LabraNet Remote Access Guide

02.10.2018

Institute of Information Technology

CONTENTS

1 Introduction

This is a guide for using LabraNet services remotely through a VPN connection. First part of the guide explains how to connect to LabraNet VPN with step-by-step instructions for the most common operating systems. Second part includes guides for accessing your home folder.

2 VPN Connection

You need a LabraNet user account for the connection.

Generic options for the connection are:

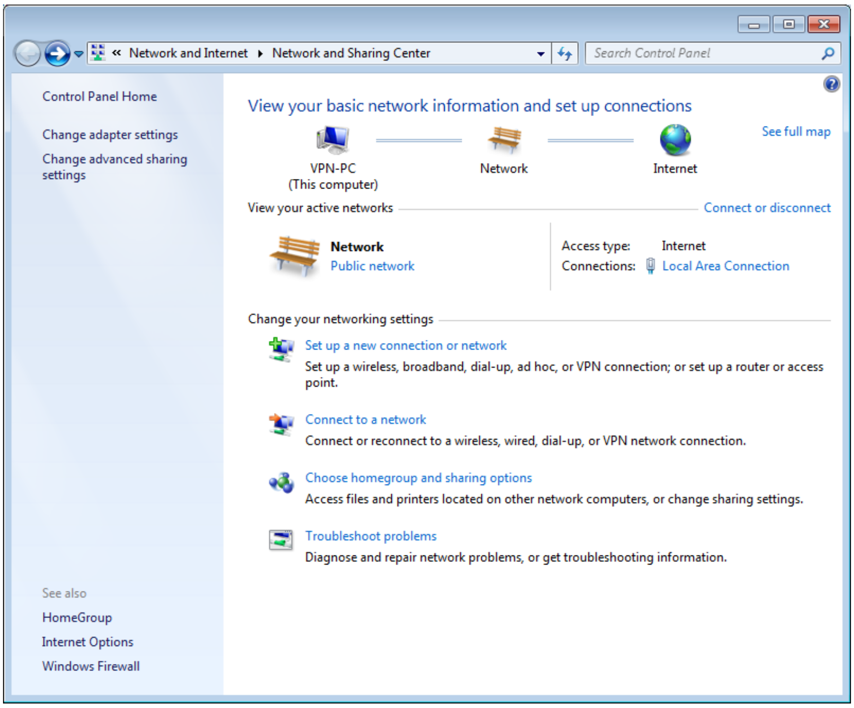
Connection type: SSTP
Authentication type: MS-CHAPv2 (Linux/MacOS) EAP-MSCHAPv2 (Win)
VPN server address: sslvpn.labranet.jamk.fi (should resolve to 195.148.26.226)

Firewall:
If for some reason your firewall blocks web traffic, you need to allow outbound TLS/SSL connections (TCP port 443)

User information:
Domain: LABRANET
User name: Your LabraNet username
Password: Your LabraNet password

3 Windows 7

Open *Control Panel -> Network and Sharing Center*. Select *Set up a new connection or network*.



View your basic network information and set up connections

View your active networks

Network
Public network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

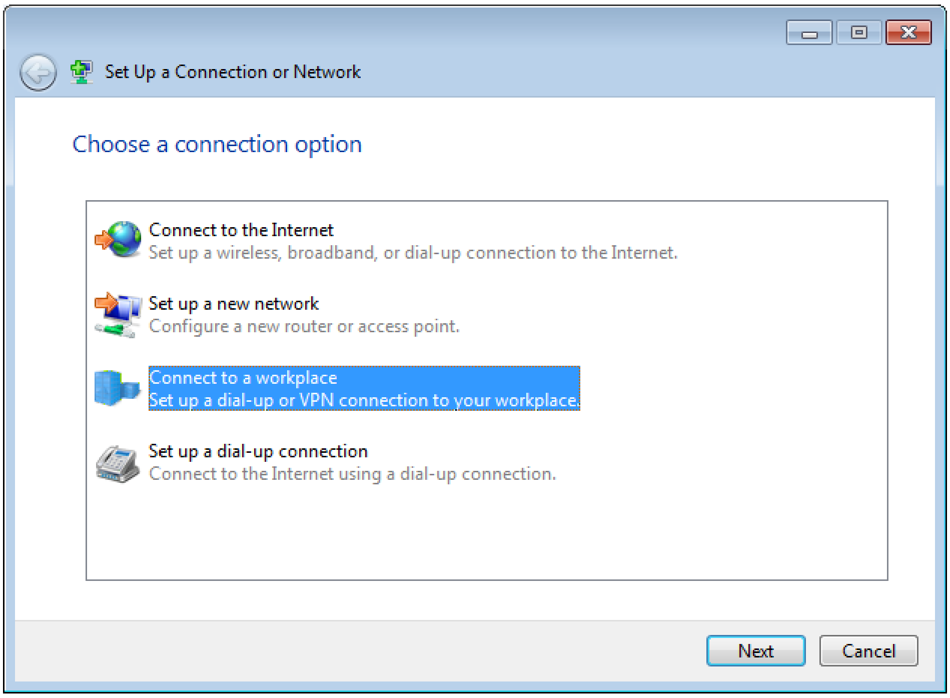
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Figure 1. Control Panel – Network and Sharing Center

Select *Connect to a workplace* and click *Next*.



Set Up a Connection or Network

Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

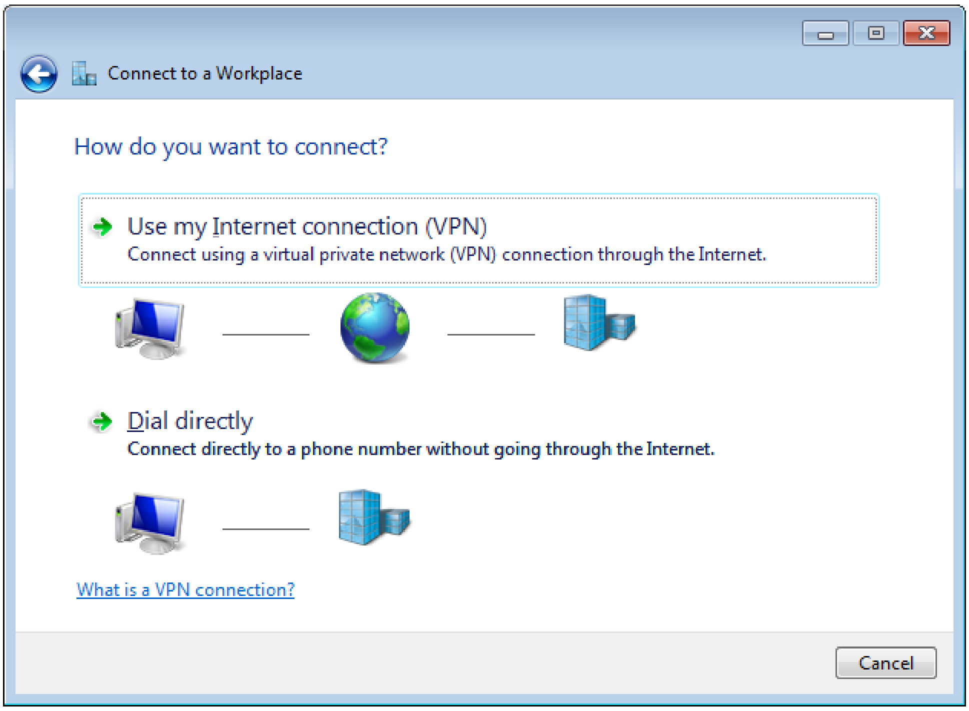
Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

Figure 2. Set Up a Connection or Network

Select *Use my Internet connection (VPN)*:



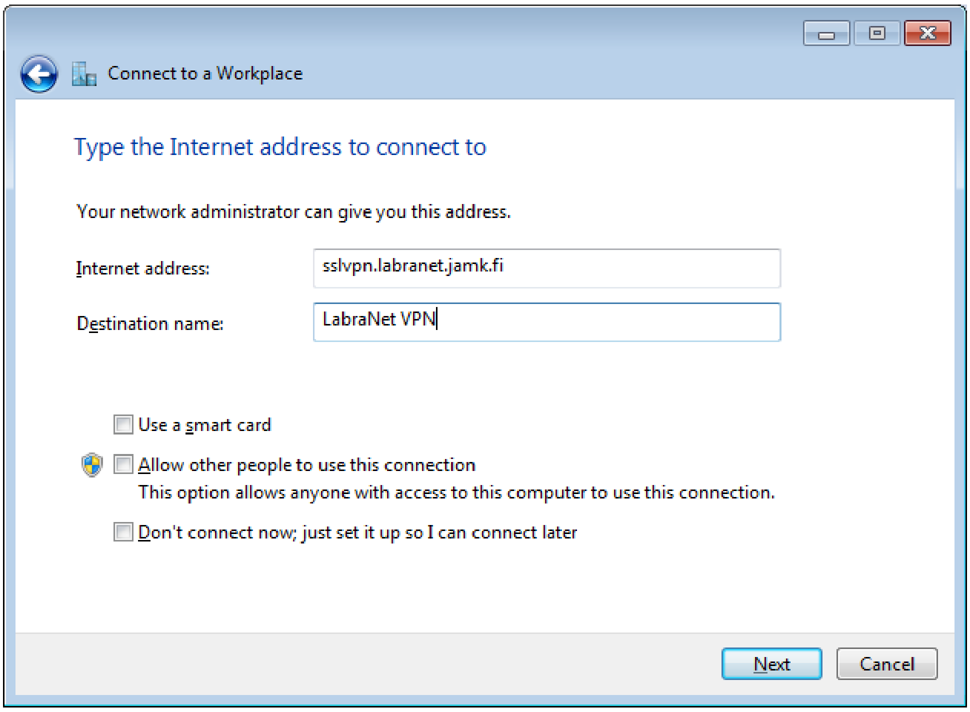
How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.

Figure 3. Connect to a Workplace

Fill in the VPN server address, give the connection a name and click *Next*.



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: sslvpn.labranet.jamk.fi

Destination name: LabraNet VPN

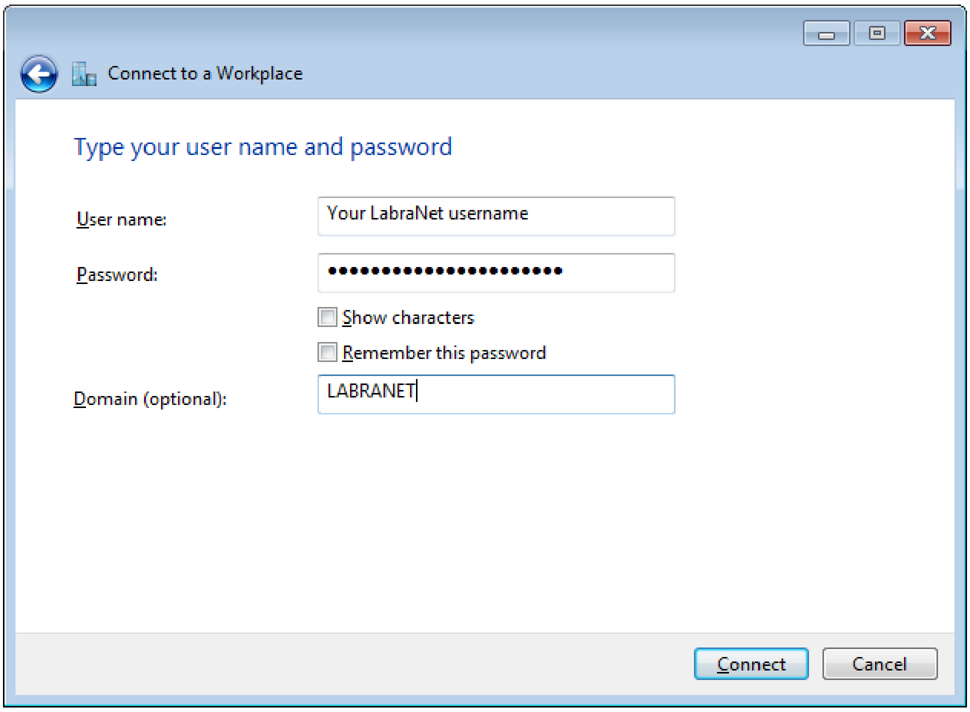
□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

□ Don't connect now; just set it up so I can connect later

Figure 4. Server address and connection name

Provide your credentials and fill in the domain info and click *Connect*.



Connect to a Workplace

Type your user name and password

User name: Your LabraNet username

Password: ••••••••••••••••••••••

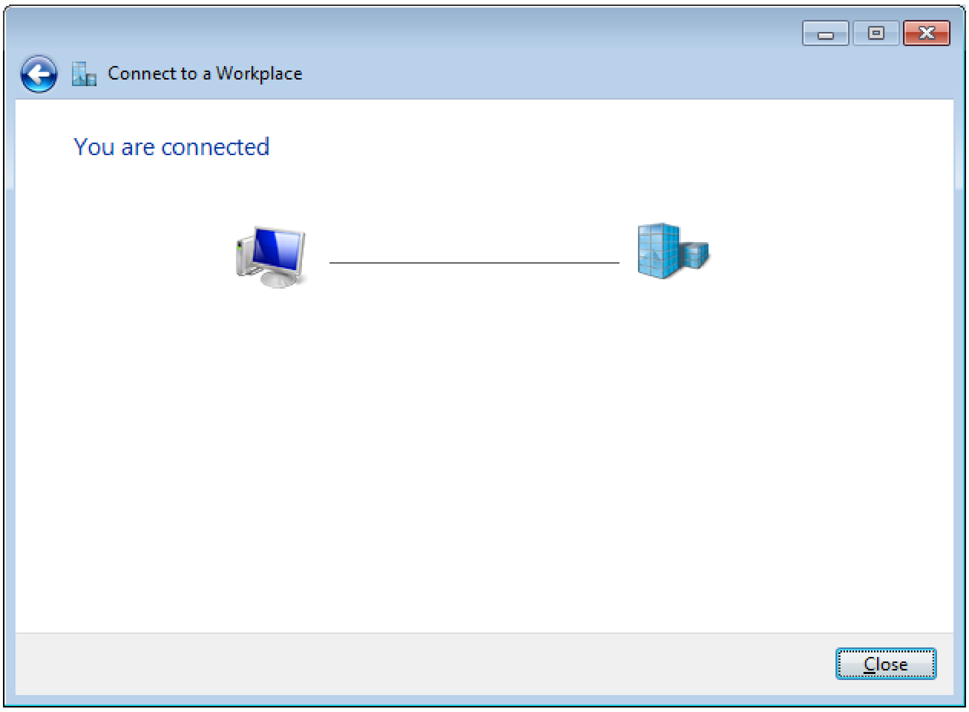
□ Show characters

□ Remember this password

Domain (optional): LABRANET

Figure 5. Credentials and domain

Windows should auto detect the settings for the connection and you should be connected.

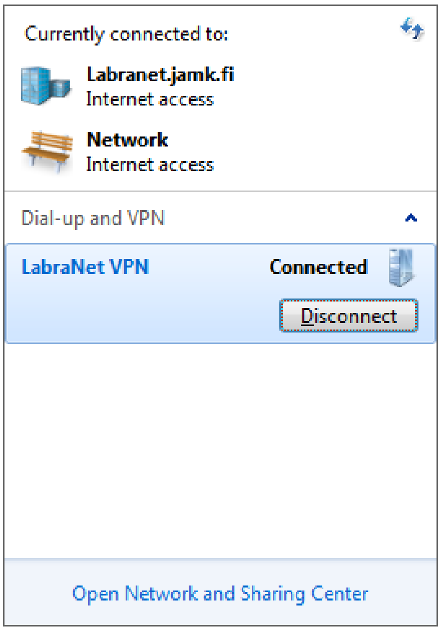


Connect to a Workplace

You are connected

Figure 6. Connection succeeds

You should now be able to connect and disconnect from the *Network* tray icon located at the right side of Windows toolbar:



Currently connected to:

Labranet.jamk.fi
Internet access

Network
Internet access

Dial-up and VPN

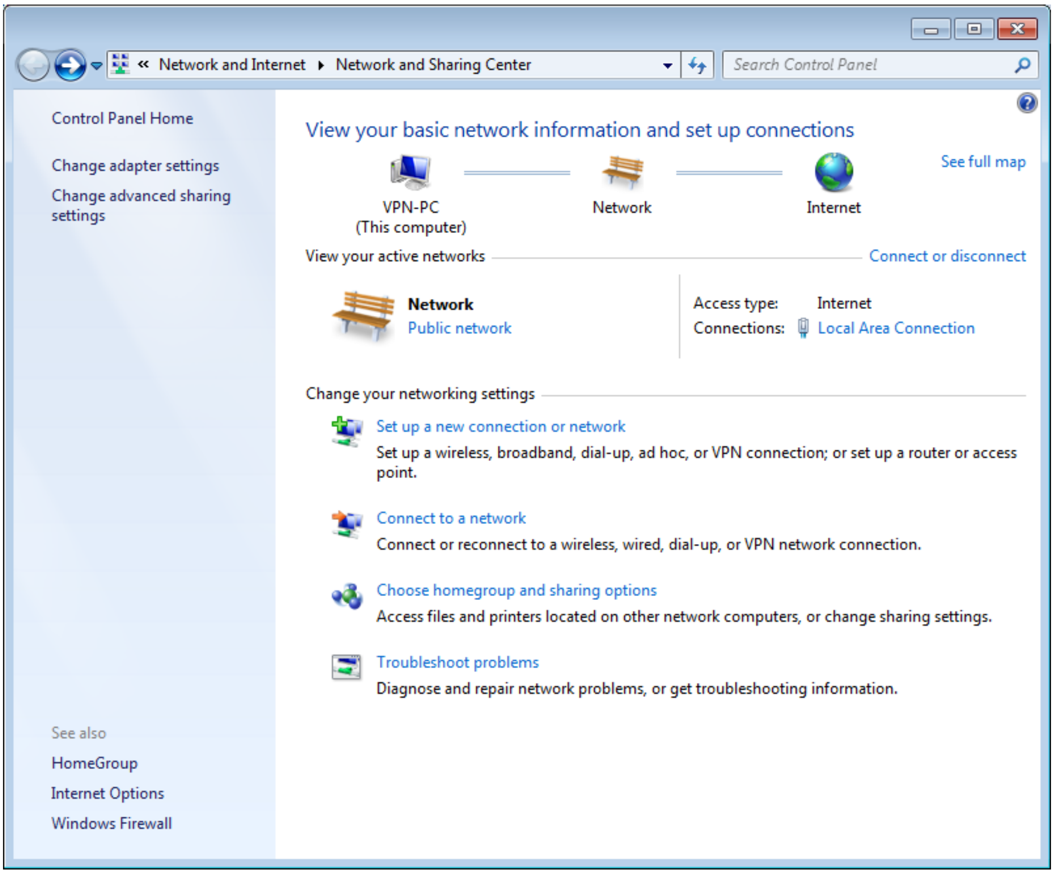
LabraNet VPN **Connected**

Disconnect

Open Network and Sharing Center

Figure 7. Network connections tray applet

Should you want to manually enforce the strongest authentication protocol, you can do so by editing the connection. Select *Change adapter settings* from the left hand panel in *Network and Sharing Center*.



View your basic network information and set up connections

View your active networks

Network
Public network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

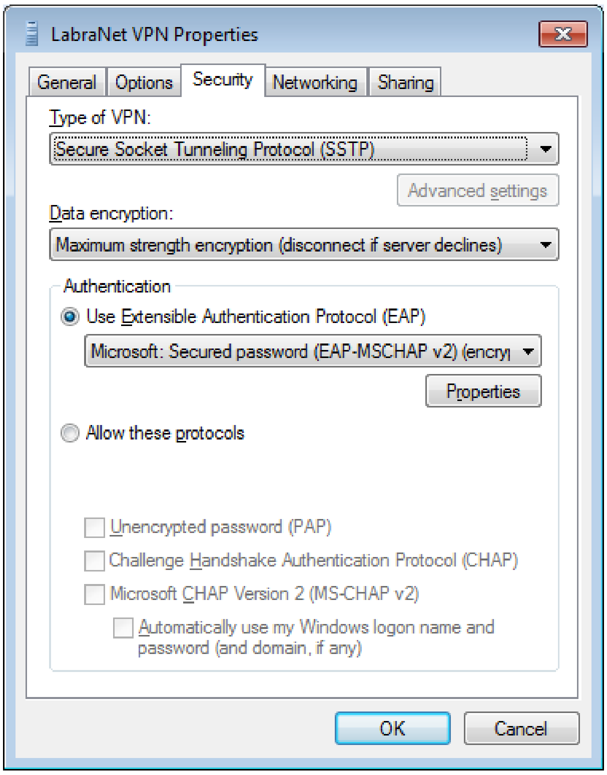
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Figure 8. Network and Sharing Center

Open the connection properties of your VPN connection and select the *Security* tab and choose the following settings.



Type of VPN:
Secure Socket Tunneling Protocol (SSTP)

Data encryption:
Maximum strength encryption (disconnect if server declines)

Authentication
● Use Extensible Authentication Protocol (EAP)
Microsoft: Secured password (EAP-MSCHAP v2) (encry

○ Allow these protocols

□ Unencrypted password (PAP)
□ Challenge Handshake Authentication Protocol (CHAP)
□ Microsoft CHAP Version 2 (MS-CHAP v2)
□ Automatically use my Windows logon name and password (and domain, if any)

Figure 9. VPN Connection security settings

Click *OK*.

4 Windows 8.1

These instructions are for Windows 8.1. If you are still using Windows 8, consider upgrading to 8.1.

NOTE: Currently you can create the VPN connection the same way as in Windows 7 if you prefer the old user interface. As this may change in future Windows 8.1 updates, the following instructions use the newer UI when possible.

On home screen, type *vpn* and select *Manage virtual private networks (VPN)*.

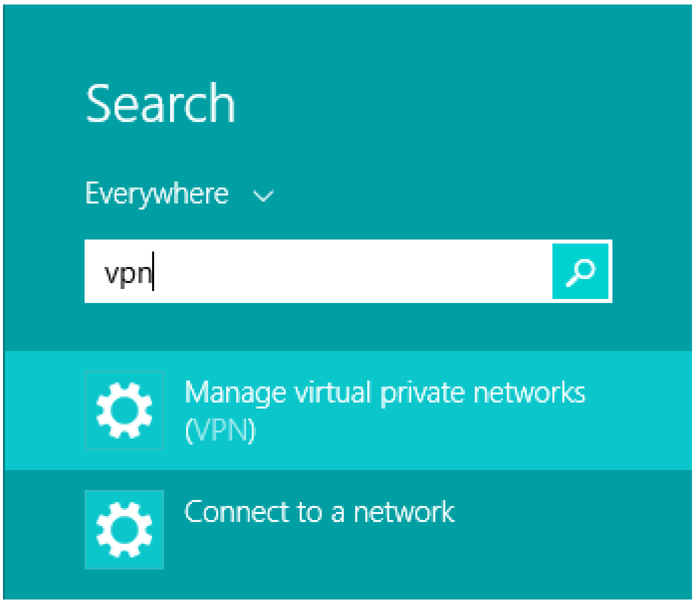


Figure 10. Search for VPN in home screen

This will open Network Connections dialog. Click *Add a VPN connection.*

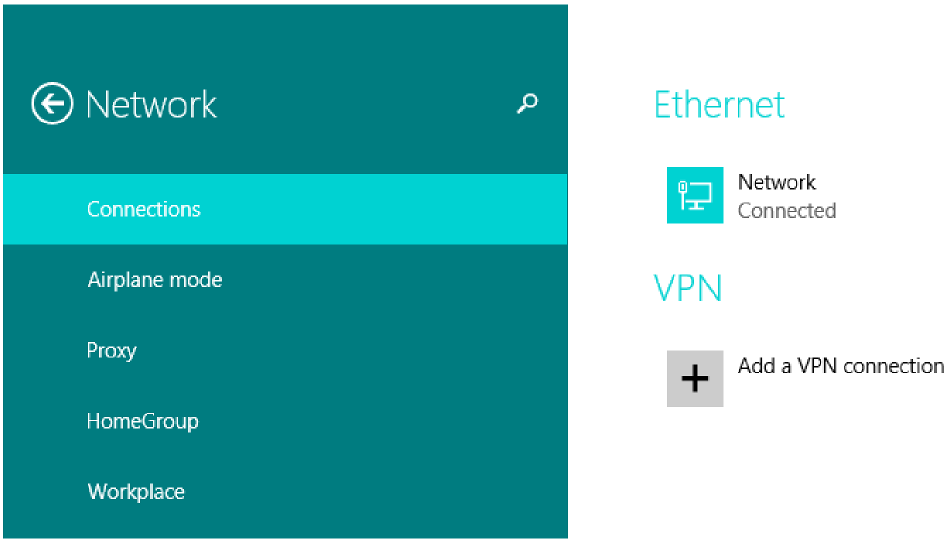
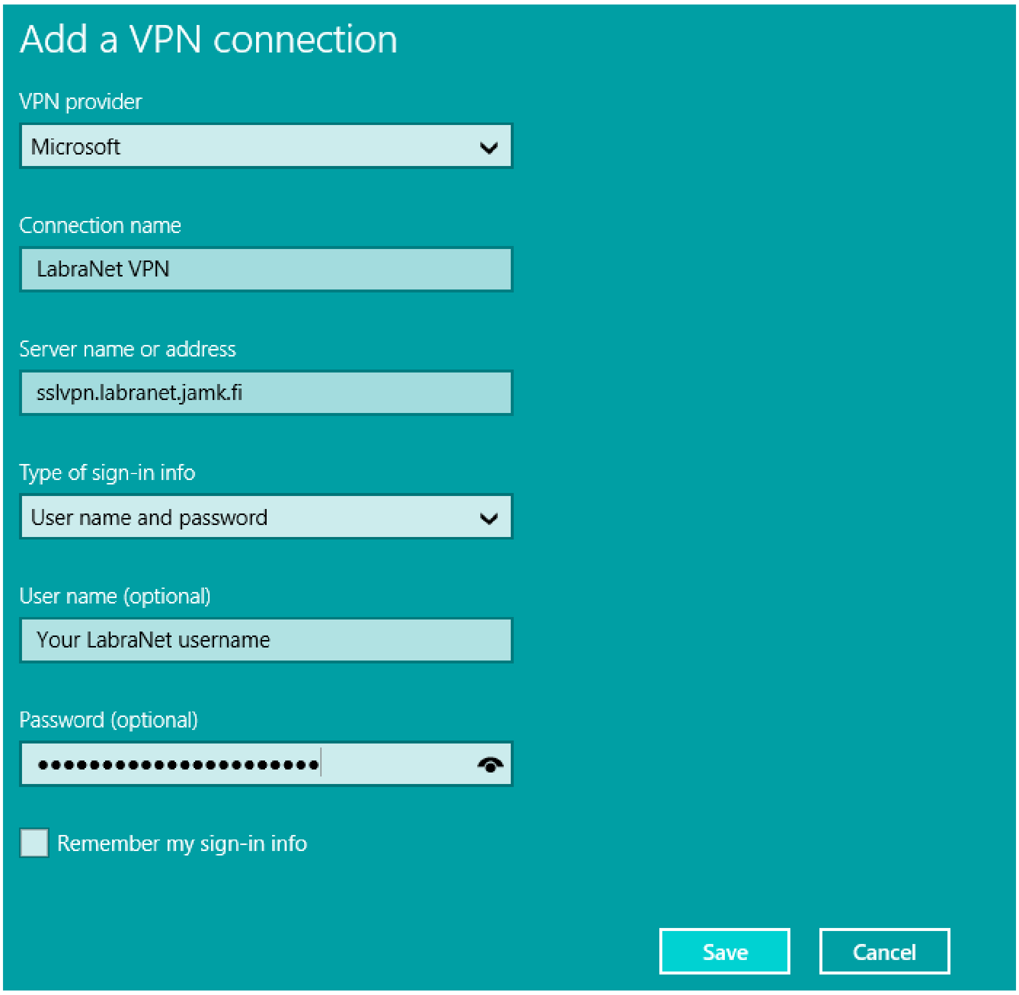


Figure 11. Network connections

Fill in the following information:

Optional: You can provide your username and password here if you wish to save them to the connection settings. Otherwise they will be asked when connecting.



Add a VPN connection

VPN provider: Microsoft

Connection name: LabraNet VPN

Server name or address: sslvpn.labranet.jamk.fi

Type of sign-in info: User name and password

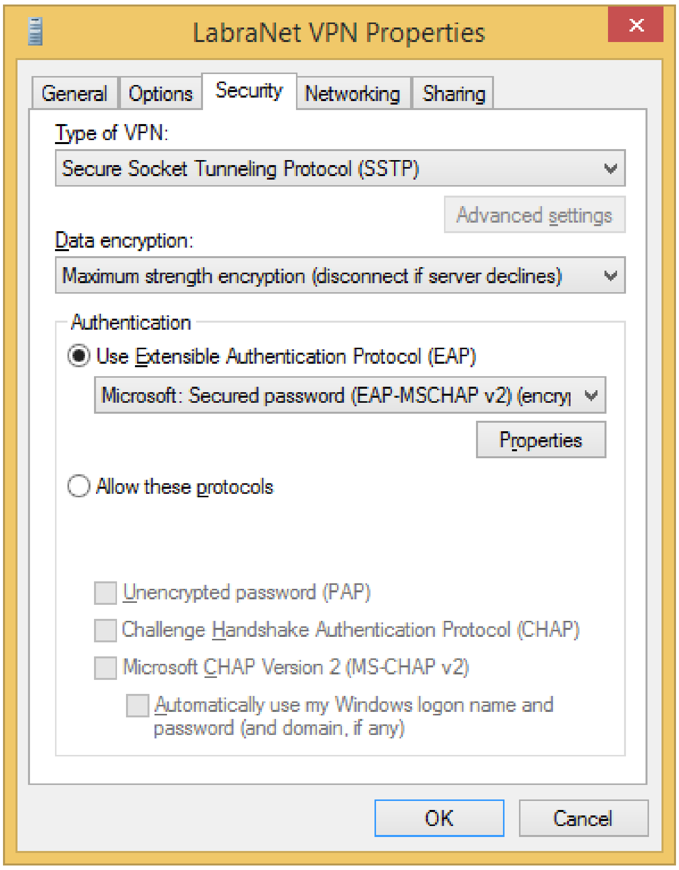
User name (optional): Your LabraNet username

Password (optional): ••••••••••••••••••••••

□ Remember my sign-in info

Figure 12. VPN Connection settings

Click Save. Do not connect yet. Go to *Control Panel -> Network and Sharing Center -> Change Adapter Settings*. Right-click the VPN Connection and select *Properties*. Select the *Security* tab and set the following options.



Type of VPN: Secure Socket Tunneling Protocol (SSTP)

Data encryption: Maximum strength encryption (disconnect if server declines)

Authentication

● Use Extensible Authentication Protocol (EAP)

Microsoft: Secured password (EAP-MSCHAP v2) (encry|

○ Allow these protocols

□ Unencrypted password (PAP)

□ Challenge Handshake Authentication Protocol (CHAP)

□ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

Figure 13. VPN Connection properties

Click *OK*.

Now you can connect to the VPN. Select it from Networks and press Connect. If you did not save the credentials, you will be asked to supply them. Otherwise the connection will be established automatically.

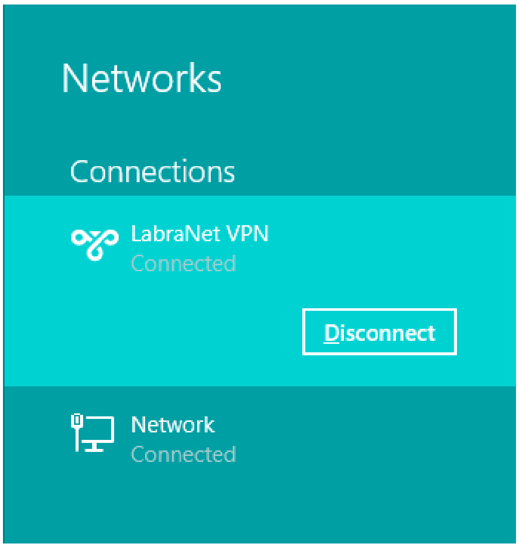


Figure 14. VPN Connection is connected

5 Windows 10

The easiest way to create the VPN connection is to use the *Change virtual private networks* – application. Open the start menu and type *vpn* in the search window.

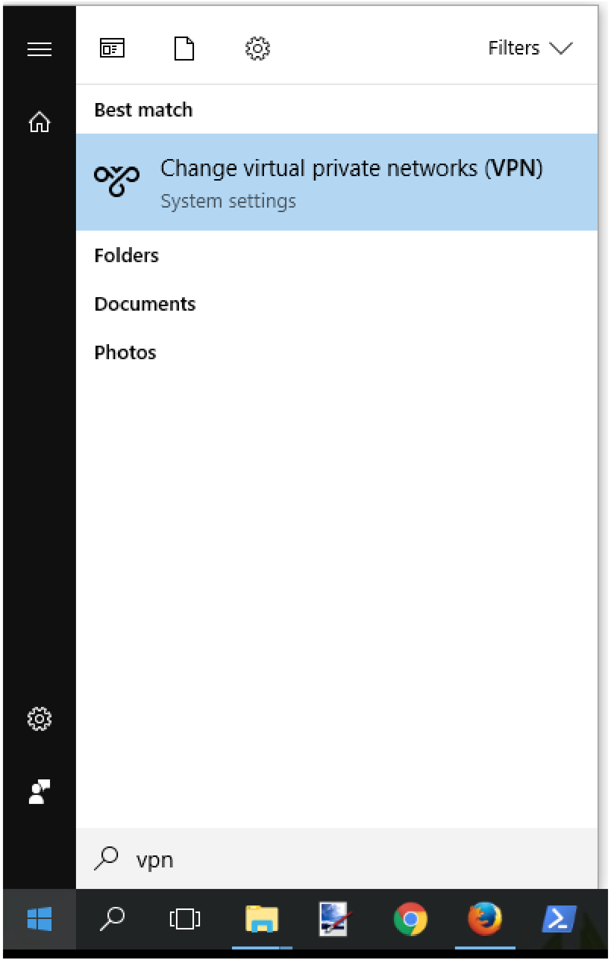
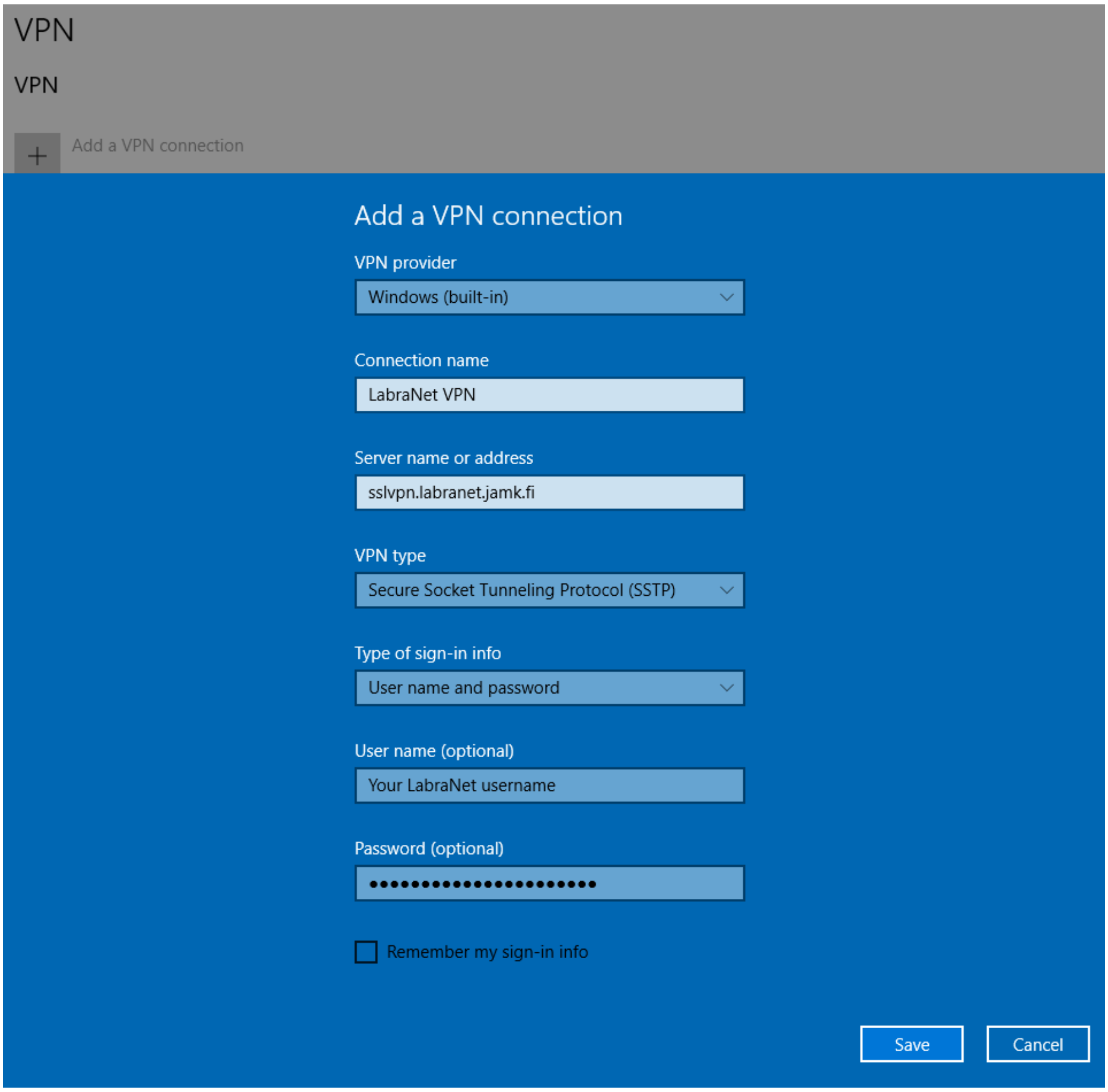


Figure 15. Change virtual private networks

Click *Add a VPN connection* in the application and fill in the connection information.



Add a VPN connection

VPN provider
Windows (built-in)

Connection name
LabraNet VPN

Server name or address
sslvpn.labranet.jamk.fi

VPN type
Secure Socket Tunneling Protocol (SSTP)

Type of sign-in info
User name and password

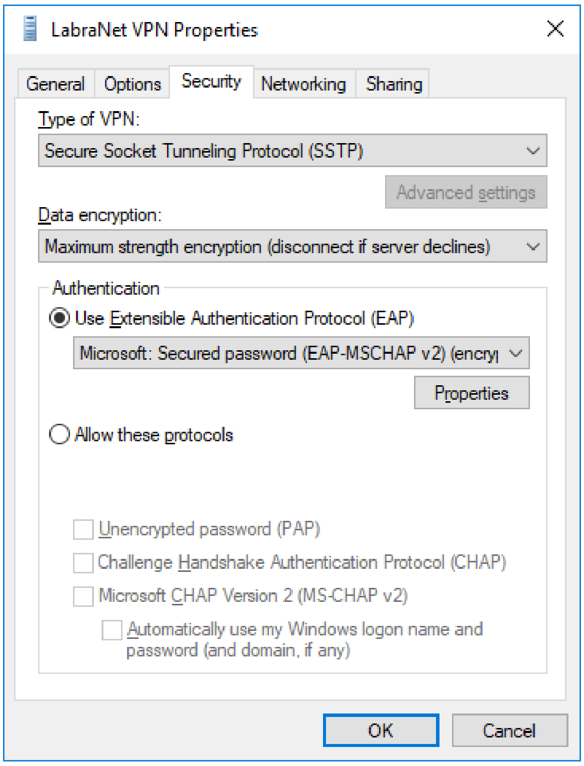
User name (optional)
Your LabraNet username

Password (optional)
•••••••••••••••••••••

□ Remember my sign-in info

Figure 16. Add a VPN connection

Edit the connection settings by opening *Network and Sharing Center* and choosing *Change adapter settings*. Right-click the VPN Connection and select *Properties*. Navigate to the *Security* tab and apply the following settings.



Type of VPN:
Secure Socket Tunneling Protocol (SSTP)

Data encryption:
Maximum strength encryption (disconnect if server declines)

Authentication
● Use Extensible Authentication Protocol (EAP)
Microsoft: Secured password (EAP-MSCHAP v2) (encry|
○ Allow these protocols
□ Unencrypted password (PAP)
□ Challenge Handshake Authentication Protocol (CHAP)
□ Microsoft CHAP Version 2 (MS-CHAP v2)
□ Automatically use my Windows logon name and password (and domain, if any)

Figure 17. VPN connection security settings

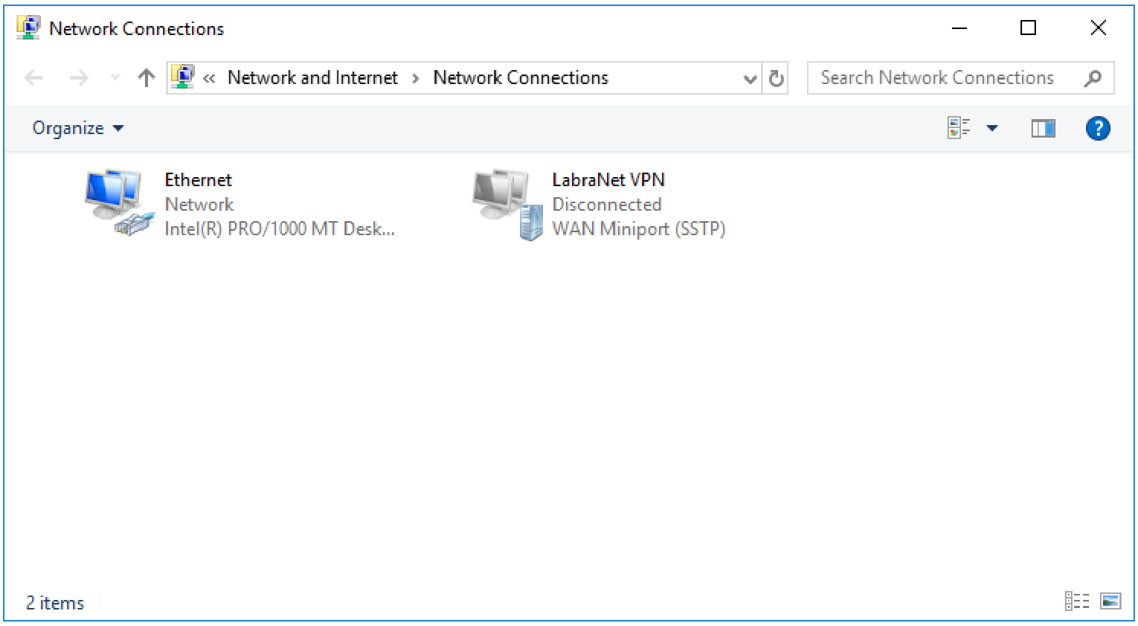
Click *OK*.

6 Windows 10 - Additional settings

To ensure functioning DNS, more configuration is recommended. Windows 10 uses *smart multihomed name resolution* to optimize name resolution. This feature causes DNS to return incorrect IP addresses for some public LabraNet services when automatic interface metric assigns the LabraNet VPN connection lower *or* equal priority compared to the connecting devices physical network adapter.

For end users, this shows up as LabraNet services (including helpdesk and gitlab) not responding when the VPN tunnel is up. It is possible to correct this either by bumping the VPN connection up in priority or lowering the physical adapters priority. This guide focuses on altering the priority of the VPN connection.

Open *Network and Sharing Center* and select *Change adapter settings.* This view shows all the network connections your device has.


Network Connections
« Network and Internet › Network Connections
Search Network Connections
Organize ▾

Ethernet
Network
Intel(R) PRO/1000 MT Desk...

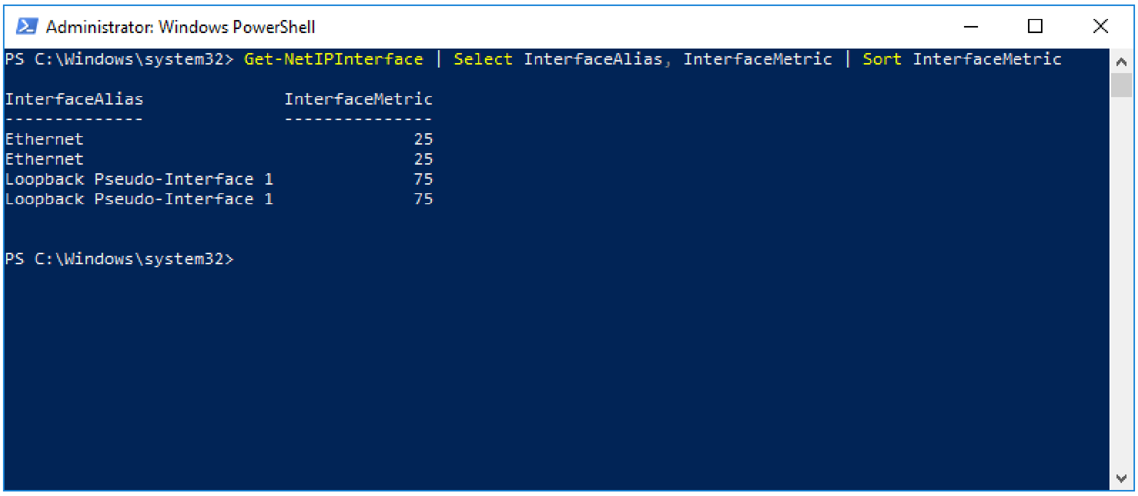
LabraNet VPN
Disconnected
WAN Miniport (SSTP)

Figure 18. Network adapter settings

Note that the name of the physical network connection is *Ethernet.* This may vary depending on the number and type of physical adapters, and installed software.

Now issue the following PowerShell command by opening *Windows PowerShell* and typing in:

Get-NetIPInterface | Select InterfaceAlias, InterfaceMetric | Sort InterfaceMetric



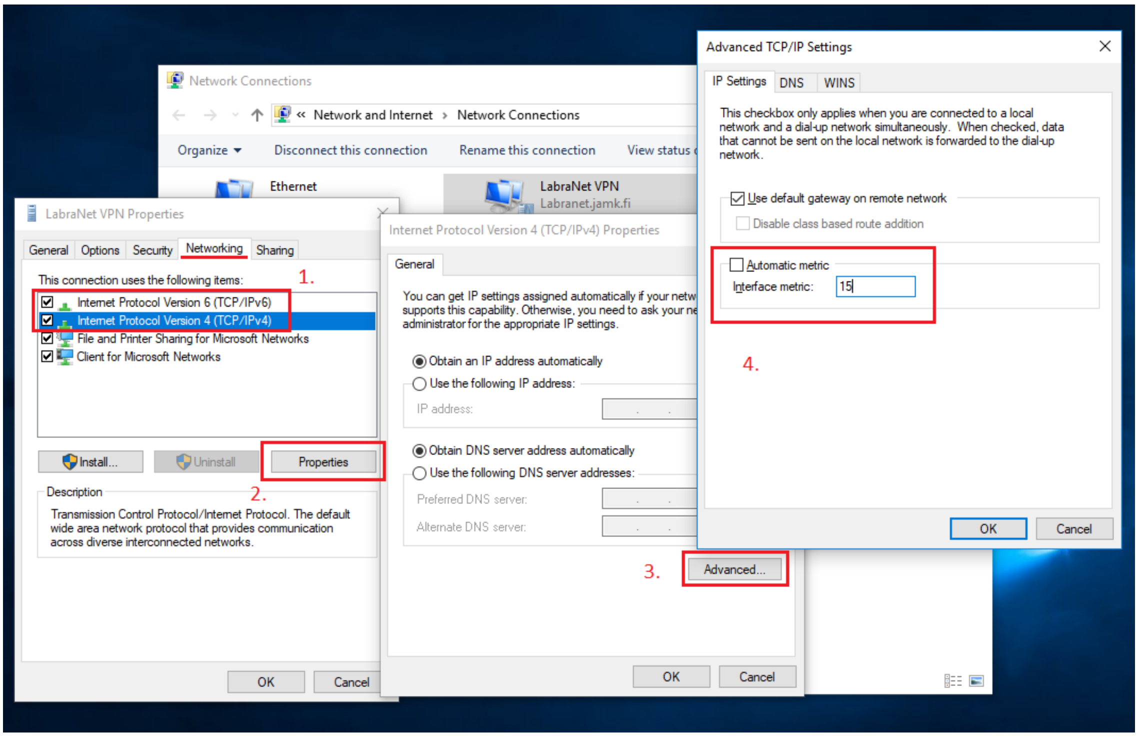
```
PS C:\Windows\system32> Get-NetIPInterface | Select InterfaceAlias, InterfaceMetric | Sort InterfaceMetric

InterfaceAlias             InterfaceMetric
--------------             ---------------
Ethernet                                25
Ethernet                                25
Loopback Pseudo-Interface 1             75
Loopback Pseudo-Interface 1             75


PS C:\Windows\system32>
```

Figure 19. List network interface metrics

Note that the *InterfaceMetric* value assigned to the connection *Ethernet* is 25 in this example. Please use the lowest number of your active connection as reference point.

Now select the newly created LabraNet VPN connection from *Network and Sharing Center* and select *Properties.* Choose the *Networking* tab and modify both the *Internet Protocol Version 6* and the *Internet Protocol Version 4* connection items (1).

Click open either one by selecting *Properties* (2). Then open the advanced settings by clicking *Advanced* (3). Clear the checkmark from *Automatic metric* and assign a value that is **less** than what the PowerShell command returned (4). This example sets the metric at 15 which is less than the 25 listed for the *Ethernet* connection.



This connection uses the following items:

- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Client for Microsoft Networks

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your netw supports this capability. Otherwise, you need to ask your ne administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.

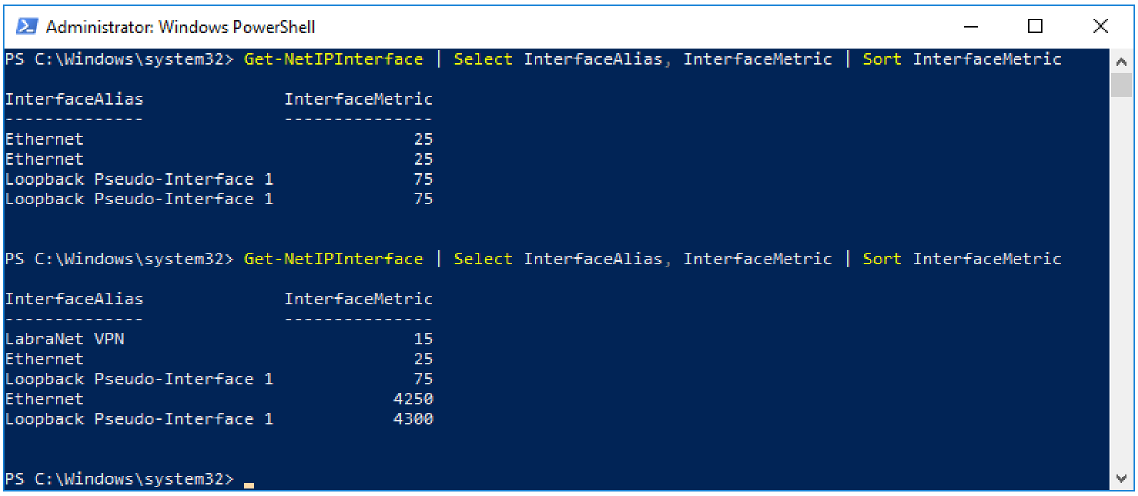
☑ Use default gateway on remote network
□ Disable class based route addition

□ Automatic metric
Interface metric: 15

Figure 20. Modify the metric value

Modify both the IPv4 and IPv6 settings the same way and click *OK* at each setting window to save the settings.

Now connect to LabraNet via the VPN connection and issue the previous PowerShell command again to check that your settings were saved correctly.



```
PS C:\Windows\system32> Get-NetIPInterface | Select InterfaceAlias, InterfaceMetric | Sort InterfaceMetric

InterfaceAlias             InterfaceMetric
--------------             ---------------
Ethernet                                25
Ethernet                                25
Loopback Pseudo-Interface 1             75
Loopback Pseudo-Interface 1             75


PS C:\Windows\system32> Get-NetIPInterface | Select InterfaceAlias, InterfaceMetric | Sort InterfaceMetric

InterfaceAlias             InterfaceMetric
--------------             ---------------
LabraNet VPN                            15
Ethernet                                25
Loopback Pseudo-Interface 1             75
Ethernet                              4250
Loopback Pseudo-Interface 1           4300


PS C:\Windows\system32> _
```

Figure 21. Check the values

LabraNet VPN should now be the first connection listed with the lowest *InterfaceMetric* value thus having the highest priority.

7 Mac OS X

These configurations have been tested up to version 10.13.4 (High Sierra).

7.1 SSTP

Using a CLI client for SSTP VPN is possible and you can install it by using Homebrew.

```
ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)" <
/dev/null 2> /dev/null
brew install sstp-client
```

After installing, create a file */etc/ppp/options* for the VPN connection parameters. This is easily accomplished as *root user* by using terminal and the following commands:

```
sudo su
printf 'usepeerdns\nrequire-mschap-v2\ndefaultroute\nrefuse-eap\nnoauth\nnoipdefault\nnoccp\n'
> /etc/ppp/options
```

The contents of the file should look like this:

```
usepeerdns
require-mschap-v2
defaultroute
refuse-eap
noauth
noipdefault
noccp
```

You should now be able to connect from the terminal window by using the command:

```
sudo /usr/local/sbin/sstpc --log-level 4 --log-stderr --user <Your LabraNet username> --password
<Your LabraNet password> sslvpn.labranet.jamk.fi
```

Optionally, you can create a shell script to do the connection. This is preferable if you use the VPN connection often. Contents of the shell script might be similar to this example:

```
#!/bin/bash
user=$1
if [[ -z "$user" ]]; then
   echo “Usage: ./vpn.sh userid"
   echo "Example: ./vpn.sh A1234"
   exit 1
fi

echo "Type in your LabraNet password and press [ENTER]:"
read -s pass

/usr/local/sbin/sstpc --log-level 4 --log-stderr --user $user --password $pass sslvpn.labranet.jamk.fi
```

7.2 L2TP

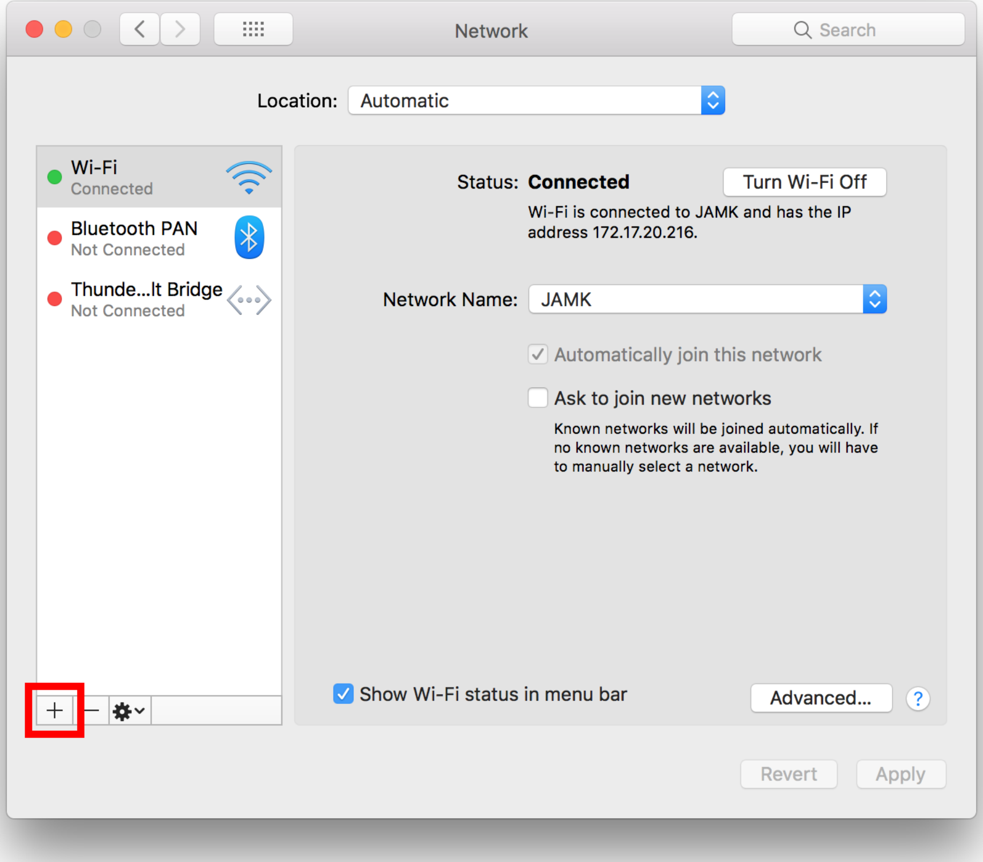
Deprecation of iSstp application leaves Mac users without a graphical tool to configure VPN settings. As command line and terminal usage might be problematic to some, LabraNet VPN server has been configured to also use Layer 2 Tunneling Protocol. L2TP has a native client in Mac OS and it is easy to configure. L2TP does not inherently provide confidentiality and therefore it is implemented with IPSec. The downsides to L2TP/IPSec are problems with Network Address Translation and the usage of a Pre-Shared Key for connection authentication. Generic options for the connection are:

Connection type: L2TP over IPSec
VPN server address: sslvpn.labranet.jamk.fi (should resolve to 195.148.26.226)
Shared Secret: LabraNetVPN

Firewall:
UDP Port 500 (IKE)
UDP Port 4500 (NAT-T)
IP protocol 50 (ESP)

User information:
Account Name: Your LabraNet username
Password: Your LabraNet password

Open *Network Preferences* from *System Preferences* to create the L2TP VPN. Select the + button under the available connections on the left side of the application window.



Location: Automatic

Status: **Connected**

Wi-Fi is connected to JAMK and has the IP address 172.17.20.216.

Network Name: JAMK

☑ Automatically join this network

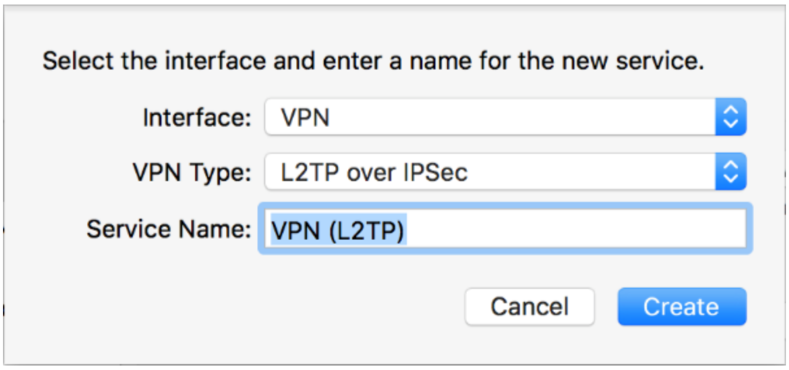
□ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

☑ Show Wi-Fi status in menu bar

Figure 22. Add a new connection

Fill in the connection type information as pictured below.



Select the interface and enter a name for the new service.

Interface: VPN

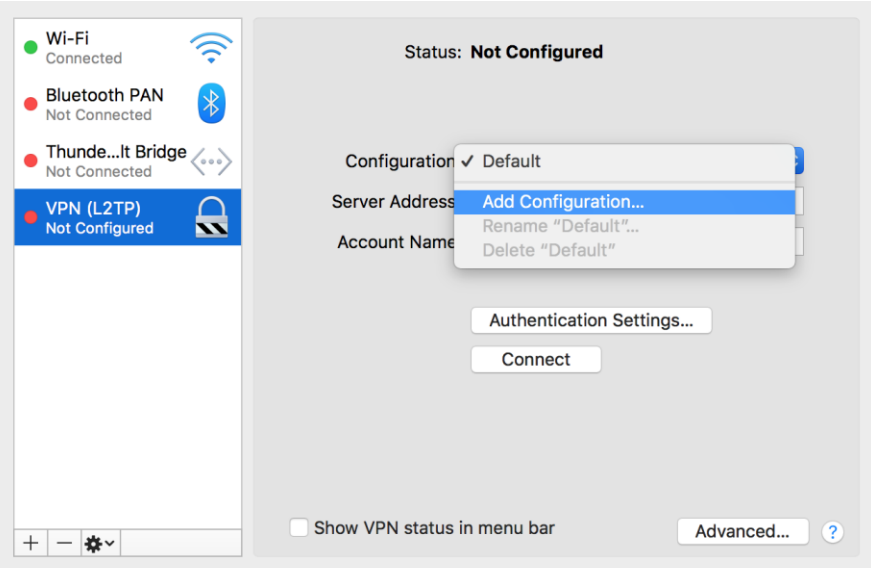
VPN Type: L2TP over IPSec

Service Name: VPN (L2TP)

Figure 23. Connection type

Click *Create*.

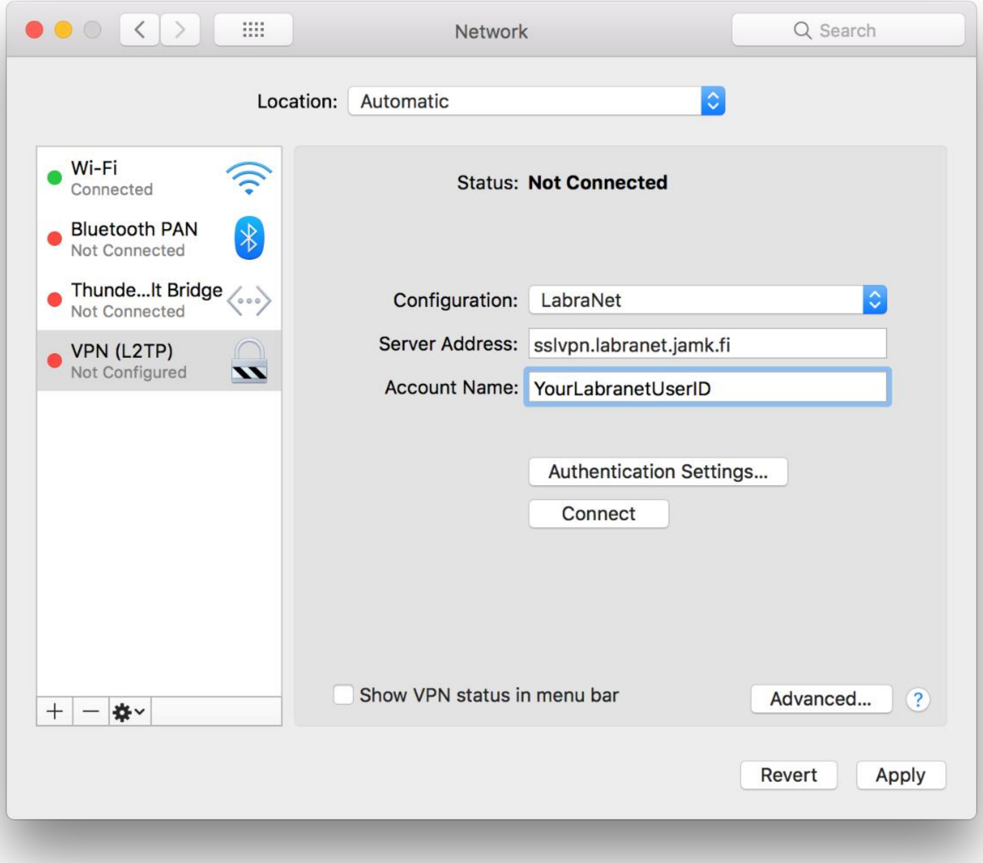
Select *Add Configuration* from the *Configuration* dropdown menu to add connection specific configurations.



Status: **Not Configured**

Figure 24. Add Configuration

Name the configuration *LabraNet* and click *Create* in the popup window. Next, configure the connection. *Server Address* is the name or IP address of LabraNet VPN server and Account Name is your personal Student ID.


Location: Automatic

Status: **Not Connected**

Configuration: LabraNet

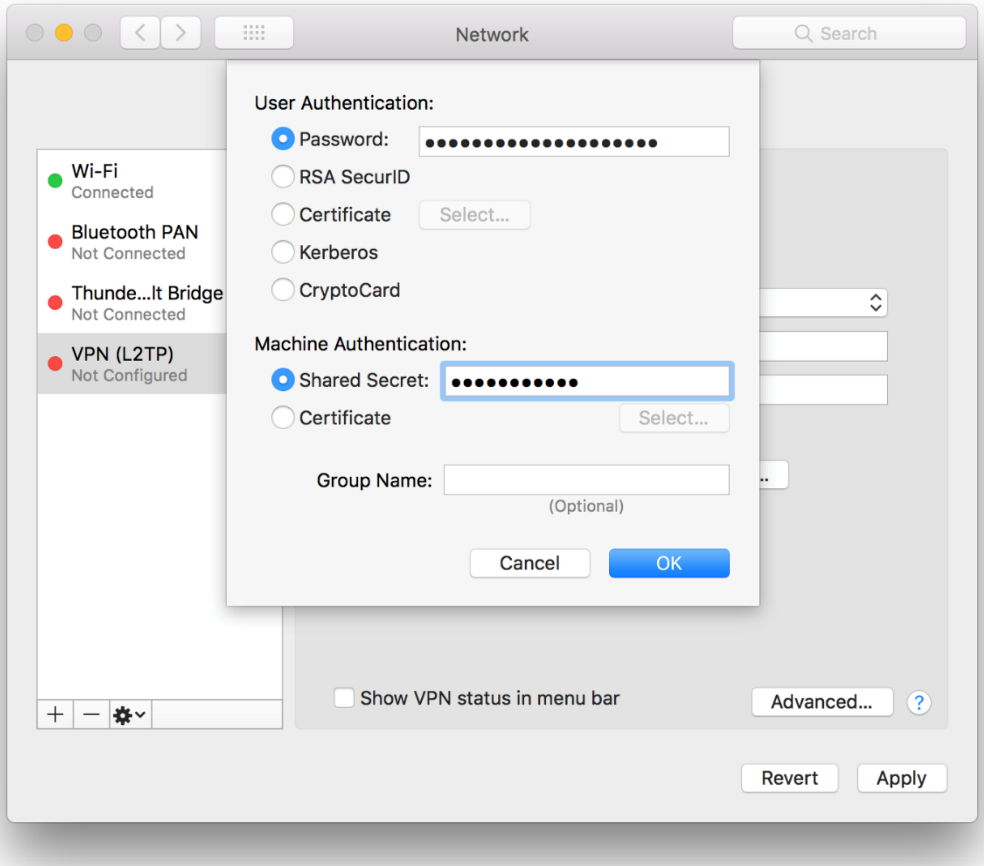
Server Address: sslvpn.labranet.jamk.fi

Account Name: YourLabranetUserID

□ Show VPN status in menu bar

Figure 25. Configure basic settings

Next, configure *Authentication Settings*. Select *Authentication Settings* menu and fill in your user password to the *Password* field and the *Shared Secret* to the *Shared Secred* field. Your password is your LabraNet password and the *Shared Secret* is “LabraNetVPN” without the quotation marks.



User Authentication:

● Password: ••••••••••••••••••••

○ RSA SecurID

○ Certificate

○ Kerberos

○ CryptoCard

Machine Authentication:

● Shared Secret: •••••••••••

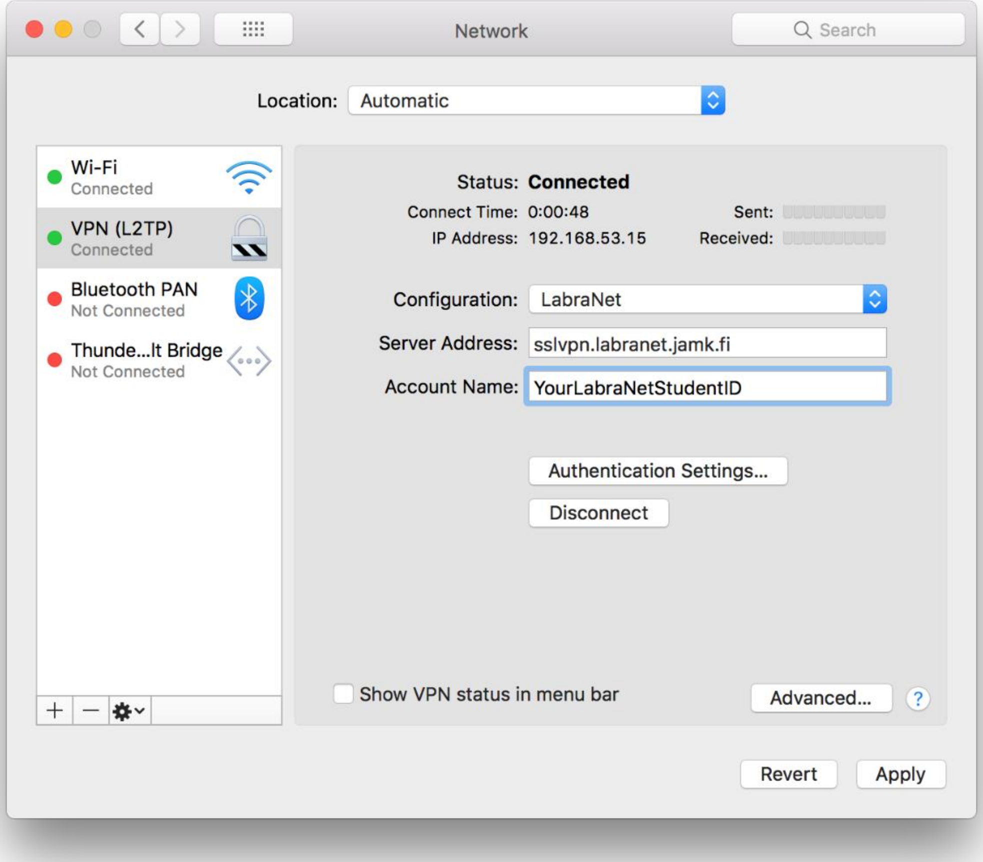
○ Certificate

Group Name: (Optional)

Figure 26. Authentication settings

Click *OK* to close the *Authentication Settings* window and Click *Apply* in the *Network Preferences* window. Your L2TP VPN connection is now ready to be used.

Click *Connect* from the *Network Preferences* window to complete the connection.



Status: Connected
Connect Time: 0:00:48
IP Address: 192.168.53.15
Sent:
Received:

Configuration: LabraNet
Server Address: sslvpn.labranet.jamk.fi
Account Name: YourLabraNetStudentID

Figure 27. Completed connection

You can disconnect from the VPN connection by clicking *Disconnect*.

8 Linux (Graphical)

These apply to Linux-distributions which use Network-Manager. In the examples we use Ubuntu 18.04 LTS. Other distributions may use a different style in the UI for Network-Manager, but the basic steps are the same.

The first step is to install sstp-client. This can be done by adding the personal packet archive of the author of network-manager sstp-client.

```
sudo add-apt-repository ppa:eivnaes/network-manager-sstp
sudo apt-get install network-manager-sstp network-manager-sstp-gnome sstp-client
```

Alternatively, you can find the packages here if you want to manually install them.

https://sourceforge.net/projects/sstp-client/files/

or

https://aur.archlinux.org/packages/sstp-client/
https://aur.archlinux.org/packages/networkmanager-sstp/

Open the Network settings and press the highlighted + button to set up the VPN connection.

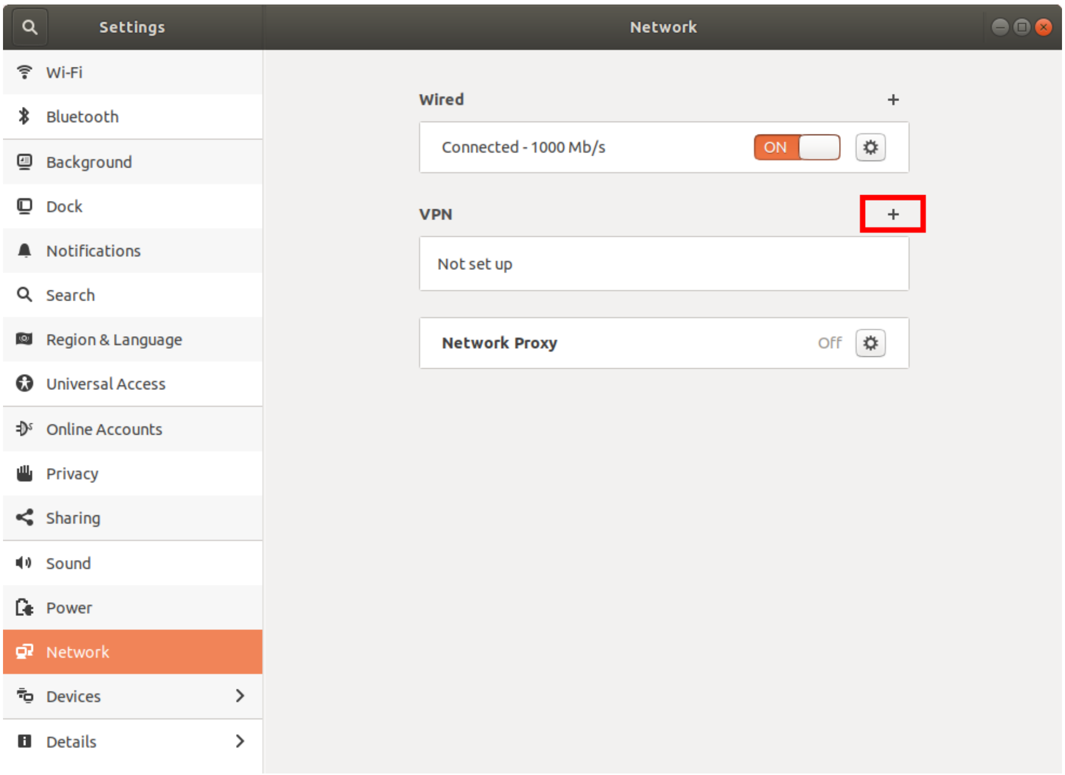
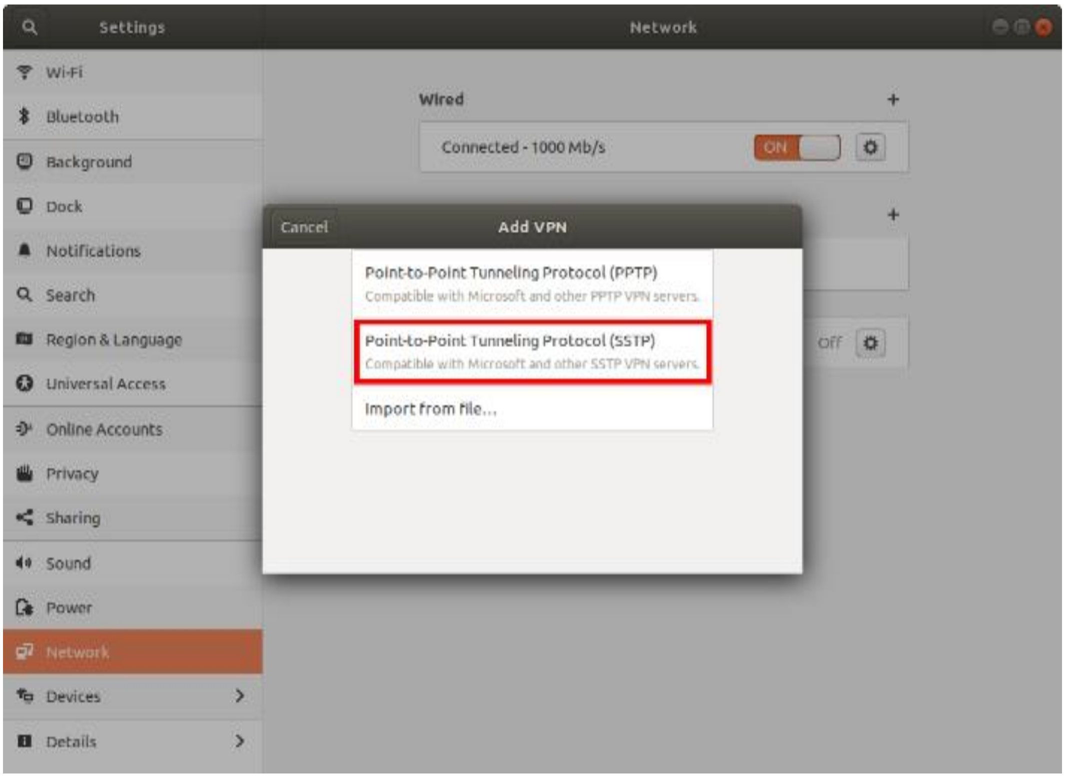


Figure 28. Network settings

Choose *Point-to-Point Tunneling Protocol (SSTP)*.



Add VPN

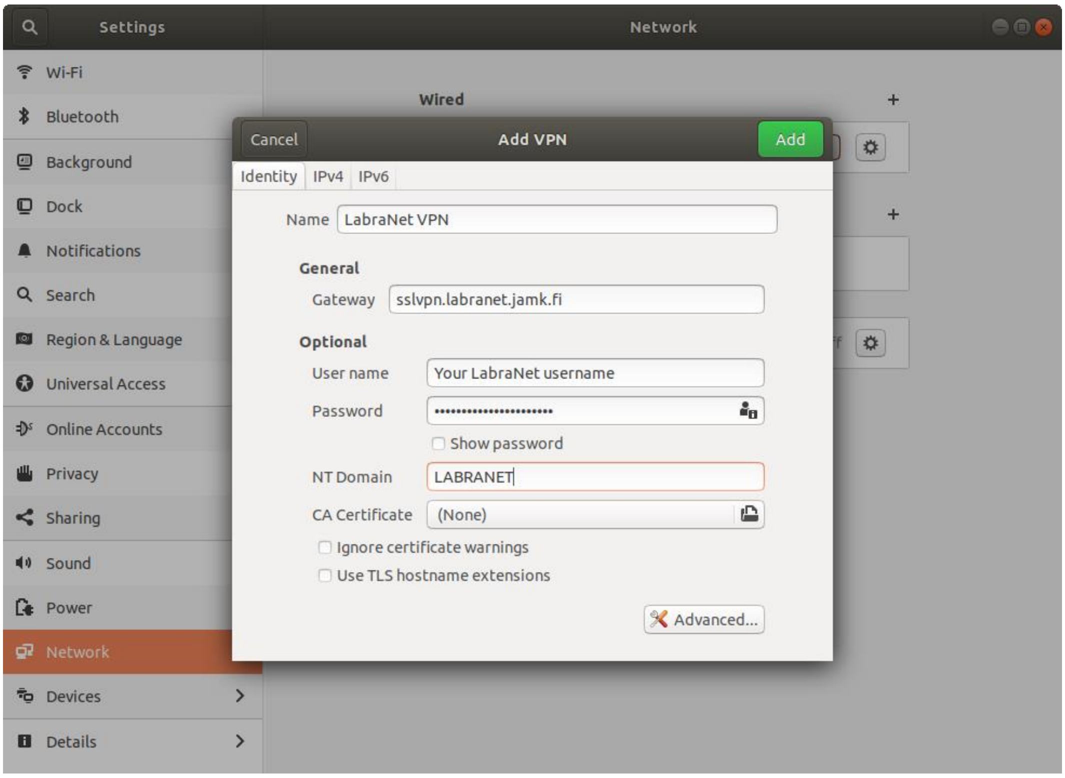
Point-to-Point Tunneling Protocol (PPTP)
Compatible with Microsoft and other PPTP VPN servers.

Point-to-Point Tunneling Protocol (SSTP)
Compatible with Microsoft and other SSTP VPN servers.

Import from file...

Figure 29. Connection type

On the next dialog, give the connection a name, fill in the gateway and your username and password.



Name: LabraNet VPN

General

Gateway: sslvpn.labranet.jamk.fi

Optional

User name: Your LabraNet username

Password: ••••••••••••••••••••••

□ Show password

NT Domain: LABRANET

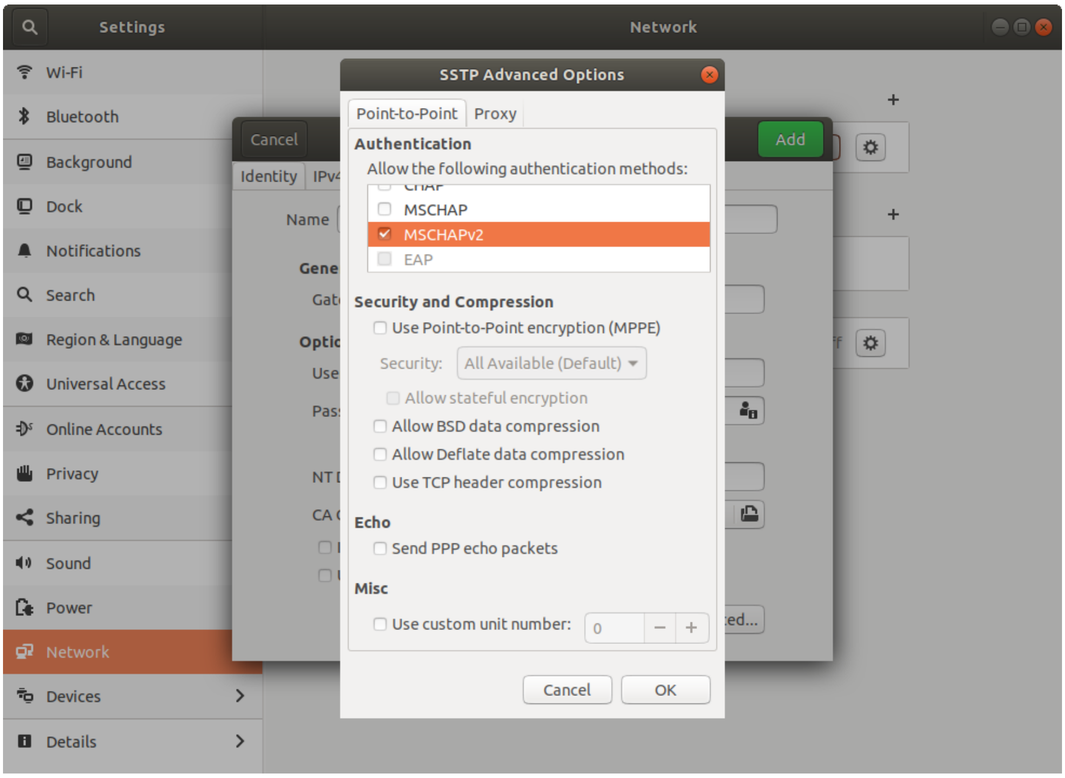
CA Certificate: (None)

□ Ignore certificate warnings

□ Use TLS hostname extensions

Figure 30. VPN Connection settings

Next click the *Advanced*-button. From the next dialog, select the following authentication method: *MS-CHAPv2*. You can leave other selections unchecked.



SSTP Advanced Options

Point-to-Point | Proxy

Authentication

Allow the following authentication methods:

□ CHAP
□ MSCHAP
☑ MSCHAPv2
□ EAP

Security and Compression

□ Use Point-to-Point encryption (MPPE)

Security: All Available (Default)

□ Allow stateful encryption
□ Allow BSD data compression
□ Allow Deflate data compression
□ Use TCP header compression

Echo

□ Send PPP echo packets

Misc

□ Use custom unit number: 0

Cancel OK

Figure 31. Advanced settings

Click *OK* and *Add*. You can now connect to LabraNet using this VPN connection from the tray applet.

9 Advanced routing

VPN tunnel can be used in full tunnel or split mode. With full tunneling, all traffic is routed through the VPN connection. In split mode, only traffic to resources in LabraNet networks are routed via the VPN connection.

This behaviour can be changed by enabling or disabling the use of gateway on the VPN connection.

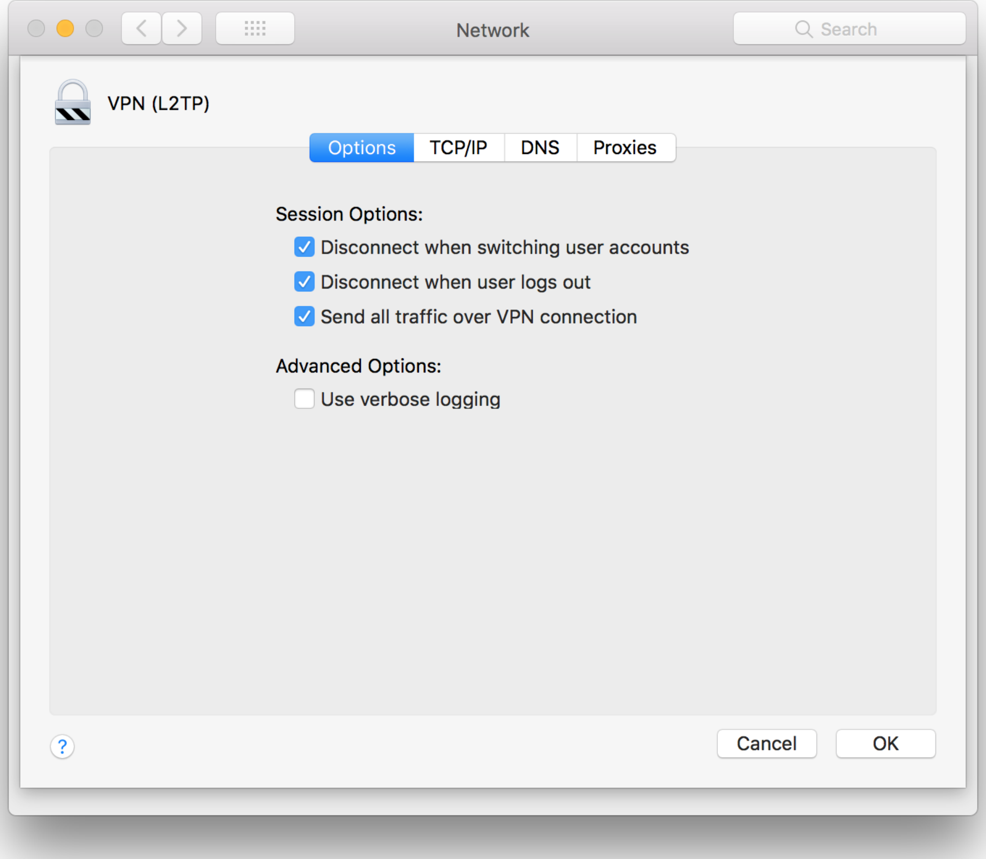
9.1 Windows

In Windows operating systems. the default mode is Full tunnel. To change the setting, go to VPN connection Properties and *Networking* tab. Select *Internet Protocol Version 4 (TCP/IPv4)* and click *Properties*. Click the *Advanced* button and on the next dialog, *Use default gateway on remote network*. When the setting is checked, Windows uses Full tunnel mode.

9.2 Mac OS X

The SSTP VPN tunnel works best in Full tunnel mode. This is achieved with the *defaultroute* parameter. Per documentation of sstp-client, changing this is not recommended.

L2TP in Mac OS uses Split tunnel by default. This can be changed from the *Advanced* menu in *Network Preferences* after selecting the VPN connection. Check the *Send all traffic over VPN connection* checkbox to use Full tunnel mode.



Session Options:

☑ Disconnect when switching user accounts

☑ Disconnect when user logs out

☑ Send all traffic over VPN connection

Advanced Options:

□ Use verbose logging

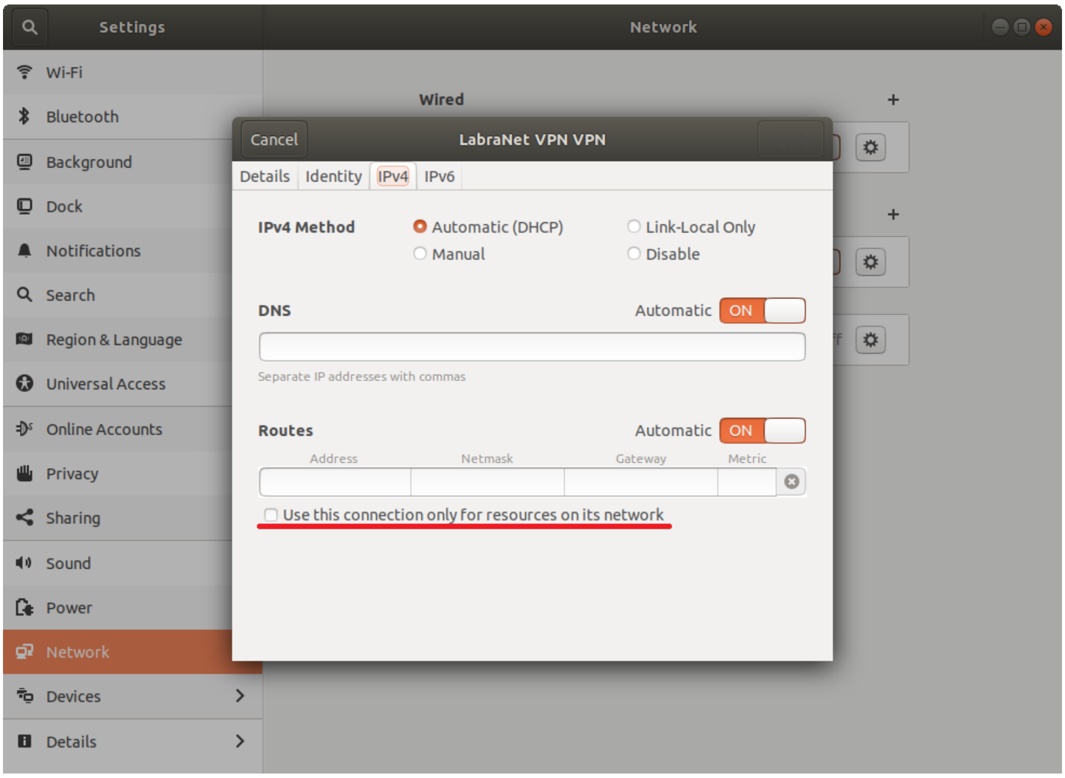
Figure 32. Full tunnel in Mac OS.

Click *OK* and *Apply*.

9.3 Linux (Graphical)

The VPN tunnel works best in Full tunnel mode. To change this, edit the *IPv4 Settings* of your VPN connection.

Check the *Use this connection only for resources on its network* checkbox. Per documentation of sstp-client, this is not recommended. When using split tunneling, ensure your distributions dhcp client supports *rfc3442-classless-static-routes option 121.* Otherwise routes to LabraNet services need to be added by hand.



IPv4 Method ● Automatic (DHCP) ○ Link-Local Only ○ Manual ○ Disable

DNS Automatic ON

Separate IP addresses with commas

Routes Automatic ON

□ Use this connection only for resources on its network

Figure 33. Advanced routing

10 Accessing Shares

After successfully connecting to VPN, you can now use shared files in a similar manner as from local LabraNet workstations. Here are guides for connecting to your home folder or any public share.

NOTE: In some cases, the VPN connection DNS servers will not be used immediately. In this case, wait for a few minutes and try again.

Your home folder can be found in the path
\\storage.labranet.jamk.fi\homes\userid

You can also use public shares, such as *\\ghost.labranet.jamk.fi\temp.*

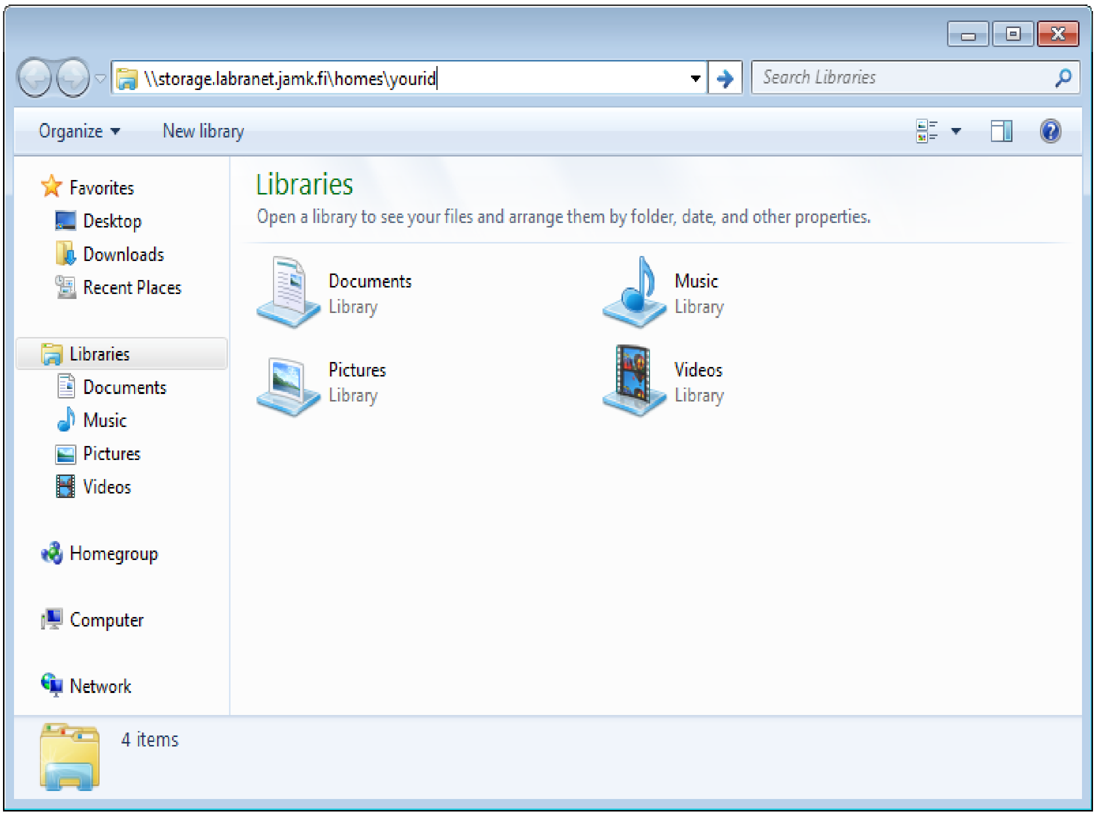
You need to authenticate to the shares separately with your LabraNet account information. Provide the username either in format *LABRANET\userid* or *userid@LABRANET*.

Replace the *network-path* with desired network path in the following examples.

More information on accessing your LabraNet shares can be found in
http://student.labranet.jamk.fi/remote-using-your-home-folder/

10.1 Windows

Open *File explorer*. Write the path to the address bar on top of the window. Windows should ask you for your LabraNet username and password.

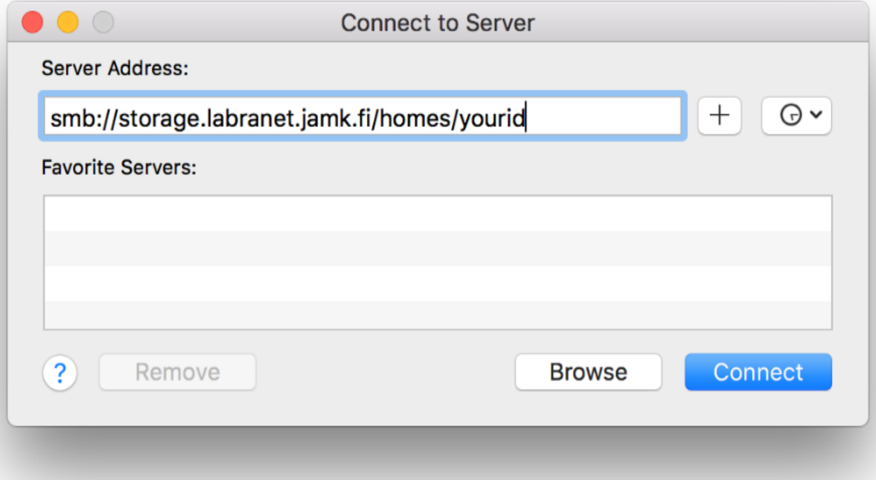


```
\\storage.labranet.jamk.fi\homes\yourid
```

Figure 34. Enter the network path

10.2 Mac OS X

Go to Finder and press Cmd+K. Enter the path to the *Server Address* –field as follows *smb://network-path:*

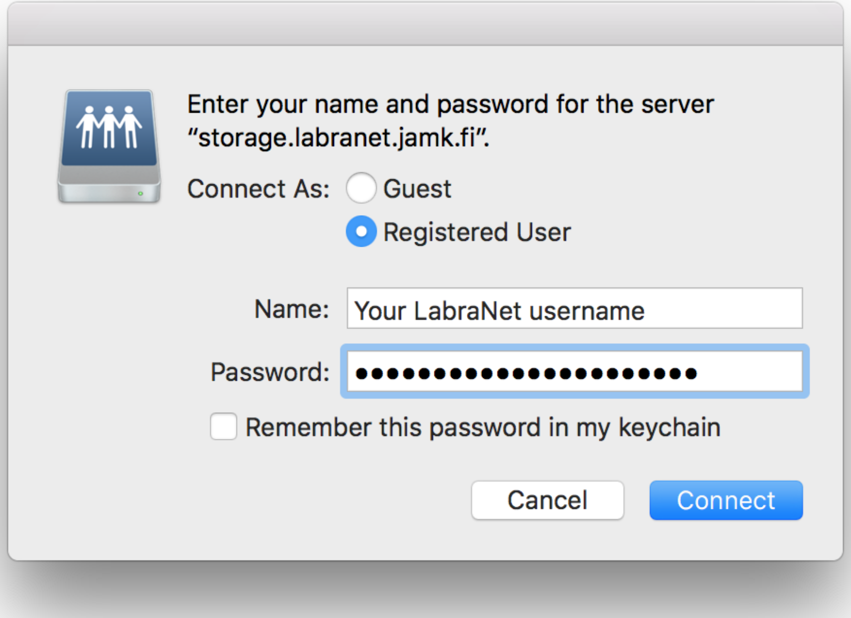


smb://storage.labranet.jamk.fi/homes/yourid

Figure 35. Connect to Server

Some versions of Mac OS X work better with cifs-protocol, path would then be *cifs://network-path*

Click *Connect*. You will be asked for your LabraNet credentials.



Enter your name and password for the server "storage.labranet.jamk.fi".

Connect As: ○ Guest
● Registered User

Name: Your LabraNet username

Password: ●●●●●●●●●●●●●●●●●●●●●●●

□ Remember this password in my keychain

Figure 36. Credentials for user

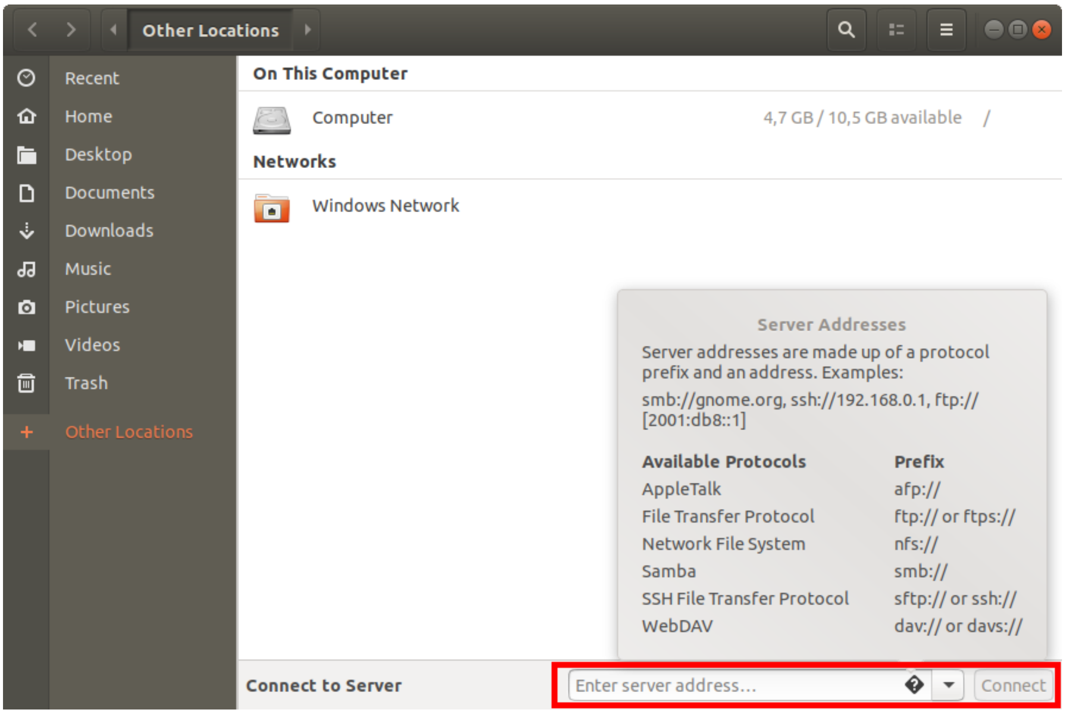
10.3 Linux (Graphical)

NOTE for older Linux distros: Due to being broken, SMBv1 has been disabled. This means you need to connect to shares with a newer version of the SMB protocol. This can be achieved by adding the following options to the *[global]* section of *smb.conf* in */etc/samba/smb.conf*.

client max protocol = SMB3

client min protocol = SMB2

Now you can connect to LabraNet network shares using your LabraNet account information.



Server Addresses

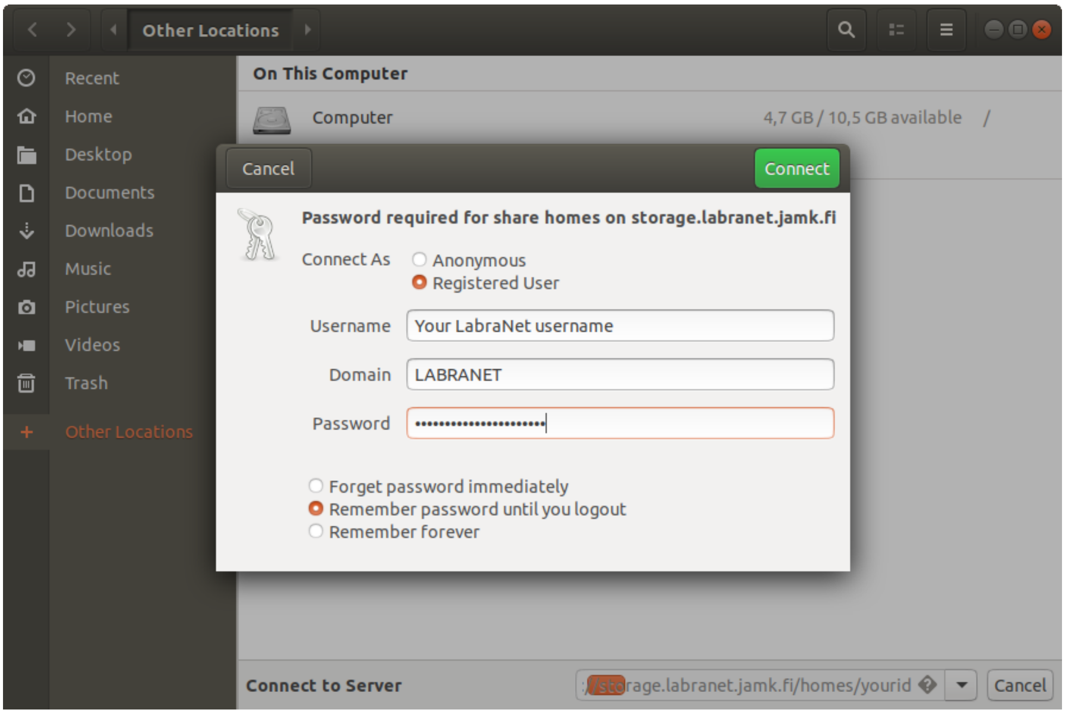
Server addresses are made up of a protocol prefix and an address. Examples:

smb://gnome.org, ssh://192.168.0.1, ftp://[2001:db8::1]

Available Protocols	Prefix
AppleTalk	afp://
File Transfer Protocol	ftp:// or ftps://
Network File System	nfs://
Samba	smb://
SSH File Transfer Protocol	sftp:// or ssh://
WebDAV	dav:// or davs://

Figure 37. Connecting to server shares

You will then be asked to fill in your LabraNet account information.



Password required for share homes on storage.labranet.jamk.fi

Connect As ○ Anonymous ● Registered User

Username: Your LabraNet username

Domain: LABRANET

Password: ••••••••••••••••••••••

○ Forget password immediately
● Remember password until you logout
○ Remember forever

:/storage.labranet.jamk.fi/homes/yourid

Figure 38. Creating the connection

10.4 Linux (Command line)

Create a mountpoint and ensure *mount.cifs, cifs-utils* or equivalent package is installed depending on the distribution you’re using.

Mount temporarily with:

sudo mount.cifs -o domain=LABRANET,username=<yourid>,vers=2.0 //network-path /mountpoint

Adding permanent mount to */etc/fstab*:

//network-path /mountpoint cifs domain=LABRANET,user=userid 0 0

You can also use *.smbcredentials* or *cifscreds* to store your credentials in a secure file or system keyring. Check your distributions documentation for more information.