A Project Report on

Installation of OS via Network

COMPUTER DEPARTMENT

by

Yuvraj Yadav (16102040)
Tanmay Sule (16102032)
Ashwin Shenolikar (16102037)

Under the guidance of

Prof. Sofiya Mujawar

Department of Computer Engineering
A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615
UNIVERSITY OF MUMBAI

Academic Year 2018-2019

Approval Sheet

This Project Report entitled ***Installation of OS via Network*** Submitted by ***Yuvraj Yadav (16102040), Tanmay Sule(16102032) and Ashwin Shenolikar(16102037)*** is approved for the partial fulfilment of the requirement for the award of the miniproject in ***Computer Department*** from ***University of Mumbai.***

Prof. Sofiya Mujawar
[Guide]

Prof. Sachin Malave
Head Department of Computer Engineering

Department Of Computer Engineering
PCT'S
APSIT

Place: A.P.Shah Institute of Technology, Thane
Date:15th April,2019

CERTIFICATE

This is to certify that the project entitled ***Installation of OS via Network*** submitted by ***Yuvraj Yadav (16102040), Tanmay Sule(16102032) and Ashwin Shenolikar(16102037)*** for the partial fulfilment of the requirement for award of a ***Miniproject*** in ***Computer Department***, to the University of Mumbai, is a bonafide work carried out during academic year 2018-2019

Prof. Sofiya Mujawar
[Guide]

Prof. Sachin Malave
Head Department of Computer Engineering

Dr. Uttam D.Kolekar
Principal

Department Of Computer Engineering
PCT'S
APSIT

External Examiner(s)

Place: A.P.Shah Institute of Technology, Thane
Date : 15th April 2019

Declaration

We declare that this written submission represents our ideas in our own words and where others ideas or words have been included, We have adequately cited and referenced the original sources. We also declare that We have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Yuvraj Yadav (16102040)

Tanmay Sule(16102032)

Ashwin Shenolikar (16102037)

Date:15th April 2019

Abstract

The majority of schools, colleges, offices and other such establishments have become reliant on computers for various purposes. As the computer industry is evolving rapidly, such institutions often find it difficult and tedious to keep every system updated.

The major objective here is to provide a very easy-to-use, reliable, and quick method to update every system connected in a network with the latest OS versions, or even to just install binaries and libraries required by the institution in all systems of the institution. Furthermore, this method also acts as the ultimate backup as soft-bricked systems can be wiped and used using this method.

The Operating Systems employed are open source linux distributions, as well as an open source cloning feature to replicate a system's exact structure onto another system. All these functionalities are packed together in a neat and user-friendly manner. This gives even a naïve user a sense of ease as simple as installing an application on their phone.

It is a self-reliant model which does not have any pre-requisite except for of course, the network itself, which consists of a minimum of 2 computers, 3 for cloning. It is a powerful way to make essential yet tedious tasks required by an organization to be carried out effortlessly.

Contents

CHAPTER 1: INTRODUCTION

Computers have become a staple in today's world. In the past decade, it is observed that there has been a huge rise in number of computers manufactured and sold. The specifications of computer technology have been improving and so has the software associated with it. It has resulted in the huge number of industries, educational institutions and any other such multi-system enterprises to rely on them almost exclusively. As a result, it is also important for these to keep updated systems in their buildings, so that they can avail of the best software. However, this is often time consuming and tedious, and in some cases, too complicated for naïve users to do. This is where our project comes in. It can help anyone to stay updated without going through a hassle.

The open source technologies used in our project work in collaboration to install operating systems in every system in a network. Also, with the help of cloning tools we can reproduce a system exactly as it is on another.

This all happens by first having the target machine booted from the network, following simple UI which gives it the option for cloning or installing operating systems. In the backend of the server, a combination of PXEboot, TFTP, and DHCP server is used to achieve file transfer through a network for installation, while PXE is used to let the NIC card act as a node.

CHAPTER 2: LITERATURE REVIEW

Sr. No.	Title Of Paper	Author	Abstract
1.	A P2P Network Booting Scheme Using a BitTorrent-Like Protocol	Wigi Vei A. Oliveros ; Cedric Angelo M. Festin ; Roel M. Ocampo	Network booting is widely used today, mostly for thin-client computing, cluster computing, and operating system installation. Popular protocols like trivial file transfer protocol (TFTP) and hypertext transfer protocol (HTTP) are used to download operating system images.
2.	A P2P Approach to Scalable Network-Booting	Shingo Takada ; Akira Sato ; Yasushi Shinjo ; Hisashi Nakai ; Akiyoshi Sugiki ; Kozo Itano	Network-booting is widely adopted in universities that have to maintain many client computers. In conventional network-booting systems, the primary bottleneck is the disk image distribution servers and the network to these servers. To eliminate this bottleneck, peer-to-peer (P2P) methods must work.

CHAPTER 3: The Essentials:

3.1 Preboot eXecution Environment (PXE)

PXELINUX is a SYSLINUX derivative, for booting Linux off a network server, using a network ROM conforming to the Intel PXE (Pre-Execution Environment) specification. PXELINUX is *not* a program that is intended to be flashed or burned into a PROM on the network card.

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 (API) that are used by the client's Basic Input/Output Operating 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 (Trivia File Transfer Protocol) 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 (BP) 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.
- Since PXE is vendor-independent, new types of computers can easily be added to the network.

3.2: TFTP

File transfer is one of the most essential technologies for client/server and computer network infrastructures.

Trivial File Transfer Protocol is very simple in design and has limited features as compared to File Transfer Protocol (FTP). TFTP provides no authentication and security while transferring files. As a result, it is usually used for transferring boot files or configuration files between machines in a local setup. Because of its simple design, it is rarely used interactively by users in a computer network. Its lack of security also makes it dangerous for use over the Internet.

TFTP is very useful for boot computers and devices that do not have hard disk drives or storage devices because it can easily be implemented using a small amount of memory. This characteristic of TFTP makes it one of the core elements of network boot protocol, or preboot execution environment (PXE).

Data transfer through TFTP is usually initiated through port 69. However, the data transfer ports are selected by the sender and receiver when the connection is initialized.

3.3: DHCP

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP. DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices. DHCP can be implemented on small local networks as well as large enterprise networks.

DHCP will assign new IP addresses in each location when devices are moved from place to place, which means network administrators do not have to manually initially configure each device with a valid IP address or reconfigure the device with a new IP address if it moves to a new location on the network. Versions of DHCP are available for use in Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

3.4: Clonezilla

Clonezilla is a partition and disk imaging/cloning program similar to True Image® or Norton Ghost®. It helps you to do system deployment, bare metal backup and recovery. Three types of Clonezilla are available, Clonezilla live, Clonezilla lite server, and Clonezilla SE (server edition). Clonezilla live is suitable for single machine backup and restore. While Clonezilla lite server or SE is for massive deployment, it can clone many (40 plus!) computers simultaneously. Clonezilla saves and restores only used blocks in the hard disk. This increases the clone efficiency. With some high-end hardware in a 42-node cluster, a multicast restoring at rate 8 GB/min was reported.

4.1: WORKING

One of the key requirements of provisioning is the hardware server's ability to boot over the network instead of a diskette or CD-ROM. There are several ways computers can boot over a network, and Preboot Execution Environment (PXE) is one of them. PXE is an open industry standard supported by a number of hardware and software vendors. PXE is part of the "Wired for Management" (WfM) specification, which is part of a bigger PC98 specification defined by Intel and Microsoft in 1998. A detailed document on PXE specification can be found at http://www.pix.net/software/pxeboot/archive/pxespec.pdf.

PXE works with Network Interface Card (NIC) of the system by making it function like a boot device. The PXE-enabled NIC of the client sends out a broadcast request to DHCP server, which returns with the IP address of the client along with the address of the TFTP server, and the location of boot files on the TFTP server. The following steps describe how it works:

1. Target Machine (either bare metal or with boot sector removed) is booted.
2. The Network Interface Card (NIC) of the machine triggers a DHCP request.
3. DHCP server intercepts the request and responds with standard information (IP, subnet mask, gateway, DNS etc.). In addition, it provides information about the location of a TFTP server and boot image (pxelinux.0).
4. When the client receives this information, it contacts the TFTP server for obtaining the boot image.
5. TFTP server sends the boot image (pxelinux.0), and the client executes it.
6. By default, the boot image searches the pxelinux.cfg directory on TFTP server for boot configuration files on the TFTP server using the following approach:

   First, it searches for the boot configuration file that is named according to the MAC address represented in lower case hexadecimal digits with dash separators. For example, for the MAC Address "88:99:AA:BB:CC:DD", it searches for the file 01-88-99-aa-bb-cc-dd.

Then, it searches for the configuration file using the IP address (of the machine that is being booted) in upper case hexadecimal digits. For example, for the IP Address "192.0.2.91", it searches for the file "C000025B".

If that file is not found, it removes one hexadecimal digit from the end and tries again. However, if the search is still not successful, it finally looks for a file named "default" (in lower case).

For example, if the boot file name is /tftpboot/pxelinux.0, the Ethernet MAC address is 88:99:AA:BB:CC:DD, and the IP address 192.0.2.91, the boot image looks for file names in the following order:

```
/tftpboot/pxelinux.cfg/01-88-99-aa-bb-cc-dd
/tftpboot/pxelinux.cfg/C000025B
/tftpboot/pxelinux.cfg/C000025
/tftpboot/pxelinux.cfg/C00002
/tftpboot/pxelinux.cfg/C0000
/tftpboot/pxelinux.cfg/C000
/tftpboot/pxelinux.cfg/C00
/tftpboot/pxelinux.cfg/C0
/tftpboot/pxelinux.cfg/C
```

7. The client downloads all the files it needs (kernel and root file system), and then loads them.
8. Target Machine reboots.

4.1.1: SOFTWARE/HARDWARE USED:

We have used PXE, TFTP and DHCP as our main technologies for our primary task, and Clonezilla for our secondary task. Apart from these, dnsmasq, gedit, and other such utilities are used to configure system settings to make our model work.

CHAPTER 5: RESULTS

We found that with the help of these tools, we can create a user-friendly and easy-to-use compiled bootloader which is used for the task of network booting. Network booting is the best choice for large scale installation or updation of multiple operating systems.

CHAPTER 6: CONCLUSIONS AND FUTURE SCOPE

The project proposes a generic method for OS installation combined with various additional optimizations. With this, educational institutes such as schools, colleges and universities will be able to keep up with the latest advances in this particular aspect of technology. But when combined with cloning, one system with all the latest software can be cloned to not only update operating systems of every node in the network, but also make it so that it comes with the latest required modules and applications which are required by the aforementioned organizations. It is found that the first step to do most computer tasks, that is, the setup, is where naïve users often get stuck in and get discouraged.

In the future, we aim to implement a universal network booting server from where a great variety of OSs can be installed with required specifications.

Acknowledgement

We have great pleasure in presenting the report on Installation of OS via Network . We take this opportunity to express our sincere thanks towards our guide Prof. Sofiya Mujawar, Department of COMPUTER, APSIT Thane for providing the technical guidelines and suggestions regarding line of work. We would like to express our gratitude towards her constant encouragement, support and guidance through the development of project. We thank Prof. Sachin Malave Head of Department, Computer, APSIT for his encouragement during progress meeting and providing guidelines to write this report. We also thank the entire staff of APSIT for their invaluable help rendered during the course of this work. We wish to express our deep gratitude towards all our colleagues of APSIT for their encouragement.

Student Name1 : Yuvraj Yadav

Student ID1 : 16102040

Student Name2 : Tanmay Sule

Student ID2 : 16102032

Student Name3 : Ashwin Shenolikar

Student ID3 : 16102037