

UNIVERSIDADE LUTERANA DO BRASIL

ULBRA – *CAMPUS* GUAÍBA

CURSO DE SISTEMAS DE INFORMAÇÃO



**CRIAÇÃO DE UM LABORATÓRIO DE  
INFORMÁTICA COM A UTILIZAÇÃO DE UM  
SERVIDOR LTSP  
RELATÓRIO DO ESTÁGIO CURRICULAR**

LUCAS COELHO XAVIER

Guaíba, 1º de Dezembro de 2009.

## **DADOS DE IDENTIFICAÇÃO**

Acadêmico: Lucas Coelho Xavier

Endereço: Rua Walter Kess, 1584 - Camaquã

E-mail: [swmxavier@gmail.com](mailto:swmxavier@gmail.com)

Fone(s): (51) 3671-3831/ (51) 9220-4701

Professor Supervisor: Newton Cunha Muller

E-mail: [mmuller.voy@terra.com.br](mailto:mmuller.voy@terra.com.br)

Local de Estágio: ULBRA – Campus Guaíba

Supervisor na Empresa: Carlos Mário Dal'Col Zeve

Endereço: BR 116, 5724. Morada da Colina – Guaíba/RS

E-mail: [si.guaiba@ulbra.br](mailto:si.guaiba@ulbra.br)

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO.....</b>	<b>4</b>
<b>2</b>	<b>APRESENTAÇÃO DA EMPRESA .....</b>	<b>4</b>
<b>3</b>	<b>FUNDAMENTAÇÃO TEÓRICA.....</b>	<b>5</b>
<b>4</b>	<b>SOLUÇÃO IMPLEMENTADA .....</b>	<b>6</b>
<b>4.1</b>	<b>O SERVIDOR.....</b>	<b>6</b>
<b>4.2</b>	<b>A INSTALAÇÃO .....</b>	<b>7</b>
<b>4.3</b>	<b>PREPARANDO OS TERMINAIS LEVES .....</b>	<b>7</b>
<b>5</b>	<b>AUTENTICANDO O SERVIDOR NO ACTIVE DIRECTORY .....</b>	<b>8</b>
<b>6</b>	<b>CONCLUSÕES E RESULTADOS ALCANÇADOS .....</b>	<b>9</b>
<b>7</b>	<b>REFERÊNCIAS .....</b>	<b>9</b>
<b>8</b>	<b>ANEXOS.....</b>	<b>11</b>

## **1 INTRODUÇÃO**

Neste relatório será apresentada, a implantação de um servidor LTSP (Linux Terminal Server Project) no LABIN da ULBRA campus Guaíba.

Este projeto visa utilizar microcomputadores com baixo poder de processamento, para rodar aplicativos atuais, sem que seja necessário, o upgrade de hardware dos microcomputadores.

O projeto terá como objetivo, diminuir os custos com a aquisição de novo hardware e licenças de software, além de proporcionar aos usuários do laboratório o contato com o sistema operacional LINUX.

Apesar de a proposta original ter sido a de utilizar microcomputadores que estavam fora de uso, por serem considerados obsoletos, o projeto aproveitou um laboratório já existente, com microcomputadores que possuem o Windows 2000 Professional instalado, porém isso também trouxe vantagens que serão apresentadas mais adiante neste relatório. Além disso, a maneira como o projeto foi implementado permite que novos laboratórios possam ser feitos, aproveitando microcomputadores que estejam fora de uso.

## **2 APRESENTAÇÃO DA EMPRESA**

Mantida pela Comunidade Evangélica Luterana São Paulo – CELSP, a Universidade Luterana do Brasil – ULBRA - tem foco na área da educação. Desde a primeira escola, fundada em 1911, até hoje, a ULBRA caracteriza-se por ser uma instituição voltada para o futuro, buscando sempre a modernização da sua infraestrutura e dos recursos pedagógicos. Assim, a Instituição se movimenta para disponibilizar serviços de qualidade para acadêmicos, professores, profissionais e toda a comunidade.

O LABIN da universidade, onde será implementado o projeto, é um espaço utilizado por alunos de todos os cursos. O LABIN possui salas especializadas para aulas de disciplinas do curso de sistemas de informação, mas também disponibiliza

salas para uso dos demais alunos da universidade, oferecendo acesso a internet para pesquisas, e impressão para a realização de trabalhos

### 3 FUNDAMENTAÇÃO TEÓRICA

Vou apresentar quais as tecnologias, serviços e protocolos envolvidos no projeto.

LTSP - Significa Linux Terminal Server Project, é um projeto baseado em Linux que tem por objetivo, utilizar microcomputadores de baixo poder de processamento, ligados a um servidor onde as aplicações são executadas

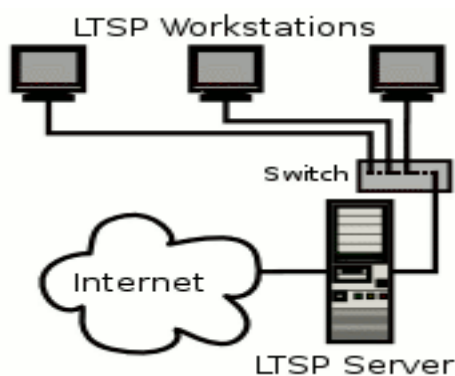


Imagem simplificada do projeto

Terminais Leves - Também chamados de Thin Clients, é a

DHCP – Dynamic Host Configuration Protocol (Protocolo de Configuração Dinâmica de Endereços de Rede), ele é um dos protocolos de serviço do TCP/IP, responsável por atribuir endereços IP, aos micros de uma rede. Este protocolo é necessário para que os terminais leves possam carregar o sistema.

Etherboot – É um “sistema de arranque” que permite a computadores carregar um sistema operacional em uma rede, o código de arranque pode ser gravado, na BIOS, EPROMs, disquetes, CDs, e HDs. Neste projeto foi utilizado o Etherboot gravado em disquete.

TFTP – Trivial File Transfer Protocol, é um protocolo simples para transferir pequenos arquivos, entre hosts, muito utilizado em redes onde terminais iniciam seu funcionamento a partir de um servidor. Envia o Kernel e boot para as máquinas clientes pela rede.

NFS – Network File System, é um protocolo desenvolvido pela Sun Microsystems, que permite a um usuário acessar arquivos em uma rede. O NFS é utilizado para que o cliente possa montar no servidor um sistema de arquivos.

LDM – LTSP Display Manager, é um gerenciador de exibição escrito especificamente para o LTSP para manipular os logins dos terminais no servidor.

SSH – Secure Shell, é ao mesmo tempo uma ferramenta e um protocolo de acesso remoto, que utiliza criptografia. Sem o SSH os terminais leves não conseguem se logar ao servidor LTSP.

## **4 SOLUÇÃO IMPLEMENTADA**

### **4.1 O SERVIDOR**

Para a realização do estágio será utilizado, como servidor LTSP um microcomputador com as seguintes configurações:

- Processador: Intel Celeron 420 1,6 Ghz;
- Memória:4 GB;
- S.O.: Linux, Distribuição Ubuntu 9.04 Server;
- HD: 80 GB.

As estações clientes possuem muitas configurações diferentes, por isso não listarei seus hardwares, mas todos os microcomputadores utilizados tanto nos restes quanto no LABIN possuem hardwares de 8 á 10 anos atrás.

A distribuição Linux escolhida para a utilização do servidor LTSP, foi o Ubuntu 9.04 server. A escolha da distribuição se deu através dos seguintes itens:

- Um ótimo suporte através de fóruns e comunidades;
- Por se tratar de uma distribuição recomendada para quem esta iniciando a utilizar o Linux;
- Por ser uma das distribuições que já trabalha com a última versão do LTSP.

## 4.2 A INSTALAÇÃO

Nesta seção apresentarei como foi feita a instalação de todos os pacotes serviços e protocolos, necessários para o funcionamento do LTSP. Ao final do relatório serão apresentados os arquivos de configuração.

Primeiro passo foi a instalação do sistema operacional. Após a instalação do Ubuntu 9.04, foi feita a atualização do sistema através do comando:

```
# sudo apt-get update
```

Depois foi feito o download e a instalação do LTSP, juntamente com o openssh utilizando o comando:

```
# sudo apt-get install openssh-server ltsp-server-standalone
```

A instalação do openssh é necessária para que os terminais possam se logar ao servidor LTSP.

O arquivo de configuração do ssh pode ser acessado através do comando:

```
# sudo nano /etc/ssh/sshd_config
```

A diretiva "X11Forwarding" deve estar setada com o valor "yes".

Esta opção só pode ficar desativada se o servidor não possuir interface gráfica.

Para a realização dos testes também foi feita a instalação do serviço de DHCP, através do comando:

```
# sudo apt-get install dhcp3-server
```

A configuração do dhcp foi feita através do comando:

```
# sudo nano /etc/ltsp/dhcpd.conf
```

## 4.3 PREPARANDO OS TERMINAIS LEVES

O próximo passo foi construir o ambiente chroot dos clientes com o comando:

```
# ltsp-build-client
```

Como as placas de rede dos micros usados não suportam boot via PXE então foi necessário gravar um disquete de boot, contendo o etherboot. Como as estações

clientes tinham placas de rede diferentes, foi usado uma imagem que contém drivers para todas as placas de rede, a imagem foi retirada do seguinte link:

[http://etherboot.anadex.de/eb\\_on\\_hd.ima](http://etherboot.anadex.de/eb_on_hd.ima)

Para gravar o disquete foi usado o comando:

```
# sudo dd if=eb_on_hd.ima of=/dev/fd0
```

Imagens do etherboot específicas para cada placa podem ser obtidas no site:

<http://www.rom-o-matic.net/>

Em seguida o disquete foi inserido nas estações e dado o boot.

O boot funcionou porém as estações estavam apenas com o modo texto. Foi necessário instalar uma interface gráfica para que as estações clientes pudessem ser utilizadas. Para isso foi utilizado o comando:

```
# sudo apt-get install ubuntu-desktop
```

Após novos testes, foi constatado problemas com resolução da tela e funcionamento dos mouses seriais. Para resolver o problema, foi editado o arquivo lts.conf.

O arquivo foi configurado através do comando:

```
# sudo nano /var/lib/tftpboot/ltsp/i386/lts.conf.
```

## **5 AUTENTICANDO O SERVIDOR NO ACTIVE DIRECTORY**

Foi feita a autenticação do servidor no AD da rede, com isso os terminais leves só conseguirão fazer logon se estiverem cadastrados no AD.

Para realizar a autenticação foram usados Winbind, Samba e Kerberos.

Todo o procedimento pode ser encontrado nos seguintes links::

<https://help.ubuntu.com/community/Samba/Kerberos>

<https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto>

Os arquivos de configuração se encontram nos anexos deste relatório.

## 6 CONCLUSÕES E RESULTADOS ALCANÇADOS

O LTSP é um ótimo projeto, pois além de reduzir custos, com a aquisição de novo hardware e licenças de software ele é relativamente fácil de implementar, sua configuração é simples, apenas algumas incompatibilidades com alguns hardwares, tornam um pouco mais trabalhoso o funcionamento de algumas estações clientes.

Os resultados acabaram sendo melhor do que o esperado, pois a intenção era de ter um laboratório, rodando apenas o sistema Linux, com a distribuição Ubuntu 9.04 (Jaunty Jackalope), mas como o laboratório utilizado para a implementação já continha micros com o S.O. Windows 2000, foi possível manter os 2 sistemas operacionais, assim em caso de algum problema com o servidor LTSP, os computadores podem fazer o boot do Windows 2000.

Como já foi citado, o principal benefício do projeto para a universidade foi a economia, com a aquisição de licenças de software e hardware novos, além da possibilidade de adição de novos terminais, que se encontrem localizados fisicamente em qualquer lugar da rede, também podendo ser utilizados laboratórios inteiros para se conectarem ao servidor LTSP, sendo necessário fazer upgrade somente no servidor LTSP para que este suporte mais estações. Outro ponto importante do projeto ser implementado no LABIN da universidade é que os alunos do curso de Sistemas de Informação podem ter contato direto com o funcionamento deste projeto.

Este estágio me possibilitou um maior contato com o S.O. Linux, além da experiência de montar um projeto que se encaixa muito bem no cenário atual de T.I. , com a crescente tendência da chamada T.I. verde que tem como um de seus focos o reaproveitamento de parques tecnológicos.

## 7 REFERÊNCIAS

FURASTÉ, Pedro Augusto. **Normas Técnicas para o Trabalho Científico: explicitação das normas da ABNT**. Porto Alegre: [s.n.], 2002. 143p.

Customizing Thin Clients. Página encontrada em <http://doc.ubuntu.com/edubuntu/edubuntu/handbook/C/customizing-thin-client.html> acessada em :23/11/2009.

LTSP 5 no Ubuntu 8.04, Página encontrada em  
<http://www.vivaolinux.com.br/artigo/LTSP-5-no-Ubuntu-8.04/>, acessada  
em:15/09/2009.

Instalação e Configuração do LTSP-5 no UBUNTU 7.04, Página encontrada em:  
<http://www.youtube.com/watch?v=9Ht2ojdmjCQ>, acessada em: 15/09/2009.

LTSP Pantaneiro, Página encontrada em:  
[http://gutocarvalho.net/mediawiki/index.php?title=LTSP Pantaneiro](http://gutocarvalho.net/mediawiki/index.php?title=LTSP_Pantaneiro) acessada em:  
15/09/2009.

Logando Clientes Linux, Página encontrada em:  
<http://www.gdhpress.com.br/redeseservidores/leia/index.php?p=cap6-10> acessada  
em: 05/11/2009

Instalando o LTSP, Página encontrada em:  
<http://wiki.sintectus.com/bin/view/GrupoLinux/LicaoLTSP> acessada em:05/11/2009

Ubuntu Linux autenticando no Active Directory, Página encontrada em:  
<http://wiki.ubuntu-br.org/AutenticandoAD> acessada em:10/11/2009

## 8 ANEXOS

Arquivo de configuração do SSH.

### **sshd.conf**

# Package generated configuration file

# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for

Port 22

# Use these options to restrict which interfaces/protocols sshd will bind to

#ListenAddress ::

#ListenAddress 0.0.0.0

Protocol 2

# HostKeys for protocol version 2

HostKey /etc/ssh/ssh\_host\_rsa\_key

HostKey /etc/ssh/ssh\_host\_dsa\_key

#Privilege Separation is turned on for security

UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key

KeyRegenerationInterval 3600

ServerKeyBits 768

# Logging

SyslogFacility AUTH

LogLevel INFO

# Authentication:

LoginGraceTime 120

PermitRootLogin yes

StrictModes yes

RSAAuthentication yes

PubkeyAuthentication yes

#AuthorizedKeysFile %h/.ssh/authorized\_keys

# Don't read the user's ~/.rhosts and ~/.shosts files

IgnoreRhosts yes

# For this to work you will also need host keys in /etc/ssh\_known\_hosts

RhostsRSAAuthentication no

# similar for protocol version 2

HostbasedAuthentication no

# Uncomment if you don't trust ~/.ssh/known\_hosts for RhostsRSAAuthentication

#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)

PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with

# some PAM modules and threads)

ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords

#PasswordAuthentication yes

# Kerberos options

#KerberosAuthentication no

#KerberosGetAFSToken no

#KerberosOrLocalPasswd yes

#KerberosTicketCleanup yes

# GSSAPI options

#GSSAPIAuthentication no

#GSSAPICleanupCredentials yes

X11Forwarding yes

X11DisplayOffset 10

PrintMotd no

PrintLastLog yes

TCPKeepAlive yes

#UseLogin no

#MaxStartups 10:30:60

#Banner /etc/issue.net

# Allow client to pass locale environment variables

AcceptEnv LANG LC\_\*

Subsystem sftp /usr/lib/openssh/sftp-server

UsePAM Yes

Arquivo de configuração do DHCP

### **dhcpd.conf**

```
authoritative;
```

```
subnet 192.168.0.0 netmask 255.255.255.0 {  
    range 192.168.0.20 192.168.0.250;  
    option domain-name "telecentro";  
    option domain-name-servers 192.168.0.1;  
    option broadcast-address 192.168.0.255;  
    option routers 192.168.0.1;  
    option subnet-mask 255.255.255.0;  
    if substring( option vendor-class-identifier, 0, 9 ) = "PXEClient" {  
        filename "/ltsp/i386/pxelinux.0";  
    }  
    else{  
        filename "/ltsp/i386/nbi.img";  
    }  
    option root-path "/opt/ltsp/i386";  
}
```

Arquivo de configuração do kerberos

### **krb5.conf**

[logging]

default = FILE:/var/log/krb5.log

[libdefaults]

default\_realm = GUAIBA.ULBRA.TCHE.BR

kdc\_timesync = 1

ccache\_type = 4

forwardable = true

proxiable = true

[realms]

GUAIBA.ULBRA.TCHE.BR = {

kdc = dc-labin.guaiba.ulbra.tche.br

admin\_server = dc-labin.guaiba.ulbra.tche.br

default\_domain = GUAIBA.ULBRA.TCHE.BR

}

[domain\_realm]

.guaiba.ulbra.tche.br = .GUAIBA.ULBRA.TCHE.BR

guaiba.ulbra.tche.br = GUAIBA.ULBRA.TCHE.BR

[login]

krb4\_convert = true

krb4\_get\_tickets = false

Arquivo de configuração do Samba

**smb.conf**

#===== Global Settings =====

[global]

security = ads  
realm = GUAIBA.ULBRA.TCHE.BR  
password server = 10.1.1.1  
workgroup = LABIN  
winbind separator = -  
winbind refresh tickets = yes  
idmap uid = 10000-20000  
idmap gid = 10000-20000  
winbind enum users = yes  
winbind enum groups = yes  
template homedir = /home/%D/%U  
template shell = /bin/bash  
client use spnego = yes  
client ntlmv2 auth = yes  
encrypt passwords = yes  
winbind use default domain = yes  
restrict anonymous = 2

Arquivo de configuração do nsswitch

### **nsswitch.conf**

# Example configuration of GNU Name Service Switch functionality.

# If you have the `glibc-doc-reference' and `info' packages installed, try:

# `info libc "Name Service Switch"' for information about this file.

passwd: compat winbind

group: compat winbind

shadow: compat

hosts: files mdns4\_minimal [NOTFOUND=return] dns mdns4

networks: files

protocols: db files

services: db files

ethers: db files

rpc: db files

netgroup: nis

## Arquivos de configuração do PAM

### **common-account**

account sufficient pam\_winbind.so

account required pam\_unix.so

### **common-auth**

auth sufficient pam\_winbind.so krb5\_auth krb5\_ccache\_type=FILE

auth sufficient pam\_unix.so nullok\_secure use\_first\_pass

auth required pam\_deny.so

### **common-session**

session required pam\_unix.so

session required pam\_mkhomedir.so umask=0022 skel=/etc/skel

### **sudo**

@include common-account

auth sufficient pam\_winbind.so

auth sufficient pam\_unix.so use\_first\_pass

auth required pam\_deny.so