1. Objectivos

Conhecer os utilitários de rede mais usados para:

trabalho remoto num servidor.

trabalho sobre ficheiros remotos.

transferências de ficheiros de e para servidores remotos.

2. Introdução

Na DEE.Net existem máquinas que se destinam a dar suporte às actividades lectivas. Disponibilizam serviços de armazenamento de ficheiros, desenvolvimento de aplicações, publicação de páginas Web pessoais, etc. A maioria destes servidores funciona sobre o sistema operativo GNU/Linux.

De uma forma geral, o acesso aos serviços disponibilizados nos servidores pode ser efectuado a partir de qualquer posto de trabalho com uma ligação à Internet, independentemente do sistema operativo utilizado. Os sistemas (hardware e software) utilizados para aceder aos serviços disponibilizados nos servidores podem ser designados por “Clientes”.

Por questões de segurança os servidores poderão não admitir o estabelecimento de sessões remotas de trabalho e de transferência de ficheiros que não estejam devidamente autenticadas através da identificação do utilizador (User / Password) ou que não implementem encriptação dos dados transmitidos.

Existem diversos aplicativos para estabelecimento de sessões remotas, quer para sistemas operativos Linux ou Windows. Geralmente, estes utilitários utilizam os mecanismos de autenticação e encriptação designados por SSL (Secure Socket Layer). Exemplos destes utilitários são o **PuTTY**, o **WinSCP**, o **scp**, o **sftp**, e o **ssh**.

Utilitários como o **telnet** e o **ftp** não implementam mecanismos de encriptação de dados. Apenas autenticam o utilizador, como é exigido pelo sistema remoto.

Todos os comandos em Linux têm um manual. Para consultar o manual de um comando usa- se o comando **man**. Por exemplo:

```
man ssh
```

3. Sessão remota de trabalho

3.1 Sessão remota de trabalho usando o comando telnet

Tal como o exemplo anterior, o comando telnet também permite o estabelecimento de sessões de trabalho em máquinas remotas a partir do ambiente de trabalho da máquina local. Este comando implementa o protocolo TELNET. Por defeito este só faz uso do mecanismo de autenticação exigido

pelo SO da máquina remota. Não é estabelecida uma ligação segura (nem cifra dos dados transaccionados nem autenticação das máquinas envolvidas). É possível que se encontrem definidas restrições à utilização deste serviço/protocolo em função da origem da ligação.

Para estabelecer uma sessão remota de trabalho usando o comando telnet, basta abrir uma consola (terminal) e digitar um dos seguintes comandos na máquina local:

```
telnet –l <nome_do_utilizador_no_ave> ave.dee.isep.ipp.pt
```

ou

```
telnet ave.dee.isep.ipp.pt
```

Dependendo do comando introduzido será necessário introduzir somente a senha (password) ou o par nome/senha (login/password) relativos à máquina de destino (login/password). Só após o utilizador estar devidamente autenticado é que é possível executar comandos Linux, em modo linha, na máquina remota. A janela onde forem executados estes comandos passa a refletir o ambiente de trabalho na máquina remota (neste caso o servidor ave). Todo o restante ambiente de trabalho (menus, janelas, barras, etc) permanece relativo à máquina local.

1. Inicie uma sessão remota no servidor ave utilizando o comando telnet.

2. Liste o conteúdo da sua conta no servidor ave (ls -la).

Para mais informações sobre o comando **telnet** é possível consultar o manual respectivo:

```
man telnet
```

Na nova sessão remota, execute os seguintes comandos e anote o que cada um deles faz.

1. `ls`
2. `pwd`
3. `hostname`
4. `who`
5. `w`

Termine a sua sessão remota com o comando:

```
exit
```

3.2 Utilizando o comando ssh

O utilitário cliente **ssh** (OpenSSH) é utilizado para estabelecer sessões seguras de trabalho numa máquina remota a partir de um terminal alfanumérico. Para estabelecer uma sessão remota de trabalho usando o comando **ssh,** basta abrir uma consola (num terminal da sua máquina local) e digitar um dos seguintes comandos:

```
ssh –l <nome_do_utilizador> <máquina_remota>
```

ou

```
ssh <máquina_remota>
```

ou

```
ssh <nome_do_utilizador>@<máquina_remota>
```

Dependendo do comando introduzido será necessário introduzir somente a senha (password) ou o par nome/senha (login/password) relativos à máquina de destino (login/password). Só após o utilizador, a máquina local e também a remota estarem devidamente autenticados é que é possível executar comandos Linux, em modo linha, na máquina remota. A janela (consola ou terminal) onde forem executados estes comandos reflete o ambiente de trabalho na máquina remota (neste caso o servidor

ave). Todo o restante ambiente de trabalho (menus, janelas, barras, etc) permanece relativo à máquina local.

Utilizando o utilitário SSH num terminal do PC local, estabeleça uma nova sessão remota no servidor ave. Para tal use as suas credenciais (login/password) pessoais. Na nova sessão remota, verifique a funcionalidade dos seguintes comandos.

1. **`ls`**
2. **`pwd`**
3. **`hostname`**
4. **`who`**
5. **`w`**
6. **`mkdir WWW`** (WWW em maiúsculas)
7. **`chmod 755 WWW`**
8. **`cd WWW`**
9. **`pwd`**
10. **`ls`**
11. **`mkdir cinem`**

Termine a sua sessão remota com o comando:

```
exit
```

Para executar remotamente apenas um comando, terminando imediatamente a sessão de trabalho, basta numa consola (terminal) digitar:

```
ssh <nome_do_utilizador_no_ave>@ave.dee.isep.ipp.pt <comando>
```

Para mais informações sobre o comando ssh é possível consultar o manual respectivo:

```
man ssh
```

4. Transferência de ficheiros

4.1 Transferência de ficheiros usando o comando scp

A transferência de ficheiros ou de diretórios entre máquinas usando o comando **scp** faz uso dos mecanismos de segurança oferecidos pelo SSH – autenticação de pessoas e máquinas, como também a cifra dos dados transacionados.

Para efectuar a cópia de ficheiros entre a máquina local e remota usando a aplicação scp, deve-se usar a seguinte sintáxe (genérica) ou outra semelhante.

```
scp <ficheiro_de_origem> <ficheiro_de_destino>
```

onde tanto <*ficheiro_de_origem*> como <*ficheiro_de_destino*> podem ser do tipo:

```
<nome_utilizador>@<máquina>:<nome_ficheiro>
```

Um <*nome_ficheiro*> pode incluir a localização do ficheiros na árvore de diretórios respectiva. Localizações iniciadas por / são referidas à raiz do sistema de ficheiros. Localizações não iniciadas por / são referidas ao diretório atual na máquina local ou ao diretório pessoal numa máquina remota.

1. Copie o ficheiro /home/docentes/jml/WWW/cinem/Guioes/lab1.pdf do servidor ave para o PC local.

```
scp user@ave.dee.isep.ipp.pt:~jml/WWW/cinem/Guioes/lab1.pdf .
```

2. Copie o ficheiro **lab1.pdf** para o directório **WWW/cinem** da sua conta no ave.

```
scp lab1.pdf user@ave.dee.isep.ipp.pt:WWW/cinem/
```

3. No campo de endereço do *browser*, introduza o localizador www.dee.isep.ipp.pt/~*utilizador*/cinem.

4.2 Transferência de ficheiros por FTP

O protocolo FTP (File Transfer Protocol) é utilizado na Internet para transferência bidireccional de ficheiros, sendo a aplicação ftp a sua interface. A versão segura desta interface é denominada por sftp e, à semelhança dos comandos anteriores permite autenticar utilizadores (por nome/senha) e máquinas (mecanismos de chave pública/certificados) e cifra dos dados transaccionados.

A utilização é idêntica em ambas as versões, sendo oferecido ao utilizador um ambiente de interação em modo texto. Para aceder a este ambiente basta digitar **ftp** ou **sftp**. Na "prompt" que surge é possível obter uma listagem dos comandos admissíveis através do comando **?** <Enter>.

Analise a seguinte sequência de comandos e experimente uma semelhante/equivalente.

```
1.  sftp user@ave.dee.isep.ipp.pt
2.  ?
3.  lls -al
4.  ls -al
5.  lmkdir store
6.  lcd store
7.  lls
8.  cd WWW
9.  ls
10. cd cinem
11. ls
12. get lab1.pdf
13. put lab1.pdf
14. bye
```

Repare que existem comandos que são executados na máquina local (tipicamente iniciam-se pela letra '**l**': **lls**, **lcd**, **lmkdir**) e comandos que são executados na máquina remota (da lista de comandos anterior: **ls** e **cd**). Os comandos get/put devem ser interpretados do ponto de vista da máquina local.

4.3 Transferência de ficheiros por HTTP

A aplicação **wget** (GNU) é classificada como "non interactive network downloader", ou seja, uma ferramenta de transferência de ficheiros que não exige a assistência do utilizador para realizar o processo de transmissão dos dados. Suporta os protocolos HTTP, HTTPS e FTP e pode ser executada em "*background*".

Suporta transferências recursivas de ficheiros permitindo assim a cópia parcial/total de sites Web ou repositórios de ficheiros. Apresenta grande capacidade de recuperação de falhas, podendo recomeçar automaticamente uma transferência interrompida devido a um problema de conectividade.

1. Utilize o comando **wget** para fazer *download* do guião da aula para o PC local.

```
wget ave.dee.isep.ipp.pt/~jml/cinem/Guioes/lab1.pdf
```

2. Verifique que o download foi realizado com sucesso.
3. Qual a opção do comando **wget** para colocar o download a correr em *background* (`man wget`)?

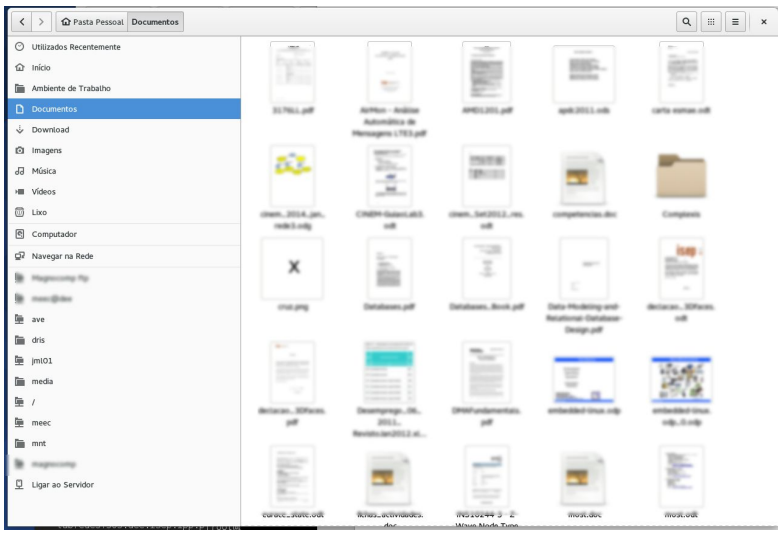
4.4 Acesso direto a ficheiros remotos

Os gestores de ficheiros normalmente disponíveis nos ambientes gráficos permitem trabalhar de forma coerente os ficheiros locais e os ficheiros localizados num servidor SFTP/SSH. O processo de estabelecimento da ligação varia com o gestor de ficheiros utilizado.

Nautilus

O gestor de ficheiros Nautilus é normalmente utilizado pelo ambiente gráfico Gnome.

Para estabelecer uma ligação a um diretório remoto através do Nautilus, utilize a opção **Ligar ao Servidor** localizada no fundo do menu do lado esquerdo



Selecione o serviço do tipo **SSH** e identifique o servidor como **ssh://ave.dee.isep.ipp.pt**.

Se necessário, identifique os seu homedir no ave como **/home/Alunos/xxxxxxx**.

Se não identificar o utilizador remoto, este será pedido no processo de ligação.

Existe a possibilidade de criar um marcador para acesso rápido a um servidor pré-configurado.

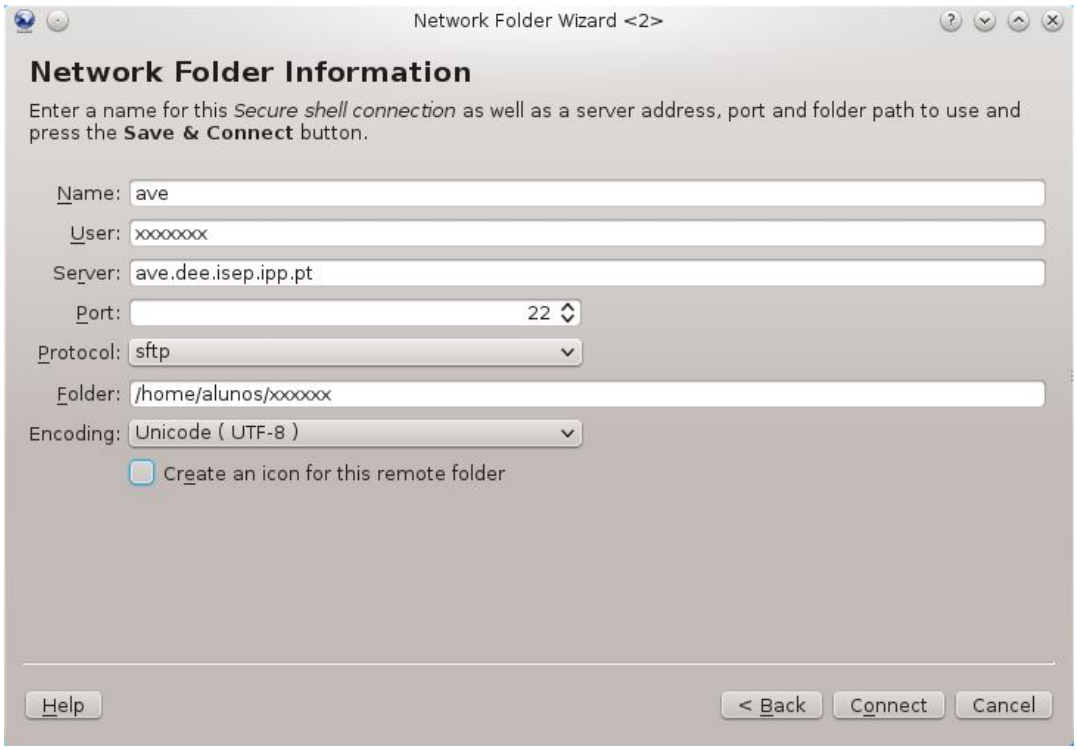
Dolphin

O gestor de ficheiros Dolphin é o normalmente utilizado nos computadores do laboratório.

Para estabelecer uma ligação a um diretório remoto através do Dolphin, selecione **Network** no painel do lado esquerdo e utilize a opção **Add Network Folder** localizada na área da direita.

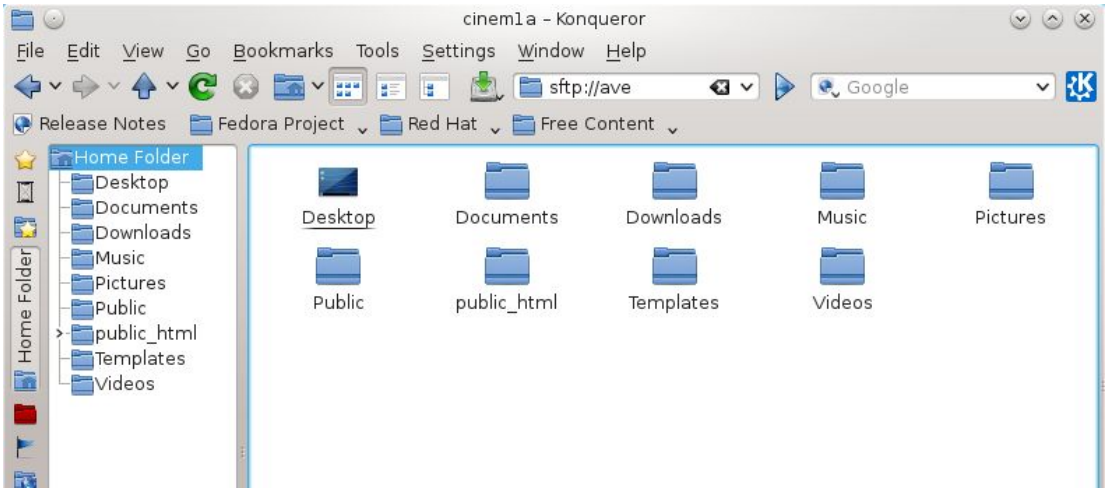
Selecione o tipo **Secure Shell (ssh).**

Identifique o servidor, o utilizador e a pasta a montar. Identifique o servidor como **ave.dee.isep.ipp.pt**. Identifique os seu homedir no ave como **/home/alunos/xxxxxxx**.



Konqueror

O Konqueror encontra-se normalmente instalado em todos os ambientes gráficos da família KDE. Integra as funcionalidades de gestor de ficheiros e de navegador Web.



Para estabelecer uma ligação a um diretório remoto através do Konqueror, identifique a pasta a montar no campo de endereço da barra superior.

Selecione o serviço do tipo **SSH** e identifique o servidor como **sftp://ave.dee.isep.ipp.pt** ou **sftp://xxxxxx@ave.dee.isep.ipp.pt**.

Se não identificar o utilizador remoto, este será pedido no processo de ligação.

5. Trabalho em ambiente gráfico remoto

A generalidade das aplicações gráficas em sistemas Linux/Unix utiliza as funcionalidades do sistema de

janelas X-Window. O X-Window é um sistema distribuído de servidores e clientes, em que os servidores estão ligados a terminais e as aplicações desempenham o papel de clientes. É assim possível manipular de forma transparente os terminais gráfico utilizados por cada aplicação, permitindo uma independência total entre a máquina onde uma aplicação é executada e o terminal utilizado para a interação com o utilizador.

Em simultâneo com o estabelecimento de um ligação para uma máquina remota, o cliente **ssh** pode preparar o servidor X residente na máquina local para permitir a ligação de clientes X da máquina remota. Para este efeito utiliza-se a opção -X.

Abra uma sessão de trabalho no servidor ave.dee.isep.ipp.pt, especificando a opção -X para permitir a abertura local de janelas a partir de aplicações remotas.

```
ssh -X <nome_do_utilizador>@ave.dee.isep.ipp.pt
```

As aplicações desencadeadas por comandos submetidos nesta janela são executados na máquina remota. Para as aplicações com interface gráfica será utilizado o computador local com o terminal. Experimente executar algumas aplicações que utilizam interface gráfica.

```
xclock

gedit teste.txt &

firefox

oowriter
```

6. Ligações Seguras em Ambientes Microsoft Windows

6.1 Sessão remota de trabalho usando o PuTTY

Para estabelecer uma sessão remota de trabalho usando o PuTTY (na secção de referências, está indicado o URL onde é possível obter este pacote) basta indicar, na janela principal da aplicação, a máquina de destino (caixa de texto) e seleccionar a opção relativa ao protocolo SSH. Em seguida, é necessário introduzir os dados do utilizador relativos à máquina de destino (login/password). Só após o utilizador, a máquina remota e eventualmente a máquina local estarem devidamente autenticados é que é possível executar comandos UNIX (Linux), em modo linha, na máquina remota.

Além da configuração básica indicada no parágrafo anterior é possível realizar outras (selecionar a categoria pretendida na caixa que se apresenta do lado esquerdo da janela) e eventualmente guardá-las para posteriores utilizações.

6.2 Transferência de ficheiros usando o Winscp

A aplicação **Winscp** destina-se a ambientes gráficos baseados em Microsoft Windows. Permite realizar as operações básicas de manipulação de ficheiros numa máquina remota Unix/Linux, usando SSH. Oferece uma interface amigável, tipo "*drag and drop*", para a transferência de ficheiros entre o sistema local Microsoft Windows e máquinas remotas Unix que suportem SSH.

6.3 Transferência de ficheiros usando o iXplorer

Esta aplicação – iXplorer - oferece uma interface amigável, a popularizada "*drag and drop*", para a transferência de ficheiros entre o sistema local Microsoft Windows e máquinas remotas Unix que suportem SSH.

A janela desta aplicação divide-se em duas zonas: uma relativa ao PC local e aos recursos disponibilizados por ele (à esquerda), e outra (à direita) relativa aos recursos da máquina remota.

7. Bibliografia

- The Linux Documentation Project, http://www.tldp.org/
- OpenSSH, http://www.openssh.com/
- OpenSSL, http://www.openssl.org/
- PuTTY: A Free Telnet/SSH Client, http://www.chiark.greenend.org.uk/~sgtatham/putty/
- Secure iXplorer Pro, vs 1.14, http://i-tree.org/
- Winscp, http://winscp.sourceforge.net/eng/download.php
- Nautilus, http://live.gnome.org/Nautilus

8. Histórico

CINEM - GuiaoLab1 - Utilitários de redes (Linux / Win) - v1.0 - 2008-09-24

CINEM - GuiaoLab1 - Utilitários de redes (Linux / Win) - v1.1 - 2008-09-30

CINEM - GuiaoLab1 - Utilitários de redes (Linux / Win) - v2.0 – 2009-10-09

CINEM - GuiaoLab1 - Utilitários de redes (Linux / Win) - v3.0 – 2010-09-27

CINEM - GuiaoLab1 - Utilitários de redes (Linux / Win) - v4.0 – 2014-09-20