

VPN connections from Linux systems (accessing the departmental internal network remotely)

There are several ways for members of the Department of Computer Science to access departmental IT resources whilst working from home: SSH (secure terminal access to Linux gateway systems), VPN (Virtual Private Network – a secure tunnel to the departmental internal network), and Remote Desktop (secure access to departmental workstations)

This guide details how to set up a VPN connection from a home system running Linux.

Note that a similar provision is available at a University level – which is configured in a very different way (although the idea is essentially the same). Details of this can be found in CSD's *Knowledge Base* – go to <https://www.liverpool.ac.uk/csd/getting-help/>, select *browse the knowledge base* and search for “VPN”.

Installation

Setting up a VPN connection on Linux relies on a couple of additional software packages.

On a Debian, Ubuntu or similar system, run the commands:

```
sudo apt-get install network-manager-vpnc
sudo apt-get install network-manager-vpnc-gnome
```

On a RedHat, Fedora or similar system, run the commands:

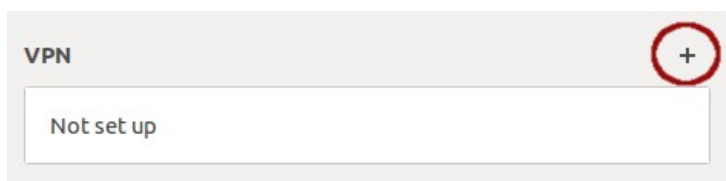
```
sudo yum install NetworkManager-vpnc
sudo yum install NetworkManager-vpnc-gnome
```

(These are also required for setting up the University-level VPN connection)

Configuration

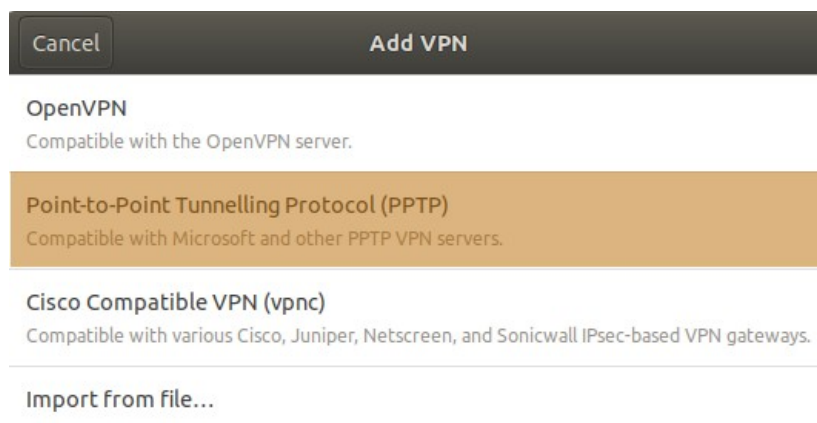
Open **Settings** and select the entry **Network**

Click the **+** in the section **VPN** to configure a new VPN connection.

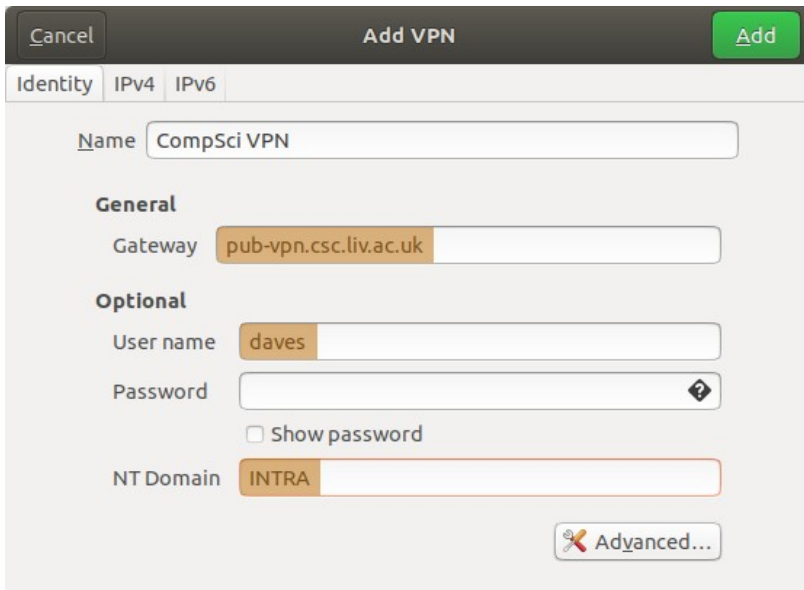


(It is perfectly possible to set up multiple VPN connections, and choose which one(s) to activate)

Select the entry *Point to Point Tunnelling Protocol (PPTP)*

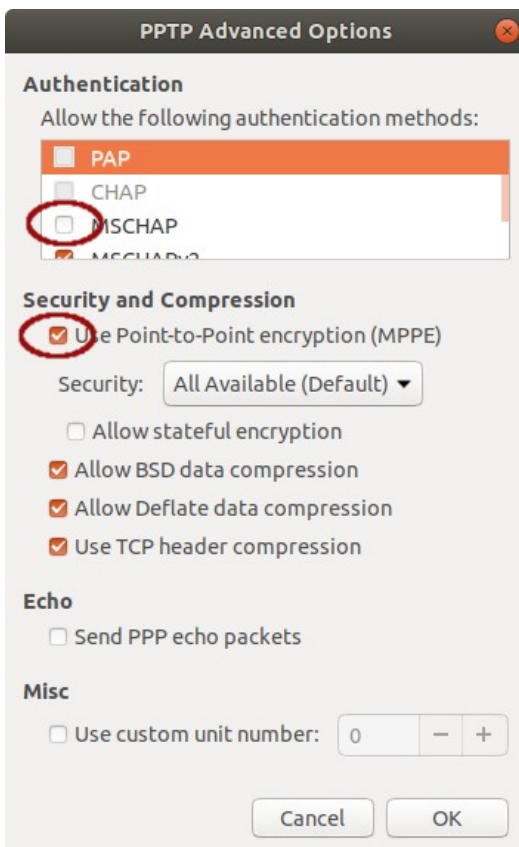


Provide a name to identify the connection (we suggest Comp Sci VPN), set the gateway to be **pub-vpn.csc.liv.ac.uk**, and enter your departmental username. This can either be given in the form `intra\{username}` (all in the User name field), or as a simple username here and the NT Domain field set to **INTRA**



You can either specify the password here (to be saved and applied automatically whenever this connection is activated), or this field can be left blank. In this case, you will be prompted for the password when you enable the VPN connection.

Then click the button Advanced



Select the checkbox next to Use Point-to-Point Encryption (MPPE) and clear the checkbox next to MSCHAP

(Note that the other authentication methods will become unavailable as soon as MPPE is selected)

The other settings can be left as they stand.

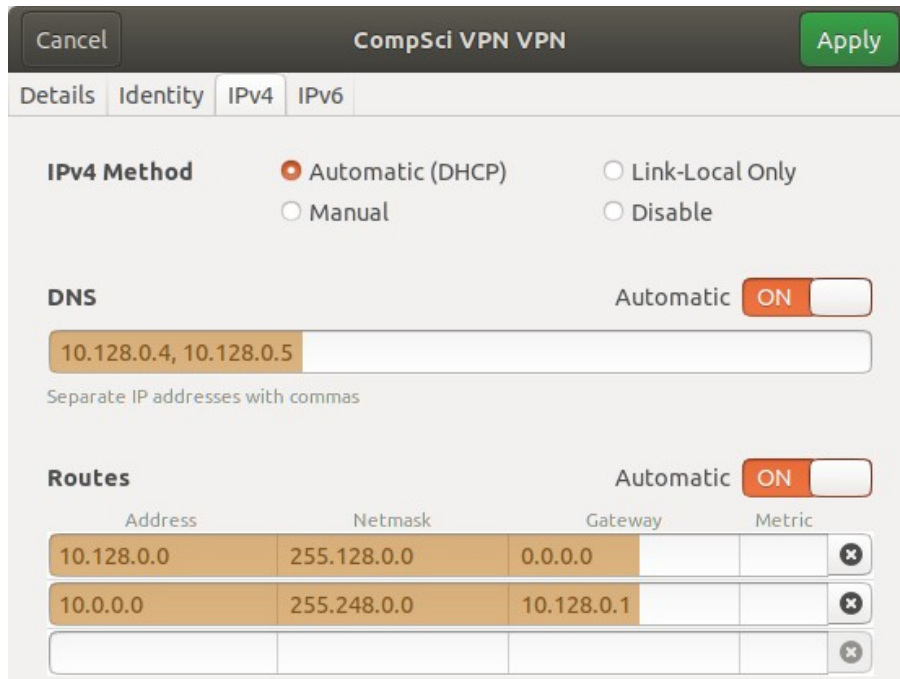
Then click OK

Select the tab IPv4, and enter the values as follows:

DNS **10.128.0.4, 10.128.0.5** *(separated by a comma)*

Routes Address **10.128.0.0** Netmask **255.128.0.0** Gateway **0.0.0.0**
 Address **10.0.0.0** Netmask **255.248.0.0** Gateway **10.128.0.1**

and ensure the checkbox next to *Use this connection only for resources on its network* is selected



Then click the button **Add** (or **Apply**)

Note that if you wish to make changes to the configuration of this VPN session, you will also need to revisit the IPv4 tab, and re-enter the null Gateway (**0.0.0.0**) for the **10.128.0.0** routing entry before being able to click **Apply**

Activating the VPN

Once the VPN has been configured, clicking the network icon in the top bar will show an entry for VPN connections (initially displaying **VPN off**). Clicking this will list the available VPN connections, which can be enabled or disabled as required.

