



# Remote Connections

## SSH en VNC

**DE HOGESCHOOL  
MET HET NETWERK**

Hogeschool PXL – Dep. PXL-IT – Elfde-Liniestraat 26 – B-3500 Hasselt  
[www.pxl.be](http://www.pxl.be) - [www.pxl.be/facebook](https://www.facebook.com/pxl.be)



# SSH

- SSH
  - Secure SHell
  - OpenSSH wordt gebruikt
    - `dpkg -S `which ssh`` geeft als package “openssh-client”
  - SSH-client
    - Standaard geïnstalleerd
  - SSH-server
    - Dient geïnstalleerd te worden op de PC die we vanop afstand willen managen
    - Bv. Een Ubuntu-server(serverack) managen vanaf je Ubuntu Desktop(laptop)



# SSH-Server

- SSH-server

- Installatie
  - sudo apt install openssh-server
- Configuratie
  - sudo vi /etc/ssh/sshd\_config

- ListenAddress - indien we op een bepaalde NIC willen luisteren
- MaxSessions - Hoeveel gelijktijdige connecties toegelaten worden
- PermitRootLogin - op “no” voor security (na login sudo...)
- DenyUsers - Deze gebruikers mogen niet inloggen over ssh
- DenyGroups - De gebruikers van deze groepen mogen niet inloggen

```
# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin without-password
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile    :h/.ssh/authorized_keys

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



# SSH-server

- SSH gebruikt poort 22 op de Server
  - grep ssh /etc/services
    - toont poort 22 over TCP en UDP
      - Maar ssh gebruikt normaal gezien enkel TCP
  - netstat -ant               => Port 22
  - netstat -at               => Port ssh



# SSH-client

- SSH-client
  - Installatie
    - ssh-client is automatisch geïnstalleerd
    - sudo apt install openssh-client
  - Configuratie
    - /etc/ssh/ssh\_config
      - staat standaard goed

```
student@ubdesk:~$ sudo apt-get install openssh-client
[sudo] password for student:
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-client is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 252 not upgraded.
```



# SSH Server Authentication

- Server Authentication
  - De Public Key van de server wordt gebruikt om zich te authenticeren bij de client
    - /etc/ssh/ssh\_host\_rsa\_key.pub
    - Via de setting StrictHostKeyChecking bij de client (/etc/ssh/ssh\_config)
      - Standaard op Ask
      - Elke eerste verbinding naar een nieuwe host wordt er gevraagd of je dit wil en zo ja wordt de public key opgeslagen op de client in de known-hosts-file (~/.ssh/known\_hosts)
    - Indien de public key van een bestaande server wijzigt, zal de client niet kunnen connecteren naar deze host
    - Op te lossen door de “oude” public key van de server te



# SSH-connecties met username/pwd

- SSH-connectie
  - ssh <gebruikersnaam>@<serverip>
  - De eerste maal wordt gevraagd of je wel wilt connecteren met deze onbekende server
    - Indien je bevestigt wordt de public key van de server opgeslaan op de client in `~/.ssh/known_hosts` (homefolder van de user)
      - kan ook server-wide ingesteld worden door handmatig de public key(s) van de ssh-server(s) op te slaan in `/etc/ssh/ssh_known_hosts`



```
student@ubdesk:~$ ssh student@172.16.217.129
The authenticity of host '172.16.217.129 (172.16.217.129)' can't be established.
ECDSA key fingerprint is 81:50:29:0b:a0:48:f1:ed:52:5d:82:9c:e7:08:b9:bc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.217.129' (ECDSA) to the list of known hosts.
student@172.16.217.129's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

 System information as of Tue Nov 25 14:59:48 CET 2014

 System load:  0.0          Processes:      239
 Usage of /:   8.8% of 18.58GB  Users logged in:    1
 Memory usage: 15%
 Swap usage:   0%

 Graph this data and manage this system at:
  https://landscape.canonical.com/

80 packages can be updated.
50 updates are security updates.

Last login: Tue Nov 25 14:59:49 2014 from 172.16.217.129
student@ubserv:~$ exit
logout
Connection to 172.16.217.129 closed.
student@ubdesk:~$ cat .ssh/known_hosts
|1|M0WF5FMB5j7mAq+G4QoN4GdaScI=|jvDQS2dsvk/eU0B3GtUMagmmiYI= ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFE0ScjJFZ4Gc6X2irl2ITQZ4HP1
```

Eerste keer aanloggen op een nog onbekende ssh-server



Nadien nogmaals aanloggen op een reeds gekende ssh-server

```
student@ubdesk:~$ ssh student@172.16.217.129
student@172.16.217.129's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
```

# SSH-connecties met keys

- SSH met keys
  - ook passwordless ssh genoemd
  - er wordt een private/public-keypair gemaakt
    - private-key blijft op de client/Desktop) en is persoonlijk
    - public-key wordt gekopieerd in de homedir van de persoon en server waarmee en waarnaar we willen connecteren over ssh
    - de public-key kan herbruikt worden om tegelijk de mogelijkheid te hebben met meerdere servers passwordless te connecteren over ssh
      - ook met dezelfde private key dus



# SSH-connecties met keys

- SSH keypair
  - Aanmaken
    - ssh-keygen -t rsa
    - private-key kan extra beveiligd worden met een passphrase
  - Het keypair staat nu in ~/.ssh
    - private-key: id\_rsa
    - public-key: id\_rsa.pub

```
student@ubdesk:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
The key fingerprint is:
5c:3f:c3:2d:b4:a9:7c:f1:b7:4f:c2:37:da:71:d2:43 student@ubdesk
The key's randomart image is:
+--[ RSA 2048]----+
| |
| |
| . .
| . . + +
| S X .E
| . . B..
| o . =+*
| . o**
| . oo|
+-----+
```

```
student@ubdesk:~$ ls -l ~/.ssh/
total 12
-rw----- 1 student student 1766 Nov 25 20:41 id_rsa
-rw-r--r-- 1 student student 396 Nov 25 20:41 id_rsa.pub
-rw-r--r-- 1 student student 222 Nov 25 19:00 known_hosts
```



# SSH-connecties met keys

- SSH keypair
  - Public-key naar de server kopieren
    - onder de gebruiker waarmee je wil inloggen over ssh
    - ssh-copy-id -i ~/.ssh/id\_rsa.pub <gebruiker>@<serverip>
      - om te mogen kopiëren naar de homefolder van deze gebruiker moeten we het wachtwoord opgeven van deze gebruiker
      - -i ~/.ssh/id\_rsa.pub moet je niet meegeven als je de default bestandsnaam (en pad) gebruikt

```
student@ubdesk:~$ ssh-copy-id student@172.16.217.129
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
student@172.16.217.129's password:
```

```
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh 'student@172.16.217.129'" and check to make sure that only the key(s) you wanted were added.
```

De public key komt op de server in authorized\_keys in de homefolder van de te connecteren user

```
student@ubservv:~$ cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQCN1sg0+uCiDGyC4a8TJhJ
zS5ckmUckVoc1q8Ci2BMJ6NUfJZrrR0Z9ZYyF8k2hRot144JKFSuvdUW6cU
RulkEXZHUVkR1eb/00jhj student@ubdesk
```

# SSH-connecties met keys

- SSH keypair
  - Verder beveiligen van de ssh-server
    - aanpassen van /etc/ssh/sshd\_config
      - PasswordAuthentication no
        - geeft aan of er met een paswoord mag worden ingelogd
        - deze regel alleen is na default-setup ook al genoeg
  - Reloaden van de sshd-configuratie
    - sudo systemctl reload ssh



# SSH-connecties met keys

- SSH keypair
  - Passwordless connecting over ssh



De passphrase om de private key te unlocken wordt gevraagd.  
Je kan aanvinken dat de private key in de toekomst automatisch wordt ge-unlocked tijdens het inloggen

```
student@ubdesk:~$ ssh student@172.16.217.129
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
```

Er wordt geen wachtwoord gevraagd



# SSH-connecties met keys

- SSH keypair
  - Passwordless connecting over ssh zonder X
    - Als je hier ook slechts éénmaal je private-key wil unlocken en vervolgens meerdere malen gebruiken voor verscheidene ssh-connecties
      - ssh-agent bash - start een nieuwe shell met de agent running
      - ssh-add ~/.ssh/id\_rsa - houdt de private key(s) in het geheugen
    - We moeten dus niet telkens opnieuw de passphrase opgeven als we een nieuwe ssh-connectie starten

```
student@ubdesk:~$ ssh-agent bash
student@ubdesk:~$ ssh-add ~/.ssh/id_rsa
Enter passphrase for /home/student/.ssh/id_rsa: [REDACTED]
Identity added: /home/student/.ssh/id_rsa (/home/student/.ssh/id_rsa)
student@ubdesk:~$ ssh student@172.16.217.129
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)
```



# SSH-connecties debuggen

- Indien een bepaalde connectie niet werkt
  - kan je gaan troubleshooten door te debuggen
  - je krijgt dan veel meer informatie op de server te zien als je met een client connectie begint te maken
    - Eerst moet je de huidige ssh-server stoppen
      - sudo systemctl stop ssh
    - Hierna kan je de versie met debugging starten
      - sudo /usr/sbin/sshd -ddd
    - Connecteer nu vanaf de client en kijk naar de meldingen in het terminal-venster van de server



# SSH - extra security

- SSH-server: extra security
  - AllowUsers (of DenyUsers)
    - aan te duiden in /etc/ssh/sshd\_config op server
    - om verbindingen van bepaalde gebruikers toe te laten of te verbieden
    - Al wie niet in de AllowUsers is opgenomen, is dan wel automatisch geweigerd !!!
      - AllowUsers gert guy@web.pxl.be tom@172.16.231.55  
bart@\*.kinopolis.be
  - Men kan ook werken met AllowGroups of DenyGroups



# SSH - extra security

- SSH-server: extra security
  - hosts.allow en hosts.deny
    - om verbindingen vanaf andere PCs toe te laten of niet
    - PCs en/of subnets toelaten
      - /etc/hosts.allow
        - sshd: 172.16.231.0/255.255.255.0
    - Alle andere PCs en subnets verbieden
      - /etc/hosts.deny
        - sshd: ALL



# SSH - motd en nologin

- SSH-server: Overige bestanden uit /etc
  - motd
    - inhoud wordt afgedrukt als in sshd\_config PrintMotd op yes staat
  - nologin
    - indien deze file bestaat, kan niemand inloggen, behalve root, en wordt de tekst in dit bestand getoond
      - touch nologin is al voldoende



# SSH - commando's sturen

- Commando's sturen over ssh
  - in plaats van een interactieve sessie te starten met ssh, kan je ook onmiddellijk een commando meegeven aan je connectie
    - `ssh <gebruiker>@<ssh-serverver> '<commando>'`
    - vb: `ssh student@172.16.231.55 'whoami; pwd; ls -la'`
    - na het uitvoeren van het commando stopt de connectie
  - Gebruik optie t voor een interactieve sessie te starten
    - `ssh -t student@172.16.231.55 'vi test.sh'`
    - connectie stopt pas nadat vi is afgesloten



# SSH - files kopiëren met scp

- Files kopiëren over ssh met scp
  - scp
    - secure copy (over ssh) tussen twee PCs, waarvan één de lokale PC moet zijn
    - scp <lokaal bestand> <user>@<serverip>:<doelmap>
      - doelmap start in de homefolder van de gebruiker waarmee geconnecteerd wordt, of er moet een absoluut pad gebruikt worden (beginnend met /)
      - scp ~/oef10\_1.sh student@172.16.231.55:Desktop/



# SSH - files kopiëren met scp

- Files kopiëren over ssh met scp
  - scp
    - je kan ook een bestand kopiëren van de server naar client
      - scp student@172.16.231.55:Desktop/oef11\_2.sh oefeningen/
    - je kan een bestand tijdens het kopiëren ook hernoemen
      - scp oef11\_3.sh student@172.16.231.55:Desktop/oef11\_3oud



# SSH - files kopiëren met scp

- Een map kopiëren over ssh met scp
  - scp -r
    - kopieert recursief de inhoud van de map en submappen
    - scp -r <lokale map> <user>@<serverip>:<doelmap>
      - doelmap start in de homefolder van de gebruiker waarmee geconnecteerd wordt, of er moet een absoluut pad gebruikt worden (beginnend met /)
      - scp -r /media/cdrom/ student@172.16.231.55:CDR/



# SSH - secure ftp

- Files kopiëren over ssh met sftp
  - sftp
    - ssh/secure file transfer protocol
    - werkt indien ssh werkt
    - sftp <gebruiker>@<serverip>
      - help
      - ls/lls
      - cd/lcd
      - pwd/lpwd
      - get/put
      - bye/quit
  - kan ook naar geconnecteerd worden vanuit Filezilla



# SSH - sshfs

- Een filesysteem mounten over ssh
  - sshfs installeren op de client
    - sudo apt-get install sshfs
  - uzelf aan de groep fuser toevoegen
    - sudo usermod -a -G fuser student + herinloggen
  - directory aanmaken onder je homedir
    - mkdir sshmount
  - directory over ssh lokaal mounten
    - sshfs student@172.16.231.55: sshmount/

VIA /etc/fstab => sshfs#student@172.16.132.55: /home/student/sshmount fuse defaults,idmap=user 0 0



# SSH - sshfs

- Een filesysteem mounten over ssh
  - zorgen dat de connectie behouden blijft
    - sudo vi /etc/ssh/ssh\_config
    - ServerAliveInterval 120
    - sudo systemctl reload ssh
  - umounten van een sshfs-mount
    - sudo fusermount -u <mountpoint>



# SSH-X11 forwarding

- X11
  - Client-Server architectuur
  - Normale toestand op een Ubuntu-desktop
    - Een grafische applicatie is de X-client
      - Vraagt aan de server om een beeld te renderen
    - De X-server maakt het beeld en brengt het naar het beeldscherm

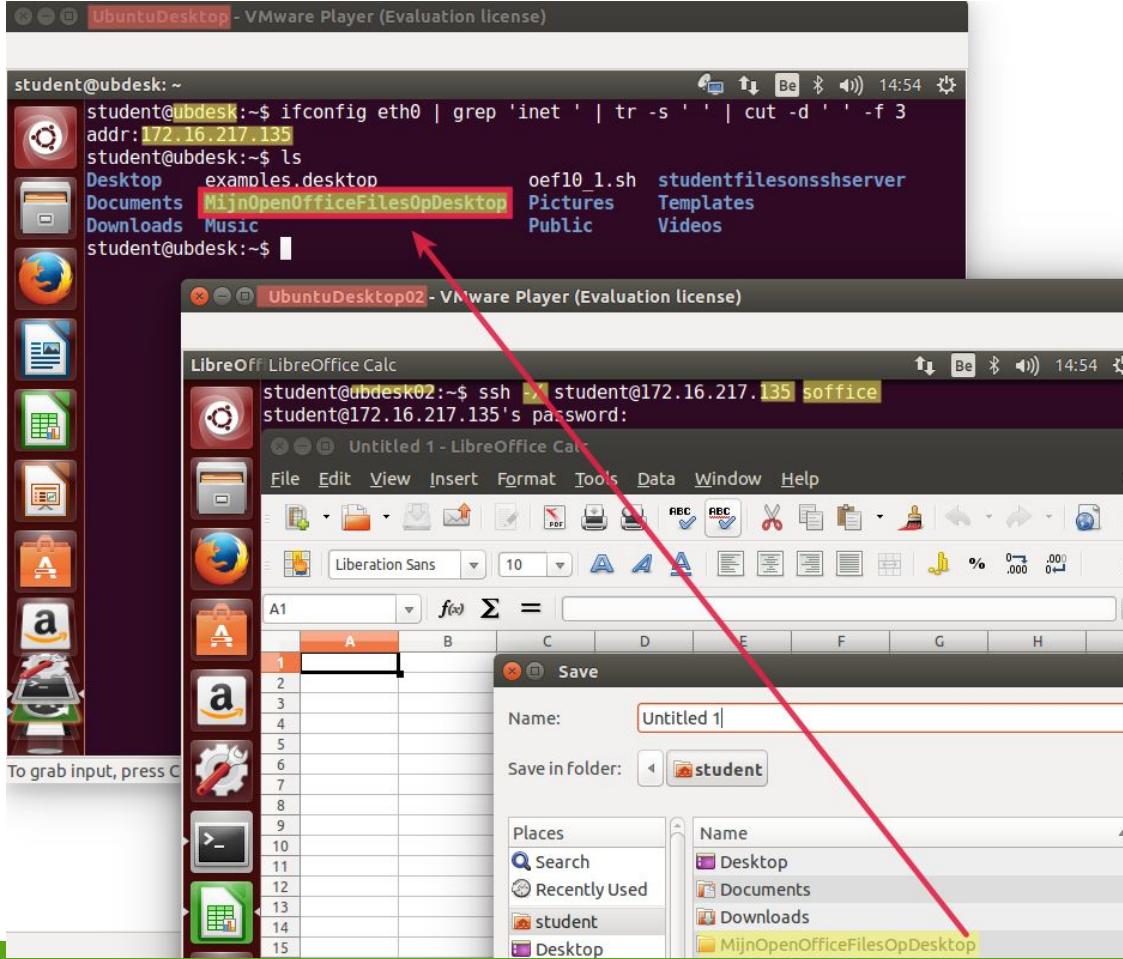


# SSH-X11 forwarding

- X11-Forwarding
  - Er wordt via SSH aangelogd op een ssh-server
  - Op deze ssh-server wordt een grafische applicatie gestart
    - Deze applicatie vraagt aan de X-server om het beeld te renderen
      - De vraag van de client wordt nu gesteld aan de X-server die draait op de SSH-client
      - Dus de connectie tussen de X-client en X-server wordt gelegd over de ssh-verbinding van X-server naar X-client



# SSH-X11 forwarding



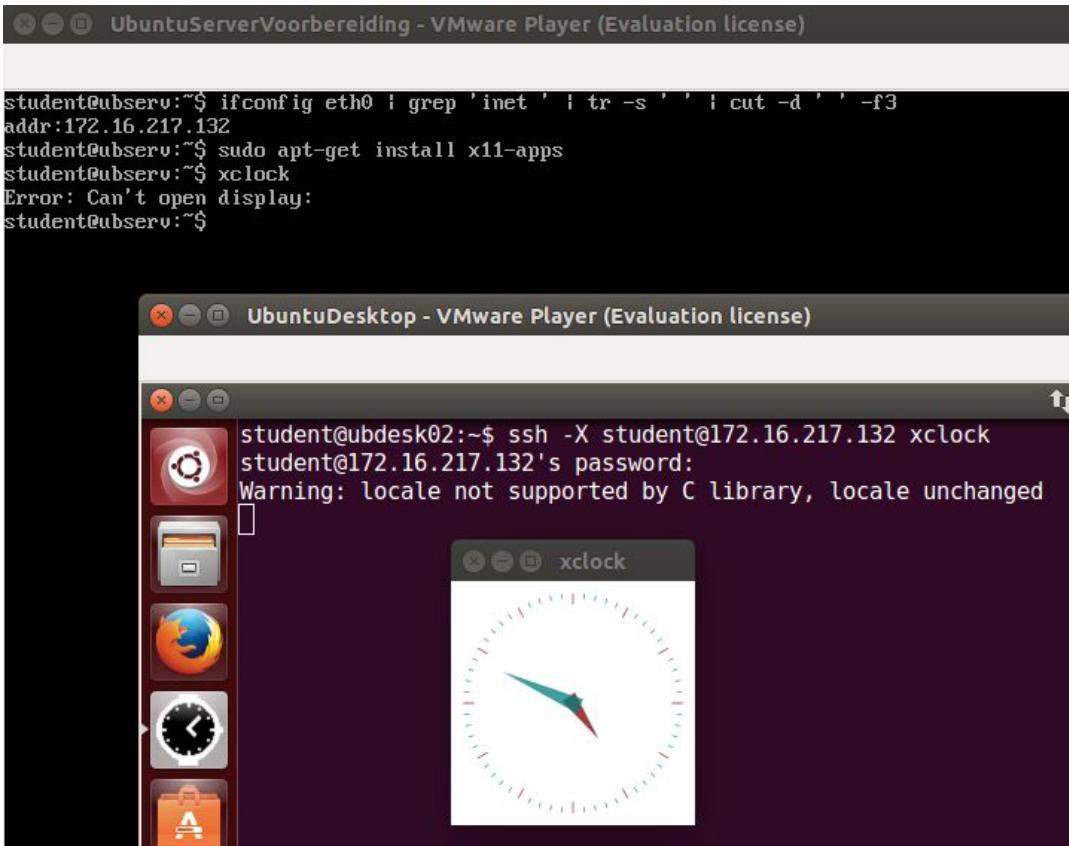
We starten vanaf ubdesk over ssh de libreoffice-calc op op ubdesk02

De applicatie draait op ubdesk (op de ssh-server)

Maar de applicatie wordt gerenderd op ubdesk02

We zien dus wel dat als we een bestand gaan opslaan, dit zal opgeslaan worden op ubdesk, waar de toepassing ook is opgestart en draait.

# SSH-X11 forwarding



Op de Server installeren we een GUI-applicatie (bvb om een FW te managen). Maar deze kan natuurlijk niet gestart worden op deze server, omdat er geen X-server aanwezig is.

Vanaf de Desktop kunnen via SSH toch de applicatie draaien op de Server.

# SSH - connecties vanuit windows

- SSH connecties maken vanuit windows
  - Putty
    - www.putty.org => klik op download
    - download putty.zip en pak uit op het bureaublad
    - putty.exe
      - ip-adres instellen en connectie maken
    - Je kan ook met een keypair werken
      - met puttygen
        - om een keypair te maken in windows
      - met pageant
        - zodanig dat je de passphrase niet telkens opnieuw moet opgeven



# VNC

- VNC
  - Virtual Network Computing
  - Remote Control via Desktop Sharing
  - Ingebakken in Ubuntu Desktop
    - Server via “Desktop Sharing” (=vino)
    - Client via “Remmina Remote Desktop Client”



# VNC - Vino Remote Desktop Server



# VNC - Remmina Remote Desktop Client

The image shows a desktop environment with several windows open:

- Remmina Remote Desktop Client**: A window titled "Remote Desktop Preference" showing a profile named "VNCconnectie naar ubdesk". The "Protocol" dropdown is set to "VNC - Virtual Network Computing". Below it are fields for "Server" (172.16.217.135), "User name", "Password", "Color depth" (High color (16 bit)), and "Quality" (Best (slowest)). There are also checkboxes for "Show remote cursor" (checked), "View only", "Disable clipboard sync", "Disable encryption", and "Disable server input". Buttons at the bottom include "Default", "Save", "Cancel", and "Connect".
- Connecting to 'VNCconnectie naar ubdesk'...**: A window showing the connection status: "Connecting to 'VNCconnectie naar ubdesk'...". It has a "VNC password" field with three dots, a checkbox for "Save VNC password", and "Cancel" and "OK" buttons.
- Question**: A purple-themed window asking if another user (IP 172.16.217.135) can view or control the desktop. It includes "Refuse" and "Allow" buttons.
- VNCconnectie naar ubdesk**: A terminal window titled "VNCconnectie naar ubdesk" showing a shell session for user "student". The command "ifconfig" is run, displaying network interface details for eth0 and lo. The output is as follows:

```
student@ubdesk:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:02:ba:f5
          inet addr:172.16.217.135 Bcast:172.16.217.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe02:baf5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:10483 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9169 errors:0 dropped:0 overruns:0 carrier:0
          RX bytes:6250246 (6.2 MB) TX bytes:10089757 (10.0 MB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:5456 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5456 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42364987 (42.3 MB) TX bytes:42364987 (42.3 MB)
```