Linux를 이용한 PC실 관리

서울시립대학교 민현수

1. 서 론

대학의 PC실, 대기업이나 중소기업의 사무실 뿐만 아니라 최근 급속히 숫자가 불어나고 있는 게임방, PC방 들과 같이 컴퓨터의 보급이 확장되면서 LAN을 이용하여 집단으로 PC를 사용하는 환경이 급속히 늘어나고 있다. 이 경우 관리자는 PC들을 사용하기 좋은 상태로 유지하는데 많은 어려움을 느끼게 된다. 하드웨어 적인 문제는 시스템의 교체나 수리를 통하여 해결해야 겠지만 훨씬 더 많은 문제가 소프트웨어 관리에서 발생한다. 특히 MS-Windows와 같이 사용자 관리가 되지 않는 시스템의 경우 더욱 어려움이 가중된다. 사용자들이 임의로 설정을 바꾸고 시스템의 중요 파일을 손상시키는가 하면 불법 소프트웨어를 설치하거나 바이러스에 감염시키기도 하여 시스템사용이 불가능하도록 만든다 이 경우 관리자는 시스템을 재설치하거나 손상된 파일을 복구하는데 많은 시간과 노력을 소모하여야 한다. 이 문서에서는 Linux시스템을 사용하여 이러한 수고를 최소화하는 PC실 관리 방법을 제시하려 하고 있다.

우선 PC실의 OS상황을 보면 대다수의 경우 MS-Windows를 사용하고 있으며 부분적으로 Windows-NT를 사용하거나 Linux를 사용하고 있다. 이 문서에서는 Windows-NT의 경우는 고려하지 않고 Linux서버를 사용하여 관리되는 Windows PC실이나 Linux PC 실을 대상으로 하고 있다. 사용하는 OS나 환경에 따라 다음의 3가지 경우를 생각할 수 있다.

(A) Local system을 갖춘 Linux PC실
(B) Local system이 없는 Linux PC실
(C) Remote-boot를 이용한 Windows PC실

2. Local system을 갖춘 Linux PC실

이 경우 각각의 PC는 하드디스크를 장착하고 있어 독립적으로 Linux system이 설치되어 있다. Linux는 PC에서 사용하는 Unix이기 때문에 Unix의 모든 관리 도구들이 그대로 사용된다. 각각의 파일은 사용자에 따라 그 권한이 별도로 설정되어 있어 임의로 파일이 삭제되거나 변형되는 일이 없다. 개개인의 사용자 파일도 다른 사람이 함부로 열람하거나 손상시킬 수 없다. 바이러스 침투의 가능성도 상대적으로 매우 작다.

이러한 장점이 있는 반면에 각 PC마다 사용자 계정을 등록하여야 하고 Home directory 관리를 하여야 하는 문제가 있다. 각 사용자도 PC를 옮겨 사용할 때마다 자신의 파일을 이동시켜야 하는 불편함이 수반된다.

이러한 문제점을 해결하기 위해 NIS와 NFS를 사용한다 NIS는 사용자의 계정과 passwd 파일을 공유하게 함으로써 각 PC마다 사용자를 등록하는 불편함을 없애 주며 PC실 내 어느 PC에서 login 하든지 동일한 id와 passwd로 login 할 수 있게 해준다. 또한 NFS를 이용하여 각 사용자의 Home directory를 공유하게 하여 어느 PC에서 login 하든지 언제나 동일한 사용자 파일이 제공 되도록 한다. NIS와 NFS 설정 방법은 다음과 같다.

2.1 NIS 설정 안내

1980년대 중반, Sun Microsystem에서는 두 가지 protocol을 내놓았는데, 바로 NFS(Network File System)와 NIS(Network Information System)이다. 이들은 Network를 통해 여러개의 Workstation들을 하나의 시스템을 사용하는 것처럼 작동시켜주는 핵심적인 방법이다. 즉, NFS는 특정 디렉토리들이 어느 시스템에서나 동일하게 보여지도록 하며, NIS는 passwd나 group 등의 네트워크 정보 파일들을 하나의 서버에서 관리하도록 하여 나머지 시스템에서 서버에서 제공하는 새로운 정보를 받을 수 있도록 하는 것이다. 현재 Sun Microsystem에서는 NIS+를 제공하고 있는데, 이는 NIS version 3에 속하며, 우리가 구축하려고 하는 NIS version은 2이다. NIS의 별명으로 YP(Yellow Page)가 흔히 사용된다.

YP system은 네트워크 기반위에 구축이 되기 때문에 네트워크 상태가 안정적이어야 된다. 네트워크 상태가 불안정하면 데이터의 손실 및 클라이언트들의 오작동 등 여러 가지 좋지 않은 현상들이 일어나게 된다. 보통 하나의 서브넷에 서버와 클라이언트들이 같이 물려있으면 괜찮다.

YP system은 server와 client로 나눌 수 있다. Server의 설정은 다음과 같다. 먼저 ypserv-1.3.9-1.i386.rpm(1999년 12월 기준)을 구한다(참고 http://www.suse.de/~kukuk/nis).

[root@nis_server]# rpm- Uhv ypserv-1.3.5-1.i386.rpm의 방법으로 server package를 설치한다. 패키지를 설치하고 나서 group 이름을 정한다. 여기서는 group 이름을 NISUOS로 하겠다. Server에서 다음의 명령을 내리자.

```
[root@nis_server]# nisdomainname NISUOS
```

이렇게 하면 group 이름이 NISUOS로 설정된 것이다. 다음으로 해줄 일은 YP server daemon들을 실행하는 일이다.

```
[root@nis_server]# /etc/rc.d/init.d/ypserv start
[root@nis_server]# /etc/rc.d/init.d/yppasswdd
 start
```

yppasswdd의 역할은 client에서 암호를 바꿀 때 이를 처리해주는 daemon이고 ypserv의 역할은 각 client들에게 정보를 주는 역할을 한다. 다음은 각 client들에게 보낼 정보를 만들어 보자.

```
[root@nis_server]# cd /var/yp
[root@nis_server]# grpconv
[root@nis_server]# pwconv
[root@nis_server]# echo NISUOS >
/etc/netgroup
[root@nis_server]# make
```

이렇게 함으로써 서버의 실행은 끝이다. 다음에 할 일은 부팅시 서버가 실행되도록 시작할때의 설정을 바꾸는 일이다.

```
[root@nis_server]# ntsysv
```

ntsysv명령은 부팅시 실행되어야 할 서버들의 목록을 나열해준다. 다음에는 /etc/rc.d/ypserv를 수정한다. "+++부분"은 에디터를 이용해서 추가해주기 바란다.

```
.....
# See how we were called.
case "$1" in
  start)
        echo -n "Starting YP server services: "
        nisdomainname NISUOS        ← +++
        daemon ypserv
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && touch
         /var/lock/subsys/ypserv
        ;;
  stop)
.. ..
```

Client에서 처음 설치시 계정관리부분에서 NIS(YP)를 사용한다고 선택하고 서버주소 또는 nis domainname(group name)을 적어주면 된다. 자세한 한글 문서는 KLDP 사이트(http://www.kldp.org) 또는 KLDP Mirror site (ftp://ftp.uos.ac.kr/pub/KLDP)에서 구할 수 있다.

주의사항 : 계정을 추가할 때마다 /var/yp의

위치로 가서 make를 해주어서 NIS정보를 갱신 시켜주어야 한다. 이런 작업이 번거로울 때는 cron을 사용하여 매일 특정 시간에 이 작업이 이루어 지도록 하면 된다.

클라이언트에서는 yppasswd명령어를 사용하여 바꾸면 관리자가 /var/yp에서 make를 칠 필요는 없다. YP를 사용 할 때 다음 사항에 주의하여야 한다. 클라이언트에서는 서버의 root 패스워드를 따르지 않는다. 즉, root는 독립적인 암호를 가질 수 있다. 만약을 위해서라도 서버와 클라이언트 사이의 root 암호는 다르게 설정하는 것이 좋다. YP system은 보안상 취약점이 많다. 일단 클라이언트쪽에 크래커가 침입하면 크래커는 서버에서 주는 계정에 대한 정보를 얻을 수 있다. 관리자는 사용자들에게 주기적으로 암호를 바꾸도록 권고하는 것이 좋다. 그리고 서버에 남아있는 log 파일을 주기적으로 조사해 보는 것도 보안상 좋은 방법 중에 하나이다. 만약 의심스러운 곳에서 속을 시도하는 것을 확인했으면 /etc/hosts.allow나 /etc/hosts,deny 파일을 설정하여 외부 침입을 막을 수 있다.

다음은 클라이언트에서 yp system에 의해 부가적으로 사용하게 될 명령어들이다. 기존 명령에 yp만을 붙였다는 것이 공통점이다.

yppasswd : 암호 바꾸기. passwd명령과 동일한 효력을 가지고 있다.

ypchfn : finger 자료 바꾸기. chfn과 같다.

ypchsh : shell을 바꾸는 명령

이밖에도 명령어가 더 있지만, 잘 사용하지 않으므로 생략한다.

2.2 NFS 설정 안내

NFS는 Network File System의 약자로, Sun Microsystem사가 내놓은 파일시스템이다. NFS의 강점은 local 머신이 아닌 다른 머신의 하드를 자신의 머신에 있는 것처럼 사용할 수 있도록 네트워크를 이용하여 만드는 가상 파일 시스템이다. 편의상 여기서 사용하게될 서버의 이름은 nfs_server1.uos.ac.kr이고, 클라이언트 이름은 nfs_client1.uos.ac.kr로 하자.

먼저 NFS서버에서 서비스 해줄 디렉토리를 정한다. 이 디렉토리를 /etc/exports에 작성하여 준다.

```
[root@nfs_server1 /etc]# vi /etc/exports
================================
/free_hard
/home
================================
```

저장을 한뒤, /etc/rc.d/init.d/nfs restart를 실행시킨다.

client host에서 /free_hard 디렉토리와 /home directory를 mount할 수 있다. 마운트하는 명령은 다음과 같다.

```
mount -t nfs nfs_server1:/home/home
```

이를 위해서 먼저 비어 있는 /home 디렉토리가 client host에 설치되어 있어야 한다.

클라이언트에서 위의 명령을 주면 서버의 /home 디렉토리가 /home에 마운트 된다.

다음의 명령으로 확인할 수 있다.

```
[root@nfs_client1 /mnt]# df
Filesystem           1024 blocks  Used Available Capacity Mounted on
/dev/hda1              1190014  955442    173086      85%  /
nfs_server1:/home      2268573 1992598    158701      93%  /home
```

mount를 자동으로 실행하기 위해서는 /etc/fstab을 수정하면 된다. 이 외 NFS의 보다 자세한 사용방법은 man page를 참조하기 바란다.

이상의 NIS와 NFS를 사용하여 계정관리와 home directory 관리를 간편하게 할 수 있다.

각 사용자가 mail을 손쉽게 보게 할 수 있도록 역시 NFS를 사용하여 mail spool을 공유하도록 하면 보다 편리한 시스템이 구성된다.

3. Local system이 없는 Linux PC실

앞 절에 기술된 PC실 운영 방법은 여러 면에서 편리하나 각각의 PC가 독립된 Linux system을 갖고 있기 때문에 system upgrade를 위해서는 모든 PC에 대해 upgrade를 하여야 하는 부담을 아직 갖고 있다. 만약에 설치되어 있는 LAN의 기능이 충분히 우수하다면 모든 자원을 server만이 갖고 각각의 PC는 local system을 갖지 않는 구성을 고려할 수 있다. 이 경우 기본적으로 2의 경우와 같이 NIS를 이용하여 사용자 관리를 하며 NFS를 이용하여 파일

들을 공유한다. 하드디스크가 없기 때문에 별도의 booting 수단을 가져야 하는 데 Network booting이 가장 저렴한 가격으로 손쉽게 구현할 수 있어 흔히 사용된다. 또 다른 특징은 NFS를 이용하여 일반 파일을 공유할 뿐 아니라 Root System까지 공유하여야 한다는 점이다. 즉 Root-NFS를 이용한다.

3.1 Network Booting

Network Booting을 위해서는 boot-rom이 필요하다 56Kbit나 1Mbit의 boot-rom이 흔히 사용된다. boot-rom이 없을때는 Floppy로 대체해서 사용할 수 있으며, boot-rom image를 만드는 소프트웨어에서 설정시 선택할 수 있다. Network Booting을 위해 갖추어야 할 소프트웨어는 bootp-2.4.3-4.i386.rpm, tftp-0.15-1와 Netboot Source가 필요하다. Netboot Source는 http://www.han.de/~gero/netboot(1999년 12월 31일 기준)에서 구할 수 있다.

Boot-rom image를 만들기 위해서는 ./configure, make, make install을 실행하여 netboot를 설치한 후 make rom을 실행시킨다. 이 프로그램은 여러 필요 사항에 대해 질문을 하는데 대부분의 경우 default 설정을 그대로 따르면 된다. 단지 network 카드에 대한 정보만 입력하면 되는데 몇 가지 network 카드의 경우는 소프트웨어 인터럽트 설정을 추가로 필요로 하는 경우가 있다. 이 때 image.flo와 image.rom이 만들어 지는데 이들은 각각 floppy와 boot-rom을 위한 image이다. 먼저 floppy image로 시험한 후 성공적이면 rom-writer로 boot-rom을 만들면 된다.

Client가 server에서 부트에 필요한 커널을 받는 순서는 다음과 같다. 모든 LAN 카드에는 고유한 MAC address를 가지고 있다. LAN 카드에 boot-rom을 장착하면 Board에서 부팅시 LAN 카드에 선점권을 주면 LAN 카드는 자신이 속한 클래스(현재 LAN에 연결되어 있는 port의 상위그룹)에 자신의 MAC address를 알리게 된다. bootpd가 설정되어 있는 서버는 LAN상에 알려진 MAC address를 자신이 가지고 있는 MAC address와 대조해서 같으면 client에 IP address를 부여한다. 이 IP address로 Network을 설정한 후 client가 다시 커널 image를 요청하고 server는 tftp를 통하여 client가 필요로 하는 파일을 보내 준다.

server는 bootp와 tftp service를 제공해야 하는데 이는 inetd를 통하여 이루어지므로 /etc/inet.conf를 수정해야 한다. 다음의 사항을 에디터를 사용해 추가/수정하기 바란다.

```
tftp    dgram   udp     wait    root \
  /usr/sbin/tcpd  in.tftpd /tftpboot
bootp   dgram   udp     wait    root \
  /usr/sbin/tcpd  bootpd
```

Client kernel을 넣어둘 장소로 /tftpboot 디렉토리를 설정하였다. 이렇게 한 뒤 inet server를 restart 해준다(/etc/rc.d/init.d/inet restart).

사실은 이보다 먼저 bootptab를 설정해 주어야 한다.

```
---------- 운영중인 bootptab 설정 부분
.default:\
        :dn=uos.ac.kr:\
        :ds=203.249.96.5:\
        :gw=210.125.178.1:\
        :sm=255.255.255.0:\
        :td=/tftpboot/:\
        to=auto.

phyterm1:tc=.default:ha=00001CB08985:bf=/tftpboot
  /vmlinuz_phyterm1:
phyterm2:tc=.default:ha=00001CB0889A:bf=/tftpboo
  t/vmlinuz_phyterm2:
phyterm3:tc=.default:ha=00001CB08411:bf=/tftpboot
  /vmlinuz_phyterm3:
phyterm4:tc=.default:ha=00001CB0877F:bf=/tftpboo
  t/vmlinuz_phyterm4
phyterm5:tc=.default:ha=00001CB08BE4:bf=/tftpboo
  t/vmlinuz_phyterm5:
phyterm6:tc=.default:ha=00001CB08790:bf=/tftpboot
  /vmlinuz_phyterm6:
phyterm7:tc=.default:ha=00001CB08340:bf=/tftpboot
  /vmlinuz_phyterm7:
phyterm8:tc=.default:ha=00001CB08C33:bf=/tftpboo
  t/vmlinuz_phyterm8:
phyterm9:tc=.default:ha=00001CB08D6F:bf=/tftpboo
  t/vmlinuz_phyterm9:

운영중인 bootpd 설정 부분 끝---------- --
```

bootptab설정에 대한 설명을 위의 예를 가지고 설명하겠다.

.default는 전체 설정 파일 중 매크로처럼 중복되는 것이 있을 때 미리 선언할 때 사용되는 부분이다. dn은 도메인 네임을 설정하며, ds는 DNS server를, gw는 gateway, sm는 subnet mask, td는 kernel의 위치, ha는 hardware address즉 client의 MAC address를 뜻한다. 위의 예제를 보면 대강 알 수 있을 것이다.

Client에서 보내줄 kernel image를 준비한다. 우선 통상적인 방법으로 kernel을 만드느데 설정에서 NFS-Root가 가능하도록 file system 컴파일 설정 메뉴에서 선택해주기 바란다. 이 때 bootp 지원이나 rarp 등은 선택하지 않는다. 만들어진 kernel은 netboot 패키지에 포함되어 있는 mknbi-linux 프로그램을 사용하여 image를 만든다. 이때 IP addresss, gateway 등 network 설정에 필요한 정보를 적절히 추가할 수 있다. 또 mknbi의 사용방법은 각 버전마다 조금씩 다르니 mknbi -h 명령을 이용, 명령을 확인하기 바란다. 필자가 사용한 mknbi의 버전은 Version 0.7.2(netboot)이다.

예제)

```
mknbi -i 210.125.178.71:210.125.178.52:210.125.178.1:255.255.255.0:test.uos.ac.kr -k vmlinuz -o vmlinuz_image
```

3.2 ROOT-NFS

다음은 Root-NFS를 위한 설정이다. Client 쪽은 이미 kernel에 필요한 설정을 준비해 두었으므로 서버 쪽 준비만 하면 된다. 앞에서 NFS에 대한 설명을 하였으므로 간단히 설명하겠다. 먼저 /etc/exports에 다음을 기록한다.

```
/tftpboot    test*.uos.ac.kr(rw,no_root_squash)
```

이 디렉토리(/tftpboot) 하부에 각 client들이 마운트할 초기 디렉토리들이 놓여 있다. test*.uos.ac.kr의 이름을 가진 machine들이 마운트 할 수 있으며 client가 가지고갈 최상위 디렉토리는 client의 이름을 디렉토리로 만든 구조물을 최상위 root로 인식해서 마운트하게 된다. 사용하게될 client의 이름이 test.uos.ac.kr이면 다음과 같은 디렉토리 구조를 가지게 된다.

```
-------------------------------------------
/tftpboot/test/     bin/
                    boot/
                    dev/
                    etc/
                    home/
                    lib/
                    misc/
                    mnt/
                    proc/
                    root/
                    sbin/
                    tmp/
                    usr/
                    var/
/tftpboot/test1/...
/tftpboot/test2/..
-------------------------------------------
```

위의 디렉토리들은 서버에서 복사해도 된다. 단, /usr, /proc, /tmp는 복사하지 말고 usr는 NFS-mount를 이용해 사용하기 바라고 proc, tmp는 그냥 빈 공백으로 만들기 바란다. 이유는 각 디렉토리별 사용목적 때문이다. proc은 kernel level에서 사용하기 때문에 그냥 빈 공디렉토리로 두면 되고, tmp는 temporary 디렉토리로서 누구나 접근해서 사용할 수 있게 접근권한을 777(chmod 777 /tmp)로 해야 한다. etc와 var directory는 client 별로 따로 만들어 주고 각 client 고유에 대한 설정을 하여 둔다. client의 etc/fstab 파일을 예로 들면 다음과 같다.

```
=========================================
210.125.178.52:/tftpboot/test /    nfs    defaults        1 1
/dev/fd0 /mnt/floppy auto    sync,user,noauto,nosuid,nodev,
        unhide 0 0
/dev/cdrom /mnt/cdrom auto    user,noauto,nosuid,exec.
        nodev,ro 0 0
none        /proc        proc    defaults        0 0
none        /dev/pts     devpts  gid=5,mode=620    0 0
210.125.178.52:/usr     /usr        nfs    defaults        1 1
210.125.178.52:/home    /home       nfs    defaults        1 3
210.125.178.52:/NFS_1   /home1      nfs    defaults        1 3
210.125.178.52:/NFS_2   /home2      nfs    defaults        1 3
210.125.178.52:/var/spool/mail /var/spool/mail
                                    nfs    defaults  1 3
=========================================
```

'/'부분이 어떻게 되어있는지 자세히 보기 바란다. client는 하드디스크가 없기 때문에 NFS에 의존하고 있다.

4. Remote-boot를 이용한 Windows PC실

위의 두 예는 PC실 전체를 Linux system으로 구성하였을 경우 적용되는 방법이다. Linux system의 우수성에 비추어 볼 때 권장하고 싶은 구성이다. 특히 대학의 PC실의 경우는 더욱 권장하고 싶다. 그러나 실제 Linux의 보급율이 MS-Windows에 비해 현저하게 낮기 때문에 실제 PC실은 MS-Windows를 근간으로 하고 있는 경우가 많다. 이 경우 각 PC의 시스템이 보호되고 있지 않고 바이러스의 감염가능성, 사용자의 실수에 의한 시스템의 파손가능성으로 인해 관리의 문제가 무척 심각하다. 이 경우 시도해 볼 만한 것이 Remote-boot의 방법이다.

이것은 스위스의 제네바 대학(http://cuiwww.unige.ch/info/pc/remote-boot/howto.html 혹은 www. bpbatch.com 참조)에서 개발되어 보급되고 있는데 다음 단계로 요약할 수 있다.

(1) 하드디스크의 정보를 사용하지 않고 앞의 예에서와 같이 boot-rom을 이용한 network boot를 한다.

(2) Server는 linux system을 사용하는데 (물론 Windows-NT를 사용할 수도 있는데 Linux가 훨씬 간편하다) DHCP나 bootp를 사용하여 network 설정에 필요한 정보를 제공한다.

(3) Client가 Network를 설정한 후 bpbatch라는 batch file interpreter를 제공한다.

(4) Bpbatch의 메뉴에 의해 시스템이 안전하다고 판단되면 local 하드디스크에 다음 bootind의 권한을 넘겨준다.

(5) 시스템이 불안전하다고 판단되면 bpbatch의 다른 기능을 이용하여 하드디스크의 Partition 변경, Format을 할 수 있으며 local 하드디스크에 미리 준비되어 있는 system(예를 들면 Windows 95/98)을 풀어 주거나 server에 있는 image를 끌고 내려와서 풀어 준다.

(6) 이상의 단계를 거쳐 깨끗하고 안전한 시스템이 제공된다.

Boot-rom과 bootp를 이용한 network booting을 앞에서 설명하였으므로 이 절에서는 bootp 대신 DHCP를 사용한 방법을 설명한다. Bootp의 설정은 /etc/booptab을 통하여 이뤄지지만 DHCP는 /etc/dhcp.conf가 설정 파일이다.

```
==========/etc/dhcp.conf의 예====
# DHCP configuration file for DHCP ISC 3.0 & BpBatch#
# Global options
  option subnet-mask 255.255.255.0;default- lease-time -1;
# Definition of PXE-specific options
# Code 1: Multicast IP address of bootfile
# Code 2: UDP port that client should monitor for
# MTFTP responses
# Code 3: UDP port that MTFTP servers are using to
# listen for MTFTP requests
# Code 4: Number of secondes a client must listen for
# activity before trying to start a new MTFTP transfer
# Code 5: Number of secondes a client must listen before
# trying to restart a MTFTP transfer option space PXE;
option PXE.mtftp-ip    code 1 = ip-address;
option PXE.mtftp-cport code 2 = unsigned integer 16;
option PXE.mtftp-sport code 3 = unsigned integer 16;
option PXE.mtftp-tmout code 4 = unsigned integer 8;
option PXE.mtftp-delay code 5 = unsigned integer 8;
# Subnet-specific options
subnet 192.168.1.0 netmask 255.255.255.0 {  option routers
192.168.1.1;
# Host specific options
host pctest {
    hardware ethernet 00:01:02:03:04:05; filename "bpbatch.P";
    next-server 192.168.1.2;  fixed-address 192.168.1.100;
    # BpBatch command-line argument  -i == interactive
    # You can also specify a script name(do not include the
    # trailing bpb extension)
      option option-135 "-i"
    # PXE specific options class "pxeclients" {
    match if substring(option vendor-class-identifier, 0, 9) =
    "PXEClient"; option vendor-class-identifier "PXEClient";
    # At least one of the vendor-specific option must be set.
    # We set the MCAST IP address to 0.0.0.0 to tell the
    # bootrom to still use TFTP (address 0.0.0.0 is considered
    # as "no address")
    option PXE.mtftp-ip 0.0.0.0; vendor  option-space PXE;}
  }}
==========
```

tftp 프로그램은 여러 가지가 제공되고 있는데 조금씩 사용 방법이 다르다 예를 들면 bpbatch의 가장 중요한 파일은 bpbatch.P인데 어떤 tftp

프로그램의 경우 끝부분의 .P를 생략하여야 하는 경우가 있고 directory 설정도 root의 위치를 달리 설정하는 경우가 있으므로 주의하여야 한다.

가장 중요한 파일은 bpbatch 프로그램인데, http://cuiwww.unige.ch/info/pc/remote-boot/soft/bpb-exe.tar.gz로 제공되고 있다. 이 파일을 받아 압축을 풀면 dynamic loader인 bpbatch.P, relocated interpreter인 bpbatch.ovl, bpbatch.hlp의 help 파일로 되어 있다. 이들 파일은 바로 사용할 수 있다.

이상으로 server쪽 준비는 완비되었다. 다음은 Windows system의 image을 만들어야 한다. 우선 1개의 client에 깨끗한 windows system을 설치한다. 이 때 msdos.sys에 AUTOSCAN=0을 추가하여 windows 시작 시 ScanDisk를 하지 않도록 한다. Linux server에 samba를 설치한 후 server의 /tftpboot directory를 disk L:로 mount 한다. 다음은 Mrzip이란 script 파일이다.

```
showlog
filter -"windows/schedlog.txt"
filter -"windows/msimgsiz.dat"
filter -"*/index.dat"
filter -"*.swp"
filter -"*.tmp"
filter -"temp/*"
fullzip "c:/" "L:/tftpboot/win.imz"
```

이 script를 사용하여 windows systerm의 image를 win.imz란 이름으로 생성할 수 있다. 이로써 image를 준비한 셈이 된다. 이제 이 image를 다시 푸는 script가 필요한데 다음과 같은 script 파일을 작성하여 server에 /tftpboot/win.bpb로 둔다.

```
hidelog
setpartitions "bigdos:1024"
setbootpart 1
fullunzip "win.imz" 1
hidebootprom
hdboot :1
```

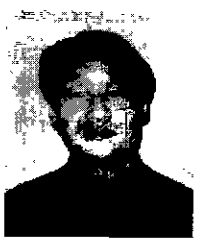
이제 bpbatch 프로그램이 실행될 때 win.bpb를 선택하면 깨끗한 windows system을 언제나 client에서 얻을 수 있다.

samba system을 같이 사용하여 windows 응용프로그램을 공유할 수 있도록 하면 이 구성의 효율성을 더욱 높일 수 있다. 또 Measurement Techniques, Inc(see http://www.lancache.com)에서 제공되는 Shared LAN Cache를 사용하면 Network의 기능을 향상시킬 수 있다.

5. 첨언

이 글에서 우리는 Linux를 사용한 3가지 다른 형태의 PC실 구성을 소개하였다. 앞에서도 언급한 것과 같이 필자는 전체 PC실을 Linux system으로 구성하는 것이 PC실 관리와 운영 또 보안의 관점에서도 가장 훌륭한 것으로 생각하나 실제 사용자의 수는 현재에는 windows의 경우가 훨씬 많으므로 세 번째의 방법이 가장 활용도가 높을 것으로 생각한다. bpbatch 회사는 한 걸음 더 나아가 부분적인 파일의 보수가 가능한 진보된 bpbatch 프로그램과 사용자 시간 관리 기능을 추가한 제품을 소개하고 있다. 이들 프로그램은 상용이므로 직접 bpbatch회사의 home page를 접속해 보기 바란다. 또 다른 가능성으로 network을 이용한 remote power-on을 생각할 수 있으나 아직 필자는 아직 실현되어 있는 방법을 찾지 못하였다. 혹시 관심이 있는 사람은 Intel의 wfm page를 참조하기 바란다.

민 현 수



1979 서울대학교 물리학과 졸업
1981 서울대학교 대학원 이학석사(물리학)
1985 서울대학교 대학원 이학박사(물리학)
1982 서울시립대학교 전임강사
현재 서울시립대학교 교수/전자계산소 소장
전공 입자물리학 이론
E-mail hsmin@dirac.uos.ac.kr