockets: An Open Interface for Network Programming Under Microsoft Windows*, Version 1.1, Revision A, 1993.

Krol, E. *The Whole Internet User's Guide and Catalog*. O'Reilly and Associates, 1992.

MacDonald, D. "Microsoft Windows NT 3.5/3.51: TCP/IP Implementation Details," *A White Paper from Corporate Network Systems and the Business Systems Division,* September 1995.

Rose, M.T. *The Simple Book*. Englewood Cliffs, NJ: Prentice Hall, 1991.

Stevens, W.R. *TCP/IP Illustrated Volume 1: The Protocols*. Reading, MA: Addison-Wesley, 1994.

Under Construction

THIS TOPIC IS CURRENTLY UNDER CONSTRUCTION.

Preliminary Notes

You need to know the following information before you install the Simple Network Management Protocol (SNMP) service on your computer:

- Community names in your network.
- Trap destinations for each community.
- IP addresses and computer names for SNMP management hosts.

To Install SNMP

Preliminary Notes

1 Click here ■ to display **Network** properties.

2 Click **Add**.

The **Select Network Service** dialog box appears.

3 In the **Network Service** list, click **SNMP Service**, and then click **OK**.

4 Type the full path to the Windows NT distribution files and click **Continue**.

After the necessary files are copied to your computer, the **Microsoft SNMP Properties** dialog box appears.

5 Continue with To Configure SNMP.

{button ,AL("A_ConfigureSNMP")} Related Topics

To Configure SNMP

1 In the **Microsoft SNMP Properties** dialog box, which appears automatically after the SNMP Service software is installed on your computer, click **SNMP Service**, and then click **Properties**.

Or, if you are reconfiguring SNMP, click here ■ to display **Network** properties, click **SNMP Service**, and then click **Properties**.

2 On the **Agent** tab, enter the appropriate Agent information (such as comments about the user, location, and services).

3 On the **Traps** tab, enter the appropriate information (such as community names and trap destinations).

4 On the **Security** tab, enter the appropriate information (such as allowable community and host names).

Note

■ If you are installing and configuring SNMP, the settings take effect after you restart the computer. If you are reconfiguring SNMP, the changes take effect immediately without restarting the computer.

{button ,AL("A_ConfigureSNMP;ToInstallSNMP;ToInstallSNMP")} Related Topics

Preliminary Notes

SNMP agent information allows you to specify comments about the user and the physical location of the computer. You can also indicate the types of service to report, which are based on the computer's configuration.

To Configure SNMP Agent Information

Preliminary Notes

1 Click here ■ to display **Network** properties, click **SNMP Service**, and then click **Properties**.

2 Click the **Agent** tab.

3 In the **Contact** box, type the computer user's name.

4 In the **Location** box, type the computer's physical location.

5 In the **Service** box, select all check boxes that indicate network capabilities provided by your Windows NT computer.

SNMP must have this information to manage the enabled services.

Note

- The settings take effect immediately. You do not need to restart the computer.

Other Considerations

{button ,AL("ToConfigureSNMP")} Related Topics

Other Considerations

If you have installed additional TCP/IP services (such as a bridge or router), you should consult RFC 1213 for additional information.

Preliminary Notes

The SNMP traps configuration identifies communities and trap destinations:

- *Communities* are groups of hosts to which a server running the SNMP service belongs. You can specify one or more communities to which the Windows NT computer that uses SNMP sends traps. The community name is placed in the SNMP packet when the trap is sent.

  When the SNMP service receives a request for information that does not contain the correct community name or match an accepted host name for the service, the SNMP service can send a trap to the trap destination(s), indicating that the request failed authentication.

- *Trap destinations* are the names or IP addresses of hosts to which you want the SNMP service to send traps with the selected community name.

If you want to use SNMP for statistics, but do not care to identify communities or traps, specify Public as the community name when you configure the SNMP service. Typically, all hosts belong to Public, which is the standard name for the common community of all hosts.

To Configure SNMP Traps

Preliminary Notes

1 Click here ■ to display **Network** properties, click **SNMP Service**, and then click **Properties**.

3 Click the **Traps** tab.

4 To identify each community to which you want this computer to send traps, type the name in the **Community Name** box.

Community names are case sensitive.

5 After typing each name, click **Add** to add the name to the list.

6 To specify hosts for each community you send traps to, after you have added the community and while it is still highlighted, click **Add** under **Trap Destination**.

7 To move the name or address to the **Trap Destination** list for the selected community, type the host name in the **IP Host/Address or IPX Address** box, and then click **Add.**

Repeat this process for any additional hosts.

Notes

- The settings take effect immediately. You do not need to restart the computer.
- To make changes to an entry in a list, click it, and then click **Edit**.
- To delete an entry from a list, click it, and then click **Remove**.

{button ,AL("ToConfigureSNMP")} Related Topics

Preliminary Notes

SNMP Security allows you to specify the communities and hosts a computer will accept requests from, and to specify whether to send an authentication trap when an unauthorized community or host requests information.

To Configure SNMP Security

Preliminary Notes

1 Click here ■ to display **Network** properties, click **SNMP Service**, and then click **Properties**.

2 Click the **Security** tab.

3 If you want to send a trap for failed authentications, select the **Send Authentication Trap** check box.

4 Under **Accepted Community Names**, click **Add**.

5 In the **Community Names** box, type a community name from which you will accept requests.

6 To move the name to the **Accepted Community Names** list, click **Add**.

Repeat this process for any additional community name.

7 To specify whether to accept SNMP packets from any host or from only specified hosts, click one of two options:

- **Accept SNMP Packets From Any Host**, if no SNMP packets are to be rejected on the basis of source computer ID.
- **Only Accept SNMP Packets From These Hosts**, if SNMP packets are to be accepted only from the computers listed. To designate specific hosts, click **Add,** type the names or addresses of the hosts from which you will accept requests in the **IP Host or IPX Address** box, and then click **Add** to move the name to the **Only Accept SNMP Packets From These Hosts** list.

Repeat this process for any additional hosts.

8 On the **Agent** tab, specify the appropriate information (such as comments about the user, location, and services).

Notes

- The settings take effect immediately. You do not need to restart the computer.
- Typically, all hosts belong to Public, which is the standard name for the common community of all hosts.
- To make changes to an entry in a list, click it, and then click **Edit**.
- To delete an entry from a list, click it, and then click **Remove**.

{button ,AL("ToConfigureSNMP;ToConfigureSNMPAgentInformation")} Related Topics

To Start or Stop the SNMP Service

1 Click here ■ to display **Services** properties.

2 In the **Service** list, click **SNMP**, click **Start** or **Stop**, and then click **Close**.

Note

- If you are adding new extensions to SNMP, you must stop and restart the service for the changes to take effect.

{button ,AL("ToInstallSNMP")} Related Topics

To Install a DHCP Server

1 Click here ■ to display **Network** properties.

2 Click **Add**.

3 In the **Network Service** list, click **Microsoft DHCP Server**, and then click **OK**.

4 Type the full path to the Windows NT distribution files, and click **Continue**.

All necessary files are copied to your hard disk.

5 Continue with To Configure TCP/IP Manually.

Note

- All the appropriate DHCP software will be ready for use after you restart the computer.

Other Considerations

{button ,AL("A_InstallDHCPserver")} Related Topics

Other Considerations

You cannot use DHCP to configure a new DHCP server, because a DHCP server is always described only by its IP address.

After you install a DHCP server, you must use DHCP Manager to perform these basic tasks:

- Define DHCP scopes. Add the DHCP server to a DHCP scope to gain the information needed to begin providing DHCP services. Define properties for the scope, including the IP address ranges to be distributed to potential DHCP clients by servers in the scope.
- Configure DHCP option types. Define default values for options such as lease duration, or create any custom options.

To Start the DHCP Manager

- Click **Start,** point to **Programs**, then to **Administrative Tools (Common)**, and then click **DHCP Manager**.

Note

- For information about how to use DHCP Manager, see the DHCP Manager Help.

{button ,AL("A_InstallDHCPserver")} Related Topics

To Start or Stop the DHCP Service

1 Click here ■ to display **Services** properties.

2 In the **Service** list, click **Microsoft DHCP Server**, click **Start**, **Stop**, **Pause** or **Continue**, and then click **Close**.

Note

- You can also start and stop the DHCP Server service at the command prompt using the commands **net start dhcpserver**, **net stop dhcpserver**, **net pause dhcpserver**, or **net continue dhcpserver**.

{button ,AL("A_InstallDHCPserver")} Related Topics

To Install a WINS Server

1 Click here ■ to display **Network** properties.

2 Click **Add**.

3 In the **Network Service** list, click **Windows Internet Name Service**, and then click **OK**.

4 Type the full path to the Windows NT distribution files and click **Continue**.

All necessary files are copied to your hard disk.

5 Continue with To Configure TCP/IP Manually.

Note

- All the appropriate WINS software will be ready for use after you restart the computer.

Other Considerations

{button ,AL("A_InstallWINSserver")} Related Topics

Other Considerations

- A computer running the WINS server should be assigned a fixed IP address.
- The WINS server computer should not be a DHCP client.
- If the WINS server computer has more than one network adapter card, make sure the binding order of IP addresses is not disturbed.
- After you install a WINS server, you use WINS Manager to configure the WINS service.

To Start the WINS Manager

- Click **Start**, point to **Programs**, then to **Administrative Tools (Common)**, and then click **WINS Manager**.

Note

- For information about how to use WINS Manager, see the WINS Manager Help.

{button ,AL("A_InstallWINSserver")} Related Topics

To Start or Stop the WINS Service

1 Click here ■ to display **Services** properties.

2 In the **Service** list, click **Windows Internet Name Service**, click **Start**, **Stop**, **Pause** or **Continue**, and then click **Close**.

Note

■ You can also start and stop the WINS Server service at the command prompt using the commands **net start wins**, **net stop wins**, **net pause wins**, or **net continue wins**.

{button ,AL("A_InstallWINSserver")} Related Topics

DNS Server Service Overview

Windows NT Server includes an RFC-compliant, Domain Name System (DNS) name server. DNS is primarily a distributed database of host information. DNS name servers resolve computer names to IP address mapping queries. These queries originate either from client computers, known as *resolvers*, or other DNS name servers. It is the latter that accounts for the distributed nature of DNS.

You can configure the Windows NT DNS name server to use WINS for host name resolution. This integration allows for a form of *Dynamic DNS* that takes advantage of the best features of both DNS and WINS. DNS resolves the upper layers of the domain name and passes the final resolution to WINS. This final WINS resolution is transparent to the client computer.

Note that the Workstation service is the component responsible for registering a computer’s name with WINS. By default, the Workstation service is started automatically when the computer starts. In general, you should leave this setting alone. If you turn it off on a computer, it will no longer be possible for the DNS server to resolve that computer’s name with a WINS lookup.

For more information about Microsoft DNS, see the *Microsoft Windows NT Server Networking Supplement.* For in-depth coverage of DNS in general, see *DNS and BIND* by Paul Albitz and Cricket Liu, published by O’Reilly and Associates.

Determining Whether You Should Maintain a DNS Server

In many cases, you do not need to maintain a DNS server. If you have a small network, or a single network rather than an internetwork, you will probably find it simpler and more effective to have the DNS client software query a nearby DNS server, such as the one maintained by your Internet service provider. Most providers will maintain your domain information for a fee.

You will want to provide your own DNS server if you have your own domain on the Internet or if you want to access DNS from your LAN, rather than going through your Internet provider.

If you do maintain a DNS server, you will probably want to assign the task to at least two computers: a primary and a secondary name server. Data should be replicated from the primary name server to the secondary name server. This lets the Internet-wide DNS locate computers on your network even if one of the name servers is down. How often you schedule replication will depend on how often names change in your domain. Replicate often enough that changes are known to both servers. Excessive replication can tie up your network and servers unnecessarily.

To Upgrade a Windows NT 3.51 Resource Kit DNS Server

1 On the **Start** menu, click **Run**.

2 Type **regedt32** and click **OK**.

3 In the **Local Machine** dialog box, click **HKEY_LOCAL_MACHINE**.

4 Double-click the System folder, then the CurrentControlSet folder, and then the Services folder.

5 Click the DNS folder.

6 On the **Edit** menu, click **Delete**.

7 Double-click the EventLog folder, and then the System folder.

8 Click the DNS folder, and, on the **Edit** menu, click **Delete**.

9 Continue with To Install a DNS Server.

Other Considerations

{button ,AL("ToInstallaDNSServer")} Related Topics

Other Considerations

When you install the new Windows NT Server 4.0 DNS Server, it will not replace your existing BOOT and CACHE files. If you want new copies of these files, rename or move your old ones before beginning the installation procedure.

To Install a DNS Server

1 If you are upgrading an existing DNS name server from the Windows NT 3.51 Resource Kit, you will need to remove some Registry entries before installing the Windows NT Server 4.0 DNS Server.

2 Click here ■ to display **Network** properties.

3 Click **Add**.

4 In the **Network Service** list, click **Microsoft DNS Server**, and then click **OK**.

5 Type the full path to the Windows NT distribution files, and click **Continue**.

All necessary files are copied to your hard disk.

6 If you are migrating your existing DNS name server to Windows NT Server, copy your DNS database files—zone files, reverse-lookup files, cache file—to the %SystemRoot%\System32\DNS folder.

Note

- The DNS server software is ready for use when you restart the computer.

Other Considerations

{button ,AL("A_InstallDNSManager;ToUpgradeaWindowsNT351ResourceKitDNSServer")} Related Topics

Other Considerations

At this point you should decide how you will administer your DNS name servers. You can use a text editor to make changes to the DNS database files (as is done under UNIX), or you can use Windows NT DNS Manager, which is a graphical, RPC-based tool similar to the WINS Manager and DHCP Manager tools. DNS Manager significantly simplifies maintenance of the DNS database files and should be used in most circumstances.

Note that DNS Manager stores the DNS Boot file information in the Windows NT Registry. Once you begin using DNS Manager, the Boot file in the %SystemRoot%\System32\DNS folder is no longer used. Once you begin using DNS Manager, do not switch back to manually editing the DNS database files.

If you remove and reinstall DNS Server it will not replace your existing BOOT and CACHE files. If you want new copies of these files, rename or move your old ones prior to reinstalling DNS Server.

To Start the DNS Manager

- Click **Start,** point to **Programs**, then to **Administrative Tools (Common)**, and then click **DNS Manager**.

Note

- For information about how to use DNS Manager, see the DNS Manager Help.

{button ,AL("A_InstallDNSManager")} Related Topics

To Start or Stop the DNS Service

1. Click here ■ to display **Services** properties.
2. In the **Service** list, click **Microsoft DNS Server**, click **Start**, **Stop**, **Pause** or **Continue**, and then click **Close**.

Note

■ You can also start and stop the DNS Server service at the command prompt using the commands **net start dns**, **net stop dns**, **net pause dns**, or **net continue dns**.

{button ,AL("A_InstallDNSManager")} Related Topics

Registering with Your DNS Parent Domain

Once you have installed and configured your DNS server or servers, you need to register with the DNS server that is above you in the hierarchical naming structure of DNS. The parent system needs the name and addresses of your name servers, and will probably want other information such as the date that the domain will be available and the names and addresses of contact people.

If you are registering with a parent below the second level, check with the administrator of that system to find out what information you need to supply and how to submit it.

DNS Support in UNC Names

The Windows Uniform Naming Convention (UNC) now supports DNS domain names. UNC names take the form \\server\sharepoint. Previously, the server portion was the NetBIOS computer name of the server on which the sharepoint was located.

You can now use a DNS domain name or IP address in the server portion of the UNC name. For example, \\Tsunami.widgets.com\public is the name for the public folder on the machine named tsunami in the Widgets.com DNS domain. If the IP address for Tsunami.widgets.com is 138.57.27.7, then \\138.57.27.7\public and \\Tsunami.widgets.com\public represent the same name.

To enable DNS support in UNC names, you must enable DNS for Windows Resolution. For more information, see To Configure TCP/IP to Use WINS.

Introduction to TCP/IP Utilities

The Windows NT TCP/IP utilities provide diagnostic and connectivity tools for connecting to other systems, network administration, and troubleshooting.

To get help on TCP/IP utilities

- At the command prompt, type a TCP/IP utility name, followed by **-?**. For example, type **ping -?**

Note

- The **ftp, ftpsvc, rexec, and telnet** utilities all rely on password authentication by the remote computer. These utilities pass the user's account name and password over the network in clear text.

  Because a user equipped with a network analyzer could steal a user's remote account password, users of these utilities should not use the same password to log onto Windows NT as the one used to log onto networks that are not secure. Logon credentials used by Windows NT, Windows 95, Windows for Workgroups, and Microsoft LAN Manager networks are always encrypted before they are sent over the network.

TCP/IP Utilities

arp

finger

ftp

hostname

ipconfig

lpq

lpr

nbtstat

netstat

nslookup

ping

rcp

rexec

route

rsh

tftp

tracert

TCP/IP Services

```
net start lpdsvc
net start snmp
net start "simple tcp/ip services"
net start "tcp/ip netbios helper"
```

Diagnostic Utilities Reference

arp

hostname

ipconfig

nbtstat

netstat

ping

tracert

Preliminary Notes

If you have trouble installing Microsoft TCP/IP on your computer, follow the suggestions in the error messages. You can also use the **ping** utility to isolate network hardware problems and incompatible configurations, allowing you to verify a physical connection to a remote computer. You can also use **ping** to test both the computer name and the IP address of the computer.

To Test TCP/IP Using Ping

Preliminary Notes

1 If the computer was configured using DHCP, use **ipconfig** to get the IP address.

2 To check the loopback address, type **ping 127.0.0.1** at the command prompt.

The computer should respond immediately.

3 To determine whether you configured IP properly, use **ping** with the IP address of your computer, your default gateway, and a remote host.

Note

- If **ping** is not found or the command fails, check the event log with Event Viewer and look for problems reported by Setup or the TCP/IP service.

What’s Next

If Ping Fails

If Ping Succeeds but Net Use Fails

If the IP Address Responds but the Computer Name Does Not

If Ping Fails

If you cannot use **ping** successfully at any point, verify the following:

- The computer was restarted after TCP/IP was installed and configured.
- The local computer’s IP address is valid and appears correctly in the **TCP/IP Configuration** dialog box.
- The IP address of the default gateway and remote host are correct.
- IP routing is enabled and the link between routers is operational.

If Ping Succeeds but Net Use Fails

If you can use **ping** to connect to other Windows NT computers on a different subnet, but cannot connect through Explorer or with **net use** \\server\share, verify the following:

- The computer is WINS-enabled (if the network includes WINS servers).
- The WINS server addresses are correct, and the WINS servers are functioning.
- The correct computer name was used.
- The target host uses NetBIOS. If not, you must use FTP or Telnet to make a connection; in this case, the target host must be configured with the FTP server service or Telnet server service, and you must have correct permissions on the target host.
- The scope ID on the target host is the same as the local computer.
- A router exists between your system and the target system.
- LMHOSTS contains correct entries, so that the computer name can be resolved.

If the IP Address Responds but the Computer Name Does Not

If the IP address responds but the computer name does not, you have a name resolution problem. In this case, consult the following lists of common problems in name resolution to find a solution.

If You Are Using HOSTS or DNS

If You Are Using LMHOSTS or WINS

If You Are Using HOSTS or DNS

Some of the common problems associated with this type of name resolution are as follows:

- The HOSTS file or DNS do not contain the particular host name.
- The host name in the HOSTS file or in the command is misspelled or uses different capitalization. (Host names are case sensitive.)
- An invalid IP address is entered for the host name in the HOSTS file.
- The HOSTS file contains multiple entries for the same host on separate lines.
- A mapping for a computer name-to-IP address was mistakenly added to the HOSTS file (rather than LMHOSTS).

If You Are Using LMHOSTS or WINS

Some of the common problems associated with this type of name resolution are as follows:

- The LMHOSTS file does not contain an entry for the remote server.
- The computer name in LMHOSTS is misspelled. (Note that LMHOSTS names are converted to uppercase.)
- The IP address for a computer name in LMHOSTS is not valid.