Novell ZENworks® for Desktops Preboot Services

3.2

www.novell.com

DEPLOYMENT

Novell®

Legal Notices

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

www.novell.com

Deployment

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

Novell Trademarks

NDS is a registered trademark of Novell, Inc., in the United States and other countries.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.
ZENworks is a registered trademark of Novell, Inc.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

About this Guide

This guide contains information that will help you understand and deploy Novell® ZENworks® for Desktops 3.2 Preboot Services.

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 Deploying Preboot Services In a Network Environment

To implement the strategies outlined in this guide, you must have a solid understanding of the TCP/IP network protocol and specific knowledge of TCP/IP routing and the DHCP discovery process. This guide is intended for network administrators and consultants who need to plan the deployment of Novell® ZENworks® for Desktops 3.2 Preboot Services (PXE) in their network.

Deploying PXE in a local area network is relatively simple process that only requires configuring the PXE server. However, PXE deployment in a routed environment is far more complex and generally requires configuration of both the PXE server and the network switches and routers that lie between the server and the PXE workstations.

Configuring the routers or switches to correctly forward PXE network traffic requires a solid understanding of the DHCP protocol, DHCP relay agents, and IP forwarding. The actual configuration of the switch or router will need to be carried out by a person with detailed knowledge of the hardware.

It is strongly recommended that you initially set up PXE in a LAN environment to ensure that the servers are configured correctly and are operational.

Minimum Requirements

For information about minimum software and hardware requirements, see Hardware and Software Requirements in Installation.

Explanation of Typical PXE Operation

When a PXE workstation starts to boot up, it performs a DHCP discovery. During this process the workstation obtains IP information for itself and also information about the PXE boot servers that it can connect to. After completing the DHCP discovery process, the workstation contacts the boot server, downloads a file through Trivial File Transfer Protocol (TFTP), and executes the file.

The DHCP discovery process is more complex for a PXE workstation than it is for other DHCP-based products. During the DHCP discovery process the PXE workstation sends out a DHCP discovery request. Both the DHCP server and Proxy DHCP service need to receive and respond to this packet. The DHCP server will respond with IP address information for the client to use, and the Proxy DHCP server will respond with information about the boot server to use as well as the name of the boot file to download and execute.

The PXE workstation downloads the boot file that was specified during the DHCP discovery process by using either TFTP or multicast TFTP (MTFTP). In the case of the default Preboot Services implementation, the PXE workstation will always use TFTP because it speeds up the boot process of the workstation. The boot file (DINIC.SYS) is very small, so downloading it through MTFTP will not significantly reduce the network utilization of the product.

Server Configuration

The PXE environment requires a DHCP server, Proxy DHCP server, TFTP boot server and Transaction server to function correctly.

DHCP Server

The DHCP server must be configured with an active scope that will allocate IP addresses to the PXE workstations. The scope options should also specify the gateway or router that the PXE workstations should use.

If the PXE services are installed on the same server as the DHCP service, then the DHCP service must be configured with a special option tag. Configure option tag 60 as a string and set it to the value **`PXEClient`**.

IMPORTANT: Installing and running the Proxy DHCP Server on a NetWare 5.*x* server that is already running a standard DHCP server is not supported.

Proxy DHCP Server

It is seldom necessary to make any changes to the default configuration.

If you want to run the Proxy DHCP server on a different server from the Transaction server or TFTP server, you can change the Proxy DHCP settings to direct PXE workstations to a server other than the Proxy DHCP server.

Transaction Server

It is seldom necessary to make any changes to the default configuration.

You can change the UDP port that the Transaction server uses for communicating with the preboot client. You should only do this if the Transaction server is conflicting with another service running on the server.

Network Configuration

This section covers the following topics:

LAN

A PXE workstation will broadcast for DHCP information and receive a response from both the DHCP and Proxy DHCP services. The workstation will then download the preboot client and check for work with the Transaction server.

No special configuration is required in a LAN environment. Make sure that the DHCP server is allocating IP addresses and that the Proxy DHCP and TFTP services are started.

WAN

In a wide area network environment, the PXE workstation is usually separated from the Proxy DHCP and DHCP servers by one or more routers. The PXE

workstation will broadcast for DHCP information, but by default the router will not forward the broadcast to the servers, causing the PXE session to fail.

There are two ways to make PXE work correctly in a WAN:

- The first, and preferable, way is to configure a DHCP relay agent or IP helper on the router serving the subnet that the PXE workstation belongs to. The helper is configured to forward all DHCP broadcasts that are detected in the subnet to the DHCP and Proxy DHCP servers. This normally requires that two helpers are configured: the first to forward DHCP broadcasts to the DHCP server, and the second to forward the DHCP broadcasts to the Proxy DHCP server.

  A DHCP broadcast is a UDP broadcast frame with the destination port set to 67.

- The second way to configure PXE is to install a Proxy DHCP server and a TFTP server on every subnet that has PXE workstations present. Configure the Proxy DHCP server so it supplies the IP address of a central Transaction server. For information about changing the Proxy DHCP configuration, see *Administration*.

  With this solution, the PXE workstation will receive a response from a Proxy DHCP server located on its subnet, but it is redirected to a single central Transaction server to check for work to do.

VLAN

In a VLAN environment, the PXE workstation is logically separated from the Proxy DHCP server and the DHCP server by a switch. At the IP level, this configuration looks very similar to a traditional WAN or routed environment.

Configuration of a VLAN is basically the same as a WAN. Configure the VLAN that the PXE workstation belongs to with a DHCP relay agent or IP helper to forward DHCP broadcasts to the DHCP server and the Proxy DHCP server, or place a Proxy DHCP server and a TFTP server in each VLAN to serve the PXE workstations directly.

Configuring Filters on Switches and Routers

Some network devices filter network traffic that passes through them. PXE makes use of several different types of traffic, and all of these must be able to pass through the router or switch successfully for the PXE session to be successful. The PXE session will use the following destination ports:

Component	Port
DHCP and Proxy DHCP	UDP Port 67
TFTP	UDP Port 69
RPC Port Map Service	UDP Port 111
Transaction Service	UDP Port 18753

Spanning Tree Protocol in Switched Environments

Spanning tree protocol (STP) is available on certain switches and is designed to detect loops in the network. When a device (typically a network hub or a workstation) is patched into a port on the switch, the switch indicates to the device that the link is active, but instead of forwarding frames from the port to the rest of the network, the switch checks each frame for loops and then drops it. The switch can remain in this listening state from anywhere between 15 to 45 seconds.

The affect of this is to cause the DHCP requests issued by PXE to be dropped by the switch, causing the PXE session to fail.

It is normally possible to see that the STP is in progress by looking at the link light on the switch. When the workstation is off, the link light on the switch is obviously off. When the workstation is turned on, the link light changes to amber, and after a period changes to a normal green indicator. As long as the link light is amber, STP is in progress.

This problem will only affect PXE or preboot clients that are patched directly into an Ethernet switch. To correct this problem, perform one of the following:

- Turn off STP on the switch entirely.
- Set STP to Port Fast for every port on the network switch where a PXE workstation is attached.

Once the problem is resolved, the link light on the port should change to green almost immediately after a workstation connected to that port is turned on.

Information about STP and its influence on DHCP can be found at Using PortFast and Other Commands to Fix End-Station Startup Connectivity Problems (http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1923.htm#xtocid897350).

WAN/VLAN Example Deployment

In the Overview of this section, an example deployment of PXE is given for a WAN/VLAN environment. Then, the following sections provide the specific steps required to configure network equipment so that they will correctly forward PXE network traffic:

- "Configuring Cisco Equipment" on page 15
- "Configuring Nortel Network Equipment" on page 15
- "Configuring Bay Network Equipment" on page 16

Overview

In this example, three VLAN are configured on a Bay Networks Accel 1200 switch running firmware version 2.0.1. One VLAN hosts the Proxy DHCP service, the second VLAN hosts the DHCP service, and the third VLAN hosts the PXE client. The PXE client's DHCP broadcast is forwarded by the switch to both the Proxy DHCP service and the DHCP service. The response from both servers is then routed correctly back to the PXE client, and the PXE client starts the PXE session correctly.

The three VLANs are all 24-bit networks, that is their subnet mask is 255.255.255.0

The first VLAN gateway is 10.0.0.1. This VLAN hosts the PXE client that is allocated an IP in the range of 10.0.0.2 to 10.0.0.128. This VLAN is named VLAN1.

The second VLAN gateway is 10.1.1.1. This VLAN hosts the DHCP server with IP 10.1.1.2. This VLAN is named VLAN2.

The third VLAN gateway is 196.10.229.1. This VLAN hosts the server running the Proxy DHCP server and the Transaction server. The server's IP is 196.10.229.2. This VLAN is named VLAN3.

Routing is enabled between all the VLANs. Each VLAN is (and must be) in its own spanning tree group.

Configuring Cisco Equipment

1. Go to Global Configuration mode.
2. Type **`ip forward-protocol udp 67`** and press Enter.
3. Type **`ip forward-protocol udp 68`** and press Enter.
4. Go to the LAN interface that serves the PXE workstation.
5. Type **`ip helper-address 10.1.1.2`** and press Enter.
6. Type **`ip helper-address 196.10.229.2`** and press Enter.
7. Save the configuration.

Configuring Nortel Network Equipment

1. Connect to the router with Site Manager.
2. Ensure that IP is routable.
3. Enable Bootp on the PXE workstation subnet/VLAN.
4. Select the interface that the PXE workstations are connected to.
5. Edit the circuit.
6. Select Protocols.
7. Select Add/Delete.
8. Ensure there is a check in the Bootp check box.
9. Press OK.
10. Select Protocols > IP > Bootp > Relay Agent Interface Table.

    The interface where Bootp was enabled will visible in the list.
11. Click Preferred Server.
12. Change the Pass Through Mode value to Bootp and DHCP.

Set up the relay agents:

1. Click Add.
2. In the Relay Agent IP Address box, type the local LAN IP address.
3. In the Target Server IP Address box, type the DHCP server IP address.
4. Click OK.
5. Change the Pass Through Mode value to Bootp and DHCP.

6. Perform steps 1-5 again and enter the Proxy DHCP server IP address at Step 3.
7. Apply the configuration.

Configuring Bay Network Equipment

Perform the following steps on the switch:

1. Enable DHCP for the client VLAN using the following command lines:

```
# config vlan1 ip
# dhcp enable
```

2. Configure ip helpers to forward DHCP requests from the workstation subnet to the Proxy DHCP service, using the following command lines:

```
# config ip dhcp-relay
# create 10.0.0.1 10.1.1.2 mode dhcp state enable
# create 10.0.0.1 196.10.229.2 mode dhcp state enable
```

   The create command has the form **`create agent server mode dhcp state enable,`** where ***`agent`*** is the IP address of the gateway that serves the PXE workstation, and ***`server`*** is the IP address of the server that the DHCP frame should be forwarded to.

3. Save the configuration.

A Acronyms

The following table lists the acronyms that are commonly used in this and other Novell® 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 Novell® ZENworks® for Desktops 3.2 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.