Laptop connectivity

Getting online

There are several networks in our buildings, both wired and wireless. For the wired connections, please make sure you connect to our designated laptop networks; connecting to the desktop network directly will not work, and may cause security issues. When in doubt, contact the computer group.

Logging in to Linux systems

SSH

SSH stands for Secure Shell, and is a standard way to get secure access to a remote machine. See SSH for further details.

VNC

Virtual Network Computing (VNC) is a remote display system which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. It is present on all out Linux desktops and some of the compute nodes and servers. See VNC for details.

X2GO is an extended type of VNC, which has built-in support for ssh tunnels and can also forward more than just the display (audio, printing and file access). X2GO is installed on the Linux desktops.

Connecting to Windows systems

It is possible to connect to windows computers (either your own windows desktop, or the central terminal server `texel`) through the remote desktop protocol (rdp). However, rdp connections should be tunneled through ssh for security, so some additional steps are needed.

- Manual at LION for remote desktop using tunnelier on a Windows client
- Microsoft Remote Desktop on a macOS client
- Microsoft Remote Desktop on a Linux client

Printing

Our printers are only accessible from the wired network, and from the UL-STRW-LION wireless network. See laptopprint for details.

Disk access: SSHFS / fuse-ssh

It is in general not possible to access the disks of our Linux and Windows desktops and workstations directly. The closest one can get to mounting a desktop disk, is using the `sshfs` tools (also known as `fuse-ssh`), available for Linux, Mac OS X and Windows. These tools create a filesystem access over ssh, so it is encrypted, and it uses your own user credentials to guarantee that no one else can access files this way.

See e.g.
https://www.digitalocean.com/community/tutorials/how-to-use-sshfs-to-mount-remote-file-systems-over-ssh

Short example (assuming you have installed sshfs on your laptop already):

```
mkdir $HOME/lorentz
sshfs -o idmap=user username@ssh.lorentz.leidenuniv.nl:/home/username
$HOME/lorentz
```

This mounts your institute home disk on a subdirectory under your local home on the laptop. Once mounted, you can treat it like any other disk, and copy files to and from it. Of course the same can be done with data disks in stead of home. The `idmap=user` option is to make sure that your files show up as yours, when user ids don't match.

To unmount:

```
fusermount -u $HOME/lorentz
```

(normally, umount should work as well but there can be permission issues, fusermount always works)

From:
https://helpdesk.strw.leidenuniv.nl/wiki/ - **Computer Documentation Wiki**

Permanent link:
https://helpdesk.strw.leidenuniv.nl/wiki/doku.php?id=generic:laptop_connectivity

Last update: **2018/07/24 07:59**