STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

2008/2009

Obor 18 - Informatika

Bezdiskové stanice na Ubuntu Linuxu

Autor:

Martin Vancl

2008/2009

VOŠ a SPŠ, Jičín

Pod Koželuhy 100

506 41 Jičín

Jičín

Čestné prohlášení autora

Prohlašuji tímto, že jsem soutěžní práci vypracoval zcela samostatně a uvedl v seznamu literatury veškerou použitou literaturu včetně zdrojů z Internetu.

V Jičíně dne 5. duben 2009

Martin Vancl

_____

vlastnoruční podpis autora

Abstrakt

Každý člověk dřív nebo později zjistí, že jeho počítač má svá nejlepší léta za sebou. To mě vedlo k úvaze nad využitím těchto starých počítačů. Staré počítače se dají s trochou vynaloženého úsilí přeměnit v bezdiskové stanice, takže stačí koupit jenom jeden nový počítač, který bude sloužit jako server. Stanice v sobě nemají operační systém, pomocí sítě používají ten ze serveru. Je tedy možné používat i na starých stanicích nejnovější programy. Díky svobodné licenci a nulové ceně použitého softwaru odpadá velká část nákladů a je možné vše přizpůsobit na míru konkrétním požadavkům.

Obsah

1 Úvod

Počítače jsou dnes už naprostý standart a život bez nich už je nemožný. S postupem času se neustále zlepšuje hardware i software. Počítač, který patřil před deseti lety k nejlepším, je dnes nepoužitelný. Vliv na to má software s neustále se zvětšujícími hardwarovými nároky. Spousta lidí je postavena před problém: „Nakoupit za desetitisíce nový hardware a licence na software nebo zůstat u stávajícího řešení?“. Pokud zůstanou u starého softwaru, brzy přijdou o veškerou kompatibilitu (např. Microsoft Office).

To mě vedlo k úvaze a následnému řešení tohoto problému. Protože mi bylo líto vyhodit staré počítače, rozhodl jsem se z nich udělat bezdiskové stanice.

Kvůli licencím a svým znalostem jsem vybral GNU/Linux. Konkrétně distribuci Ubuntu s předinstalovaným Linux Terminal Server Project [1]. Pro účely testování jsem měl čtyři počítače:

1. Intel Celeron 433MHz, 64MB RAM
2. Intel Pentium 233MHz, 16MB RAM
3. VIA 667MHz, 256MB RAM
4. Intel Celeron M 1866MHz, 1,5GB RAM

Jako server posloužil počítač Intel Pentium 4 2,4GHz, 1,5GB RAM, 80GB disk a dvě 100Mb/s síťové karty. Pouze u prvního a druhého se vyskytly problémy. První po drobné úpravě také fungoval, druhý se mi zprovoznit nepodařilo.

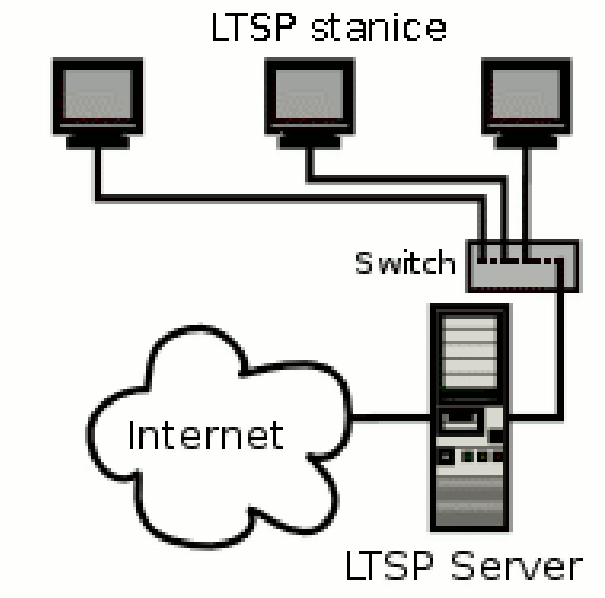
1.1 Minimální požadavky

Požadavky na server se liší dle počtu připojovaných stanic. Obecně je však dobrou volbou použití dvoujádrového nebo čtyřjádrového procesoru a minimálně 1GB RAM. Vyplatí se server osadit dvěma až čtyřmi GB RAM. Dále jsou potřeba dvě síťové karty. Alespoň po dobu nastavení a instalaci programů je nezbytně nutné připojení k Internetu.

Jako klienty lze použít skoro všechny staré počítače. Podmínkou je síťová karta, velikou výhodou je, pokud BIOS podporuje bootování ze sítě.

1.2 Názorná ukázka

Pro lepší pochopení uvádím jednoduché schéma:



Jeden počítač funguje jako server a jsou k němu připojeny pomocí switche všechny bezdiskové stanice. Server má připojení na Internet.

2 Základní instalace serveru

2.1 Získání operačního systému

Jako operační systém jsem zvolil Ubuntu [2] Linux. Ten je na Internetu zdarma ke stažení ve formě ISO obrazu. Pro účely terminál serveru důrazně doporučuji stáhnout 32 bitovou verzi `Alternate Install CD` [3], ta má na rozdíl od ostatních verzí Ubuntu pouze textový instalátor, ale není potřeba dodatečně instalovat terminál server. Zvolením 32 bitové verze si také ušetříte mnoho problémů.

Po stažení je potřeba obraz vypálit. V prostředí MS Windows k tomu lze použít např. svobodný vypalovací program `Infra Recorder` [4].

2.2 Instalace základního systému

2.2.1 Spuštění instalace

Pokud už máte vypálené CD s Ubuntu, můžete se pustit do instalace. Vložte CD do mechaniky a restartujte počítač, po chvíli by se měla zobrazit následující nabídka:

Pokud se nezobrazí, budete muset upravit pořadí bootování v BIOSu.

Po výběru češtiny stiskněte `<F4>` a zvolte `Nainstalovat LTSP server`. Nyní v hlavním nabídce vyberte `Nainstalovat Ubuntu`, tím by se měla spustit instalace. Hned na začátku instalátor zjistí od uživatele rozložení klávesnice.

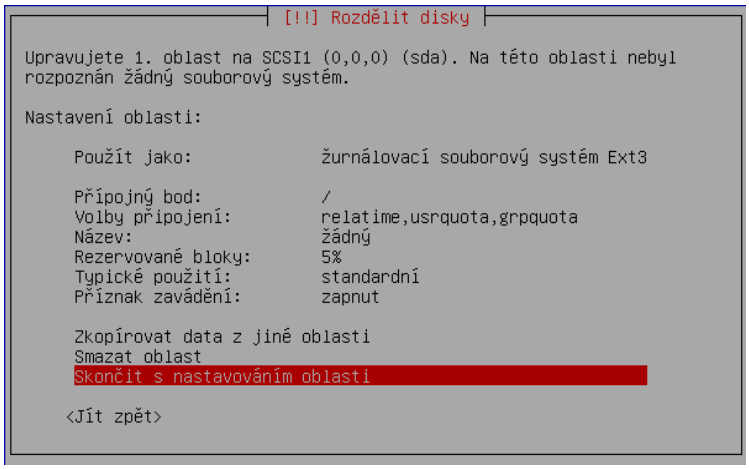
2.2.2 Rozdělení disku

Po nastavení sítě a názvu počítače je na řadě rozdělení disku. V nabídce vyberte `Ruční`

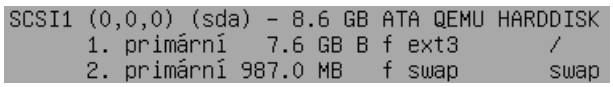
rozdělení a typ disku:

Kvůli bezpečnosti je dobré odstranit ostatní operační systémy (v případě dual bootu můžete z aktivního systému libovolně upravovat aktuálně nespuštěný systém). Poté vyberte VOLNÉ MÍSTO.

Pokud vytvoříte pro systém i data uživatelů jeden oddíl (pro začátek to stačí), vytvořte oddíl minimálně 10GB. Souborový systém zvolte ext3 a přípojný bod nastavte na / . V nabídce volby připojení zatrhněte kvůli rychlosti relatime a podporu pro diskové kvóty – usrquota a grpquota. Pro uživatele root nechte standartně nastavených 5% místa disku a zapněte příznak zavádění.



Pro swap vytvořte 1 – 2GB oddíl. Výsledné rozdělení by mělo vypadat asi jako na následujícím obrázku:



Nyní už následuje instalace základního systému.

2.2.3 Dodatečná nastavení

Po instalaci základního systému vyzve instalátor k vytvoření nového uživatele. Tento uživatel bude moci pomocí sudo spravovat systém, proto vyberte dostatečně kvalitní heslo! Pro jednoduchost pojmenujte nového uživatele **spravce**.

Instalátor nabízí volbu vytvoření šifrovaného adresáře pro každého uživatele, tato funkce nebude potřeba, proto zvolte NE.

3 Nastavení serveru

Už po základní instalaci Ubuntu je možné nabootovat ze stanic. Systém však v tomto stavu není nejlepší na běžnou práci, proto je lepší nejdříve provést nastavení. Všechny příkazy spouštějte pod uživatelem root (v Ubuntu pomocí příkazu `sudo`).

3.1 Nastavení připojení k síti

Na serveru jsou potřeba dvě síťové karty – jedna pro připojení serveru k internetu a druhá pro připojení bezdiskových stanic. Nastavení sítě je v souboru `/etc/network/interfaces` . V celém dalším textu budu předpokládat, že síťová karta `eth0` je připojená k internetu a k `eth1` jsou připojeny bezdiskové stanice. Editaci souboru spusťte příkazem:

```
gedit /etc/network/interfaces
```

V případě, že síťová karta připojená do internetu má statickou IP adresu, bude pro ni takovýto záznam:

```
auto eth0
iface eth0    inet static              # static => statická IP
   address    192.168.0.1              # IP adresa
   netmask    255.255.255.0            # maska
   gateway    192.168.0.254            # brána
```

Jestliže `eth0` získává adresu z DHCP serveru, bude záznam jednodušší:

```
auto eth0
iface eth0 inet dhcp          # dhcp => nastavení z DHCP
```

Druhá síťová karta `eth1`, musí mít nastavenou statickou IP adresu. Nastavení pro ni bude následující:

```
auto eth1
iface eth1    inet static
   address    192.168.1.1
   netmask    255.255.255.0
   gateway    192.168.1.254
```

Dále je potřeba ještě nastavit loopback rozhraní:

```
auto lo
iface lo inet loopback
```

Celé nastavení tedy bude vypadat následovně:

```
auto lo                                 # MÍSTNÍ SMYČKA
iface lo inet loopback

auto eth0                               # INTERNET
iface eth0    inet static
   address    192.168.0.1
   netmask    255.255.255.0
   gateway    192.168.0.254

auto eth1                               # BEZDISKOVÉ STANICE
iface eth1    inet static
   address    192.168.1.1
   netmask    255.255.255.0
   gateway    192.168.1.254
```

3.2 Instalace užitečného softwaru

Ubuntu neobsahuje ve výchozím stavu mnoho potřebných programů, většinou je to kvůli licenčním podmínkám. Instalace těchto programů je však s použitím balíčkovacího systému otázkou několika minut.

Zde popisované úkony provádím v příkazovém řádku, většinu z nich však lze nastavit i pomocí grafických nástrojů.

3.2.1 Java

Java je potřeba ke spuštění programů psaných pod Javou (např. BitTorrent klient Azureus) a některé banky ji požadují kvůli svému internetovému bankovnictví. K instalaci jsou potřeba dva balíčky a to: sun-java6-jre (obsahuje běhové prostředí Javy) a sun-java6-plugin (přidá podporu Javy do Firefoxu). Instalace se provede příkazem:

```
apt-get install sun-java6-jre sun-java6-plugin
```

Po instalaci ještě často bývá potřeba vybrat výchozí verzi Javy, to lze udělat následujícím příkazem:

```
update-java-alternatives -s java-6-sun
```

3.2.2 Flash

Flash animace dnes najdete skoro na každém webu, proto je vhodné nainstalovat rozšíření do Firefoxu. Ubuntu nabízí několik druhů flash rozšíření, svobodnou verzi (má omezené možnosti) a originální nesvobodnou od Adobe.

Pro potřeby bežných uživatelů je výhodnější použit verzi od Adobe z balíčku `flashplugin-nonfree`:

```
apt-get install flashplugin-nonfree
```

3.2.3 Thunderbird

Jako e-mailový klient lze použít program `Evolution`, který je ve výchozí instalaci Ubuntu, mně se však osvědčil program `Mozilla Thunderbird`. Je to jednoduchý e-mailový klient s podporou rozšíření. Není nijak zvlášť náročný na hardware a v základu nemá žádné zbytečné funkce. Jelikož sám Thunderbird neumí běžet v oznamovací oblasti, je potřeba použít rozšíření `traybiff`, nebo program `alltray`. Osobně považuji jednodušší použít rozšíření `traybiff`. Někteří uživatelé mohou chtít své e-maily šifrovat pomocí `GnuPG`, proto raději nainstalujte i rozšíření `enigmail`.

```
apt-get install thunderbird enigmail thunderbird-traybiff
```

3.2.4 Gnome Commander

Z operačního systému Microsoft Windows je většina uživatelů zvyklá na nějakého dvou-panelového správce souborů jako `Total Commander` nebo `Altap Salamander`. V Ubuntu je k

dispozici alternativa ve formě programu Gnome Commander.

```
apt-get install gnome-commander
```

3.2.5 OpenOffice.org

Kancelářský balík je obsažen už v základní instalaci, bohužel však jenom ve verzi 2.x a není úplný. Chybí databáze, bez které není například možné vytvářet seznam použité literatury.

Do vydání Ubuntu 8.10 se už nedostala nová řada 3.x, proto je potřeba použít neoficiální zdroj balíčků [5]. Na konec souboru /etc/apt/sources.list vložte následující dva řádky:

```
deb http://ppa.launchpad.net/openoffice-pkgs/ubuntu intrepid main
deb-src http://ppa.launchpad.net/openoffice-pkgs/ubuntu intrepid main
```

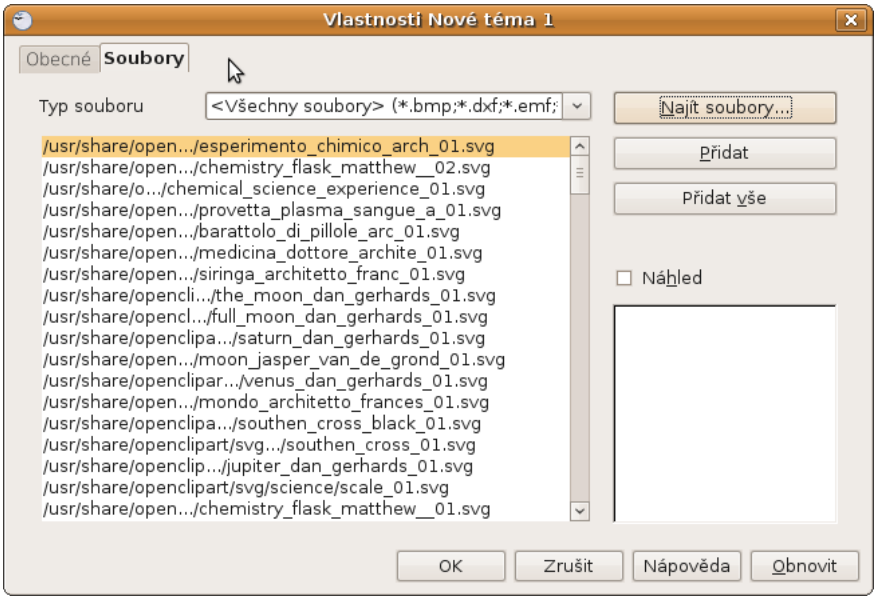
Po aktualizaci zdrojů balíčků nainstalujte balíčky openoffice.org a openclipart. První nainstaluje samotný OpenOffice a druhý galerii obrázků OpenClipart.

```
apt-get update
apt-get install openoffice.org openclipart
```

Po instalaci je potřeba nastavit OpenClipart galerii. Spusťte OpenOffice pomocí

```
oowriter
```

Tím se spustí OpenOffice s právy uživatele root. Nyní v menu Nástroje zatrhněte Galerie. Zobrazí se galerie, v ní vyberte Nové téma, nyní přejděte na kartu Soubory a klepněte na tlačítko Najít soubory. Galerie se nachází v /usr/share/openclipart pomocí Přidat vše načtěte galerii a vypněte OpenOffice. Teď už by měli mít všichni uživatelé přístup k OpenClipart galerii.



3.2.6 Komprimační nástroje

Komprimované soubory se vyskytují skoro všude. V Linuxu jsou to převážně `tar` archivy komprimované programem `gzip` nebo `bzip2`, na Windows je zase masově rozšířený formát `zip` a `rar`. `7-Zip` je moderní komprimační formát využívající algoritmu `LZMA`, takže má výborný komprimační poměr.

```
apt-get install rar unrar bzip2 p7zip-full p7zip-rar zip unzip
```

3.3 Nastavení terminálového serveru

Už po instalaci Ubuntu by mělo být možné nabootovat ze stanic. Většinou to však „není ono“ a je potřeba systém upravit podle svých požadavků.

3.3.1 Počeštění systému

Při instalaci Ubuntu z Alternate CD [3] se nenainstaluje kompletní česká lokalizace systému. Počeštění systému proveďte následovně:

```
apt-get install language-pack-cs language-pack-gnome-cs language-pack-kde-cs \
language-support-cs
```

3.3.2 Vypnutí PC Speakeru

Tato funkce je spíš na obtíž, než pro užitek. Pokud je v místnosti větší počet stanic, pípání se stává protivným. Pro vypnutí stačí zakázát modul jádra `pcspkr`.

```
echo „blacklist pcspkr“ > /opt/ltsp/i386/etc/modprobe.d/blacklist-pcspkr
```

Aby se změny projevily, je potřeba aktualizovat chroot obraz, který se distribuuje stanicím a restartovat všechny stanice. Při každé změně nastavení serveru je potřeba aktualizovat chroot obraz. Aktualizace je poměrně zdlouhavá, u mne trvala skoro 3 minuty.

```
ltsp-update-image
```

3.3.3 Statické IP adresy pomocí DHCP

Server přiděluje stanicím IP adresy pomocí DHCP serveru, jeho nastavení se nachází v souboru `/etc/ltsp/dhcpd.conf`. Pokud potřebujete přidělovat určitým počítačům vždy stejné IP adresy, musíte pro každý takový počítač přidat záznam právě do tohoto souboru.

```
host stanice07 {
   hardware ethernet 00:00:e8:63:0d:cd;   # MAC adresy síťové karty stanice
   fixed-address 192.168.0.201;   # IP adresa, která bude tomuto počítači vždy přidělena
}
```

3.3.4 Skrytí souborů v Nautilusu

Nautilus [6] je výchozí správce souborů pro Gnome. Stojí za to zvážit, zda neskrýt zobrazování adresářů v `/`, uživatelé je stejně k ničemu vidět nepotřebují a alespoň se jim nebudou zbytečně plést.

Důležité je, uvědomit si, že nastavení se týká pouze Nautilusu a různých systémových dialogů. Pomocí např. `Midnight Commanderu` [7] nebo příkazu `ls` je možné adresáře stále zobrazit.

Nautilus se při skývání řídí souborem `.hidden` v aktuálním adresáři. Pokud tedy budete chtít skrýt adresáře v `/`, vytvořte soubor `/.hidden` a do něj napište všechny adresáře, které se mají skrýt. Syntaxe je jeden soubor/adresář na řádek. Rozumné nastavení vypadá asi takto:

```
bin
boot
dev
etc
initrd
lib
lost+found
mnt
opt
proc
root
sbin
srv
sys
tmp
usr
var
initrd.img
initrd.img.old
vmlinuz
vmlinuz.old
lib32
```

3.3.5 Swapování po síti na disk

Pokud používáte stanice s velmi malým množstvím paměti (méně než asi 48MB RAM), je potřeba použít swap. Protože stanice nemají disk, je potřeba swapovat po síti. Nastavení je jednoduché – do souboru `/var/lib/tftpboot/ltsp/i386/lts.conf` přidejte následující řádky (sekce `[Default]`):

```
[Default]
   NBD_SWAP = True
```

Velikost swapu se nastavuje v souboru `/etc/ltsp/nbdswapd.conf`. Je potřeba mít dostatek místa na disku. Obsazené místo vypočítejte podle vzorce POČET-STANIC x VELIKOST-SWAPU. Mně se osvědčil swap o velikosti 150MB.

```
echo „SIZE=150“ > /etc/ltsp/nbdswapd.conf
```

Kvůli chybě v LTSP [8] je potřeba přidat do souboru `/etc/hosts.allow` tento řádek: `nbdswapd: ALL: keepalive` .

```
echo „nbdswapd: ALL: keepalive“ >> /etc/hosts.allow
```

Nyní aktualizujte chroot obraz a restartujte server i stanice.

```
ltsp-update-image ; reboot
```

Pokud jste postupovali správně, můžete po připojení stanic sledovat v adresáři `/tmp` swap soubory jednotlivých stanic (jejich velikost je stejná, jako jste nastavili v `/etc/ltsp/nbdswapd.conf`.

3.3.6 Automatické přihlášení na stanici

Jestliže chcete zpřístupnit jeden počítač pouze pro přístup na Internet, hodí se možnost automatického přihlašování. Nastavení je opět v souboru `/var/lib/tftpboot/ltsp/i386/lts.conf`.

```
[Default]
   LDM_AUTOLOGIN = True

[00:aa:00:62:c6:09]                    # MAC adresa stanice
   LDM_USERNAME = uzivatel
   LDM_PASSWORD = heslo
```

Nejdříve je potřeba povolit v sekci `[Default]` automatické přihlašování. Poté už lze vytvářet sekce s nastavením pro jednotlivé stanice. Těmto stanicím musí DHCP server přidělovat statickou IP adresu! Z ukázky je patrná syntaxe souboru. V názvu sekce se uvádí statická IP adresa stanice. Jméno i heslo musí být zapsáno v souboru s nastavením, tudíž tento soubor nesmí být čitelný běžným uživatelům!

3.4 Bootování stanic

Jestliže jako stanice použijete rozumně staré počítače, jako minimum myslím zhruba 400MHz procesor, 32MB RAM, síťovou kartu s podporou PXE, dále pak musí mít základní deska rozumně starý BIOS, který podporuje bootování ze sítě, bude vše fungovat na první zapnutí.

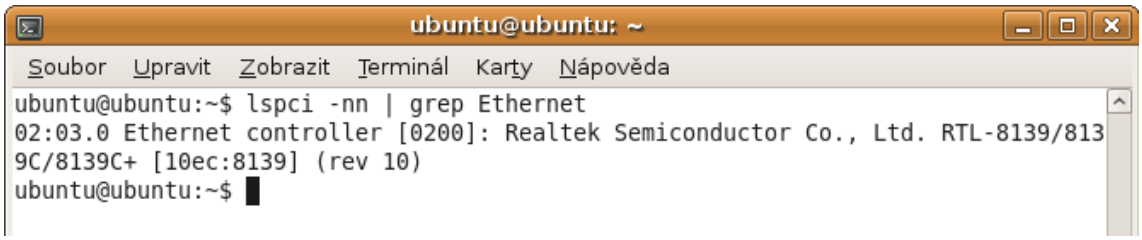
Staré stanice nabootovat nepůjdou. V tomto případě musí počítač nabootovat minimální část systému z média, kterému rozumí. Tím může být nejčastěji CD, pevný disk nebo disketa. Sice už bezdisková stanice nebude úplně „bezdisková“, ale je to nejjednodušší řešení. Stanice si při zapnutí načte tento systém a potom už komunikuje se serverem a toto médium nadále nepotřebuje.

Na vytvoření bootovacího média lze použít dva programy, buď aktuálně používaný `gPXE`, nebo starý, nadále nevyvíjený `Etherboot`.

Nejjednodušší je použití on-line nástroje na webu http://rom-o-matic.net/. Na těchto stránkách stačí vybrat typ síťové karty a médium, pro který chcete obraz vytvořit. Důležité je vybrat správný typ karty, například jedné z nejčastěji používaných 100Mb/s karet Realtek 8139 existuje mnoho typů:

```
...
rtl8139:13d1ab06 -- [13d1,ab06]
rtl8139:14eaab06 -- [14ea,ab06]
rtl8139:14eaab07 -- [14ea,ab07]
rtl8139:dfe690txd - [1186,1340]
...
```

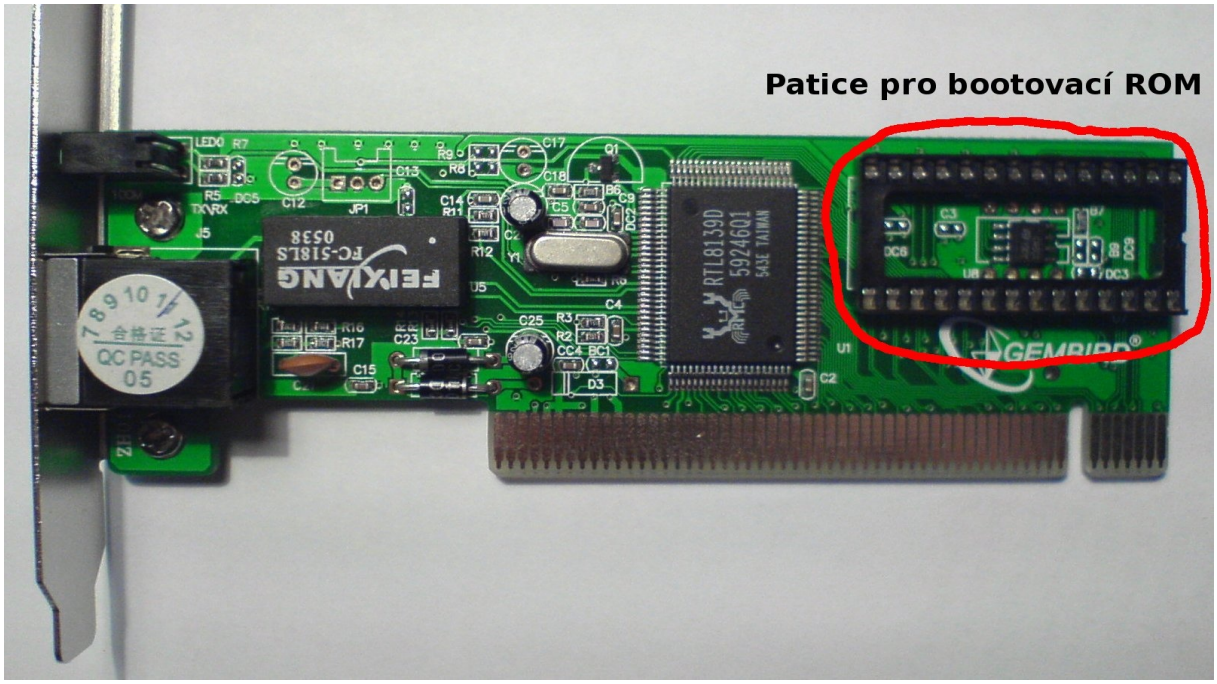
Tento typ zjistíte příkazem `lspci -nn | grep Ethernet` spuštěným na stanici. Výstup bude vypadat podobně:



typ karty je tedy **rtl8139 10ec:8139**

Já jsem pro tyto účely použil starou disketovou mechaniku. Tu jsem přilepil na dno PC skříně, aby k ní nebyl přístup. Na stránkách rom-o-matic.net jsem vygeneroval obraz na disketu o velikosti pouhých 50kB.

Disketa se dřív nebo později stejně rozbije, proto jestli to myslíte vážně, bylo by nejlepší použít ROM paměť s obrazem přímo na síťové kartě [9]. Není to však zrovna levné řešení, na Internetu se dá jedna naprogramovaná paměť koupit kolem $18, nebo si můžete sehnat prázdnou paměť a naprogramovat ji - k tomu je však potřeba programátor. Tuto metodu jsem nezkoušel.


Patice pro bootovací ROM
FEIXIANG
FC-5181LS
0538
RTL8139D
5924601
GEMBIRD

4 Zabezpečení

V dnešní době je zabezpečení před různými útoky jednou z nejdůležitějších věcí. Ani u malé sítě s několika málo uživateli nelze toto téma podceňovat.

4.1 Viry

Na Unixových systémech jako je Linux viry prakticky neexistují. Sice bylo vytvořeno malé množství virů, ty však většinou napadly pouze neaktualizované systémy a nezpůsobily mnoho škod.

To je dáno hlavně systémem uživatelských oprávnění. Vir může udělat pouze to, co uživatel, který ho spustil. Uživatel maximálně přijde o svá data, ale systému a datům ostatních uživatelů se nic nestane. Nebezpečí hrozí zejména u SUID [10] programů. Každý administrátor musí dbát zvýšené opatrnosti, než jakémukoli programu nastaví SUID práva. U disků se souborovým systémem ext3 je rozumné tyto disky připojit s parametrem nosuid. Ukázka souboru /etc/fstab:

```
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
/dev/sda3      /home            ext3    relatime,nosuid   0       2
```

Některé antivirové programy jsou dostupné i pro Linux. Jejich využití má smysl například na souborových nebo mail serverech, kde „odchytávají“ viry pro počítače s Windows. Pokud nejste paranoidní, je použití antiviru zbytečné.

4.2 Fyzický útok při bootování

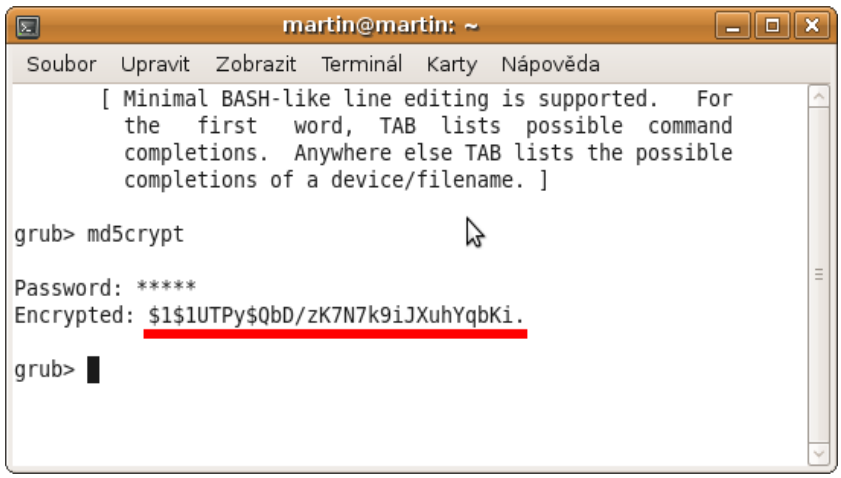
Linuxové distribuce používají pro zavedení jádra jeden ze dvou nejznámějších zavaděčů, těmi jsou LILO [11] a Grub [12]. Lilo se už dnes moc nepoužívá, proto se o něm dál nebudu zmiňovat.

4.2.1 Zabezpečení GRUBu

První možností zneužití GRUBu je možnost upravit bootovací parametry jádra. Nejedná se o chybu, ale o vlastnost zavaděče, která v případě potřeby (např. havárie systému) může být velice užitečná.

V bootovací nabídce GRUBu stačí vybrat operační systém a stisknout `e`, poté už je možné libovolně měnit parametry jádra [13]. Nejlepší řešení spočívá ve vypnutí editace záznamů GRUBu. Editace se sice nedá vypnout úplně, ale dá se chránit heslem [14].

Spusťte příkaz `grub`, objeví se příkazový řadek GRUBu (zjednodušený `bash`). V něm zadejte příkaz `md5crypt` a následně své heslo.



Výsledkem bude `md5 otisk` hesla (na obrázku je heslo podtrženo červeně). Toto heslo je potřeba zapsat do konfiguračního souboru GRUBu, ten se nachází v `/boot/grub/menu.lst`. Jako root přidejte do tohoto souboru následující řádek s heslem:

```
password --md5 VASE_HESLO_V_MD5
```

Důležité je přidat heslo před řádek `BEGIN AUTOMAGIC KERNELS LIST`, pokud byste to neudělali, při instalaci nového jádra (a aktualizaci GRUBu) by se heslo ze souboru smazalo! Mělo by to vypadat následovně:

```
password --md5 $1$fqUPy$8Vk/wRuUPUViCFGc7ZOPw.

# Put static boot stanzas before and/or after AUTOMAGIC KERNEL LIST
### BEGIN AUTOMAGIC KERNELS LIST
 ...
```

Ve druhém případě lze zneužít záchranného režimu Ubuntu. V zavaděči se zobrazuje následovně:

```
Ubuntu 8.10, kernel 2.6.27-9-generic (recovery mode)
```

Po nabootování do záchraného režimu získá uživatel přístup k systému s root právy. Pokud někdo získá přístup s root právy, systému už není možné věřit, útočník mohl i během chvíle umístit v systému „zadní vrátka“, pomocí kterých získá do budoucna úplnou kontrolu nad strojem. Nejlepší řešení je pak reinstalace celého systému. Abyste se tomuto nebezpečí vyhnuli, je nejlepší odtranit z nabídky zavaděče všechny záznamy se záchranným režimem.

V souboru s nastavením (`/boot/grub/menu.lst`) je potřeba najít následující část

```
## should update-grub create alternative automagic boot options
## e.g. alternative=true
##      alternative=false
# alternative=true
```

a změnit ji na

```
## should update-grub create alternative automagic boot options
## e.g. alternative=true
##      alternative=false
# alternative=false
```

Znak # na začátku řádku je v pořádku a musí tam zůstat!

Poté už stačí jenom znovu vygenerovat nastavení GRUBu:

```
update-grub
```

4.3 Práva domovských adresářů

Jednotliví uživatelé mají přístup k datům ostatních uživatelů (domovský adresář má nastavena práva na hodnotu 755). To je z bezpečnostního hlediska nepřijatelné. Já používám hodnotu 750,

vlastník má práva rwx a skupina uživatele rx, ostatní nemají žádná práva. Pro již existující uživatele se práva nastaví takto:

```
chmod 750 /home/UZIVATEL
```

Je vhodné změnit nastavení programu adduser, tím zajistíte, že nově vytvořeným uživatelům se automaticky nastaví práva domovského adresáře na 750. Nastavení je v souboru /etc/adduser.conf:

```
# If DIR_MODE is set, directories will be created with the specified
# mode. Otherwise the default mode 0755 will be used.
DIR_MODE=0750
```

4.4 Firewall

Internet už dávno není bezpečný jako v době svého vzniku, a proto je firewall nutností. Linuxové jádro má přímo v sobě zabudovaný firewall Netfilter [15], který se nastavuje pomocí nástroje iptables [16]. Tento nástroj sice má prakticky neomezené možnosti, ale jeho použití není pro běžného člověka zrovna pohodlné. Já jsem si pro nastavení firewallu oblíbil sadu skriptů jménem Shorewall [17]. Syntaxe nastavení je velmi jednoduchá a Shorewall sám vše nastaví.

Instalaci provedete pomocí příkazu

```
apt-get install shorewall
```

Po instalaci se Shorewall z bezpečnostních důvodů automaticky nespouští. Pro spuštění po startu systému je potřeba upravit soubor /etc/default/shorewall (startup musí být nastaveno na 1)

```
# prevent startup with default configuration
# set the following varible to 1 in order to allow Shorewall to start

startup=1
```

V hlavním konfiguračním souboru Shorewallu (/etc/shorewall/shorewall.conf) je potřeba upravit dvě věci. STARTUP_ENABLED musí být nastaveno na Yes – jinak se firewall

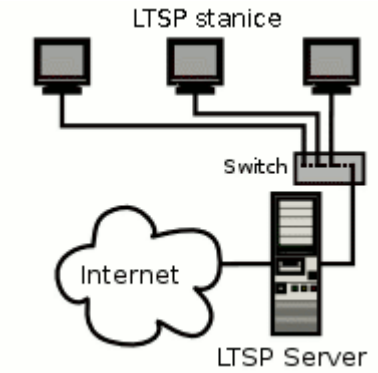
nebude automatiky spouštět při bootování a `IP_FORWARDING` na `On` – bez něj nebude na stanicích fungovat připojení k Internetu.

```
STARTUP_ENABLED=Yes
IP_FORWARDING=On
```

K samotnému nastavení pravidel používá Shorewall textové soubory s nastavením, ty musejí být umístěny v adresáři s nastavením (`/etc/shorewall`). Ve většině případů stačí použít pouze následující soubory:

- `zones`
- `interfaces`
- `masq`
- `rules`
- `policy`
- `routestopped`

Zones – v tomto souboru je potřeba nastavit jednotlivé zóny. V případě sítě jako je na obrázku to budou tři zóny:




```
fw              firewall
net             ipv4
loc             ipv4
```

`fw` je počítač, na kterém běží firewall (server), `net` je zóna pro venkovní síť (Internet) a `loc` je zóna pro síť se stanicemi.

V souboru interfaces je potřeba přiřadit zóny k síťovým kartám:

```
net             eth0            detect
loc             eth1            detect
```

Na kartu `eth0` bude připojen Internet a ke kartě `eth1` budou připojeny stanice.

Soubor masq – nastavení NATu. První je síťová karta připojená k Internetu a druhá je karta pro vnitřní síť.

```
#VSTUP          VYSTUP
eth0            eth1
```

Kvůli NATu je potřeba ještě soubor routestopped, v tom se nastavuje síťová karta, která bude fungovat v případě, že se nepodaří firewall spustit. Routestopped se musí vždy použít!

```
eth1
```

V policy jsou nadefinována samotná pravidla pro provoz:

```
#ZDROJ          CIL             PRAVIDLO            UROVEN LOGOVANI

$FW             net             ACCEPT
$FW             loc             ACCEPT
net             $FW             DROP                info
net             all             DROP                info
loc             $FW             ACCEPT
loc             net             ACCEPT


# THE FOLLOWING POLICY MUST BE LAST
#
all               all             REJECT              info
```

Server (`$FW`) bude mít přístup (`ACCEPT`) jak do Internetu (`net`), tak do místní sítě (`loc`). Všechny přístupy z Internetu na server a na všechna ostatní zařízení se zahodí (`DROP`) a tato událost se zapíše do systémového logu. Ze stanic bude možné přistupovat na server i na Internet. Jako poslední je nebytně nutné poslední pravidlo – to odmítne (`REJECT`) všechen ostatní provoz a zapíše ho do logu.

V případě, že budete potřebovat nastavit nějakou vyjímku, například povolit `ssh` přihlášení na server z Internetu nebo nastavit směrování portů, musíte tuto vyjímku uvést v souboru rules:

```
#AKCE          ZDROJ           CIL     PROTOKOL    CILOVY PORT(Y)
#ACCEPT        net             $FW     <protocol>  <port>
```

```
Ping/ACCEPT    all              $FW
 #povoli ping ze vsech zarizeni na firewall (vyuziva se makro shorewallu)

ACCEPT         net              $FW      tcp         22
 #povoli ssh z Internetu (ale ne z mistni site se stanicemi)


ACCEPT         net:192.168.0.1          $FW         udp   514
 # povoli vzdalene logovani do syslogu z pocitace s uvedenou IP
```

5 Sledování uživatelů na stanicích

Ve školách, internetových kavárnách a podobných organizacích je skoro nezbytné mít možnost kontrolovat aktivitu uživatelů na stanicích. Blokování některých stránek a podobná opatření jsou samozřejmostí. U těchto řešení však stále není kontrola nad uživatelem. Tu získáte např. pomocí programu iTALC [18]. Jednou z největších výhod iTALCu je cena – program je zdarma včetně zdrojových kódů (licence GNU GPL). iTALC je navíc multiplatformní, to znamená že ho můžete provozovat jak na Windows, tak na Linuxu.

Pomocí tohoto řešení může správce/učitel nebo kdokoliv, kdo je u serveru a má potřebná oprávnění, kontrolovat a ovládat stanice.

Instalaci na serveru proveďte následovně:

```
apt-get install libitalc italc-client italc-master
```

Na stanicích je to o trochu složitější. Nejdřív se přepněte do adresáře /opt/ltsp/i386 a nainstalujte klientskou aplikaci iTALCu.

```
chroot /opt/ltsp/i386
apt-get install italc-client
```

Po instalce zkopírujte veřejný klíč serveru do adresáře s obrazem stanic, jinak nebude možné stanice ze serveru ovládat.

```
cp /etc/italc/keys/public/teacher/key /opt/ltsp/i386/etc/italc/keys/public/teacher/key
ltsp-update-image
```

Poté je potřeba povolit v souboru /var/lib/tftpboot/ltsp/i386/lts.conf spouštění iTALCu a aktualizovat obraz pro stanice.

```
[Default]
   START_ITALC = True
```

```
ltsp-update-image
```

iTALC si při ukončení neuloží své nastavení a po opětovném spuštění má výchozí nastavení. To může být výhoda i nevýhoda. Jednou to natavíte a když uživatel něco pokazí, samo se to opraví.

Pro uložení nastavení vytvořte adresář `/etc/italc/configfiles` a zkopírujte do něj své nastavení:

```
mkdir -p /etc/italc/configfiles
cp ~/.italc/globalconfig.xml /etc/italc/configfiles
```

Ještě musíte říci iTALCu, kde má nastavení hledat, konkrétně je to sekce `[paths]` v souboru `/etc/xdg/iTALC Solutions/iTALC.conf`.

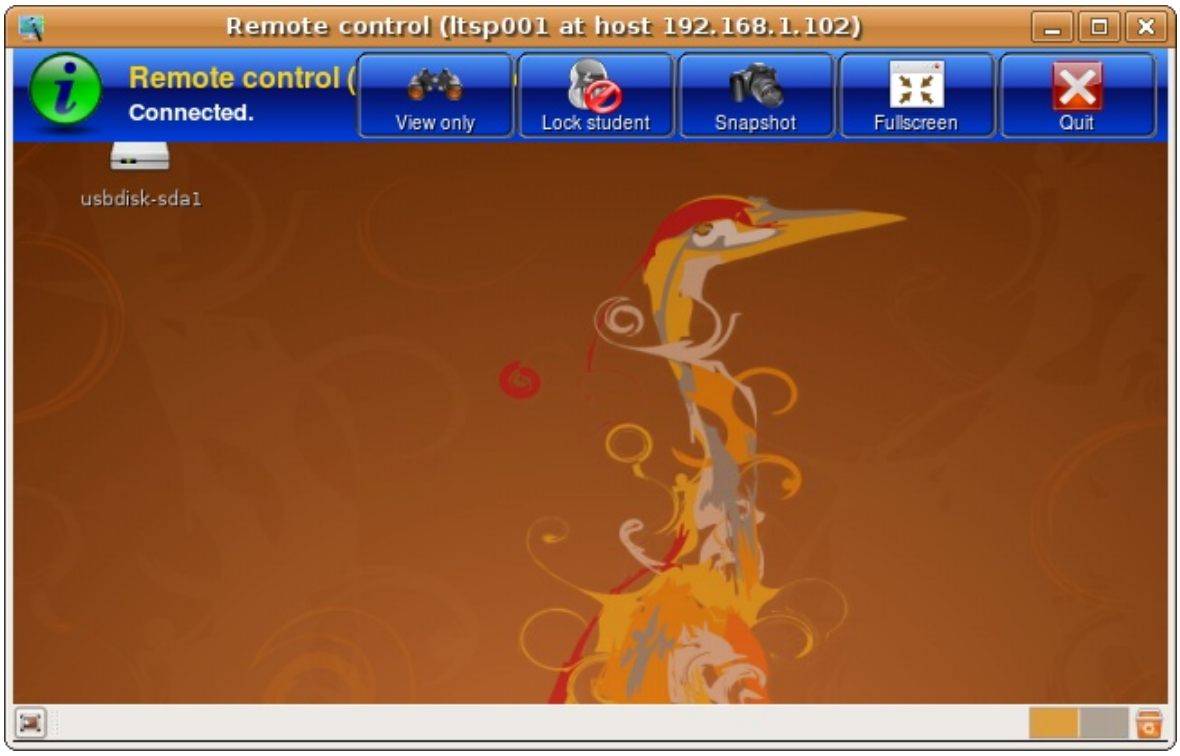
```
. . . . . .

[paths]
   globalconfig=/etc/italc/configfiles/globalconfig.xml
```

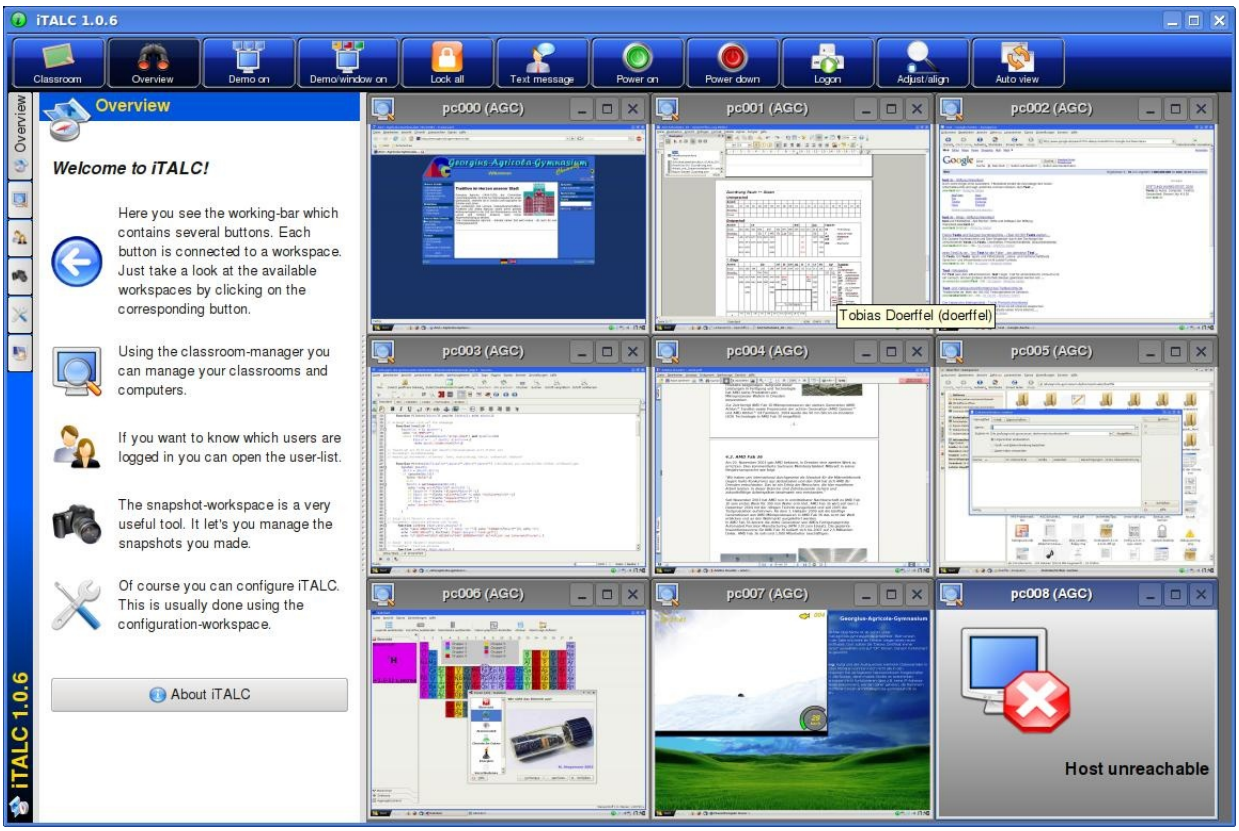
Kvůli bezpečnosti je lepší u souborů s nastavením nastavit jako vlastníka uživatele root.

```
chown -R root:root /etc/italc
chmod 755 /etc/italc/configfiles/globalconfig.xml
```

U dynamických IP adres pravděpodobně nastanou problémy, proto raději stanicím, na kterých chcete používat iTALC nastavte statickou IP adresu (viz kapitola 3.2.3).

Po zapnutí programu na serveru se zobrazí okno s náhledy pracovních ploch stanic. Pokud je vidět podezřelá aktivita, je možné zobrazit plochu stanice přes celou obrazovku nebo ji rovnou zamknout. Užitečná je také možnost vytvořit screenshot, ten obsahuje i přesný čas a jméno přihlášeného uživatele.


Remote control (ltsp001 at host 192.168.1.102)
Remote control (
Connected.
View only
Lock student
Snapshot
Fullscreen
Quit
usbdisk-sda1


iTALC 1.0.6
Classroom
Overview
Demo on
Demo window on
Lock all
Text message
Power on
Power down
Logon
Adjust/align
Auto view
Overview
Welcome to iTALC!
Here you see the working-bar which contains several buttons. Each button is connected to a workspace. Just take a look at the available workspaces by clicking on the corresponding button.
Using the classroom-manager you can manage your classrooms and computers.
If you want to know which users are logged in you can open the user-list.
The snapshot-workspace is a very useful tool. It let's you manage the snapshots you made.
Of course you can configure iTALC. This is usually done using the configuration-workspace.
About iTALC
pc000 (AGC)
pc001 (AGC)
pc002 (AGC)
Tobias Doerffel (doerffel)
pc003 (AGC)
pc004 (AGC)
pc005 (AGC)
pc006 (AGC)
pc007 (AGC)
pc008 (AGC)
Host unreachable

6 Použité zkratky a termíny

Linux

Svobodné jádro operačního systému. Často se tak nesprávně říká celé distribuci.

GNU/Linux

Celá Linuxová distribuce, to znamená jádro a programy.

NAT

Je technologie pro překlad IP adres, ta umožňuje sdílet jednu veřejnou IPv4 adresu skupině uživatelů a ti pak mohou mít přístup na Internet [19].

Bezdisková stanice

Bezdisková stanice je starý, nebo málo výkonný počítač bez disku a operačního systému, která nabootuje ze sítě a přenáší uživatelův vstup (klávesnice, myš) na server, na kterém běží všechny programy, výstup se zpětně přenáší na stanici.

Ubuntu Alternate Install CD

Instalační CD Ubuntu GNU/Linuxu, které obsahuje přednastavený LTSP server a má textový instalátor.

ext3 [20]

Žurnálovací souborový systém používaný ve většině moderních Linuxových distribucí.

swap

Odkádací prostor na disku, který se používá při nedostatku RAM. Je mnohanásobně pomalejší než RAM. Unixové systémy pro swap typicky používají samostatný diskový oddíl, lze však swapovat i do souboru, jako to je například v MS Windows.

sudo

S pomocí tohoto programu může i běžný uživatel spouštět některé programy s právy roota.

setuid, suid

Speciální příznak, díky kterému jádro při spuštění nastaví programu práva vlastníka. Používá se například u programu `ping` (/bin/ping), tento program může používat pouze root, proto má nastaven setuid bit, aby ho mohli používat i běžní uživatelé.

DHCP

Protokol, který se stará o automatické přidělování IP adres. Dále se používá pro přidělení masky, brány, adres DNS serverů, …

Gnome [21]

Prostředí pracovní plochy používané v unixových operačních systémech. Je postaveno na knihovně GTK+, původně určené pro grafický editor GIMP.

PXE

Zkratka z `Preboot eXecution Environment`. Technologie navržená Intelem umožnující bootování operačního systému po síti.

gPXE

Je svobodný síťový zavaděč. Poskytuje náhradu za uzavřené PXE zavaděče. Podporuje bootování pomocí TFTP, FTP a HTTP.

LILO , GRUB

Zavaděče operačního systému. Modernější GRUB poskytuje mnohé užitečné funkce, jako je možnost editaci bootovacích parametrů přímo ze zavaděče.

iptables

Mocný nástroj pro nastavení síťové komunikace v Linuxu. Pomocí iptables lze nastavit různé typy firewallů.

screenshot

Snímek obrazovky v podobě grafického souboru (obrázku).

iTALC

Software vyvinutý pro školy, který umožňuje monitorovat činnost počítačů a blokovat neukázněné uživatele.

7 Odkazy

1 : Linux Terminal Server Project (http://ltsp.org/)

2 : Ubuntu GNU/Linux (http://www.ubuntu.cz/)

3 : Ubuntu Linux Alternate CD 32bit (http://releases.ubuntu.com/intrepid/ubuntu-8.10-alternate-i386.iso)

4 : Infra Recorder (http://infrarecorder.org/)

5 : Zdroj balíčků OpenOffice.org (https://launchpad.net/~openoffice-pkgs/+archive)

6 : Nautilus (http://projects.gnome.org/nautilus/)

7 : Midnight Commander (http://www.midnight-commander.org/)

8 : Chyba v LTSP (problém s NBD swapováním) (https://bugs.launchpad.net/ubuntu/+source/ltsp/+bug/281501)

9 : Paměť PROM pro bootování ze sítě (http://etherboot.org/wiki/burningroms)

10 : Set User ID - program se spustí s právy jiného uživatele ( )

11 : LInux LOader ( )

12 : Grand Unified Bootloader ( )

13 : Martin Vancl - editace záznamů v Grubu (http://martin.vancl.eu/jak-se-dostat-do-zaheslovaneho-linuxu)

14 : Martin Vancl - zabezpečení Grubu (http://martin.vancl.eu/zabezpeceni-grubu)

15 : Netfilter - firewall v Linuxovém jádře (http://netfilter.org/)

16 : Seriál o IPTABLES na root.cz (http://www.root.cz/serialy/vse-o-iptables/)

17 : Shorewall - skripty pro nastavení firewallu (http://www.shorewall.net/)

18 : Intelligent Teaching And Learning with Computer ( )

19 : NAT na wikipedii (http://cs.wikipedia.org/wiki/Network_address_translation)

20 : Souborový systém ext3 (http://cs.wikipedia.org/wiki/Ext3)

21 : GNOME - prostředí pracovní plochy (http://cs.wikipedia.org/wiki/GNOME)

8 Použité zdroje

Domovská stránka Linux Terminal Server Project - http://ltsp.org/

Dokumentace komunity na Ubuntu.com - https://help.ubuntu.com/community/UbuntuLTSP

Ubuntu GNU/Linux - http://www.ubuntu.cz/

LTSP dokumentace - file:///usr/doc/ltsp-server

Hacking Bez tajemství LINUX - ISBN: 80-7226-869-4

Seriál o Shorewallu - http://www.linuxexpres.cz/praxe/shorewall-1-dil-1

Domovská stránka Shorewallu - http://shorewall.org

PC Slovník - http://www.abclinuxu.cz/slovnik

iTALC - http://italc.sourceforge.net/wiki/

Domovská stránka Asmo Koskinena - http://www.arkki.info/

Linuxsoft „SUDO“ - http://www.linuxsoft.cz/article.php?id_article=493

Wikipedie, otevřená encyklopedie - http://cs.wikipedia.org/

Seriál „Vše o iptables“ - http://www.root.cz/serialy/vse-o-iptables/