However, the proxy agent cannot be run on a computer that is also a WINS server. Consult with the network administrator to determine whether your computer should be configured as a WINS proxy agent, as ~~only~~oniy a few computers on each subnetwork should be configured for this feature.

~~11~~. When you are done setting advanced options, choose the OK button. When the TCP/IP Configuration dialog box reappears, choose the OK button. When the Network Settings dialog box reappears, choose the OK button to complete advanced TCP/IP configuration.

You must restart the computer for the changes to take effect.

. . . . l
|9n¢¢ wan:m1=mr.. ~- - -- -- --~~----~ ---~~ "7."* ----~-- -,;*..*
"""""""--"":: " --- i ,~ ..=a mmw- "WM w~¢=#\wrwmu~==~1= ws#=
_fiend Trap with Community Hamas
Egmmunity Names
lrap Destination fm engineering
IP HnstfhddIeee or
MP1-"El1'& fpyq hddress
Installing and Configuring Microsoft TCP/IP and SNMP 9 of13

Configuring SNMP

The SNMP service is installed when you check the SNMP Service option in the Windows ~~NTTCP!IP~~NT TCP/lP Installation Options dialog box. After the SNMP service software is installed on your computer, you must configure it with valid information for SNMP to operate.

You must be logged on as a member of the Administrators group for the local computer to configure SNMP.

The SNMP configuration information identifies communities and trap destinations.

~~1~~

~~Acommunity~~A Community is a group of hosts to which a Windows ~~NTcomputer~~NT computer running the SNMP service belongs. You can specify one or more communities to which the Windows ~~NTcomputer~~NT computer using SNMP will send 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 and does not match an accepted host name for the service, the SNMP service can send ~~atrap~~a trap to the trap destination(s), indicating that the request failed authentication.

~~1~~l 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~~.~~,

You might want to use SNMP for statistics, but may not care about identifying communities or

traps. In this case, you can specify the "public" community name when you
configure the
SNMP service.
~~.,..~~To configure the SNMP service
1. Start the Network option in Control Panel to display the Network Settings
dialog box. ~~In~~ln the
Installed Network Software list box, select SNMP Service, and choose the
Configure
button. The SNMP Service Configuration dialog box appears.
~~SNMP Service Configuratmn~~
~~-end Trap with eo unity N ,~~
~~01 J~~
~~-I<·Add.1~~
~~Ie.ne.-·· I~~
~~L__j IRIIIIM·>I~~
~~Is- I~~
~~1rap Destination for engineering----------, IP Host/Address or IAaeaL,.J iPX~~
~~Address~~
~~I<·AIM I I a●. I~~
~~IR. .. >1~~
~~Chapter 2 Installing and Configuring Microsoft TCPnP and SNMP~~

~~2.~~ . To identify each community to which you want this computer to send traps,
type the name
in the Community Names box. After typing each name, choose the Add button to
move the
name to the Send Traps With Community Names list on the left.
Typically, all hosts belong to public, which is the standard name for the
common
community of all hosts. To delete an entry in the list, select it and choose
the Remove
button.
Note
Community names are case sensitive.
~~3.~~ . To specify hosts for each community you send traps to, after you have
added the
community and while it is still highlighted, type the hosts in the ~~1P~~IP
Host/Address Or IPX
Address box. Then choose the Add button to move the host name or ~~1P~~IP address
to the
Trap Destination for the ~~selected~~se/ecfed community list on the left.
You can enter a host name~~,~~. its ~~1P~~IP address~~,~~. or its ~~1PX~~IPX address.
To delete an entry in the list, select it and choose the Remove button.
~~4.~~
. To enable additional security for the SNMP service, choose the Security
button. Continue
with the configuration procedure, as described in the next section,
"Configuring SNMP
Security."

~~5.~~
. To specify Agent information (comments about the user, location, and
services), choose

the Agent button. Continue with the configuration procedure, as described in "Configuring
SNMP Agent Information" later in this chapter.

~~6.~~
. When you have completed ~~all~~atl procedures, choose the OK button. When the Network
Settings dialog box reappears, choose the OK button.
The Microsoft SNMP service has been configured and is ready to start. lt is not necessary
to reboot the computer.

8 Send fxglhentiealion Trap
-heeepted Community jiames
Cobrglmunity Name
'O Ageept SNMP Packete from Any Host
-Lil" .Qnly .¢|.¢;:c:&pt SHHP Packets fmm These Hosts:
[F Hestfhddress or
IPX Address:
ublic
=JiL1|li[" mm- g
11.101.41.121
Installing and Configuring Microsoft TCP/IP and SNMP 10<>f13
Configuring SNMP
Configuring SNMP Security
SNMP security allows you to specify the communities and hosts ~~acomputer~~a computer will accept
requests from, and to specify whether to send an authentication trap when an unauthorized
community or host requests information.
~~llJJ>~~
To configure SNMP security
1. Start the Network option in Control Panel to ~~display~~dispiay the Network Settings dialog box. In the
Installed Network Software list box, select SNMP Service and choose the Configure button~~.~~
2. In the SNMP Service Configuration dialog box, choose the Security button.

~~SNMP Security Configuration~~
~~[81 Send Aythenlication TI ap~~
~~Accepted c ,ll I !! I~~
~~pt.dic I <;l!;j COWIIII'itJN- I c.IW-~~
~~io.;jff,l L J I •. . .:j~~

~~0 -SNMP Packeta hu. Ant Hoal~~
~~j® !1.111, Accept SNMP Packets hu. These Hoala:~~
~~IP HOatJAddleaa 111 fPX Addlrm:~~
~~I <·lt.d~~
~~(11.101.41.1- IIRjjijt~~
3. If you want to send a trap for failed authentications, select the Send ~~Authentication~~Autnentication Trap
check box in the SNMP Security Configuration dialog box.

~~Chapter 2 Installing and Configuring Microsoft TCPnP and SNMP~~
4. In the Community Name box, type the community names you will accept requests from~~.~~
Choose the Add button ~~atler~~after typing each name to move the name to the Accepted
Community Names list on the left.
~~Ahost~~A host must belong to a community that appears on this list for the SNMP service to accept
requests from that host. Typically, all hosts belong to public, which is the standard name
for the common community of all hosts. To delete an ~~entry~~ently in the list, select it and choose
the Remove button.

~~5.~~
. Select an option to specify whether to accept SNMP packets from any host or from only
specified hosts.
~~1~~' If the Accept SNMP Packets From Any Host option is selected, no SNMP packets are
rejected on the basis of source host ID. The list of hosts under Only Accept SNMP
Packets From These Hosts has no effect.
~~1~~
~~If~~' lf the Only Accept SNMP Packets From These Hosts option is selected, SNMP
packets will be accepted only from the hosts listed. In the ~~1P~~IP Host/Address Or IPX
Address box, type the host names, ~~1P~~IP addresses, or IPX addresses of the hosts from
which you will accept requests. Then choose the Add button to move the host name or
IP address to the list box on the left. To delete an entry in the list, select it and choose
the Remove button.
~~6.~~
. Choose the OK button. The SNMP Service Configuration dialog box reappears.
To specify Agent information (comments about the user, location, and services), choose
the Agent button. Continue with the configuration procedure, as described in the next
section.

~~7.~~
. After you complete all procedures, choose the OK button. When the Network Settings
dialog box reappears, choose the OK button.
The Microsoft SNMP service and SNMP security have been configured and are ready to
start. You do not need to reboot the computer.

-nn-n-4
Qnntact:
Location:
' S ewice

Ehysical _Qatalink .»" Subnetwork
internet >< ind-tu-End
><: igpplicatiorzsi
. . .H. . . . .
Ernest Ayde|0He
Bldg. T, mum 823
Installing and Configuring Microsoft TCP/IP and SNMP 11 of13
Configuring SNNIP

Configuring SNMP Agent Information

SNMP agent ~~infonnation~~information allows you to specify comments about the user and the physical
location of the computer and to indicate the types of service to report. The types of service that
can be reported are based on the computer's configuration.

~~_ . ,~~ To configure SNMP agent information

~~1.~~ 1. Start the Network option in Control Panel to display the Network Settings dialog box. ~~In~~ln the
Installed Network Software list box, select SNMP Service and choose the Configure button.

2. In the SNMP Service Configuration dialog box, choose the Agent button.

~~SNMPAgent~~
.~~!;.ontact: IErnest Aydelotte • . J~~ i
~~.location: I8ldg. 7. 10011 823~~
~~I c..tl~~
~~SM- .~~
~~0 fhfsical 0 Jlatalink I Subnetwork u..w.:J~~
~~0 internet (81 [nd to E nd~~
~~(gl-J~~
~~_~~

3. In the SNMP Agent dialog box, type the computer user's name in the Contact box and the
computer's physical location ~~in~~ln the Location box. These are comments that will be used as
text and cannot include embedded control characters.

4. Select the services to report in the Service box. Check all boxes that indicate network
capabilities provided by your Windows NT computer. SNMP must ~~have~~nave this ~~infonnation~~information to
manage the enabled services.

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

Option Meaning
Physical Select this option if this Windows NT computer manages any
physical TCP~~+~~/IP device, such as a repeater.
Datalink/Subnetwork Select this option if this Windows NT computer manages a TCP~~+~~/IP
subnetwork or ~~datalink~~dataiink, such as a bridge.
~~Chapter 2 Installing and Configuring Microsoft TCPnP and SNMP~~
~~Option Meaning~~
Internet Select this option if this Windows NT computer acts as an ~~1P~~IP
gateway.
End-to-End Select this option if this Windows NT computer acts as an ~~1P~~IP
host.

This option should be selected for all Windows NT installations.
~~Applications Select this option if this Windows NT computer includes any applications that use TCP/IP, such as electronic mail. This option should be selected for all Windows NT installations.~~

~~5.~~. Choose the OK button.
~~6.~~. When the SNMP Service Configuration dialog box reappears, choose the OK button.
When the Network Settings dialog box reappears, choose the OK button.
SNMP is now ready to operate without rebooting the computer.
Applications Select this option if this Windows NT computer includes any applications that use TCP/IP, such as electronic mail. This option should be selected for all Windows NT installations.

Installing and Configuring Microsoft TCP/IP and SNMP 12 of13
Removing TCP/IP Components
If you want to remove the TCP/IP protocols or any of the services installed on a computer, use
the Network option in Control Panel to remove it.
When you remove any network software, Windows NT warns you that the action permanently
removes that component. You cannot reinstall ~~acomponent~~a component that has been removed until after
you restart the computer.
~~..,.~~To remove any TCP/IP component
~~1.~~1. In Control Panel, choose the Network option.
2. In the Installed Network Software list in the Network Settings dialog box, select the
component that you want to remove.
3. Choose the Remove button.

Installing and Configuring Microsoft TCP/IP and SNMP 1a0f13
Configuring RAS for Use with TCP/IP
Windows NT users who install Remote Access Service (RAS) for remote networking maintain
all the benefits of TCP/~~IP~~lP networking, including access to the WINS and DNS capabilities of
Microsoft TCP/IP. RAS clients can be configured to use Point to Point Protocol (PPP) or Serial
Line Internet Protocol (~~SLIP~~SLlP) to allow TCP/IP dial-up support for existing TCP/~~IP~~lP internetworks
and the ~~Internet~~internet. When PPP is configured on a Windows NT Remote Access server, it can
function as a router for RAS clients. ~~SLIP~~SLlP client software is provided to support older
implementations~~;~~, it does not support multiple protocols.
As with all network services, you install RAS by using the Network option in Control Panel.
During RAS installation and configuration, you can specify the network protocol settings to use
for RAS connections, which also allows you to specify TCP/IP configuration settings. When the
network administrator installs a Microsoft RAS server, IP addresses are reserved for use by

RAS clients.
Users with RAS client computers can use the Remote Access program to enter and maintain
names and telephone numbers of remote networks. RAS clients can connect to and
disconnect from these networks through the Remote Access program. You can also use the
Remote Access Phone Book application to select the network protocols to use for ~~aspecific ~~a specific
Phone Book entry. ~~1fTCP!~~If TCP/IP is installed, the Phone Book automatically selects TCP~~!~~/IP over
PPP as the protocol.
If a RAS client computer has a serial COM port, you can use the Remote Access Phone Book
application to configure SLIP for use with ~~aselected~~a selected Phone Book entry. If you configure a RAS
client computer to use the SLIP option, when you dial in for ~~aconnection~~a connection to the selected Phone
Book entry, the Terminal screen appears, and you can begin an interactive session with ~~aSLIP ~~a SLIP
server. When you use SLIP, Remote Access Phone Book bypasses user authentication. You
will not be asked for a ~~usemame~~username and password.
For complete information about setting up RAS servers and clients and using RAS with
Windows NT, see ~~Windows~~VW/vdows NT ~~Server~~Sen/er Remote Access Service.
~~CHAPTER 3~~

Networking Concepts for TCP/IP
~~!~~This chapter describes how TCP/IP fits in the Windows NT network architecture and explains
the various components of the ~~Internet~~internet Protocol suite and IP addressing. As part of the
discussion on name resolution in Windows networking, this chapter also describes NetBIOS
over TCP/IP and Domain Name System (DNS). For additional information about these topics,
see the books listed in ~~!!~~"Finding More ~~Information~~lnformation" in "Welcome~~.~~,"
~~!~~This chapter also provides conceptual information about ~~two~~tvvo key features for Microsoft TCP/IP:
Dynamic Host Configuration Protocol (DHCP) and Windows Internet Name Service (WINS).
~~!~~The ~~following~~foiiowing topics appear in this chapter:
~~•~~l TCP/IP and Windows NT networking
~~•~~' Internet protocol suite
~~•~~' IP addressing
~~•~~' Name resolution for Windows networking
~~•~~l SNMP

SIIIUP RPC
Windows So-ckas
Applications
Wiruziosna Sockets
Interface
Windows
HdB103 .Fhpplications
Haslos Intaface
naslos wer TCPJIP
i~
NDIS Ul'i\|El'S sun PPP
TCPIIP

The architecture of the Microsoft Windows NT operating system with integrated networking is
protocol-independent. This architecture, illustrated in the following figure, provides
Windows NT file, print, and other services over any network protocol that uses exports from
the TDI interface. The protocols package network requests for applications in their respective
formats and send the requests to the appropriate network adapter via the ~~network~~nefwork device
interface ~~.\pecification~~specification (NDIS) interface. The NDIS specification allows multiple network
protocols to reside over a wide variety of network adapters and media types.

~~Windows Windows Sockets NetBIOS Applications Applications~~
~~Windows SocketsNetBIOS Interface Interface~~
Transnort Deviw..
lmterface
Stardard
Tcpnp
Mcdules
~~Network~~Metxmork Driver
~~NDIS Drivers, SLIP, PPP~~
~~Interlace~~
Interface
~~Physical Network~~Phyafcel Tdatxmcrk Layer
Architectural Model of Windows NT with TCP/IP

Under the Windows NT transport-independent architecture, TCP/~~IP~~lP is a protocol family that can
be used to offer Windows networking capabilities. The TCP/~~IP~~lP protocol gives Windows NT,
Windows for Workgroups, and LAN Manager computers transparent access to each other and
allows communication with non~~-~~-Microsoft systems in the enterprise network.

~~Chapter 3~~ Networking Concepts for ~~TCPnP~~TCP/IP
~~Internet Protocol Suite~~
and Windows NT Networking
2of17

TCP/IP refers to the Internet suite of protocols. It includes a set of standards that specify how
computers communicate and gives conventions for connecting networks and routing traffic

through the connections.
The Internet protocols are a result of a Defense Advanced Research Projects
Agency
(DARPA) research project on network interconnection in the late ~~1970~~1970s.~~It~~
It was mandated on all
United States defense long-haul networks in 1983 ~~but was~~butwas not widely
accepted until it was
integrated with 4.2 Berkeley Software Distribution (BSD) UNIX. The popularity
~~ofTCP~~of TCP/IP is
based on: ~~1~~
Robust client-server framework. TCP/~~IP~~lP is an excellent client-server
application platform,
especially in wide-area network (WAN) environments.
~~1~~
~~Information~~l information sharing. Thousands of academic, military,
scientific, and commercial
organizations ~~share~~snare data, electronic mail, and services on the Internet
using TCP/IP.
~~1~~l General availability. Implementations ~~ofTCP~~of TCP/IP are available on
nearly every popular
computer operating system. Source code is widely available for many
implementations.
Vendors for bridges, routers, and network analyzers all offer support for the
TCP/IP
protocol suite within their products.
The following discussion introduces the components of the ~~IP~~lP protocol suite.
Some knowledge
of the architecture and interaction between TCP/IP components is useful for
both
administrators and users, but most of the details discussed here are
transparent when you are
actually using TCP/IP.
Networking Concepts for TCP/IP
Internet Protocol Suite
3of17

Internet Protocol Suite
Transmission Control Protocol and Internet Protocol
Transmission Control Protocol (TCP) and Internet Protocol (IP) are only two
members of the IP
protocol suite. IP is a protocol that provides packet delivery for all other
protocols within the
TCP/IP family. IP provides a best-effort, connectionless delivery system for
computer data.
That is, IP packets are not guaranteed to arrive at their destination, nor
are they guaranteed to
be received in the sequence in which they were sent. The protocol's checksum
feature
confirms only the IP header's integrity. Thus, responsibility for the data
contained within the IP
packet (and the sequencing) is assured only by using higher- level protocols.
Perhaps the most common higher-~~levelIP~~level IP protocol is TCP. TCP supplies
a reliable,

connection-based protocol over (or encapsulated within) IP. TCP guarantees the delivery of packets, ensures proper sequencing of the data, and provides ~~achecksum~~a checksum feature that validates both the packet header and its data for accuracy. ~~In~~ln the event that the network either corrupts or loses ~~aTCP~~a TCP/IP packet during transmission, TCP is responsible for retransmitting the faulty packet. This reliability makes TCP/IP the protocol of choice for session-based data transmission, client-server applications, and critical services such as electronic mail.

This reliability has a price. TCP headers require the use of additional bits to provide proper sequencing of information, as well as a mandatory checksum to ensure reliability of both the TCP header and the packet data. To guarantee successful data delivery, the protocol also requires the recipient to acknowledge successful receipt of data.

Such acknowledgments (or ~~ACK.s~~ACKS) generate additional network traffic, diminishing the level of data throughput in favor of reliability. To reduce the impact on performance, most hosts send an acknowledgment for every other segment or when an ACK timeout expires.

Networking Concepts for TCP/IP 4of17

Internet Protocol Suite

User Datagram Protocol

~~If~~lf reliability is not essential, User Datagram Protocol (UDP), ~~aTCP~~a TCP complement, offers a connectionless datagram service that guarantees neither delivery nor correct sequencing of delivered packets (much like ~~IP~~IP). Higher-level protocols or applications may provide reliability mechanisms in addition to UDP/IP. UDP data checksums are optional, providing a way to exchange data over highly reliable networks without unnecessarily consuming network resources or processing time. When UDP checksums are used, they validate both header and data. ~~ACKs~~ACKS are also not enforced by the UDP protocol~~;~~, this is left to higher-level protocols.

UDP also offers one-to-many service capabilities, because it can be either broadcast or multicast.

Networking Concepts for TCP/IP 50f17

Internet Protocol Suite

Address Resolution Protocol and Internet Control Message Protocol

Two other protocols in the IP suite perform important functions, although these are not directly related to the transport of data: Address Resolution Protocol (ARP) and ~~Internet~~internet Control

Message Protocol (ICMP). ARP and ~~ICMP~~ICMP are maintenance protocols that support the ~~IP~~IP framework and are usually invisible to users and applications.

IP packets contain both source and destination IP addresses, but the hardware address of the destination computer system must also be known. IP acquires a system's hardware address by broadcasting a special inquiry packet (an ARP ~~request packet~~requesfpackef) containing the IP address of the system with which it is attempting to communicate. ~~All~~Ali of the ARP-enabled nodes on the local IP network detect these broadcasts, and the system that owns the ~~IP~~IP address in question replies by sending its hardware address to the requesting computer system in an ARP reply packet. The hardware/IP address mapping is then stored in the requesting system's ARP cache for subsequent use. Because the ARP reply can also be broadcast to the network, it is likely that other nodes on the network can use this information to update their own ARP caches. (You can use the arp utility to view the ARP tables.)

~~Chapter 3 Networking Concepts for TCPnP~~

ICMP allows two nodes on an IP network to share IP status and error information. This information can be used by higher-level protocols to recover from transmission problems or by network administrators to detect network trouble. Although ICMP packets are encapsulated within IP packets, they are not considered to be a higher~~-~~-level protocol (ICMP is required in every TCP/IP implementation). The ping utility makes use of the ICMP echo ~~request~~requesf and echo reply packets to determine whether a particular IP node (computer system) on a network is functional. This is useful for diagnosing IP network or gateway failures.

Networking Concepts for TCP/IP 6of17

~~IP Addressing~~

~~Ahost~~A host is any device attached to the network that uses TCP/IP. To receive and deliver packets ~~successfully~~ successfuily between hosts, TCP/IP ~~relies~~reiies on three pieces of information that the user provides: IP address, subnet mask, and default gateway.

The network administrator provides each of these pieces of information for configuring TCP/IP on a computer. Windows NT users on networks with DHCP servers can take advantage of automatic system ~~contiguration~~configuration and do not need to manually configure TCP/IP parameters.

This section provides details about IP addresses, subnet masks, and IP gateways.

Networking Concepts for TCP/IP

IP Addressing

7of17

IP Addressing

IP Addresses

Every host interface, or node, on ~~aTCP~~a TCP/IP network is identified by a unique IP address. This address is used to identify a host on a network~~;~~, it also specifies routing information in an internetwork. The IP address identifies ~~acomputer~~a computer as a 32-bit address that is unique across a TCP/IP network. An address is usually represented in dotted decimal notation, which depicts each octet (eight bits, or one byte) of an ~~IP~~lP address as its decimal value and separates each octet with a period. An IP address looks like this:

102.54.94.97

Important

Because IP addresses identify nodes on an interconnected network, each host on the internetwork must be assigned a unique IP address, valid for its particular network.

Network ID and Host ID

Although an ~~lP~~IP address is a single value, it contains two pieces of information: the network ~~lD~~ID and ~~the~~tne host (or system) ~~lD~~ID for your computer.

~~1~~' The ~~network lD~~nefwork ID identifies a group of computers and other devices that are all located on the same logical network, which are separated or interconnected by routers. In internetworks (networks formed by ~~acollection~~a collection of local area networks), there is a unique network ~~lD~~ID for each network.

~~1~~' The ~~host ID~~hosf /D identifies your computer within a particular network ~~lD~~ID. (A host is any device that is attached to the network and uses TCP/IP.)

Networks that connect to the public Internet must obtain an official network ~~lD~~ID from the lnterNIC to guarantee ~~lP~~IP network ~~lD~~ID uniqueness. The ~~lnterNIC~~InterNlC can be contacted via electronic mail at info@internic.net (for the United States, ~~1 800 444 4345~~18004444345 or, for Canada and overseas, ~~619 455 4600~~ 6I94554600). Internet registration requests can be sent to hostmaster@internic.net. You can also use FTP to connect to is.internic.net, then log in as anonymous, and change to the /~~INFOSOURCE~~lNFosouRcE/FAQ directory.

After receiving a network ~~lD~~ID, the local network administrator must assign unique host IDs for computers within the local network. Although private networks not connected to the Internet can choose to use their own network identifier, obtaining a valid network ~~ID~~lD from ~~InterNIC~~lnterNlC allows a private network to connect to the ~~Internet~~internet in the future without reassigning addresses.

The Internet community has defined address classes to accommodate networks of varying
sizes. Each network class can be discerned from the first octet of its ~~1P~~IP address. The following
table summarizes the relationship between the first octet of a given address and its network ~~1D~~ID
and host ID fields. ~~It~~lt also identifies the total number of network IDs and host IDs for each
address class that participates in the Internet addressing scheme. This sample uses w.x.y.z to
designate the bytes of the ~~1P~~IP address.
~~Chapter 3 Networking Concepts for TCPnP~~
IP Address Classes
~~Available Available~~
Networking Concepts for TCP/IP 8of17
Class ~~wvaluesl.2 NetworkiD~~wvalues1,2 Network ID Host ID Available Available
networks hosts per
net
A ~~1-126 w~~1126 W x.y.z 126 ~~16,777,214~~16.777214

B ~~128-191 w.x~~128191 W.X y.z 16,384 ~~65,534~~65.534
~~c 11J2-223~~C 192223 w.x.y z ~~2,097,151~~2,097,1 51 254
~~I~~1 Inclusive range for the first octet in the IP address.
2 The ~~:1ddress~~address 127 is reserved for loopback testing and interprocess
communication on the local ~~cumputer;~~computer, it is not a valid network
address.
Addresses 224 and above are reserved for special protocols (IGMP
multicast and others), and cannot be used as host addresses.
~~Anetwork~~A network host uses the network ID and host ID to determine which packets it should receive
or ignore and to determine the scope of its transmissions (only nodes with the same network ~~10~~ID
accept each other's ~~1P~~IP-level broadcasts).
Because the sender's ~~1P~~IP address is included in every outgoing ~~1P~~IP packet, it is useful for the
receiving computer system to derive the originating network ID and host ID from the ~~1P~~IP address
field. This is done by using subnet masks, as described in the following
section.
Subnet Masks
Subnet masks are 32-bit values that allow the recipient of lP packets to distinguish the network
ID portion of the lP address from ~~the~~tne host ID. Like an ~~1P~~IP address, the value of ~~asubnet~~a subnet mask is
frequently represented in dotted decimal notation. Subnet masks are determined by assigning
1's to bits that belong to the network ~~10~~ID and 0's to the bits that belong to the host ID. Once the
bits are in place, the 32-bit value is converted to dotted decimal notation~~,~~.
as shown in the
following table.
Default Subnet Masks for Standard IP Address Classes ~~Address class Bits for subnet mask Subnet mask Class A 11111111 00000000 00000000 00000000 255 .0.0.0~~

~~Class B 1111111111111111 () (}() () () () () (00000000 255.255.0.0 Class C 11111111 1111111111111111 00000000 255.255.255.0~~

The result allows TCP/IP to determine the host and network ~~IDs~~IDS of the local computer. For example, ~~when~~wnen the ~~IP~~IP address is 102.54.94.97 and the subnet mask is ~~255.255.0.0.~~255.255.0.0, the network ID is 102.54 and the host ID is 94.97.

Although configuring a host with ~~asubnet~~a subnet mask might seem redundant after examining the previous tables (since the class of a host is easily determined), subnet masks are also used to further segment an assigned network ~~10~~ID among several local networks.

For example, suppose a network is assigned the Class-~~8~~B network address 144.100. This is one of over 16,000 Class-~~8~~B addresses capable of serving more than 65,000 nodes. However, the worldwide corporate network to which this ID is assigned is composed of 12 international LANs with 75 to ~~I00~~100 nodes each. ~~Instead~~instead of applying for 11 more network IDs, it is better to use subnetting to make more effective use of the assigned ID 144.100. The third octet of the IP address can be used as a subnet ID, to define the subnet mask 255.255.255.0. This splits the Class-~~8~~B address into 254 subnets: 144.100.1 through 144.100.254, each of which can have 254 nodes. (Host ~~IDs~~IDS 0 and 255 should not be assigned to a computer~~;~~, they are used as broadcast addresses, which are typically recognized by all computers.) Any 12 of these network addresses could be assigned to the international LANs in this example. Within each LAN, each computer is assigned ~~aunique~~a unique host ID, and they all have the subnet mask 255.255.255.0.

The preceding example demonstrates a simple (and common) subnet scheme for Class-~~Baddresses~~B addresses. Sometimes it is necessary to segment only portions of an octet, using only a few

Address class	Bits for subnet mask	Subnet mask
Class A	11111111 00000000 00000000 00000000	255.0.0.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

bits to specify subnet ~~IDs~~IDS (such as when subnets exceed 256 nodes). Each user should check with the local network administrator to determine the network's subnet policy and the correct subnet mask. For all systems on the local network, the subnet mask must be the same for that network ID.

Important

All computers on a logical network must use the same subnet mask and network ID~~;~~, otherwise, addressing and routing problems can occur.

IP Addressing

Routing and IP Gateways

TCP/IP networks are connected by gateways (or routers), which have knowledge of the networks connected in the internetwork. Although each IP host can maintain static routes for specific destinations, usually the default gateway is used to find remote destinations. (The default gateway is needed only for computers that are part of an internetwork.)

~~Chapter 3 Networking Concepts for TCPnP~~

When ~~1P~~IP prepares to send a packet, it inserts the local (source) IP address and the destination address of the packet in the ~~1P~~IP header and checks whether the network ID of the destination matches the network ID of the source. If they match, the packet ~~is~~Is sent directly to the destination computer on the local network. ~~Ifthe~~If the network IDs do not match, the routing table is examined for static routes~~.~~, If none are found, the packet is forwarded to the default gateway for delivery.

The default gateway is ~~acomputer~~a computer connected to the local subnet and other networks that has knowledge of the network IDs for other networks in the internetwork and how to reach them.

Because the default gateway knows the network IDs of the other networks in the internetwork, it can forward the packet to other gateways until the packet is eventually delivered to a gateway connected to the specified destination. This process is known as routing.

N!{I0[E\
Network
A
*\ Network
Dther _ C
networks
~~Internetwork~~lnternetwork Routing Through Gateways

On networks that are not part of an internetwork, IP gateways are not required. If a network is part of an internetwork and a system does not specify ~~adefault~~a default gateway (or ~~ifthe~~if the gateway computer is not operating properly), only communication beyond the local subnet is impaired.

Users can add static routes by using the route utility to specify a route for ~~aparticulara~~a particular system.

Static routes always override the use of default gateways.

If the default gateway becomes unavailable, the computer cannot communicate outside its own subnet. Multiple default gateways can be assigned to prevent such a problem. When ~~acomputera~~a computer is configured with multiple default gateways, retransmission problems result in the system trying the other routers in the configuration to ensure ~~intemetworking~~internetworking communications capabilities. To configure multiple default gateways in Windows NT, you must provide an ~~1P~~IP address for each gateway in the Advanced Microsoft TCP/IP Configuration dialog box, as described in Chapter 2, "Installing and Configuring Microsoft TCP/IP and SNMP."

Networking Concepts for TCP/IP 9of17

IP routeu

"To other 1

lDEKWDIkS1:|

IP ra-ute}`e*;; WP router

I

IP Addressing

Dynamic Host Configuration Protocol

Assigning and maintaining ~~1P~~IP address information can be an administrative burden for network administrators responsible for internetwork connections. Contributing to this burden is the problem that many users do not have the knowledge necessary to configure their own computers for ~~intemetworking~~internetworking and must therefore rely on their administrators.

The Dynamic Host Configuration Protocol (DHCP) was established to relieve this administrative burden. DHCP provides safe, reliable, and simple TCP/IP network configuration, ensures that address conflicts do not occur, and helps conserve the use of IP addresses through centralized management of address allocation. DHCP offers dynamic configuration of IP addresses for computers. The system administrator controls how ~~IP~~lP addresses are assigned by specifying lease durations, which specify how long a computer can use an assigned ~~IP~~lP address before having to renew the lease with the DHCP server.

As an example of how maintenance tasks are made easy with DHCP, the IP address is released automatically for a DHCP client computer that is removed from a subnet, and ~~anew~~ a new address for the new subnet is automatically assigned when that computer reconnects on another subnet. Neither the user nor the network administrator needs to intervene to supply new configuration information. This is a most significant feature for mobile computer users with portables that are docked at different computers, or for computers that are moved to different offices frequently.

The DHCP client and server services for Windows NT are implemented under Requests for Comments (RFCs) 1533, 1534, 1541, and 1542.

~~Chapter 3 Networking Concepts for TCPnP~~ The following illustration shows an example of a DHCP server providing configuration
~~The following illustration shows an example of a DHCP server providing configuration~~ information on two subnets. ~~If~~lf, for example, ClientC is moved to Subnet 1, the DHCP server ~~will~~
Will automatically supply new TCP/IP configuration information the next time that ClientC is started.

~~Router~~
DHCP sefuwl
DHCP clientps a 5U3|-,gf
DHCP"
sums
nHc|3"
~~(with BOOTP forwarding enabled)~~ client()
~~OHCP~~DHCP Clients and ~~Servers~~Sewers on a Routed Network

DHCP uses ~~aclienta~~a client-server model and is based on leases for IP addresses. During system startup (the initializing state), a DHCP client computer sends a discover message that is broadcast to the local network and may be relayed to all DHCP servers on the private

Networking Concepts for TCP/IP 10of17
Router
fvwilh BOOTP fowardhg enabled)

Initializing
seeming
leque-Qing Renevirvg
L

internetwork. Each DHCP server that receives the discover message responds with an offer message containing an IP address and valid configuration information for the client that sent the request.

The DHCP client collects the configuration offerings from the servers and enters a selecting state. When the client enters the requesting state, it chooses one of the configurations and sends a request message that identifies the DHCP server for the selected configuration.

The selected DHCP server sends a DHCP acknowledgment message that contains the address first sent during the discovery stage, plus a valid lease for the address and the TCP~~+IP~~/lP network configuration parameters for the client. After the client receives the acknowledgment, it enters a bound state and can now participate on the TCP~~+IP~~/lP network and complete its system startup. Client computers that have local storage save the received address for use during subsequent system startup. As the lease approaches its expiration date, it attempts to renew its lease with the DHCP server, and is assigned a new address if the current ~~1P~~IP address lease cannot be renewed.

~~Lease expires~~
~~discover Initializing~~
~~Rebinding~~
~~·__......,......,........~; Lease approaches~~

~~--L-----, expiration (87.5%)~~
~~Renewing acknowledgment~~
~~-· ··} ' Lease approaches acknowledgment -   e xp ir ati on (5_0_%_)""' "'~~

DHCP Client State Transition During System Startup

~~1n~~In Windows NT Server, the network administrator uses DHCP Manager to define local policies for address allocation, leases, and other options. For information about using this tool, see Chapter 4, "Installing and Configuring DHCP Servers." For information about the steps for setting up TCP~~+~~/IP using DHCP, see "Configuring TCP~~+IP~~/lP" in Chapter 2, "~~Installing~~lnstalling and Configuring Microsoft TCP~~+~~/IP and SNMP." For information about setting up DHCP relaying, see the documentation for your router.

d iscxzmar
,.4»~
o11'er
Leam expires
IRehinclng 1~lease Epprcxazhas ||
.a>q:»iratior\ C37-5°f<>J
request
esse
azknardedgmerlt
azkromiadgrrent 1- Bound
apprclazfes
a"><pirati:n 55044) _,I

Networking Concepts for TCP/IP 11 of17

Name Resolution for Windows Networking

Configuring Windows NT with TCP~~+~~/IP requires the IP address and computer name, which are unique identifiers for the computer on the network. The ~~1P~~IP address, as described earlier in this chapter, is the unique address by which ~~all~~ati other TCP~~+~~/IP devices on the internetwork recognize that computer. For TCP/IP and the Internet, the computer name is the globally known system name plus ~~aDNS~~a DNS domain name. (On the local network, the computer name is the NetBIOS name that was defined during Windows NT Setup.) ~~Chapter 3 Networking Concepts for TCPnP~~

Computers use IP addresses to identify each other, but users usually find it easier to work with computer names. ~~Amechanism~~A mechanism must be available on ~~aTCP~~a TCP/IP network to resolve names to IP addresses. To ensure that both name and address are unique, the Windows NT computer using ~~TCPIIP~~TCP/IP registers its name and IP address on the network during system startup. ~~AWindows~~A Windows NT computer can use one or more of the ~~following~~foiiowing methods to ensure accurate name ~~resolution~~ resoiution in TCP/IP ~~intemetworks~~internetworks:

' Windows Internet Name Service

Windows NT computers can use WINS if one or more WINS servers are available that contain ~~adynamic~~a dynamic database mapping computer names to IP addresses. WINS can be used in conjunction with broadcast name resolution for an ~~internetwork~~internetvvork where other name resolution methods are inadequate. As described in the following section, WINS is a NetBIOS over TCP/IP mode of operation defined in RFC 1001/1002 ~~asp~~as p-node.

' Broadcast name resolution

Windows NT computers can also use broadcast name resolution, which is a NetBIOS over TCP~~!IP~~/lP mode of operation defined in RFC 1001/~~1002~~1 002 as b-node. This method relies on a computer making IP-~~Ievel~~level broadcasts to register its name by announcing it on the network. Each computer in the broadcast area is responsible for challenging attempts to register a duplicate name and for responding to name queries for its registered name.

' DNS name resolution

The Domain Name System (DNS) provides ~~away~~a way to look up name mappings when connecting ~~acomputer~~a computer to foreign hosts using NetBIOS over TCP~~!IP~~/lP or Windows Sockets applications such as ~~FfP~~FTP. DNS is a distributed database designed to relieve the traffic problems that arose with the exploding growth of the Internet in the early 1980s.

1 An LMHOSTS file to specify the NetBIOS computer name and IP address mappings, or a

HOSTS file to specify the DNS name and IP address
On a local computer, the HOSTS file (used by Windows Sockets applications to
find
TCP~~i~~/IP host names) and LMHOSTS file (used by NetBIOS over ~~TCPIIP~~TCP/IP to
find Microsoft
networking computer names) can be used to list ~~known~~Known IP addresses mapped
with
corresponding computer names. LMHOSTS is still used for name resolution in
Windows NT for small-scale networks or remote subnets where ~~WINS~~WlNS is not
available.
This section provides details about name resolution in Windows NT after first
presenting some
background information about the modes of NetBIOS over TCP~~i~~/IP that can be
used in
Microsoft networks.

Name Resolution for Windows Networking

NetBIOS over ~~TCPnP~~TCP/IP and Name Resolution
NetBIOS over TCP/IP is the session-layer ~~network~~nefwork service that performs
name-to~~ 1P~~-IP address
mapping for name resolution. This section describes the modes of NetBIOS over
TCP/IP, as
defined in RFCs 1001 and 1002 to specify how NetBIOS should be implemented
over TCP/IP.
The modes of NetBIOS over TCP/IP define how network resources are identified
and
accessed. The two most important aspects of the related naming activities are
registration and
resolution. Registration is the process used to acquire a unique name for each
node (computer
system) on the network. ~~Acomputer~~A computer typically registers itself when
it starts. Resolution is the
process used to determine the specific address for ~~acomputer~~a computer name.
The NetBIOS over TCP/IP modes include the ~~following~~foI\owing:
~~1~~ l b-node, which uses broadcasts to resolve names
~~1~~ ' p-node, which uses point-to-point communications with a name server to
resolve names
~~1~~ ' m-node, which uses b-node first (broadcasts), then p-node (name queries)
if the broadcast
fails to resolve a name
~~1~~ l h-node, which uses p-node first for name queries, then b-node if the name
service is
unavailable or if the name is not registered in the WINS database
For DHCP users on ~~aWindows~~a Windows NT network, the node type is assigned by
the DHCP server.
When WINS servers are in place on the network, NetBIOS over TCP/IP resolves
names on ~~aclient~~a
client computer by communicating with the WINS server. When WINS servers are
not in place,
NetBIOS over TCP/IP uses b-node broadcasts to resolve names~~.~~, NetBIOS over
TCP/IP in
Windows NT can also use LMHOSTS files and DNS for name resolution, depending
on how

TCP/~~IP~~lP is configured on ~~aparticulara~~a particular computer. ~~In~~ln Windows NT
3.5, the ~~NETBT.SYS~~NETBTSYS module
provides the NetBIOS over TCP/IP functionality that supports name
registration and resolution
modes.
Windows NT version 3.5 supports all of the NetBIOS over TCP/IP modes described
in the
following sections. NetBIOS over TCP/IP is also used with the LAN Manager 2.x
Server
message protocol.
~~Chapter 3 Networking Concepts tor TCPnP~~
B-Node
The b-node mode uses broadcasts for name registration and resolution. That
is, if NT~~-PC1-~~_PC1
wants to communicate with NT -PC2 it ~~will~~Will broadcast to all machines that
it is looking for
NT_PC2 and then ~~wait~~Wait a specified time for NT_PC2 to respond. B-node has
two major
problems:

' In ~~alargea~~a large environment, it loads the network with broadcasts.

" Routers do not forward broadcasts, so computers that are on opposite sides
of a router will
never hear the requests.
P-Node
~~1~~The p-node mode addresses the issues that b-node does not solve. In ~~ap~~a p-node
environment,
computers neither create nor respond to broadcasts. All computers register
themselves with
the WINS server, which is a ~~NetBIOS~~NetBlGS Name Server (NBNS) with
enhancements. The WINS
server is responsible for knowing computer names and addresses and for
ensuring no
duplicate names exist on the network. All computers must be configured to know
the address
Networking Concepts for TCP/IP 12 of17

of the WINS server.
In this environment, when NT_~~PC1 wants~~PC1 Wants to communicate with NT_PC2,
it queries the WINS
server for the address of NT_PC2. When NT_~~PC1~~PC1 gets the appropriate address
from the
WINS server, it goes directly to NT_PC2 without broadcasting. Because the name
queries go ~~directly~~
directiy to the WINS server, p-node avoids loading the network with
broadcasts. Because
broadcasts are not used and because the address is received directly,
computers can span
routers.
The most significant problems with p-node are the ~~following:~~foliowingz

l All computers must be configured to know the address of the WINS server
(although this is
typically configured via DHCP)

l If for any reason the WINS server is down, computers that rely on the WINS
server to
resolve addresses cannot get to any other systems on the network, even if they
are on the
local network
M-Node
~~Them~~The m-node mode was created primarily to solve the problems associated
with b-node and
p-node. This mode uses a combination of b-node and p-node. ~~In~~ln an m-node
environment, a
computer first attempts registration and resolution using b-node. ~~If~~lf that
is successful, it then
switches to the p-node. Because this uses b~~-~~~node first, it does not solve
the problem of
generating broadcast traffic on the network. However, m-node can cross
routers. Also,
because b-node is always tried first, computers on the same side of a router
continue to
operate as usual if the WINS server is down.
M-node uses broadcasts for performance optimization, because in most
environments local
resources are used more frequently than remote resources. Also, in a Windows
NT network,
m-node can cause problems with ~~Netlogon~~NetLogon in routed environments.
H-Node
The h-node mode, which is currently in RFC draft form, is also ~~acombinationa~~a
combination of b-node and
p-node that uses broadcasts as a last effort. Because p-node is used first,
no broadcasts are
generated if the WINS server is running, and computers can span routers.
~~Ifthe~~If the WINS server
is down, b-node is used, so computers on the same side of a router continue
to operate as ~~usual.~~
usuai
The h-node mode does more than change the order for using b-node and p-node.
If the WINS ~~server~~
sewer is down so that local broadcasts (b-node) must be used, the computer
will continue to
poll the WINS server. As soon as the WINS server can be reached again, the
system switches
back to p-node. Also, optionally on a Windows network, h-node can be configured
to use
LMHOSTS after broadcast name resolution fails.
The h-node mode solves the most significant problems associated with
broadcasts and
operating in a routed environment. For Microsoft TCP/~~IP~~lP users who configure
TCP/IP
manually, h-node is used by ~~defaul-~~default, unless the user does not specify
addresses for WINS

servers when configuring TCP/IP.
~~8~~B-Node with LMHOSTS and Combinations
Another variation is also used in Microsoft networks to span routers without
a WINS server and
p-node mode. In this mode, b-node uses a list of computers and addresses stored
in an
LMHOSTS file. ~~Ifab~~If a b-node attempt fails, the system looks in LMHOSTS to
find a name and
then uses the associated address to cross the router. However, each computer
must have this
list, which creates an administrative burden in maintaining and distributing
the list. Both
Windows for Workgroups 3.11 and LAN Manager 2.x used such a modified b-node
system.
Windows NT uses this method if WINS servers are not used on the network. In
Windows NT~~, —~~.

some ~~-xtensions~~extensions have been added to this file to make it easier to
manage (as described in
Chapter 6, "Setting Up LMHOSTS"), but modified b-node is not an ~~ideal~~ideai
solution.
~~Chapter 3 Networking Concepts for TCPnP~~
Some sites may need to use both b-node and p-node modes at the same site.
Although this
configuration can work, administrators must exercise extreme caution in doing
so, using it only
for transition situations. Because p-node hosts disregard broadcasts and
b-node hosts rely on
broadcasts for name resolution, the two hosts can potentially be configured
with the same
NetBIOS name, leading to unpredictable results. Notice that if a computer
configured to use
b-node has a static mapping in the WINS database, ~~acomputer~~a computer
configured to use p-node
cannot use the same computer name.
Windows NT computers can also be configured as WINS proxy agents to help the
transition to
using WINS. For more details, see the next section.

Name Resolution for Windows Networking
Windows Internet Name Service and Broadcast Name
Resolution
WINS provides a distributed database for registering and querying dynamic
computer
name-to-~~IP~~lP address mappings in a routed network environment. ~~Ifyou~~lf you
are administering a
routed network, WINS is your best first choice for name resolution, because
it is designed to
solve the problems that occur with name resolution in complex
~~intemetworks~~internetworks.
WINS reduces the use of local broadcasts for name resolution and allows users
to easily locate
systems on remote networks. Furthermore, when dynamic addressing through DHCP
results in

new ~~IP~~lP addresses for computers that move between subnets, the changes are automatically updated in the WINS database. Neither the user nor the network administrator needs to make manual accommodations for name resolution in such ~~acase~~a case.

The WINS protocol is based on and is compatible with the protocols defined for NBNS in RFCs 1001~~i~~/1002, so it is interoperable with any other implementations of these RFCs~~.~~,

This section provides an overview of how WINS and name query broadcasts provide name resolution on Windows networks. For information about setting up WINS servers, see Chapter 5, "~~Installing~~installing and Configuring WINS Servers."

WINS in ~~aRouted~~a Routed Environment

WINS consists of two components: the WINS server, which handles name queries and registrations, and the client software, which queries for computer name resolution.

Windows networking clients (WINS-enabled Windows NT or Windows for Workgroups 3.11 computers) can use WINS directly. Non-WINS computers on the internetwork that are b-node compatible as described in RFCs ~~1001~~1001 and ~~I002~~1002 can access WINS through proxies, which are WINS-enabled computers that listen to name query broadcasts and then respond for names that are not on the local subnet or are p-node computers.

On a Windows NT network, users can browse transparently across routers. To allow browsing without WINS, the network administrator must ensure that the users' primary domain has Windows NT Server or Windows NT Workstation computers on both sides of the router to act as master browsers. These computers need correctly configured LMHOSTS files with entries for the domain controllers across the subnet.

~~With~~Witn WINS, such strategies are not necessary because the WINS servers and proxies transparently provide the support necessary for browsing across routers where domains span the routers.

The following illustration shows a small internetwork, with three local area networks connected by a router. Two of the subnets include ~~WINS~~WlNS name servers, which can be used by clients on both subnets. WINS-enabled computers, including proxies, access the WINS server directly, and the computers using broadcasts access the WINS server through proxies. Proxies only pass name query packets and verify that registrations do not duplicate existing systems in the WINS database. Proxies, however, do not register b-node systems in the WINS database.

~~Non-WINS enabled~~
~~Non-WINS enabled~~
~~: : : :~~
Networking Concepts for TCP/IP 13 of17

1 : Q u 9 rg
\4qn\1\vS.9****€¢ ¢.1v\{****
'\. . . N
'<
"<~ a
4 4,4
\ ¢ . ; * r ~ 1 \ \ f 1 <
H on-Wllf-IS
EM'\dJ|B=d
WINS Pf0*¢!J'
Sui |;f" Wll S
WINS saver,
saver Database
replioadon
WINS
enabled Rmler
uhm
\h ET" 3
uorwums* 2
enabled Rnuta' wms`
~~WINS ~~proxy
Example of an Internetwork with WINS ~~Servers Chapter 3 Networking Concepts for TCPnP~~Sewers

The proxy communicates with the WINS server to resolve names (rather than maintaining its own database) and then caches the names for a certain time. The proxy serves as an intermediary, by either communicating with the WINS server or supplying a name-to-IP address mapping from its cache. The following illustration shows the relationships among WINS servers and clients, including proxies for non~~-~~-WINS computers and the replication between WINS servers.

~~WINS server1~~
~~ClientA (WINS)~~

~~WINS database • _,:eplication~~
~~WINS server2~~
~~ClientC (WINS proxy)~~
~~ClientS (non-WINS)~~
°""> 93482
<:EmB (non-WIN S)
~~Broadcast ~~Eroadcaa
Example of Clients and ~~Servers~~Sewers Using WINS

In the above illustration, ClientA can ~~resolve~~resoive names by first querying the WINS server and, if that fails, then using broadcast name queries. ~~ClientB~~CiientB, which is not WINS-enabled, can only

resolve names using broadcast name queries, but when ClientC receives the
broadcast, it ~~forwards~~
fon/vards the request to the WINS server and returns the address to
~~ClientB~~CIientB.
However, a complex environment presents additional problems. For example, an
internetwork
might consist of two subnets, with all the computers belonging to DomainA
attached to ~~Subnet1~~
Subnett, all the computers in DomainB attached to Subnet2, and computers from
DomainC
attached to either of the subnets. ~~In~~ln this case, without WINS, DomainA
computers can browse ~~Subnet1~~
Subnett, DomainB computers can browse Subnet2, and DomainC computers can
browse both
subnets as long as the primary domain controller for DomainC is available~~.~~,
With WINS,
computers from all domains can browse all subnets if their WINS servers share
databases.
cuerm {WlI'lS)
Query WINS.
then broadcast me-rg
WINS s=mler1
WINS database
_ re-plicaEcn Wm 5
2: Eircwad-cast 5
3
5
CIia1tC (WINS proxy)

If the Windows NT client computer is also DHCP~~-~~~enabled and the administrator
specifies
WINS server information as part of the DHCP options, the computer will usually
be
automatically configured with WINS server information. You can manually
configure WINS
settings, as described in Chapter 2, "Installing and Configuring Microsoft
TCP/IP and SNMP":

l To enable WINS name resolution for ~~acomputer~~a computer that does not use
DHCP, specify WINS
server addresses in the TCP/IP Configuration dialog box

" To designate ~~aproxy~~a proxy, check the Enable WINS Proxy Agent option in the
Advanced
Microsoft TCP/IP Configuration dialog box
With WINS servers in place on the internetwork, names are resolved using two
basic methods,
depending on whether WINS resolution is available and enabled on the
particular computer.
Whatever name resolution method is used, the process is transparent to the
user after the
system is configured.

~~If WINS~~lfWlNS is not enabled The computer registers its name by broadcasting name registration
request packets to the local subnet via UDP datagrams. To find a particular computer, the
non-WINS computer broadcasts name query request packets on the local subnet, although this
broadcast cannot be passed on through IP routers. ~~If~~lf local name resolution fails, the local
LMHOSTS file is consulted. These processes are followed whether the computer is a network
server, a workstation, or other device.
~~If WINS~~lfWlNS is enabled The computer first queries the WINS server, and if that does not succeed, it
broadcasts its name registration and query requests via UDP datagrams (h-node), in the
following series of steps:
1. During TCP/IP configuration, the computer's name is registered with the WINS server, and
the IP address of the WINS server is stored ~~locally~~Iocally so the WINS ~~server~~sewer can be found on
the internetwork. The WINS database is replicated among all WINS servers on the
internetwork.
'wma
" saver
~~Chapter 3 Networking Concepts for TCPnP~~ Payroll
2. ~~Aname~~A name query request is sent first to the WINS server, including requests from remote
clients that are routed through an IP router. This request is a UDP datagram. If the name is
found in the WINS database, the client can establish a session based on the ~~addres"~~address
mapping received from ~~WINS~~W|NS.
, > *L, l,
1% E 13 ff;'§1J
mms
381.'841
wma
~~WINS~~ .database
Com.
U1

11T~ .., ;orpU1
12.3.0.5 Pagrd
Com_
01
natuae *.'\4333,n'oll`publio
P3Wd|
3. ~~Ifquerying~~If querying the WINS server does not succeed and if the client computer is configured as
an h-node, the computer broadcasts name query request packets in the same manner as
a non-WINS-enabled computer.

4. Finally, if other methods fail, the local LMHOSTS file is checked. This also includes a
search of any centralized LMHOSTS files referred to in #INCLUDE statements, as
described in Chapter 6, "Setting Up LMHOSTS."
WINS servers accept and respond to UDP name queries. Any name-to-IP address mapping
registered with a WINS server can be provided reliably as a response to a name query.
However, a mapping in the database does not ensure that the related device is currently
running, only that a computer claimed the particular IP address and it is ~~acurrently~~a currently valid
mapping.
WINS Name Registration
Name registration ensures that the computer's name and IP address are unique for each
device.
~~If WINS~~lfWlNS is enabled The name registration request is sent directly to the WINS server to be added
to the database. ~~AWINS~~A WINS server accepts ~~or~~cr rejects a computer name registration depending on
the current contents of its database. ~~Ifthe~~If the database contains
~~adifferenta~~a different address for that name~~,~~.
WINS challenges the current entry to determine whether that device still claims the name. If
another device is using that name, WINS rejects the new name registration request. ~~Otherwise~~
Othen/vise, WINS accepts the entry and adds it to its local database together with a timestamp,
an incremental unique version number, and other information.
~~If WINS~~lfWlNS is not enabled For a non-WINS computer to register its name, ~~anamea~~a name registration
request packet is broadcast to the local network, stating its computer name and IP address.
Any device on the network that previously claimed that name challenges the name registration
with a negative name registration response, resulting in an error. ~~If~~lf the registration request is
not contested within ~~aspecifica~~a specific time period, the computer adopts that name and address.
Once a non-WINS computer has claimed a name, it must challenge duplicate name
registration attempts and respond positively to name queries issued on its registered name by
sending ~~apositivea~~a positive name query response. This response contains the IP address of the
computer so that the two systems can establish a session.
WINS Name Release
WINS
3€|"JB|'|:
wus
.datab

When a computer finishes with a particular name (such as when the Workstation service or Server service is stopped), it no longer challenges other registration requests for the name. This is referred to as releasing a name.

~~Chapter 3 Networking Concepts for TCPnP~~

If WINS is enabled Whenever a computer is shut down properly, it releases its name to the WINS server, which marks the related database entry as released. ~~If~~lf the entry remains released for a certain period of time, the WINS server marks it as ~~extinct~~exfincf, and the version number is updated so that the database changes will be propagated among the WINS servers. Extinct entries remain in the database for a designated period of time to enable the change to be propagated to all WINS servers.

If a name is marked released at a WINS server and a new registration arrives using that name but ~~adifferent~~a different address, the WINS server can immediately give that name to the requesting client because it knows that the old client is no longer using that name. (This might happen, for example, when a DHCP-enabled laptop changes subnets.) ~~If~~lf that computer released its name during an orderly shutdown, the ~~WINS~~WlNS server will not challenge the name. ~~If~~lf the computer restarts because of a system reset, the name registration with a new address will cause the WINS server to challenge the registration, but the challenge will fail and the registration will succeed, because the computer no longer has the old address.

~~If WINS~~lfW|NS is ~~not enabled~~notenabled When a non-WINS computer releases ~~a~~e name, ~~a~~e broadcast is made to allow any systems on the network that might have cached the name to remove it. Upon receiving name query packets specifying the deleted name, the computer simply ignores the request, allowing other computers on the network to acquire the name that it has released.

For non-WINS computers to be accessible from other subnets, their names must be added as static entries to the WINS database or in the LMHOSTS file(s) on the remote system(s), because they will only respond to name queries that originate on their ~~local~~Iocai subnet.

WINS Name Renewal

~~Arenewal~~A renewal is a timed reregistration of ~~acomputer~~a computer's name with the WINS server. When the WINS server registers a name, it returns a renewal interval for the name, and the client must reregister within that time~~; otherwise~~, othen/vise, the WINS server will mark the name as released and available for use. ~~Arequest~~A request for name renewal is treated the same as a new name registration.

Renewal provides registration reliability through periodic reregistering of names with the WINS servers.

Networking Concepts for TCP/IP 14 of17
Name Resolution for Windows Networking

IP Addressing for RAS

Remote Access Service (RAS) provides remote networking for telecommuters, mobile workers, and system administrators who monitor and manage servers at multiple branch offices. Users with RAS on a Windows NT computer can dial in to remotely access their networks for services such as file and printer sharing, electronic mail, scheduling, and SQL database access.

Windows NT RAS works with IP routing for RAS servers so that RAS clients can use TCP~~!~~/IP networks. (RAS can also work with IPX routing for clients that use NetWare networks.)

Windows NT also uses the industry-standard Point to Point Protocol (PPP) and Serial Line IP (SLIP) standards. These standards ensure that Windows NT is interoperable with third-party remote-access server and client software. RAS clients can use DNS and WINS for name resolution services, and it can create TCP sessions with systems on the local network.

'Windowa HT
~~Windows NT NetBEUI host~~ [.16i8EU| Inst
(or LAN ~~Manager)~~Maregerl
~~Windows~~Mndowa NT ~~running~~mnning IPX
(~~or~~cf NetWare~~)~~]
~~Windows NT running TCPnP (or UNIX, VMS, and others)~~
~~Windows NT Remote Access Server (or third party)~~
~~NetBEUI over PPP TCP/IP over PPP IPX overPPP~~
~~Windows NT Earlier versions of Microsoft RASRASclient~~
~~(Windows NT 3.1, LAN Manager 2.x)~~
~~(or third party with~~
~~PPP or SLIP)~~

~~NetBEUI over~~
'lfvindouma HT mrning TGPIIP
(or UN DQ, 'JI'u18_ ad others]
-.
".f\.4nd:wa NT Renwota >%:r:=aaa Sawer
for th ird parh/J
N98 EU I CUE! p pp
TC PXIP cnet PP P
IP>< OJEI P pp
Windowa NT Ealiar vers bm 6 rv1i@m9@f1
RAS dxawt RAS