Novell ZENworks™ for Desktops 3.2 Preboot Services

3.2

www.novell.com

ADMINISTRATION

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

U.S. Patent Nos. 5,349,642; 5,594,863; 5,633,931; 5,692,129; 5,758,069; 5,761,499; 5,781,724; 5,781,733; 5,859,978; 5,893,118; 5,905,860; 6,023,586; 6,105,069; 6,115,594; 6,173,289; 6,144,959. Patents Pending.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Administration
September 2001
103-000185-001

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

Third-Party Trademarks

Contents

About this Guide

This guide contains information that will help you understand and administer ZENworks™ for Desktops 3.2 Preboot Services. It is divided into the following sections:

- "Administering ZENworks for Desktops Preboot Services" on page 9
- "Acronyms" on page 21
- "Glossary" on page 23

Documentation Conventions

In Novell® documentation, a greater than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

1 Administering ZENworks for Desktops Preboot Services

This section includes information about setting up ZENworks™ for Desktops (ZfD) 3.2 Preboot Services and the problems you may encounter when configuring the system. It contains the following sections:

- "Overview" on page 9
- "Designing a PXE Network" on page 11
- "Configuring ZfD 3.2 Preboot Services" on page 13

Overview

ZfD 3.2 Preboot Services consists of a number of distinct components that can be installed in different configurations, allowing the system to adapt to various management requirements and to any network design. It consists of the following components:

- "ZfD 3.2 Preboot Services Client" on page 9
- "ZfD 3.2 Preboot Services Proxy DHCP Server" on page 10
- "ZfD 3.2 Preboot Services TFTP and MTFTP Servers" on page 10
- "ZfD 3.2 Preboot Services Transaction Server" on page 10

ZfD 3.2 Preboot Services Client

The Preboot Services client is downloaded by a workstation during a Preboot Execution Environment (PXE) session to enable the workstation to be managed by ZfD 3.2 Preboot Services. The Preboot Services client provides the workstation with the ability to communicate with the Preboot Services servers in the network, allowing the workstation to be managed and to request management intervention.

The client consists of a preboot component that makes the workstation available on the network before the operating system has loaded. This component ensures that the workstation can notify the Transaction Server of its presence on the network even when there is no operating system installed on the workstation. It also enables system healing, operating system installation, and software installation on the workstation.

The Preboot Services client uses the Proxy DHCP Server to establish the network address of the Preboot Services TFTP Server and Preboot Services Transaction Server.

The Preboot Services clients make use of the Preboot Services Transaction Server to determine what management actions should be performed on the client as well as using the Transaction Server to store information about the client in the data store. The clients can request files from the TFTP Server if the clients need to perform complex actions.

ZfD 3.2 Preboot Services Proxy DHCP Server

The Preboot Services Proxy DHCP Server runs alongside a standard DHCP Server to inform Preboot Services clients of the network address of the TFTP Server and Transaction Server. The Preboot Services Proxy DHCP Server also responds to PXE clients to indicate to the client which boot server to use.

ZfD 3.2 Preboot Services TFTP and MTFTP Servers

The Preboot Services TFTP and MTFTP servers can be used by the Preboot Services client to request files that are needed to perform complex tasks. This allows clients to increase the number of tasks that they can perform by requesting the necessary files from the server. The TFTP Server also provides a central repository for these task files, meaning that it is not necessary to update every Preboot Services client in order to make use of a new feature. A PXE client will use this service to download the Preboot Services client.

ZfD 3.2 Preboot Services Transaction Server

The Preboot Services clients connect to the Transaction Server to check if there are any actions that need to be performed on the client. The clients can also use the Transaction Server to get or set values in the data store.

Designing a PXE Network

A number of considerations and rules need to be observed when implementing the Preboot Execution Environment (PXE) in a network. Your implementation of the PXE system will be affected by the number of ZfD 3.2 Preboot Services PXE clients that are to be supported as well as the network bandwidth that is available. The use of network bandwidth across wide area network (WAN) links requires special consideration. You will also have to make configuration changes to the PXE system if the network spans multiple subnets.

This section contains information on the following topics:

- "Understanding the Client to Server Component" on page 11
- "Network Design Considerations" on page 12

Understanding the Client to Server Component

Design your Client to Server component so that Preboot Services clients can effectively connect to the Transaction Server as well as to the TFTP or MTFTP Servers. The important points here include the number of Preboot Services clients to be installed on the network and the bandwidth available to service these clients.

When a ZfD 3.2 Preboot Services client or a PXE client executes on a workstation, it will typically perform six steps:

1. Broadcast a request for a DHCP Server to provide the client with an IP address. Either a Preboot Services client or a PXE client executing on the workstation will perform this step. In the case of a PXE client this step is used to get the information necessary to download the Preboot Services client.

   The standard DHCP Server will respond to provide the client with the necessary IP address. The Preboot Services Proxy DHCP Server will also respond to the client to provide the client with two IP addresses: an address for the Transaction Server and an address for the TFTP and MTFTP servers.

   NOTE: The Preboot Services Proxy DHCP does not provide an IP address to the Preboot Services client, it only supplies the client with the IP addresses of the servers that the client needs to connect to for a successful PXE session.

2. If the client that executed in Step 1 was a PXE client, then the PXE client will download the Preboot Services client from the MTFTP Server. The

address of the MTFTP Server was obtained in Step 1 from the Preboot Services Proxy DHCP Server. This step will require the client to download a single file of less than 64 kilobytes. In the case where the Preboot Services client was already executing (for example, Preboot Services Boot Diskette or Preboot Services Boot Sector) this step will not occur.

3. If a Preboot Services client was downloaded in Step 2, then it will perform a network broadcast to request IP address information. The standard DHCP Server and Preboot Services Proxy DHCP Server will respond again with the same information that they provided in Step 1. It is not important for the standard DHCP Server to provide the same client IP address in Steps 1 and 3.
4. The Preboot Services client connects to the Preboot Services Transaction Server and authenticates with the server. The Transaction Server will determine if any actions should execute on the client and return the necessary information to the client. If the Transaction Server does not have any actions for the client to execute, the client will shut down and the client workstation will continue to execute normally.
5. If an action was given to the Preboot Services client, the client will connect to the TFTP Server to download the specified action file. The size of the download file can vary a great deal depending on the action to be performed and can range from a few kilobytes for an action such as hardware inventory, to over a megabyte for a complex action such as system healing.

Once the action has been completed, the Preboot Services client will go to Step 4 to determine if there are any more actions outstanding.

Network Design Considerations

Use the following guidelines as you consider how to design your network for Preboot Services:

- Only one Proxy DHCP Server should be installed per DHCP Server scope
- Only one Proxy DHCP Server should exist on a subnet
- It is typical to have only one Proxy DHCP Server on the network

TFTP Servers should be installed so that Preboot Services clients have access to a TFTP Server within their LAN. The bulk of network traffic generated by Preboot Services is between the Preboot Services clients and the TFTP Server. A good design will ensure that a client will not need to connect to its TFTP Server through a slow WAN link.

Configuring ZfD 3.2 Preboot Services

This section explains the installation of the ZfD 3.2 Preboot Services system. It contains the following topics:

- "System Requirements" on page 13
- "Setting Up Preboot Services Servers in Windows NT" on page 14
- "Setting Up Preboot Services Servers in NetWare" on page 17
- "Configuring IP Port Usage in ZfD 3.2 Preboot Services" on page 19

System Requirements

To function correctly, ZfD 3.2 Preboot Services requires a local area network (LAN) with IP layer support. The following are also required:

Network Server Requirements

Specification	Minimum Requirement
Processor	Pentium* II, 350 MHz or faster
Network Operating System	One of the following: ◆ Windows* NT* with SP6a (or later) applied ◆ Windows 2000 ◆ NetWare® 5.x
Available Disk Space	10 MB
RAM	128 MB
LAN Connection	Ethernet or token ring

Client Workstation Requirements

Specification	Minimum Requirement
Processor	Pentium, 75 MHz or faster
Network Card	PXE-enabled

Specification	Minimum Requirement
Available Disk Space	1 MB
RAM	16 MB
Graphics Display	VGA; 16-bit color

Setting Up Preboot Services Servers in Windows NT

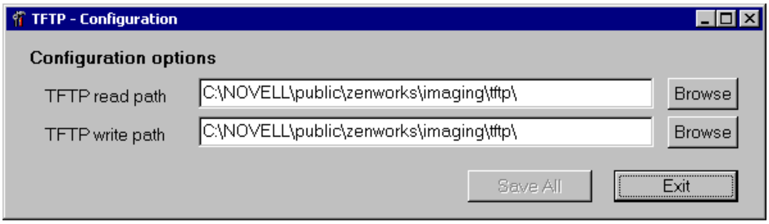
The following sections will help you to set up the various servers required by ZfD 3.2 Preboot Services:

- "Configuring the TFTP Server" on page 14
- "Configuring the TFTP Server" on page 14
- "Configuring the Proxy DHCP Server" on page 16

Configuring the TFTP Server

It is seldom necessary to change the default TFTP Server configuration values. Use the following procedure if you need to change them:

1. From the Windows Desktop, click Start > Programs > ZEN Preboot Services > ZEN Preboot Services Configuration > TFTP Configuration. The TFTP Configuration window is displayed.



TFTP read path: C:\NOVELL\public\zenworks\imaging\tftp\

TFTP write path: C:\NOVELL\public\zenworks\imaging\tftp\

2. Fill in the fields:

   TFTP Read Path: The read path should point to a directory where the TFTP Server will look for files that are requested by clients.

   TFTP Write Path: The write path should point to a directory where the TFTP Server will write files sent by clients.

   NOTE: The read and write fields use the same path.

3 Click Save All to save new settings.

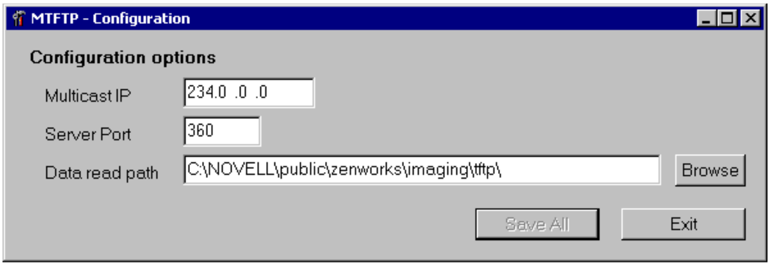
or

Click Exit to terminate the configuration utility without saving changes.

Configuring the MTFTP Server

It is seldom necessary to change the default MTFTP Server configuration values. Use the following procedure if you need to change them:

1 From the Windows Desktop, click Start > Programs > ZEN Preboot Services > ZEN Preboot Services Configuration > MTFTP Configuration. The MTFTP Configuration window is displayed.



Multicast IP: 234.0 .0 .0

Server Port: 360

Data read path: C:\NOVELL\public\zenworks\imaging\tftp\

2 Fill in the fields:

Multicast IP: Specify the address to be used as a destination during multicast transfers. Ensure that the address used falls within the IP Address range designated for multicast. If you change this value, be sure to update the corresponding entry in the Proxy DHCP configuration.

Server Port: Specify the port number that the server will expect to receive requests on. If you change this value, be sure to update the corresponding entry in the Proxy DHCP configuration.

Data Read Path: Specify the directory where the MTFTP Server will read the files that are requested by clients.

3 Click Save All to save new settings.

or

Click Exit to terminate the configuration utility without saving changes.

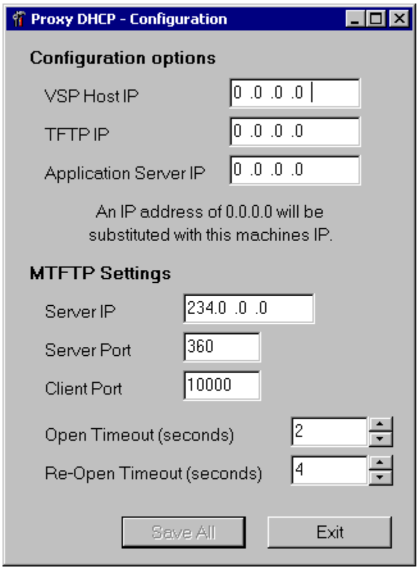
Configuring the Proxy DHCP Server

The Proxy DHCP Server provides Preboot Services clients with the information that they require to be able to connect to the Preboot Services system.

The DHCP Server needs to have option 60 (decimal) added to the DHCP tags. This option should be a string type and must contain the letters **PXEClient**.

The procedure to configure the DHCP Server varies from one DHCP Server to another, so it is not possible to provide step-by-step instructions on configuring the server. Use the following steps to check the settings of the Proxy DHCP Server:

1 From the Windows Desktop, click Start > Programs > ZEN Preboot Services > ZEN Preboot Services Configuration > Proxy DHCP Configuration. The Proxy DHCP Configuration window is displayed.



Configuration options

VSP Host IP: 0 .0 .0 .0

TFTP IP: 0 .0 .0 .0

Application Server IP: 0 .0 .0 .0

An IP address of 0.0.0.0 will be substituted with this machines IP.

MTFTP Settings

Server IP: 234.0 .0 .0

Server Port: 360

Client Port: 10000

Open Timeout (seconds): 2

Re-Open Timeout (seconds): 4

2 Check the fields:

Transaction Server IP: This IP Address will be returned to Preboot Services clients requesting Proxy DHCP information and should contain the IP address of the Preboot Services Transaction Server that the Preboot Services client should connect to.

TFTP IP: This IP address will be returned to Preboot Services clients requesting Proxy DHCP information and should contain the IP Address of the Preboot Services TFTP Server that the Preboot Services client should connect to when it needs to download files.

Application Server IP: This IP address will be returned to Preboot Services clients requesting Proxy DHCP information and should contain the IP Address of the Preboot Services TFTP Server that the Preboot Services client should connect to when it needs to request an application from the system.

The MTFTP settings in this window should be the same as the settings that appear in the MTFTP Configuration Utility. Do not modify the Client Port, Open Timeout, and Reopen Timeout settings from their default values.

3. Click Save All to save new settings.

   or

   Click Exit to terminate the configuration utility without saving changes.

You can set any of the IP Address fields in the configuration utility to 0.0.0.0. The server replaces these entries with the IP address of the first network adapter installed in the server.

Setting Up Preboot Services Servers in NetWare

Once ZfD 3.2 Preboot Services has been installed, it is seldom necessary to change the default server values. If you do decide to change the settings, however, you can do so by editing the appropriate .INI file for the server you want to change. These .INI files can be found on the Preboot Services server in the SYS:\SYSTEM directory.

This section contains the following information:

- "Configuring the MTFTP/TFTP Module" on page 18
- "Configuring the Proxy DHCP Module" on page 18
- "Configuring the Transaction Server Module" on page 19

Configuring the MTFTP/TFTP Module

You can set the path that the MTFTP/TFTP module will use for file access by modifying the TFTP.INI file. The following options are available:

ReadPath: Set the path that the MTFTP/TFTP module will use for read access. The default value for this setting is SYS:\TFTP\.

WritePath: Set the path that the MTFTP/TFTP module will use for write access. The default value for this setting is SYS:\TFTP\.

WriteProtect: Set the value to 0 to cause the MTFTP/TFTP module to accept write requests, or set the value to 1 to disallow write requests.

NOTE: The variable names (for example, ReadPath) are case sensitive.

Configuring the Proxy DHCP Module

You can set the parameters that the Proxy DHCP module will use by modifying the PDHCP.INI file. The following options are available:

VSP_IP: The IP address of the Transaction Server that will be supplied to PXE clients when they request Proxy DHCP information.

TFTP_IP: The IP address of the TFTP Server that will be supplied to PXE clients when they request Proxy DHCP information.

APP_IP: The IP address of the application server that will be supplied to PXE clients when they request Proxy DHCP information.

USE_DHCP_PORT: Specify whether to bind to the DHCP Server socket (67). Set this to 0 if you are running a DHCP Server on the same machine as the Proxy DHCP module, and make sure that you have set up a PXEClient DHCP Option Tag on the DHCP Server.

USE_BINL_PORT: USE_BINL_PORT - Whether to bind to the BINL socket (4011). This is only necessary if you are running proxy DHCP and another DHCP Server on the same machine. Set this to 1 to bind to the BINL port.

BOOT_MENU_TIMEOUT: Set this option to set how long (in seconds) the boot menu should be shown to the user. A value of 0 means that the Preboot Services boot will be auto-selected by PXE, and a value of 255 means wait indefinitely. Change this value if you have other PXE type services on the network, like Microsoft* RIS.

NOTE: The variable names (for example, VSP_IP) are case sensitive.

Configuring the Transaction Server Module

You can set the parameters that the Transaction Server module will use by modifying the DTS.INI file. The following option is available:

Server UdpPort: Set this value to the UDP port number you want to use.

NOTE: This variable name is case sensitive.

Configuring IP Port Usage in ZfD 3.2 Preboot Services

This section describes the network ports used by ZfD 3.2 Preboot Services. Using this information in this section, you can configure routers or firewalls to correctly forward the network traffic generated by Preboot Services.

Available Ports

ZfD 3.2 Preboot Services uses both well-known and proprietary IP ports.

The well-known IP ports include:

- **67 decimal:** The Proxy DHCP services listens on this port for PXE information requests. This is the same port used by a standard DHCP service.
- **69 decimal:** The TFTP service listens on this port for file requests from PXE or Preboot Services clients.
- **111 decimal:** Port mapper port. Refer to RFC 1057 (http://sunsite.iisc.ernet.in/collection/rfc/rfc1057.html) for a description of this server.

The proprietary IP ports include:

- **18753 decimal:** Transaction Server client connection port. The Transaction Server receives all connection requests from the Preboot Services clients on this port.
- **360 decimal:** The MTFTP service listens on this port for MTFTP requests from PXE or Preboot Services clients.

Changing Port Usage in Windows NT 4.0 Server

The Transaction Server service and MTFTP service can be configured to use different ports if necessary. To change the port, use the following procedure:

1. From the Windows server desktop, click Start > Programs > ZEN Preboot Services > ZEN Preboot Services Configuration > *preboot_service_configuration.*
2. Change the relevant settings in the configuration.
3. Stop and start the services for the changes to take effect.

Changing Port Usage in NetWare

1. Edit the DTS.INI file located in the same directory as the DTS.NLM module.
2. Set ServerUdpPort to the port number you want to use.
3. Stop and start DTS.NLM for the changes to take effect.

A Acronyms

The following table lists the acronyms that are commonly used in this and other ZENworks™ for Desktops 3.2 Preboot Services documentation.

Acronym	Description
API	Application program interface
BIOS	Basic input/output operating system
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
LAN	Local area network
MTFTP	Multicast Trivial File Transfer Protocol
NBP	Network bootstrap program
NDS™	Novell® Directory Service
NFS	Network File System
NTFS	New Technology File System
PXE	Preboot Execution Environment
TFTP	Trivial File Transfer Protocol
WAN	Wide area network
WfM	Wired for Management
ZfD	Novell ZENworks for Desktops

Glossary

The terminology and concepts used in the ZENworks™ for Desktops Preboot Services documentation are listed in this section.

application program interface (API)

An application program interface (API) is the specific method prescribed by a computer operating system or by another application program by which a programmer writing an application program can make requests of the operating system or application.

Bootstrap Protocol

BOOTP (Bootstrap Protocol) is a protocol that lets a network user be automatically configured (receive an IP address) and have an operating system boot or initiate without user involvement. The BOOTP Server, managed by a network administrator, automatically assigns the IP address from a pool of addresses for a certain duration of time.

BOOTP is the basis for a more advanced network manager protocol, the Dynamic Host Configuration Protocol (DHCP).

client

A client is the requesting program or user in a client/server relationship. For example, the user of a Web browser is effectively making client requests for pages from servers all over the Web. The browser itself is a client in its relationship with the computer that is getting and returning the requested HTML file. The computer handling the request and sending back the HTML file is a server.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocols (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a “lease” or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It’s especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

FTP

File Transfer Protocol. A part of the TCP/IP suite of control procedures for downloading files from a remote host computer to a local computer. FTP can be implemented either from a Telnet client by using mostly UNIX commands, or by using a software program such as LAN WorkPlace that automates many of the functions for you. The FTP protocol is also supported by many World Wide Web browsers such as Mosaic* and Netscape*.

host

On the Internet, the term "host" means any computer that has full two-way access to other computers on the Internet. A host has a specific "local or host number" that, together with the network number, forms its unique IP address.

If you use Point-to-Point Protocol (PPP) to get access to your access provider, you have a unique IP Address for the duration of any connection you make to the Internet and your computer is a host for that period. In this context, a "host" is a node in a network.

The term generally means a device or program that provides services to some smaller or less capable device or program.

HTTP

Hypertext Transfer Protocol. The protocol that Web servers and Web browsers use to communicate with each other on the World Wide Web (WWW). Web browsers submit HTTP requests; Web servers use HTTP to respond with the requested document. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

Essential concepts that are part of HTTP include (as its name implies) the idea that files can contain references to other files whose selection will elicit additional transfer requests. Any Web server machine contains, in addition to the HTML and other files it can serve, an HTTP daemon, which is a program that is designed to wait for HTTP requests and handle them when they arrive. Your Web browser is an HTTP client, sending requests to server machines. When the browser user enters file requests by either opening a Web file (typing in a URL) or clicking on a hypertext link, the browser builds an HTTP request and sends it to the IP address indicated by the URL. The HTTP daemon in the destination server machine receives the request and, after any necessary processing, the requested file is returned.

IP address

An IP address is a 32-bit number that identifies each sender or receiver of information that is sent in packet across the Internet. Consisting of network and node portions, the address is represented in standard decimal notation (for example, 123.45.6.7).

When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message. It then sends it to the IP address that is obtained by looking up the domain name in the URL you requested or in the e-mail address you're sending a message to. At the other end, the recipient can see the IP address of the Web page requester or the e-mail sender and can respond by sending another message using the IP address it received.

An IP address has two parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. On the Internet itself—that is, between the routers that move packets from one point to another along the route—only the network part of the address is looked at.

Point-to-Point Protocol

An industry-standard protocol that enables point-to-point transmissions of routed data. The data is sent across transmission facilities between interconnected LANs by using a synchronous or an asynchronous serial interface.

Preboot Execution Environment

The Preboot Execution Environment (PXE) is an industry standard client/ server interface that allows networked computers that are not yet loaded with an operating system to be configured and booted remotely by an administrator. The PXE code is typically delivered with a new computer on a read-only memory chip or boot disk that allows the computer (a client) to communicate with the network server so that the client machine can be remotely configured and its operating system can be remotely booted. PXE provides three things:

1. The Dynamic Host Configuration Protocol (DHCP), which allows the client to receive an IP address to gain access to the network servers.

2. A set of application program interfaces (APIs) that are used by the client's basic input/output system (BIOS) or a downloaded Network Bootstrap Program (NBP) that automates the booting of the operating system and other configuration steps.

3. A standard method of initializing the PXE code in the PXE ROM chip or boot disk.

The PXE process consists of the client notifying the server that it uses PXE. If the server uses PXE, it sends the client a list of boot servers that contain the operating systems available. The client finds the boot server it needs and receives the name of the file to download. The client then downloads the file using Trivial File Transfer Protocol (TFTP) and executes it, which loads the operating system. If a client is equipped with PXE and the server is not, the server ignores the PXE code, preventing disruption in the DHCP and Bootstrap Protocol operations.

The advantages of using PXE include:

- The client machine does not necessarily need an operating system or even a hard disk.

- The client machine can be rebooted in the event of hardware or software failure. This allows the Administrator to diagnose and perhaps fix the problem.

- Because PXE is vendor-independent, new types of computers can easily be added to the network.

Proxy Server

In an enterprise that uses the Internet, a Proxy Server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A Proxy Server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

A Proxy Server receives a request for an Internet service (such as a Web page request) from a user. If it passes filtering requirements, the Proxy Server, assuming it is also a cache server, looks in its local cache of previously downloaded Web pages. If it finds the page, it returns it to the user without needing to forward the request to the Internet. If the page is not in the cache, the Proxy Server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from the server on the Internet. When the page is returned, the Proxy Server relates it to the original request and forwards it on to the user.

To the user, the Proxy Server is invisible; all Internet requests and returned responses appear to be directly with the addressed Internet server. (The proxy is not quite invisible; its IP address must be specified as a configuration option to the browser or other protocol program.)

An advantage of a Proxy Server is that its cache can serve all users. If one or more Internet sites are frequently requested, these are likely to be in the proxy’s cache, which will improve user response time. In fact, there are special servers called cache servers. A proxy can also do logging.

The functions of proxy, firewall, and caching can be in separate server programs or combined in a single package. Different server programs can be in different computers. For example, a Proxy Server may in the same machine with a firewall server or it may be on a separate server and forward requests through the firewall.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP). A protocol suite developed by the Advanced Research Projects Agency (ARPA). It includes TCP (Transmission Control Protocol) as the primary transport protocol and IP (Internet Protocol) as the network layer protocol.

TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you have direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer.

Many Internet users are familiar with the even higher layer application protocols that use TCP/IP to get to the Internet. These include the World Wide Web's Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), Telnet, which lets you log on to remote computers, and the Simple Mail Transfer Protocol (SMTP). These and other protocols are often packaged together with TCP/IP as a "suite."

Telnet

A protocol in the TCP/IP suite that governs character-oriented terminal traffic. Telnet supports character terminals, block terminals, and graphics terminals. It is used for remote login on an Internet network.

Trivial File Transfer Protocol

TFTP (Trivial File Transfer Protocol) is a network application that is simpler than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP).

UDP

User Datagram Protocol. A transport protocol in the Internet suite of protocols. UDP, like Transmission Control Protocol (TCP), uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgement or guaranteed delivery.

URL

A URL (Uniform Resource Locator) is the address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol. Using the World Wide Web's protocol, the Hypertext Transfer Protocol (HTTP), the resource can be an HTML page, an image file, a program such as a common gateway interface application or Java* applet, or any other file supported by HTTP. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

On the Web (which uses the Hypertext Transfer Protocol), an example of a URL is:

```
http://www.novell.com/documentation
```

This describes a Web page to be accessed with an HTTP (Web browser) application that is located on a computer named www.novell.com. Specific files are located in the directory named /documentation.